

CENTRAL FORENSIC LABORATORY OF THE POLICE

<https://clkp.policja.pl/cfl/news/174605,CYBER-CRIME-THREATS-AND-TRENDS-CEPOL-TRAINING.html>
2020-09-26, 21:22

„CYBER CRIME THREATS AND TRENDS” CEPOL TRAINING

Publication date 12.03.2019

The training, with the participation of the representatives of law enforcement agencies and institutions established to fight cybercrime, took place in the headquarters of CEPOL in Budapest (Hungary) on 19–22 March 2019. Among over 40 participants were representatives of Belgium, the Czech Republic, Finland, France, Spain, Ireland, Germany, Portugal and Italy. Poland was represented by the officers from the Central Forensic Laboratory of the Police and Central Investigation Bureau.

The key European organizations, institutions and initiatives related to combating the most modern forms of cybercrime (EUROPOL, IOCTA and SOCTA, ENISA, EUROJUST) were presented during the training. The discussed subjects included cooperation with the private sector (i.e. financial institutions and network service providers), legal solutions which support combating cross-border computer crime (including MLA - Mutual Legal Assistance and EIO - European Investigation Order). The attention was also paid to the international cooperation as well as education and exchange of experience. On the first day, a general picture of the challenges posed by the latest cyber threats was outlined, such as darkweb and its underground forums devoted to i.e. cryptocurrencies, pedophilia, terrorism or malware. The concept of IT specialization of organized crime towards CaS (Crime-as-a-Service) and the idea of J-CAT (Joint Cybercrime Action Taksforce) were presented. The second day was devoted mainly to the subject of financial (cyber)crime (cryptocurrencies, skimming, money laundering). ENISA (European Union Agency for Network and Information Security) was also presented as the coordinating body for the activities of CSIRT (Computer Security Incident Response Team), law enforcement agencies and courts. The last day of the training was dedicated to the case study on obtaining financial benefits from CSAM (Child Sexual Abuse Materials), OSINT tool and issues related to the security of government and institutional information systems in the face of cyber threats. The training ended with a practical task aiming at the development of a report on a terrorist attack based on OSINT tools. The obtained information will be forwarded during scientific events organized by the CFLP as well as during meetings with experts and certified specialists of the Police forensic laboratories, which will allow for even better performance of activities commissioned to IT examination units.