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)

Cybercrimes: The new risks to global security

Resolution adopted by consensus[*] by the 146th IPU Assembly
(Manama, 15 March 2023)

The 146th Assembly of the Inter-Parliamentary Union,

Condemning all forms of cybercrime and *reaffirming* the need to combat such acts through international cooperation,

Reaffirming the existing United Nations framework for responsible State behaviour in the use of information and communications technologies (ICTs) and the need to implement this framework,

Recognizing the need to build trust and mutual understanding between countries in response to the malicious use of ICTs by State as well as non-State actors, who recognize neither boundaries nor borders,

Observing the growing use of and dependence on ICTs worldwide,

Cognizant of the increase in cybercrime activities due to increasing digitalization, accelerated by the COVID-19 pandemic,

Noting the responsibility of parliaments to build a regulatory framework that protects citizens in cyberspace with new infrastructure and resources, in the same way as in the physical world,

Recalling United Nations General Assembly resolution 31/72 of 10 December 1976 on the *Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques*, resolutions 55/63 of 4 December 2000 and 56/121 of 19 December 2001 on *Combating the criminal misuse of information technologies*, and resolution 57/239 of 31 January 2003 on the *Creation of a global culture of cybersecurity*,

Recalling also the annual resolutions of the United Nations General Assembly on *Developments in the field of information and telecommunications in the context of international security*, and in particular resolution 69/28 of 2 December 2014, resolution 73/266 of 22 December 2018 establishing the Group of Governmental Experts on advancing responsible State behaviour in the context of international security, and resolution 75/240 of 31 December 2020 establishing the Open-ended Working Group on security of and in the use of information and communications technologies 2021–2025, and *highlighting* the voluntary and non-binding norms of responsible State behaviour in the use of ICTs in the context of international security, developed by the Group of Governmental Experts and endorsed by United Nations General Assembly resolution 70/237 of 23 December 2015, which calls on United Nations Member States to be guided by these norms, as well as the establishment, through United Nations General Assembly resolution 77/37 of 7 December 2022, of a United Nations programme of action to discuss existing and potential threats and to support States' capacities and efforts to implement and advance commitments,

[*] The delegation of India expressed reservations on operative paragraph 25.
The delegation of the Russian Federation expressed reservations on preambular paragraph 11 and operative paragraph 1

Recalling further the United Nations *Convention against Transnational Organized Crime* of 15 November 2000 and the United Nations *Convention against Corruption* of 31 October 2003,

Stressing the importance of regional conventions on cybercrime, transnational organized crime, exchange of information and administrative assistance, including the Council of Europe *Convention on Cybercrime* of 23 November 2001 and its *Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems* of 28 January 2003, the *Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization* of 16 June 2009, the *Arab Convention on Combating Information Technology Offences* of 21 December 2010, the Latin American and Caribbean Parliament (Parlatino) *Model Law on Cybercrime* of November 2013 and its updates, the Parlatino *Model Law on Social Prevention of Violence and Crime* of November 2015, the Parlatino *Model Law on Computer Crimes* of February 2021, and the Parlatino *Model Law on Combating Illicit Trade and Transnational Crime* of February 2021, the *Agreement on Cooperation among the Member States of the Commonwealth of Independent States in the Field of Ensuring Information Security* of 20 November 2013, the *Agreement on Cooperation among the Member States of the Commonwealth of Independent States in the Fight Against Crimes in the Field of Information Technology* of 28 September 2018, and the African Union *Convention on Cyber Security and Personal Data Protection* of 27 June 2014,

Stressing also that the Council of Europe *Convention on Cybercrime*, which is open for accession by any country, has become an instrument of global significance, with States Parties from, and impact in, all regions of the world,

Recalling the IPU's work on the various new risks faced by our increasingly digitized societies, including the IPU resolutions *Cyber warfare: A serious threat to peace and global security* (adopted at the 132nd Assembly, Hanoi, 1 April 2015), and *Legislation worldwide to combat online child sexual exploitation and abuse* (adopted at the 143rd Assembly, Madrid, 30 November 2021), which also recalls the Council of Europe *Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse* (the "Lanzarote Convention") of 25 October 2007,

Commending the work of the United Nations on advancing responsible State behaviour in cyberspace,

Commending also the efforts of the United Nations to enact, through General Assembly resolution 74/247 of 27 December 2019, an international cybercrime convention, and *welcoming* the creation of an ad hoc committee charged with drafting this convention,

Welcoming the participation of the IPU in the multi-stakeholder consultation process of that ad hoc committee in order to ensure that the voice of parliaments is heard,

Noting the need for a global approach to the issue of cybercrime and its serious consequences for citizens, as well as the need to protect global peace, security and economic stability while upholding the basic tenets of human rights including freedom of speech,

Recognizing the urgent need for legislators, governments and all stakeholders to take more proactive national steps to combat cybercrime, given its renewed intensity and rapidly evolving nature,

Recognizing also that all actions in this field need to have respect for human rights and fundamental rights at their centre,

Noting the uneven development in countries' ICT application capacity and ability to protect ICT infrastructure, and *emphasizing* the need for increased technical assistance and collaboration, especially for developing countries,

Noting also that States shall act in accordance with their obligations under international human rights law, including but not limited to the *International Covenant on Civil and Political Rights*, the *Convention on the Rights of the Child*, the *Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment*, the *Convention on the Elimination of All Forms of Discrimination against Women*, and additional protocols and other relevant international human rights instruments,

Recognizing the need for common, international parliamentary action to advance awareness and implementation of voluntary and non-binding norms regarding responsible State behaviour in the use of ICTs,

Noting that cybercrime may constitute a serious threat to democratic processes, especially interference in elections through cybersecurity breaches or false social media accounts,

Acknowledging that women, young people, children, elderly people, people with disabilities, and racialized communities are particularly vulnerable to cybercrimes,

Acknowledging also the need for efforts to promote gender equality and the empowerment of women and girls in all their diversity, including through gender mainstreaming, in the development, implementation and application of policies, programmes and legislation in this field,

Noting the nature of the threats and risks of transnational cybercrime to international peace and security, and the tremendous developments in cyberspace, as a result of which the methods used by cybercriminals are becoming increasingly sophisticated,

Noting also that cybercrime includes but is not limited to attacks on computer systems, breaches of privacy, the creation and deployment of malware, and, increasingly, the facilitation of attacks on critical civilian infrastructure, as well as other acts that can occur offline and be facilitated by computer systems, including online fraud, drug trade, money-laundering, hate crimes, human trafficking, and technology-facilitated gender-based violence such as sexual harassment, threats, stalking, bullying, sexist hate speech, and the sexual exploitation of women and children via the internet – all of which negatively affect global security and economic stability,

Considering that most national laws were enacted before cybercrime arose and therefore do not always adequately address these threats,

1. *Encourages* parliaments to consider taking the necessary steps for their country to accede, if it has not yet done so, to existing international instruments that address the use of ICTs for criminal purposes, including the Council of Europe *Convention on Cybercrime*, which is the most comprehensive multilateral cybercrime treaty in force and is open for accession by all States;

2. *Calls upon* parliaments to make sure their legislation on cybercrime is up to date and relevant, in accordance with international law, including international human rights instruments, to allocate the necessary resources to this end and to engage all stakeholders, including the private sector, academia, civil society and the technical community, considering the ongoing increase in the scale, scope, speed, complexity and frequency of such acts and their implications for national security, international peace and security, and global economic stability, as well as to include in such legislation extraterritorial jurisdiction to enable the prosecution of criminal acts, irrespective of where those acts were committed and whether they constitute offences in the foreign jurisdiction in question;

3. *Urges* parliaments to ensure that human rights impact assessments are embedded in all legislative processes on cybercrime;

4. *Calls upon* parliaments to enhance the capacity of law enforcement officers, including investigative authorities, prosecutors and judges, in the field of cybercrime, and to equip them to effectively investigate, prosecute and adjudicate cases of cybercrime offences;

5. *Encourages* parliaments to make full use of their oversight function to ensure that governments have the tools, including appropriate resources and capacity, to prevent and combat the rapid increase in cybercrimes and to protect the cybersecurity, identity, privacy and data of citizens while safeguarding human rights and freedoms;

6. *Strongly recommends* that parliaments ensure that their national legislative frameworks on the protection of critical national infrastructure, including the infrastructure that supports the internet, are up to date, or that they establish such frameworks where necessary;

7. *Encourages* parliaments to promote an open, free and secure cyberspace by calling on their governments to abide by the United Nations norms of responsible State behaviour in cyberspace, to cooperate in fighting cybercrime as well as cybercriminals and malicious actors, to respond to requests for assistance and capacity-building, if possible in real time, in accordance with the rule of law and fully respecting international human rights law and fundamental freedoms, to secure the supply chain of companies in their countries, to report voluntarily on potential vulnerabilities to third parties to assist them in preventing future incidents, and in particular to support and protect all cyber incident response teams within and beyond their borders;

8. *Also encourages* parliaments to draft gender-responsive legislation promoting cross-cutting cybersecurity services that prioritize prevention (awareness-raising, auditing and training), incident detection (24 hours a day, 7 days a week), and an instant and efficient response to cyber threats, through a victim-centric approach

9. *Recommends* that parliaments promote the establishment of relevant institutions and bodies – such as national cybersecurity centres, computer emergency response teams, computer security incident response teams and security operations centres – where these do not already exist in their country;

10. *Also recommends* that all parliaments ensure that such institutions and bodies have adequate budgetary resources and specialized personnel, including women cybersecurity experts, to allow for an agile, timely and effective response to cybercrime and to protect critical civilian infrastructure, public institutions, companies and citizens without breaching privacy, while taking into account that the increasing digitalization of public services and utilities could imply major exposure to digital risks;

11. *Urges* parliaments to promote international coordination between such institutions and bodies in order to monitor, prevent, detect, investigate and respond to cyber threats;

12. *Invites* parliaments to encourage their governments to provide specific cybersecurity training in order to help increase the number of cybersecurity professionals and to strengthen their performance;

13. *Reaffirms* that an open, secure, stable, accessible and peaceful ICT environment is essential for all and requires effective cooperation among States to reduce risks to international peace and security, and *calls upon* the international community to promote full respect for human rights and fundamental freedoms;

14. *Calls upon* parliaments to encourage investment in research and development, incorporating into the design of each project specific cybersecurity provisions, with appropriate budget allocation, in order to anticipate and protect against possible emerging cyber threats;

15. *Encourages* parliaments to partner with industry, academia and all other stakeholders, including civil society, with their respective governments as key facilitators, in order to foster a strong and collaborative cybersecurity ecosystem that fully respects human rights principles and international human rights obligations;

16. *Calls upon* parliaments and parliamentarians to actively engage in promoting a shared, up-to-date national understanding of the nature of cybercrime as experienced by citizens, organizations and institutions;

17. *Urges* parliaments to help foster a true “culture of cybersecurity” by developing educational curricula focused on training future generations, from childhood onwards, in digital literacy and technological know-how, covering both the great opportunities presented and the serious risks posed by technology;

18. *Recommends* that parliaments broaden protections for women, young people, children, elderly people, people with disabilities, and racialized communities in cyberspace, taking respect for human rights and the prevention of gender-based violence into account in the development of educational policies on the use of social media;

19. *Urges* parliaments to take the necessary action to protect critical moments in democracy, and especially those periods when citizens exercise their right to vote, in order to avoid attacks and interferences that seek to influence, change or violate the free formation of public opinion during the electoral process;

20. *Calls upon* the international community to take action to protect democracy by ensuring that all parliaments worldwide, as institutions representing the will of the people, are afforded special protection through their inclusion in lists of critical civilian infrastructure and essential services;

21. *Stresses* the need to further enhance international cooperation and assistance in the area of ICT security and capacity-building, as a means to bridge digital divides and strengthen the response to cyber threats globally;

22. *Calls upon* parliaments to deepen their understanding of the complex and rapidly evolving nature of cybercrime by enabling the open sharing of knowledge, experience and expertise, and by holding specialized seminars, workshops and conferences on this subject;

23. *Invites* the IPU Secretariat, in partnership with other relevant organizations, to promote this new vision of cybersecurity by supporting parliaments in their capacity-building endeavours;

24. *Recommends* that the IPU, as the global organization of parliaments, play a leading role in preventing and combating cybercrime, and in stimulating cyber-resilience, by participating in all relevant international forums, including those led by the United Nations, with a view to ensuring that the voice of parliaments is heard;

25. *Promotes* the creation of a working group on cybercrime, subsidiary to the Governing Council of the IPU, whose specific mission shall be to comply with the mandates and objectives established in this resolution, and whose powers shall include both supporting the process for the promotion of an international convention on cybercrime within the framework of the United Nations, and strengthening the capacities of IPU Member Parliaments in terms of law-making, oversight and budgeting;

26. *Recommends* that the IPU raise awareness among parliaments on achieving the Sustainable Development Goals through, above all else, their universal commitments to digital security.