IGF Internet Governance Forum

Inter-Parliamentary Union
For democracy. For everyone.

Output document from the Parliamentary Track
17th UN Internet Governance Forum

Addressing cyberthreats: National, regional and international approaches

1 December 2022

We, parliamentarians taking part in the Parliamentary Track at the 17th UN Internet Governance Forum,

Coming together in the context of the 17th United Nations Internet Governance Forum (IGF) and discussing issues relating to national, regional and international approaches – State-led, multilateral, and multistakeholder – to addressing cyberthreats,

Welcoming the continuation and strengthening of the IGF Parliamentary Track, and building on the recommendations of the 2019, 2020 and 2021 editions that national parliaments cooperate and exchange good practices in dealing with digital policy issues,

Acknowledging the role of the United Nations Department of Economic and Social Affairs (UN DESA), the Inter-Parliamentary Union (IPU) and the House of Peoples' Representatives of Ethiopia in co-organizing the IGF 2022 Parliamentary Track, as well as the support provided by the IGF Secretariat,

Recalling United Nations General Assembly resolution 74/304 of 9 September 2020 which encourages strengthened cooperation between the United Nations, national parliaments and the Inter-Parliamentary Union,

Taking note of the United Nations Secretary-General's *Roadmap for Digital Cooperation* and *Our Common Agenda* report, which emphasize the importance of strengthened multistakeholder cooperation in ensuring online safety and security,

Noting that, as the Internet and digital technologies increasingly shape our economies and societies, they also create vulnerabilities for individuals, public and private entities, critical infrastructures, and much more,

Recalling that "cybersecurity" and "cybercrime" are related but distinct issues, "cybersecurity" being something that needs to be improved and "cybercrime" being something to be prevented, *Noting* the importance of international instruments such as the Council of Europe's Convention on Cybercrime (Budapest Convention) to which there are currently 68 State Parties, and of regional instruments such as the African Union's Convention on Cyber Security and Personal Data Protection (Malabo Convention), and the role that such instruments can play in furthering international and regional cooperation,

Acknowledging that geopolitical concerns are never absent from discussions on cybersecurity, while affirming that all countries share a common interest in enhancing cybersecurity and combatting cybercrime,

Acknowledging also that the cyber landscape is complex and that countries are at different levels of readiness to deal with cyberthreats,

Noting that cybersecurity and cybercrime issues have cross-organizational and cross-border dimensions, and that tackling them requires:

a) Whole-of-government and whole-of-society approaches involving strong partnerships and coordinated efforts between relevant authorities and agencies, the private sector, the technical community, academia, and civil society,
b) Efficient and effective regional and international cooperation, both intergovernmental, multilateral and multistakeholder,

1. *Call upon* parliaments, governments and all other stakeholders to work together to develop policy, regulatory and legislative frameworks for enhancing cybersecurity and tackling cybercrime and *recommend* that such frameworks:

a) Are developed in an open and transparent manner, with the involvement from the onset of all relevant governmental and non-governmental actors;
b) Embed a human-centred security approach and incorporate the principles of rule of law, judicial oversight, proportionality, accountability, and transparency;
c) Provide sufficient funding to ensure that the authorities tasked with the implementation of those frameworks are adequately equipped – in terms of financial, technical, and human resources – to perform their tasks;
d) Clearly define the roles and responsibilities of relevant public and private actors in a manner that allows meaningful and effective collaboration towards a more secure cyberspace;
e) Draw upon internationally agreed technical standards for cybersecurity;
f) Are coherent with existing legislation developed for the analogue world, for example, legislation to combat hate speech or fraud;

2. *Also call upon* parliaments to ensure a proper balance between measures to enhance cybersecurity and tackle cybercrime, on the one hand, and the protection of internationally recognized human rights and fundamental freedoms, on the other hand, and in particular to:

a) Ensure that cybersecurity frameworks are complemented by strong data protection laws;
b) Encourage effective cooperation between the intelligence services and other government departments, and seek transparency and accountability from intelligence services tasked with cybersecurity;

c) Avoid the use of cybersecurity measures for political purposes, for example to target opposition politicians;

3. *Further call upon* parliaments to:

a) Engage in regular dialogue with relevant ministries and agencies, ensure that the government is paying appropriate attention to addressing cyberthreats, and hold authorities to account for progress in enhancing cybersecurity and combatting cybercrime;
b) Consider the most appropriate institutional mechanisms for addressing cyberthreat-related issues in parliaments, including by clarifying the mandate of existing parliamentary committees or creating dedicated committees;
c) Encourage effective cooperation between public authorities and the private sector in strengthening cybersecurity and the creation of an environment of trust conducive of such cooperation;
d) Examine the potential for digital technologies such as artificial intelligence to be used in the fight against cybercrime, and the appropriate human rights safeguards needed to avoid misuse of such technologies;

4. *Call upon* parliamentarians to:

a) Contribute to efforts to raise awareness, build capacities and develop a culture of cybersecurity across society;
b) Translate cybersecurity issues into concepts that are accessible to people, help the public to understand what is at stake, and build political will to address cyberthreats;
c) Use every opportunity to encourage members of the public to practice good cyber-hygiene;
d) Focus attention on encouraging women to take up careers in the field of cybersecurity, as well as on combatting cybercrime incidents that have women as targets;
e) Find ways to bring the conversation on cyberthreats into the mainstream political debate, attract media attention and increase pressure for governmental action;
f) Consider organizing special events in parliaments to focus attention on cyberthreats, such as dedicated “cybersecurity days” or a question time with relevant ministries and agencies;

5. *Encourag*e parliaments, considering the potential of regional and international instruments in fostering harmonization of legal and regulatory frameworks for cybersecurity and cybercrime, as well as strengthening international cooperation, to:

a) Consider the ratification of existing international instruments such as the Council of Europe’s Convention on Cybercrime (Budapest Convention) and regional instruments such as the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention);
b) Ensure that ratified conventions are reflected in national policies, regulations and legislation, and are properly implemented at national level;
c) Encourage their governments to participate in the negotiation of new instruments on cybercrime at the United Nations level, and in international processes on norms for responsible state behaviour in cyberspace;
d) Also encourage their governments to ensure that their positions in such processes are informed by a multistakeholder dialogue and that any new instruments work in partnership with existing standards on the rule of law and human rights instruments;

6. *Call upon* international development partners to:

a) Involve parliaments at all stages in initiatives dedicated to supporting the development of policy, regulatory and legislative frameworks for enhancing cybersecurity and tackling cybercrime;

b) Build the capacity of parliamentarians to work on issues related to cybersecurity and cybercrime, as well as on broader digital policy topics, including through training and skills building;

7. *Invite* parliaments to strengthen dialogue and exchanges of experiences with other parliaments and parliamentary bodies, including sharing information about existing and new legislative initiatives related to cybersecurity and cybercrime at a national and regional level;

8. *Call upon* parliaments and parliamentarians to:

a) Contribute to the strengthening of national multistakeholder dialogue on policy issues pertaining to the Internet;

b) Continue and strengthen their engagement with the IGF, take part in national and regional IGF initiatives, and consider the work carried out in these forums as resources to inform their parliamentary discussions and activities;

c) Engage in global processes dedicated to strengthening digital cooperation, such as the development of the Global Digital Compact proposed by the United Nations Secretary-General;

9. *Acknowledge* with appreciation the publication by the IGF Secretariat of the *Guide to key digital policy issues and related processes and organizations: Toolkit for parliamentarians*, and

a) Encourage parliamentarians to make use of this toolkit to inform, as relevant, their work on digital policy issues;

b) Encourage also the maintenance of the toolkit as a living, evolving document;

10. *Call upon* the IGF to further institutionalize the Parliamentary Track and to facilitate regular exchanges between parliamentarians and other IGF stakeholders.