

# Cybercrime Digest

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

1-15 July 2020

Source: Council of  
Europe

## The Budapest Convention on cybercrime in operation: new T-CY report

Date: 09 Jul 2020

“The Cybercrime Convention Committee (T-CY) has finalised a new report illustrating the benefits and impact of the Budapest Convention on legislation, domestic and international investigations, public/private cooperation and the strengthening of criminal justice capacities globally. The report highlights: ‘Practical experience shows that the Budapest Convention is more than a legal document. Backed up by the T-CY and the [C-PROC](#) specialised Cybercrime Programme Office for global capacity building, it is a framework that permits hundreds of practitioners from all over the world to share experience and create relationships that facilitate cooperation in specific cases, including in emergency situations, beyond the specific provisions foreseen in this Convention.’ [...] Read the full report: *The Budapest Convention on Cybercrime: benefits and impact in practice* ([EN](#) / [FR](#)) ” [READ MORE](#)

Source: Court of  
Justice of the  
European Union

## The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU- US Data Protection Shield

Date: 16 Jul 2020

“The General Data Protection Regulation provides that the transfer of personal data to a third country may, in principle, take place only if the third country in question ensures an adequate level of data protection. According to the GDPR, the Commission may find that a third country ensures, by reason of its domestic law or its international commitments, an adequate level of protection. In the absence of an adequacy decision, such transfer may take place only if the personal data exporter established in the EU has provided appropriate safeguards, which may arise, in particular, from standard data protection clauses adopted by the Commission, and if data subjects have enforceable rights and effective legal remedies. Furthermore, the GDPR details the conditions under which such a transfer may take place in the absence of an adequacy decision or appropriate safeguards. [...] In today’s judgment, the Court of Justice declares Decision 2016/1250 invalid.” [READ MORE](#)

Source: Council of  
Europe

## C-PROC series of cybercrime webinars continue: materials available, next topics and dates announced

Date: 15 Jul 2020

Initiated in April, the C-PROC series of webinars on cybercrime have continued in the first half of July with more sessions, respectively dedicated to [Cybercrime and Criminal Justice in Cyberspace: Sharing Experience with the African Region](#), co-organized by the European Union and the Council of Europe in the framework of the GLACY+ Project and [International standards on collection and handling of electronic evidence](#), organized under the CyberSouth Project. New webinars are scheduled for the next period: [Cybercrime and Criminal Justice in Cyberspace: Sharing Experience with Latin America and the Caribbean Region](#) (Latin America and Caribbean, EN - 20 July; Latin America and Caribbean, ES - 22 July). For further updates, please check our webinars dedicated [webpage](#).

Source: Council of Europe

## First responders course for African gendarmeries delivered online

Date: 1 Jul 2020

“After being confined at the “Ecole des Officiers de la Gendarmerie National” for three months as a group due to the Covid-19 pandemic, forty-seven gendarmerie officers of seventeen African countries successfully concluded the Council of Europe’s, Regional Training of trainers First responders’ course on cybercrime and electronic evidence gathering. The five-day course was conducted on-line within the framework of the Global Action on Cybercrime Extended project (GLACY+), in collaboration with the Organization of African Gendarmeries (OGA) and the French Gendarmerie. [...] Since the start of this Regional training programme in 2016, over 230 Gendarmerie officers of Benin, Burkina Faso, Cameroun, Congo, Cote d’Ivoire, Djibouti, Gabon, Guinee, Equatorial Guinee, Madagascar, Mali, Mauritania, Niger, Central African Republic, Togo and Senegal were trained as first responders’ instructors.” [READ MORE](#)

Source: Eurojust

## Italian and Romanian judicial authorities, with Eurojust’s support, dismantle major criminal network in financial fraud, cybercrime and money laundering

Date: 07 Jul 2020

“Judicial authorities and police in Italy and Romania, with Eurojust and Europol support dismantled a criminal network responsible for big-scale financial fraud, cybercrime and money laundering. The illicit profits are estimated to over €20 million resulting from the losses suffered by citizens throughout Europe. 12 suspects were arrested today (8 in Italy and 4 in Romania), including the two leaders of the organised criminal group. 12 house searches took place and several assets were seized, including vehicles, credit cards, jewellery, properties, and a numismatic collection with an overall estimated value of over €1.5 million. Today’s action day, coordinated by Eurojust, was the result of intensive cooperation between the judicial and law enforcement authorities in both countries” [READ MORE](#)

Source: Europol

## Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe

Date: 02 Jul 2020

“At a joint press conference today, French and Dutch law enforcement and judicial authorities, [Europol](#) and [Eurojust](#) have presented the impressive results of a joint investigation team to dismantle EncroChat, an encrypted phone network widely used by criminal networks. Over the last months, the joint investigation made it possible to intercept, share and analyse millions of messages that were exchanged between criminals to plan serious crimes. For an important part, these messages were read by law enforcement in real time, over the shoulder of the unsuspecting senders. The information has already been relevant in a large number of ongoing criminal investigations, resulting in the disruption of criminal activities including violent attacks, corruption, attempted murders and large-scale drug transports. Certain messages indicated plans to commit imminent violent crimes and triggered immediate action. The information will be further analysed as a source of unique insight, giving access to unprecedented volumes of new evidence to profoundly tackle organised criminal networks.” [READ MORE](#)

### RELATED ARTICLES

Schneier On Security, [EncroChat Hacked by Police](#), 03 July 2020

Source: Europol

Date: 08 Jul 2020

## Massive investigation in Italy combating online child sexual abuse

"A successful investigation to tackle online child abuse conducted by the Italian State Police (Polizia di Stato) of Turin and supported by Europol, has led to 50 investigations and several searches across the country. Working from referrals through Europol by the Canadian National Child Exploitation Coordination Centre (NCECC), investigators targeted suspects producing, exchanging and possessing child sexual abuse material. Europol handles the receipt, processing and onward distribution of these intelligence reports from Canada to all of the EU Member States. In this case, the data was sent by Europol in mid-January 2019. The Turin Prosecutor's Office directed the "Operation 50 Community" investigation which was coordinated by the Italian Postal and Communications Police National Centre for Countering Child Abuse Online (CNCPO) and involved 200 investigators across Italy." [READ MORE](#)

Source: UN News

Date: 06 Jul 2020

## Terrorist groups must not be allowed to exploit 'fragilities' caused by global health pandemic

"While the [coronavirus](#) has put the international community in the crosshairs of a crisis like no other since the founding of the United Nations 75 years ago, António Guterres noted that "like the virus, terrorism does not respect national borders". "It affects all nations and can only be defeated collectively", he said, opening the second annual gathering of UN and international experts known as [Counter-Terrorism Week](#), held virtually this year, with a call to "harness the power of multilateralism to find practical solutions". Acknowledging that it is "too early to fully assess the implications of [COVID-19](#) on the terrorism landscape" the UN chief [told](#) the first of series of virtual interactive discussions on strategic and practical challenges of countering terrorism during a global pandemic that ISIL, Al-Qaida, neo-Nazis and other hate groups "seek to exploit divisions, local conflicts, governance failures and grievances to advance their objectives". [READ MORE](#)

Source: France  
Diplomatie

Date: 01 Jul 2020

## Déclaration conjointe de la France et de l'Estonie sur la coopération dans le domaine de la cybersécurité

"Le cyberspace joue un rôle désormais central dans le fonctionnement de nos sociétés sous l'effet de la transformation numérique et des évolutions technologiques (intelligence artificielle, objets connectés, robotique, 5G et bientôt 6G, informatique en nuage, informatique et communication quantiques...). Celles-ci produisent leurs effets au niveau national mais aussi européen et mondial. La pandémie de COVID19 a renforcé davantage ce rôle et a confirmé à quel point il est essentiel de défendre un cyberspace sûr, stable, ouvert et libre dans une situation de recours massif aux outils numériques pour accéder à l'information, travailler, apprendre et maintenir des liens sociaux. (...) Sur le plan bilatéral, la France et l'Estonie ont érigé les enjeux de cybersécurité en tant que priorité stratégique de leur politique étrangère. Nous avons conclu ensemble plusieurs protocoles d'entente et agréé des feuilles de route communes dans différents domaines de la cybersécurité et de la cyberdéfense." [READ MORE](#)

Source: *Sénat  
France*

Date: 09 Jul 2020

## Cybercriminalité: un défi que les sénateurs appellent à relever aux niveaux national et européen

"La commission des lois et la commission des affaires européennes du Sénat, réunies conjointement le 9 juillet 2020, ont adopté le rapport d'information de Sophie Joissains et Jacques Bigot, rapporteurs, sur la lutte contre la cybercriminalité. La cybercriminalité est une délinquance protéiforme, dont l'actualité fournit des exemples quotidiens ("rançongiciels", contenus frauduleux et trafics divers en ligne, en particulier sur le *dark web*, "hameçonnage", etc.) qui concernent tant les entreprises ou les administrations que les particuliers. Son ampleur reste difficile à évaluer car les plaintes et signalements sont loin d'être systématiques." [READ MORE](#)

Source: *CNN  
Business*

Date: 15 Jul 2020

## Twitter blames 'coordinated' attack on its systems for hack of Joe Biden, Barack Obama, Bill Gates and others

"Twitter accounts belonging to Joe Biden, Bill Gates, Elon Musk and Apple, among other prominent handles, were compromised on Wednesday in what Twitter said it believes to be an attack on some of its employees with access to the company's internal tools. "We detected what we believe to be a coordinated social engineering attack by people who successfully targeted some of our employees with access to internal systems and tools," Twitter's support team said late Wednesday. The attackers posted tweets that appeared to promote a cryptocurrency scam." [READ MORE](#)

Source: *Security  
Intelligence*

Date: 07 Jul 2020

## COVID-19 Cybercrime Capitalizing on Brazil's Government Assistance Program

"We examine how cybercriminals are capitalizing on COVID-19 in Brazil — the most populous country in South America and second in the world for the number of coronavirus infections as of early June — by delivering malicious email, SMS text and WhatsApp messages and creating hundreds of malicious sites since March 2020. In particular, our analysts found that over 693 new COVID-19-related Brazilian cybercriminal malicious websites have been created this year, many capitalizing on the country's government assistance program related to the pandemic." [READ MORE](#)

Source: *Politico*

Date: 06 Jul 2020

## Early Covid-19 tracking apps easy prey for hackers, and it might get worse before it gets better

"The push to use smartphone apps to track the spread of coronavirus is creating a potential jackpot for hackers worldwide. [...] In the Qatar Covid-19 app, researchers found a vulnerability that would've let hackers obtain more than a million people's national ID numbers and health status. In India's app, a researcher discovered a security gap that allowed him to determine who was sick in individual homes. And researchers uncovered seven security flaws in a pilot app in the U.K. The U.S. is just starting to use these contact tracing apps — which track who an infected person may have had contact with — but at least one app has already experienced a data leak. North Dakota conceded in May that its smartphone app, Care19, had been sending users' location data to the digital marketing service Foursquare." [READ MORE](#)

Source: SA  
Government News  
Agency

Date: 02 Jul 2020

## South Africa: NCOP approves Cybercrimes Bill, two amendment bills

"The National Council of Provinces (NCOP) has passed the Cybercrimes Bill, Civil Union Amendment Bill and the Science and Technology Laws Amendment Bill during its sitting on Wednesday. The Cybercrimes Bill was initially introduced as the Cybercrimes and Cybersecurity Bill in 2017, and was referred to the fifth democratic Parliament's Select Committee on Security and Justice from the National Assembly on 27 November 2018. The Bill was thoroughly advertised for public participation in 2019, where substantive inputs were provided by various stakeholders and individuals. (...) The objectives of the Bill are, among others, to create offences and impose penalties which have a bearing on cybercrime, to criminalise the distribution of data messages which are harmful and to provide for interim protection orders, and to further regulate jurisdiction in respect of cybercrimes. The bill also aims to regulate the powers to investigate cybercrimes, to further regulate aspects relating to mutual assistance in respect of the investigation of cybercrimes and to provide for the establishment of a 24/7 Point of Contact. The bill further imposes obligations on electronic communications service providers and financial institutions to assist in the investigation of cybercrimes. It also provides that the executive may enter into agreements with foreign states to promote cybersecurity."

[READ MORE](#)

Source: Punch

Date: 10 Jul 2020

## Nigeria, ECOWAS Court orders Federal Government to repeal cybercrime law

"The ECOWAS Court of Justice sitting in Abuja, on Friday, ordered the Federal Government of Nigeria to repeal or amend the provision of its cybercrimes law which violates citizens' right of expression. Delivering the judgment of the three-man panel of the court, Justice Januaria Costa ordered the Nigerian government to make the law to align with its obligation under Article 1 of the African Charter on Human and Peoples' Rights and the International Covenant on Civil and Political Rights. A summary of the judgment released by the court's media unit on Friday stated that the verdict "held the Nigerian government liable for the violation of the right to freedom of expression" with the enactment of section 24 of the Cybercrime Act, 2015."

[READ MORE](#)

Source: Cross-  
Border Data Forum

Date: 6 Jul 2020

## How African countries can benefit from the emerging reform initiatives of cross-border access to electronic evidence

"How do African law enforcement authorities access African data held by US companies for the purpose of legitimate criminal investigations? How—and to what extent— can African countries benefit from the cross-border data access reform initiatives emerging in Europe and the US? How should African stakeholders approach the internet's increasing cross-border legal challenges? These are some of the questions raised at one of the sessions of the recent virtual conference hosted by the Internet & Jurisdiction Policy Network (I&J) in partnership with the African Union Commission (AUC). The conference brought more than 130 participants of key regional stakeholders together to discuss a range of transnational and regional challenges in cyberspace, including cross-border access to electronic evidence."

[READ MORE](#)

Source: Forbes  
México

Date: 09 Jul 2020

## Mexico: Coparmex propone reformas para combatir ciberataques

“La Confederación Patronal de la República Mexicana (Coparmex) propuso este jueves reformas a la Ley Federal de Telecomunicaciones para combatir y sancionar casos de hackeo, sabotaje y cualquier tipo de delito cibernético. La organización propuso agregar a la ley un artículo 190 bis 2 para añadir que la obligación de preservar una dirección IP durante tres meses en vivo y tres de almacenamiento, tal como establece el Convenio de Budapest sobre ciberdelincuencia, a fin de permitir que el ministerio público cuente con información, previa orden judicial.” [READ MORE](#)

Source: FBC News

Date: 08 Jul 2020

## FIJI: FHRDC supports enactment of proposed Cybercrime Bill

“The Fiji Human Rights and Anti-Discrimination Commission has supported the enactment of the proposed Cybercrime Bill (2020). In its submission to the Parliamentary Standing Committee on Justice, Law and Human Rights the Commission has recommended that the moral and legal imperatives of this legislation be balanced with the States human rights obligations under the Fijian Constitution and its obligations under international law. Director Ashwin Raj also recommended that Fiji considers ratification of the Convention on Cybercrime or the Budapest Convention to ensure compliance with normative instruments.” [READ MORE](#)

Source: ABC News

Date: 10 Jul 2020

## Australia: Australia's cyber security watch room is monitoring threats 24/7. Here's what it's like inside

“For a dedicated few, keeping Australia safe online starts in the early hours of the morning. That's when the day shift starts for analysts in the Australian Cyber Security Centre's 24/7 watch room. Their Canberra headquarters looks like any other nondescript government building but, a few steps inside the lobby, a lattice made up of zeros and ones provides a clue as to what's going on inside. Now more than ever, Australians are living their lives online. And every connection for work, school or leisure creates a new vulnerability. Prime Minister Scott Morrison's [unusual press conference](#) in June declaring that Australia was under sustained attack came after months of warnings that the COVID-19 pandemic [was providing a valuable opportunity](#) for criminals..” [READ MORE](#)

## Latest reports

- Council of Europe, [Cybercrime and COVID19 webpage](#), updated weekly
- EndOCSEA@Europe, [Publication of the "So this is sexual abuse?" booklet, laid out in eight languages](#), 9 July 2020
- Council of Europe, [Second plenary meeting of the Ad Hoc Committee on Artificial Intelligence \(CAHAI\)](#), 6 July 2020
- INTERPOL, [Report: Criminals infiltrating Africa's booming mobile money industry](#), 06 July 2020
- Europol, [CONSOLIDATED ANNUAL ACTIVITY REPORT \(CAAR\) 2019](#), 02 July 2020
- ENISA, [Cybersecurity Certification: EUCC Candidate Scheme](#), 02 July 2020
- ENISA, [Trust Services Security Incidents 2019 Annual Analysis Report](#), 10 July 2020
- Europol, [Online Safety – Advice for young children, parents and carers](#), 08 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 July, Participation in the First Virtual Meeting of FOPREL on impacts of COVID 19 in the region, [GLACY+](#)
- 16 July, Online meeting on Adaptation of Judicial Training Manual, Tunisia, [CyberSouth](#)
- 16-17 July, Online Regional Workshop on Cybercrime Legislation in Caribbean Region, in collaboration with CARICOM IMPACS, [GLACY+](#)
- 20 July, EU-CoE joint **Webinar** on Criminal justice and cybercrime in cyberspace for Latin America and the Caribbean Region (EN), [GLACY+](#)
- 20-22 July, Online workshop, West African School on Internet Governance (v-WASIG) ECOWAS, [GLACY+](#)
- 21 July, GLACY+ 8th Steering Committee online meeting, [GLACY+](#)
- 21-22 July, Desk Study on review of cybercrime legislation and online national workshop for presentation of results, Papua New Guinea, [GLACY+](#)
- 22 July, EU-CoE joint **Webinar** on Criminal justice and cybercrime in cyberspace for Latin America and the Caribbean Region (ES), [GLACY+](#)
- 23-24 July, Online workshop, First HELP Working Group Meeting, [GLACY+](#)
- 28 July, Online regional workshop on Establishment and functioning of the 24/7 POC Network in Africa, [GLACY+](#)
- 29 July, Online regional workshop on Establishment and functioning of the 24/7 POC Network in Asia-Pacific, [GLACY+](#)
- 29-30 July, Online workshop for Review of cybercrime legislation and On-line national workshop for presentation of results, Maldives, [GLACY+](#)
- 29 July, Regional online Event on Legislation and International Cooperation, [CyberSouth](#)
- 30 July, **Webinar** on Cyberviolence against Women on 30 July (dates TBC), [CyberEast](#)
- 30 July, Online regional workshop on Establishment and functioning of the 24/7 POC Network in Latin America, [GLACY+](#)
- 31 July, Desk Study for the review of Cybercrime Legislation of Botswana, [GLACY+](#)

- 31 July, Desk Study on the review of the Introductory Judicial Course on Cybercrime and Electronic Evidence, [GLACY+](#)
- By 31 July, Production of thematic video on election interference to support elections security in Georgia, [CyberEast](#)
- By 31 July, Desk studies for International Cooperation and Judicial Training systems and capabilities, [CyberSouth](#)
- By 31 July, Desk research: Assessment of compliance of procedural law frameworks in line with Articles 16 to 21 Budapest Convention and related legislation (including data protection), Albania, [iPROCEEDS-2](#)
- By 31 July, Desk research: Assessment of compliance of procedural law frameworks in line with Articles 16 to 21 Budapest Convention and related legislation (including data protection), Montenegro, [iPROCEEDS-2](#)
- By 31 July, C-PROC, Desk research: Assessment of compliance of procedural law frameworks in line with Articles 16 to 21 Budapest Convention and related legislation (including data protection), North Macedonia [iPROCEEDS-2](#)
- 30 July, **Webinar** on Cyberviolence against Women on 30 July (dates TBC), [CyberEast](#)
- By 31 July, Production of thematic video on election interference to support elections security in Georgia, [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](mailto:cybercrime@coe.int)

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

