الأمم المتحدة S/2023/412

مجلس الأمن

Distr.: General
7 June 2023
Arabic
Original: English

رسالة مؤرخة 6 حزيران/يونيه 2023 موجهة إلى رئيسة مجلس الأمن من الممثل الدائم لألبانيا لدى الأمم المتحدة

على إثر اجتماع صيغة آريا الذي نظّمته الولايات المتحدة الأمريكية وألبانيا وشارك في رعايته كل من إستونيا وإكوادور بشأن موضوع "مسؤولية الدول عن الهجمات السيبرانية على البنى التحتية الحيوية واستجابة الدول لمثل هذه الهجمات"، والذي عُقد في 25 أيار/مايو 2023، يسرّني أن أحيل طيّه مجموعة تضمّ جميع العروض التي قدّمها المشاركون في حلقة النقاش والبيانات التي أدلت بها الدول الأعضاء المشاركة في الاجتماع، باللغات الأصلية التي تم التكلّم بها (انظر المرفق).

وقد رُتّبت عناصر المجموعة وفقاً لترتيب قائمة المتكلمين، وبما يشمل البيانات التي أُدلي بها في صيغة مختصرة أو التي لم يُدل بها في الاجتماع لضيق الوقت.

وأرجو ممتناً تعميم هذه الرسالة ومرفقها باعتبارهما وثيقة من وثائق مجلس الأمن.

(توقيع) فريد **خوجا**
الممثل الدائم لألبانيا لدى الأمم المتحدة

140623 140623 23-10871 (A)

مرفق الرسـالة المؤرخة 6 حزيران/يونيه 2023 الموجهة إلى رئيسـة مجلس الأمن من الممثل الدائم لألبانيا لدى الأمم المتحدة

[الأصل: بالإسبانية والإنكليزية والروسية والصينية والعربية والفرنسية]

UNITED NATIONS SECURITY COUNCIL ARRIA-FORMULA MEETING ON

THE RESPONSIBILITY AND RESPONSIVENESS OF STATES TO CYBERATTACKS ON CRITICAL INFRASTRUCTURE

PRESENTATIONS AND STATEMENTS
25 MAY 2023

List of speakers

Panelists

Under-Secretary General and High Representative, UNODA - Ms. Izumi Nakamitsu

Distinguished organizers and co-sponsors,

Members of the Security Council,

Distinguished delegates,

Dear participants,

Ladies and gentlemen,

I am honoured to have been invited to brief this Arria-formula meeting today.

I wish to express my appreciation to the Permanent Missions of Albania and the United States for organizing this meeting as well as to the Permanent Missions of Ecuador and Estonia for serving as co-sponsors.

I last briefed the Security Council on matters related to the peace and security of cyberspace in December of 2021 also in the format of an Arria-Formula.

At that meeting, I emphasized the importance of the Security Council's engagement on matters related to malicious activity in this domain given the very clear international peace and security implications.

In this regard, I am pleased to see that the Council remains seized of the very serious and critical issue of potential conflict and hostilities in cyberspace.

More than 15 months since the last Arria-Formula meeting, we convene today to consider malicious activity targeting critical infrastructure and questions related to accountability, responsibility and response.

The current international security landscape reminds us of the absolute urgency of finding answers to these questions.

The number of publicly reported State-sponsored cyber incidents increased fifteen-fold between 2005 and 2020. Since then, this steep uptick has only continued.

And the threats posed to civilians and human life are amongst the most worrisome.

We see a proliferation of malicious cyber incidents impacting infrastructure providing services to the public and critical to the functioning of society.

Malicious cyber activity affecting public access to electricity, the Internet, healthcare systems, and transportation services have been well-documented, including several in the last year.

There is broad acknowledgement that a number of States are developing cyber capabilities for military purposes and that the use of information and communications technologies in future conflicts between States is becoming more likely.

Non-state actors, including terrorists and violent extremist groups, are also active in cyberspace, and utilize it to plan and prepare cyberattacks against critical sectors.

This assessment brings into sharp focus the importance of action by the Security Council in ensuring a secure and peaceful cyberspace—beginning with substantive exchanges such as this one today.

Dear participants,

Cyber activity that intentionally damages critical infrastructure or otherwise impairs the use and operation of infrastructure that provides services to the public poses an elevated risk of harm to the population and can have cascading domestic, regional and global effects, possibly leading to conflict.

While these risks and dangers are considerable, States are not without tools to mitigate them.

As the Secretary-General has often said, cyberspace is not a lawless space.

Significant progress in the General Assembly over the last two decades has yielded key gains.

First and foremost, States have agreed that international law, in particular the United Nations Charter, is applicable and essential to maintaining peace and stability in the cyber domain and for promoting an open, secure, stable, accessible and peaceful cyberspace.

Secondly, States have agreed to be guided in their use of information and communications technology by a set of concrete norms of responsible State behaviour.

Included in these norms are three measures that specifically address threats to critical infrastructure, including a commitment not to conduct or knowingly support malicious activity that intentionally damages this type of infrastructure. States also commit to respond to related requests for assistance by another State whose critical infrastructure is subject to malicious acts.

The norms also seek to ensure cooperation and information exchange, prevent escalation including as a result of misattribution of responsibility for an incident, and uphold human rights.

This normative framework is underpinned by a commitment to capacity-building to support States in their implementation of the agreed norms. States also continue to explore confidence-building measures to further mitigate tension.

The ongoing Open-ended Working Group on security of and in the use of information and communications technologies, under the able chairing of Ambassador Burhan Gafoor of Singapore, has a critical role to play in taking forward and expanding on this progress.

A primary task of States is to consider how to implement the norms of responsible State behaviour—essentially filling in the details so that they can become operational.

As we speak now, the Open-ended Working Group is convening for informal intersessional meetings.

The Working Group continues to unpack existing and potential threats to the peace and security of cyberspace and evaluate the normative framework against that background to ensure it is fit-for-purpose.

For example, applications of emerging technologies such as artificial intelligence and quantum technologies are posing new risks by enabling attackers to easily generate malicious codes, identify system-level vulnerabilities, and break encryption methods.

The Working Group is also a platform to exchange on how international law, including the Charter, applies to cyberspace.

Generating common understandings on the applicability of international law, in particular to protect civilians from malicious cyber activity, is a difficult but necessary task.

Dedicated discussions on applicability of international law would allow States to consider highly relevant principles such as State sovereignty, State responsibility and due diligence. These principles strike at the heart of several of the guiding questions provided in the concept note for this meeting today.

Distinguished delegates,

Dear participants,

The urgency of efforts to protect the peace and security of cyberspace, including to safeguard critical infrastructure from malicious activity, is only growing.

Firstly, States must unequivocally acknowledge the particular vulnerability of infrastructure essential for public services and to functioning of society and commit to protect it accordingly. Such infrastructure must be “off-limits” to any malicious activity.

Secondly, the principle of accountability is essential to tackling concerns of trust and, equally important, mistrust in cyberspace.

To this end, States are encouraged to identify ways of facilitating resolution of cyber incidents involving other States and in enhancing compliance with relevant agreed norms and principles of responsible State behaviour, with a view to deterring and preventing future such activity.

In the framework of the Open-ended Working Group, States have decided to establish a global points of contact directory, which could facilitate coordination and communication in the event of an ICT incident, thus reducing tensions and misunderstandings that may arise.

I am hopeful States will reach agreement on modalities for the directory in the short-term so that it can quickly become operational.

Finally, I wish to briefly reference the important contributions of nongovernmental stakeholders, including civil society, the private sector and academia, to efforts to secure cyberspace.

In addition to their technical expertise, the private sector's ownership and management of much of the information and communications technologies infrastructure, including critical infrastructure, requires its meaningful participation in relevant policy discussions and its cooperation in implementation.

Distinguished delegates,

Dear participants,

The cyber threat landscape continues to evolve and so must our collective responses.

The United Nations remains your steadfast partner in this endeavour.

I look forward to listening to the views of Member States and I thank you very much for your attention.

International Policy Director, Stanford Cyber Policy Center - Ms. Marietje Schaake

Your excellencies, ladies and gentlemen, thank you for inviting me to be a part of this Arria-formula meeting. In particular the Permanent Missions that tabled this important topic. I hope today's exchange will lead to an improvement of prevention of and accountability after cyberattacks, and a stronger leadership role for the UN in finding agreement between states in these polarized times. The rules based international order, peace, security and human rights are also under threat in cyberspace.

Two days ago, Microsoft reported it found Chinese malware in US Critical Infrastructure. In coordination with their 'five eyes' partners, the NSA then published an advisory report. Thus far the verdict seems that the aim was espionage, but concerns were voiced that access gained to networks could be weaponized in the future. The Chinese government says the claim lacks evidence.

This latest incident underlines some of the key issues I would like to address today, about the Roles of Stakeholders, the Rules we have and need, and the Reactions to cyberattacks:

-Firstly, about the roles of stakeholders. Companies have tremendous power in owning infrastructure, performing risk and threat assessments, and providing cybersecurity services, they decide whether to communicate, or not, to coordinate with state entities, or not. It puts them in a position of governance, access to information and agency that long rested exclusively in the hands of states. The privatization of governance is a game changer currently not reflected in the requirements visavis companies. There is a need for more clarity on the responsibility and liability on the part of those that build systems and software. Attackers after all, whether state of non-state, always exploit vulnerabilities in software for each successful penetration. As the previous speaker mentioned, AI, quantum and other emerging technologies will also bring new cybersecurity risks and accelerate known ones.

-Secondly, the rules and definitions we currently have are out of sync with the changed realities due to technological disruption. The physical and digital are merging, yet definitions of critical infrastructure tend to focus predominantly on the physical.

Other lines, such as those between war and peace time, are not as clear when we look at cyber attacks, and neither are those between state and non-state actors.

There continues to be a lack of clarity about how international law as it exists currently applies in the context of cyber-attacks, the same goes for the UN Charter. These laws are stonger than norms and already agreed. Even if intrusions are brazen and attackers bold, it is often unclear whether and how

international law has been breached. This lack of clarity perpetuates a lack of accountability and plays into the hands of attackers.

-Thirdly, reactions to attacks are often mute. Attribution currently seems easier for companies than for governments, while governments hold the policy instruments to attach consequences, such as sanctions.

My recommendations today focus on addressing the preconditions for reducing cyberattacks on critical infrastructure through more clarity on roles, rules, and reactions:

1) Clarify the chains of agency and responsibility between private and public actors, focus not only on responsible state behavior but also on responsible corporate behavior. Think critically whether the problem is a really the misuse of a technology, or the use exactly as intended, for example in the case of spyware.
2) The UN Security Council should facilitate a mapping in terms of who owns critical infrastructure, who scans it for risk as well as attempts to attack. Since the developers of critical infrastructure, particularly when the infrastructure is digital, are companies, the ones scanning for risk and defending data, software and infrastructure are companies, the lines of liability and responsibility needs to be clarified.
3) Recognize the merging of the physical and the digital, review spell out definitions of what qualifies as critical infrastructure. There is typically a precedent for physical infrastructure, but what about data infrastructure? Knowledge and information infrastructure?
4) Offer formal guidelines on how international law and the UN Charter apply in the context of digitization broadly and cyberattacks. While there is no discussion about whether international law applies in digital contexts, the lack of clarity in terms of how, leads to confusion and duplications through the establishment of norms. Ultimately there is an unnecessary accountability gap.
5) Close the accountability gap by developing an international attribution mechanism and even arbitration court to hold perpetrators to account with processes that are independent, and that facilitate the use of evidence gathered by victims, states and companies.

Thank you,

Cybersecurity Researcher in the Security and Technology Programme, UNIDIR – Ms. Moliehi Makumane

Chair

Heads of Mission and members of the diplomatic corps.

Ladies and Gentlemen

At the outset, I would like to thank the organisers and co-sponsors for the invitation to brief this meeting on responsibility and responsiveness of States to cyberattacks on critical infrastructure. I would like to concur with the assessments and recommendations of the USG, Ms Nikamitsu and Ms Schaake.

To add to these assessments, as the concept note states - failure to address potentially escalatory cyber activity emanating from a state's territory can also be destabilizing. – I present three factors that could cause escalation

- Firstly, the Cascading effects of malicious cyber-attacks against CI – we have learned from the health sector, that disruption of vaccine development had an impact on the public purse. The recovery costs of the attacks combined with new investments in cyber security have diverted funding away from research at a moment when significant investment in research was most needed

- Secondly, the Spill Over effects into other countries – a malicious attack on CI in one country can easily as we have seen affect another country. In the energy and water sector transnational pipelines are dispersed nationally, regionally and internationally

- And last, International ICT Security challenges take place within existing geo-political environment and in most instances reinforce existing dynamics - Most countries continue to struggle with the most basic aspects of critical infrastructure protection. In developing countries, the impact can be significant, including in terms of the ability to fully recover from a serious ICT incident

And now Chair, I turn to Responsiveness

The word "respond" appears in the UNGGE report 15 times demonstrating the weight and expectation that the experts and the GA in endorsing that report place on it. The majority of those references are in

Norm 13 (h) States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty.

The GGE report provided additional guidance in response to calls for clarity and included

1. Precondition for request and incident – this norm refers to those acts that have the potential to threaten international peace and security and complement existing mechanisms for day-to-day ICT incident management and resolution
2. Layer of responsibility:
    - Upon receiving a request for assistance, States should offer any assistance they have the capacity and resources to provide, and that is reasonably available and practicable in the circumstances.
    - A State receiving a request for assistance needs to determine, in as transparent and timely a fashion as possible and respecting the urgency and sensitivity of the request, whether it has the capabilities, capacity and resources to provide the assistance requested. States from which the assistance is requested are not expected to ensure a particular result or outcome
    - Where the malicious activity is emanating from a particular State's territory, its offer to provide the requested assistance and the undertaking of such assistance may help minimize damage, avoid misperceptions, reduce the risk of escalation and help restore trust
3. Options for affected State: A State may choose to seek assistance bilaterally, or through regional or international arrangements. States may also seek the services of the private sector to assist in responding to requests for assistance.

The guidance has certain assumptions, which are in turn recommendations for operationalisation of this norm

- The existence of national policies, legislation, structures and mechanisms that facilitate cooperation across borders
- States have positions (e.g., regarding incident notification, information-sharing and incident response and recovery
- Classification and Designation of CI – which is a national competence -
- Information sharing between States and private sector (CI owners and operators)
- The allocation of adequate resources – predictable and sustainable funding arrangements for CI-related projects in developing countries and workforce

Chair and distinguished delegates, as the USG said, States are not without tools. For two decades, the framework for responsible state behaviour has encouraged States to

- Survey their capacities – policy and regulation, structure and processes, partnerships and networks, people and skills and technology. We can only improve what we can measure
- Encouraged States to be transparent about their Critical infrastructure, in line with national polices and global commitments – by sharing sectors, services.
- And the UNIDIR Cyber Policy Portal which hosts States strategies, relevant agencies and policies and this information is updated regularly

I am convinced the UNSC has a role in encouraging States to survey their capabilities and be transparent about their policies, strategies and designated critical infrastructure. capacity building is very important. Notes the relationship between recipients, providers and implementers of capacity building, context, and national and regional dynamics. On this norm alone, several targeted capacity building projects can be initiated. capacity building is never done and is needed for all States and specifically on the topic of today – competence for what to do when an incident occurs is already too late – so I think, capacity building should be for states readiness – pre -incident, mid -incident and post incident. The Council can contribute by encouraging as has consensus report – states in a position to do, provide capacity building in line with agreed principles of capacity building

Chair, the strength of the Framework for responsible state behaviour lies in the fact that with every iteration of a GGE or a Working Group, States can incorporate lessons learned including from malicious incidents, making the norms guidance relevant and adaptable, giving impetus to CBMs, increasing commitment to capacity building and engaging in critical conversations about international law.

I reiterate my previous statement that malicious ICT incidents take place in existing geo-political environment – a look at the Council's agenda gives a glimpse – as you may be aware – malicious ICT incidents could amplify existing situations of instability and erode trust – and as a cross cutting issue that threatens peace (not just the absence of war- freedom to enjoy fundamental human rights) – must be a regular item on the agenda with regular briefings – Council to remain of new ways in which incidents could cause escalation that threatens international peace

Thank you

Co-organizers

Albania

Dear Colleagues,

I would like to thank USG Nakamitsu, Ms. Marietje Schaake and Ms. Moliehi Makumane for their important insights and thoughtful suggestions.

Despite the passing of time, despite the challenges and developments, the values and principles agreed upon in the UN Charter 78 years ago remain just as valid today. Upholding them in the ever-growing digital life is of the utmost importance for the present and the future.

We live in an evolving world, one that is changing every day. Fast developing technology and uninterrupted innovation are impacting every aspect of our lives, defining the future. But it is up to us to determine the path it takes so that the disruptive force of technology serves individual empowerment, and strengthens knowledge, progress and equality.

In the course of the last decade, we have gradually built a growing digital society in Albania. Nowadays, more than 1200 core government services are offered online. Our routine public administration is becoming increasingly paperless. These trends will only continue to grow. This requires a free, open, stable, and secure cyberspace.

While we enjoy the benefits, rapid technological progress also carries risks and challenges. As we have witnessed increasingly in the course of the last years, malicious actors, state and non-state actors, can use - or better misuse - cyberspace to wreak havoc. Imagine what would happen if during winter months, a country's power grid was disrupted, if water distribution was stopped, if healthcare facilities were prevented from working, or if the transportation network is brought to chaos. Such acts can undermine the security, economic development, and stability of any country and the humanitarian effects could be devastating.

Colleagues,

We are deeply concerned by an alarming increase in cyberattacks targeting States and their critical infrastructures. Only this year, more than forty cyberattacks have affected 19 countries.

We have experienced first-hand the destructive power of sophisticated attacks, aimed at destroying critical infrastructure, the permanent wiping of critical data, the destruction of the entire system, leaving behind a scorched earth, with a view to destabilize and create chaos and insecurity. It happened in Albania in July 2022. Critical services and the core of our democracy were put in danger.

Months of thorough investigation have revealed unquestionable evidence that this cyberattack was orchestrated and sponsored by Iran through the engagement of several non-state actors who carried out this assault. It represents a flagrant violation of the norms of responsible state behavior in cyberspace, an attack against a sovereign country. The damage was contained, and the attempt failed to reach its aims, but it was a testimony of the brutality of the malicious cyber activity, especially through the combined involvement of State and non-State actors. Such acts constitute a threat to international peace and security and must be treated as such.

I take this opportunity to thank our partners (the US, the UK and Israel) who have and are working hand in hand with us to build resilience. Together we have succeeded in thwarting successive attacks, protecting our critical infrastructure and our people. Last month, the National Authority for Electronic Certification and Cyber Security in Albania signed a Memorandum of Understanding with the Cyber Security Council of the United Arab Emirates, boosting cooperation in the field of Cyber Security between the two countries.

But Iran is not alone in this. It is common knowledge that Russia's actions have caused communications failures, including against critical infrastructure, not only in Ukraine, but also in other parts of Europe, by deliberately attacking the Viasat satellite on 24 February 2022, just one hour before the start of the unprovoked and unjustified war against Ukraine.

Countries in the Western Balkans are systematically targeted by campaigns of interference and manipulation of information, to trigger political instability and undermine their Euro-Atlantic aspirations.

DPRK has become a notorious example of repeated malicious activities and cyberattacks to generate illegal revenue, which is used to finance its weapons of mass destruction and proliferation policies, in violation of international law and resolutions of the Security Council.

Colleagues,

All Member States are bound to respect the Charter, including respect for human rights and fundamental freedoms, and should promote a global, open, stable, and secure cyberspace. We all have a role to play and it starts by establishing and respecting commonly agreed rules.

This is why Albania supports the establishment of the Program of Action (PoA), initiated by France and Egypt, to provide a framework for international cooperation and dialogue on cybersecurity, the development and implementation of existing norms and principles, and capacity building. We remain committed also to further advancing the framework already developed by the General Assembly for responsible state behavior in ICTs in the context of international security.

I would like to also emphasize that the Security Council must, with a view to discharging its duties under the Charter, take a leading role in promoting norms of responsible State behavior and underscoring the applicability of international law to Member States use of ICTs. By identifying and condemning counter-normative or unlawful State conduct and encouraging positive actions to improve

the security and stability of cyberspace, the Security Council can reduce the risk of conflict arising from malicious actions or omissions.

Colleagues,

We have learned throughout decades that we can achieve more when we come together, through dialogue and cooperation, to benefit from new opportunities for progress and deal with challenges on the way.

Albania reiterates its position in favor of a global, open, free, stable and secure cyberspace where international law, human rights and fundamental freedoms are respected, to the benefit of social, political and economic development,

For Albania Internet and technology are not and should not become a weapon; they must remain a force for good.

Thank you.

The United States of America

Thank you, Minister Xhaçka for co-hosting this Arria with us, as well as Ecuador and Estonia for joining us as co-sponsors. And thank you to our briefers for informing and shaping today's conversation. And finally, thank you to all of you for being here this afternoon.

We convened this meeting for a simple reason: the technology, internet, and digital services that we rely on, are under invigorated and escalating attack. This includes news sites and government pages, internet services that monitor our air and water, control our electricity and transportation, and facilitate our day to day lives.

More and more often, the threats we are facing online are not only coming from rogue actors, but also from states seeking to disrupt critical infrastructure. And in some cases, those very same states – and we know who they are – are putting forward bad-faith side-efforts to shape our laws and norms around cybersecurity.

The United Nations in general, and the Security Council in particular, is charged with maintaining international peace and security. And as Member States have repeatedly affirmed, malicious cyber activity to intentionally damage critical infrastructure, whether it's initiated or endorsed by a state, can instigate a conflict or exacerbate one. These attacks can be even used as weapons of war. We have to work together to stop them.

For those who used to doubt the seriousness and global scale of the cybersecurity threat, the past few years have put any debate to rest. In the early stages of Russia's unprovoked and unjustified war against Ukraine, Russian state-affiliated actors launched offensive cyber operations aimed at destabilizing Ukraine by targeting its power grid and satellite communications. Russian and Russia-aligned cyber actors have continued to target Ukrainian public and private sector entities throughout the course of the invasion.

Last year, as we just heard, we witnessed one of the most damaging peacetime cyberattacks in recent memory, when the Government of Iran conducted a cyberattack on Albania that destroyed government data and disrupted numerous public services.

Meanwhile, the DPRK has launched indiscriminate cyber attacks that have impacted networks, including critical infrastructure networks, in more than 150 countries. The DPRK has also stolen more than a billion dollars through cybercrime, threatening the economic stability of every Member State, to fund its unlawful WMD and ballistic missile program.

The United States has long been concerned by China's behavior in cyberspace as well, including its development of a cyber hacker enterprise where government-affiliated actors engage in ransomware attacks and other malicious activity. Non-state actors, particularly those engaging in ransomware activities, also pose an increasing threat to the public and private sectors.

Given these myriad, serious, and dynamic threats, all of us are looking to the UN, for both prevention and response. To that end, it is exciting to see three cybersecurity-related meetings this week convening simultaneously here at UN headquarters. These activities make it clear: international cybersecurity is a priority for the international community.

Given these multiple lines of efforts, our work in the Security Council must complement and build upon the existing work in other fora. The Security Council must take a leading role in raising awareness, condemning, and holding actors accountable for malicious cyber activity for the purpose of preventing and deterring such behavior. And we need to be promoting a shared understanding of what rules and norms apply in cyberspace, and specifically, the framework of responsible state behavior in cyberspace.

Fortunately, the Group of Governmental Experts developed such a framework, and the General Assembly has, by consensus, repeatedly affirmed it. The framework's toplines are straightforward: international law applies in cyberspace. States are expected to uphold voluntary norms of state behavior during peacetime. And states should understand* practical cooperative measures to enhance their cybersecurity. We urge all countries to uphold the framework. And for the framework to be effective, we must uphold it together.

That's what the Program of Action, which Member States strongly supported last fall, is all about. The POA would provide a permanent body focused on implementing the framework and building states' cyber capacity. To that end, I look forward to the Secretary-General's report on Member States' views on the POA this summer. We must urgently continue our conversation about the POA's establishment.

In the meantime, individual states have a responsibility to cooperate and mitigate the effects of malicious cyber activity. That includes incident response support in the immediate aftermath of cyber attacks, and mid-to-long term cyber capacity building. States are also expected to address malicious cyber activity being carried out from their territories and affecting the interests of other states. And states can also use confidence building measures to communicate and request assistance during significant cyber incidents.

Colleagues, overall, given the escalating nature of international cybersecurity threats, many of us have demonstrated an extraordinary willingness to reach consensus on these issues. It is now time to turn that good will into good action. We look forward to working with all Member States to realize our shared goal of an open, secure, and stable cyberspace that benefits us all.

Security Council members

Ecuador

Gracias señora Ministra por darme la palabra,

Agradezco a Albania y Estados Unidos por organizar esta reunión y a los expositores por sus presentaciones. El Ecuador decidió copatrocinar esta Arria junto con Estonia cuya contribución en el tema reconocemos dentro y fuera del Consejo de Seguridad, incluso por la organización del Debate Abierto del Consejo en junio de 2021.

El Ecuador reconoce e insiste que el Derecho Internacional incluyendo el derecho internacional humanitario aplica en el ciberespacio. Defendemos el uso exclusivamente pacífico del ciberespacio. La Carta de la ONU prohíbe el uso de la fuerza, por lo que toda disputa o conflicto debe procesarse por medios pacíficos, incluyendo en lo relativo al ciberespacio.

Rechazamos los ciberataques que afecten cualquier infraestructura crítica, indistintamente de su origen, pues socavan los esfuerzos mundiales por un uso pacífico del ciberespacio.

Reiteramos la vigencia de diferentes herramientas sobre la lucha contra terrorismo, incluyendo la resolución 2341 (2017) que reconoce que la protección de infraestructuras críticas entraña entre otras cosas la ciberseguridad.

Reconocemos también la necesidad de avanzar en el robustecimiento de las normas de comportamiento responsable, así como en la estructura normativa internacional en la materia, para lo cual valoramos y apoyamos las recomendaciones y conclusiones de los Grupos de Expertos Gubernamentales y del Grupo de Trabajo de Composición Abierta de 2021 reflejadas también en las resoluciones de la Asamblea General en la materia. Reconocemos también el trabajo que viene llevando a cabo el segundo Grupo de Trabajo de Composición Abierta que se encuentra reunido en este momento.

El fomento de confianza y construcción de capacidades para la reducción de las asimetrías son herramientas indispensables para superar las amenazas de ciberseguridad y favorecer un entorno abierto, estable, seguro, accesible y pacífico, en beneficio de todos.

Recordamos que con los rápidos cambios tecnológicos las amenazas en el ciberespacio también tienen un impacto diferenciado sobre las mujeres y las niñas. Reiteramos además la necesidad de asegurar una participación igualitaria, plena y efectiva de las mujeres en los procesos de negociación sobre ciberseguridad y sobre otros ámbitos que incluyan la dimensión ciberespacial entre sus componentes.

El Consejo de Seguridad en los esfuerzos de mantenimiento de la paz y de consolidación de la paz, debe aprovechar el rol de las organizaciones regionales, en particular en materia de ciberdelito y ciberterrorismo.

La estrecha colaboración entre los sectores público y privado favorece la protección efectiva de las infraestructuras críticas por medio de acciones concretas como el intercambio de información, la creación de plataformas de colaboración y programas de capacitación y concienciación, el establecimiento de equipos de respuesta a incidentes, la participación en ejercicios y simulacros conjuntos.

Al encontrarnos en la semana de protección de civiles, recordamos la obligación de los Estados de tomar las medidas necesarias para proteger a la población en contextos de conflicto, de todos los riesgos e impactos digitales sobre las personas.

Concluyo reiterando nuestro compromiso frente al uso responsable de las tecnologías de la información y la comunicación como clave para garantizar la estabilidad y seguridad en el ciberespacio. El Consejo de Seguridad por su parte debe considerar mecanismos de fortalecimiento del uso de las tecnologías como medios de consolidación de la paz en complemento a los esfuerzos regulares.

Muchas gracias.

Malta

Thank you, Chair

Let me start by thanking Albania and the US for organizing this meeting on cyber-attacks against critical infrastructure underscoring the engagement of the Security Council on cyber issues, which deserve particular attention.

I also thank Ms. Izumi Nakamitsu, Under-Secretary General and High Representative, UN Office for Disarmament Affairs, as well as Ms. Marietje Schaake and Ms. Moliehi Makumane, for their briefings.

Cyberattacks targetting critical infrastructure can no longer be described as a new form of assault. The attack on vital systems - fundamental for the functioning of society - has profound implications for the maintenance of international peace and security.

President, It is now more pressing for the Security Council to assume responsibility for evaluating associated risks, and, most importantly, preventing conflict and the civilian harm arising from cyberattacks. States must act responsibly in cyberspace and comply with and uphold the United Nations Charter and international law.

Cyberattacks have increased and have recently become more sophisticated. Hackers sometimes spend months or even years lurking undetected on targeted computer systems partaking in malicious activities such as phishing and malware distribution campaigns and denial-of-service attacks, causing massive system breakdowns, and threatening the ability of States to deliver critical public services.

Malta recognizes the perilous and constantly changing cybersecurity threats and the importance for countries to be prepared and able to counter such threats. We need to establish further cooperation in the field, both at a regional and global level. Strengthening cooperation and partnerships with other countries as well as the private sector and civil society is essential to protecting our way of life as well as mitigating the risks of such threats and attacks.

Global resilience is a key element to address the challenges associated with the digitalization of economies and societies, as well as to reduce the ability of potential perpetrators to misuse ICTs for malicious purposes. With ICTs now a fundamental aspect of societies and economies, their security is becoming more relevant to national and international security. Malta strongly supports the ongoing process the Ad Hoc Committee on Cybercrime, which will build on existing treaties, including the 2001 Budapest Convention. The intersessional consultations with multi-stakeholders represent a crucial exercise in fostering public-private partnerships which will help us to develop the most effective strategies in countering cybercrime.

Chair,

Cyber operations have become a reality in armed conflicts around the world. In this respect, Malta supports the view of the ICRC that IHL has an indispensable role in limiting the damage and dangers which these operations can have on civilian populations.

Just like any other weapons, Cyberattacks can critically damage infrastructure indispensable to the survival of the civilian population. They can be used to steal and ransom medical data across a healthcare system. They can take critical water and electricity services offline.

Malta believes that respect for international law, including international humanitarian law, and the continued work in the United Nations to implement the norms of responsible state behaviour is essential to maintaining international security and stability in cyberspace and should guide our collective efforts. The Security Council has already further recognised the obligation to protect infrastructure indispensable to the survival of civilian populations in conflict settings through Resolution 2573.

Chair,

Malta stresses that capacity building in cybersecurity is vital for States to be able to guarantee adequate security for their infrastructure and to protect their citizens. However, there might be limitations with resources, both human and financial, further stressing the need for cooperation among States also relating to training and sharing of best practices.

To this end, Malta will continue to participate in further discussions on security and stability in cyberspace, in the UN, including within the existing frameworks such as GGE and OEWG, as well as within relevant regional organisations such as the OSCE, to foster a stronger common understanding of threats faced in cyberspace and a common approach, while building and strengthening capacities.

We live in an interconnected and dynamic world. International law is the foundation of a rules-based international order. For cyberspace to fall within that order; international law must be upheld and enforced also in this domain. By committing to the Charter and International Law we contribute to a rules-based system, effective multilateralism, and robust global governance. This approach ensures that cyberspace remains open, stable, and secure, fostering an environment that benefits everyone.

Thanks

Japan

First, I would like to thank Minister Xhacka, and Ambassador Thomas-Greenfield for organizing this meeting. Also, I thank the distinguished briefers for their informative contributions.

A ransomware cyber operation targeted a hospital in Japan last November, causing a system failure of its electronic medical records. As a consequence, surgeries and other medical services were suspended for several weeks.

Cyberattacks similar to this terrifying incident, or even more severe ones, are frequently targeted at critical infrastructure, directly impacting the people in affected areas in many parts of the world.

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. There are no borders in cyberspace. That is why international cooperation is not an option but an absolute necessity for all of us.

Today, I would like to outline Japan's key priorities to address this pressing issue.

First, we must promote the rule of law in cyberspace. The cyber domain is not a lawless space. International law, including the UN Charter and international humanitarian law, is applicable in cyberspace. Given the rapidly changing nature of the ICT environment, our priority should be focused on engaging in further concrete discussions on how existing international law applies, rather than initiating a process to create a new legally binding instrument.

Regarding the norms of responsible State behavior, we highly value the work accumulated through the GGE and OEWG processes. We have to redouble our efforts to deepen the understanding of and to implement the 11 norms of responsible State behavior, which all Member States have agreed upon.

Japan takes the view that an act of causing physical damage or loss of functionality by means of cyber operations against critical infrastructure, including medical institutions, may constitute an unlawful intervention, depending on the circumstances, and at any rate, may constitute a violation of sovereignty.

The due diligence obligation may provide grounds for invoking the responsibility of the State from the territory of which a cyber operation not attributable to any State originated.

Our second priority is developing confidence-building measures. Enhancing mutual understanding among States regarding their cyber strategies, policies, laws and regulations can help mitigate the risk of tensions or escalations resulting from miscalculations or misunderstandings.

To that purpose, we welcome and support the ongoing discussion at the OEWG aimed at establishing global Points of Contact (PoC). In synergy with similar initiatives at multilateral or regional levels, these

multiple PoC networks can serve as platforms for information sharing on critical infrastructure incidents and facilitating the matching of needs and offers of assistance.

Our third priority is capacity-building. Japan has been supporting capacity-building projects, with a particular focus on ASEAN countries.

The ASEAN-Japan Cyber Security Policy Meetings, which we have organized since 2009, have provided opportunities to enhance capacity-building among local authorities and foster industry-government-academia collaboration for the protection of critical infrastructure.

Distinguished Co-Chairs,

Japan supports the establishment of a Programme of Action (PoA). Japan believes that a PoA, as an action-oriented framework, can provide an appropriate forum for continuing discussions on responsible State behavior in cyberspace. We will also continue to constructively participate in ongoing discussions at the OEWG on the topics I have addressed today.

Japan is firmly committed to safeguarding a free, fair and secure cyberspace. The Security Council should remain seized more frequently on the emerging security risks associated with the ICTs, and Japan will spare no effort in collaborating with other Council members to address this issue.

I thank you.

Brazil

Thank you. At the outset, allow me to thank the briefers. Brazil shares the assessment, contained in the concept note for this meeting, that secure digital technologies are essential to economic growth and for stable and prosperous societies. We further share the concerns about the evolution of a wide range of threats in the digital domain. We also believe that an open, secure, stable, peaceful and accessible ICT environment is essential to achieve peace and stability in cyberspace.

For these reasons, Brazil has been an active participant in the processes in the General Assembly that have sought to discuss norms, principles and rules related to ICTs, including the Framework for responsible State behavior, the Group of Governmental Experts and the Open Ended Working Groups on ICTs in the context of international security. Brazil has put forward its national position on the discussions about a regular institutional dialogue under the UN auspices and our delegation to the OEWG is working constructively towards the establishment of a cyber Points of Contacts directory as we speak.

Madam President,

Creating yet another forum for cyber discussions in the Council could work at cross-purposes with the goal of having a single, global track for the formulation and discussion of cyber norms and activities, diverting scarce resources and making it harder for us to reach consensus in our debates. This does not mean the Council has no role to play. The Council may be called upon to respond to specific cyber incidents that have tangible impacts on peace and security, and fall under its mandate.

Nevertheless, when discussing cybersecurity, we must keep in mind its unique characteristics. Cybersecurity involves several aspects that are closely linked to issues that go beyond the strict realm of security, such as SDGs, human rights, privacy, capacity building, reinforcing national, regional and global resilience and so on. Further, the diversity of actors, stakeholders and interests in the field of cybersecurity means that this is a topic best handled by the General Assembly. The GA has been able to take concrete steps, including defining, by consensus, norms of responsible state behaviour.

In our meetings at the current OEWG, we have made significant efforts to bridge the gap between different positions on the next steps for these processes. One of our main priorities for the OEWG is to build further consensus around a unified track for our future discussions in order to avoid duplication of work and uphold multilateralism.

I thank you.

Switzerland

Madame la Présidente,

Je remercie l'Albanie et les États-Unis d'avoir convoqué ce débat. Je remercie également Mme la Secrétaire générale adjointe Izumi Nakamitsu, Mme Marietje Schaake et Mme Moliehi Makumane pour leurs interventions.

La Suisse est particulièrement préoccupée par les cyber-opérations menées ou tolérées par des États d'une manière incompatible avec le droit international. Il est inquiétant que des acteurs étatiques et non-étatiques prennent pour cible des infrastructures critiques et la société civile par le biais de cyber opérations. Ceci inclut des infrastructures médicales et humanitaires, comme la cyber opération contre le CICR découverte en novembre 2021. On est aussi préoccupé par les effets non-intentionnels « spill-over » ainsi que les nouvelles technologies qui peuvent - si pas sécurisées - être susceptibles à des cyber activités malveillantes.

J'aimerais souligner trois points :

Premièrement, le droit international est applicable au cyberespace. L'Assemblée générale l'a reconnu dans plusieurs résolutions et par le Cadre pour un comportement responsable des États dans le cyberespace. Le droit applicable inclut les règles de la Charte des Nations Unies, le droit de la responsabilité des États, les droits de l'homme et le droit international humanitaire dans le contexte des conflits armés. Les cyber-opérations dans les conflits armés peuvent avoir des conséquences réelles et graves. Nous devons prioriser une compréhension commune de la mise en œuvre du droit international existant, et ceci avant de discuter d'un nouvel instrument juridiquement contraignant.

Deuxièmement, il faut créer et renforcer la coopération afin d'augmenter la sécurité face aux cyber risques. Le secteur privé est un partenaire important, car il possède et exploite l'infrastructure d'internet. Depuis avril la Suisse possède une nouvelle cyber stratégie. Elle préconise une coordination accrue au niveau gouvernemental et encourage les partenariats public-privé. Au niveau international le Programme d'Action sur la cybersécurité devra renforcer la coopération entre les Etats et d'autres acteurs dans ce domaine.

Troisièmement, un cyberespace stable, ouvert, libre et pacifique nécessite d'intégrer toute la société. Une recherche soutenue par la Suisse et menée par le Global Network of Women Peacebuilders et la Fondation ICT4Peace sur l'influence de la cyber sécurité sur l'agenda femmes, paix et sécurité montre que les femmes sont souvent victimes de cyber-menaces de manière disproportionnée. Les mesures pour atténuer les risques de cybersécurité liées au genre sont insuffisantes. Une approche sensible au genre permettra d'améliorer l'accès des femmes aux outils relatives à la cybersécurité ainsi que des réponses plus holistiques et efficaces face aux cybermenaces.

Madame la Présidente,

Le Conseil de sécurité peut jouer un rôle. Il peut envoyer un message fort en promouvant le respect du droit international et le Cadre sur le comportement responsable des États dans le cyberespace. En cas de menace contre la paix et la sécurité, le Conseil devrait utiliser les pouvoirs que lui confère la Charte, et favoriser le règlement pacifique de conflits.

Je vous remercie.

The People's Republic of China

主席女士：

我感谢中满泉高级代表及两位专家的通报。

信息通信技术革命日新月异，人类社会加速迈进数字文明的新时代。与此同时，网络安全风险挑战有增无减，网络攻击、网络犯罪和网络恐怖主义突出，给各国关键基础设施带来严峻隐患。

针对有关问题，我愿分享以下几点看法：

第一，防止网络空间战场化对保护关键基础安全至关重要。网络空间是国际公域，各方应反对网络军备竞赛，切实遵守《联合国宪章》宗旨和原则，特别是主权平等、不使用或威胁使用武力、和平解决争端等原则，维护网络空间和平属性，通过对话与合作解决网络安全威胁。个别国家将网络空间定为军事行动疆域，制定进攻性的网络安全战略，甚至提出“将他国关键基础设施纳入战时网络攻击目标"，这些不负责任的做法严重加剧各国关键基础设施面临的安全风险。

第二，要以专业、负责任的态度开展网络攻击溯源国际合作。可被证实的溯源是应对网络攻击关键基础设施的前提，也是讨论各国责任和义务的基础。网络空间因其虚拟属性，在进行有效追踪溯源方面面临诸多困难。贸然给他国“定罪"，甚至散布虚假消息、恶意抹黑，只会加剧对立对抗，影响各国通过对话合作解决网络安全挑战的努力。中国呼吁建立政府间的溯源国际机制，在此基础上共商解决网络攻击之道。

第三，应确保各方广泛参与制定关于网络空间治理的新规则。中方一贯主张，应根据信息通信技术特点和形势发展需要，在责任共担、权利共享的基础上制定新规则，特别是要保障发展中国家的权利，联合国相关报告已就此形成共识。各方应在新规则中明确承诺，不利用信息通信技术破坏他国关键基础设施，不破坏或窃取他国关键基础设施重要数据。

第四，安理会可在维护网络安全、保护关键基础设施方面发挥重要作用。安理会应鼓励各方共同建设和平的网络空间，推动各国特别是大国遵守联合国“负责任国家行为框架"，避免网络空间变为新的战场。安理会还应支持各国开展相关经验和技术交流，增进技术创新、预警防范、应急响应、标准规范等国际合作。

主席女士，

在当前网络安全威胁与挑战不断增多的背景下，国际社会更应坚持多边主义，坚守公平正义，兼顾安全与发展，深化对话与合作，推进网络安全治理和国际规则制定。中方愿与各方一道，共同推动相关国际讨论走深走实，为维护全球网络空间繁荣与稳定、构建网络空间命运共同体作出不懈努力。

谢谢主席女士。

France

Madame la Présidente,

Les comportements malveillants dans le cyberespace n'ont cessé de croître au cours des dernières années. Ils constituent un véritable défi pour la sécurité de nos Etats, la résilience de nos économies ou encore la cohésion de nos sociétés.

Si la menace la plus présente reste celle du cyber-espionnage, nous constatons avec une grande préoccupation la recrudescence d'attaques de type « rançongiciels » qui peuvent occasionner le blocage des infrastructures essentielles d'un pays. Deux grands hôpitaux français ont ainsi été touchés en 2022.

Nous le savons, ce qui se passe dans le cyberespace a des conséquences bien réelles. La cadence et la sophistication des tirs de missiles balistiques nord-coréens sont rendus possibles par les attaques cyber que ce pays mène à grande échelle pour subtiliser des informations sensibles et financer ses programmes proliférant.

Madame la Présidente,
Le cyberespace est aujourd'hui devenu un terrain d'affrontement et de compétition stratégique. L'arme cyber est désormais utilisée à l'appui d'opérations militaires.

Le 24 février 2022, une heure avant d'envahir l'Ukraine, la Russie a déclenché une cyber attaque contre le réseau satellitaire KA-SAT. Plusieurs autorités publiques, entreprises et utilisateurs en Ukraine ont vu leurs communications interrompues et perturbées, et certains États membres de l'Union Européenne ont été touchés. Cette cyberattaque illustre les risques d'un cyber espace non régulé à l'heure où s'affirment les stratégies hybrides.

C'est pourquoi la France s'est elle-même dotée d'une doctrine et de moyens, en toute transparence et en conformité avec le droit international. Car dans l'usage de leurs capacités, les Etats sont naturellement astreints à respecter certaines règles, visant notamment à empêcher les effets de débordement liés à leurs actions.

Madame la Présidente,

L'enjeu pour les années à venir est donc de bâtir une régulation qui garantisse un cyberespace ouvert, stable, sûr, accessible et pacifique. Les rapports des différents groupes de travail des Nations Unies rappellent ce qui devrait être une évidence : le droit international, s'applique dans son intégralité au

cyberspace, y compris la Charte des Nations Unies. Cela implique que le droit international humanitaire s'impose également aux opérations cyber conduites lors des conflits armés.

Au-delà, nous nous sommes accordés sur des normes de comportement responsable. Ces normes appellent à ne pas porter intentionnellement atteinte aux infrastructures critiques et à prendre les mesures nécessaires pour les protéger. Les normes relatives à la diligence requise sont cruciales afin d'encourager les Etats à prévenir les cyberattaques prenant origine sur leur territoire et favoriser une réponse coopérative aux incidents. Notre priorité doit être de préciser ce cadre normatif, tout en soutenant sa mise en œuvre.

C'est pourquoi la France, avec un groupe transrégional d'Etats, promeut l'idée d'un Programme d'action. Cette idée a été saluée en 2022 par l'Assemblée générale, qui a appelé à la poursuite des travaux en vue de son établissement. Ce Programme d'action offre un processus permanent, flexible, tourné vers les résultats. L'un de ses objectifs est de soutenir les Etats, par des programmes ciblés de renforcement de capacités, dans leurs efforts de mise en œuvre des normes agréées à l'ONU. Il permettra d'accroitre la coopération avec les acteurs privés qui ont une responsabilité évidente dans la résilience de nos réseaux.

Cet engagement collectif, multi-acteurs, est le seul susceptible de produire des résultats utiles afin que le cyberespace ne devienne pas le champ de bataille du XXI° siècle.

The United Arab Emirates

I would like to begin by thanking Albania and the United States for organizing this Arria formula meeting today on a topic that is both timely and decisive for our future societies. I welcome the Minister of Foreign Affairs of Albania and reaffirm our excellent cooperation in this field. And I also wish to extend my thanks to the briefers for their presentations today.

Our use and dependence on information and communication technologies – including artificial intelligence - continues to grow. Opportunities to make our societies more intelligent and sustainable have expanded, but so too have the risks associated with these new technologies.

The UAE would like to make two points on this topic today.

First, at the state level, the use of cyber technologies should be firmly guided by international law and the principle of responsible state behaviour.

International law continues to apply in cyberspace. That means that the UN Charter, sovereignty, non-interference in the internal affairs of another state, state responsibility, and the laws of armed conflict must continue to be respected, where relevant.

To ensure this, member states should work to further develop norms and mechanisms that uphold and maintain these laws as these technologies develop.

This discussion has been far outpaced by the rapid developments in cyber capabilities and threats globally and we must close the normative gaps. We would see value in considering an accountability framework in relation to cyberattacks, including guidance on best practices on public statements of attribution of attacks.

Second, the proliferation of tools that enable non-state actors to conduct attacks requires increased attention.

These tools are vulnerable to exploitation, for example, by terrorists aiming to radicalize and recruit.

In recent years, we have seen government databases hacked and threats to critical infrastructure risking the security of entire populations and systems. We have also seen a striking rise in blackmail threatening the most sensitive data of individuals stored online. All possible avenues to combat such threats should be considered, including strengthening public-private partnerships, investing in capacity-building of relevant state institutions, and fully utilizing all tools available to the Security Council.

In the UAE we have recently been attacked by various non-state actors, including terrorist groups in the form of DDoS, Ransomware, and phishing campaigns. It not only affected the financial sector, but it also caused some disruptions in other critical infrastructures such as government services and health services.

The private sector is well positioned to share best practices in detecting transnational threats. Technical assistance, intelligence-sharing, as appropriate, and training programs could enable more effective responses.

In contrast, when wielded correctly, new technologies also offer new ways to prevent and counter terrorist threats such as the detection and removal of online terrorist content.

In the UAE, we believe that responsible development of new technologies is key. Our motto for applying and developing Artificial Intelligence specifically is the B.R.A.I.N. acronym - 'Building a Responsible Artificial Intelligence Nation'. Cyberspace should be a public good, something safe and beneficial to all.

The UAE appointed the first Minister of State for Artificial Intelligence back in 2017. That same year we launched our AI Strategy including an ethics toolkit. Since then, we have been exploring avenues to use A.I. machine learning to assist with pattern detection, to be able to track the adverse effects of climate change, such as water depletion. We are committed to driving a society-wide digital transformation through innovation, entrepreneurship, and digital startups. And as we move towards the transformation to a digital society, this is why we need to protect our future infrastructure, economies, and citizens from malicious cyber threats.

To conclude, the responsibility to mitigate the related risks of new technologies rests with all of us. That includes both those public and private actors at the forefront of developing new technologies and the members of the Security Council.

We need multi-stakeholder engagement to create a shared vision for new technologies. And we welcome the efforts by UNESCO and others to consider ethical guardrails by developing global standards or codes of conduct for A.I. These agreed upon standards would help us to manage the risks of reproducing the real-world biases and discrimination that fuel divisions.

The UAE will continue to work with the rest of the international community to advance responsible behavior in cyberspace.

Thank you.

Mozambique

Excellencies, Co-Chairs

Mozambique thanks the Permanent Missions of Albania, the United States and form the co-sponsors for organizing this important Arria formula meeting.

We also thank the briefers for their expert insights, particularly USG Nakamitsu for her thorough assessment of where the international conversation on today's topic stands.

Co-Chairs

The rapid development of the digital and cyber landscape is greatly changing the world for good but also in nefarious ways.

The Internet of Things (IoT), the metaverse, AI, technology driven changes are happening at the proverbial speed of the internet, so much so that we are most of the time left figuring out how to deal with their profound social, political, and indeed security implications, as we go.

As USG Nakamitsu reminded us in her brief, no day goes by without reports of some ransomware attempt, a denial-of-service attack or a hacking for coercion incident, directed at critical and sometimes lifesaving infrastructure, business, government agency by a criminal hacking group or a state agent.

Indeed, we can arguably talk of pandemic levels of cyber threats!

The question is therefore, in a world where we increasingly rely on technology to improve efficiency and effectiveness of both basic and complex critical infrastructure, what actions can be taken domestically and internationally to protect ourselves against the threat of such far-reaching incidents affecting our lives?

This Arria formula is part of the answer!

Mozambique believes that action is urgently needed at the domestic and international levels to improve the cybersecurity of critical infrastructure—and to bring those responsible for malicious and disruptive attacks to justice.

We know that lack of experience with actual cyberattacks, as it is the case with our own country, can create indecision on how to respond to one when it does occur.

Many difficult legal debates are ongoing over how to apply the laws of armed conflict, for instance, to cyber actions as a way of gauging whether to take retaliatory action.

Though cyber actions are routinely called “attacks,” the implicit threshold that countries consider in determining how to respond is whether a cyber action qualifies as the “use of force.”

Despite decades of incidents of cyber espionage and crime around the world, only a handful of cyber actions to date have crossed the use-of-force threshold.

However, with systemic attacks on supply chains or critical infrastructure, it only takes one misstep to produce catastrophic collateral damage with real human casualties.

As the impressive multi-media project hosted by Switzerland and the ICRC currently on display here in the building innovatively illustrates: Digital Dilemmas, have Real Life Consequences!

Co- Chairs

Let me add two modest contributions to the wealth of proposals put forward today by many of you.

First, prevention. There’s need to improve general security standards for all IT companies, private industries and public services. The inclusion of the private sector in this conversation is critical.

Second. There’s need for increased information-sharing in relation to cyber incidents and how to patch up vulnerabilities and foolproof the systems, platforms and processes, so critical to modern daily life.

Strengthening domestic resilience is an essential starting point, but as cybercrime is inherently international in nature, international cooperation and exchange of know-how and real time threat assessment, will have to improve, including the question of attribution and how to bring those responsible to justice.

While there are plenty of agreed-upon norms, there is still no international consensus on what the consequences should be for a state that flouts the rules.

Notions of cyber sovereignty will have to be rethought.

We must not replicate the capability asymmetries of the physical world in the cybersphere.

As the reliance on smart infrastructure proliferates and the associated cyber vulnerabilities multiply, governments and private sector actors must get their act together and improve the cooperation needed to actively avert cyberattacks to critical infrastructure, at the risk of promoting a sense of impunity in cyber space with grave and yet unknown real-life consequences.

Going forward, Mozambique will remain engaged in these important discussions.

I thank you.

Ghana

Co-Chairs, Excellencies,

At the outset, I wish to thank Albania, United States, for convening this very important Arria formula meeting. I also thank the briefers for their insightful perspectives.

Undoubtedly, digital technologies is the defining issue of our time and has evolved to impact every facet of our lives.

While these technologies can be deployed in a manner that can impact positively on our development, it can also be exploited by non-state actors to contribute to instability and exacerbate conflict situations, including through the spread of online disinformation, hate speech as well as the destruction of state infrastructure.

In this regard, it is important to leverage the tools available at the international, regional and national level in a manner that would enable us to harness the benefits of technologies for development and curtail the vices associated with it.

Co-chairs

At this juncture, we wish to advance four (4) points which we think are critical in enhancing efforts in addressing the negative use of digital technologies as follows: first the need to leverage on the tools available in the multilateral system including the principles of the UN Charter and other tools in the General Assembly, second strategic deployment of tools in the Security Council including the enhancement of trust building, third obligation of States, and fourth adopting a whole-of-society approach.

Regarding the mechanisms in the multilateral system, we reaffirm our support for the purposes and principles of the UN Charter as well as processes in the General Assembly such as the Open-ended Working Group (OEWG) on security of and in the use of information and communications technologies. These mechanisms provide a useful framework to bolster a general understanding of how international law applies in the use of ICTs. It enhances the exchange of ideas and cooperation in comprehensively dealing with the issue.

Pertaining to the role of the Security Council, we share the view that support for the use of digital technologies in transforming UN peacekeeping is one of the useful ways by which we can impact positively on the resolution of conflicts. The continuous prioritisation of digital technologies by the Council in supporting peacekeeping operations and the protection of civilians, as well as post-conflict peacebuilding efforts remain crucial.

In building trust among member states, it is pertinent for the Security Council to embrace deliberate diplomatic actions consistent with the Diplomatic Convention, to sustain mutual trust, including by emphasizing dialogue. It is important to place value on deepening our common understandings of the application of existing international law to States' behaviour in the use of ICTs. This would increase the predictability of State behaviour, lower the risk of miscalculation and clarify the consequences of unlawful State behaviour.

While upholding the sovereignty and territorial integrity of States, we believe that States adherence to their obligations within the global normative frameworks governing cyber space is key. This enhances responsiveness to cyber-attacks on critical infrastructure. We welcome the adoption of Human rights resolution 49/21 which call on States to take measures in addressing the negative tendencies pertaining to the arbitrary use of technologies, which in effect can cause more harm than its intended positive benefits.

The multilateral and regional frameworks in place, including the UN Charter are tools that underpin States ability to notify a second State of malicious activity emanating from its territory. The principles embodied in these mechanisms apply to the use of ICT and require States to observe the principle of international law, peaceful settlement of disputes and non-interference in the affairs of other States. It also places a moral obligation on states to cooperate in addressing infractions that arise from malicious activities in the cyberspace.

Lastly, we believe that one of the sustainable ways of addressing cyberattacks for a peaceful cyberspace is to embrace a whole-of-society approach by deepening partnerships with critical stakeholders including the tech giants, civil society organisations and other partners in developing strategies and enhancing ownership of the processes in dealing with cyberattacks and other negative tendencies associated with its use.

In concluding, Ghana believes that we can enhance State responsibility and responsiveness to avert attacks on critical infrastructure if States demonstrate stronger political will, together with deeper cooperation at the multilateral and regional levels.

I thank you

The Russian Federation

Уважаемые коллеги,

Российская Федерация стояла у истоков многосторонней дискуссии по международной информационной безопасности (МИБ). Еще в 1998 году мы подняли этот вопрос в Генассамблее ООН, добились того, что он на постоянной основе вошел в ее повестку дня. Мы уже почти двадцать пять лет является авторами соответствующей резолюции Генассамблеи, которая год от года принимается при широкой поддержке государств-членов. По нашей инициативе много лет работала сначала профильная группа правительственных экспертов по МИБ, а затем инклюзивная, открытая для всех государств-членов Рабочая группа ООН открытого состава.

Хочу напомнить, что наши западные коллеги всем этим инициативам долгое время сопротивлялись. Они сначала были против создания группы правительственных экспертов, потом последовательно голосовали в Генассамблее против РГОС по МИБ. Они внесли в Генассамблею, где десятилетие был консенсус по теме МИБ, раскол, пытаясь создать «спойлеры» российским инициативам.

Это в том числе те страны, которые выступают организаторами сегодняшней «Аррии». Все вопросы, которые сегодня вынесены на обсуждение, рассматриваются полным составом Генассамблеи буквально в соседнем зале, где сейчас проходит заседание упомянутой РГОС. Что мешает обсудить их там, на профильной площадке? В Генассамблее все 193 государства-члена Организации имеют возможность на равных обмениваться мнениями по широкому набору тем, включая все виды угроз в сфере МИБ, правила, нормы и принципы ответственного поведения государств, вопросы применимости международного права к сфере использования ИКТ и другие аспекты, о важности которых говорят организаторы сегодняшней «Аррии». К слову, в

отношении последнего они намеренно некорректно трактуют выводы РГОС – международному сообществу еще только предстоит выработать общее понимание того, как именно международное право применяется к сфере использования ИКТ государствами. Очевидно, что практические шаги в целях формирования мирного и безопасного информационного пространства, а также мнение других стран на этот счет США и их союзников волнуют мало. Все, что им нужно – политический и пропагандистский эффект.

В этом контексте попытки западных делегаций обвинить Россию во всех «кибергрехах», перекладывая с «больной головы на здоровую», нас не удивляют.

Их цель очевидна - прикрыть собственные агрессивные действия в информационном пространстве. Западные высокопоставленные должностные лица не то что не стесняясь, а с гордостью рассказывают о проведении наступательных операций с использованием ИКТ против нашей страны. Приведу ряд примеров.

Согласно информации Федеральной службы безопасности Российской Федерации, с начала 2022 года было зафиксировано более пяти тысяч хакерских атак на критическую инфраструктуру нашей страны. Роль «плацдарма» для них и «испытательного полигона» для новых видов вредоносного программного обеспечения отведена Украине, в которую вливаются соответствующие финансовые средства, обучаются кадры, оказывается техническое содействие в наращивании наступательного потенциала. При этом западные спонсоры киевского режима предпочитают закрывать глаза на то, что созданная при их помощи группировка IT Army of Ukraine уже начинает совершать преступления против их же граждан. Нам известно и о том, что США активно практикуют «сотрудничество» с различными международными хакерскими группировками.

Мы все эти атаки, конечно, успешно отражаем. Но жертвой такой агрессии в ИКТ-сфере со стороны США может стать любое государство. За примерами вмешательства Вашингтона во внутренние дела других стран – причем даже их союзников, о чем последние предпочитают смиренно молчать – далеко ходить не приходится: мир прекрасно помнит разоблачения Эдварда Сноудена. Американскими спецслужбами налажена глобальная система использования шпионского программного обеспечения и перехвата персональных данных. В феврале этого года администрация Дж.Байдена продлила действие закона «О наблюдении за иностранной разведкой», который позволяет США вести неограниченную электронную слежку и перехват личных данных по всему миру в нарушение основополагающих прав и свобод.

Россия решительно выступает против т.н. «порядка, основанного на правилах» в информационном пространстве, который на самом деле означает «право сильного». Мы продолжаем предпринимать энергичные усилия для формирования мирной, безопасной, справедливой ИКТ-среды, в которой были бы защищены интересы всех государств вне зависимости от уровня их развития.

Мы последовательно выступаем за принятие универсального юридически обязывающего инструмента в сфере использования ИКТ. Вместе с соавторами мы внесли на рассмотрение Генассамблеи концепцию конвенции ООН об обеспечении международной информационной безопасности. Мы предложили инициативу по формированию глобального реестра контактных пунктов в сфере ИКТ, которая способствовала бы снижению напряженности в цифровой сфере, укреплению доверия и налаживанию контактов между компетентными ведомствами государств. Рассчитываем на скорейшее согласование ее параметров в рамках РГОС и приветствуем активные усилия, предпринимаемые в этих целях ее председателем, постпредом Сингапура Бурханом Гафуром.

Уважаемые коллеги,

Как бы западные страны ни пытались изобразить себя поборниками МИБ, думаю, очевидно, что они попросту эксплуатируют эту тему в своих корыстных интересах, стремясь при этом сохранить «свободу рук». Россия же будет и далее отстаивать принципы формирования мирной и безопасной среды ИКТ в глобальном масштабе. Мы готовы к взаимодействию в этих целях со всеми конструктивно настроенными государствами.

Благодарю Вас.

The United Kingdom of Great Britain and Northern Ireland

Thank you to our hosts for organising this important discussion and to the briefers for their valuable insights.

The UK is committed to advancing an open, peaceful and secure cyberspace through responsible behaviour.

As the briefers highlighted, UN Member States agreed a consensus Framework for Responsible State Behaviour in cyberspace in the General Assembly. We also all agree on the applicability of existing international law, including the UN Charter, to state activity in cyberspace.

Despite this, some states – including permanent members of this Council – continue to act irresponsibly.

Russia has used sophisticated cyber capabilities and information campaigns to undermine international peace and security, carrying out multiple disruptive attacks against Ukrainian critical national infrastructure as well as the OPCW. Iran has carried out reckless cyber activity against Albania, causing significant disruption to government services. This sort of activity has real world impacts. Cascading effects from attacks on critical infrastructure can be escalatory and have devastating security, economic, social and humanitarian consequences.

Upholding and implementing the Framework and existing International Law is the most effective means of ensuring peace and security in cyberspace.

The Security Council should affirm this Framework and the need for all states to implement it.

The Council also has a responsibility to uphold the Charter. In doing so, it should reaffirm this central point: our obligations under the Charter apply in the cyber domain just as they do in the physical world.

The United Kingdom is committed to playing its part in implementing, and supporting other States to implement the Framework.

We continue to elaborate our understanding of how international law applies in cyberspace – in line with the speech by our Attorney-General last year – and encourage others to do the same. This will yield common understandings, enhance Member States capacities and promote stability.

We support proposals in the First Committee for a permanent UN mechanism to discuss issues relating to international security in cyberspace [outlined in GA Resolution 77/37 with the support of 157 Member States]. A permanent mechanism will help all states to implement, and develop, our existing commitments. We look forward to working in partnership with Member States to take these proposals forward.

Gabon

Je remercie les briefeurs pour leurs exposés.

Monsieur le président,

La présente réunion est particulièrement importante parce qu'elle porte sur un nouvel éventail de menaces à la paix et à la sécurité contre laquelle de nombreuses nations sont impuissantes.

En effet, le paysage des menaces cybernétiques est en constante évolution, avec l'émergence de nouvelles technologies telles que l'intelligence artificielle, qui présentent à la fois des opportunités et des risques.

La connectivité des infrastructures essentielles tels que les réseaux de production ou de distribution de l'Energie, les systèmes de santé, les systèmes bancaires ou de protection des données, expose les Etats et les entreprises à des perturbations qui peuvent avoir des effets dévastateurs sur les populations et sur le fonctionnement des Etats.

Dans les régions touchées par les conflits, le niveau de risques est particulièrement élevé, concernant les attaques délibérées visant les infrastructures essentielles.

La sécurité du cyber espace se révèle ainsi comme une exigence à laquelle il faut répondre de façon collective, et cela, au moyen du droit, eu égard à l'interconnexion du monde, dans le but de mettre les TIC au service de la paix et la sécurité internationales.

la résolution A/RES/70/237 constitue une étape significative dans l'approche normative de la communauté internationale sur cette menace. Il convient de poursuivre la réflexion dans les formats dédiés de l'Assemblée générale sur l'applicabilité du droit international, y compris de la Charte des Nations Unies, et des autres normes internationales existantes, aux activités des États dans le cyberespace.

Il est évident que la promotion de comportements responsables des États dans le cyberespace, assorti de normes communes, doivent être les guides de référence dans l'utilisation des technologies de l'information et de la communication (TIC) ainsi que les rapports du Groupe d'experts gouvernementaux et du Groupe de travail à composition non limitée sur le développement dans le domaine des technologies de l'information et des communications, dans le contexte de la sécurité internationale.

Madame la Présidente,

Les cyberattaques visant des infrastructures critiques représentent une menace directe pour la paix et la sécurité internationales. Qu'elles soient le fait d'acteurs non étatiques à la recherche de gains financiers, ou utilisées à des fins de propagande ou de désinformation, leur effet est susceptible de créer le chao.

La communauté internationale doit pouvoir se prémunir de telles menaces et soutenir les Etats fragiles à prendre les mesures appropriées pour renforcer les capacités technologiques des Etats à répondre de façon efficacee à ce type de menaces transnationales.

Le Conseil de sécurité a un important rôle à jouer dans l'évaluation et la prévention des risques liés aux cyberattaques ainsi que la promotion d'un comportement responsable de la part des États.

La construction de la confiance entre les États est essentielle pour assurer un cyberespace sécurisé et pacifique. Le Conseil de sécurité peut jouer un rôle clé en facilitant le dialogue et en encourageant des mesures de renforcement de la confiance entre les États membres sur la base des normes internationales.

En conclusion, la sécurisation du cyberespace et la prévention des conflits découlant de l'utilisation malveillante des technologies de l'information et de la communication exigent une action résolue et collective.

Le Conseil de sécurité, en tant qu'organe principal chargé du maintien de la paix et de la sécurité internationales, doit s'investir dans la promotion de normes de comportement responsable des États et souligner l'applicabilité du droit international à l'utilisation des TIC par les États membres.

Je vous remercie.

UN members, starting with co-sponsors and groups

Estonia

Thank you Chair.

Allow me to start by expressing my appreciation to Albania and the United States for convening this very timely Arria-formula meeting of the Security Council. I also thank the briefers for their insightful perspectives.

We are honoured to co-sponsor this event which continues to draw the Security Council's attention to the implications of cyber threats to international peace and security. Since Estonia brought the topic of cybersecurity to the Council two years ago, the security and stability of cyberspace remain to be of great concern. Malicious cyber operations are on the rise worldwide, employed against public and private targets as well as part of military conflict.

Madam Chair,

Critical infrastructure is essential for the functioning of our societies. However, our dependence on digital solutions and the use of ICTs in critical infrastructure systems renders such systems more vulnerable. Cyberspace is not separate from the physical world, and cyber operations against critical infrastructure – such as energy and water – may have devastating results, sometimes with spill-over effects. As such, cyber-attacks against critical infrastructure have also clear implications on international peace and security, calling for the attention of the Security Council.

How to mitigate these risks and how can the Security Council contribute?

First, in order for the Security Council to uphold international peace and security in a comprehensive way it needs to be up to date with cyber threat landscape. The current Russian aggression against Ukraine has clearly demonstrated that cyber operations are employed to support conventional military operations and form an integral part of the modern armed conflict. The increasing number of ransomware attacks is another issue of great concern that can bring along devastating effects. In some countries they have constituted a state of national emergency.

Second, the Security Council must take a clear and firm stance in underlining the application of the framework of responsible state behaviour, and in particular, international law in cyberspace. A broad consensus exists that the long-standing principles set by the existing international law apply in cyberspace. Existing international law, including the UN Charter, provides guidance as to what conduct in cyberspace by States is acceptable and which is forbidden. The principle prohibiting one state from

attacking others applies here as it does elsewhere. To ensure the protection of civilians and civilian infrastructure in situations of armed conflict, which the Security Council also regularly discusses, it is vital that any use of cyber capabilities in this context would be subject to obligations deriving from international humanitarian law.

Third, the Security Council has an essential role in managing conflicts. These conflicts may include cyber operations, including attacks against critical infrastructure. Managing conflicts may entail measures for de-escalating violence, offering a platform for communication and information sharing in times of crisis, enabling humanitarian access to those most suffering, or building pressure on those responsible for such illegal behaviour.

To conclude – by raising awareness of the threat landscape, stressing the consensus agreement on the applicability of international law in cyberspace, and upkeeping the role of managing conflicts – the Security Council can contribute to reducing the risk of conflict arising from malicious cyber operations and mitigating their negative effects. This work entails also awareness raising and training professionals – for this reason, Estonia is hosting another Summer School of Cyber Diplomacy in June with a global focus and participants from almost 50 countries.

I thank you.

Australia

Chair,

I speak on behalf of Canada, New Zealand, and my own country Australia.

Australia, Canada, and New Zealand welcome the opportunity to discuss cyber threats and malicious cyber activities against critical infrastructure.

The Security Council has a crucial role to play in preventing conflicts arising from the malicious use of ICTs by states.

UN Member States have sent an unambiguous message that States' activities in cyberspace have limitations and are subject to obligations, just as they are in the physical domain.

All Members of the UN have agreed, by consensus, that existing international law – in particular the UN Charter in its entirety – applies in cyberspace.

For example, under articles 2(3) and 33 of the UN Charter, States have agreed they will settle any dispute that is likely to endanger the maintenance of international peace and security by peaceful means, such as negotiation, mediation and judicial settlements.

States should be unequivocal in their commitment to develop and use cyberspace in accordance with international law, as well as agreed, voluntary norms of responsible State behaviour. What we need now are not more - or new - rules, but adherence to the rules we have already agreed.

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

Such an affirmation can have real effect on the protection of critical infrastructure and recovery from cyber incidents, reinforcing international law and in particular the UN Charter.

It reinforces the normative commitments made by all states to protect critical infrastructure, refrain from committing internationally wrongful acts against critical infrastructure, and assist other States whose infrastructure has been targeted.

The framework acknowledges and respects differing levels of capability.

It may not be reasonable to expect, or even possible, for a State to prevent all malicious use of ICT infrastructure located within its territory.

The norms recommend that States respond to appropriate requests by taking reasonable steps, consistent with their capabilities, to end the harmful activity, and thereby minimise misperceptions and help restore trust.

The evolving equities of non-government stakeholders in cyberspace make public-private partnerships important for effective responsiveness when cyber incidents take place – because the private sector is often the first affected by cyber incidents and the protectors of critical infrastructure.

We encourage all states to implement their normative commitments in collaboration with non-government stakeholders.

We also encourage engagement with affected but underrepresented groups. The value of gender equality and women's participation in decision making, leadership and peace-building associated with international peace and security in cyberspace is indisputable.

Cyber and critical technology issues are strategic foreign policy issues – and it is vital that they are treated as such by the international community.

Thank you.

Denmark

I have the pleasure to speak on behalf of the Nordic countries: Finland, Iceland, Norway, Sweden and my own country, Denmark.

Let me start by thanking Albania and the US – with the support of Ecuador and Estonia – for taking the initiative to organise a meeting on this very important topic.

We wish to make three points today:

First, international law applies in cyberspace.

Our meeting today allows us to build on the agreement that international law, including the UN Charter, applies in cyberspace as has been affirmed by all UN member states through numerous consensus reports and the General Assembly. Similarly, we should build on the agreement on the 11 voluntary norms of responsible state behaviour in cyberspace as affirmed by the General Assembly in 2021.

Second, since Council members last discussed threats to international peace and security linked to cyberspace, we have witnessed a number of worrying developments in the landscape of cyber threats.

In the past year alone, there has been a long string of incidents where the critical infrastructure of a State has been targeted with disastrous consequences.

The most significant among them is Russia's illegal full-scale war of aggression against Ukraine, where cyber-attacks on critical infrastructure have been irresponsibly integrated into the assault. Only hours before the start of the invasion, a Russian cyber-attack targeted the satellite network equipment owned by the private company Viasat. In addition to the damage the attack wreaked on communication infrastructure within Ukraine, the attack had significant impact in several other states in Europe with effects on both the telecommunications sector and the energy sector. According to Viasat, the internet connections of tens of thousands customers across Europe were affected.

Ransomware attacks, like the one carried out against Costa Rica in 2022, have emerged as a significant threat to international security and stability. These are often carried out by non-state actors. States however, need to live up to their due diligence obligation under international law to not knowingly allow their territory to be used for acts contrary to the rights of other States.We are also worried about North Korea cyber activities using sophisticated cyber techniques to steal information of potential value, including to its weapons of mass destruction programme.

Third, we should recognise the importance of multistakeholder engagement for cybersecurity.

As illustrated by the Viasat attack, the private sector plays an essential role in cyberspace, not least during crisis and conflict. The tech and cyber security companies are often the first to discover and respond to cyberattacks. And they have unique and privileged access to global data and information.

The private sector is also playing a significant role in Ukraine's cyber defence. We must better leverage its knowledge and capabilities in our efforts to ensure peace and stability in and through cyberspace. And cooperate more closely on a technical as well as a diplomatic level. Governments and the tech industry have a shared interest in a free, global, open, stable and secure cyberspace based on international law and agreed voluntary norms.

Mdm. Chair,

In conclusion, we – the Nordics – stress that State actors carrying out cyber-attacks against critical infrastructure do so in clear violation of international law and fail to live up to the agreed voluntary non-binding norms, which all Member States have endorsed by consensus in General Assembly resolution 70/237. This is unacceptable.

All States have an important role to play in promoting and upholding a rules-based, global, open, free, and secure cyberspace. The members of the Security Council have a particular obligation to maintain peace and stability in and through cyberspace. We believe that the members of the Council should take on this responsibility by ceasing all national cyber activity that conflicts with international law and work towards a Council that is able to call out transgressions of international law in cyberspace that threatens international peace and security.

Thank you, Mdm. Chair.

The European Union

Chair,

Thank you for the opportunity to participate at this topical meeting. I have the honour to speak on behalf of the European Union.

Chair,

Malicious behaviour in cyberspace from both State and non-State actors has intensified in recent years, including a sharp and constant surge in malicious activities targeting the EU and its Member States' critical infrastructure, supply chains and intellectual property, as well as a rise in ransomware attacks against our businesses, organisations and citizens.

Cyberattacks are a threat to peace and security and a game changer in conflict and the conduct of war.

Well-targeted attacks, including on critical infrastructures, have increasingly harmful effects on economies and daily lives, including on EU Member States and our partners. Last year's attacks against Ukraine as well as on Montenegro and Albania, EU candidate countries, or the ransomware attacks affecting Costa Rica, are just mere examples here.

With the attacks, perpetrators affected critical digital government infrastructure and direct impact the delivery of public services to people and businesses.

The EU expressed solidarity with the victims of such attacks and continues to strongly condemn this unacceptable behaviour in cyberspace.

Such destabilizing and irresponsible behaviour seeks to threaten the integrity and security of a sovereign country, its institutions, values and principles. It also attempts to undermine democratic institutions and societies at large, and could potentially have spill-over effects to other countries. We continue to urge states to respect international law and to refrain from such conduct in cyberspace.

As mentioned in the UNSG Our Common Agenda Report, cyberattacks are one of the main strategic risks we are currently facing. To meaningfully address them, we should implement stronger measures to prevent, detect, deter and respond to cyber-attacks, notably those on critical as well as on civilian infrastructure and to ease cyber related tensions.

With the unstable cyber threat landscape, all States need to continue to step up their ability to strengthen situational awareness, prevent infrastructure on their territory from being misused, enhance their ability to handle cyber incidents and ensure solidarity and mutual assistance. We continue

to work with partners to address cyber-attacks by strengthening cyber resilience, through effective cyber crisis management, dealing with the causes and the impact, as well as by enhancing accountability in cyberspace. The lessons learned from the Russian aggression against Ukraine in cyberspace is that enhanced resilience and preparedness is essential to face such malicious behaviour in cyberspace.

Adding to the EU's tools to address cyber-attacks, the recently proposed EU Cyber Solidarity Act aims notably at increasing preparedness of critical entities across the EU as well as the solidarity by developing common response capacities against significant or large-scale cybersecurity incidents, with the support on the private sector. Trusted cybersecurity service providers could be an amplifier of public capacities in particular in a context of skills shortages across the world. At EU level, the creation of a Cyber Emergency Mechanism is a step in the right direction to continue to build an efficient cyber crisis management ecosystem.

In particular with regard to the protection of critical infrastructure, while recognising the central role of States, the private sector has a wide range of expertise, knowledge and capabilities to maintain cyberspace global, open, free, stable and secure. The industry has an overview of the most prominent vulnerabilities, threats and activities, to reinforce situational awareness and cooperation to prevent, detect and mitigate the impact of cyber-attacks.

Chair,

The EU and its Member States are continuously reinforcing their capacity to prevent, discourage, deter and respond to and immediately recover from malicious cyber activities. The revision of the EU Cyber Diplomacy Toolbox, also part of the EU's full-spectrum approach to address cyber-attacks, allows the EU to use diplomatic, political, legal, strategic communication, technical, operational or economic measures to enhance resilience, effectively respond to cyber-attacks, and by that contribute to conflict prevention, cooperation and stability in cyberspace.

What should be clear to everyone is that cyberspace is not a lawless domain. All United Nations Member States have agreed that international law, including the UN Charter in its entirety, applies in cyberspace. With that, States bear responsibilities to ensure international peace and security in cyberspace and can gain support from international law to protect them against malicious cyber activities.

To strengthen international security, we should advance our common understanding of the application of international law in cyberspace. What is illegal in the physical domain, is also prohibited in the cyber domain, and we should work together to ensure international law is respected. To this end, we should hold states that engage in irresponsible and unlawful behaviour in cyberspace accountable, as is also done in the physical world. Existing international law provides us tools for doing so – the rules of legal attribution under the law of state responsibility, means of peaceful settlement of disputes, including the possibility of turning to international courts and tribunals.

Last but not least, it is to be recalled that through the OEWG on ICT, we continued to strive to find common ground on the whole range of efforts to enhance international security, including the identification of existing and potential threats, capacity building, CBMs and/or regular institutional dialogue. The establishment of a permanent platform to discuss these issues within the First Committee through a Cyber Programme of Action will allow us to continue our work, in addition as to cooperation on cyber capacity building. With that we can make a significant effort to make the digital as well as the real world a more secure place, prepared to face the new challenges.

Thank you.

Costa Rica

Mr. President

Costa Rica would like to express its appreciation to Albania, the United States, Ecuador and Estonia for organizing this even, and the speakers for their insightful presentations.

Ransomware has emerged as one of the most pressing cyber threats against national stability and international peace and security. Whether employed as a commercial service or for political purposes, ransomware can cripple the operations of private entities and entire governmental organs.

One year ago, the theft and encryption of confidential governmental and personal data, led to unprecedented disruptions to Costa Rica´s finance, social security, healthcare, and other sectors, which are still felt.

At the same time, advances in artificial intelligence are adding a level of unpredictability both in terms of scale and impact of cyber-attacks. AI can be used to launch several attacks simultaneously contributing to the difficulty in response and prevention of wider damage. AI-enabled malware evades conventional cybersecurity methods and requires the use of new tools.

In this regard, please allow me to stress three points:

First, Costa Rica joins the global consensus of States that international humanitarian law (IHL) is applicable in cyberspace and to cyber operations during armed conflicts. We consider that he application of IHL to the use of ICTs during armed conflict does not legitimize cyber warfare or encourage the militarization of cyberspace in any way.

Second, civilian datasets, including medical data, social security data, tax records, corporate and financial data, or electoral lists, are critical components of digitalized societies and play a vital role in the functioning of many aspects of civilian life. Deleting or damaging such data can have severe consequences for government services and private businesses, potentially causing more harm to civilians than the destruction of physical objects. Therefore, in Costa Rica's view, the protection of civilian objects under IHL extends to civilian data.

Lastly, In Costa Rica's view, it is also imperative not to lose sight of the gendered impact of cyber operations. Women, girls, members of the LGBTQ+ community, and other vulnerable groups may be especially targeted by malicious uses of ICTs, including cyber surveillance, doxing, online harassment and hate speech. Likewise, Costa Rica notes that access to and knowledge of ICTs is still unequal among different genders and societal groups.

I thank you.

The Republic of Korea

Thank you, Co-Chairs

At the outset, I would like to begin by thanking Albania and the United States for convening this important and very timely meeting. My gratitude also goes to the co-sponsors and briefers for their insightful remarks. As we speak now, international news media is broadcasting the probably largest cyberattack on the US critical infrastructures. My gratitude also goes to the co-sponsors and briefers for their insightful remarks.

Today's meeting is a solemn reminder of the urgency and significance of maintaining stability and security in cyberspace. Already complex and sophisticated, cyber threats are evolving at an unprecedented pace, at a rate that relevant law-making processes cannot possibly keep up with. Malicious actors are illicitly deploying cyber tools to pursue their own terrorist, authoritarian, criminal, and military interests. Cyberattacks on critical infrastructures including energy, financial, transportation, health, water, and other public services facilities can have devastating security consequences comparable to a heavy kinetic use of force.

We have witnessed a number of cases of how cyberattacks can present threats to international peace and security. As recently as in 2022, one Member State suffered from such severe ransomware attacks that it had to declare a national state of emergency. A massive cyberattack on another Member State led to a severance of diplomatic relations with the country suspected of the attack.

Furthermore, the DPRK which conducted many cybercrimes in the past and even heisted a foreign central bank is now deploying more sophisticated cyber techniques to steal classified information and virtual assets worth of nearly one billion dollars last year alone. This illicit revenue has been presumably used to finance its nuclear and missile programs in violation of multiple Security Council Resolutions. It is very troubling that its authorities continue to recruit and train the elite corps of cyber hackers.

No country is in the safe zone in this domain. Developing countries in particular with relatively weak cyber defense capacities are more likely to become targets of cyberattacks.

Co-Chairs,

It was only in 2021 when the very first Security Council Open Debate on cybersecurity was hosted by Estonia. But much more needs to follow. With the recent dramatic surge of cyberattacks in both quantity and quality, the Security Council's active deliberation on cybersecurity is more than necessary; in fact, it is long-overdue. Today's Arria formula meeting is a timely stepping stone in this regard.

The Security Council, as the primary organ responsible for the maintenance of international peace and security, must take the lead in our joint efforts to raise global awareness, send a clear message to the international community and promptly respond to large-scale cyber-attacks.

The Council's active engagement on this matter will not duplicate or undermine other existing platforms like the OEWG in the General Assembly. Rather, the work of the Security Council on this issue will complement and reinforce the past achievements and ongoing discussion in the General Assembly regarding the framework for responsible state behaviors in cyberspace.

To conclude, Co-Chairs,

As one of the most digitally connected countries, and also a country facing malicious actors on our doorstep, the Republic of Korea is exposed to imminent and persistent cyber threats. As such, we are deeply committed to enabling the international community, in particular the Security Council, to better cope with and effectively respond to challenges related to cyber threats.

The Republic of Korea will strive to make a meaningful contribution to this end.

I thank you, Co-Chairs.

Israel

Thank you, Minister and dignitaries, for the opportunity to participate in this important event. First and foremost, Israel wishes to commend the United States and Albania for initiating this relevant and very timely meeting, and I take the opportunity to also thank today's briefers for the thought-provoking discussion.

The 2015 GGE - which Israel was part of - adopted the 11 UN Norms of Responsible State Behavior in Cyberspace, and described Malicious Cyber activities against critical infrastructures as a major threat to international security. 8 years later, the scope of multilateral discussions on Cybersecurity expanded, but unfortunately, the levels of risks and threats posed to states seem to have expanded even more. Threats to critical infrastructures are becoming more and more sophisticated and the malicious use of Ransomware is growing. The impacts of Ransomware – both immediately and strategically - are clear and put our lives and our economies at constant risk, as Ransomware targets our health, energy and transportation systems.

Israel is an active contributor to the global discussions on strengthening Cybersecurity and Countering Cybercrime. While the notion that International Law's applicability to Cybersecurity is consensual, Israel remains a strong voice supporting multilateral efforts to continue exploring and better understanding how existing international law is applicable to Cyberspace. Alongside, Israel is dedicated to promoting global cyber resilience and international cooperation in order to better face the evolving global Cyber threats.

Here are a few fundamental principles that should be stressed with regard to states' response to Cyber threats –

First, each state has a responsibility to protect its critical infrastructures, as Cybersecurity is not just a technical aspect but it is directly tied to national security interests.

Second, it is vital to continue the global discussion on building a consensual normative foundation focused on the responsible usage of Cyberspace by states. In light of that, Israel supports elaborating discussions on a global mechanism that will enable Early Warning and Information Sharing, which will improve states' readiness to threats.

Third, we must remember the need to work together with multi-stakeholders, namely, the tech companies, the civil society and academia. We have seen important examples of how private bodies supplied solutions in times of Cyber emergency, and have seen governments who were able to incentivize private companies to create safer products and services that reduce risks.

Fourth, let us remember that we are only as strong as our weakest link and that Cybersecurity is not a task states can accomplish on their own. International cooperation is a vital component of states' Cyber resilience, and thus sharing of Best Practices and experiences - and by that improving Situational Awareness - are all critical to our ability to challenge the risks we face. Israel is working bilaterally with many states with regard to Capacity Building and shares the knowledge acquired in its Cyber ecosystem. Israel also works with international institutions and banks to strengthen Cyber preparedness. We believe Cybersecurity development is not just important to protecting our national systems but is also a tool to promote economic growth with regard to advancing technology and human capital.

While one considers risks in the Cyber domain, it is no secret that Iran poses a real and immediate threat to the stability of the Middle East and the whole world. As you all know, Iran has a clear purpose to spread its extremist ideology and does so by directing and supporting terror. It had recently used Cyber to damage critical infrastructures - in national and private institutions alike – located in different countries in the region, Israel included. Iran does not stop in the Middle East but had expanded its malicious activity to different areas in the world and had only lately targeted Albania, a European NATO member. Iran is an example of a state that uses the vulnerability of the Cyber domain to harm and threat other states, and together we must act to stop it.

In conclusion, we reiterate the urgency of addressing cybersecurity threats to critical infrastructure, and call the UN Security Council to play a larger and more active role in promoting awareness to the risks states face now and will face in the future. The Security Council should also act to promote international cybersecurity cooperation that will enhance preparedness and joint action by states. Israel on its behalf expresses its ongoing commitment to working collaboratively with states and international organizations towards a making a secure, safe and resilient cyberspace for all nations.

Thank you.

Latvia

Latvia welcomes this Arria debate organized by Albania and the US. This meeting continues the important work championed by Estonia to address cybersecurity in the Security Council. Latvia fully supports these efforts. We thank all the briefers for their valuable presentations. Latvia aligns itself with the statement of the EU.

It has been proven over again in the course of history of mankind that discovery and exploration of new realms - be it high seas or space - bring vast opportunities for progress and development, but also reveal new risks and challenges. Although cyberspace is entirely constructed by humans and knows no physical borders, it nevertheless poses similar dilemmas. Furthermore, the cyberspace is a domain which keeps evolving and changing at a rapid pace.

In the context of emerging technologies, such as artificial intelligence and quantum computing, ensuring integrity, rule of law and security of the cyberspace becomes even more important task. Threats in the cyber space despite their digital form are not abstract. They manifest the results of malicious actions by individuals, groups or states. Therefore, the path to achieving secure cyberspace is through ensuring adherence to the same fundamental rules and principles that have been established to uphold peace in the physical world.

As outlined in the concept note of this meeting, the International Law, including the UN Charter in its entirety, is applicable to the cyberspace. This includes Article 2(4) of the UN Charter on the prohibition of use of force. We welcome debates within the UN on how international law applies in cyberspace, which have, inter alia, resulted in establishment of the Framework for responsible state behavior in cyberspace.

We would see a role for the Council to monitor the progress made in implementing the Framework and to hold periodic debates on ensuring a stable and peaceful cyberspace. Equally, we would expect that members of the Council would themselves uphold the norms of responsible behavior to their highest standard. Unfortunately, this is not always the case. Russia in particular has concerning track record in this regard. We recall the attack against Viasat’s KA-SAT network, which facilitated Russia’s launch of the full-scale invasion and war of aggression against Ukraine last year.

Without doubt, the international community can be the most effective in contributing to stability and security of cyberspace, when working together, including in the area of strengthening resilience of critical infrastructure. As a first step, states need to continuously exchange positions on the implementation of the Framework for responsible State behavior in the cyber domain. Second, those in need should receive assistance to improve their cyber defenses and resilience through capacity building programs. Third, with more than 40 billion devices connected to the internet and emerging new technologies, it is clear that private sector, too, should be involved in the debate on cyber security.

For these very reasons, Latvia supports the establishment of the Programme of Action as the first permanent institutional mechanism in the UN that would focus on advancing cyber security in inclusive and transparent way. As we proceed towards establishment of this permanent instrument it would be prudent to also consider developing procedures for its interaction with the Council. Such interaction would help ensure that the Council is kept abreast with the relevant developments in the cyber domain and can take timely decisions.

Guatemala

Muchas gracias por darme la palabra,

Quiero iniciar felicitando a las delegaciones de los Estados Unidos de América y de Albania, así como a Ecuador y Estonia, por organizar esta reunión, y por la elaboración de la nota conceptual. Hemos escuchado atentamente a cada uno de los panelistas y resaltamos que es urgente superar los desafíos actuales relacionados con la ciberseguridad.

Tomando en cuenta los ciberataques que han ocurrido en el pasado, así como su incremento durante la época de la pandemia, valoramos que se aborde este tema en un formato incluyente, en virtud que este flagelo podría afectar a los sectores más vulnerables de nuestra sociedad.

Nuestro país ve con preocupación que las tecnologías emergentes amplien los riesgos y las amenazas en un escenario de crecientes crisis y desigualdades. Es un tema que tiene varias aristas a tener en cuenta, incluidas las consideraciones legales, técnicas y presupuestarias involucradas en el desarrollo y la implementación de estas tecnologías.

Aun cuando el crecimiento acelerado en el uso y dependencia de los sistemas de información digital es evidente a nivel mundial, la ausencia de coordinación, colaboración y cooperación entre las naciones, las instituciones y los sectores, así como una escasa cultura de ciberseguridad en la sociedad, ha limitado el desarrollo de una estrategia holística para atender este flagelo. Es sumamente preocupante que varios Estados estén desarrollando capacidades digitales con fines militares y que el uso de estas tecnologías en futuros conflictos entre Estados, sea cada vez más probable.

Por ello, Guatemala considera valioso fortalecer la labor del Consejo de Seguridad garantizando el pleno cumplimiento de la Carta de las Naciones Unidas y las funciones atribuidas en su mandato respecto a garantizar la paz y seguridad a nivel mundial, contribuyendo a un orden internacional basado en normas y el respeto a los derechos humanos.

En este contexto, es importante que el orden jurídico internacional brinde suficiente certeza a los Estados sobre sus respectivos derechos y responsabilidades, con el objetivo de prevenir conflictos y contar con los mecanismos efectivos para la resolución pacífica de controversias. En tal sentido, se deben continuar con los esfuerzos realizados en el marco del Grupo de Expertos Gubernamentales sobre Ciberseguridad, evitando la duplicación de esfuerzos y avanzando en el Grupo de Trabajo de Composición Abierta sobre Información y las Comunicaciones Tecnológicas 2021-2025, tomando en cuenta las recomendaciones ya realizadas.

Guatemala reitera la aplicabilidad del Derecho Internacional al comportamiento de los Estados en el ciberespacio, incluido el Derecho Internacional Humanitario, así como las normas voluntarias no

vinculantes de comportamiento de los Estados aplicables en tiempo de paz. Por ello, la implementación de las Medidas de Fomento de la Confianza (CBM) siguen siendo cruciales. En este contexto, la principal prioridad para mi delegación es la protección de las infraestructuras críticas y servicios esenciales, garantizando la protección del ser humano.

Respecto a las nuevas tecnologías emergentes, es crucial la supervisión humana, la aceptación de principios comunes y el enfoque humanitario, de seguridad y de perspectiva ética. Es alarmente que la legislación internacional vigente aún no este adaptada a los desafíos que plantea un posible uso de armas autonomas letales (LAWS) y por ello Guatemala favorece la adopción de un instrumento internacional jurídicamente vinculante que prevea la prohibición de éstas armas autónomas para suplir los vacíos de rendición de cuentas existentes. Los riesgos son elevados ante el uso de dichas tecnologías, especialmente dada la naturaleza civil y de doble uso del ciberespacio y las redes digitales, que pueden ser utilizadas por grupos criminales o terroristas.

Exhortamos a los Estados a continuar colaborando con la Comisión de Derecho Internacional, con la finalidad de aclarar dilemas respecto al régimen jurídico internacional aplicable a ataques cibernéticos, la cuestión de la atribución, la debida diligencia y la responsabilidad.

Excelencias,

Ante las brechas existentes entre países en materia de ciberseguridad y defensa, mi país da especial interés a los esfuerzos de creación de capacidades para crear un entorno que permita combatir el ciberdelito, fomentar el desarrollo y contribuir a la paz y la seguridad internacionales. Debemos tomar en cuenta el trabajo de la Oficina de Naciones Unidas contra la Droga y el Delito (UNODC) y dar prioridad al respeto de los derechos humanos en línea, luchar contra la desinformación, el discurso de odio y garantizar la libre expresión, fortaleciendo el acceso a servicios de educación, salud, protección social, entre otros.

Asimismo, mi delegación resalta la importancia del trabajo del Comité Especial encargado de negociar una Convención internacional general para contrarrestar el uso de las tecnologías de la información y la comunicación con fines delictivos. Este futuro instrumento contribuirá a fortalecer la cooperación de los Estados en la lucha contra la ciberdelincuencia, y llenará brechas en la regulación internacional de los crímenes cometidos en contra de estas tecnologías y a través de ellas. Guatemala reitera la necesidad de que este instrumento sea consistente con las disciplinas internacionales en materia de Derechos Humanos, incluida la protección de la privacidad y la libertad de expresión, tanto en línea como en el mundo presencial. Asimismo, este instrumento debe responder a las preocupaciones legítimas de los Estados en cuanto a la integridad de sus infraestructuras críticas.

Guatemala cuenta actualmente con una Estrategia Nacional de Ciberseguridad cuyo principal objetivo es fortalecer las capacidades del país, creando el ambiente y las condiciones necesarias para asegurar

la participación, desarrollo y ejercicio de los derechos de las personas en el ciberespacio. Además, cuenta con un Centro de Respuesta a Incidentes Cibernéticos (CERT), que brinda servicios de auditoría de seguridad cibernética, escaneo de vulnerabilidades y clasificación de alertas. Ambos se lograron con el acompañamiento de la Organización de los Estados Americanos. Valoramos el acompañamiento de la Organización de los Estados Americanos para la creación de capacidades, como una muestra del importante rol de las organizaciones regionales.

Apoyamos un abordaje integral en la creación del Pacto Digital Global, que incorpore los pilares de trabajo de la Organización de las Naciones Unidas, siendo estos: paz y seguridad, derechos humanos y desarrollo sostenible. En esa línea, apoyamos la transferencia de tecnología y la promoción de un entorno digital inclusivo y abierto, generando resiliencia incluso ante incidentes de esta naturaleza.

Finalizo recordando que estamos ante un momento decisivo para dar soluciones transformadoras a los retos interconectados, entre estos los vinculados a la seguridad regional y transnacional. Nuestro futuro dependen de ello.

Muchas gracias

Italy

Mesdames Presidents,

I would like to strongly commend Albania, Ecuador, Estonia and the United States for organizing this important and timely meeting. I also would like to thank High Representative Nakamitsu and the representatives of the civil society for their insightful briefings.

While Italy aligns itself with the statement delivered by the European Union especially when it conveys our solidarity to the cyberattacks Albania suffered last year, I wish to add some additional remarks in my national capacity.

Cyberattacks by State and non-State actors are on the rise, as proven also by the full scale Russian aggression against Ukraine exploiting the cyberspace. Critical infrastructures and essential services are increasingly at risk of malicious activities. Urgent action is therefore needed to tackle such threats and to ensure the stability of cyberspace. We praise the members of the Security Council for their continuing attention to this matter. In our view, cyber security cannot be addressed separately from old and emerging threats to world stability and peace.

The pace of digitalization is picking up at a global level and, along with the benefits associated with this development, comes the challenge to maintain cyberspace as a global, open, and stable domain. The surge in incidents, at times targeting critical infrastructures and imposing high costs to world economies, is deplorable. Some of the attacks offered a glimpse into the loss of human life that these actions can cause. The destructive potential of the misuse of new technologies is becoming more and more evident and so is the need to keep them in check.

This also applies to Artificial Intelligence. Italy recognizes that AI and other emerging technologies are key drivers of economic progress. Given its likely impact on global economy and our everyday lives, it is imperative that we work towards a human-centric and innovation-friendly approach to AI based on fundamental rights and fundamental values such as democracy and the rule of law.

Italy believes that the UN are the best positioned for this task and for promoting cyber peace and stability. While underlining the applicability of international law in cyberspace, including IHL and human rights law, the importance of adhering to norms of responsible State behavior, and the usefulness of confidence building measures as a practical means to prevent conflict, we also wish to highlight the important role that regional organizations can exert in the field of cybersecurity.

As staunch supporters of multilateralism, we encourage the dialogue between the UN and regional organizations also with regard to cybersecurity. In an increasingly interconnected world, dialogue becomes even more essential to promote shared understandings and increase opportunities for

cooperation. In this spirit, we support the dialogue of the EU with the UN and with regional organizations, notably the AU, ASEAN-ARF and OSA.

Through regional organizations, Member States can maximize their own bilateral contacts, sharing best practices and lessons learned, thus ensuring that regional approaches do not diverge. Further efforts should be dedicated to mechanisms for the peaceful settlement of disputes, as well as to initiatives to develop cyber-diplomacy and cyber mediation.

We believe that the cyber domain should stay open, free, secure and stable, as a means for States to implement policies that will enable societies to thrive and guarantee sustainable development for all, contributing to the attainment of the SDGs. The importance of capacity building cannot be underestimated, as it guarantees homogeneous resilience of States, increases awareness and stimulates the development of capabilities.

Much more needs to be done in this sector, and we believe that the Programme of Action to Advance Responsible State Behavior in Cyberspace can represent the priority platform from which to coordinate and promote this endeavor. The PoA can also be the forum where the multistakeholder approach is shaped and Public-Private Partnerships are developed.

It is our collective interest that the UNSC will remain focused on cyber issues, monitor progress and be ready to call non-compliant States to their obligations. Hopefully such instances will be very few as Member States converge on the need to dedicate time and effort to a positive cybersecurity agenda – one which develops trust, transparency and inclusiveness.

Thank you, Mesdames Presidents.

Côte d'Ivoire

Monsieur le Président,

Ma délégation salue l'Albanie et les Etats-Unis d'Amérique pour l'initiative de ce débat sur un enjeu sécuritaire de premier ordre qu'est la sureté de l'espace numérique.

Je tiens à adresser mes remerciements à Madame la Haute Représentante aux Affaires de Désarmement et aux autres briefers pour leurs interventions édifiantes.

Monsieur le Président,

L'utilisation malveillante des technologies de l'information et de la communication par des acteurs étatiques et non étatiques, y compris les attaques contre les infrastructures critiques et les services essentiels, est une menace croissante, surtout depuis la pandémie de la COVID-19 et dans le contexte des tensions géopolitiques actuelles.

Face à ce phénomène qui compromet la paix et la sécurité mondiales, la communauté internationale n'est heureusement pas démunie. En effet, la réflexion de plus d'une décennie menée sous les auspices des Nations Unies sur la question, a permis de mettre en place un cadre de comportement responsable des Etats dans le cyberespace.

L'enjeu pressant aujourd'hui est l'application effective de ce cadre de référence, visant à favoriser un espace numérique pacifique et stable. Il est donc primordial que chacun des acteurs œuvre à cet objectif.

A cet égard, le Conseil de sécurité, garant du maintien de la paix et de la sécurité internationale, a un important rôle à jouer, en particulier, dans la mise en œuvre du principe de l'applicabilité du droit international au cyberespace, y compris la Charte des Nations Unies, essentiel pour instaurer un environnement numérique sûr.

Le Conseil peut également soutenir la mise en pratique des normes volontaires de comportement responsable des Etats en tant de paix, de même que la prise de mesures spécifiques de confiance et de coopération internationale, notamment en matière de renforcement des capacités des acteurs les plus vulnérables.

Monsieur le Président,

La volonté de mise en œuvre concrète du cadre de comportement responsable par mon pays s'est matérialisée par l'adoption par le Gouvernement ivoirien, le 22 décembre 2021, de la Stratégie

Nationale de Cybersécurité 2021-2025. La protection des infrastructures critiques en constitue un des piliers principaux.

En outre, la Côte d'Ivoire participe pleinement à l'Assemblée générale, aux délibérations du Groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation. Au regard des défis liés aux propriétés en évolution constante des technologies numériques, elle est favorable à la mise en place d'un mécanisme permanent, inclusif et orienté vers l'action, qui contribuerait à consolider le cadre actuel.

C'est le sens du plein appui de mon pays à l'établissement d'un Programme d'action destiné à promouvoir le comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale, en co-sponsorisant la résolution y relative. Notre plaidoyer est qu'une vision collective partagée se dégage sur le bien-fondé d'un tel Programme d'action et sur les modalités de sa mise en place.

Je vous remercie.

Qatar

السيد الرئيس،

نشكر الدول الراعية لهذا الاجتماع على إتاحة الفرصة لنا للمشاركة في مناقشة هذه المسألة الهامة. كما نقدر الإحاطات القيّمة من الممثلة السامية السيدة ناكاميتسو، وكذلك السيدة سخاكا، والسيدة ماكوماني.

مع التسارع الهائل في تطور تكنولوجيا المعلومات والاتصالات والترابط الرقمي العالمي والاعتماد على التكنولوجيا الرقمية في مختلف مناحي الحياة، يزداد التهديد الذي تشكله إساءة استخدام الفضاء الإلكتروني، سواءً من قبل الجهات الفاعلة الحكومية وغير الحكومية بما فيها الجماعات الإرهابية والإجرامية. وهذا التهديد يشكل خطرا أكبر عندما يمس الخدمات الرقمية الحساسة والبنى التحتية الأساسية، التي قد يؤدي تعطيلها إلى آثار تهدد الأرواح والصحة والرفاه. ولا يوجد أي بلد في منأى عن هذه التهديدات، التي قد تشكل تهديدا للسلم والأمن والاستقرار إقليميا ودوليا، الأمر الذي تدركه بلادي جيدا خاصة وأنها تعرضت بالفعل لقرصنة إلكترونية كانت لها آثار خطيرة.

ولذلك، تستحق هذه المسألة الاهتمام الواجب من قبل الدول والأمم المتحدة، وفي هذا الخصوص ننوه بالاهتمام الخاص الذي أولاه الأمين العام للأمم المتحدة إذ جعل من ضمن أولوياته العمل على تعزيز بيئة سلمية لتكنولوجيا المعلومات والاتصالات.

السيد الرئيس،

إن حماية البنى التحتية الحرجة من الهجمات الإلكترونية يتطلب دراسة التهديدات والثغرات ومواكبة التطور التكنولوجي السريع، ووضع استراتيجيات إقليمية ووطنية متوائمة مع مبادئ التعاون الدولي وتبادل الخبرات وأفضل الممارسات. وتعد الاستراتيجيات الوطنية مهمة لتوجيه العمل والتنسيق بين أصحاب المصلحة المعنيين، بمن فيهم القطاع الخاص الذي يعتبر دوره محوريًا فيما يتعلق بالتكنولوجيا الرقمية. وفي هذا الصدد، تسعى دولة قطر إلى توفير بيئة سيبرانية آمنة وقوية على المستوى الوطني، وقد اتخذت إجراءات حثيثة لتسخير أحدث التقنيات للحفاظ على أمن المعلومات والبنى التحتية، وطورت من الخبرات والقدرات في مجالات مثل منع الهجمات الإرهابية على الأهداف غير المحصنة والمنشآت الرياضية.

وفيما يتعلق بالأُطر الدولية، هناك حاجة لبحث انعكاسات إساءة استخدام الفضاء السيبراني على الاستقرار والوقاية من النزاعات، وما يمكن اتخاذه من جهود جماعية لتعزيز الاستخدام السلمي للفضاء الإلكتروني والتقنيات الرقمية المتقدمة، وتعزيز البيئة الأمنية الإقليمية والدولية لمواجهة محاولات إساءة استخدام هذه التكنولوجيات. وينبغي إيلاء الاعتبار لانطباق القانون الدولي على استخدام الدول لتكنولوجيا المعلومات والاتصالات، ومواصلة الارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي، والنظر في اعتماد صك دولي مُلزِم للحفاظ على أمن المعلومات علاوة على المعايير والقواعد والمبادئ للسلوك المسؤول في استخدام تكنولوجيات المعلومات والاتصالات بغية الحد من المخاطر التي تهدد السلام والأمن والاستقرار على الصعيد الدولي.

وفي الوقت نفسه، نؤكد على أن من الضروري في هذا المجال مراعاة سيادة القانون وحقوق الإنسان والحريات الأساسية والتدفق الحر للمعلومات في بيئة رقمية مفتوحة وآمنة ويمكن للجميع الوصول إليها.

وختاما، نعيد التأكيد على التزام دولة قطر بالمساهمة في الجهود العالمية لضمان أن يكون الفضاء السيبراني وسيلة للتقدم والرفاه، والحد من التهديدات التي قد يشكلها.

وشكرا لكم.

The Kingdom of the Netherlands

Madam President

Allow me to thank the organizers, briefers and many speakers for joining this important discussion.

The rapid digitalization of our global society is beyond any measure. From our personal phones to expansive industrial control systems; digital technologies drive human, economic and social development at an unprecedented pace.

Besides many opportunities, the reliance on digital technologies also makes us vulnerable. State and non-State actors are using technologies for malicious purposes – conducting harmful cyber campaigns that are increasing in scale, severity, and sophistication.

And we've seen plenty of examples in the recent past: from Costa Rica to Albania, from the US to my own country.

These examples remind us that cyber incidents may rise to the level of international security, thereby warranting the attention of the Security Council. Furthermore, the misuse of new technologies, including artificial intelligence and eventually quantum computing, may exacerbate these challenges.

Madam President,

The international community has not been sitting idly by. Under the First Committee of the General Assembly, a cumulative and evolving framework for responsible State behavior has emerged. One that all States have committed to be guided by, in their use of ICTs. This is no small feat.

Let me make three points in this regard:

Firstly, States agreed by consensus that international law, in particular the Charter of the United Nations, applies in cyberspace. Bearing primary responsibility for the maintenance of international peace and security, the Security Council should address severe international cyber incidents and take appropriate action, including through its role in the peaceful settlement of disputes.

Secondly, in the current geopolitical environment, States should redouble their efforts to build confidence in the of use these technologies in the context of international security. Confidence-building measures can prevent misinterpretation and unintended escalation arising from an ICT incident. In this vain, the Netherlands fully supports the establishment by the OEWG of a global Point of Contact Directory.

Thirdly, that the normative framework we all agreed to is only a first step. More work is to be done so that all States can observe and implement the framework, while simultaneously continuing discussions to further develop it. To this end, the Netherlands supports the Egyptian-French initiative to establish a Programme of Action to advance responsible State behaviour in cyberspace. As a permanent, inclusive and action oriented platform, the PoA could also bring in the unique perspectives of non-governmental stakeholders in the cyber domain.

To conclude, Madam President, while it is incumbent on the international community to harness the benefits of ICTs against cyber threats, we must approach broader cyber challenges holistically. Our efforts to advance stability in cyberspace must go hand in hand in with bridging the digital divide, respecting human rights and building resilient cyber infrastructure that helps drives sustainable development.

Thank you.

Sri Lanka

Excellencies, distinguished delegates, ladies, and gentlemen,

As the frequency and complexity of cyber security threats are expected to continue growing and evolving, hence, Sri Lanka recognizes the importance of taking proactive measures to mitigate cyber security risks and effectively address these challenges.

We believe that organizing this meeting at this particular moment to discuss the vital matter of state responsibility and responsiveness in countering cyberattacks on critical infrastructure is highly appropriate. In today's interconnected world, where our reliance on digital systems is extensive, safeguarding critical infrastructure against cyber threats has become an urgent priority for maintaining international peace and security.

It is crucial for states to take responsibility in protecting their critical infrastructure against such malicious activities, while recognizing the Security Council's emphasis on the significant threats posed by cyberattacks targeting critical infrastructure. These threats not only undermine the functioning of essential services and national security but also jeopardize the overall stability of states. We strongly support the call for enhanced international cooperation and dialogue to foster the development of effective strategies and responses to combat these cyber threats.

Like many technologies at our disposal, ICTs are dual use technologies but with a capacity to affect positively or negatively all three pillars of our United Nations and thereby all walks of life. Therefore, building digital trust and security lie at the core of efforts to reap the benefits of the digital domain and utilize it for development gains, including the 2030 Agenda.

Sri Lanka unequivocally condemns all forms of cyber attacks on critical infrastructure, which have the potential to disrupt essential services, undermine public safety, and cause economic damage. Such attacks violate international law and threaten the stability and security of states and the global community as a whole. We endorse this meeting as a platform for member states, experts, and stakeholders to share their experiences, insights, and best practices regarding the responsibility and responsiveness of states to cyberattacks on critical infrastructure. It provides an opportunity to highlight the challenges faced by states in protecting their infrastructure and explore potential solutions to enhance resilience and mitigate the impact of such attacks.

In today's interconnected world, where our societies place great reliance on digital systems, the protection of critical infrastructure against cyber threats has become a top priority for ensuring international peace and security. Needless to say consequences of cyberattacks on vital infrastructure can be far-reaching, impacting essential services, compromising national security, and destabilizing entire states.

Addressing the guiding questions as a whole. What are the possible actions the Security Council can undertake to address cyber threats and cyberattacks against critical infrastructure by States?

In order to protect critical infrastructure from malicious activities, states must take on the responsibility of safeguarding them. The Security Council's recognition of cyberattacks targeting critical infrastructure as significant threats highlights the urgent need for action. These attacks not only disrupt essential services but also directly undermine the stability and sovereignty of nations. However, it is important to acknowledge that reaching Article 39 determinations and recommendations for the use of force is a highly challenging process. Lengthy deliberations and potential veto power by permanent Security Council members make it difficult to obtain timely responses. Given the intricate and ambiguous nature of cyber attacks, it is reasonable for states to consider exercising their right to self- defense to address such incidents. In such cases, strengthening the local legal framework becomes crucial.

The Security Council plays a vital role in ensuring a secure and peaceful cyberspace while preventing conflicts from malicious use of information technologies. This includes advocating for responsible state behavior, facilitating diplomatic efforts, and supporting cyber capacity-building. By encouraging states to adhere to norms of responsible behavior, refraining from activities that harm critical infrastructure, and promoting trust-building dialogues, the Security Council can prevent cyber conflicts. Additionally, it can support member states in enhancing their cyber security capabilities through technical assistance and capacity-building programs. Strengthening cyber security capacities reduces the potential for conflicts arising from cyber activities. The Security Council's adoption of resolutions, promotion of responsible state behavior, support for diplomatic efforts, and encouragement of cyber capacity-building are crucial for addressing cyber threats and preventing conflicts in the use of information and communication technologies.

States have various mechanisms at their disposal to notify a second state of malicious activity originating from its territory. These include diplomatic channels, established communication channels between cyber security agencies or CERTs, and international platforms and organizations specializing in cyber security. Upon receiving a notification of malicious activity, the second state has a responsibility to promptly and thoroughly investigate the reported incident. They should assess the credibility of the information provided and take appropriate measures to mitigate and respond to the cyber threat. Cooperative and transparent communication with the notifying state is crucial to exchange relevant information, facilitate investigations, and coordinate actions.

Victim states effected by cyberattacks can request assistance from other states through established mechanisms of cooperation and mutual assistance. This can involve bilateral or multilateral agreements, regional security frameworks, or invoking international legal frameworks like Article 51 of the United Nations Charter. Victim states may seek technical expertise, intelligence sharing, forensic analysis, or operational support from other states to effectively respond to the cyberattacks.

Enhancing the partnership between public and private entities in several ways can facilitate open and constructive dialogue, enabling participants to exchange ideas and perspectives, leading to mutual understanding and trust. It can promote problemsolving and consensus-building by bringing together diverse stakeholders to collaboratively address complex issues and generate actionable recommendations.

We must allow private entities to contribute their expertise and perspectives to policy discussions, influencing the shaping of policies and regulations that impact their industries and sectors and can act as a confidence-building measure, particularly in situations where trust is lacking or relations are strained, by fostering dialogue and cooperation in a non- official setting. Moreover, promoting capacity building and knowledge exchange through workshops, seminars, and joint projects, leading to improved capabilities and outcomes is essential to emphasize and complement official diplomatic channels rather than replace them, working in coordination with government efforts to ensure coherence and effectiveness in addressing broader policy goals.

Venues and mechanisms for closer public-private partnerships in cyber security are vital for a concerted defense against cyberattacks. These include information sharing platforms, joint exercises and training, public-private partnerships, regulatory frameworks and standards, and sector-specific collaboration. Information sharing platforms facilitate real-time threat intelligence exchange and collaboration. Joint exercises and training programs enhance preparedness and promote collaboration between public and private entities. Public-private partnerships involve formal collaborations between government agencies, CERTs, critical infrastructure operators, and cyber security companies for information sharing and coordinated incident response. Regulatory frameworks and standards encourage cooperation while protecting sensitive information and privacy. Sector-specific collaboration, such as ISACs and cyber security forums, enables threat intelligence exchange and coordinated responses within specific industries. Fostering public-private partnerships through these mechanisms is crucial for effective information sharing, coordinated responses, and a collective effort to protect critical infrastructure from cyber threats.

As we know AI systems like other information technologies can be a target of and tool for criminal activity. It must be observed that both are within the scope of the 2001 Budapest Convention on cybercrime, and have also being dealt within the Council of Europe framework with active participation of non-member states from the outset. While universal ratification may be possible for political reasons, one of the principal objectives of the treaty is to harmonize What are the possible venues and mechanisms for a closer partnership between public and private entities for concerted and coherent defense and responses to cyberattacks?

Domestic substantive and procedural criminal law as a precondition for more effective international cooperation. Being the first and most widely ratified multilateral treaty on cybercrime this treaty can

achieve its objectives we believe without formal global participation, as it simply serves as a model instrument.

The provisions have been supplemented by guidance notes in order to facilitate the effective use of the Convention.

The convention also catches up computer related forgery, computer related fraud, offenses related to child pornography and offenses related to the infringement of copyright. It is interesting to note that like all other criminal offenses, offenses contained in the convention require criminal intent that may be difficult to prove. It is our respectful view that this position must be revisited with a view to examine the proposition whether the concept of fixed liability can be used, thereby calling for an explanation from the respondent with regard to a matter that is particularly within his knowledge.

North Macedonia

Mr. Chairman,

Thinking about the future, we could not avoid thinking about the future of our Cyber space. This new space, created in common work of the world scientific community, is our main hope, in confronting the contemporary challenges. We have already all agreed that the progress in science and technology offers the broadest positive opportunities for the further development of civilization. We need to further encourage and empower the science in order to maximize the benefits of the fourth industrial revolution.

Mr. Chairman, the Secretary General in his new agenda for peace is recognizing the cyber related risks as one of the main strategic risks we are facing today. Confronted with the new situation when new technologies are placing the capacity to disrupt global stability in the hands of many actors, the responsibility of the UN member states is growing. My government has included in its risks strategy activities to prevent the misuse of new technologies. We consider that the cyber-attacks on critical infrastructure should be addressed by the Security Council as a threat for maintaining international peace and security. We are encouraging further development of norms for responsible state behavior in cyber space. We believe that the Security Council should play an important role in encouraging actions from all stake holders to jointly build an environment for maximum use of the benefits of new technologies.

We consider that the current security situation in the world is demanding Security Council activity also in the sphere of cyber space, identification of the malicious actors and use, as a response to the threats to international peace and security, the UN Charter and already established international law.

Mr. Chairman I would like to use this opportunity to congratulate our neighbor Albania, member of the Security Council and the United States for convening this Arria-formula meeting and allowing a great number of states to address this important security issue.

I thank you.

Bangladesh

Distinguished Co-chairs,

I thank the Permanent Missions of Albania and United States for organizing this meeting. I also thank the briefers for their valuable insights on this important topic.

Let me begin by sharing our own experience of devastating cyber-attack in 2016, when more than US$ 80 million from Bangladesh Central Bank was siphoned by hackers. Eventually, a large portion of the money reportedly reached to another country's casino system through its banking channel. The breach of the supposedly secure global money transfer system by hackers is deeply concerning.

The 2023 Global Cybersecurity Outlook report reveals that 93 percent of participants anticipate a "catastrophic" cyber security event in the next two years. Emerging technologies like artificial intelligence further amplify these threats.

Co-Chairs,

It is projected that by 2025, cybercrime will cost the global economy a staggering $10.5 trillion annually. These figures underscore the urgent and significant nature of the issue.

To answer some of your guiding questions let me highlight the followings:

First, cybercrime and cybersecurity rank as the 8th most severe risks according to Global Risks Report 2023, threatening international peace and security. This global threat necessitates a coordinated and enhanced response.

Therefore, the Council can play a prudent role in countering this urgent challenge by promoting international norms, fostering trust between states, and facilitating dialogue and cooperation to prevent conflicts arising from malicious use of ICT.

Second, addressing cyberattacks on critical infrastructure requires a collaborative approach involving states, public and private entities, and international organizations. Public-private partnerships are crucial in developing effective strategies to combat cyber threats and protect critical infrastructure.

In this regard, we call for a new social contract for the digital age that redefines the relationship between public and private sectors and establishes new obligations. Private sector firms must prioritize security and resilience in their hardware manufacturing and software development, while the government should provide support.

Third, Bangladesh emphasizes the applicability of international law, including the UN Charter, to maintain peace, stability, and an open, secure, stable, accessible, and peaceful ICT environment. However, we acknowledge existing legal gaps, such as the attribution of cyberattacks, State responsibility threshold, and the use of force in cyberspace. The Council could complement the work of GGEs and OEWG on ICT by enhancing understanding of international law in cyberspace.

Fourth, Closing the Skill Gap demands collective action, particularly in the global south. This includes enhancing digital literacy, technical skills, promoting cybersecurity education, and fostering international cooperation. The Council could play a vital role in promoting confidence building measures and effective information sharing to mitigate cyber threats.

Finally, Bangladesh emphasizes a comprehensive approach to safeguard critical infrastructure and address evolving cyber threats. We have implemented the Bangladesh Cybersecurity Strategy 2021-2025; and achieved the 11th rank in the Asia Pacific Digital Security Index. However, more is needed.

We seek robust international cooperation, harnessing digital technology, and upholding international law for a safer and resilient digital world.

I thank you.

Ukraine

Madame Chair,

Our delegation thanks Albania and the United States and all co-sponsors for convening this timely meeting on cybersecurity. We also extend our appreciation to all briefers for their remarks.

We are witnessing a dramatic increase of malicious cyber activity directed at critical infrastructure, including against the infrastructure delivering essential services to the public, such as medical facilities, water, energy and sanitation infrastructure.

During the last decade, Member States have agreed on a normative framework for more secure, peaceful and stable cyberspace. Unfortunately, concrete States do not adhere to this framework. We are concerned that they deliberately use non-State actors by allowing them to conduct malicious cyber activities from their territory with impunity.

Ukraine has been facing massive cyber-attacks for 9 years in a row. Since 24 February 2022, when russia started its full-scale invasion of my country, the number of cyber-attacks against Ukraine has only increased.

A majority of malicious cyber operations against Ukraine are carried out by hacker groups affiliated with the russian federation. The main targets are governmental entities, banking structures and hospitals. The primary goal is to undermine public confidence in capabilities of the public authorities, the Security and Defense Forces, as well as to spread fear and disorientation among people.

Notwithstanding the large-scale cyber activities against my country, thanks to the support of our partners, we have demonstrated great cyber-resilience throughout last year and up till now.

There is a strong need to continue promoting implementation of the agreed norms of responsible State behaviour and deepen our understanding on how international law applies in cyberspace. As one of co-sponsors of the Programme of action, Ukraine believes that the establishment of this framework within the UNGA mandate is the best way to move towards responsible implementation of already agreed set of norms.

Ukraine supports the continued exchange of information and best practices within the UN and between States at a regional and bilateral level. Public-private partnership can also contribute to reinforcing State's capability to oppose cyber threats, building human resources capacity, as well as strengthening resilience.

We regret that the misuse of veto power prevented the Security Council from taking decisive actions to maintain international peace and security has also affected the Council's response to cyber threats.

To conclude, States should work together to hold accountable those Members, who act contrary to the framework of responsible behavior in cyberspace.

Thank you.

Bahrain

At the outset, I would like to thank the Permanent Missions of Albania, Ecuador, Estonia, and

the United States for organising today's meeting, as well as the briefers for their important remarks.

As a responsible member of the international community, the Kingdom of Bahrain recognises the importance of ensuring a secure and peaceful cyberspace, as well as preventing conflicts arising from malicious activities in cyberspace. Indeed, the rapid development of digital technology has changed the way the world operates and impacted all aspects of modern life. While this development brings benefits to all of us, it also comes at the cost of exposing us to a wide range of threats. It is imperative for the international community to work together to address these challenges.

In this regard, the Kingdom of Bahrain wishes to stress the following points:

1. There is a need to establish international norms and standards for cyberspace based on the principles of international law, including the Charter of the United Nations, and respect for human rights and fundamental freedoms. They should also be designed to promote responsible behaviour in cyberspace and prevent malicious activities.
2. It is crucial to promote transparency and confidence-building measures between States in cyberspace. This includes the establishment of channels for the notification of malicious activities and the sharing of information and best practices.
3. Due to the existing digital divide, there is a growing need for cooperation in preventing and responding to cyberattacks. We believe that there should be a clear mechanism that states can utilise to request assistance from other States in these matters.
4. It is important to foster a closer partnership between public and private entities for concerted and coherent defence and responses to cyberattacks. This partnership can support the development of effective cybersecurity strategies and solutions, including sharing intelligence and best practices.

In conclusion, the Kingdom of Bahrain stands ready to work with other States to establish international norms and standards for cyberspace, promote transparency and confidencebuilding measures, and foster cooperation in preventing and responding to cyberattacks.

I thank you.

Pakistan

Pakistan welcomes the convening of this important debate on Responsibility and Responsiveness of States to Cyber attacks on Critical Infrastructure convened by the United States and Albania.

Mr.President,

Cyber warfare has emerged as a new domain of warfare. Conducted by both state and non-state actors alike, it is diminishing trust and confidence among States, lowering the threshold of war and undermining international peace and security.

Cyber attacks are taking place with an increased intensity across the entire spectrum of our social, economic and political domains, with devastating impact on critical infrastructure and societies. Dissemination of fake news and hate crimes through digital platforms is just one manifestation of this new form of warfare.

Against this backdrop, ensuring the peaceful use of ICTs and preventing cyber warfare is the critical challenge of our time.

We appreciate the efforts undertaken by the United Nations through the establishment of the GGEs and OEWGs to evolve consensus on how to mitigate this threat and chart a way forward through an inclusive and consensual processes.

Mr. President,

Our fundamental objective is to create a safe, secure, stable and peaceful ICT-environment. We all agree that the international law particularly the Charter of the UN applies to the Cyber domain.

The UN Charter provisions particularly those relating to sovereignty, territorial integrity, non-interference in the internal affairs of States and peaceful settlement of disputes lay down a solid framework to regulate the activities and address the threats and challenges falling within the domain of cyber space.

Yet, we have to address the issues relating to attribution and enforcement of law.

Since the Council has yet not taken this issue on its agenda, and also currently suffers from a paralysis, it would be a challenge for the Council to pronounce on these issues objectively even if it considers addressing threat to peace and security at some stage in near future.

It would therefore be salient to suggest that only a legally binding instrument tailored exclusively to address the specific conditions that address the interests of all states would be the best way forward.

At the same time, capacity building has a crucial role to play to enable the Member states to understand and respond effectively to the challenges emanating from cyberspace and impacting the international security.

Therefore, we call upon the international community, especially the developed world, to provide fair, equitable and unconditional technical assistance, capacity-building support, and technology transfers to assist States, especially those with limited resources, in strengthening their cybersecurity infrastructure.

I thank you.

Germany

Mister Chairman,

Germany wishes to thank Albania and the United States for putting this important topic on the agenda.

The increase in state sponsored malicious cyber activity is extremely worrying. In our view, it undoubtedly represents a significant threat to international peace and security.

It is enough to look at Europe in 2022. We have seen Russia's unprecedented cyberwar against Ukraine with significant spill-over effects into European networks. But also Albania and Montenegro experienced massive cyber-attacks crippling core public institutions. Cyber incidents of similar magnitude have hit other world regions, causing considerable economic damage.

The gravity of these incidents must serve as an urgent call to action. The Council needs to confront the realities of a new conflict that is taking place in the cyber space.

In this regard, we would like to acknowledge the leadership role of Estonia. The high level open debate on cyber security held in this Council in June 2021 was a milestone.

Mr. Chair,

We would like to set out three areas, which the Security Council should explore in order to make an effective contribution to safeguarding international peace and security and promote an open, secure, stable, accessible and peaceful cyberspace.

These proposals are based on our firm belief that international law fully applies to the cyber domain, without any reservation. In this regard, the UN Charter fulfils a core function when it comes to the maintenance of international peace and security—also in relation to cyber activities.

First, we believe that the Security Council should assume an investigative role. Art. 34 of the UN Charter clearly authorizes the Security Council to investigate into any situation that might lead to international friction or give rise to a dispute. The Council can also act in a more general sense, by holding regular in-depth discussions or providing analyses of risks emanating from cyber-attacks.

Second, the Security Council should engage in dispute resolution, deriving from its tasks enshrined in Chapter VI of the UN Charter. Where required, a more robust response to maintain or restore international peace and security must be considered as well.

Third, and finally, Germany sees a strong potential of the Security Council in trust-building.

By keeping cyber issues on its agenda, by investigating specific situations of cyber conflict or by facilitating their peaceful settlement, the Council can contribute to building the evolving framework of responsible state behavior in cyber space, all based on international law, complemented by voluntary UN norms, and confidence building measures.

I thank you, Mr. Chairman.

Viet Nam

Distinguished co-Chairs,

At the outset, I would like thank the United States and Albania for convening this meeting. I also appreciate the briefers' valuable information and insights.

Co-Chairs,

The digital revolution has brought about remarkable advancements for our societies. Along with the progress, we have also been faced with an array of complex challenges. One of the most pressing issue is the escalating threat of cyberattacks against our critical infrastructure. A successful cyberattack can have far-reaching implications, from paralyzing economies to jeopardizing national security.

Given the nature of cyber attacks, no country is immune from these threats. Viet Nam, unfortunately, is no exception. Our critical infrastructure systems have fallen prey to multiple incidents and considerable damages have been inflicted.

Meanwhile, the current state of cyber defense is lagging behind the increasingly advanced capabilities of attackers. The high degree of complexity and interconnectivity in our critical infrastructure systems makes them not only vulnerable to attacks but also more difficult to defend.

Addressing this complex issue requires a multi-faceted approach. Within the United Nations, this subject has been extensively debated, particularly within the ongoing OEWG on ICTs. And given its mandate on international peace and security, the UN Security Council should give more attention and priority to this issue.

At the policy level, governments must prioritize cybersecurity in their national agendas. Existing legislation needs to be bolstered to enforce mandatory cybersecurity standards and guidelines within critical infrastructure sectors. In this regard, Viet Nam took a significant step in 2018 with the enactment of the Cybersecurity Law that embraces a comprehensive, society-wide approach to the protection of critical infrastructure. Promoting cybersecurity awareness and literacy is essential. It is also important to foster public-private partnerships as private entities often own and operate significant portions of these critical systems. Governments should also take bolder steps to assist these entities in building their capabilities to safeguard their systems against cyberattacks.

International cooperation is another crucial element. As outlined in the UNGA Resolution 70/237, and other relevant agreements, Member States need to work together in good faith and promote collective efforts. Even in the absence of bilateral agreements, any State cognizant of malicious activities originating from its territory should promptly notify the targeted State. The receiving State is also responsible for collaborating with the notifying State. This cooperation should include sharing pertinent information and mutual legal assistance.

Last but not least, we need to shift from a reactive to a proactive approach. Investments in state-of-the-art cybersecurity technologies, such as AI and Machine Learning, can significantly bolster these efforts, enabling the prediction and prevention of attacks before they inflict damage.

I thank you!

Czechia

Chair,

Recent developments clearly demonstrate that cybersecurity is an area that needs to be given increased attention. The number of cyber-attacks continues to rise, as does their severity. It is a global problem that requires a global solution.

Czechia denounces unequivocally the use of cyberspace for any wrongful acts. We believe that cyberspace should be a domain of peace, cooperation, and innovation, where democracy, rule of law, and fundamental freedoms apply.

The fight against malicious cyber activity needs more intensive international cooperation to maintain a free, open, safe, secure and stable cyberspace. We therefore need to build strong partnerships across existing political and regional divides to tackle cyber threats.

When it comes to cyberattacks, we are all in the same boat. All of us are vulnerable to ransomware, cybercrime, and increasingly reckless attacks on critical infrastructure. In recent years, Czechia has been repeatedly advocating in different UN fora that attacks directed against medical facilities – that are considered as part of the critical infrastructure - are one of the most alarming and reprehensible. We know what we are talking about as some of our medical facilities have been subjected to cyber attacks.

Although states have conducted some of the most concerning malicious cyber activities, cyber criminals as non-state actors seeking financial and other kinds of gain also conduct a wide range of disruptive, destructive, or otherwise destabilizing cyber activities.

The UN's unique convening power can play a key role in cybersecurity. Therefore, Czechia strongly supports and actively participates in processes within the UN dealing with cybersecurity – these are the Open Ended Working Group for cybersecurity and Ad-hoc Committee on Countering the Use of Information and Communication Technologies for Criminal Purposes. Both of these working groups have been endorsed by consensus at UNGA.

We believe that the UN Security Council should also help to promote the framework of responsible state behaviour in cyberspace, which includes the applicability of international law, adherence to voluntary norms of state behaviour during peacetime, and the undertaking of practical cooperative measures between states. The Security Council and GA processes should be complementary in advancing goals such as fostering stability and accountability in cyberspace.

Finally, I would like to draw your attention to the fact that Russia's unjustified war against Ukraine has brought back the threat of malicious cyber activity as a tool of state-on-state warfare. This war has greatly increased the frequency and intensity of cyberattacks, targeting not only the critical infrastructure of Ukraine, but also of the states that support Ukraine. We strongly denounce such attacks.

Colleagues,

We know full well where the UN Charter, international law and international humanitarian law stand on the use or threat of force, or the principle of proportionality and humanity. These rules and principles apply to states' activities in cyberspace as well.

I thank you.

The Maldives

Mr. President/Chair, members of the United Nations Security Council, and esteemed colleagues,

My delegation extends its appreciation to the Albania, Ecuador, Estonia, and United States, for convening this meeting. We also thank the briefers for their insights.

In our interconnected world, the integrity of cyberspace is paramount to the peace, security, and prosperity of all nations, large and small. We believe that the Security Council, as the custodian of international peace and security, has a big part to play in shaping a secure and peaceful cyberspace.

Mr. President/Chair,

Information technology is revolutionizing modern life by fostering innovation, cultural exchange, and free expression, thus bringing the global community closer. However, challenges to this vision have been raised, with increasing misuse of cyberspace for malicious activities, targeting critical infrastructure, citizens, and undermining peace and security.

In the wake of the adoption of General Assembly Resolution 70/237, Member States have committed to a framework comprising 11 voluntary norms intended to steer state behavior in cyberspace. This framework has been highlighted in three consecutive UN Groups of Governmental Experts' reports from 2010, 2013, and 2015. In its latest report, the Group underscored the significance of adhering to international law and promotion of responsible use of cyberspace.

The report also highlighted the protection of critical infrastructure, capacity building, and the implementation of confidence-building measures. In this context, my delegation firmly believes that fostering dialogue and implementing trust-building measures among states represents a vital area where the Security Council can play an active role.

Mr. President/Chair,

The Maldives lacks the capacity to protect against and respond to major cybersecurity incidents. As a small island developing State (SIDS), our limited resources, geographical isolation, access to technology and human capital bring unique challenges to the implementation and further development of a robust Cybersecurity infrastructure. In this context, my delegation advocates for dedicated support mechanisms that would give SIDS access to financial resources, technical support for increasing their capability, and support for monitoring and reporting malicious cyber activities. Over the past four years, my country has undertaken efforts to protect its limited cybersecurity infrastructure. We have enacted the Electronics Transactions Act in 2021, the first ever digital legislation in the Maldives. In 2022, the Maldives launched the Cybersafe Maldives Initiative which outlines our commitment to enhancing human capacity, building resilient digital infrastructure, and ensuring legal and regulatory measures which align with global best practices.

Mr. President/Chair,

As a thriving democracy, we deeply value the benefits of a free, open, and secure cyberspace for the prosperity of future generations. However, we acknowledge the growing menace of artificial intelligence-driven cyber threats and the potential for technology misuse, which can exacerbate ongoing conflicts or instigate new ones. We also believe that cybersecurity encompasses more than just defensive measures—it demands resilience and preparedness. A comprehensive strategy including all facets of our society—including government agencies, private corporations, local communities, and individual citizens —is required to achieve robust cybersecurity.

It is imperative to promote extensive dialogue between governments and technology companies to foster innovation and establish swift countermeasures against ever-evolving cyber threats. Encouraging private sector entities to invest in cybersecurity capacity building, particularly in developing nations, will yield benefits for all stakeholders involved.

In this spirit, the Maldives urges the Security Council to adopt a comprehensive, inclusive, and forward-thinking approach to cybersecurity. Together, we can ensure that the digital realm remains a space of peace, cooperation, and sustainable development, and prevent it from becoming a battleground.

As a responsible state, the Maldives is steadfast in our commitment to the international rules-based order, and we look forward to working with all Member States to combat cyber threats.

Thank you.

Lichtenstein

Mr. President,

We have a duty to ensure the rule of law can respond to 21st century challenges such as the digitization of warfare. This includes clarifying how international law applies to malicious cyberattacks. In particular, having a clear understanding of the application of the Rome Statute of the International Criminal Court to cyberattacks against critical infrastructure will act as an important deterrent against such attacks and contribute to accountability.

The Russian aggression against Ukraine is the first major conflict where large-scale cyber operations have been carried out. These operations were used to create disorder – to, among other things, take down critical infrastructure. Such cyber operations can inflict grave suffering on civilians. There is general agreement that malign cyber operations do not occur in a law-free domain but are subject to various bodies of international law, including international humanitarian law and international criminal law. The ICRC has stated that the law is clear on the matter: IHL limits cyber operations during armed conflicts just as it limits the use of any other weapon. Therefore, irrespective of whether an act is kinetic or conducted through cyber means, Article 8 of the Rome Statute of the International Criminal Court governing war crimes applies if IHL is triggered.

Additionally, as this technology continues to advance and cyber operations are increasingly used by both State and non-state actors, the Security Council must recall its power to refer situations to the ICC to ensure accountability and further deter such crimes. And, as discussions on the application of international law to cyberspace continue in several fora at the United Nations, we must include the Rome Statute and international criminal law more generally in these analyses as a matter of prevention. This is why, together with ten other State Parties to the Rome Statute, Liechtenstein created a Council of Advisers that helped produce an in-depth report of the application of the Rome Statute to cyber warfare which informs our intervention today. In our view, such crimes are currently prosecutable at the ICC without the need for statutory amendment, including with respect to the ICC's investigation in Ukraine.

I thank you.

Poland

Excellencies, Distinguished Colleagues,

We thank delegations of Albania and the United States, as well as Ecuador and Estonia, for their initiative, which is especially important because the topic of cybersecurity is rarely discussed in the works of the Security Council. Given the growing number of challenges in this particular area, the discussion we are having today is most timely and very much needed.

Among various malicious activities in cyberspace, cyberattacks on critical infrastructure are one of the most consequential. They generate the highest social and economic costs not only for states, but most importantly for their societies suffering from harmful or even life-threatening effects of cyberattacks. Publically known and attributed recent attacks against Ukraine or Albania are one of the most relevant examples. In light of the rapid growth of new technologies, it is crucial to ensure that cyberspace is used only for peaceful purposes and serves for the common good of all. Particular attention must be given to the security of all elements of state's critical infrastructure, which needs to be resilient to threats stemming from cyberattacks. They originate in virtual networks spanning such areas as emergency medical services, traffic control or energy supply systems, to name just a few, but they have tangible, physical results affecting lives of millions of our citizens.

In recent months, Poland has also been a target of massive cyberattacks, which are mostly carried out from behind our eastern border. Since the beginning of Russia's invasion on Ukraine, their intensity has increased significantly. It is our common responsibility to spare no effort to correctly attribute all those attacks and to bring cyber criminals to justice.

In order to do that, we need to be able to harness the wide array of existing instruments stemming from the international law as well as non-binding norms and rules which oblige states, and indirectly also non-state actors, to behave in a responsible way in cyberspace. The reports of the Groups of Governmental Experts as well as of the UN Open-ended Working Group are important building blocks of the existing international framework. These reports contain fundamental norms and good practices which were affirmed by the UN General Assembly. Let me quote a few relevant norms and good practices related to the protection of critical infrastructure that Poland fully supports and subscribes to:

1. States should not conduct or knowingly support ICT activity that intentionally damages critical infrastructure;
2. States should take appropriate measures to protect their critical infrastructure;
3. States should respond to appropriate requests for assistance by other states whose critical infrastructure is subject to malicious ICT acts.

We believe that only by intensifying international cooperation in global and regional dimension and by developing confidence-building measures as well as capacity building we can achieve a satisfactory level of a secure cyberspace.

Cyberattacks both by state actors as well by non-state actors shall be condemned, and states which territories were used to conduct malicious activities must make every possible effort to identify and to punish the perpetrators.

Excellencies, Distinguished Colleagues,

The Security Council shall continue to discuss various challenges related to malicious activities in cyberspace. In our view, states should consider a voluntary exchange of information on cyberattacks against critical infrastructure and seek assistance in this regard from the willing partners. We strongly believe that instruments and practices developed within regional organizations, like e.g. OSCE confidence-building measure 15, which is focused on ICT-related security of critical infrastructure, can be extrapolated to the UN level.

Thank you for your attention.

Romania

Mr. Chair,

Thank you for organizing this meeting.

International peace and security are endangered by malicious cyber activities from both State and non-State actors.

Attacks on critical infrastructures and on essential services can have disruptive, destructive and destabilizing effects, as well as cross-border spillover impact in neighboring countries and even across regions.

Since the beginning of the Russian illegal, unprovoked and unjustified aggression against Ukraine, we have witnessed cyberattacks carried out in preparation of, or during an armed conflict, with collateral effects impacting countries not directly involved in the conflict.

We have also seen a striking and concerning number of hackers and hacker groups indiscriminately targeting essential entities globally.

Also, the cyberattacks against Albania, conducted with a complete disregard for International Law, show the increased resolve of State and non-State actors to undermine our democracies, our economies and our societies.

Malign cyber activities from other State and not-State actors target the global financial sector trampling in the meantime Security Council Resolutions and responsible State behavior.

Even more, the use of cyberattacks combined with aggression and disinformation, reveal a cyber-threat landscape evolving at a pace that requires continuous and increased efforts to protect our common values.

These concern us all.

The Security Council is entitled to address such issues that impact on the maintenance of international peace and security.

States have in cyberspace the same obligation to act in a responsible manner, in line with the International Law, including the UN Charter.

We are not in a legal vacuum.

International Law applies to cyber space.

Malicious cyber activities aimed at critical infrastructure and affecting essential public services are against International Law and violate Human Rights.

Respecting International Law and the norms of responsible State conduct in cyberspace should be our benchmark for an effective commitment to avoiding conflict and safeguarding international peace and security in cyberspace and for further action.

Romania always supported and encouraged dialogue and cooperation between UN Member States at bilateral, regional and multilateral level in mitigating risks to international peace and security emanating from cyberspace.

Romania will continue to work hard for a global open, secure, stable, accessible and peaceful cyberspace.

The new European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) became operational on 9 May 2023 in Bucharest and is expected, inter-alia, to boost the research and innovation efforts in the field of new cybersecurity solutions to shield our societies and economies from cyberattacks.

Romania remains a proud member of the Counter-Ransomware Initiative and looks forward to its consolidation as a coordinated international response to this set of threats.

In concluding, irresponsible conduct in cyber space creates risks to international peace and security and cannot be tolerated.

Their costs – we all bear them!

Burundi

Merci Mr le Président

À l'entame de mon propos, je voudrais d'abord vous remercier pour avoir organisé cette séance afin de discuter sur un sujet aussi sensible qu'est la cybersécurité et je remercie également tous les briefer pour leurs présentations riches en information.

M. le Président

L'usage des TIC a profondément bouleversé, notre façon d'interagir, de travailler, et surtout de collecter de traiter et de transmettre les informations. Nous vivons dans un monde où les États, les entités publiques et privées et les individus sont tous interconnectés et les échanges d'informations sensibles à tous les niveaux sont fréquent d'où la nécessité de renforcer la sécurité dans le cyberespace. Cependant, il est triste de constater qu'avec le temps, les cyberattaques ont pris une ampleur inquiétante et les dégâts causés sont considérables au point de menacer la paix et la sécurité d'un État, entre États et du monde.

M. le Président,

Le cyberespace ne connait point de frontière et a transformé notre planète en un petit village où toutes formes d'interactions sont possibles en un temps éclair. De plus en plus d'infrastructures ont été créées et les échanges entre États se multiplient chaque jour. A mesure que la technologie évolue et se développe, il en va de même pour la complexité de la protection de toutes les infrastructures critiques existantes tant au niveau national qu'international et il serait insensé de se limiter à ses propres frontières étant donné que les attaques peuvent provenir de n'importe quel endroit du globe.

Afin de mieux garantir une meilleure protection des infrastructures critiques et une bonne collaboration en États pour endiguer ce fléau, ma délégation estime que certains aspects essentiels doivent être couvert à savoir :

Premièrement : Réduire le fossé entre les États en investissant dans le développement du capital humain, les échanges d'expérience et le transfert de technologies afin que les niveaux de compétence soient les plus proches possible.

Deuxièmement : La mise en place d'un mécanisme international contraignant permettant la coopération entre les pays, une coopération qui serait orientée sur l'échange d'informations, la communication transparente, et la coopération en matière d'enquête et une cour d'arbitrage en cas de conflit dans le cyberespace.

Pour Conclure, Il est de l'entière responsabilité de l'État d'assurer la sécurité de ses infrastructures critiques, mais compte tenu de l'aspect sans frontières du cyberespace, il est absolument crucial que les États ouvrent des portes au soutien mutuel et à la coopération en matière de cybersécurité, et de protection des infrastructures critiques non seulement pour leur sécurité individuelle mais aussi pour préserver la paix et la sécurité internationale.

Je vous remercie

Croatia

Thank you, Madam Co-Chairs.

I wish to thank the briefers, and the Permanent Missions of Albania and the United States for organizing this very timely meeting.

The increasing frequency and sophistication of cyberattacks on critical infrastructure pose a significant threat to global peace and security. In light of an alarming rise in violations of peace through malicious cyber activities, it is imperative that the Security Council play a more prominent role in addressing cyber threats to peace and security.

Cyberattacks have devastating consequences, from compromising national security to seriously harming civilians. By bringing this issue under the purview of the Security Council, the international community can provide for improved prevention.

Croatia condemns all forms of malicious cyber activities, particularly those targeting critical infrastructure, as exemplified by the recent incident in Albania and Montenegro. Such acts undermine the security of nations and their populations, and it is our collective responsibility to counter them.

We call upon Member States to collaborate closely, including on implementing existing frameworks for responsible state behavior and confidence-building measures, as agreed upon in the "Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security" and the "Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security".

These bodies have made significant progress in establishing norms, rules, and principles to govern state behavior in cyberspace. Encouraging States to implement these policies will create a more secure and predictable environment.

States should also establish mechanisms for information sharing, early warning, and incident response to swiftly address cyberattacks.

By exchanging technical expertise and best practices, States can enhance their capabilities to prevent, detect, and respond to cyber threats.

Finally, states have a responsibility to protect critical infrastructure from cyberattacks, as they pose a significant threat to the civilian population. The cooperation among States in implementing relevant policies, confidence-building measures, and the involvement of the Security Council to condemn attacks on critical infrastructure and insist on accountability of the perpetrators, including through their referral to the ICC, are crucial elements in effectively addressing this issue.

By working together and taking proactive measures, the international community can mitigate the risks posed by cyber threats and safeguard the stability and security of our interconnected world.

I thank you.

Portugal

Mr. Chairman,

Digitalization of national critical infrastructure, technological developments, like artificial intelligence and quantic computing, and their dissemination in collective and personal life demand from us a steady work on countering insecurity in a multi-stakeholder cyberspace. Such work must be fully consistent with, and supportive of, International Law, including the UN Charter, the Geneva Conventions and the Universal Declaration of Human Rights.

The applicability of these instruments to conflicts in cyberspace has been often and unambiguously reiterated by the General Assembly.

The General Assembly has also endorsed a framework of voluntary norms, with a view to increasing the stability, security and safety of cyberspace while upholding its openness, neutrality and accessibility.

Among those eleven voluntary norms of responsible state behavior in cyberspace, due diligence is, in our view, one of the most deserving of a further layer of common understanding.

The growing use of proxies by hackers, including official proxies, is very worrying and can precipitate the use of unjustified countermeasures, especially dangerous in an armed conflict.

Therefore, before resorting to cyber weapons to retaliate against malicious operations apparently originated in another state, this state must be immediately called upon by the victim to confirm swiftly if digital devices on its territory have indeed been manipulated.

Despite the technical obstacles, we should not desist from agreeing on a set of standards that increase the attractiveness of due diligence, as a means to afford a pause before precipitating a crisis generated by an attack against a critical infrastructure.

Given that the vast majority of critical infrastructures in our societies are privately owned and/or managed, some form of due diligence applicable to the private sector could also be devised.

Mr. Chairman,

As we speak, the Open-Ended Working Group on security of Information and Communication Technologies is having informal consultations. We hope that this Working Group will soon discuss the Secretary General's report on the possible establishment of a Programme of Action to advance responsible state behavior in this domain.

At the same time, we look forward to the successful conclusion of the International Convention on Cybercrime. This instrument is of paramount importance, namely because so many times criminal

entities that attack critical infrastructures have links with official entities, which must therefore be weakened and eventually severed through a concerted international effort.

Finally, we hope that the ongoing review of the UN Global Counterterrorism Strategy may consider the impact of new and emerging technologies, and contribute to encouraging Member States to develop or improve strategies for reducing risks to critical infrastructure from terrorist attacks.

Mr. Chairman,

In “Our Common Agenda”, the Secretary-General calls for a new agenda for peace, as an opportunity to reduce strategic risks, in particular through strengthening digital transformation and promoting innovation by United Nations peace and security entities, banning cyberattacks on civilian infrastructure and putting in place measures to de-escalate cyber-related risks and tensions.

The UN system in its fullness, including the Security Council, is the indispensable place where multilateral work against insecurity in cyberspace can and must be carried out. Therefore we are highly thankful for the convening of this very timely session.

Thank you, Mr. Chairman.

Montenegro

Madam Chair,

Let me begin by expressing our gratitude to the permanent missions of Albania and the United States as well as cosponsors for organizing this significant event as well as briefers for their insightful inputs. Today's topic is of the utmost importance given the fact that the protection of critical infrastructure from cyber-attacks has become a pressing concern for all of us.

Madam Chair,

In today's rapidly evolving world, characterized by a multitude of crises, our security environment has become highly unpredictable. Climate change, unprecedented health crises, terrorism and Russia's unprovoked and illegal invasion of Ukraine, including through cyber attacks, serve as stark reminders of the critical importance of resilience of our societies and protection of the critical infrastructure in the face of diverse threats and crises.

Cybersecurity has emerged as a critical factor in shaping international peace and security in the digital age. The interconnectedness of our world through information technology has given rise to a new domain of conflict and vulnerability. The impact of cybersecurity breaches extends beyond individual nations and has the potential to disrupt the stability of the international community as a whole. The increasing sophistication and frequency of cyber-attacks, as well as the range of capacities and instruments of both non-state and state attackers poses a serious threat to all of us. Government departments, in particular, are attractive targets owing to their access to sensitive information and reliance on ICTs to provide services to its citizens. Nonetheless, effective cybersecurity measures and responsible state behavior not only protect national interests but also contribute to the preservation of international peace and security. In this regard, international cooperation and collaboration are crucial to safeguarding global stability and maintaining trust among nations.

Madam Chair,

In the past year, the Western Balkans experienced a series of cyberattacks that disrupted public services and resulted in data loss. In August 2022, Montenegro faced simultaneous cyberattacks targeting critical infrastructure and public service delivery. Montenegrin Government responded promptly, taking necessary measures to protect the network and preserve crucial services. In this regard, we are grateful for the support received from countries such as the USA, France, UK, Estonia, Romania, and other partners as well as the EU.

Montenegro has made significant progress since in its cyber security regulatory framework, including the adoption of a Cybersecurity strategy for the period 2022-2026 since the attacks and is working on strengthening institutional and legal framework even more. But the recent cyber incidents in the region highlighted the need to also enhance capacities and resilience in countering hybrid threats,

including disinformation, cyber security, and protection of critical services and infrastructure. In this context, Montenegro aims to launch a robust Cyber Security Programme with support from partners, recognizing that investment in Montenegro's cyber capabilities benefits the Western Balkans and the European cyber ecosystem as a whole. As part of this effort, Montenegro is establishing Regional Cyber Security Center in collaboration with France and Slovenia, facilitating education and expertise improvement in the field of cyber security at the regional level and increase capacity and resilience of our societies.

Madam Chair,

International law, norms, capacity building, and confidence-building measures shape responsible state behavior in cyberspace. As mentioned, we have already agreed on 11 norms of responsible state behavior in cyberspace, which include measures that specifically address threats to critical infrastructure and we look forward on establishing the Programme of Action. Maintaining communication between states through confidence-building measures is crucial to defuse conflicts and prevent escalation. To enhance norm and confidence-building measure implementation, we should learn from regional organizations' experiences and leverage existing synergies between UN discussions and regional initiatives on capacity building and confidence-building measures, including but not limited to the AU, ASEAN, EU, OSCE etc. In addition, the Security Council can promote and encourage international cooperation in combating cyber threats. We believe that a coordinated and comprehensive approach, involving the Security Council and other relevant stakeholders, is crucial to effectively address the growing threat of cyber-attacks and promote a secure and stable cyberspace as well as responsible behavior in accordance with the UN Charter and international law.

Thank you.

The Slovak Republic

Mr. Chairman,

I would like to thank you for organizing this important meeting. Slovakia associates itself with the statement delivered by the European Union. I would like to make some additional remarks in national capacity.

Mr. Chairman,

The ICTs threat landscape continues to evolve rapidly and malicious behaviour in cyberspace increase with a speed that we all find difficult to keep up with. Security of and in the use of ICTs is not limited to physical borders and questions concerning State behaviour in cyberspace are today closely intertwined with issues of peace and security in general. Malicious cyber activities against vital sectors and services have destabilizing effects and may ultimately threaten international peace and security.

Therefore, it is absolutely crucial to keep cyberspace global, open, stable, peaceful and secure. It is important to support and promote cyberspace, where human rights and fundamental freedoms are fully obeyed and where the rule of law fully applies and to discourage all state and non-state actors from misusing cyberspace particularly with regard to cyberattacks targeting critical infrastructure.

Slovakia strongly supports multilateralism which helps to manage and tackle current and future challenges in cyberspace. We are convinced that the stability in cyberspace should be based on existing international law, including the Charter of the United Nations in its entirety, international humanitarian law, and international human rights law.

Mr. Chairman,

Slovakia fully supports the applicability of existing international law to state conduct in cyberspace as recognized by consensus reports of Groups of Governmental Experts endorsed by the UN General Assembly.

We condemn any malicious cyber activities that violate the voluntary norms of responsible state behaviour in cyberspace. We express solidarity with all countries that are victims of these activities.

I would like to conclude by calling for strengthening of our common determination to increase global cyber resilience in order to efficiently prevent, discourage and respond to malicious cyber activities.

Thank you, Mr. Chairman.

Civil Society Organizations

International Committee of the Red Cross (ICRC) and the International Federation of the Red Cross/Red Crescent (IFRC)

Excellencies,

We are honoured to address the Council on behalf of the International Committee of the Red Cross and the International Federation of Red Cross and Red Crescent Societies.

Today, the international community agrees that cyber operations against critical infrastructure risk having 'potentially devastating humanitarian consequences'. Such risks to humans are acute at all times. Our experience shows, however, that disrupting critical civilian infrastructure has particularly severe consequences in societies already weakened by armed conflict and other emergencies.

On this, we would like to underscore three points.

First, international humanitarian law restricts all means and methods of warfare, be they new or old, cyber or traditional.

The core rules of IHL are concrete, practical, and well-established. There should not be any doubt about the prohibition to attack civilian infrastructure during armed conflict, whether through missiles or malware.

This prohibition applies to all civilian objects, irrespective of whether they are formally designated as 'critical infrastructure'. This includes water and electricity plants as well as hospitals, including the data that enables them to function, private property, civilian government ICT equipment, or any other civilian object.

Second, we call on all States to protect civilians and civilian infrastructure against the effects of cyber operations in peacetime as well as in conflict.

For instance, States should cultivate a strong culture of cyber resilience and ensure that civilian infrastructure is protected to the highest possible standard, and to engage with their National Red Cross and Red Crescent Societies and other key actors in contingency planning on addressing any humanitarian impacts from potential future attacks.

Whenever feasible, armed forces should segregate military networks from civilian cyber infrastructure, thus limiting the spread of harmful effects onto civilian networks in case a military network is attacked.

And States are encouraged to proactively offer their support to their national societies, as providers of essential services, to protect their cyber infrastructure and counter disinformation.

Third, to support States' work towards common understandings of how IHL protects civilians and civilian infrastructure against cyber harm during armed conflicts, we would like to highlight several capacity-building initiatives.

The ICRC leads a series of regional State consultations on cyber and IHL, with publicly available reports. So far, they were held in Latin America, Central and Eastern Europe, and in Asia/Pacific, co-organized with Mexico, Estonia, and Indonesia respectively.

In partnership with others, the ICRC has also developed the widely used Cyber Law Toolkit. It contains several scenarios that provide practical insight on the legal limits on cyber operations impacting on critical civilian infrastructure.

And finally, the ICRC has recently published a series of short papers on how and when IHL applies to the use of ICTs. Two of them – those on the principles of distinction and proportionality – provide further detail on the protection of civilian infrastructure.

Thank you.