Cybercrime Digest

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

16-30 November 2017

Source: Council of Europe

Date: 29 Nov 2017

Mutual legal assistance effectiveness and cyberviolence in the focus of the 18th T-CY Plenary

"The Cybercrime Convention Committee is holding its 18th plenary session on 27 and 28 November at the Council of Europe in Strasbourg. Some 160 participants from 65 countries and international organisations focus their deliberations on the effectiveness of mutual legal assistance and on cyberviolence. The Republic of Korea is represented as ad-hoc observer with a large delegation. In the afternoon of 28 and on 29 November, the Committee will continue the negotiation of an Additional Protocol to the Budapest Convention on enhanced international cooperation and access to electronic evidence in the cloud." READ MORE

RELATED ARTICLES

Council of Europe, T-CY Drafting Group, Summary report of the 1st Meeting of the T-CY Protocol Drafting Plenary (Strasbourg 28 – 29 November 2017), Workplan and working methods, 29 Nov 2017

Source: GFCE

Date: 24 Nov 2017

Delhi Communiqué on a GFCE Global Agenda for Cyber Capacity Building

"We, the members, partners and advisory board of the Global Forum on Cyber Expertise (GFCE), use the opportunity of the Global Conference on Cyberspace 2017 in New Delhi, India, to announce a GFCE Global Agenda for Cyber Capacity Building, which derives from best practices and lessons learned in the development, security and technical communities. […] Cybercrime – a. Enact and enforce a comprehensive set of laws, guidelines, policies and programmes relating to cybercrime in line with existing international standards that allow for effective international cooperation, such as the Budapest Convention on Cybercrime. b. Modernize and strengthen domestic criminal justice systems to deal with cybercrime and crimes involving electronic evidence, including the effective prevention, detection, investigation, prosecution and adjudication of such crimes in all their forms." READ MORE

Source: Sur Actual

Date: 24 Nov 2017

Diputados convierte en ley la ratificación del convenio para luchar contra el ciberdelito en Argentina

"La Cámara de Diputados convirtió en ley la adhesión del país a la Convención de Budapest para la lucha contra el ciberdelito, que establece criterios, protocolos y legislaciones locales tanto para el combate de estafas informáticas como para la pornografía infantil. Se trata de la adhesión del país a ese tratado supranacional que la cámara baja aprobó esta tarde y dio así sanción definitiva a ese convenio. El Convenio de Budapest entró en vigencia el 23 de noviembre de 2001 y se ocupa de estandarizar criterios, protocolos y legislaciones locales para el combate contra las estafas informáticas, la distribución de pornografía infantil, las infracciones vinculadas a la propiedad intelectual y los atentados contra la integridad del sistema." READ MORE

Source: Star On Line

Date: 29 Nov 2017

Malaysia eyeing membership in Budapest Convention on Cybercrime

"Malaysia is exploring the possibility of becoming a member of the Budapest Convention on Cybercrime, said Minister in the Prime Minister's Department Datuk Seri Azalina Othman Said. She said the Government had formed several committees within various government departments, including law enforcement agencies, to study the provisions of the convention and determine the policy, legal, technical and administrative requirements that need to be fulfilled. "Our study on Malaysia's legislation framework has identified that our Computer Crimes Act 1997 and Mutual Assistance in Criminal Matters Act 2002 need to be amended to fulfill the legal requirements under the Budapest Convention," she said." READ MORE

Source: The Economic Times

Date: 27 Nov 2017

Budapest Convention can be foundation for cyber security law: British Minister

"As the world talks about crimes in cyber space and the need for a universal law to fight these, a British Minister is of the view that the Budapest Convention can be the foundation for such a global law to ensure cyber security. "If you go back in recent history, you would have seen that within the Council of Europe, there was a convention called Budapest Convention which set certain conventions and certain premises in place on how this space can be managed," Lord Tariq Ahmad, Britain's Minister of State for the Commonwealth and the United Nations, said." READ MORE

Source: Eurojust

Date: 22 Nov 2017

159 arrests and 766 money mules identified in global action week against money muling

"Law enforcement authorities from 26 countries, supported by Europol, Eurojust and the European Banking Federation, have joined forces in the third coordinated global action against money muling, with the European Money Mule Action 'EMMA3'. […]. Money mules are recruited by criminal organisations as money laundering intermediaries to receive and transfer illegally obtained funds between bank accounts and/or countries. […] With the support of 257 banks and private-sector partners, 1 719 money mule transactions were reported, with total losses amounting to almost EUR 31 million. Among those money mule transactions, more than 90% were linked to cyber-related crimes, such as phishing, online auction fraud, Business Email Compromise (BEC) and CEO fraud." READ MORE

Source: Naked Security

Date: 17 Nov 2017

Skype faces fine after refusing to allow eavesdropping

"Skype's looking at a €30,000 fine from a Belgian court that wants to eavesdrop on conversations – something that Microsoft-owned Skype said is 1) technically impossible and 2) shouldn't apply because the laws are for telecoms, which it isn't. Skype lost an appeal of the fine in a Belgian court on Wednesday. According to the Belgian newspaper, the trouble began in 2012, when Belgian authorities came knocking, wanting to listen in on conversations that an organized crime gang conducted mostly on Skype. According to public prosecutor Tim Van hoogenbemt, Skype only complied with part of the request. In other words, it only handed over metadata: e-mail addresses, user histories, account details and IP addresses." READ MORE

Source: Europol

Date: 22 Nov 2017

Europol brings together three regions of the world to tackle payment card fraud

"On 20-21 November 2017, Europol's European Cybercrime Centre (EC3), with the support of the European Association for Secure Transactions (EAST), hosted an international meeting to address payment card fraud across Europe and beyond. In its sixth occurrence since it was first organised in Singapore in 2015, this meeting was held for the first time at Europol's headquarters in The Hague, bringing together representatives from 3 regions of the world: 8 EU Member States (Portugal, Greece, France, Denmark, Spain, Romania, Bulgaria and Italy), Latin America (Argentina, Dominican Republic, Chile, Colombia and AMERIPOL) and Asia (Malaysia, Philippines, Thailand and ASEANPOL). […] This meeting between law enforcement agencies of Europe, Asia and Latin America gave experts the opportunity to create an overview of the criminality seen the past year and prepare for threats in 2018. These meetings also help provide valuable insights into the activities of international organised crime groups and help law enforcement agencies better respond to them." READ MORE

Source: Council of Europe

Date: 21 Nov 2017

The African Union and the Council of Europe renew their joint commitment against cybercrime

"The Cybercrime Programme Office (C-PROC) of the Council of Europe was invited by the African Union Commission to participate in the second meeting of the Specialized Technical Committee on Communication and ICT formed by Ministers of Communication and Information Technologies from the African region. […] The meeting offered also an occasion to renew the agreement for cooperation with the African Union Commission to jointly assist African Countries in the strengthening of: their domestic legislation on the basis of the "Budapest Convention on Cybercrime" and the "African Union Convention on Cyberspace Security and Protection of Personal Data - Malabo Convention"; institutional capacities, training and international/regional cooperation; cybercrime policies and strategies." READ MORE

Source: Agence Ecofin

Date: 16 Nov 2017

La France annonce l'ouverture d'une école régionale de cybersécurité au Sénégal

"Lors du Forum international de Dakar sur la paix et la sécurité, tenu du 13 au 14 novembre 2017, la France a dévoilé son ambition d'ouvrir une école de cybersécurité au Sénégal. L'annonce a été faite par le ministre français des Affaires étrangères et de l'Europe, Jean Yves Le Drian. Intervenant lors de la plénière sur « l'Afrique et les nouveaux enjeux sécuritaires », Jean Yves Le Drian a exprimé son souhait de voir ce projet réalisé dans les plus brefs délais. L'idée, le ministre français a indiqué en avoir déjà discuté avec le président de la République du Sénégal, Macky Sall. Cette école régionale de cybersécurité est « un projet innovant en vue de renforcer les capacités de réponse de nos partenaires africains aux menaces du cybersécurité [...]. Il s'agit d'une réponse contre les cyberattaques mais aussi la lutte contre la cybercriminalité et le terrorisme qui sont des menaces tout à fait réelles et qui ne sont pas limitées au monde européen ou au monde américain. Nous allons mettre cela en œuvre avec une dimension africaine affirmée à partir du Sénégal. J'espère que d'ici le prochain forum, nous aurons le constat de ce caractère opératoire de cette école», a affirmé Jean Yves Le Drian." READ MORE

Internet bank fraudsters now in recession in Nigeria

"A Deputy Governor of the Central Bank of Nigeria in charge of Operations, Mr. Adebayo Adelabu has declared that internet fraudsters in the banking sector are now in recession and would never recover again. Adelabu said this was because the apex bank will continue to strengthen the fight against e-fraud in Nigeria. […] While commending the feats recorded in the last six years by the Nigeria Electronic Fraud Forum (NeFF), Adelabu said that the organization in collaboration with other stakeholders had successfully implemented the Cybercrime Prohibition and Prevention Act 2015, under the theme; Tackling Enforcement Challenges Under The Cybercrime Act." READ MORE

Cybercriminalité: Des mesures de lutte en Afrique

"Les ministres de la Sécurité des cinq pays de l'Afrique de l'Ouest regroupés au sein Conseil de l'Entente ont pris une batterie de mesures pour lutter contre la cybercriminalité qui sévit dans leur espace, à l'issue d'une réunion tenue du 21 au 23 novembre à Lomé, la capitale togolaise. Le fléau de la cybercriminalité connaît un développement exponentiel dans les pays membres du Conseil de l'Entente, favorisé par l'essor rapide des TIC et leur facilité d'accès, ont constaté les ministres. Aussi, ont-ils proposé l'adoption, dans chaque Etat membre, d'une stratégie nationale et la centralisation de la lutte autour d'une structure unique chargée du partage des informations aux autres unités d'investigations. " READ MORE

Uber Paid Hackers to Delete Stolen Data on 57 Million People

"Hackers stole the personal data of 57 million customers and drivers from Uber Technologies Inc., a massive breach that the company concealed for more than a year. This week, the ride-hailing firm ousted its chief security officer and one of his deputies for their roles in keeping the hack under wraps, which included a $100,000 payment to the attackers. Compromised data from the October 2016 attack included names, email addresses and phone numbers of 50 million Uber riders around the world, the company told Bloomberg on Tuesday. The personal information of about 7 million drivers was accessed as well, including some 600,000 U.S. driver's license numbers. No Social Security numbers, credit card information, trip location details or other data were taken, Uber said." READ MORE

Protecting children from sexual risks online: Council of Europe experts offer quick tips to parents

"Ahead of the European Day to Protect Children from Sexual Exploitation and Sexual Abuse, marked on the 18th of November, the Council of Europe has published a series of online video tutorials to protect children from the new risks of sexual nature they encounter online, and help them safely navigate the digital environment. "All of us – parents, teachers, communities, governments, – must ensure that technology and new media help children to explore, learn and develop, and not to fall prey to sexual exploitation and abuse," Secretary General of the Council of Europe Thorbjørn Jagland said, stressing the importance of not shying away from the problem of sexual exploitation and sexual abuse of children online." READ MORE

Source: Europol

Date: 30 Nov 2017

Teaming up for 'Combating the Online Sexual Exploitation of Children' (COSEC)

"At the end of October 2017, the 18th Europol training course on 'Combating the Online Sexual Exploitation of Children (COSEC), took place in Selm, Germany, at the Police Academy of North Rhine Westphalia. This 10-day course provided training for 65 representatives from EU Member States, non-EU States , Europol and INTERPOL. The training was delivered by police trainers from Europol, Australia, Belgium, Czech Republic, Denmark, France, New Zealand, OLAF, Portugal and one from Ireland on behalf of INHOPE. Trainers had extensive knowledge and experience in investigating and combating the sexual abuse of children online. The objective of this course is to give investigators and magistrates the required knowledge to understand the environment in which these crimes are committed." READ MORE

Source: L'Orient Le Jour

Date: 30 Nov 2017

Le Liban de plus en plus ciblé par les cyberattaques

"Dans un rapport publié hier, la société de sécurité informatique McAfee a affirmé craindre une augmentation de la cybercriminalité dans le monde en 2018, tandis que l'année en cours a déjà été marquée par plusieurs attaques informatiques de grande ampleur. Cette intensification devrait également se faire ressentir au Liban, selon Jan Kaastrup, directeur de la technologie au sein de la société danoise CSIS Security Group, qui s'attend à une « multiplication de plusieurs types d'offensives » au courant des mois à venir – rançongiciel (ransomware), fraude au fournisseur/président, ou encore hameçonnage (phishing) ciblé, principalement. " READ MORE

Source: The Jamestown Foundation

Date: 20 Nov 2017

Kazakhstan Launches 'Cyber Shield' Concept

"The government of Kazakhstan has approved an action plan, on October 28, to implement the country's cybersecurity concept—"Cyber Shield"—by 2022. The document outlines key areas of state policy that will be required to build a modern yet reliable system to mitigate and prevent cyberattacks and threats from hybrid ("new type") warfare. The amount of illegal online content reaching Kazakhstan has grown by a factor of 40 in the last three years. Both government agencies and domestic financial institutions frequently suffer from cyberattacks. Ruslan Abdukalikov, the deputy chairman of the Committee on Information Security in the Ministry of Defense and Aerospace Industry, recently pointed out that the number of cyber threats to the state's electronic systems increases by 2–2.5 times every year." READ MORE

Source: The Hindu

Date: 30 Nov 2017

Many cybercrime cases not investigated in India

"More than 12,000 incidents of cybercrime were reported in 2016, but nearly the same number of such crimes carried forward from the previous years had not been investigated, the data released by the National Crime Records Bureau (NCRB) said. In 2016, 12,317 such incidents were reported and in 2015 the figure stood at 11,592, a jump of 6.3%. Only in 30% cases reported in 2016, the police or the investigating agency filed a charge sheet. In absolute numbers, 7,990 persons were arrested for the crimes, which included 147 women and charge sheets were filed against 4,913 accused. Illegal gain (5,987 incidents) and revenge (1,056) were the two top motives that accounted for cybercrimes. Sexual exploitation (686), insulting the modesty of women (569) and causing disrepute (448) constituted 13% of the crimes." READ MORE

Source: EU Observer

European foundation demands release of Turkish journalist

Date: 28 Nov 2017

"Turkish authorities seized Zaman in March 2016 and appointed pro-government trustees, four months before the coup and closed the newspaper right after the failed putsch. Sources who followed the court case told EUobserver that judge ruled on the case solely on the existence of the ByLock app on her mobile. The judge later discarded her tweets as evidence. However, sources who want to remain anonymous said the evidence submitted to the court about ByLock was dubious and would be inadmissable in an international court." READ MORE

Latest reports

- Council of the European Union, Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU - adoption, 20 Nov 2017
- The Financial Action Task Force, FATF Recommendations, Updated in November 2017
- Europol, Drugs and the Darknet: Perspectives for enforcement, research and policy, 22 Nov 2017
- ENISA, Baseline Security Recommendations for IoT, 20 Nov 2017
- Google Research, Data Breaches, Phishing, or Malware? Understanding the Risks of Stolen Credentials, November 2017
- Malware Bytes, Cybersécurité : Malwarebytes dévoile les grandes tendances 2018, November 2017

Upcoming events

- 4-7 December, Belgrade, Serbia – Pilot introductory training course on cybercrime, electronic evidence and online crime proceeds for judges and prosecutors, iPROCEEDS
- 4-7 December, Accra, Ghana – Support to the regional delivery of Introductory Course on cybercrime and electronic evidence for Judges and prosecutors of the Anglophone Countries of the ECOWAS region, GLACY+
- 4-7 December, Belgrade, Serbia – Case simulation exercises on cybercrime and financial investigations, iPROCEEDS
- 5-7 December, Santo Domingo, Dominican Republic – Hemispheric Forum on International Cooperation against Cybercrime, GLACY+
- 12-14 December, Cebu, Philippines – International Workshop on Judicial Training Strategies, with the participation of GLACY+ countries and ASEAN member states, GLACY+

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