Cybercrime Digest

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

16-30 November 2018

Source: Council of Europe

Date: 29 Nov 2018

Strategic directions of the Cybercrime Convention Committee for 2019

"The Cybercrime Convention Committee (T-CY) with 160 members and observers gathered at the Council of Europe to discuss international challenges and shape the strategic directions of its work for 2019 as reflected in the workplan adopted by the T-CY. The 2019 agenda will be largely shaped by the preparation of the 2nd additional Protocol on enhanced international cooperation and access to evidence in the cloud. Good progress was made by the Protocol Drafting Plenary on 28 and 29 November. Consultations with data protection experts on 26 November indicated options to ensure that additional solutions on access to evidence are compatible with data protection requirements. Parties shared their concerns on election interference via computer systems and agreed to prepare a Guidance Note on this question." READ MORE

T-CY, 20th Plenary Meeting report, 27 November 2018

Source: Council of Europe

Date: 23 Nov 2018

17th Anniversary of the Budapest Convention

"On 23 November, the Council of Europe celebrated the 17th Anniversary of the Budapest Convention on Cybercrime. On this occasion, Permanent Representations of Parties and Observers to the Council of Europe were briefed on current challenges of cybercrime and the Council of Europe response. The meeting was organized at the initiative of Ambassador Corina Calugaru, Permanent Representative of Moldova and Thematic Coordinator on Information Policy. Since 2001, the Budapest Convention has become one of the most influential treaties of the Council of Europe on a global scale, providing a comprehensive and coherent framework on cybercrime and electronic evidence. The Convention serves as a guideline for any country developing national legislation against cybercrime and as a framework for international cooperation between State Parties to this treaty. The Convention on Cybercrime has now 61 States Parties. A further 10 States have signed it or been invited to accede." READ MORE

RELATED ARTICLES

Council of Europe, Update of current challenges and the CoE response, 23 Nov 2018

Council of Europe, Acceding to the Budapest Convention: Benefits, 23 Nov 2018

Source: Euro-Méditerranée

Date: 25 Nov 2018

CyberSud : Atelier sur la Convention de Budapest sur la cybercriminalité en Jordanie

"Un atelier sur la législation en matière de la cybercriminalité et la preuve numérique a eu lieu à Amman, en Jordanie les 8 et 9 octobre 2018, dans le cadre du projet CyberSud, un programme joint de la Commission européenne et du Conseil de l'Europe. L'objectif était de réunir les autorités compétentes impliquées dans le processus législatif et les autorités policières ayant des responsabilités dans le renforcement de la législation sur la cybercriminalité, afin de discuter de la Convention de Budapest sur la cybercriminalité en tant que norme législative internationale dans ce domaine et de la législation nationale en Jordanie." READ MORE

Source: Daily Mirror

Date: 28 Nov 2018

EU supports Philippines and the ASEAN countries in efforts to boost capability vs cybercrime

"The European Union (EU) Delegation to the Philippines on Friday showed its support on a four-day "Introductory Training of Trainers Course on Cybercrime and Electronic Evidence." The training course was organized by the Supreme Court of the Philippines and the Council of Europe. Around 30 participants from 9 countries of the ASEAN region were trained by previously formed Philippines trainers on "cybercrime legislation and procedural powers in relation to electronic evidence and tools for international cooperation." Justice Secretary Menardo Guevarra said during the opening of the regional training that the mass of trainers is needed to fight against cybercrime. "[…] A critical mass of trainers is necessary if we are to establish a web of experts that can contain, neutralize and protect our entire region from the pernicious effects of cybercrime," he said in a statement. […] The EU and the Council of Europe, through the joint project on Global Action on Cybercrime Extended (GLACY+), have been working with countries to develop sustainable training programs on cybercrime and electronic evidence, both for the judiciary and for the law enforcement." READ MORE

Source: ICANN

Date: 21 Nov 2018

WHOIS and GDPR, ICANN publishes initial report on Temporary Specification for gTLD Registration Data. Public comment period is now open

"The Temporary Specification approved by ICANN Board on 25 May 2018, expires one year from that date. The Expedited Policy Development Process (EPDP) Team is working in a short period of time to provide a replacement policy for ICANN Board approval before the expiration date. […] The Initial Report responds to the call on the EPDP Team, mandated by the charter, to answer a set of questions and determine if the Temporary Specification for gTLD Registration Data should become a GDPR-compliant ICANN Consensus Policy as is, or one with modifications. […] This Initial Report provides preliminary recommendations and questions for the public to consider. The EPDP Team reached tentative agreement on many of these but there was no call for consensus. The EPDP Team members did not reach agreement on many other areas of discussion. The Initial Report describes areas of disagreement and provides specific questions on which the public may consider and provide comments with the purpose of guiding the EPDP Team's deliberations." READ MORE

Source: Eurasianet

Date: 27 Nov 2018

Hackers eyeing Kazakhstan as a safe haven

"Kazakhstan is proving especially appealing to online crooks thanks to the combination of lax legislation and weak cybercrime prevention bodies, experts warn. "One of the world's most dangerous hacker groups, Cobalt, which specializes in hacking into bank accounts, is moving into Kazakhstan," director of the Center for Cyberattack Analysis and Research (TsARKA), Arman Abdrasilov said. When TsARKA raised the alarm, which it issued earlier this year on the back of research done by Moscow-based cybersecurity company Positive Technologies, it caused a few ripples but has generated little by way of a visible response from the authorities. […]Abdrasilov says security experts have recorded a spike in the number of computers in Kazakhstan being hijacked by Cobalt. When $81 million was stolen from the Bangladesh Bank in February 2016, it was done in part through hacked servers located in Kazakhstan, he says." READ MORE

Source: U.S. Department of Justice

Date: 18 Nov 2018

U.S. Deputy Attorney General delivers remarks at the Interpol 87th General Assembly

"I am proud that the United States takes seriously our responsibility to help secure evidence that our international partners need for their investigations. We receive thousands of requests for mutual legal assistance each year, and we do all that we can to comply. We employ expert attorneys and staff dedicated to assisting with foreign requests for electronic evidence. We devote additional resources when necessary to meet your needs. We call upon each of you to do the same. […] My country recently enacted a new law to remove legal impediments to compliance with foreign court orders in cases that involve serious crimes. The legislation demonstrates our commitment to the vision of the Budapest Convention on Cybercrime, the primary treaty for harmonizing national interests and enhancing international cooperation against cybercrime. Sixty-one nations have fully ratified the treaty, agreeing that national laws should include authority to compel providers to disclose data they control, even when it is held elsewhere. New cyber conventions are sometimes proposed that would limit the free flow of information between nations. But that would dangerously impede efforts to investigate cybercrime. It would protect criminals and allow cyber threats to proliferate and grow in scale and sophistication. That is untenable in a world in which criminals using computers shielded by layers of anonymity can harm innocent victims in any one of our nations, anywhere in the world. […] No nation should exempt itself from just and reasonable law enforcement cooperation." READ MORE

Source: Le Monde

Date: 22 Nov 2018

Au Sénégal, un centre pour former les Africains à la cybersécurité

"Les ministres français et sénégalais des affaires étrangères ont inauguré, mardi 6 novembre à Dakar, une école de cybersécurité à vocation régionale. « Aucun pays ne peut se prémunir à lui seul des cyberattaques », a déclaré le chef de la diplomatie sénégalaise, Sidiki Kaba, à l'occasion du cinquième Forum international de Dakar sur la paix et la sécurité en Afrique. Présenté lors de l'édition précédente du forum, le projet a été conçu pour développer les compétences des pays africains en matière de lutte contre la cybercriminalité et le cyberterrorisme, mais pas seulement. « Cette école n'est pas qu'un projet de défense mais répondra aussi aux besoins de régulation économique dans l'espace numérique ». " READ MORE

Source: El Periodico

Date: 18 Nov 2018

Aumento del cibercrimen en Guatemala

"El uso de Internet en Guatemala ha tenido un crecimiento vertiginoso en los últimos años. La cantidad de personas con acceso a a la red supera los 7.2 millones de usuarios, de acuerdo con Internet World Stats (dic. 2017), con un porcentaje de penetración de 39.4 por ciento. […] Estas son parte de las cifras que maneja el Observatorio de Delitos Informáticos en Guatemala (OGDI), oenegé que, de acuerdo con su fundador, José R. Leonett, nace a partir de la necesidad de frenar el incremento de la cibercriminalidad en Guatemala y de la falta de estadísticas sobre estos hechos. […] Un dato comparativo de la Policía Nacional Civil indica que en 2017 hubo 338 delitos informáticos en Guatemala. Los más recurrentes fueron las amenazas y el ciberacoso. El segundo más reportado fue la violación a la intimidad sexual. Solo en el primer trimestre de 2018, se registraron 236 casos. " READ MORE

Source: IT Web

Date: 28 Nov 2018

Cyber Crimes Bill inches closer to becoming law in South Africa

"South Africa's Cyber Crimes Bill was passed by the National Assembly yesterday. With the completion of the National Assembly process, the Bill will be transferred to National Council of Provinces for agreement, whereby it will eventually reach the president to be signed into law. The Bill, initiated by the South African government, through the Department of Justice and Constitutional Development (DOJ), seeks to create offences which have a bearing on cyber crime, to criminalise the distribution of data messages which are harmful, and to provide for interim protection orders, among other issues. The initial draft Bill received some backlash with several critics saying it was too broad and open to abuse, and it threatened the fundamental democratic spirit of the Internet. However, following public comment and discussion, the Bill was revised and the DOJ tabled a new version before Parliament's Portfolio Committee on Justice and Correctional Services in October." READ MORE

Source: The Straits Times

Date: 20 Nov 2018

Indonesia and US reach agreement to cooperate on cyber security

"Indonesian National Police and the United States Attorney-General's Office have agreed to strengthen bilateral cooperation against transnational cyber and financial crime. Indonesian police chief Tito Karnavian and US Deputy Attorney-General Rod Rosenstein reached the agreement on Monday (Nov 19), on the sidelines of the 87th Interpol General Assembly being held in Dubai this week. General Tito said the pact with the US Attorney-General's Office will also see Indonesian police officers undergoing law enforcement-related training programmes conducted by their American counterparts." READ MORE

Source: Reuters

Date: 19 Nov 2018

Cyber attack targets Italian certified email accounts

"Unknown hackers gained access to thousands of Italian certified email accounts, including those of magistrates and security officials, in a major cyber attack earlier this month, a senior official said on Monday. Certified emails guarantee the validity of a sender's identity, as well as the date and time of sending and receiving the email, giving them a clear legal status. […] Hackers could have accessed data from around 500,000 accounts, including those of some 9,000 magistrates as well as members of a top inter-governmental security agency. It was not clear if the accounts of any ministers, spy chiefs or military bigwigs had been breached." READ MORE

Source: The Guardian

Date: 21 Nov 2018

Amazon hit with major data breach days before Black Friday

"Amazon has suffered a major data breach that caused customer names and email addresses to be disclosed on its website, just two days ahead of Black Friday. The e-commerce giant said it has emailed affected customers but refused to give any more details on how many people were affected or where they are based. The firm said the issue was not a breach of its website or any of its systems, but a technical issue that inadvertently posted customer names and email addresses to its website." READ MORE

Source: France 24

Date: 21 Nov 2018

Le Parlement français adopte la loi contre la "manipulation de l'information" en période électorale

"Les deux textes constituent la mouture définitive du cadre de la lutte contre les "fake news" en période électorale. Cette loi offre, pour la première fois, une définition des "fausses informations" qui, au terme du texte, sont "des allégations ou imputations inexactes ou trompeuses d'un fait de nature à altérer la sincérité du scrutin". Les dispositions nouvelles doivent permettre à un candidat ou parti de saisir le juge des référés pour faire cesser la diffusion de "fausses informations" durant les trois mois précédant un scrutin national. Les principales plateformes numériques - Facebook, Twitter ou encore Google - sont aussi appelées en renfort pour lutter contre les risques de manipulations de l'information. Elles auront l'obligation de fournir les informations sur les publicités politiques qu'elles diffusent contre rémunération sur leur site. Elles doivent rendre public le montant payé pour des messages électoraux, et mettre à disposition des électeurs un registre en ligne avec les informations sur l'identité des promoteurs de ces publicités électorales." READ MORE

Source: Nature

Date: 20 Nov 2018

The spread of low-credibility content by social bots

"The massive spread of digital misinformation has been identified as a major threat to democracies. Communication, cognitive, social, and computer scientists are studying the complex causes for the viral diffusion of misinformation, while online platforms are beginning to deploy countermeasures. Little systematic, data-based evidence has been published to guide these efforts. Here we analyze 14 million messages spreading 400 thousand articles on Twitter during ten months in 2016 and 2017. We find evidence that social bots played a disproportionate role in spreading articles from low-credibility sources. Bots amplify such content in the early spreading moments, before an article goes viral. They also target users with many followers through replies and mentions. Humans are vulnerable to this manipulation, resharing content posted by bots. Successful low-credibility sources are heavily supported by social bots. These results suggest that curbing social bots may be an effective strategy for mitigating the spread of online misinformation." READ MORE

Latest reports

- Council of the European Union, EU Cyber Defence Policy Framework (2018 update), 19 Nov 2018
- Center for Internet and Society – India, The Budapest Convention and the Information Technology Act of India, 20 Nov 2018
- The New York Times, The New Radicalization of the Internet, 24 Nov 2018
- International Association of the Chiefs of Police (IACP), 2018 Resolutions, adopted November 2018
- The Dialogue, Data Localisation in a Globalised World: the Indian perspective, November 2018
- J. Daluwengo, M. Mutemi, Treatment of Kenya's Internet Intermediaries under the Computer Misuse and Cybercrimes Act, 2018
- M. Adamou, Les infractions à caractère numérique au regard de l'évolution récente du droit positif béninois, 19 Nov 2018
- A. Moiseienko, O. Kraft, From Money Mules to Chain-Hopping: Targeting the Finances of Cybercrime, 29 Nov 2018
- Cybercrime Convention Committee (T-CY), Conditions for obtaining subscriber information in relation to dynamic versus static IP addresses: overview of relevant court decisions and developments, 25 October 2018

Upcoming events

- 2-6 December, Algiers, Algeria – Advanced judicial training on cybercrime and electronic evidence for magistrates, CyberSouth
- 3 December, Skopje, "the former Yugoslav Republic of Macedonia" – Workshop on online fraud and credit card fraud, iPROCEEDS
- 4 December, Dublin, Ireland – Conferring Ceremony of the long-distance master programme, iPROCEEDS
- 6-7 December, Baku, Azerbaijan – National Cybercrime Cooperation Forum with participation of law enforcement and Internet industry, in cooperation with BakuTEL 2018, Cybercrime@EAP 2018
- 10-13 December, Ankara, Turkey – Participation in the workshop on cybercrime, iPROCEEDS
- 10-13 December, Rabat, Morocco – Study visit of the cybercrime unit of the National Police, CyberSouth
- 10-14 December, Abuja, Nigeria – Training on Trainers on cybercrime and electronic evidence for First Responders, GLACY+
- 10-14 December, Dublin, Ireland – Support in participation in long-distance master programme (Winter examination), iPROCEEDS
- 10-14 December, Freetown, Sierra Leone – Advisory mission on harmonization of legislation on cybercrime and electronic evidence, GLACY+ / Cybercrime@Octopus
- 10-14 December, Niamey, Niger – Advisory mission on harmonization of legislation on cybercrime and electronic evidence, Cybercrime@Octopus
- 10-14 December, Dakar, Senegal – ECTEG Course, Cybercrime and digital forensics specialized training for law enforcement officers, GLACY+
- 11-13 December, Tbilisi, Georgia – Regional Conference on Cybercrime Strategies and Closing Conference for Cybercrime@EAP Projects/Launching for Cyber East Programme, Cybercrime@EAP 2018
- 12 December, Bucharest, Romania – Awareness raising meeting on the Budapest Convention, benefits and challenges for Embassies of priority countries in Romania, CyberSouth
- 14 December, Beirut, Lebanon – Training on electronic evidence and related procedures for law enforcement, prosecutors and judges, CyberSouth

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