Preventive Measures

José Cepeda
Senator from Spain

Second Intersessional Consultation of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes
Introduction

• The IPU is the global organization of national parliaments
• 178 Parliaments and 14 Associate Members
• The IPU works for peace, democracy, human rights, gender equality, youth empowerment, climate action and sustainable development through political dialogue, cooperation and parliamentary action.
The Context of Action
Global context

- Increased dependence on ICTs
- Increase in occurrences of cyberattacks
- Broad usage of disruption methods on critical infrastructure
- Heightened tensions on the international scene
The Context of Action

Global responsibility

- Cybersecurity of countries requires strong partnerships and coordinated efforts from society as a whole (government, private sector, academia, multilateral and regional partnerships…)
- It is necessary to build a global culture on cybersecurity
The Context of Action

Economic development leads to:
• technological development
• reliable and safe environment
• high level staff training

Proposal: dedicate at least 20% at cybersecurity of all new investments in ICT

Invest in cybersecurity

International coordination:
Preventive and defensive

Geopolitical context (increased dissuasion)
Cyberspace new demonstration of power
Countries require more cyber defence capabilities

Early warning systems (UN global coordination system)
Share: Knowledge, Techniques, Tactics and Intentions
Self-Sovereign Digital Identity Systems (SSI) - Block Chain

Cybersecurity prevention
Cyber intelligence

Define institutional spaces: Critical Infrastructures (incl. Parliaments)
Define critical instances: Electoral Process

Protecting Democracy
The IPU’s Proposal
# The IPU’s proposal

## The Role of Parliaments
- Parliaments need to be involved in negotiations on new conventions on cybercrime
- Parliaments as institutions are targets of cyberattacks
- Parliamentarians can allocate more funds to cybersecurity
- Parliaments can strengthen multilateral networks of communication

## Critical Infrastructures
- Parliaments need to be considered a critical infrastructure
- Parliaments need to pass legislation to protect the country’s critical infrastructure networks
- Parliaments can foster partnerships with the private sector

## Critical Democratic Junctures
- Cyberattacks are often targeted at nations during electoral processes
- Strengthen protection efforts during electoral processes
- Rebuilt trust in democratic institutions
## The IPU’s proposal

<table>
<thead>
<tr>
<th>Implementation of the Convention</th>
<th>Support for parliaments</th>
<th>International Mechanisms</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Parliaments have a role in the implementation and ratification of conventions</td>
<td>• Creation of toolkits and exchanges of good practices to assist parliaments take concrete steps</td>
<td>• Inclusion of parliaments in the creation of international definitions for cybercrime</td>
</tr>
<tr>
<td>• Inclusion of parliamentary perspective to the UN mechanisms</td>
<td>• Meaningful partnerships with international organizations like UNODC</td>
<td>• International consultations for the application of International Humanitarian Law to cyberspace (Tallinn Manual)</td>
</tr>
<tr>
<td>• Strengthening and application of already existing conventions/treaties</td>
<td></td>
<td>• Application of international conventions (Budapest convention)</td>
</tr>
</tbody>
</table>
The IPU’s proposal

Balanced Actions

- Fine balance is needed between defining terms and adapting to new forms of cyberattacks
- Ensure that the freedoms and liberties of citizens are respected where action is taken in cyberspace
- Prevent institutions to misuses and abuse of power, strengthen accountability and transparency

Vulnerable Groups

- Protect the rights of minorities in cyberspace
- Prevent acts of sexual abuse, especially on children

International conventions

- Cybercrime is a crime and shall be treated as such
- The convention on cybercrime shall be implemented on par with other UN crime-related conventions in Vienna
The IPU’s proposal

<table>
<thead>
<tr>
<th>Normative Steps</th>
<th>Post-attack Assistance</th>
<th>Dedicated networks of action</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Adoption of strong norms for the behaviour of states and institutions in cyberspace</td>
<td>• Coordination of response and assistance to the victims</td>
<td>• Creation of computer emergency response teams (CERT) responsible for the protection against, detection of and response to an organization's cybersecurity incidents</td>
</tr>
<tr>
<td>• Due diligence, strong international standards, transparency, multilateral agreements, code of conduct</td>
<td>• National legislation to investigate and strongly punish acts of cybercrime (Interpol)</td>
<td></td>
</tr>
</tbody>
</table>
Multilateral, coordinated action is necessary to sustainably address the issue of cyberattacks.

The IPU wishes to contribute to the integration of parliamentary perspectives to the Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.
Thank you for your attention!

José Cepeda
Senator from Spain
jose.cepeda@senado.es
@Cepeda
jcepedagar