Cybercrime Digest

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

1-15 December 2018

Source: Council of Europe

Date: 3 Dec 2018

Ghana accedes to the Budapest Convention on Cybercrime

"The Republic of Ghana has deposited the instruments of accession to the Budapest Convention on Cybercrime on 3 December 2018. With Ghana's accession, the Convention on Cybercrime has now 62 states parties. A further 9 States have signed it or been invited to accede. Ghana is also one of the five African priority countries of the GLACY+ project, aimed at strengthening national criminal justice capacities to apply legislation on cybercrime and electronic evidence." READ MORE

RELATED ARTICLES

GhanaWeb, Government to set up Cyber Security Authority, 13 Dec 2018

Source: Council of Europe

Date: 11 Dec 2018

Romanian Presidency of the Council of the European Union in cooperation with the Council of Europe. Criminal Justice in Cyberspace

"Criminal justice is an important element of the response to cybercrime and other crime in cyberspace involving electronic evidence. While cyber threats and their impact are increasing and touching upon core values of societies in Europe and worldwide, criminal justice authorities are faced with complex challenges. At the same time, solutions are in place or are being developed. Examples are the E-evidence proposals at the European Union or the preparation of an additional Protocol to the Budapest Convention on Cybercrime at the Council of Europe. And both organisations have been supporting capacity building on cybercrime worldwide for many years. Under the Romanian Presidency of the Council of the European Union, a conference on "Criminal Justice in Cyberspace" will be organised by the Ministry of Justice of Romania in cooperation with the Council of Europe, on 25 - 27 February 2019, in Bucharest, Romania." READ MORE

Source: Council of Europe

Date: 5 Dec 2018

Towards a Protocol to the Budapest Convention: Further consultations

"Following consultations with data protection, civil society, industry and others, during the Cybercrime Convention Committee (T-CY) meeting from 29 November 2018, additional contributions are now sought. Stakeholders are invited to send written comments by 20 February 2019 on the provisional draft text on "emergency mutual assistance" and "languages of requests" (to be sent to cybercrime@coe.int). Provisional draft text of provisions: Language of requests; Emergency MLA available here".

RELATED ARTICLES

International Association of Privacy Professionals, Alexander SEGER on the new Protocol to the Convention on Cybercrime, 3 Dec 2018

Council of Europe, Report of the 3rd Meeting of the T-CY Protocol Drafting Plenary, 29 Nov 2018

Source: European Commission

Date: 11 Dec 2018

A Europe that Protects: Commission welcomes the adoption of stronger rules to stop cyber-criminals

"Today, the European Parliament and the Council reached political agreement on the Commission's proposal to strengthen rules to combat fraud and counterfeiting of non-cash means of payment – such as bank cards, cheques, mobile payments and virtual currencies. An important element of the EU's scaled up response to cybercrime, the new rules will help Member States to crack down on cyber-criminals while better assisting victims of online payment fraud. […] Fraud and counterfeiting of non-cash means of payment is an important source of income for organised crime, often enabling other criminal activities such as terrorism, drug trafficking and trafficking in human beings. The new rules will boost Member States' capacity to deter, prosecute and sanction cyber-criminals: (i) Expanded scope of offences; (ii) Harmonised rules on penalties; (iii) Stronger protection of victims; (iv) Greater cross-border cooperation; (v) Better reporting." READ MORE

Source: Council of Europe

Date: 13 Dec 2018

Cybercrime@EaP 2018: Regional Conference on Cybercrime Strategies and Closing Event of the Project

"These two events aimed to summarize the joint action of the European Union and the Council of Europe, performed through capacity building activities on cybercrime and electronic evidence from 2015 to 2018, while also aiming to identify threats, challenges and strategic priorities for cybercrime and electronic evidence in the Eastern Partnership region. Findings of region-wide studies on threats, challenges and strategies to address cybercrime and discussions on two specific topics of child protection and cooperation with multinational service providers shaped the agenda of the event. The event reconfirmed the need to have renewed focus on the cybercrime policies and strategies, as defined by the Declaration on Strategic Priorities for the Cooperation against Cybercrime in the Eastern Partnership region and the EU Deliverables 2020 for the Eastern Partnership region." READ MORE

Source: Hurriyet Daily News

Date: 16 Dec 2018

Turkey identifies over 92,000 ByLock users

"Turkey has so far identified over 92,000 users of ByLock, an encrypted smartphone app used by members of FETÖ, the country's interior minister said on Dec. 11. "We have identified 92,702 individual users and 215,092 accounts in the encrypted communication program ByLock," Süleyman Soylu said at the 5th International Cybercrimes Workshop in the capital Ankara. "Somehow, they [FETÖ] have included everyone they communicate with in the system. As I said, they have not only sent viruses to computers, but reinforced real attacks to cyber-attacks by having people like viruses work on the computers," Soylu also said. ByLock is an encrypted mobile phone application used by FETÖ members to communicate during and after the 2016 failed coup attempt. […] He said nearly 54,374 cybercrimes were committed in Turkey in 2018, while 18,330 people were detained and went through judicial proceedings. " READ MORE

RELATED ARTICLES

Council of Europe, Presentation held at the International Workshop on Cybercrime in Ankara, 10-13 Dec 2018

Source: The Jordan Times

Date: 11 Dec 2018

Jordan, Cybercrime bill redrafted with new hate speech definition, reduced slander penalty

"The Cabinet on Monday approved a new draft amending the cybercrime law ahead of sending it to the Lower House, after having withdrawn a previous controversial bill from the Chamber the day before. The amendments to the withdrawn bill, which was referred to Parliament by the previous government, touched on the definition of hate speech, as well as Article 11, which addresses the penalty for slander. Under the new amendments, the definition of hate speech was revisited to now include "every writing and every speech or action intended to provoke sectarian or racial sedition, advocate violence or foster conflict between followers of different religions and various components of the nation". […] As for comments on social media platforms, including comments on news websites' pages, the draft law states that only the person who makes the comment is accountable." READ MORE

RELATED ARTICLES

The Jordan Times, Jordan Government withdraws cybercrime bill, 10 Dec 2018

Source: Night Watch

Date: 16 Dec 2018

Sierra Leone Poised To Enact 1st Cyber Crime & Electronic Evidence Law

"Sierra Leone is set to enact the first cybercrime and electronic evidence law after concluding a successful consultative workshop organized by the Ministry of Information and Communications with technical support from the Council of Europe in Freetown. The three days session witnessed technical presentations from the country's Attorney General and Ministry of Justice, the Right to Access Information, Consultants, Mobile Network Operators, regulators and other relevant players around the need for a cybercrime and electronic evidence law for Sierra Leone in line with international and global demands. The Deputy Minister of Information and Communications, Solomon Jamiru, disclosed that the three-day workshop emanated out of an invitation extended by the Ministry to the Council of Europe to support them technically towards having legislations in place to address cybercrime and any other related matters to electronic evidence. He noted that cybercrime is a global issue and that Sierra Leone, as a country, is looking at the Budapest Convention and other regional documents like the Malabo Convention as benchmarks in dealing with cybercrime." READ MORE

Source: Europol

Date: 4 Dec 2018

Over 1500 money mules identified in worldwide money laundering sting

"Working together with Europol, Eurojust and the European Banking Federation, police forces from over 20 States arrested 168 people as part of a coordinated money laundering crackdown, the European Money Mule Action. This international swoop, the fourth of its kind, was intended to tackle the issue of 'money mules', who help criminals launder millions of euros worth of dirty money. […] Across Europe and beyond, 1504 money mules were identified and 837 criminal investigations were opened. More than 300 banks, 20 bank associations and other financial institutions helped to report 26376 fraudulent money mule transactions, preventing a total loss of €36,1 million. […] To raise awareness of this type of fraud, the money muling awareness campaign #DontBeAMule kicks off today across Europe." READ MORE

Source: 2M

Date: 4 Dec 2018

Cybercriminalité : les avantages de l’adhésion du Maroc à la Convention de Budapest

“L'adhésion du Maroc à la Convention de Budapest sur la cybercriminalité a placé le Royaume parmi les pays leaders en matière des législations modernes, a souligné le procureur général du Roi près la Cour de Cassation, président du ministère public, Mohamed Abdennabaoui. L’adhésion du Maroc à ce processus lui a également permis de tirer profit des moyens juridiques que cette Convention vise à atteindre et qui consistent essentiellement en l’harmonisation du Code pénal national avec ses dispositions et la mise en place d’un régime rapide et efficace de coopération internationale, a expliqué Abdennabaoui, dans une allocution à l’ouverture d’une journée d’étude, initiée par la Présidence du ministère publique sur « les mesures de coopération internationale conformément aux dispositions de la Convention de Budapest sur la cybercriminalité ».” READ MORE

Source: Samaa TV

Date: 5 Dec 2018

Pakistan’s new National Action Plan to revamp cyber security to counter terror

“The Ministry of Interior recently announced it would introduce NAP-2 and restructure the National Counter Terrorism Authority (NACTA). FIA Cyber Crime Wing Director Capt. Muhammad Shoaib said that the agency deals with cybercrime and not cyber security, which requires a legal framework. […] Cyberspace is regulated under a 2016 law, which focuses more on comparatively mundane violations instead of denying space to terrorists. […] “What do you do when a particular act is classified as a crime here (Pakistan) but not abroad?”, FIA officials say that Pakistan should ideally be a signatory to the Budapest Convention so they can seek cooperation from other countries, where a crime may have originated in cyberspace. The laws dealing with the spectrum of this threat, ranging from cyberspace to nailing facilitators, are either insufficient or have lapsed.” READ MORE

Source: INTERPOL

Date: 14 Dec 2018

Asia: INTERPOL task force identifies 27 victims of online child sexual abuse

“An INTERPOL task force has identified 27 victims of child sexual abuse as part of a victim identification operational exercise. In its first meeting in Asia, the INTERPOL Victim Identification Task Force gathered specialized officers from 17 countries to focus on images, videos and audio files depicting abuse believed to have taken place in Asia, or include Asian victims. […] INTERPOL’s Crimes against Children unit is now providing support to member countries to help safeguard the children concerned.” READ MORE

Source: New Straits Times

Date: 3 Dec 2018

Malaysia, national cyber security policy to be introduced next year

“A national cyber security policy will be introduced in the first quarter of next year to curb cyber-attacks, said Communications and Multimedia Minister Gobind Singh Deo. He said the policy aimed to curb cyber-attacks from within and outside the country, including protecting personal information of Internet users.” READ MORE

Source: IT News

Date: 6 Dec 2018

Australia gets world-first encryption busting laws

"Australia's law enforcement agencies have a wide range of new encryption-busting powers after Labor dropped all opposition to a highly contentious bill and let it passes without extra changes it claimed all day were needed. The bill passed into law by 44 votes to 12 in the senate. The law gives law enforcement the power to ask technology companies to create - and then seed – a vulnerability on" one or more target technologies that are connected with a particular person"." READ MORE

RELATED ARTICLES

BBC, Australia data encryption laws explained, 7 Dec 2018

Financial Review, Australian encryption laws under fire from Apple, Facebook, Google and Microsoft, 12 Dec 2018

Source: Mondaq

Date: 3 Dec 2018

Central Bank of Nigeria issues draft Cybersecurity Guideline for Banks and Payment Service Provider

"The Central Bank of Nigeria recently published a draft guideline on cybersecurity for Deposit Money Banks and Payment Service Providers. The guideline is borne out of the persistent and increasing cyber-attacks on financial institutions and platforms in the country. […] The CBN is empowered under the Central Bank of Nigeria Act and Banks and Other Financial Institutions Act (BOFIA) to issue guidelines to regulate the nation's financial institutions and service providers in the country. […] Nigeria is witnessing a burgeoning growth in its banking sector and fintech space with increasing record transactions. […] Section 5 of Cybercrimes Act criminalises attack on sectors designated as critical national infrastructure punishable by imprisonment term not less than 15 years without an option of fine. Part 7.5 of the National Cybersecurity Policy designates financial services sectors amongst other sectors as National Critical Information Infrastructure (NCII)." READ MORE

Latest reports

- European Commission, Strengthening Europe's Cybersecurity, 10 Dec 2018
- ICMEC, Child Sexual Abuse Material: Model Legislation & Global Review, 9th Edition, December 2018
- Twitter, Transparency Report Jan-Jun 2018, December 2018
- Duo, Anatomy of Twitter Bots: Amplification Bots, 10 Dec 2018

Upcoming events

- 17-19 December, Mauritania – Advisory mission on harmonization of legislation on cybercrime and electronic evidence in Mauritania, in preparation for the accession to the Budapest Convention, Cybercrime@Octopus
- 17-21 December, Dakar, Senegal – ECTEG Course on Investigating Darknet and Virtual currencies for Senegalese Law Enforcement Agencies, GLACY+
- 20-21 December, Astana, Kazakhstan – Workshop on legislation related to cybercrime and electronic evidence, Cybercrime@Octopus

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

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

www.coe.int/cybercrime