Cybercrime Digest

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

1 – 15 July 2022

Source: European Parliament

Date: 5 July 2022

Digital Services: landmark rules adopted for a safer, open online environment

"On Tuesday, Parliament held the final vote on the new Digital Services Act (DSA) and Digital Markets Act (DMA), following a deal reached between Parliament and Council on 23 April and 24 March respectively. The two bills aim to address the societal and economic effects of the tech industry by setting clear standards for how they operate and provide services in the EU, in line with the EU's fundamental rights and values. The Digital Services Act was adopted with 539 votes in favour, 54 votes against and 30 abstentions. The Digital Markets Act - with 588 in favour, 11 votes against and 31 abstentions." READ MORE

RELATED ARTICLES:

Ecommerce Europe, European Parliament's plenary adopts the Digital Services Act and Digital Markets Act, 7 July 2022

European Parliament, Digital Services Act: agreement for a transparent and safe online environment, 23 April 2022

European Parliament, Deal on Digital Markets Act: EU rules to ensure fair competition and more choice for users, 24 March 2022

Source: NATO

Date: 14 July 2022

NATO and the European Union work together to counter cyber threats

"Following the NATO Summit in Madrid last month, senior officials from NATO and the European Union (EU) met on 14 July 2022 to take stock of recent developments in the cyber threat landscape and explore further areas of engagement on cyber defence. Officials discussed recent policy developments, including the new NATO Strategic Concept and the EU's Strategic Compass. The discussions focused on the evolving cyber threat landscape, including in the context of Russia's war of aggression against Ukraine, as well as respective efforts to enhance cyber resilience and assistance." READ MORE

Source: State Watch

Date: 6 July 2022

EU: End game approaching for e-evidence negotiations, says French Presidency

"Negotiations on the EU's controversial "e-evidence" proposals may be coming to a close soon, according to a note circulated by the French Presidency of the Council on 16 June. The proposals, which aim to ease cross-border requests for and exchange of electronic data for use in criminal cases, are made up of two new laws – a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, and a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings." READ MORE

Source: Council of Europe

Date: 13 July 2022

GLACY+: Reviewing project progress and planning activities during the project's 12th Steering Committee meeting

"On 13 July 2022, the Council of Europe together with the European Union and INTERPOL, hosted the 12th meeting of the GLACY+ Steering Committee to discuss developments in priority countries, review GLACY+ project activities held in the first half of 2022 and shape future project activities. During the meeting, the project team, GLACY+ priority and hub countries and project partners actively engaged in a review of the key activities delivered in the first half of 2022, including support to strengthen national legislation, strategies and policies on cybercrime and electronic evidence in line with international standards. Representatives of GLACY+ priority and hub countries shared key national developments also supported by the project and further indicated their priorities for activities to take place in the second half of 2022." READ MORE

Source: CISA

Date: 6 July 2022

CISA, FBI and Treasury release advisory on North Korean state-sponsored cyber actors use of MAUI ransomware

"The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the U.S. Department of the Treasury today released a joint Cybersecurity Advisory (CSA) that provides information on Maui ransomware, which has been used by North Korean state-sponsored cyber actors since at least May 2021 to target Healthcare and Public Health (HPH) Sector organizations. The CSA […] provides technical details and indicators of compromise observed during multiple FBI incident response activities over a period of more than a year and obtained from industry analysis of Maui samples. North Korean state-sponsored actors were observed using Maui ransomware to encrypt HPH servers responsible for providing healthcare services. In some cases, the malicious activity disrupted the services provided by the victim for prolonged periods." READ MORE

RELATED ARTICLES:

CSA, North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector, 6 July 2022

The Guardian, 'Lives are at stake': hacking of US hospitals highlights deadly risk of ransomware, 14 July

Microsoft, North Korean threat actor targets small and midsize businesses with H0lyGh0st ransomware, 14 July 2022

Source: Forbes

Date: 7 July 2022

Apple Offers $2M To Hackers Who Can Break Its New Lockdown Mode

"Apple announced a new Lockdown Mode today which will be available in iOS 16, scheduled to launch later this year. Lockdown mode is intended for those who are high-value targets for hacking and makes iPhone one of the most secure phones available. To ensure it stays that way, Apple is offering up to $2,000,000 prizes for hackers who can find Lockdown Mode bypasses and break in." READ MORE

RELATED ARTICLE:

BBC, Apple launches Lockdown Mode to block spyware attacks on at-risk users, 6 July 2022

Source: Council of Europe

Date: 12 July 2022

Kick-off meeting of the Ad Hoc Working Group on judicial training strategies on cybercrime and electronic evidence

"The Ad Hoc Working Group on judicial training strategies on cybercrime and electronic evidence established under the umbrella of the International Network of National Judicial Trainers on cybercrime reunited online on 12 July for the kick-off meeting on the preparation of a guidebook on judicial training strategies on cybercrime and electronic evidence. The members exchanged views on the principles of judicial training strategies to be considered for the elaboration of the future guidebook and shared their national perspectives on this matter." READ MORE

Source: EUROJUST

Date: 7 July 2022

Closer stakeholder cooperation essential for ransomware investigations to succeed

"The scale and impact of ransomware attacks have increased significantly over the past years, in part due to the COVID-19 pandemic. As such, the success of criminal investigations and prosecutions depends more than ever on close cross-border cooperation between public authorities, private companies and victims. Public-private cooperation is particularly valuable in such cases, as companies can preserve and provide the data and evidence investigators need to investigate crimes and identify criminals. […] This includes the reporting of ransomware attacks by victims, the preservation and possible analysis of digital evidence by private companies, and the investigation and prosecution by public authorities. The international dimension of investigations and the complexity of identifying criminals require early and close cross-border coordination between judicial and law enforcement authorities. Actions by each stakeholder group play a key role in the mitigation of damages, disruption of attacks and the identification and prosecution of perpetrators." READ MORE

Source: ENISA

Date: 6 July 2022

How to map the Cybersecurity Threat Landscape?

“With a cyber threat landscape in constant evolution, the need for updated and accurate information on the current situation is growing and this a key element for assessing relevant risks. This is why ENISA releases today an open and transparent framework to support the development of threat landscapes. The ENISA methodology aims to provide a baseline for the transparent and systematic delivery of horizontal, thematic and sectorial cybersecurity threat landscapes (CTL) thanks to a systematic and transparent process for data collection and analysis.” READ MORE

RELATED REPORT:

ENISA, Threat Landscape Methodology, 6 July 2022

Source: Tripwire

Date: 14 July 2022

10,000 organisations targeted by phishing attack that bypasses multi-factor authentication

“Microsoft has shared details of a widespread phishing campaign that not only attempted to steal the passwords of targeted organisations, but was also capable of circumventing multi-factor authentication (MFA) defences. The attackers used Attacker-in-The-Middle reverse-proxy sites to pose as Office 365 login pages which requested MFA codes, and then use them to log into the genuine site. According to Microsoft’s detailed report on the campaign, once hackers had broken into email inboxes via the use of stolen passwords and session cookies, they would exploit their access to launch Business Email Compromise attacks on other targets. By creating rules on victims’ email accounts, the attackers are able to then ensure that they are able to maintain access to incoming email even if a victim later changes their password.” READ MORE

Source: The Guardian

Date: 7 July 2022

FBI and MI5 leaders give unprecedented joint warning on Chinese spying

“The head of the FBI and the leader of Britain’s domestic intelligence agency have delivered an unprecedented joint address raising fresh alarm about the Chinese government, warning business leaders that Beijing is determined to steal their technology for competitive gain. In a speech at MI5’s London headquarters intended as a show of western solidarity, Christopher Wray, the FBI director, […] reaffirmed longstanding concerns about economic espionage and hacking operations by China, as well as the Chinese government’s efforts to stifle dissent abroad. “We consistently see that it’s the Chinese government that poses the biggest long-term threat to our economic and national security, and by ‘our’, I mean both of our nations, along with our allies in Europe and elsewhere,” Wray said. He told the audience the Chinese government was “set on stealing your technology, whatever it is that makes your industry tick, and using it to undercut your business and dominate your market”.” READ MORE

RELATED ARTICLE:

FBI, FBI Director Concludes Meetings with U.K. Partners, 9 July 2022

Source: AS/COA

Date: 13 July 2022

LatAm in Focus: Cyber Attacks in Costa Rica Expose a Regional Threat

"A series of hacks pummeled Costa Rica. Cybersecurity expert Belisario Contreras covers what it showed about the region's digital vulnerabilities. They called it "El Hackeo." Starting April 17, Costa Rica was the victim of a massive cyberattack that lasted over two months. The attack, perpetrated mainly by the pro-Russia Conti criminal gang, paralyzed all kinds of operations in the country, with over 30 ministries targeted. Government employees couldn't get paid. Trade halted. Thousands of doctors' appointments were cancelled. Conti initially asked for a ransom of $10 million. Costa Rica refused to pay and the attacks ended up costing the country roughly $30 million a day." READ MORE

Source: The Hill

Date: 7 July 2022

Experts say US must not let EU lead on cybersecurity

"Cybersecurity experts argued on Tuesday that the U.S. is falling behind the European Union when it comes to being a leader in the realm of cyber security. Experts called the bloc's General Data Protection Regulation, a law governing data privacy and security rules, the global standard. The law, adopted in 2018, renewed how businesses handle personal data in Europe, with large fines for companies that fail to comply." READ MORE

Source: La Tribuna

Date: 13 Julio 2022

Acusan falta de legislación frente a delitos informáticos como el robo de redes sociales

"Países de Europa han avanzado hacia la formación del derecho a la protección de datos almacenados en servicios de comunicación, que de ser aplicados en Chile ayudarían a toda la población. La ley chilena no persigue legalmente robos o fraudes cometidos en contra de cuentas de redes sociales, frente a lo cual autoridades y fiscalizadores en la materia se han visto sobrepasados por una falta de actualización de los protocolos y las penas por este tipo de delitos. […] Francisco Javier Parada Barriga explicó que existe una ley 'que establece las normas del delito informático y modifica otros cuerpos legales donde no se habla de redes sociales en sí, y ahí es donde está el vacío, porque Carabineros y la Fiscalía no reconocen a las redes sociales como un ente informático de una persona individual. En Chile nos regimos bajo el Convenio de Budapest, donde las naciones que están adscritas a él tienen un convenio sobre cómo utilizar la legislación del país para combatir el cibercrimen.'" READ MORE

Source: JDSUPRA

Date: 8 July 2022

DOJ’s Public Struggles with Electronic Evidence Underscore the Need for Counsel to Demand Discovery Early and Often

“The U.S. Department of Justice’s (DOJ) dismissal last week in a Foreign Corrupt Practices Act case in Boston is the latest in a string of bad outcomes for the government due to discovery mishaps. While the government works to revise its discovery policies and seeks resources to collect, review, and analyse the vast amount of electronic evidence attendant to nearly every federal criminal investigation, defence counsel should hold the government to account and formally demand discovery early and often.” READ MORE

Source: Andina

Date: 7 July 2022

Conoce cómo trabajan los fiscales peruanos que investigan delitos de ciberdelincuencia

“Además de una mayor adopción de medios digitales, la pandemia también evidenció un incremento de las denuncias de delitos informáticos en el Perú. A escala nacional, entre enero y abril de 2022, el Ministerio Público ha recibido 7,297 denuncias que son investigadas por los fiscales peruanos, quienes recurren al uso de mecanismos tecnológicos para rastrear las evidencias digitales. Para facilitar su labor en 34 distritos fiscales, a inicios de 2021 se creó la Unidad Fiscal Especializada en Ciberdelincuencia, que realiza el acompañamiento técnico de los fiscales a través del uso de recursos tecnológicos.” READ MORE

Source: KBS World

Date: 13 July 2022

Yoon Pledges to Nurture Cybersecurity Workforce

“President Yoon Suk Yeol has vowed to strengthen Korea's cyber response capabilities based on close cooperation between the public and private sectors, saying that cybersecurity comprises one of the key elements of national security. […] Yoon also expressed the government’s commitment to international cooperation in cybersecurity by pledging to promptly join the Budapest Convention, an international treaty dedicated to addressing cybercrime.” READ MORE

Source: The Guardian

Date: 11 July 2022

SMS scams: mobile companies could face fines of up to $250,000 under new Australian code

“Mobile phone companies could face up to $250,000 in fines for failing to comply with a new code to block SMS scam messages. The code, registered by the Australian Communications and Media Authority (Acma) on Tuesday, will require the companies to trace, identify and block SMS scam messages, and publish information for customers on how to identify and report scams. The companies will also be required to share information about scams between each other and authorities. According to Australian Competition and Consumer Commission (ACCC) data, SMS scams accounted for 32% of all reported scams this year to date, accounting for $6.5m in losses compared to $2.3m in the same period last year.” READ MORE

Source: Council of Europe

Date: 28-29 June 2022

Fiji becomes the 18th priority country of GLACY+ project: initial assessment of criminal justice capacities on cybercrime and e-evidence concluded

"On 28-29 June 2022, the GLACY+ Project, a joint action of the European Union and the Council of Europe, together with its implementing partner INTERPOL and Octopus project, in cooperation with the Ministry of Communications in Fiji organized a two-day workshop with the scope of identifying the capacity building needs in Fiji, in view of its inclusion among the priority countries of the GLACY+ project for further cybercrime capacity-building support. The team of international experts engaged with the representatives of the national authorities and private sector dealing with cybercrime-related matters on specific challenges and capacity needs with the aim to acquire a general outlook of the national capacities in dealing with cybercrime and cases involving electronic evidence. Conclusions and recommendations will integrate the identified country's needs in terms of training and institutional developments that will serve as a baseline for further project support." READ MORE

Source: The Guardian

Date: 8 July 2022

Philippines' Nobel laureate Maria Ressa loses appeal against cyber libel conviction

"The Filipino Nobel peace prize winner Maria Ressa has lost her appeal against a conviction for cyber libel, her news website, Rappler, has said, in the latest blow for the veteran journalist. Ressa and her former colleague Rey Santos Jr face lengthy jail sentences, but the company said they would "avail of all legal remedies available to them", including taking the case to the supreme court. The ruling comes less than two weeks after the Philippine authorities ordered Rappler to shut down ahead of the former president Rodrigo Duterte's last day in office." READ MORE

Source: Business Standard

Date: 9 July 2022

India becomes 68th country to join Interpol's child sexual abuse database

"India on Friday joined the Interpol's international child sexual exploitation (ICSE) database which will allow it to draw links between victims, abusers and crime scene using audio-visual data. The CBI, which is India's nodal agency for Interpol matters, joined the database making India the 68th country to connect to it, according to a statement from the Interpol." READ MORE

Source: Council of Europe

Date: 23-30 June 2022

GLACY+ and Octopus: Stakeholder series of workshops on new national cybercrime legislation concluded in Fiji

"On 23-30 June 2022, the GLACY+ Project, a joint action of the European Union and the Council of Europe, together with Octopus project, in cooperation with the Ministry of Communications in Fiji organised a series of four workshops on the new national cybercrime legislation targeting judiciary, law enforcement agencies (LEA), financial investigators, prosecutors and service providers. The series was opened by the Ambassador of the European Union to Fiji and the Pacific, His Excellency Sujiro Seam, who welcomed the adoption of the new legal framework and emphasised the importance of international cooperation on cybercrime and electronic evidence." READ MORE

Source: The Phnom Penh Post

Date: 5 July 2022

Cambodia: Authorities seek to address online child sex abuse

"According to statistics from the US-based National Centre for Missing and Exploited Children (NCMEC), the number of reported cases of child sexual abuse on the internet had increased by 35 per cent in 2021 from 2020 or a jump from around 20 million up to 29 million reported cases. According to statistics from the Cambodian Ministry of Posts and Telecommunications, about 400,000 cases were reported in Cambodia for 2021, which is more than double the number reported in 2020." READ MORE

Source: BBC

Date: 8 July 2022

Security warning after sale of stolen Chinese data

"President Xi Jinping has urged public bodies to "defend information security" after a hacker offered to sell stolen data of one billion Chinese citizens. In an advert on a criminal forum, later removed, the user said the data was stolen from Shanghai National Police. The hacker claims the information includes names, addresses, National ID numbers and mobile phone numbers. Cyber-security experts have verified that at least some of a small sample of the data offered is real. The 23 terabytes of data is thought to be the largest ever sale of data on record and was being offered for $200,000 (£166,000) until the post was removed on Friday." READ MORE

RELATED ARTICLE:

The Register, Billion-record stolen Chinese database for sale on breach forum, 5 July 2022

Source: OSIRIS

Date: July 2022

La Tunisie déploie l'identité numérique mobile

"Le ministère des Technologies de la Communication a signé, vendredi 1er juillet, un accord de partenariat avec l'Agence nationale de certification électronique et les opérateurs télécoms pour la mise en œuvre de l'identité numérique mobile « mobile ID ». Ce projet naissant permettra d'associer le numéro de carte d'identité nationale des citoyens à leur numéro de téléphone." READ MORE

Source: CEPOL

Date: 14 July 2022

WB PaCT and iPROCEEDS-2 projects deliver training on cyber-attacks to Western Balkans beneficiaries

"The CEPOL WB PaCT project, in partnership with iPROCEEDS-2, the joint project of the European Union and the Council of Europe, organised an on-site training course on interagency and international cooperation on cyber-attacks to enhance the knowledge of the beneficiaries from the Western Balkans. The activity took place on 4-8 July in Bucharest, Romania. The course benefited from the participation of a large community of 32 law enforcement officials, prosecutors, investigators from the police, border police, customs officers and members of the Computer Emergency Response Teams fighting cyber-attacks and cybercrime from Albania, Bosnia and Herzegovina, Kosovo*, Montenegro, North Macedonia, Serbia and Turkey." READ MORE

RELATED ARTICLE:

Council of Europe, Workshop on Interagency and International Cooperation on Cyberattacks delivered in partnership with CEPOL for the South East region and Türkiye authorities, 4-8 July 2022

Source: UK Gov

Date: 6 July 2022

New measures will go further in tackling child sexual abuse online than ever before

"Greater powers to tackle child sexual abuse online will be introduced through an amendment to the Online Safety Bill, the Home Secretary announced today. The amendment will give Ofcom extra tools to ensure technology companies take action to prevent, identify and remove harmful child sexual abuse and exploitation (CSAE) content. Ofcom, the UK's regulatory authority for telecommunications, will be able to demand that technology companies such as social media platforms roll out or develop new technologies to better detect and tackle harmful content on their platforms. If they fail to do so, Ofcom will be able to impose fines of up to £18 million or 10% of the company's global annual turnover, depending on which is higher." READ MORE

Source: The Hacker News

Date: 4 July 2022

Ukrainian Authorities Arrested Phishing Gang That Stole 100 Million UAH

"The Cyber Police of Ukraine last week disclosed that it apprehended nine members of a criminal gang that embezzled 100 million hryvnias via hundreds of phishing sites that claimed to offer financial assistance to Ukrainian citizens as part of a campaign aimed at capitalizing on the ongoing conflict. "Criminals created more than 400 phishing links to obtain bank card data of citizens and appropriate money from their accounts," the agency said in a press statement last week. "The perpetrators may face up to 15 years behind bars." The law enforcement operation culminated in the seizure of computer equipment, mobile phones, bank cards as well as the criminal proceeds illicitly obtained through the scheme." READ MORE

Source: Council of Europe

Date: 12-14 July 2022

Another Specialised Judicial ToT delivered for Serbian prosecutors

"During 12 – 14 July 2022 the iPROCEEDS-2 project, a joint project of the European Union and the Council of Europe has delivered another Specialised Judicial Training of Trainers on Training Skills, this time for Serbian prosecutors, in Belgrade, Serbia. A cohort of 17 prosecutors delegates took part in this training with the aim to ensure that training can effectively contribute to increasing their capacities in relation to cybercrime, as well as on training methodology, by following a didactic-style teaching and training. The goal was to ensure that trainings implemented at national level are in line with the principles of adult education, and sufficiently hands-on to be able to address not only knowledge but also the skills and practical competences of participants, using a variety of different methods that will also make them able to trigger interests amongst members of the judiciary." READ MORE

Source: UK Parliament

Date: 13 July 2022

Treasury Committee launches inquiry into crypto assets

"The Treasury Committee today calls for written evidence as it launches a new inquiry into crypto assets. In the inquiry, the Committee will explore the role of crypto assets in the UK, as well as the opportunities and risks they bring to consumers and businesses. The Committee requests written evidence submissions which examine whether crypto currencies are likely to replace traditional currencies, what opportunities and risks the use of crypto assets pose for individuals and the economy, and their impact on social inclusion. MPs will also explore how regulation could be balanced to provide protection for consumers without stifling innovation." READ MORE

Source: AP News

Date: 6 July 2022

Polish PM claims Russia hacked, tweaked, leaked govt emails

"Poland's prime minister on Wednesday accused Russian agencies of hacking into government systems and manipulating and leaking emails that allegedly expose his administration's links with the judiciary. Premier Mateusz Morawiecki labelled the leaks a "provocation" by Russian and Belarusian secret services aiming to sow discord in Poland in revenge for Warsaw's support for Ukraine amid Russia's invasion." READ MORE

Latest reports

- Academic Health Science Networks, ‘How to involve and engage patients in digital health tech innovation – An Evidence Based Guide’, June 2022
- InfoSec Insider, A Guide to Surviving a Ransomware Attack, 30 June 2022
- Techtarget, Ransomware in 2022: Evolving threats, slow progress, 5 July 2022
- ENISA, Threat Landscape Methodology, 6 July 2022
- CSA, North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector, 6 July 2022
- The Nigeria Lawyers, Electronic Evidence: Simple Documents Generated From Computers Require No Authentication Under Section 84 Of The Evidence Act, 2011, 6 July 2022
- VARONIS, 166 Cybersecurity Statistics and Trends [updated 2022], 8 July 2022
- RAPAPORT, Report: Brazil must do more to encrypt, back up data, 8 July 2022
- Arcticwolf, The Top Cyber Attacks of June 2022, 8 July 2022
- Trend Micro, Private 5G Network Security Expectations Part 3, 11 July 2022
- RAPAPORT, Gone Phishing: How to Stay Safe from Cybercrime, 11 July 2022
- J-PAL, Evidence for digital and bundled services: Framing a research agenda for the Digital Agricultural Innovations and Services Initiative, 14 July 2022
- Eurojust, Newsletter - Q2 2022, 15 July 2022
- Council on Foreign Relations, Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet, July 2022

Upcoming events

- 15-31 July, C-PROC, *(online),* Translation of the HELP Course on Cybercrime into French, Spanish and Portuguese, OCTOPUS
- 15-22 July, C-PROC, *(online),* Publication of new training materials available in multiple languages on Octopus platform, OCTOPUS
- 15-31 July, C-PROC, *(online),* Further development of the cyberviolence online resource, including OCSEA country profiles, OCTOPUS
- 18 July, C-PROC, *(online),* Training session "H5P Interactive tools for Online Training": development of online e-learning platform, OCTOPUS
- 18-20 July, C-PROC/INTERPOL/AFRICA, *(in-person),* 9th African Working Group meeting on Cybercrime for Heads of Units, GLACY+
- 18-21 July, C-PROC/UKRAINE, (in-person in Suceava, Romania), Judicial Training Course on Electronic Evidence, CyberEAST
- 19 July, C-PROC/PHILIPPINES, *(online),* Cybercrime Regulation Responses (Professional Course on Digital Governance and Cybersecurity), GLACY+
- 21-22 July, C-PROC/INTERPOL/RWANDA, *(online),* Channels and Avenues - Regional workshop for Africa, GLACY+
- 25-29 July, C-PROC/INTERPOL/CAPE VERDE, *(hybrid),* ECTEG Course, Cybercrime, and digital forensics specialized training for law enforcement officers (in cooperation with OCWAR-C project), GLACY+
- July-August, C-PROC, Developing a Guide on Ransomware investigation, iPROCEEDS-2

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