Comments on the pre-draft of the OEWG report - URUGUAY

As a faithful defender and contributor to the maintenance of international peace and security, Uruguay considers cybersecurity as an essential element of the last decades in the prevention of international conflicts. That is why it reaffirms the commitment to the work of the Open-ended Group and the Group of Experts, which will undoubtedly have a direct impact on this task.
Our country understands that this work should continue to be guided by the principles of transparency, inclusiveness, trust, shared responsibility and the promotion of an environment of information and communication technologies, open, secure, stable, accessible and peaceful.
In this sense, the approach must be centralized with a perspective of Human Rights and fundamental freedoms which must be respected and protected "online" and “offline”.

Application of International Law in the subject of Information and Communication Technologies.

1.Uruguay supports the consensus reached in the Reports of the Expert Groups of 2010, 2013 and 2015, considering the respect and application of Public International Law, International Human Rights Law and Humanitarian Law as fundamental and necessary in the use of ICT within the framework of the provisions of the Charter of the United Nations Organization. Therefore, the sovereignty of each State in the decisions to be taken and implemented in the future, as well as the guiding principles of the international law, must be respected without exception.

2.Our country maintains a long tradition in the defense of Human Rights, and considers that cyberspace cannot be the exception. The application of Human Rights norms in Cyberspace and for the use of information and communication technologies, especially the right to freedom of expression and online privacy, constitutes the pillars that the States must not ignore, but rather must guarantee and promote.

3.The eleven voluntary and non-binding norms included in the Report of the Group of Experts-GGE-of the year 2015, represent an inescapable guide for the responsible behavior of States in cyberspace. In this regard, for Uruguay, the OEWG should base its work on implementing the recommendations of the aforementioned Report.

4.The development of the Internet in Uruguay is located within the institutional and legal framework that follows international guidelines for the respect of Human Rights. In

addition, it is part of international organizations that promote the development and compliance with standards of transparency and access to information, such as the Open Government Partnership, the Electronic Government Network of Latin America and the Caribbean (GEALC) and Digital Nations.

5. Likewise, the country maintains an active participation in international forums related to the information society such as: World Summit on the Information Society (WSIS), Internet Governance Forum (IGF) and the International Telecommunication Union.

6. It also exchanges experiences with member of countries of the Digital 9 (D9) which are recognized for their level of development in the provision of digital services to citizens, while holding the Group Presidency for the period 2019-2020.

7. The elaboration of policies for technological development and good practices seeks to align itself with international trends, seeking interoperability and insertion of the country at the regional level. Such is the case of the country's adaptation to the European regulations on Personal Data Protection and electronic identification.

8.Uruguay does not carry out or support activities that may damage the informational systems of the incident response centers in other States. It also does not carry out activities that seek to attack other centers from the CertUy.

9. Since the creation of the Electronic Government Agency and the Information and Knowledge Society (AGESIC) in 2007, it has maintained an advisory Cybersecurity Council made up of the Ministry of Defense, Ministry of the Interior, Presidency of the Republic, University of the Republic and the National Telecommunications Administration.

10.Uruguay's strict compliance with the norms and principles of International Law is seen in the participation in multiple forums and activities for the exchange of information and capacity building that our country has carried out since 2014.

International Cooperation and Assistance in Capacity Building

1. Uruguay considers it essential to have a stronger and more consolidated capacity-building system to advance the responsible conduct of States in cyberspace. It is understood that the principles that guide the capacity building system are: multidisciplinary, multi stakeholder, modular and measurable.

2. The construction of an open, safe and reliable cyberspace cannot be a task only for governments. Participation in capacity building is important not only for state actors but also international organizations, civil society and the technical community. The participation of non-governmental actors within the processes should be promoted, both in the Group of Experts and the Open-Ended Working Group, in order to achieve a true democratic and participatory approach.

3. The capacity building strategy should include not only training in cyber diplomacy, but also training in diplomatic matters for technicians. It could also include, as it already exists at the regional level, joint exercise and training programs between the countries of the region, from a gender perspective, understanding training as a measure of confidence-building.

4. The creation of Regional Research Centers (or Centers of Excellence) that allow the exchange of information, the execution of courses, seminars, and dissemination activities would be an invaluable pillar for the transfer of knowledge and for countries to gradually build trust which is necessary to raise levels of cooperation.

5. Uruguay has identified as vital services for the operation of the government and the country's economy the services related to health, public order, emergency services, energy, telecommunications, transport, drinking water supply, ecology and environment, agro-industry, public services, banking and financial services or any other service that affects more than 30% of the population.

6. In 2014, Uruguay approved Decree No. 92/014 that establishes the technical requirements for data centers that store information from the Public Administration.

7. Likewise, a Cybersecurity Framework was approved based on the guidelines of the National Institute of Standards and Technology (NIST CSF) for the improvement of cybersecurity in critical and contextualized infrastructures for public administration organizations. The Framework was disseminated in various national and international spaces, being presented as a success story at the annual event of the National Institute of Standards and Technologies (NIST) in the United States.

8. In 2019, audits were carried out based on the Cybersecurity Framework in organizations of the Central Administration, Health organizations and in the Central Bank of Uruguay (BCU).

Confidence Building Measures

1. A measure that would contribute to building trust between countries could be achieved through collaboration between regional organizations and through periodic regional consultations to build regional positions.
On this point, it is important to highlight that the Organization of American States has made calls for regional consultations that allow a better understanding between countries that share similar realities on the continent. The exchange of experiences and the consolidation of points of agreement are essential for progress in this regard.

2. Another confidence-building measure is an open and inclusive participation, based on the incorporation of non-state actors, civil society organizations, the technical community, academia and the private sector in these processes, seeking a broad dialogue between different perspectives and interest groups.

3. Uruguay maintains an active participation in international and regional forums related to the information society (World Summit on the Information Society, Internet Governance Forum, International Telecommunication Union, among others).

4. Experiences are shared with the member of the countries of Digital Nations which are recognized for their level of development in digital services for citizens.

5. It is important to note that in 2008, our country created the Computer Security Incident Response Center (CertUy). This system has led the development of the national cybersecurity policy in Uruguay.

6. CertUy has incident detection and response capabilities within the national territory. It is made up of an incident response unit, a cybersecurity operations center (SOC), a laboratory, and a coordination table where it actively coordinates with other stakeholders in the country.

7. Likewise, it carries out multiple instances of technical and legal training throughout the year aimed to judges, prosecutors, various actors in the legal community and police related to the subject, in order to improve the capabilities of prosecution and judicial action of computer crimes .

8. The referred center is a benchmark at the regional level and has actively collaborated with countries in the region such as Peru, Jamaica, Colombia, and Panama, among others, and with other regional actors such as the OAS, IDB, LACNIC, ISOC, etc. The center also

integrates various regional and international cooperation networks between CERTs and CSIRTs (FIRST, CICTE).

9. On the other hand, CERTuy, in addition to the processing of events and incidents, carries out Ethical Hacking actions and vulnerability analysis on different systems.

Good national practices related to capacity building programs and initiatives.

1. At the national level, the approach adopted by the Incident Response Center on computer security (CertUy) also bets on collaboration with the different actors in the ecosystem. In this sense, it has an active coordination space with its target community (Cybersecurity Coordination Table), which includes service providers from both the public and private sectors.

2. The cybersecurity communities of the health and social security sector were created, extending the existing communities of the State and financial sector.

3. Last year, the CyberWomen Challenge was held. It was an exclusive cybersecurity activity for women in the sector sponsored by the Organization of American States (OAS). The winners of this activity competed in the Cybersecurity Symposium of the Americas, where the Uruguayan team was the winner.

4. This year it is planned to create a Center of Excellence at CERTuy with the purpose of promoting the development of national capacities by encouraging research and development on the subject.

5. From the private sector, the Uruguayan Chamber of Information Technologies (CUTI) has a special cybersecurity table, in which CERTuy actively participates.

Comments on the proposal for a Regular Institutional Dialogue

1. Regarding the coexistence between the Group of Governmental Experts and the Open-Ended Working Group, Uruguay supports the existence of both groups since experience has shown that both mechanisms work in a complementary way, enriching the discussion at the global level.

2.In this sense, the implementation of a Regular Institutional Dialogue involving both groups would be important.

3. Uruguay supports a space for regular institutional dialogue with broad participation under the auspices of the United Nations, as well as dialogue through bilateral, regional and multilateral forums, and other international organizations.

4.This dialogue mechanism should not overlap with other existing ones. But it must enable the exchange with other United Nations mechanisms such as: the IGF and the HLPDC, and work together with them.

5.Uruguay supports the maintenance of the Open-Ended Working Group by the General Assembly that acts by consensus to continue considering progress in the field of information and telecommunications in the context of international security.

6. Likewise, our country understands that it is necessary for States to be encouraged to consider the establishment of sponsorship programs and other support mechanisms to guarantee broad participation, either from new funds or by relocating globally available resources and regional.