# Cybercrime Digest

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

1-15 March 2019

*Source: Council of Europe*

*Date: 8 Mar 2019*

## San Marino joins the Budapest Convention and its Protocol on Xenophobia and Racism

"San Marino deposited the instrument of ratification of the Budapest Convention on Cybercrime and its Additional Protocol on Xenophobia and Racism. With San Marino, the Convention on Cybercrime has now 63 Parties. A further 8 States have signed it or been invited to accede."

RELATED ARTICLES

Council of Europe, State of signatures, ratifications and accessions to the Budapest Convention on Cybercrime and its Protocol on Xenophobia and Racism, 8 Mar 2019

---

*Source: New Europe*

*Date: 13 Mar 2019*

## European Parliament adopts Cybersecurity Act

"European parliamentarians approved at the Strasbourg plenary a certification on cybersecurity for products, processes, and services sold in EU countries and, in a separate resolution, expressed concern over the threat that Chinese technology poses to data protection. In addition to the certification system, the EU gave the go-ahead for an extension of the mandate of the EU Agency for Cybersecurity and decided to allocate more resources to carry out its tasks. The resolution highlighted Europe's growing concern about China's market position in the development of 5G infrastructure equipment, which is sold on the international market by telecom giant Huawei. Worries about Huawei stem from a widely-held belief that the Chinese security services and other Chinese manufacturers have designed programmes that can gain unauthorised access to personal data and telecommunications information. The European Members of Parliament called on the Commission and all EU members to provide guidance on how to combat cyber-threats." READ MORE

---

*Source: KOACI*

*Date: 12 Mar 2019*

## Côte d'Ivoire : Vers la ratification de la Convention de Budapest sur la cybercriminalité

"Abidjan abrite depuis ce mardi l'Atelier d'information sur la Convention de Budapest sur la cybercriminalité, dans la perspective de sa ratification par la Côte d'Ivoire. Le Ministre de l'Economie Numérique et de la Poste, Monsieur Claude Isaac DE a souligné que cette convention est un formidable instrument de lutte contre la cybercriminalité, comme rapporté par ses services. Il a exhorté les participants à se pencher sur tous aspects relatifs à la lutte contre la cybercriminalité, afin d'orienter les décisions de l'Etat ivoirien pour commencer sa ratification. Aussi, a-t-il rassuré le Conseil de l'Europe de sa disponibilité et de l'ensemble des parties prenantes à travailler « d'arrache-pied » en vue de l'adhésion de la Côte d'Ivoire à la Convention de Budapest. […] Pour sa part, le Secrétaire Exécutif du Comité de la Convention sur la cybercriminalité du Conseil de l'Europe, Alexander SEGER, a fait observer que parce que les TIC sont utilisées dans tous les domaines de la vie, la sécurité des individus et des organisations est affectée par la cybercriminalité." READ MORE

*Source: Council of the European Union*

*Date: 8 Mar 2019*

## E-evidence package: EU agrees on rules to appoint legal representatives for the gathering of evidence

"The EU is taking steps to improve cross-border access to e-evidence by creating a legal framework that will enable judicial orders to be addressed directly to service providers operating in the EU. The Council today reached its position on the directive on the appointment of legal representatives for the gathering of evidence in criminal proceedings. This directive will be an essential tool for the application of the future regulation on European production and preservation orders for electronic evidence in criminal matters, on which the Council adopted its position last December, as it sets out the rules for the appointment of service providers' legal representatives, whose role is to receive and respond to such orders. The creation of legal representatives was necessary because of the lack of a general legal requirement for non-EU service providers to be physically present in the Union when providing services within the Union. Moreover, the legal representatives designated under this directive could be used for domestic procedures as well." READ MORE

*Source: SELEC – Southeast European Law Enforcement Center*

*Date: 14 Mar 2019*

## Kick-off meeting for updating the curricula of the European Cybercrime Training and Education Group

"The Cybercrime Program Office of the Council of Europe and the Southeast European Law Enforcement Center (SELEC) organized the kick-off meeting for updating the curricula of the European Cybercrime Training and Education Group (ECTEG), Training on Darkweb and virtual currencies investigations, under the EMPACT OAP 2019. The kick-off meeting took place in the period 11-13 March 2019 at SELEC's Headquarters in Bucharest, Romania and gathered 15 law enforcement officers from Austria, Belgium, Spain and Norway, as well as representatives from Council of Europe, Europol, Interpol and UNODC. […] The meeting focused on the update and upgrade of the existing training package on Darkweb and virtual currencies investigations that will be used for the upcoming pilot trainings." READ MORE

*Source: New York Times*

*Date: 13 Mar 2019*

## Facebook's data deals under criminal investigation

"Federal prosecutors are conducting a criminal investigation into data deals Facebook struck with some of the world's largest technology companies, intensifying scrutiny of the social media giant's business practices as it seeks to rebound from a year of scandal and setbacks. A grand jury in New York has subpoenaed records from at least two prominent makers of smartphones and other devices, according to two people who were familiar with the requests and who insisted on anonymity to discuss confidential legal matters. Both companies had entered into partnerships with Facebook, gaining broad access to the personal information of hundreds of millions of its users. The agreements, previously reported in The New York Times, let the companies see users' friends, contact information and other data, sometimes without consent. […] The sharing deals empowered Microsoft's Bing search engine to map out the friends of virtually all Facebook users without their explicit consent, and allowed Amazon to obtain users' names and contact information through their friends. Apple was able to hide from Facebook users all indicators that its devices were even asking for data." READ MORE

*Source: EU Neighbors*

*Date: 7 Mar 2019*

## Cybercrime, a Georgian prosecutor on challenges and EU support

"Cyber blackmail, internet scams, dissemination of private videos, hacking of private bank accounts and theft – these are just some of the cases on which Mariam Gogoreliani, supervising prosecutor of the Prosecutor's Office of Georgia, has been working since 2015. Fighting cybercrime within a single country is actually impossible, says the prosecutor, which is why she considers "Cybercrime@EaP" an important project. The project was a joint EU and Council of Europe initiative aimed at researching cybercrime and electronic evidence threats, challenges and strategies in the Eastern Partnership (EaP) region and improving cooperation. "Sometimes this cooperation was one of the most important mechanisms for the investigation of a case," says Gogoreliani." READ MORE

*Source: Politica Nacional de Ciberseguridad*

*Date: 13 Mar 2019*

## Chile, Senado aprueba nueva norma por delitos informáticos

"En concreto, el proyecto tipifica en un cuerpo normativo específico los ilícitos penales informáticos, adecuando los actuales a los términos del Convenio de Budapest y agregando otros nuevos; entrega las normas procedimentales para la persecución y juzgamiento de tales delitos; define los conceptos comunes a estos tipos, modifica el Código Procesal Penal y la ley sobre Responsabilidad Penal de las Personas Jurídicas, estableciendo obligaciones y procedimientos para hacer efectiva la dificultosa investigación de estos ilícitos. De la misma forma, la nueva legislación introducirá nuevos tipos penales como la falsificación y el fraude informático, así como el abuso de dispositivos." READ MORE

*Source: The Japan Times*

*Date: 7 Mar 2019*

## Cybercrimes in Japan edge up to record high, with over 2,000 child porn and prostitution cases

"The number of cybercrimes confirmed by police nationwide in 2018, including many cases of child pornography and fraud, stood at 9,040, rising slightly to reach a record high for the third consecutive year, National Police Agency data showed. The figure was up by just 26 from a year before, but it marked an increase of more than 1,000 from 2014. The situation "remains serious," NPA official said. Among the 9,040 cybercrimes, the highest number, 2,057, were related to child prostitution and child pornography, followed by 972 cases of fraud and 926 related to juveniles, such as sexual misconduct involving youth age 18 or younger through online dating." READ MORE

*Source: Mailife*

*Date: 8 Mar 2019*

## Attorney General of Fiji: Build Our ICT Capacity Or We Will Get Left Behind

"We have, of course, cyber-crime. We have had cyber-attacks, generally in the financial systems. Our own people needed to be better trained and educated in this capacity so we could deal with these issues, he said. "We have drafted Fiji's first national cyber security strategy after various consultations." He said, adding that Fiji was also making its way into the Budapest Convention, an international treaty seeking to address Internet and computer crime by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations." READ MORE

*Source: Amnesty International*

*Date: 1 Mar 2019*

## Iraq: Draconian cybercrimes law threatens freedom of expression

"A new cybercrimes law that would impose heavy prison sentences and hefty fines against peaceful critics who express themselves online would be a devastating setback for freedom of expression in Iraq, Amnesty International said today. The organization has highlighted its serious concern over the draft "Law on Information Technology Crimes" in an open letter signed by nine other NGOs. The letter was submitted to the Iraqi authorities this morning and warns that the proposed law would "establish a climate of self-censorship in the country." "If passed, this draconian cybercrime law will be a devastating blow for freedom of expression in Iraq. The vague and overly broad wording of the law means it could easily become a tool for repression in a country where the space for critical voices is already severely restricted," said Razaw Salihy, Iraq researcher at Amnesty International. The proposed law would criminalize acts that fall under freedom of expression and give Iraqi authorities excessive powers to impose harsh sentences, including life imprisonment, for vaguely worded offences such as undermining the country's "independence, peace and political, military security and economic interests". READ MORE

*Source: Bloomberg*

*Date: 13 Mar 2019*

## Thailand's Cyber Law Raises Fear Military Could 'Cage' the Internet

"Critics say the broad and vague language in the Cyber Security Bill -- passed by the country's unelected lawmakers on Feb. 28 -- may give the current military government powers to seize data and electronic equipment without proper legal oversight. The law will come into effect once it is published in the Royal Gazette, the timing of which is unclear. […] In the event of a cyber threat to national security, the new bill allows a watchdog committee headed by the prime minister to seize computers, servers and data without a court order, according to the latest version of the law posted on the Senate's website. […] The Asia Internet Coalition, an industry organization that represents companies such as Alphabet Inc., Amazon.com Inc., Apple Inc., Facebook and Twitter Inc., said in statement on the day the law was passed the bill would give the military regime "sweeping powers to monitor traffic online" under a "loosely-defined national security agenda." READ MORE

*Source: IT Web*

*Date: 15 Mar 2019*

## Cyber Crimes Bill now a matter of urgency in South Africa

"The initial draft Bill was not well received, with critics saying it was too broad and open to abuse, and was a threat to the fundamental spirit of the Internet, which is open and democratic. Subsequent changes to the Bill, including the removal of some of the security obligations, saw it drop the 'security' part of the originally named Cyber Crimes and Cyber Security Bill. […] Corien Vermaak, cyber security specialist at Cisco, says historically SA relied on a light definition of computer crime encapsulated in the Electronic Communications and Transactions Act. Comparing SA to its international counterparts, Vermaak says: "We are very late to adopt legislation; in the UK, computer crime was maturely criminalised in the 90s. The Budapest convention was signed in November 2001 and the African Union accepted model legislation in this regard in 2012 already." This is now a matter of urgency for South Africa." READ MORE

*Source: Flashpoint - Intel*

*Date: 12 Mar 2019*

## Encrypted Messaging Apps Facilitating Cybercrime in Latin America

"As Spanish- and Portuguese-speaking markets continue to drop off the Deep & Dark Web (DDW), criminals are migrating more and more to encrypted chat-services platforms for communication and commerce. Markets operating in either language have been scarce and have been shutting down due to poor sales and/or management. Buyers and sellers who bypassed markets and used underground forums to meet, were finalizing negotiations or communicating directly instead over encrypted platforms. While this is a stark contrast to operators in Eastern Europe and North America who still heavily trade on the DDW, criminals in Latin America prefer the convenience and relatively high levels of baseline security found in encrypted chat apps. Some of this is due to a relative lack of technological sophistication within the region." READ MORE

*Source: Venezuelanalysis*

*Date: 10 Mar 2019*

## Venezuela Suffers Major Power Outages After Alleged Cyber Attack

"An electricity blackout has affected most of Venezuela for several days after an alleged cyber-attack crashed the country's main electricity generator, the Simon Bolivar Hydroelectric Plant in Bolivar State, commonly known as the Guri Dam. Starting around 5 PM on Thursday, the outage affected 70 percent of the country, with only several eastern states unaffected. By Saturday morning, power had been restored to most of Caracas and to central states such as Miranda, Aragua and Carabobo, when a second major outage took place as a result of a renewed cyber-attack, according to Venezuelan authorities." READ MORE

*Source: Osiris*

*Date: 13 Mar 2019*

## Le Congo Brazza sur le chemin de la sécurisation de son cyberespace : sept textes adoptés

"[…] La législation pénale congolaise actuelle n'étant pas adaptée aux spécificités de la délinquance numérique, aussi bien en droit substantiel qu'en droit procédural, il est apparu, dès lors, nécessaire de renforcer les dispositions du Code pénal en vigueur dans notre pays, en ajoutant les infractions commises par le biais des TIC. De fait, le texte proposé s'inspire largement des instruments juridiques internationaux et communautaires, et résout ainsi la question de la transposition, dans la législation nationale, des normes régionales et communautaires." READ MORE

*Source: Bloomberg*

*Date: 12 Mar 2019*

## Indonesia Says Election Under Attack From Chinese, Russian Hackers

"Chinese and Russian hackers are attacking Indonesia's voter data base in a bid to disrupt the country's upcoming presidential election, according to a senior election commission official. As Indonesia prepares for simultaneous presidential and legislative polls on April 17, authorities are facing a wave of cyber incursions they say may be aimed at discrediting the polling process. The head of Indonesia's General Elections Commission, Arief Budiman, said some of the attacks originated in Russia and China, and include attempts to "manipulate or modify" content as well as to create so-called ghost voters, or fake voter identities." READ MORE

*Source: Daily Sabah*

*Date: 13 Mar 2019*

## 130 detained in nationwide operations against FETÖ

"In Istanbul, prosecutors issued arrest warrants for 102 suspects accused of using ByLock, an encrypted messaging app developed and exclusively used by FETÖ members. Forty-five suspects were detained in operations when Daily Sabah went to print. The Interior Ministry announced earlier this month that investigations into Bylock found 4,676 new Bylock users recently, while more than 95,000 users were already identified in previous probes." READ MORE

RELATED ARTICLES
Turkish intelligence agency's secret profiling of critics exposed, 15 March 2019

# Latest reports

- Council of the European Union, Justice and Home Affairs Council Meeting, Background note, 7 Mar 2019
- Europol and INTERPOL, 7th Europol-INTERPOL Cybercrime Conference, 9-11 Oct 2019
- ICANN, GDPR/WHOIS issue: Draft Technical Model for Access to Non-Public Registration Data, 7 Mar 2019
- Australia – International Cyber Engagement Strategy, 2019 PROGRESS REPORT, March 2019
- Bromium, Cybercriminals earn over $3.25 billion annually from social media-enabled cybercrime; enterprises infected with cryptomining malware doubled, 2 Mar 2019
- The European Sting, The biggest cybercrime trends of 2019, 5 Mar 2019

# Upcoming events

- 16 – 21 and 23 March, Amman, Jordan – Advanced Judicial Training, CyberSouth
- 18 March 2019, Albania and Kosovo* – Advice on lessons learnt from case simulation exercises, iPROCEEDS
- 18 – 19 March, Accra, Ghana – National conference on the technical implementation of the Budapest Convention, GLACY+
- 18 – 22 March, Hong Kong – Participation in the Cyber Command Course organized by the Hong Kong Police, GLACY+
- 20 – 22 March, Accra, Ghana – In-country advisory mission on national integration/mainstreaming of judicial training modules on cybercrime, GLACY+
- 25 – 27 March, Banjul, Gambia – Support to the drafting of cybercrime legislation, GLACY+
- 25 – 29 March, Bucharest, Romania – Undercover Online Investigations training, CyberSouth
- 27 – 30 March 2019, Vienna, Austria – Participation in the UN intergovernmental expert group meeting on cybercrime
- 29 March 2019 – Bucharest, Romania – 6th Meeting of the Project Steering Committee, iPROCEEDS