

Cybercrime Digest

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

16 – 30 April 2021

Source: Council of
Europe

Date: 29 Apr 2021

European states must step up efforts to protect children's privacy in digital environment, especially in the COVID-19 pandemic context, says Committee of Ministers of the Council of Europe

"The Committee of Ministers reminded that information and communication technologies, in general, are an important tool in children's lives, but the use of these technologies can at the same time generate risks. Notably, the traceability of children's activities in the digital environment may expose them to criminal activities, such as the solicitation of children for sexual purposes, sexual extortion, child sexual exploitation (including exploitation of sexually explicit content generated by children), or otherwise illegal or harmful activities, such as discrimination, bullying, stalking and other forms of harassment." [READ MORE](#)

Source: European
Commission

Date: 21 Apr 2021

Fostering a European approach to Artificial Intelligence

"Faced with the rapid technological development of AI and a global policy context where more and more countries are investing heavily in AI, the EU must act as one to harness the many opportunities and address challenges of AI in a future-proof manner. To promote the development of AI and address the potential high risks it poses to safety and fundamental rights equally, the Commission is presenting both a proposal for a regulatory framework on AI and a revised coordinated plan on AI." [READ MORE](#)

RELATED ARTICLES

European Commission, [Proposal for a Regulation laying down harmonised rules on artificial intelligence](#), 21 Apr 2021

European Commission, [Coordinated Plan on Artificial Intelligence](#), 21 Apr 2021

Source: GovInsider

Date: 29 Apr 2021

How Interpol is hunting down cybercriminals with data

"Cybercrime has a "very dispersed crime scene", Jones says. Malicious actors can commit crime around the world from one location, using infrastructure in another country. This borderless nature of cybercrime can make it difficult to track down criminals. [...] To tackle this, Interpol is working to aggregate data from different countries and companies on a "cyber fusion" platform, he says. The platform collects data on where the victims are and how they have been attacked. [...] Interpol has a knowledge exchange platform with its 194 member countries and private partners, Jones says. It shares information on the latest threats, prevention strategies, detection and investigation techniques. It's "a bit like a 'cyber Wikipedia,'" he adds. Interpol recently set up a cybercrime desk in the Africa region, and plans to do it in the Americas region as well, he says. It is also planning to expand the ASEAN desk and bring in China, Australia and New Zealand." [READ MORE](#)

<p>Source: Council of Europe</p> <p>Date: 25 Feb 2021</p>	<h2>INTERPOL & GLACY+: Spanish Series of Technical Webinars on Decrypting Communication Algorithms</h2> <p>"The Spanish edition of technical webinars on cryptography organized by INTERPOL under the GLACY+ Project, a joint action of the European Union and the Council of Europe, has gathered a record number of participants: more than 900 registrations and more than 500 participants connected at the same time." READ MORE</p>
<p>Source: Council of Europe</p> <p>Date: 20 Apr 2021</p>	<h2>The International Network of National Judicial Trainers: First Steering Committee</h2> <p>"On 20 April 2021, the Steering Committee of the International Network of the National Judicial Trainers on Cybercrime and Electronic Evidence held its first coordination call, with the support of GLACY+, iPROCEEDS-2, CyberSouth and CyberEast projects in their capacity as Secretariat of the Network. Alongside with the Secretariat, the Steering Committee is expected to ensure implementation of the overall strategy adopted by the Plenary of the Network on 29 January 2021. Moreover, the first Steering Committee coordination call served as a platform to reach consensus on the workplan and its medium and long-time implementation, as well as a space for advancing new proposals. Over 40 representatives from 16 countries (Algeria, Brazil, Cape Verde, Chile, Costa Rica, Dominican Republic, Georgia, Ghana, Jordan, Lebanon, Morocco, Paraguay, Philippines, Senegal, Tunisia and Ukraine) attended and actively engaged in debating challenges of judicial training and the future areas of action of the Network." READ MORE</p>
<p>Source: Ministry of Information of Kiribati</p> <p>Date: 21 Apr 2021</p>	<h2>Kiribati: Cybercrime Bill approved by the Parliament</h2> <p>With the help of the Council of Europe and the Australian Attorney General's Department, "Kiribati has been working on a comprehensive proposal for a cybercrime legislation that could enable its criminal justice sector to effectively tackle the increasing threat posed by cybercrime and its cross-border dimension." During the month of April the Parliament has approved the Cybercrime Bill, joining the global response to "cybercrime and to challenges posed by electronic evidence." The GLACY+ Project will continue supporting the country's efforts and "in defining possible next steps towards the accession of Kiribati to the Budapest Convention." READ MORE</p> <p>RELATED ARTICLES</p> <p>Council of Europe, GLACY+: Kiribati works on cybercrime legislation in line with international standards, December 2020</p>
<p>Source: Council of Europe</p> <p>Date: 26 Apr 2021</p>	<h2>CyberSouth: Regional Workshop on judicial international cooperation and police-to-police cooperation on cybercrime and electronic evidence</h2> <p>"Participants representing criminal justice authorities from the priority countries attended this workshop and discussed about the legal framework, channels and challenges of international cooperation. This regional workshop was an opportunity to assess the capacities for police-to-police and judicial international cooperation on cybercrime and e-evidence of the priority countries." READ MORE</p>

<p>Source: <i>Institute for Security and Technology</i></p> <p>Date: 29 Apr 2021</p>	<h2>Combating ransomware: a comprehensive framework for action</h2> <p>“Ransomware attacks present an urgent national security risk around the world. This evolving form of cybercrime, through which criminals remotely compromise computer systems and demand a ransom in return for restoring and/or not exposing data, is economically destructive and leads to dangerous real-world consequences that far exceed the costs of the ransom payments alone. [...] The immediate physical and business risks posed by ransomware are compounded by the broader societal impact of the billions of dollars steered into criminal enterprises, funds that may be used for the proliferation of weapons of mass destruction, human trafficking, and other virulent global criminal activity. Despite the gravity of their crimes, the majority of ransomware criminals operate with near-impunity, based out of jurisdictions that are unable or unwilling to bring them to justice. This problem is exacerbated by financial systems that enable attackers to receive funds without being traced. Additionally, the barriers to entry into this lucrative criminal enterprise have become shockingly low. The “ransomware as a service” (RaaS) model, allows criminals without technical sophistication to conduct ransomware attacks.” READ MORE</p>
<p>Source: <i>Europol</i></p> <p>Date: 29 Apr 2021</p>	<h2>Three arrested in Spain for encouraging terrorist attacks against France and its interests abroad</h2> <p>“In the early hours of 27 April, officers of the Spanish National Police (Policia Nacional) with the support of Europol swooped on the members of a terrorist cell in the city of Granada. A total of three individuals were arrested on suspicion of encouraging terrorist attacks against France. After the French magazine Charlie Hebdo republished caricatures of the Prophet Muhammad in September of last year, the arrestees posted numerous videos on their social media accounts threatening to carry out violent actions against France, its citizens and interests abroad to avenge the said-publication. The Spanish National Police used its specialist capabilities to identify the individuals behind these social media profiles with totalled almost 19 000 followers.” READ MORE</p>
<p>Source: <i>BalkanInsight</i></p> <p>Date: 16 Apr 2021</p>	<h2>Turkey Moves to Ban Cryptocurrency Payments, Citing Crime Risks</h2> <p>“The Turkish Central Bank has banned payments in cryptocurrencies, as more and more Turks flock to the unregulated crypto market amid a fall in the value of the national currency and a hike in inflation. [...] The new legislation on cryptocurrencies and assets will be put into effect by April 30. Bitcoin lost nearly 3 per cent of its value after the Central Bank decision.” READ MORE</p>
<p>Source: <i>Council of Europe</i></p> <p>Date: 26-28 Apr 2021</p>	<h2>CyberEast: Second Regional Meeting on the Development of Mutual Legal Assistance Guidelines</h2> <p>“The Budapest Convention on Cybercrime is the most relevant international treaty on cybercrime and electronic evidence, with currently 66 Parties and 10 Observer States. Work on the Second Additional Protocol on enhanced cooperation commenced in September 2017 and is expected to be finalized by the end of 2021. Nevertheless, mutual legal assistance in criminal cases concerning cybercrime and electronic evidence remains and will continue to remain a challenge due to a multitude of factors.” READ MORE</p>

<p>Source: Council of Europe</p> <p>Date: 26-27 Apr 2021</p>	<h2>GLACY+: Maldives pursues strong commitment to Budapest Convention</h2> <p>“GLACY+ project, a joint project of the European Union and Council of Europe teamed up with the US Department of Justice (USDoJ) to support the current national efforts to align the Maldivian legal framework on cybercrime and electronic evidence to the provisions of the Budapest Convention. [...] Support for developing Maldives’ cybercrime and electronic evidence related legislation will continue with the organization of multiple online briefings between the Council of Europe experts and the Maldivian drafting teams, currently engaged in developing and updating a Cybercrime Bill and the Evidence Act.” READ MORE</p>
<p>Source: Council of Europe</p> <p>Date: 20-21 Apr 2021</p>	<h2>Octopus Project: Workshop on Criminal Justice Capacities on Cybercrime and Electronic Evidence and accession to the Budapest Convention organised with national authorities of Guyana</h2> <p>“The Council of Europe’s approach to addressing cybercrime was discussed, as well as current threats and challenges worldwide and the need for a strategic approach and international cooperation. To this end, the Budapest Convention on Cybercrime and the benefits of signing and ratifying the Treaty have been presented, together with the envisioned elements of the future Second Additional Protocol [...]. The related domestic legislation of Guyana was also in the focus of the discussions, with the starting point of it having been previously assessed as largely consistent with the substantive and procedural provisions of the Budapest Convention.” READ MORE</p>
<p>Source: Council of Europe</p> <p>Date: 30 Apr 2021</p>	<h2>Octopus project: New translations of the Guide on seizing cryptocurrencies now available</h2> <p>“The Guide on seizing cryptocurrencies developed in the framework of iPROCEEDS-2 project is now available in Portuguese, French and Spanish, in addition to the earlier available versions in English, Albanian, Serbian, Macedonian and Turkish. The Guide aims to serve as “toolbox” for investigators all over the world in hands-on activities related to virtual currencies. It can only be obtained upon request, from the Octopus Platform page. In order to gain access to the document that is restricted to the use of state authorities, an Online request form must be filled-in.” READ MORE</p>
<p>Source: US Department of Justice</p> <p>Date: 28 Apr 2021</p>	<h2>Individual Arrested and Charged with Operating Notorious Darknet Cryptocurrency “Mixer”</h2> <p>“A dual Russian-Swedish national was arrested [...] on criminal charges related to his alleged operation of the longest-running bitcoin money laundering service on the darknet. [...] Over the course of its decade-long operation, Bitcoin Fog moved over 1.2 million bitcoin – valued at approximately \$335 million at the time of the transactions. [...]The Department of Justice’s Office of International Affairs provided invaluable assistance, as did Europol; the Swedish Economic Crime Authority, the Swedish Prosecution Authority, and the Swedish Police; and the General Inspectorate of Romanian Police, Directorate for Combatting Organized Crime and the Directorate for Investigating Organized Crime and Terrorism.” READ MORE</p>

<p>Source: <i>Jornal de Negócios</i></p> <p>Date: 28 Apr 2021</p>	<h2>Portugal: Combate ao cibercrime leva à detenção de seis pessoas na grande Lisboa</h2> <p>“Seis pessoas foram [...] detidas pela Unidade de Combate ao Cibercrime e à Criminalidade Tecnológica da PJ, que realizou 31 buscas numa operação de combate ao acesso indevido a contas bancárias através da internet. Fonte da Polícia Judiciária (PJ) disse à agência Lusa que a operação decorre na zona da grande Lisboa e estão envolvidos cerca de 120 inspetores.” READ MORE</p>
<p>Source: <i>Le Nouvelliste</i></p> <p>Date: 28 Apr 2021</p>	<h2>La criminalité 2.0, une menace invisible pour Haïti</h2> <p>“[...] Même si Haïti a encore le niveau d’interconnexion et d’utilisation d’internet le plus faible de la région”, le “pays commence néanmoins à expérimenter aussi certains aspects de la criminalité cybernétique. [...] les seuls instruments de lutte dont dispose pour l’instant le gouvernement haïtien contre les menaces cybernétiques n’est qu’une simple cellule nouvellement créée au sein du bureau des enquêtes spéciales de la DCPJ, dénommée justement « Cellule contre les crimes cybernétiques (CCCC) ». [...] L’un des premiers efforts diplomatiques à accomplir par le gouvernement haïtien dans ce sens serait de ratifier la Convention de Budapest [...] sur la cybercriminalité.” READ MORE</p>
<p>Source: <i>Ministerio de Relaciones Exteriores y Culto, República de Costa Rica</i></p> <p>Date: 20 Apr 2021</p>	<h2>Costa Rica y Austria sostienen diálogo sobre ciberseguridad</h2> <p>“Funcionarios de la Cancillería y del Ministerio de Ciencia y Tecnología sostuvieron un encuentro virtual con sus contrapartes de Austria [...] con el propósito de intercambiar información y buenas prácticas sobre ciberseguridad. [...] Ambas partes reafirmaron la importancia de la coordinación y cooperación a nivel internacional, destacaron la implementación del Convenio de Budapest como herramienta jurídica. [...] Estos son claros ejemplos de cómo la ciencia y tecnología y la política deben darse la mano para avanzar en un objetivo común. Costa Rica sigue a través de sus diversas representaciones diplomáticas promoviendo los espacios de diplomacia científica y cooperación en el proceso de recuperación post pandemia.” READ MORE</p>
<p>Source: <i>Fiji Village</i></p> <p>Date: 17 Apr 2021</p>	<h2>Fiji: AG says cyber incident contained & more than 30 govt websites accessible</h2> <p>“Minister for Communications and Attorney General, Aiyaz Sayed-Khaiyum confirms the government’s ITC Department has contained the cyber incident identified on the government network. [...] He says the ITC Department is in the advanced stages of a whole-of-government restoration effort following the precautionary service disruptions previously announced. Sayed-Khaiyum adds the remainder of internal systems currently offline, including govnet, are being steadily restored in line with the ITC Department’s internationally-recognised security protocols.” READ MORE</p>

Latest reports

- CRIMRXIV, [Evaluating Criminal Transactional Methods in Cyberspace as Understood in an International](#), 29 April 2021
 - GetTech, [Tech domains cryptocurrency report: the year of the bitcoin bull](#), 15 April 2021
 - Europol, [Internet Organised Crime Threat Assessment \(IOCTA\) 2020](#), April 2021
 - Europol, [European Union Serious and Organised Crime Threat Assessment](#), 12 April 2021
 - CompariTech, [300+ Terrifying Cybercrime and Cybersecurity Statistics & Trends \(2021 EDITION\)](#), 28 April 2021
 - Eset, [A new report reveals London has the highest rate of cybercrime in the UK](#), 20 April 2021
 - ElUniversalDiario: [Relatório de pesquisa de tamanho de mercado Cibercrime e Segurança de 2021 por participação, tendências emergentes, crescimento, segmentação, dinâmica de mercado, receita de vendas e previsão para 2024](#), 30 April 2021
 - Deloitte, [La evolución de la ciberseguridad en el sector de la salud](#), 28 April 2021
 - Le club des juristes, [Le droit pénal à l'épreuve des cyberattaques](#), April 2021
 - Netscout, [Threat intelligence report](#), April 2021
 - Institute for Security and Technology, [RTF Report: Combatting Ransomware](#), 28 April 2021
 - Kaspersky, [Ransomware by the numbers: Reassessing the threat's global impact](#), 23 April 2021
-

Upcoming events

- 4-7 May, C-PROC/AZERBAIJAN, (on-line), Pilot session of online judicial training, [CyberEast](#)
- 6 May, C-PROC/KIRIBATI, Desk Study, Review of the cybercrime and electronic evidence bill (in view of the upcoming second reading in the Parliament), [GLACY+](#)
- 6 May, C-PROC/T-CY, (on-line), Public stakeholders consultations on the 2nd Additional Protocol, [T-CY](#), [Octopus](#)
- 6-7 May, C-PROC/ARMENIA, (on-line), National training exercise on templates of cooperation, [CyberEast](#)
- 7 May, C-PROC/NIGERIA, Desk study on cybercrime legislation and human rights, [GLACY+](#)
- 11 May, C-PROC/ KOSOVO* (on-line), Workshop on cybercrime and cybersecurity trends as well as for criminal justice statistics, [iPROCEEDS-2](#)
- 11 May, C-PROC/ KOSOVO* (desk assessment), Reports on cybercrime and cybersecurity trends as well as for criminal justice statistics, [iPROCEEDS-2](#)
- 11-12 May, C-PROC/MOLDOVA, (on-line), Development of SOPs for CSIRTs/Law Enforcement, stage II (with Cybersecurity EAST project), [CyberEast](#)
- 13 May, C-PROC, (on-line), Webinar on the 2nd Additional Protocol to the Budapest Convention in cooperation with the International Association of Prosecutors(1/4), [GLACY+](#), [Octopus](#)
- 13-14 May, C-PROC/AZERBAIJAN, (on-line), National training exercise on templates of cooperation, [CyberEast](#)
- By 15 May, C-PROC/MALDIVES, Desk Study, Supporting the national effort of aligning the cybercrime legal framework to the provisions of the Budapest Convention, [GLACY+](#)
- May, C-PROC, Desktop Study, Preparation of the country profiles on OCSEA for Benin, Argentina, Brazil, Chile, [Octopus](#), [EndOCSEA@Europe](#)
- May, C-PROC, translation of the Cybercrime and Data Protection Conventions into Amharic language (Ethiopia), [Octopus](#)

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 May have been rescheduled to a later date.

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