Octopus Conference 2019

Cooperation against Cybercrime

20-22 November 2019

Palais de l'Europe, Council of Europe, Strasbourg, France

Version 22 November 2019

Key messages

Some 470 cybercrime experts from more than 115 countries – including from public sector but also international and private sector organisations, civil society organisations and academia – met at the Council of Europe in Strasbourg, France, from 20 to 22 November 2019 for the Octopus 2019 Conference on cooperation against cybercrime. The Conference was opened by the Secretary General of the Council of Europe and ministers and other senior officials from Costa Rica, France, Gambia, Ghana and Japan.

Key messages resulting from Octopus 2019 are:

- The Budapest Convention with currently 64 Parties, eight countries that have signed it or been invited to accede and several accession requests in process, is likely to remain the most relevant international legally binding agreement in the years to come whatever happens in other fora. It has provided guidance to the domestic legislation of some 150 countries worldwide. It is backed up by assessments and follow up by the Cybercrime Convention Committee and capacity building programmes, and it is being adapted to new challenges through guidance notes and protocols. This is difficult to replicate.

- Interference with elections through malicious cyber activities against computers and data used in elections and election campaigns undermines free, fair and clean elections and trust in democracy. Disinformation operations, as experienced in particular since 2016, may have the same effect. Measures to counter such threats may in turn create risks to other core values such as the freedom of expression. Therefore, it is important to ensure competencies and awareness of all stakeholders throughout the electoral process. International instruments as well as national legislation which includes clear criminal justice responses should be strengthened. It is crucial to counteract new threats and vulnerabilities through cooperation between all stakeholders, including private sector and public institutions. These measures, together, should allow voters to make an informed decision, freely cast their votes as well as ensure reliable election results and public trust.

- The need for urgent international cooperation, including with the private sector, is particularly obvious in emergency situations such as the recent terrorist attacks in Christchurch in New Zealand and the Easter attacks in Sri Lanka. Procedures for immediate response such as proposed in the "Christchurch Call" are available. The provisions for cooperation in emergency situations under consideration in the future Protocol to the Budapest Convention would strengthen the legal basis for such cooperation.

- The protection of children against online sexual exploitation and abuse requires integrated responses and cooperation between multiple stakeholders. Victims need to be identified and supported to make a full recovery and offenders need to be investigated and prosecuted. To this end, definitions and legislation need to be harmonised across jurisdictions. In this respect the Lanzarote and Budapest Conventions of the Council of Europe provide a blueprint of what is required. Cooperation at national and international level needs to be strengthened. Raising awareness among all sectors of society by engaging with children and other stakeholders is necessary to effectively prevent and combat such crime.

- These challenges confirm that the criminal justice response must be made more effective. If only a minuscule share of cybercrime is reported and results in a conclusive criminal justice outcome, competencies will further shift from the criminal justice arena with rule of law safeguards to the national security arena with more limited protections of individual rights.

- The future Protocol to the Budapest Convention on Cybercrime on enhanced international cooperation and access to electronic evidence in the cloud is designed to ensure more effective investigations and prosecutions and international cooperation on cybercrime and electronic evidence. Effectiveness and efficiency need to be reconciled with human rights and rule of law protections and consider the impact on the private sector as underlined by stakeholders during consultations on draft provisions of the Protocol.

- Procedures for criminal investigations need to consider the rights to privacy and the protection of personal data. Often the goals of criminal justice and of data protection are seen as contradictory with the latter considered an obstacle to effective criminal investigations. Examples include lack of access to WHOIS data, court decisions on data retention or the treatment of dynamic Internet Protocol addresses needed to identify subscribers suspected of criminal offences. Further dialogue is needed so that the goals of an effective criminal justice response and the protection of privacy and personal data are achieved. The modernised data protection Convention 108+ of the Council of Europe represents an international framework in this respect that is open for accession by any country.

- Cooperation and information sharing at all levels must be improved. While measures for cybersecurity and the criminal justice response to cybercrime are linked, information sharing between cybersecurity actors, such as Computer Security Incident Response Teams (CSIRTs), and criminal justice authorities remain limited. Cooperation should be enhanced through: accepted taxonomies defining the terms of cyber incidents and cybercrime; clear legal frameworks and operational agreements defining the scope of action for cybersecurity actors and law enforcement; common safeguards and guarantees applicable to both communities recognising the differences in scope and action; inter-agency, public-private and international cooperation in preventing, handling and post-event analyses of cyberattacks (including attacks on critical information infrastructure); and focused capacity building efforts to link cybersecurity and cybercrime communities supporting cooperation in the operational process.

- 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 required. Capacity building is most effective if the organisations to be supported have clearly defined objectives such as adoption of

legislation in line with the Budapest Convention or international cooperation on the basis of this treaty. Capacity building efforts such as those of the Cybercrime Programme Office of the Council of Europe (C-PROC) must be multiplied.

Octopus 2019 was the 12th Conference on Cybercrime of its kind. The bottom line and overall message remain the same:

COOPERATE!

The Octopus Conference is part of the Cybercrime@Octopus project which is funded by voluntary contributions from Estonia, Hungary, Japan, Monaco, Netherlands, Romania, Slovakia, United Kingdom and the USA

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

www.coe.int/cybercrime