23rd Annual Meeting

Asia Pacific Parliamentary Forum

Sponsored by: Mexico, Chile, Ecuador, Korea, Indonesia, Canada, Australia

RESOLUTION ON CYBER SECURITY AND RIGHT TO PRIVACY

Recalling the Busan Declaration on the Future Role of Telecommunications / ICTs adopted at the Ministerial Meeting of ICT in Busan, Korea, in October 2014;

Highlighting the importance of the Tunis Agenda for the Information Society to ensure stability and security of the Internet and ensure the legitimacy that requires its governance, based on the participation of all stakeholders;

Reaffirming that the same rights that people have outside internet must be protected when they are connected to the network, as established by resolution A / HRC / 20 / L.131 June 2012 and A / HRC / RES / 26 / 132 June 2014 the United Nations Human Rights Council and the resolution A / C.3 / 68 / L.45 / Rev.13 November 2013, the UN General Assembly;

Bearing in mind the fact that information and communication technologies are heavily used by children; increasing the risk of their exposure to exploitation, violence-related matters, and child pornography; and in this regard recalling the Convention of the Rights of the Child and the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography;

Recalling the 2010 UN General Assembly Resolution 65/230 on the importance of a comprehensive study on cybercrime; UN General Assembly Resolution 2011/33 on the prevention, protection and international cooperation against the use of new information technologies to abuse and/or exploit children;

Highlighting the need for efforts to build a secure and reliable cyber space as cyber security problems arise as a result of rapid development and increasing dependence on information and communication technologies, or ICT;

Acknowledging that cyberspace is abused for criminal and terrorist activities and that this is a critical problem that can cause serious damage not only to property but also the loss of human lives and agreeing that anonymity and interconnectivity in cyberspace present major challenges in taking appropriate measures to combat the abuse of cyber space for cyber attacks crimes and cyber terrorism;

Recognizing that it is not a desirable approach for the government alone to address cyber threats, since most internet infrastructure is privately owned;

Noting that the existing digital divide between countries hinders efforts to ensure a safe and reliable cyberspace;

Aware of the borderless nature of cyber space, the individual efforts of a country to address the problems of cyber security are not sufficient;

Whereas the Universal Declaration of Human Rights determines that no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation;

Taking into account the resolution of the United Nations General Assembly A / RES / 68/167 of January 21, 2014 on the right to privacy in the digital age, adopted by the General Assembly on December 18, 2013, which provides for the protection and promotion of the right to privacy;

Aware of the need to ensure the Protection of Human Rights and Fundamental Freedoms (1950), the International Covenant on Civil and Political Rights (1966), and other applicable international human rights agreements that reaffirm every person's right to defend their opinions without interference, as well as freedom of expression, which includes freedom to seek, obtain and communicate information and ideas of all kinds, as well as the right to privacy; and together with the OECD that issued a series of standards for the safety of information systems in 1992, aimed at the creation of bases for the states and the private sector to build a security framework for information systems;

Referring to Resolution a 22 / RES-03 on Cooperation in the fight against organized crime and the implementation of new policies on drugs, adopted at the 22nd Annual Meeting in Puerto Vallarta, Mexico, where the need to deal with traditional and non-traditional threats that pose several risks for peace and stability, such as terrorism, the conflict of territorial sovereignty and the risks of cybercrime that must be addressed with an innovative regional approach were discussed;

Recalling Joint Ministerial Statement (Joint Ministerial Statement), in particular Annex A "APEC Statement on Promoting the Use of Interoperable Global Data Standards" ("APEC Statement on Promoting the Use of Interoperable Global Data Standards") issued in Beijing, on November 8, 2014, on the 22nd Annual Meeting of Ministers of APEC Economies, which states that as the relevance of transactions increases, both of governments and of the private sector, the importance of ensuring that the systems of key players are interoperable also increases; therefore, it appreciates the efforts to achieve a dialogue on policies aimed at global standards for computer data;

Recalling also Annex F "APEC Initiative of Cooperation to Promote Internet Economy" (APEC Initiative of Cooperation to Promote Internet Economy) to Joint Ministerial Statement of the 22nd Annual Meeting of APEC Ministers held in recent years, the ICTs were integrated into traditional industries turning them into a new, more integrated economic ecosystem, thus these technologies facilitate trade, access to information, which empowers consumers; and improve opportunities for small and medium companies as well as individual entrepreneurs;

Aware of the need to ensure that the same rights that people enjoy offline must also be protected online;

Recognizing that lawful surveillance, subject to appropriate safeguards within legal processes duly established and oversight, may be an important tool in support of the duty of governments to ensure the safety and security of their citizens, and to protect the human rights of persons in their territory and subject to their jurisdiction;

Concerned, however, that unlawful mass surveillance of online communications could violate the right to privacy, of individuals or of the sovereignty and security of states and could interfere with freedom of expression;

Interested in establishing mechanisms to share experiences and knowledge to tackle cyber crime and espionage;

Convinced that the reality described calls to defend human rights, civil liberties, to foster regional and national independence in the provision of telecommunications services and internet, as well as the defense of international law and the principle of

network neutrality;

RESOLVES TO:

1. **Urge** the nations to promote legislative action or public policies to reject and inhibit espionage and mass surveillance that violate the Human Rights and violates International Law and threatens the economy and markets independence and affect international relations and respect among States;

2. **Promote** cooperation between the public and private sectors to share the cyber security strategy defined by governments and international organizations and formulate measures in terms of technology and management, and sharing best practices among countries;

3. **Strengthen** measures to protect individual freedom and privacy and to improve cooperation between governments, agencies concerned, private companies and civil society to counter cyber attacks and crimes, and request a strong partnership for technology support and capacity building to combat cyber crimes;

4. **Encourage** member states to share ICTs where practicable and help with capacity building efforts through the strengthening of human talent to achieve best practices in cyber security and training programs to protect key information and communications infrastructure;

5. **Invite** member states to develop a mechanism that allows taking joint action to deal with cyber security problems;

6. **Reaffirm** the commitment of member countries of the Asia Pacific Parliamentary Forum to respect human rights at all levels, especially those related to privacy, freedom of expression including in the digital environment;

7. **Urge** the APPF Member States to have and adjust where necessary efficient legal regulations to provide whistleblowers appropriate means to report wrongdoing within government, including illegal activity that violates civil rights;

8. **Strengthen** where necessary mechanisms and powers of parliamentary oversight over the activities of the intelligence services to ensure that they are always kept under the law;

9. **Promote** regional agreements and framework laws that ensure that the powers of national intelligence agencies respect international laws in this regard;

10. **Strengthen** cooperation among governments, concerned agencies, private companies and the civil society to counter cyber attacks, crimes and cyber terrorism, and request a strong partnership for technology support and capacity building to combat cyber crimes and cyber terrorism;

11. **Promote** a legal framework that allows the internet to be free of cyber attacks;

12. **Promote** the use of free software where practical, which allows encrypting communication and technology design, thus incorporating safeguards for the privacy of users in the countries of the Asia Pacific region;

13. **Encourage** establishment for a regional consensus for defining and classifying the behaviors of information and cybercrime to legislate as necessary to ensure the protection of society against crimes. And promote the creation of an International

Agency to fight cybercrime. And ensure relevant enforcement agencies and the Judicial Systems properly skilled in ICTs;

14. **Call** upon APPF Member States to establish laws and regulations protecting minors from becoming victims of cyber crime;

15. **Emphasize** the importance of strengthening regional and bilateral cooperation through Mutual Legal Assistance (MLA) in criminal matters.

Quito, January 14th, 2015