



28th ANNUAL ASIA-PACIFIC PARLIAMENTARY FORUM MEETING (APPF)

Canberra, Australia, 13-16 January 2020

“Promoting cooperation to strengthen cybersecurity”

Resolution Proposal sponsored by the Chilean House of Representatives

Remembering the Sustainable Development Goals from the 2030 Agenda adopted in September 2015, whose Goal 16 has the purpose of promoting peace, justice and the building of efficient, inclusive and transparent institutions, which implies the obligation of guaranteeing access to public information;

Bearing in mind the 2016 Report of the World e-Parliament, prepared by the Interparliamentary Union, which confirms that information and communication technologies (ICT) can transform parliaments, that parliaments must commit to digital transformation and that social networks are important tools that allow citizens to easily connect with their elected representatives;

Reaffirming the current international treaties, especially that set out in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, where every person is entitled to participate in their country’s government, as well as having the right to a private life, freedom of expression and freedom of association;

Reasserting that the same rights people have outside the Internet must be protected when they connect the web, just as established in resolutions A/HRC/20/L.131 from 29 June 2012 and A/HRS/RES/26/132 from June 2014 of the United Nations Human Rights Council;

Considering that, although ICTs have a great potential to foster civic participation and progress towards strengthening democracy, they are vulnerable to surveillance, interception and wrongful collection of personal information by States, companies and other non-governmental sectors;

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

Bearing in mind that children use ICTs a lot, increasing the risk that they are exposed to exploitation, violence and child pornography, and remembering in this regard the Convention on the Rights of the Child and the Optional Protocol to the Convention on the Rights of the Child related to child trafficking, child prostitution and the use of children in pornography;

Remembering United Nations General Assembly Resolution 65/230 from 2010 on the importance of an exhaustive study about cybercrime;

Considering Resolution 68/167 approved in 2013 by the United Nations General Assembly where, apart from acknowledging the global and open nature of the Internet and of information and communication technology, the progress of ICTs as a tool that is capable of accelerating development in many areas, the right of every person to a private life, States are urged to guarantee the protection of people’s private lives, of their rights, as well as to review their procedures, practices and legislation regarding information surveillance, interception and wrongful collection of personal information;



Bearing in mind the resolution of the United Nations General Assembly 68/167 about the right to privacy in the digital era, adopted by the General Assembly on 18 December 2013, which considered the protection and promotion of the right to privacy;

Acknowledging that legal surveillance, subject to suitable safeguards within the framework of duly established and supervised legal processes, can be an important instrument in supporting the duty of governments to guarantee the safety of their citizens and of protecting the human rights of people within their territory that are subject to their jurisdiction;

Concerned, however, by the fact that the indiscriminate illegal surveillance of online communications can violate the right to a private life, of the people or the sovereignty and security of the States and can interfere with freedom of expression;

Acknowledging that cyberspace is inappropriately used for illegal and terrorist activities and that this is a critical problem that can cause serious damage not only to property but also lead to the loss of human lives;

Agreeing that anonymity and interconnectivity in cyberspace contemplate important issues when it comes to adopting suitable measures to combat the wrongful use of cyberspace regarding cyberattacks and cyberterrorism;

Acknowledging that it is not desirable that the Government alone addresses the cyber threats, since most of the Internet infrastructure is private property;

Considering that the digital gap there is between countries complicates efforts to guarantee a safe and reliable cyberspace;

Aware that given the borderless nature of cyberspace, the individual efforts of a country to address the issues of cybersecurity are insufficient;

Acknowledging that the Asia-Pacific region is a geographical area that is subject to large scale natural disasters and that ITC, especially cyberspace, is an invaluable tool to reinforce education and sensitize communications about the reduction of disaster risks, as reflected in the Sendai Framework for Disaster Risk Reduction 2015-2030;

Ratifying the principles of the Asia-Pacific Parliamentary Forum destined to consolidate peace, freedom, democracy and the respect of human rights contained in the Declaration of Tokyo from 1993, the Declaration of Vancouver from 1997, the Declaration of Valparaiso from 2001 and the New Declaration of Tokyo from 2012;

Observing that the promotion of civic commitment is key for strengthening democracy and that the 2015 APEC Leaders' Declaration acknowledges the fact that to achieve inclusive growth, it is necessary to have participation from all sectors and segments of society, including women, young people, disabled people, indigenous peoples, low income groups, among others;

Acknowledging that innovation can help face the challenges and create progress towards sustainable development, just as mentioned in the 2016-2025 Strategic Plan of the APEC Policy Partnership on Science, Technology and Innovation and Resolution N°10 about Promoting Innovation and Connectivity, approved during the 24th Annual Meeting of the Asia-Pacific Parliamentary Forum;

Recalling the Joint Ministerial Declaration, in particular its Addendum A "the APEC Statement on Promoting the Use of Interoperable Global Data Standards", adopted in Beijing, on 8 November 2014, in the 22nd Annual Meeting of APEC Ministers, which confirms that as the relevance of transactions, of governments and the private sector increases, the importance of safeguarding the



interoperability of key players' systems also increases; so efforts to reach a dialog about the policies destined to establish international IT data standards are appreciated;

Also **recalling** Addendum F "APEC Initiative of Cooperation to Promote Internet Economy" of the Joint Ministerial Declaration of the 22nd Annual APEC Ministers Meeting, ICTs are integrated to the traditional industries, converting them into a new more integrated economic ecosystem, where these technologies facilitate trade, access to information, which in turn empowers consumers; and where these improve opportunities for small and medium sized companies as well as for individual businessmen and women;

Resolving hereby to:

Strengthen the commitment of the member countries of the Asia-Pacific Parliamentary Forum to respect human rights in cyberspace, especially those related to privacy and freedom of expression;

Reaffirm the commitment of the member parliaments of the APPF to protect freedom of expression and privacy, and to foster cooperation between governments, stakeholder organizations, private companies and civil society to counter cybercrime and cyberattacks, solidifying technological collaboration and the creation of capacity to fight cybercrime;

Encourage member parliaments of the APPF to effectively legislate to provide affected parties with suitable means to report irregularities in the government, including illegal activities which violate civil rights;

Urge parliamentarians to promote legislative actions to reject and inhibit widespread espionage and surveillance that violates Human Rights and International Law, threatens the economy and the independence of the markets and that affects international relations and respect between States;

Reinforce parliamentary supervisory powers and mechanisms of intelligence service activities in cyberspace to guarantee that laws are always respected;

Encourage competent authorities to promote regional cooperation projects to define regional standards which guarantee that domestic intelligence entities respect international cyberspace laws;

Encourage the use of free software which allows encrypting communication in cyberspace, thus incorporating safeguards for the privacy of the region's users;

Promote a regional consensus to define and classify the behavior of information and cybercrime, to legislate as needed to guarantee society's protection against crime;

Promote the creation of a regional agency to fight cybercrime and guarantee that the entities in charge of enforcing the law along with the legal systems are duly trained in ICT related matters;

Foster cooperation between the public and private sector, in APPF member countries in cybersecurity strategies in technology and administration aspects, defined by the governments and international organizations;

Invite member parliaments to develop mechanisms that allow launching joint actions to face cybersecurity problems;

Promote cooperation between governments, competent entities, private companies and civil society to fight cyberattacks, cybercrime and cyberterrorism, and request a solid association for technological support and the creation of capacity to fight cybercrime and cyberterrorism.

Encourage the exchange of best practices in legislative matters to allow harmonizing legal frameworks to protect the Internet from cyberattacks;



Encourage Member States to collaborate in capacity creation efforts by strengthening human talent and training programs to protect key information and communication infrastructure;

Invite the member States to disclose and share their best practices regarding the use of cyberspace.