Security Council Arria Formula Meeting: Cyber Stability and Conflict Prevention

22-5-2020

I would like to thank Estonia for convening this meeting and co-hosts Belgium, Indonesia and Kenya.

We also thank all the briefers for their interventions.

There is no doubt that the extraordinary development experienced by Information and Communication Technologies (ICTs) has turned cyberspace into a vital resource for the normal development of modern societies, since it favors and simplifies the relationship between citizens, public administrations and companies, constituting a basic piece for the provision of essential services worldwide.

However, the increasing dependence on cyberspace, also brings about an increase in the level of exposure to its threats and vulnerabilities. It is evident, therefore, the importance that for the good development of organizations supposes an appropriate knowledge of their cybersecurity -an adequate awareness of their situation in cyberspace, and of the threats that this entails for the normal and safe development in this new environment.

In 2007, the Dominican Republic enacted Law 53-07 against High Technology Crimes, to deal with the issue of cybercrime, and in 2018 established a National Cybersecurity Strategy which created the National Cybersecurity Center by means of Presidential decree 230-18, seeking to establish adequate cybersecurity mechanisms to protect the country, its inhabitants, and in general, national security.

National cybersecurity strategies are a crucial component of capacity building. While their elements and principles are usually similar, the level of their implementation varies. The clarity of objectives and mandate for each organization is critical to apportioning responsibilities.

The legal framework that affects issues related to cybersecurity, and the capacities of specialized and competent units to prevent, detect, investigate and prosecute high-tech crimes need to be strengthened. We must ensure the continuous operation and protection of the information stored in the national critical infrastructures and relevant Information Technology (IT) infrastructures of the State.

It must also remain of high importance, the inclusion of cybersecurity training at all levels of the educational system and the promotion of a national culture of cybersecurity. Likewise, the establishment of national and international

alliances between the public and private sectors, as well as with civil society and international organizations and institutions.

There is little doubt capacity building requires international coordination. There are multiple aspects to consider before ensuring a cyber security plan works for the global community. We must take into consideration elements of prevention, enforcement, local regulations, state policies, and capabilities. International cooperation is imperative for two main reasons: first, cyber-related threats know no borders; and second, the scope of investment needed to take full advantage of the opportunities offered by ICTs exceeds the capacities of any single nation. Without a cohesive and easily defined path for the global division of tasks and labor, each aspect is likely to be weakened.

The international debate on cybersecurity has focused on developing standards to promote responsible state behavior, the application of international law to cyber conflict, cybersecurity capacity in all nations, and agreement on confidence-building measures.

In our search for a model of international cooperation, both donor and beneficiary agents should focus their efforts on identifying best practices, capacity building efforts and sharing and coordinating resources. Between 2010 and 2015, there was considerable progress on these issues. Much of this work was carried out in the United Nations Group of Governmental Experts.

These non-binding norms constitute a key component in establishing how international law applies in cyberspace. Creating and enacting policies and legislations to address these many issues is certainly challenging, but nevertheless

doable. A good example of such rules and principles are those proposed by Oxford University in their statement on the International Law Protections against Cyber Operations Targeting the Health-Care Sector.

The Dominican Republic recognizes cyberspace as a necessary component of securing critical national and international infrastructure and an essential foundation for economic and social activity online.

Thank you.