EUROPOL

EUROJUST

Common challenges in combating cybercrime

As identified by Eurojust and Europol

June 2019

JOINT REPORT
Europol and Eurojust Public Information

Contents

1 Objective and Background

The objective of this document is to identify and categorise the common challenges in combating cybercrime[1] from both a law enforcement and a judicial perspective. Eurojust and Europol's European Cybercrime Centre (EC3) have identified the challenges based on and informed by operational and practical experience, joint deliberations and expert input. Other sources used include final reports of several thematic and strategic meetings with national experts and relevant stakeholders, strategic reports and assessments such as Europol's EC3's Internet Organised Crime Threat Assessment (IOCTA), as well as various open sources. Despite the availability of information, both in- and external, on the obstacles, the discussion can certainly benefit from more extensive (and broader) research and a closer comparison of existing legislation at national and international levels.

The challenges identified fall into five main areas (*see also* Figure 1 below):

- loss of data;
- loss of location;
- challenges associated with national legal frameworks;
- obstacles to international cooperation; and
- challenges of public-private partnerships.

This document further examines some of the practical implications of these challenges.

In addition, this document lists some of the most relevant ongoing activities and open issues regarding each of the challenges identified. For this purpose, a short overview is given at the end of each chapter. **Additional information on some of the ongoing activities as well as some of the open issues can be found in the Annex**.

[1] For the purpose of this document, the term cybercrime is used in a broad sense and referencing Europol's and Eurojust's mandates, i.e. attacks on information systems (cyber-attacks), cyber-enabled crimes (such as non-cash payment frauds and various crimes related to child sexual exploitation online) and investigations in cyberspace, in the context of organised and serious cross-border criminality.

Figure 1: Common Challenges in Combating Cybercrime

This document identifies the evolving cyber threat landscape and resulting expertise gap as a cross-cutting challenge that impacts on all other categories identified herein. As cybercrime continues to evolve rapidly, at an unprecedented scale, volume and speed, current and expected future trends require an increasing and constantly adapting level of expertise from law enforcement and prosecution practitioners. Additionally, new cybercrime legislation should strive to be technologically neutral to the extent possible, to avoid the need for regular updates in the future or limiting investigative and prosecutorial possibilities.

The present assessment also allows Eurojust and Europol's EC3 to provide input to ongoing discussions with relevant stakeholders about possible approaches to address the observed challenges to combating cybercrime. Simultaneously, this document can also inform and complement existing initiatives and projects. Given the mandates of both Eurojust and Europol, these discussions should, *inter alia,* include the strengthening and further alignment of legal frameworks and practical instruments concerning mutual legal assistance and the (expedited) exchange of information and e-evidence for the purpose of investigation, prosecution, protection against and prevention of cybercrime. In any case, solutions to the observed challenges – be they legislative or practical in nature – should strike a fair balance between security and civil liberties, such as the right to privacy and the right to free speech.

This version of the document constitutes an update of the document of March 2017,[2] taking into consideration the pertinent developments since then. Previous versions of this document are herewith superseded.

[2] Council Document #7021/17, Europol Document #866212.

2 List of Common Challenges in Combating Cybercrime

2.1 Loss of Data

a) Data Retention

The overturning of the Data Retention Directive (DRD) by the European Court of Justice (CJEU) in its ruling of 8 April 2014[3] has left law enforcement and prosecutors uncertain about the possibilities to obtain data from private parties. In some European Union Member States (EU MS), legislation is still in place to ensure that Internet Service Providers (ISPs)[4] retain data for law enforcement purposes, whereas in other MS, national legislation has been annulled in the wake of the CJEU judgement. In those MS, ISPs retain some data for commercial or accounting purposes, but have no data available to specifically support criminal investigations. Such discrepancies impede the work of the cyber-competent authorities and may result in the loss of investigative leads and ultimately affect the ability to effectively prosecute criminal activity online. Additionally, the current situation creates unjust pressure on the investigating authorities to prioritise their operational activities in accordance with the different data retention frameworks currently in place, rather than focusing on the high-value targets. The CJEU's ruling of 21 December 2016 in the Tele2 Sverige and Watson cases[5] and the resulting requirements for targeted data retention and access criteria for competent authorities[6] have further exacerbated this problem.[7]

Since the Court's rulings, the lack of unified retention of electronic communication data across the EU has proven a key challenge to investigating cross-border cybercrime. The operational experiences of both agencies have shown that electronic communication data is the key to successful investigation and prosecution of serious crimes, including cybercrime. The absence of a unified data retention obligation is felt in all of the mandated cyber areas: cyber-attacks, online child sexual exploitation, transnational payment fraud, and criminality on the Dark Web. Comprehensive analyses performed by Eurojust,[8] and Europol's Data Protection Function[9] after the 2014 CJEU ruling, have underlined the value of electronic communication data for criminal investigations and prosecutions and have shown that the majority of law enforcement and judicial authorities in the MS would support a legislative framework at EU level.

The Justice and Home Affairs (JHA) Council meeting of December 2015[10] reiterated the need for an EU-wide approach to mitigate the fragmentation of the legal framework on data retention

[3] ECLI:EU:C:2014:238 (case C-293/12).
[4] In the context of the DRD Art. 1, Internet Service Providers (ISPs) is understood as 'providers of publicly available electronic communications services or of public communications networks'.
[5] ECLI:EU:C:2016:970 (case C-203/15 and C-698/15).
[6] Requirements of the Tele2 judgement regarding data retention (Council Document #11110/17), July 2017.
[7] Eurojust's *Cybercrime Judicial Monitor*, Issue 3, Dec 2017, 6/L/2017; Data Retention-State of play in the Member States (Council Document #WK 5206/2017), July 2017.
[8] Eurojust Document #13085/15.
[9] Europol Document #848769, developed on the basis of a survey to the EU MS and Eurojust's analysis (Eurojust Document #13085/15).
[10] Outcome of the Justice and Home Affairs Council meeting (Dec 2015), Council Document #14937/15, available at: https://www.consilium.europa.eu/en/meetings/jha/2015/12/03-04/.

across the EU and called for a new legislative initiative to be set forth. Given the cross-border nature of cybercriminal investigations, the majority of the MS stressed the importance of a common European approach.[11] The European Council also underlined the importance of the availability of data.[12] Europol's[13] and the General Secretariat of the Council's compilation of cases[14] further substantiates the practical needs of competent authorities related to the retention of communication data for the purposes of prevention and prosecution of crime.

Ongoing activities:

- Discussion of different options to address data retention matters by the Council Working Party DAPIX;
- Development of the concept of restricted data retention and targeted data access by Europol based on two expert workshops held at Europol in March and May 2018; and
- Monitoring by Eurojust and Europol of the impact on the practice of criminal investigations and prosecutions, including judicial cooperation, of the annulment of the Data Retention Directive as well as the CJEU's ruling in the Tele2 Sverige and Watson cases.

Open issues:

- Need for a new legislative framework regulating data retention for law enforcement purposes at EU-level.

b) Internet Governance-Related Challenges

Carrier-Grade Network Address Translation (CGN)

The challenge of the loss of data is also felt from the widespread implementation of Carrier Grade Network Address Translation (CGN) technologies by ISPs.[15] CGN technology has led to a serious online capability gap in law enforcement efforts to investigate and attribute crime.[16]

Given the exhaustion of IP addresses under Internet Protocol Version 4 (IPv4)[17], CGN technologies are used by ISPs to share one single public IPv4 address among multiple subscribers (end-users) at the same time (possibly several thousands) (*see* Figure 2 below).

[11] Ibid.
[12] European Council conclusions on security and defence (June 2017), available at: https://www.consilium.europa.eu/en/press/press-releases/2017/06/22/euco-security-defence/.
[13] Europol Document #892624.
[14] Retention of communication data – compilation of cases (Council Document #WK 5296/2017 INIT), May 2017.
[15] Carrier Grade NAT (CGN) is a technology that allows a single IP address to be shared by potentially thousands of subscribers/end-users on the same network simultaneously. CGN is used by 95% of mobile providers (network operators and mobile virtual network operators) and close to 50% of traditional Internet Service Providers (ISPs: cable, fibre and ADSL) worldwide.
[16] IOCTA 2017, available at: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017.
[17] Only 4 billion IPv4 addresses exist, and many more devices are connected to the internet.

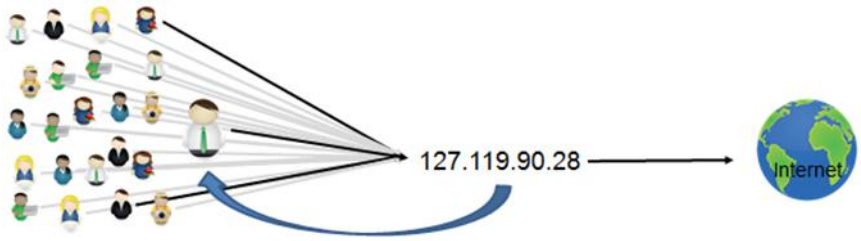

Figure 2 Carrier-Grade Network Address Translation (CGN)

For ISPs to be technically able to identify an end-user behind a CGN based on a public IPv4, law enforcement needs to provide them with an IPv4 address, the precise time of connection and the source port number[18]. Unfortunately, the source port number, which is essential to identify the subscriber, is typically not retained by Electronic Service Providers (ESPs), such as social media platforms, webmail services, hosting services, etc. In the absence of the source port number, ISPs cannot differentiate between end-users connected to the same ESP with the same shared IPv4 address at a given point in time. Cyber investigators are then confronted with lists of potentially hundreds or even thousands of end-users associated with a particular public IPv4 address, the investigation of which requires many resources, incurs long delays and generates privacy issues for many innocent customers. For these reasons, authorities may move to drop the case. Europol has documented many cases of investigations being delayed or severely hampered by CGN technologies in all EU MS, affecting every type of criminal investigation, from terrorism, cyber-dependent crime and fraud to child sexual exploitation online. In a recent child abuse case, only 25% of the members of a child abuse forum who did not hide their IP addresses could be identified directly by the ISP because of CGN, constituting less than 10% of the forum, which comprised 62 000 members actively involved in distributing and producing child abuse material.

The new Internet Protocol version 6 (IPv6), which offers a vast increase in the number of addresses, is the preferred long-term solution to the online crime attribution challenge related to CGN. However, time and resources are required to deploy IPv6 across the internet because it is not compatible with IPv4 and requires all network equipment to support it. This situation leads operators to develop transition mechanisms, such as CGN technologies, instead of investing in the IPv6 transition. Incentives for ISPs and ESPs to transition quickly to IPv6 are lacking.

Complementarity to the full transition to IPv6 is to bring about the routine logging of source port information at internet-facing servers (ESPs). The Internet Engineering Task Force (IETF) has published the results of a study that looks at the reasons why source port information is not routinely logged by internet-facing servers, and makes recommendations to help improve the situation.[19] Some experts argue that this issue could be solved with coordinated, distributed action by a large number of organisations to bring about the required change in standards.

Limiting the negative impact of CGN technology on criminal investigations calls for an open dialogue with ISPs and ESPs.[20]

[18] IETF Document RFC 6302 - June 2011.
[19] https://tools.ietf.org/html/draft-daveor-cgn-logging-04.
[20] IOCTA 2017(ibid.).

Ongoing activities:

- In 2017, EU MS included three specific action points to address the CGN challenge in the *Action Plan for the implementation of the 2017 EU strategy on building strong cybersecurity for the EU:*
    - EU MS should propose voluntary codes of conduct to ISPs to limit the number of subscribers behind each IPv4;
    - The European Commission should raise the issue of source port number logging with ESPs and especially with social media platforms within the framework of the EU Internet Forum; and
    - The European Commission should incentivize the private sector deployment of IPv6 in public procurements through the introduction of IPv6 requirements.

Open issues:

- These action points have not yet been implemented by the EU Member States and the European Commission; and
- In the short term, social media platforms should be encouraged to log source port numbers as part of their corporate social responsibility activities.

WHOIS

The WHOIS database is a publicly available and decentralised database of registration and contact information of the owners (registrants) of domain names (www.example.com). Registries (wholesalers of domain names) and registrars (retailers of domain names) have a contractual obligation with ICANN[21] to collect and publish online the information that is used to register domain names online in the WHOIS database.

The WHOIS database is an essential element of online accountability, as it is the only place on the internet on which one can find out who is responsible for a certain domain name and who is responsible for e-mails and websites that use this domain name[22]. These questions are the starting points of any investigation into a domain/DNS[23]-based crime.

Indeed, criminals need domain names to run almost any online criminal infrastructure. They need to register domains to launch phishing attacks, to spread malware, to send spam, to control botnets, to sell counterfeit goods or to spread terrorist propaganda and recruit online. Even though criminals might use fake or stolen identities to register domain names, these fake identifiers provide patterns that are invaluable for detecting and preventing internet crime and for identifying and locating victims.

[21] The Internet Corporation for Assigned Names and Numbers (ICANN) is a non-profit organisation that maintains and coordinates internet-critical resources, namely Internet Protocol (IP) addresses and the Domain Name System (DNS), without which the internet cannot function. ICANN also accredits domain registries and registrars.
[22] Name, telephone number, address and e-mail address of individuals and companies that register domain names (www.example.com).
[23] Domain Name System.

WHOIS information is also used by many public and private entities to protect consumers, critical infrastructure and intellectual property rights.[24] Therefore, if such key information is no longer directly available, the public interest and the rule of law online are significantly harmed, and efforts to address cybercrime and improve cybersecurity are undermined.

As of May 2018, the international law enforcement community lost direct access to WHOIS, after the ICANN Board adopted a Temporary Specification implementing ICANN's proposed GDPR Interim Compliance Model[25]. The Temporary Specification[26] mandates all registry operators and registrars to redact all personal data from publicly available WHOIS records. However, the document fails to provide a clear policy for access to non-public WHOIS data from third parties with a legitimate need (public task, public interest). Registries and registrars are only required to provide 'reasonable access' to personal data in registration data to third parties[27]. As a consequence, the Temporary Specification has created a fragmented system for providing access, consisting of potentially thousands of distinct policies, depending upon the registrar involved. This lack of consistent policies to access of non-public information causes delays in investigations and has serious operational consequences.

Under the temporary model, if investigators do not receive a satisfactory response to their request for disclosure, they need to initiate a formal legal process and issue mutual legal assistance requests to obtain WHOIS information.[28] This need comes with a substantial administrative burden as well as long delays, which may be much longer than the period for which the data in question is being retained. By the time formal procedures are concluded, the data may therefore no longer exist.

Ongoing activities:

- The ICANN-established expedited Policy Development Process (ePDP) is an attempt to develop a consensus-based policy to replace the Temporary Specification;
- Implementation is likely to be delayed, with prolongation of the Temporary Specification; and
- ePDP will not address disclosure of non-public data to LEA immediately.

Open issues:

- Issue of third-party access to non-public WHOIS information is highly controversial in the ICANN community; and
- Unlikely that the ICANN community will succeed in adopting a consensus policy on LEA access to non-public WHOIS information, leaving the law enforcement community without any alternative solutions.

[24] Cybersecurity investigators (CSIRT community, security and anti-virus companies, etc.), intellectual property rights holders (including trademark, patent or copyright owners), non-governmental public safety and health organisations (NCFTA, the Internet Watch Foundation, NCMEC, etc.) use WHOIS information.
[25] https://www.icann.org/en/system/files/files/gdpr-compliance-interim-model-08mar18-en.pdf.
[26] https://www.icann.org/resources/pages/gtld-registration-data-specs-en.
[27] *See* Appendix A Section 4 of the Temporary Specification.
[28] *See* the European Judicial Cybercrime Network (EJCN) statement on WHOIS database reform – 29 May 2018 Council Document #WK 6398/2018 INIT.

c) Encryption

Strong encryption is an essential element of our digitalised democracies, and helps to ensure the protection of our most fundamental human rights and the security of our digital economy. Nevertheless, the utility and effectiveness of these technologies also facilitates significant opportunities for criminals.

EU law enforcement authorities indicate that a significant and increasing percentage of cybercrime investigations involve the use of some form of encryption to hide relevant data and communications evidence. This is a cross-cutting challenge that affects all crime areas, including cybercrime, serious organised crime and terrorism.

A growing number of Electronic Service Providers implement encryption by default in their services. At the same time, tools that enable personal encryption and/or anonymisation of communications and other data are widely available and promoted. As a consequence, existing investigative techniques, such as the lawful interception of communication, are becoming less effective or even technically impossible. The increased implementation of encryption also negatively affects digital forensic analysis, leading to a situation in which criminals are able to effectively and indefinitely hide critical evidence and their illicit activities from law enforcement.

The increasing misuse of encryption and anonymisation tools by criminals to protect their communications or stored data, obfuscate their financial transactions and avoid detection was also recognised as a considerable challenge in the IOCTA assessments[29], leading to the loss of critical intelligence, attribution possibilities and evidence. The criminal use of Virtual Private Networks (VPNs), anonymising networks such as Tor, and the use of encryption to effectively and indefinitely hide critical evidence were particularly noted. Law enforcement has also observed the increasing misuse of and reliance by cybercriminals upon secure communication apps and channels providing end-to-end encryption.[30] The use of encryption is an established trend in all cybercrime areas and is indicative of a strong and increased operational security. Ransomware also demonstrates the 'active' abuse of encryption by criminals.

The observed strengthening and widening adoption of operational security measures such as the use of multi-layered encryption by cybercriminals, as well as other serious organised criminal groups and terrorists[31], create significant challenges for investigations. Child sex offenders, for example, are continuously and increasingly using online anonymity and

[29] IOCTA 2015, 2016, 2017, 2018, available at https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment.
[30] IOCTA 2017 (ibid.); Flashpoint (2017), Cybercrime Economy: An analysis of criminal communication strategies, available at https://www.flashpoint-intel.com/blog/cybercriminal-communication-strategies/.
[31] IOCTA 2016, 2017, 2018 (ibid.); TrendMicro, Dark Motives Online: An Analysis of Overlapping Technologies Used by Cybercriminals and Terrorist Organizations (2016) available at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/overlapping-technologies-cybercriminals-and-terrorist-organizations; Flashpoint, Tech for Jihad: Dissecting Jihadists' Digital Toolbox (2016), available at https://www.flashpoint-intel.com/wp-content/uploads/2016/08/TechForJihad.pdf.

encryption tools, including end-to-end encrypted apps,[32] to store and share material with lower risks of detection, a situation that poses a major challenge for the detection and removal of online child sexual exploitation material (CSEM).[33]

These developments have serious repercussions for cybercriminal investigations, as they interfere with the ability of law enforcement and judicial authorities to obtain the information needed as evidence and to prosecute and convict the criminals.[34]

No EU-wide legislation exists. In attempting to fill this gap, some MS have adopted legislative measures, such as compulsory disclosure provisions, to address the criminal abuse of encryption. Apart from the legal challenges, disclosing the data or circumventing the encryption is not always technically possible.

Ongoing activities:

- Implementation of measures presented in the European Commission's 11th and 13th Security Union Progress Reports, including:
  - an encryption observatory function provided by the European Cybercrime Centre at Europol, Eurojust and the European Judicial Cybercrime Network (EJCN) to assess relevant technical and legal developments; and
  - support for Europol to further develop its decryption capability.

Open issues:

- Providing law enforcement with the full set of tools, techniques and expertise needed to counter the criminal abuse of encryption.

d) Crypto-Currencies

The price increase of some of the most popular crypto-currencies skyrocketed at the end of 2017, attracting many investors who wanted to capitalise on future price growth. For Bitcoin, the number of transactions grew to more than 300 000 transactions per day. Unsurprisingly, given the fact that criminals are typically quick to exploit new opportunities, this growth, together with a wider adoption, also led to a growth in the use of crypto-currencies for illicit transactions. The widening criminal use of de-centralised crypto-currencies[35], combined with the increased misuse of tumbler/mixer services[36] and crypto-currency exchangers,[37] complicate the

[32] https://www.europol.europa.eu/newsroom/news/global-action-tackles-distribution-of-child-sexual-exploitation-images-whatsapp-39-arrested-so-far; https://www.europol.europa.eu/newsroom/news/eight-arrested-for-distribution-of-child-sexual-abuse-material-through-skype-and-darknet.
[33] IOCTA 2018 (ibid.).
[34] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20171018_eleventh_progress_report_towards_an_effective_and_genuine_security_union_en.pdf.
[35] Unlike centralised virtual currencies such as WebMoney and PerfectMoney, decentralised virtual currencies such as Bitcoin do not have a single administrating authority that controls the currency.
[36] A tumbler or a mixer is a service that attempts to break the links between the original and the final address by using several intermediary wallets. The service may also randomise transaction fees and add time delays to transactions.
[37] Crypto-currency exchangers are central hubs for the flow of crypto-currencies and are used to convert fiat money into crypto-currencies or vice versa; they also facilitate the conversion from one crypto-currency to another (e.g. Bitcoin to Monero).

possibilities for detection and asset recovery as well as the prevention of fraudulent transactions. The lack of (minimum) standards for due diligence and Know-Your-Customer (KYC) creates further challenges for cybercrime investigations.

Crypto-currencies continue to be exploited by cybercriminals, with Bitcoin being the currency of choice in criminal markets and as payment for cyber-related extortion attempts, such as ransomware and Distributed Denial of Service (DDoS) attacks.[38] Consequently, Bitcoin is the primary crypto-currency encountered by law enforcement in the context of criminal investigations.

While the abuse of Bitcoin remains one of the key enablers for cybercriminality on the internet (e.g. for purchasing or renting cybercrime tools/services), other more privacy-focused crypto-currencies, such as Monero, have been gaining popularity within the digital underground since 2017.[39]

Other recent trends include the increasing number of offenders using Bitcoin ATMs, the number of which is steadily growing.[40] On the other hand, the abuse of Bitcoin topped-up debit cards decreased significantly after access to anonymous cards was obstructed in early 2018. The latest developments indicate that legitimate crypto-currency users and companies are themselves increasingly becoming victims of cybercrime.[41]

In the reporting period, a growing number of cybercrime investigations involved crypto-currencies and blockchain analytics, indicative of the need to ensure that law enforcement and judicial authorities have the expertise, tools and legislative and regulatory means at their disposal to address the associated challenges. While knowledge of and experience in how to investigate, trace and seize crypto-currencies continues to grow in the law enforcement and judicial community, enhanced by various private sector tools for attribution, this knowledge is often limited to Bitcoin, and not to other crypto-currencies emerging in the criminal market. [42]

Ongoing activities:

- Established partnerships with crypto-currency exchangers and payment processors;
- Annual Virtual Currencies Conference;
- Crypto-currency guide for investigators;
- Best practice for contacting Virtual Currency Exchanges; and
- Due diligence and KYC regulation through Fifth Anti-Money Laundering (AML) Directive.

[38] IOCTA 2017, 2018 (ibid.).
[39] IOCTA 2017 (ibid.).
[40] https://coinatmradar.com/.
[41] IOCTA 2018 (ibid.).
[42] IOCTA 2017 (ibid.).

Open issues:

- Continuous effort needed to identify solutions for crypto-currency investigations;
- Law enforcement (LE) and judiciary must continue to develop, propagate and share knowledge to raise level of expertise;
- Continue to invest in relationships and trust with crypto-currency-related businesses;
- Increased usage of security measures by criminals complicate investigations and seizures; and
- Increased adoption of crypto-currencies leads to larger potential victim base.

2.2 Loss of Location

Recent trends, such as the increasing level of criminal misuse of encryption and/or anonymisation tools, crypto-currencies and the Dark Web[43], have also led to situations in which law enforcement may no longer (reasonably) establish the physical location of the perpetrator, the criminal infrastructure or electronic evidence. In these situations, the country with jurisdiction is often unclear, as well as the legal framework that regulates the (real time) collection of evidence or the use of special investigative powers, such as monitoring of criminal activities online and various undercover measures.

Moreover, the growing use of cloud-based storage and services means that data stored in the cloud could be physically located in different jurisdictions.

The loss of location may also result in uncertainty about the enforcement jurisdiction regarding procedural measures,[44] underlining the need for early involvement of judicial authorities through Eurojust, direct police-to-police channels for cooperation and communication facilitated by Europol, and continuous innovation in the process of operational collaboration.[45]

Ongoing activities:

- Negotiation of the European Commission's legislative proposal on e-evidence of 17 April 2018, including the clarification of the irrelevance of data storage location for disclosure and preservation obligations of service providers;
- Similar clarification by the Clarifying Lawful Overseas Use of Data Act (CLOUD Act); and
- Negotiation of a 2nd Protocol to the Council of Europe Budapest Convention, including solutions for trans-border access to data.

[43] According to the IOCTA 2015 and 2016, cybercriminals, such as child sex offenders and producers, make increasing use of the Darknet and other similar areas. The Darknet and other environments offering a high degree of anonymity are also increasingly hosting hidden services and marketplaces devoted to traditional types of crime, such as the drug trade, selling stolen goods, firearms, compromised credit card details, forged documents, fake IDs, and the trafficking of human beings.

[44] Due to the cross-border nature of online services, electronic evidence can be stored in a different location from the one in which the service is being provided; such situations result in challenges in defining which authority has competence for the investigatory measures – the one in which the service is provided or the one in which the data is physically stored.

[45] One example is the Joint Cybercrime Action Taskforce (J-CAT), which is hosted and supported by Europol.

Open issues:

- An international legal framework for direct cross-border access to data (including cloud storage).

2.3 Challenges Associated with National Legal Frameworks

Despite the existence of international legislative instruments, differences between domestic legal frameworks in the MS and international instruments often prove to be a serious impediment to international criminal investigation and prosecution of cybercrime, partly due to an incomplete transposition of international instruments into domestic legislation.

The main differences regard the criminalisation of conduct and provisions to investigate cybercrime and gather e-evidence. For example, different measures and penalties exist across the MS with regard to combating non-cash means of payment fraud. Adaptation and alignment of legal frameworks are often time-consuming and difficult, due to the rapid evolution of the cybercrime threat landscape. Case law (jurisprudence) can be a valuable tool to compensate for the lack of specific legislation, but, unfortunately, not much case law exists dealing with new developments (e.g. the criminal abuse of crypto-currencies, anonymisation tools and various technology-driven criminal *modi operandi*). Furthermore, existing operational processes (such as the mutual legal assistance (MLA) process) could benefit from better harmonising and streamlining. Equally, forensic-technical standards for the collection and transfer of e-evidence could be further developed, promoted and adopted.

The same situation applies to dedicated legislation that more specifically regulates law enforcement presence and action in an online environment. Such legislation should be harmonised at EU level, which would allow for more effective joint operational actions such as large-scale botnet and/or underground criminal forum takedowns. Specifically, possibilities to monitor criminal activities online and to lawfully collect critical evidence on the Deep Web and Dark Web could be harmonised across the EU to allow for effective operational activities and subsequent introduction of evidence in judicial proceedings.

This matter is of growing importance due to the increased operational security measures adopted by criminals on the Dark Web (e.g. two-factor authentication, encrypted messaging, multi-signature escrow, etc.) following successful operations, such as the takedown of Hansa and AlphaBay,[46] as well as RAMP in 2017.[47] Although the underground fora remain a vital part of the cybercriminal business model, a growing affinity among cybercriminals for modern chat services offering end-to-end encryption has also been observed.[48] This situation creates further obstacles for law enforcement to harness intelligence and further investigate such online crimes.

[46] https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.
[47] https://www.bleepingcomputer.com/news/security/russian-authorities-announce-takedown-of-ramp-dark-web-marketplace/.
[48] Flashpoint, Modern Chat Services and Cybercrime (2018), available at https://www.flashpoint-intel.com/blog/modern-chat-services-cybercrime/.

Ongoing activities:

- Legislative procedures at EU level, including common standards in certain areas (e-evidence and combating fraud and counterfeiting of non-cash means of payment);
- Adjustment of national legislation, e.g. by the US Cloud Act;
- Development of a Roadmap towards a Coordinated EU Law Enforcement Approach to Addressing Criminality on the Dark Web; and
- New Europol Dark Web team to provide operational support.

Open issues:

- The development of an EU-wide legal framework for conducting online investigations, specifically on the Deep Web and Dark Web.

2.4 Obstacles to International Cooperation

a) Mutual Legal Assistance (MLA)-Related Challenges

In an international context, no common legal framework exists for the *expedited sharing* of evidence (as does exist for the *preservation* of evidence). This situation means that, in practice, even though evidence is preserved, a long period of time may elapse before the evidence is available for the criminal investigation or judicial proceedings in the requesting country. However, the collection of electronic evidence is often a time-sensitive issue. The current process of MLA is perceived by practitioners as being too slow to gather and share electronic evidence effectively. The differences in legal systems and frameworks require early coordination and involvement of judicial authorities, with a clear need to streamline the MLA process wherever possible, for example by aligning and using existing model requests and a common taxonomy of cybercrime terminology. The use of the European Investigation Order (EIO) may go some way towards addressing these issues for the majority of MS. However, the EIO framework may not provide the speed that is required to capture electronic evidence. Moreover, the EIO Directive does not contain provisions that specifically facilitate the collection of common types of electronic evidence, meaning that additional tools need to be developed to facilitate the collection of electronic evidence under the EIO framework.

Simultaneously, the various existing legal tools and mechanisms could be better promoted at practitioner level.

A better mechanism for cross-border communication and the exchange of information for the purpose of investigation, prevention and protection is clearly needed, but also to ensure that any ensuing MLA request conforms to all the relevant legal requirements of the requested country. In this context, differentiation between data requests that need to follow the MLA process (e.g. content data) and requests that typically do not need to follow the MLA process, because effective alternatives exist (e.g. the possibility of directly requesting non-content data from US-based Electronic Service Providers) may be relevant. In other cases, cooperation in parallel investigations is a simple way to avoid multiple MLA requests. If this cooperation occurs within a joint investigation team (JIT), the authorities involved can exchange evidence and conduct cross-border investigative measures without the need for additional formal requests.

Furthermore, the current differences in legal frameworks and ineffective international cooperation may lead to the emergence of online criminal hot spots and (virtual) safe havens, in which criminal investigation and prosecution, as well as evidence collection, prove to be challenging.

Ongoing activities:

- Negotiation of the European Commission's legislative proposals on e-evidence of 17 April 2018, introducing new instruments for direct cross-border cooperation with service providers;
- Development of a secure online portal for the exchange of European Investigation Orders and e-evidence;
- Development by Europol in cooperation with Eurojust of the SIRIUS platform on best practice regarding the cross-border gathering of e-evidence;
- New concept for direct cross-border cooperation with US-based service providers regarding content data introduced by the US Cloud Act; and
- Drafting of a 2nd Additional Protocol to the Budapest Convention, including the streamlining and simplification of MLA requests.

Open issues:

- Completion of a consistent international legal framework for efficient cross-border cooperation.

b) Challenges in Responding to Large-Scale Cyber-Attacks

Large-scale cyber-attacks constitute a specific challenge to international cooperation. The extent to which incident-driven and reactive responses to major cyber-attacks are insufficient to address effectively the rapidly evolving cybercriminal *modi operandi* was underlined by WannaCry and NotPetya, two cross-border cyber-attacks of unprecedented scale that took place in 2017. A noteworthy component of these attacks was the wide variety of industries that were affected simultaneously, all located across divergent geographic regions and sectors, as well as the speed of the attacks. A combination of lack of digital hygiene and poor cybersecurity practice, facilitated by increased connectivity and hyper-convergence of networks, broadens the attack surface and the opportunities to commit large-scale cyber-attacks of extraordinary scale and scope.

WannaCry and NotPetya further underlined the challenges in providing a collective response to such major cyber-attacks and the duplication of efforts among the key actors in the EU cyber security ecosystem. Cognisant that attacks committed in the cyber domain can have serious repercussions in the physical world and can rapidly impact multiple countries worldwide has highlighted a pressing need for improved international cooperation, streamlining of activities, and clearly defined procedures with specific roles and responsibilities. Once developed, such procedures should be operationalised.

In light of the vital role that law enforcement and the judiciary play in investigating large-scale cyber security incidents or crises of a suspected malicious nature,[49] their early involvement in the planned response activities is fundamental. Their proactive participation in cyber-simulated exercises is also crucial, as such activity facilitates the trust and collaboration with the network and information security community.

Ongoing activities:

- Blueprint for coordinated response to large-scale cross-border cybersecurity incidents and crises;
- Framework for Joint EU Diplomatic Response to Malicious Cyber Activities;
- EU Law Enforcement Emergency Response Protocol (EU LE ERP); and
- Joint Memorandum of Understanding (MoU) between Europol, the European Union Agency for Network and Information Security (ENISA), the European Defence Agency (EDA), and the Computer Emergency Response Team for the EU Institutions, Agencies and Bodies (CERT-EU) was signed in 2018.

Open issues:

- Operationalising the Blueprint; and
- Ensuring the involvement of law enforcement and the judiciary in cyber-simulated exercises and emergency response.

2.5 Challenges of Public-Private Partnerships

a) Legal Framework

Cooperation with the private sector is vital in combating cybercrime. The private sector holds much of the evidence of cybercrime, and private party takedowns of criminal infrastructures, removal of illicit content and reporting of data breaches to law enforcement are among the most effective measures employed to fight cybercrime. Public-private partnerships also play a key role in mitigating cybercrime and increasing cybersecurity through prevention and awareness. However, little consensus exists on the legal framework that is required to facilitate effective and trust-based cooperation with the private sector,[50] while at the same time regulating legal and transparency issues surrounding that cooperation. Moreover, data protection regulation and fear of liability may result in limitations to cooperation with private industry.

A need has been demonstrated for standardised rules of engagement with private industry, as well as a clear understanding of the extent to which private parties can obtain evidence

[49] Electronic evidence-gathering and analysis, secure communication channels, existing 24/7 points of contact at national level, network of public and private partners of relevance, etc.
[50] For example, whether national legal measures are applicable to service providers offering a service in that country but based in another jurisdiction; the new rules stemming from the new EU Data Protection Regulation and Directive and their implementation, etc.

themselves and the legal implications of their actions, e.g. for the admissibility of such evidence in court proceedings.

Ongoing activities:

- Ongoing discussion regarding the ePrivacy Regulation and the impact on law enforcement and private sector activities to combat cybercrime; and
- New Communication on Tackling Illegal Content Online – Towards an Enhanced Responsibility of Online Platforms.

Open issues:

- Striking a legislative balance between privacy-related needs and proportionate measures to allow the private sector to continuously support law enforcement in the fight against cybercrime; and
- Clear and transparent rules on private parties' involvement in the gathering of evidence.

b) Jurisdiction

In an international context, establishing the proper jurisdiction to regulate the preservation and collection of evidence from Electronic Service Providers, which are often established in many different countries, is often difficult and time-consuming.

Law enforcement experts share the opinion that organised crime networks actively exploit existing jurisdictional boundaries in their criminal business models to avoid detection and prosecution. Due to the borderless nature of cybercrime, jurisdictional boundaries based on geographical borders could undermine the security of EU citizens or the digital single market (e.g. due to the proliferation of non-cash payment fraud).

Ongoing activities:

- Negotiation of the European Commission's legislative proposals on e-evidence, including an obligation for service providers offering services in the EU to designate legal representatives in the EU; and
- Proposal by the European Commission of a Directive on combating fraud and counterfeiting of non-cash means of payment, including common rules on jurisdiction.

Open issues:

- Enforcement of obligations of service providers, which are not established in the EU.

c) Challenges Associated with New and Emerging Technologies

Recent developments also show a growing need for regulation concerning the lack of security and privacy in design features of internet-facing devices (e.g. the emergence of Internet of Things botnets) and common cybersecurity rules at EU level for the consumer market[51].

As the criminal misuse of technology has become an engine of (cyber)crime,[52] the increasing volume and heterogeneity of the data intrinsic to today's law enforcement investigations has also brought about significant challenges in providing a timely and effective response. For example, the volume of seized media and material for forensic analysis obtained over the course of cybercriminal investigations could result in backlogs. Recent estimates indicate that the reported average volume of data per cyber investigation is now close to 3TB.[53] Particularly in the area of online child sexual exploitation, a typical case could include 1-10 million images and thousands of hours of video footage to be analysed as part of the criminal investigative process.[54]

We anticipate that these challenges will continue, especially as technology continues to develop. Particularly relevant with respect to encryption, for example, are developments in the area of quantum computing, artificial intelligence and 5G.[55]

Ongoing activities:

- Cybersecurity certification framework;
- European Cybersecurity Competence Network;
- eIDAS Regulation; and
- EU Communication on Artificial Intelligence for Europe.

Open issues:

- Further exploration and use of solutions offered by big data analytics; and
- Necessity for adaptive and increasing expertise, skills and tools in the area of digital forensics.

[53] *See* https://www.euractiv.com/section/innovation-industry/news/commission-plans-cybersecurity-rules-for-internet-connected-machines/.
[52] SOCTA 2017 (ibid.).
[53] IOCTA 2016 (ibid.).
[54] IOCTA 2017 (ibid.).
[55] For more information, please see https://www.europol.europa.eu/publications-documents/first-report-of-observatory-function-encryption.

3 Conclusion

With the increasing digitalisation of all parts of society, electronic evidence can be expected to replace classical forms of evidence as the basis for the investigation and prosecution of any kind of criminal conduct, meaning that the challenges listed above – though being of special relevance for combating cybercrime – go far beyond this area and have the potential to seriously impede criminal proceedings in general.

In addition, the update of the description of the challenges listed in this assessment also, more than ever, illustrates their rapidly increasing sophistication. Actors on both law enforcement and judicial levels try to keep pace by constantly stepping up specialised expertise. This specialisation, on the other hand, inevitably must go hand in hand with enhanced coordination and cooperation among all sides involved. Together with the borderless nature of cyberspace, the latter gives a key role to agencies such as Eurojust and Europol, as well as to platforms and networks dedicated to the sharing of knowledge and best practice[56].

This assessment also shows that a number of the legislative and practical measures addressing the identified challenges are making progress on both national and international levels. Nonetheless, the need for a comprehensive international legal and practical framework to address fundamental problems, such as access to cloud data and encryption, is more pressing than ever.

[56] E.g. the SIRIUS project developed by Europol and Eurojust and the increasing consolidation of formats such as the European Judicial Cybercrime Network (EJCN) and the European Cybercrime Taskforce (EUCTF).

4 Annex: Additional Information on Ongoing Activities and Open Issues

This Annex provides additional information on ongoing activities as well as open issues regarding each of the challenges identified in the main document. For ease of reference, the numbering in the Annex corresponds to the numbering of the chapters in the main document.

2.1. Loss of Data

a) Data Retention

Ongoing activities:

- Discussion of different options to address data retention matters by the Council Working Party DAPIX:

The developments in relation to data retention in the Member States are being closely monitored at EU level by the Council of the EU Working Party on Information Exchange and Data Protection (DAPIX)[57] group.

DAPIX was mandated to look into different options to address data retention matters. During the reporting period, the Working Party and the respective Presidencies held extensive expert discussions on the elements of the CJEU's rulings and possible ways forward, including a number of legislative and non-legislative options to tackle the issue.[58] The links with the draft e-Privacy Regulation were also examined, together with the Council Working Party on Telecommunications and Information Society (TELECOM).

- Development of the concept of restricted data retention and targeted data access by Europol based on two expert workshops held at Europol in March and May 2018:

The three main elements set forth regarding the new data retention regime for the purpose of prevention and prosecution of crime, including cybercrime, were (i) ensuring availability of the data, (ii) restricting the scope of the data retention framework, and (iii) setting out strong safeguards for access to retained data based on necessity and proportionality.

Europol actively supported the development of the concept of restricted data retention and targeted data access[59], which is in line with the criteria established by the Court, and takes into account law enforcement needs. The concept entails restriction on the type of data categories to be retained and higher safeguards with regard to the storage, access and use of the data with

[57] https://www.consilium.europa.eu/en/council-eu/preparatory-bodies/working-party-information-exchange-data-protection/.
[58] Data retention: Retention of electronic communication data – policy debate (Dec 2017), Council Document #14480/1/17.
[59] Europol Document #909633.

the ultimate goal of ensuring overall proportionality. Two expert workshops were held at Europol in March and May 2018, during which the proposed data matrix developed by Europol was discussed with the MS experts.

- Monitoring by Eurojust and Europol of the impact on the practice of criminal investigations and prosecutions, including judicial cooperation, of the annulment of the Data Retention Directive as well as the CJEU's ruling in the Tele2 Sverige and Watson cases.

Open issues:

- Need for a new legislative framework regulating data retention for law enforcement purposes at EU level.

Notably, the CJEU did not deem data retention to be non-compliant with fundamental rights. It highlighted that the fight against serious crime 'genuinely satisfies an objective of general interest', and can therefore also justify serious interference with the right to private life and data protection.[60]

In addition, in Ministerio Fiscal, the CJEU demonstrated that the right to data protection is not absolute. The Court clarified that criminal offences that are not particularly serious may justify access to personal data retained by providers of electronic communications services, provided that that access does not constitute a serious infringement of privacy.[61]

Legislators at EU level are therefore called upon to put forward a new legislative framework regulating data retention for law enforcement purposes.

b) Internet Governance-Related Challenges

Carrier-Grade Network Address Translation (CGN)

Ongoing activities:

- In 2017, EU MS included three specific action points to address the CGN challenge in the *Action Plan*[62] *for the implementation of the 2017 EU strategy on building strong cybersecurity for the EU*[63]:

Limiting the negative impact of CGN technology on criminal investigations calls for an open dialogue with the ISPs and with ESPs to identify feasible solutions.[64] The online crime attribution challenges associated with CGN technology were identified as a priority under the Estonian

60 http://curia.europa.eu/juris/document/document_print.jsf;jsessionid=9ea7d2dc30dd68a532a2a63a44efa183f62acdc79ea2.e34KaxiLc3qMb40Rch0SaxuQahj0?doclang=EN&text=&pageIndex=0&part=1&mode=DOC&docid=162437&occ=first&dir=&cid=531194.

61 http://curia.europa.eu/juris/document/document_print.jsf?docid=206332&text=&dir=&doclang=EN&part=1&occ=first&mode=lst&pageIndex=0&cid=280855.

62 Council Document #15748/17.

63 https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505294563214&uri=JOIN:2017:450:FIN.

64 IOCTA 2017 (ibid.).

Presidency in their efforts to improve the EU's fight against cybercrime.[65] An expert workshop was held in October 2017, facilitated by Europol and the European Commission's DG HOME, during which the MS experts agreed that coordinated action at EU level was needed.[66]

As a result, Member States included three action points to address the CGN challenge in the Action Plan[67] for the implementation of the 2017 EU strategy on building strong cybersecurity for the EU:[68]

- EU MS should propose voluntary codes of conduct to local ISPs providing internet access to limit the number of subscribers behind each IPv4. This voluntary approach has been successfully implemented in several EU MS, such as Belgium.
- The European Commission should raise the issue of source port number logging with Electronic Service Providers and especially with social media platforms within the framework of the EU Internet Forum.
- The European Commission should incentivise private sector deployment of IPv6 through the introduction of IPv6 requirements in public procurements.

Open issues:

- These action points have not yet been implemented by the EU Member States and the Commission.
- In the short term, social media platforms should be encouraged to log source port numbers as part of their corporate social responsibility activities.

WHOIS

Ongoing activities:

- ICANN established a new expedited Policy Development Process (ePDP) in June 2018, which includes, as part of its mandate, work on a standardised access model (i.e. not only for LEA but also for any other actors that have an alleged 'legitimate interest' in access to non-public WHOIS information, such as private cybersecurity companies and intellectual property rights holders);
- Implementation likely to be delayed, with prolongation of the Temporary Specification; and
- ePDP will not address disclosure of non-public data to LEA immediately.

Open issues:

- The issue of third-party access is very controversial in the ICANN community, and a compromise on LEA access is being held back because of the lack of consensus on access for private parties such as intellectual property rights holders.

[65] Council Document #11809/17.
[66] Council Document #13461/17.
[67] Council Document #15748/17.
[68] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505294563214&uri=JOIN:2017:450:FIN.

- The likelihood of the ICANN community adopting a consensus policy on LEA access to non-public WHOIS information is very small, leaving the law enforcement community without any alternative solutions.

c) Encryption

Ongoing activities:

- Implementation of measures presented in the European Commission's 11th and 13th Security Union Progress Reports, including:
  - an encryption observatory function provided by the European Cybercrime Centre at Europol, Eurojust and the European Judicial Cybercrime Network (EJCN) to assess relevant technical and legal developments; and
  - support for Europol to further develop its decryption capability.

Following the request by the JHA Council in December 2016 to present its view on the role of encryption in criminal investigations, the European Commission launched an expert consultation process to gather and analyse the necessary information from all stakeholder groups. The discussions were structured in two streams – a technical one (including Europol, the European Union Agency for Network and Information Security (ENISA), MS' law enforcement agencies, and industry partners) and a legal one (including Eurojust, the European Judicial Cybercrime Network (EJCN), the European Agency for Fundamental Rights (FRA), and civil society).

As a result, a set of common technical and legal measures was identified in 2017 to support law enforcement and judicial authorities to overcome the encryption challenges to criminal investigations and better protect EU citizens. In the 11th Security Union Progress Report, the Commission presented these measures:

1) support for Europol to further develop its decryption capability,

2) establishment of a network of points of expertise,

3) development of a toolbox of alternative investigation techniques for MS authorities,

4) improved and more structured collaboration and dialogue between authorities, service providers and other industry partners,

5) training programmes for law enforcement and judicial authorities, and

6) a continuous assessment of technical and legal aspects of the role of encryption in criminal investigations, which will include the establishment of an encryption observatory function to assess relevant technical and legal developments.

In the 13th Security Union Progress Report (January 2018)[69], the Commission committed to supplement Europol's budget by EUR 5 million to further develop its decryption capabilities for

[69] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20180124-progress-report-13-towards-effective-and-genuine-security-union.pdf.

data at rest in support of MS' investigations. The necessary activities are currently ongoing. The envisaged solution has the potential to substantially increase Europol's current decryption capability of data at rest.

The objective of the aforementioned observatory function is to continuously assess the technical and legal aspects of the role of encryption in criminal investigations. It has been set up in collaboration with EC3 at Europol, the EJCN and Eurojust. The function will deliver annual reports which will examine the landscape, including new and emerging trends and developments, and will highlight the challenges faced by law enforcement and judicial authorities with respect to encryption.

Open issues:

- Providing law enforcement with the full set of tools, techniques and expertise needed to counter the criminal abuse of encryption.

Encryption technology should not prevent law enforcement agencies from intervening in the lawful exercise of their functions in the public interest, for example in combating terrorism or fighting cybercrime.

Therefore, law enforcement needs to have the necessary tools, techniques and expertise to counter the criminal abuse of encryption.

Europol and Eurojust continue to support the relevant discussions at EU level in relation to the role of encryption in the context of criminal investigations, including lawful interception.

d) Crypto-currencies

Ongoing activities:

- Established partnerships with crypto-currency exchanges and payment processors:

In terms of practical measures, the crypto-currency service providers, such as exchanges and payment processors, have become key partners in investigating and prosecuting cybercrime, as the data they hold is valuable for the identification of suspects and the seizure of their criminal proceeds.

- Annual Virtual Currencies Conference, crypto-currency guide for investigators, best practice for contacting virtual currency exchangers:

Europol hosts the annual Virtual Currencies Conference[70], attended by both private sector and law enforcement representatives. In 2018, in addition to the crypto-currency guide for investigators, Europol also produced a list of best practice for contacting crypto-currency exchangers.[71] Europol also holds dedicated training workshops for law enforcement investigators under the EMPACT umbrella.

[70] https://www.europol.europa.eu/newsroom/news/cryptocurrency-meets-law-enforcement-europol%E2%80%99s-5th-virtual-currencies-conference.
[71] Intelligence Notification No 11/2018.

Regarding legislative measures, a wide variety of laws, guidance and regulation have been applied to the use of crypto-currencies such as Bitcoin over the last few years,[72] as well as different legal and policy measures surrounding crypto-currencies around the world.[73]

- Due diligence and KYC regulation through Fifth Anti-Money Laundering (AML) Directive:

Due diligence and KYC for crypto-currency-related service providers will be partially dealt with by the implementation of the 5th Anti-Money Laundering Directive (5th AMLD). [74]

Open issues:

- Continuous efforts needed to identify solutions for crypto-currency investigations:

As crypto-currencies continue to gain popularity among cybercriminals and several newer currencies are already establishing themselves on the criminal markets, continuous efforts are needed to identify solutions to investigating those emerging crypto-currencies that utilise additional obfuscation measures that further hamper lawful investigations and prosecutions.[75]

- Law enforcement and the judiciary must continue to develop, share and propagate knowledge on how to recognise, track, trace, seize and recover crypto-currency assets.
- Additionally, building trust-based relationships with any crypto-currency-related businesses operating in their jurisdiction could increase their capacity to effectively tackle issues raised by crypto-currencies during investigations.[76]
- The increasing levels of encryption in software wallets and growth of pin/password protected hardware wallets complicate seizures of funds originating from criminal activities.
- The acceptance of crypto-currencies by the general population increases the pool of non-expert crypto-currency users susceptible to theft of data and phishing.

2.2. Loss of Location

Ongoing activities:

- Negotiation of the European Commission's legislative proposal on e-evidence of 17 April 2018, including the clarification of the irrelevance of data storage location for disclosure and preservation obligations of service providers:

The European Commission's legislative proposal on e-evidence of 17 April 2018[77] clarifies that the location of data storage does not have any influence on the obligation of a service provider

[72] The Law of Bitcoin (2015), P. Anning et al.
[73] https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf.
[74] http://europa.eu/rapid/press-release_STATEMENT-18-3429_en.htm.
[75] IOCTA 2017 (ibid.).
[76] IOCTA 2017, 2018 (ibid.).
[77] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en (*see* Article 1 Nr. 1 of the proposed regulation).

offering services in the EU to disclose or preserve data based on the order of a competent authority.

- Similar clarification by the Clarifying Lawful Overseas Use of Data Act (CLOUD Act)[78]:

A similar clarification relating to orders addressed to US-based providers by US authorities can also be found in CLOUD Act[79], which came into force in the USA in March 2018.

- Negotiation of a 2nd Protocol to the Council of Europe Budapest Convention, including solutions for trans-border access to data:

Additionally, the Council of Europe's Cybercrime Convention Committee (T-CY) is searching for solutions to a broad range of issues related to the cross-border gathering of electronic evidence in the context of drafting a 2nd Protocol to the Council of Europe Budapest Convention.

Open issues:

- An international legal framework for direct cross-border access to data (including cloud storage):

The European Commission has included the question of how to improve the legal framework for direct cross-border access to data (including cloud storage) in the expert process based on the JHA Council conclusions of 9 June 2016 on improving criminal justice in cyberspace. However, the European Commission's legislative proposal on e-evidence of 17 April 2018[80] covers only cross-border cooperation with service providers and excludes the topic of direct cross-border access to e-evidence.

Further steps towards the development of an international legal framework for practitioners to build upon when investigating cybercrime across national borders or without certain knowledge of the location of the targeted evidence or perpetrators are still needed.

New binding and non-binding policy measures related to electronic evidence should take into consideration the needs of law enforcement and judicial authorities and should strive for a common approach to avoid fragmentation.

2.3. Challenges Associated with National Legal Frameworks

Ongoing activities:

- Adjustment of national legislation, e.g. by the Cloud Act:

[78] https://www.congress.gov/bill/115th-congress/house-bill/4943/text.
[79] Ibid.
[80] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en.

At this moment, several countries are changing and adapting their cybercrime legislation, with the above-mentioned Cloud Act (*see* 2.2 above and 2.4 below) being one example.

- Legislative procedures at EU level, including common standards in certain areas (e-evidence and combating fraud and counterfeiting of non-cash means of payment):

While legal conditions and safeguards for domestic cooperation with service providers vary widely between different MS, the European Commission's legislative proposal on e-evidence of 17 April 2018 would introduce a common standard for cross-border cooperation with service providers.

The European Commission has also set forth a proposal for an EU-wide Directive on combating fraud and counterfeiting of non-cash means of payment to replace the 2001 Council Framework Decision[81] and to address new developments and associated challenges to such investigations (including the differences in national legislation).

- Development of a Roadmap towards a Coordinated EU Law Enforcement Approach to Addressing Criminality on the Dark Web:

In the absence of a unified legal framework for conducting online investigations on the Dark Web, a Roadmap towards a Coordinated EU Law Enforcement Approach to Addressing Criminality on the Dark Web[82] was developed in 2017 by Europol's EC3 and the Estonian Presidency of the EU. The Roadmap facilitates the coordination and alignment of activities in Dark Web investigations and mitigates the challenges stemming from the different legal approaches in the area.

The Roadmap is being implemented within the new EU Policy Cycle and is in line with the newly adopted horizontal cross-crime strategic goal to address the illicit online trade in goods and services (including on the Dark Web).

- New Europol Dark Web team to provide operational support:

Europol, through the EC3, has been supporting the investigation of criminal marketplaces on the Dark Web for several years by sharing tools, tactics and techniques, and supporting major international operations. However, to enhance the response to these complex threats, a new dedicated Europol Dark Web team was officially formed in May 2018,[83] thereby employing a 360° strategy against criminality on the Dark Web (both cybercrime and cyber-facilitated organised crime such as the illicit online trade in drugs and firearms). The Dark Web team follows the approach of the Roadmap and works together with EU partners and law enforcement globally to reduce the size of the illegal underground economy by implementing different response measures in line with national capabilities and priorities in the field.

[81] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:0489:FIN.
[82] Council Document #15738/17.
[83] https://www.europol.europa.eu/newsroom/news/crime-dark-web-law-enforcement-coordination-only-cure.

Open issues:

- The development of an EU-wide legal framework for conducting online investigations, specifically on the Deep Web and Dark Web:

The development of an EU-wide legal framework for conducting online investigations, specifically on the Deep Web and Dark Web, could significantly improve law enforcement efforts in the area.

2.4. Obstacles to International Cooperation

a) Mutual Legal Assistance (MLA)-Related Challenges

Ongoing activities:

- Negotiation of the European Commission's legislative proposals on e-evidence of 17 April 2018, introducing new instruments for direct cross-border cooperation with service providers:

The negotiation of the European Commission's legislative proposals on e-evidence of 17 April 2018 has meanwhile advanced to a General Approach by the Council of the European Union on the draft Regulation on the European Production and Preservation Orders[84]. The envisaged new instruments have the potential to simplify and accelerate cross-border gathering of e-evidence held by service providers.

- Development of a secure online portal for the exchange of European Investigation Orders and e-evidence:

At the same time, the ongoing development of a secure online portal by the European Commission, in cooperation with Member States, for the exchange of both EIOs and electronic evidence between competent authorities of the Member States may lead to the creation of a tool to standardise and streamline cross-border cooperation within the EU.

- Development by Europol in cooperation with Eurojust of the SIRIUS platform on best practice regarding the cross-border gathering of e-evidence:

In 2017, the SIRIUS secure web platform[85] for competent authorities was launched to facilitate the exchange of best practice on electronic evidence-gathering and -handling, and to share tools to facilitate online investigations, among others.

- New concept for direct cross-border cooperation with US-based service providers regarding content data introduced by the CLOUD Act:

In parallel with developments in the EU, the USA adopted the CLOUD Act[86] in March 2018. One of the objectives of the CLOUD Act, among others, is to generate legal clarity with respect to

[84] https://data.consilium.europa.eu/doc/document/ST-15292-2018-INIT/en/pdf.
[85] https://www.europol.europa.eu/newsroom/news/europol-launches-sirius-platform-to-facilitate-online-investigations.

foreign requests addressed to US service providers for user data. The CLOUD Act addresses this issue by extending the permission for US providers to comply with foreign requests for user data also to content data, provided that the US government has entered into an executive agreement with the requesting country. The EU is currently developing its approach to future collaboration within this framework. The executive agreements under the CLOUD Act are considered to be bilateral instruments that allow differentiation to be made between EU MS. Three options are possible for MS:

- No agreement: the regular MLA process would continue
- Limited/tailor-made agreement subject to conditions
- Full agreement

- Drafting of a 2nd Additional Protocol to the Budapest Convention, including the streamlining and simplification of MLA requests:

On the level of the Council of Europe, a 2nd Protocol to the Cybercrime Convention is being drafted, which, among others, lays down provisions to improve the effectiveness of MLA between the various MS through the simplification of MLA requests for subscriber information, as well as cooperation between judicial authorities, issuing international production orders, joint investigation teams, requests in English and emergency MLA procedures. The Protocol is also balanced with safeguards for both data protection and trans-border access to data.

Open issues:

- Completion of a consistent international legal framework for efficient cross-border cooperation:

The effects of the new CLOUD Act on the practice of investigating cybercrime and gathering e-evidence must still be assessed. In addition, what remains unclear is how the concepts for direct cross-border cooperation with service providers underlying the US CLOUD Act, on the one hand, and the European Commission's legislative proposals on e-evidence, on the other hand, can be brought into harmony.

b) Challenges in Responding to Large-Scale Cyber-Attacks

Ongoing activities:

- Blueprint for Coordinated response to large-scale cross-border cybersecurity incidents and crises[87]:

Further to the 2017 EU Cyber Resilience, Deterrence and Defence Strategy,[88] the European Commission developed a Blueprint for Coordinated response to large-scale cross-border cybersecurity incidents and crises.[89]

[86] https://www.congress.gov/bill/115th-congress/house-bill/4943/text.
[87] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=EN.
[88] Ibid.
[89] Ibid.

- A Framework for Joint EU Diplomatic Response to Malicious Cyber Activities[90] was also adopted in 2017.
- EU Law Enforcement Emergency Response Protocol (EU LE ERP)[91]:

To complement these and other EU-level cyber crisis response mechanisms, an EU Law Enforcement Emergency Response Protocol (EU LE ERP) was developed in 2017-2018. Development was identified as a priority by the Estonian Presidency of the EU in 2017 to improve the overall preparedness and capability of law enforcement across the EU to effectively respond to cyber attacks like WannaCry and NotPetya. The objective of the EU LE ERP is to determine clear procedures for law enforcement agencies on the exchange of critical information and the overall coordination and de-confliction of actions in the immediate aftermath of large-scale cybersecurity incidents and crises of a suspected malicious nature.

The EU LE ERP was elaborated on the basis of two expert workshops held with MS' law enforcement experts and partner agencies in September 2017 and April 2018, discussions at meetings of the Standing Committee on Operational Cooperation on Internal Security (COSI) held between September 2017 and September 2018, as well as a written expert consultation process with the MS and partner agencies. The EU LE ERP has also been included within the EMPACT Priority on Attacks Against Information Systems. The EU LE ERP was recognised as one of the main mechanisms for providing an EU-wide coordinated response to large-scale cybersecurity incidents and crises.[92]

- Joint Memorandum of Understanding (MoU) between Europol, the European Union Agency for Network and Information Security (ENISA), the European Defence Agency (EDA), and the Computer Emergency Response Team for the EU Institutions, Agencies and Bodies (CERT-EU), signed in 2018:

A joint MoU between Europol, ENISA, EDA and CERT-EU was signed in 2018 to enhance cooperation on this and other key topics.[93]

Open issues:

- Operationalising the Blueprint.
- Ensuring the involvement of law enforcement and the judiciary in cyber-simulated exercises and early involvement in crisis response.

[90] https://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/.
[91] Council Document #10086/18.
[92] Ibid.
[93] https://www.europol.europa.eu/newsroom/news/four-eu-cybersecurity-organisations-enhance-cooperation.

2.5. Challenges of Public-Private Partnerships

a) Legal Framework

Ongoing activities:

- Ongoing discussion regarding the ePrivacy Regulation and the impact on law enforcement and private sector activities to combat cybercrime:

For instance, the EU is currently in the final stage of adopting new rules to strengthen the respect for private life and the protection of personal data in electronic communications within the framework of the new ePrivacy Regulation.[94] While the objective of the new provisions is to guarantee essential confidentiality of communications, the law enforcement community is concerned that, as presently worded, some of the provisions may also adversely impact activities undertaken by Electronic Service Providers, private security companies and cybersecurity researchers and other important stakeholders that play an indispensable role in investigating, disrupting, preventing and mitigating malicious cyber incidents and cybercrimes such as illegal distribution of online child sexual exploitation materials.

- New Communication on Tackling Illegal Content Online – Towards an Enhanced Responsibility of Online Platforms[95]:

The European Commission's recent Communication on Tackling Illegal Content Online – Towards an Enhanced Responsibility of Online Platforms[96] sets forth guidelines and principles for online platforms, particularly to step up the fight against illegal content online (such as online child sexual exploitation material) in cooperation with MS' competent authorities.

Open issues:

- Striking a legislative balance between privacy-related needs and proportionate measures to allow the private sector to continuously support law enforcement in the fight against cybercrime:

New legislative proposals should balance the privacy-related needs with proportionate measures to allow the private sector to continuously support law enforcement in the fight against cybercrime by facilitating the detection and investigation of various forms of cybercrime.

- Clear and transparent rules on private parties' involvement in the gathering of evidence.

[94] https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation.
[95] https://ec.europa.eu/digital-single-market/en/news/communication-tackling-illegal-content-online-towards-enhanced-responsibility-online-platforms.
[96] Ibid.

b) Jurisdiction

Ongoing activities:

- Negotiation of the European Commission's legislative proposals on e-evidence, including an obligation for service providers offering services in the EU to designate legal representatives in the EU:

In its legislative proposal on e-evidence of 17 April 2018, the European Commission included an obligation for service providers who offer services in the EU to designate certain legal representatives to gain more certainty on where exactly to send data requests, which are addressed to service providers that often have complex corporate structures or are established outside the EU.

- Proposal by the European Commission of a Directive on combating fraud and counterfeiting of non-cash means of payment, including common rules on jurisdiction:

The new legislative proposal for a Directive on combating fraud and counterfeiting of non-cash means of payment could facilitate the handling of jurisdictional challenges to international payment fraud investigations.

Open issues:

- Enforcement of obligations of service providers, which are not established in the EU:

No solution has been found for the efficient enforcement of obligations for legal representation in the EU of service providers offering services in the EU, when these service providers are not established in the EU. Such obligations would eventually need to be enforced in third States and would therefore still need to rely on traditional cooperation procedures.

c) Challenges Associated with New and Emerging Technologies

Ongoing activities:

- Cybersecurity certification framework and European Cybersecurity Competence Network:

The current efforts at EU level regarding a cybersecurity certification framework and a European Cybersecurity Competence Network and Centre[97] could add value in addressing some of these challenges and staying abreast of the technological developments and their implications for the cybercriminal investigative process.

- eIDAS Regulation:

[97] https://ec.europa.eu/digital-single-market/en/proposal-european-cybersecurity-competence-network-and-centre.

The EU-wide legislation on electronic identification (eIDAS Regulation)[98] enables cross-border recognition of electronic IDs and promotes innovative authentication services (such as seals or time stamps). As such, its successful implementation could help to safeguard cross-border internet shopping and prevent certain forms of e-commerce fraud and phishing.[99]

- In 2017, Europol called for the adoption of the Cyber-investigation Analysis Standard Expression (CASE) as a standard digital forensic format.

- In April 2018, the EU also set forth the new Communication on Artificial Intelligence for Europe[100], along with a series of measures in the field, including ensuring an appropriate ethical and legal framework.

Open issues:

- Further exploration and use of solutions offered by big data analytics opportunities:

The opportunities for big data analytics solutions to support the cybercriminal investigative process should be further exploited. The new big data-driven tools or solutions for combating cybercrime should take into consideration the specific needs of the law enforcement community to overcome challenges.

- Necessity for adaptive and increasing expertise, skills and tools in the area of digital forensics:

For law enforcement, new and emerging technologies pose technical and investigative challenges, e.g. in terms of digital forensics. These challenges call for an increasing and constantly adapting level of expertise, skills and adequate tool support for law enforcement and judicial practitioners.

[98] https://ec.europa.eu/digital-single-market/en/news/cross-border-digital-identification-eu-countries-major-step-trusted-digital-single-market.
[99] https://ec.europa.eu/digital-single-market/trust-services-and-eid.
[100] http://europa.eu/rapid/press-release_IP-18-3362_en.htm.