Cybercrime Digest

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

01 – 15 April 2021

Source: Council of Europe

Date: 14 Apr 2021

Towards a Protocol to the Convention on Cybercrime: additional stakeholder consultation

"The Cybercrime Convention Committee (T-CY) invites interested stakeholders to submit written comments on the draft 2nd Additional Protocol to the Budapest Convention by 2 May 2021 and/or to participate in an online meeting on 6 May 2021. While stakeholders previously submitted contributions or participated in discussions on individual articles, the first complete draft of the Protocol is now available, including the chapter on safeguards. Some sections of the Explanatory Report are still under preparation.[…] The provisions of this Protocol will be of operational and policy benefit and will ensure that the Budapest Convention continues to stand for a free Internet where governments meet their obligation to protect individuals and their rights in cyberspace." READ MORE

Source: Council of Europe

Date: 09 Apr 2021

C-PROC marks its seventh anniversary: online briefing with the diplomatic community in Bucharest

"This year, the Council of Europe's Cybercrime Programme Office (C-PROC) based in Bucharest, Romania celebrates its seventh anniversary. The Bucharest Office became operational in April 2014 and is responsible for assisting countries worldwide in strengthening their criminal justice capacities to respond to the challenges of cybercrime and electronic evidence on the basis of the standards of the Budapest Convention on Cybercrime." READ MORE

Source: EU CYBER DIRECT

Date: 12 Apr 2021

Paths for multi-stakeholder engagement in the fight against cybercrime

"The fight against cybercrime cannot be siloed. On a national, regional and international level, the meaningful and sustained collaboration of governments, the private sector, experts and civil society organisations is the only way to mitigate and control the challenges cybercrime poses to an open and secure cyberspace. In May 2021, a new UN process starts, mandated with working towards a possible comprehensive international convention on countering the use of information and communications technologies (ICTs) for criminal purposes. The modalities for this process, including the role of civil society, are yet to be decided." READ MORE

RELATED ARTICLE:

CHATHAM HOUSE, Paths for multi-stakeholder engagement in the fight against cybercrime, 14 April 2021

Source: European Commission

Date: 14 Apr 2021

EU Strategy to tackle Organised Crime & EU Strategy on combatting Trafficking in Human Beings: Questions and Answers

"Despite progress made by Member States over the years in this area, the threat posed by organised crime groups remains high as they are constantly adjusting their 'modi operandi', using new technologies and seizing opportunities to make illicit profits. […] The Strategy sets out actions to develop technological solutions and training activities to improve the tools and skills for law enforcement to conduct investigations in the digital world." READ MORE

RELATED ARTICLE:

EUROPOL, European Union Serious and Organised Crime Threat Assessment, 12 April 2021

Source: ENISA

Date: 08 Apr 2021

EU Cybersecurity Market: New Ad Hoc Working Group open for applications!

"The ENISA Ad Hoc Working Group (AHWG) on the EU cybersecurity market will support ENISA in analysing market trends and segments, with a focus on cybersecurity solutions to meet the market needs of the stakeholders. While the focus will be on the EU cybersecurity market, the global cybersecurity market may also be considered, for example when addressing the EU dependency (on) or requirements to market actors outside the Digital Single Market. READ MORE

Source: Australian Strategic Policy Institute

Date: 01 Apr 2021

The intersection of cybercrime and terrorist activity

"Terrorists have been using the 'darknet' in the same way as they have been using the surface web—to recruit, radicalise and influence, as well as to finance and coordinate attacks. Since 2015, there has been a significant increase in the use of Telegram (an encrypted instant messaging platform) by terrorist actors. Telegram has become the preferred online platform for Islamic State supporters to distribute propaganda, coordinate and communicate, replacing social media applications such as Twitter and Facebook. Telegram was used to coordinate attacks inspired or directed by IS in Paris, Brussels (2016), Berlin (2016) and Istanbul (2017)." READ MORE

Source: Les Echos

Date: 12 Apr 2021

La cybercriminalité, principal risque pour l'économie

"L'an dernier, de nombreuses agences gouvernementales américaines ont été l'objet d'attaques et les regards se sont portés vers la Russie, soupçonnée d'avoir orchestré cette vague sans précédent. Jusqu'ici, la Fed a réussi à limiter les dégâts mais la paralysie de son système provoquerait un chaos sur les marchés et pour les entreprises américaines. Lorsque son système de paiement, par lequel transitent 3.000 milliards de dollars tous les jours, a été victime d'une panne pendant quatre heures, en février, des milliers d'entreprises ont vu certaines transactions retardées." READ MORE

Source: Deutsche Welle

Date: 04 Apr 2021

Facebook data on millions of user accounts leaked online in latest breach, 04 April 2021

"Data from hundreds of millions of Facebook users was leaked online on Saturday, including personal information such as phone numbers, full names, and email addresses. The leaked data from 533 million users in 106 countries was posted on an obscure hacking forum. The data is believed to be more than a year old, but security experts say the information could still be used by criminals to commit identity fraud." READ MORE

RELATED ARTICLES:

The Record, Phone numbers for 533 million Facebook users leaked on hacking forum, 4 Apr 2021

Computer Weekly, Egypt, Italy and US most affected in Facebook leak, 9 Apr 2021

Source: Europol

Date: 07 Apr 2021

Dark Web Hitman Identified Through Crypto-Analysis

"Europol supported the Italian Postal and Communication Police (Polizia Postale e delle Comunicazioni) in arresting an Italian national suspected of hiring a hitman on the dark web. The hitman, hired through an internet assassination website hosted on the TOR network, was payed about €10 000 worth in Bitcoins to kill the ex-girlfriend of the suspect." READ MORE

Source: Council of Europe

Date: 20 Apr 2021

International Network of National Judicial Trainers: First coordination call of the Steering Committee

"The Steering Committee will aim on its first meeting to reach further coordination on the overall strategy and advance the necessary efforts to ensure the implementation of the workplan of the Network. Focus points from at least 15 countries (Algeria, Cape Verde, Chile, Costa Rica, Dominican Republic, Georgia, Ghana, Jordan, Lebanon, Morocco, Paraguay, Philippines, Senegal, Tunisia and Ukraine) confirmed their participation. It is expected that the Steering Committee will meet quarterly, starting with the first quarter of 2021." READ MORE

Source: Council of Europe

Date: 31 Mar – 01 Apr 2021

CyberSouth and GLACY+: Workshop on the functioning and role of 24/7 Networks of Contact Points

"During 31 March – 1 April 2021, the CyberSouth and GLACY+ projects organised a Workshop on the functioning and role of 24/7 Networks of Contact Points in the international cooperation on cybercrime and e-evidence, together with INTERPOL. Approximately 170 participants, representing criminal justice authorities (investigators, prosecutors, judges and representatives from the central authority of mutual legal assistance) from the priority countries of the C-PROC's GLACY+, CyberSouth, CyberEast, and iPROCEEDS-2 projects attended this workshop." READ MORE

Source: Council of Europe

Date: Jan- Apr 2021

iPROCEEDS-2: Second round of business analyses CERT- LEA. Guidelines on sharing of data by CERTs with criminal justice authorities

"In the landscape of growing threat of cybercrime further exacerbated by COVID-19 pandemic, Computer Security Incident/Emergency Response Teams (CSIRTs/CERTs/) play an important role in preventing cyber-attacks and overall coordinate responses at national level. […] It is therefore essential that CERTs and criminal justice authorities put in place an efficient and effective collaboration mechanism, where roles, responsibilities and segregation of duties are defined and agreed upon." READ MORE

Source: INTERPOL

Date: 14 Apr 2021

INTERPOL-Brazil: Two arrested in global hunt to catch child predators

"SALGUEIRO, BRAZIL: A Brazilian Federal Police operation last Sunday (11 April) in the Northwestern states of Pernambuco and Piauí has resulted in the rescue of a five-year-old victim of sexual abuse and the arrest of the alleged perpetrators. In August 2020, disturbing footage of a young child being sexually abused by two adults, male and female, was uploaded to INTERPOL's ICSE database by the US-based National Center for Missing and Exploited Children. The ICSE database uses image and video comparison software to help investigators worldwide in the daunting task of identifying the victims, abusers and places that appear in such materials" READ MORE

Source: Ecuador 221

Date: 07 Apr 2021

Ecuador: Asamblea Nacional promueve legislación para sancionar la violencia sexual digital

"La Asamblea Nacional tramitó en primer debate el proyecto de Ley Orgánica Reformatoria del Código Orgánico Integral Penal y de la Ley Orgánica Integral para Prevenir y Erradicar la Violencia contra las Mujeres, para Prevenir y Sancionar la Violencia Sexual Digital, recogiendo el informe de la Comisión de Justicia. Esta propuesta es el resultado de la unificación de dos proyectos: de reformas al Código Penal para Tipificar los Delitos de Sexting y Hostigamiento; y para Prevenir la Violencia, el Acoso Digital y la Violación a la Intimidad, de autoría de los legisladores Franklin Samaniego y Mae Montaño, respectivamente." READ MORE

Source: Inforpress

Date: 01 Apr 2021

Cabo Verde adere a rede de combate ao cibercrime gerida pelos EUA

"[...] Cabo Verde, que já é um Estado Membro da Convenção de Budapeste sobre cibercrime, no âmbito da qual mantém um Ponto de Contacto 24/7, na PGR, passou a ter, em matéria de cibercriminalidade, mais um canal expedito de comunicação com outros Estados, em especial os que ainda não fazem parte da Convenção de Budapeste", refere o comunicado.
O Ministério Público acrescentou ainda que por essa via o País pode solicitar preservações expeditas de dados para subsequentes pedidos de Assistência Jurídica Mútua (MLA, na sigla em inglês)." READ MORE

Source: Asamblea Legislativa de la República de Salvador

Date: 13 Apr 2021

El Salvador: Buscan actualizar legislación para perseguir delitos informáticos

"De acuerdo a lo planteado por los expertos en la materia, esta legislación debe de actualizarse para permitir la persecución de delitos que se cometen desde las diferentes plataformas de las tecnologías de la información y la comunicación; […] Además, los legisladores urgieron en la necesidad de que el país se adhiera al Convenio de Budapest sobre ciberdelincuencia, ya que este es el primer tratado internacional que busca combatir los delitos informáticos y los delitos en Internet mediante la armonización de leyes entre naciones, la mejora de las técnicas de investigación y el aumento de la cooperación." READ MORE

Source: ABC News

Date: 13 Apr 2021

Australia: Ransomware attack to blame for Federal Group's casino pokies outage in Tasmania

"Tasmania's lone casino operator has confirmed it is being held to ransom in a cyber attack that has impacted its pokies machines and hotel bookings system for more than a week. […] Multiple former IT employees at Federal Group told the ABC they believed historic credit card details stored in the hotel booking system could have been compromised, as well as the electronic gaming systems at both casinos." READ MORE

Latest reports

- Europol, EU SOCTA 2021, 12 April 2021
- ENISA, Report on the European Cybersecurity Month campaign of 2020, 15 April 2021
- UNODC, Compilation of all preliminary conclusions and recommendations suggested by Member States during the meetings of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in 2018, 2019 and 2020, 08 April 2021
- FBI, 2020 Internet Crime Report, 09 April 2021
- Philippines - Senate, Rules on Electronic Evidence, 11 April 2021
- Trilateral Research, Better visualisation of electronic evidence to improve digital forensic capabilities, 01 April 2021
- Portail de l'IE, La cyber dissuasion, une solution imparfaite pour un cyberespace plus sûr, 9 April 2021
- Threat Research HP, Nation States, Cyberconflict and the Web of Profit, April 2021
- McAfee, Threats Report: April 2021
- Bit Defender, 2020 Consumer Threat Landscape Report, April 2021
- Secure List, Financial Cyberthreats in 2020, 31 Mar 2021
- Kaspersk, Brazil: América Latina é uma das principais criadoras de ameaças financeiras, 06 April 2021

Upcoming events

- 16 April, C-PROC/INTERPOL, (on-line), Series of GLACY+ & INTERPOL webinars on encryption in Spanish, GLACY+
- 15 - 16 April, C-PROC/UKRAINE, (on-line), Workshop with personal data protection authorities and national communications regulators on trust and cooperation, CyberEast
- 19 April, C-PROC, Desk Study, New materials for the Training Skills and Certification Programme for Council of Europe Trainers on Cybercrime and Electronic Evidence, GLACY+
- 19 - 20 April, C-PROC/MALDIVES, (on-line), Advisory mission on legislation, GLACY+
- 20 April, C-PROC, (on-line), First Coordination of the Steering Committee of the International Network of the Judicial Training, GLACY+
- 20 - 21 April (TBC), C-PROC/FIJI, (on-line), Stakeholder webinar on new cybercrime legislation and accession to Budapest Convention, GLACY+
- 20 - 21 April, C-PROC/GUYANA, (on-line), Workshop on Criminal Justice Capacities on Cybercrime and Electronic Evidence and accession to the Budapest Convention, Octopus project in cooperation with CARICOM IMPACS
- 20 - 22 April, C-PROC/NORTH MACEDONIA, (on-line), Specialised Judicial Training Course on International Cooperation, iPROCEEDS-2
- 23 April, C-PROC/AZERBAIJAN, (on-line), Workshop with Azerbaijani authorities on the reform of criminal procedure legislation, CyberEast
- 26 April, C-PROC, (on-line), Regional Workshop on judicial international cooperation and police-to-police cooperation in cybercrime and electronic evidence, CyberSouth
- 26 - 28 April, C-PROC, (on-line), Second Regional Meeting on development of mutual legal assistance guidelines (with Eurojust), CyberEast

- 26 - 28 April, C-PROC/ BOSNIA AND HERZEGOVINA, (on-line), Specialised Judicial Training Course on International Cooperation, iPROCEEDS-2
- 27 - 29 April (TBC), C-PROC/COTE D'IVOIRE, (on-line), Advisory mission on legislation, GLACY+
- 28 April (TBC), C-PROC/ARGENTINA, Support to the establishment of a regional training center on cybercrime and electronic evidence and a certification programmes for criminal justice authorities in Latin America, GLACY+
- 29 April, C-PROC, (on-line), Series of monthly thematic webinars for the International Network of the National Judicial Trainers (4/7), GLACY+
- By 30 April, C-PROC, Desk study, Guide for first responders to cybercrime investigations, CyberSouth
- By 30 April, C-PROC/Children's Rights Division, Consolidation and revision of the translations in 11 languages of the lesson plans, presentations and chapters of the introductory training module to build the capacities of law enforcement, prosecutors and judges on online child sexual exploitation and abuse (OCSEA), EndOCSEA@Europe.
- By 30 April, C-PROC, Desk Study, Preparation of Country Profiles on Online Child Sexual Exploitation and Abuse for Botswana, Mauritius, Nigeria, Ghana, Kenya, Octopus project in cooperation with EndOCSEA@Europe project
- By 30 April, C-PROC, Translation of the Guide on Seizing Cryptocurrencies into French, Spanish and Portuguese, Octopus project
- By 30 April, C-PROC, Desk Study, New materials for the Advanced Judicial Course on Cybercrime and Electronic Evidence, GLACY+
- By 30 April, C-PROC/Children's Rights Division, Layout of 12 language translations of the awareness material (booklet and Parental advice) 'Kiko and the Manymes' for the project countries, EndOCSEA@Europe

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 April have been rescheduled to a later date.

The Cybercrime Digest appears bi-weekly. News are selected by relevance to the current areas of interest to C-PROC and do 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