Cooperation against Cybercrime

Octopus Conference 2021

16 -18 November 2021 – Online

Version 18 Nov 2021

Key messages

About 1200 cybercrime experts from some 120 countries – including from public sector but also international and private sector organisations, civil society organisations and academia – participated in the Octopus Conference on Cybercrime from 16 to 18 November 2021. The conference took place online on account of the Covid-19 pandemic.

The conference commenced on 16 November with a special event on the occasion of the 20th anniversary of the Budapest Convention on Cybercrime and on the forthcoming Second Additional Protocol to the Convention on enhanced cooperation and disclosure of electronic evidence. It was opened by the Minister of Interior of Hungary on behalf of the Hungarian Chairmanship of the Committee of Ministers of the Council of Europe, and by the Secretary General of the Council of Europe. Interventions by ministers, prosecutors general and other senior officials from all regions of the world confirmed the global impact and benefits of the Convention and the need for the new Protocol.

Participants welcomed the formal adoption of the Second Additional Protocol on the following day by the Committee of Ministers of the Council of Europe and that it will be opened for signature in Spring 2022.

The special event on 16 November and the fourteen workshops, two rounds of lightning talks and three outlook sessions underlined, inter alia, that:

- Cybercrime – that is, offences against and by means of computer systems – has evolved into a significant threat to fundamental rights, democracy and the rule of law, as well as to international peace and stability, and has major social and economic impact. Ransomware attacks are currently considered the priority threat and are paralysing government and private sector organisations, including hospitals and other critical infrastructure and businesses of sizes; and they are causing risks to the life of people. Democratic processes, including elections, continue to be at risk of cyber-attacks and interference. The Covid-19 pandemic is accompanied by increasing cybercrime, exploiting the reliance of individuals, businesses and organisations on information technology. Cybercrime offenders exploit this reliance, social engineering, such as phishing, and other techniques to commit crime and to launder crime proceeds; and they are increasingly organised making use of crime-as-a-service. At the same time, the ability of the criminal justice system to respond to this surge in crime is limited by Covid-19 related restrictions. The online sexual exploitation and sexual abuse of children is exacerbated by the pandemic in the form of increased child sexual abuse materials, online grooming, online abuse communities, online risk taking by minors and live streaming of abuse. The problem of attribution of cybercrime and of providing an effective criminal justice response is further compounded where offenders are supported by government authorities.

- The idea that cybercrime affects individuals insignificantly "is a myth". On the contrary, cybercrime often represents a serious interference with the rights and lives of victims. Governments have the obligation to make the means available to protect individuals against crime, including through more effective criminal justice measures. States need to take additional measures for better protecting and supporting victims of cybercrime, for example, through regular victimisation surveys, more specialised support to victims, concrete responses to harm such as restorative justice or more opportunities for reporting online crime.

- At the same time, more research should be undertaken to come to a better understanding and a typology of offenders. Given that an important share of cybercriminals are young adults or even minors, crime prevention measures should be strengthened to prevent them from becoming offenders.

- Tools for a more effective criminal justice response are available and should be made use of:

  - Globally, the majority of States have adopted legal frameworks providing in their criminal law for offences against and by means of computers, for powers to investigate and prosecute cybercrime and to secure electronic evidence, and for international cooperation on the basis of the Budapest Convention on Cybercrime.

  - Tools and good practices area also available to counter and investigate ransomware attacks, trace, search and seize crime proceeds in the form of cryptocurrencies, detect and report child sexual abuse materials or make use of artificial intelligence for the detection, analysis or investigation of crime online.

  - The authorities of many countries are benefiting from capacity building programmes and are increasingly equipped to investigate, prosecute and adjudicate cybercrime and other cases involving electronic evidence and to cooperate internationally.

  - Public/private cooperation and partnerships are essential and many initiatives and good practices are now available and can be made use of.

  - The new Second Additional Protocol to the Convention on Cybercrime will provide additional tools for cooperation and the disclosure of electronic evidence. These include direct cooperation with service providers across borders to obtain information needed to identify offenders, as well as means for expedited cooperation in emergency situations.

- Reconciling the effectiveness of measures for the investigation of crime with human rights and rule of law, including data protection safeguards is challenging. The automated detection of child sexual abuse materials is one example. On the other hand, the new Protocol to the Budapest Convention illustrates how efficient means to obtain electronic evidence also across borders can be accompanied by an effective system of safeguards.

- Looking into the future,

  - all stakeholders are encouraged to make best possible use of the tools, initiatives and programmes that are available and create further synergies to address the challenges of cybercrime and electronic evidence;

  - States are, therefore, also encouraged to join the Budapest Convention (if they have not yet done so) and to sign the Second Additional once it will be opened for signature in Spring 2022;

  - at the same time, as new challenges will emerge, the search for additional solutions will need to continue, for example in relation to artificial intelligence or cryptocurrencies.

Octopus 2021 was the 13th edition of this conference. The bottom line of all the previous ones had been a call to "cooperate". The one for Octopus 2021 is the same but includes a supplement:

COOPERATE, THE TOOLS ARE THERE!