Cybercrime Digest

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

16 – 31 July 2023

Source: ICANN

Date: 17 July 2023

A new and simplified way to request nonpublic gTLD Registration Data

"ICANN organization (org) is currently developing the Registration Data Request Service (RDRS), a new ticketing system designed to handle requests for access to nonpublic registration data related to generic top-level domains (gTLDs). This new, free, and global service will simplify and standardize the way nonpublic data requests are made for both registrars and requestors through the use of a single platform." READ MORE

Source: EUROPOL

Date: 19 July 2023

Internet Organised Crime Assessment (IOCTA) 2023

"Cybercrime, in its various forms, represents an increasing threat to the EU. Cyber-attacks, online child sexual exploitation, and online frauds are highly complex crimes and manifest in diverse typologies. Meanwhile the perpetrators behind these crimes are becoming increasingly agile, exploiting new situations created by geopolitical and technological changes. The Internet Organised Crime Assessment (IOCTA) is Europol's assessment of the cybercrime landscape and how it has changed over the last 24 months." READ MORE

Source: US DOJ

Date: 17 July 2023

U.S. Departments of Justice and Commerce and the European Commission reaffirm shared values, welcome finalized EU-U.S. Data Privacy Framework

"[…] Last week, the Departments of Justice and Commerce welcomed the European Commission's adequacy decision for the EU-U.S. Data Privacy Framework, to which President Biden and European Commission President von der Leyen agreed in March 2022. Transatlantic data flows underpin more than $7 trillion in cross-border trade and investment per year and create greater economic opportunities for companies and citizens on both sides of the Atlantic." READ MORE

Source: New York Times

Date: 26 July 2023

Russia's Online Censorship Has Soared 30-Fold During Ukraine War

"What's the difference between Russia's internet before and after the invasion of Ukraine? The answer: a thirtyfold increase in censorship. That was the finding of a report published on Wednesday by Citizen Lab, a group from the University of Toronto that studies online censorship in authoritarian countries. The new report was one of the first attempts to quantify the extent of Russian internet censorship since the war began in February 2022." READ MORE

RELATED ARTICLE:

Citizen Lab, Not OK on VKAn analysis of in-platform censorship on Russia's VKontakte, 26 July 2023

Source: EDRi20

Date: 18 July 2023

EU Parliament's position on Directive combatting gender-based violence a step in the right direction, with some misses on protecting privacy

"On Wednesday, 12 July, the European Parliament reached an agreement on their final position regarding the Directive on combatting violence against women and domestic violence. The final position of the Parliament succeeded in shifting the narrative from the original criminalisation approach to combat gender-based violence (including cybercrimes) to a more holistic approach that includes victims' perspectives. Notably, the Directive now recognises online platforms as crucial players in preventing and removing illegal content. The overall outcome represents a positive step towards safeguarding women and LGBTQ+ rights on the internet, even though the Parliament didn't heed to some of the provisions that digital rights groups advocated for to strengthen this Directive." READ MORE

RELATED ARTICLE:

European Parliament, Combating violence against women and domestic violence

Source: Council of the European Union

Date: 19 July 2023

Cyber resilience act: member states agree common position on security requirements for digital products

"[…] The draft regulation introduces mandatory cybersecurity requirements for the design, development, production and making available on the market of hardware and software products to avoid overlapping requirements stemming from different pieces of legislation in EU member states. The proposed regulation will apply to all products that are connected either directly or indirectly to another device or network. […] The proposal aims to fill the gaps, clarify the links, and make the existing cybersecurity legislation more coherent by ensuring that products with digital components, for example 'Internet of Things' (IoT) products, become secure throughout the whole supply chain and throughout their whole lifecycle." READ MORE

Source: US Department of Justice

Date: 19 July 2023

Amazon agrees to injunctive relief and $25 million civil penalty for alleged violations of Children's Privacy Law relating to Alexa

"The Justice Department, together with the Federal Trade Commission (FTC), today announced that Amazon.com Inc. and its wholly-owned subsidiary Amazon.com Services LLC (collectively Amazon), have agreed to a permanent injunction and a $25 million civil penalty as part of a settlement to resolve alleged violations of the Children's Online Privacy Protection Act (COPPA), the Children's Online Privacy Protection Rule (COPPA Rule) and the Federal Trade Commission Act (FTC Act) relating to Amazon's voice assistant service Alexa." READ MORE

Source: United Nations

Date: 18 July 2023

International community must urgently confront new reality of generative, artificial intelligence, speakers stress as Security Council debates risks, rewards

"The international community must urgently confront the new reality of generative and other artificial intelligence (AI), speakers told the Security Council today in its first formal meeting on the subject as the discussion that followed spotlighted the duality of risk and reward inherent in this emerging technology. António Guterres, Secretary-General of the United Nations, noting that AI has been compared to the printing press, observed that — while it took more than 50 years for printed books to become widely available across Europe — "ChatGPT reached 100 million users in just two months". Despite its potential to turbocharge global development and realize human rights, AI can amplify bias, reinforce discrimination and enable new levels of authoritarian surveillance." READ MORE

RELATED ARTICLES:

Reuters, UN Security Council meets for first time on AI risks, 19 July 2023

Reuters, Factbox: Governments race to regulate AI tools, 19 July 2023

Source: The Register

Date: 27 July 2023

NATO probes hacktivist crew's boasts of stolen portal data

"NATO is investigating claims by miscreants that they broke into the military alliance's unclassified information-sharing and collaboration IT environment, stole information belonging to 31 nations, and leaked 845 MB of compressed data. On July 23, SiegedSec, a crew that describes itself as "gay furry hackers" and typically targets governments in politically motivated stunts, shared what was said to be stolen NATO documents via the gang's Telegram channel. The hacktivists' Telegram postincluded screenshots of the alleged files and a link, now defunct, to download the data." READ MORE

RELATED ARTICLE:

Cyberscoop, NATO investigating apparent breach of unclassified information sharing platform, 26 July 2023

Source: European Commission

Date: 17 July 2023

EU-Latin America and Caribbean: Joint Declaration on a Digital Alliance

"The European Union (EU) and Argentina, The Bahamas, Barbados, Brazil, Chile, Colombia, Costa Rica, the Dominican Republic, Ecuador, El Salvador, Guatemala, Honduras, Jamaica, Mexico, Panama, Paraguay, Peru, Suriname, Trinidad and Tobago, and Uruguay have agreed to deepen our partnership by establishing an EU–LAC Digital Alliance. The EU-LAC Digital Alliance is an informal, values-based framework for cooperation, open to all Latin American and Caribbean (LAC) countries and EU Member States who may participate through their respective governments and agencies related to the digital agenda." READ MORE

Source: Ministério da Justiça e Segurança Pública

Date: 27 July 2023

Brazil: PF deflagra Operação Coringa contra suspeito de ataque a sites do Governo

"Polícia Federal deflagrou, na quinta-feira (27/7), em parceria com o Ministério Público Federal – MPF, a Operação Coringa, com o objetivo de cumprir dois mandados de busca e apreensão em endereços em São Paulo. A operação visa apurar a conduta de um hacker que invadiu sites do Governo Federal e de instituições privadas, como bancos e empresas de telefonia, tanto no Brasil quanto no exterior. Os acessos indevidos, que se davam por meio de programas maliciosos, eram anunciados e vendidos em fóruns hospedados na DarkWeb. Os pagamentos tinham que ser feitos por meio de criptomoedas e com a intermediação de um garantidor." READ MORE

Source: UNFPA

Date: 19 July 2023

Argentina's journalists speak out against online gender-based violence

"Hate speech is rising around the world, including sexist and sexualized hate speech often targeted at women – and women journalists in particular – driving them from precisely the spaces where their voices are most needed. "In Argentina, it is a widespread problem," Mariana Iglesias told UNFPA, the United Nations sexual and reproductive health agency. Ms. Iglesias has reported for the major Argentinian newspaper, Diario Clarín, since 1996, is the country's first journalist to carry the title of gender editor – a role that has made her extremely familiar with digital violence." READ MORE

Source: Quadrin Mexico

Date: 26 July 2023

Mexico: Visualizan un Código Penal único que tipifique 14 delitos cibernéticos

"Ante el uso de servicios de IPs dinámicas por parte de proveedores de telecomunicaciones en México que alimenta los delitos cibernéticos, Felipe de Jesús Gallo Gutiérrez, titular de la Agencia de Investigación Criminal de la Fiscalía General de la República (FGR), urgió a que México se adhiera al Convenio de Budapest y se homologue un sólo Código Penal en el país. En el foro 'El futuro de la tecnología en procesos penales', convocado por la senadora Olga Sánchez Cordero del Grupo Parlamentario de Morena, el funcionario advirtió de una serie de actos delictivos que no están tipificados correctamente y que a diario trascienden a la sociedad de manera grave." READ MORE

Source: Trinidad Express

Date: 17 July 2023

Trinidad and Tobago: Budapest Convention and Cybercrime in T&T

"[…] Trinidad and Tobago currently faces a significant challenge in combating cybercrime due to the lack of comprehensive legislation in this area. The existing legal framework is limited, with computer crimes only classified as public mischief and punishable by meagre fines. Such inadequate legislation provides room for cybercriminals to exploit gaps and engage in illegal activities with relative impunity. By ratifying the Budapest Convention, Trinidad and Tobago would fill these legislative gaps and establish a comprehensive legal framework that defines and criminalises various cyber offenses. This would ensure consistent prosecution and impose appropriate penalties on offenders." READ MORE

Source: ICANN

Date: 31 July 2023

Coalition for Digital Africa: second location for ICANN managed root server installation

“The Coalition for Digital Africa and the Internet Corporation for Assigned Names and Numbers (ICANN) have announced that Cairo, Egypt, will be the second location for the deployment of the ICANN Managed Root Server (IMRS) installation in Africa. This is part of a Coalition initiative launched in 2022, which is slated to be deployed in September. […] With two separate IMRS deployment locations in Africa, and higher bandwidth and data processing capacity, the risk of the Internet being impacted because of a DDOS cyberattack is significantly reduced.” READ MORE

Source: Managers

Date: 31 July 2023

Le FBI soutient la Tunisie pour la ratification de la Convention de Budapest sur la cybercriminalité

“La Tunisie réaffirme l’importance d’une coordination internationale pour échanger des expériences et lutter contre les dangers de l’espace numérique. C’est ce qu’a déclaré le ministère des Technologies de la communication dans un communiqué rendu public dimanche, à l’issue d’une réunion entre le ministre des Technologies de la communication, Nizar Ben Neji, la cheffe du département des sciences et des technologies au FBI, Katie Noyes, et une délégation de haut niveau du Bureau fédéral d’investigation (FBI) relevant du ministère américain de la Justice.” READ MORE

Source: Innovation Village

Date: 18 July 2023

Nigerian Government takes proactive step to combat cybercrime with new Cybersecurity Lab

“The National Information Technology Development Agency (NITDA) says it is partnering with the Chartered Institute of Forensic and Certified Fraud Investigator of Nigeria (CIFCFIN) to build a cybersecurity lab in 2024. This collaborative effort aims to enhance Nigeria’s cybersecurity capabilities and combat the growing threat of cybercrime. The Director General of NITDA, Kashifu Inuwa, expressed concern over the harmful consequences of cybercrime on the nation’s economy, organisations, and individuals.” READ MORE

Source: Ghana Web

Date: 19 July 2023

Ghana: Editorial by B&FT: Strengthening the fight against cybercrime

“According to the Cybercrime Unit of the Criminal Investigation Department (CID), an amount of US$19million was lost to cybercrime in 1,097 cases reported in 2020. Indeed, Cyber fraud is becoming a menace to efforts at digitalising the economy. […] This is why Ghana’s decision to sign the Council of Europe Second Additional Protocol to the Convention on Cybercrime (Budapest Convention) will play a pivotal role in addressing the challenges presented by cybercrime.” READ MORE

RELATED ARTICLE:

B&FT Online, Boost for cybercrime investigations, 20 July 2023

Source: BBC

Date: 30 July 2023

Kenya cyber-attack: Why is eCitizen down?

“Kenya's government has been fighting off a huge cyber-attack that has affected services on a key government online platform for almost a week. The attack has also affected some private companies, although the extent is not yet clear. There are still questions over who was behind it and what was the motive.” READ MORE

Source: News 24

Date: 17 July 2023

SA on the brink of being Africa's capital of cybercrime, say digital experts

“South Africa is rapidly emerging as the cybercrime capital of Africa as the country is poised to surpass Nigeria and its ‘Nigerian Price’ in cybercrimes. This is according to recent data from TCG Forensics - a private forensic company specialising in digital forensics. Jackie Smith - head of Buyers Trust, a subsidiary of Ooba Group, - said that thousands of South Africans continue to fall prey to cybercrimes despite substantial investments from both the private and public sector in boosting cyber security and the passing of the Cybercrimes Act in 2021.” READ MORE

Source: RFS

Date: 21 July 2023

Proposed cybercrime law would deal new blow to press freedom in Jordan

“Reporters Without Borders (RSF) urges Jordan’s parliament to reject the draconian, government-backed cybercrime bill that it has been discussing since 15 July, which would probably impact journalists’ work negatively and restrict their freedom to report the news. The proposed law criminalises use of the Internet by any person, including journalists, to disseminate “false news,” commit acts of “defamation” (article 15) or cause “damage to reputation” (article 16) or “to national unity” (article 17).” READ MORE

RELATED ARTICLES:

Dig watch, Jordan’s cybercrime bill amendments raise concerns over freedom of expression and press, 21 July 2023

The new Arab, Jordanian parliament points to 'immorality' as reason for cybercrime law, 28 July 2023

Source: FBI

Date: 17 July 2023

UAE: International cyber fraudster sentenced to more than 8 years in federal prison

“A resident of the United Arab Emirates who orchestrated an $8 million cyber fraud scheme targeting several United States-based companies has been sentenced to more than eight years in a U.S. prison. OLALEKAN JACOB PONLE, also known as “Mr. Woodbery,” and “Mark Kain,” 31, was living in the UAE in 2019 when he worked with co-schemers to engage in numerous business email compromise schemes. The co-schemers used phishing links to gain unauthorized access to email accounts and then created false instructions directing employees of the victim companies to wire money to bank accounts opened by money mules at Ponle’s direction.” READ MORE

Source: Money Control

Date: 26 July 2023

Digital India Act: Here's how it should fix India's cybersecurity weaknesses

"It took eight years after the passage of the Information Technology (IT) Act for India to recognise cybersecurity as an agenda that needed legislation. The incoming Digital India Act (DIA), which promises to provide a safe and secure internet to Indians, is an opportunity to develop a future-ready cybersecurity framework. In India, the current cybersecurity landscape is a mishmash of various agencies with the attendant gaps and inefficiencies" READ MORE

Source: Reuters

Date: 29 July 2023

Malaysia reverses plan to take legal action against Meta over harmful content

"Malaysia may not go through with a plan to take legal action against Facebook parent Meta Platforms (META.O) following "positive" engagement with the firm on tackling harmful content on the social media platform, communications minister Fahmi Fadzil said in an interview on Friday. Last month, the Malaysian Communications and Multimedia Commission (MCMC) said it would take legal action against Meta for failing to act against "undesirable" content relating to race, royalty, religion, defamation, impersonation, online gambling, and scam advertisements." READ MORE

Source: Bangkok Post

Date: 29 July 2023

Thailand: Alert issued over surging cybercrime

"Cyberthreats are expected to cause roughly 772 billion baht's worth of damage per day to victims around the world this year, of which 85 million baht per day would be realised in Thailand, according to Stock Exchange of Thailand's (SET) Research Department." READ MORE

Source: Reuters

Date: 21 July 2023

Taiwan probes alleged leak of classified reports, diplomatic cables

"Taiwan is investigating a possible leak of official documents including diplomatic cables and classified reports on the island's sensitive bid to join a global trade pact, according to two officials familiar with the probe. One official said initial findings showed some parts of the documents, posted on online message board 8kun and reviewed by Reuters, are real while bits were forged, without giving details." READ MORE

Source: Nikkie Asia

Date: 27 July 2023

ChatGPT tech to be adopted by Japan government for administrative tasks

"Microsoft will supply Japan's government with the technology underpinning its ChatGPT generative AI for use in clerical work and analysis, Nikkei has learned, including crafting draft responses to parliamentary queries. For the system to handle confidential information, Microsoft has recently installed equipment with high processing power that will be used for generative AI at its data centers in Tokyo and Osaka, the first time the technology will be deployed in Asia." READ MORE

Source: New Zealand Government

Date: 26 July 2023

New Zealand: Government strengthens cyber security

“A lead operational agency will be established to strengthen cyber security readiness and response as well as make it easier for people and organisations to get help, Minister for the Public Service Andrew Little says. “The cyber security threats New Zealand faces are growing in scale and sophistication. We’re committed to staying ahead of the hackers, to protect communities, businesses and our public services.” READ MORE

Source: Nikkei Asia

Date: 14 July 2023

Solomons says China will assist in cyber, community policing

“Solomon Islands has denied suggestions by Australia and others its policing deal with Beijing is "a threat to the Pacific region peace" and says China will enhance the capability of its 1,500 police officers in cybersecurity and community policing. The U.S., Australia, New Zealand and Solomon Islands' opposition party have called for Prime Minister Manasseh Sogavare to "immediately" publish details of the policing deal signed in Beijing on Monday, amid concern it will invite further regional conflict.” READ MORE

RELATED ARTICLE:

Reuters, Australia raises concern over Solomon Islands policing plan with China's top diplomat, 14 July 2023

Source: KrebsOnSecurity

Date: 16 July 2023

Russia sends cybersecurity CEO to jail for 14 years

“The Russian government today handed down a treason conviction and 14-year prison sentence on Iyla Sachkov, the former founder and CEO of one of Russia’s largest cybersecurity firms. Sachkov, 37, has been detained for nearly two years under charges that the Kremlin has kept classified and hidden from public view, and he joins a growing roster of former Russian cybercrime fighters who are now serving hard time for farcical treason convictions.” READ MORE

RELATED ARTICLE:

Info security magazine, Group-IB founder sentenced in Russia to 14 years for treason, 26 July 2023

Source: Forbes

Date: 21 July 2023

As Many As 700,000 Turkish TikTok Accounts Were Hacked Before The Country’s Presidential Election

“Weeks before Turkey’s authoritarian president, Recep Tayyip Erdoğan, eked out a narrow reelection in May, TikTok’s acting security chief, Kim Albarella, received a piece of bad news: As many as 700,000 TikTok accounts in Turkey had been compromised by a hack that allowed attackers to access users’ private information and control their accounts.” READ MORE

Source: CYWARE Social

Date: 25 July 2023

Chinese cyberespionage group APT31 targets Eastern European entities

"A China-linked group APT31 (aka Zirconium) has been linked to a cyberespionage campaign targeting industrial organizations in Eastern Europe. In this campaign, the attackers aimed to steal valuable intellectual property from victims, including data stored on air-gapped systems." READ MORE

RELATED ARTICLE:

Lookout, Lookout attributes advanced Android surveillanceware to Chinese espionage group APT41, 19 July 2023

Source: Council of the European Union

Date: 27 July 2023

Statement by the High Representative on behalf of the EU on the alignment of certain third countries concerning restrictive measures against cyber-attacks threatening the Union or its Member States

"On 15 May 2023, the Council adopted Decision (CFSP) 2023/964[1]. The Council Decision extends the validity of the restrictive measures until 18 May 2024. The candidate countries North Macedonia, Montenegro, Albania, Ukraine, Republic of Moldova and Bosnia and Herzegovina[2], the EFTA country Norway, member of the European Economic Area, align themselves with this Council Decision." READ MORE

Source: Cybersecurity Insiders

Date: 24 July 2023

DdoS attack on 12 Norway government websites

"Norway is experiencing serious cyber threat from state funded actors and has become a latest victim to a distributed denial of service attack aka DdoS attack. According to the Norway's Ministry of Local and Regional Development about 12 of its websites were experiencing unusual web traffic because of a software vulnerability at the technology service provider." READ MORE

RELATED ARTICLES:

Reuters, Norway government ministries hit by cyber attack, 24 July 2023

Bleeping Computers, Norway says Ivanti zero-day was used to hack govt IT systems, 25 July 2023

Source: BBC

Date: 28 July 2023

Cyber-attack affects two south England ambulance services

"Two ambulance trusts have been left without access to electronic patient records after a cyber attack. South Central Ambulance Service (SCAS) and South Western Ambulance Service (SWASFT), which serve a population of 12 million people, are both affected. The attack targeted a third-party technology company used by the trusts. NHS England has confirmed it is investigating the incident alongside the police, and work is ongoing to reconnect the system." READ MORE

Source: Reuters

Date: 21 July 2023

Exclusive: AI being used for hacking and misinformation, top Canadian cyber official says

“Hackers and propagandists are wielding artificial intelligence (AI) to create malicious software, draft convincing phishing emails and spread disinformation online, Canada's top cybersecurity official told Reuters, early evidence that the technological revolution sweeping Silicon Valley has also been adopted by cybercriminals.” READ MORE

RELATED ARTICLE:

Verdict, Canadian cybercrime head says AI is being used for hacking, 21 July 2023

Latest reports

- Bleeping Computer, Thousands of images on Docker Hub leak auth secrets, private keys, 16 July 2023
- EUROPOL, IOCTA 2023: forget hackers in a hoodie, cybercrime has become a big business, 17 July 2023
- Fortinet, Threat trends: threat actors add .zip domains to their phishing arsenals, 17 July 2023
- The Security Affairs, Admins of Genesis Market marketplace sold their infrastructure on a hacker forum, 17 July 2023
- Symantec by Broadcom, FIFIN8 Uses Revamped Sardonic Backdoor to Deliver Noberus Ransomware, 18 July 2023
- Decoded, HotRat: the risks of illegal software downloads and hidden autohotkey script within, 19 July 2023
- Mandiant, Escalating privileges via third-party Windows installers, 19 July 2023
- Social Europe, 'Social media': the harms to women and girls, 19 July 2023
- ZD Net, WormGPT: What to know about ChatGPT's malicious cousin, 20 July 2023
- Radio Free Europe, 'I Can't Keep Quiet:' Roma Activist Fights Back Against Online Hate Speech By Far-Right Party, 20 July 2023
- TechCrunch, Fake passports, real bank accounts: How TheTruthSpy stalkerware made its millions, 20 July 2023
- Security Affrairs, Shadowserver reported that +15K Citrix servers are likely vulnerable to attacks exploiting the flaw CVE-2023-3519, 23 July 2023
- ARCOM, Lutte contre la diffusion de contenus haineux en ligne: bilan des moyens mis en oeuvre par les plateformes en ligne en 2022 et perspectives, 24 July 2023
- Sentinel One, Deconstructing PowerShell Obfuscation in Malspam Campaigns, 24 July 2023
- Mandiant, North Korea Leverages SaaS Provider in a Targeted Supply Chain Attack, 24 July 2023
- MS Magazine, How the International Women's Media Foundation Fights for Women in Journalism and Strengthens Press Freedom, 24 July 2023
- The Spin Off, Speaking out about the silencing of women, 25 July 2023
- Infoblox, Decoy dog is no ordinary pupy: separating a sly DNS malware from the pack, 25 July 2023
- Sygnia, Breaking down the Casbaneiro infection chain – Part II, 25 July 2023
- Naked security by Sophos, Zenbleed: How the quest for CPU performance could put your passwords at risk, 26 July 2023
- ITIF, How the G7 can use "data free flow with trust" to build global data governance, 27 July 2023
- Team Cymru, Inside the IcedID BackConnect Protocol (Part 2), 28 July 2023
- Secure List by Kapersky, Anomaly detection in certificate-based TGT requests, 28 July 2023
- Help Net Security, Blocking access to ChatGPT is a short term solution to mitigate risk, 28 July 2023
- Santa Monica Mirror, Operation Online Guardian: LA ICAC Task Force Apprehends Predators in Online Crackdown, 28 July 2023

- Adroit Market Research, Digital Evidence Management market Segmentation by Application, 31 July 2023
- American Press Institute, Journalists and mental health: An API resource guide, 31 July 2023
- IBM, Cost of a Data Breach Report 2023, July 2023
- Acronis, From innovation to risk: managing the implications of AI-driven cyberattacks, July 2023
- CERT EU, Threat landscape report 2023Q2 – main malicious activities, July 2023

Upcoming events

- 2–3 August 2023, CYBERCRIME DIVISION/ARGENTINA, (*in-person*), Second Summit Conference on cybernetic issues, Octopus
- 14-15 August 2023, C-PROC/KENYA, *(in-person)*, Training of Trainers - training skills and certification programme for CoE judicial trainers, GLACY+
- Mid-August 2023, CYBERCRIME DIVISION/APCO, (*in person*), Participation in the session "What Intent Standard is Essential to the Convention?", T-CY
- August 2023, C-PROC, (*on-line*), Countries' assessment on the developments in the fight against cybercrime in the MENA region, 2017-2023 , CyberSouth
- August 2023, C-PROC, (*on-line*), Meeting of the working group on the online training platform, Octopus
- August 2023, C-PROC, *(on-line)*, Maintaining cyberviolence portal, 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