Strasbourg, 6 June 2025

Over 500 cybercrime experts from more than 100 countries – from public sector but also international, private sector and civil society organisations and academia – met at the Council of Europe in Strasbourg, France, from 4 to 6 June 2025 for the Octopus Conference on cooperation against cybercrime. The Conference was opened by Alain Berset (Secretary General of the Council of Europe), Jonathan Attard (Minister of Justice, on behalf of the Presidency of Malta of the Committee of Ministers) and Samuel Nartey George (Minister for Communication, Digital Technology and Innovations of Ghana).

Participants welcomed that São Tomé and Príncipe as well as Vanuatu deposited instruments of accession to the Convention on Cybercrime, that Fiji signed the Second Protocol on electronic evidence to this treaty, and that Malta joined the First Protocol on xenophobia and racism during the Conference.

Key messages resulting from Octopus 2025 are:

- Cybercrime – including ransomware, cyber interference with democracy, impunity for crime online, hate crime and hate speech, artificial intelligence (AI) crime, the criminal use of virtual assets, and other cyberthreats contribute to current international crises, conflicts and insecurity; violations of international law; injustice and human rights violations; or authoritarianism, nationalist populism and democratic back-sliding. Therefore, more cooperation, human rights and justice, accountability and effective criminal justice responses are needed.

- Participants in the Octopus Conference 2025 are all experts in their fields and are prepared to cooperate with each other; their actions and their cooperation will make a difference.

- The **Convention on Cybercrime** with its Protocols and backed up by the Cybercrime Convention Committee (T-CY) and capacity building by the Cybercrime Programme Office of the Council of Europe (C-PROC) remains a highly relevant and attractive framework as reflected in increasing membership. Following accessions during the Octopus Conference, 80 States are now Parties to this Convention.

- The **Second Protocol to the Convention on Cybercrime** (CETS 224) provides for effective and efficient means for enhanced cooperation and disclosure of electronic evidence. These tools are urgently needed by criminal justice practitioners. Private sector stakeholders welcome a comprehensive framework and are willing to cooperate to make the provisions of the Second Protocol operational. There are common expectations from judicial authorities, law enforcement and service providers: the Second Protocol is expected to bring more legal clarity and standardization of procedures in the cross-border exchange of electronic evidence. Implementation of this Protocol on domestic law, followed by ratification, should be a priority for Parties to the Convention on Cybercrime. C-PROC is offering capacity building support.

- **Capacity building by C-PROC** had a significant impact on the implementation of the Convention on Cybercrime, on legislation, criminal justice capabilities and international cooperation worldwide since 2014. Capacity building is the most effective way towards more effective investigation, prosecution and adjudication of cybercrime and other offences involving electronic evidence. A massive surge in resources and skills for criminal justice authorities, including the judiciary, is needed. More resources for more capacity building are required, also to address threats related to cyber interference with democracy, to child abuse online and other cyberviolence, to artificial intelligence and to virtual assets.

- With the United Nations treaty against cybercrime – to be opened for signature in Hanoi, Vietnam, in October 2025 ("**Hanoi Convention**") – additional options will soon be available for cooperation with and between States that are not able to join the Convention on Cybercrime. Governments are encouraged to sign this treaty and to ensure its implementation consistent with the Convention on Cybercrime and the conditions and safeguards of the new treaty.

- Interference with elections and other forms of cyber interference pose serious threats to democracy. "**Cyber interference with democracy**" refers to the use of information and communication technologies to manipulate or undermine democratic institutions, processes, or public trust in governance. Countering disinformation, making ("analogue") rules governing elections and election campaigns (including political financing and advertising) more effectively applicable to the digital environment, investigating and prosecuting cyber interference (including through the tools of the Convention on Cybercrime and its Second Protocol), taking national security measures against cyber interference also by foreign actors, and strengthening the cybersecurity of election infrastructure are critical for democratic security. Where such interference relies on the infrastructure and modus operandi of organised crime groups ("cyber interference with democracy as a service"), criminal law measures are particularly appropriate.

- Criminal justice measures to counter **disinformation**, and cybercrime in general, must meet human rights and rule of law requirements. It is of concern that in some countries, criminal law provisions cover mis- or disinformation or similar conduct in broad and vague terms that restrict the freedom of expression in a way that may not be compatible with principles of international and regional human rights law, such as legality, necessity and proportionality.

- **Artificial intelligence (AI)** is reshaping cybercrime, both in terms of offences (against, by and by means of AI systems) and in terms of opportunities to investigate crime and collect electronic evidence. This raises a number of complex legal and practical questions, including the question of the applicability of treaties such as the Convention on Cybercrime and its Protocols. The Octopus session on AI underscored that the criminalisation provisions and its cooperation tools under the Budapest Convention framework are likely to be applicable to a varied typology of AI-related scenarios. In this respect, the mapping study currently being prepared by the Working Group on Artificial Intelligence of the Cybercrime Convention Committee (T-CY) is expected to offer further insights and a more in-depth analysis of these issues. Capacity building to permit criminal justice authorities to address challenges related to AI is needed.

- **"Pig butchering"** scams have emerged as a pressing global concern. These may be committed at an industrial scale by persons in compounds who may themselves be victims of human trafficking and modern-day slavery. Collaboration among law enforcement agencies, financial institutions, technology companies and virtual asset service providers (VASPs), focusing on the sharing of information and resources, and in particular the search and seizure of virtual assets, is vital for taking down such criminal networks. This effort should be backed by strong capacity building especially for financial investigations and the recovery of crime proceeds. Task forces

that incorporate cybercrime, financial, and human trafficking investigators can improve the response to this type of threat.

- Criminal activities often rely on **virtual assets**. Enhancing cooperation among criminal justice authorities, financial intelligence units and VASPs across borders is crucial for effective investigations. Making more use of international treaties such as the Convention on Cybercrime to counter the criminal use of virtual assets would be most valuable. The mapping exercise currently being carried out by the Cybercrime Convention Committee (T-CY) to study the applicability of the Convention to virtual assets and VASPs, therefore, is much welcome. More capacity building to permit criminal justice authorities to search, seize and confiscate crime proceeds in the form of virtual assets is needed. Targeting virtual assets that are crime proceeds should be mainstreamed into criminal investigations. Despite challenges such as issues related to jurisdiction, limited resources for both law enforcement, and others, progress in investigating virtual asset-related crime is advancing through increased VASP cooperation, stablecoin issuer involvement, growing compliance by decentralized finance, and strengthened international partnerships.

- **War crimes**, in principle, can be committed through the use of computer systems and data, including cybercrime offences under the Convention on Cybercrime. Conditions of severity of damage, principles of distinction and proportionality, and other applicable principles of international law are instrumental in legal assessment of cyberattacks and cybercrime as war crimes. While the existing provisions and principles can be applied and interpreted, some new areas such as use of AI and autonomous weapons systems may necessitate more specific regulation. Irrespective of legal qualification of cybercrime as war crime, the principles of gathering, handling of and co-operation on electronic evidence through specialized tools and powers – including those provided by the Budapest Convention and its related standards - remain fully applicable to criminal investigation of war crimes and related offences. The Russian war of aggression against Ukraine is the most current and profound example demonstrating necessity and practical impact of designating cybercrime as war crime.

- Tackling **cyberviolence**, including in the form of the **non-consensual dissemination of intimate images (NCDII)** requires concerted and prioritised action. The convergence of international standards – such as the UN Convention against Cybercrime and the EU Directive on combating violence against women and domestic violence – presents an unprecedented opportunity to harmonize legal responses for the criminalisation of NCDII and to strengthen cross-border cooperation. Domestic laws must also allow for clear and careful legal qualification of cases, ensuring that responses are proportionate, context-sensitive and avoid over-criminalisation. Criminal justice professionals need appropriate legal and technical tools to investigate and prosecute effectively, while applying a survivor-centred approach that respects the rights and dignity of those affected. Strong cooperation with online platforms is equally essential to ensure the timely removal of content, preservation of evidence, and timely enforcement.

- **AI-generated child sexual abuse material** (CSAM) remains a serious and growing threat to children requiring an effective criminal justice response. Legislative and policy gaps persist in some jurisdictions. Prosecution is often hindered by definitional ambiguities, evidentiary challenges, and the cross-border nature of online abuse. The harm caused by AI-generated CSAM – whether to survivors of past abuse or to societal perceptions of child sexual exploitation and sexual abuse – is real and significant. Addressing this threat requires legal definitions to be adapted to include synthetic content, investigators to be equipped with tools to distinguish AI-generated from CSAM featuring an identifiable child victim, and international cooperation to be strengthened through instruments such as the Lanzarote Convention and the Budapest Convention on Cybercrime, including its Second Additional Protocol. Leveraging

AI for detection and analysis, while ensuring strong safeguards and oversight, is also critical to an effective and child-centred response.

- **Young people** are deeply embedded in the digital world, not only as victims of online threats such as cyberbullying, sextortion, and hate speech, but also, at times, as perpetrators or facilitators of offences including "hacking", financial scams or the dissemination of illegal content. Yet they are not only vulnerable – they are also key allies in building safer digital environments. Addressing youth and cybercrime requires a balanced and rights-based approach that protects young people from harm while prioritising education, empowerment, and prevention. Law enforcement, policymakers, and technology platforms must engage directly with young people, not only to address threats, but to design solutions that are relevant, inclusive, and sustainable. Restorative justice, specialised youth cybercrime units, and youth-informed policies can ensure responses are proportionate and future-focused

- **Regional priorities and capabilities** for addressing cybercrime vary significantly, shaped by unique economic, political, and cultural contexts. Nevertheless, targeted and tailored capacity building is a necessity common to all regions. Self-sustainable, domestically driven initiatives to effectively combat cyber threats should be promoted. This involves:

  - Support to robust policies and legal frameworks tailored to domestic needs, while fully consistent international treaties; and development of guides and materials to support the governments of small states to enact reforms on cybercrime and pursue successful implementation of such reforms. Challenges like logistical constraints, limited technical expertise, and fragmented policy frameworks can undermine progress. Debates during the regional workshop for the **Pacific** confirmed that harmonizing cybercrime legislation in line with international standards is essential for Pacific Island States to effectively address rapidly evolving threats posed by cybercriminals.

  - Support to integrating a gender-sensitive perspectives on cybercrime within the criminal justice system. The fight against cybercrime requires, along other measures, the active involvement of women in the criminal justice chain, alongside understanding the different impact that cybercrime has on gender. The regional workshop for **Asia** recognized that gender-sensitive policies and practices on cybercrime are vital to address the vulnerabilities of female victims and ensure an effective and balanced criminal justice response.

  - Support to setting up /developing models for domestic and regional interagency cooperation in the investigation of online fraud. The regional workshop for **Africa** substantiated that the establishment of domestic interagency mechanisms for information sharing, identification of common crime typologies and the development of procedures for investigating online fraud schemes are crucial to level up the fight against online scams, which remain the main form of cybercrime in the African region.

  - Transnational collaboration as an effective response to sophistication of cybercrime and modus-operandi of cybercriminals. The regional workshop for the **Americas** highlighted challenges faced by judicial authorities, public prosecutors and law enforcement agents at the time of applying domestic legislation in situations that cross borders, e.g. online fraud and cryptocurrencies. Although legal differences exist in relation to the criminalisation of offenses, jurisdiction, domestic proceedings and operational responses; complementarities and opportunities can be explored by using transnational cooperation mechanisms, cross-border collaboration, harmonization of laws and joint investigative efforts to combat cybercrime more effectively.

Octopus 2025 was the 15th Conference on Cybercrime of its kind. The bottom line and overall message remain the same:

COOPERATE!

The Octopus Conference is part of the Octopus Project of the Council of Europe which is currently funded by voluntary contributions from Canada, France, Hungary, Iceland, Italy, Japan, Malta, Netherlands, UK and US

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

www.coe.int/cybercrime