Cybercrime Digest

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

16 – 31 May 2023

Source: Council of Europe

Date: 31 May 2023

Mauritius becomes 37th State to sign the Second Additional Protocol to Convention on Cybercrime

"Today, 31 May 2023, H.E. Mr Vijayen Valaydon, Ambassador of the Republic of Mauritius to France, signed the Second Additional Protocol to the Convention on Cybercrime, on enhanced co-operation and disclosure of electronic evidence. The event took place in Strasbourg in the presence of Deputy Secretary General of the Council of Europe Bjørn Berge. This accounts for 1 ratification and 36 signatures not yet followed by ratification." READ MORE

Source: Council of Europe

Date: 23 May 2023

Save the date: Octopus Conference 2023!

"Held every 12 to 18 months by the Council of Europe, the Octopus Conference constitutes one of the biggest and finest platforms of exchange on cybercrime. This year's Conference will take place in Bucharest, Romania between 13-15 December, providing an opportunity for cybercrime experts from public and private sectors as well as international and non-governmental organisations from all over the world to share experience." READ MORE

Source: Diplo

Date: 16 May 2023

The UN process to negotiate the cybercrime convention: Key takeaways from the fifth session

"The almost two-week-long fifth session of the UN's Ad Hoc Committee (AHC) to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purpose came to a close. The UN member states continued to discuss the consolidated negotiating document (CND) (21 April 2023), particularly focusing on the preamble, the provisions on international cooperation, preventive measures, technical assistance, and mechanisms for the implementation of the future convention." READ MORE

Source: Council of Europe

Date: 16 May 2023

Time for urgent action to stop democratic backsliding, Secretary General tells Summit

"Secretary General Marija Pejčinović Burić has called on Europe's leaders to act urgently to reverse a slide in democracy. Speaking at the opening session of the fourth Council of Europe Summit of Heads of State and Government, she stressed that Russia's aggression against Ukraine was an extreme example of democratic backsliding. Freedom of expression – especially in the media, freedom of association, and a rise in discrimination and hate speech against minority groups were also apparent. "You can stop this. You can reverse these trends. You can answer Russia's spiral of descent by lifting Europe up – and ensuring the peace and democratic security that come when the rights of every individual are respected. This summit provides you with that opportunity… And not just in words, but by deeds," she said." READ MORE

Source: Council of Europe

Date: 26 May 2023

Public consultation on CM Recommendation on Combating Hate Crime

"The public consultation on the draft text of the Committee of Ministers Recommendation on Combating Hate Crime is open from 26 May to 3 July 2023. This recommendation will provide non-binding guidance for member states and other key stakeholders on a comprehensive approach to addressing hate crime within a human rights framework." READ MORE

Source: The Unites States Department of Justice

Date: 16 May 2023

Russian National Charged with Ransomware Attacks Against Critical Infrastructure

"The Justice Department today unsealed two indictments charging a Russian national and resident with using three different ransomware variants to attack numerous victims throughout the United States, including law enforcement agencies in Washington, D.C. and New Jersey, as well as victims in healthcare and other sectors nationwide." READ MORE

RELATED ARTICLE:

Krebs on security, Russian Hacker "Wazawaka" Indicted for Ransomware, 16 May 2023

Source: The Record

Date: 23 May 2023

Spying campaign targets Ukraine, Israel, India, Kazakhstan and others, cyber agency says

"Ukraine's computer emergency response team, CERT-UA, has identified a cyber-espionage campaign targeting an undisclosed government agency in Ukraine. A threat actor identified by researchers as UAC-0063 "has also shown interest" in targeting Mongolia, Kazakhstan, Kyrgyzstan, Israel and India, according to the report published on Monday. Researchers initially detected activity associated with UAC-0063 in 2021, but the group's origins remain unclear. The goal of its attacks, according to CERT-UA, is gathering intelligence." READ MORE

RELATED ARTICLE:

Dark Reading, Russia's War in Ukraine Shows Cyberattacks Can Be War Crimes, 26 May 2023

Source: European Council

Date: 16 May 2023

Digital finance: Council adopts new rules on markets in crypto-assets (MiCA)

"The EU brings crypto-assets, crypto-assets issuers and crypto-asset service providers under a regulatory framework. Setting an EU level legal framework for this sector for the first time, the Council today adopted a regulation on markets in crypto-assets (MiCA). […] MiCA will protect investors by increasing transparency and putting in place a comprehensive framework for issuers and service providers including compliance with the anti-money laundering rules. The new rules cover issuers of utility tokens, asset referenced tokens and so-called 'stablecoins'. It also covers service providers such as trading venues and the wallets where crypto-assets are held." READ MORE

Source: CISA *Date: 23 May 2023*	## CISA, FBI, NSA, MS-ISAC Publish Updated #StopRansomware Guide "The Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), National Security Agency (NSA), and Multi-State Information Sharing and Analysis Center (MS-ISAC) today published the #StopRansomware Guide—an updated version of the 2020 guide containing additional recommended actions, resources, and tools. " READ MORE
Source: Europol *Date: 26 May 2023*	## Six sexually-abused children rescued as a result of Europol victim identification taskforce "Six victims of child sexual abuse have been identified and removed from harm as a result of the 12th Victim Identification Taskforce organised by Europol's European Cybercrime Centre (EC3). Between 8 and 19 May, over 30 victim identification specialists from across the world joined forces at Europol's headquarters and online to identify victims and offenders depicted in child sexual abuse material. " READ MORE
Source: Eurojust *Date: 22 May 2023*	## Main administrator of iSpoof website sentenced to 13 years "iSpoof, a website that allowed criminals to impersonate trusted corporations, was taken down in November 2022 in an international joint action that led to 142 arrests. The main administrator of the website has now been sentenced to 13 years and 4 months of imprisonment by Southwark Crown Court in the United Kingdom. Eurojust supported the investigation and played a key role in facilitating judicial cross-border cooperation between all parties involved. […] From August 2021 to August 2022, around 10 million fraudulent calls were made globally via iSpoof. At the point of closure, the website had 59,000 registered users." READ MORE
Source: Poder Judicial del Peru *Date: 24 May 2023*	## Peru: Magistrados del Poder Judicial y del Ministerio Pùblico se especializan en ciberdelincuencia y pruebas electrónicas "En el marco del Convenio de Budapest sobre la Ciberdelincuencia, el Proyecto "The Global Action on Cybercrime Extended (GLACY+), cofinanciado por la Comisión Europea y el Consejo de Europa, a través del Poder Judicial, dio inicio al Programa de Especialización en Formación de Formadores sobre Ciberdelincuencia y Pruebas Electrónicas, en la sede de la Academia de la Magistratura, del 22 al 26 de mayo, con la participación de 13 jueces y 15 fiscales seleccionados por sus respectivas instituciones." READ MORE RELATED ARTICLES: Council of Europe, GLACY+: First part of the ToT on Cybercrime and Electronic Evidence for judges and prosecutors in Peru, 22-26 May 2023 Council of Europe. GLACY+: Peruvian training institutions for judges and prosecutors to streamline cybercrime and electronic evidence, 24-25 April 2023

Source: Ministerio Publico Federal

Date: 24 May 2023

Brazil: MPF e Conselho da Europa promovem Encontro Internacional das Redes de Ministérios Públicos sobre Cibercriminalidade e Provas Digitais

"Conselho da Europa, em parceria com MPF, realiza 1º evento após promulgação pelo Brasil, em abril de 2023, da Convenção sobre Crime Cibernético. "O tema da criminalidade cibernética é estratégico e prioritário para o Ministério Público Federal brasileiro". A afirmação é do secretário de Cooperação Internacional do MPF, Hindemburgo Chateaubriand, que deu início, na tarde da terça-feira (23), ao Encontro Internacional das Redes de Ministérios Públicos sobre Cibercriminalidade e Provas Digitais. Promovido pelo MPF em parceria com o Conselho da Europa (COE), o evento reuniu integrantes do Fórum Cibercrime e Prova Digital da Comunidade de Países de Língua Portuguesa (CPLP) e da Rede de Cibercrime da Associação Ibero-americana de Ministérios Públicos (Aiamp), além de autoridades nacionais do Ministério Público e do Judiciário." READ MORE

RELATED ARTICLE:

Ministério Público, Encontro de redes cibercrime de magistrados da CPLP e da Ibero-América, 24 May 2023

Source: Policy modelling

Date: 26 May 2023

Brazil's recent ratification of the budapest convention on cybercrime

"By signing the Budapest Convention, Brazil joins over 60 countries – as of today, precisely 68 countries are parties to the Convention and 20 others have signed or been invited to accede. The Budapest Convention is over 20 years old now and there have undeniably been immense changes in society and technology in the years since then. […] These circumstances are currently inspiring the United Nations' attempt to propose its own convention on cybercrime, which has been under discussion since 2019. Although Brazil's ratification of the Budapest Convention occurred much later than most developed countries, this landmark decision is expected to contribute to advances in legislation and in the practices of prevention and prosecution bodies." READ MORE

Source: Dig Watch

Date: 29 May 2023

Colombian government suffers cyberattacks by hacktivist groups

"The Colombian government websites have become targets of hacktivist groups SiegedSec and GhostSec, according to threat intelligence platform FalconFeedsio. Allegedly, these groups have claimed responsibility for leaking a substantial 6GB of data, which includes emails, confidential documents, and ID cards. The affected entities include Corponor – Regional Autonomous Corporation of the Northeastern Border, Bucaramanga Municipal Social Protection Fund, District Secretariat Of Government, IBAL SA ESP, Colombian Agricultural Institute, Subred Sur, Central Board of Accountants, and Local Hospital of Piedecuesta." READ MORE

Source: Ministerio Publico Fiscal

Date: 24 May 2023

Argentina: La inclusión de evidencia digital en investigaciones fue aprobada por la Cámara de Diputados

"Durante la sesión de este martes, se otorgó media sanción al proyecto que impulsa modificaciones en el Código Procesal Penal Provincial, con la finalidad de incluir el tratamiento de la evidencia digital como medio de prueba y la creación de figuras tales como la del agente encubierto digital y la creación de equipos conjuntos de trabajo en la etapa de investigación de delitos informáticos." READ MORE

Source: DPL news

Date: 29 May 2023

República Dominicana: El reto de una nueva diplomacia en el ciberespacio

"Dada la propia naturaleza del Internet con un alcance que trasciende fronteras políticas y geográficas, se requiere de la colaboración y cooperación entre naciones para combatir el cibercrimen, enmarcada en una estrategia de diplomacia y política exterior, indicó en entrevista Claudio Peguero Castillo, embajador y asesor de asuntos cibernéticos del Ministerio de Relaciones Exteriores de República Dominicana." READ MORE

Source: BBC

Date: 26 May 2023

Venezuela: 'I'm paid to tweet state propaganda'

"Rafael - not his real name - is a massive internet nerd. At 59 years old, he is active on all the main social media platforms, dabbles in cryptocurrencies and even calls himself an influencer. But that is not all he does online. Rafael is also part of a group of Venezuelans being paid by the state to tweet propaganda." READ MORE

Source: Council of Europe

Date: 29-31 May 2023

CyberSouth: Training course on electronic evidence for judges and prosecutors

"The CyberSouth and AP-JUST projects, joint endeavours of the Council of Europe and European Union, co-organised the training course on electronic evidence for Tunisian judges and prosecutors, in co-operation with the Institut Supérieur de la Magistrature, during 29-31 May 2023, in Tunis, Tunisia" READ MORE

Source: Dig Watch

Date: 27 May 2023

Senegal: Senegalese government websites suffer major cyberattacks

"The hacker group Mysterious Team has carried out major cyberattacks on a number of Senegalese government websites, leaving dozens of sites inaccessible. The Senegalese government spokesman confirmed this major cyberattack in a statement. The hacker group said it wanted to 'liberate Senegal from dictatorship' and send a message to President Macky Sall as a final warning against a tense political backdrop in which Senegal's public prosecutor is seeking a 10-year prison sentence for opposition leader Sonko, allegedly aimed at derailing his 2024 presidential bid." READ MORE

Source: CNN

Date: 25 May 2023

Uganda: 'People find us easy targets': Women politicians face a torrent of online abuse but say they won't stop their work

"Doreen Nyanjura is a modern politician. She announced on Twitter that she would be standing in Uganda's 2026 presidential election; has a name for her supporters -- the Nyanjuraholics -- and has characterized her platform with a catchy hashtag: #ThePoliticalAntidote. But with this presence online, Nyanjura says she faces the now-standard challenges of being a woman in politics: in addition to the tweets of support or derision that most politicians on social media have become accustomed to, Nyanjura also receives tweets of misogynistic mockery." READ MORE

Source: Reuters

Date: 25 May 2023

Kenya: Chinese hackers attacked Kenyan government as debt strains grew

"Chinese hackers targeted Kenya's government in a widespread, years-long series of digital intrusions against key ministries and state institutions, according to three sources, cybersecurity research reports and Reuters' own analysis of technical data related to the hackings. Two of the sources assessed the hacks to be aimed, at least in part, at gaining information on debt owed to Beijing by the East African nation […]. A Kenyan cybersecurity expert described similar hacking activity against the foreign and finance ministries." READ MORE

Source: Peoples Gazette

Date: 24 May 2023

Nigeria: We'll strengthen, enhance cybersecurity's existing legal framework: Malami

Attorney General of the Federation and Minister of Justice, Abubakar Malami, SAN, says the ministry will continue to strengthen and enhance the existing legal framework on cybersecurity to have a secured nation. Mr Malami said this at the first national consultation on the cybercrimes legal framework jointly sponsored by the GLACY+ and OCWAR-C, both EU-funded projects, in collaboration with the Federal Ministry of Justice." READ MORE

RELATED ARTICLE:

Voice of Nigeria, Nigeria Partners With AU, EU To Tackle Cybercrime, 24 May 2023

Source: Reuters

Date: 25 May 2023

TikTok tests AI chatbot 'Tako' in the Philippines

"Social media platform TikTok said on Thursday it is in the early stages of exploring a chatbot called "Tako" that can converse with users about short videos and help them discover content and is conducting tests with select users in the Philippines. OpenAI, backed by Microsoft Corp (MSFT.O), last year launched chatbot ChatGPT, offering arguably the most natural interaction to date. That triggered a race to develop features based on game-changing generative artificial intelligence (AI), including TikTok rival Snap Inc (SNAP.N) whose "My AI" is powered by ChatGPT technology." READ MORE

Source: Medium

Date: 31 May 2023

Uppsala Security participated at the GLACY+ (Global Action on Cybercrime Extended) in Sri Lanka, organized by INTERPOL and Council of Europe

"Uppsala Security, a state-of-the-art provider of award-winning security tools and services for Crypto AML/CTF, Transaction Risk Management, Regulatory Compliance and Transaction Tracking, recently had the privilege of participating in the GLACY+ (Global Action on Cybercrime Extended) event held in Sri Lanka. The event, organized by INTERPOL and Council of Europe, was the GLACY+ Project's Advisory Workshop on Search, Seizure, and Confiscation of Online Crime Proceeds. Held from 22nd to 25th May 2023, the workshop aimed to enhance knowledge and expertise among cybercrime and financial crime investigators." READ MORE

Source: Council of Europe

Date: 17 May 2023

GLACY+: Co-operation with Timor-Leste on the legislative reform on cybercrime and electronic evidence

"On 17 May 2023, the GLACY+ Project, a joint action of the European Union and the Council of Europe, in co-operation with the Ministry of Justice of Timor-Leste, organised a one-day workshop to discuss the draft law currently being prepared by the national authorities in view of implementing the Convention cybercrime in the domestic legislation. […] Timor-Leste was invited to accede to the Convention on Cybercrime in October 2022. Under the framework of GLACY+ project, the Council of Europe will continue the co-operation with the authorities of Timor-Leste on the legislative reform, to ensure full transposition of the provisions of the Budapest Convention into the national legal framework." READ MORE

RELATED ARTICLE:

Council of Europe, GLACY+ welcomes Timor-Leste as a priority country, 15-16 May 2023

Source: The Guardian

Date: 16 May 2023

Australian government threatens tougher regulation as eSafety commissioner decries Twitter's 'sewer rats'

"The Australian government would consider a tougher crackdown on Twitter if the company fails to comply with online safety laws and takedown notices, the communications minister has said. In February, Michelle Rowland wrote to Twitter's vice-president for trust and safety, Ella Irwin, expressing concern over the axing of the company's Australian presence after billionaire Elon Musk's takeover of the platform. Her concerns centred on the impact it would have for government agencies and law enforcement communicating with the company." READ MORE

Source: Council of Europe

Date: 23 May 2023

CyberEast: Seventh Steering Committee Meeting takes place in Chisinau

"During the Seventh Steering Committee Meeting of the CyberEast project, representatives of the country teams, members of the European Commission (joining online) and of the C-PROC team reviewed major outcomes of the project and established a workplan for the remainder of 2023. On this occasion, the participants also discussed a proposal for the new CyberEast+ regional project, currently negotiated with the European Commission." READ MORE

Source: Council of Europe

Date: 24-25 May 2023

CyberEast: Regional meeting between cybercrime experts, financial investigators and financial intelligence units to improve international co-operation and information sharing

"The Regional meeting to improve international co-operation and information sharing, which took place on 24-25 May 2023 in Chisinau, Moldova, brought together cybercrime and financial investigators, prosecutors and representatives of financial intelligence units (FIUs) from the project countries. The discussions, led by Council of Europe international consultants, focused on parallel financial investigations and intelligence, online crime proceeds, financial fraud and money laundering offences in the Eastern Partnership countries. Participants showcased national practices and legislation on virtual currencies and Darknet investigations in the context of the "follow the money" concept." READ MORE

Source: OSCE

Date: 22 May 2023

OSCE launches project on prevention of cyberbullying in Brčko District of BiH

"The OSCE Mission to BiH (the Mission), in co-operation with the Brčko District Government's Police and Education Department, launched the "No to Internet violence!" project today. The project focuses on preventing and addressing cyberbullying. The launch was attended by representatives of schools, NGOs, and the media, as well as the Brčko Municipal Committee for Youth, the Brčko District Police, and the Education Department of the Brčko District Government." READ MORE

Source: POLITICO

Date: 22 May 2023

EU hits Meta with record €1.2B privacy fine

"U.S. tech giant Meta has been hit with a record €1.2 billion fine for not complying with the EU's privacy rulebook. The Irish Data Protection Commission announced on Monday that Meta violated the General Data Protection Regulation (GDPR) when it shuttled troves of personal data of European Facebook users to the United States without sufficiently protecting them from Washington's data surveillance practices." READ MORE

RELATED ARTICLE:

The Guardian, EU, U.S. data transfer pact expected by summer, EU Commission says after Meta fine, 22 May 2023

Source: CySecurity

Date: 23 May 2023

How hackers launched an attack on European spacecraft

"Space warfare is unavoidable, and the space ecology must be ready at all times. The European Space Agency (ESA) issued a challenge to cybersecurity specialists in the space industry ecosystem to interfere with the operation of the ESA's "OPS-SAT" demonstration nanosatellite in a capability demonstrator during an annual event on cybersecurity for the space industry." READ MORE

Source: Grapevine

Date: 16 May 2023

Icelandic web domains targets of cybercrime

"On May 16, Icelandic cyber defence force CERT-IS confirmed that Icelandic web domains have been under fire by hackers. The Russian hacker group NoName057 has assumed responsibility for the cybercrimes, citing support for Russia as their motive. DDoS attacks were made against Icelandic websites and web hosts, temporarily shutting them down. Among the victims was Alþingi's official web page." READ MORE

Source: US Embassy in Croatia

Date: 12 May 2023

United States and Croatia sign agreement on cybercrime cooperation

"On May 22, the United States and Croatia signed a memorandum of understanding to facilitate new cybercrime cooperation. Minister of Justice and Public Administration Ivan Malenica, Croatia's State Attorney General Zlata Hrvoj-Šipek, and U.S. Deputy Chief of Mission Amy Davison signed the memorandum of understanding in Šibenik. "This agreement demonstrates the United States' strong commitment to work closely and vigilantly with allies globally to improve cybersecurity and combat cybercrime," said Deputy Chief of Mission Amy Davison." READ MORE

Source: Wired

Date: 22 May 2023

Leaked Government Document Shows Spain Wants to Ban End-to-End Encryption

"SPAIN HAS ADVOCATED banning encryption for hundreds of millions of people within the European Union, according to a leaked document obtained by WIRED that reveals strong support among EU member states for proposals to scan private messages for illegal content. The document, a European Council survey of member countries' views on encryption regulation, offered officials' behind-the-scenes opinions on how to craft a highly controversial law to stop the spread of child sexual abuse material (CSAM) in Europe." READ MORE

Source: Reuters

Date: 18May 2023

Polish news websites hit by DDoS attacks

"Several Polish news websites were hit by distributed denial-of-service (DDoS) attacks that the government said could be the action of Russian hacking groups, the digitalisation minister was quoted as saying on Thursday. Warsaw has positioned itself as one of Ukraine's staunchest allies since Russia invaded the country, and Poland says it frequently faces Russian attempts to destabilise the situation in the country. […] According to PAP, the websites affected included those of daily newspapers Gazeta Wyborcza, Rzeczpospolita and Super Express." READ MORE

Source: CyberPeace

Date: 25 May 2023

G7 on cybercrime and artificial intelligence

"The G7 nations, a group of the most powerful economies, have recently turned their attention to the critical issue of cybercrimes and (AI) Artificial Intelligence. G7 summit has provided an essential platform for discussing the threats and crimes occurring from AI and lack of cybersecurity. These nations have united to share their expertise, resources, diplomatic efforts and strategies to fight against cybercrimes. In this blog, we shall investigate the recent development and initiatives undertaken by G7 nations, exploring their joint efforts to combat cybercrime and navigate the evolving landscape of artificial intelligence. We shall also explore the new and emerging trends in cybersecurity, providing insights into ongoing challenges and innovative approaches adopted by the G7 nations and the wider international community." READ MORE

RELATED ARTICLES:

The Guardian, UK will lead on 'guard rails' to limit dangers of AI, says Rishi Sunak, 18 May 2023

Foreign Policy, China's Tech Threat Hangs Over the G-7, 19 May 2023

Source: The Record

Date: 17 May 2023

Ukraine, Ireland, Iceland and Japan officially join NATO's cyber defense center

"The flags of Ukraine, the Republic of Ireland, Iceland and Japan were hoisted in Tallinn, Estonia, on Tuesday as the four nations officially joined NATO's Cooperative Cyber Defense Center of Excellence (CCDCOE). The CCDCOE was founded in 2008, a few years after Estonia joined NATO, in the wake of a wave of cyberattacks targeting the country when it relocated a Soviet war memorial from the center of the capital Tallinn to a military cemetery a few kilometers away." READ MORE

Latest reports

- Team CYMRU, Visualizing QakBot Infrastructure, 16 May 2023

- National Police Chiefs' Council, National Violence Against Women and Girls (VAWG) Strategic Threat and Risk Assessment (STRA), 18 May 2023

- APT, Activity Report Q42022-Q1 2023, 22 May 2023

- The Good Men Project, Why Feminist Research Is Necessary to Address Technology-Facilitated Gender-Based Violence: Recommendations and Way Forward, 22 May 2023

- El Pais, Is digital violence in an AI era yet another threat to women?, 22 May 2023

- Fortinet, WINTAPIX: A New Kernel Driver Targeting Countries in The Middle East, 22 May 2023

- We live security, Android app breaking bad: From legitimate screen recording to file exfiltration within a year, 23 May 2022

- SecureList, Meet the GoldenJackal APT group. Don't expect any howls, 23 May 2023

- ENISA, 5G Security Controls Matrix, 24 May 2023

- ENISA, DNS Identity, 24 May 2023

- JournalduCoin, Cybercriminalité: 70 % de hacks en moins sur ce début d'année 2023, 24 May 2023

- CISCO, Mercenary mayhem: A technical analysis of Intellexa's PREDATOR spyware, 25 May 2023

- CitizenLab, Pegasus infections in Armenian Civil Society, 25 May 2023

- CyberPeace Foundation, G7 on cybercrime and artificial intelligence, 25 May 2023

- Security Journal, Foundations and trends in the darknet-related criminals in the last 10 years: a systematic literature review and bibliometric analysis, 28 May 2023

- Lexology, Recent Developments To The EU'S Cyber Resilience Framework, 29 May 2023

- JP CERT, GobRAT malware written in Go language targeting Linux routers, 29 May 2023

- We live security, Tricks of the trade: How a cybercrime ring operated a multi-level fraud scheme, 30 May 2023

- EDRI, Open letter: Gender-inclusive and safe digital world that is free from violence for all, 30 May 2023

- Microsoft, Cyber Signals, May 2023

- European Council, Cybersécurité: comment l'UE lutte contre les cybermenaces, May 2023

- Microsoft, The Confidence Game: Shifting Tactics Fuel Surge in Business Email Compromise, May 2023

- Australian Government, Data and Digital Government Strategy: The data and digital vision for a world-leading APS to 2030, May 2023

Upcoming events

- 1 June, C-PROC/TUNISIA, *(in-person),* 10th Steering Committee of CyberSouth, CyberSouth

- 1-2 June, C-PROC/GEORGIA, *(in person),* Training on cyber incident and cybercrime taxonomy and handling in accordance with agreed SOPs, CyberEast

- 5-6 June, C-PROC/AZERBAIJAN, *(in person),* Training on cyber incident and cybercrime taxonomy and handling in accordance with agreed SOPs CyberEast

- 5-7 June, C-PROC/ SAUDI ARABIA*, (in-person),* Support to the 14th Middle East and North Africa Working Group meeting on Cybercrime for Heads of Units (organised by Interpol), CyberSouth

- 5–8 June, C-PROC/COSTA RICA *(in-person*), 12th Summit of RightsCon, Octopus, GLACY+

- 6-8 June, ISS/Czech Republic, *(in-person*), ISS World Europe Conference, iPROCEEDS-2

- 6-7 June, C-PROC/IRELAND, *(in-person),* Visit to multinational Service Providers of a delegation of representatives from Algeria, Jordan, Lebanon, Morocco and Tunisia at their EMEA HQ in Dublin, CyberSouth

- 6-7 June, C-PROC/GHANA, *(in-person),* Advisory workshop on cybercrime reporting and criminal justice statistics, GLACY+

- 8-9 June, C-PROC/MOLDOVA & UKRAINE, *(in-person*), Training on cyber incident and cybercrime taxonomy and handling in accordance with agreed SOPs CyberEast

- 8–9 June, C-PROC/GHANA *(in-person),* Workshop on enhanced cooperation and disclosure of electronic evidence, Octopus, T-CY, GLACY+

- 12 - 13 June, C-PROC/ BENIN*, (in-person),* Advisory workshop on integration/ mainstreaming of training modules in curricula of judicial training institutions and prosecutors' training institution, GLACY+

- 12-15 June, C-PROC/Serbia, *(in-person*), Specialised Judicial Training Course on International Cooperation and workshops, iPROCEEDS-2

- 13-16 June, C-PROC/Albania, *(in-person*), Regional Specialised Judicial Training Course on Electronic Evidence and workshop, iPROCEEDS-2

- 13-16 June, C-PROC/ ALBANIA, *(in-person),* Support for participation to the Regional Judicial Training Course on Electronic Evidence, GLACY+

- 14 June*, (in-person),* Cyber Project Community meeting, Brussels, Belgium, GLACY+, T-CY

- 15 June, C-PROC/ GHANA, *(in-person),* Advisory workshop on mainstreaming regional training centres on cybercrime and electronic evidence training strategies, GLACY+

- June 2023, C-PROC*, (online),* Meeting of the working group on online training platform, Octopus

- Mid-June 2023, C-PROC*, (online),* publication of additional resources on the cyberviolence portal, Octopus

- June 2023, C-PROC/SEYCHELLES, *(online),* Advisory mission on cybercrime and electronic evidence legislation and accession to the Convention on Cybercrime for Seychelles, Octopus, T-CY

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