Octopus Conference 2016
Cooperation against Cybercrime

16 – 18 November 2016

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

Version 20 November 2016

Key messages

Some 300 cybercrime experts from 90 countries, 12 international and 40 private sector, civil society organisations and academia met at the Council of Europe in Strasbourg, France, from 16 to 18 November 2016 for the Octopus 2016 Conference on cooperation against cybercrime. The Conference was opened by Thorbjørn Jagland, Secretary General of the Council of Europe, and commenced with a special session on the occasion of the 15th anniversary of the Budapest Convention on Cybercrime. Andorra deposited the instrument of ratification of the Convention during this session to become the 50th Party to this treaty.

Key messages resulting from Octopus 2016 are:

- Increasing cybercrime, attacks against critical infrastructure, fraud, hate speech and terrorist misuse of information technologies are considered major threats. Cloud computing and encryption enhance the complexity of the challenge. The capacity of criminal justice authorities to counter such threats and to ensure the rule of law remains limited. At the same time, mass surveillance, control of online content and restrictions to the freedom of speech also raise concerns. The prevention and control of cybercrime and other forms of crime online must meet human rights and rule of law, including data protection requirements. The debate on encryption is a reflection of a dilemma that is sometimes difficult to resolve. Article 15 of the Budapest Convention on conditions and safeguards remains more important than ever.

- The Budapest Convention, 15 years on, remains the most relevant international agreement on cybercrime and electronic evidence not only as a guideline for domestic legislation and as a basis for international cooperation, but also a catalyst for capacity building and a framework for multi-stakeholder cooperation as demonstrated by this Octopus Conference. By addressing issues such as access to evidence in the cloud, it will remain relevant in the years to come. States are encouraged to accede to the Budapest Convention and its Protocol on Xenophobia and Racism as well as the data protection 108 of the Council of Europe.

- Access to evidence on servers in the cloud, that is, in foreign, unknown, shifting or multiple jurisdictions for criminal justice purposes is necessary for governments to meet their obligation of protecting society and individuals against crime. Voluntary cooperation by multi-national service providers – in the disclosure of subscriber information and in emergency situations also of other data – is most valuable but also raises concerns. The draft Guidance Note on Production Orders for Subscriber Information (Article 18 Budapest Convention) should help put such cooperation on a clearer legal basis. Measures such as an online tool on provider policies and on powers for production orders in Parties to the Budapest Convention, regular meetings of major providers with the Cybercrime Convention Committee and participation by providers in capacity building activities should facilitate cooperation in practice. A common procedure and platform for all requests to major providers should be given consideration. At the same time, a Protocol to the Budapest

Convention is considered necessary. The proposals made by the Cloud Evidence Group of the Cybercrime Convention Committee have received broad support during the Conference.

- Capacity building remains one of the most effective ways to help societies address the challenges of cybercrime and electronic evidence. Practical examples demonstrate the feasibility of this approach. Ingredients for success include designing programmes in support of holistic processes of change with political commitment as a prerequisite, commencing projects with a detailed situation and needs analysis, embedding training within training institutions to ensure sustainability, and involving the private sector in capacity building projects. Closer cooperation between organisations offering assistance would result in more effective use of resources and more sustainable impact.

- Legislation

  - In the Asia/Pacific region, reforms of legislation on cybercrime and electronic evidence have accelerated, often with the Budapest Convention serving as a guideline to ensure compatibility with international standards. Where legal reforms are accompanied by capacity building efforts – for example with the support of Japan, South Korea, UNODC or the Council of Europe – criminal investigations, prosecutions and adjudication of cases of cybercrime and other offences involving electronic evidence increase.

  - In Africa, several countries have moved ahead with reforms of domestic legislation, often using the Budapest Convention as a guideline. At the same time, more than half of African countries do not yet have the necessary legislation in place. Countries with draft laws should advance and complete their reforms, including rule of law safeguards to law enforcement powers. The Malabo Convention of the African Union reflects a clear political commitment by African leaders with regard to cybersecurity, data protection and cybercrime, but would need to be backed up by the Budapest Convention for operational criminal justice measures and international cooperation in practice. Reform of legislation needs to be followed by capacity building.

  - In Latin America, many countries have reformed their substantive criminal law using the Budapest Convention as a guideline, while specific procedural law provisions on cybercrime and electronic evidence remain a challenge. Given the similarity of the procedural law of countries of Latin America, many countries may move ahead in a similar way to deal with electronic evidence.

- Terrorist misuse of information technology, such as cyberattacks against computer systems, including critical infrastructure, their use for logistical purposes, including the planning of terrorist attacks or the dissemination – often via social media - of illegal contents, including terrorist threats, promotion of or incitement to terrorism, recruitment or training, xenophobia, racism or other forms of hate speech contributing to violent extremism, radicalisation and terrorism, is a serious threat. At the same time, countering terrorist misuse of ICT raises concerns regarding the freedom of expression, right to private life and other human rights. Strengthening criminal justice capacities, counter-narrative, and public/private and international cooperation as well as full implementation of international agreements are important elements of the solution. Encryption protects privacy but also represents one of the main obstacles for criminal investigations. Practical solutions with appropriate safeguards need to be found.

- Proceeds-generating crime online is increasing considerably. Follow-the-money approaches should also be pursued with regard to crime online. Good practices include closer inter-agency cooperation between financial intelligence and financial investigation units on the one hand and cybercrime units on the other. Tasks forces with banks, Internet service providers, Computer Security Incidents Response Teams and Internet industry for sharing

malware and threat intelligence will help prevent attacks at an early stage. Training of the judiciary and other capacity building are needed.

- Rendering international cooperation more efficient is essential. Follow up should be given to the Recommendations adopted by the Cybercrime Convention Committee in December 2014. Full use should be made of mechanisms such as 24/7 networks of the G7, INTERPOL and the Council of Europe, or of EUROJUST or of instruments such as the European Investigation Order. Practical proposals for a more effective role of 24/7 points of contact are available and should be implemented. Annual meetings of 24/7 points of contact should be organised. Procedures for requests for data in emergency situations via mutual legal assistance should be established.

- Cooperation between different organisations and initiatives towards the common goal of preventing and controlling cybercrime is improving steadily as the benefits of such cooperation become more obvious. Online tools and databases made available by organisations facilitate cooperation and enable governments to identify needs, establish baselines and measure progress. Efforts to generate synergies between organisations will need to continue.

Octopus 2016 was the 10th Conference on Cybercrime of its kind. The bottom line and overall message remains the same:

COOPERATE!

The Octopus Conference is part of the Cybercrime@Octopus project which is funded by voluntary contributions from Estonia, Japan, Monaco, Romania, United Kingdom, USA and Microsoft. Estonia, Japan and USA have made funding specifically available for the Octopus conference.

www.coe.int/cybercrime

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Programme overview

WED, 16 NOVEMBER			
Plenary session	*Hemicycle*		
9h00	Special Session: BUDAPEST CONVENTION – 15th ANNIVERSARY *(English/French/Russian/Spanish)*		
Workshop sessions	*Room1 (E/F/S/R)*	*Room 2 (E/F)*	*Room 3 (E)*
14h30	Workshop 1: ► Capacity building on cybercrime: good practices, success stories and lessons learnt	Workshop 2: ► Legislation on cybercrime and capacity building in the Asia/Pacific region	Workshop 3: ► Service provider/law enforcement cooperation on cybercrime and electronic evidence
20h00 Social dinner in an Alsatian restaurant			
THU, 17 NOVEMBER			
Workshop sessions	*Room1 (E/F/S/R)*	*Room 2 (E/S/F)*	*Room 3 (E)*
9h30	Workshop 4: ► Terrorism and information technology: the criminal justice perspective	Workshop 5: ► Legislation on cybercrime and electronic evidence in - Africa - Latin America	Workshop 6: ► International cooperation: workshop for 24/7 points of contact and MLA authorities
Workshop sessions	*Room1 (E/F/S/R)*	*Room 2 (E/F)*	*Room 3 (E)*
14h30	Workshop 7: ► Seeking synergies: Initiatives of international and private sector organisations	Workshop 8: ► Targeting proceeds from crime online	Workshop 9: ► Crime and jurisdiction in cyberspace: access to electronic evidence
FRI, 18 NOVEMBER			
Plenary session	*Room 1 (E/F/S/R)*		
9h30	Plenary: ► Results of workshops ► Human rights and rule of law in cyberspace: threats and safeguards ► Conclusions		
13h00	*End of conference*		