Council of the European Union

Brussels, 25 March 2025
(OR. en)

7442/25

COPEN 67
CYBER 83
EUROJUST 3
ENFOPOL 97
JAI 372

NOTE

From:	General Secretariat of the Council
To:	Delegations
Subject:	Common challenges in cybercrime, report by Eurojust and Europol

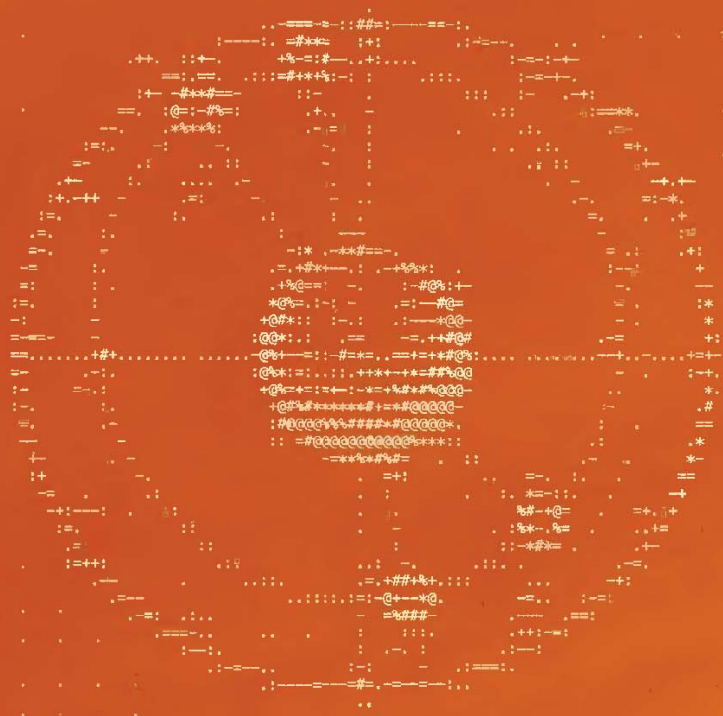
Delegations will find attached the abovementioned report, which is collaborative effort between Eurojust and Europol addressing both persistent and emerging challenges in the realm of cybercrime and investigations involving digital evidence.

The report is also available online.

EUROPOL

EUROJUST

COMMON CHALLENGES IN CYBERCRIME



2024 REVIEW BY
EUROJUST AND EUROPOL

Common Challenges in Cybercrime
2024 Review by Eurojust and Europol

ISBN 978-92-95236-63-9 doi: 10.2813/3243780 QL-01-24-005-EN-N

This report is jointly issued by Eurojust and Europol, the European Union Agency for Law Enforcement Cooperation.

Neither Europol or Eurojust nor any person acting on behalf of one of the agency is responsible for the use that might be made of the following information.

Luxembourg: Publications Office of the European Union, 2025

Cite this publication: Eurojust and Europol (2025), Common Challenges in Cybercrime - 2024 review by Eurojust and Europol, Publication Office of the European Union, Luxembourg

2

Contents

Executive Summary 4

Introduction 5

Common challenges 6

- Common challenge 1: Data volume 6
- Common challenge 2: Loss of data 7
- Common challenge 3: Access to data 11
- Common challenge 4: Anonymisation services 15
- Common challenge 5: Obstacles to international cooperation 17
- Common challenge 6: Challenges in public-private partnerships 21

Legislative responses to some of the enduring challenges 22

- JUDEX 22
- EU Electronic Evidence legislative package 23
  - Regulation (EU) 2023/1543 23
  - Directive (EU) 2023/1544 26
- Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC 27
- European Union Artificial Intelligence Act 28
- Second Additional Protocol to the Budapest Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence 29
- Clarifying Lawful Overseas Use of Data Act– CLOUD Act 30

Conclusions 31

Endnotes 32

Executive Summary

The 2024 report on 'Common Challenges in Cybercrime' is a collaborative effort between Eurojust and Europol that addresses both persistent and emerging challenges in the realm of cybercrime and investigations involving digital evidence. This year's report provides updates on significant developments and introduces new legislative tools aimed at enhancing the effectiveness of measures for fighting cybercrime.

The report underscores the ongoing collaboration between Eurojust and Europol which goes from strength to strength. Examples are the success of the SIRIUS Project, through serious crime investigations, numerous joint training programmes, and comprehensive reporting. The report highlights several new EU legislative frameworks, such as the e-evidence Package and the Digital Services Act. These frameworks were crafted to address the increasing volume of data, the ongoing issues related to loss of access to data, and challenges presented by anonymisation services in the context of investigation and prosecution of crimes. The aim of the frameworks is to streamline processes and make it easier for competent authorities working in criminal investigations and prosecutions to manage large data sets and foster international cooperation more effectively.

Key cybercrime challenges are identified in the report. One important challenge is data management, which requires law enforcement agencies to deal with massive volumes of data, triggering a need for advanced analytic techniques and significant resources which are currently beyond the reach of many agencies. The report notes the ongoing impact of legal uncertainties following the invalidation of the Data Retention Directive, which continues to affect the availability of data for investigations. Additionally, technologies that obscure user identities and locations or block the lawful access to data are creating substantial barriers to tracing illicit activities. International cooperation also faces legal and logistical barriers that complicate the fight against cybercrime and often span several jurisdictions. Furthermore, collaboration between public and private partners, crucial for resolving cybercrimes, often run into obstacles such as data-sharing restrictions and the sensitivity of investigations.

This 2024 report outlines the common strategic directions of Eurojust and Europol in combating cybercrime. Moreover, it gives an overview of the use of new legislative tools and the practical application of these new legislative measures. The effectiveness of these tools will depend on their integration into current strategies and their adoption in the field by practitioners. At the same time, there are ongoing efforts aimed at enhancing the technical and operational capacities of law enforcement authorities in the EU, and ensuring that they are properly equipped to handle the complexities of modern digital investigations.

Introduction

The objective of this report is, as in previous editions, to identify and categorise common challenges in combating cybercrime, from both the law enforcement and judicial perspectives. However, the second part of the report this time puts the focus on legislative tools that potentially alleviate the identified challenges.

Eurojust and Europol have collaborated on many serious crime investigations, provided numerous training events, and drafted several reports since the publication of the previous report in 2019[1]. The SIRIUS Project[2], co-implemented by the two agencies, is perhaps the best-known example of strategic cooperation between Eurojust and Europol. This report provides an overview of relevant developments in cybercrime challenges, particularly in view of the new legislative instruments recently adopted in the field of e-evidence.

In addition, there are updated insights in the report into ongoing activities and open issues related to these various challenges, complemented by brief reflections on the current state of affairs following the introduction of new EU legislation and available tools for the law enforcement and judicial authorities.

The identified challenges are:

- data volume;
- data loss;
- access to data;
- anonymisation services;
- obstacles to international cooperation;
- rapid response, prevention and awareness; and
- challenges for public-private partnerships.

Since the 2019 report, several new EU legislative instruments aimed at addressing these issues have been introduced. These developments are a step in the right direction, although their effectiveness depends on how they are implemented in practice. It is important to state that the previously identified challenges still exist, but there are now additional legislative tools available to address them. In this report, the practical implications of these challenges are examined in this new legislative context. Another focus of the report is on how these new legislative tools can be used to good effect and integrated into existing strategies to mitigate the challenges of digital investigations.

The following legislation is discussed in the report:

- e-Evidence Package (European Production and Preservation Orders), Regulation (EU) 2023/1543 and Directive EU 2023/1544.
- Digital Services Act Regulation (EU) 2022/2065.
- European Union's Artificial Intelligence Act ('EU AI Act').
- Second Additional Protocol to the Budapest Convention on Cybercrime CETS 224.
- CLOUD Act and the developments regarding the Executive Agreement between the EU and the USA.

Common challenges

Common challenge 1: Data volume

An increasing number of investigations contain large amounts of data. Investigations may involve terabytes or even petabytes of data, making it difficult to store, manage, and effectively analyse without significant knowledge, computational resources and specialised tools. The data volume can be overwhelming for investigators and lead to higher processing times and storage capacity issues. This problem also affects service providers who must retain the data.

In the context of cybercrime, data streams can be continuous. Effective investigations demand real-time analysis to be effective, along with advanced analytics and monitoring tools. This requires specialised knowledge and expertise. Ongoing investment in technology and training is needed to be able to adapt to these modern large investigations.

Data comes in many forms, from structured data such as Simple Query Language (SQL) databases to unstructured databases and data such as emails, social media posts, and images. A common challenge for investigating large and complex datasets is related to the methods of data processing and analysis. There are many different ways in which datasets are structured, stored and displayed. These are referred to as data models, which determine how investigators can work with the data.

A common data model is often not available between, or even within agencies.

This can lead to long delays when processing such data due to the lack of interoperability, i.e. when the data models being used are different and might require data to be reformatted and restructured for processing before investigators can jointly work on it. Law enforcement agencies (LEAs) often receive data in non-standardised formats, which may be difficult to interpret *(e.g., what time-zones the timestamps are in)* or in an unstructured manner, all of which complicate processing and working with the data.

The omnipresence of data has led to a new reality to which investigators have to adapt. Investigators often try to find cross-matches between data sets in large (cybercrime) investigations, which can be technically complex. Typically, cyber and other criminals use obfuscation techniques to hide their identity (real names, nationality, geolocation, IP address, and payment information). To get a better insight into the relationships between these identifiers, and to uncover hidden patterns that can deanonymise criminals, investigators need advanced analytical techniques.

The need for these specialised tools and skills to process and analyse large and complex data sets is a significant challenge. Many LEAs lack the necessary resources for such tools and for training their staff. This leads to additional issues and delays in processing large data sets.

Ongoing activities

- Joint efforts in awareness-raising and capacity building.
- Creation of common data models, which can greatly reduce the time and complexity to process large data sets.

Open issues

- The increased variety and volume of data make data processing more time-consuming.

- Data storage issues caused by the growth of data require the continual expansion of secure storage infrastructures, which is costly and complex.
- Many LEAs lack the necessary information technology (IT) (software and hardware) and capacity-building resources for training staff.
- LEAs struggle to hire and retain specialised expertise – such as data scientists, digital forensics and other experts. This leads to additional delays in processing and analysing large data sets.
- LEAs may be faced with inadequate numbers of staff, limiting their ability to dedicate the necessary manpower to data analysis.
- There are no standard reporting formats for service providers, nor a standard request format for government agencies.
- There is a need for aligning data models in and across LEAs, but ideally also in judicial/competent authorities and related private companies.

Common challenge 2: Loss of data

Loss of data remains an important challenge in cybercrime investigations. The invalidation of the Data Retention Directive by the Court of Justice of the European Union (CJEU)[a] left the legal landscape on data retention for law enforcement purposes in disarray across Europe. As a result, it is unclear if and what kinds of data is being retained by service providers, and, if so, for how long.

As currently there is no standardised EU legal framework for data retention for law enforcement purposes, in some EU Member States (MSs) there is no data retention period while in others data are retained for only a few days[b]. This means that in some cases – for instance when a crime is discovered days or weeks after it occurs, or in lengthier cross-border requests – data requests reach service providers after the data retention period has expired, and therefore there is no available information to continue with the investigation. These discrepancies hinder investigations, and may result in investigative leads being lost, because the data are not retained/available[c].

Already in the March 2023 Lisbon Declaration[d], European Police Chiefs highlighted their specific concerns about the repercussions at national and international levels from the lack of clear guidelines on data retention for traffic and location data at EU level. They emphasised that this ambiguity prevents them from carrying out their duties and it affects society as a whole. In addition, they raised issues regarding the potential impact on citizens' rights, freedoms, and guarantees, which could, in turn, affect the democratic rule of law. This is because certain types of crimes can only be prevented and investigated if non-content data retention is permitted.

In 2023, the High-Level Group (HLG) on access to data for effective law enforcement[e] was

a Joined cases C-293/12 and C-594/12, Digital Rights Ireland Ltd and others https://curia.europa.eu/juris/documents.jsf?num=c-293/12
b For more detailed information on national legislative initiatives to fill the data retention gap, see SIRIUS EU Digital Evidence Situation Report 2022, December 2022.
c For more detailed information see Cybercrime Judicial Monitor – Issue 6 | Eurcjust | European Union Agency for Criminal Justice Cooperation (europa.eu)
d https://www.europol.europa.eu/media-press/newsroom/news/european-police-chiefs-call-for-industry-and-governments-to-take-action-against-end-to-end-encryption-roll-out
e https://home-affairs.ec.europa.eu/networks/high-level-group-hlg-access-data-effective-law-enforcement_en

created. This initiative was co-chaired by the EU Commission and the rotating Presidency of the Council of the EU and explored challenges that law enforcement practitioners in the Union face in their daily work in connection to data access, including data retention.

This was a multi-stakeholder initiative supported by the EU MS, academia, and other EU partners, including Europol and Eurojust. The HLG published a set of potential solutions to overcome the challenges flagged by law enforcement practitioners.

Several EU-wide regulations have the aim of addressing challenges posed by digital evidence in legal proceedings. These regulations are focused on ensuring that electronic evidence is preserved, accessible, and admissible in legal cases, while also respecting data protection and privacy norms. Examples of these include the General Data Protection Regulation (GDPR) and the e-Evidence Regulation. These will be discussed further in the 'Legislative responses to some persisting challenges ' section of this report.

Internet Governance-Related Challenges (CGNAT, WHOIS, End User assignment, DNS)

As unallocated IPv4 addresses have become depleted since 2011, network address translation (NAT) has been one way of changing the Internet Protocol (IP) header of packets and for mapping several IP addresses into one. With Carrier-Grade Network Address Translation (CGNAT), this method is done at scale. It is a workaround technology that allows for the sharing of one IP address by up to around 65 000 users at the same time. In practice, it means that a user is not identified solely by the IP address they use but by the IP address and the assigned port number. The challenge here is that the individual ports assigned to individual users are not usually logged, and that leads to difficulties in identifying the origin of an internet connection. This aggregation measure is having a negative impact on the granularity of answers provided by Internet Service Providers (ISPs). CGNAT is most commonly used by small ISPs and mobile operators.

CGNAT allows ISPs to share the limited pool of publicly available IPv4 addresses, and in doing so delays the implementation of IPv6. With IPv6, each connection can have its own IP address, which will make it easier to uniquely identify devices and therefore users. Another temporary solution, which some European countries have already adopted, is limiting the number of subscribers to a maximum of between 16 and 64 users per IP address, thus simplifying identification processes. Another solution that could be considered is to enforce the storage of individual ports per user for ISPs, which would significantly help in identifying users behind CGNAT IP addresses.

LEAs have developed methods to improve data extraction and analysis to resolve IPv4 addresses and attribute them to a suspect or user. This helps LEAs increase the chance of identifying suspects, but there are still various difficulties that lead to inaccurate results. Therefore, more permanent solutions are also encouraged, such as a further move to IPv6, port logging and / or limiting the number of subscribers per IP address.

WHOIS is a publicly available and decentralised database of registration and contact information of the owners (registrants[f]) of domain names. The International Corporation for Assigned Names and Numbers (ICANN) runs the WHOIS database. The WHOIS database was previously a crucial resource for LEAs in attributing a domain name to a person or company. However, in 2018, when the GDPR came into effect, ICANN instructed all registry operators and registrars to redact all personal data from publicly available WHOIS records. There were no exceptions for third (governmental) parties such as law enforcement authorities or the judiciary.

Since 2018, WHOIS data are no longer visible to the general public. However, ICANN recently started running a pilot to test a tool for managing access requests to WHOIS data, over a period of two years.

f Registrars facilitate the domain name registration process for internet end-users (registrants). After registration, registrars send the information to a registry, which enters the information in a centralised database.

This service, called 'Registration Data Request Service' (RDRS)[3], connects requestors seeking non-public registration data with the relevant ICANN-accredited registrars for generic top-level domain names (gTLDs) who are participating in the service. Non-public data contains information such as a name, home address, email address, and phone number related to a domain. The pilot tool is a positive step, but this system is still a voluntary service, where registries and registrars can decide if they want to participate or not. This could still lead to the lack of access to crucial evidence for identifying who is behind a malicious domain. Yet another issue with the RDRS system is confidentiality when it comes to requests for domain registration data. ICANN has indicated that the design of the system does not provide functionalities for maintaining law enforcement request confidentiality[4]. This is a major deterrent for LEAs against using the system.

Aside from ICANN, other parties have also started to implement alternative initiatives in an attempt to replace the WHOIS directory with other sources. The DAP.LIVE system by the DNS Research Foundation is one example[5]. INTERPOL has also developed a pilot test model of a portal that provides automated access to non-public domain registration information data and is only accessible to vetted law enforcement entities[6]. Such initiatives gather information on domain names and their provenance from other (industry) sources than ICANN's, such as phishing data sets, GDPR breaches, blockchain domains, and others. Some of them also allow for users to add their own data. These solutions can be useful for strategic crime analysis and may be of some value for investigations. However, they are unsystematic, costly and the information reliability and traceability are difficult to determine, potentially undermining their validity for judicial proceedings.

Furthermore, if some measures in discussion amongst the partners of Réseaux IP Européens Network Coordination Centre (RIPE NCC) are adopted, the potential for swiftly identifying IP addresses could be hampered. RIPE NCC is the regional internet registry for Europe, the Middle East, and parts of Central Asia.

The RIPE database historically provided comprehensive details of IP addresses of end-user entities, akin to domain name ownership. These measures in discussion would eliminate end user assignment data from the public registry in the RIPE Database[7].

Investigators would lose direct access to RIPE, and would have to go to local registries instead. Consequently, it would require additional steps or inquiries to ascertain the specifics of how an IP address has been used, potentially delaying investigative processes. The granularity of available data would also be reduced. The potential change in accessing end-user assignment data in the RIPE Database would mean that LEAs and the judiciary would have to obtain court orders to access information from public network operators. Direct access has helped many investigators to work swiftly, which would be hindered if these measures are adopted as they may lead to delays in investigations.

For many years, the Domain Name System (DNS), which translates domain names into IP addresses, has been abused by criminals to carry out illegal activities. DNS records can be manipulated to redirect users to domains containing malware or phishing websites. Examples of DNS abuse include domain hijacking, phishing, malware, botnets, spam, and more. The information available in DNS lookups has become gradually less comprehensive.

The EU Commission's NIS 2 Directive[8] has highlighted that one of the key factors for maintaining the integrity of the internet depends on the reliability, resilience, and security of the DNS. For 2024, ICANN has set itself a goal to enhance the ways in which to combat DNS abuse[9]. To this end, ICANN initiated the process to amend the 2013 Registrar Accreditation Agreement (RAA) and the base gTLD Registry Agreement (Base RA) to strengthen the existing abuse mitigation obligations[10]. With these new obligations, rather than confirming receipt of a complaint, registrars would need to act on that complaint. This would be a step in the right direction, as these measures may minimise DNS abuse and possibly reduce the number of victims affected by this type of malicious action.

Ongoing activities

- Monitoring of legal and case-law developments on data retention through Eurojust's Cybercrime Judicial Monitor (yearly product)[11].
- The effect of the CJEU case-law on national data retention regimes and judicial cooperation in the EU", prepared by Eurojust and the European Judicial Cybercrime Network (EJCN) was published on the Eurojust website in November 2024.
- Europol's EC3 actively presents the LEA needs on internet governance in various high-level groups, such as at RIPE or ICANN, while monitoring the United Nations (UN) process[12].
- Europol's EC3 is preparing training on the challenges of internet governance and existing capacities and tools to access data. The goal of the training is to improve investigation capacities and threat assessments by enhancing data access.
- The SIRIUS team is working on updating their 2022 report on 'Data Retention in the EU'. Via its restricted platform, SIRIUS provides guidelines and best practices on how EU competent authorities can access registries and request registrars to lawfully disclose data for criminal investigations.
- As regards lawful disclosure requests to registry operators or registrars, there are ongoing discussions with ICANN over an appropriate timeline to respond to requests in emergency circumstances.
- Registries and registrars are currently voting on amendments to the registrar accreditation agreement to strengthen the existing abuse mitigation obligations. This would mean that rather than simply confirming receipt of a complaint, registrars would need to act on that complaint.
- The European Judicial Cybercrime Network (EJCN) has provided training on Internet Governance with ICANN in relation to Art.°6 of the Second Additional Protocol of the Budapest Convention.

Open issues

- Permanent access for LEAs to non-public WHOIS information that is both swift and efficient.
- RDRS is still a voluntary service and there is currently no process to safeguard the confidentiality of law enforcement requests on domain registration data.
- End-user assignment data are deleted from the public registry in the RIPE Database, which leads to additional steps or inquiries to ascertain the usage details of an IP address, i.e. on the owners of domain names.

Common challenge 3: Access to data

A. Lawful access to encrypted communication

The EU Innovation Hub for Internal Security[13] recently published its First Report on Encryption[14]. In this report, encryption is referred to as the process of transforming information into a secure format to protect it from unwanted access or modifications by third parties, typically referred to as confidentiality and integrity of data. Encryption is an integral part of our current daily life, contributing to technological developments, security, privacy, and authentication. However, criminals increasingly use encryption technologies to ensure anonymity. This enables their communications and illegal actions to remain secret and helps them stay out of the reach of law enforcement and judicial authorities[g]. Europol and Eurojust have jointly produced three reports on the challenges posed by encryption[15] [16] [17].

The various toolboxes available to EU Member States' general legal provisions on accessing encrypted information vary enormously. For example, in one MS, law enforcement allows proportionate coercion to make a suspect unlock a seized device, without the approval of a judge. In others, it is possible to hack a suspect's devices. However, in some EU countries, a suspect's password cannot even be used when it is found in a house search. There are more details on this, and on the legal landscapes and case law in the Encryption Observatory Reports[18], and in the Cybercrime Judicial Monitors[19].

In the 2019 Common Challenges for Combating Cybercrime report, the EU law enforcement authorities indicated that a significant and increasing percentage of cybercrime investigations involve the use of some form of encryption to hide relevant data and evidence of communications. At the same time, Electronic Service Providers were increasingly implementing encryption by default. This has only increased since then.

Encryption used by criminals to hide evidence of their activity continues and poses significant challenges for law enforcement and judicial authorities. This has significantly complicated access to criminal communications, which in turn has obstructed the collection and use of digital evidence in court proceedings. Victims affected by the abuse of encryption occur not only in cyber-enabled and cyber-dependent crimes, but in all crime areas, ranging from weapon trafficking, terrorism-related crimes, fraud schemes to money laundering, and so on.

Criminal use of encrypted communication channels

In recent years, various encrypted communication platforms, mainly used by criminals, have been taken down. Main examples include EncroChat[20], Sky ECC[21], and Exclu[22], and these provided invaluable insight into the unprecedented amount of information exchanged between criminals.

Information gathered from this type of criminal platform highlight how important encrypted communication channels are to criminals. They provide law enforcement authorities with enormous insight into criminal networks and in turn have caused major disruption to a wide variety of criminal activities, ranging from violent attacks to large-scale drug transportation.

There have been several positive court judgments given in the EU Member States on the use of evidence gathered from encrypted communication channels (e.g. SkyECC and EncroChat). The EncroChat case is a landmark ruling given by the CJEU on 30 April 2024, which clarifies the conditions for the transmission and use of evidence in criminal cases with a cross-border dimension[23h].

Since the dismantling of various encrypted communication platforms, criminals have been searching for new ways to communicate secretly. More on this can be found on the EU Innovation Hub for Internal Security which recently published its report on encryption[24].

g The judiciary involves the prosecution services, trial and investigative judges of the Member States. This term does not include law enforcement authorities.

h Discussed in detail in the 1st Report on Encryption by the EU Innovation Hub for Internal Security.

> Additionally, there is the Wickr Me judgment on a messaging app that provided end-to-end encrypted communication for its users. The application was shut down by its owner – Amazon – at the end of 2023, because it became a place for exchanging images of child sexual abuse and a hub for drug dealers and extremists.

The use of encryption in telecommunication technologies (e.g. 4G and 5G) complicates the LEA capabilities to carry out effective investigations and may prevent them from carrying out their duties in the digital world.

For example, 5G standards introduce end-to-end encryption (E2EE) for voice calls over 5G stand-alone networks. Similarly, the challenge exists also in 4G networks when a service provider enables privacy enhancing technologies in Home Routing[i] [25]. This means that clients using roaming services abroad (e.g. calls, messages, data) cannot be lawfully intercepted by LEAs of the country they are visiting or residing in[26].

5G-SA networks also support network slicing, which allows multiple virtual networks to operate on the same physical hardware. Each slice can be optimised for specific types of services and traffic, potentially using different security protocols and measures. This makes it challenging for LEAs to monitor a target's data as a whole without access to each relevant slice. In addition, the dynamic IP allocation in 5G-SA networks frequently changes users' IP-addresses, which increases the effort needed to reliably identify and monitor a specific user or device over time.

The use of rich communication services (RCS) to exchange SMS messages with end-to-end encryption is an additional area of concern, for which LEAs need solutions.

Technologies such as these block traditional communication service providers (CSPs) from being able to access the information, and restrict the LEAs ability to lawfully access (content) data in real time.

In the realm of Domain Name System (DNS) encryption, two competing approaches have surfaced. The DoT/DoO approach means that the DNS traffic is encrypted over the transport layer security (TLS) protocol, whereas the DoH/DoHTTP/3 approach uses Hypertext Transfer Protocol Secure (HTTPS). In general, the aim of both approaches is to enhance users' security and privacy, but the implications for law enforcement differ greatly. The former approach (DoT/DoO) still allows the filtering of a suspect's DNS traffic, while the latter (DoH/DoHTTP/3) makes it indistinguishable from regular browsing traffic. In both cases, lawfully accessing the DNS content of a suspect relies more on the DNS service providers' cooperation[27].The European Electronic Communications Code (EECC)[28], which came into force in 2018, harmonised the telecommunications regulatory framework across the EU. It enabled lawful interception by competent national authorities, not only for telecommunications providers, but also to over-the-top (OTT) service providers[j] active but not physically present in the EU. However, some service providers do not comply with this and there is currently no enforcement mechanism to make such service providers comply without a prior court order.

An international agreement and an enforcement mechanism could be solutions to ensure that service providers (including OTTs) allow LEAs and judicial authorities to lawfully access criminal data and communications. This does not mean weakening the security of communications by undermining the E2EE, but could be done by applying the 'lawful access by design' principle. This means implementing encryption protocols in a way that allows LEAs and judicial authorities to access data in cleartext format.

i Home Routing refers to a scenario when a customer travels internationally and their communications (calls, messages and data) are still processed through their home network rather than the network of the country they are visiting.

j Over-the-top (OTT) media service refers to media and communication services offered directly to users via the internet, typically provided by third-parties without the involvement or control of an internet service provider (ISP).

Access by design in the context of lawful wiretapping refers to the principle of designing telecommunications networks and services in such a way that they include built-in capabilities to allow law enforcement agencies to lawfully intercept communications when authorised by national judicial authorities.

This concept is part of a broader set of design principles to ensure that regulatory, safety, and legal requirements are integrated into technology systems from the start, systematically and not in an *ad hoc* way. In other words, the design of lawful access mechanisms should be implemented without undermining cybersecurity or privacy, and by emphasising the concept of designed-in exceptional access[29].

Ongoing activities

- Eurojust is following national and CJEU case-law developments in relation to the admissibility of data gathered from encrypted communication platforms.
- Numerous high-level initiatives focus on creating tools, techniques, and policies that allow law enforcement and judicial authorities to access encrypted data and/or metadata when essential for criminal investigations, while concurrently upholding privacy and data protection laws. Europol and Eurojust actively collaborate with various Justice and Home Affairs' partners on these matters.

Open issues

- New technologies complicate the ability of competent authorities to lawfully intercept criminal communications.
- The lack of enforcement mechanisms in the EECC enabling lawful access to OTT service providers.

B. Cryptocurrencies

In recent years, there has been a large uptake of cryptocurrencies by criminals. Cybercriminals carry out their financial transactions almost exclusively in cryptocurrencies. These transactions are not generally sent directly to exchanges and other cryptocurrency services. Cybercriminals commonly use obfuscation techniques, in an attempt to anonymise the origin of their criminal funds, before cashing out at an exchange. Examples of obfuscation techniques include mixers, swappers, over-the-counter trading, and decentralised exchanges.

Cryptocurrencies are also increasing in popularity in other crime areas, i.e. not only related to cybercrime. For example, as described in Europol's IOCTA 2024[30], fraud is the most frequently identified predicate offence that involves the misuse of cryptocurrencies. Furthermore, cryptocurrencies are the most reported investment fraud products, leading to many victims across the EU and beyond.

Since the publication of the 2019 Common Challenges report by Europol and Eurojust, there has been a significant uptake in the usage of Decentralised Finance (DeFi) to launder criminal funds. Examples include decentralised cryptocurrency exchanges[k], liquidity protocols[l],

k Such as Uniswap, PancakeSwap, etc.
l Such as AAVE, Balancer, Curve.fi, etc.

the usage of non-fungible tokens (NFTs), and more. As these technologies rely on decentralised technologies, personal data can no longer be requested through centralised entities. Hence, there is a loss of relevant data for LEA investigations. However, as all transactions are stored in smart contracts available for analysis through public blockchains[m], there are also new opportunities for investigators when dealing with transactional data.

Even if criminal funds end up at centralised entities, LEAs do not always manage to obtain the data, because of legal restrictions. This can be for a variety of reasons, such as companies based in jurisdictions where a slow mutual legal assistance (MLA) process hampers the sharing of data. However, other companies do not even have a physical presence in such jurisdictions, and purposefully ignore lawful requests and turn a blind eye to criminal funds on their platforms. Eventually, this may lead to law enforcement actions and legal repercussions, for example the case against Bitzlato[31], because such lack of cooperation amounts to an obstruction of justice.

Novel encryption techniques may also complicate tracing cryptocurrency transactions. In the majority of cases, LEAs investigate cryptocurrency addresses appearing on public blockchains. However, there are several trends aimed at obscuring the visibility of cryptocurrency transactions. Mixers and privacy coins have been complicating tracing for years, but cryptographic developments such as Zero Knowledge Proofs and layer 2 solutions may further obscure visibility and access to criminal cryptocurrency addresses, financial balances and transactions.

In April 2023, the EU Parliament gave a greenlight to EU rules on tracing crypto-asset transfers, common rules on supervision, and customer protection. This includes Markets in crypto-assets (MiCA) and the Travel Rule[32]. The Travel Rule states that information has to travel from the source to the beneficiary and be stored by both parties. This means that if a person transfers funds from one of their accounts on exchange *x* to another account on exchange *y*, both companies need to store information on both parties. The adoption of these rules is ongoing. For example, the European Banking Authority (EBA) has recently issued 'Travel Rule Guidelines' to prevent the abuse of crypto-asset transfers for the purposes of money laundering and terrorism financing[33].

Ongoing activities

- Europol developed free gamified training for law enforcement and the judiciary: Cryptopol 1.0 in 2019 (focus on Bitcoin) and Cryptopol 2.0 in 2023 (focus on Ethereum, DeFi, and related developments).
- Europol developed guides for investigators on Bitcoin and Ethereum. Europol is also working on a report on operational best practices for cryptocurrency seizures.
- Europol organises yearly conferences on virtual currencies and helps investigators identify best practices to reach out to cryptocurrency companies in investigations.
- The EU Parliament has adopted the MiCA and the Travel Rule.
- To counter money-laundering risks, the European Securities and Markets Authority (ESMA) will set up a public register for non-compliant crypto-asset service providers that operate in the European Union without authorisation.

m Such as the Ethereum blockchain through public explorers Etherscan or DeBank

- The European Cybercrime Judicial Network[34] is drafting the 2nd edition of the Crypto Assets Guide for judicial authorities including contact information for decentralised financing (DeFI) platforms and crypto-asset service providers (CASPs).
- EJCN training for the judiciary on crypto assets, in cooperation with the private sector.

Open issues

- The use of cryptocurrency by criminals is commonplace and becoming more sophisticated.
- Constant training and development of investigative skills on cryptocurrencies for law enforcement authorities and the judiciary are needed.
- Many law enforcement agencies cannot afford basic cryptocurrency tracing tools.
- Understaffing – some law enforcement agencies do not have resources to train or recruit cryptocurrency experts.
- Criminals are using all the time more advanced ways to obfuscate funds.
- Cooperation with some cryptocurrency companies could be improved, especially those in off-shore jurisdictions.
- Investment fraud and ransomware are the top reasons for using cryptocurrencies, but the use of cryptocurrencies in a wider variety of crimes is on the rise[35].

Common challenge 4: Anonymisation services

It is often difficult to establish the physical location of cybercriminals and their operations. It is also often unclear where their data are stored. Even when this can be established, it sometimes leads to (multiple) jurisdictions that are difficult to reach by law enforcement authorities or the judiciary.

Countries have traditionally relied on MLAs and European Investigation Orders (EIOs) to obtain electronic evidence from other jurisdictions. However, these legal instruments often cause long delays in investigations. Data in cybercrime cases can move from one data centre to another in seconds, whereas it can take months for an answer to be given in MLA or EIO procedures. There are ongoing efforts to modernise and streamline methods of requesting information. In some countries, LEAs are able to contact foreign service providers via their law enforcement portals or dedicated email addresses and are able to quickly acquire information, as a first step towards evidence needed for judicial purposes. In other countries, quick reference systems for the judiciary are used to better target these requests, leading to a faster response to requests by private companies. Other solutions to these issues are the e-evidence package, which will make it easier for EU Member States to obtain electronic evidence directly from service providers, and the Second Additional Protocol to the Budapest Convention, which will enhance international cooperation on the

disclosure of electronic evidence. The e-evidence package and Second Additional Protocol to the Budapest Convention will be discussed in the section of this report on Legislative responses to some of the persisting challenges. There are also technical challenges for law enforcement in establishing the physical location of perpetrators or infrastructure[36]. For several years, there has been significant criminal usage of Virtual Private Networks (VPNs), Virtual Private Servers (VPS), and other services that obfuscate attackers' IP addresses, traffic content, etc. Some services, such as bulletproof VPNs, are specifically created for criminals. This is why several such services have been taken down in recent years. Examples include DoubleVPN in 2021[37] and VPNLab in 2022[38]. Such services provided a safe haven for cybercriminals, shielded communications, and supported serious criminal acts such as ransomware deployments. Investigations can be seriously hampered when such services have been used, as there generally is no or very limited cooperation with LEAs. The administrators of such services are often based in countries that are non-cooperative with law enforcement authorities or the judiciary, whereas the data hosting often happens across the world in countries with advanced and affordable internet infrastructures. Furthermore, companies abused by cybercriminals are often legally registered in off-shore locations, where they may only have a mailbox (shell corporations). This is occasionally even the case for prominent companies, such as popular messaging applications or cryptocurrency exchanges.

Data hosting on the internet is becoming more decentralised. Such infrastructure decentralisation is another challenge for law enforcement and the judiciary. Criminal services, such as Dark Web marketplaces, are often hosted on Virtual Private Servers (VPS). Data hosted on such cloud-based storage can easily be moved or distributed at other data centres in other countries. Data can also be mirrored, this allows for multiple instances of the same server or backups that criminals can use if there is a takedown by LEAs. Furthermore, legal uncertainties about data seizure arise as evidence tends to be scattered across jurisdictions when stored on different cloud services.

Another related issue is distributed storage. An example of this is the development of information storage on blockchains, such as Bitcoin Ordinals[39], which allows for the storage of non-fungible tokens (NFTs), namespaces, and more. Another example is the Interplanetary File System (IPFS)[40], which allows for the distributed storing of files across various 'nodes'. These novel storage methods such as public blockchains and IPFS make it impossible for law enforcement authorities to send a request to a hosting provider to remove illegal content. This may lead to the technical inability to remove, for example, child sexual abuse material, terrorism-related content, and other illicit content. Therefore, novel technical and judicial methods to deal with distributed networks have to be developed.

Ongoing activities

- Quick reference systems and dedicated law enforcement portals, or email addresses in some cases, could facilitate a swifter law enforcement alternative to MLAs and EIOs.

Open issues

- Difficulty to reach companies holding important leads in investigations, for example due to off-shore status.
- Decentralised services and distributed computing, which can hamper the removal of illegal content, or requests for information about owners of information.

Common challenge 5: Obstacles to international cooperation

Due to the borderless nature of cybercrime, international cooperation is of paramount importance and generally inevitable. Extensive international coordination is the only way to solve serious international cybercrime threats. In the recent disruption of LockBit ransomware group, ten countries cooperated in a complex joint investigation.

> LockBit was widely recognised as the world's most prolific and harmful ransomware, causing billions of euros worth of damage.
>
> In February 2024, an international sweep followed a complex investigation led by the UK's National Crime Agency in the framework of an international taskforce known as 'Operation Cronos', coordinated at European level by Europol[41] and Eurojust[42].
>
> The operation, over several months, resulted in compromising LockBit's primary platform and other critical infrastructure that enabled their criminal enterprise. 34 servers were taken down in the Netherlands, Germany, Finland, France, Switzerland, Australia, the United States of America, and the United Kingdom. The authorities also froze more than 200 cryptocurrency accounts linked to the criminal organisation.
>
> In addition, two LockBit actors were arrested in Poland and Ukraine at the request of the French judicial authorities. Three international arrest warrants and five indictments were issued by the French and U.S. judicial authorities.
>
> In May 2024, authorities from the United Kingdom, United States and Australia issued sanctions against the administrator and developer of LockBit[43].
>
> Europol's European Cybercrime Centre (EC3) organised 27 operational meetings, and four technical one-week sprints to develop investigative leads in preparation for the final phase of the investigation. Europol provided analytical, crypto-tracing and forensic support to the investigation, and facilitated information exchange in the framework of the Joint Cybercrime Action Taskforce (J-CAT) hosted at its headquarters.
> The Eurojust case was opened in April 2022 at the request of the French judicial authorities. Eurojust organised 5 coordination meetings for the judiciary of 10 countries to support the exchange of evidence between the authorities involved, to discuss investigation and prosecution strategies for the joint actions, and to solve potential jurisdiction conflicts.
>
> Victims of this ransomware attack can find decryption tools on the NoMoreRansom platform[44].

If the coordination of joint actions works well, the legal obstacles of one country can even be complemented by the task division and actions of another country, so that investigations are conducted effectively and legal obstacles are minimised. For example, investigating country *a* might have difficulties in requesting information from a cryptocurrency exchange based in off-shore country *x*. However, country *b*, another member of the investigating coalition might have more success in requesting information from country *x*. In these ways, joint investigations can facilitate optimal information-gathering conditions.

However, joint investigations require extensive investment in resources, in the form of trained personnel, funds and time. In practice, most (minor) investigations are conducted by one country alone. The most common challenges for such investigations are blocked routes in international evidence-gathering, and a lack of data deconfliction resulting in hampered access to data.

Electronic evidence can be stored anywhere in the world. Furthermore, similarly to the findings in the last report, criminal hot spots and safe havens still prevail and in these jurisdictions evidence collection is complicated.

This leads to an increasing number of suspects hosting their criminal services and funnelling their illicit funds to such jurisdictions. For LEAs, determining which country's laws apply and navigating the legal requirements to access data stored in different jurisdictions present significant obstacles to conducting successful investigations. Traditional mechanisms for international legal cooperation, such as MLAs, are often required to obtain information. In many cases, however, it is not even clear where a company is legally based.

Legal processes connected to jurisdiction issues lead to significant delays. For example, in a cybercrime investigation into ransomware, investigators might trace criminal cryptocurrency from a ransomware operator to an exchange. In reality, the suspect can transfer cryptocurrency in a question of minutes from one cryptocurrency exchange based in the Seychelles, to another exchange based in the United States, then to an exchange based in the British Virgin Islands. The minutes it takes for the criminal to do this, requires weeks of work from the police, prosecution, translation services, postal services, etc. to follow the formal procedures required. In principle, to request data in this example, a prosecutor or judge would have to issue three MLAs. It could take months to receive an answer for each MLA.

However, the investigator will at first only find the exchange in the Seychelles and will only find out about the next investigative steps in the process after receiving answers to the consecutive MLAs. After finally receiving all the answers, the suspect will have moved the funds numerous times again. In this way, it is nearly impossible for investigators to respond in a timely way and to potentially seize the funds.

Coordination and deconfliction are main tasks of Europol and Eurojust. Deconfliction in cybercrime investigations in practice means avoiding that EU Member States and operational partners are targeting the same suspects and groups, without being aware of each other's investigations. In certain cybercrime fields, such as cyber-attacks and online fraud particularly, countries often target the same suspects and organised crime groups. If there is no data deconfliction this leads to inefficiencies, as entire investigations may be derailed if, for example, another country unwittingly arrests a suspect first. Moreover and above all, deconfliction pursues and upholds the ne bis in idem principle. On occasions, several countries may request information on the same suspect(s) from the same companies. Due to the borderless nature of cybercrime, tools such as information sharing, coordination and deconfliction are essential for investigating cases successfully and optimising resources.

Rapid response, prevention and awareness

To prepare for major cross-border cyber-attacks, an EU Law Enforcement Emergency Response Protocol (LE ERP) has been adopted by the Council of the European Union. The LE ERP complements the existing EU crisis management mechanisms protocols and was developed in response to large-scale cyber-attacks in 2017. The LE ERP is part of the EU Blueprint for Coordinated Response to Large-Scale Cross-Border Cybersecurity Incidents and Crises[45].

Europol's Cybercrime Centre (EC3) has a central role in the LE ERP. The LE ERP supports EU law enforcement as a tool to facilitate rapid assessment, secure critical information-sharing, set up 24/7 contact points, and ensure effective international coordination.

The most prominent cybercrime threat of the last years in this regard is ransomware. The rise of supply chain attacks shows that cybercriminals' attack surface is extending and that companies need not just to focus on their own security, but also that of their suppliers and customers within their network. The response to these threats remains a major challenge and would benefit from streamlined responses at EU level. Various international initiatives have been put in place to effectively fight the threat of ransomware. One example is the No More Ransom project[46]. The nomoreransom.org website is an initiative by the National High Tech Crime Unit of the Netherlands' police, Europol's European Cybercrime Centre, Kaspersky and McAfee with the goal of helping victims of ransomware retrieve their encrypted data without having to pay criminals for it. In terms of prevention, the public-private initiative NoMoreRansom[47] has successfully provided ransomware victims

with decryption keys for over seven years. Their advice is not to pay the ransom and to report it[48]. Training is an important part of awareness and prevention initiatives. Cryptopol[49] is a well-known example of such an initiative. Another example is eFirst training[50], being developed by the European Cybercrime Training and Education Group (ECTEG). The aim of the training course is to provide the necessary cybercrime knowledge to first responders of LEAs. In addition, the course has the aim of teaching first responders how to better advise (potential) victims of cybercrime. ECTEG is also planning to develop another version of the eFirst training for judicial authorities.

The cybercrime prevention initiatives have the following two main objectives:

- To help citizens, businesses and governments to better protect themselves against various forms of cybercrime.
- To discourage cybercriminals and potential cybercriminals from committing such crimes through proactive preventive intervention to teach young people about cybercriminal behaviour, and to redirect them to alternatives for using their skills in a positive and lawful way.

To achieve these objectives the following measures, amongst others, have been adopted:

- Positive operational results are presented together with clear public awareness and offender prevention messages;
- Educational materials are developed together with relevant partners to develop materials that target cybercrime prevention in general and cybercrime offender prevention;
- Work is done with the International Cyber Offender Prevention Network (InterCOP) to support, and to develop and disseminate intervention based on Cyber Offender Prevention.

As ransomware actors and facilitators are often based in jurisdictions that are difficult to reach for law enforcement, reporting and prevention is very important in this field. Increased reporting of ransomware is an area that can potentially contribute to more prevention and diminished profitability. For example, since April 2023, victims of cyber-attacks in France have 72 hours to file a complaint with the judiciary or police, if they wish to be reimbursed under cybersecurity insurance[51]. More proactive reporting of intrusion data, stolen data samples and other evidence to competent investigative authorities can significantly benefit investigations.

In addition to the international initiatives to combat ransomware offences, the European Union launched in 2022 a regulatory package to ensure resilience and response capability against cyber-attacks[52]. Part of the package is the Directive on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). The NIS 2 Directive introduces new cyber hygiene requirements and incident notification mechanisms for a broader range of entities belonging to different sectors, and ensures that the majority of the entities concerned put into place adequate cybersecurity practices.

For example, in Article 23 it provides that any essential and important entity shall notify its Computer Security Incident Response Team (CSIRT) of any incident that has a significant impact on the provision of their services. The CSIRT must respond with initial feedback within 24 hours. If such incidents are deemed to be of a criminal nature, the CSIRT will also provide guidance on reporting them to law enforcement authorities.

Ongoing activities

- Operational work of Europol and Eurojust, such as facilitating cross-border cooperation between LEAs and judicial authorities, coordinating investigations, defining a common strategy for specific cases, planning joint action days, supporting joint investigation teams[n] (JIT), and more.
- The Joint Cybercrime Action Taskforce[53](J-CAT) is a unique operational taskforce of cybercrime liaison officers embedded at Europol's EC3. The J-CAT has been active since 2014.
- Eurojust, the EJCN and the European Judicial Network (EJN) foster judicial cooperation and provide practical solutions on handling cross-border electronic evidence. Efforts to enhance the knowledge and skills of legal practitioners across the EU contribute to overcoming challenges related to different national legal systems.
- Capacity-building events, such as the Europol Cybercrime Conference, Virtual Currencies Conference, InterCOP Conference, among others.
- Prevention initiatives, such as NoMoreRansom[54], InterCOP prevention network[55], among others.
- The SIRIUS Project serves as a central reference point in the EU for knowledge-sharing on cross-border access to electronic evidence. It offers a variety of services, such as guidelines, training and tools, to help with accessing data held by SPs.

Open issues

- Existing cybercriminal hot spots and safe havens from which it is difficult to obtain information from these jurisdictions.
- Mechanisms to streamline the EIO and MLA procedures to enhance their current effectiveness and operational speed.

Common challenges in cybercrime as identified by Eurojust and Europol

n https://www.europol.europa.eu/partners-collaboration/joint-investigation-teams

20

Common challenge 6: Challenges in public-private partnerships

Private entities often hold crucial pieces of evidence that can solve investigations, and can be paramount in taking down cybercriminal infrastructures, removing illicit content, and in preventing cybercrimes by adequately defending their data, systems, and customers. This has not changed since the 2019 Common Challenges report.

However, in the 2019 report, the need for standardised rules of engagement with the private sector was identified. In June 2022, key amendments to the Europol Regulation entered into force. The European Parliament and the Council agreed to strengthen Europol's capacity to better support the EU Member States in combating serious and organised crime and terrorism. In practice, amongst other things, this means that Europol can receive data directly from private parties[56]. Although, due to the sensitivity of law enforcement data, Europol can only share data back to private parties 'in specific cases where necessary and proportionate'[57].

Such personal data, under certain conditions, may be shared for the purposes of removing terrorist content and online child sexual abuse material from private party platforms, particularly when 'exponential multiplication and virality of that content and material across multiple online service providers ar anticipated'[58].

EC3 has dedicated advisory groups in place since 2013 to foster closer cooperation with leading non-law enforcement partners. These private partners help to strengthen practical cooperation between law enforcement and key domains, such as internet security, telecommunications and financial services. The private partners bring knowledge and expertise to EC3 on the impact of cybercrime and can assist in prioritisation and prevention initiatives[59]. The advisory group members can share extensive data and information on recent modus operandi of the cybercrimes they have encountered and investigated, but Europol can only share information with the advisory group members in limited conditions.

Due to the sensitivity of law enforcement investigations, data sharing tends to be a 'one-way street', as information can often not be shared by law enforcement and the judiciary with private partners for legal reasons. However, companies are also bound to protect the personal data of their customers, and an inconsistent application of GDPR provisions may therefore lead to a complete absence of information-sharing. However, past initiatives have shown that when just enough information is shared, such as cybercriminal modus operandi, both public and private parties can benefit from this in their investigations and in cleaning up platforms.

Ongoing activities

- EC3 organises advisory groups on internet security, financial services, and communication providers.
- The Europol Platform for Experts[60], and various collaborative web platforms facilitate the sharing of best practices, innovation, and knowledge. In some communities, private partners are welcomed.
- Joint projects with academia, such as the award-winning initiative Cryptopol[61], and the upcoming Advisory Group on Research and Development.
- Various capacity-building events are attended by private partners.

- Many prevention initiatives include strong public-private partnerships, such as NoMoreRansom[62], InterCOP prevention network[63], and others.
- In June 2022, key amendments to the Europol Regulation entered into force, enabling Europol to receive data directly from private parties.
- Ongoing joint work by Europol and Eurojust on the framework of the SIRIUS project, on best practices regarding the cross-border access to e-evidence. Via its restricted platform, SIRIUS provides guidelines and best practices on how EU competent authorities can address online service providers and other private sector entities, such as registries and registrars for the disclosure of data in criminal investigations.

Open issues

- Effective and legal sharing of data and modus operandi, to aid investigations and private party efforts.
- Challenges faced by EU competent authorities in pursuing voluntary public-private cooperation actions for the disclosure of data in the framework of criminal investigations. The SIRIUS Electronic Evidence Situation Report 2023 offers a complete overview.

Legislative responses to some of the enduring challenges

In contrast to the 2019 Common Challenges report, the 2024 report will also focus on legislative developments that can be seen as common solutions to some of the above identified common challenges. This section will examine the practical implications for law enforcement and the judiciary in relation to these developments in new legislative contexts. The report will specifically focus on the e-Evidence Digital Exchange System, the EU Electronic Evidence legislative package, the Second Additional Protocol to the Council of Europe Convention on Cybercrime, the CLOUD Act, the Digital Services Act, and the AI Act.

JUDEX°

The e-Evidence Digital Exchange System (eEDES) , recently renamed as JUDEX as it covers more than evidence gathering instruments, is a critical innovation designed to enhance the efficiency of cross-border judicial cooperation within the European Union. Developed in response to the increasing demand for quick access to data in criminal investigations and the need to advance international judicial cooperation, and it will become the obligatory channel to transmit cooperation instruments.

o Previously e-Evidence Digital Exchange System

The primary objective of JUDEX is not to introduce new judicial instruments but to digitise and streamline the channels to transmit judicial existing instruments of judicial cooperation. It aims to standardise the cooperation processes, secure data transmission, and ensure the integrity and authenticity of exchanged judicial documents. This is accomplished through a decentralised IT system where a secure communication channel links judicial authorities from both requesting and executing EU Member States, as well as private entities (service providers) when the European Production and Preservation Order Certificates (under the EU Electronic Evidence legislative package) are involvedp. This is supported by the e-Justice Communication via Online Data Exchange (e-CODEX), which provides a robust infrastructure for communication that provides the underlying technology for secure and efficient transmission of data.

Security is paramount within the JUDEX framework, incorporating features such as two-factor authentication and end-to-end encryption to protect communications and data. The system can be accessed by judicial authorities of EU Member States and the National Desks at Eurojust. It ensures that sensitive information remains within a controlled environment and thus protects the chain of evidence.

The system will cover all judicial cooperation instruments and will include European Production and Preservation Order Certificates (EPOC and EPOC-PR) as of 18 August 2026[p].

EU Electronic Evidence legislative package

The EU Electronic Evidence legislative package (e-evidence package) is an EU legislative initiative aimed at simplifying the process of obtaining electronic evidence across borders for judicial authorities. It is comprised of Regulation (EU) 2023/154364[64] and Directive EU 2023/1544[65], each addressing different aspects of cross-border electronic evidence acquisition in criminal proceedings.

The Regulation enables judicial authorities from EU Member States to issue European Production Orders and European Preservation Orders for electronic evidence as instruments of judicial cooperation based on the principle of mutual recognition. The Directive establishes a harmonised system on the designation of establishments and the appointment of legal representatives for private sector entities for the purpose of gathering electronic evidence in criminal proceedings.

Both the Regulation and the Directive were signed on 12 July 2023, and entered into force on 18 August 2023. The Regulation will be directly applicable from 18 August 2026, whereas the Directive must be fully transposed into the national legislation of EU Member States by 18 February 2026. Denmark has opted out from the Regulation.

Regulation (EU) 2023/1543[q]

The Regulation enables EU judicial authorities to issue European Production Orders and European Preservation Orders. European Production Orders allow a judicial authority in one EU Member State to directly order the production of electronic evidence from a service provider offering services in the EU and established or represented in EU Member State. Service providers must respond within 10 days, or 8 hours in emergency situations, to such orders. European Preservation Orders enable a judicial authority in one EU Member State to order a service provider offering services in the EU and established or represented in another EU Member State to preserve specific data for up to 60 days with a possibility of extension for another 30 days, in anticipation of a subsequent production order (or EIO or MLA request) for such data. Non-compliance with these orders can have legal consequences for service providers.

p Regulation (EU) 2023/2844 of the European Parliament and of the Council of 13 December 2023, Article 3.

q The full official name of the Regulation is: Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings.

The Regulation applies to any service provider operating within the EU – as defined in Article 3(3) of the Regulation – including those legally established within an EU Member State, as well as those not established in the EU but offering services to users in an EU Member State and having a significant connection to that EU Member State. A substantial connection is deemed to exist if the service provider either has an establishment in an EU Member State, serves a large number of users in the EU, or specifically targets activities toward one or more EU Member States. The issuance of a European Production or Preservation Order for electronic evidence corresponds to a judicial authority (directly or via validation of an order issued by a different authority).

The Regulation differentiates between different types of data – namely subscriber data, data requested for the sole purpose of identifying the user, traffic data, and content data – each requiring the involvement of either prosecutors or judges, depending on the type of data requested. European Production and Preservation Orders may be initially drafted by investigative authorities but require validation by a judicial authority. In emergency situations, orders for subscriber data or for data requested for the sole purpose of identifying the user can, under certain circumstances, be issued by other authorities, subject to retroactive validation within 48 hours.

European Production Order

Police and other competent authorities as defined by the issuing State - none alone, may issue European Production Orders only with the validation of the appropriate judicial authority, depending on the category of data at stake.

Prosecutor - can issue alone European Production Orders for subscriber data and data requested for the sole purpose of identifying the user; may also issue European Production Orders for traffic data and content data, with validation by a judge, court or investigative judge.

Judge, court or investigative judge – can issue alone European Production Orders for all categories of data (subscriber data, data requested for the sole purpose of identifying the user, traffic data, and content data).

European Preservation Orders:

European Preservation Orders for any data category may be issued by a public prosecutor, judge, court or investigative judge. With validation from a public prosecutor, judge, court or investigative judge, such orders may also be issued by any other competent authority as defined by the issuing State. Data requested for the sole purpose of identifying the user means IP addresses and, where necessary, the relevant source ports and time stamp, namely the date and time, or technical equivalents of those identifiers and related information, where requested for the sole purpose of identifying the user in a specific criminal investigation.

Common challenges in cybercrime as identified by Eurojust and Europol

Emergency cases:

'Emergency case' means a situation in which there is an imminent threat to the life, physical integrity or safety of a person, or to a critical infrastructure, where the disruption or destruction of such critical infrastructure would result in an imminent threat to the life, physical integrity or safety of a person, including through serious harm to the provision of basic supplies to the population or to the exercise of the core functions of the State. Critical infrastructure is defined in Article 2(a) of Directive 2008/114 ECs as an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions. In these cases, the issuing authority can be any authority recognised under national law, with the caveat that in 48 hours the competent authority has to validate the order. This option can only be used if because of the emergency there is no time to issue an order pursuant the Regulation.

In accordance with Regulation (EU) 2023/1543, European Production and Preservation Orders can be issued for all criminal offences, with varying requirements depending on the type of data requested. For more sensitive data, such as traffic and content data, stricter thresholds apply, including offences punishable by at least three years of imprisonment or specifically listed offences, such as fraud, sexual abuse, illegal access to information systems, and terrorism, among others. In addition in the Regulation, the roles and obligations are defined of service providers acting as data controllers or processors under the General Data Protection Regulation (GDPR).

Language accessibility is a crucial factor in such communications, as certificates and forms must be issued in a language accepted by the receiving service provider or, where no language has been notified by the service provider, in the official language of the EU Member State where the service provider is established. Recipients of production orders can communicate challenges for implementation, which will be resolved by the enforcing and issuing authorities.

In instances where legal complexities arise, particularly those involving immunities or professional privileges, entities such as Eurojust or the European Judicial Network are available for additional assistance, and to ensure that the particular aspects of such cases are properly addressed.

The decision to retract a European Preservation Order is made by the issuing authority, based on a recommendation from the enforcing authority.

Grounds for non-execution include concerns related to immunities, privileges, freedom of the press and expression, impact on fundamental rights, and lack of dual criminality. Recipients must promptly inform individual(s) whose data are subject to the order, unless non-disclosure is requested by the issuing authority. Compliance with enforcement and financial penalties for non-compliance are the remit of the enforcing authority.

Access to secure IT systems and electronic communication channels is essential for implementing orders, ensuring reliable transmission and accepting requests and answers. Electronic documents provided under the scope of the Regulation have the same legal effect as paper-based ones. National authorities cannot refuse to accept the electronic execution of orders, neither can they request that the response is sent to them in a paper-based format.

Regulation (EU) 2023/1543 introduces the legal obligation for cooperation between public authorities and private entities, particularly of internet service providers and other digital service platform providers, to ensure compliance with European Production and Preservation Orders for the acquisition of electronic evidence.

Directive (EU) 2023/1544[r]

Directive (EU) 2023/1544 establishes rules on the designation of designated establishments and the appointment of legal representatives for service providers offering their services within the EU. The Directive's purpose is to regulate the receipt, compliance with, and enforcement of decisions and orders relating to the gathering of electronic evidence in criminal proceedings. It applies to service providers – as defined in Article 2(2)[s] – offering their services within the EU, excluding those established on the territory of a single EU Member State and offering services exclusively within that EU Member State. EU Member States may not impose – for the same purpose – additional obligations on service providers beyond those outlined in the Directive.

In accordance with the Directive, EU Member States are required to ensure that service providers designate or appoint at least one recipient for receiving, complying with, and executing decisions and orders issued by the competent authorities of EU Member States regarding the gathering of evidence for criminal proceedings. This requirement applies to service providers established in the EU as well as to those not established within the EU but offering their services within. Furthermore, service providers established in an EU Member State not participating in Regulation 2023/1543 must appoint a legal representative in a participating EU Member State. The designated representative must be established or reside in an EU Member State where the respective service provider offers its services, and must be able to be subject to enforcement procedures.

Designated establishments and legal representatives must receive the necessary powers and resources from their parent organisation to be able to cooperate with competent authorities and comply with relevant orders and decisions. Both the designated establishment or legal representative and the service provider can be held jointly and separately liable for non-compliance. Service providers must designate establishments or appoint representatives by 18 August 2026 in one of the EU Member States bound by Regulation 2023/1543 (that is, excluding Denmark). They must notify the central authority – as designated pursuant to Article 6 of the Directive – of the EU Member State where its designated establishment is established or where its legal representative resides of the contact details of their designated establishment or legal representative, and this information should be made publicly available. Each EU Member State must designate a central authority which collaborates with other central authorities and the EU Commission, and provides necessary information and assistance for the effective implementation of the Directive.

> The primary difference between designated establishments and legal representatives lies in the entity's location (within or outside the EU), and the country's relationship with the e-evidence package (participating in it, or opted out from it). A 'designated establishment' means an establishment with legal personality designated by a service provider established in an EU Member State taking part in the Regulation 2023/1543 (i.e. located in an EU Member State partaking in the Regulation 2023/1543). A 'legal representative' means a natural or legal person appointed by a service provider not established in an EU Member State taking part in Regulation 2023/1543 (i.e. located outside of the EU or in an opted out EU MS). Such legal representative must be located in an EU Member State that is partaking in Regulation 2023/1543).

Service providers offering services in the EU on or before 18 February 2026 must set up designated

r The full name of the Directive is: Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings

s Service provider means any natural or legal person that provides one or more of the following categories of services – with the exception of financial services – electronic communication services, internet domain name and IP numbering services (such as IP address assignment, domain name registry, domain name registrar and domain name-related privacy and proxy services), other information society services that enable their users to communicate with each other or make it possible to store or otherwise process data on behalf of users to whom the service is provided; provided that the storage of data is a defining component of the service provided to the user.

establishments or appoint legal representatives by 18 August 2026. Those starting to offer services after 18 February 2026 must have a designated establishment or appoint a legal representative within six months from the start of their services. Service providers are required to notify the central authority of an EU Member State about their designated establishment or legal representative. The notification should include contact details and any changes, as well as specify the official language(s) in which they can be addressed. If a service provider has multiple establishments or representatives, the territorial scope and languages for each should be specified. This information will be made publicly available on the e-Evidence designated section[66] of the webpage of the European Judicial Network (EJN)[67] and any other information received will be incorporated into the Judicial Atlas.

EU Member States are required to designate one or more central authorities to ensure the consistent and proportionate application of the Directive. They must inform the EU Commission of the designated central authority/authorities. The EU Commission will then create and share a list of the central authorities.

More detailed information on the new e-Evidence package can be found in the Cybercrime Judicial Monitor No 8[68] and on the SIRIUS video on Eurojust's Youtube channel[69].

Data volume, Data loss, Anonymisation are not mentioned explicitly in the Directive.

The Directive outlines mechanisms for accessing data, through designated establishments or legal representatives that handle requests for electronic evidence. These entities serve as single points of contact for foreign-based service providers in the European Union.

The obligation to establish a legal entity within the European Union enables the competent authorities to directly address a service provider operating within their jurisdiction and this entity has to provide the requested data regardless of the actual location of the data in question.

The Directive addresses obstacles to international cooperation by establishing a harmonised legal framework across the EU Member States, which includes the designation of central authorities, the standard application of rules, and the legal obligation on service providers to set up legal representation within the EU, with the power and task to respond to requests from law enforcement and judicial authorities.

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC

Regulation (EU) 2022/2065, also known as 'the Digital Services Act' (DSA)[70], is an EU regulation aimed at creating a safe and trusted online environment for users by guaranteeing access to legal and safe content, goods, and services, while safeguarding fundamental rights. It is part of the digital services package introduced by the EU Commission in response to the need to regulate the digital space and make it safer for consumers and businesses. The DSA along with the Digital Markets Act (DMA) forms the centrepiece of new EU digital regulation aimed at improving the functioning of the EU single market.

The DSA follows the principle that what is illegal offline should also be illegal online and seeks to establish clear and uniform responsibilities for providers of online intermediary services for greater public oversight. It applies to intermediary services offered to recipients in the EU, irrespective of where the services are headquartered.

Intermediary services are categorised into three levels of responsibility. 'Mere conduit' services include network infrastructure providers, such as ISPs, which do not store or modify content. They are typically exempt from liability unless ordered by a court or administrative authority to address illegal content or activities.

'Caching' services temporarily store data to facilitate efficient data transmission and are generally exempt from liability if they comply with conditions related to illegal content removal.

'Hosting' services involve storing data provided by users and are liable for the content they store if they have knowledge of illegal activity and do not promptly remove or disable access to it.

The DSA imposes specific obligations on hosting services regarding illegal content management, transparency, and cooperation with the authorities.

Providers of intermediary services are encouraged to conduct voluntary investigations to detect and remove illegal content and comply with EU and national law. However, they are not obliged to actively monitor for illegal activity.

Article 10 of the DSA introduces common rules on the content and format of cross-border orders for data disclosure directed at service providers. Without setting out a legal basis for such orders, which must be based on either EU or national law, Article 10 of the DSA sets minimum conditions that such orders must meet and establishes complementary requirements for processing them.

The DSA includes provisions for notifying authorities of actions taken to comply with orders related to illegal content. It specifies the legal basis of orders and stipulates the information required in such orders. It also regulates the language accessibility and transmission of orders among relevant parties.

Providers of intermediary services must designate a point of contact to communicate with authorities and publish relevant contact information. They must also appoint a legal representative in an EU Member State where they offer services to ensure compliance with regulatory provisions decisions and enforcement.

Hosting service providers must implement a notice and action mechanism, allowing users to report illegal content. Notices should contain precise and substantiated information, and the provider must acknowledge receipt, promptly notify the submitter of their decision, and provide information on redress options. Hosting providers must also notify relevant authorities of serious crimes involving threats to life or safety.

Trusted flaggers, entities proficient in detecting and reporting illegal content, receive priority in the processing and prompt reporting of notices. They must publish annual reports on notices submitted, which are made publicly available without personal data. Digital Services Coordinators distribute information on trusted flaggers to relevant parties.

During a crisis posing a serious threat to public security or health, the EU Commission may require Very Large Online Platforms[t] and Very Large Search Engines to take certain actions to mitigate the threat[71]. These actions must be necessary, justified, and proportionate to the threat.

EU Member States are responsible for determining penalties for violation of the regulation by intermediary service providers, with fines not exceeding 6% of the provider's annual worldwide turnover. Penalties are also specified for supplying incorrect information, or for failing to reply or rectify it.

The DSA was signed on the 19 October 2022, it entered into force on 16 November 2022 and has been directly applicable since 17 February 2024.

The DSA does not directly address common cybercrime challenges in the traditional sense, instead, it sets regulatory standards for digital platforms to manage and control the content on their platforms, particularly concerning illegal content.

European Union Artificial Intelligence Act[u]

In response to the demand for reliable development and legal AI governance,

t Very large online platforms and very large online search engines are defined in a way that they have a number of average monthly active recipients of the service in the Union equal to or higher than 45 million, and which are designated as very large online platforms or very large online search engines by the Commission.

u REGULATION (EU) 2024/... OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of ... laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)

the European Union (EU) has adopted the European Union AI Act, which aims to regulate the development, deployment, and use of AI systems within the EU. The Act seeks to strike a balance between promoting innovation and protecting individual rights and societal values. It categorises AI applications into four risk levels: minimal, limited, high, and unacceptable. Unacceptable risk AI systems, such as those that manipulate human behaviour or exploit vulnerabilities, will be prohibited. High-risk AI systems, including those used in critical infrastructure and specific areas, will be subject to registration and assessment. Limited risk AI systems must comply with transparency requirements to inform users' decisions. The use of minimal risk AI systems involve minimal or no risks, and therefore there are no mandatory measures foreseen in the AI Act.

The AI Act includes provisions for remote biometric identification systems (RBI) used for law enforcement purposes, with safeguards and exceptions in place. Law enforcement can use 'post- remote' RBI for targeted searches of convicted or suspected criminals and 'real-time' RBI for specific purposes such as preventing terrorist threats. The Act designates national supervisory authorities to enforce the rules, conduct investigations, and impose penalties for non-compliance. Serious violations can result in fines of up to EUR 30 million or 6% of the entity's annual global turnover.

The AI Act entered into force on 1 August 2024. The Act becomes fully applicable on 2 August 2026, although certain provisions will apply earlier to address specific risks and requirements related to AI systems.

The AI Act does not directly address common cybercrime challenges, instead, its primary concern is with the regulation and governance of AI systems to prevent potential harm that could arise from their misuse, including privacy breaches and discriminatory outcomes.

Second Additional Protocol to the Budapest Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence

The Second Additional Protocol to the Cybercrime Convention, also known as CETS No 224 (Second Protocol)[72], is an extension of the original Council of Europe Convention on Cybercrime (also known as the Budapest Convention)[73]. It was created to address the evolving challenges of cybercrime and enhance international cooperation and the exchange of electronic evidence. The Second Protocol streamlines the processes for obtaining electronic evidence by introducing mechanisms for direct cooperation with service providers and registrars in different countries, as well as by enhancing cooperation between the Parties to the Second Protocol.

One of the key aspects of the Second Protocol is its focus on improving international cooperation. The Second Protocol adapts the legal framework to technological advances and cybercrime methodologies, ensuring that the Budapest Convention remains relevant in the digital age.

The Second Protocol grants competent authorities[v] of States Parties several key powers, such as the ability to directly requesting domain name registration and to order the production of subscriber information and traffic data. It provides tools for extraordinary measures in cases of emergency and establishes procedures for video-conferencing in evidence gathering.

It is important to note that any measures listed in the Second Protocol are only obligatory for States Parties. In other words, requests and orders under the Second Protocol cannot be sent to countries that have not signed and ratified both the Budapest Convention and the Second Protocol (or to service providers and entities providing domain name registration services established therein).

The Second Protocol establishes a single

v In the Second Additional Protocol, a 'competent authority' refers to a judicial, administrative or other law enforcement authority that is empowered by domestic law to order, authorise or undertake the execution of measures under the Protocol for the purpose of collection or production of evidence with respect to specific criminal investigations or proceedings.

authority in each State Partythat will receive notifications for prior notification requests and maintains a register of these authorities. States Parties need to amend their legislation to allow their competent authorities to issue orders for subscriber and traffic data directed at service providers located abroad and empower domestically located service providers to answer to such orders from other countries.

Emergency disclosure requests can be issued through the 24/7 network established in accordance with Article 35 of the Budapest Convention, giving a clear description of the emergency facts. The requested Party can ask for written confirmation if an oral request is made. Parties can also issue emergency mutual assistance requests, providing proof of the emergency, and the requested Party must act as soon as possible. All parties must ensure that they have a 24/7 on-call service to receive and answer these requests.

The Second Protocol includes rules on access to data, addressing issues such as the languages used in international cooperation, requests for domain name registration information, production orders for subscriber information and traffic data and emergency mutual assistance. Other identified common challenges are not directly addressed.

The Second Protocol was opened for signature by the Parties to the Budapest Convention in May 2022 and will enter into force after being ratified by at least five Parties.

Clarifying Lawful Overseas Use of Data Act– CLOUD Act

The Cloud Act[74], also known as the Clarifying Lawful Overseas Use of Data Act, is a US federal law enacted in 2018. It was created to address the challenges caused by the global nature of cloud computing and digital information storage. The Cloud Act grants US law enforcement agencies access to electronic data held by US technology companies, regardless of where they are physically stored. The Cloud Act allows US authorities to request data stored abroad and establish agreements with foreign governments for reciprocal data sharing.

The main objective of the Cloud Act is to address the difficulties associated with accessing electronic information held by US-based global providers by foreign partners investigating serious crimes. It enables the US to enter into executive agreements with foreign partners, allowing access to electronic evidence regardless of its location, while protecting privacy and civil liberties. These agreements aim to reduce the burden on the MLA system.

The Cloud Act clarifies that US law requires cloud service providers subject to US jurisdiction to disclose data for valid US legal processes, regardless of where they are stored. This clarification restores the ability of the US to fulfil MLA requests and ensures compliance with international principles. It does not expand US investigative authority or provide new legal authority to acquire data.

Executive agreements under the Cloud Act are bilateral legal frameworks established between the US and foreign governments. These agreements allow law enforcement agencies from each country to directly request electronic data from service providers in the other country for the purposes of criminal investigations, bypassing the MLA procedure. The aim is to streamline cross-border access to data while ensuring that privacy and civil liberties are protected.

It is important to note that the Cloud Act simply clarified existing US law and did not change the existing standards for authorities to require disclosures of electronic data.

Negotiations between the EU and the US regarding an Executive Agreement under the Cloud Act began in September 2019. The aim of these discussions was to establish a framework for cross-border access to digital evidence in criminal matters. The key points of negotiation include addressing differences between EU and US perspectives, particularly concerning the agreement's scope and structure. So far no individual EU Member States or the EU itself have signed an executive agreement with the US.

Conclusions

This report makes clear that the realm of cybercrime is not static but an ever-evolving battleground where new challenges and solutions continually emerge. The report examined the persistent issues but also highlighted the proactive strides made through collaboration and legislative advancements aimed to strengthen the defences against cybercrime.

The integration of new legislative tools such as the e-Evidence Package and the Digital Services Act, and the ongoing adaptation of the AI Act and the Second Additional Protocol to the Budapest Convention, represent significant progress in equipping law enforcement and judicial authorities with the means to tackle the complexities of cybercrime more effectively. However, the real test lies in the practical application of these tools and the seamless integration into existing frameworks that will make them fully effective.

The report highlights critical areas such as the management of vast volumes of data, the challenges posed by anonymisation services, and the hurdles in international cooperation which underscore the necessity for robust, scalable solutions that can adapt to the dynamic nature of cyber-threats. The strategic move towards enhancing technical and operational capacities within law enforcement signifies a clear recognition of the need to keep pace with technological advancements.

Moreover, the increasing challenges of the unavailability of data during criminal investigations due to technological developments and lack of data retention, jurisdictional barriers, and the complications inherent in public-private partnerships call for a nuanced approach that balances stringent security measures with the preservation of individual privacy and civil liberties.

As we look to the future, the need for continuous innovation, training, and international collaboration is indisputable. It is through these concerted efforts that EU law enforcement and judicial authorities can aspire to not only manage the existing challenges but also pre-emptively counteract emerging threats. The path forward involves a collaborative framework between agencies such as Eurojust and Europol, along with their partners across borders, working as one to foster a safer cyber environment.

In conclusion, while significant strides have been made, the road ahead remains steep and fraught with challenges that will demand a dynamic and adaptive approach. The continued success of initiatives such as the SIRIUS Project, public-private partnerships such as the No More Ransom Project, and the strategic use of legislative tools will be pivotal in shaping the future landscape of cybercrime prevention and related enforcement. Through persistent efforts and a commitment to innovation and cooperation, EU law enforcement and judicial authorities can aim to not only mitigate the impact of cybercrime but also enhance the security and resilience of our digital world.

Endnotes

1 Europol & Eurojust, 'Common challenges in combating cybercrime, as identified by Eurojust and Europol', 2019, accessible at: https://www.eurojust.europa.eu/publication/common-challenges-combating-cybercrime-identified-eurojust-and-europol.

2 Europol, Eurojust, European Judicial Network, 'SIRIUS project, SIRIUS Cross-Border Access To Electronic Evidence', [last accessed on 8-10-2024], (https://www.europol.europa.eu/operations-services-innovation/sirius-project).

3 More information on the ICANN Registration Data Request Service is available on https://rdrs.icann.org/

4 ICANN, 'ICANN | GAC Governmental Advisory Committee Communique', March 2023, [last accessed on 8-10-2024], (https://gac.icann.org/advice/communiques/icann76-cancun-communique-es.pdf).

5 More information on DAP.LIVE available at https://dnsrf.org/docs/dap-live/introduction-to-dap-live/index.html.

6 More information on INTERPOL's pilot testing model https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Documents/INTERPOL_submission_to_AHC_2nd_international_cooperation.pdf.

7 For more information on the elimination of end user assignment from the RIPE database see https://www.ripe.net/participate/policies/proposals/2023-04.

8 Full text of NIS 2 directive available here: https://eur-lex.europa.eu/eli/dir/2022/2555.

9 For more information on ICANN goals for 2024, see https://www.icann.org/en/blogs/details/icann-interim-president-and-ceo-shares-goals-for-fiscal-year-2024-27-09-2023-en.

10 https://www.icann.org/en/blogs/details/icann-contracted-parties-set-to-vote-on-proposed-dns-abuse-amendments-05-10-2023-en.

11 https://www.eurojust.europa.eu/cybercrime-judicial-monitor.

12 For more information on the United Nations Cybercrime convention, see: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home.

13 For more information on the EU Innovation Hub for Internal Security see: https://www.europol.europa.eu/operations-services-innovation/innovation-lab/eu-innovation-hub-for-internal-security.

14 EU Innovation Hub for Internal Security, 'First Report on Encryption by the EU Innovation Hub for Internal Security', 2024, accessible at: https://www.europol.europa.eu/publications-events/publications/first-report-encryption).

15 Europol & Eurojust, 'First report of the observatory function on encryption', 2019, accessible at: https://www.europol.europa.eu/publications-events/publications/first-report-of-observatory-function-encryption.

16 Europol & Eurojust, 'Second report of the observatory function on encryption', 2020, accessible at: https://www.europol.europa.eu/publications-events/publications/second-report-of-observatory-function-encryption.

17 Europol & Eurojust, 'Third report of the observatory function on encryption', 2021, accessible at: https://www.europol.europa.eu/publications-events/publications/third-report-of-observatory-function-encryption.

18 Europol & Eurojust, 'First, Second and Third report of the observatory function on encryption', 2019, 2020, 2021, accessible at https://www.eurojust.europa.eu/publication/first-report-observatory-function-encryption, https://www.eurojust.europa.eu/publication/second-report-observatory-function-encryption, https://www.eurojust.europa.eu/publication/third-report-observatory-function-encryption.

19 Eurojust, 'Cybercrime Judicial Monitor', accessible at: https://www.eurojust.europa.eu/cybercrime-judicial-monitor.

20 Euronews, 'EncroChat: European authorities compromise phone network to arrest 'untouchable' criminals in sting', Jul 2020, [last accessed on 8-10-2024], (https://www.euronews.com/my-europe/2020/07/02/encrochat-european-authorities-compromise-phone-network-to-arrest-untouchable-criminals-in).

21 Europol, 'New major interventions to block encrypted communications of criminal networks, Europol Newsroom', March 2021, [last accessed on 8-10-2024], (https://www.europol.europa.eu/media-press/newsroom/news/new-major-interventions-to-block-encrypted-communications-of-criminal-networks).

22 Eurojust, 'New strike against encrypted criminal communications with dismantling of Exclu tool', February 2023, [last accessed on 8-10-2024], (https://www.eurojust.europa.eu/news/new-strike-against-encrypted-criminal-communications-dismantling-exclu-tool).

23 For more information on case C-670/22, please see: https://curia.europa.eu/juris/documents.jsf?num=C-670/22.

24 EU Innovation Hub for Internal Security, 'First Report on Encryption by the EU Innovation Hub for Internal Security', 2024, accessible at: https://www.europol.europa.eu/publications-events/publications/first-report-encryption).

25 Europol (2024), Position paper: Home routing and risks to lawful interception, available at: https://www.europol.europa.eu/publications-events/publications/position-paper-home-routing-and-risks-to-lawful-interception.

26 EU Innovation Hub for Internal Security, 'First Report on Encryption by the EU Innovation Hub for Internal Security', 2024, accessible at: https://www.europol.europa.eu/publications-events/publications/first-report-encryption).

27 EU Innovation Hub for Internal Security, 'First Report on Encryption by the EU Innovation Hub for Internal Security', 2024, accessible at: https://www.europol.europa.eu/publications-events/publications/first-report-encryption).

28 Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast)Text with EEA relevance, accessible at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018L1972.

29 EU Innovation Hub for Internal Security, 'First Report on Encryption by the EU Innovation Hub for Internal Security', 2024, accessible at: https://www.europol.europa.eu/publications-events/publications/first-report-encryption).

30 Europol, 'Internet Organised Crime Threat Assessment (IOCTA) 2024', 2024, accessible at https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024.

31 Europol, 'Bitzlato: senior management arrested', 2023, [last accessed on 8-10-2024] (https://www.europol.europa.eu/media-press/newsroom/news/bitzlato-senior-management-arrested).

32 European Parliament, 'Crypto-assets: green light to new rules for tracing transfers in the EU', April 2023 [last accessed on 8-10-2024], (https://www.europarl.europa.eu/news/en/press-room/20230414IPR80133/crypto-assets-green-light-to-new-rules-for-tracing-transfers-in-the-eu'.

33 European Parliament, 'Crypto-assets: green light to new rules for tracing transfers in the EU', April 2023 [last accessed on 8-10-2024], (https://www.europarl.europa.eu/news/en/press-room/20230414IPR80133/crypto-assets-green-light-to-new-rules-for-tracing-transfers-in-the-eu'.

34 Eurojust, 'Cybercrime Judicial Monitor', [last accessed on 8-10-2024], (https://www.eurojust.europa.eu/cybercrime-judicial-monitor).

35 Europol, Internet Organised Crime Threat Assessment (IOCTA) 2024, 2024, Publications Office of the European Union, Luxembourg, accessible at https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024.

36 Europol, 'Bitzlato: senior management arrested', 2023, [last accessed on 8-10-2024] (https://www.europol.europa.eu/media-press/newsroom/news/bitzlato-senior-management-arrested).

37 Europol, 'Coordinated action cuts off access to VPN service used by ransomware groups', 2021, [last accessed on 8-10-2024], (https://www.europol.europa.eu/media-press/newsroom/news/coordinated-action-cuts-access-to-vpn-service-used-ransomware-groups).

38 Europol, 2022, 'Unhappy New Year for cybercriminals as VPNLab.net goes offline', [last accessed on 8-10-2024], (https://www.europol.europa.eu/media-press/newsroom/news/unhappy-new-year-for-cybercriminals-vpnlabnet-goes-offline).

39 Decrypt, 'What Are Ordinals? A Beginner's Guide to Bitcoin NFTs', 2023, [last accessed on 8-10-2024], (https://decrypt.co/resources/what-are-ordinals-a-beginners-guide-to-bitcoin-nfts).

40 More information on the Interplanetary File System (IPFS), please see: https://ipfs.tech/.

41 Europol, 'Law enforcement disrupt world's biggest ransomware operation', 2024, [last accessed on 8-10-2024], (https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation).

42 Eurojust, 'Eurojust supports international operation against world's largest ransomware group', 2024, [last accessed on 8-10-2024], (https://www.eurojust.europa.eu/news/eurojust-supports-international-operation-against-worlds-largest-ransomware-group).

43 Europol, 'New measures issued against Lockbit', 2024, [last accessed on 8-10-2024]: (https://www.europol.europa.eu/media-press/newsroom/news/new-measures-issued-against-lockbit).

44 More information on the NoMoreRansom decryption tools, please see: https://www.nomoreransom.org/en/decryption-tools.html.

45 Europol, 'Law enforcement agencies across the EU prepare for major cross-border cyber-attacks', 2019, [last accessed on 8-10-2024], (https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-agencies-across-eu-prepare-for-major-cross-border-cyber-attacks).

46 More information on the NoMoreRansom, please see: https://www.nomoreransom.org/en/index.html.

47 More information on the NoMoreRansom, please see: https://www.nomoreransom.org/en/index.html.

48 More information on the NoMoreRansom, please see: https://www.nomoreransom.org/en/index.html.

49 More information on Cryptopol, please see: https://www.europol.europa.eu/media-press/newsroom/news/game-for-europol-and-centric and https://www.shu.ac.uk/news/all-articles/latest-news/security-innovation-awards.

50 More information on eFirst, please see: https://www.ecteg.eu/running/first-responders/.

51 Marsh, 'The French Interior Ministry's Orientation and Programming law (LOPMI)', April 2023, [last accessed on 8-10-2024], (https://www.marsh.com/fr/en/services/cyber-risk/insights/programming-law-lopmi-2023.html).

52 For more information on cybersecurity policies of the EU, please see: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies.

53 More information on the J-CAT, please see: https://www.europol.europa.eu/operations-services-and-innovation/services-support/joint-cybercrime-action-taskforce.

54 More information on the NoMoreRansom, please see: https://www.nomoreransom.org/en/index.html.

55 More information on the InterCOP, please see: https://www.europol.europa.eu/partners-collaboration/networks/intercop-international-cyber-offender-prevention-network.

56 Europol, 'Europol's amended Regulation enters into force', 2022, [last accessed on 8-10-2024], (https://www.europol.europa.eu/media-press/newsroom/news/europols-amended-regulation-enters-force).

57 Official Journal of the European Union, 'Regulation (EU) 2022/991of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation', 2022, [last accessed on 8-10-2024], (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R0991).

58 Official Journal of the European Union, 'Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation', 2022, [last accessed on 8-10-2024], (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R0991).

59 More information on EC3 partners, please see: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/ec3-partners.

60 More information on the Europol Platform for Experts (EPE), please see: https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/europol-platform-for-experts.

61 European Commission, '2023 Security Innovation Award: Promoting innovation that protects the security of EU citizens', 2023, [last accessed on 8-10-2024], (https://home-affairs.ec.europa.eu/news/2023-security-innovation-award-promoting-innovation-protects-security-eu-citizens-2023-11-09_en).

62 More information on the NoMoreRansom, please see: https://www.nomoreransom.org/en/index.html.

63 More information on the InterCOP, please see: https://www.europol.europa.eu/partners-collaboration/networks/intercop-international-cyber-offender-prevention-network.

64 European Union, 'Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings', 2023, [last accessed on 8-10-2024], https://eur-lex.europa.eu/eli/reg/2023/1543/oj.

65 European Union, 'Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings', 2023, [last accessed on 8-10-2024], https://eur-lex.europa.eu/eli/dir/2023/1544/oj.

66 European Judicial Network, 'EJN Fiches Belges on Electronic Evidence – National Legal and practical information provided by the Contact Points', 2024, [last accessed on 8-10-2024], https://www.ejn-crimjust.europa.eu/ejn2021/ContentDetail/EN/6/88.

67 And here: https://www.ejn-crimjust.europa.eu/ejn2021/Home/EN.

68 Eurojust, 'Cybercrime Judicial Monitor 8', 2023, [last accessed on 8-10-2024], https://www.eurojust.europa.eu/publication/cybercrime-judicial-monitor-issue-8.

69 See the video on the E-Evidence regulation here: https:/www.youtube.com/watch?v=HaODvpSGy-c.

70 European Commission, 'The Digital Services Act package', 2024, [last accessed on 8-10-2024], https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.

71 Find the updated list here: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413.

72 Please find more information on the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence here: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224.

73 Please find more information on the Budapest Convention and its protocols here: https://www.coe.int/en/web/cybercrime/the-budapest-convention.

74 Please find more information on the CLOUD Act here: https://www.congress.gov/bill/115th-congress/senate-bill/2383/text.