WORKING PAPER SUBMITTED BY THE DELEGATION OF CUBA TO THE OPEN-ENDED WORKING GROUP ON DEVELOPMENTS IN THE FIELD OF INFORMATION AND TELECOMMUNICATIONS IN THE CONTEXT OF INTERNATIONAL SECURITY (OEWG)

INTRODUCTION

Building a useful, beneficial, peaceful, safe, open and cooperative cyberspace, which also contributes to sustainable modernization and responsible action by States in it, represents a priority for the international community. The need to design and implement norms, rules and principles of behavior that complement the principles of International Law and the Charter of the United Nations, on sovereignty, territorial integrity, non-interference in the internal affairs of States and refraining from the use or threat of use of force, becomes a priority.

The Groups of Governmental Experts established in the years 2010, 2013 and 2015 have made very significant contributions to promoting international cooperation through confidence-building measures, transparency and capacity-building, while their reports have gradually increased the visibility of this situation and incorporated elements that set the way forward for cyberspace regulation. Today, several world powers have signed bilateral cooperation agreements in the area of cybersecurity, making it possible to advance in the attainment of common objectives that promote international peace.

It is necessary to reinforce the vital role of the United Nations in the development of international legal norms for information security and coordination among relevant international organizations, as endorsed in the framework of

the Groups of Governmental Experts established in the years 2010, 2013 and 2015.

Similarly, it should be noted that, given the economic and technological difficulties faced by developing countries, the implementation of one of the agreements adopted at the World Summit on the Information Society, which states that "*all States should have an equal role in and responsibility for international Internet governance*", is becoming more complex; which is not possible to fulfill in the developing countries considering that economic conditions do not exist and only the most developed and industrialized countries have access to, conduct and concentrate research and the development of information and communications technologies, as well as their operation, particularly in outer space.

Cyber security is closely related to international Internet governance which must be democratic and participatory, based on the UN Charter, international law and multilateralism.

The use of Information and Communication Technologies (ICTs) has created new conditions for the socio-economic development of mankind, accelerates productivity and improves the quality of life of citizens, making the safe use of these technologies a critical issue for international and state security.

The absence of international regulations on the Internet and cybersecurity is a matter of concern, which could bring about harmful effects for the peaceful and developmental use of ICTs. This situation also affects the resolution of conflict escalation and cyber incidents, potentially causing the

multiplication of cyber-attacks and the promotion of terrorism through ICTs.

In addition, Cuba attaches high priority to promoting the peaceful and legitimate use of ICTs, as well as the numerous opportunities offered by cyberspace for the development and well-being of humanity, while expressing great concern over the covert and illegal use by individuals, organizations and States of other nations' information systems to attack third countries, because of their potential to spark off international conflicts, since some governments have even expressed the possibility of retaliating against such attacks using conventional weapons.

The evidence of the above, as well as the proliferation of cybercrime and cyberterrorism, confirms the need for effective and urgent measures within the framework of international cooperation to counteract these threats and to promote an open, secure, stable and peaceful cyberspace from which all Member States can benefit.

The 2015 report of the Group of Governmental Experts did not endorse the approach that, for the purposes of International Law, cyber-attacks should be considered comparable to armed attacks, and that, therefore, in the event of a cyber-attack, the country under attack would have the right to act with measures of force or sanctions, invoking Article 51 of the Charter of the United Nations, which recognizes the right of States to self-defense in the event of (armed) aggression. This becomes a problem because there is not an accepted definition of what "aggression" using ICTs entails, using the one contained in General Assembly resolution A/RES/29/3314 of 1974, which does not take into account the use of ICTs by one State to attack another.

In line with its mandate, the OEWG should draft its reports based on the previous reports, but seeking a more pragmatic and operational approach to results with regulations that call for the strengthening of cooperation mechanisms at the political, operational and technical levels of the competent authorities from all countries, taking into account the complexity and transnational nature of cyberspace. The objective to be achieved should be the enactment of regulations consistent with the norms, principles and policies agreed upon at the national and international levels, which will help to make the Internet a zone of peace and prosperity.

In this regard, it is necessary to promote the elaboration and implementation of international norms in cyberspace, based on the respect for the sovereignty, independence and integrity of States, the self-determination of peoples, sovereign equality, the rejection of the interference in the internal affairs of States and international cooperation for mutual and equitable benefit and interest, as well as peaceful relations among States.

States must preserve their pivotal role irrespective of the involvement of private actors or other sectors, as they have a high impact in relation to the development of policies and regulations, crisis prevention and can prevent conflict escalation. In this regard, they must have equal relevance and participation in Internet governance, especially in the decision-making regarding public policies, as well as greater cooperation that allows public administrations to discharge their duties under equal conditions.

The fundamental objective of this contribution is to ratify Cuba's commitment to international peace and security in

cyberspace and to the resolution of conflicts between States through peaceful means.

ASPECTS TO BE MENTIONED IN THE FINAL REPORT

The final report of the OEWG should have a pragmatic and action-oriented approach, with concrete recommendations to the Secretary-General, calling for the appropriate commitment of States to a safe and peaceful cyberspace. In that regard, it is proposed that the following aspects be incorporated:

(1) Addressing issues arising from the potential application of international law and the Charter of the United Nations in cyberspace, in particular Article 51.

(2) Addressing the issue of countermeasures, on the understanding of counteracting their harmful effect with an approach to conflict prevention in cyberspace;

(3) Addressing the issue of attribution and due diligence, defining the need for their application in the face of cyber-attacks;

4) Speak out against the militarization of cyberspace.

EXISTING AND POTENTIAL THREATS

Threats are of a changing nature and the new technologies do not pose a threat per se, but it is their dangerous use which could bring about challenges for international peace. In that regard, work should be focused on the responsible use of ICTs by States. It is also important to take into consideration the deployment on the Internet of emerging technologies that pose risks for the security of cyberspace when they have public IP addresses associated (*resources*

with potential for inappropriate use), as is the case of the Internet of Things (IoT).

The variety of actors participating in cyberspace significantly increases the risks, an element to be considered in terms of responsibility in the face of harmful actions that may stir up conflicts between States.

PROTECTION OF CRITICAL INFRASTRUCTURE

Critical infrastructures are indispensable elements for social the stability and national security of countries, which is why their protection becomes a priority. To this end, it is considered appropriate to propose the following measures:

a) Elaborate an agreed definition of international critical infrastructure by category;

(b) Protect Internet protocols subject of the possible perpetration of cyber-attacks;

(c) Promote cooperation and information exchange regarding specific-purpose malicious code activity on networks (e.g. *Stuxnet*) without compromising the capabilities and national security of States;

d) Promote specific rules to prevent one State from attacking the critical infrastructure of another.

INTERNATIONAL RIGHT

Cuba reaffirms the application of the principles of international law and the Charter of the United Nations in cyberspace, in particular those relative to sovereignty, territorial integrity and non-interference in the internal affairs of States, to the use of ICTs, since the cybersecurity, although it involves other actors, is a responsibility of States.

It is unacceptable to equate the malevolent use of ICTs with the concept of armed attack provided for in Article 51 of the Charter, with which the alleged applicability of the self-defense is intended to be justified, in that context.

We emphasize the importance of the balanced approach to issues such as the free flow of information and human rights, particularly with regard to freedom of expression and opinion, taking into account the provisions set out in the main international instruments, particularly article 19 of the Covenant on Civil and Political Rights, and respect for the principles and purposes of the Charter of the United Nations.

Cuba advocates the recognition of education, culture and development, highlighting the particular relevance of the latter due to the obstacles faced by developing countries, such as the lack of resources to expand investment and connectivity, lack of infrastructure, problems with intellectual property and technology transfer.

Cyberspace has characteristics that make it different from the kinetic world. It is an environment in which tracking down the route of a cyber-attack in real time becomes a major challenge. Behind an IP address, scenarios which are complex to model are revealed. For example, zombie networks (*botnets*), used to attack country targets through devices located in third-party networks, make it difficult to establish the true source of the attacks. The foregoing also poses a challenge to the problem of attribution.

International norms must enable and call for conflict prevention, ensure a peaceful cyberspace and stable development. Similarly, they must lead to political commitments by States with tangible expressions, beyond simple statements. In this connection, the legislation in force

against cybercrime or the Budapest Convention does not have universal application and was not negotiated within the United Nations.

This situation calls for the implementation of specific regulations complementary to international law aimed, among others, at the following equally important elements:

(a) Preventing the application of unilateral measures and measures against states measures that hinder universal access to the benefits offered by ICTs.

(b) Mitigating the malignant effects of attribution in the face of cyber-attacks;

(c) Preventing the militarization of cyberspace;

(d) Protecting citizens' private data more effectively by promoting international regulations in this respect;

(e) Complementing legislation on cyberterrorism in order to face cybersecurity incidents and problems, such as cyberattacks.

(f) Define by consensus what is understood by a cyber-attack;

g) Operationalizing the application, with greater objectivity, of the principles of international law in this area.

CONFIDENCE-BUILDING MEASURES, TRANSPARENCY AND CAPACITY-BUILDING

Confidence-building, transparency and capacity-building measures are applicable and desirable, because they make an important contribution to the peaceful resolution of conflicts and make cooperation among States possible. Nevertheless, it is very important to draw up and implement

specific international regulations or norms for cybersecurity, which would strengthen international law.

It is important to agree on confidence-building measures as a complementary way to enhance cooperation and transparency and to reduce the risk of conflicts.

Cuba's cooperation with various countries has strengthened the social informatization and thus has allowed for the increase of the country's capabilities. The changing nature of ICTs makes them evolve rapidly, therefore, in this area, that the most important aspect of capacity-building is linked to the training and development of human resources, a process that must be characterized by periodicity.

It is necessary work towards building capacity especially in developing countries, which are the most vulnerable, in order to increase their potentialities of coping with threats and to reduce the existing digital divide.

It is important to take into consideration that the implementation of these measures must ensure the non-interference in the internal affairs of States and a thorough review, in the case of ICTs, that ensures the absence of backdoors and other hidden functions in devices that could compromise the national security of the receiving States. Furthermore, this should be in line with the particular needs of States and meet the specific requests from States.

Having expressed the above elements and as part of Cuba's participation in the OEWG, it is considered appropriate to propose the following measures:

1. Increase cooperation to address cyber incidents, exchanging information that does not compromise the

privacy of States with respect to their capabilities or contravene national laws;

2. Establish a central mechanism under the auspices of the United Nations for the verification processes among states in order to mitigate the potential harmful effect of "peer review", which is a complex issue as its inadequate implementation could be detrimental to the sovereignty, interests and internal affairs of States;

3. Implement mechanisms for technical assistance, based on respect for the national legislation of States;

4. Publish studies related to vulnerabilities and hidden functions identified in ICTs, without compromising the national security, infrastructures or services of States;

5. Exchange good practices in tackling cyber incidents, especially among CERTs, in order to increase the operational capabilities of countries in addressing cyber-attacks;

6. Standardize, as far as possible, the classification of cyber incidents in the search for a common terminology, with a view to facilitate the exchange of information among international incident response mechanisms;

7. Establish official focal points among States, at the technical and political levels, in order to ensure the proper processing of the information exchanged and the expeditious coordination of actions in the face of cyber incidents.

8. Combine efforts among the States' technical oversight mechanisms in order to ensure the mutual update of the knowledge base and, consequently, to enhance research and operational capacity;

9. Implement certification programs (with financing facilities) for specialists, mainly from developing countries, in areas related to ICT security;

10. Offer courses on a regular basis with updated content that add tangible value to the countries' cyber incident management processes;

11. Provide Incident Response Teams with tools to capture and process digital evidence, contributing to increase their operational capability.