

## RESOLUTION ON STRENGTHENING CYBER SECURITY IN THE ASIA-PACIFIC REGION

### *Draft Resolution Sponsored by Thailand*

We, the parliamentarians of the Asia-Pacific Parliamentary Forum (APPF), gathering in Bangkok, Thailand, for the 30<sup>th</sup> Annual Meeting of the APPF under the theme *Parliaments and the Post-COVID-19 Sustainable Development*:

**Recalling** the 73<sup>rd</sup> Session of the United Nations General Assembly resolutions on developments in the field of information and telecommunications in the context of international security (A/RES/73/27) and on advancing responsible State behavior in cyberspace in the context of international security (A/RES/73/266), which were adopted in 2018;

**Bearing** in mind the 2030 Agenda for Sustainable Development, which highlights the importance of information and communication technologies (ICTs) and digitalization as powerful enablers of socio-economic growth and the need of national and international efforts to address an increase in cyberattack attempts;

**Reaffirming** the 132<sup>nd</sup> Inter-Parliamentary Union (IPU) Assembly resolution on cyber warfare: a serious threat to peace and global security in 2015, which calls on all Member Parliaments to review their countries' legal framework to examine how to best adapt to potential threats which may arise from the evolution of cyberspace and to ensure their national laws do not condone the criminal use of cyber technology with the purpose of instigating conflict between States;

**Recalling** all the APPF relevant resolutions on cyber security, including the 23<sup>rd</sup> APPF resolution on cyber security and rights to privacy adopted in Quito, Ecuador, in 2015, the 27<sup>th</sup> APPF resolution (APPF27/RES/13) on strengthening parliamentary cooperation in promoting the responsible use of cyberspace (information space) for social progress adopted in Siem-Reap, Cambodia, in 2019 and the 28<sup>th</sup> APPF resolution (APPF28/RES/18) on promoting cooperation towards enhancing cyber security adopted in Canberra, Australia, in 2020;

**Noting** the public's concern on the growing frequency and severity of cyber crimes and cyberattacks as a result of the increased dependence on the use of internet network in all aspects, particularly following the outbreak of the COVID-19 pandemic;

**Expressing** concern that unauthorized access to information systems and illegal activities in borderless cyberspace would threaten individual privacy, public safety and impose risks on national security at an unprecedented level;

**Recognizing** that cyber governance is essential for protecting the right of privacy and freedom of expression, and hence meaningful cooperation among all stakeholders including governments, private sector, intergovernmental agencies is urgently needed to address cyber threats and to promote open, safe, secure, accessible, interoperable, peaceful and resilient cyber environment; and

**Noting** that APPF Member Parliaments can play a role in exchanging standard of best practices and establishing a common legislative framework to help combat cyber threats, such as computer viruses, malware, and phishing attacks, among others.

**RESOLVE TO:**

1. **Call on** APPF Member Parliaments to exchange parliamentary best practices in dealing with cyber threats and attacks on information infrastructures with an aim to create a common legislative framework for cyber security in the Asia-Pacific region including their domestic laws to effectively address challenges in cyber security;

2. **Raise** awareness among parliamentarians of APPF Member Parliaments on the use of information and communication technologies (ICTs) in achieving the SDGs with universal commitments to digital peace;

3. **Recommend** APPF Member Parliaments to observe good governance principles, based on accountability, responsiveness, efficiency and effectiveness, to promote an open, secure, stable, accessible and peaceful cyber environment in accordance with respective domestic laws and international obligations, with an aim to address cases of abuses, and the use of the internet for malicious purposes;

4. **Encourage** APPF Member Parliaments to work closely and continuously together with their respective governments to support new initiatives on cyber security, risk mitigation strategies and new tools to address the severity of potential adverse effects in political, economic and social aspects in cyberspace; and

5. **Encourage** APPF Member Parliaments to engage the public and private sector, and civil society in formulating a common legislative framework, in order to bridge the digital divide and promote digital literacy among the peoples in the Asia-Pacific region.

-----