Inter-Parliamentary Union
For democracy. For everyone.

146TH IPU ASSEMBLY
المنامة، البحرين
MANAMA, BAHRAIN
11-15 MARCH 2023 - ١١-١٥ مارس ٢٠٢٣

146th IPU Assembly
Manama (11–15 March 2023)

Standing Committee on
Peace and International Security

C-I/146/M
17 January 2023

Cyberattacks and cybercrime: The new risks to global security

***Explanatory memorandum* submitted by the co-Rapporteurs**
Mr. J. Cepeda (Spain) and Ms. S. Falaknaz (United Arab Emirates)

1. We live in a cyber world. Millions of people interact with each other via the internet, connecting using all sorts of devices and sharing their data, personal information, identity and daily activity with the world. Our everyday lives, personal data, health services, infrastructure and security are powered by networks in cyberspace.

2. As technologies have advanced and our dependency on them has increased, cybercrime and cyberattacks, against citizens, vulnerable groups, institutions, governments or States, have also increased, along with the need to ensure our safety and security.

3. The COVID-19 pandemic, with waves of lockdowns in all countries, prompted the purchase and use of electronic devices to facilitate people's connection with the outside world. This process of forced digitalization led to a sharp increase in crimes in the digital world.

4. Parliaments are aware of the risk of this situation for their citizens. To that end, the co-rapporteurs have initiated this resolution to protect people from a hostile cyberspace and to raise awareness in the international community of the need to address cybercrime and cyberattacks, by cooperating and sharing a common vision to act effectively against criminals and hackers who know no boundaries nor borders.

5. The purpose of the resolution is also to examine the challenges involved in combating cybercrime and cyberattacks, strengthening the role of parliaments in facing the associated risks, and contributing to international efforts in this regard.

6. Some of the challenges involved in combating cybercrime and cyberattacks include disagreement on the definitions, outdated legislation and a prevalence of actions that compromise the confidentiality, integrity and availability of computer data. Differences in laws from one State to another often delay the litigation process. The rapid and fast-changing nature of such crimes calls for greater international cooperation.

7. Several cybercrime initiatives have already been launched at the regional and international levels, including the establishment by the United Nations General Assembly of an ad hoc committee charged with elaborating a comprehensive international convention on countering the use of information and communications technologies for criminal purposes. That convention is due to be adopted by the General Assembly at its seventy-eighth session, in 2024. The IPU has also addressed the issue of conflicting interactions in cyberspace through a resolution entitled *Cyber warfare: A serious threat to peace and global security* (2015).

8. Due to the nature of these crimes and their increasing pace, new areas of action and new initiatives at the regional and international level have flourished. For instance:

   (a) the second additional protocol of the Budapest Convention on Cybercrime of the Council of Europe, approved in 2021, which develops a legal shield for the protection of human rights, the rule of law and personal data;

   (b) the new initiatives promoted by some institutions on the obligation for "secure certifications" by manufacturers or suppliers of ICT products or services in their territories or the development of new models for secure and reliable electronic identification and authentication, for example through a personal digital wallet stored in mobile phones using blockchain technology, which may offer new solutions on guarantees, traceability and identity on the internet that some organizations, such as INTERPOL, are requesting in order to prosecute crime.

9. In preparation for the draft resolution, the co-Rapporteurs participated in the following meetings:

   - the second session of the above-mentioned United Nations Ad Hoc Committee, in Vienna in May-June 2022;
   - two multi-stakeholder intersessional consultation meetings hosted by the Chair of the Ad Hoc Committee (June and November 2022), at which they conveyed information on the work of the IPU in the area of combatting cybercrime and cyberattacks;
   - the expert hearing on the theme of the resolution organized by the Standing Committee on Peace and International Security during the 145th IPU Assembly in Kigali, in October 2022, at which they received input from experts and colleagues from different regions of the world, as well as from the Forum of Young Parliamentarians;
   - the parliamentary track of the Internet Governance Forum in Ethiopia in December 2022 to present the importance of a parliamentary vision when addressing future cyberthreats to citizens and shaping a safer and more secure digital space;
   - the online hearing *Creating a safe cyberspace for democracy*, organized in December 2022 by the IPU in collaboration with the Chair of the Ad Hoc Committee to facilitate the inclusion of parliamentary voices in the drafting process of the convention on cybercrime and gather contributions to the present IPU resolution.

10. The co-Rapporteurs also held bilateral meetings with various organizations such as the Organized Crime and Illicit Trafficking Branch of the United Nations Office on Drugs and Crime (UNDOC) and INTERPOL and have been able to see some of the systems for protection against cyberattacks in situ in countries such as Albania, Argentina, Costa Rica, the Dominican Republic, Mexico, Spain and the United Arab Emirates, where they also learnt about the work of security structures and intelligence services, as well as the responses of parliaments and institutions.

11. All these meetings and visits helped to identify various levels where action is needed:

   (a) Cyberattacks between States as part of hybrid warfare actions. The issue of conflict and war in cyberspace has already been studied by the IPU in its 2015 resolution on *Cyber warfare: A serious threat to peace and global security*, which mentions that cyber-defence and cybercrime control measures complement each other. It is worth noting that governments may use the services of non-State actors to carry out cyberattacks on other nation States. This can lead to escalation and may be a threat to international peace.

   (b) Cyberattack campaigns in the form of cyber-espionage, theft of intellectual property, extortion of data and information held by government agencies, parliaments, public or private institutions (ransomware attacks), or attacks on the critical infrastructure of a country carried out by cybercriminals. Some of these campaigns can be defined as “advanced persistent threats” (APTs), which are significantly more complex, large-scale cyberattacks in which intruders establish an illicit, long-term presence on a network in order to mine highly sensitive data.

(c) Cybercrime attacks directed by individuals and related to minor online offences, by which criminal activities are committed using the Internet or other forms of digital communication and which target citizens as a priority. Their aims include, among other offences, identity theft, fraud, distribution of illegal or copyrighted material, drug purchases, money laundering, hate crimes, propaganda, extremist indoctrination and sexual exploitation of women and children, and use different tactics, techniques, and procedures such as phishing, hacking, use of bots or denial of service, making cyberspace an unsafe and hostile place for any citizen anywhere in the world.

12. The response to cybercrime, whether large-scale cyberattacks perpetrated by organized groups or minor online offences perpetrated by individuals, can only be based on international cooperation, with countries pooling intelligence and knowledge of the tactics, techniques and procedures of these hackers.

13. The draft resolution:

- calls upon parliaments to enact new legislation and develop new international cooperative efforts to fight cybercrime and cyberattacks considering the ongoing increase in such acts against citizens, vulnerable groups, institutions, governments or States, their links with fundamental freedoms such as privacy and freedom of expression, the fact that they must not infringe upon or diminish the ability of citizens to enjoy these freedoms, and their implications on international peace and security and global economic stability;
- encourages parliaments to support the efforts of the United Nations to enact a new convention on cybercrime and to use it as a means of strengthening national legislation and increasing international cooperation against cybercrime and cyberattacks;
- calls on parliaments to make the most of their oversight tools to ensure that governments control the rapid increase in cybercrime while taking into account the privacy of cyberspace users;
- also calls on the IPU Secretariat to play an important role in helping parliaments building their capacities by holding specialized seminars, workshops and conferences that can contribute to the understanding and countering of the complex and rapidly evolving nature of cybercrime and cyberattacks.