

# Cybercrime Digest

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

16-31 July 2017

Source: Europol

## Massive blow to criminal dark web activities after globally coordinated operation

Date: 20 Jul 2017

"Months of preparation and coordination have resulted today, 20 July 2017, in the takedown of two of the largest criminal Dark Web markets, AlphaBay and Hansa. Two major law enforcement operations, led by the Federal Bureau of Investigation (FBI), the US Drug Enforcement Agency (DEA) and the Dutch National Police, with the support of Europol, have shut down the infrastructure of an underground criminal economy responsible for the trading of over 350 000 illicit commodities including drugs, firearms and cybercrime malware. The coordinated law enforcement action in Europe and the US ranks as one of the most sophisticated takedown operations ever seen in the fight against criminal activities online." [READ MORE](#)

### RELATED ARTICLES

US Department of Justice, [AlphaBay, the Largest Online 'Dark Market,' Shut Down](#), 20 Jul 2017

Source: US  
Department of  
Justice

## High-Level US Justice Department Official Addresses INTERPOL on Cyber and Financial Crime

Date: 17 Jul 2017

"During his remarks, Raman reinforced the importance of the Budapest Convention on Cybercrime, which is the first international treaty on crimes committed via the Internet and other computer networks. It deals specifically with copyright infringement, computer-related fraud, child pornography, hate crimes, and violations of network security. Its main purpose is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation. Raman called the Budapest Convention "the governance architecture to address internet crime." He said that there is no need for a new international cyber agreement, as called for by some countries. He called for countries to "focus on capacity building and training efforts proven so successful in facilitating law enforcement operations and partnerships." He also lauded INTERPOL's efforts in building capacity by training police and promoting universal participation in the fight against cyber-crime." [READ MORE](#)

Source:  
Cointelegraph

## Greek Police Arrest Man Who Laundered \$4 bln in Bitcoin Over 6 Years

Date: 26 Jul 2017

"The largest Russian-language cryptocurrency exchange BTC-e was closed on "unscheduled technical work." The owners of BTC-e diligently kept anonymity. However, our source from qugla.com ICO marketing agency has revealed to Cointelegraph that Alexander Vinnik is one of the owners and administrators of the exchange. Earlier today, Greek police have arrested Alexander Vinnik accused of heading a group which laundered \$4 bln in Bitcoin over six years. "There was practically no KYC on the exchange, and, as a result, the cash flows were unregulated," the source explains." [READ MORE](#)

Source: *The Scotsman*

## Scotland witnessing 'significant' growth in cybercrime

Date: 22 Jul 2017

"According to Police Scotland, cyber crime has infiltrated areas like child exploitation, human trafficking, extortion and online abuse. But the most often seen types of cyber crime are malware proliferation, ransomware, social engineering, phishing and online fraud. [...] Since 2015, police forces in England and Wales have been required to flag cyber crimes, but there is no equivalent requirement in Scotland. In Scotland, just one person was convicted in Scotland last year under the Computer Misuse Act (1990). This covers offences including hacking, unauthorised access to computer systems and purposefully spreading malicious and damaging software such as viruses. Almost 900 people were convicted in Scottish courts under the Communications Act in 2015-16, including 719 under section 127 (1), which includes sending offensive messages. Offences under both acts were deemed by the Scottish Government to be the only ones identifiable as cyber crime." [READ MORE](#)

---

Source: *Associated Press*

## Russian parliament bans use of proxy Internet services, VPNs

Date: 21 Jul 2017

"Russia's parliament has outlawed the use of virtual private networks, or VPNs, and other Internet proxy services, citing concerns about the spread of extremist materials. The State Duma on Friday unanimously passed a bill that would oblige Internet providers to block websites that offer VPN services. Many Russians use VPNs to access blocked content by routing connections through servers outside the country. The lawmakers behind the bill argued that the move could help to enforce Russia's ban on disseminating extremist content online." [READ MORE](#)

---

Source: *KyivPost*

## Ukraine to deepen cooperation with France in cyber crime counteraction

Date: 21 Jul 2017

"Ukrainian Interior Minister Arsen Avakov and French Ambassador to Ukraine Isabelle Dumont have agreed on the expansion of Ukrainian-French cooperation in the field of civil security and in the field of countering cyber crime. "France and Ukraine are expanding cooperation in the field of civil security and countering cyber crime. And I want to thank you for your support and the significant contribution of France to the reform of the Interior Ministry system," the press service of the Interior Ministry quoted Avakov as saying on July 21. The minister also informed about the progress of the reform of the law enforcement sector, which, he said, has increased the disclosure of crimes by 20 percent." [READ MORE](#)

---

Source: *Apa*

## Azerbaijan's State Security Service exposes int'l cybercrime group

Date: 25 Jul 2017

"A cybercrime group operating abroad has illegally entered the computer system of a commercial bank of public importance in Azerbaijan, stealing an estimated total amount of 3,700,000 manats by ways of money transferring, making contactless money withdrawals from ATMs, etc., the PR department of Azerbaijan's State Security Service said Tuesday. Investigations reveal that similar crimes have been committed against others banks based in foreign countries." [READ MORE](#)

---

Source: *The Guardian*

## European Court of Justice to rule on whether 'right to be forgotten' can stretch beyond EU

Date: 20 Jul 2017

"The European court of justice (ECJ) is set to rule on a landmark case over whether or not the so-called "right to be forgotten" can and should stretch beyond EU borders. It will be the final step in a three-year legal battle between Google and France to determine how far the search engine should go to guarantee the privacy of European citizens who want their pasts to be wiped from the historical record. [...]France's concern is that the right is only worth anything if it applies universally. [...]On the other side, Google argues that the extension of the right would pose a serious risk that other countries with more egregious limitations on freedom of speech would similarly attempt to universalise their restrictions." [READ MORE](#)

Source: *Europol*

## New Eurasean investigative network on combating cyber fraud

Date: 26 Jul 2017

"The increasing threat posed by fraudulent payment card activities by organised crime groups has led to the creation of the Investigative Network of Law Enforcement specialists from the European Union and ASEAN countries. This initiative, led by Europol, is supported by both ASEANAPOL and INTERPOL, with the assistance of the European Association for Secure Transactions (EAST) representing the private sector. This network comprises law enforcement officers from EU Member States and 10 ASEAN countries, namely Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam." [READ MORE](#)

Source: *The Economic Times*

## One cybercrime in India every 10 minutes

Date: 22 Jul 2017

"According to the Indian Computer Emergency Response Team, 27,482 cases of cybercrime were reported from January to June. These include phishing, scanning or probing, site intrusions, defacements, virus or malicious code, ransomware and denial-of-service attacks. With more Indians going online, cyber experts said putting in place critical infrastructure to predict and prevent cybercrimes was crucial." [READ MORE](#)

### RELATED ARTICLES

The Times of India, [Online cybercrime reporting system launched in India](#), 26 Jul 2017

Source: *Agence de Presse Sénégalaise*

## L'extrémisme violent, la cybercriminalité, les nouveaux défis sécuritaires en Afrique

Date: 19 Jul 2017

"Le ministre des Affaires étrangères et des Sénégalais de l'extérieur, Mankeur Ndiaye, a exposé, mercredi, devant le Conseil de sécurité de l'ONU les nouveaux défis dans le domaine de la paix et de la sécurité en Afrique, citant l'extrémisme violent, la cybercriminalité, et la sécurité maritime. [...] Avec plus de 20.000 attaques enregistrées par année en Afrique, la cyber sécurité constitue un des défis majeurs qui mettra à rude épreuve nos capacités à faire face aux procédés ingénieux et sophistiqués de leurs auteurs", a-t-il alerté." [READ MORE](#)

Source: @bidj@n

Date: 28 Jul 2017

## **Afrique de l'Ouest : Vers l'identification des actions concrètes pour lutter contre les menaces cybernétiques**

"La 9ème édition du Forum sur la gouvernance de l'Internet en Afrique de l'Ouest, visant à identifier les actions concrètes qui doivent être prises pour lutter efficacement contre les menaces cybernétiques dans l'espace communautaire ouest-africaine, s'est ouvert jeudi à Cotonou. [...] S'exprimant à l'ouverture de ce Forum, le Commissaire de la Communauté économique des Etats de l'Afrique de l'Ouest (CEDEAO), Isaias Barreto da Rosa, a indiqué que la vision de la CEDEAO est de créer une Afrique de l'Ouest intégrée avec la libre circulation des personnes, des biens et des services. [...] "Il n'y aura pas de marché numérique unique en Afrique de l'Ouest sans un cyber espace sécurisé dans la sous-région. Par conséquent, nous devons veiller à ce que, en s'attaquant au fléau de la cybercriminalité, nous favorisons également la cyber sécurité en Afrique de l'Ouest", a-t-il indiqué." [READ MORE](#)

Source: AFP

Date: 21 Jul 2017

## **Une société du Liberia derrière la cyber-attaque de l'Allemand Deutsche Telekom**

"Un Britannique jugé en Allemagne pour une vaste attaque informatique qui avait touché en novembre plus d'un million de clients de l'opérateur allemand Deutsche Telekom a reconnu vendredi avoir agi pour le compte d'une société du Liberia. [...] Devant le tribunal, qui le juge pour "tentative de sabotage informatique", il a déclaré avoir agi pour le compte d'une entreprise de télécommunication du Liberia qui voulait s'en prendre à une autre entreprise libérienne concurrente." [READ MORE](#)

Source: GhanaWeb

Date: 21 Jul 2017

## **Ghana, CID plans cyber intelligence lab**

"Plans are underway by the Criminal Investigations Department (CID) to establish a Cyber Intelligence Laboratory to monitor criminals who use the cyber space to commit crime. The Director in-charge of the Cyber Crime Unit, Chief Superintendent Dr Gustav Herbert Yankson, said criminals who use the cyber space have devised a strategy to share information." [READ MORE](#)

Source: IT News Africa

Date: 28 Jul 2017

## **Tanzania continues to fight cybercrime**

"In a bid to protect citizens and businesses from malicious hackers and cyber-criminals, the government of Tanzania is drafting new internet legislation. The government hopes to cooperate with China to introduce the Personal Data Protection Act to make cyberspace more secure and protect users. The new cyber law could add onto the two cyber-crime laws dubbed Cybercrimes Act 2015 and Electronic Transactions Act 2015." [READ MORE](#)

Source: Euronews

Date: 19 Jul 2017

## **Man behind blue whale suicide 'game' is jailed**

"One of the founders of a controversial online challenge that encourages participants to kill themselves has been jailed. Philipp Budeikin, who pleaded guilty to inciting teenagers to commit suicide, was given a three-year jail term by a Russian court." [READ MORE](#)

Source: República  
Guatemala

## Primer Foro de Gobernanza de Internet se realiza en Guatemala

Date: 28 Jul 2017

"El primer foro de gobernanza de internet de Guatemala (IGF), se llevó a cabo con el fin de reunir a diferentes partes interesadas, incluyendo a los gobiernos, el sector privado, la sociedad civil, la comunidad técnica y la academia, en la discusión de temas relacionados a internet a nivel mundial. [...] Por parte del Congreso se está creando una iniciativa que pretende combatir la inseguridad en internet. La Ley de Ciberdelincuencia 5254 pretende reunir a varias instituciones para hacer un esfuerzo en común contra este flagelo. [...] Esta iniciativa se trabajó con MP, Ministerio de Gobernación, PNC, Unicef, Ministerio Público, PNC para hacer una ley que cumpliera con lo establecido en el convenio de Budapest." [READ MORE](#)

Source: El  
Universal

## OEA, la delincuencia en la red es lucrativa

Date: 20 Jul 2017

"[...] "Falta mucho por hacer en la región, pues los Estados están en una situación tanto vulnerable", insistió Contreras, quien aseguró que también países muy desarrollados de América o Europa, sufren estos ataques mundialmente conocidos. Para el experto colombiano es importante también generar una conciencia en todos los niveles del Estado, "solo así podremos fortalecer la seguridad en Internet", aclaró. En ese sentido, el Convenio Budapest sobre ciberdelincuencia, que entró en vigor en 2004, es un instrumento legal europeo que permite intercambiar evidencias, pruebas y homogeneizar los procedimientos entre los estados. "Este convenio, firmado y ratificado por Chile, República Dominicana y Panamá, entre otros, es importante por la respuesta multinacional que propone", aseveró Contreras." [READ MORE](#)

Source: Huffington  
Post

## How A Billion-Dollar Internet Scam Is Breaking Hearts And Bank Accounts

Date: 20 Jul 2017

"In the U.S., romance scams account for the highest financial losses of all internet-facilitated crimes, the FBI reports. The bureau's Internet Crime Complaint Center said it received 15,000 romance scam complaints last year — a 20 percent increase over the previous year. Reported losses exceeded \$230 million, but the FBI puts the true number much higher, estimating that only about 15 percent of these crimes are even being reported. The odds of recovering that money, the bureau notes, are very low. Some of the money scammed by international criminal networks even winds up in the hands of terrorist operations like Boko Haram, according to Interpol." [READ MORE](#)

Source: The  
Namibian

## Namibia: online bullying, harassment – a crime

Date: 21 Jul 2017

"ONLINE bullying and harassment should be treated as crimes and the perpetrators jailed, says Ruth Herunga, chairperson of the Namibian Women Lawyers' Association. She was reacting to a social media post when she urged government to enact and implement the Electronic Transactions and Cybercrime Bill as a matter of urgency on Tuesday. Herunga's comments stem from the arrest of a Windhoek man, Khama Nakandungile, on Monday after he posted malicious material involving his wife on Facebook." [READ MORE](#)

## Latest reports

- Council of the European Union, [Evaluation Report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime" - Report on Sweden](#), declassified on 27 July 2017
- Council of the European Union, [Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime" - Report on Austria](#), declassified on 28 July 2017
- Electronic Frontiers Foundation, [Online Service Providers' Privacy and Transparency Practices Regarding Government Access to User Data](#), July 2017
- Stanford Law Review, [Government Hacking to Light the Dark Web](#), July 2017
- Kaspersky, [Cybersecurity Index 2H2017](#), July 2017
- CSO Online, [2017 U.S. State of Cybercrime: Security events decline, but not the impact](#), 28 Jul 2017

## Upcoming events

- 9-13 August, Sri Lanka – Residential workshop on cybercrime for intake of new judges, [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