COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

www.coe.int/cybercrime

Strasbourg, 17 November 2026

T-CY (2026)14

Cybercrime Convention Committee (T-CY)

T-CY 35

Compilation of written contributions and oral interventions submitted in connection with the 35th T-CY Plenary (12-13 October 2026)

ITEM 3

MALAWI

STATEMENT BY THE REPUBLIC OF MALAWI

on the Progress of the Cybercrime Bill

and Accession to the Convention on Cybercrime

(Budapest Convention)

Delivered at the

35th Plenary of the Cybercrime Convention Committee (T-CY)

&

Octopus Conference 2026

Council of Europe

Strasbourg, 12–16 October 2026

Excellencies,

Distinguished Delegates,

Ladies and Gentlemen,

It is a distinct honour and privilege for me, on behalf of the Government of the Republic of Malawi, to address this august gathering on the occasion of the 35th Plenary of the Cybercrime Convention Committee and the Octopus Conference 2026, convened under the auspices of the Council of Europe. Malawi attaches particular significance to this year's proceedings, which mark the twenty-fifth anniversary of the Convention on Cybercrime — the Budapest Convention — a landmark instrument that continues to guide the international community in the fight against cybercrime.

Allow me at the outset to express the profound appreciation of the Government of Malawi to the Council of Europe, the Cybercrime Programme Office (C-PROC), and the partners of the GLACY-e and Octopus projects for the sustained technical assistance and capacity-building support extended to our national authorities. This cooperation has been instrumental in advancing Malawi's legislative and institutional preparedness in the domain of cybercrime and electronic evidence.

We further wish to express our sincere gratitude to the Council of Europe under GLACY-e project at INTERPOL and Cybercrime Programme Office (C-PROC), specifically for the technical support and funding provided for the upcoming national cyber drill and conference, scheduled to take place at on 26th to 29th October 2026 in Malawi hosted by Malawi Computer Emergency Response team (Malawi CERT). This important initiative will further strengthen

our national capacity to respond to cyber threats and foster greater collaboration among stakeholders

Progress towards Accession to the Budapest Convention

Following the decision of the Committee of Ministers of the Council of Europe on 9 October 2024, the Republic of Malawi was formally invited to accede to the Convention on Cybercrime. This invitation, valid for a period of five years, constitutes a significant milestone in Malawi's journey towards full integration into the global framework for international cooperation against cybercrime.

The Government of Malawi welcomes this invitation with the utmost seriousness and remains firmly committed to completing the necessary domestic processes leading to accession. Accession to the Budapest Convention is viewed not merely as a formal legal step, but as a strategic imperative for strengthening our national cybersecurity posture, enhancing the effectiveness of criminal justice responses to cyber-enabled offences, and facilitating swift and reliable cross-border cooperation in the investigation and prosecution of cybercrime.

Progress on the Cybercrime Legislation

Malawi currently relies on the Electronic Transactions and Cyber Security Act of 2016 as the principal statute addressing computer-related offences and electronic evidence. While this legislation has provided a foundational framework, the Government recognised the need for a more comprehensive and modern instrument fully aligned with the standards of the Budapest Convention.

To that end, national authorities, with the valuable technical support of the Council of Europe under the GLACY-e project, have advanced the drafting of a dedicated Cybercrimes Bill. Extensive consultations were undertaken, including a national workshop held in Lilongwe in May 2024, which brought together representatives of the Malawi Communications Regulatory Authority (MACRA), relevant Government departments, law enforcement agencies, and other stakeholders. The purpose of these consultations was to ensure that the draft Bill incorporates the substantive offences, procedural powers, and international cooperation provisions required by the Convention.

Following the consultation process, the drafting team conducted further internal reviews to incorporate recommendations and model provisions provided by the Council of Europe. The proposed legislation is designed to criminalise offences related to computer systems and information and communication technologies; to establish clear procedures for the preservation, collection, and use of electronic evidence; and to facilitate mutual legal assistance and other forms of international cooperation.

Complementing these efforts, Malawi has also strengthened its broader digital legal framework through the enactment of the Data Protection Act, which came into force in 2024. This legislation strengthens the framework for lawful, fair and transparent processing of personal data. It introduces modern data-subject rights, mandatory breach notification, and institutional arrangements for the protection of personal data, thereby reinforcing the safeguards necessary for a rights-respecting approach to cybercrime investigation and prosecution.

Institutional and Operational Developments

Beyond legislative reform, Malawi continues to invest in the institutional capacity required to combat cybercrime effectively. The Malawi Computer Emergency Response Team (CERT-MW), established under the Electronic Transactions and Cyber Security Act and hosted by MACRA, serves as the national focal point for the detection, analysis, and response to cybersecurity incidents.

These investments have yielded measurable results. Malawi's score on the Global Cybersecurity Index improved substantially from 36 per cent in 2020 to 80 per cent in 2024, reflecting the tangible impact of sustained national commitment combined with international cooperation.

Furthermore, recognising the rising incidence of technology-enabled crime — including mobile money fraud, impersonation, and the misuse of artificial intelligence — national authorities have intensified inter-agency collaboration. The Malawi Communications Regulatory Authority and the Malawi Police Service are working closely to strengthen investigative capacity, facilitate the tracing of offenders, and ensure that perpetrators of cyber-related offences are brought to justice.

The Way Forward

The Government of Malawi remains steadfast in its resolve to finalise and enact the Cybercrimes Bill in alignment with the Budapest Convention, and thereafter to complete the accession process within the period of validity of the invitation. We are conscious that effective participation in the Convention requires not only legislative approximation but also the continuous strengthening of institutional capacity, the training of investigators, prosecutors and judges, and the establishment of efficient channels for international cooperation.

In this regard, Malawi looks forward to continued partnership with the Council of Europe and the wider community of Parties and observers to the Convention. We are confident that, upon accession, Malawi will be in a position to contribute actively to the work of the Cybercrime Convention Committee and to the collective effort to make cyberspace safer for all.

As we commemorate twenty-five years of the Budapest Convention, Malawi reaffirms its commitment to the principles of international cooperation, mutual legal assistance, and respect for human rights and the rule of law that underpin this historic treaty. We stand ready to play our part in ensuring that the digital transformation of our societies is accompanied by robust legal, institutional, and technical safeguards against the misuse of technology for criminal purposes.

I thank you for your kind attention.

BUDAPEST CONVENTION ON CYBERCRIME, SECOND ADDITIONAL PROTOCOLS AND SRI LANKA'S LEGAL COMPLIANCE

Sri Lanka acceded to the Budapest Convention on Cyber Crime in year 2015 becoming the first country in South Asia. Sri Lanka signed the Second Additional Protocol to the Budapest Convention on Cyber Crime on 30th November 2022. Sri Lanka as a country in compliance with the International obligations has enacted several legislative provisions. The Computer Crimes Act No. 24 of 2007 was enacted for the purpose of identification of Computer crimes and to provide the procedure for the investigation and for the prevention of such crimes.

In addition, Personal Data Protection Act No. 09 of 2022 was enacted for the purpose of providing for the regulation of processing of personal data, to identify and strengthen the rights of data subjects in relation to the protection of personal data and to provide for the establishment of the Data Protection Authority. In order to provide a future ready enforcement regime and to equally support both public and private sector adoption of digital strategies, while ensuring the rights of data subjects the aforesaid Act was amended subsequent to a wider stakeholder consultation including both the private sector and public sector participation. The Act No. 22 of 2025 which amends the principal enactment includes provisions to specify different operational dates for different parts of the principal enactment, and provides provisions for the inclusion of new data subject rights, data protection officer appointments, personal data protection Impact assessments and for cross border data transfers. In addition, based on the recent legal compliance, Sri Lanka's data protection regime will be entered in to a new phase with the commencement of the key provisions of the personal data protection Act on 1st January 2027.

The provisions in the Mutual Assistance in Criminal Matters Act No. 25 of 2002 which was amended by Act No.24 of 2018 provides provisions to obtain and to render assistance for various requests in criminal matters. The legislative provisions permit to provide assistance in the absence of an Agreement or a Treaty on a reciprocity basis. Further, provisions had been introduced in relation to expedited preservation of stored data in relation to computer crimes and specially to lay down the procedure to be followed in receipt of emergency Mutual Assistance requests. In addition, the law provides provisions for Joint Investigations. In order to streamline the process of Mutual Assistance, Sri Lanka has entered into 10 agreements including a Memorandum of

Understanding and 12 new Agreements are being considered by the Ministry of Justice & National Integration which is designated as the Central Authority in Mutual Assistance in Criminal Matters.

The payment devices frauds Act No. 30 of 2006 was enacted for the purpose of preventing the possession and use of unauthorized or counterfeit payment devices, to create offences connected with the possession or use of unauthorized payment devices, to protect persons lawfully issuing and using such payment devices, to make provision for the investigation , prosecution and punishment of offenders.

Provisions of Anti-Corruption Act No. 09 of 2023 also provides provisions to conduct Joint Investigations with Foreign States upon request.

The Assistance to and Protection of Victims of Crime and Witnesses Act No.10 of 2023, in the interest of Justice and as a measure of protection, permits victims of crime or witnesses or law enforcement authority to give or obtain such evidence or to make a statement by using contemporaneous audio-visual linkage between such Court or Commission and a specified remote location within or outside Sri Lanka.

Online safety Act No. 9 of 2024 was enacted for the purpose of establishing the Online Safety Commission, to provide safety from prohibited statements made online, to prevent the use of online accounts and unauthentic online accounts for prohibited purposes, to make provisions to identify and declare online locations used for prohibited purposes in Sri Lanka and to suppress the financing and other support of communication of prohibited statements. The policy approval had been granted by the Cabinet of Ministers to review the Act through the appointment of an Expert Committee to propose amendments when and where necessary.

Sri Lanka officially signed the United Nations Convention against Cybercrime (UNCC) on 25th October 2025 in Vietnam.

ITEM 5

AUSTRALIA

Australia's National Statement – T-CY Plenary

Oral statement:

Thank you Chair for giving me the floor.

As we mark the 25th anniversary of the Budapest Convention, Australia would like to acknowledge its enduring value across the globe.

We also express our strong appreciation for the work of the T-CY and the important role it has played in strengthening our collective responses to cybercrime.

The Budapest Convention is more than just a legal framework. It is a trusted global community that connects practitioners, builds relationships and facilitates international crime cooperation against cybercrime.

For 25 years, it has provided a platform for sharing legal, technical and operational expertise, strengthening capacity, and fostering the mutual trust that underpins effective international cooperation.

That trust has also enabled Parties to evolve the Convention over time, including through the development of supplementary protocols that strengthen and modernise the framework.

The T-CY and the Budapest Convention has never been more important. The cybercrime landscape is evolving at an unprecedented rate. Technological advances and increasingly sophisticated criminal methodologies are creating new challenges for law enforcement, while the scale and complexity of electronic evidence continue to grow.

Looking ahead, developments such as artificial intelligence will continue to reshape the threat environment. We must continue to ensure the Convention remains responsive, relevant and equipped to address the evolving challenges of the digital age.

Australia sees significant value in the T-CY continuing to serve as a forum to share experiences, promote consistent implementation of the Convention and its safeguards, and develop practical guidance that supports its effective application in combatting cybercrime.

Australia remains committed to the Budapest Convention, as a comprehensive framework for domestic legislation, a cornerstone of international cooperation and a key mechanism for building global capacity to combat cybercrime. We want to see the T-CY continue to be a practical and forward-looking forum - one that responds to emerging challenges, strengthens cooperation between members, and maintains the community of trust that has been central to its success.

As we look ahead internationally, we must also ensure our domestic frameworks keep pace – Australia is committed to ensuring our policies and legislation continue to protect the Australian community, businesses and government services from emerging cyber threats.

Australia is a strong advocate for online safety and combating cybercrime. This includes world-leading online safety legislation that holds digital platforms accountable for preventing online harms, as well as new measures to better protect young Australians online.

As cybercrime continues to evolve, no country can address these challenges alone. Australia looks forward to working with all Parties to ensure the Convention remains a practical, trusted and effective framework for international cooperation in the years ahead.

Thank you, Chair.

Written update:

We thank the T-CY for the opportunity to provide Australia's update.

Critical and emerging technologies, particularly artificial intelligence (AI), are reshaping the threat landscape, enabling more sophisticated forms of cybercrime and creating new challenges for online safety. In response, Australia continues to advance key measures to safeguard Australians online and ensure its frameworks remain fit for purpose in a rapidly evolving digital environment.

The Australian Government is developing legislation to implement a Digital Duty of Care under the *Online Safety Act 2021* (the Act). This reform will shift greater responsibility onto platforms to prevent online harms, requiring them to take proactive steps to design safe services that prevent foreseeable harms, rather than relying on users to report harms after they occur. This includes addressing illegal and harmful material and conduct, particularly where it affects young people, as well as minimising the risk of harm from features such as AI and algorithms. The reforms will complement Australia's social media minimum age legislation, which aims to protect young Australians from pressures and risks that users can be exposed to while logged in to social media accounts.

Australia is also reviewing our domestic cybercrime and child sexual abuse offences to ensure these frameworks are modernised and remain fit for purpose to respond to evolving online harms. We are also working to restrict access to applications that 'nudify' adults or children and undetectable online stalking tools. These reforms will help to proactively prevent abuse facilitated by evolving technologies and protect young Australians online from life-changing harms.

Australia is considering how to feed insights from emerging research into our policy responses to child sexual exploitation and abuse, including the impacts and opportunities of artificial intelligence, as part of the development of the Second Action Plan under Australia's *National Strategy to Prevent and Respond to Child Sexual Abuse 2021-2030*.

Australia is also continuing to progress major reforms to our electronic surveillance laws to ensure electronic surveillance powers for law enforcement and security agencies are fit-for-purpose in a modern technological environment.

CANADA

Item 5 T-CY 35 Plenary

Canada's written contribution on recent legislative developments relevant to the fight against cybercrime, the Convention and its Protocols:

On June 18, 2026, significant reforms to Canada's *Criminal Code* and other pieces of legislation to confront modern threats and protect victims received Royal Assent. Most of these reforms **came into force on July 18, 2026**.

These reforms represent one of the most consequential updates in generations to address delays, protect victims and survivors of gender-based violence, including sexual violence and intimate partner violence, and to keep our kids safe from predators, including online.

These reforms include a criminal law response to sexually explicit deepfakes and sextorsion, including the sextorsion of children.

See all of the details here:

Protecting Victims Act: Legislation to protect victims and keep kids safe from predators

Item 5 de l'ordre du jour de la réunion plénière T-CY 35

Contribution écrite du Canada sur des développements législatifs récents pertinents à lutte au cybercrime, la Convention et ses protocoles :

Le 18 juin 2026, d'importantes réformes du *Code criminel* du Canada et d'autres textes législatifs visant à répondre aux menaces modernes et à protéger les victimes ont reçu la sanction royale. La plupart de ces réformes sont entrées **en vigueur le 18 juillet 2026.**

Ces réformes constituent l'une des mises à jour les plus importantes depuis des générations pour remédier aux délais, protéger les victimes et les personnes survivantes de violence fondée sur le sexe, y compris la violence sexuelle et la violence entre partenaires intimes, et pour garder nos enfants à l'abri des personnes prédatrices, y compris en ligne.

Ces réformes incluent notamment une réponse législative criminelle aux hypertrucage sexuellement explicites et à la sextorsion, y compris celle visant les enfants.

Pour de plus amples détails, voir :

Loi visant à protéger les victimes : projet de loi visant à protéger les victimes et à garder les enfants à l'abri des personnes prédatrices

COLOMBIA

Ministerio de Relaciones Exteriores

INTERVENCIÓN-INFORMACIÓN SOBRE EL 25 ANIVERSARIO DEL CONVENIO
35ª Sesión Plenaria del Comité del Convenio sobre Ciberdelincuencia

FECHA : 12 de octubre de 2026

ELABORÓ: DIRECCIÓN DE ASUNTOS POLÍTICOS MULTILATERALES

Señor Presidente,

Nos encontramos en un momento en el que la evolución de las amenazas en materia de ciberdelincuencia genera desafíos sin precedentes para los gobiernos, y los instrumentos que la comunidad internacional ha creado para enfrentarla.

El ecosistema criminal se ha profesionalizado: el ransomware y el modelo de cibercrimen como servicio han reducido la barrera de entrada para actores con pocos conocimientos técnicos, mientras que la inteligencia artificial permite automatizar y escalar el phishing, los fraudes y la creación de contenidos falsos con un costo y esfuerzo mínimo. A ello se suman la extorsión sexual y la explotación sexual infantil en línea, las estafas y los ataques contra infraestructura crítica y cadenas de suministro.

Pero el desafío va más allá de los delitos informáticos en sentido estricto: hoy casi todos los delitos tienen un componente digital, ya sea en la planificación, la comunicación, la financiación o la ejecución. Esto significa que la evidencia electrónica ha dejado de ser un recurso especializado para convertirse en un elemento presente en la gran mayoría de las investigaciones penales, lo que exige marcos de cooperación ágiles, capacidades técnicas ampliadas y salvaguardias que se apliquen de forma consistente.

En este contexto, es indispensable aprovechar con decisión y responsabilidad todas las herramientas disponibles. El Convenio de Budapest es, un acuerdo de valores y un conjunto de instrumentos prácticos para enfrentar desafíos colectivos cada vez más complejos. Acordar una noción común de las conductas punibles, preservar la evidencia con estándares compartidos y sostener canales permanentes de cooperación ante solicitudes transfronterizas son decisiones que reflejan una visión común sobre qué se protege y por qué. Más que compromisos técnicos, son compromisos con el bienestar de las personas y con la estabilidad del ecosistema digital global.

Señor Presidente,

Colombia considera que el Convenio de Budapest seguirá respondiendo a los desafíos actuales y emergentes porque su diseño lo permite. Sus disposiciones sobre tipificación, medidas procesales y cooperación internacional son neutrales frente a la tecnología, lo que le ha permitido abarcar fenómenos que no existían en 2001. Sin embargo, para que continúe teniendo la efectividad esperada, se requiere que su orientación esté enfocada en resultados verificables y con instrumentos concretos.

En este esfuerzo, los estudios, las notas de orientación del T-CY y las herramientas de capacitación son pilares fundamentales, pues traducen el marco normativo en productos prácticos para las Partes.

Entre estas herramientas, Colombia desea destacar el fortalecimiento de capacidades. Su valor no se limita a la oferta de cursos y seminarios, que sin duda enriquecen el intercambio de conocimientos, sino que radica también en la capacidad de escuchar con atención las necesidades de cada país, de acompañar conversaciones complejas con múltiples sectores, de promover cursos de acción adaptados al contexto y a los tiempos nacionales, y de comprender las particularidades locales sin perder de vista la perspectiva regional y global.

El proyecto GLACY-e es una muestra de ello: ha demostrado que la asistencia técnica puede ser flexible, respetuosa y sensible a la complejidad institucional de cada país. Por eso, para lograr resultados concretos en la aplicación de las disposiciones del Convenio, es fundamental seguir prestando especial atención a este componente, porque la seguridad de un país depende, en buena medida, de la capacidad de sus socios para prevenir, investigar y cooperar frente a la ciberdelincuencia.

Para concluir, Colombia considera que ningún marco normativo, por sólido que sea, funciona sin confianza. Veinticinco años de trabajo conjunto han generado relaciones entre autoridades, puntos de contacto y operadores de justicia que permiten atender con rapidez una solicitud de asistencia. Frente a fenómenos transnacionales que ningún Estado puede enfrentar de manera aislada, el desafío es traducir esa confianza en cooperación operativa: la ratificación y la implementación efectiva del Segundo Protocolo, el uso activo de la red 24/7 y el fortalecimiento de las capacidades. Así, el Convenio seguirá siendo un instrumento vivo, capaz de responder a los desafíos del presente y de anticipar los del futuro.

Muchas gracias.

COSTA RICA

35th Plenary of the Cybercrime Convention Committee

October 2026

Strasbourg, France

Delegation of Costa Rica

Item 5 – *25th anniversary of the Budapest Convention: responding to current and emerging challenges*

Costa Rica is honored to commemorate the twenty-fifth anniversary of the Budapest Convention, an instrument that has enabled us to build a common framework to address cybercrime. Since our country joined the Convention in 2017, it has progressively transformed the Costa Rican State's capacity to respond.

In 2018, with the support of the Council of Europe, cybercrime experts assessed our domestic legislation to identify necessary reforms and areas for improvement. At the same time, our participation in the T-CY and related programs enabled our national authorities to receive specialized training, thereby strengthening the legal, technical, and operational capacities required for the effective implementation of the Convention.

This became particularly significant in 2022, when Costa Rica was targeted by large-scale cyberattacks that affected more than 30 public institutions and compromised critical systems related to public finances, foreign trade, and social security. The support received from other Parties within the framework of the Convention was crucial to restoring the affected systems in a timely manner and protecting the Costa Rican population's sensitive information.

The rapid development of technologies, platforms, and digital services poses new challenges for the authorities. At the same time, the growing use of virtual assets and the increasing sophistication of artificial intelligence systems have enhanced the capacity of criminal organizations to carry out large-scale attacks, affect a greater number of people, conceal illicit proceeds, and make it more difficult to identify their members. This trend demonstrates that the Convention is more necessary today than ever before.

The adoption of the Second Additional Protocol is a clear example of the Convention's capacity to adapt to new cooperation needs. Against this background, Costa Rica took part in its negotiation and deposited its instrument of ratification in April of this year.

At the domestic level, this process has been accompanied by the strengthening of institutional, technical, and operational capacities, including the recent establishment of the Deputy Prosecutor's Office against Cybercrime, which has been operational since May of this year.

However, the effective application of this framework requires continuous training, appropriate technical tools, interinstitutional coordination, and close communication with service providers and foreign authorities. In this regard, the work carried out by the T-CY through guidance notes, assessment reports, practical guides, and exchanges of experience enables the identification of common problems, the sharing of solutions, and the maintenance of a continuous process of improvement.

Likewise, we consider it essential to continue promoting training programs for prosecutors, judges, police officers, and technical personnel; to implement mechanisms for verifying the authenticity of requests; and to maintain channels for dialogue with service providers, international organizations, academia, and civil society.

In addition, Costa Rica considers it essential for this process to be inclusive. The effectiveness of international cooperation depends on all Parties having sufficient capacities to request, receive, and carry out the measures provided for under the Convention and its Second Protocol, regardless of their size, geographical location, or level of technological development, thereby working toward effective global cooperation against cybercrime.

During its first twenty-five years, the Budapest Convention has enabled us to build a common foundation for cooperation, trust, and institutional strengthening. The challenge for the future will be to adapt these existing foundations to technological change and to ensure that all Parties have the capacities necessary to take full advantage of this cooperation framework.

TRINIDAD AND TOBAGO

STATEMENT OF TRINIDAD AND TOBAGO AT THE 35th PLENARY OF THE COUNCIL OF EUROPE, 12 to 13 OCTOBER 2026, STRASBOURG, FRANCE

Thank you, Mr. Chairman.

The Government of the Republic of Trinidad and Tobago extends its sincere appreciation to the Council of Europe for its ongoing support and valuable assistance.

RECENT CYBER INITIATIVES IN TRINIDAD AND TOBAGO

The Government of Trinidad and Tobago maintains its firm commitment to establishing a modern and robust legislative framework against cybercrime. To this end, Mr. Chairman, I wish to highlight the following developments since our last country report at the 34th Plenary:

1. Cybercrime Policy and Draft Legislation

Mr. Chairman, as reported at the 34th Plenary, a Cyber Bill and Cybercrime Policy were submitted to Cabinet for its consideration. Upon Cabinet's approval, the Bill would be introduced into Parliament for debate and enactment.

Briefly, the Bill has 4 parts and contains 32 clauses, and seeks to create numerous cybercrime offences. It also provides for the investigation and prosecution of cybercriminals, and facilitates international co-operation in combating cybercrime offences. The Bill will repeal the Computer Misuse Act of 2000.

2. Cabinet Approval to Accede to the Budapest Convention on Cybercrime

I am pleased to report that on the 3rd of September, 2026, Cabinet approved the accession of Trinidad and Tobago to the Budapest Convention on Cybercrime. The 5-year period given to Trinidad and Tobago to accede to the Convention expires on 21 October 2026.

However, unexpected legislative backlogs and administrative transitions have delayed the finalisation of our parliamentary approval procedures. Consequently, additional time is required to conclude our domestic procedures and formally deposit our instrument of accession. On 6 October, the Honourable Attorney General, on behalf of the Government of the Republic of Trinidad and Tobago, wrote to the Secretary General requesting an extension of the invitation to accede for an additional one (1) year. This extension will ensure that our domestic legislation is robustly harmonised with the pillars of the Convention, guaranteeing effective international cooperation and procedural safeguards.

3. Other Cyber Initiatives

In 2026, the Government of Trinidad and Tobago has strengthened national and regional cyber resilience through inter-agency partnerships and institutional engagements coordinated by the Trinidad and Tobago Cyber Security Incident Response Team (TT-CSIRT). Some of the main cyber initiatives are as follows:

1. **AI & Cybersecurity Committee:** The Government formed a dedicated national coordinating body comprised of officials from the Ministry of Homeland Security, Ministry of Finance, Office of the Attorney General, and the Police Service. This Committee is tasked with blocking proactive AI fraud schemes, strengthening police investigative capacity, and identifying legislative gaps in order to strengthen our cyber security landscape.

2. **OAS Strategic Engagements:** In August 2026, the Minister of Homeland Security met with the Organization of American States (OAS) Chief of Cybersecurity, to expand national capabilities against complex digital threats.

3. **Partnership with LAC4:** In July 2026, the Government signed a Letter of Intent with the Latin America and Caribbean Cyber Competence Centre (LAC4), supported by the European Union. This agreement establishes a framework for collaboration aimed at strengthening cybersecurity governance, building technical expertise and improving cooperation to combat cyber threats across the region.

4. **Regional Collaboration with CARICOM IMPACS**: On July 17, 2026, TT-CSIRT met with the Caribbean Community Implementation Agency for Crime and Security (CARICOM IMPACS) in Port of Spain to align national and regional cyber defense strategies and protect critical infrastructure and financial networks.

Closing Remarks

Mr. Chairman, these are the updates for Trinidad and Tobago since the 34th Plenary. The Government of Trinidad and Tobago remains committed to completing the process to achieve ratification of the Budapest Convention. I thank you.

Office of the Attorney General

Government of the Republic of Trinidad and Tobago

TUNISIA

Contribution by the Representative of Tunisia

35th Meeting on the Budapest Convention on Cybercrime (TCY-35)

It is an honour and a pleasure for Tunisia to participate in this meeting and to reaffirm its commitment to strengthening international cooperation in the fight against cybercrime.

Tunisia has made important progress in this field, most notably through its accession to the Budapest Convention in 2024, marking a significant milestone in our cooperation with the Council of Europe and our commitment to addressing the challenges of an increasingly interconnected digital environment.

As we mark the 25th anniversary of the Budapest Convention, Tunisia wishes to commend its enduring contribution to the development of a common international framework for combating cybercrime, strengthening criminal justice cooperation and facilitating access to electronic evidence.

This anniversary is also an opportunity to look ahead and further enhance the Convention's impact. In our view, this requires broader international participation, more effective and timely operational cooperation, sustained investment in capacity-building, and the continuous adaptation of our tools and practices to emerging threats, including those arising from artificial intelligence. Above all, these efforts must be underpinned by mutual trust, respect for national legal systems, and robust safeguards for human rights and fundamental freedoms.

The cooperation triggered ever since Tunisia has ratified and joined the Budapest Convention has yielded considerable and noticeable results and impacts on the national efforts to fight cybercrime and circumvent its threats both nationally and internationally. The latest development was the latest evolution witnessed by Tunisia's national legal framework which continues to evolve in response to emerging challenges. In this regard, it is worth recalling that Decree-Law No. 54 of 2022 was initially adopted to address specific threats to national security, social cohesion and stability. Its recent amendment reflects Tunisia's ongoing efforts to align its national legal framework with international standards, while upholding human rights and fundamental freedoms. Tunisia remains firmly committed to combating cybercrime and all forms of cyber abuse, in a manner consistent with the rule of law and the protection of fundamental rights.

Tunisia is also committed to strengthening institutional coordination and developing the technical and judicial expertise necessary to investigate cybercrime and handle electronic evidence effectively. Our cooperation with the Council of Europe, including through the CyberSouth+ programme, reflects our determination to pursue these objectives through partnership and the exchange of expertise.

International cooperation remains indispensable in combating cybercrime. By its very nature, cybercrime transcends national borders: perpetrators, victims, digital infrastructure and electronic evidence may be located in different jurisdictions. No country can effectively address these challenges in isolation.

The fight against cybercrime faces increasingly complex challenges. The use of cryptocurrencies and other digital assets can complicate the tracing of illicit financial flows, while artificial intelligence is creating new opportunities for fraud, identity theft, disinformation and highly sophisticated cyberattacks. The rapid evolution of technology, the volatility of digital evidence, difficulties in attributing attacks and differences between national legal frameworks further complicate investigations. Addressing these challenges requires stronger international cooperation, specialised technical expertise and legal frameworks capable of adapting to emerging threats, while ensuring respect for human rights and fundamental freedoms.

The Budapest Convention provides a valuable common framework for facilitating mutual legal assistance, improving access to electronic evidence and strengthening cooperation between

competent authorities. We must continue to invest in operational cooperation, specialised training, capacity-building and the exchange of good practices.

At the same time, our collective efforts must ensure that the fight against cybercrime is conducted in accordance with human rights, the rule of law and the protection of fundamental freedoms.

Tunisia looks forward to further strengthening its cooperation with the Council of Europe and all participating countries, with a view to building a safer, more resilient and more trustworthy digital environment for our citizens.

In conclusion, I will reiterate Tunisia's full satisfaction and gratitude to the Council of Europe in general and to the Budapest Convention team including the Cybercrime Division, C-Proc as well as the Council's Bureau in Tunis for an excellent cooperation and perfect, harmonious and fruitful collaboration.

ITEM 11

COSTA RICA

35th Plenary of the Cybercrime Convention Committee

October 2026

Strasbourg, France

Delegation of Costa Rica

Item 11 – Operationalization of the Second Protocol on enhanced cooperation and disclosure of electronic evidence

As reported at the last Plenary, on April 15, Costa Rica deposited its instrument of ratification of the Second Additional Protocol, becoming the first country in the Americas and the fourth State Party to ratify this instrument.

In this context, the legal and institutional conditions necessary for its operationalization were analyzed, particularly the powers of the national authorities, the procedures for processing the new forms of cooperation, and the provisions that require adjustments to domestic law.

In 2023, several criminal law reforms were adopted, including the addition of Article 154 bis to the Code of Criminal Procedure. This provision expressly empowers national authorities to provide cooperation to foreign authorities and receive cooperation from them, including the possibility of providing information and evidence; coordinating investigations; receiving testimony and statements; and providing any other form of assistance in accordance with international instruments.

In addition, the reform adjusted the powers of the Public Prosecutor's Office and the criminal courts for handling these requests. Accordingly, the Public Prosecutor's Office is responsible for carrying out measures that fall within its investigative powers, while measures requiring judicial authorization must be handled by the courts.

This legal analysis leads us to conclude that there is a sufficient basis for implementing cooperation mechanisms between authorities. Among them is the mechanism provided for under Article 8 of the Second Protocol for obtaining subscriber information and traffic data, through a legal assessment equivalent to that which would be carried out as part of a domestic investigation.

At the same time, the Judiciary established the Deputy Prosecutor's Office against Cybercrime, which has been operational since May of this year. This new specialized prosecution office, with nationwide jurisdiction in this field, will provide technical support and facilitate the coordination of the measures necessary for handling these new mechanisms.

In summary, Costa Rica has a legal and institutional framework that will enable it to implement the cooperation mechanisms between authorities established under Articles 8, 9, and 10. At the same time, the legislative reforms necessary for the full implementation of the direct cooperation procedures provided for under Articles 6 and 7 are currently under development.

Throughout this process, the exchange of solutions and experiences among the Parties, together with technical assistance, is particularly valuable, especially regarding direct cooperation with service providers, the authentication of requests, and domestic procedures for the application of these mechanisms. Costa Rica appreciates the support provided by the Council of Europe and looks forward to continuing to benefit from these opportunities as it advances the adjustments necessary for the full implementation of the Second Additional Protocol.

ITEM 12

BENIN

DÉCLARATION DE LA DÉLÉGATION DE LA RÉPUBLIQUE DU BÉNIN

35e session du Comité de la Convention sur la cybercriminalité (T-CY) Point : Les centres d'escroquerie en ligne et les formes connexes de criminalité organisée facilitée par les technologies numériques

Monsieur le Président,

Mesdames et Messieurs les représentants des États Parties, Mesdames et Messieurs,

La délégation de la République du Bénin remercie le Comité d'avoir inscrit à l'ordre du jour de cette session la question des centres d'escroquerie en ligne, dont le développement constitue une menace croissante pour la sécurité des personnes, la stabilité économique et la confiance dans l'économie numérique.

Le Bénin considère que ce phénomène dépasse largement le cadre de la cybercriminalité. Il se situe au croisement de la criminalité organisée, de la traite des êtres humains, du travail forcé, du blanchiment de capitaux et de l'exploitation frauduleuse des services financiers numériques.

Pour l'Afrique de l'Ouest et l'Afrique en général, cette menace appelle une vigilance particulière. La progression des services numériques et des paiements mobiles offre des opportunités considérables à nos populations, mais crée également de nouvelles possibilités d'exploitation criminelle. Les réseaux peuvent recruter dans un pays, organiser leurs activités dans un autre, collecter les fonds dans plusieurs juridictions et cibler des victimes partout dans le monde.

Nous devons notamment prendre en compte trois évolutions.

Premièrement, **l'utilisation de l'intelligence artificielle** facilite l'automatisation des escroqueries, la personnalisation des messages frauduleux, l'imitation de voix ou d'images, ainsi que la création de faux profils et de fausses identités. Ces technologies permettent aux réseaux criminels d'accroître la crédibilité, le volume et la portée de leurs opérations.

Deuxièmement, **le détournement des services de mobile money et des paiements numériques** peut faciliter la collecte, le fractionnement et le transfert rapide des produits de l'escroquerie, notamment au moyen de comptes intermédiaires et de prête-noms. La coopération entre les services d'enquête, les opérateurs de télécommunications, les prestataires de paiement et les cellules de renseignement financier est donc essentielle.

Troisièmement, **les fausses offres d'emploi, de prêts financiers en ligne** constituent un autre mode d'exploitation préoccupant. Des victimes peuvent être attirées par des promesses de crédit rapide, puis contraintes de payer des frais fictifs, de communiquer leurs données personnelles ou bancaires, voire d'entrer dans des circuits frauduleux. Ces pratiques peuvent aggraver leur vulnérabilité économique et favoriser d'autres formes d'exploitation.

Par ailleurs, les personnes découvertes dans ces centres ne sont pas toutes nécessairement des participants volontaires. Certaines peuvent avoir été recrutées par de fausses offres d'emploi, déplacées, menacées ou contraintes de commettre des escroqueries. Notre réponse doit donc distinguer les organisateurs et bénéficiaires des réseaux des personnes susceptibles d'être victimes de traite ou de coercition.

Monsieur le Président,

Le Bénin estime que la Convention de Budapest et les mécanismes de coopération qui lui sont associés offrent un cadre important pour renforcer les enquêtes, la préservation des preuves électroniques et la coopération transfrontière, en complément des autres instruments internationaux applicables.

À cet égard, notre délégation souhaite soumettre **quatre propositions concrètes**.

Premièrement, créer au sein du T-CY un groupe de travail sur les centres d'escroquerie en ligne et la criminalité organisée facilitée par les technologies numériques.

Ce groupe aurait pour mandat d'analyser les modes opératoires émergents, notamment l'utilisation de l'intelligence artificielle, le détournement du mobile money, les fausses offres de prêts et les mécanismes de blanchiment. Il pourrait élaborer, dans un délai initial de douze mois, des orientations pratiques destinées aux enquêteurs, magistrats et autorités compétentes, ainsi que des recommandations sur la coopération internationale. Ses travaux devraient associer, selon les besoins, des experts d'INTERPOL, de l'ONUDC, d'AFRIPOL, de la CEDEAO et du secteur privé.

Deuxièmement, renforcer la coopération opérationnelle et la préservation des preuves électroniques.

Nous encourageons une utilisation plus efficace des points de contact disponibles 24 heures sur 24 et 7 jours sur 7, des mécanismes d'entraide judiciaire et des procédures applicables de coopération avec les prestataires de services. L'objectif est de réduire les délais de préservation des données, de faciliter les enquêtes conjointes et de remonter jusqu'aux organisateurs et aux bénéficiaires financiers.

Troisièmement, renforcer les capacités et la coopération régionale en Afrique.

Nous proposons des formations conjointes associant enquêteurs, magistrats, spécialistes de la criminalité financière et autorités chargées de la lutte contre la traite. Ces formations devraient porter sur l'investigation numérique, le traçage des actifs virtuels, l'analyse des transactions de mobile money et l'identification des victimes. Une coopération accrue entre les pays africains, la CEDEAO, AFRIPOL et INTERPOL permettrait de mieux coordonner les signalements et les opérations transfrontières.

Quatrièmement, adopter une approche centrée sur les victimes et les droits fondamentaux.

Nous encourageons l'élaboration de lignes directrices permettant d'identifier les personnes victimes de traite ou contraintes de participer aux escroqueries, de garantir leur accès à une assistance appropriée et d'évaluer leur responsabilité individuelle conformément au droit applicable. Nous appelons également à une coopération renforcée avec les plateformes numériques et les prestataires financiers pour prévenir les fraudes, détecter les circuits suspects et faciliter, lorsque les conditions légales sont réunies, le gel et la récupération des avoirs criminels.

Monsieur le Président, Mesdames et Messieurs,

Le Bénin estime que notre réponse collective doit poursuivre trois objectifs : **démanteler les réseaux criminels, assécher leurs circuits financiers et protéger les personnes exploitées ou victimes d'escroquerie.**

Nous invitons donc le T-CY à examiner favorablement la création du groupe de travail proposé, avec un mandat précis, un calendrier de mise en œuvre et des résultats mesurables.

Face à des réseaux qui opèrent sans considération des frontières, notre coopération doit être rapide, coordonnée et fondée sur le droit. C'est à cette condition que nous pourrons préserver les bénéfices de la transformation numérique, renforcer la confiance de nos populations et lutter efficacement contre cette criminalité organisée.

Je vous remercie de votre aimable attention.

Représentant du Bénin au T-CY, Chef de délégation

MEXICO

Buenos días Señor Presidente, mesa directiva y delegados,

Antes de iniciar me permito mencionar que México agradece al Consejo de Europa la invitación a participar en esta (trigésima quinta) 35ª sesión plenaria del T-CY y felicita al Comité por el 25º aniversario de la apertura a la firma del Convenio sobre la Ciberdelincuencia. Durante un cuarto de siglo, el Convenio de Budapest ha moldeado la legislación penal y las prácticas de cooperación mucho más allá de sus Estados parte — incluidos México y América Latina— y ha proporcionado una base común para los profesionales de diversas regiones. México reconoce que el Convenio de Budapest sigue siendo un referente internacional en la lucha contra la ciberdelincuencia y agradece la oportunidad de participar en este espacio en donde a través del intercambio de experiencias se buscará reforzar las capacidades y buenas prácticas dentro de nuestra nación.

● *México aprecia la inclusión del fenómeno de los centros de ciberestafas en la agenda del T-CY. Se trata de un tipo de cibercrimen híbrido que combina el fraude facilitado por medios digitales y electrónicos implementados por la delincuencia organizada para la trata de personas, el lavado de dinero y el uso de activos virtuales que no se limitan a una sola región.*

● *En México, los centros de ciberestafas han evolucionado de células aisladas a estructuras organizadas y transnacionales que operan bajo un modelo de negocio con redes integradas por ciudadanos mexicanos y extranjeros. Si bien su actividad principal es el ciberfraude a través de centros de llamadas falsos, ingeniería social, bases de datos filtradas, ofertas de empleo fraudulentas, aplicaciones de préstamos abusivos, alertas bancarias y tiendas en línea falsas, también están vinculados al narcotráfico, el lavado de dinero, la trata de personas y la extorsión y, dependen cada vez más de la inteligencia artificial. Destacamos que las autoridades mexicanas han llevado a cabo operaciones de alto impacto para desmantelar centros de llamadas y complejos residenciales utilizados para estos fines.*

● *México considera que cualquier respuesta debe centrarse en las víctimas. Muchas de las personas que trabajan en estos centros han sido reclutadas mediante ofertas de empleo falsas y sometidas a coacción.*

● *México está particularmente preocupado por el reclutamiento y la explotación de niños y adolescentes por parte de estas redes a través de redes sociales, juegos en línea y plataformas digitales.*

● *Desde una perspectiva operativa, nuestra experiencia destaca el valor de los equipos multidisciplinarios que se implementaron a partir del 2016 a través de un Modelo de Unidades de Policías Cibernéticas que han trabajado en conjunto en la lucha contra el cibercrimen colaborando de manera estrecha en los mecanismos de preservación inmediata de evidencia digitla y electrónica especialmente durante las primeras horas de una investigación cuando es más probable obtener registros técnicos útiles.*

● *Como parte de los esfuerzos nacionales para reforzar nuestras capacidades, en el marco del Consejo de Europa, México ha participado en actividades de fortalecimiento en el proceso de investigación sobre ciberdelincuencia y evidencia electrónica. Por ejemplo, del 2 al 4 de septiembre de 2026, los proyectos GLACY-e y CyberSPEX, en colaboración con la Fiscalía General del Estado de Querétaro, impartieron capacitación práctica a peritos, analistas, personal de investigación y fiscales, incluyendo la cooperación internacional mediante el Convenio de Budapest y su Segundo Protocolo.*

● *México reconoce que el desafío radica también en correlacionar cuentas de mensajería, dominios, números telefónicos, dispositivos y flujos financieros con la antelación suficiente para identificar roles, infraestructura y ganancias ilícitas.*

● *La inteligencia financiera ha sido un componente clave de estas investigaciones, por ello en 2004 se creó la Unidad de Inteligencia Financiera de México que analiza los reportes de operaciones inusuales provenientes del sistema financiero para identificar patrones vinculados a esquemas de ciberfraude como *phishing*, *smishing* y *pharming*, incluyendo la forma en que se reciben, transfieren y dispersan los fondos ilícitos, así como las conexiones entre transacciones que no serían evidentes si se analizaran de forma aislada. El intercambio oportuno de información entre Unidades de Inteligencia Financiera, a través de canales como la red segura de Egmont (Egmont Secure Web), debe articularse mejor con la cooperación policial y judicial.*

● *La cooperación con los proveedores de servicios de activos virtuales es igualmente esencial para obtener información de identificación del cliente (KYC), historiales de transacciones, direcciones IP y registros de acceso, a fin de facilitar la localización, el congelamiento, el decomiso y la eventual recuperación de activos, con las salvaguardias legales correspondientes. El desafío consiste en pasar de investigaciones aisladas sobre usuarios, cuentas o transacciones a investigaciones exhaustivas de redes delictivas transnacionales.*

● *Estos casos requieren el uso combinado de diversos marcos: las facultades procesales y los instrumentos de cooperación del Convenio de Budapest y su Segundo Protocolo, la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y su Protocolo sobre la Trata de Personas, la Convención de las Naciones Unidas sobre la Ciberdelincuencia y las normas del Grupo de Acción Financiera (GAFI) relativas a los activos virtuales.*

● *México alienta al Comité del Convenio sobre Ciberdelincuencia (T-CY) para mantener los esfuerzos en el combate a este tipo de Cibercrimen que dañan psicologica y económicamente a las poblaciones.*

● *Como posibles pasos a seguir, México apoyaría un ejercicio de mapeo o de elaboración de orientaciones sobre el uso de los instrumentos del Convenio en casos relacionados con centros de fraude —vinculado estrechamente al seguimiento del estudio sobre activos virtuales (punto 14)—, así como la cooperación con la UNODC, INTERPOL, el Grupo de Acción Financiera Internacional y otras organizaciones pertinentes.*

● *Finalmente, México se suma a la propuesta de Australia y Chile para generar una mesa de diálogo que permita atender de manera integral este fenómeno.*

Agradeciendo las atenciones que sirvan al presente, reciban todo un cordial saludo.

CHILE

Intervención de Chile

Punto 12 – (Cyber Scam Centres)

Muchas gracias, señor Presidente.

Chile agradece la oportunidad de intercambiar opiniones sobre los centros de estafas cibernéticas y sus crecientes implicancias para la cooperación internacional en la lucha contra la ciberdelincuencia.

Consideramos que este fenómeno refleja una tendencia cada vez más relevante: la convergencia entre la ciberdelincuencia y el crimen organizado transnacional, incluyendo , el lavado de activos, la utilización ilícita de activos virtuales y otras actividades delictivas graves.

Lo que hemos observado en nuestro país es un aumento sostenido tanto en la cantidad de casos como el impacto económico de los mismos. Hemos detectado múltiples variantes de este fenómeno criminal , entre las que se encuentran, por ejemplo, los fraudes con redirección de pagos, (Business Email Compromise (BEC), la instalación de programas maliciosos o malware, el phishing (robo de datos), los fraudes con tarjetas de crédito y pasarelas de pago, los fraudes de suplantación de identidad en redes sociales y telecomunicaciones, el fraude mediante plataformas de inversión en línea (trading), los fraudes románticos y las estafas de empleo mediante ofertas falsas de trabajo, entre otras,

En virtud de lo anterior, nuestro país estima que estos delitos deben ser abordados como una manifestación de criminalidad económica que trasciende el tipo penal específico en que pueda subsumirse cada conducta. Su persecución requiere una visión integral del fenómeno, que no se limite al análisis aislado de cada causa, sino que permita identificar a defraudadores prolíficos, detectar patrones de actuación y establecer la participación de quienes facilitan sus cuentas bancarias para recibir y dispersar los fondos obtenidos mediante fraude.

Advertimos tambien, constituye una importante fuente de ingresos para la delincuencia organizada, facilitando la comisión de otros delitos, como el terrorismo, el tráfico de drogas y la trata de personas, entre otras. Representa además una amenaza permanente y sofisticada para la prevención del lavado de activos, pues las organizaciones criminales procuran incorporar al sistema financiero los recursos provenientes del fraude y otros delitos con el fin de ocultar su origen ilícito.

Los centros de estafas cibernéticas demuestran que la ciberdelincuencia ya no puede abordarse exclusivamente como una cuestión técnica o especializada de justicia penal. En determinadas circunstancias, estas estructuras criminales también pueden plantear desafíos más amplios para la seguridad pública, la integridad institucional y la estabilidad regional.

Desde nuestra perspectiva, esta amenaza requiere una respuesta integral y coordinada, que involucre a distintos actores.

En este sentido, Chile esta año **constituyó una MESA NACIONAL CONTRA FRAUDE FINANCIERO TRANSNACIONL, cuyo objeto**Establecer un marco estratégico de cooperación y coordinación intersectorial entre el Ministerio Público, los organismos reguladores: SII, Sernac y CMF y el sector privado financiero: ABIF y el Retail Financiero destinado a prevenir, detectar y perseguir eficazmente el fraude financiero en Chile.

Este ecosistema de colaboración busca reducir la incidencia de delitos económicos y financieros mediante el intercambio sistemático de información estadística y técnica, que permita levantar patrones, la adopción de estándares internacionales emanados de la ONU (Cumbre Mundial contra el Fraude 2026) y la optimización de los procesos de respuesta ante el aumento crítico de causas judiciales, garantizando con ello la integridad del sistema financiero y la protección efectiva de los activos de los ciudadanos

Desde otra perspectiva, consideramos especialmente importante prestar atención a las personas que son obligadas a participar en actividades criminales dentro de estos centros. Las respuestas de los Estados deberían tener en cuenta su posible condición de víctimas de trata de personas, procurando que las medidas de justicia penal sean coherentes con las obligaciones internacionales aplicables en materia de derechos humanos y los principios de protección de las víctimas.

En cuanto al papel de los instrumentos jurídicos internacionales existentes, Chile considera que el Convenio de Budapest y sus Protocolos proporcionan herramientas importantes para apoyar las investigaciones y la cooperación internacional, particularmente en materia de prueba electrónica y cooperación transfronteriza.

Al mismo tiempo, la naturaleza compleja de estos centros requiere una coordinación eficaz con otros instrumentos internacionales pertinentes, incluidos aquellos relativos a la delincuencia organizada transnacional, la trata de personas y el lavado de activos.

En este sentido, estimamos que la complementariedad entre los marcos jurídicos existentes debería continuar siendo un principio orientador, evitando duplicaciones innecesarias y promoviendo su implementación efectiva.

Respecto de los posibles trabajos futuros del T-CY, Chile favorecería una aproximación que promueva el intercambio de experiencias nacionales, la identificación de buenas prácticas y una cooperación más estrecha con las organizaciones internacionales con iniciativa en la temática , incluyendo la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) e INTERPOL.

Finalmente, Chile estima que el T-CY se encuentra en una posición privilegiada para contribuir a una mejor comprensión y el combate de este fenómeno.

Por consiguiente, acogemos favorablemente la continuación de estas discusiones, con miras a identificar ámbitos concretos en los que el T-CY pueda aportar un valor agregado a las Partes.

Muchas gracias, señor Presidente.

COLOMBIA

Ministerio de Relaciones Exteriores

INTERVENCIÓN- CENTROS DE ESTAFAS EN LÍNEA

35ª Sesión Plenaria del Comité del Convenio sobre Ciberdelincuencia

FECHA : 13 de octubre de 2026

ELABORÓ: DIRECCIÓN DE ASUNTOS POLÍTICOS MULTILATERALES

Señor Presidente,

Colombia valora que el T-CY inicie este intercambio. Los centros de ciberestafas ya no son un fenómeno regional, INTERPOL ha documentado su expansión a diferentes partes del mundo, con víctimas de más de 80 nacionalidades. Estos centros operan como estructuras criminales organizadas, que distribuyen funciones de reclutamiento, supervisión, soporte tecnológico y servicios financieros. Su modus operandi, que capta a personas con ofertas laborales engañosas y las obliga a cometer fraudes en línea, evidencia que ya no podemos separar el análisis de la ciberdelincuencia del de la trata de personas. Esa convergencia existe, está en incremento y exige respuestas que integren ambos enfoques.

Conscientes de esta realidad, Colombia fortaleció su marco normativo con la Ley 2608 de 2026, que actualiza la legislación sobre trata de personas. La ley establece como circunstancia de agravación punitiva que la conducta se ejecute mediante tecnologías de la información y las comunicaciones o servicios digitales, incluidas las redes sociales, las aplicaciones móviles y las plataformas en línea. Además, reconoce la delincuencia forzada como una forma de explotación y dispone que las víctimas de trata no serán criminalizadas por delitos cometidos como consecuencia de esa situación, un principio central frente a las dinámicas de los centros de estafa, cuyos operadores forzados son, ante todo, víctimas.

La ley también ordena capacitar a las autoridades en investigación en entornos digitales y en ciberseguridad, fortalecer la cooperación internacional con protocolos expeditos de actuación conjunta, intercambios seguros de información y mecanismos de reacción rápida frente a la trata en entornos digitales y transfronterizos, así como promover el trabajo con plataformas y aplicaciones digitales.

En este contexto, es claro que el marco del Convenio de Budapest ofrece herramientas esenciales para enfrentar estos fenómenos, a través de la preservación expedita de evidencia

digital, la asistencia mutua y la red 24/7 de puntos de contacto, mientras que el Segundo Protocolo prevé mecanismos adicionales más ágiles, como la cooperación directa con proveedores de servicios y la asistencia de emergencia. Sin embargo, para aprovechar plenamente estas herramientas es necesario consolidar buenas prácticas de cooperación con el sector privado, cuya participación es indispensable para acceder a los datos, rastrear los flujos financieros y los activos virtuales, y actuar con rapidez frente a redes criminales que se adaptan constantemente.

Por ello, Colombia propone que el T-CY considere, como posible curso de acción, la elaboración de un estudio de mapeo sobre el uso del Convenio frente a los centros de ciberestafas y la delincuencia organizada facilitada por medios cibernéticos. Este ejercicio permitiría identificar cómo las Partes han aplicado herramientas ya disponibles, como la preservación expedita, la asistencia mutua y la red 24/7, y qué buenas prácticas y obstáculos han surgido en la cooperación con el sector privado. Permitiría, además, analizar la relevancia que tendrán los mecanismos del Segundo Protocolo una vez entre en vigor, lo que daría una razón adicional para promover su firma y ratificación. Con el fin de que el estudio sea útil y evite duplicar esfuerzos, convendría que se apoye en el trabajo que ya adelantan organizaciones como INTERPOL y UNODC, y que lo complemente desde la perspectiva específica del Convenio y su marco de cooperación.

Para concluir, Colombia desea subrayar la importancia del fortalecimiento de capacidades como condición para que las herramientas del Convenio y de su Segundo Protocolo se traduzcan en resultados concretos. Enfrentar los centros de ciberestafas y las demás modalidades de delincuencia organizada facilitada por medios cibernéticos exige fortalecer a todos los actores de la cadena de justicia penal. Las autoridades de aplicación de la ley necesitan estar preparadas para ejecutar operativos policiales, adelantar investigaciones coordinadas y capturar a las estructuras criminales; los fiscales y los jueces, para manejar evidencia electrónica compleja, solicitar y valorar cooperación internacional y juzgar estos casos con las garantías del debido proceso; y la ciudadanía, para reconocer y evitar estos engaños mediante campañas de prevención. Ningún Estado puede lograrlo de manera aislada. Por ello, Colombia hace un llamado a seguir fortaleciendo la cooperación y la capacitación, para que ningún Estado quede rezagado frente a estas amenazas.

Muchas gracias.

PHILIPPINES

35th Plenary of the Cybercrime Convention Committee (T-CY)
Agenda Item 12: Cyber Scam Centers
13 October 2026 | Strasbourg, France

Republika ng Pilipinas

KAGAWARAN NG KATARUNGAN

Department of Justice

Manila

BAGONG PILIPINAS

INTERVENTION OF THE PHILIPPINES

35th Plenary of the Cybercrime Convention Committee (T-CY)
Agenda Item 12: Cyber Scam Centers
13 October 2026 | Strasbourg, France

Representative of the Philippines to the T-CY

INTRODUCTION

Thank you, Mr. Chair, and good morning to our distinguished colleagues. I am honored to share the Philippine experience in dismantling cyber scam centers and addressing their links to trafficking in persons and transnational organized crime.

Allow me to briefly share the Philippine experience, the challenges we have encountered, and possible areas for further work by the Cybercrime Convention Committee.

I. THE PHILIPPINE EXPERIENCE

A significant case involved a law enforcement operation in March 2024 against a Philippine Offshore Gaming Operator, or POGO, in Bamban, Tarlac, a province in the northern Philippines.

The law enforcement operation was prompted by reports of individuals being illegally detained and forced to work inside the compound. The operation involved several government agencies, including the Presidential Anti-Organized Crime Commission, the Philippine National Police, and the Inter-Agency Council Against Trafficking of the Department of Justice.

Authorities rescued hundreds of individuals and uncovered suspected online scamming and trafficking activities.

What makes this case particularly significant is that the investigation did not end with the individuals found inside the compound.

Authorities examined corporate records, business permits, property ownership, and other evidence, and discovered connections to Alice Guo, who was then the Mayor of Bamban, Tarlac.

Although Alice Guo was not among those apprehended during the raid, subsequent investigations found her involvement in the corporate entities associated with the facility, including the company that owned the property where the POGO operated.

These investigations eventually led to her prosecution and conviction for qualified trafficking in persons in November 2025.

This case illustrates an important lesson: dismantling a cyber scam center requires investigators to look beyond the physical facility and the individuals found operating within it.

Investigations must also examine corporate structures, beneficial ownership, financial transactions, and other connections to identify those who organize, finance, control, or facilitate these criminal operations.

More recently, a little more than a week ago, on the 2nd of October, an operation was conducted in the southern part of the country, apprehending 244 foreign nationals and recovering 3,000 electronic devices and SIM cards believed to have been used for online scams. The operation involved civilian law enforcement agencies, including the Bureau of Immigration and the National Bureau of Investigation, with the Armed Forces of the Philippines, for security support.

II. INVESTIGATIVE AND PROSECUTORIAL CHALLENGES

From the Philippine experience, I would highlight three challenges.

First, handling and access to electronic evidence.

Seized devices may contain communications, account information, and financial transactions. It is necessary for the personnel to be **trained** to properly handle this evidence and ensure its admissibility in court. Moreover, subscriber information and other data may be held by foreign service providers, making timely access difficult.

Second, identifying organizers and trafficking victims.

Investigators must distinguish co-conspirators from individuals deceived or coerced, ensuring that trafficking victims receive appropriate screening and protection.

Also, those arrested may not be the ones actually directing the illegal activities. Specialized corporate and financial investigators must examine financial statements, corporate records, and beneficial ownership documents to identify those who ultimately control and profit from these operations.

Third, cross-border financial networks and asset recovery

Victims, suspects, and financial flows may span multiple jurisdictions. Stolen funds can move through layered transactions, various mule accounts, and virtual-asset channels.

And then even when proceeds are traced and frozen, their forfeiture may require separate proceedings and international coordination.

III. PHILIPPINE RESPONSES

Our approach balances strengthened investigation powers with due process safeguards. We have laws on cybercrime, financial accounts, SIM cards, money laundering, and most recently, POGOs.

In 2025, we developed standard operating procedures for various government agencies for online scam center investigations. This was signed in April of this year.

We are also considering a National Anti-Scam Hub to coordinate law enforcement, financial institutions, and telecommunications entities, but its formal establishment has yet to be finalized.

IV. THE BUDAPEST CONVENTION AND POSSIBLE NEXT STEPS

In the POGO cases, the mechanisms of the Convention and especially of the 2nd Additional Protocol, on evidence preservation, disclosure, and investigative assistance could help identify transnational networks, support prosecution, and trace criminal proceeds.

That is why we are pursuing the domestic steps for accession to the Second Additional Protocol.

In relation to these experiences, we encourage this body to consider guidance notes on the implementation of the Convention and 2nd Additional Protocol, particularly on financial

investigations and asset tracing and recovery. We should also consider capacity building programs integrating cybercrime investigations with trafficking in persons, corporate ownership, and money laundering.

CONCLUSION

Mr. Chair, to conclude, we hope that sharing our experience will help our discussions on how the Convention and Protocols can be further leveraged to address scam centers, trafficking in persons, and transnational organized crime. We thank you for the time and look forward to the fruitful exchange of views.

ITEM 15

MEXICO

Agenda de la 35a Reunión Plenaria del T-CY (Convenio de Budapest) y Conferencia de Cooperación contra la Ciberdelincuencia (Octopus)

Punto de la agenda No. 15. Ciberviolencia

- México celebra la actualización del Recurso sobre Ciberviolencia y apoya la labor continua del T-CY en este tema. La ciberviolencia incluye diversas conductas como: amenazas, acoso, extorsión, difusión no consentida de imágenes íntimas, suplantación de identidad y abuso coordinado generando consecuencias reales fuera del ámbito digital y afecta gravemente a mujeres, a la niñez y a las víctimas de estas conductas delictivas.

- En México se ha desarrollado marcos jurídicos en esta materia, como la Ley Olimpia, que reconoce la violencia digital en la Ley General de Acceso de la Mujer a una Vida Libre de Violencia y tipifica como delito las violaciones de la intimidad sexual en el Código Penal Federal, así como La Ley General para Prevenir, Sancionar y Erradicar los Delitos en Materia de Trata de Personas, que sanciona en todas sus modalidades a nivel federal, con reformas adoptadas por la mayoría de nuestros estados. México estaría encantado de compartir esta experiencia y contribuir a mantener actualizado el Recurso.

- Nuestra experiencia también demuestra que la ciberviolencia va más allá de las violaciones de la privacidad sexual y no afecta únicamente a mujeres y niñas. Otros colectivos han sufrido daños psicológicos y económicos a través de conductas perseguidas como fraude, robo de identidad, material de abuso sexual infantil o cobro ilegítimo de deudas. Una comprensión amplia del fenómeno, junto con herramientas prácticas para la preservación de pruebas electrónicas y el intercambio de información en tiempo real, contribuiría a subsanar las deficiencias que aún persisten.

- Para las autoridades de justicia penal, el reto consiste en actuar con rapidez protegiendo a las víctimas, preservando el contenido y los metadatos, vinculando cuentas y dispositivos, cooperando con las plataformas y aplicando medidas de protección sin comprometer la integridad de las pruebas ni provocar una revictimización.

- México considera que el Recurso sería especialmente útil si incorporara taxonomías compatibles, ejemplos de evidencia pertinente, vías de cooperación, criterios de preservación y buenas prácticas para evitar la revictimización. El T-CY también podría analizar la relación entre las facultades procesales de la Convención y su Segundo Protocolo y el alcance de la Convención de las Naciones Unidas sobre la Ciberdelincuencia.
- México ha avanzado en la prevención y judicialización de estas violencias digitales, logrando la desarticulación de células delictivas de estafas cibernéticas, además de que ha logrado grandes sentencias condenatorias de agresores sexuales en línea que afectan a las niñas, niños y adolescentes.

- Agradecemos la invitación a México para participar como observador, en este 25 aniversario del convenio de Budapest, sin duda la cooperación internacional, intercambio de información, herramientas y buenas prácticas son esenciales para lograr grandes resultados, por lo cual México sigue sumando esfuerzos para colaborar con diferentes agencias policiales y organismos internacionales en el combate a la ciberdelincuencia.