Cybercrime Digest

Bi-weekly update and global outlook by the
Cybercrime Programme Office of the Council of Europe (C-PROC) 15–28 February 2023

Source: Council of Europe

Date: 16 Feb 2023

Convenio sobre ciberdelincuencia: Argentina firma el protocolo sobre divulgación de pruebas electrónicas

"Argentina se ha convertido en el 35º Estado en firmar el Segundo protocolo adicional al Convenio sobre ciberdelincuencia, que pretende mejorar la cooperación internacional y la divulgación de pruebas electrónicas. El ministro de Seguridad de Argentina, Aníbal Fernández, ha firmado el tratado en Estrasburgo en presencia de la secretaria general, Marija Pejčinović Burić. […] En una reunión tras la firma, la secretaria general y el ministro debatieron sobre la necesidad de que el futuro tratado de las Naciones Unidas sobre ciberdelincuencia contenga sólidas salvaguardias en materia de derechos humanos y de Estado de derecho, y que sea coherente con el Convenio sobre ciberdelincuencia del Consejo de Europa." READ MORE

RELATED ARTICLES:

Ministerio de Seguridad Argentina, Argentina y la Unión Europea unen esfuerzos para combatir el ciberdelito, 16 de febrero de 2023

Baker McKenzie, Argentina suscribió al Segundo Protocolo Adicional a la Convención de Budapest sobre Ciberdelincuencia, Febrero 2023

Source: Council of Europe
Date: 27 Feb 2023

Albania becomes 36th State to sign the Second Additional Protocol to Convention on Cybercrime

"Today, 27 February 2023, Ambassador Dastid KORESHI, Permanent Representative of Albania, 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.The Second Additional 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." READ MORE

Source: IT Pro

Date: 22 Feb 2023

The UN's cybercrime treaty could be a privacy disaster

"Cyber crime is hard to define and even more difficult to attribute and prosecute, especially given cyber attacks strike regularly across borders. With this in mind, a United Nations (UN) committee has been in negotiations this year to flesh out a new international cyber crime treaty. […] In theory, the treaty is positive, but it's been heavily criticised too, with experts saying its impact will be limited – especially since the 2001 Budapest Convention already in place addresses many of the issues outlined." READ MORE

RELATED ARTICLE:

Cyber Peace Institute, A year of United Nations cybercrime negotiations, 28 February 2023

Source: France 24

Date: 28 Feb 2023

Accountability and justice: Gathering digital evidence of war crimes in Ukraine

"As the UN Human Rights Council meets to discuss expanding its investigation into war crimes committed in Ukraine, individuals and organisations are gathering their own digital evidence of human rights violations. Social media posts, satellite imagery and online videos are some of the images being used to create a digital archive of war crimes in real time. At the opening of a UN Human Rights Council meeting in Geneva on Monday, UN Secretary-General Antonio Guterres said the Russian invasion of Ukraine had led to "most massive violations of human rights" in the world today, including cases of sexual violence, forced disappearances, arbitrary detentions and violations of the rights of prisoners of war documented by the UN human rights office." READ MORE

RELATED ARTICLES:

The Register, Ukraine invasion blew up Russian cybercrime alliances, 19 February 2023

Security Week, A Year of Conflict: Cybersecurity Industry Assesses Impact of Russia-Ukraine War, 24 February 2023

Axios, Russia's yearlong cyber focus on Ukraine, 24 February 2023

Google, Fog of war: how the Ukraine conflict transformed the cyber threat landscape, 16 February 2023

Source: Eurojust

Date: 23 Feb 2023

Start of operations of Core International Crimes Evidence Database and new International Centre for Prosecution of the crime of Aggression to be based at Agency

"Almost one year after the start of the war in Ukraine, Eurojust has taken crucial steps in support of the judicial response to alleged core international crimes. An important milestone is the start of operations of the Core International Crimes Evidence Database (CICED). A new International Centre for Prosecution of the crime of Aggression (ICPA) will also be based at Eurojust. With CICED, the Agency has introduced a tailor-made judicial database to preserve, store and analyse evidence of core international crimes in a secure mode." READ MORE

Source: Council of Europe

Date: 22 Feb 2023

First ever launch of the Council of Europe HELP course "Cybercrime and Electronic Evidence"

"The HELP course on Cybercrime and Electronic Evidence was launched for the first time on 22 February for a selected group of 120 lawyers from Slovakia and Bulgaria.The cross-border event, held at the premises of the Slovak Bar Association in Bratislava, was organised in the framework of the EU-CoE project "HELP in the EU III", funded under the European Union's Justice Programme (2021-2027)." READ MORE

Source: Council of the European Union

Date: 21 Feb 2023

Combatting violence against women: Council requests the consent of the European Parliament to conclude the Istanbul convention

"The Council today requested the consent of the European Parliament to adopt the decisions on the conclusion by the EU of the convention on preventing and combatting violence against women and domestic violence (Istanbul convention). […] By pledging to implement the convention the EU will be confirming its commitment to combatting violence against women within the EU and globally." READ MORE

Source: Council of Europe

Date: 14-16 Feb 2023

Regional training on Joint Investigative Teams under the Second Additional Protocol to the Convention on Cybercrime (Budapest Convention)

"Between 14 and 16 February 2023, the Regional training on Joint Investigative Teams and improved co-operation with foreign service providers under the Second Additional Protocol to the Convention on Cybercrime (Budapest Convention) brought together participants from over 34 countries. This activity was organised by the joint European Union and Council of Europe projects CyberEast, CyberSouth, GLACY+ and iPROCEEDS-2, in collaboration with the Council of Europe Octopus Project, and in partnership with the Prosecutor General's Office of Portugal." READ MORE

Source: ENISA

Date: 16 Feb 2023

Coordinated Vulnerability Disclosure: Towards a Common EU Approach

"With the new Directive on measures for a high common level of cybersecurity across the Union (NIS2) adopted on 16 January 2023, Member States will need to have a coordinated vulnerability disclosure policy adopted and published by 17 October 2024. In addition, other ongoing legislative developments will also address vulnerability disclosure, with vulnerability handling requirements already foreseen in the proposed Cyber Resilience Act (CRA)." READ MORE

Source: The Record

Date: 17 Feb 2023

Civilian hackers could become military targets, Red Cross warns

"Civilians taking to cyberspace to participate in hostilities between Russia and Ukraine could be lawfully exposed to military actions in response, a senior official from the International Committee of the Red Cross (ICRC) warned on Friday. Mauro Vignati, the ICRC's advisor on the digital technologies of warfare, told the Munich Cyber Security Conference that the organization is concerned about the potential for undermining humanitarian laws protecting civilians during wartime. Digital volunteers, he said, are complicating the legal calculus." READ MORE

Source: Council of Europe

Date: 27 Feb 2023

Delegation of Curaçao visits the Council of Europe

"A delegation from Curaçao, led by the Minister of Traffic, Transport and Spatial Planning Charles Cooper visited the Council of Europe on 27 February 2023. During the meeting with the Deputy Secretary General of the Council of Europe Bjørn Berge and the Ambassador of the Kingdom of the Netherlands Tanja Gonggrijp, the Minister expressed the interest of Curaçao in strengthening its capacities and legislation on cybercrime and electronic evidence. The importance of international co-operation in addressing the growing threat of cybercrime was emphasized as well as the relevance of the tools offered by the Budapest Convention on Cybercrime and related standards." READ MORE

Source: The Hacker News

Date: 28 Feb 2023

APT-C-36 Strikes Again: Blind Eagle Hackers Target Key Industries in Colombia

"The threat actor known as Blind Eagle has been linked to a new campaign targeting various key industries in Colombia. The activity, which was detected by the BlackBerry Research and Intelligence Team on February 20, 2023, is also said to encompass Ecuador, Chile, and Spain, suggesting a slow expansion of the hacking group's victimology footprint. Targeted entities include health, financial, law enforcement, immigration, and an agency in charge of peace negotiation in Colombia, the Canadian cybersecurity company said." READ MORE

Source: El Dia

Date: 28 Feb 2023

Cerca de 40 mil usuarios de RD han sido víctimas de crimen cibernético

"Santo Domingo .-Unas 30,992 denuncias de casos de crímenes y delitos de alta tecnología se han registrado en los últimos seis años en el país. Esa cantidad de denuncias recibidas por las autoridades dominicanas parece mínima, pero de sumarse los casos no notificados esta cifra podría multiplicarse. De acuerdo a las Estadísticas del Ministerio Público, el 2022 fue el año de mayor cantidad de denuncias recibidas, con 8,330, y aunque no describe el tipo de crimen, estudios señalan que las estafas y fraudes por internet representan el principal delito efectuado en territorio dominicano." READ MORE

Source: La Republica

Date: 27 Feb 2023

Hackers trataron de atacar a Costa Rica dos mil millones de veces el año pasado

"En un promedio superior a los cinco millones de intentos de vulneraciones por día, los ciberatacantes trataron de comprometer sistemas informáticos públicos y privados costarricenses en al menos dos mil millones de veces en 2022, según reveló la firma especializada Fortinet. A pesar de ello, nuestro país no se ubica en el podio de este estudio, que coloca a México como el país más atacado de América Latina, seguido de Brasil y Colombia. A nivel regional, los intentos por dañar servidores y end points sumaron más de 360 mil millones el año pasado." READ MORE

Source: Indigo

Date: 21 Feb 2023

México vulnerable ante la ciberdelincuencia

"Debido a la falta de una cultura de ciberseguridad, a la poca inversión tecnológica y a una actitud reactiva, México es el blanco perfecto para los ciberdelincuentes que atacan a entes públicos, empresas privadas y llenan sus bolsillos de dinero robado. México se encuentra vulnerable ante la ciberdelincuencia y el hackeo masivo de información confidencial de la Secretaría de la Defensa Nacional (Sedena), perpetrado por la organización Guacamaya Leaks, pone evidencia el atraso que tenemos en ciberseguridad." READ MORE

Source: Forbidden Stories

Date: 20 Feb 2023

When your "friends" spy on you: The firm pitching Orwellian social media surveillance to militaries

"Hidden in a trove of leaked Colombian military documents, Forbidden Stories found a confidential brochure – linked to a shadowy company called S2T Unlocking Cyberspace – illustrating how open-source intelligence tools can be used to target journalists and activists. […] Forbidden Stories found the brochure in a trove of more than 500,000 documents belonging to the Military Forces of Colombia, leaked to Forbidden Stories by a collective of hackers known as Guacamaya." READ MORE

Source: ADF

Date: 28 Feb 2023

La CEDEAO aspire à améliorer la cybersécurité en renforçant la confiance et la coopération

"La croissance rapide de l'utilisation de l'Internet en Afrique de l'Ouest suscite des recommandations pour que la région coopère en matière de cybersécurité. Une approche conjointe pourrait protéger les individus, les entreprises, les institutions gouvernementales et l'infrastructure critique contre les attaques en ligne, selon l'experte en cybersécurité Folake Olagunju. « Ce doit être une approche pan-sociétale », déclare Mme Olagunju pendant une interview de podcast avec l'International Partners Academy de l'UE. Elle est chef de programme pour l'Internet et la cybersécurité de la CEDEAO (Communauté économique des États de l'Afrique de l'Ouest)." READ MORE

Source: CIPESA

Date: 15 Feb 2023

Building Cyber Smart Women Entrepreneurs in Nigeria

"According to the Global Entrepreneurship Monitor, Nigeria is among the countries with the highest number of women entrepreneurs, most of whom conduct their business online. However, with the increasing prevalence of cyber attacks and fraud, the success of women-owned Small and Media Enterprises (SMEs) in the country is under threat. In Nigeria, Africa's largest economy, Sophos reports that 71% of businesses were hit with ransomware attacks in 2021." READ MORE

Source: QUARTZ

Date: 22 Feb 2023

How Ghana and Gambia are planning to bolster their digital economies

"As legacy economies continue to fall out of favor the world over, Ghana and Gambia are ramping up efforts to build tech-based economies.In a time when most economies run by oil, manufacturing, and agriculture are shifting to digital economies, the two countries with a combined population of 35 million don't want to be sidelined. Now, they have joined Nigeria, Rwanda, Morocco, and Djibouti as members of the Digital Cooperation Organization (DCO) that aims to link Africa and Gulf countries in the realization of a common digital economy agenda." READ MORE

Source: Master Card

Date: 27 Feb 2023

Helping Nigerian SMEs fight cybercrime

"The world is witnessing a surge in cybercrime, and Nigeria is no exception. According to the Nigerian Communications Commission, the country loses an estimated USD0.5 billion every year due to cybercrime. SMEs are an easy target for cybercriminals, as they typically lack the resources to protect themselves from threats or to put up effective defenses once they have been breached. The health and sustainability of SMEs is essential for economic prosperity. According to the World Bank, SMEs represent about 90% of companies worldwide and employ more than 50% of the global workforce." READ MORE

RELATED ARTICLE:

The World Bank, Small and Medium Enterprises (SMEs) Finance

Source: Council of Europe

Date: 17 Feb 2023

CyberSouth: National workshop on data protection for multiple Lebanese stakeholders

"A Specialised Course on International Co-operation for Albanian judges and prosecutors was delivered within the framework of the EU-CoE Joint Project iPROCEEDS-2 between 31 January – 1 February 2023. Back-to-back with the course, a workshop on Sharing Electronic Evidence in International Investigations took place on 1 February. The participants discussed the need to amend the current national legislation on data protection and reviewed the proposed amendments, reflected in a draft law pending parliamentary approval." READ MORE

Source: CajNews Africa

Date: 22 Feb 2023

Internet providers urge immediate action against ransomware

"SOUTH Africa's Internet Service Providers' Association (ISPA) has urged local companies to routinely evaluate ransomware defences and regularly test disaster recovery procedures as local firms are increasingly in the sights of organised cyber criminals. ISPA warned that with the average cost of remediating a ransomware attack in the country estimated last year by cyber security firm Sophos to be R6,4 million (US$350 542), there are significant financial and legal risks to exposure to the online realm." READ MORE

Source: Cio mag

Date: 16 Feb 2023

Côte d'Ivoire – Cybersécurité et protection des données : vers la ratification de la Convention de Malabo

"Le projet de loi autorisant la ratification de la convention de Malabo sur la cybersécurité et la protection des données à caractère personnel a été adopté par le Conseil des ministres le mercredi 15 février à Abidjan. Selon le communiqué dudit Conseil, la ratification de cette convention permettra à la Côte d'ivoire, de concert avec les Etats membres de l'Union africaine, de consolider la stratégie de répression de la cybercriminalité, en vue de faire face à cette menace qui fragilise la sécurité des réseaux informatiques et le développement de la société de l'information africaine, en construction." READ MORE

Source: CyberNews

Date: 23 Feb 2023

Threat group using ancient Hindu sage name as smokescreen, analyst suggests

"A new threat group has appeared on the cybercrime scene and appears to be going after targets in Asia – however, it is not known which country it is affiliated to, with indicators suggesting India likely to be "false flags", according to researcher Symantec. Dubbed Clasiopia by the cyber analyst, the threat group was observed targeting a research body in Asia with what looks to be a custom-made malware tool known as Backdoor.Atharvan. The latter takes its name from a legendary Hindu sage in ancient Vedic scripture, though Symantec believes this could simply be a red herring left by cunning threat actors." READ MORE

Source: Bank Info Security

Date: 24 Feb 2023

Asia-Pacific Faced the Highest Share of Cyberattacks in 2022

"The Asia-Pacific region had the dubious distinction of being the global region that faced the most cyberattacks during 2022, as observed by IBM's threat intelligence platform. IBM says the region accounted for 31% of all incidents monitored during 2022, putting it slightly ahead of Europe at 28% and North American at 25%. The numbers come from an annual report detailing the threat landscape. It finds that Asia-Pacific - specifically Japan - was the epicenter of a spike of Emotet malware that coincided with Russia's February 2022 invasion of Ukraine." READ MORE

Source: CDN

Date: 24 Feb 2023

Philippines: Cybercrime units will soon be opened in Lapu-Lapu police stations

"LAPU-LAPU CITY, Cebu, Philippines — The Lapu-Lapu City Police Office (LCPO) plans to create cybercrime units especially now that the city government has launched the Paleng-QR PH program in the its markets.Police Colonel Elmer Lim, city director of LCPO, said that they first had to capacitate or train their investigators about cybercrimes and how to handle them.Due to this, Lim said that they would be coordinating with the Cybercrime Unit in doing training and capacitating their investigators on these kinds of crimes."READ MORE

Source: Fijivillage

Date: 28 Feb 2023

Vodafone Fiji urging public to be aware of money-making scammers online

"Vodafone Fiji is advising members of the public not to fall into the money-making scam by sending their hard-earned money to fake schemes and must immediately report this matter to the police cybercrime unit. This comes after certain posts being circulated on Facebook showing some people posting screenshots of their M-Paisa balance and videos of them thanking particular persons for transferring thousands of dollars to their M-Paisa accounts. Vodafone Fiji Head of eCommerce & Digital Financial Services, Shailendra Prasad says the large amount of money being shown on the screenshot taken from the M-Paisa app to convince unsuspecting people is doctored and falsified by manually changing the balance to make it look real." READ MORE

Source: The Guardian

Date: 22 Feb 2023

Australia: Twitter, TikTok and Google forced to reveal what they do to combat child abuse

"Twitter, TikTok and Google will be forced to answer questions about how they tackle child sexual abuse and blackmail attempts on their platforms after the Australian eSafety commissioner issued legal notices to the companies.The tech companies, as well as gaming platforms Twitch and Discord, will have 35 days to respond to the commissioner's questions or risk fines of up to $687,000 a day. The legal demands come six months after similar notices were issued to Apple, Meta, Microsoft, Snap and Omegle, which revealed some tech platforms were not using well-known safety measures to detect abusive content and protect users."READ MORE

Source: Euractiv

Date: 23 Feb 2023

European Commission bans TikTok from corporate devices

"The EU executive's IT service has asked all Commission employees to uninstall TikTok from their corporate devices, as well as the personal devices using corporate apps, citing data protection concerns. The request to uninstall the Chinese-owned social media app was communicated via email to EU officials on Thursday morning (23 February). "To protect the Commission's data and increase its cybersecurity, the EC [European Commission] Corporate Management Board has decided to suspend the TikTok application on corporate devices and personal devices enrolled in the Commission mobile device services," said the email, seen by EURACTIV." READ MORE

Source: Bitdefender

Date: 16 Feb 2023

Scandinavian Airlines website hit by cyber attack, customer details exposed

"A group calling itself "Anonymous Sudan" has claimed responsibility for a cyber attack which knocked the website of Scandinavian Airlines (SAS) offline earlier this week, and left customer data exposed.In a statement published on its corporate website, the airline explained that it and "several other companies" had been targeted in an attack that left its website and smartphone app down for some hours." READ MORE

Source: Security affairs

Date: 17 Feb 2023

German airport websites hit by DDos attacks once again

"Experts are investigating the failures of several German airports after some media attributed them to a possible hacking campaign. On Thursday, the websites of several German airports were unreachable, experts launched an investigation speculating a possible cyberattack on a large scale against the critical infrastructure." READ MORE

Source: Krebson Security

Date: 26 Feb 2023

When Low-Tech Hacks Cause High-Impact Breaches

"Web hosting giant GoDaddy made headlines this month when it disclosed that a multi-year breach allowed intruders to steal company source code, siphon customer and employee login credentials, and foist malware on customer websites. Media coverage understandably focused on GoDaddy's admission that it suffered three different cyberattacks over as many years at the hands of the same hacking group." READ MORE

Source: The Register

Date: 17 Feb 2023

Norway finds a way to recover crypto North Korea pinched in Axie heist

"Norwegian authorities announced on Thursday that they had recovered $5.9 million of cryptocurrency stolen in the Axie Infinity hack – an incident widely held to have been perpetrated by the Lazarus Group, which has links to North Korea.The Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (Økokrim) has called the seizure among the largest ever money seizures – and the largest-ever related to crypto – made by Norway." READ MORE

Source: Info Migrants

Date: 16 Feb 2023

German court rejects phone searches of asylum seekers

"Germany's Federal Office for Migration and Refugees (BAMF) may not look at records and data on the cell phones of refugees without good reason, according to a court ruling.According to the final court decision issued in the case, the Federal Office for Migration and Refugees (BAMF) is not allowed to assess any information held on the cell phones of asylum seekers -- unless they have a good reason to do so." READ MORE

Source: Spain in English

Date: 19 Feb 2023

Spain orders extradition of British man to US for alleged hacking & cybercrime

"Spain's National Court has agreed to the extradition to the United States of a British citizen who allegedly took part in computer attacks, including the July 2020 hacking of Twitter accounts of public figures such as Joe Biden, Barack Obama and Bill Gates. […] He is accused of hacking around 130 Twitter accounts. The court document said he is also wanted for hacking the Snapchat account of an unidentified public figure whom he allegedly tried to extort with the threat of publishing nude photographs of the person." READ MORE

Source: Cryptonews

Date: 21 Feb 2023

Cybercrime, crypto scams on the rise in Portugal, say prosecutors

"Cybercrime has "skyrocketed" in Portugal – with crypto scams and ransomware attacks becoming more commonplace in the nation. Sapo reported that, per the nation's Attorney-General, 2,124 cybercrimes were reported in 2022. The number included an unspecified number of crypto scams." READ MORE

Source: BBC

Date: 25 Feb 2023

Signal would 'walk' from UK if Online Safety Bill undermined encryption

"The encrypted-messaging app Signal has said it would stop providing services in the UK if a new law undermined encryption. If forced to weaken the privacy of its messaging system under the Online Safety Bill, the organisation "would absolutely, 100% walk" Signal president Meredith Whittaker told the BBC." READ MORE

Source: The Conversation

Date: 26 Feb 2023

Albanese government to appoint Coordinator for Cyber Security, amid increasing threat to systems and data

"The federal government is further stepping up its efforts to improve Australia's protection against increasing cyber threats, with Prime Minister Anthony Albanese on Monday announcing the establishment of a Coordinator for Cyber Security. The aim is to "ensure a centrally coordinated approach" to the government's cyber security responsibilities. This would include coordinating and "triaging" action after a major incident." READ MORE

Source: Bank Info Security

Date: 17 Feb 2023

Computer Crime: Britain Plans to Overhaul 32-Year-Old Law

"The British government is proposing to give itself more law enforcement powers against hackers in a public consultation critics say is marred by a lack of concrete proposals to shield security researchers acting in good faith.The conservative government of Prime Minister Rishi Sunak unveiled this month proposed updates to the U.K.'s principal anti-hacking law, the Computer Misuse Act of 1990." READ MORE

Source: Info Risk today

Date: 27 Feb 2023

FBI IC3: Healthcare Sector Faced Most Ransomware Attacks Last Year

"The FBI's Internet Complaint Center last year received 870 complaints that "indicated organizations belonging to a critical infrastructure sector were victims of a ransomware attack," said David Scott, deputy assistant director of the FBI's Cyber Division, speaking at the Futurescot conference Monday in Glasgow, Scotland. Critical manufacturing and the government, including schools, followed healthcare as the most-attacked sectors, IC3 data shows." READ MORE

Source: The Washington post

Date: 28 Feb 2023

Canada is latest country to ban TikTok on government phone

"Canada on Monday followed the lead of the U.S. and European Commission and banned the TikTok app from government-issued devices, citing an "unacceptable" level of risk to privacy and security. The Canadian government said it had carried out a review of the video-sharing app owned by a Chinese company and "determined that it presents an unacceptable level of risk to privacy and security." READ MORE

Latest reports

- ENISA, Sustained activity by specific threat actors, 15 February 2023
- European Parliament, Fighting cybercrime: new EU cybersecurity laws explained, 16 February 2023
- Africa.com, Cybersecurity in Africa: Many Still Believe Cybercrime 'Won't affect them', 16 February 2023
- Abnormal, BEC groups wage multilingual executive impersonation attacks targeting companies worldwide, 16 February 2023
- Council of the European Union, Digital files - state of play, 17 February 2023
- Security Affairs, CISA adds Cacti, Office, Windows and iOS bugs to its Known Exploited Vulnerabilities Catalog, 17 February 2023
- INSIDER, How Putin's Russian goon squad used Mexican gig workers to troll an American election, 18 February 2023
- Huma Rights Watch, Middle East, North Africa: Digital Targeting of LGBT People, 21 February 2023
- Forbes, How Women In Tech Are Transforming Social Impact, 21 February 2023
- Trend Micro, A Deep Dive into the Evolution of Ransomware Part 1, 21 February 2023
- IBM, X-Force Threat Intelligence Index, 22 February 2023
- ENISA, Demand Side of Cyber Insurance in the EU, 23 February 2023
- Techcabal, Opinion: How can Africa's financial industry thwart the cybercrime menace?, 23 February 2023
- African Business, Africa's cybersecurity threat, 23 February 2023
- Humanities and Social Science Communications, Exploring the global geography of cybercrime and its driving forces, 23 February 2023
- Nature Portfolio, Exploring the global geography of cybercrime and its driving forces, 23 February 2023
- Team CYMRU, Desde Chile con Malware (From Chile with Malware), 24 February 2023
- Help Net Security, Defenders on high alert as backdoor attacks become more common, 24 February 2023
- Recorded Future, Russia's War Against Ukraine Disrupts the Cybercriminal Ecosystem, 24 February 2023
- Observer Research Fondation, Towards the Integration of Emerging Technologies in India's Armed Forces, 24 February 2023
- ENISA, A Governance Framework for National Cybersecurity Strategies, 28 February 2023
- ENISA, Building Effective Governance Frameworks for the Implementation of National Cybersecurity Strategies, 28 February 2023
- Bitdefender, Bitdefender Releases Decryptor for MortalKombat Ransomware, 28 February 2023
- Council of Europe/Parliamentary Assembly, Parliamentary Toolkit on Hate Speech, February 2023
- Council of Europe/Children's Rights Division, Outcome report of the expert workshop on EU proposed regulation on preventing and combating child sexual abuse, February 2023

Upcoming events

- 1 March, C-PROC/GEORGIA, Donor Coordination Meeting with Ministry of Internal Affairs *(in-person),* CyberEast
- 1 March, C-PROC, (*online*), Bureau meeting, T-CY
- 6 March, C-PROC/MOROCCO, *(in-person)*, Operational meeting Case Hilli, GLACY+
- 6-7 March, C-PROC/MOROCCO, *(in-person)*, Regional conference on international judicial cooperation on cybercrime and electronic evidence enhanced by the Second Additional Protocol, CyberSouth, GLACY+, Octopus
- 9-10 March, C-PROC/BENIN, *(in-person)*, Advisory mission on search, seizure, and confiscation of online proceeds of crime, GLACY+
- 9 March, C-PROC/PERU*, (hybrid),* Workshop for the Special Commission dealing with accession to international treaties - on SAP, GLACY+
- 13-14 March, C-PROC/ SENEGAL, *(in-person)*, Advisory mission on search, seizure, and confiscation of online proceeds of crime, GLACY+
- 13-17 March, C-PROC/ARMENIA, Advanced Judicial Training on Cybercrime and Electronic Evidence *(in-person*), CyberEast
- 14-15 March, C-PROC/MONTENEGRO, *(in-person*), Domestic simulation exercises on effective sharing of data between cybersecurity and cybercrime communities, iPROCEEDS-2
- March-April, C-PROC/EaP, Virtual meetings on implementation of Lanzarote and Istanbul Conventions (*on-line*), CyberEast
- Mid-March, C-PROC, (*online*), publication of additional resources on the cyberviolence portal, Octopus

www.coe.int/cybercrime