PARLIAMENTARY HANDBOOK ON COMBATING CYBERCRIME

Parliamentarians *for* Global Action

TABLE OF CONTENTS

Introduction 3
Glossary 4
How do Parliamentarians Address Cybercrime? 5
The Budapest Convention on Cybercrime 6
How does PGA promote the Budapest Convention on Cybercrime? 7
The Adverse Impact of Cybercrime 9
Examples of Legislation Addressing Cybercrime Against Women 10
Sample Parliamentary Questions to Ministers 11
How to Explain the Benefits of the Budapest Convention on Cybercrime 12
PGA Members' Commitments to Promoting the Budapest Convention 13
Regional Workshops 13
Selection of Outcomes and Achievements 14

Introduction

Cybercrime has a devastating impact on governments, economies, hospitals, schools, businesses, utility companies, supply chains, as well as on the lives of millions of citizens worldwide. Left unchecked, it can pose a serious threat to peace and security, democracy, fundamental human rights and the rule of law.

Parliamentarians play a decisive role in combatting cybercrime, both as advocates and as lawmakers. They are uniquely positioned to develop national legislation that protects against cybercrime and provides support for international cooperation. Parliaments and parliamentarians themselves have often been targeted by cybercriminals. This first-hand experience and exposure to cybercrime only serves to strengthen the resolve of legislators worldwide to continue being active in addressing this serious threat to national, regional and international peace and security.

The objective of this Parliamentary Handbook on Combating Cybercrime is to raise awareness and share concrete tools and resources surrounding the vital and often catalytic contributions that the legislative branch of power can make in tackling this global scourge. As cybercrime continues to evolve and grow, often aided by emerging technologies like artificial intelligence, it is essential that legislators worldwide continue to prioritize engagement in this arena to mitigate the devastating consequences of cybercrime in all its forms.

Photo: PGA Regional Parliamentary Asia Pacific Workshop Addressing Cybercrime

Glossary

Cybercrime - Refers to criminal activities involving or targeting computers, networks, or digital systems. It includes offenses like hacking, online fraud, identity theft, ransomware attacks, child sexual exploitation online, and the distribution of illegal content through digital means.

Cybersecurity - Is the practice of protecting systems, networks, devices, and data from digital attacks, damage, unauthorized access, or disruption. It includes technologies, processes, and practices designed to ensure confidentiality, integrity, and availability of information in cyberspace.

The Budapest Convention on Cybercrime - Also known as the Convention on Cybercrime, is the first international treaty aimed at addressing crimes committed via the internet and other computer networks.

First Additional Protocol to the Budapest Convention – Also known as the Additional Protocol to the Convention on Cybercrime, concerns the criminalization of acts of a racist and xenophobic nature committed through computer systems (2003)

Second Additional Protocol to the Budapest Convention – Also known as the Second Additional Protocol to the Convention on Cybercrime, enhanced the co-operation and disclosure of electronic evidence by providing tools to deal more effectively with cybercrime and other offences (2022).

Cyberbullying – Is the use of digital technologies (e.g., social media, messaging apps, forums) to harass, threaten, embarrass, or target another person.

Cyber-Harassment - Involves the persistent and unwanted use of digital communication to intimidate, threaten, or otherwise harm someone.

Cyberstalking - Is a form of online harassment that includes repeated, targeted, and threatening behavior.

Cyberviolence - Refers to harmful actions carried out through digital means — such as the internet, social media, messaging apps, or other online platforms — that cause psychological, emotional, or social harm to an individual or group. It includes a range of abusive behaviors that occur in cyberspace.

Cybercrime Programme Office of the Council of Europe (C-PROC) - Is the Council of Europe's program office for capacity-building on cybercrime and electronic evidence. C-PROC supports countries worldwide in implementing the Budapest Convention and improving legislative and operational capabilities to combat cybercrime.

Deepfake - Is a type of synthetic media created using artificial intelligence (AI to manipulate or generate audio, video, or images in a way that makes them appear real, even though they are false or fabricated.

Doxxing - Is the act of publicly revealing or publishing private, personal information about an individual without their consent, often with malicious intent

Hacking - Is the act of gaining unauthorized access to or control over a computer system, network, or digital device, often by exploiting technical vulnerabilities or security weaknesses.

Ransomware - Is a type of malicious software (malware) that blocks access to a victim's data or system typically by encrypting files until a ransom is paid, usually in cryptocurrency.

How Can Parliamentarians Address Cybercrime?

Parliamentarians address cybercrime through a combination of legislative measures including oversight and appropriation, as well as engaging with a wide range of stakeholders such as law enforcement, international bodies, and the private sector.

In the context of legislation and regulation, parliamentarians draft and debate different laws that directly criminalize various types of cybercrime, such as cyber-harassment, ransomware, hacking, identity theft, online fraud, and the distribution of child sexual abuse material. Many countries worldwide have adopted extensive regulations and legislation in this field. This also includes legislation and regulation governing national security to the extent that cybercrime can frequently be utilized to undermine national security, both in terms of national defense structures but also in assaulting core democratic principles, including the conduct of elections and the exercise of many fundamental human rights.

Parliamentarians also play an important role in drafting and adopting data protection and privacy laws. Cybercrime, in particular, flourishes where sensitive personal information online is inadequately safeguarded. Members of regional parliaments are similarly engaged in adopting legislation addressing

One of the more important prerogatives at the disposal of parliamentarians is their exercise of oversight and accountability over the executive branch of government, including those agencies whose mandate is to address cybercrime. Another weighty responsibility of parliamentarians is to ensure that these agencies are adequately supported and properly financed to discharge their mandates. In addition to law-enforcement agencies, this funding may also extend to educational and digital literacy initiatives surrounding capacity-building in identifying and mitigating cybercrime. More generally, parliamentary committees frequently also have the authority to assess government and corporate responses to cybercrime.

By its very nature, cybercrime is frequently a trans-border operation. Parliamentarians are mindful of this reality and can mobilize in support of international frameworks and treaties that address this reality. Within Parliamentarians for Global Action's network, many of our members have actively and effectively engaged with colleagues in both the legislative and executive branches of government in support of the Budapest Convention on Cybercrime, as well as its two additional protocols — the first prohibiting online xenophobia and racism, and the second promoting enhanced cooperation in the sharing of electronic evidence. Consequently, parliamentarians are often invited, as key stakeholders and 'champions', to participate in regional and international meetings that seek to improve existing mechanisms and/or identify new solutions in confronting cybercrime.

The Budapest Convention on Cybercrime

Parliamentarians can play a vital role in promoting the Budapest Convention on Cybercrime, which is the first international treaty aimed at addressing internet and computer crime. The Budapest Convention on Cybercrime was adopted in 2001 and is a key instrument in the fight against cybercrime. Over 80 countries worldwide have already formally acceded to this Convention. Typically, two to three countries are invited to join annually, at the request of their respective governments, drawn from all regions worldwide. Sixteen additional countries in total have signed or been invited to accede to the Budapest Convention on Cybercrime.

As a parliamentarian, you can advocate for your country's government to accede to the Budapest Convention if it hasn't already. You can highlight the benefits of becoming a party to the convention, such as enhanced international cooperation and supported legal frameworks to fight cybercrime. Parliamentarians can also advocate for, as well as being directly involved in, the drafting of new or revised legislation to ensure that measures taken to fight cybercrime are adequately addressed by national legislation.

Cybercrime is constantly changing and evolving into different and new forms to exploit new-found vulnerabilities, necessitating frequent assessment by both the executive and legislative branches of government around the continued capacity of existing legislation to address it. Cybercrime attacks have grown increasingly sophisticated in recent years, sometimes aided by developments in different emerging technologies, including AI. Parliamentarians must also be mindful of AI regulations in the discharge of their legislative responsibilities in this space.

Photo: PGA Regional Caribbean Parliamentary Workshop Addressing Cybercrime

How does PGA promote the Budapest Convention on Cybercrime?

Parliamentarians for Global Action, or PGA, is a global multiparty network of over 1,000 legislators from all regions of the world advocating for human rights, democracy, and the rule of law; peace and human security; gender equality and inclusion; protection of the environment; and justice in all its forms. PGA has long track record advocating for the promotion and implementation of key global agreements and treaties, particularly in the fields of peace and security, human rights, and international law.

The Budapest Convention on Cybercrime is the first international treaty that seeks to address internet and computer crime by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. Our Campaign to Address Cybercrime encourages parliamentarians to take the following actions:

1. Advocacy for Accession

We encourage parliamentarians to advocate for accession to the Budapest Convention on Cybercrime in their respective countries. To date, PGA Members in Cameroon, Ghana, The Gambia, Malawi, Seychelles, Sierra Leone, Fiji, New Zealand, Vanuatu, Trinidad and Tobago, Jamaica, Grenada and St. Lucia, among others, have all made important catalytic contributions in this connection. To learn more about these activities, please see the resources section at the end of this Parliamentary Handbook.

2. Initiating and promoting legislative actions

The Budapest Convention on Cybercrime requires countries to implement national laws aimed at addressing cybercrime, including cyber-attacks, online fraud, ransomware, identity theft, child exploitation, and illegal dissemination of content. We encourage parliamentarians to review their respective countries' legal frameworks, in consultation with the Council of Europe Cybercrime Office and other relevant stakeholders, to ensure conformity with the Budapest Convention.

3. Fostering International Cooperation

The Budapest Convention promotes international cooperation in addressing cybercrime. By its very nature, cybercrime often transcends national borders. We emphasize the importance of global collaboration to combat cybercrime and facilitate networking opportunities for parliamentarians from many different countries and regions, including encouraging and facilitating invitation of parliamentarians to regional and international meetings that take an inclusive and holistic approach to addressing cybercrime.

4. Capacity Building and Training

We organize regional workshops and webinars inviting parliamentarians, expert regional organizations, relevant government ministries and other key stakeholders with the objective of equipping parliamentarians with all they need to make vital contributions in addressing cybercrime in their respective countries and regions. To chart the way forward, participants in

these workshops adopted plans of action that have directly contributed to many tangible steps such as encouraging their governments to join the Budapest Convention on Cybercrime and ensuring the passage of legislation necessary for this purpose. We also track, monitor, and keep our global membership regularly informed of significant recent developments pertaining to the Budapest Convention on Cybercrime to facilitate and encourage continued advocacy.

Photo: PGA Executive Committee Member Hon. Angela Browne Burke, MP (Jamaica)

The Adverse Impact of Cybercrime

Parliaments and individual parliamentarians have been themselves the target of cybercrimes. The Parliaments of Estonia, United Kingdom, Ukraine, United States, Brazil, Germany, Australia, Finland, Norway, India, Belgium, the European Parliament and South Korea have experienced targeted attacks in the past fifteen years.

Many prominent female PGA members worldwide have been drawn to PGA's Campaign to Address Cybercrime given the often disproportionately adverse impact of cybercrime on women, including the tailoring of certain cybercriminal activity to directly target women. Women legislators, like other women in positions of authority, are also often particularly vulnerable to and subjected to specific forms of online abuse such as cyberstalking, cyber-harassment, cyberbullying, doxing, as well as the dissemination of deep fake images. Patriarchal views still prevail in many countries questioning the involvement of women in political life which can lead to online abuse. Additionally, women in the public eye are more likely to be targeted, especially those with new-found visibility and influence. Cybercriminals may believe that women may be more likely to respond to their demands, given the devastating personal impact of some of the customized cybercriminal activity to which they can be subjected.

Photo: Hon. Tangariki Reete, past Speaker of Parliament of Kiribati

Women policy and decision makers, even today, often face a disproportionate backlash, especially if their views do not reflect those of certain majorities. The psychological toll of continuous online harassment can lead to anxiety, depression and can force some women to step back from public life or abandon entirely their political careers.

Threats to safety from cybercrime, especially when combined with doxing or physical threats, can lead to real-world violence. In response, some countries have passed stronger cybercrime laws to combat online harassment and protect affected individuals from cybercriminals. Training is now being offered in some countries on how to be more vigilant and better protect against cybercrime targeting women, including the introduction of more user-friendly reporting mechanisms and wider public awareness campaigns.

Numerous PGA members, predominantly female, have been directly and personally impacted by cybercrime, frequently targeting them on an individual basis. In addition to promoting awareness on the Budapest Convention on Cybercrime, regional workshops organized by PGA can provide a cathartic opportunity for women to share their experiences with other colleagues similarly targeted in a wider regional forum, build solidarity among them to better understand and challenge these attacks. Our Stop Violence Against Women Initiative is an example of our commitment to promote and protect women's political participation.

Examples of Legislation Addressing Cybercrime Against Women

An important deterrent to cybercrime violence targeting women is the adoption of cybercrime legislation addressing and criminalizing these acts. In this regard, parliamentarians, as lawmakers can make substantial and decisive contributions. Some examples of legislation adopted at the regional and national levels which substantively, if not exclusively, address cybercrime against women include:

- In the **European Union**, Directive (EU) 2024/1385 on combating violence against women and domestic violence criminalizes, across all members states, non-consensual sharing of intimate images, cyberstalking, cyber-harassment, and cyber incitement to hatred or violence.

- In **Botswana**, the Cybercrime and Computer Related Crimes Act, 2018 includes provisions that criminalize cyber-harassment and cyberstalking.

- In **Australia** — the Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Act 2018 focuses on situations where intimate images are shared without the subject's consent. It creates legal obligations and remedies for victims. It is part of a broader framework that recognizes the harms from technology-facilitated abuse, including when such abuse disproportionately affects women.

- In **Ireland**, the Harassment, Harmful Communications and Related Offences Act 2020 ("Coco's Law") introduced offenses such as the taking, distribution, publication, or threat to distribute intimate images without consent. The law distinguishes between cases where there was intent to cause harm versus those without such intent, with different penalties

- In **Mexico**, the Olimpia Law is a body of legislation named after a survivor-advocate, designed to criminalize non-consensual sharing of intimate imagery (often called "image-based sexual abuse").

- In **South Korea**, "Digital Sex Crimes" legislation includes taking or distributing photos/videos of persons without consent.

- In the **United States of America**, the "Take It Down Act" (2025) is a federal law that criminalizes the non-consensual publication of intimate images (including deepfakes) without consent.

Sample Parliamentary Questions to Ministers

Below are some examples of parliamentary questions that you can pose to your Ministers to learn more about your country's policy and legal framework in this field.

- "In light of the significant and increasing toll of cybercrime on the economy and people of our country, and as an integral part of our national strategy to improve cybersecurity and address cybercrime, is the Government now giving due consideration to seeking an invitation to join the Budapest Convention on Cybercrime as well as exploring the possibility of accession to its two Additional Protocols addressing xenophobia and racism online and facilitating enhanced cooperation in the sharing of electronic evidence?" "If not, why not?"

- "Is the Government aware of the significant complimentary assistance on offer from the Council of Europe and from governments who have already joined the Budapest Convention and many governmental and non-governmental organizations worldwide to facilitate implementation of the Budapest Convention on Cybercrime in our country? This complimentary assistance could include drafting and revision of national legislation to ensure its adequacy to meet evolving cybercrime threats as well as offering technical capacity building workshops for law enforcement and judicial officers."

- "Is the Government aware that 81 countries worldwide to date have joined the Budapest Convention on Cybercrime, with an additional 13 countries having requested invitations to join and having been invited to join the Convention?" (as of October 2025)

- "Is the Government aware that many core provisions of the Budapest Convention on Cybercrime have already been implemented in the national legislation of over 120 countries worldwide?"

- "Is the Government aware of the many other benefits of joining the Budapest Convention on Cybercrime, including access to a global network of countries and governments and global institutions closely assisting and cooperating with each other in combatting cybercrime? These include facilitating vital and prompt exchanges of key information and evidence, when needed, which is essential in the fight against cybercrime."

- "Is the Government aware that there is no annual assessed financial contribution to be made by countries joining the Budapest Convention on Cybercrime, nor are there any onerous annual reporting requirements that need to be met, as can sometimes arise in the context of joining other international treaties?"

- "Does the Government understand that by continuing to choose to remain outside of the Budapest Convention on Cybercrime, we as a nation are foregoing vital, substantial, and free tools and assistance that would otherwise greatly help us fighting cybercrime within our national borders and beyond?"

How to Explain the Benefits of the Budapest Convention on Cybercrime

By joining the Budapest Convention on Cybercrime, we as a country, will:

- Be eligible for consideration for significant, complimentary assistance, including the drafting/revision of our national legislation to ensure it is adequate to address rapidly evolving cybercrime threats. Our law enforcement and judicial officials will improve and become more effective in fighting back against cybercrime as a result of becoming eligible to receive consideration to receive tailored assistance from the Cybercrime Office of the Council of Europe, individual States or from regional or international organizations addressing cybercrime.

- Get access to a global network of countries, governments, and international organizations who closely cooperate with each other in combating cybercrime.

- Generate higher levels of confidence in the security safeguards and infrastructure in place in our country, potentially attracting more investment from other countries and international corporations that require high levels of reassurance that steps on protecting against, or mitigating, cybercrime have been taken, or are being taken.

- Make our country safer, more prosperous, and better protect our people from cybercrime and its devastating consequences.

Photo: PGA Regional African Parliamentary Workshop Addressing Cybercrime

PGA Members' Commitments to Promoting the Budapest Convention

From 2023 - 2025, PGA members made several concrete commitments to raise awareness about the benefits of joining the Budapest Convention on Cybercrime in their respective countries, in line with plans of action adopted at our regional workshops. These commitments include:

- Drawing attention to the benefits of joining the Budapest Convention on Cybercrime and sensitizing fellow parliamentarians and other relevant stakeholders on the importance of advocating for sufficient allocation and subsequent appropriation of funds to ensure effective implementation of relevant legislation addressing cybercrime.

- Encouraging their governments to take different and innovative approaches to generate an improved understanding of the many and diverse threats posed by cybercrime among the population of their countries, including the criminalization of such activities.

- Liaising with relevant stakeholders beyond government such as different platforms, internet service providers and users to ensure that they also play their respective roles in combatting cybercrime.

- Seeking to engage more female parliamentarians for their more active involvement in this field, taking into account the well documented disproportionate adverse impact of cybercrime on women.

Regional Workshops

To learn more about our activities, regional workshops, and results, please visit the following dedicated webpages on PGA's website:

- African Regional Workshop on the Universalization of the Budapest Convention on Cybercrime and its Additional Protocols

- Caribbean Regional Workshop on the Universalization of the Budapest Convention on Cybercrime and its Additional Protocols

- Promoting Accession to the Budapest Convention on Cybercrime in the Pacific

Selection of Outcomes and Achievements

Cameroon
https://www.pgaction.org/news/cameroon-instrument-budapest-convention.html

Fiji
https://www.pgaction.org/news/pacific-region-cybercrime.html

Vanuatu
https://www.pgaction.org/news/vanuatu-ascension-budapest-convention.html

Seychelles
https://www.pgaction.org/inner.php/news/seychelles-requests-invitation-budapest-convention.html

Sierra Leone
https://www.pgaction.org/news/sierra-leone-budapest-convention.html

Grenada
https://www.pgaction.org/news/grenada-budapest-convention.html

Jamaica
https://www.youtube.com/watch?v=z3zsnJ7Kz-c&t=8230s

Tanzania
https://polis.parliament.go.tz/questions/10360

Trinidad and Tobago
https://trinidadexpress.com/opinion/columnists/budapest-convention-and-cybercrime-in-t-t/article_894ca59a-2507-11ee-8afa-b38f086cc38a.html

Senate Debate - 19th Sitting of the Senate - 4th Session - 12th Parliament
https://youtu.be/CchQPNu9bNM?t=24012
https://youtu.be/CchQPNu9bNM?t=24561