Inter-Parliamentary Union
For democracy. For everyone.

145th IPU Assembly

Kigali, Rwanda
11-15 October 2022

145th IPU ASSEMBLY
2022 | Kigali, Rwanda

Standing Committee on
Peace and International Security

C-I/145/6-Inf.1
13 September 2022

Expert hearing on the theme *Cyberattacks and cybercrimes: The new risks to global security*

Friday 14 October 2022, 14:30 – 16:30
(Room MH1, ground floor, Kigali Convention Centre (KCC))

Concept note

Today, we live in a situation of largescale global conflicts. No government or parliament in the world could foresee the suffering of all our planet's citizens in the face of a pandemic such as COVID-19.

To protect our citizens, all governments made the decision to subject millions of people in the world to restrictive measures and lockdowns.

As a result of being locked down at home, there was an increase in interconnections to networks and in the acquisition of devices, cameras, computers and smartphones to be able to connect to companies and schools, or simply to communicate with family and friends.

This enforced digitization allowed the population to maintain communicative social and professional links with work centres, schools and universities, and especially with public health institutions and the media. People were therefore able to learn in real time about the evolution of the pandemic and the measures being taken in their respective countries.

Rapid and enforced digitization has opened up new spaces that many people did not know about until now. However, at an individual and collective level, riskier new spaces have also appeared where cybercriminals have increased their scope of action using new cyberattack systems.

On the other hand, the serious conflict that we are witnessing in Ukraine has led to hostilities that Europe has not experienced since the Second World War. It has revealed that cyberattacks can also be used to wage war at periods of maximum tension.

We must work towards a ban on lethal autonomous weapons (also known as "killer robots"), prioritize the protection of all nuclear infrastructure from possible external cyberattacks, and prevent a new escalation in the global nuclear threat.

Massive disinformation and propaganda campaigns use digital platforms to contaminate and influence groups, regions or countries. The campaigns are delivered through organized cyber-activists who know that there is a lack of international legal cooperation frameworks.

Direct attacks on a country's critical-infrastructure computer systems put at risk the basic distribution networks for essential goods in our societies.

All this should make us reflect and delve deeper into the global reality that surrounds us as parliamentarians. Knowing the truth today is becoming an increasingly precious asset.

A new digital context also requires action from our parliaments and the United Nations. This will allow the benefits and potential of our knowledge society to be maximized, while minimizing the serious risks that threaten us.

According to article 19 of the Universal Declaration of Human Rights, everyone has the right to receive and impart information and ideas through any media, regardless of frontiers. Therefore, we must guarantee that all citizens in our societies can freely access objective, truthful and good-quality information.

In the spirit of the Universal Declaration of Human Rights, we must ensure public discourse develops so that, rather than confronting, dividing, polarizing or destroying our coexistence with viral hate messages, our democracies can grow stronger and stronger.

We must have the right to protect our data and personal information, which are used to manipulate and change our behaviours, control us, violate our human rights, and undermine democratic institutions.

Legislation is needed to define the limits of opaque algorithms and the use of psychographic profiles by large corporations so as to prevent malicious organizations and cybercriminals from using social networks to influence and manipulate the trends of voters.

We must encourage the public sector, the private sector and civil society to adopt new legislative and self-regulatory frameworks that develop a safe space for global digital cooperation.

As parliamentarians, we must establish international legal cooperation frameworks to be able to effectively combat cybercriminals who work outside any type of control and who can serve dark interests to attack critical infrastructure in our countries.

As they know the limitations of countries' abilities to pursue them, cybercriminals act globally, and develop largescale attacks on users. They deploy all kinds of social engineering and attack techniques. These include: attacks on personal passwords, such as phishing, vishing, smishing and spam; attacks on connections, such as fake wifi, spoofing, cookies, DDoS, SQL and sniffing; and malware attacks, such as viruses, adware, spyware, Trojans, backdoors, keyloggers, stealers, ransomware, rootkits, botnets, rogueware, cryptojacking and other malicious apps.

In 2015, IPU Members adopted a resolution at the Assembly in Hanoi on cyberwarfare, which also addressed cybercrime. The resolution called for an international convention on these crimes.

As for our parliaments, we must offer operational structures capable of protecting particularly vulnerable sectors (such as women, youth, children, companies and critical infrastructure) and seek to develop initiatives that allow us to identify, catalogue, analyse and prevent cyberattacks.

In the context of the Convention on Cybercrime, the IPU can and should make a valuable contribution to the United Nations in the global effort to provide services to prevent, raise awareness, detect and adequately respond to cybersecurity incidents in any country of the world.