Cybercrime Digest

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

1 – 15 July 2023

Source: Council of Europe

Date: 03 July 2023

Kiribati invited to join the Convention on Cybercrime

"Today, on 3 July 2023, Kiribati was invited to accede to the Budapest Convention on Cybercrime. This invitation to accede is valid for five years from its adoption. This new invitation brings the number of countries invited to accede to 21." READ MORE

Source: European Commission

Date: 10 July 2023

Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows

"The EU-U.S. Data Privacy Framework introduces new binding safeguards to address all the concerns raised by the Euhropean Court of Justice, including limiting access to EU data by US intelligence services to what is necessary and proportionate, and establishing a Data Protection Review Court (DPRC), to which EU individuals will have access. The new framework introduces significant improvements compared to the mechanism that existed under the Privacy Shield. For example, if the DPRC finds that data was collected in violation of the new safeguards, it will be able to order the deletion of the data. The new safeguards in the area of government access to data will complement the obligations that US companies importing data from EU will have to subscribe to." READ MORE

RELATED ARTICLE:

European Commission, Questions & Answers: EU-US Data Privacy Framework, 10 July 2023

Source: European Commission

Date: 11 July 2023

Towards the next technological transition: Commission presents EU strategy to lead on Web 4.0 and virtual worlds

"On 11 July 2023, the Commission has adopted a new strategy on Web 4.0 and virtual worlds to steer the next technological transition and ensure an open, secure, trustworthy, fair and inclusive digital environment for EU citizens, businesses and public administrations. Virtual worlds will impact the way people live together, bringing both opportunities and risks that need to be addressed. The new strategy aims for a Web 4.0 and virtual worlds reflecting EU values and principles, where people's rights fully apply and where European businesses can thrive." READ MORE

RELATED ARTICLES:

European Commission, Virtual Worlds and Web 4.0 - Factsheet, 11 July 2023

European Commission, An EU initiative on virtual worlds: a head start in the next technological transition, 11 July 2023

Source: Lexology

Date: 11 July 2023

The European electronic evidence framework on the home stretch

"While much recent European data legislation has passed through the legislative process in record time, the electronic evidence framework (the Framework) proposal has been stuck in the pipeline for over five years. After discussions surrounding the Framework heated up during the winter of 2021 and early 2022 (see our blog), it is now on the verge of being adopted. Now, the Council formally agreed to the European Parliament's position on the Framework based on a provisional agreement of the trilogues from January 2023." READ MORE

Source: ICANN

Date: 03 July 2023

Thousands Rally Worldwide to Support a Multilingual Internet

"The Internet Corporation for Assigned Names and Numbers (ICANN) and the Universal Acceptance Steering Group (UASG) have released participation figures from the first-ever Universal Acceptance (UA) Day in a new report published today. According to the report, thousands of members of the global Internet community across five continents took part in the milestone event. […] UA Day marked the first time a diverse set of technical and language communities, companies, governments, and Domain Name System (DNS) industry stakeholders mobilized to champion UA and a multilingual Internet on a global scale." READ MORE

RELATED ARTICLE:

ICANN, Universal Acceptance Day, 1 June 2023

Source: EUROPOL

Date: 06 July 2023

Europol Strategy adopted by Management Board

"The Europol Management Board has now adopted the Agency's updated corporate strategy. The document, entitled "Delivering Security in Partnership", came about following an extensive consultation of Member States and partners. Europol's new mandate, a number of key policy developments, and crises such as the COVID-19 pandemic and the war in Ukraine meant the Agency had to reconsider its strategic direction." READ MORE

Source: The Hacker News

Date: 10 July 2023

RomCom RAT Targeting NATO and Ukraine Support Groups

"The threat actors behind the RomCom RAT have been suspected of phishing attacks targeting the upcoming NATO Summit in Vilnius as well as an identified organization supporting Ukraine abroad. The findings come from the BlackBerry Threat Research and Intelligence team, which found two malicious documents submitted from a Hungarian IP address on July 4, 2023." READ MORE

RELATED ARTICLES:

Bleeping Computer, RomCom hackers target NATO Summit attendees in phishing attacks, 10 July 2023

IT Wire, Behind the war in Ukraine is a shady war of cyber attackers reveals Radware research, 9 July 2023

Source: The Commonwealth

Date: 06 July 2023

Commonwealth launches a cybercrime and electronic evidence e-learning course

The Commonwealth Secretariat has launched a set of new foundational online courses designed to equip law enforcement officials, prosecutors and judicial officials with the skills necessary to investigate, prosecute and adjudicate over cybercrime cases involving electronic evidence." READ MORE

Source: Just Security

Date: 05 July 2023

Digital Evidence Collection at the Int'l Criminal Court: Promises and Pitfalls

"This summer, evidence collection at the International Criminal Court (ICC) took a major step forward with the introduction of OTPLink. The new online platform provides a more accessible avenue for witnesses of international crimes – including rape, torture, murder, and enslavement – to directly submit information to prosecutors in real-time. OTPLink complements the ICC's larger digitalization initiative, Project Harmony, which uses cloud computing capabilities and artificial intelligence to review large quantities of complex information and evidence." READ MORE

Source: World Economic Forum

Date: 14 July 2023

Cybercrime: Critical infrastructure is at risk and needs a combined private - and public-sector response

"Supply chain cyberattacks have been rife over the last few months, affecting a large number of governmental agencies, law enforcement, companies and universities in the US and Europe. A prominent example of such cyberattacks is the exploitation of a zero-day vulnerability in the file sharing software MOVEit, which is widely used by organizations to transfer data." READ MORE

Source: The Hacker News

Date: 10 July 2023

New TOITOIN banking trojan targeting Latin American businesses

"Businesses operating in the Latin American (LATAM) region are the target of a new Windows-based banking trojan called TOITOIN since May 2023. "This sophisticated campaign employs a trojan that follows a multi-staged infection chain, utilizing specially crafted modules throughout each stage," Zscaler researchers Niraj Shivtarkar and Preet Kamal said in a report published last week." READ MORE

Source: The Record

Date: 10 July 2023

Trinidad and Tobago facing outages after cyberattack

"Trinidad and Tobago's justice department is dealing with a cyberattack that has impacted the ministry's operations. The island nation of more than 1.4 million people announced on Friday that its Ministry of Digital Transformation discovered a cyberattack targeting the country's Office of the Attorney General and Ministry of Legal Affairs (AGLA) in recent days." READ MORE

Source: PGA

Date: 11 July 2023

Caribbean regional workshop on the universalization of the Budapest Convention on Cybercrime and its Additional Protocols

"PGA's International Peace and Security Program (IPSP) successfully organized a Regional Caribbean Workshop on engaging female and male parliamentarians in promoting (i) universality and implementation of the Budapest Convention on Cybercrime and its two Additional Protocols and (ii) raising awareness on the differentiated impact of cyber incidents on the basis of gender that was held in Port-of-Spain, Trinidad and Tobago, on 5-6 July 2023. […] Thirteen parliamentarians from Barbados, Grenada, St Lucia, Suriname, and Trinidad and Tobago participated in the workshop." READ MORE

Source: MPFS

Date: 06 July 2023

Argentina: Ciberdelincuencia: Es Ley la inclusión de la evidencia digital en investigaciones judiciales

"Este martes, durante la 15º Sesión Ordinaria de la Cámara de Senadores de la Provincia de Salta, se aprobó en definitiva el proyecto de Ley en Revisión por el cual se promueve la reforma del Código Procesal Penal de Salta. El objetivo de esta reforma, es el de establecer procedimientos específicos para la investigación de delitos informáticos y aquellos casos en los que se requiera el análisis de evidencia digital." READ MORE

Source: INTERPOL

Date: 05 July 2023

West Africa: Suspected key figure of notorious cybercrime group arrested in joint operation

"Over the last four years, a highly organized criminal organization has targeted financial institutions and mobile banking services with malware, phishing campaigns and large-scale Business Email Compromise (BEC) scams. Known as OPERA1ER, with aliases such as NXM, DESKTOP Group and Common Raven, the group is believed to have stolen an estimated USD 11 million - potentially as much as 30 million - in more than 30 attacks across 15 countries in Africa, Asia and Latin America." READ MORE

RELATED ARTICLE:

Homeland security, Suspected Key Figure of Notorious Cybercrime Group Arrested in Joint Operation, 7 July 2023

Source: we are Tech.Africa

Date: 12 July 2023

Le Ghana a signé le 2e protocole additionnel à la Convention de Budapest sur la cybercriminalité

"Le Ghana a récemment signé le deuxième protocole additionnel à la Convention sur la cybercriminalité (convention de Budapest) […]. Selon Ursula Owusu-Ekuful, la ministre ghanéenne des Communications et de la Numérisation qui a signé le protocole au nom du Ghana, l'adoption du protocole renforcera les efforts d'enquête sur la cybercriminalité et permettra de mieux juger les affaires de cybercriminalité à l'échelle mondiale." READ MORE

Source: Tech Economy

Date: 13 July 2023

Nigeria Moves to Repeal Cybercrime Act 2015

"Ade Shoyinka, President of Cyber Security Experts Association of Nigeria (CSEAN), has called on the Nigerian governments, private sector, and civil society groups to join forces against cyber threats in the country. […] Shoyinka expressed concerns over the persistent occurrence of cybercrime by individuals or groups not affiliated with the government, emphasising that without sufficient preemptive actions, Nigeria's progress towards achieving the 2030 Sustainable Development Goals (SDGs) would be jeopardised." READ MORE

Source: The Africa Report

Date: 03 July 2023

Côte d'Ivoire, Congo, Morocco: Cybastion expanding aggressively in Africa

"Already well-established in sub-Saharan Africa, the American group specialising in cybersecurity and intelligence, Cybastion, is growing across the continent. It is counting on its knowledge of the African context to strengthen its role as a technology integrator for governments. Cybastion has rapidly earned its stripes in Francophone Africa." READ MORE

Source: The Star

Date: 03 July 2023

Kenyan businesses experience 82% rise in cyber-attacks - report

"Cyber-attacks on Kenyan businesses have increased by 82 percent, 90 per cent of these having experienced a data breach in the past year. This is according to a Pan-African cyber security 2022 report released by Liquid C2, a business unit of Liquid Intelligent Technologies." READ MORE

Source: End violence against children

Date: 07 July 2023

Kenya launches groundbreaking training handbook to combat online child sexual exploitation and abuse

"Kenya's National Council on the Administration of Justice (NCAJ) has launched a training handbook on the investigation and prosecution of online child sexual exploitation and abuse (OCSEA) in Kenya. The handbook was developed with technical support from UNICEF Kenya, a grantee of the Safe Online Initiative at the End Violence Partnership […]." READ MORE

Source: LBC International

Date: 12 July 2023

Lebanon: Minister Khoury: Digital evidence became fundamental source of evidence relied upon by judges

"Caretaker Minister of Justice Henry Khoury believed on Wednesday that judges are facing new crimes being committed online, which require extensive expertise from both security forces, who conduct investigations, and judges, who must prosecute such criminal behavior. "Digital evidence has become a fundamental source of evidence relied upon by judges to prosecute most cyber crimes in our day," he added." READ MORE

Source: Jordan News

Date: 12 July 2023

Jordan: Draft cybercrime law set to be presented to Lower House by July 16

"The Minister of Government Communication and official spokesperson, Faisal Al-Shboul, announced on Monday that the draft cybercrime law will be submitted to the Lower House prior to the upcoming special parliamentary session. Shboul revealed that the Legal Committee in the Cabinet is currently finalizing the drafting process, as reported by Al-Mamlaka TV. In response to a Royal Decree, Parliament has been summoned to convene in an extraordinary session on Sunday, July 16, 2023, to review and pass several draft laws, including the proposed cybercrime legislation." READ MORE

Source: Dark Reading

Date: 03 July 2023

Israel Aided UAE in Defending Against DDoS Attack

"Israel earlier this year aided the United Arab Emirates (UAE) in helping repel a major distributed denial-of-service (DDoS) attack. Speaking at last week's Cyber Week in Tel Aviv, UAE head of cybersecurity Mohamed Al Kuwaiti said that attacks "continuously come and go" and praised the Abraham Accords, which were ratified in 2020 to strengthen Middle East relations. "Thank God for the partnership, with the relationship that we have; it helped us elevate as well as to prepare an early warning system," he said." READ MORE

Source: The Friday Times

Date: 13 July 2023

Misinformation and Online Violence: Impact on Pakistani Transgender Communities

"Pakistan is experiencing a rampant rise in misinformation on transgender communities primarily because of hate campaigns run by religiopolitical groups, such as the Jamaat-e-Islami (JI) and the Jamiat Ulema-e-Islam-Fazl (JUI-F), against local trans communities. This was revealed in a report prepared by the Digital Rights Monitor titled "Online Violence Against Women, Misinformation Campaigns, and Big Tech Accountability: The Case of Asia." The report, compiled by journalist Zebunnisa Burki, states that religious parties vehemently opposed the Transgender Act and created a controversy over universally accepted terminology, such as "trans" and "intersex"." READ MORE

Source: Dig watch

Date: 06 July 2023

Asia: How the police handle data overload when collecting digital evidence

"Commercial firms are not the only entities facing data overload troubles: law enforcement agencies have had to rapidly transform to cope. The alarming rise in cybercrimes and online scams globally underscores the urgent need for robust digital evidence collection, storage, management, and analysis capabilities. Law enforcement agencies are increasingly investing in advanced technologies and skilled personnel to effectively gather and examine digital evidence, enhancing their ability to combat modern-day crimes. Security cameras help deter crimes all over the world, and when crimes are recorded those video recordings provide vital evidence." READ MORE

Source: Dig Watch

Date: 06 July 2023

Singapore Parliament passes legislation to combat scams, cybercrime and online sexual offences

"On Wednesday, 5 July, new legislation was passed by the Singaporean Parliament to address online content that aids scams and harmful cyber activities. After initially being introduced to Parliament at the beginning of May, the Online Criminal Harms Bill (or Online Criminal Harms Act, dubbed 'the Bill') covers a wide range of criminal acts, although the threshold for action on fraud, scams, and cybercrime charges will be lower than for other offences." READ MORE

Source: The straits times

Date: 11 July 2023

Singapore hosts new Asean forum to tackle child sexual abuse scourge

"A new forum, organised by the Singapore Police Force (SPF) and the US' Homeland Security Investigations (HSI) to fight child sexual abuse and exploitation in South-east Asia, is being held here from Tuesday to Thursday. About 150 representatives, including subject-matter experts, investigators and non-governmental organisation members from Singapore, the US and nine other South-east Asian countries, are attending the Crimes Against Children Regional Forum 2023." READ MORE

Source: Khmer Times

Date: 13 July 2023

UNICEF digital campaign fights child sexual exploitation in Cambodia

"The United Nations Children's Fund (UNICEF), in partnership with Cambodia's Ministry of Social Affairs, Veterans and Youth Rehabilitation, is implementing the "Let's Chat" digital campaign to address the vulnerability of Cambodian adolescents to online sexual predators. The UN agency said in a press release on Wednesday that the three-month campaign from June 1 to Aug 30 sought to decrease the number of internet-using children who experience online sexual exploitation and abuse through an innovative and interactive campaign that addresses predatorily "grooming" practices online." READ MORE

Source: IT news

Date: 06 July 2023

Australian gov says 'sensitive' data caught in HWL Ebsworth breach

"Sensitive personal and government information held by "a number" of Australian federal entities was "released" as part of an attack on law firm HWL Ebsworth in May, according to Australia's national cyber security coordinator. Air Marshal Darren Goldie, who took on the coordinator role at the start of the week, said in a statement that his "first order of business" was to deal with the fallout of the HWL Ebsworth breach." READ MORE

RELATED ARTICLES:

ABC News, HWL Ebsworth hack affected government departments, cyber security coordinator says, 5 July 2023

IT Brief, Cyber attacks continue to target critical infrastructure, demand to secure assets, 7 July 2023

Source: The Record

Date: 05 July 2023

Russian railway site allegedly taken down by Ukrainian hackers

"The Russian state-owned railway company RZD said Wednesday that its website and mobile app were down for several hours due to a "massive" cyberattack, forcing passengers to only buy tickets at railway stations. The Ukrainian hacktivist group IT Army claimed responsibility for the attack on its Telegram channel. "The terrorist state is heading non-stop to the station called Chaos," the hackers said. The group's claims could not be immediately verified." READ MORE

Source: Politico

Date: 04 July 2023

Russia illegally used facial recognition to arrest protestor, human rights court rules

"Russia's use of facial recognition technology to arrest a protester on the Moscow subway violated his human rights, the European Court of Human Rights (ECHR) ruled Tuesday. "The use of facial-recognition technology in his case ha[s] been incompatible with the ideals and values of a democratic society governed by the rule of law," the court said in its ruling. " READ MORE

Source: CYBLE

Date: 10 July 2023

The Turkish Government Masqueraded Site Distributing Android RAT

"In the ever-expanding digital landscape, where our lives are increasingly intertwined with technology, threats to our online security have become more prevalent than ever before. Phishing attacks, in particular, have emerged as a nefarious method employed by cybercriminals to trick unsuspecting users into revealing sensitive information or unknowingly downloading malware onto their devices. Cyble Research & Intelligence Labs (CRIL) recently identified a phishing site hxxps://scanyalx[.]online masquerading as a legitimate government platform from Turkey which not only aims to deceive users but also distributes a dangerous Android Remote Access Trojan (RAT)." READ MORE

Source: The Hacker News

Date: 04 July 2023

DDoSia Attack Tool Evolves with Encryption, Targeting Multiple Sectors

"The threat actors behind the DDoSia attack tool have come up with a new version that incorporates a new mechanism to retrieve the list of targets to be bombarded with junk HTTP requests in an attempt to bring them down. DDoSia is attributed to a pro-Russian hacker group called NoName(057)16. Launched in 2022 and a successor of the Bobik botnet, the attack tool is designed for staging distributed denial-of-service (DDoS) attacks against targets primarily located in Europe as well as Australia, Canada, and Japan. Lithuania, Ukraine, Poland, Italy, Czechia, Denmark, Latvia, France, the U.K., and Switzerland have emerged as the most targeted countries over a period ranging from May 8 to June 26, 2023." READ MORE

Source: ERR

Date: 03 July 2023

Estonia launches cyber awareness campaign this July

"This July, the Estonian State Information System Authority (RIA) is launching a cyber awareness campaign to draw attention to some of the dangers that lurk in Estonian cyberspace and may lead to both businesses and individuals being deprived of important data, access to accounts and money. The campaign calls on people to be more aware of their online behavior and to test their IT skills." READ MORE

Source: Bitdefender

Date: 03 July 2023

Dublin Airport staff pay details stolen by hackers after MOVEit attack at third-party provider

"Staff at Dublin Airport have been warned that their personal data has fallen into the hands of hackers, following a data breach at a third-party service provider. Some 2000 employees of DAA, the operator of Dublin airport, have had their pay and benefit details stolen after cybercriminals exploited a vulnerability in the MOVEit - a file-transfer tool used by many businesses to transfer files." READ MORE

RELATED ARTICLES:

CISA, Progress Software Releases Service Pack for MOVEit Transfer Vulnerabilities, 7 July 2023

TechCrunch, More organizations confirm MOVEit-related breaches as hackers claim to publish stolen data, 6 July 2023

Source: The Hacker News

Date: 04 July 2023

Swedish Data Protection Authority Warns Companies Against Google Analytics Use

"The Swedish data protection watchdog has warned companies against using Google Analytics due to risks posed by U.S. government surveillance, following similar moves by Austria, France, and Italy last year. The development comes in the aftermath of an audit initiated by the Swedish Authority for Privacy Protection (IMY) against four companies CDON, Coop, Dagens Industri, and Tele2. "In its audits, IMY considers that the data transferred to the U.S. via Google's statistics tool is personal data because the data can be linked with other unique data that is transferred," IMY said." READ MORE

Source: European Roma rights Centre

Date: 10 July 2023

Bulgaria: extremist VMRO-BND party fined for 'gypsy issue' online hate

"In a welcome move, Bulgaria's Commission for Protection against Discrimination (CPC) took action against racist hate speech, fined the far-right political party, VMRO-Bulgarian National Movement (VMRO-BND) and prohibited them from publishing content on their website that incites hatred against certain ethnic minorities. […] In its reasoning, the CCP held that such generalisations based on ethnicity constitute discrimination which is prohibited by law. Freedom of expression and free speech claims by VMRO-BND were rejected on the grounds that the offending articles constituted hate speech of a kind that violated human rights and democratic principles." READ MORE

Source: The Register

Date: 10 July 2023

Liberté, Égalité, Spyware: France okays cops snooping on phones

"With riots rocking the country, French parliamentarians have passed a bill granting law enforcement the right to snoop on suspects via "the remote activation of an electronic device without the knowledge or consent of its owner." That's the direct (via machine translation) language used in the French Senate's version of a justice reform bill passed earlier. According to French publication Le Monde, The French General Assembly just passed their version, albeit with a few amendments that will require the Senate to OK the changes before it can become law. Under the provision, French police will have the right to activate cameras and microphones remotely, as well as gathering location data from devices belonging to suspects accused of committing crimes that are punishable by at least five years in jail." READ MORE

Source: UK National Cyber Security Centre

Date: 06 July 2023

Support from British businesses crucial in removing over 235,000 scams, new figures reveal

"BRITISH BUSINESSES and citizens reported a suspicious email or website every five seconds in 2022, a new report from GCHQ's National Cyber Security Centre (NCSC) has revealed (Thursday). 7.1 million suspicious emails and URLs were flagged by UK organisations and citizens via the NCSC's free Suspicious Email Reporting Service (SERS) between January 2022 and December 2022 – the equivalent of nearly 20,000 reports a day." READ MORE

Source: Tech Crunch

Date: 05 July 2023

Security researchers latest to blast UK's Online Safety Bill as encryption risk

"Nearly 70 IT security and privacy academics have added to the clamour of alarm over the damage the U.K.'s Online Safety Bill could wreak to, er, online safety unless it's amended to ensure it does not undermine strong encryption. Writing in an open letter, 68 U.K.-affiliated security and privacy researchers have warned the draft legislation poses a stark risk to essential security technologies that are routinely used to keep digital communications safe." READ MORE

Latest reports

- Krebs on security, Who's behind the DomainNetworks Snail mail scam?, 3 July 2023

- SentinelOne, Neo_Net | The Kingpin of Spanish eCrime, 3 July 2023

- Forbes, Beyond the common border: how to combat overtourism with technology, 3 July 2023

- Politico, How the FBI hacked Hive, 4 July 2023

- Technautas, Crece comercio electrónico y se coloca como objetivo principal de la ciberdelincuencia, 4 July 2023

- ADF News, Digital Forensics: The military's secret weapon to combat cyber threats, 5 July 2023

- ENISA, Checking-up on Health: Ransomware Accounts for 54% of Cybersecurity Threats, 5 July 2023

- Forbes, How cyber insurance can help relieve the financial burden of a cyberattack, 5 July 2023

- CISCO, Cisco ACI multi-site CloudSec encryption information disclosure vulnerability, 5 July 2023

- CSO, Greatest cyber threats to aircraft come from the ground, 6 July 2023

- Proofpoint, Welcome to New York: Exploring TA453's Foray into LNKs and Mac Malware, 6 July 2023

- Help Net Security, Is your browser betraying you? Emerging threats in 2023, 7 July 2023

- HELP Net Security, Scammers using AI voice technology to commit crimes, 7 July 2023

- The Cyber Express, Cybercrime Legislation and International Cooperation: closing the enforcement gap, 8 July 2023

- The age, The 'nightmare' cybersecurity scenario being war gamed by government, 8 July 2023

- Blackberry Blog, RomCom Threat Actor Suspected of Targeting Ukraine's NATO Membership Talks at the NATO Summit, 8 June 2023

- Forbes, The promise and challenges of AI in healthcare, 10 July 2023

- eSafetyCommissioner, Protecting our (increasingly younger) children from cyberbullying, 10 July 2023

- GROUNDVIEWS, Online child abuse: a lack of laws or a lack of implementation?, 11 July 2023

- NVST, StackRot, a new Linux Kernel privilege escalation vulnerability, 11 July 2023

- ICANN Blog, The Key to the Internet and Key Ceremonies: An Explainer, 11 July 2023

- CISA, Enhanced Monitoring to Detect APT Activity Targeting Outlook Online, 12 July 2023

- SOFREP, Modern espionage: Information warfare in the digital age, 14 July 2023

- The White House, National Cybersecurity Strategy Implementation Plan, July 2023

- Balkan insight, A rise in cyberattacks in Balkans as more systems use biometrics and digital IDs, July 2023

- CSET, China's cognitive AI research: emulating human cognition on the way to general purpose AI, July 2023

- Liquid C2, The Evolving Cyber Security Landscape in Africa 2022, June 2023

Upcoming events

- 15-30 July, C-PROC, (online), Translation into Arabic of the Basic Judicial Training Course on Cybercrime for Lebanon, CyberSouth

- 17 July–25 August, C-PROC/LATAM, (online), FOSI Training course, GLACY+

- 18-19 July, C-PROC/COLOMBIA, (in person), National Cybercrime Conference, GLACY+

- 25 July, C-PROC/RWANDA, (online), Workshop with the Sector leadership (MoICT), GLACY+

- 26-28 July, C-PROC/TANZANIA, (online), East Africa Legislative Summit on the Budapest Convention, GLACY+

- 26-27 July, C-PROC/ INTERPOL/FRANCE, (in-person), International Child Sexual Exploitation (ICSE) Database Training, iPROCEEDS-2

- 20 July, C-PROC, (online), Meeting of the working group on the online training platform, Octopus

- 26-28 July, C-PROC/TANZANIA, (in person), East Africa Legislative Summit on the Budapest Convention, Octopus, GLACY+

- 31 July-3 August (TBC), C-PROC/NAURU, (online), Refresher workshop with the legal drafters on the envisaged legal reform, GLACY+

- by 30 July, C-PROC/MOZAMBIQUE, (online), Desk study on cybercrime and electronic evidence legislation (part of the wider advisory mission on legislation), GLACY+

- by 30 July, C-PROC/MALAWI, (online), Desk study on cybercrime and electronic evidence legislation (part of the wider advisory mission on legislation), GLACY+

- July, C-PROC, (online), Maintaining cyberviolence portal, Octopus

- July-September, C-PROC, (online), Countries' assessment on the developments in the fight against cybercrime, 2017-2023, CyberSouth

---

www.coe.int/cybercrime

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE