

APPF28/RES/18

RESOLUTION ON PROMOTING COOPERATION TOWARDS ENHANCING CYBERSECURITY

(Co-Sponsored by Chile and Australia)

We the parliamentarians of the Asia Pacific Parliamentary Forum (APPF), gathering in Canberra, Australia, for the 28th Annual Meeting of the APPF under the theme *Parliamentary Partnerships for 2020 and Beyond*:

Recalling all relevant resolutions of the UN General Assembly and the UN Human Rights Council, the most recent of which are Assembly resolution 73/17 of 26 November 2018 on the impact of rapid technological change on the achievement of the Sustainable Development Goals and targets, Assembly resolution 73/179 of 17 December 2018 and Council resolution 37/2 of 22 March 2018 on the right to privacy in the digital age, Assembly resolution 73/218 of 20 December 2018 on the information and communications technologies for sustainable development, and Council resolution 38/7 of 5 July 2018 on the promotion, protection and enjoyment of human rights on the Internet, and Council resolution 41/11 of 11 July 2019 on new and emerging technologies and human rights;

Reasserting that the same rights people have outside the internet must be protected when they are connected, as established in resolution A/HRC/20/L/131 from June 29, 2012 and A/HRC/RES/26/132 from June 2014 from the United Nations Commission on Human Rights;

Taking note of the UN Secretary-General's strategy on new technologies, including the work of the High-level Panel on Digital Cooperation and the report submitted by the Panel to the Secretary-General on 10 June 2019;

Acknowledging the work of the United Nations, including the Open Ended Working Group and the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE), and its 2010, 2013 and 2015 UNGGE Reports;

Welcoming the conclusions of the Group of Governmental Experts, in its 2013 and 2015 reports, that international law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful cyberspace. Also that agreed norms, rules and principles of responsible behaviour of States in the use of cyberspace can reduce risks to international peace, security and stability, and that, given the unique attributes of such technologies, additional norms can be developed over time;

Noting that considerable progress has been achieved in developing and applying the latest information technologies and means of telecommunication;



Affirming that we see in this progress the broadest positive opportunities for the further development of civilization, the expansion of opportunities for cooperation for the common good of all States, the enhancement of the creative potential of humankind and additional improvements in the circulation of information in the global community;

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;

Recognising the vital importance of cyber security for the digital economy, given that an open, secure, stable, accessible, and peaceful cyber environment is critical to connectivity and economic development, as well as the digital economy's increasingly important role as a driver of global economic growth, and further emphasising our resolve to promote a peaceful, secure and resilient cyberspace, which can contribute to regional security and stability; and

Noting that the dissemination and use of information technologies affect the interests of the entire international community and that optimum effectiveness is enhanced by broad international cooperation.

RESOLVE TO:

1. **Support** capacity-building including the development of regional approaches to capacity-building, which would be beneficial, as they could take into account specific cultural, geographic, political, economic or social aspects and allow a tailored approach, and the development and use of e-learning, training and awareness-raising with respect to cyber security;
2. **Provide** assistance to build capacity in the area of cyber security which is essential for international security, by improving the capacity of APPF Member Countries for cooperation and collective action and promoting the use of such technologies for peaceful purposes;
3. **Reaffirm** the commitment of the member parliaments of the APPF to protect freedom of expression and privacy;
4. **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;
5. **Urge** parliamentarians to promote legislative actions to reject and inhibit widespread 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;

-
6. **Recommend** APPF Member Countries exchange information and invest in communication technologies and human resources, where practicable, to strengthen capacity to manage threats in cyberspace;
 7. **Recommend** that APPF member countries coordinate within the region utilising global mechanisms to enhance cyber-security and combat cybercrime and terrorist use of ICT;
 8. **Foster** cooperation to support secure and resilient digital infrastructure, and effective information exchange within the region;
 9. **Call** on APPF Member Countries to share best practices and means, including exchange of information, technical assistance, and enactment of laws and regulations on responsible use of cyberspace, in formulating and implementing cyber-security strategies;
 10. **Endorse** APPF Member Countries' cooperation between public and private sectors in cyber security capacity building, noting that the private sector owns and operates most of the region's telecommunications infrastructure; and
 11. **Encourage** APPF Member Countries to put more effort into raising awareness and promoting responsible use of cyberspace through formal digital literacy education programs.