Report of Georgia on

Resolution 73/27 on Developments in the field of information and telecommunications in the context of international security

Resolution 73/266 on Advancing responsible State behavior in cyberspace in the context of international security

Georgia highly values and greatly appreciates the work undertaken under UN auspices on advancing responsible state behavior in cyberspace in the context of international security. Georgia has closely been following the discussion process within Group of Governmental Experts on developments in the Field of Information and Telecommunications in the context of International Security (A/65/201, A/68/98, A/70/174) since 2010. Georgia takes into account the assessments and recommendations contained in the reports of the GGE and this report is a brief summary of Georgia's cybersecurity endeavors during last years.

Georgia is fully committed to adhering international law and UN Charter in its activities related to the cyber domain; All those rights and freedoms Georgian citizens and other individuals within Georgian jurisdiction enjoy, are equally applicable to the online world; this is the core and fundamental principle that Georgian Government considers in full extend when enacting new laws, executing policies or operationalize cybersecurity nationwide. State actions and activities in cyber domain are founded on the UN Charter principles and international legal doctrines, such as refraining from the threat or use of force against the territorial integrity or political independence of any State, non-intervention in the internal affairs of other States; guaranteeing rule of law, human rights and fundamental freedoms; using proportional, adequate and necessary measures and performing every activity in a way that international peace, security and justice are not endangered.

Georgia is committed to following present international legal regime by participating in UN dialogues and cooperation formats as well as in future norm building processes in order to make States responsible for their activities in the cyber domain and thus develop international peace and security. Although Georgia strongly considers that cyber is not a law-free zone and international legal regimes apply to online world the same way as it does with offline transactions, but notwithstanding the abovementioned, Georgia believes that UN GGE dialogue should continue its work to clearly interpret the applicability of rules and legal doctrine.

Aside applicability of international law and norm-setting process, Georgia is following GGE's recommendations in the confidence building and capacity building directions. Mainly, Georgia's efforts can be lined-up into 10 core pillars, these are:

1) Cybersecurity has a high standing in Georgian political agenda. Georgia has a well-developed capacity to design and deliver cybersecurity policy and strategy which is essential to reinforce cybersecurity agenda across government, as well as to prioritise cybersecurity as an important policy area, to determine responsibilities and mandates of key government and non-governmental cybersecurity actors. In the time frame of 2012-

2018, Georgia adopted and implemented two-sets of national cybersecurity strategies and respective action plans. Both strategy iterations concentrated on following strategic priorities: research and analysis; legislative and regulatory frameworks; institutional coordination; public awareness and education, and international cooperation. Georgia is in the process of elaborating a new strategy for consecutive five years that will demonstrate national vision and government's strategic development path for cyber development. All the past efforts and ongoing work demonstrate that Georgia is well-stand to enhance cybersecurity resilience through effective policy and strategy dimensions;

2) Georgia is a trusted partner and an active participant of regional and international forums: Georgia is part of a regular dialogues on internet governance and human rights on domestic, regional, European and international levels, under the UN auspices and other bilateral and multilateral forums with the aim to build-up common understanding of present and future goals to make cyberspace secure and stable field for everyday operations. Georgian information and cyber security authorities strive to cooperate with like-minded states on bilateral formats as well: annually Georgian authorities sign 2-3 new MoUs on information and experience sharing in the field of cyber security with different countries. Georgian technical security community is also part of European and International cyber incident sharing platforms (CERT.EU; Trusted Introducer; Team Cymru, etc.,);

3) Georgia considers cybersecurity as a whole-of-nation challenge – Safety and security of cyberspace is not only a government's responsibility, but it entails individual and industrial duties and obligations, in a broader sense. While role of government is to provide enabling frameworks for open, trusted, secure and transparent cyberspace, it does not substitute corporate industrial sectors' roles in safeguarding their own ICTs, as well as end-users' commitments towards essential security requirements;

4) Protection of Critical Information Infrastructure - Under the Law on Information Security, promulgated in 2012, two first sets of civilian and military entities have been identified as Critical Information System Subjects (CISSs) – Critical infrastructures. Government facilitates adoption of information security policies and standards as well as cyber security measures in critical information systems and services. From 2019 Georgia plans to elaborate new sectoral lists of critical information infrastructures and harmonize Georgian legislation with European Directive on Security of Network and Information Systems (NIS Directive);

5) Georgia has achieved considerable advances in cyber operational capacity, CERT is mandated to act as authority for managing cyber-security incidents within government networks and at the national level. CERT.GOV.GE is the responsible entity for handling critical incidents within Georgian government, especially those targeting critical information infrastructures. In addition, Information Security Act introduced mandatory Incident reporting requirements for all organisations identified as critical information

infrastructure. Reports are to be sent to CERT.GOV.GE, which also receives and responds to voluntary reports and requests for assistance from public and private sector organisations not designated as critical. CERT gained a high professional reputation and trust from public and private stakeholders and it is the primary guardian of Georgian cyberspace from different types of cyber threats, incidents and attacks. Within the scope of its authority, CERT.GOV.GE performs preventive and protective measures, it is not involved in offensive and disruptive activities. CERT.GOV.GE never uses its powers against other nations' CERT/CSIRT community or critical information infrastructures;

6) Responsible disclosure on threats and incidents to authorized state agencies (CERT/CSIRT, law-enforcement) is a key area of current work and future development for Georgian Government. CERT.GOV.GE monitors the cyberspace of Georgia and shares information about incidents and threats with the relevant stakeholders. Additionally, it has a central repository for incident-monitoring, which includes information from international threat-intelligence data providers as well as public reporting. CERT.GOV.GE also has an information feed available for both public and private organizations, based on which all the relevant stakeholders are duly notified of emerging threats. Georgia puts a lot of emphasis on stimulating responsible disclosure from the side of the private sector, creating cyber threats and incident sharing platforms and elaborating relevant procedures and rules for reporting or responding to national-level incidents not only in critical infrastructures or government, but also within nation-wide scope. Formal national incident coordinating architecture will be elaborated and consolidated list of national level incidents will be created that can be used to identify trends and common causal themes;

7) The cyber-ecosystem in Georgia has already gained a good speed of evolvement across government, the private sector, and also in the information society, in general. ICT security awareness and capacity-building, identification and engagement of young talents, building-up cyber education in each and every academic stage are the top strategic priorities for the country. After a comprehensive and systematic awareness raising campaigns initiated by the government in the last couple of years, there are clear signs that the general public begins to develop a more detailed cybersecurity mind-set, gains in awareness appear within different target groups across Georgia (pupils, teachers, municipal civil servants, media representatives, civil servants, SMSs, etc.,). There is an increasing trend in the concerns of surveyed population about the security or privacy aspect of using Internet services. Cybersecurity awareness and cyber-consciousness are mostly present in the mind-set of employees in the government sector. In the coming years Georgia will put more and more resources and efforts in developing cyber security human capital within its information society;

8) Cyber- and information security professionals in Georgia form a close-knit and collaborative public-private community that runs on common values, trust and respect. Multi-stakeholderism is the key guiding principle for resolving cybersecurity challenges

in Georgia and both public and private sides equally understand each other's importance in this process.

To facilitate the development of professional networks, Georgian government cyber authority has been organising, now in its seventh year, the Cybersecurity Forum. Convening 40 to 50 participants, the forum serves as a platform for exploring public-private partnerships. Georgian government tries to institutionalise the platform, giving the network more systematic and regular character and encompass a larger number of diverse stakeholders in order to firstly, inform targeted recommendations and to explicitly gauge the awareness of these stakeholders about practices, processes, and programmes already in place, and, secondly to initiate common mutually beneficial projects and activities.

It is already 11th year since the Georgian information technology conference GITI provides opportunities for 400 participants from more than 30 countries in Central and Eastern Europe, the Caucasus, and Central Asia to exchange best practices in the field of cyber and information security. The conference was an important fixture for security professionals in the region, facilitating the identification of counterparts and valuable points of contacts in neighbouring countries for cross-border cooperation. The setting also offers possibilities for information exchanges between policy-makers and the technical community;

9) Formal mechanisms of international cooperation have been established in order to handle cyber incidents, collect and provide digital evidence to the requesting foreign partners and prevent and combat cybercrime by facilitating its detection, investigation and prosecution, with established communication channels. Georgia cooperates with the EU, the US and other third countries on the basis of bilateral and multilateral agreements on criminal matters, as well as based on bilateral MoUs for partnership and cooperation during cross-national cyber crisis and security incidents coming from or through Georgian territory. Georgia is committed to utilize its human and technical resources in cross-national cyber operations, technical, policy and legal assistance to combat cyber-crime and other cyber related threats and attacks;

10) Georgia has made a conscious decision to expand its international cooperation with like-minded states and trusted partners by sharing its knowledge and experience and thus building trust and ties with international partners. Georgia is a forerunner in the field of cybersecurity among South Caucasus, Black Sea and other EaP countries, based on ITU Global Cybersecurity Index Georgia ranks #9 in Europe and #18 globally in terms of its endeavours to improve own cybersecurity posture.

Georgia has numerous involvements in international experience sharing activities. Georgia helped other countries in transition in developing of their cyber capabilities, conducted trainings and capacity sharing activities for foreign counterparts (also through NATO SPS program), including provision of consultancy and ICT audit services, recommending legal and institutional framework design. On a yearly basis, Georgia hosts multiple delegations of foreign countries interested in acquiring knowledge on successful ICT and cyber reforms undergoing in Georgia. Georgia hosts professional workshops on

strategic, legal, regulatory and technical aspects of cyber security with the involvement of foreign colleagues and counterparts

The importance of Cyber Security for state and global security is recognized by every nation. Countries that strive for technological development are responsible to the society to protect its own cyber space, provide its security and dynamic progress.

Large-scaled cyber-attacks experienced by Georgia in 2008-2011 highlighted the necessity for elaboration of Cyber Security Policy in order to provide safe and credible functioning of critical information systems. In 2013 with the support of the NATO Liaison Office in Georgia, the working group of the Ministry of Defence of Georgia studied the existing situation in cyber security in the MoD. Cyber security core problems and challenges were identified: there were no cyber security threat/risk monitoring, analysis and prevention tools available in the MoD. Since cyber security assurance in Defence forces has its specificity, **Cyber Security Bureau** was established within the system of Ministry of Defence in 2014. Establishment of Cyber Security Bureau was preceded by the NATO Liaison Office supported Roadmap summarizing existing situation, threats and challenges related to cyber-defence within the system of the Georgian Defence Ministry. This Document identified cyber security gaps and discrepancies in Georgian defence sector and recommended creation of the agency that would be focused on cyber-defence issues in Georgian Defence Forces. Georgian authorities took into consideration recommendations provided by NATO Liaison Office and thus CSB was created. Bureau is responsible for handling cyber incidents directed against information systems of the Georgian Defence Forces on 24/7 basis as well as ensuring installment of secure cyber connections inside defence sector. Cyber Security Bureau also prescribes information security standards withinGeorgian defence sector and elaborates relevant binding legal acts, responds cyber incidents directed against Ministry of Defence through CSIRT (Computer Security Incident Response Team).

In 2014, CSB with cooperation of NATO Liaison Office of Georgia developed **Cyber Security Policy Document for 2014-2016**. This keynote document was designed to be used as a basis for various strategies and guidelines that orient to actions towards establishing and enhancing cyber security. It must be continuously evaluated and updated due to dynamic changes and impacts in cyber space. The Policy fully responds to global challenges in cyber space and complies with principles of NATO and the EU countries in the field of cyber security. The Policy defines core approaches and priorities of the MoD and provides all strategic objectives in the field of cyber security the execution of which will significantly contribute to the MoD to work and act in a safe, effective and resilient environment and ensure confidentiality, integrity and availability of information systems. This constitutes solid basis for National Security.
On the basis of the "Cyber Security Policy" was elaborated "**Cyber Security Development Action Plan**", which represents the core document of Cyber Security Bureau for 2017-2021 to implement and develop cyber security in the defence sector, describing the actions, steps and methods necessary for attaining the goals set forth in Cyber Security Policy. The document

should be continuously evaluated and updated due to dynamic changes and impacts in cyber space.

Apart from this, Bureau is actively involved in the elaboration of the third edition of the National Cyber Security Strategy, along with other national cyber stakeholders. The document is designed to set goals, roles and responsibilities among the public and private sector representatives in the sphere of cyber security.

GEO MoD leadership considers cyber security as one of the top priorities in the defence sphere. As a result, 2019 was announced as the "Year of Cyber" in the Defence Forces which intensifies a focus towards cyber security and its development.

In order to integrate cyber capabilities in defence forces CSB has participated in different military and cyber exercises on national/international levels.

Taking into account that one of the top priorities for Cyber Security Bureau as well as for the Ministry of Defence of Georgia is to care and support the wounded soldiers, CSB initiated the **Wounded Warrior Project** in 2016. The goal of the Project is to facilitate wounded soldiers in their adaptation process to social environment and reintegration into the society and also assist them to develop their IT skills. More precisely, Bureau promotes further professional development by providing basic cyber security and IT course. Now 2 retrained wounded warriors are employed in the Bureau and are involved in cyber awareness campaign.

Besides, in 2018 Cyber Security Bureau introduced the **Cyber Reserve** project. The strategic objective of this project is to develop and strengthen cyber capabilities which ultimately will enhance the country's defence capabilities, through recruiting of highly professional cyber specialists employed in private sector. The function of the Cyber Reserve is the development/strengthening of cyber capabilities of defence sphere during the peace, crisis, war and/or a state of emergency or based on national security interests. According to the schedule, in early spring 2019 cyber reservists took part in cyber exercise "Paintball", organized by the Michigan state NG, together with Bureau's personnel and participated in the specialized training conducted by the US cyber experts.

Since the weakest point in cyber security is an end-user and considering the lack of knowledge in the sphere of cyber security, Bureau has elaborated **special obligatory course** for MoD employees. Different trainings, workshops and exercises are conducted on a regular basis. In order to check the level of awareness of end-users fishing exercises are conducted occasionally. The next step of this project is an implementation of Cyber Hygiene Platform within the defence system.

In order to integrate cyber capabilities with defence forces Bureau's personnel has been participated in the different military and cyber exercises on national/international levels. It is worth mentioning NATO-GEO 19 multinational military exercise, where Cyber Security Bureau was responsible for information and cyber security of the exercise.

In today's world, filled with hybrid, asymmetric threats and multidimensional provisions of security, cyber domain represents one of the key aspects for maintaining stability in the Black

Sea region. It is without doubt, that providing cyber security in isolation is impossible, therefore collaboration and active cooperation with the partners represents vital platform in countering cyber threats emanating from the adversaries.

In order to secure own domains, nations need to work together sharing cyber capabilities and understanding. Considering this fact, Cyber Security Bureau, under the auspices of the Ministry of Defence is planning cyber security conference - Intermarium Cyber Security Forum 2019, which aims to deepen international cooperation in cyber security sphere through information sharing on cyber threats and thus increase the effectiveness of responding to cyber incidents, improve security enhancement measures, build trust between countries and open doors to new opportunities.

In order to strengthen cooperation with the EU side, Cyber Security Bureau in cooperation with the European External Action Service is planning Cyber Security Workshop for EaP countries in Tbilisi, Georgia. The event will create an excellent platform for discussing the contemporary challenges in the cyber domain, facilitate experience sharing among the participants and allow identifying the best practices/policies applicable in this field.

Finally, despite the progress achieved, Cyber Security Bureau, as well as other Georgian cybersecurity agencies still necessitate assistance in the process of capacity building since cybersecurity is relatively new field in Georgia. In that regard, gaining broader access to NATO and the EU cyber trainings and exercises will significantly facilitate Georgia's cyber capability development and this, on its behalf will contribute to the Country to be a credible player in cyber domain.