Cybercrime Digest

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

16-30 June 2019

Source: Council of Europe

Date: 21 Jun 2019

Benin invited to accede to the Budapest Convention on Cybercrime

"On 21 June 2019, Benin was invited to accede to the Budapest Convention on Cybercrime. Earlier this year, Benin received a visit of a delegation of the Cybercrime Convention Committee (T-CY) and held a workshop on the Budapest Convention which confirmed that the country has the necessary legislation and institutional capacity to join this treaty. In 2018, the Parliament of Benin had adopted the Code du Numérique in line with the Convention and its Protocol and has established specialised bodies for matters of cybercrime and electronic evidence. […] In total, 63 States are now Parties and another nine States have either signed or been invited to accede. At least another seventy countries have drawn on this treaty when developing domestic legislation." READ MORE

Source: Lawfare

Date: 21 Jun 2019

The Budapest Convention Offers an Opportunity for Modernizing Crimes in Cyberspace

"The Budapest Convention's member parties are in the process of negotiating a Second Additional Protocol, meant to address new and emerging criminal activities in cyberspace. Negotiations officially began in June 2017 and are currently scheduled to end in December 2019, though they may be extended beyond that point if required. The negotiations are focused on four areas: international cooperation among governments; cooperation between governments and private internet service providers; standards for access and security; and more general data protection requirements. To date, the protocol's drafting group has published provisional text for two articles on "emergency mutual assistance" and "language of requests." The drafting group is also discussing additional articles on video conferencing, an endorsement model for subscriber information requests, jurisdiction issues, direct cooperation with service providers, international production orders, extending searches and access based on credentials, joint investigations and joint investigation teams, and investigative techniques." READ MORE

Source: Council of Europe

Date: 20 Jun 2019

CyberEast: Action on Cybercrime for Cyber Resilience in the Eastern Partnership Region has launched

"Following exchange of signatures between the European Union and the Council of Europe in June 2019, the joint European Union / Council of Europe project "CyberEast: Action on Cybercrime for Cyber Resilience in the Eastern Partnership Region" has formally commenced on 20 June 2019. […] The CyberEast project will focus on improvement of legal framework and strengthening international and public/private cooperation – but also with added focus on areas of cybercrime policies and strategies; continuous training of law enforcement, prosecution and judiciary on matters of cybercrime and electronic evidence; and increased interagency cooperation between criminal justice and cybersecurity experts." READ MORE

Source: ENISA

Date: 27 Jun 2019

The European Union Agency for Cybersecurity - A new chapter for ENISA

"On Thursday 27 June 2019, the EU Cybersecurity Act (CSA) enters into force. ENISA will become the European Union Agency for Cybersecurity, with a new permanent mandate. […] The Agency is henceforth mandated to perform the following new tasks: (i) Cybersecurity certification; (ii) Cyber resilience; (iii) Policy; (iv) Vulnerability disclosure." READ MORE

RELATED ARTICLES

European Union, Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA, entered into force on 27 Jun 2019

Source: European Union External Action

Date: 21 Jun 2019

Joint Elements Statement on the Sixth EU-U.S. Cyber Dialogue

"On May 24, 2019, the United States hosted the European Union for the sixth U.S.-EU Cyber Dialogue in Washington, DC. Robert Strayer, Deputy Assistant Secretary for Cyber and International Communications Information Policy, U.S. Department of State, and Rory Domm, Acting Head of Division for Security and Defence Policy, European External Action Service, co-chaired the dialogue. […] The United States and the European Union reaffirmed the importance of the Budapest Convention as a basis for national legislation and international cooperation in fighting cybercrime. They welcomed the increasing number of states acceding to the convention and affirmed that no new legal instrument was necessary for addressing global cybercrime or global cyber issues. They exchanged information on their respective capacity building efforts to advance global capacities to tackle cybercrime and increase cyber resilience." READ MORE

Source: Government of Ghana

Date: 27 Jun 2019

Maiden Regional Conference on Data Protection and Privacy underway in Accra

"The maiden Africa Regional Data Protection and Privacy Conference on the theme "A Conference in Africa, by African Authorities, Focused on Africa", is underway in Accra. The week-long conference, which was formally opened on behalf of Vice President Dr. Mahamudu Bawumia by Professor George Gyan-Baffour, the Planning Minister, is being attended by heads of Data Protection Agencies from across Africa. It is worth noting that in Africa, less than 15 out of the 54 countries in the region have passed a Data Protection Law; the digital divide and knowledge deficit of the subject area have global implications and impact on the protection of individuals. The recently modernised Council of Europe's Convention 108+ on data protection is the legal binding instruments that had been for decades, the international best practice standard open to all countries in the world. The conference is being hosted by the Ghana Data Protection Commission in collaboration with the Network of African Data Protection Authorities and the Ministry of Communication. Its objective is to create a platform for experts to discuss how Africa as a region rises to the challenge of the Global Data Protection, which is the safeguarding of personal data as a fundamental human right." READ MORE

RELATED ARTICLES

GhanaWeb, Ghana preparing to accede to Convention 108+, 27 Jun 2019

Source: Le Monde

Date: 25 Jun 2019

Facebook transmettra plus rapidement à la justice les adresses IP d'auteurs de messages haineux

"Facebook s'est engagé à transmettre, via une procédure accélérée, les adresses IP (Internet Protocol, l'adresse d'une machine connectée à Internet) permettant d'identifier les auteurs de messages appelant à la haine, a annoncé le secrétaire d'Etat au numérique, Cedric O, dans un entretien à l'agence Reuters. « Ils nous ont annoncé que (…), eu égard aux discussions qu'ils ont eues avec nous, ils allaient transmettre les adresses IP pour les contenus de haine en ligne qui seraient demandées par la justice. Ce qui est une énorme nouvelle, a dit M. O. Jusqu'ici, quand la justice française demandait des adresses IP, Facebook ne les donnait que s'il s'agissait de dossiers relevant du terrorisme ou de la pédopornographie. » En réalité, Facebook transmettait bien déjà les adresses IP, pour tous les types de dossiers, lorsqu'elles étaient demandées par la justice française. Mais la procédure, qui passe par une demande d'entraide internationale auprès des autorités américaines, est lourde et lente. Le réseau social s'est désormais engagé à transmettre les adresses IP d'auteurs de messages haineux via une procédure simplifiée, similaire à celle déjà en place pour les dossiers de terrorisme et de pédopornographie, explique-t-on au cabinet de M. O. Ces informations seront fournies volontairement par Facebook." READ MORE

Source: The Guardian

Date: 18 Jun 2019

Libra: Facebook launches cryptocurrency in bid to shake up global finance

"Facebook has announced a digital currency called Libra that will allow its billions of users to make financial transactions across the globe, in a move that could potentially shake up the world's banking system. Libra is being touted as a means to connect people who do not have access to traditional banking platforms. With close to 2.4 billion people using Facebook each month, Libra could be a financial game changer, but will face close scrutiny as Facebook continues to reel from a series of privacy scandals." READ MORE

RELATED ARTICLES

Libra, An Introduction to Libra, 18 Jun 2019

Source: Reuters

Date: 18 Jun 2019

U.N. surveillance expert urges global moratorium on sale of spyware

"David Kaye, the U.N. special rapporteur on freedom of expression, submitted his recommendations in a report published on Tuesday to the U.N. Human Rights Council, which will open a three-week session next week. Kaye said he had received detailed testimony about governments using spyware developed and supported by private companies, but the market was shrouded in secrecy. "Surveillance of specific individuals – often journalists, activists, opposition figures, critics and others exercising their right to freedom of expression – has been shown to lead to arbitrary detention, sometimes to torture and possibly to extrajudicial killings," he wrote. "States should impose an immediate moratorium on the export, sale, transfer, use or servicing of privately developed surveillance tools until a human rights-compliant safeguards regime is in place." READ MORE

Source: DFR Labs

Date: 23 Jun 2019

Suspected Russian intelligence operation worked across platforms to spread lies and impersonate political figures

"A Russian-based information operation used fake accounts, forged documents, and dozens of online platforms to spread stories that attacked Western interests and unity. Its size and complexity indicated that it was conducted by a persistent, sophisticated, and well-resourced actor, possibly an intelligence operation. The operation shows online platforms' ongoing vulnerability to disinformation campaigns. Far more than on Facebook, which exposed it, or Twitter, the operation maintained fake accounts on platforms such Medium and Reddit, and online forums from Australia to Austria and from Spain to San Francisco. Its level of ambition was very high, but its impact was almost always low." READ MORE

RELATED ARTICLES

DFR Labs, Russian Op 6: EU elections, 23 Jun 2019

Source: Institute for Security Studies – Africa

Date: 26 Jun 2019

Is Africa cybercrime-savvy?

"Africa needs to be better prepared for both cyber-dependent crimes, in which new computer-based technologies form the basis of new crimes, and cyber-enabled crimes, in which new technologies are used to commit old-style crimes, such as money laundering. In more developed economies there's been an increase in attacks from 'hacktivists' who use the dark arts of cyber to embarrass, advocate or protest. According to cyber analytics firm Kaspersky Lab, there are 13 842 cyber attacks daily in South Africa. That equates to more than 570 attacks every hour. Bank fraud, particularly the use of malware on mobile phones, has also increased dramatically, says the South African Banking Risk Information Centre. […] Just four African states have ratified the [Malabo] convention [of the African Union], limiting its enforcement power. The same goes for the Budapest Convention, widely considered the global 'Gold Standard'. Only Cabo Verde, Ghana, Mauritius, Morocco and Senegal have incorporated it into national law. Countries such as South Africa, which has not yet ratified, are preferring to go it alone." READ MORE

Source: Daily Trust

Date: 18 Jun 2019

Nigeria, Lawyers, others fault Cybercrimes Act

"The Cybercrime (Prohibition, Prevention etc.) Act 2015, was passed into law in May 2015 to among others, prevent the use of the internet for perpetuation of various forms of cyber offences. Before its passage, Nigeria failed to enact any laws regulating cybercrimes. […] The opponents said that there is a window of judicial intervention since two cases have travelled up to the apex court, including Okedara's case. The participants at the parley said the act was copied hook, line and sinker from the United Kingdom Postal Act of 1918, adding that the bill creating the Act was passed in a hurry by the National Assembly to avoid delay. They unanimously declared the Nigeria's Cybercrimes Act as "repressive, oppressive and unconstitutional," adding that "The Act should immediately be repealed or dropped, as many of its provisions blatantly offend the rights to freedom of expression, association and media freedom." The act prescribes death penalty for an offence committed against a system or network that has been designated critical national infrastructure of Nigeria […]" READ MORE

Source: Forbes

Date: 18 Jun 2019

NASA confirms that its Jet Propulsion Laboratory has been hacked

"The U.S. National Aeronautics and Space Administration (NASA) this week confirmed that its Jet Propulsion Laboratory (JPL) has been hacked. An audit document from the U.S. Office of the Inspector General was published by NASA this week. It reveals that an unauthorized Raspberry Pi computer connected to the JPL servers was targeted by hackers, who then moved laterally further into the NASA network. How much further? Well, the hackers apparently got as far as the Deep Space Network (DSN) array of radio telescopes and numerous other JPL systems. The extent of the breach, which happened in April 2018, was such that the Johnson Space Center, with responsibility for programs including the International Space Station, decided to disconnect from the gateway altogether." READ MORE

Source: Reuters

Date: 26 Jun 2019

Hackers hit global telcos in espionage campaign

"Hackers have broken into the systems of more than a dozen global telecoms companies and taken large amounts of personal and corporate data, researchers from a cyber security company said on Tuesday, identifying links to previous Chinese cyber-espionage campaigns. Investigators at U.S.-Israeli cyber security firm Cybereason said the attackers compromised companies in more than 30 countries and aimed to gather information on individuals in government, law-enforcement and politics." READ MORE

Source: NetBlocks

Date: 22 Jun 2019

Internet shutdown in Ethiopia amid reports of attempted coup

"Ethiopia's internet has been largely disconnected starting 8:15 p.m. UTC Saturday 22 June 2019 and having nationwide impact as of 9:00 p.m. UTC, as reports emerge of an attempt to unseat the regional government in Bahir Dar, Amhara state, north of capital Addis Ababa. Real-time network data show that national IP connectivity dropped to 2% of normal levels as the Prime Minister's secretariat appeared live on Ethiopian Television to explain, "armed men tried to unseat the Amhara Regional State Government by force but their attempt has been foiled."." READ MORE

Source: ContraReplica

Date: 21 Jun 2019

Mexico, exhortan a tipificar violencia de género y acoso en internet

"La Comisionada Ciudadana del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México (INFO), Elsa Bibiana Peralta Hernández, se pronunció por tipificar las conductas de violencia de género y acoso en Internet. Lamentó que las Tecnologías de la Información y Comunicación (TIC) sean utilizadas para cometer muchos crímenes, pero "más allá de condenar al medio que es el Internet, se debe castigar y tipificar las conductas y motivaciones de las personas que realizan estos ilícitos". […] Por ello, hizo un llamado para que México firme y se sume al Convenio de Budapest que tiene como propósito enfrentar los delitos informáticos en Internet, así como los fraudes, la pornografía infantil, la incitación al odio o las violaciones de seguridad de la vida privada, entre otros." READ MORE

Source: Europol

Date: 21 Jun 2019

EC3 Advisory Groups – LE and Private Sector Meetings to Discuss Latest Cybercrime Threats and Challenges

"Europol's European Cybercrime Centre (EC3) continues to strengthen its work with the private sector in the joint fight against cybercrime. This week, EC3's three industry Advisory Groups met at Europol in The Hague to discuss the latest cyber-related threats and trends, including 5G, new forms of online payments, and attacks against critical infrastructure. The goal of the Advisory Groups is to provide a forum for LE and the private sector to cooperate on cybercrime-related threats and challenges, fostering collaboration on both a strategic and operational level." READ MORE

Latest reports

- European Union Agency for Fundamental Rights, Cybercrime and Fundamental Rights – 2nd Expert meeting – Summary outcome, June 2019
- European Union Agency for Fundamental Rights, Widespread data protection abuses highlighted by GDPR, 21 Jun 2019
- Mondaq, Analyzing The Impact Of The EU GDPR On Access To WHOIS Data, One Year On, 19 Jun 2019
- Mondaq, Egypt: The New Egyptian Anti-Cybercrime Law Regulates Legal Responsibility For Web Pages And Their Content, 21 Jun 2019
- Stanford University, Securing American Elections, June 2019
- Trend Micro, Crimeware for Sale: The Commoditization of ATM Malware in the Cybercriminal Underground, 28 Jun 2019
- HackRead, How Phishing Has Evolved in 2019, 26 Jun 2019
- Hosting Tribunal, 15 of the Biggest Data Breaches in The Last 15 Years, 27 Jun 2019

Upcoming events

- 1 – 3 July, El Salvador – Advisory mission and workshop on legislation during Forum of Presidents of Legislative Powers of Central America and the Caribbean Basin (FOPREL), GLACY+
- 8 July, Brussels, Belgium – Study visit of Sri Lankan judges to Belgium and workshop on cybercrime and electronic evidence, GLACY+
- 8 – 11 July, Strasbourg, France – Participation in the 21st T-CY plenary and 4th PDP plenary, iPROCEEDS, CyberSouth, GLACY+
- 9 July, Strasbourg, France – 3rd Project Steering Committee, CyberSouth
- 10-12 July, Strasbourg, France – First International Meeting of the national trainers on cybercrime and electronic evidence, iPROCEEDS, CyberSouth, GLACY+
- 15-18 July, Nigeria - Development of Cybercrime Investigation Unit and Data Forensics Unit, 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

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE