AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

SIGURIA KIBERNETIKE – PRIORITET KRYESOR NË AGJENDËN E KOMBEVE TË BASHKUARA

Sesioni i katërt i "Open-Ended Working Group (OEWG) on security of and in the use of information and communications technologies" zhvilloi punimet e tij në datat 6 - 10 Mars 2023, fokusuar në kërcënimet globale të sigurisë kibernetike, Masat e Ndërtimit të Besimit (MNB) dhe ngritjen e kapaciteteve, si dhe normat e sjelljes së përgjegjshme të shteteve në hapësirën kibernetike.

Shqipëria, përfaqësuar me Misionin e Përhershëm pranë OKB dhe përfaqësuesit e AKCESK, theksoi me deklaratën e parë trajtimin e kërcënimeve të mundshme në hapësirën kibernetike. Në një deklaratë të dytë, u vu theksi te masat që mund të ndërmarrin shtetet për forcimin e besimit mes tyre, në funksion të paqes e sigurisë mes vendeve, si dhe në mënyrë më të detajuar mbi çështjen prioritare për Shqipërinë, atë të forcimit dhe ndërtimit të kapaciteteve, në linjë me angazhimet ndërkombëtare e ndërajonale, si me politikat e Bashkimit Evropian dhe MNB të OSBE.

Në deklaraten e saj Shqipëria, në kuadër të masave të ndërtimit të besimit, theksoi rëndësinë e shkëmbimit të informacionit nëpërmjet platformave rajonale dhe globale, jo vetëm si një mjet për mbrojtje ndaj kërcënimeve kibernetike, por edhe si një mjet për ndërtimin e besimit ndaj shteteve. Në këtë kontekst, Shqipëria deklaroi angazhimet e saj në linjë me MNB të OSBE.

Në lidhje me ngritjen e kapaciteteve, Shqipëria theksoi se është në linjë të plotë me deklaratën e BE dhe prezantoi progresin në terma të: harmonizimit të kuadrit ligjor me kornizën e Bashkimit Evropian; ngritjes së CSIRT Kombëtar; trajnimeve për rritje kapacitetesh të CSIRT-eve sektoriale; konsolidimin e kapaciteteve për diplomacinë kibernetike dhe qeverisjen kibernetike; trajnimeve dhe fushatava te ndërgjegjësimit në fushën e sigurisë kibernetike për administratën publike, industrinë, fëmijët e të rinjtë; si dhe trajtimin e temave të sigurisë kibernetike në kurrikulat arsimore.

Njëkohësisht, Shqipëria vlerësoi në deklaratën e saj bashkëpunimin me organizatat ndërkombëtare si ITU, OSBE, BE, RCC etj, faciliuese e kontribuese të rritjes së kapaciteteve.

Së fundi, delegacioni falenderoi Departamentin Amerikan të Shtetit, Hollandën dhe *Global Forum on Cyber Expertise* për kontributin e tyre në promovimin e grave në fushën e sigurisë kibernetike, nëpërmjet programit *Women in International Security and Cyberspace*.

Sesioni i pestë i OEWG do të zhvillohet në datat 24-28 Korrik 2023, gjatë të cilit pritet të trajtohet, ndër të tjera dhe ngritja e *Intergovernmental Points of Contact Directory,* në linjë me *Annual Progress Report A/77/275*, në të cilin "*Shtetet pranojnë të krijojnë, bazuar në punën e bërë në nivel rajonal, një drejtori pikash kontakti globale, ndërqeveritare*".

Intergovernmental Points of Contact Directory do të shërbejë si një Masë Ndërtimi Besimi (MNB) dhe do të ofrojë kornizën për implementimin e MNB-ve të tjera, të cilat mundësojnë një mjedis të hapur, të sigurt, të qëndrueshem, të aksesueshëm dhe paqësor për teknologjitë e informacionit dhe komunikimit.

Të dyja deklaratat që Shqipëria mbajti gjatë sesionit të katërt të OEWG, gjenden më poshtë.

AKCESK | AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

07.03.2023

Statement by

Mrs. Naureda Breshanaj, Counsellor

Permanent Mission of the Republic of Albania to the UN

Fourth Substantive Session of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021-2025 6 to 10 March 2023

Agenda: Existing and Potential Threats

Thank you Mr. Chair,

Dear colleagues,

At the outset, allow me to extend our appreciation and support to you, Ambassador Gafoor as Chair of this group and to your team for your efforts in facilitating a focused discussion, guided by the First Annual Progress Report, addressing issues that concern today each of us at national, regional and international level.

Albania aligns with the statements delivered by EU Delegation on multi-stakeholder participation, as well as on the issue of threats in cyberspace, for which I would like to make the following statement on our national capacity.

Mr. Chair,

Technological advances are dramatically impacting international peace and security. The potential for misuse by states or non-state actors is significantly growing.

Some countries are continuously trying to deliberately mislead information, distort facts, interfere in democratic processes of others, spread hatred, discrimination, incite violence or conflicts by misusing digital technologies. In the same vein, we see with concern unlawful internet shutdowns, restrictions, or denial of human rights and freedoms in using them.

Allow me to recall that our region is systematically targeted by campaigns of interference and manipulation of information, which aim to create political instability and hinder the peace, development and stability. Cyber-attacks have tried to suspend the online work of public institutions in these countries.

We are deeply concerned by the malicious information and communications technology activities aimed at critical infrastructure and critical information infrastructure facilities, affecting essential services to the public.

As rightfully recalled by previous speakers, Albania's critical infrastructure went under two massive cyber-attacks last year, of complex nature, in an unsuccessful attempt by one state to inflict damage to the critical infrastructure, erase digital systems, steal data, trying to paralyze on-line public services, that constitute 95 % of all public service, trying to paralyze the whole country, to create chaos and insecurity. It was a blatant breach of norms of a responsible State behavior in cyberspace, in violation of the principles of the UN Charter and the international laws.

Albania recognizes cyber security as a top priority. We will bring this issue to the attention of the Security Council during this year. In this regard, we are taking the appropriate actions to protect ourselves from potential cyber threats based on cooperation with the strategic national and international partners, by implementing security measures in critical information infrastructure and, more concretely, by building the National Security Operations Center (SOC) to effectively respond against cyber threats.

Cyberattacks and cyber-threats are unlawful acts, must be condemned and must be treated accordingly. Impunity for these illegal activities by state or non-state actors should be properly addressed in our discussion.

In this sense, Albania believes in the imperative to defining rules that ensure security and stability in cyberspace within the framework of the United Nations, grounded in the UN Charter and existing international laws, international humanitarian law, and international human rights law.

In July 2022, member states recalled that the PoA should be further elaborated including at the 2021-2025 Open-Ended Working Group process. We look forward and encourage member states to further elaborate during this session the proposal put forward by France and Egypt for the Programme of Action to Advance Responsible State Behavior in Cyberspace. This permanent mechanism could be very instrumental in bringing resilience and stability in cyberspace.

Finally, Mr. Chair, allow me to reiterate Albania's firm position for a global, open, free, stable and secure cyberspace where international law, including respect for human rights and fundamental freedoms fully apply, supporting social, political and economic development.

We believe that multilateral efforts, the United Nations play an important role in continuing the dialogue between member states.

Thank you.

AKCESK | AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

09.03.2023

Statement by

Mrs. Naureda Breshanaj, Counsellor

Permanent Mission of the Republic of Albania to the UN

Fourth Substantive Session of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021-2025 6 to 10 March 2023

Agenda: Capacity building

Thank you Mr. Chair,

Dear colleagues,

As we did not take the floor on confidence building measures, allow me to add the importance of information sharing at regional and global platforms, that is a tool not only for protection or prevention from ongoing or future cyber-attacks, but also as a tool for building trust between states. In case of my country, Albania is sharing information on cyber threats with other Cyber Incident Response Teams, to facilitate implementation of best practices in this field, based on OSCE Confidence Building Measures, aiming promotion of international cooperation for a safer global cyber ecosystem.

On the issue of capacity building, Albania aligns with the statement delivered by EU Delegation and would like to highlight the following.

Mr. Chair,

Albania learned the hard way that cybersecurity capacity building is fundamental when it comes to maintenance of a secure and peaceful cyberspace and also for the prevention from cyber threats and cyber-attacks.

We recognize the critical importance of capacity-building in cyber security. Speaking from the perspective of a small state, with limited capacities, we want to highlight the importance of assistance, be it financial, logistical, educational, information sharing from other states, regional and international organizations, as well as from private sector and multinational corporations, in setting the foundations for the right necessary capacities, directly contributing to a stable, peaceful and secure environment in cyberspace.

Albania has undertaken significant steps in terms of strengthening its cybersecurity, by adopting its National Strategy on Cybersecurity and its Action Plan 2020-2025, outlining specific policy goals and strategic objectives to ensure cybersecurity at national level, harmonize its cybersecurity legal framework with European Union legislation.

Albania is actively working to develop its own cybersecurity capacities, enhance its cyber resilience, focused on the following measures:

- establishing effective national and other sectoral Computer Security Incident Response Team in line with the sectors defined with EU norms (energy, financial, health, transport, digital, government and water supplies sector);
- educational and professional capacity building policies on Information and Communication Technology (ICT) through revision of curricula, trainings, scenarios, cyber exercises dedicated to the CIRT's responsible staffs, to respond to potential cyber-threats;
- increasing capacities, through cyber courses on International Cyber Law for relevant responsible experts on cyber security issues, as for example Tallinn Manual on cyber warfare, to increase capacities and responsibilities at the national level against cyber threats;
- consolidating capacities in cyber-diplomacy and cyber-governance;
- trainings on cyber hygiene, personal data protection and awareness raising campaigns for public institutions and industry, which access digital essential services related to critical information infrastructures;
- integration of dedicated topics on online safety and education of children in the use of information technology in their curricula.

AKCESK | AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

Mr. Chair,

Regional and international cooperation, partnership and networking are excellent opportunities to build synergies and coordination in building capacities in cybersecurity. Here in the OEWG we could make best use building from best practices and research already made by these regional and international organizations, in our case, its ITU, OSCE, EU, RCC, etc, that already have delivered with objectives and recommendation on how to improve capacities and build cyber resilience for our region.

A multi-stakeholder involvement in capacity building is vital for a more whole-of-a-society approach, including contribution from private sector, business, industry, academia, civil society.

In an appreciation note, I would like to thank US, Netherlands and the Global Forum on Cyber Expertise (GFCE) for their contribution in promoting female cyber experts in our team, through Women in International Security and Cyberspace fellowship.

Diversity and gender balance should be further strengthened in terms of capacity-building in cybersecurity. It is encouraging to see a positive trend of women cyber experts, including in this very hall. We welcome all efforts, by all stakeholders, for a meaningful and effective inclusion of women in all cyber-related agendas, with equal rights as men.

Thank you.