

Cybercrime Digest

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

16-31 August 2017

Source: Council of
Europe

The Budapest Convention and its explanatory report finally available in Arabic

Date: 16 Aug 2017

"Within the framework of CyberSouth, the Budapest Convention on Cybercrime and its explanatory report have been translated in Arabic. This is a first step before the launching of activities. The European Union/Council of Europe funded project officially started on 1 July 2017. The Additional Protocol on racism and xenophobia and its explanatory report are also available in Arabic now." [READ MORE](#)

Source: Presidencia
de la Republica de
Colombia

Colombia, Gobierno presentó proyecto de ley para adherir al Convenio de Budapest contra la ciberdelincuencia

Date: 16 Aug 2017

"El Gobierno Nacional, en cabeza de la Cancillería y los Ministerios de Justicia, Defensa y Tecnologías de la Información y las Comunicaciones (TIC), presentó al Congreso de la República un proyecto de ley para que Colombia se adhiera al Convenio de Budapest, que busca construir una política mundial común contra la ciberdelincuencia. El proyecto de ley comenzará su trámite legislativo en la Comisión Segunda del Senado y una vez cursados los cuatro debates en el Congreso, pasará a revisión de la Corte Constitucional y posteriormente a sanción presidencial. Luego, la Cancillería hará oficial la adhesión al convenio, que le permitirá a Colombia no solo avanzar en temas de cooperación internacional contra delitos informáticos, sino también fortalecer las leyes y regulaciones nacionales contra el ciberdelito en todos los niveles." [READ MORE](#)

Source:
Independent

Ireland a 'prime target' for cyber-criminals

Date: 19 Aug 2017

"Ireland is dangerously vulnerable to cyber-crime according to Fianna Fail Seanad Spokesperson for Justice, Children and Youth Affairs and Fingal representative, Senator Lorraine Clifford Lee. Senator Clifford Lee said has said that despite cyber-crime growing at an unprecedented rate worldwide, the Government's poor response leaves Ireland as a prime target for cyber-hackers and criminals. New figures released to Fianna Fáil indicate that there has been a further decrease in numbers allocated to the Garda Cyber Crime Bureau. In 2016 there were 29 Gardaí tasked with policing cyber crime, that has now fallen to 23." [READ MORE](#)

Source:
112.International

Security Service of Ukraine warns about cyber-attack on Ukrainian institutes and enterprises

Date: 18 Aug 2017

"The Security Service of Ukraine warns about possible cyber-attack on the networks of the Ukrainian institutes and enterprises and asks to stick to the worked out recommendations as the press service of the department reported. A large-scale cyber attack hit dozens of companies and enterprises across Ukraine on June 27 due to the usage of the malicious software identified as Pety.A virus. It was established during the analysis of the consequences that the data harvesting about the Ukrainian enterprises (e-mails, passwords of the accounts used by the enterprises and the workers, access

details of the command and control servers and hash data of the account in the attacked systems and other confident information), hiding of it in the cookies files and mail of it to the command server preceded the cyber attack. The SBU specialists think that exactly this data was the aim of the first wave of the cyber-attack and it can be used by the real initiators for cyber intelligence or further attacks." [READ MORE](#)

Source: Jerusalem
On Line

Israel Police Commissioner declares launch of cyber-crime unit to combat pedophilia

Date: 30 Aug 2017

"Israel Police Commissioner Roni Alsheikh declared the launch of a cyber-crime unit today: "The police will be everywhere youth are found – Facebook, Twitter and Snapchat." Alsheikh also revealed that tens of thousands of Israelis downloaded pedophilic content to their computers." [READ MORE](#)

Source: Republic of
Mauritius

Cabinet agrees to the adoption and implementation of the Cybercrime Strategy in Mauritius

Date: 25 Aug 2017

"Cabinet has agreed to the adoption and implementation of the Cybercrime Strategy, which is in line with the requirements of the Budapest Convention on Cybercrime, to strengthen the capacity of law enforcement agencies to detect, handle and prosecute cybercriminals, and the Judiciary to better address the issue whenever cases are brought before Courts." [READ MORE](#)

Source: Daily FT

National cyber security strategy in Sri Lanka to amp up defense in cyberspace

Date: 31 Aug 2017

"The Government is looking to make substantial investments in cyber security in the coming months under a freshly formulated national cyber security strategy, a senior Cabinet Minister revealed yesterday. Speaking at the 10th Annual National Conference on Cyber Security in Colombo, Telecommunications and Digital Infrastructure Minister Harin Fernando said the country's relatively high internet and smartphone penetration rates and the cost of a successful attack are at the heart of the Government's decision to develop a national strategy on cyber security. [...] Noting that that the Council of Europe has named Sri Lanka their training and capacity building hub under the Budapest Convention's Cybercrime Conventions Committee, the Minister went on to say that cyber crime remains a global challenge." [READ MORE](#)

Source: Council of
Europe

Special program on cybercrime and e-evidence for the judiciary in Nepal delivered by Sri Lankan trainer-justices

Date: 20 Aug 2017

"Organized under the GLACY+ framework, on the initiative of the National Judicial Academy of Nepal and of the Sri Lanka Judges' Institute, the Special Program on cybercrime and electronic evidence for Nepalese judges represents the first regional experience of judicial training on cybercrime in South Asia, where a group of selected and experienced Justices from Sri Lanka, already accredited trainers on the national level, committed to share their knowledge and expertise with colleagues from Nepal, on the basis of the GLACY+ training modules." [READ MORE](#)

Source: *La Tercera*

Ley de ciberdelitos de Chile será actualizada en base al Convenio de Budapest

Date: 16 Aug 2017

“Gobierno prepara proyecto que será enviado al Congreso para adecuar normas tras la entrada en vigencia este mes de la convención de Budapest contra el cibercrimen. Para cambiar legislación actual, que data de 1993, se sumarán ocho conductas criminales, como la captación y divulgación de imágenes obtenidas sin autorización. [...] “El proyecto es el primer esfuerzo de magnitud que se desarrolla por actualizar una normativa que data de 1993, cuando internet era una novedad, cuando no había comercio electrónico en Chile y cuando las tarjetas de crédito eran un lujo. Así, hoy, además de tener la tasa de penetración de internet más alta de Latinoamérica, tenemos 37 millones de tarjetas de crédito y débito bancarias, con más de 1.700 millones de transacciones por año”, señala el subsecretario Mahmud Aleuy, quien agrega que contar con una tipificación de delitos más precisa contribuye a perseguir criminal y más eficientemente a los responsables.” [READ MORE](#)

Source: *Republica del Paraguay*

Paraguay, apuntan a atacar delitos cometidos por medios informáticos

Date: 29 Aug 2017

“La comisión de Ciencia y Tecnología, que preside el diputado Asa González (PLRA-Misiones), dictaminó favorablemente con respecto a la “Convención sobre la ciberdelincuencia” [...]. La exposición de motivos, remitida por el Poder Ejecutivo, junto al proyecto de convención, resalta la importancia del compromiso entre los Estados Partes, de emprender y concretar acciones puntuales que han sido identificadas como claves para la lucha contra la ciberdelincuencia, y que involucran a múltiples actores y sectores del mismo, cada uno desde un ámbito de acción. Además, resalta que la convención sobre ciberdelincuencia dará a nuestro país un respaldo formal para las colaboraciones que podamos requerir de los Estados Partes, a fin de mitigar los incidentes de ciberseguridad que se detecten y que eventualmente estén ocasionando daño al Estado paraguayo y/o ciudadanía paraguaya.” [READ MORE](#)

Source: *The News Guru*

Cybercrimes cannot continue in Nigeria, Minister of Communication says

Date: 29 Aug 2017

“The Minister of Communication, Adebayo Shittu, has lamented the spate of cybercrimes rocking nations, saying the menace cannot be allowed to thrive in Nigeria. [...] He said government will continue to provide appropriate law enforcement response, as well as information and education to the population regarding the threats on the internet. “However, at the same time, we also expect providers of services to play their part by providing those who feel threatened with support and information and with links to law enforcement bodies. [...] In 2015, the federal government passed the national cybersecurity act into law which provides directives to guide regulate and protect the use and deployment of critical information infrastructure in the Nation. The bill describes classes of cybercrime and also includes robust clauses for criminal prosecution following cybersecurity crimes.” [READ MORE](#)

RELATED ARTICLES

IT News Africa, [Cyber security awareness a key priority in Nigeria](#), 28 Aug 2017

Source: NetRich

India's Cybersecurity Challenge

Date: 16 Aug 2017

"India has come some way toward implementing security regulations in specific verticals, along with a couple of key regulations across the board. The watershed regulation was the IT Act 2008. This amended an original 2000 Act, adding specific information security and privacy measures. It also labeled cybercrime a punishable offense under the Indian Penal Code. In 2011, the Reserve Bank of India (RBI) introduced a set of recommendations, including the formation of separate information security groups within banks. [...] Most recently, India's new national cyber security policy set out plans for an effective IT security framework throughout the country, and includes several priorities. A 24/7 mechanism for cybersecurity emergency response is among these, creating situational awareness regarding threats to information and communications technology infrastructure. The policy also promises a legal framework for safe operations in cyberspace." [READ MORE](#)

RELATED ARTICLES

Hindustan Times, [10,000 cybercrime cases, only 34 convictions in Maharashtra between 2012 and 2017](#), 21 Aug 2017

Source: Agence de Presse Africaine

Cybercriminalité : La Banque centrale du Kenya lance un ultimatum aux institutions bancaires

Date: 23 Aug 2017

"La Banque centrale du Kenya (CBK) a lancé mercredi un ultimatum aux banques kenyanes afin qu'elles présentent, au plus tard le 30 novembre, leurs politiques en matière de cybersécurité. La CBK a déclaré que les banques devraient définir leurs stratégies, politiques, procédures et activités connexes visant à atténuer le cyber-risque et, par la suite, créer un cyberspace plus sûr et plus sécurisé qui soutient les priorités en matière de sécurité du système d'information et favorise la stabilité du secteur bancaire kenyan. Selon le rapport 2016 sur la cybersécurité en Afrique, le Kenya est le pays le plus touché par la cybercriminalité en Afrique de l'est, le pays ayant perdu 171 millions de dollars l'année dernière, suivi de la Tanzanie, qui a perdu 85 millions de dollars, tandis que l'Ouganda a perdu 35 millions." [READ MORE](#)

Source:
ZimDeveloper

The continental context behind the development of Zimbabwe's ICT laws

Date: 18 Aug 2017

"There has been renewed interest in Zimbabwe in regard to its draft Computer Crime and Cybercrime Bill, which has been criticised for its provisions that violate fundamental rights such as the right to privacy, the right to freedom of speech and the right to access information. [...] According to a 2014 discussion paper sent to the Cybercrime Convention Committee, a committee that represents the State Parties to the Budapest Convention on Cybercrime, the ITU-EU model laws: 'appear to be sourced from a draft prepared by ITU consultants who attempted to use the general framework and much of the language from the Commonwealth Model Law but with substantial modifications, additions and deviations from international best practice. In particular, introducing provisions that would raise human rights and freedom of speech concerns, enable content control, and regressive powers without safeguards which substantially impact industry, online providers and users' [...]." [READ MORE](#)

Source: *The Horn Observer*

Somalia: Senate Passes National Communication Act

Date: 21 Aug 2017

"The Upper House of Somalia's parliament has on Monday passed the National Communications Act, highlighting the first act that is approved by this new House to Somalia's legislative system, amid the Ministry opened a post office in Djibouti, following bilateral agreement recently signed, officials said. [...] Somali Ministry of Posts said in a statement that "the law will help the government increase revenues and contribute to security. It will also improve rights of the consumers and attract more investment for the sector, among other benefits." [READ MORE](#)

Source: *Bloomberg Technology*

Cryptocurrency Cyber Crime Has Cost Victims Millions This Year

Date: 24 Aug 2017

"Here's another reason to be leery of the initial coin offerings being done at a staggering pace in the cryptocurrency world: there's a one-in-10 chance you'll end up a victim of theft. Phishing scams have helped push up criminal losses to about \$225 million this year, according to Chainalysis, a New York-based firm that analyzes transactions and provides anti-money laundering software. In such scams, investors are tricked into sending money to internet addresses pretending to be funding sites for digital token offerings related to the ethereum blockchain technology. More than 30,000 people have fallen prey to ethereum-related cyber crime, losing an average of \$7,500 each, with ICOs amassing about \$1.6 billion in proceeds this year, Chainalysis estimates." [READ MORE](#)

RELATED ARTICLES

Coin Journal, [India Continues to Ponder Bitcoin Regulations as Cybercrime Soars](#), 25 Aug 2017

Source: *Reuters*

Turkey hunts more coup suspects, detains 30 for suspected PKK links

Date: 15 Aug 2017

"Turkish police have launched operations to track down 33 former staff of a national scientific research agency who are alleged to have been involved in last year's failed coup attempt, the state-run Anadolu news agency said on Tuesday.

Anadolu said the suspects were alleged to have used ByLock, an encrypted messaging app which the government says was used by the network of U.S.-based cleric Fethullah Gulen, whom it accuses of orchestrating the abortive putsch in July 2016."

[READ MORE](#)

Source: *MIS Asia*

Asia Pacific records 45 percent growth in cybercrimes

Date: 23 Aug 2017

"The Asia Pacific region has seen a 45% growth in cybercrime year-on-year, according to the newly released ThreatMetrix Cybercrime Report. Findings indicated that the attack levels have increased globally and cybercriminals have begun to target emerging digital business models, such as ride-sharing apps and media streaming organisations. The Asia Pacific region was found to experience strong growth in organised attacks that primarily focus on account takeovers and payment fraud. The region also has the highest instance of device spoofing and identity spoofing." [READ MORE](#)

Source: *China Law Blog*

Date: 16 Aug 2017

China Establishes Its First Cyber-Court in Hangzhou

"China has adopted a plan to establish a cyberspace court in Hangzhou lately. The plan is for this court to accept filings electronically, try cases via livestream and hear only e-commerce and Internet related cases. As a general rule of Chinese civil procedure law, lawsuits must be brought in the place of the defendant's domicile. For companies, domicile means their principal place of business or the place where it has its registered address. Hangzhou is home to Alibaba and to many other technology companies, it has been dubbed the "capital of Chinese e-commerce," and it is the site of the China Cross-Border E-Commerce Comprehensive Test Zone. Hangzhou courts have experienced a considerable increase in the number of e-commerce related cases, from 600 cases accepted in 2013 to more than 10,000 in 2016." [READ MORE](#)

Latest reports

- European Parliament, Committee on Civil Liberties, Justice and Home Affairs, [Report on the fight against cybercrime](#), 26 Jul 2017
- ENISA, [Supply Chain Attacks](#), 29 Aug 2017
- Estonian Information System Authority, [Annual Cyber Security Assessment 2017](#), August 2017
- Global Security Review, [How is Cyber Warfare Conceptualized in International Law?](#), 27 Aug 2017
- Akamai, [DDoS attacks are back on the rise](#), 21 Aug 2017

Upcoming events

- 7-8 September, Kyiv, Ukraine – Visits on memorandum of cooperation: finalization of text, [Cybercrime@EAP III](#)
- 9-10 September, Odessa, Ukraine – Presentation of draft memorandum at Telecom meeting in Odessa, [Cybercrime@EAP III](#)
- 11-12 September, Chisinau, Moldova – Regional meeting on safeguards, guarantees and legislation, plus hearing of two reports prepared by C-PROC, [Cybercrime@EAP III](#)
- 11-13 September, Abuja, Nigeria – Regional meeting in the ECOWAS region in view of sharing good practices and promote harmonisation of legislation on Cybercrime and E-Evidence, [GLACY+](#)
- 14 September, Chisinau, Moldova – Discussion on Law reform implementing the Joint Opinion of the VC/DGI, [Cybercrime@EAP III](#)

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

