Cybercrime Digest

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

01 – 15 June 2022

Source: Council of Europe

Date: 14 June 2022

Costa Rica becomes 24th State to sign the Second Additional Protocol to the Convention on Cybercrime

"The new Protocol on enhanced co-operation and disclosure of electronic evidence was opened for signature on 12 May 2022 within the framework of an international conference in Strasbourg, France. Yesterday, 13 June 2022, Mr Sergio Vinocour Fornieri, Chargé d'affaires a.i. of Costa Rica in France, also signed the Protocol in the presence of Björn Berge, Deputy Secretary General of the Council of Europe, bringing the number of signatories up to 24. He underlined that the massive cyberattacks against Costa Rican institutions last month demonstrated the urgent need for States to implement and ratify this Protocol so that its tools become available as soon as possible." READ MORE

RELATED ARTICLE:

Ministerio de Relaciones Exteriores, Costa Rica firma protocolo internacional para acceder a asistencia mutua de urgencia y combatir la Ciberdelincuencia, 14 June 2022

Source: Global Initiative Against Translational Organized Crime

Date: 15 June 2022

Under the microscope. Delegates get into the details as UN cybercrime negotiations move forward

"Member states appeared to be in relative agreement on the overall purpose of the treaty, which would have three main objectives: combating and preventing crimes committed using ICTs; promoting international cooperation; and technical assistance, following the broad structure and purposes of the UN Convention against Transnational Organized Crime and UN Convention Against Corruption. However, critical debates on key terminology persist, such as the term 'computer data' (used in the Budapest Convention) versus 'digital information', Russia's preferred expression. These highly detailed questions relate to the issues of how broad the convention will be, what norms it will set for cyber issues and how much will be taken from existing agreements or redefined." READ MORE

RELATED ARTICLE:

Gacetin Madrid, El senador José Cepeda solicita catalogar a los parlamentos del mundo como «infraestructuras críticas» por el aumento de ciberataques tras la pandemia, 1 June 2022

Article 19, UN: Cybercrime treaty must enhance human rights protections - ARTICLE 19, 1 June 2022

Source: The Print

Date: 10 June 2022

7 yrs after 'draconian' Sec 66A was quashed, India proposes identical steps at UN conference

"New Delhi: An Indian delegation to a UN conference on cybercrime in Vienna has proposed the use of measures that are almost identical to those in the controversial Section 66A of the Indian Information Technology Act, which was struck down as unconstitutional by the Supreme Court in 2015. […] According to this law, which was introduced by the then UPA government in 2008, any individual found sending "grossly offensive", "menacing", and incorrect information could be prosecuted. These infractions were "punishable with imprisonment for a term which may extend to three years and with fine." READ MORE

RELATED ARTICLE:

The Wire, Modi Government Defies Supreme Court, Seeks Return of 66A Curbs on Online Speech Via UN Treaty, 9 June 2022

Source: Interpol

Date: 1 June 2022

New campaign highlights digital extortion threats and how to keep safe

"INTERPOL's latest awareness campaign wants to remind the public that cyberattacks can happen to everyone, and at any time. Launched today, the #YouMayBeNext campaign will focus on cybercrimes that involve extortion including: sextortion, ransomware, and distributed Denial-of-Service (DDoS) attack. […] More than 60 countries, private-sector partners, non-governmental organizations (NGOs) and international organizations will take part in this campaign. Specifically, they will support INTERPOL's outreach efforts by sharing information on recent cybercrime trends, as well as the tools that members of the public can use to protect themselves." READ MORE

Source: Europol

Date: 08 June 2022

Suspect arrested in Slovakia for spreading hate speech and 3D printed weapons manuals

"An investigation by the Slovak National Crime Agency (Národná kriminálna agentúra/NAKA), the Slovak Military Intelligence (Vojenské spravodajstvo), the Slovak Police (Príslušníci / PZ SR), supported by the Czech National Organized Crime Agency (Národní centrála proti organizovanému zločinu/NCOZ), the US FBI, Europol and Eurojust, led to the arrest of a dangerous right-wing extremist. The individual, known in the international far-right cyberspace, is suspected of spreading extremist hate speech and terrorist activities. Linked to groups and individuals spreading neo-Nazi, far-right and white supremacist extremist propaganda, he is part of the so-called Siege extremist movement. This online extremist community is connected online, though simultaneously grounded in 'offline action'." READ MORE

Source: Council of Europe

Date: 2 June 2022

International Network of National Judicial Trainers: first 2022 call of the Steering Committee

"The focal points of participating countries in the International Network of National Judicial Trainers reunited online for the 2022 first meeting of the Steering Committee, the advisory board of the community. The Secretariat recollected the decisions of the last Plenary meeting that took place in March 2022 and facilitated the discussions on setting up the ad-hoc working groups, as well as on the working methods and the expected calendar for implementing the activities of each of the three groups: draft a guidebook/toolkit on judicial training strategies on cybercrime and electronic evidence, elaborate a mapping study on cyberviolence legislation, and develop a study on best practices on admissibility of electronic evidence." READ MORE

Source: Europol

Date: 1 June 2022

Takedown of SMS-based FluBot spyware infecting Android phones

"An international law enforcement operation involving 11 countries has resulted in the takedown of one of the fastest-spreading mobile malware to date. Known as FluBot, this Android malware has been spreading aggressively through SMS, stealing passwords, online banking details and other sensitive information from infected smartphones across the world. Its infrastructure was successfully disrupted earlier in May by the Dutch Police (Politie), rendering this strain of malware inactive." READ MORE

Source: EUROJUST

Date: 14 June 2022

Judicial experts discuss cryptocurrency challenges

"During the 12th EJCN Plenary, judicial experts and practitioners in the field of cybercrime will analyse the current EU framework on virtual currencies and how it can address cyber-enabled crime. Various legal and practical aspects of the seizure of virtual currencies and blockchain-based assets will be presented at the meeting. Based on the experience of the takedown of the Hydra Marketplace, the world's largest marketplace on the dark web, participants will explore the advantages of cooperating with the private sector when it comes to seizing assets and compensating victims of cybercrime." READ MORE

Source: Krebs on Security

Date: 14 June 2022

Ransomware Group Debuts Searchable Victim Data

"Cybercrime groups that specialize in stealing corporate data and demanding a ransom not to publish it have tried countless approaches to shaming their victims into paying. The latest innovation in ratcheting up the heat comes from the ALPHV/BlackCat ransomware group, which has traditionally published any stolen victim data on the Dark Web. Today, however, the group began publishing individual victim websites on the public Internet, with the leaked data made available in an easily searchable form." READ MORE

Source: The Guardian

Date: 14 June 2022

US defence contractor in talks to take over NSO Group's hacking technology

"The US defence contractor L3Harris is in talks to take over NSO Group's surveillance technology, in a possible deal that would give an American company control over one of the world's most sophisticated and controversial hacking tools. Multiple sources confirmed that discussions were centred on a sale of the Israeli company's core technology – or code – as well as a possible transfer of NSO personnel to L3Harris. But any agreement still faces significant hurdles, including requiring the blessing of the US and Israeli governments, which have not yet given the green light to a deal." READ MORE

Source: Tech Crunch

Date: 14 June 2022

Nigeria's internet regulator releases draft to regulate Google, Facebook, TikTok and others

"Nigeria has announced plans to regulate internet companies like Facebook, WhatsApp, Instagram (all owned by Meta), Twitter, Google and TikTok in a draft shared by the country's internet regulator. […] NITDA's draft is the latest development on this front, and according to some Nigerians, it'll probably end there. But others worry that the Nigerian government might take things too far and suspend the operations of these internet platforms just as it did with Twitter, should they not adhere to its regulations." READ MORE

Source: MENA FN

Date: 14 June 2022

Kenya establishes forensic lab to combat cybercrime

"Kenyan President Uhuru Kenyatta launched the national forensic laboratory on Monday to enhance the country's fight against cybercrime, which has been escalating due to the fast expansion of the country's digital economy. Kenyatta stated that the government will use training and increased public participation to combat rising security risks as cybercrime, terrorism, and human trafficking." READ MORE

Source: ADIAC-Congo

Date: 9 June 2022

Cyberespace : le Congo initie l'Alliance africaine pour la cybersécurité

"L'Alliance africaine pour la cybersécurité a été officiellement lancée à Marrakech, lors de la neuvième édition du forum sur la cybersécurité, Sitafrica, dédié aux décideurs africains en la matière, qui s'est tenu les 17, 18, 19 et 20 mai dernier. Ayant comme objectif de réunir les clubs DSI africains afin de créer un réseau de collaboration et d'échange autour de meilleures pratiques de cybersécurité, cette alliance a été matérialisée le 19 mai par la Déclaration de Marrakech avec l'ensemble des signataires." READ MORE

Source: The Namibian

Date: 8 June 2022

Govt criticised for 'enabling online violence'

"The Namibian government has been criticised for its lack of urgency to put in place cybercrime and data-protection laws. This has led to online gender-based violence (GBV) thriving in the country, a report launched yesterday, says. […] "The government's lack of urgency in introducing appropriate legislative measures, enforcing existing laws, and providing supportive education seems to be enabling rather than curtailing online violence in Namibia," the report reads. […] This claim was highlighted by the police's cybersecurity department head, chief inspector Ratjindua Tjivikua, who says there is no political will to address online crimes in the country, and civil society has been dormant on the matter. "The cybercrime bill has been pushed around. It went up to parliament, but it was pushed back. Afterwards, we had a lot of consultations regarding that bill. We need political will, and support of civil society. We are stagnated," he says." READ MORE

Source: OSIRIS Senegal

Date: 13 June 2022

Lutte contre la cybercriminalité : fructueux partenariat entre l'Office Central de Répression de la Cybercriminalité (OCRC) du Bénin et le Service de Sécurité Intérieure (SSI) de l'ambassade de France

"La récente condamnation par la justice béninoise de sept (7) individus qui avaient été interpellés le 12 mars 2021 par l'OCRC, appuyé techniquement par le SSI de l'ambassade de France, témoigne de la qualité du partenariat franco-béninois en matière de lutte contre la cybercriminalité. Les mis en cause ont été déclarés coupables d'escroquerie par le biais d'un système informatique." READ MORE

Source: STJ

Date: 14 June 2022

Syria: Cybercrime Law is an Additional Tool for Suppressing Freedom of Expression

"On 18 April 2022, Syrian President Bashar al-Assad issued Law No. 20 of 2022, relative to cybercrime. The law provides for reorganizing criminal legal rules governing digital crime included in Legislative Decree No. 17 of 2012. The target degree frames the enforcement of the provisions of the Law of Network Communication against Cybercrime. The Syrian legislative authority commented on the law's timing, saying the law responds to peaking rates of cybercrime within the Syrian community due to technical and technological progress. Therefore, the law was issued to protect legal interests, regulate freedoms in cyberspace, and limit "misuse of technology." READ MORE

Source: Civicus Monitor

Date: 14 June 2022

Freedom Of Expression At Risk As Cybercrime Legislation Used To Prosecute Online Critics In Vanuatu

"The state of civic space in Vanuatu is rated as 'narrowed' by the CIVICUS Monitor. There are new concerns about restrictions to freedom of expression in Vanuatu following the arrest of individuals for allegedly posting comments on social media speculating that politicians were responsible for the country's current COVID-19 outbreak. The charges relate to alleged comments on Facebook claiming that two politicians in the country had breached COVID quarantine protocols, one of whom had played a role in the community transmission of the virus. According to The Guardian, a police crackdown on 11th May 2022 saw four people on two separate islands arrested as part of a major investigation by Vanuatu's Serious Crime Unit, including a factory worker, a printer, a business owner and a Facebook page moderator. They face charges of cyber stalking, cyber slander and cyber libel and face up to three years in prison and excessive fines of up to three million Vatu (USD 25,838)." READ MORE

Source: Check Point research

Date: 14 June 2022

Iranian Spear-Phishing Operation Targets Former Israeli and US High-Ranking Officials

"Check Point Research uncovers a recent Iranian-based spear-phishing operation aimed against former Israeli officials, high-ranking military personnel, research fellows in research institutions, think tanks, and against Israeli citizens. The attacks use a custom phishing infrastructure, as well as a wide array of fake email accounts to impersonate trusted parties. To establish deeper trust with new targets, the threat actors performed an account takeover of some victims' inboxes, and then hijacked existing email conversations to start attacks from an already existing email conversation between a target and a trusted party and continue that conversation in that guise." READ MORE

Source: Caracol

Date: 6 June 2022

Fuerte aumento de ataques Ransomware a América latina preocupa expertos

"Después de que se presentaran varios ataques Ransomware a instituciones importantes latinoamericanas, como al gobierno de Costa Rica (que afectó a múltiples organismos), la Secretaría de Estado de Finanzas de Río de Janeiro y la Agencia de Inteligencia de Perú, los analistas en ciberseguridad están preocupados porque lo mismo suceda en Colombia. [...] Según el experto no hay protocolos claros de seguridad, razón por la cual muchas personas y empresas son blancos fáciles de los ciberdelincuentes. Además asegura que en Colombia hay una vulnerabilidad latente debido a la desinformación sobre el tema." READ MORE

Source: Krebs on Security

Date: 3 June 2022

What Counts as "Good Faith Security Research?"

"The U.S. Department of Justice (DOJ) recently revised its policy on charging violations of the Computer Fraud and Abuse Act (CFAA), a 1986 law that remains the primary statute by which federal prosecutors pursue cybercrime cases. The new guidelines state that prosecutors should avoid charging security researchers who operate in "good faith" when finding and reporting vulnerabilities. […] The new DOJ policy comes in response to a Supreme Court ruling last year in Van Buren v. United States, a case involving a former police sergeant in Florida who was convicted of CFAA violations after a friend paid him to use police resources to look up information on a private citizen. But in an opinion authored by Justice Amy Coney Barrett, the Supreme Court held that the CFAA does not apply to a person who obtains electronic information that they are otherwise authorized to access and then misuses that information." READ MORE

RELATED ARTICLES:

JD Supra, DOJ Revises CFAA Charging Policy to Provide Clarity for Cybersecurity Research and Terms of Use, 2 June 2022

Cyber Scoop, DOJ changes to CFAA guidance are overhyped, lawyers say, 7 June 2022

Source: Bahia Jornal

Date: 8 June 2022

Brasil foi alvo de ataques do grupo de crimes cibernéticos Lazarus

"Durante a conferência ESET World 2022, especialistas da ESET, empresa líder em detecção proativa de ameaças, apresentaram uma nova investigação sobre o grupo Lazarus APT. O diretor responsável pela pesquisa ESET Threat Research, Jean-Ian Boutin, repassou novas campanhas praticadas pelo grupo Lazarus contra empresas de defesa em todo o mundo entre o final de 2021 e março de 2022." READ MORE

Source: Reuters

Date: 14 June 2022

Canada wants companies to report cyber attacks and hacking incidents

"Canadian businesses operating in critical infrastructure sectors would be required to report cyber attacks to the federal government and would have to fortify their cyber systems under a new law introduced on Tuesday. […] Bill C-26, which has not yet been debated or passed, would also bar telecom companies from using the products and services of high-risk suppliers, according to a statement from the government." READ MORE

RELATED ARTICLE:

Cision, Government introduces new legislation to protect Canada's cyber security, 14 June 2022

Source: Bloomberg

Date: 15 June 2022

Evidence Avalanche Prompts Less-Is-More Pivot by US Prosecutors

"Prosecutors struggling to pore through mushrooming amounts of electronic data they uncover during corporate crime investigations are beginning to hear counterintuitive advice from the Justice Department: Collect less evidence. The nascent strategy of selectively seizing fewer computers, cell phones, and hard drives coincides with an exponential growth of available e-data. It comes amid repeated DOJ failures in processing and turning over evidence to the defense." READ MORE

Source: El Nuevo Herald

Date: 1 June 2022

Nuevo ciberataque afecta sistemas de seguridad en Costa Rica

"Un nuevo ciberataque obligó el martes a la Caja Costarricense del Seguro Social (CCSS) a apagar todos sus sistemas informáticos para evitar el secuestro de sus bases de datos. […] Según la CCSS, solo han identificado 30 de sus más de 1.500 servidores como infectados con el ransomware que identificaron como "Hive", que sería distinto al utilizado por Conti en sus ataques anteriores a entidades del gobierno en Costa Rica." READ MORE

Source: PC Mag

Date: 9 June 2022

DOJ: China Is Still the Biggest US Cyber Threat, But Don't Ignore Russia

"Russia's invasion of Ukraine and its accompanying geopolitical turmoil may be occupying US adversaries, but they're still a threat to the US in cyberspace. That's the message Matthew Olson, Assistant Attorney General for National Security at the Department of Justice, had for attendees at this year's RSA Conference in San Francisco." READ MORE

RELATED ARTICLE:

VOA News, US Justice Department Braces for More Russian Cyberattacks, 2 June 2022

Source: ENISA

Date: 9 June 2022

Cyber Europe 2022: Testing the Resilience of the European Healthcare Sector

"If health services and infrastructures in Europe were the object of a major cyber-attack, how would we respond and coordinate at both national and EU level to mitigate the incidents and prevent an escalation?

This is the question Cyber Europe 2022 sought to answer using a fictitious scenario. Day one featured a disinformation campaign of manipulated laboratory results and a cyber-attack targeting European hospital networks. On day two, the scenario escalated into an EU-wide cyber crisis with the imminent threat of personal medical data being released and another campaign designed to discredit a medical implantable device with a claim on vulnerability." READ MORE

Source: Poynter

Date: 9 June 2022

Turkish 'disinformation law' will make it a crime to spread 'fake news'

"A "disinformation law" that, if passed, would impose up to three-year jail sentences for the spread of "fake news" or "disinformation," has been sitting in Turkish parliament for years. While the bill itself makes no attempt to define fake news or false information, independent journalists in the country speculate the so-called "disinformation" law may be a euphemism. In fact, the law could be a way of securing authoritarian control in the country by giving outsized power to censor and restrict information flow to President Recep Tayyip Erdoğan's government." READ MORE

Source: The Wall Street Journal

Date: 14 June 2022

Ukraine Has Begun Moving Sensitive Data Outside Its Borders

"Ukrainian government officials have begun storing sensitive data outside the country to protect it from Russian cyber and physical assault, and are negotiating with several European nations to move more databases abroad. Since the start of the war, around 150 registries from different government ministries and offices, or backup copies of them, have been moved abroad or are in discussions to be transferred, said George Dubinskiy, Ukraine's deputy minister of digital transformation." READ MORE

Latest reports

- Insight Crime, From Copper Theft to Ransomware - Chile's Criminal Challenges Begin to Mount, 1 June 2022
- Jus.com Brazil, Lei Geral de Proteção de Dados: A discussão da Implementação, regulamentação e responsabilização da LGPD dentro das empresas e advocacias na realidade brasileira, 1 June 2022
- Bloomberg Linea, Las 10 empresas con más ataques de phishing podría ser una de las que estás usando, 2 June 2022
- MediaNama, Ransomware And Human Exploitation The Two Biggest Threat Patterns To Cybersecurity: Verizon Report, 3 June 2022
- Conteudo juridico, Crimes virtuais: crimes cibernéticos e as considerações sobre a criminalidade na internet, 3 June 2022
- Wired, Smartphones Blur the Line Between Civilian and Combatant, 6 June 2022
- ASPI, Countering the Hydra: A proposal for an Indo-Pacific hybrid threat centre, 7 June 2022
- CISA, People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices, 7 June 2022
- Computer weekly, Ataques amenazan las inversiones digitales de las empresas, 7 June 2022
- Global Village Spac, Cyber-crimes and cyber security in Pakistan, 8 June 2022
- Lawyer Monthly, The Impact of Digital Forensics on Legal Proceedings, 9 June 2022
- This Day, Rising Trends of Cyberattacks in Nigeria, 9 June 2022
- Data News Belgium, Les cyber-attaques lancées sur les structures industrielles coûtent des millions aux firmes, 9 June 2022
- Manila Times, Cybersecurity skills gap contributed to 71% of breaches in Asia, 11 June 2022
- Munich Re, Global Cyber Risk and Insurance Survey 2022, June 2022
- Cybereason, Ransomware: The True Cost to Business, June 2022

Upcoming events

- 14 - 16 June, C-PROC/CZECH REPUBLIC, (in person), participation of Bosnia and Herzegovina authorities at ISS World Europe 2022, iPROCEEDS-2
- 15 June, C-PROC/BOSNIA AND HERZEGOVINA, (in person), Domestic meetings to support public/private initiatives at domestic level with a focus on cooperation between service providers and criminal justice authorities, iPROCEEDS-2
- 15 June, C-PROC/KOSOVO, (in person), Domestic meetings to support public/private initiatives at domestic level with a focus on cooperation between service providers and criminal justice authorities, iPROCEEDS-2
- 15/17 June, C-PROC/TURKIYE, (in person), Training skill certification programme for judges and prosecutors delivering Council of Europe judicial training on cybercrime and electronic evidence, iPROCEEDS-2
- 16-17 June, C-PROC, (in-person), 8th Steering Committee Meeting, Bucharest, Romania), CyberSouth
- 20 - 22 June, C-PROC/INTERPOL/PARAGUAY, (hybrid), Advisory mission on search, seizure, and confiscation of online proceeds of crime, GLACY+
- 20 June – 8 July, C-PROC/INTERPOL/ECOWAS, (online), Training of Trainers E-FIRST ECTEG Course, Cybercrime, and digital forensics specialized training for law enforcement officers, GLACY+
- 20 - 21 June, C-PROC/CAPE VERDE, (hybrid), Advisory workshop on the streamlining of procedures for mutual legal assistance enhanced by the Second Additional Protocol related to cybercrime and electronic evidence, GLACY+
- 20 - 22 June, C-PROC/ITALY, (hybird), Participation in EuroDIG 2022 / Subtopic 3 on Budapest Convention, CyberEast
- 20-24 Jun, C-PROC/SENEGAL, (hybrid), 1st Responders Training of Trainers for the Petty Officers Gendarmerie of Senegal, GLACY+
- 21 June, C-PROC/ALGERIA, (online), National Workshop on the Second Additional Protocol, CyberSouth
- 22 - 24 June, C-PROC/CAPE VERDE, (hybrid), Specialized course on International Cooperation for Prosecutors and Judges, GLACY+
- 22 - 23 June, C-PROC/Romania (in person), International meeting on launching version 3.0 of the Electronic Evidence Guide, workshops on best practices when collecting E-evidence, iPROCEEDS-2
- 23 June, C-PROC/FIJI, (in-person), Series on workshops on the new cybercrime act and international standards: first workshop for judges, GLACY+, Octopus
- 23 - 24 June, C-PROC/ROMANIA, (in person), Regional cooperation forum of cybercrime and cybersecurity experts (with CyberSecurity EAST) - Cooperation networks, CyberEast
- 24 June, C-PROC/FIJI, (in-person), Series on workshops on the new cybercrime act and international standards: second workshop for prosecutors, police & FIU, GLACY+, Octopus
- 24 June, C-PROC/LATAM, (online), Series of roundtables on the Second Additional Protocol for LATAM and Caribbean, GLACY+, Octopus

- 24 June, C-PROC, (in person), iPROCEEDS-2 5th Steering Committee Meeting, iPROCEEDS-2
- 27 - 29 June, C-PROC/DOMINICAN REPUBLIC, (hybrid), Specialized course on International Cooperation for Prosecutors and Judges, GLACY+
- 27 Jun - 1 Jul, C-PROC/REGIONAL, (hybrid), Training of Trainers for the 1st responders of African Gendarmeries, GLACY+
- 27 June, C-PROC/FIJI, (in-person), Series on workshops on the new cybercrime act and international standards: third workshop for service providers, GLACY+ · 28-30 June, C-PROC/FIJI, (in person), Initial assessment, GLACY+
- 28-30 June, C-PROC/GEORGIA, (in person), Law enforcement training for investigators with MIA Academy – Intermediate level, CyberEast
- 28 June, C-PROC, (online), Series of monthly thematic webinars for the International Network of the National Judicial Trainers, GLACY+
- 28 June, C-PROC/LEBANON, (online), National Workshop on the Second Additional Protocol, CyberSouth
- 30 June - 1 July, C-PROC/ DOMINICAN REPUBLIC, (hybrid), Advisory workshop on the streamlining of procedures for mutual legal assistance enhanced by the Second Additional Protocol related to cybercrime and electronic evidence, GLACY+
- 30 June – 1 July, CoE, (in person), HELP Network Conference 2022, presentation of the HELP course on cybercrime, Octopus
- June – July, C-PROC, Translation of the HELP Course on Cybercrime into French, Spanish and Portuguese, Octopus

The Cybercrime Digest appears bi-weekly. The news is selected by relevance to the current areas of interest to C-PROC and does 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