Cybercrime Digest

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

16 – 31 May 2022

Source: Council of Europe

Date: 20 May 2022

Ministers of Foreign Affairs call for signature and ratification of the e-evidence Protocol to the Budapest Convention

"The Ministers of Foreign Affairs of Council of Europe members meeting in Turin, Italy, on 20 May, inter alia called on all Parties to the Convention on Cybercrime to sign and ratify the new, Second Additional Protocol to this treaty. Andorra signed this instrument during the meeting to become the 23rd signatory State. Ministers also adopted Recommendation CM/Rec(2022)16 on combating hate speech. Ministers firmly condemned Russia's aggression against Ukraine and its violations of human rights and international law."

Source: European Data Protection Supervisor

Date: 20 May 2022

A new United Nations convention on cybercrime: fundamental rights come first

"The EDPS published on 18 May 2022 its Opinion concerning the EU's participation in the United Nations' negotiations for a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (the future UN convention on cybercrime). While reiterating support, in principle, to international cooperation in combatting cybercrime, the EDPS includes in its Opinion recommendations to ensure that the future UN convention upholds individuals' data protection and privacy rights according to EU law. The EDPS is concerned that, if not specifically addressed, the future UN convention risks weakening the protection of individuals' fundamental rights, including the rights to data protection and privacy guaranteed under EU law, given the large number of countries, which each have their own legal system, that are partaking in its negotiations. As such, the EDPS advises the EU not to become party to the future UN convention on cybercrime, if its final draft does not guarantee these fundamental rights." READ MORE

RELATED ARTICLE:

The record, EU data protection authority raises alarm over UN cybercrime treaty negotiations, 20 May 2022

Source: Council of Europe

Date: 12 May 2022

Government of Japan makes voluntary contribution to the Octopus Project

"The Government of Japan has made a voluntary contribution of EUR 45 000 to support the prevention of violence against women and the Council of Europe action against cybercrime through the Octopus Project. The agreement was signed on 16 May 2022 by Ambassador Takeshi Akamatsu, Permanent Observer of Japan to the Council of Europe, and Mr Bjørn Berge, Deputy Secretary General. Japan has been a Party to the Budapest Convention on Cybercrime since 2012, being one of the 66 countries worldwide to have joined the Convention on Cybercrime thus far." READ MORE

Source: Council of Europe

Date: 20 May 2022

Council of Europe proposes a comprehensive legal and policy framework to combat hate speech

"The Council of Europe has issued a set of guidelines to its 46 member states aimed at preventing and combating hate speech, both online and offline. In a Recommendation adopted during its annual session held in Turin, the Council of Europe Committee of Ministers calls on governments to develop comprehensive strategies to prevent and fight hate speech, including the adoption of an effective legal framework and implementing adequately calibrated and proportionate measures. When doing so, national authorities should carefully balance the right to private life, the right to freedom of expression and the prohibition of discrimination." READ MORE

Source: INTERPOL

Date: 25 May 2022

INTERPOL Secretary General: Online child sexual abuse at record levels

"The massive increase in online child sexual abuse and exploitation sparked by the COVID-19 pandemic continues unabated, INTERPOL Secretary General Jürgen Stock told the World Economic Forum in Davos. In a panel on cyber security, Secretary General Stock said reporting by private industry and public hotlines, in addition to law enforcement exchanges, has shown a consistently rising number of online child abuse images, with 2021 the worst year on record. The growth of Internet connectivity is set to see even greater numbers of children being abused and exploited online. […] Self-generated content, where a child victim is groomed and coerced into creating images and video of their abuse has grown significantly." READ MORE

RELATED ARTICLE:

Security Affairs, Nation-state malware could become a commodity on dark web soon, Interpol warns, 24 May 2022

Source: US Department of Justice

Date: 31 May 2022

WeLeakInfo.to and Related Domain Names Seized

"The FBI and the U.S. Department of Justice announced today that they have seized the internet domain name weleakinfo.to and two related domain names, ipstress.in and ovh-booter.com, following an international investigation into websites allowing users to buy access to stolen personal information or to perform attacks on victim networks. […] The WeLeakInfo.to website had claimed to provide its users a search engine to review and obtain the personal information illegally obtained in over 10,000 data breaches containing seven billion indexed records – including, for example, names, email addresses, usernames, phone numbers, and passwords for online accounts. The website sold subscriptions so that any user could access the results of these data breaches, with subscriptions providing unlimited searches and access during the subscription period (one day, one week, one month, three months, or lifetime)." READ MORE

Source: INTERPOL

Date: 30 May 2022

Online scamming fraud: three Nigerians arrested in INTERPOL Operation Killer Bee

"An INTERPOL-led operation targeting malware cyber fraud across Southeast Asia has led to the Nigeria arrest of three suspected global scammers. […] The Nigerian sting operation comes as part of a global operation codenamed "Killer Bee" involving INTERPOL's General Secretariat headquarters and National Central Bureaus (NCBs) and law enforcement agencies in 11 countries across Southeast Asia. […] Operational partners included Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Nigeria, Philippines, Singapore, Thailand and Vietnam." READ MORE

Source: BBC

Date: 20 May 2022

Cyber security: Global food supply chain at risk from malicious hackers

"Modern "smart" farm machinery is vulnerable to malicious hackers, leaving global supply chains exposed to risk, experts are warning. It is feared hackers could exploit flaws in agricultural hardware used to plant and harvest crops. Agricultural manufacturing giant John Deere says it is now working to fix any weak spots in its software. […] The UK government and the FBI have warned that the threat of cyber-attacks is growing." READ MORE

Source: Hack Read

Date: 23 May 2022

Anonymous Declares Cyber War Against Pro-Russia Hacker Group Killnet

"The Pro-Russia Hacker Group Killnet recently targeted European institutions, while Anonymous hackers are already claiming to have leaked the group's personal information in a database dump. The Anonymous hacktivists collective announced declaring cyberwar against pro-Russia hackers Killnet. The hacktivist group posted about this recent development on their Twitter handle, @YourAnonOne. The tweet read: "The #Anonymous collective is officially in cyberwar against the pro-Russian hacker group #Killnet." READ MORE

Source: US Department of Justice

Date: 19 May 2022

Department of Justice Announces New Policy for Charging Cases under the Computer Fraud and Abuse Act

"The Department of Justice today announced the revision of its policy regarding charging violations of the Computer Fraud and Abuse Act (CFAA). The policy for the first time directs that good-faith security research should not be charged. Good faith security research means accessing a computer solely for purposes of good-faith testing, investigation, and/or correction of a security flaw or vulnerability, where such activity is carried out in a manner designed to avoid any harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security or safety of the class of devices, machines, or online services to which the accessed computer belongs, or those who use such devices, machines, or online services. " READ MORE

Source: Council of Europe

Date: 23 May 2022

Council of Europe & IAP – 5th Webinar: Spotlight on data protection safeguards and principles in cross-border investigations

“The fifth webinar in the series dedicated to the Second Additional Protocol (SAP) to the Budapest Convention, jointly organised by the International Association of Prosecutors (IAP) and the Council of Europe through the GLACY+ and Octopus Projects, took place on 23 May 2022. This webinar was focused specifically on the new provisions regarding data protection safeguards set out in the 2nd Additional Protocol to the Budapest Convention. The experts provided insight, from both US and European perspective, on the new legal tools provided by the Protocol to ensure data protection is protected in cross-border investigations.” READ MORE

RELATED ARTICLE:

Techy New Zone, Council of Europe & IAP – fifth Webinar: Highlight on knowledge safety safeguards and rules in cross-border investigations, 30 May 2022

Source: Threat Post

Date: 26 May 2022

Cybergang Claims REvil is Back, Executes DDoS Attacks

“Actors claiming to be the defunct ransomware group are targeting one of Akami’s customers with a Layer 7 attack, demanding an extortion payment in Bitcoin. The defunct REvil ransomware gang is claiming responsibility for a recent distributed denial of service (DDoS) campaign against a hospitality customer of cloud networking provider Akamai. However, it’s highly possible the attack is not a resurgence of the infamous cybercriminal group but a copycat operations, researchers said.” READ MORE

RELATED ARTICLE:

Akamai, REvil Resurgence? Or a Copycat?, 25 May 2022

Source: Krebs on Security

Date: 31 May 2022

Costa Rica May Be Pawn in Conti Ransomware Group’s Bid to Rebrand, Evade Sanctions

“Costa Rica’s national health service was hacked sometime earlier this morning by a Russian ransomware group known as Hive. The intrusion comes just weeks after Costa Rican President Rodrigo Chaves declared a state of emergency in response to a data ransom attack from a different Russian ransomware gang — Conti. Ransomware experts say there is good reason to believe the same cybercriminals are behind both attacks, and that Hive has been helping Conti rebrand and evade international sanctions targeting extortion payouts to cybercriminals operating in Russia.” READ MORE

RELATED ARTICLES:

Reuters, Cyber attack on Costa Rica grows as more agencies hit, president says, 17 May 2022

Bleeping Computer, Conti ransomware shuts down operation, rebrands into smaller units, 19 May 2022

Source: Universidad de Chile, Facultad de Derecho

Date: 26 May 2022

Ciclo de charlas analiza nueva legislación en torno a los delitos informáticos

"El Centro de Estudios en Derecho Informático (CEDI) organizó una serie de conferencias que en esta oportunidad se centraron en los delitos informáticos, cuya regulación se encuentra próxima a convertirse en ley, después de varios años en discusión parlamentaria. […] La segunda conferencia abordó algunos aspectos problemáticos de la nueva regulación que recogió en gran medida el texto del Convenio de Budapest, pero que innovó en ciertas materias como el hacking ético, el que fue finalmente penalizado en nuestra legislación. En esta sesión se contó con las exposiciones de Verónica Rosenblut, profesora de Derecho Penal de la Pontificia U. Católica de Chile, y de Alejando Hevia, profesor del Departamento de Ciencias de la Computación de la U. de Chile." READ MORE

Source: We are tech Africa

Date: 26 May 2022

Le Cameroun adhère à la convention de Budapest sur la cybercriminalité et renforce son dispositif de lutte

"Le président de la République du Cameroun Paul Biya a signé, lundi 23 mai, un décret autorisant l'adhésion du Cameroun à la Convention de Budapest (Hongrie) sur la cybercriminalité. Ce traité international rédigé par le Conseil de l'Europe, signé en novembre 2001 et entré en vigueur le 1er juillet 2004, est consacré à la lutte contre les crimes informatiques et les crimes sur Internet, y compris la pornographie infantile, l'atteinte au droit d'auteur et le discours de haine." READ MORE

Source: Council of Europe

Date: 23 - 26 May 2022

Moroccan magistrates acquire new training skills on cybercrime and electronic evidence

"On 23 May 2022 the Council of Europe Office in Rabat and the Cybercrime Programme Office of the Council of Europe (C-PROC), in co-operation with the Public Prosecution Office and the High Judicial Council of Morocco opened the training course Judicial Training of Trainers (ToT) on cybercrime and electronic evidence for magistrates in Rabat. The four-day course focuses on training methodology and role of trainer, with the aim to facilitate the establishment of a pool of national trainers who can further deliver in-country judicial training courses on cybercrime and e-evidence to their peers." READ MORE

Source: We are tech Africa

Date: 24 May 2022

Le Niger ratifie la convention de l'Union africaine sur la cybersécurité et la protection des données personnelles

"L'Assemblée Nationale de la République du Niger a entériné une série de projets de lois de ratification lundi 23 mai. Réunis en séance plénière, les députés ont donné leur accord pour la ratification entre autres de la Convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel adoptée le 27 Juin 2014 à Malabo (Guinée Equatoriale)." READ MORE

Source: INTERPOL

Date: 25 May 2022

Suspected head of cybercrime gang arrested in Nigeria

"The cybercrime unit of the Nigeria Police Force arrested a 37-year-old Nigerian man in an international operation spanning four continents, coordinated and facilitated by the recently created Africa operations desk within INTERPOL's cybercrime directorate. The suspect is alleged to have run a transnational cybercrime syndicate that launched mass phishing campaigns and business email compromise schemes targeting companies and individual victims. Law enforcement and cybersecurity firms have witnessed the striking increase in many forms of cybercrime in recent years, exploiting the context of COVID-19 and forming what INTERPOL Secretary General Jürgen Stock has called a "parallel pandemic"." READ MORE

RELATED ARTICLES:

Security Affairs, International police operation led to the arrest of the SilverTerrier gang leader, 25 May 2022

Homeland Security, Suspected Head of Transnational Cybercrime Gang Arrested in Nigeria, 27 May 2022

Source: SN Radio

Date: 25 May 2022

Sierra Leone: Judicial Training on Cybercrime and Collecting of Electronic Evidence Commence

"The Judiciary of Sierra Leone through the Judicial and Legal Training Institute (JLTI) in Collaboration with the National Cyber Security Coordination Centre and the OCWAR-Project have commenced a 4-day Judicial Training on Cybercrime and Collecting of Electronic Evidence for 20 Judges of the Superior Court of Judicature. […] "We have no doubt that we will forge ahead with one direction,…we will broaden our ambition and be smarter, more innovative and be more empowered than the rogues in the Cyber space," Deputy Minister of Information and Communications affirmed." READ MORE

Source: Times Now

Date: 18 May 2022

Syria's cybercrime law is another way for Assad to rule by fear

"After months of rumors, the Syrian regime recently passed far-reaching cybercrime legislation that goes beyond what is necessary to keep the internet safe. Despite tackling issues like cyberbullying and fraud, the most serious legal and financial penalties introduced by the new legislation are reserved for those who criticise the president, the Constitution, or the state. […] Al Assad approved Law No 20 on April 18, updating an existing law from 2012 that defined terms and conditions of using the internet, as well as punishments for internet-related crimes. Starting this month, network service providers and users in Syria will face penalties of up to 15 years in prison and fines of 15 million Syrian pounds ($5,530) for running afoul of the new measures." READ MORE

Source: Council of Europe

Date: 18 May 2022

GLACY+: Support for data protection legislation in Vanuatu – Workshop for drafting the Data Protection and Privacy Bill

"As a continuation of the support provided by the Council of Europe to the Vanuatuan authorities, the fourth workshop on developing data protection legislation for Vanuatu was organised on 18 May 2022 by the GLACY+ project, in conjunction with the Council of Europe's Data Protection Unit. The workshop focused on the finalisation of the draft Data Protection and Privacy Policy, before the first discussion on the draft text of the Data Protection and Privacy Bill took place. Both the draft Policy and the draft Bill have been prepared with support from the Council of Europe." READ MORE

Source: The Sydney Morning Herald

Date: 29 May 2022

More than 100 ADF personnel to be sent to PNG to help with election, cyber threats

"More than 100 Australian Defence Force personnel will travel to Papua New Guinea in coming months to help the country conduct its national election, combat cyber threats and conduct joint exercises amid a growing tussle for influence between Australia and China in the region. A Defence spokesperson said Australia would support the PNG election at the request of its government. This support will include air force, army and cyber personnel to help PNG with logistics and planning, including air lifts to help in distributing and collecting votes." READ MORE

Source: The Hill

Date: 31 May 2022

Ukraine joins its first NATO cyber defense center meeting

"Ukrainian officials met for the first time on Monday with the steering committee of the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) in Tallinn, Estonia, following the country's successful bid to join the cyber center. Ukraine first applied to join the organization in August 2021. Its application was unanimously approved by all members of the steering committee in March. According to a blog post released by Ukraine's National Security and Defense Council, members of the committee are finalizing a technical agreement on the accession that will formalize Ukraine's participation in the organization." READ MORE

Source: Mondaq

Date: 23 May 2022

Uzbekistan: Uzbekistan Adopts Cybersecurity Law

"The Law of the Republic of Uzbekistan "On Cybersecurity" No. ???-764 dated April 15, 2022 (the "Cybersecurity Law") will enter into force on July 17, 2022. The Cybersecurity Law consists of 40 articles and is intended to regulate relations in the field of cybersecurity. The Cybersecurity Law defines such concepts as cybercrime, cyberspace, cyber threat, cybersecurity, cyber defense, cyberattack, critical information infrastructure." READ MORE

Source: Council of Europe

Date: 16 - 20 May 2022

Turkish Judges and Prosecutors exchanged with their peers during the Study Visit to Paris and the Council of Europe

"During the period between 16 and 20 May 2022, representatives of the Turkish Ministry of Justice and judges and prosecutors attended a tailored programme on combatting cybercrime in France. In the first part of the visit in Paris, the Turkish Delegation visited French institutions (both judicial and law-enforcement institutions) such as Cybercrimes Section of Judicial Court of Paris (J3), Cyberspace Gendarmerie Command (COMCYBERGEND), Central Office for Combating Crime Linked to Information and Communication Technologies of French Police Department and Directorate of Criminal Affairs and Pardons of French Ministry of Justice." READ MORE

Source: Malware Bytes

Date: 16 May 2022

Custom PowerShell RAT targets Germans seeking information about the Ukraine crisis

"Populations around the world—and in Europe in particular—are following the crisis in Ukraine very closely, and with events unfolding on a daily basis, people are hungry for information. […] This week our analysts discovered a new campaign that plays on these concerns by trying to lure Germans with a promise of updates on the current threat situation in Ukraine. The downloaded document is in fact decoy for a Remote Access Trojan (RAT) capable of stealing data and executing other malicious commands on a victim's computer. Threat actors registered an expired German domain name at collaboration-bw[.]de that was formally used as a collaboration platform to develop new ideas for the Baden-Württemberg state." READ MORE

Source: BBC

Date: 17 May 2022

UK: New app to help spot online spies

"A new app has been launched by the UK government to prevent people falling victim to online approaches by foreign spies. MI5 says it has seen 10,000 UK nationals targeted by fake social media profiles on sites like LinkedIn and Facebook. The spies are seeking to lure people into passing on sensitive information. The Think Before You Link app will help people spot suspicious approaches. Spies have long approached people with access to sensitive information, but the online world has allowed this to happen at huge scale and at distance." READ MORE

Source: Reuters

Date: 15 May 2022

Italy prevents pro-Russian hacker attacks during Eurovision contest

"Italian police thwarted hacker attacks by pro-Russian groups during the May 10 semi-final and Saturday final of the Eurovision Song Contest in Turin, authorities said on Sunday. […]During voting and the performances, the police cybersecurity department blocked several cyber attacks on network infrastructure by the "Killnet" hacker group and its affiliate "Legion", police said. The police also gathered information from the pro-Russian group's Telegram channels to prevent other critical events and identified the attacks' geographic location." READ MORE

Source: Gov Info Security

Date: 23 May 2022

Cyberattack Affects Greenland's Healthcare Services

“Greenland's healthcare services have been "severely limited" due to a cyberattack that has lasted for at least two weeks to date, says the Naalakkersuisut, the country's government. All IT systems and servers associated with the healthcare services of the country were forced to restart due to the cyberattack, cutting off access to patient records. The attack, the government says, has also affected the healthcare service's email system. "The health services are therefore severely limited and increased waiting time must be expected," the government says. Some people may experience a delay in agreed schedules, but "acute inquiries will of course continue to be met and you can contact the health service by phone." READ MORE

Latest reports

- Africa News, Africa: Can a strong cybersecurity strategy be an engine for growth?, 16 May 2022
- Prodaft, Wizard Spider Group In-Depth Analysis, 16 May 2022
- Bleeping Computer, Third-party web trackers log what you type before submitting, 16 May 2022
- Security Week, Hackers Can Abuse Low-Power Mode to Run Malware on Powered-Off iPhones, 16 May 2022
- CISA, Joint Cybersecurity Advisory on Weak Security Controls and Practices Routinely Exploited for Initial Access, 17 May 2022
- Malware Bytes Lab, Long lost @ symbol gets new life obscuring malicious URLs, 17 May 2022
- KrebsonSecurity, When Your Smart ID Card Reader Comes With Malware, 17 May 2022
- Wiley Online Library, e-Evidence Cooperation in Criminal Matters from an EU Perspective, 18 May 2022
- MITECHNEWS, What Are The Biggest Cybersecurity Threats For The Coming Years In Australia?, 18 May 2022
- Sentinel Labs, CrateDepression | Rust Supply-Chain Attack Infects Cloud CI Pipelines with Go Malware, 19 May 2022
- Observatorio español de Delitos Informáticos: Estudio sobre la Violencia de Genero Digital, 21 May 2022
- Microsoft, Beneath the surface: Uncovering the shift in web skimming, 23 May 2022
- Verizon: 2022 Data Breach Investigations Report, 24 May 2022
- Europol, Misleading invoice fraud targeting the owners of intellectual property rights- crime situation 2021, 24 May 2022
- Europol, Online Jihadist Propaganda - 2021 in review, 24 May 2022
- Help Net Security, Vishing cases reach all time high, 24 May 2022
- SoK (APWG, EUROJUST), Cross-border Criminal Investigations and Digital Evidence, 25 May 2022
- FBI, Compromised US Academic Credentials Identified Across Various Public and Dark Web Forums, 26 May 2022
- D.business: Report: Identity Attacks a Top Cybersecurity Threat in 2022, 26 May 2022
- Techxplore, Paper reveals a quarter of the world's internet users rely on infrastructure that is susceptible to attacks, 26 May 2022
- RFI, Afrique: le défi de la cybersécurité, 27 May 2022
- IT Brief Australia, 4/10 Australian SMEs fallen victim to cyber-attacks since pandemic, 27 May 2022

Upcoming events

- 30 May–3 June, C-PROC/CEPOL, (*online*), CEPOL, Cross-border exchange of Electronic Evidence, OCTOPUS
- 30 May-10 June, C-PROC/AUSTRIA, *(hybrid),* UN Ad Hoc Committee 2nd meeting on new UN Treaty, GLACY+, iPROCEEDS-2, CyberSouth, OCTOPUS31 May-2 June, C-PROC/FRANCE, *(in-person),* EuroMed Justice Programme Conference on e-evidence and data protection in criminal matters in the Euro-Mediterranean Region 2022, CyberSouth
- 1 June, C-PROC/TUNIS, *(in-person),* Conference on data protection: "La protection des données personnelles, une opportunité et un impératif pour la région", CyberSouth, GLACY+
- 2 June, C-PROC , *(online),* First Coordination Call of the Steering Committee of the International Network of Judicial Trainers, GLACY+
- 2 June, C-PROC/UKRAINE, *(online)*, Roundtable Discussion on admissibility of electronic evidence for Prosecutor's Office, CyberEast
- 6-7 June, C-PROC/BRAZIL, *(online),* Series of webinars on Budapest Convention and cybercrime legislation, GLACY+
- 6-8 June, C-PROC/MOLDOVA, *(online)*, Law enforcement training for investigators (Intermediate level), CyberEast
- 8 June, C-PROC, *(online),* Euromed Police Steering Committee Meeting, CyberSouth
- 10 June, C-PROC, *(online)*, CyberEast Steering Committee meeting, CyberEast
- 14 June, T-CY, *(online),* Meeting of the Working Group on undercover investigations and extension of searches, T-CY
- 14-17 June, C-PROC/PARAGUAY, *(in-person),* Introductory Training on Cybercrime and electronic evidence for judges, magistrates and prosecutors, GLACY+
- 14-16 June, C-PROC/CHILE, *(in-person),* Advisory mission on search, seizure, and confiscation of online proceeds of crime, GLACY+
- 14-16 June, C-PROC/CHILE, *(in-person),* Development of Cybercrime investigations, digital forensics capabilities combined with in-country workshops and advice on interagency cooperation and private public partnerships to fight cybercrime, GLACY+
- 14-16 June, C-PROC/CZECH REPUBLIC, *(in-person),* ISS World Europe 2022, participation of Bosnia and Herzegovina authorities, iPROCEEDS-2
- 15 June , C-PROC, *(online),* Series of monthly thematic webinars for the International Network of the National Judicial Trainers, GLACY+
- 15 June, C-PROC/BOSNIA AND HERZEGOVINA, *(in-person,* Domestic meeting to support public/private initiatives on cooperation between service providers and criminal justice authorities, iPROCEEDS-2
- 15 June, C-PROC/KOSOVO*, *(in-person),* Domestic meeting to support public/private initiatives on cooperation between service providers and criminal justice authorities, iPROCEEDS-2

- 15-17 June, C-PROC/TURKEY, *(in-person)*, Training skill certification programme for judges and prosecutors delivering Council of Europe judicial training on cybercrime and electronic evidence, iPROCEEDS-22
- June, C-PROC/ARMENIA, *(online),* Expert review of the new Code of Criminal Procedure - compliance with the Convention, CyberEast

The Cybercrime Digest appears bi-weekly. The news is selected by relevance to the current areas of interest to C-PROC and does not represent official positions of the Council of Europe. You receive this digest as you have taken part in Council of Europe activities on cybercrime. It is not intended for general publication.

For any additional information, contributions, subscriptions or removal from this distribution list, please contact: cybercrime@coe.int

www.coe.int/cybercrime

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE