

# Cybercrime Digest

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

1-15 July 2017

Source: Council of  
Europe

## Nigeria invited to join the Budapest Convention on Cybercrime

Date: 11 Jul 2017

"Yesterday, Nigeria was invited to accede to the Budapest Convention on Cybercrime. This is the result of number of years of cooperation between Nigerian authorities and the Council of Europe. In total, 55 States are now Parties and another 14 States have either signed or been invited to accede." [READ MORE](#)

Source: Estonian  
Presidency of the  
Council of the  
European Union

## EU and Eastern Partnership justice and home affairs ministers discuss priorities for cooperation

Date: 7 Jul 2017

"The ministers affirmed their commitment to meeting the essential deliverables of the Eastern Partnership for 2020 pertaining to the justice and home affairs area, and focussed their discussions on the following priorities: the fight against cybercrime, the fight against corruption, and essential judicial reforms. [...] The ministers reiterated their joint commitment to take further action to combat cybercrime and strengthen cybersecurity in an effective manner. The ministers discussed their most important legislative and operational challenges in the fight against cybercrime, with the perspective of enhancing cooperation at both regional and international levels and pursuing further action in the framework of the Eastern Partnership rule of law panel." [READ MORE](#)

Source: Europol

## 14 arrests in takedown of massive child sexual abuse platform

Date: 7 Jul 2017

"In the past five weeks, the German Federal Prosecutor's Office and Federal Criminal Police Office have arrested a number of individuals suspected of the serious sexual abuse of children and the distribution of large amounts of child abuse material online. The German authorities have also taken down the child abuse platform Elysium. The Elysium platform, built as a forum, has existed since the end of 2016 and was only accessible via the Darknet. With over 87 000 members worldwide, the platform was used to exchange child abuse material as well as to make appointments for the sexual abuse of children. Elysium also encompassed chat groups in German, French, Spanish and Italian." [READ MORE](#)

Source: Intellinews

## Small East European nations in vanguard of cyber-defence

Date: 10 Jul 2017

"Estonia and Georgia have made the top 10 in the UN International Telecommunication Union's (ITU's) latest Global Cybersecurity Index (GCI), with experts assessing that the small nations have responded very effectively since suffering cyber-attacks from Russia. [...] The ITU GCI surveyed 195 countries, basing its research on countries' legal, technical and organisational institutions, educational and research capabilities and cooperation in information-sharing networks." [READ MORE](#)

Source: Maurice  
Info

## Eastern African countries meet in Mauritius to address the growing threat of cybercrime

Date: 8 Jul 2017

"The Government of Mauritius, the International Association of Prosecutors and the Council of Europe jointly organized the East Africa Regional Conference on Cybercrime and Electronic Evidence, gathering representatives of 12 countries in the region to improve international cooperation against cybercrime. [...] Recent research shows that the Eastern African region is particularly vulnerable to the emerging threat of cybercrime, with countries such as Nigeria, Malawi or Uganda ranking among the top ten most exposed countries on the global level. The higher vulnerability in this region can be linked to multiple causes: the overall lag, compared to other African states, in the legislative response to cybercrime, low cybersecurity infrastructure investment or criminal justice authorities' limited experience in handling cybercrime cases and electronic evidence." [READ MORE](#)

---

Source: Reuters

## Austria drafts law to let police access messaging data

Date: 10 Jul 2017

"Austria is pursuing plans to give police authority to monitor messaging services such as WhatsApp and Skype in an attempt to "close the gap" on criminals who increasingly avoid communicating via telephone. The government asked political, technology, civil rights and legal experts to review draft legislation that would give it authority to monitor real-time conversations using new messaging services and applications, Justice Ministry officials told Reuters on Monday." [READ MORE](#)

---

Source: AP News

## Australia plans law to force technology companies to decrypt messages

Date: 14 Jul 2017

"The Australian government on Friday proposed a new cybersecurity law to force global technology companies such as Facebook and Google to help police by unscrambling encrypted messages sent by suspected extremists and other criminals. But some experts, as well as Facebook, warned that weakening end-to-end encryption services so that police could eavesdrop would leave communications vulnerable to hackers. The new law would be modeled on Britain's Investigatory Powers Act, which was passed by the British Parliament in November and gave intelligence agencies some of the most extensive surveillance powers in the Western world, the government said." [READ MORE](#)

---

Source: Brave New  
Coin

## Fourth largest Bitcoin exchange, Bithumb, hacked for billions of Won

Date: 4 Jul 2017

"The largest bitcoin and ether exchange in South Korea by volume, Bithumb, was recently hacked. Monetary losses from compromised accounts have started to surface, and are quickly reaching into the billions of won. With a reported 75.7% share of the South Korean bitcoin market volume, Bithumb is one of the five largest bitcoin exchanges in the world and hosts over 13,000 bitcoins worth of trading volume daily, or roughly 10 percent of the global bitcoin trade. The exchange also hosts the world's largest ether market. While trade in the South Korean won currently makes up the fourth largest currency market for bitcoin, trailing the US dollar, Chinese yuan and Japanese yen, the won market is Ethereum's largest." [READ MORE](#)

---

Source: *Tonga Broadcasting Commission*

Date: 3 Jul 2017

## Tonga, national co-operation is required to combat cybercrime

"The Deputy Prime Minister – Hon. Siasoi Sovaleni has urged the nation to work collaboratively to protect our people and nation from cyber crimes as Tonga is vulnerable to cyber attack as majority of the population have access to the Internet and technology daily. [...] The Head of the Cyber Crime from the Council of Europe – Alexander Seger is currently in Nuku'alofa to assist Tonga's capabilities on dealing with cyber crime. It includes amending the law for criminal activities and encouraging the law officers on using the technology. This is part of Tonga's benefit from acceding to the Budapest Convention on Cybercrime." [READ MORE](#)

### RELATED ARTICLES

Ministry of Information and Communication of the Kingdom of Tonga, [Tonga, the first Pacific island to be a party to the BUDAPEST Convention](#), 3 Jul 2017

Source: *UNIAN*

Date: 9 Jul 2017

## Ukraine, U.S. reach agreement on combating cybercrime

"As a result of our highly developing cooperation, it is confirmed by the fact that Ukraine is having not only powerful bipartisan support in the U.S. Congress, but mighty support in the White House, in the Department of State, and the American administration" Poroshenko said Sunday during his joint press conference with U.S. Secretary of State Rex Tillerson. Read also U.S. Special Envoy for Ukraine to stay in Kyiv for several days - Poroshenko Addressing Mr Tillerson, Petro Poroshenko added: "I am confident that our today's visit will facilitate the extension of our cooperation in many sectors, starting from the defense; security; cyber crime prevention, where we have reached important arrangements; economic; energy; and cultural, as well as many other sectors." [READ MORE](#)

Source: *The New York Times*

Date: 6 Jul 2017

## Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say

"Since May, hackers have been penetrating the computer networks of companies that operate nuclear power stations and other energy facilities, as well as manufacturing plants in the United States and other countries. [...] The joint report carried an urgent amber warning, the second-highest rating for the sensitivity of the threat." [READ MORE](#)

Source: *Enter.co*

Date: 5 Jul 2017

## Colombia tiene con qué defenderse de un ciberataque

"La seguridad digital es un tema presente en la agenda del gobierno colombiano. Muestra de ello fue el Foro de Seguridad Digital: Confianza y Corresponsabilidad, realizado por el Ministerio de las Tecnologías de la Información y las Comunicaciones en Bogotá. En este, el ministro TIC David Luna, junto a un panel de expertos internacionales, hablaron de la importancia de la educación y el buen uso de las tecnologías de la información. [...] con la idea de seguir fortaleciendo la seguridad del país, Luna hizo varios anuncios importantes. El primero es que el 20 de julio MinTIC presentará la solicitud ante el Congreso de la República para que se acoja el Convenio de Budapest." [READ MORE](#)

Source: Noticias  
Chihuahua

Date: 12 Jul 2017

## Urge consolidar un marco regulatorio que proteja de ciberataques en Mexico; así como ratificar el Convenio de Budapest

“El estado mexicano debe contar con los esfuerzos para formar una sólida política de ciberseguridad que proteja al país de las amenazas que aumentan día a día, advirtió la diputada Sharon Cuenca Ayala, vicepresidenta de la Mesa Directiva de la Cámara de Diputados, durante el Foro “Hacia una Estrategia Nacional de Ciberseguridad”. El país, agregó, no cuenta con un marco regulatorio que proteja, en caso de un ciberataque, proveniente del interior o del extranjero, por lo que se debe buscar una normatividad que brinde los parámetros de seguridad en las nuevas formas de delincuencia. Recordó que la Comisión Permanente solicitó a las instancias correspondientes la adhesión de México al Convenio de Budapest, para acceder a cooperación técnica de la Unión Europea en esta materia.” [READ MORE](#)

Source: Koaci

Date: 5 Jul 2017

## Le FBI aux trouses de 602 présumés cybercriminels au Cameroun

“D’après « Kalara », - un journal privé spécialisé dans les informations judiciaires et paraissant à Yaoundé-, le FBI est au Cameroun, aux trouses de 602 présumés cybercriminels, impliqués dans une vaste escroquerie de 4 milliards FCFA. Selon ce journal, 90 suspects ont déjà été interpellés pour le moment dans les villes de Yaoundé, Douala, Bamenda, Buea et Kumba. Il est reproché aux 602 présumés cybercriminels, d’avoir arnaqué via Facebook, 2700 personnes.” [READ MORE](#)

Source:  
Government of  
Mauritius

Date: 7 Jul 2017

## Mauritius, national Cybercrime Strategy in preparation to cater for future challenges

“A National Cybercrime Strategy will soon be approved by Government so as to promote a coordinated approach and to cater for challenges as the capabilities of law enforcement agencies need to be enhanced to detect, handle and prosecute cybercriminals, and for the judiciary to improve their technical understanding whenever cases are brought before Courts”. The Minister of Technology, Communication and Innovation, Mr Yogida Sawmynaden, made this announcement yesterday at the launching of a two-day workshop on Cybercrime and Cybersecurity Policies and Strategies at the Mauritius Research Council, in Ebène Cybercity. The event is organised by the Ministry of Technology, Communication and Innovation in collaboration with the Council of Europe in the context of the GLACY+ (Global Action on Cybercrime Extended) Project.” [READ MORE](#)

Source: The Phnom  
Penh Post

Date: 12 Jul 2017

## Gaps persist in laws protecting kids in Cambodia

“A draft United Nations Office on Drugs and Crime (UNODC) report released at a workshop on Monday praises efforts to crack down on sexual abuse of children but calls for measures to curb child pornography. According to the report, the Law on Suppression of Human Trafficking and Sexual Exploitation addresses the sale and prostitution of children, and the sale of child pornography, but does not criminalise possession. It describes the government’s current consideration of a draft cybercrime law as imperative in addressing child pornography online.” [READ MORE](#)

Source: Ministry of Communications and Information, Singapore

Date: 10 Jul 2017

## Public consultation on the draft Cybersecurity Bill in Singapore

"Cyber-attacks are getting increasingly frequent, sophisticated and impactful. [...] In Singapore, the recent Advanced Persistent Threat attacks targeting two of our universities, and the occurrence of the global WannaCry and Petya/Petna malware attacks which also reached our shores, serve as stark reminders of Singapore's vulnerability to cyber threats. [...] The proposed Cybersecurity Bill will establish a framework for the oversight and maintenance of national cybersecurity in Singapore, and will empower CSA to carry out its functions." [READ MORE](#)

### RELATED ARTICLES

Open Gov Asia, [Public-private alliance launched by Singapore Police Cybercrime Command](#), 5 Jul 2017

Source: INTERPOL

Date: 12 Jul 2017

## INTERPOL Dialogue unites public and private sectors to combat cyber and financial crimes

"A high-level dialogue hosted by INTERPOL is bringing together senior public and private sector officials to identify areas for closer cooperation to more effectively combat cyber and financial crime. Nearly 190 representatives from law enforcement, financial, telecommunications and Internet sectors are taking part in the two-day (12 and 13 July) Countering Cyber and Financial Crime: A High-level Dialogue for a New Governance Architecture, and will develop recommendations aimed at streamlining the global response in the face of escalating cyber and financial crime threats." [READ MORE](#)

Source: The Hacker News

Date: 13 Jul 2017

## AlphaBay Shut Down After Police Raid; Alleged Founder Commits Suicide in Jail

"AlphaBay Market — one of the largest Dark Web marketplaces for drugs, guns, and other illegal goods — that mysteriously went dark earlier this month without any explanation from its admins has reportedly been shut down by the international authorities. [...] the disappearance of the AlphaBay came after authorities in the United States, Canada, and Thailand collaborated to conduct a series of raids and arrest Alexandre Cazes, who allegedly was one of the AlphaBay's operators. [...] AlphaBay, also known as "the new Silk Road," also came in the news at the beginning of this year when a hacker successfully hacked the AlphaBay site and stole over 200,000 private unencrypted messages from several users." [READ MORE](#)

Source: Tripwire

Date: 7 Jul 2017

## Man Admits to Phishing for Bitcoins on Dark Web Forums

A man has admitted that he committed fraud and money laundering as part of a phishing scheme to steal Bitcoins on dark web forums. [...] He reportedly committed this theft by abusing more than 10,000 sets of usernames and passwords for online marketplaces, login credentials which law enforcement officials found on Richo's computer when they arrested him on 5 October 2016. [...] U.S. District Judge Vanessa L. Bryant will sentence Richo on 28 September 2017." [READ MORE](#)

---

## Latest reports

- ENISA, [Cyber Europe 2016: After Action Report](#), 30 June 2017
- European Parliament, LIBE Committee, [Fight Against Cybercrime](#), May 2017, voted in the Committee on 11 Jul 2017
- Pew Research Center, [Online Harassment 2017](#), 11 Jul 2017

---

## Upcoming events

- 28-30 July, Sri Lanka – Residential workshop for High Court Judges on cybercrime and electronic evidence, [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](mailto:cybercrime@coe.int)

**[www.coe.int/cybercrime](http://www.coe.int/cybercrime)**

---

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE