



Inter-Parliamentary Union
For democracy. For everyone.

151st IPU Assembly

Geneva
19–23 October 2025



Assembly
Item 9

A/151/9-DR
22 October 2025

Parliamentary action against transnational organized crime, cybercrime and hybrid threats to democracy and human security

Draft resolution submitted by the drafting committee

Rapporteur: Mr. H. Aden Gueddi (Djibouti)

The 151st Assembly of the Inter-Parliamentary Union,

- (1) *Recalling* the purposes and principles of the Charter of the United Nations, including respect for national sovereignty, territorial integrity, non-intervention in internal affairs, and the peaceful resolution of disputes, as well as of the Universal Declaration of Human Rights, the United Nations Convention against Transnational Organized Crime (UNTOC, 2000), the United Nations Convention against Corruption (UNCAC, 2003), and other relevant international instruments,
- (2) *Reaffirming* the commitment of the IPU, alongside other institutions and civil society, to democracy, peace, human rights and the rule of law as the foundations of legitimate governance, and *taking note* of the forthcoming United Nations Convention against Cybercrime,
- (3) *Alarmed* by the growing convergence between transnational organized crime, drug trafficking, cybercrime and hybrid threats, which endangers democratic institutions, national security and global stability, and undermines democracy, corrupts institutions and destroys the social and economic fabric of our societies,
- (4) *Deeply concerned* about attacks, threats, online gender-based violence and assassinations targeting parliamentarians, journalists, and political, civic and business leaders for their role in defending transparency and the rule of law,
- (5) *Recognizing* the need to strengthen cooperation among national parliaments, the United Nations, the International Criminal Police Organization (INTERPOL) and regional organizations to harmonize legislative frameworks and counter these evolving threats, particularly cyber-enabled fraud, human trafficking, illicit drugs, money laundering, and related abuses that are increasingly transnational in scope,
- (6) *Taking note* of the Letter of Intent signed between the IPU and the United Nations Office on Drugs and Crime (UNODC) in June 2025 and their shared commitment to strengthen parliamentary capacities in the fight against organized crime,
- (7) *Alarmed* by a recent UNODC report¹ that reveals the industrial-scale proliferation of scam compounds across Southeast Asia, where hundreds of thousands of victims from more than 70 countries around the world have been trafficked and coerced into cyber scams,
- (8) *Deeply alarmed* that scam compounds are rapidly transforming from regional criminal hubs into a globalized shadow economy, that they exploit governance gaps in developing regions under the facade of investment, city-building or entertainment complexes, often enabled by complicit local power brokers, and that they are now generating revenues rivalling national GDPs and are expanding globally,

¹ UNODC, [Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia](#), April 2025.

(9) *Acknowledging* the reports of UNODC (2025) and others, which reveal alarming levels of digital scam exploitation, human trafficking, disinformation and corruption by State and non-State actors, including operations directly linked to organized criminal syndicates, illicit online marketplaces and underground banking systems, generating annual revenues exceeding USD 50-75 billion,

(10) *Deeply concerned* by recent instances of both State and non-State actors using coordinated cyber intrusions, sabotage of critical infrastructure, espionage, and targeted disinformation campaigns affecting multiple countries across continents,

(11) *Recalling* that transnational criminal networks exploit governance gaps, special economic zones, conflict-affected areas and casinos to launder the proceeds of crime, fuelling corruption, destabilizing communities, violating human rights, undermining sovereignty, threatening regional stability, hindering development, and challenging international efforts to combat organized crime and uphold the rule of law,

(12) *Recalling also* striking examples of the destructive use of hybrid tactics by State actors, including indiscriminate use of military force, cyber operations and psychological warfare,

(13) *Concerned* that victims, including women, children and other vulnerable groups, are subjected to forced cyber scams under threat of torture and detention, and often risk re-trafficking or additional violations of their rights,

(14) *Recognizing* the role of parliaments in strengthening legislation, oversight and cooperation to address the intersection between cybercrime, human trafficking, money laundering and corruption, while ensuring that countermeasures fully uphold humanitarian and human rights principles,

(15) *Considering* that the transnational and technologically advanced nature of criminal organizations creates an asymmetry that strengthens their expansion and influence, requiring justice and security institutions to respond through supranational institutions and technologically advanced strategies and means, and *recognizing* that such threats become even more serious when the actors involved are States or operate with State support,

(16) *Recognizing* the IPU's role and policy focus in providing a global platform for multilateral dialogue among national parliaments on peace and security issues, and in facilitating tangible solutions through its 2022–2026 Strategy under Strategic Objective 4: Catalysing collective parliamentary action,

1. *Declares* that the fight against transnational organized crime, drug trafficking, cybercrime and hybrid threats — whether perpetrated by State or non-State actors — is a global priority requiring unified parliamentary action and strong democratic governance, and *urges* parliaments to consider measures to ensure accountability for perpetrators of such crimes;
2. *Condemns* all forms of organized crime, including cyber-enabled human trafficking, forced criminality and modern slavery, perpetrated by both State and non-State actors, with particular attention to the disproportionate impact on women and children, and *urges* parliaments to adopt legislation and policies that promote victim-centred approaches and ensure the protection and rehabilitation of all victims and survivors;
3. *Stresses* the importance of addressing the root causes of vulnerability, including poverty, lack of education, inequality, human trafficking, conflict and corruption, which fuel recruitment into scam compounds, and *urges* the relevant authorities to implement practical solutions to tackle these issues;
4. *Urges* IPU Member Parliaments to update national legislation in a manner consistent with applicable international laws to combat State and non-State participation in cybercrime and improve parliamentary oversight mechanisms of security and intelligence agencies, ensuring respect for the rule of law and human rights, while also ensuring that cybercrime measures do not result in violations of humanitarian principles or secondary victimization of trafficked persons;

5. *Urges* parliaments to strengthen national legal frameworks to:
 - (a) criminalize coercion for the purpose of cyber scams;
 - (b) increase sanctions on security companies implicated in abuses;
 - (c) close legal loopholes exploited by illicit online gambling, cryptocurrency laundering and underground banking systems;
 - (d) review electoral, financial and transparency laws to prevent the infiltration of organized crime and foreign interference in democratic institutions;
 - (e) enhance independent oversight of State security and law enforcement bodies to prevent complicity in trafficking and cybercrime;
 - (f) increase sanctions on any civil servants and governments involved in abuses;
6. *Calls for* the protection of parliamentarians and *requests* the IPU Committee on the Human Rights of Parliamentarians to monitor and document attacks against them;
7. *Invites* governments and parliaments to address the structural causes of vulnerability — poverty, inequality, institutional weakness and corruption — through inclusive and sustainable policies;
8. *Supports* the work of existing regional, international and global legal and security bodies combating transnational organized crime under the UNTOC — such as the UNODC, INTERPOL, and regional agencies against organized crime — and the creation of new institutions to address organized crime in the transnational sphere in which it operates, such as an international court against corruption, the Latin American and Caribbean Criminal Court against Transnational Organized Crime (COPLA), or a MERCOSUR agency against transnational organized crime;
9. *Invites* IPU Member Parliaments, in accordance with international law and emerging international criminal jurisprudence to recognize that actions of transnational organized crime — whether committed by non-State actors or by a State or its agents acting in an organized or systematic manner — may constitute crimes against humanity;
10. *Recommends* developing joint cybersecurity frameworks and standards among Member Parliaments to protect critical infrastructure and public information systems, in line with the IPU resolution *Cybercrimes: The new risks to global security*, adopted at the 146th Assembly (Manama, 11–15 March 2023);
11. *Calls for* stronger regulation of cryptocurrencies, online platforms and cross-border financial flows to curb illicit money laundering linked to scam compounds, and *urges* global financial institutions to adopt enhanced due diligence;
12. *Encourages* parliaments to work jointly with the private sector and civil society to foster technological innovation that counters disinformation and digital exploitation, while upholding civil liberties, safeguarding privacy, and ensuring full respect for human rights in all measures addressing digital threats;
13. *Recognizes* that hybrid threat tactics — including cyber-enabled sabotage, disinformation and attacks on critical infrastructure — when conducted or sponsored by State or non-State actors, may constitute violations of international law and, in certain cases, acts of terrorism, and therefore *urges* full respect for international humanitarian law and human rights norms;
14. *Denounces* the use of airspace violations, coordinated influence operations and targeted cyber intrusions as tools of intimidation, aggression and interference in the internal affairs of sovereign States;
15. *Requests* the IPU to utilize its existing bodies to facilitate legislative cooperation in tackling coerced criminality, financial crimes, and violations of human rights and international humanitarian law, and monitor implementation;
16. *Suggests* including this matter under a standing agenda item, “Democracy, Governance and Global Security”, and to review progress at future IPU Assemblies.