Octopus Conference 2023

Iolanda VASILE
The Romanian Association for Information Security Assurance

The Council of Europe organised the Octopus Conference on 13-15 December 2023. The Octopus Conference is part of the Octopus Project, funded by voluntary contributions from Canada, Hungary, Iceland, Italy, Japan, Netherlands, the UK and the USA.

The 2023 edition concentrated on:

• Utilising available tools for securing and sharing electronic evidence.

• Reviewing the impact and prospects of a decade of the Cybercrime Programme Office (C-PROC) in capacity building on cybercrime and electronic evidence.

Key messages of the Octopus Conference 2023:

• Cyber-attacks, cybercrime, disinformation, and online hate contribute to global issues like wars, law violations, and rights abuses. Addressing these requires more cooperation, a focus on human rights and justice, accountability, and better criminal justice responses.

• Digital threats such as cyber-attacks and online hate contribute to global crises, including conflict and human rights violations. Collaborative efforts emphasizing human

rights, justice, and accountability are needed to combat these issues, alongside enhanced criminal justice approaches.

• Experts in cybercrime can utilize the Budapest Convention and its Protocols on xenophobia, racism, and electronic evidence to align national laws with international standards. Over 130 states had done so by December 2023.

• It's crucial that anti-cybercrime measures honor human rights and the rule of law. Some nations' disinformation laws may inadvertently restrict free speech and not comply with human rights standards. These laws must be legal, necessary, and proportionate.

• Authorities should better leverage the Budapest Convention, particularly Article 26's "spontaneous information" for sharing investigative data. The growing use of the Convention's 24/7 contact network, especially with the new e-evidence Protocol, calls for increased capacity building.

• Ransomware poses a persistent threat. Collaboration through the Budapest Convention and the Counter Ransomware Initiative is vital, as is the synergy between cybercrime and financial investigations to manage virtual currency-related crime.

• Combating cyber threats like ransomware requires improved collaboration and data sharing between justice authorities and cybersecurity entities, including incident response teams, which can be bolstered by stronger cybersecurity policies and training.

• Criminals utilize services like crypto-mixers and bulletproof hosting to evade detection. Justice authorities must improve their tracing, financial investigation, and international cooperation capabilities, using existing tools for data access and evidence gathering.

• Artificial Intelligence, including Generative AI, introduces new cybercrime risks and detection methods. The Council of Europe's forthcoming AI convention and the EU's AI Act will provide frameworks to address AI's impact on cybercrime, including defining AI crimes, using AI in investigations, and enhancing international cooperation.

• Online child sexual exploitation and abuse (OCSEA) remains a dire problem, with harmful content remaining accessible for extended periods. Although automated detection is useful, it must respect human rights. Legal improvements and better coordination between service providers and law enforcement are crucial to eradicating such material and safeguarding children.

Held every 12 to 18 months by the Council of Europe, the Octopus Conference constitutes one of the biggest and finest platforms of exchange in cybercrime, gathering experts from more than 100 countries, international organisations, the private sector and academia.