Version 15 Dec 2023

Some 500 cybercrime experts from about 100 countries – including from public sector but also international and private sector organisations, civil society organisations and academia – participated in the Octopus Conference on Cybercrime, held in Bucharest, Romania, from 13 to 15 December 2023.

A special session focused on ten years of capacity building by the Cybercrime Programme Office of the Council of Europe (C-PROC) which was addressed by Bjørn Berge (Deputy Secretary General of the Council of Europe) and Traian Hristea (State Secretary, Ministry of Foreign Affairs, Romania). Two plenary sessions, 14 workshops, three project events and a series of inspiring lightning talks underlined the following:

- Cyberattacks, cybercrime, impunity for crime online, dis-/misinformation, hate crime and hate speech and other cyberthreats contribute to current international crises such as wars, conflicts and insecurity; violations of international law; injustice and human rights violations; or authoritarianism and democratic back-sliding. Therefore, more cooperation, human rights and justice, accountability and effective criminal justice responses are needed.

- The participants in the Octopus Conference 2023 are all experts in their fields and are prepared to cooperate with each other; their actions will make a difference.

- They can rely on the Convention on Cybercrime (Budapest Convention) – supplemented by its first Protocol on xenophobia and racism and its Second Protocol on electronic evidence, 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) in Bucharest – that provides them with a dynamic and lasting framework.

- This framework continues to attract the interest of countries from all regions of the world as reflected in the accession to the Convention by Cameroon during the Octopus Conference, or the recent invitations to accede to Kazakhstan, Kiribati, Republic of Korea, Rwanda, São Tomé and Príncipe, Sierra Leone and Uruguay.

- Its impact is also reflected in the continuing global trend towards more alignment of the domestic legislation of countries with the Convention on Cybercrime. By December 2023, more than 130 States had broadly aligned their substantive criminal law with the provisions of this treaty.

- Criminal justice measures to counter cybercrime must meet human rights and rule of law requirements. It is of concern, therefore, 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.

- The experience of the war of aggression by the Russian Federation against Ukraine underlines that electronic evidence and the use of open-source intelligence are also needed to ensure accountability for war crimes and gross-violations of human rights. The Convention and its Second Protocol provide important tools in this

respect, but these need to be accompanied by substantial capacity building activities.

- Criminal justice authorities should make more use of tools provided in the Convention and its Protocols. One of these is Article 26 on "spontaneous information" which is particularly useful for the sharing of valuable information that may assist the authorities of another country in a criminal investigation.

- Use of the 24/7 network of contact point of the Convention has been rising rapidly in the recent past. Once the Second Protocol on e-evidence is in force, contact points will have additional responsibilities, in particular with respect to the disclosure of evidence in emergency situations. There is much demand for further capacity building in this respect by new and future Parties to the Convention.

- Offences related to ransomware remains a primary challenge. The tools of the Budapest Convention but also mechanisms such as the Counter Ransomware Initiative permit joint actions to counter these threats. Given the close links between ransomware and the use of virtual currencies, synergies between cybercrime and financial investigations need to be strengthened; more capacity building on the confiscation of virtual currencies that are crime proceeds, is essential.

- In order to permit more effective criminal justice action against ransomware, critical infrastructure attacks and other threats, cooperation and sharing of information and experience between criminal justice authorities and institutions responsible for cybersecurity, in particular Computer Incident Response Teams (CSIRTs), must be further improved, including through cybersecurity policies but also capacity building.

- Offenders and criminal organisations utilize crypto-mixer services, "cybercrime as a Service" or bulletproof hosting services to avoid detection, preserve anonymity, access advanced malicious tools and operate globally. In response, criminal justice authorities should enhance their capabilities for attribution, financial investigations and cooperation at all levels. They should make use of legal and technical tools that are available to access data, obtain evidence and bring offenders to justice.

- Artificial intelligence – in particular Generative AI – provides new opportunities for cybercrime but also for effective ways to detect crime, analyse vast amount of data or manage criminal proceedings. With the forthcoming Framework Convention on Artificial Intelligence of the Council of Europe and the Artificial Intelligence Act of the European Union there may soon be a basis to explore challenges and solutions that are specific to cybercrime and criminal justice, such as the definition of AI-related offences, the use of AI in the investigation of crime, and the collection of evidence and its use in criminal proceedings, or international cooperation with the use of AI.

- Online child sexual exploitation and abuse (OCSEA) remains one of the most severe criminal threats in cyberspace. OCSEA materials tend to remain available in cyberspace for years. The automated detection of OCSEA materials by multi-national service providers has been highly effective and provides large amounts of leads for criminal investigations. Reconciling such methods with human rights and rule of law requirements is challenging. Progress is being made towards the development of legal frameworks with procedural safeguards. Further cooperation between service providers and criminal justice authorities is needed for effective notice and take down and removal of materials to prevent their proliferation and re-victimisation of children.

- While the Convention on Cybercrime comprises a limited list of criminal offences, its effectiveness is enhanced through synergies with treaties such as the Lanzarote Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, the Istanbul Convention on Violence against Women and Domestic Violence or the Convention on Trafficking in Human Beings of the Council of Europe. Crime prevention, protection of victims/witnesses, and action against cyberviolence are further areas for joint responses.

- The Octopus Conference 2023 considered global challenges and solutions but also provided a platform to address issues that are of common regional interest, such as the implementation of cybercrime law in small jurisdictions of the South Pacific, data protection and

criminal justice action in Asia, interagency cooperation on cybercrime and e-evidence in Latin America and the Caribbean, or the use of the Budapest Convention and its Second Protocol for international cooperation by African countries.

- Capacity building remains one of the most effective means to address the challenges of cybercrime and electronic evidence. This has been demonstrated by C-PROC. Created in October 2013 under an agreement between the Government of Romania and the Council of Europe, and operational as from April 2014, C-PROC has since supported more than 140 countries through over 2000 activities. Numerous examples are available of activities as "game changers" that have made a real difference. Partnerships with multiple other organisations have been crucial for their scope and impact. The closing events of the CyberEast, CyberSouth, GLACY+ and iPROCEEDS-2 joint projects of the Council of Europe and the European Union, that were held during the Octopus Conference, confirmed the achievements of these projects.

- The "Strategic Priorities for the cooperation against Cybercrime in the Eastern Partnership Region", adopted during the Conference at the CyberEast project event by Armenia, Azerbaijan, Georgia, Moldova and Ukraine will provide guidance to action on cybercrime in this region.

- C-PROC projects have been joint projects with the European Union or projects funded by voluntary contributions, including recently by the United States, the United Kingdom and Japan. This also permitted the organization of the Octopus Conference 2023. Given growing membership in the Budapest Convention and increasing demand for support, more resources will be needed to continue the strengthening of a global criminal justice response to the challenges of cybercrime and e-evidence that meets human rights and rule of law requirements.

Octopus 2023 was the 14th edition of this conference. The bottom line of Octopus 2023 is similar to previous ones: