Cybercrime Digest

Bi-weekly update and global outlook by the
Cybercrime Programme Office of the Council of Europe (C-PROC)

16 – 30 November 2021

Source: EUReporter

Date: 17 Nov 2021

Security and justice in the digital world: Marking 20 years of international co-operation under the Budapest Convention on Cybercrime

"Home Affairs Commissioner Ylva Johansson has delivered a video message at the opening of the Council of Europe's 'Octopus' conference on the fight against cybercrime. The event marks the 20th anniversary of the Budapest Convention, which lies at the heart of a global alliance against Cybercrime. 66 countries are party to the Convention. It has been signed by all EU Member States. The Budapest Convention is the foundation for of anti-cybercrime legislation in 80% of countries worldwide. A Second Additional Protocol to the Convention, concerning enhanced cooperation and disclosure of electronic evidence, is expected to be approved by the Council of Ministers of the Council of Europe tomorrow. [...] The Commission negotiated the Protocol on behalf of the European Union." READ MORE

Source: Microsoft Blog

Date: 16 Nov 2021

Cooperating against cybercrime: 20 years on from the Budapest Convention

"[…] As a company, we are strongly committed to safeguarding users' privacy, security, and safety, and their fundamental rights, as outlined in our Trusted Cloud Principles. To honor this commitment, Microsoft has partnered with the Council of Europe's Global Project on Cybercrime since 2006. In 2013, we expanded our work with an agreement to bolster our efforts in assisting countries' implementation of the Budapest Convention. Since then, our engagement with the Council of Europe has evolved to include other areas related to the rule of law and human rights through the Partnership with Digital Companies program. […] We believe a rapid adoption of the e-evidence proposal, a swift ratification of the 2nd Additional Protocol and a robust EU-U.S. law enforcement agreement will establish a lasting solution with respect to data access for law enforcement purposes through modern and principled bilateral and multilateral agreements. The Budapest Convention clearly demonstrates that these efforts can be pursued in an environment where countries respect each other's national sovereignty, as well as the fundamental rights and liberties of all citizens." READ MORE

Source: Euractiv

Date: 17 Nov 2021

Council of Europe adopts additional protocol to tackle cybercrime

"Ministers at the Council of Europe […] adopted the second Additional Protocol to the Budapest Convention on Wednesday (17 November) to tackle the current surge in cybercrime. The Budapest Convention, which turned 20 on Tuesday, is the first and one of the most important international treaties on cybercrime and is ensuring a common criminal policy approach and fostering international cooperation. The Second Additional Protocol is modernising the Convention to make it ready for the challenges of the 21st century. […] Among the 66 states that have currently ratified the Budapest Convention are not only most of the EU member states, but also countries from other continents, including the United States, Chile, Ghana, or

Japan, thus making it a global standard for the fight against cybercrime." READ MORE

Source: European Commission

Date: 25 Nov 2021

Security and justice in the digital world: Commission proposals for ratification of new international instrument to improve cooperation on access to electronic evidence

"Today, the Commission adopted two proposals to authorise EU Member States to sign and to ratify the Second Additional Protocol to the Council of Europe Budapest Convention on Cybercrime. This Protocol will improve access to electronic evidence necessary for criminal investigations and strengthen law enforcement and judicial authorities' capacity to fight against cybercrime. […] The Protocol also includes strong safeguards to protect fundamental rights, including the right to privacy and the right to the protection of personal data. [...] The Budapest Convention lies at the heart of a global alliance against cybercrime and has been signed by all EU Member States. It is the foundation of anti-cybercrime legislation in 80% of countries worldwide."

European Commission, Proposal for a COUNCIL DECISION authorising Member States to sign, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, 25 November 2021

European Commission, Proposal for a COUNCIL DECISION authorising Member States to ratify, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, 25 November 2021

Source: Eurojust

Date: 24 Nov 2021

Cross-border access to electronic evidence: update and impact of the pandemic on data requests

"Europol, Eurojust and the European Judicial Network publish today the third annual edition of the SIRIUS European Union Digital Evidence Situation Report. This year, the report goes beyond a comprehensive status update by including an assessment of the impact of the COVID-19 pandemic on the access of EU authorities to electronic evidence held by foreign-based online service providers (OSPs) in 2020. Cross-border access to digital evidence is crucial to most investigations, and it became even more relevant during the pandemic, when there was an acceleration in the digitalization of everyday life. In one case mentioned in the report, for instance, law enforcement officers had to react quickly to prevent phishing scams for digital signatures – a crime area on the rise because of the pandemic." READ MORE

Source: Europol

Date: 24 Nov 2021

Germany, the UK and Europol target violent jihadist websites

"A total of 50 websites dedicated to the distribution of online terrorist propaganda and promoting violent jihadist ideology were targeted over the course of a referral action that took place in the last week of October. The European Union Internet Referral Unit (EU IRU) at Europol's European Counter Terrorism Centre (ECTC) coordinated the referral activity, which involved law enforcement authorities from Germany and the United Kingdom. […]Out of 50 websites, including sites

supporting the so-called Islamic State and al-Qaeda terrorist organisations and their affiliates, 21 were suspended following referrals to the relevant OSP." READ MORE

Source: Interpol

Date: 26 Nov 2021

More than 1,000 arrests and USD 27 million intercepted in massive financial crime crackdown

"An operation coordinated by INTERPOL codenamed HAECHI-II saw police arrest more than 1,000 individuals and intercept a total of nearly USD 27 million of illicit funds, underlining the global threat of cyber-enabled financial crime. Taking place over four months from June to September 2021, Operation HAECHI-II brought together specialized police units from 20 countries, as well as from Hong Kong and Macao, to target specific types of online fraud, such as romance scams, investment fraud and money laundering associated with illegal online gambling. […] The following countries participated in Operation HAECHI-II: Angola, Brunei, Cambodia, Colombia, China, India, Indonesia, Ireland, Japan, Korea (Rep. of), Laos, Malaysia, Maldives, Philippines, Romania, Singapore, Slovenia, Spain, Thailand, and Vietnam." READ MORE

Source: Europol

Date: 29 Nov 2021

12 online fraudsters arrested in global operation against counterfeiters

"From 1 May 2021 until 14 November 2021, Operation In Our Sites took place leading to the arrest of 12 suspects, the seizure of €2.6 million worth of counterfeit goods and cash to the value of €460 468. The joint international operation involved law enforcement authorities from 30 countries and was supported by Europol's Intellectual Property Crime Coordinated Coalition (IPC3), Eurojust and INTERPOL. IPC3 is co-funded by EUIPO (European Union Intellectual Property Office) to combat intellectual property crime. The operation specifically targeted websites that offer counterfeit goods and are involved in online piracy." READ MORE

Source: Interpol

Date: 24 Nov 2021

INTERPOL General Assembly resolution calls for increased safeguards against online child sexual exploitation

"INTERPOL's General Assembly has adopted a resolution addressing the challenges faced by law enforcement investigating cases of online child sexual exploitation and abuse. Through the resolution, member countries expressed their concern at the increased use of end-to-end encryption (E2EE) to conceal illicit online crimes against children such as grooming, live streaming of sexual abuse and the distribution of child sexual abuse material." READ MORE

Source: Sierra Leone News

Date: 17 Nov 2021

Sierra Leone: President Bio signs Cybersecurity and Crime Bill into law

"[…] The law will help reform Sierra Leone's criminal justice system in many ways. The powers and procedures in the new law will address unauthorised access to protected systems, unauthorised data interception or interference, computer-related forgery, identity theft and impersonation," Attorney General and Minister of Justice, Anthony Brewah noted. […] Minister Swaray further disclosed that the new law would strengthen the country's capacity to apply legislation on cybercrime in a fulfilled commitment to the Malabo and ECOWAS convention on cybercrime,

the EU and Budapest convention, all of which guaranteed human rights, privacy, and freedom of speech." READ MORE

Source: Council of Europe

Date: 24 Nov 2021

C-PROC: 2021 Annual Meeting of the 24/7 Network of Contact Points of the Budapest Convention on Cybercrime

"The Council of Europe through its Cybercrime Programme Office in Bucharest (C-PROC) supports the functioning of the 24/7 Network established according to Article 35 of the Budapest Convention and facilitates capacity building support to the new members or countries interested to join the Network, on the establishment of contact points and their role and responsibilities. […] This year, the meeting was attended by more than 70 representatives of the 24/7 contact points of 45 Parties and Observers to the Budapest Convention who exchanged views and best practices on the role and responsibilities of the Network." READ MORE

Source: UNICEF

Date: 18 Nov 2021

Uganda to develop a National Action Plan on online child sexual abuse and exploitation

"Uganda will be the first country to develop a National Child Protection Action Plan that will implement recommendations from a recent study that found disturbing evidence of online child sexual exploitation and abuse in the country. The Commissioner for Children and Youth in the Ministry of Gender, Labour and Social Development, Fred Ngabirano, announced the plans during the launch of the 'Disrupting Harm' report at Protea Hotel in Kampala on 16 November 2021.'' READ MORE

Source: Council of Europe

Date: 25 Nov 2021

CyberSouth: Training of Trainers on cybercrime and e-evidence for magistrates in Tunisia

"CyberSouth project delivered the first Judicial Training of Trainers (ToT) on cybercrime and electronic evidence for judges and prosecutors of Tunisia on 22, 23 and 25 of November 2021. The ToT course is part of the objective on mainstreaming the judicial training on cybercrime and e-evidence in the priority countries and aimes at increasing the knowledge and skills of the Tunisian magistrates on the training methodologies, the role of trainer, training matrix, online learning – challenges and solutions. […] The gained competences will enable the Tunisian trainers to instruct and equip their peers with the skills and knowledge required for investigating and prosecuting cybercrime." READ MORE

Source: krebsonsecurity.com

Date: 22 Nov 2021

Arrest in 'Ransom Your Employer' Email Scheme

"In August, KrebsOnSecurity warned that scammers were contacting people and asking them to unleash ransomware inside their employer's network, in exchange for a percentage of any ransom amount paid by the victim company. This week, authorities in Nigeria arrested a suspect in connection with the scheme — a young man who said he was trying to save up money to help fund a new social network. […] the majority of the cybercrime that originates from Africa — think romance scams, Business Email Compromise (BEC) fraud, and unemployment/pandemic loan fraud — does not target Nigerian citizens, nor does it harm African banks. On the contrary: This activity pumps a great deal of Western money into Nigeria.'' READ MORE

Source: Council of Europe

Date: Nov 2021

CyberEast supports Law Enforcement in the Eastern Partnership in the Europol's Training and Operational Partnership Against Organised Crime (TOPCOP)

"The Darkweb is becoming increasingly a place where illegal activity thrives and criminals function in perceived anonymity. Reportedly, almost 30% of hidden services on Tor relate to some form of illicit activity, such as selling illicit drugs, weapons, compromised data, counterfeit documents, pharmaceuticals, chemicals and other illicit products. […] During 08-12 November and 22-26 November 2021 respectively, corresponding courses were delivered by TOPCOP project to a group of law enforcement officers from Armenia, Georgia and Azerbaijan, to which CyberEast project have contributed by experts' input on matters related to cybercrime and Darkweb." READ MORE

Source: BankInfoSecurity

Date: 25 Nov 2021

Ukraine's Secret Service Busts 5 Alleged 'Phoenix' Hackers

The Secret Service of Ukraine has arrested five Ukrainian citizens on suspicion of being members of an international hacking group called Phoenix. All have been charged with targeting hundreds of victims over the past two years, including accessing their mobile devices, stealing personal data and selling hacking as a service to others, the SSU says." READ MORE

Source: Inquirer.net

Date: 18 Nov 2021

Philippines: Bank clients lose over P1 billion to cybercrime

"The Bankers Association of the Philippines (BAP) estimated that more than P1 billion worth of hard-earned money has gone down the drain so far this year due to fraud, including unauthorized bank withdrawals and fund transfers, as cybercriminals more aggressively prowled the digital space as locked-down consumers shifted to digital channels. The industry-wide loss was based on data gathered by the BAP from reports filed by fraud victims, said BAP cybersecurity committee vice chair Ramon Jocson, who is also executive vice president of Bank of the Philippine Islands. [...]The BAP signed on Wednesday a memorandum of understanding with the Kapisanan ng mga Brodkaster ng Pilipinas (KBP) to enlist local broadcasters in the war against cybercriminals." READ MORE

Source: The Hacker News

Date: 17 Nov 2021

U.S., U.K. and Australia Warn of Iranian Hackers Exploiting Microsoft, Fortinet Flaws

"Cybersecurity agencies from Australia, the U.K., and the U.S. on Wednesday released a joint advisory warning of active exploitation of Fortinet and Microsoft Exchange ProxyShell vulnerabilities by Iranian state-sponsored actors to gain initial access to vulnerable systems for follow-on activities, including data exfiltration and ransomware. […] The agencies did not attribute the activities to a specific advanced persistent threat (APT) actor. Targeted victims include Australian organizations and a wide range of entities across multiple U.S. critical infrastructure sectors, such as transportation and healthcare" READ MORE

Source: HackReaD

Date: 23 Nov 2021

Brazil: WiFi software management firm exposed millions of users' data

"Brazil-based WiFi management software firm WSpot exposed extensive details of high-profile firms and millions of customers. WSpot provides software to let businesses secure their on-premise WiFi networks and offer password-free online access to their clients. Some of the notable clients of WSpot include Sicredi, Pizza Hut, and Unimed. [...]Around 226,000 files got exposed in this data leak. The leaked information included personal details of at least 2.5 million users who connected to WSpot's client's public WiFi networks." READ MORE

Source: BleepingComputer

Date: 29 Nov 2021

Telegram channel admins who sold fake vaccine cards arrested

"The Italian financial crime agency (Guardia di Finanza – GdF) has announced the arrest of several individuals suspected of managing Telegram channels to promote fake vaccine certificates, aka 'Green Passes.' The operation was supported by evidence collected by investigators at Group-IB's high-tech crime unit, who managed to unmask the criminals despite measures to keep their identities hidden. [...] The actors operated at least 35 Telegram channels that had a combined audience of 100,000 users, promising "authentic" and valid vaccination certificates for €100 ($113)." READ MORE

Latest reports

- Council of Europe, Council of Europe Office on Cybercrime in Bucharest: C-PROC activity report for the period October 2020 – September 2021, 15 November 2021
- Council of Europe, List of the activities of the Cybercrime Programme Office (October 2020 – September 2021), 15 November 2021
- UK Government, Digital Imaging and Multimedia Procedure v3.0, 16 November 2021
- Council of Europe, Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, 17 November 2021
- YOU Tell, 30 statistiques qui montrent que la cybercriminalité s'est banalisée, 17 November 2021
- Press Afrik, Les dégâts de la cybercriminalité sur l'économie africaine, 18 November 2021
- GURU99, 15 BEST Computer (Digital) Forensic Tools & Software in 2021, 19 November 2021
- Eurojust, SIRIUS EU Digital Evidence Situation Report, 24 November 2021
- Cornell University, COVID-19 vaccination certificates in the Darkweb, 25 November 2021
- ENISA, Railway Cybersecurity - Good Practices in Cyber Risk Management, 25 November 2021
- Electronic Frontier Foundation, Coalition Against Stalkerware Celebrates Two Years of Work to Keep Technology Safe for All, 25 Nov 2021
- National Cyber Security Center, Weekly Threat Report, 26 November 2021
- Kaspersky, Cyberthreats to financial organizations in 2022, 23 November 2021
- ENISA, Raising Awareness of Cybersecurity, 29 Nov 2021
- LCL Banque et assurance, Baromètre Fraude et Cybercriminalité 2021, 29 Nov 2021
- El Derecho, Geolocalización y derechos fundamentals, 29 November 2021
- Eurojust, European Judicial Cybercrime Network Newsletter, Issue 3, 30 November 2021
- The Daily Californian, Human Rights Study shows increasing violations of freedom of online expression in Gulf Nations, 30 Nov 2021
- Cybereason, Ransomware Attackers Don't Take Holidays, November 2021
- Grand Thornton Ireland, The Economic Cost of Cybercrime, November 2021

Upcoming events

- 29 November-2 December, C-PROC/JORDAN, (*in-person*), Training of Trainers workshop on cybercrime and e-evidence for Jordanian magistrates, CyberSouth
- 30 November-2 December, C-PROC/CARICOM IMPACS, (*online*), Regional Trainings in the Caribbean region on cybercrime investigations for law enforcement and security practitioners, OCTOPUS
- 2-3 December, C-PROC/ALBANIA (*hybrid*), Regional meeting with all project countries/area with recommendations for more efficient and swift MLA procedures and integration of provisions of Second Additional Protocol to the Budapest Convention, iPROCEEDS-2
- 3 December, C-PROC/BARBADOS, (*online*), Advisory mission on cybercrime legislation - follow-up meeting, OCTOPUS
- 3 December, C-PROC/NAURU, (*online*), Advisory mission on OCSEA legislation - first de-briefing meeting, OCTOPUS

- 3 December, C-PROC/ALBANIA, (*hybrid*), Forth meeting of the Project Steering Committee, iPROCEEDS-2
- 6-7 December, C-PROC, (*online*), Third meeting of the expert group on the FRA-CoE Handbook on Cybercrime and Fundamental Rights, GLACY+
- 6-8 December, T-CY/C-PROC, (*online*), SIRIUS Conference 2021: E-evidence Across Borders organised by EUROJUST, T-CY, OCTOPUS
- 6-8 December, C-PROC/ALBANIA, (*in-person*), Coordination meeting on promoting the unique online platform for blocking access of websites with illegal and harmful content, iPROCEEDS-2
- 7 December, C-PROC/ KOSOVO*, (*online*), Best online reporting platforms presented by developing and implementing authorities. Making an informed decision on the future reporting system in Kosovo*, iPROCEEDS-2
- 7 December, C-PROC/IAP, (*online*), Series of webinars on the 2nd Additional Protocol: Party request of expedited production of subscriber information and traffic data, OCTOPUS, GLACY+
- 7 December, T-CY/C-PROC, (*online*), Institut des Hautes Etudes en défense nationale (IHEDN) Webinar on Digital sovereignity and cybersecurity, T-CY, OCTOPUS
- 7 December, C-PROC, (*online*), Second Roundtable on COVID-19 and cybercrime in Asia, OCTOPUS
- 7-9 December, C-PROC/ARMENIA, *(online),* Joint training of law enforcement and judiciary in cooperation with judicial and police academies, CyberEast
- 8 December, C-PROC/PGA, (*online*), Series of regional webinars to promote universality and implementation of the Budapest Convention on Cybercrime, OCTOPUS, GLACY+
- 9 December, C-PROC, (*online),* Seventh meeting of the Project Steering Committee, CyberSouth
- 13 December, C-PROC/NAURU, (*online*), Advisory mission on legislation, GLACY+
- 13-17 December, C-PROC/ASIA&PACIFIC region, (*online*), Cyber-enabled fraud training, GLACY+
- 14 December, C-PROC, (*online*), Advisory mission on cybercrime and electronic evidence legislation for Nauru - second de-briefing meeting, OCTOPUS, GLACY+
- 14 December, C-PROC/MEDITERRANEAN region, (*online*), Workshop on Data protection and cybercrime and electronic evidence, GLACY+
- 14-16 December, C-PROC/PANAMA, (*hybrid*), Advisory workshop on the streamlining of procedures for MLA enhanced by the 2nd Additional Protocol related to cybercrime and electronic evidence combined with Specialized course on international cooperation, GLACY+
- 15 December, C-PROC, (*online*), Second Regional Workshop on the promotion of the Second Additional Protocol to the Budapest Convention, CyberSouth

Due to the COVID-19 pandemic outbreak and the countermeasures applied by most of the countries worldwide, in-country activities of the C-PROC capacity building initiatives foreseen in the month of December have been rescheduled to a later date.

The Cybercrime Digest appears bi-weekly. The news is selected by relevance to the current areas of interest to C-PROC and does not represent official positions of the Council of Europe. You receive this digest as you have taken part in Council of Europe activities on cybercrime. It is not intended for general publication.

For any additional information, contributions, subscriptions or removal from this distribution list, please contact: cybercrime@coe.int

www.coe.int/cybercrime

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE