Cybercrime Digest

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

1-15 March 2018

Source: Scientific American

Date: 1 Mar 2018

Supreme Court Skeptical of Microsoft's Ireland E-Mail Privacy Claims

"Justices are considering whether a law passed prior to the Web and cloud computing allows companies to hide data stored abroad. The Stored Communications Act (SCA) gives law enforcement with a warrant the authority to compel companies to hand over e-mails stored on U.S. soil that are relevant to an investigation. Congress passed that law in 1986, however, before the dawn of the Web and cloud computing. As a result, the legislation's powers have been limited by the lawmakers' inability to imagine a time when data could be stored anywhere in the world and accessed easily over a computer network." READ MORE

Source: Project Syndicate

Date: 8 Mar 2018

How Will New Cybersecurity Norms Develop?

"Last month, United Nations Secretary-General António Guterres called for global action to minimize the risk posed by electronic warfare to civilians. Guterres lamented that "there is no regulatory scheme for that type of warfare," noting that "it is not clear how the Geneva Convention or international humanitarian law applies to it.". […] Many observers have called for laws and norms to secure this new environment. But developing such standards in the cyber domain faces a number of difficult hurdles. Although Moore's law about the doubling of computing power every two years means that cyber time moves quickly, human habits, norms, and state practices change more slowly. […] Cyber tools are dual use, fast, cheap, and often deniable, verification and attribution are difficult, and entry barriers are low. Moreover, while the Internet is transnational, the infrastructure (and people) on which it relies fall within the differing jurisdictions of sovereign states. And major states differ in their objectives, with Russia and China stressing the importance of sovereign control, while many democracies press for a more open Internet." READ MORE

Source: Le Faso

Date: 14 Mar 2018

Répression de la cybercriminalité au Burkina Faso : Un avant-projet de loi en gestation

"Le Burkina Faso veut renforcer son arsenal juridique contre la 3e grande menace planétaire, la cybercriminalité. Réunis à Ouagadougou du 12 au 15 mars 2018, à l'appel du ministère de la Justice, des droits humains et de la promotion civique, une vingtaine de spécialistes du domaine informatique, du secteur privé et de la recherche prennent part à l'atelier national d'élaboration d'un avant-projet de loi relatif à la répression de la cybercriminalité. La cérémonie d'ouverture a eu lieu, ce lundi en présence du ministre en charge de la justice René Bagoro, qui avait à ses côtés sa collègue du développement de l'économie numérique et des postes, Hadja Ouattara/Sanon. […] «Cet avant-projet dont nous espérons l'adoption rapide devra nous permettre d'adapter notre législation et ainsi satisfaire à nos obligations internationales, mais aussi de pouvoir demander à adhérer à la convention de Budapest qui est une base de coopération judiciaire entre les pays qui en sont membres en matière de répression de la cybercriminalité», a expliqué le ministre Bagoro." READ MORE

Source: Europol

Date: 2 Mar 2018

Two arrested in France for major CEO fraud

"House searches in France have led to the arrests of two individuals suspected of large-scale CEO fraud. The criminals belonged to an organised crime group involved in at least 24 cases of CEO fraud causing EUR 4.6 million worth of damage. With the support of Europol, the French National Gendarmerie carried out the searches in Paris and Lille and made the subsequent arrests on 20 February 2018. The French National Gendarmerie organised an operational meeting in Bordeaux on 14 February where experts and investigators from Belgium, Romania, Israel and Switzerland joined French law enforcement specialists, exchanged their findings and agreed on a mutual action plan for the near future. The investigation was launched in June 2016 when French law enforcement discovered two French companies had fallen victim to CEO fraud, incurring an estimated EUR 1.2 million in losses." READ MORE

Source: Europol

Date: 2 Mar 2018

Europol's EU Internet Referral Unit partners with Belgium, France and the Netherlands to tackle online terrorist content

"This week Europol's EU Internet Referral Unit (IRU) launched a pilot project with the Internet Referral Units of Belgium, France and the Netherlands. The project aims to improve the detection, analysis and referral of online terrorist content. The partners involved now benefit from a Europol-hosted centralised platform which improves the speed of detecting terrorist content, streamlining the referral process and standardising the reporting and communication with the Online Service Providers (OSPs). As a result, this platform facilitates cooperation between European law enforcement authorities and OSPs in their shared fight against online terrorism in the context of the EU Internet Forum. The project is developed under Europol's EU IRU mandate to coordinate and share detection tasks (flagging) of online terrorist content with relevant partners, and to carry out and support referrals quickly, efficiently and effectively in close cooperation with the industry." READ MORE

Source: The Japan Times

Date: 13 Mar 2018

ICANN meets as internet overseers weigh website owner privacy

"The group overseeing internet addresses is scrambling to balance the privacy of website owners and the right to know who is behind online pages. The nonprofit Internet Corporation for Assigned Names and Numbers (ICANN) began a weeklong meeting Monday focused on the fate of the public Whois database, which shows contact information for those who own websites. The General Data Protection Regulation set to take effect in the European Union on May 25 could make revealing personal information about website owners in Whois illegal. […] If ICANN were to simply discontinue the Whois index in Europe, that could create a haven for those from other parts of the world who want to hide which websites they own. […] ICANN is refining a plan to divide Whois into two tiers — one open to the public […] and a second that could be accessed as needed by police, researchers or others with legitimate queries." READ MORE

RELATED ARTICLES

ICANN, More Details Published on ICANN-proposed Interim Model, 8 Mar 2018

Source: IMF Blog

Date: 13 Mar 2018

IMF addresses the Dark Side of the Crypto World

"The same reason crypto-assets—or what some people call crypto-currencies—are so appealing is also what makes them dangerous. These digital offerings are typically built in a decentralized way and without the need for a central bank. This gives crypto-asset transactions an element of anonymity, much like cash transactions. The result is a potentially major new vehicle for money laundering and the financing of terrorism. […] The same innovations that power crypto-assets can also help us regulate them. To put it another way, we can fight fire with fire. Regulatory technology and supervisory technology can help shut criminals out of the crypto world. More broadly, we are seeing crypto-asset exchanges in some countries that are subject to know-your-customer requirements. These advances will take years to refine and implement. Two examples highlight the promise of this approach over the long term: Distributed ledger technology; […] Biometrics, artificial intelligence, and cryptography." READ MORE

Source: FBI

Date: 15 Mar 2018

International Criminal Communication Service Dismantled

"International organized crime and drug trafficking groups were dealt a blow by the takedown of an encrypted communication service they used to plan and commit their crimes, the FBI and its international partners announced yesterday. Canada-based Phantom Secure was a criminal enterprise that provided secure communications to high-level drug traffickers and other criminal organization leaders. The group purchased smartphones, removed all of the typical functionality—calling, texting, Internet, and GPS—and installed an encrypted e-mail system, so the phones could only communicate with each other. If a customer was arrested, Phantom Secure destroyed the data on that phone, which is obstruction of justice under U.S. law. In an attempt to thwart law enforcement efforts, the company required new customers to have a reference from an existing user. Given the limited functionality of the phones and the fact that they only operate within a closed network of criminals, all of Phantom Secure's customers are believed to be involved in serious criminal activity." READ MORE

Source: Mada Masr

Date: 14 Mar 2018

Egypt, Parliament in haste to approve cybercrime bill: Ambiguous provisions, loose definitions, legalized web censorship

"[…] 14 articles of the cybercrime prevention bill were approved by Parliament's Communications and Information Technology Committee on Tuesday. The government-drafted bill, which is composed of 45 articles and includes 29 penalties sentencing offenders to up to five years in prison or fines of between LE,10,000 and LE20 million, was referred by the legislature's speaker to the committee early this month and has largely been approved in principle. The bill's significance stems from the fact that, in the event that it is passed, it would be the first piece of legislation to regulate what is published on social media and establish principles to confront cybercrimes such as piracy and the hacking of private and government websites. Most importantly, the bill would set a precedent in regulating web censorship. The gap in opinion between detractors and proponents of the bill does not center so much on whether cybercrime legislation is necessary, however, but on protection of data and the broad leeway the legislation would grant to authorities to place limitations on liberty." READ MORE

Source: World Economic Forum

Date: 1 Mar 2018

Here is what's holding back Africa's digital revolution

"Cyberspace is Africa's new nervous system. From Algiers to Cape Town, the internet is changing people's lives and transforming economic sectors such as agriculture, banking and transport. The rapid adoption of smartphones combined with the world's youngest population have helped position Africa first on the global internet penetration growth ranking. Digital connectivity increased from 167.3 million people in 2012 to 412 million as of December 2017, hinting at a promising future. […] Africa's cyberspace is a hotbed of risk. Governments and private companies are facing an explosion of cyber threats. The wider public is affected by malware intrusions, financial cybercrime, phishing attacks and mass surveillance. Cybercrime in Africa is increasingly sophisticated, generating exorbitant financial losses. In 2016 alone, the cost of cybercrime was estimated at $2 billion […]. The situation is worsened by a lack of technology and skills to fend off such attacks." READ MORE

Source: Citizen TV

Date: 2 Mar 2018

Kenya, long jail terms and hefty fines for fake news and cyber bullying

"Generating and spreading fake news on social media could now land you in jail for at least five years, or leave you with millions of shillings to pay in court fines. This, if Parliament passes the Computer and Cyber Crime Bill. WhatsApp group administrators who condone sharing of fake news or information meant to incite ethnic hatred are also marked for severe punishment once the proposed law is enacted." READ MORE

Source: The Guardian

Date: 13 Mar 2018

Myanmar: UN blames Facebook for spreading hatred of Rohingya

"Facebook has been blamed by UN investigators for playing a leading role in possible genocide in Myanmar by spreading hate speech. Facebook had no immediate comment on the criticism on Monday, although in the past the company has said that it was working to remove hate speech in Myanmar and ban the people spreading it. More than 650,000 Rohingya Muslims have fled Myanmar's Rakhine state into Bangladesh since insurgent attacks sparked a security crackdown last August. Many have provided harrowing testimonies of murders and rapes by Myanmar security forces. The UN human rights chief said last week he strongly suspected acts of genocide had taken place. Myanmar's national security adviser demanded "clear evidence"." READ MORE

Source: The Guardian

Date: 13 Mar 2018

Muslim Cyber Army: a 'fake news' operation designed to derail Indonesia's leader

"Police in Indonesia believe they have uncovered a clandestine fake news operation designed to corrupt the political process and destabilise the government. In a string of arrests across the archipelago in recent weeks, authorities have revealed the inner workings of a self-proclaimed cyber-jihadist network known as the Muslim Cyber Army. The network is accused of spreading fake news and hate speech to inflame religious and ethnic schisms; fan paranoia around gay men and lesbians, alleged communists and Chinese people; and spread defamatory content to undermine the president." READ MORE

Source: Wion

Date: 1 Mar 2018

Is China curtailing freedom in the name of cybersecurity?

"The Great Firewall of China, not a physical barrier but a virtual one, prevents harmful information from entering the country. Apparently, it seems it was not enough as China's cyber administration has recently released a new cybersecurity law to tighten control and strengthen the oversight mechanism over Internet discussion. These regulations demand that all social media users register accounts only with proper identification; a prior censorship for all Internet comments in the form of first approve then post system; Internet companies to assist public security organisations in protecting national security, and allowing the state to establish undefined systems for cybersecurity monitoring. […] Moreover, China's refusal to accede to the Budapest Convention on Cyber Crime reflects its developing state-centric approach to international agreements on cyberspace." READ MORE

Source: INTERPOL

Date: 8 Mar 2018

INTERPOL study finds boys and very young children at greater risk of severe online sexual abuse

"A study of photos and videos in INTERPOL's International Child Sexual Exploitation (ICSE) database has found the younger the victim, the more severe the abuse was likely to be. A report published today by INTERPOL and ECPAT International also highlights the urgent need for better understanding of online exploitation and for more resources to be allocated towards victim identification. Information on more than one million media files of child sexual exploitation and abuse material from around the world and stored in the ICSE database was analyzed as part of the ground-breaking research." READ MORE

RELATED ARTICLES

INTERPOL/ ECPAT, Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material, February 2018

Latest reports

- European Commission, A multi-dimensional approach to disinformation, Report of the independent High level Group on fake news and online disinformation, 28 Feb 2018
- ICANN, Governmental Advisory Committee, GAC Communiqué ICANN 61, 15 Mar 2018
- M. Mann, I. Warren, S. Kennedy, The legal geographies of transnational cyber-prosecutions: extradition, human rights and forum shifting, Global Crime Journal, 9 Mar 2018
- FTR, ATM Fraud Prevention Framework, March 2018
- Kaspersky, The Slingshot APT, 6 March 2018
- McAfee, Hidden Cobra Targets Turkish Financial Sector With New Bankshot Implant, 8 Mar 2018

Upcoming events

- 15-16 March, Ljubljana, Slovenia – 2nd Western Balkans Integrative Internal Security Governance (IISG) Board Meeting, iPROCEEDS
- 16-18 March, Colombo, Sri Lanka – Residential workshop for District Judges and Magistrates on cybercrime and electronic evidence, GLACY+
- 19-23 March, Manila, Philippines – Introductory Training of Trainers (ToT) on cybercrime and electronic evidence for judges from the ASEAN Region, GLACY+
- 20-22 March, The Hague, the Netherlands – ECTEG General Assembly, GLACY+
- 21-22 March, Sarajevo, Bosnia and Herzegovina – Workshop for cybercrime units, economic crime units, financial investigators, FIU and specialised prosecutors on online financial fraud and credit card fraud, iPROCEEDS
- 21-23 March, Tunis, Tunisia – CyberSouth Launching Conference, CyberSouth
- 26-27 March, Dakar, Senegal – Advisory mission on the streamlining of procedures for mutual legal assistance related to cybercrime and electronic evidence, GLACY+
- 27-30 March, Chisinau, Moldova – Regional Meeting: Cybercrime Cooperation Exercise, Cybercrime@EAP 2018 / 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

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

www.coe.int/cybercrime