ENCRYPTION AS A CHALLENGE FOR EUROPEAN LAW ENFORCEMENT AGENCIES

Milana Pisarić, PhD[1]
Faculty of Law, University of Novi Sad, Serbia

Abstract: Strong encryption is of great importance to digital economy and digital privacy. At the same time the use of encryption by criminals was recognized by *Europol and national law enforcement authorities* as a significant challenge for *detection and investigation* of cybercrime and cyber-facilitated crime, rendering traditional investigative techniques ineffective. Since encryption is continuously depriving law enforcement of evidential opportunities, EU member states started to demand a European solution to questions around encryption as a threat to security in Europe. However, there are many political inconsistencies among EU institutions and member states on encryption. The aim of this paperwork is to present and analyze the current state of legal and practical implications of criminal use of encryption and to consider alternative approaches, mainly those aimed to enhance the law enforcement agencies' decryption capabilities of lawfully obtained encrypted data in criminal investigations.

Keywords: encryption, cybercrime, law enforcement, European Union.

INTRODUCTION

Although no one can deny the importance of strong encryption for digital economy and digital privacy, it is a fact that legitimate anonymity and encryption services and tools are being misused for criminal activity. The more and more common use of encryption by offenders to protect their communications or stored data poses a serious challenge for detection and investigation of crime, denying law enforcement the access to electronic evidence. This challenge is not present only in cybercrime investigation, but in investigation of all criminal offences which are enabled by information technologies whose traces may be found in digital devices or whose offenders use these technologies to communicate and conceal their identity and/or location. Because of that many traditional investigative techniques and digital forensic analysis are used not in their full potential or even ineffectively. These issues are recog-

1 mpisaric@pf.uns.ac.rs

nized as a major problem by national law enforcement agencies (LEA) of Member States (MS) and by key stakeholders in fight against cybercrime, organized crime and terrorism in European Union (EU). As the commercial use of strong encryption technology has been on the increase since 2014 and the use of encryption by criminals was recognized by Europol and national LEA as a significant challenge for detection, investigation, and prosecution of all areas of cyber-facilitated crime with cross-border dimension, depriving law enforcement of evidential opportunities, EU has debated how to regulate encryption in order to tackle this "Going dark" problem. The fundamental policy question involving encryption is how to balance competing values: how to promote privacy and spur economic growth and at the same time find proper tools for crime prevention and investigation which are tackled by destructive consequences of encryption misuse. The aim of this paper is to present and analyze the current state of encryption debate and possible legal and technical solutions for it at the EU level.

ENCRYPTION AS AN OBSTACLE IN CRIMINAL INVESTIGATION

Since 2016 the ability of LEA to access the data needed to conduct criminal investigations has been recognized as an increasing challenge, as a result of the enhanced use of encryption.

In September 2016, the Council asked MS to provide answers in a questionnaire in order to map the situation and identify the obstacles faced by LEA when gathering or securing encrypted evidence for the purposes of criminal proceedings (Council of the European Union (2016a). Replies revealed that in the majority of MS encryption is encountered often or almost always in the context of criminal investigations, and this experience is present both with regard to online (in the form of encrypted emails or other forms of e-communication and/or commercial applications such as Facebook, Skype, WhatsApp or Telegram) and offline encryption (most often criminal investigation involving encrypted digital devices and encrypting applications). While national legal framework aimed at securing e-evidence when encrypted is considered sufficiently effective, the main problem is of technical nature: the lack of sufficient technical capacity, in terms of efficient technical solutions to decrypt and respective equipment, is among the top three challenges followed by the lack of sufficient financial resources and personal capacity, in terms of numbers and training of staff.

In 2016 Europol in its Internet Organized Crime Threat Assessment (IOCTA) pointed to encryption as a key threat and serious impediment to the detection, investigation, and prosecution of criminal activity (Europol, 2016a: 50). Twenty European countries reported the use of encrypting software by cybercriminals to protect their stored data, while eight MS specifically stated that dealing with encryption is a major challenge to investigating cybercrime. It was noticed that encryption is no longer restricted to desktop computers, but it is being used on mobile devices. Furthermore, almost half of MS indicated that their investigations involved the use of some form of encrypted communications, such as WhatsApp and Viber, which introduced encryption by default, by way of end-to-end encryption, making communication hard to intercept.

A combination of legislative and technical factors, which deny LEA access to timely and accurate electronic communications data and digital forensic opportunities, such as lack of data retention and encryption, were recognized in IOCTA 2017 as leading to a loss of both investigative leads and the ability to effectively attribute and prosecute online criminal activity (Europol, 2017a: 13). While the implementation of the European Investigation Order was expected to simplify cooperation between judicial authorities and expediting investigations, existing legal frameworks and operational processes

need to be further harmonized and streamlined for dealing with cross-border e-evidence. Such measures, as well as the parallel EU policy processes on encryption, data retention and internet governance challenges, should thoroughly consider the specific law enforcement needs and strive for practical and proportionate solutions to empower innovative, efficient and effective approaches to conducting lawful cybercrime investigations. The growing prevalence and sophistication of cybercrime requires dedicated legislation that more specifically enables law enforcement presence and action in an online environment (Europol, 2017a: 17).

Communication and storage applications and devices increasingly come with encryption by default, which along with data protection and privacy issues, means that law enforcement can increasingly be denied access to the relevant data it needs to locate and identify offenders and to secure evidence (Europol, 2017a: 41). LEA highlighted the difficulties posed by encrypted communication apps and software, and the use of encryption to effectively and indefinitely hide critical evidence, applicable across all aspects of cybercrime (Europol, 2017a: 63).

Owing to the expansion of Internet enabled mobile devices, the wide diversity of platforms and services used, the easy availability of online anonymity and encryption tools and the growing use of the Darknet, it became easier for offenders to store and share material with lower risks of detection, especially in connection with online Child Sexual Exploitation Material (CSEM) (Europol, 2018a: 9) and ransomware (Europol, 2018a: 26).

In June 2019, Europol and Eurojust issued assessment on the common challenges in combatting cybercrime. It is noted that encryption is more and more a cross-cutting challenge that affects all crime areas, including cybercrime, serious organized crime and terrorism. EU LEA 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. Since growing number of electronic service providers implement encryption by default in their services, law enforcement has also observed the increasing misuse of and reliance by cybercriminals upon secure communication apps and channels providing end-to-end encryption, leading to that i*nvestigative techniques*, such as lawful interception, *are becoming increasingly* less effective or even technically impossible (Europol, Eurojust 2019a:10). The increased implementation of encryption also negatively affects digital forensic analysis. Apart from the legal challenges, disclosing the data or circumventing the encryption is not always technically possible. This assessment however concludes with that although a number of the legislative and practical measures addressing the identified challenges are making progress on both national and international levels, 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 (Europol, Eurojust 2019a: 20).

The criminal abuse of encryption technologies, whether it be anonymization via VPNs or Tor, encrypted communications or the obfuscation of digital evidence (especially in cases of CSEM) is represented as a significant threat highlighted by respondents to 2019 survey (Europol, 2019a: 56-57). However, inaccessibility of relevant data also comes due to legislative barriers or shortcomings, which we must overcome to enhance cross-border access to electronic evidence and the effectiveness of public-private cooperation through facilitated information exchange (Europol, 2019a: 7). As criminals adapt, law enforcement and legislators must also innovate in order to stay ahead, and seek to capitalize on new and developing technologies. To do so, however, law enforcement needs the knowledge, tools and legislation required to do so quickly and effectively. This is also recognized as the main direction of EU policy on encryption.

EU POSITION ON ENCRYPTION

Although since 2016 the encryption has globally been considered as a major obstacle for criminal investigation, opposite to Five eyes countries commitment to legislating backdoors (Five Country Ministerial 2018), there is a clear opposition to this approach in the EU.

Europol and ENISA agreed that built-in backdoors to encryption do not provide a secure fix to police frustrations. The directors of the two agencies said that while [backdoors] would give investigators lawful access in the event of serious crimes or terrorist threats, it would also increase the attack surface for malicious abuse, which consequently would have much wider implications for society (Europol, ENISA 2016). As both France and Germany suffered terrorist attacks throughout 2015/2016, including attack in Paris in November 2015 and in Nice in July 2016, at the meeting of French and German interior ministers on August 23rd 2016, they called for feasible solutions to decryption, but without weakening the protective mechanisms, both in legislation and through continuous technical evolution that would afford security agencies the ability to access encrypted data and enable courts to demand that Internet companies decrypt data to help further criminal investigations (Tech Crunch (2016, August 24). In December 2016, ENISA issued opinion in which it recognized requests of law enforcement for creating means to circumvent encryption as protection measures as legitimate, but also stressed out that limiting the use of cryptographic tools would create vulnerabilities that can in turn be used by terrorists and criminals, and lower trust in electronic services, which would eventually damage industry and civil society in the EU (ENISA 2016, 16).

Because all MS, except five of them, favored the need for practically orientated measures (more resources and tools) prevailed over the need for adoption of new anti-crypto legislation at the EU level, the Council endorsed the four-steps approach as basis for the future work in this regard: A. Launch of a reflection process on the challenges faced by criminal justice in relation to the use of encryption with the purpose to define practical solutions that would allow the possible disclosure of encrypted data/devices through an integrated EU approach and framework; B. Explore possibilities for improving the technical expertise both at the national and EU level to face current and future challenges stemming from encryption; C. Encourage the members of the European Judicial Cybercrime Network to bring to its forum for discussion, exchange of information, good practices and expertise also the practical/operational aspects related to encryption; D. Deepen the practical/operational aspects of the encryption-related trainings for LEA provided by EU entities and increase the capacity building efforts (Council of the European Union, 2016b).

In the Resolution passed in early October 2017, the European Parliament explicitly asked MS to refrain from enforcing measures that may weaken the networks or services that encryption providers offer. The Resolution stressed that feasible solutions must be offered, via both legislation and continuous technological evolution, in aligning the conditions for the lawful use of investigative tools online (European Parliament 2017).

Besides, the Cybersecurity strategy (European Commission 2017a) recognized encryption as a vital tool for the protection of personal data and fundamental rights, the Commission adopted on 18 October 2017 its position on encryption used by criminals, embedding it in its anti-terrorism package in the Eleventh progress report towards an effective and genuine Security Union (European Commission 2017b). The Commission set out a package of anti-terrorism measures including measures to support law enforcement and judicial authorities when they encounter the use of encryption by criminals in criminal investigations. These includes (a) legal measures to facilitate access to encrypted evidence, and (b) technical measures to enhance decryption capabilities. As for the legal measure,

creation of appropriate legal framework for cross-border access to electronic evidence that would overcome challenge of cross-border access to electronic evidence located in another country was announced. Technical measures do not mean prohibiting, limiting or weakening encryption. Instead of that 1) the Commission will support Europol to further develop its decryption capability; 2) a network of points of expertise should be established, with Europol as a network hub to facilitate collaboration among them; 3) MS authorities should have a toolbox of alternative investigation techniques at their disposal to facilitate the development and use of measures to obtain needed information encrypted by criminals, and the European Cybercrime Centre (EC3) at Europol should be the best-placed to set up and keep a repository of those techniques and tools; 4) the attention should be paid to the important role of service providers and other industry partners in providing solutions with strong encryption; 5) training programs for law enforcement and judicial authorities should ensure that responsible officers are better prepared to obtain necessary information encrypted by criminals; 6) the Commission will support the development of an observatory function in collaboration with the EC3 at Europol, the European Judicial Cybercrime Centre (EJCN) and Eurojust. So, instead of legislating backdoors, the Commission appears to be exploring alternative approaches, including investing in decryption. Although the Commission opted for non-legislative approach by building on Europol's existing toolbox of decryption capabilities, because these technical measures could mean anything, they could highlight the shortcomings of current laws and policies and thus fail to safeguard encryption in the longer term, leaving the door open to future legislation toward the so-called backdoors for LEA to access private data.

The Commission proposed to fund and develop means to break encryption without prohibiting, limiting or weakening encryption, but workarounds applied in achieving this goal could pose a legal challenge, especially if it is in a form of government hacking developed and used without an adequate legal framework and often without respect for national or international human rights safeguards. Since the current debate about encryption has become too polarized, with tech companies unnecessarily framing the issue as a zero-sum game, in which any tool that provides lawful access to law enforcement will necessarily compromise user privacy, the EU advocates targeted approaches to the development of new investigative tools that are proportionate to the crime that was committed. This approach is consistent with the Commission's prior commitment to research functional encryption: technologies that would change the way data is encrypted in the first place to allow law enforcement to gain selective access to data in certain circumstances, instead of granting all or nothing law enforcement access to a device (European Commission 2019). In other words, the aim is to come up with a solution that could be later implemented by service providers and device manufacturers so that all three sides of the "Going dark" debate (the user, the provider and the government) are satisfied.[2]

ROLE OF EUROPOL

The current non-legislative approach to encryption in EU is focused on enhancing the technical capabilities already available within Europol and encouraging their use by MS in the respective limits of its mandate, as well as the further developing of Europol as European Centre of expertise on encryption.

2 For instance, EU will contribute over EUR 4.2 million to FENTEC project developing "functional encryption" ("FE") technology. FE has recently been introduced as a new paradigm of encryption systems with the aim to overcome all-or-nothing limitations of classical encryption. In an FE system the decryptor deciphers a function over the message plaintext: such functional decryptability makes it feasible to process encrypted data (e.g. on the Internet) and obtain a partial view of the message plaintext. These systems would effectively encrypt private messages and data and at the same time they would allow law enforcement to obtain a partial view of the message plaintext.

As concluded in Report in 2017 that most MS do not have access to the right level of expertise and technical resources, which seriously challenges law enforcement and judicial authorities' ability to access encrypted information in criminal investigations, the Commission has supported Europol ever since to further develop its decryption capability.

Since 2014, Europol has been offering Member States support in decrypting data carriers or mobile phones. The unit is based at the EC3. EC3 provides operational capabilities, such as advanced digital forensic, technology tools and platforms. According to Consolidated Annual Activity Reports (CAAR), this decryption platform was so far used on 35 occasions during 2014 with no indication of successful results (CAAR 2014, 15), [3] on 26 occasions during 2016 with no indication of successful results (Europol 2016b: 30), during 2017 it was used on 28 occasions achieving successful results 9 times (Europol, 2017b: 30), during 2018 on 32 occasions achieving successful results 12 times (Europol, 2018 b: 38), and on 59 occasions during 2019 with a 39% successful decryption rate (Europol, 2019b: 28).

Additional resources were provided for Europol to enable its EC3 support to MS to address challenges related to encryption in criminal investigations.[4] While in the Report from December 2017 (European Commission (2017c), the Commission stressed that the assessment of the specific needs for additional resources was ongoing, in January 2018 the Commission declared it would amend the 2018 Europol budget with an additional EUR 5 million to reinforce Europol's capabilities to decrypt information lawfully obtained in criminal investigations (European Commission, 2018).[5] This amount was aimed to set up a new dedicated Decryption Platform in cooperation with the EU Joint Research Centre (JRC), which was finally created in early 2020.[6]

IOCTA 2019 declared that EUROPOL is at the forefront of law enforcement innovation and acts as a knowledge platform for the provision of EU policing solutions in relation to encryption and other issues. In order to play an active role in the efforts of law enforcement against the use of encryption for criminal purposes, EC3 focuses on digital forensics and cross-departmental encryption support

3 There are no available data on the use of decryption platform in 2015 in CAAR 2015.

4 The Commission proposed a total of 86 additional security-related posts for Europol (19 more than in the 2017 budget), in particular to reinforce Europol's EC3. Future technological developments should be taken into account on the basis of research and development under the Horizon 2020 program and other EU-funded programs.

5 After that, encryption has not been mentioned in the reports, concluding the 20th Report from 30th October 2019.

6 These funds were received in May 2018 (CAAR 2018, 9). Meetings with the different stakeholders to capture the requirements were held and different cooling technologies and equipment contracting options were considered. Service Level Agreement (SLA), facility and security requirements and budget planning with regards to the off-site platform located within one of the premises of the JRC were finalized in 2018. One decryption expert was recruited and worked on the development of a decryption manual that would serve as valuable input for the project. In May 2019, Europol addressed a note to the European Parliament and the Council with information regarding decryption platform at Europol, in which they explained that the JRC computing room and involved services were used by Europol to support the decryption activities to be conducted by Europol. The support would consist of the setup and maintenance of high-performance computing platform for decryption located in one of the JRC's premises. The realization was planned for 2019 – 2020 (operational use in 2020), while afterwards an addendum would be attached and signed for the maintenance period. Europol and the JRC finalized a service level agreement (SLA) which covered the design, procurement, installation, configuration, maintenance and administration of a High Performance Computing decryption platform at Ispra (Italy). The first meeting of the Steering Committee took place in June and the first equipment and tests were scheduled for Q4, with the go-live planned for Q1 2020. However, due to some challenges the JRC was facing with the contractor working on the building integration the go-live of the project was delayed to Q2 (Europol, 2019b: 27).

for recovering encrypted criminal data and will be further developing and utilizing its potential to perform as a European center of expertise on decryption (Europol 2018 b:15, 24). Europol has the function of a network hub to facilitate collaboration among national expertise points[7] and Europol's EC3 was elected as the best-placed to set up and keep a repository toolbox of alternative investigation techniques and tools at disposal to MS to facilitate the development and use of measures to obtain needed information encrypted by criminals. EC3 will expand the toolbox available to law enforcement officers across Europe and beyond, increasing their technical and forensic capabilities (Europol, 2019a: 4). Such a toolbox has not been developed yet, and one may doubt that national LEAs might be willing to share sensitive encryption-cracking forensic tools and expertise across borders without the impetus of legislation. Europol's EC3 has observatory function in collaboration with the European Judicial Cybercrime Centre (EJCN) and Eurojust. Europol and Eurojust released joint "First Report of the observatory function on encryption" in January 2019 (Europol, Eurojust (2019b) and "Second Report of the observatory function on encryption" in February 2020 (Europol, Eurojust (2020) containing relevant statements or propositions made with respect to how law enforcement can potentially cope with encryption and its related challenges.

CONCLUSION

Encryption is more and more a cross-cutting challenge that affects all crime areas, including cybercrime, serious organized crime and terrorism, and significant and increasing percentage of investigations involve the use of some form of encryption to hide relevant data and communications evidence. Because growing number of electronic service providers implement encryption by default in their services, law enforcement has also observed the increasing misuse of and reliance by cybercriminals upon secure communication apps and channels providing end-to-end encryption, leading to that i*nvestigative techniques*, such as lawful interception, *are becoming increasingly* less effective or even technically impossible. Apart from the legal challenges, disclosing the data or circumventing the encryption is not always technically possible. This assessment however concludes with that although a number of the legislative and practical measures addressing the identified challenges are making progress on both national and international levels, 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.

Since 2016 encryption has been recognized as an obstacle to criminal investigation and therefore a threat to security in Europe. As data access policies and capabilities differ among MS, problems with encryption in criminal investigations vary from one MS to another. There is also the problem with legal frameworks for cooperation between MS and states outside the EU, while they are considered as slow and inadequate for addressing forms of cross-border criminal cases involving encrypted information. In order to counter the criminal abuse of encryption, LEA need proper tools, techniques and expertise in digital forensics. They must be equipped with adequate training and resources to obtain and handle electronic evidence in situ using techniques, such as live data forensics. LEA should

7 For example, capacity building for LEA community continued and three training courses on Hashcat were organized and delivered by the Forensic team to (24) MS representatives. Additionally, an internal course on applied Python programming was delivered to Europol staff by members of the Forensic team. Two decryption expert groups were created in 2019. The first one for practitioners who attended the Hashcat training course delivered by Europol and the second one (End-to-End Encryption - E2EE) for those experts who attended the Encryption Network meetings organized by the Forensic team. Europol acquired new tools to enable the extraction of data from password protected mobile devices (Europol (2019b: 28).

continue to monitor trends in the use of applications and software by cybercriminals and maintain awareness of the different investigative opportunities and challenges that each provides. It is essential for LAE to build and maintain relationships with academia and private industry as they may be able to assist or advise law enforcement where it lacks the technical capability.

REFERENCES

1. Council of the European Union (2016a). *Encryption of data – Questionnaire*. Accessed on July 15, 2020. http://data.consilium.europa.eu/doc/document/ST-12368-2016-INIT/en/pdf.
2. Council of the European Union (2016b). *Encryption: Challenges for criminal justice in relation to the use of encryption - future steps - progress report*. Accessed on July 15, 2020. https://data.consilium.europa.eu/doc/document/ST-14711-2016-INIT/en/pdf.
3. ENISA (2016). *Opinion Paper on Encryption Strong Encryption Safeguards our Digital Identity*. Accessed on July 15, 2020. https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisas-opinion-paper-on-encryption.
4. European Commission (2017a). Joint Communication to the European Parliament and the Council Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, 13.9.2017. Accessed on July 15, 2020. https://ec.europa.eu/transparency/regdoc/rep/10101/2017/EN/JOIN-2017-450-F1-EN-MAIN-PART-1.PDF.
5. European Commission (2017b). Communication from the Commission to the European Parliament, the European Council and the Council, *Eleventh progress report towards an effective and genuine Security Union* COM/2017/0608 final. Accessed on July 15, 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017DC0608&from=EN.
6. European Commission (2017c). Communication from the Commission to the European Parliament, the European Council and the Council, *Twelfth progress report towards an effective and genuine Security Union*, 12.12.2017. Accessed on July 15, 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017DC0779&from=EN.
7. European Commission (2018). Communication from the Commission to the European Parliament, the European Council and the Council, *Thirteenth progress report towards an effective and genuine Security Union*, COM/2018/046 final, 24.1.2018. Accessed on July 15, 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018DC0046&from=EN.
8. European Commission (2019). *Functional Encryption Technologies*, 6.9.2019. Accessed on July 15, 2020. https://cordis.europa.eu/project/rcn/213111/factsheet/en.
9. European Parliament (2017). *Resolution of 3 October 2017 on the fight against cybercrime (2017/2068(INI))*. Accessed on July 15, 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017IP0366&from=EN
10. Europol (2014). *Consolidated Annual Activity Report (CAAR)*. Accessed on July 15, 2020. https://www.europol.europa.eu/sites/default/files/documents/consolidated_annual_activity_report_caar_2014_0.pdf.
11. Europol (2016a). *The Internet Organised Crime Threat Assessment (IOCTA) 2016*. Accessed on July 15, 2020. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016

12. Europol (2016b). *Consolidated Annual Activity Report (CAAR)*. Accessed on July 15, 2020. https://www.europol.europa.eu/sites/default/files/documents/europol_annual_activity_report_2016.pdf.

13. Europol (2017a). *Internet Organised Crime Threat Assessment (IOCTA) 2017*. Accessed on July 15, 2020. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017.

14. Europol (2017b). *Consolidated Annual Activity Report (CAAR)*. Accessed on July 15, 2020. https://www.europol.europa.eu/publications-documents/consolidated-annual-activity-report-caar-2017.

15. Europol (2018 b). *Consolidated Annual Activity Report (CAAR)*. Accessed on July 15, 2020. https://www.europol.europa.eu/publications-documents/consolidated-annual-activity-report-caar-2018.

16. Europol (2018a). *Internet Organised Crime Threat Assessment (IOCTA) 2018*. Accessed on July 15, 2020. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018.

17. Europol (2019a). *Internet Organised Crime Threat Assessment (IOCTA) 2019*. Accessed on July 15, 2020.HTTPS://WWW.EUROPOL.EUROPA.EU/ACTIVITIES-SERVICES/MAIN-REPORTS/INTERNET-ORGANISED-CRIME-THREAT-ASSESSMENT-IOCTA-2019.

18. Europol (2019b). *Consolidated Annual Activity Report (CAAR)*. Accessed on July 15, 2020. file:///C:/Users/mpisaric/Downloads/consolidated_annual_activity_report_2019.pdf.

19. Europol, ENISA (2016). *Joint Statement: On lawful criminal investigation that respects 21st Century data protection*. Accessed on July 15, 2020. https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/on-lawful-criminal-investigation-that-respects-21st-century-data-protection

20. Europol, Eurojust (2019a). *Common challenges in combating cybercrime*. Accessed on July 15, 2020. https://www.europol.europa.eu/publications-documents/common-challenges-in-combating-cybercrime

21. Europol, Eurojust (2019b). *Joint Report First Report of the observatory function on encryption*. Accessed on July 15, 2020. https://www.europol.europa.eu/publications-documents/first-report-of-observatory-function-encryption

22. Europol, Eurojust (2020). *Joint Report Second Report of the observatory function on encryption*. Accessed on July 15, 2020. https://www.europol.europa.eu/publications-documents/second-report-of-observatory-function-encryption

23. Five Country Ministerial (2018). *Statement of Principles on Access to Evidence and Encryption*. . Accessed on July 15, 2020. *https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/five-country-ministerial-2018*.

24. Lomas, N. (2016, August 24). Encryption under fire in Europe as France and Germany call for decrypt law. *Tech Crunch*. Accessed on July 5, 2020. https://techcrunch.com/2016/08/24/encryption-under-fire-in-europe-as-france-and-germany-call-for-decrypt-law/?guccounter=1&guce_referrer_us=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_cs=sMnhNkTpqBEB3VgCB0PgRA.