Cybercrime Digest

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

1-15 June 2020

Source: Council of Europe

Date: 15 Jun 2020

C-PROC series of cybercrime webinars continue: materials available, next topics and dates announced

The C-PROC series of webinars on cybercrime have continued in the first half of June with two more sessions, respectively dedicated to *Election interference: attacks on critical information systems*, conducted in the framework of the CyberEast Project on 4 June, *Cybercrime and Terrorism: The criminal justice response*, co-organized by the UN Office of Counter-Terrorism and the Council of Europe in the framework of the GLACY+ Project on 12 June. In addition, materials and recordings have been made available for recently concluded webinars on Online child sexual exploitation and abuse in times of the COVID-19 pandemic, held on 28 May, and CSIRTs and criminal justice authorities.

The appointment for the second half of June is dedicated to *Introduction to cyberviolence*, conducted in the framework of the CyberEast Project and scheduled on 18 June. For further updates, please check our webinars dedicated webpage.

Source: Council of Europe

Date: 16 Jun 2020

Cybercrime and criminal justice: EU-CoE webinars kick off with Asia-Pacific

"The European Union and the Council of Europe are launching a series of five online regional webinars on cybercrime and criminal justice in cyberspace, in preparation of the UN-level negotiation on a new treaty on 'countering the use of information and communications technologies for criminal purposes'. Co-organized in the framework of the GLACY+ joint project of the EU and the Council of Europe, the webinars are designed to provide a key opportunity for sharing challenges in the field, key principles and experience between the criminal justice practitioners – the beneficiaries of a future UN treaty on cybercrime, and foreign policy experts – who will be negotiating this treaty, in preparation for the work starting this fall." READ MORE

Source: Council of Europe

Date: 16 Jun 2020

Cybercrime in Africa and the challenges of international cooperation

"In the framework of the GLACY+ Project, the U.S. Department of Justice and the Council of Europe organized on 16 June 2020 an online workshop on the challenges of international cooperation on cybercrime and electronic evidence in the Africa region. Some 60 participants from twelve countries attended: Benin, Burkina Faso, Cabo Verde, Cote d'Ivoire, the Gambia, Ghana, Kenya, Liberia, Mauritius, Morocco, Nigeria, Senegal and Tunisia. […] The workshop focused on: (i) practical aspects and technical challenges of international investigations on dark web markets and relevant case studies; (ii) a review of INTERPOL's work in international cooperation, resources for investigations and COVID-19 related case studies; (iii) key lessons learned from representatives of Ghana and Nigeria, who showcased the approach adopted in the respective national contexts to facilitate international cooperation and streamline the use of the Budapest Convention; (iv) the tools that the Budapest Convention offers for international cooperation." READ MORE

Source: The Brussels Times

Date: 10 Jun 2020

EU steps up its response to disinformation around the pandemic

"To counter the disinformation, the Commission published on Wednesday (10 June) a joint communication to the other EU institutions: "Tackling COVID-19 disinformation – Getting the facts right". The communication analyses the immediate response and proposes concrete action that can be quickly set in motion. In a non-exhaustive list of examples, the communication lists different types of disinformation during the corona virus crisis, such as misleading healthcare information, conspiracy theories that may endanger human health and lead to public violence, Illegal hate speech blaming a particular ethnic or religious group for the spread of COVID-19, consumer fraud and cybercrime." READ MORE

Source: The Center for Internet and Society – India

Date: 8 Jun 2020

The debate over internet governance and cyber crimes: West vs the rest?

"A realistic analysis of the [Budapest] Convention would reveal that it is the best instrument at hand to deal with cyber crimes. The Convention, establishing common standards for its signatories, along with the Cybercrime Convention Committee (the "Committee") that oversees its implementation and Programme Office on Cyber Crime (the "C-PROC") dedicated towards capacity building, provides a dynamic framework for effectively tackling cybercrimes. The Committee ensures that the convention is adapted to address evolving crimes such as denial of service attacks and identity thefts, which did not exist at the time the convention was adopted, by issuing guidance notes and draft protocols. Similarly on the issue of procedural law, despite new developments such as cloud servers, the Committee is actively working on addressing the complicated challenges posed by it. It has proposed an additional protocol to specifically deal with access to evidence in the cloud by facilitating more efficient mutual legal assistance amongst the signatories and direct cooperation with service providers, while striking a balance between rule of law and human rights. […] A look at Russia's resolution and its draft cyber crime convention would indicate that it might not be the appropriate solution to the problem at hand. The resolution as well as the draft convention, which is supposed to serve as a framework for the treaty, are drafted without due regard for human rights concerns. A mere reference to human rights, requiring use of ICTs to be in compliance with human rights and fundamental freedoms, is insufficient to safeguard it while combating cyber crimes. […] In short, the resolution and the draft convention are proposing a Leviathan model vesting state with excessive control over the internet. In practice, it would bear resemblance to the "sovereign internet law" of Russia and the "Golden Shield Project" of China. Such models are widely criticized for eschewing democratic principles in the name of ensuring security of the state from cyber attacks. " READ MORE

Source: Europol

Date: 3 Jun 2020

Arrest in Spain for dissemination of jihadist terrorist propaganda via Internet

"On 3 June 2020, Europol supported the Spanish National Police (Policía Nacional) in arresting a man in Madrid on suspicion of radicalisation and for dissemination of jihadist terrorist propaganda via the internet. The individual's constant activity on social media where he glorified the so-called Islamic State (IS) attacks brought him to the attention of investigators. Whilst under surveillance, he showed a high level of radicalisation in his closed circle, and demonstrated a full adherence to the postulates of terrorist groups, fully justifying their violent actions." READ MORE

Source: Council of Europe

Date: June 2020

Legislative Development and Training Activities on Cybercrime in Ukraine

"The issue of combating cybercrime is one of the pressing challenges for Ukraine. The Law of Ukraine «On Ratification of the Cybercrime Convention» entered into force on July 1, 2006, but the criminal procedural legislation of Ukraine does not yet comply with the provisions of the Budapest Convention. This complicates the prosecution of criminals, public-private cooperation and international cooperation in our work to combat cybercrime. It is necessary to develop appropriate changes to the current Ukrainian legislation. On the initiative of the Chairperson of the Committee of the Verkhovna Rada of Ukraine on Law Enforcement, Denys Monastyrskyi, and with the support of the People's Deputies of Ukraine a working group was set up to develop amendments which will increase the effectiveness of pre-trial cybercrime investigations and the use of electronic evidence. As a result, amendments to the Criminal Procedure Code of Ukraine, the Criminal Code of Ukraine, the Laws of Ukraine "On Operative Activity" and "On Telecommunications" were elaborated, which will: enable law enforcement agencies to urgently retain information which will greatly increase the effectiveness of tracking and preventing cyberattacks (implementation of Article 16 of the Budapest Convention); enable to temporarily access to non-personal information provided by Internet service providers (ISPs) in exceptional cases of urgency without court decision (implementation of Article 17 of the Budapest Convention); gain legal access to computer systems that are physically located outside of the location of the search, to overcome logical protection systems, to obtain information about the peculiarities of the functioning of the computer systems and the security measures applied to them (implementation of Article 19 of the Budapest Convention); improve the public-private cooperation between law enforcement agencies and ISP during pre-trial investigations." READ MORE

Source: Council of Europe

Date: June 2020

The Work of the New Department for Investigation of Cybercrimes and High Technology Crimes (DICHTC) within the Investigative Committee of Armenia

"The DICHTC's activity is highly comprehensive, with several main directions of activity. One of them is investigation of cybercrimes and high-tech crimes, including theft (fraud) and other financial crimes committed with the use of Internet and computer systems. The plan is that, after certain retraining, the investigators will be highly specialized. Also, through our Department support to all subdivisions of the Investigative Committee is offered for the examination of computer systems, implemented through the laboratory of the Department. We also provide international cooperation to obtain electronic evidence on criminal cases investigated by all subdivisions of the Committee (including through sending and receiving inquiries to the competent authorities and ISPs of other states, seeking at the same time to improve and develop the cooperation between state and private sectors), as well as training, retraining and training of trainers (ToTs) of relevant investigators of the Committee on cybercrime cases and how to obtain electronic evidence. We also prepare methodological guidelines and examination methodology, and implement activities related to the development of legislative reforms, legal and normative-legal acts. Our colleagues also work on organizing and implementing activities on prevention of cybercrime and high-tech crimes on cyber hygiene. Within each of the mentioned directions, our new Department has concrete and tangible progress and results – at the same time, there is still a lot to do." READ MORE

Source: Motherboard

Date: 10 Jun 2020

Facebook Helped the FBI Hack a Child Predator

"For years, a California man systematically harassed and terrorized young girls using chat apps, email, and Facebook. He extorted them for their nude pictures and videos, and threatened to kill and rape them. He also sent graphic and specific threats to carry out mass shootings and bombings at the girls' schools if they didn't send him sexually explicit photos and videos. Buster Hernandez, who was known as "Brian Kil" online, was such a persistent threat and was so adept at hiding his real identity that Facebook took the unprecedented step of helping the FBI hack him to gather evidence that led to his arrest and conviction, Motherboard has learned. Facebook worked with a third-party company to develop the exploit and did not directly hand the exploit to the FBI; it is unclear whether the FBI even knew that Facebook was involved in developing the exploit. According to sources within the company, this is the first and only time Facebook has ever helped law enforcement hack a target." READ MORE

Source: El Pais

Date: 15 Jun 2020

Un curso online de ciberseguridad de la Policía se convierte en un inesperado éxito sin precedentes

"Todo empezó con un tuit de la cuenta de la Policía a sus 3,4 millones de seguidores el pasado miércoles: "Comienza la inscripción para #C1b3rWallAcademy. El curso es gratuito y dirigido a toda aquella persona que quiera formarse en ciberseguridad", decía. En 24 horas había 10.000 inscritos. Solo tres días después, el pasado domingo, esa cifra se había doblado hasta más 20.000, que llegaban desde 62 países. [...] El C1b3rWall Academy es la primera edición de un curso online abierto masivo (conocidos por sus siglas en inglés, MOOC) sobre ciberseguridad organizado por la Policía española, junto a la Universidad Autónoma de Madrid y el grupo que reúne la formación en cibercrimen de las policías europeas (ECTEG). [...] La formación está pensada como una introducción a la ciberseguridad en 200 horas divididas en 15 módulos como "Principios de criptografía y esteganografía", "Análisis forense" o "Ciberinteligencia". Los ponentes son 130 y hay 38 comunidades profesionales de hackers que participarán, tanto españolas como del resto de Europa y toda América, con dos de Estados Unidos." READ MORE

Update 17 June – Registrations are closed, but materials and recorded sessions will remain freely available on the website of the course [Spanish version] [English version]

Source: Council of Europe

Date: 10 Jun 2020

GLACY+: Workshop for Maldivian authorities to raise awareness on the Budapest Convention

"An introductory workshop on cybercrime legislation for Maldivian criminal justice authorities was co-organized by the U.S. Department of Justice and the Council of Europe on 9 and 10 June 2020. The on-line seminar, organized in the framework of the GLACY+ Project, was intended to kick-off a triangular cooperation with national authorities, including the Maldives' Police Force and the Prosecutor General's Office, and the U.S. DoJ, aimed at aligning the Maldives' legal framework on cybercrime and electronic evidence with the Budapest Convention and at enhancing criminal justice capacities accordingly. Sessions included interventions from: the Sri Lanka ICT Agency, who was the leading force that guided the country to accede to the Budapest Convention in 2015 and showcased the journey undertaken to get to it; INTERPOL, who presented elements for a successful cybercrime investigations; the Council of Europe, who provided an overview of the substantive and procedural provisions covered by the Budapest Convention." READ MORE

Source: Ministerio de la Defensa Pública, Paraguay

Date: 2 Jun 2020

El Ministerio de la Defensa Pública participa en Revisión y taller en línea sobre legislación de delitos cibernéticos y evidencia electrónica en Paraguay

"El Ministerio de la Defensa Pública esta participando los días 1-2 de junio 2020, del Revisión y taller en línea sobre legislación de delitos cibernéticos y evidencia electrónica en Paraguay. […] El instrumento legal de referencia al que se hace referencia es el Convenio de Budapest, el único tratado internacional abierto sobre ciberdelito y prueba electrónica, y se brinda asistencia a los países que han solicitado la adhesión, o han sido invitados a adherirse, o acaban de acceder, en un esfuerzo conjunto con los gobiernos nacionales para fortalecer aún más las capacidades de las autoridades de justicia penal. Paraguay adhirió al Convenio de Budapest en julio de 2019 y ahora puede beneficiarse de estar en la lista de países respaldados por el Proyecto GLACY+." READ MORE

Source: All Africa

Date: 12 Jun 2020

South Africa: Committee Adopts Cybercrimes Bill

"The Select Committee on Security and Justice has adopted the Cybercrimes Bill, among several other pieces of legislation. The Cybercrimes Bill aims to create offences that have a bearing on cybercrime; criminalise the distribution of harmful data messages and to provide for interim protection orders; further regulate jurisdiction in respect of cybercrimes; further regulate the powers to investigate cybercrimes, and also further regulate aspects relating to mutual assistance in respect of the investigation of cybercrime. The bill provides for the establishment of a designated point of contact; further provides for the proof of certain facts by affidavit; imposes obligations to report cybercrimes; provides for capacity building, and provides that the executive may enter into agreements with foreign states to promote measures aimed at the detection, prevention, mitigation and investigation of cybercrimes […]." READ MORE

Source: Ghanaweb

Date: 14 Jun 2020

Ghana to serve on Global Internet Forum to Counter Terrorism advisory committee

"Ghana has been appointed as a member of the Independent Advisory Committee (IAC) of the Global Internet Forum to Counter Terrorism (GIFTC). […] A statement said the nomination was due to Ghana's political commitment and human right-centric approach to developing its cybersecurity as well as its active engagement at the regional and international levels to promote the responsible use of the internet. […] A statement said the nomination was due to Ghana's political commitment and human right-centric approach to developing its cybersecurity as well as its active engagement at the regional and international levels to promote the responsible use of the internet." READ MORE

Source: Bleeping Computer

Date: 3 Jun 2020

Ransomware gangs team up to form extortion cartel

"Ransomware gangs are teaming up to extort victims through a shared data leak platform, and the exchange of tactics and intelligence. In November 2019, the Maze Ransomware operators transformed ransomware attacks into data breaches after they released unencrypted data of a victim who refused to pay. Soon after, they launched a dedicated "Maze News" site used to shame their unpaid victims by publicly releasing stolen data. This extortion tactic was quickly adopted by other groups, which now includes thirteen active ransomware operations known to leak stolen data if not paid. The Maze gang is once again stirring up the threat landscape by creating a cartel of ransomware operations to share resources and extort their victims." READ MORE

Source: ProPakistani

Date: 4 Jun 2020

Pakistan, 189% increase in online harassment during coronavirus lockdown

"According to a recently published report by the Digital Rights Foundation (DRF), cyber harassment complaints in Pakistan have increased manifold (+189%) during the Coronavirus-induced lockdown. […] Sexual harassment, surveillance, unauthorized and non-consensual use and dissemination of personal data, and blackmailing and manipulation using personal information, images, and videos are some of the forms of complaints of online harassment reported by women during March and April. The report recommends the government to streamline the process of online complaint registration and initiate legal proceedings against the perpetrators at the earliest. To ensure public health and safety during case proceedings amid COVID-19 pandemic, the report recommends the government to turn to technology and adopt video-based testimony. It further suggests that law enforcement officials, prosecutors, and judges need to be sensitized to gendered risks that women and gender minorities face online. To achieve this goal, the report suggests the inclusion of cybercrime laws, internet governance, digital forensics, and digital rights into the curriculum of law enforcement officials and judges. Lastly, the report calls on Pakistan's government to ratify the Budapest Convention on Cybercrime for enhanced international cooperation and data sharing on cybercrime." READ MORE

Latest reports

- Council of Europe, Cybercrime and COVID19 webpage, updated weekly
- ENISA, Tips for secure user authentication, 04 Jun 2020
- ENISA, Spotlight on incident reporting of telecom security and trust services, 09 Jun 2020
- FBI, Increased Use of Mobile Banking Apps Could Lead to Exploitation, 10 Jun 2020
- Ministerio del Interior, Espana, Estudio sobre Cibercriminalidad de 2019, 8 Jun 2020
- Medianama, Lt Gen. (Dr) Rajesh Pant on India's National Cyber Security Strategy, Indo-US cooperation, end-to-end encryption and more, 2 Jun 2020
- Hacked, How to File a Police Report for Cybercrime, 07 Jun 2020
- NordVPN, Cyber Risk Index, 04 Jun 2020
- MalwareBytes, Cybercrime tactics and techniques - Q2 2020, 3 Jun 2020

Upcoming events

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 May have been rescheduled to a later date.

- 16 June, **Webinar** on *Cybercrime and International Cooperation in the Africa Region*, in collaboration with the U.S. Department of Justice, GLACY+
- 18 June – 10 July, C-PROC, Desk research: Assessment of compliance with substantive law provisions of Articles 2 to 12 of the Budapest Convention on Cybercrime and relevant EU standards, Bosnia and Herzegovina, iPROCEEDS-2
- 18 June – 10 July, C-PROC, Desk research: Assessment of compliance with substantive law provisions of Articles 2 to 12 of the Budapest Convention on Cybercrime and relevant EU standards, North Macedonia, iPROCEEDS-2
- 23 June, Desk Review of Cybercrime Legislation of Liberia, GLACY+

- 24 June, EU-CoE joint **webinar** on *Criminal Justice and Cybercrime in Cyberspace for the Asia-Pacific Region*, GLACY+
- 29 June - 3 July, Regional Training of Trainers for Gendarmerie of Francophone countries from Africa, GLACY+
- 30 June, Report on Cybercrime Statistics, in collaboration with INTERPOL, GLACY+
- 30 June, Report on Cybercrime in Africa – Policies and Legislation, International Cooperation, Capacity building (First African Forum), GLACY+