# Cybercrime Digest

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

01 – 15 August 2020

*Source: Council of Europe*

*Date: 28-30 Jul 2020*

## GLACY+: Online Regional Workshops in Africa, Asia-Pacific and Latin America on Establishment and functioning of the 24/7 Points of Contact Network

"A series of three online regional workshops were conducted by the Council of Europe, focusing on *Establishment and functioning of the 24/7 Points of Contact Network under the Budapest Convention*. The events were held on 28, 29 and 30 July 2020, being respectively addressed to Africa, Asia-Pacific and the Americas regions. [...] The online workshops were dedicated to designated 24/7 points of contact and other staff (from the prosecution service, police, Ministry of Justice) currently dealing with international cooperation on cybercrime." READ MORE

*Source: Council of Europe*

*Date: 13 Aug 2020*

## iPROCEEDS-2: Starting of the long-distance master programme on forensic computing and cybercrime investigation

"The iPROCEEDS-2 project will support the participation of 15 representatives from Cybercrime Units and Prosecution Services from Albania, Bosnia and Herzegovina, Montenegro, North Macedonia, Serbia, Turkey and Kosovo* in the long-distance master programme MSc Forensic Computing and Cybercrime Investigation offered by the University College Dublin, Ireland. The programme will start on September 2020 and run for 24 months covering modules like Computer Forensics, Network Investigations, Financial Investigation Techniques – Following the Money, Mobile Devices Investigation, Programming for Investigators, Live Data Forensics, VoIP and Wireless Investigations and others. The learning methods will consist in a mix of lectures, hands-on labs, case studies, reading, small group and individual exercises, tool demonstrations and in depth-discussions." READ MORE

*Source: Associated Press*

*Date: 7 August 2020*

## UN reports sharp increase in cybercrime during pandemic

"A 350% increase in phishing websites was reported in the first quarter of the year, many targeting hospitals and health care systems and hindering their work responding to the COVID-19 pandemic, the U.N. counterterrorism chief, Mr. Vladimir Voronokov said. He told the U.N. Security Council that the upsurge in phishing sites was part of "a significant rise in cybercrime in recent months" reported by speakers at last month's first Virtual Counterterrorism Week at the United Nations. [...] "The pandemic has the potential to act as a catalyst in the spread of terrorism and violent extremism by exacerbating inequalities, undermining social cohesion and fueling local conflicts," Voronkov said." READ MORE

RELATED ARTICLES

DPI Cuantico, Algunas medidas de ciberseguridad en Argentina, Colombia, Cuba, Egipto, Francia, Grecia, Japón, Singapur y Turquía, 6 Aug 2020

Agencia Angola Press, Covid-19: Interpol alerta para aumento "alarmante" do crime informático, 4 Aug 2020

*Source: Council of Europe*

*Date: 11 Aug 2020*

## Discussions at CEELI Institute deal with issues addressed by Council of Europe guidelines on electronic evidence

"The CEELI Institute, in Prague, launched a four-part webinar discussion series as part of its program with the Central and Eastern European Judicial Exchange Network in April 2020. The first of these series which focuses on "Videoconferencing in Support of Remote Access to Courts" took place in April/May 2020 and the webinar 4 (held on 19 May 2020) was devoted to "The Technical Requirements for Using Videoconferencing in the Courts". Barrister Stephen Mason participated in the discussion on The Legal Requirements for Using Videoconferencing in the Courts. The second series on "Access to Justice During and After the Pandemic" took place in June/July 2020 and looked at broader justice issues raised by the pandemic. Mr. Mason also participated in webinar 3 of this series (held on 30 June 2020) on Electronic Evidence and Dealing with Witnesses in Videoconference Hearings. The Committee of Ministers of the Council of Europe adopted, in January 2019, guidelines on electronic evidence in civil and administrative proceedings." READ MORE

*Source: INTERPOL*

*Date: 27 Jul 2020*

## INTERPOL: Online crime in Africa a bigger threat than ever before, INTERPOL report warns

"A new INTERPOL report on online organized crime in Africa shows how digitalization is transforming almost every major crime area across the continent. "Online crime now represents a bigger security issue for law enforcement in Africa than ever before," reads the report, which goes on to detail how the different layers of the Internet (surface web, deep web and dark web) are being used by organized crime groups in Africa to perpetuate crimes. [...] Relatively low rates of online connectivity have not stopped organized crime groups from taking advantage of the Internet. Malware incidents are increasingly prevalent in Africa. In one East African country alone, the cost of cyber fraud more than doubled between 2017 and 2018, reaching nearly USD 6.5 million. [...] As in other world regions, organized crime groups in Africa also use the Internet to facilitate the sexual exploitation and abuse of children, leveraging digital tools to contact and solicit victims as well as sell child sexual abuse materials." READ MORE

*Source: US Department of Justice*

*Date: 13 Aug 2020*

## USDOJ: Global Disruption of Three Terror Finance Cyber-Enabled Campaigns

"The Justice Department today announced the dismantling of three terrorist financing cyber-enabled campaigns, involving the al-Qassam Brigades, Hamas's military wing, al-Qaeda, and Islamic State of Iraq and the Levant (ISIS). This coordinated operation is detailed in three forfeiture complaints and a criminal complaint unsealed today in the District of Columbia. These actions represent the government's largest-ever seizure of cryptocurrency in the terrorism context. These three terror finance campaigns all relied on sophisticated cyber-tools, including the solicitation of cryptocurrency donations from around the world. The action demonstrates how different terrorist groups have similarly adapted their terror finance activities to the cyber age. Each group used cryptocurrency and social media to garner attention and raise funds for their terror campaigns. Pursuant to judicially-authorized warrants, U.S. authorities seized millions of dollars, over 300 cryptocurrency accounts, four websites, and four Facebook pages all related to the criminal enterprise." READ MORE

*Source: dw.com*

*Date: 11 Aug 2020*

## Germany launches cybersecurity agency to strengthen 'digital sovereignty'

"The German government has signed up to create an agency to protect the country's cybersecurity. The defense minister described the project, initially funded with €350 million ($412 million), as a "milestone." The agency, whose creation was agreed upon in the 2018 coalition contract of Germany's ruling parties, is to coordinate innovative research on cybersecurity and help turn it into practicable approaches to combat cyberthreats. Some 100 people will be employed at the institution, which is to be headed by Christoph Igel, an expert on artificial intelligence. In comments quoted by the Defense Ministry, Igel said the most urgent task would be to gain the services of the best minds in Germany in the field of cybersecurity." READ MORE

*Source: naked security*

*Date: 03 Aug 2020*

## GandCrab ransomware hacker arrested in Belarus

Law enforcement in Belarus has announced the arrest of a 31-year-old man who is alleged to have extorted more than 1000 victims with the infamous GandCrab ransomware in 2017 and 2018. He apparently demanded payments ranging from $400 to $1500 in Bitcoin. Unlike more targeted attacks where crooks break into networks first and directly infect them with ransomware later, the unnamed suspect is said to have gone after victims by the more traditional route of spamming out booby-trapped emails across the globe. The Belarus Ministry of Interal Affairs claims that computers that the suspect managed to infect were in more than 100 different countries, notably India, US, Ukraine, UK, Germany, France, Italy and Russia." READ MORE

*Source: arstechnica.com*

*Date: 01 Aug 2020*

## Florida teen charged as "mastermind" in Twitter hack hitting Biden, Bezos, and others

"Authorities on Friday charged three people with orchestrating this month's epic hack of Twitter and using it to generate more than $100,000 in a bitcoin scam promoted by hijacked accounts of politicians, executives, and celebrities. […] The three suspects stand accused of using social engineering and other techniques to gain access to internal Twitter systems. They then allegedly used their control to take over what Twitter has said were 130 accounts. A small sampling of the account holders included former Vice President Joe Biden, Tesla founder Elon Musk, pop star Kanye West, and philanthropist and Microsoft founder, former CEO, and Chairman Bill Gates." READ MORE

*Source: CITI NewsRoom*

*Date: 11 Aug 2020*

## Ghana: CID, national cyber security centre nabs operator of empress leak website

"The National Cyber Security Centre (NCSC) of the Ministry of Communications, in collaboration with the Criminal Investigation Department (CID) of the Ghana Police Service and the National Cyber Security Technical Working Group, have nabbed the administrator of the notorious website, empress leak. Empress leak is a website known for the publication of child pornographic and adult sexual content. […] An investigation to clamp down on activities of empress leak was launched after a female Senior High School student, filed a report on January 6th, 2020, with the Computer Emergency Response Team (CERT-GH) of the NCSC. "[…] As part of Government's efforts towards the protection of Ghana's cyberspace, the National Cyber Security Centre in 2019 launched a Cybercrime/Cybersecurity Incident Reporting Point of Contact (PoC), to provide an effective mechanism for citizens to report suspected and identified cybercrime and cybersecurity incidents." READ MORE

*Source: Global Times Sierra Leone*

*Date: 04 Aug 2020*

## Sierra Leone: Cybercrime Bill Discussed Openly

"The Ministry of Information and Communications, Members of Parliament and the public including CSOs, have perused the National Cybercrime Bill Act 2020 which seeks to enhance Government's vision of creating a digitally inclusive society and economy empowered by a digital innovation, entrepreneurship and improve service delivery. […] "The threat of cybercrime is growing and the number of cybercrimes is witnessing an alarming growth especially from the ECOWAS region", the Minister of Information and Communications, Mohamed Rahman Swaray said at a national stakeholders' consultative meeting at Country Lodge Hotel in Freetown. The Minister said "We are witnessing an increase in the use of digital technology in our daily activities… There are about 700,000 active social media subscribers (principally WhatsApp and Facebook) with an average growth rate of 15 percent" in the country, noting that there is need to protect the fundamental human rights of those subscribers. He revealed that Sierra Leone has no specific legislation on cybercrime or electronic evidence for purposes of investigation and prosecution. The Acting Chairperson of the National Telecommunications Commission, Mrs. Madiana Samba said, "Sierra Leone can no longer tolerate child pornography", adding that Government considers data protection and electronic offences as very key to ending cybercrime in a bid to ensure progressive development." READ MORE

*Source: Burkinaonline.com*

*Date: 08 Aug 2020*

## Burkina Faso. Cybercriminalité : Une nouvelle brigade pour traquer les cyber-arnaqueurs

Les arnaques en ligne sont devenues un phénomène récurrent au Burkina Faso. Avec la persistance du fléau et les interpellations des populations, les autorités ont décidé de prendre le phénomène à bras-le-corps. L'on note que les cas les plus récurrents sont les arnaques via les services de transfert d'argent, qui a déjà causé aux victimes un préjudice de plus de 70 000 000 F CFA. C'est au regard de la recrudescence de ces infractions en ligne que les autorités ont jugé bon de mettre en place une brigade qui sera centralisée pour traiter de ces questions. Ainsi, la Brigade centrale de lutte contre la cybercriminalité (BCLCC) a été mise sur pied en janvier 2020 et a commencé ses activités en mai 2020. Il s'agit d'une nouvelle brigade créée pour lutter spécifiquement contre la cybercriminalité dont les arnaques via les services de transfert monétaire. Elle est rattachée au ministère de la Sécurité et à une compétence nationale en matière d'enquêtes sur les infractions liées à l'informatique ou celles commises au moyen des technologies de l'information et de la communication. » READ MORE

*Source: club-k.net*

*Date: 3 Aug 2020*

## O combate aos Crimes Informáticos em Angola

"Aderindo a Convenção de Budapeste, Angola irá cooperar internacionalmente com uma legislação harmonizada, visto que isto é fundamental para que os crimes não passem impunes. A legislação é fundamental para que a investigação possa ser feita, os crimes possam ser adjudicados e possam haver condenações. O objectivo no fundo é não haver paraísos de cibercrime porque os prevaricadores podem usar esses países para perpetrar os ataques. Na CPLP países como Cabo Verde e Portugal já aderiram à Convenção de Budapeste, sendo que se espera que os outros países possam também dar este passo. A não adesão à Convenção de Budapeste reduz o espaço de manobra das autoridades no combate aos crimes informáticos porque as acções de prevenção e combate deste tipo de criminalidade não podem ser levadas a cabo por um Estado de forma isolada sem a cooperação de outros Estados. A Adesão de Angola à Convenção de Budapeste deve ser encarada como uma das prioridades no combate aos crimes informáticos." READ MORE

*Source: Agenda for International Development*

*Date: 12 Aug 2020*

## Cybersecurity: A brief analysis on the Central American context

"[…] Countries like Guatemala and El Salvador have come forward with the Council of Europe to request cooperation through their Global Action on Cybercrime Extended (GLACY+) Program to implement a cybercrime act that can enable those countries to adhere to the Budapest Convention. This will enable them to exchange information and build capacities with other members more efficiently and be part of the solution to crack cybercrime globally. In this sense, Guatemala has taken significant steps in implementing a cybercrime act aligned with the Budapest Convention to the point where an official invitation was extended in February of 2020 by the Council of Europe for Guatemala to adhere to the convention." READ MORE

*Source: Convergencia digital*

*Date: 07 Aug 2020*

## Brasil: PGR volta a pressionar por adesão à Convenção de Budapeste

O procurador-geral da República, Augusto Aras, solicitou aos presidentes da Câmara dos Deputados, Rodrigo Maia, e do Senado Federal, Davi Alcolumbre, agilidade na tramitação da ratificação legislativa da adesão do Brasil à Convenção de Budapeste sobre o Cibercrime. A iniciativa atende a pedido da Câmara Criminal do Ministério Público Federal (2CCR), que defende a internalização do tratado no ordenamento jurídico brasileiro desde 2011. Os ofícios são acompanhados de nota técnica elaborada pelo Grupo de Apoio sobre Criminalidade Cibernética (GACC) da 2CCR, documento que lista os benefícios da adesão ao tratado e esclarece dúvidas referentes ao funcionamento da Convenção. O parecer do MPF destaca a sofisticação e o aumento exponencial do número de crimes cibernéticos, com a migração de delitos comuns como fraudes, estelionatos, ameaças e extorsões para o meio digital. Alerta ainda que esses delitos não têm encontrado nem capacitação para o seu combate, nem ferramentas jurídicas aptas a permitir a persecução penal efetiva, aumentando a insegurança da vida diária e dificultando a prevenção. Da mesma forma, a necessidade de obtenção de provas digitais para a comprovação da autoria e materialidade de delitos como homicídios, corrupção, crimes financeiros e outros, cuja elucidação pode depender de e-mails, interceptações telemáticas, arquivos armazenados na "nuvem", tornou-se uma rotina para os operadores do direito, alerta a nota técnica. READ MORE

*Source: APWG.EU, LOCARD Project*

*Date: August 2020*

## Why blockchain technology can be useful for the processing of digital evidence?

"The ubiquitous nature of digital devices such as smartphones, laptops and the IoT, makes digital evidences extremely relevant for criminal investigations on all kinds of criminal behaviour, including contraband, human trafficking, child pornography and murder. The LOCARD's holistic platform aims to ensure the chain of custody through the forensic workflow, by storing digital evidence metadata in a blockchain. […] The use of a blockchain within the LOCARD platform endows trustworthiness, integrity, authenticity and transparency throughout the entire forensic workflow, i.e. from the collection of digital evidences, going through the processing of the stored data to realise incidents reporting, to the final prosecution in a court of law. The blockchain's properties prevent disputing the chain of custody of digital evidences during a judicial procedure, a common challenge for many law enforcement agencies and forensic laboratories in spite of properly documenting the entire forensic workflows. LOCARD's D4.3 deliverable (see HERE) provides an extensive review of the state of the art on blockchain technologies, some of them implemented in the LOCARD platform." READ MORE

*Source: thecrimereport.org*

*Date: 13 Aug 2020*

## FBI Warns of Cybercrime Threat to Online Students

"While many educational institutions and businesses continue to maintain online instruction for the fall due to the pandemic, the FBI warns that the online learning structure will make students and families increasingly vulnerable to cyber-attacks, Border Report details. This warning comes as the FBI's Cyber Division experts and Internet Crime Complaint Center (IC3) division reported a 300 percent increase in cybercrime activity — including a 273 percent increase in "large-scale data breaches" — since the start of the COVID-19 pandemic, CNBC News outlines." READ MORE

*Source: the Next Web*

*Date: 3 Aug 2020*

## New AI tool detects child sexual abuse material with '99% precision'

"Child sexual abuse material on the web has grown exponentially in recent years. In 2019, there were 69.1 million files reported to the National Center for Missing and Exploited Children in the US — triple the levels of 2017 and a 15,000% increase over the previous 15 years. A new AI-powered tool called Safer aims to stem the flow of abusive content, find the victims, and identify the perpetrators. The system uses machine learning to detect new and unreported child sexual abuse material (CSAM). Thorn, the non-profit behind Safer, says it spots the content with greater than 99% precision. […] The non-profit's ultimate goal is to eliminate child sexual abuse material from the open web." READ MORE

## Latest reports

- INTERPOL, Cybercrime: COVID19 impact, August 2020
- Inter-American Development Bank, Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y El Caribe
- BBC, 'Hundreds dead' because of Covid-19 misinformation, 12 August 2020
- USA: Black Hat USA 2020, Global Incident Response Threat Report Detailing Surge in Cyberattacks Amid COVID-19, 4 August 2020
- CANADA, COVID-19: Scams, frauds and misleading claims, 4 August 2020
- Crime Science Journal, AI-enabled future crime, 5 August 2020
- Forensics Focus, Day-To-Day Challenges In Digital Forensics, 4 August 2020
- State of Ransomware in the US, Report and Statistics for Q1 and Q2 2020, July 2020

## Upcoming events

Due to the COVID-19 pandemic outbreak and the countermeasures applied by most of the countries worldwide, in-country activities of the C-PROC capacity building initiatives foreseen in the month of July have been rescheduled to a later date.

- 16 August, Desk Study, Review of the Draft Cybersecurity Bill 2020, Ghana, GLACY+
- 28 August, Desk Study, Review of cybercrime legislation for Papua New Guinea, GLACY+
- 28 August, Technical webinar, Preparation for Elections Security, Georgia, CyberEast
- By 31 August, Desk Study, Report on Cybercrime Statistics, in collaboration with INTERPOL, GLACY+
- By 31 August, Desk Assessment, Compliance of procedural law frameworks in line with Articles 16 to 21 Budapest Convention and related legislation (including data protection), Bosnia and Herzegovina, iPROCEEDS-2
- By 31 August, Desk Assessment, Compliance of procedural law frameworks in line with Articles 16 to 21 Budapest Convention and related legislation (including data protection), Turkey, iPROCEEDS-2
- 31 August - 2 September, Workshop on Development of Standard Operating Procedures for Cooperation between CSIRTs and Law Enforcement, Armenia, CyberEast

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