THIRD REPORT OF THE OBSERVATORY FUNCTION ON ENCRYPTION

Joint report

EUROPOL EUROJUST

Manuscript completed in June 2021.
Europol and Eurojust Public Information
Neither the European Commission nor any person acting on behalf of the Commission is responsible
for the use that might be made of the following information.

CONTENTS

LIST OF ABBREVIATIONS

AES	Advanced Encryption Standard
AFP	Australian Federal Police
APFS	Apple File System
ASIO	Australian Security Intelligence Organisation
BPF	Browser Password Field
CDT	Center for Democracy & Technology
DNS	Domain Name System
DoH	DNS-over-HTTPS
DPP	Domain Password Policies
E2ee	End-to-end encryption
EC3	European Cybercrime Centre
ECHR	European Court of Human Rights
EIO	European Investigation Order
EJCN	European Judicial Cybercrime Network
EU	European Union
FBI	Federal Bureau of Investigation
FDE	Full disk Encryption
HBE	Hardware-based Encryption
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IP	Internet Protocol
ISP	Internet Service Provider
JHA	Justice and Home Affairs
JIT	Joint Investigation team
LEA	Law Enforcement Authority
MLA	Mutual Legal Assistance Request
NCMEC	National Centre for Missing and Exploited Children
ODoH	Oblivious DNS over HTTPs
QSC	Quantum-Safe Cryptography
SSD	Solid State Drive
TPM	Trusted Platform Module
TLS	Transport Layer Security

1. EXECUTIVE SUMMARY

Access to data-in-clear of encrypted communications and stored data presents several difficult and controversial issues and continues to create tensions between key stakeholders, including law enforcement and the judiciary and civil society organisations, leaving policy makers with the mammoth task of balancing all the important considerations in this debate. Thus far efforts to identify technical solutions that are feasible and proportionate and which safeguard fundamental rights have struggled to reconcile all the equities. In the midst of this discussion encryption continues to develop and become the main means to safeguard a number of online technologies, including electronic communication services, online storage spaces, mailboxes etc…This further complicates the encryption landscape, and significantly challenges criminal investigations.

This third report of the Observatory Function on encryption builds on previous reports and looks at the relevant technical and legislative developments, re-visiting some topics, which deserved further consideration. In the interim between this and previous reports, there have only been a few developments in European Union (EU) Member States' national legal regimes to incorporate new provisions that tackle the challenge of encryption in criminal investigations. These new approaches can be categorised into two distinct parts: one deals with tools that directly tackle encryption and the others category provides for tools to gain access to content before it is encrypted, or after it is decrypted and bypass encryption altogether. This is further underpinned by jurisprudence that exemplifies the use of the provisions mentioned. Insights are shared on encryption in the context of cross-border cases. Eurojust here identifies two key focuses; cases in which decryption of the tool used by criminals is the main focus of the investigation and 'spin-off cases' where the focus is on other aspects rather than decryption, but where the decrypted communications among criminals are required as evidence. An analysis of considerations ancillary to decryption, such as the need to find legal means to decrypt electronic communications, admissibility of evidence obtained from decrypted devices, and the sharing of such data with other law enforcement agencies in the context of cross-border cases is explored.

The report elaborates on the challenges faced by law enforcement in environments where encryption is a default setting for many user devices and services, presenting recent developments in products that make use of encryption or develop it further. The report takes a detailed look at hardware based encryption, the Bcrypt password hashing function and increased iteration counts. It also provides information on the increasing robustness of browser password checking mechanisms employed by companies to help users generate and utilise stronger passwords ensuring that they remain safe online. Linking up from previous reports, this piece of work introduces the concept of oblivious DNS (Domain Name System) over HTTPs (Hypertext Transfer Protocol Secure) that separates IP (Internet Protocol)addresses from search queries. This is done by adding a layer of encryption around the DNS query before it is sent to the proxy serve that acts as a go-between for the internet user and the website they want to visit. This technology shields the sender of the query from the DNS resolver. All these developments reflect the increasing dependence on encryption to safeguard cybersecurity, data protection and privacy of communications. In itself this is a welcome and necessary development. Unfortunately, this technology can equally be used for criminal purposes, complicating further criminal investigations.

Quantum computing may in the next decade offer some possibilities to help mitigate these difficulties. Quantum technology is set to have a significant effect on cryptography, however it remains hard to predict the timing and the concrete effects it would have on encryption. The report explores what quantum computers might be able to achieve in the future.

Another important element in this report is an overview of the EncroChat case. It is an example of good practice that incorporated the right technical and legislative elements that have underpinned this delicate operation. A background and insights into the case shed more light on the effort and quantifies the developments and the next steps.

For the first time, the report introduced a third viewpoint, cataloguing the key policy developments taking place in regions and countries around the world. This complements the other parts of the report and aims to provide readers with a more complete understanding of this complex topics and set out with more clarity and helps piece together the interactions between the technical, legislative and policy challenges. In this first inclusion, the report highlights developments inside the EU, particularly the adoption by the Council of the EU of the resolution on encryption and it provides information on the US EARN IT act that is being taken forward in Congress. The report also covers the discussion on encryption taking place in the Five Eyes Country alliance and the adoption by the UK, US, Australia, Canada New Zealand, Japan and India of the international statement on end-to-end encryption and public safety. This is followed by a piece on Australia's Access and Assistance Act of 2018.

2. INTRODUCTION

As we continue to spend more of our lives online, we expect more digital security to safeguard our activities. Whilst encryption technology on its own does not solve the challenge of providing effective security for data and systems, it is at the heart of digital security, making it part of our daily lives and fuelling developments in this area of technology and others reliant on it.

At the same time, the wider usage of encryption technology continues to be increasingly exploited by criminals, both as part of their modus operandi and as a mean to enable secret communication and illegal activities by putting them out of law enforcement's reach. This continues to create challenges for both the law enforcement and the judiciary communities and significantly hampers these authorities' ability to investigate and prosecute.

The first Observatory Function report provided a brief overview and historical background of encryption, and explored the challenges faced in the context of law enforcement and prosecution. The second report provided a comprehensive update of the encryption challenge and looked at the potential of a number of options that could help law enforcement mitigate the issues arising from encryption and related challenges. This third report is similarly structured to provide an update capturing the legal and technical developments that have taken place since the previous report, and what they mean in practical terms. A number of topics presented in previous reports, such as quantum computing are re-visited here as developments continue to take place in these specific areas. A third aspect has been included in this report looking at a number of policy developments on encryption inside the European Union (EU) and in other key regions.

This report, like those before it, functions as a reference on the topic of encryption and other closely related developments in the context of criminal investigations and prosecution. The report, as the tangible outcome of the observatory function jointly held by Europol and Eurojust, aims to provide a balanced resource for decision-making. In this third report, the agencies have been supported by the European Judicial Cybercrime Network (EJCN) through the yearly contribution of relevant data, and for the first time the Joint Research Centre and the Directorate general for Home Affairs and Migration of the European Commission have further enriched the document with technical content and supported the chapter on policy developments.

3. THE LEGAL ASPECTS OF HANDLING ENCRYPTION IN CRIMINAL INVESTIGATIONS

3.1 LEGISLATIVE OVERVIEW OF LEGAL FRAMEWORKS RELATING TO ATTACKING ENCRYPTION

3.1.1. BACKGROUND

In an ever more digitalized world, encryption has become a basic feature of several products and services, increasingly becoming the default standard for social media and communication platforms. Meanwhile, along with this scenario of legitimate use, criminals are not only misusing encryption possibilities of mainstream platforms but also using dedicated communication channels providing end-to-end encryption (e2ee), consequently making it impossible or highly resource intensive to obtain intelligence or gather evidence.

In the first Encryption Observatory Report, it was described how law enforcement and judicial authorities can gain access to digital evidence under encryption: by either attacking encryption or bypassing encryption. The second Encryption Observatory Report focussed in more detail on bypassing encryption in a targeted manner by requesting or compelling a suspect to provide data in a decrypted format or hand over an access key.

Following the EncroChat case brought to Eurojust, as well as its further developments and other cases in which encryption tools were used by criminals, the focus of the current report is on the topic of attacking encryption in parallel with the consequences of this action in relation to admissibility of evidence.

The use of encryption technology by international criminal organisations, as seen in the EncroChat case, poses challenges to law enforcement and judicial authorities to intercept their communications and gather digital evidence for court proceedings. As a result, solutions to gather encrypted digital evidence need to ensure the protection of fundamental rights and the prevention, detection and prosecution of crime in a targeted manner subject to the principles of necessity and proportionality. However, the legal answers to this challenge are complex and often unclear in several jurisdictions.

The following sections provide an overview of the legislative frameworks in relation to encryption in EU Member States, particularly the legal provisions related to attacking encryption, with law enforcement tools and techniques, as well as some legal and practical challenges faced by competent authorities, namely in relation to the admissibility of evidence.

3.1.2. CURRENT LEGISLATIVE OVERVIEW ON ENCRYPTION

Below, an overview is given of the legal provisions applied by 19 Member States plus Switzerland in relation to the topic of attacking encryption[1]. In the majority of countries, general legal provisions are applied.

No recent changes occurred in the legal framework related to encryption[2], with the exception of Sweden[3] and The Netherlands[4].

[1] The information was gathered via a questionnaire distributed in July 2018 to members of the EJCN. In November 2020, a request for an update to this amended questionnaire was distributed.

[2] No changes since 1 January 2019.

[3] Act (2020: 62) issued on the 27 February 2020.

[4] Computer Crime Act III entered into force on 1 March 2019.

Legal Provisions on Attacking Encryption by Law Enforcement

COUNTRY	LEGAL PROVISIONS
Austria	General provisions
Czech Republic	Section 113 Code of Criminal Procedure
Croatia	Article 257 - 263 (searches) Article 332 - 339 (special collection of evidence)
Denmark	Sections 780-781 Administration of Justice Act (interception of communications) Section 791 b Administration of Justice Act (data copying) Sections 793-794 Administration of Justice Act (searches)
Estonia	§83 Code of Criminal Procedure (inspection and inquiries to electronic communications undertakings) §91 Code of Criminal Procedure (searches) §1265 and Code of Criminal Procedure (covert surveillance, covert collection of comparative samples and conduct of initial examinations, covert examination and replacement of things) §1267 Code of Criminal Procedure (wire-tapping or covert observation)
France	Article 230-1 to 230-5 Criminal Code (deciphering) Article 706-102-1 to 706-102-7 Criminal Code (GOVWARE)
Germany	Sections 94, 98 and 102 Code of Criminal Procedure (stored data) Section 100a, para 1 Code of Criminal Procedure (real-time interception - source interception enabling access to unencrypted data) Section 51 para 2 new Law on the BKA (real-time interception - terrorism prevention)
Greece	General provisions Articles 258 et seq., article 264 Code of Criminal Procedure
Ireland	General provisions - where the devices or accounts, etc., are accessed on the basis of a legal authority such as a search warrant, the investigators may utilize any means to gain access and give effect to the provisions in the warrant
Lithuania	General Provisions of the Code of Criminal Procedure: Article 145 (searches) Article 154 (control, recording and accumulation of information transmitted through electronic communications networks) Article 158 (actions of covert pre-trial investigation officers) Article 208 (expert examination)
Luxembourg	General provisions
Poland	Article 19 §7 Police Act (request for the use of hacking techniques)
Portugal	General provisions
Romania	Article 138 §1 and §3 Criminal Procedure Code (access to computer systems)
Slovak Republic	Sections 90, 116 §6, 118 Code of Criminal Procedure (stored data) Section 115 §1 and §11 Code of Criminal Procedure (real-time interception of device)

Slovenia	General provisions
Spain	General provisions which can be applied in practice for decryption Articles 588bis a. – 588ter m. Criminal Procedure Code Articles 588sexies a. – 588sexies c. Criminal Procedure Code Article 588septies Criminal Procedure Code (remote access, through the technique of installing software or spy programs) Law enforcement agencies (LEAs) are allowed to use decryption techniques, under judicial authorization, with no other limitation than the assessment by the investigating judge of the applicability of the general principles contained in art. 588 bis a. and the impossibility of using physical violence against the person.
Sweden	Act (2020: 62) on secret data reading. Secret data reading means that a court can authorize that data, intended for automated processing, can be secretly and with a technical aid, read by or recorded in a readable information system.
Switzerland	General provisions on search and seizure. Specific provision regarding the use of government software to access encrypted data.
The Netherlands	Computer Crime Act III amending the Dutch Criminal Code and Code of Criminal Procedure with a view to improve and reinforce investigations and prosecutions of cybercrime Articles 126nba and 126ffa of the Code of Criminal Procedure

Table 1: Legal Provisions on Attacking Encryption by Law Enforcement.

The above table shows that, only Denmark, France, Germany, Poland, Sweden, Switzerland and The Netherlands have provisions that specifically address the use by law enforcement authorities of technical tools to attack encryption. Other countries can apply general legal provisions. A distinction can be made between provisions permitting attacking directly encrypted content and those providing for the use of tools to gain access to content before it is encrypted or after it is decrypted.

In Denmark, section 791 b of the Administration of Justice Act allows for copying of data, inaccessible to the public, from an information system or device, namely by the undercover placement of software to provide law enforcement a copy of all entries or commands made by the user on the information system or device. The use of such software can allow an attack to encryption by obtaining the password to the encrypted data, without the knowledge of the suspect.

The evidence gathered under this provision is fully admissible as long as it fulfils the applicable legal requirements. Authorisations for data copying are given by the court in the form of a court order, which shall state the information system or device, which the measure concerns. Furthermore, a number of other legal requirements must be satisfied.

These include, inter alia:

1. There must be specific reasons to presume that the information system is used by a suspect in relation to planned or committed criminal activity as mentioned in point 3 below;
2. The measure is presumed to be of crucial importance to the investigation;
3. The investigation concerns an offence, which under the law can be punished with++ at least six years of imprisonment, or an intentional violation of Chapter 12 or 13 of the Criminal Code (which includes certain grave offences, including terrorism-related offences); and
4. Data copying cannot be conducted if it would be disproportionate, considering the purpose of the measure, the significance of the case, and the offence and inconvenience which the invasion can be presumed to cause to the concerned person or persons.

France has quite an extensive and detailed legislation on the topic of encryption, covering both the bypassing and attacking of encryption that proved relevant in the EncroChat case. It can also be said that the work of the French authorities was supported by a robust legal framework on encryption that contributes to legal certainty and supports the firm admissibility of evidence in Court proceedings.

Under this framework, providing EncroChat product was considered from the start of the investigation a criminal offense, since the encrypted device was not previously reported, in accordance to article 30 Law No. 2004-575[5] for confidence in the digital economy, which states that: "*The supply, the transfer from a member state of the European Community or the importation of a means of cryptology which does not provide exclusively authentication or integrity control functions are subject to a prior declaration to the Prime Minister*". The non-compliance with this provision is punishable with one-year imprisonment and € 15,000 fine, (article 35).

In addition, the use of encryption to commit a criminal offense, as done by EncroChat users, constitutes an aggravating circumstance to the main offense, according to articles 132-79 of the Criminal Code. From a procedural perspective, articles 230-2 and 706-102-1 of the Code of Criminal Procedure, allow technical tools to be installed by competent authorities to capture encrypted data and the use of tools by a competent body to decrypt the content of seized devices.

There are no legal limitations to the use of tools or techniques in **Germany** to break the encryption of data. Technical means may be applied to intercept and record telecommunications in an unencrypted format according to Section 100a, par. 1 Code of Criminal Procedure. In **Poland**, given the specific provision that allows for the use of technical tools for lawful access to data, the setting is identical.

Sweden has recently passed legislation to address the topic of attacking encryption. On 1 April 2020, a new law regarding secret data reading, entered into force. Currently, under Swedish jurisdiction, a court can authorize that data intended for automated processing can secretly and with the use of the necessary technical tools be read by or recorded in a readable information system. According to this new legislation, in investigations regarding serious crime, under certain safeguards specified in the law, law enforcement authorities can install the software or devices deemed necessary to access encrypted digital evidence, without the knowledge of the suspect. The new law is valid for five years and will then be reviewed.

In Switzerland, although general provisions on search and seizure allow authorities to break encryption, a specific provision exists regarding the use of government software, allowing the installation of software on a device in order to access encrypted communication before it is encrypted or after it is decrypted by the receiving device.

The Netherlands have specific provisions regarding the access to encrypted data and the use of technical tools to gather encrypted digital evidence, since the Computer Crime Act III entered into force on 1 March 2019, aimed at improving the investigative powers and prosecution of cybercrime. In the Dutch Code of Criminal Procedure, the use of technical tools to gain access to digital evidence without the knowledge of the suspect was added (section 126nba, DCCP) as an investigative method.

This thoroughly regulated provision can bring a solution in investigations of serious crime and cybercrime specifically, overcoming problems with encryption by covertly and remotely accessing a device (or "automated work" in use by a suspect) in order to access information before it is encrypted. In deploying this special investigatory power, law enforcement authorities can, but are not obliged to, make use of a technical tool ("technisch hulpmiddel"). The technical tools are subject to a thorough inspection, of which the requirements are laid down in secondary legislation and detailed in a (non-public) inspection-protocol, by an inspection services appointed by the Minister of Justice and Security.

Law enforcement authorities are also allowed to use commercial technical tools. Only the tools that are used to carry out investigative activities are subject to an inspection. Intrusion software is not subject to inspection. However, the providers of these intrusion tools are checked by the Dutch General Intelligence Service and should not do business with "dubious" regimes, according to the 2017 coalition agreement.

Despite the fact that only a few countries have specific provisions on encryption or on the use of tools to attack encryption, the interception of encrypted data or the decryption of seized data is usually allowed under general provisions.

[5] Loi n 2004-575 june 2004 pour la confiance dans l'économie numérique (1)

However, the absence of specific provisions on the use of software or devices to attack encryption, although covered in theory under general provisions, can pose challenges to the admissibility of the evidence gathered.

The topic of encryption, in particular legal challenges to the admissibility of electronic evidence gathered by attacking encryption, is still new in Court proceedings of several jurisdictions and only a few countries reported relevant recent rulings on the subject, to be mentioned below.

3.1.3. RELEVANT JURISPRUDENCE

Austria

An attempt was made to specifically regulate the lawful access to encrypted data, namely to e2ee communications, by introducing a new provision in the Code of Criminal Procedure (§ 135a StPO). However, the provision was considered unconstitutional by the Austrian Constitutional Court[6] before this provision could enter into force on 1 April 2020.

The Constitutional Court argued that the new provisions of the Code of Criminal Procedure were incompatible with Art. 8 ECHR, since its wider spread use could allow law enforcement authorities to draw comprehensive conclusions about a person's preferences, inclinations, orientation, attitudes and lifestyle. According to the Constitutional Court, such an encroachment on the private sphere, protected under Art 8 ECHR, requires a serious public interest to justify it and is only permissible within extremely narrow limits, for the protection of corresponding heavy legal interests. Moreover, the technical tool would provide access to the communications of all users and not only the suspects. The Court concluded that the new provisions, as they were drafted, did not respect the legal interests and limitations in cases of less serious crimes, where they would be allowed by the order of a prosecutor and court authorisation, without effective monitoring by an independent supervision authority. The Court also addressed the effectiveness of the supervisory system.

France

The Court of Cassation, by its verdict from 13 October 2020[7], in relation to the legal obligation to surrender the access code to unlock a device, declared that a smartphone could be considered as an encryption device. As such, the refusal to surrender, upon request, the unlocking code is a criminal offense (according to article 434-15-2 of the French Criminal Code).

Italy

The Italian jurisprudence has recognised the legality of the use of Trojan software during investigations into the most serious criminal offenses. The Trojan is a software that, when inserted into a device, is able to intercept data and communication flows. More specifically, this tool allows obtaining hidden access to data stored in the infected device and recording incoming and outgoing data. Trojan software follows the user wherever he/she goes and can activate the microphone enabling to intercept the conversations of those who are within the device field as well. By using such a tool, investigators can make a bypass and access the conversations and communications before they are encrypted.

In this regard, the Joint Sections of the Supreme Court of Cassation rendered a decision in 2016[8]. The Court stated that the use of such an investigative tool is only allowed in proceedings relating to the most serious offences foreseen in Article 51, paragraphs 3-bis and 3-quarter of the Italian Criminal Procedure Code (i.e. terrorist offenses, criminal organised crimes, reduction into slavery). Consequently, the results of interceptions of conversations and communications recorded by making use of a Trojan can be legally admitted in Court as evidence.

Slovak Republic

In the Slovak Republic, there have been rulings from the Special criminal court and Supreme court, in which the courts assessed the use of evidence, gathered from an extraction of data from the Threema[9] application on a phone. The Slovak police and Europol experts extracted communications from the devices and restored several deleted messages. In both cases, the decrypted text messages revealed a conversation between the accused persons, which the prosecution argued was proof of their involvement in the criminal activity.

In the first case, the judge directly stated that the decrypted data communication of the Threema app, submitted by the prosecutor as evidence, was admissible for the court trial and the evidence was used for proving the guilt of the accused person. This judgement is final.

[6] Constitutional Court ruling on 11 December 2019
[7] https://www.courdecassation.fr/jurisprudence_2/chambre_criminelle_578/1804_13_45671.html
[8] Decision n. 26889/2016 of the Court of Cassation, Joint Sections
[9] https://threema.ch/en/

In the second case, on the murder of the journalist Kuciak, the first instance court considered the decrypted data from the Threema app as admissible evidence; however, it did not accept it as a direct evidence for proving the guilt of some of the accused, who were acquitted. This decision has been appealed by the prosecutor, and is currently pending before the Supreme court.

The Netherlands

According to the decision from the District Court of Rotterdam, from 22 February 2019[10], the access and use of a suspect's account to recover messages under e2ee is allowed by the Court. Since the service provider does not surrender the data, the location where the data is physically located "in the cloud" is unknown and the data cannot be read due to the e2eewithout using the end user's account. The Court took into account the fact that based on forthcoming legislation (the Computer Crime Act III entering into force on 1 March 2019), far-reaching investigative powers will become possible in a digital environment with the authorisation of the investigative judge. In this case, the rejection (of the prosecutor's request) by the investigating judge was annulled by the Court and replaced by the decision to grant the authorisation to the prosecutor to access the suspect's account. It is not possible to appeal this decision of the Court, taken in the investigation phase of a case, and thus it is irreversible and final.

3.1.4. CASEWORK EXPERIENCES RELATED TO THE USE OF ENCRYPTION TOOLS BY CRIMINALS

As already mentioned above, criminals are increasingly making use of encryption tools to avoid or complicate access by others, including police and judicial authorities, to devices and electronic communication. Such encryption tools and techniques come in different formats. EncroChat (see below) is a well-known, recent example of such an encryption tool. The EncroChat devices aimed at avoiding law enforcement gaining access to communication between users, were designed to guarantee full anonymity of communications and offered functions intended to ensure the impunity of its users.

These encryption tools are used for communication between criminals in a range of different crime types. The majority of cases concerned drug trafficking and organised crime, but cybercrime, murder, money laundering and fraud are among the crime types for which the encryption tools are used.

Each encryption tool or technique requires a tailor-made approach by law enforcement to try and break the encryption and gain lawful access to the unencrypted data. As a prerequisite, these decryption attempts need to be legally valid. The techniques used by police to attack encryption need to be covered by national legal provisions, be it general or specific. In addition, the procedural rules governing the technical application of the decryption technique need to be followed correctly. In cross-border cases, where users/criminals, victims, committed crimes and infrastructure or servers are located in different countries, it becomes even more challenging to conduct investigations and have a successful outcome, given the different legal frameworks in place.

Taking a closer look at these cross-border cases, registered at Eurojust, two main categories can be identified. Firstly, there are cases in which the decryption of the technical tool itself, used by the criminals for encryption, is the focus of the investigation. Secondly, in the so-called 'spin-off cases', where the focus of the case is on other aspects rather than the decryption (which happened in a different case of the first category), but the decrypted communications from the criminals are needed as evidence (e.g. further investigations into drug trafficking cases following the successful decryption of EncroChat communications).

In relation to the first type of cases where law enforcement and judicial authorities need to find a way to legally decrypt the data, many different challenges and obstacles need to be addressed:

First and foremost, law enforcement authorities need to be able to find a way to break the encryption, both from a legal and a technical point of view.

Secondly, good cooperation and coordination between the different countries involved in the investigation, is important. These types of cases require a collective approach and effort, as different legal frameworks are applicable in parallel and practical considerations and available resources at national levels have a cross-border (case) impact. It is essential for the successful outcome of the case, i.e. breaking of the encryption and further use of the unencrypted data as evidence in court proceedings, that all steps to be taken happen in a legally correct way. Sharing of information and evidence, discussing strategy and next steps, resolving possible conflicts of jurisdiction, as well as agreeing on a possible joint action day need

[10] https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBROT:2019:2712

to be discussed. The possibility of setting up a Joint Investigation Team[11] (JIT) can be considered, in view of facilitating cooperation and information and evidence exchange.

Thirdly, in relation to the evidence sharing between countries, it is crucial that the electronic evidence gathered by one country, i.e. the unencrypted data, is obtained in a legal way by another country. Indeed, if authorities from a certain country want to use the unencrypted data for their own investigation, they need to obtain this evidence legally, usually via a European Investigation Order (EIO) or Mutual Legal Assistance request (MLA).

In the second type of cross-border cases, authorities required the content of the communications between suspects in view of prosecuting them for the crimes they were involved in. The content of the (previously encrypted) messages is therefore needed as proof of the committed crime(s), and has to be obtained from another country. As mentioned above, in this case, an EIO or MLA will be sent to the country that lawfully decrypted the data, in view of obtaining the data as evidence from that country.

It is important to underline that, without law enforcement legally attacking encryption and lawfully gaining access to encrypted data, the electronic evidence gathered through the decryption attempts might be considered inadmissible at a later stage, whether in the country that performed the decryption or in the country, that has subsequently received the unencrypted data.

Admissibility of legally obtained unencrypted data as evidence in courts of other countries will be determined by the national law of these countries. Thus, the sharing of the unencrypted data afterwards with such countries also needs to be done in respect of the national laws. As these types of cases usually involve multiple countries, the abovementioned description of a collective and coordinated approach to a case, ensuring that all applicable legal frameworks are respected and electronic evidence is gathered and shared in a correct and legal way is the best way to minimise the risk of evidence being rendered inadmissible at a later stage. Because of its legal expertise, knowledge and prior experience in such cases, Eurojust is well placed to assist law enforcement and judicial authorities of the Member States in coordinating these kind of cases and providing advice on the best way to proceed in a case to ensure a successful outcome.

In parallel with the legal challenges mentioned above that impact the admissibility of evidence, law enforcement and judicial authorities continue to be confronted with technical and practical challenges when trying to gain access to encrypted data, such as the absence or high cost of forensic tools, the time-consuming nature of breaking encryption, the lack of or insufficient number of experts for decrypting and the lack of training[12].

These practical and technical challenges have intensified by the increased use of new technologies and messaging services that provide encrypted services by default, which are free for all users and often entail that data is deleted after a fixed time. The encryption offered by these kinds of services is often strong enough to withstand "brute forcing[13]" and dictionary attacks[14] deployed by law enforcement, even when such resources are available.

The use of "Govware" or legal access tools to obtain evidence, installed undercover in a targeted device, can also pose practical and legal challenges, namely the difficulty to inject such tools without an action from the suspect and the fact that its use is not clearly stated in the procedural provisions of most jurisdictions.

In conclusion, a technical development such as encryption, is essential to safeguard fundamental rights and EU digital sovereignty and innovation but can also provide criminals with a more efficient way of committing crimes and hiding their traces. The advantages of encryption should be preserved as well as law enforcement authorities' ability for targeted access to data of suspected persons.

[11] An advanced tool used in international cooperation in criminal matters. It comprises of a team of prosecutors, law enforcement authorities and judges established for a fixed period of time based on a legal agreement between competent authorities of two or more States for the purpose of carrying out criminal investigations. Eurojust's mission includes provision of operational, legal and financial support to JITs and enabling access to expertise of the JITs network.

[12] As reported in the Eurojust Cybercrime Judicial Monitor 4

[13] Brute-forcing consists in submitting many passwords/passphrases with the hope of eventually guessing the right combination. Passwords are systematically checked until the correct one is found.

[14] A dictionary attack is a form of brute-forcing that tries to determine the decryption key/passphrase by using guessing options in a pre-arranged listing such as words found in a dictionary or from lists recovered from the open Internet of past data breaches. 'Dictionaries' may also be suspect specific, including combinations that reflect the suspect's lifestyle, likes, hobbies etc...

4. TECHNICAL DEVELOPMENTS AND THEIR EFFECTS ON INVESTIGATION EFFORTS

The previous chapter highlighted the challenges to law enforcement and judicial authorities to intercept communications and gather digital evidence for court proceedings. This chapter provides an update on the challenges faced by law enforcement in an environment where encryption is a default setting for many user devices and discusses recent developments in services and products that use or improve encryption. The chapter elaborates on the stronger encryption of hardware and entire communication devices, triggering additional challenges for lawful access to suspect devices or lawfully monitoring communication. Subsequently, the chapter reflects on the impact of new password policies introduced by private companies to improve user security. Finally, the chapter considers the upcoming opportunities and challenges expected with progresses observed in quantum computing.

By identifying these services, our research aims to contextualise the challenges introduced by encryption in criminal investigations. In doing so, we used internal expertise and open source research. Important to note here is that most of the services and products described are generally used by all types of users. However, Europol also witnessed an emerging trend of encrypted devices that are produced with a criminal target group in mind.

4.1 HARDWARE BASED ENCRYPTION

Disk encryption aims to protect data at rest (e.g. on a disk drive), as opposed to data in transit (e.g. email communications). The first Observatory Function discussed Full-disk encryption (FDE), i.e. disk encryption protecting an entire volume. FDE is particularly useful for small electronic devices vulnerable to theft or loss, such as laptops, phones or USB media storage, and is an increasingly widespread phenomenon.

Disk encryption is often classified into two categories: software-based and hardware-based encryption (HBE). Software-based encryption uses the same computing resources as the ones used by other programs running on the device. In contrast, HBE uses separate and tamper-proof resources dedicated to the encryption of data. It is self-contained and does not require additional software support. In this last scenario, nothing, from the encryption keys to the authentication of the user, is exposed in the memory or processor of the host computer, making the system less vulnerable to actions aimed at the encryption key.[15] As an example, the Trusted Computing Group, proposed specifications for the Trusted Platform Module (TPM, standardised as ISO/IEC 11889), a hardware chip intended to be physically attached to the motherboard of a computer[16]. More recently, Apple started including secure enclaves[17] in some of its processors and later independent security chips in its devices (see below the T2 security chip example)[18].

While HBE offers stronger resilience against common cyber-attacks, it also provides a more sophisticated environment for criminals to secure their data and criminal assets. In general, access to the devices will not be possible as the crypto module will shut down the system and possibly compromise data after a certain number of password-cracking attempts. This results in the inability for law enforcement to conduct offline decryption. There are exceptions where law enforcement may be able to extract a key from a hardware device and then mix in the key to the entire hashing algorithm in order to conduct offline decryption. Similarly, if the device under investigation is seized while it is unlocked, its content is available without the need to extract the key.

[15] https://www.infosecurity-magazine.com/magazine-features

[16] Arthur, Will, et al. A Practical Guide to TPM 2.0 : Using the New Trusted Platform Module in the New Age of Security. Springer Nature, 2015, doi:10.1007/978-1-4302-6584-9.

[17] A secure enclave is another type of secure element directly integrated into systems on chip, but isolated from the main processor.

[18] https://manuals.info.apple.com/MANUALS/1000/MA1902/en_US/apple-platform-security-guide.pdf

Technical box 1:

The T2 security chip in Apple devices

Apple first introduced the T2 with the iMac Pro in late 2017. Subsequently, it was added to MacBook Pro computers earlier in 2020 – and most recently, it has been implemented into the new MacBook Air and Mac Mini.[19] The new T2 chip provides a built-in hardware encryption engine that encrypts all of the data stored on the Solid State Drive (SSD) with a unique security key on each Mac. This means that all of the data on a Mac can only be read by that Mac, even if the SSD is removed.[20] The T2 sits between Apple's disks (denoted as NAND storage on Figure 1) and the Intel processor, and makes use of the native encryption functions in the Apple File System (APFS)[21]. This combination makes permanent, FDE possible. As long as FileVault[22] is switched on, this makes it extremely unlikely that third parties could access the data in storage files by attempting to enter the physical storage components.[23]

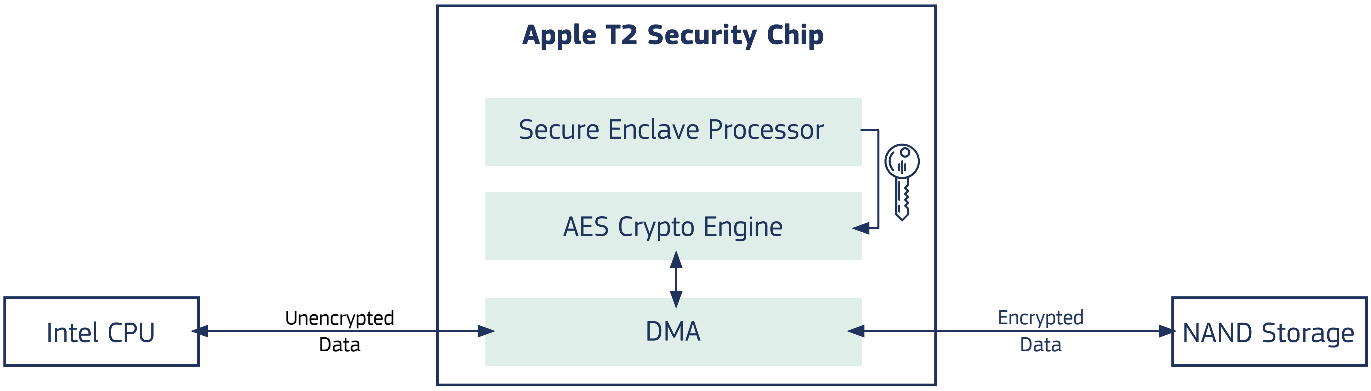

Figure 2 HBE in Apple devices using the T2 security chip[24]

[19] https://threatpost.com/apple-modernizes-its-hardware-security-with-t2/138904/#

[20] Ibid.

[21] Ibid.

[22] FileVault is a full-disk encryption program found in Mac OS X10.3 and later. It uses XTS-AES-128 encryption with a 256-bit key to help prevent unauthorised access to the information on a Mac's startup disk.

[23] Ibid.

[24] Source: https://support.apple.com/en-au/guide/security/sec4ea70a303/web

4.2 ENCRYPTED COMMUNICATION DEVICES USING A VARIETY OF DIFFERENT ENCRYPTION ALGORITHMS STANDARDS

As explained in the second Observatory Function report, one of the main challenges for law enforcement is the use of encrypted communication devices by organised crime groups. Criminal usage of encrypted communication mobile devices is a recurring difficulty in investigations, ranging across the different crime areas. Such devices provide criminals with a manner of communication, which allows them to circumvent law enforcement means of interception. In early 2020, EncroChat was one of the largest providers of encrypted digital communication with a very high share of users engaged in criminal activity. Further details on the EncroChat case can be found under a separate section of this report.

Similar to EncroChat, other providers like Phantom Secure show the impact and the scale of the use of mobile encryption tools by organised criminal groups as discussed in the second report of the Observatory Function.

These are just two examples of a number of global providers offering these mobile devices to criminal target groups. The system of distributing the devices is and was through strict referral – only existing clients could recommend new ones. To ensure highest anonymity and encryption, providers include home-grown algorithms in these ''crypto phones''. The encryption algorithms are not entirely developed from scratch, but are based on the cascading technique. Providers use the cascading technique to layer different encryption standards/crypto primitives over one another to ensure the highest encryption and security for the – in most cases – criminal users. The costs vary from €1 500 to €2 800 depending on the provider and the length of the subscription[25]. The alternatives – encrypted online communication tools – are also readily available as freely downloadable applications available for other types of smartphones. The case of EncroChat shows that providers offered "ready to use" and "all inclusive'' devices, going beyond previous cheaper or even free "do it yourself" solutions[26].

The market for encrypted communication providers dedicated to organised crime groups is increasing. These providers promise their customers enhanced security and privacy. These types of communication devices are attractive and criminals use them to make their communication inaccessible for law enforcement. This brings further challenges for the successful investigation of crime to law enforcement, since decrypting and gaining access to crypto phones leads to time consuming reverse engineering and time consuming integration for law enforcement. This process, especially the reverse engineering, requires too much time for many investigations.

4.3 BCRYPT PASSWORD HASHING AND INCREASED ITERATION COUNT

The encryption of criminal material is a cross-cutting challenge that affects all crime areas. Since 2016, Europol's European Cybercrime Centre (EC3)'s Decryption Platform has been used to support multiple investigations in various Europol mandated crime areas, such as cyber-dependent crime, child sexual exploitation, payment card fraud, weapons trafficking, drugs trafficking, money laundering, counter-terrorism, migrant smuggling and murder, among others. In late 2020, Europol inaugurated the new decryption platform, developed in close cooperation with the European Commission's Joint Research Centre, which will significantly increase Europol's capability to decrypt information lawfully obtained in criminal investigations as new password hashing standards arise and iteration count increases, e.g. when bcrypt replaces the MD5 standard in PHP application for password hashing.[27] Access to online profiles of suspects can be key to solving a criminal case.

Most of the web application frameworks are written in the programming language PHP. The programming language did not provide a specific password hashing algorithm and in absence of such a specific hashing algorithm, developers used MD5. MD5 is an unsuitable password hashing algorithm, which allowed law enforcement to decrypt hashlists of suspects' profiles. These decrypted hashlists provided law enforcement the ability to identify patterns in passwords as a means to assist in criminal investigations. These patterns then were transformed into decryption rules that law enforcement could use for ongoing criminal cases.

[25] See also Second Report of the Observatory Function.
[26] Tutorial to deploy encrypted chat service relying on freemium components
[27] https://www.information-age.com/homegrown-encryption-threatens-millions-smart-grid-devices-123459466/

The bcrypt is a password-hashing function designed by Niels Provos and David Mazières, based on the Blowfish cipher and presented at USENIX in 1999.[28] The bcrypt hashing function allows users to build a password security platform that scales with computation power and always hashes every password with a ''salt''.[29] Salting describes the default of adding random identifiers to user passwords. The user picks a password e.g.: 12345 and the provider adds "salt" to it, meaning 3-5 more characters to change the hash value. Due to the salting, the hash value for the same password is different, making it impossible for law enforcement to analyse multiple hashes simultaneously. MD5 is not "salted'' by default, making password detection easier, especially as suspects tend to reuse passwords.

Besides incorporating a salt to protect against rainbow table attacks (see technical box 2 below), bcrypt is an adaptive function: over time, the iteration count can be increased to make it slower, so it remains resistant to brute-force search attacks even with increasing computation power.[30] This iteration count is therefore a trade-off between the security of the service and the computational load on the authentication server side. The original bcrypt article[31] explains how to select such iteration count and the impact it has on security. A more recent research article from C. Percival[32] tackles the impact of iteration count on hash functions, including bcrypt, considering the price it costs to crack a password in 1 year.

Only a few years ago the "normal" iteration count on law enforcement relevant algorithm (such as WPA2 or TrueCrypt) was in the area 1.000 – 10.000. Nowadays the iteration count is in the area 10.000 – 1.000.000. Since the time it takes is now 10 – 100 times longer, the impact on the decryption platform is linear; it can be directly translated to the current need to use 1000 GPUs instead of 10-100 previously to perform the same decryption task in the same amount of time. An increased iteration count leads to slower processing and a lower success rate for law enforcement decryption. This technological development leads to disadvantages for law enforcement when attempting to gain lawful access to criminal devices.

[28] https://www.information-age.com/homegrown-encryption-threatens-millions-smart-grid-devices-123459466/
[29] https://dev.to/devmazee2057282/php-security-passwords-1moi#
[30] https://dev.to/devmazee2057282/php-security-passwords-1moi#
[31] https://www.usenix.org/legacy/events/usenix99/provos/provos.pdf
[32] http://www.tarsnap.com/scrypt/scrypt.pdf

Technical box 2:

Rainbow tables in a nutshell

A rainbow table is a data structure created by P. Oechslin[33] improving the Hellman table, a time-memory trade-off. They allow retrieving the input of a one-way function, also called the preimage, in a very short time at the price of a heavy but unique pre-computation step and the storage of tables. This structure can therefore be used to retrieve the password from a hash value under certain conditions. The pre-computation and recovery steps are described below before underlining the requirements to make rainbow tables useful in practice.

The **pre-computation step** aims at building multiple hash chains. Each chain starts with a password, typically randomly selected. This password is hashed and the output is given to a reduction function which generates a new password. This succession of hashing and reduction is done several thousand times until a certain ending condition is met depending of the type of table used. Only the first and last elements of each chain are stored.

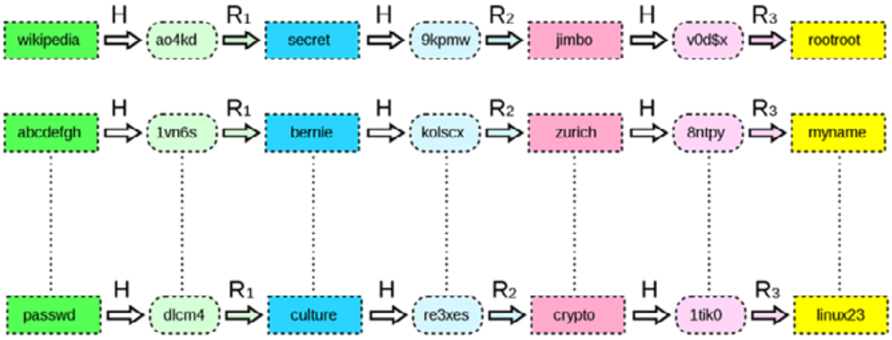

Figure 3 Pre-computation step[34]

The recovery step consists in re-building a chain from the known hash value. Each obtained value is compared with all the ends of chains stored in the table. In case of a match, the chain is reconstructed from the starting value that is stored in the table. In ideal conditions, the password will therefore be contained in the chain and properly recovered.

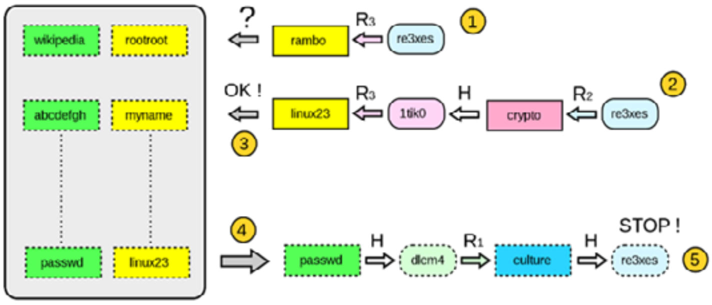

Figure 4 Recovery Step[35]

Constraints: A rainbow table is constructed for a pre-defined search space, e.g. all passwords up to 8 characters. The purpose of a table is to have, ideally, a full coverage of this space and therefore the pre-computation step should compute at least once every potential input. In practice, the coverage of a rainbow table is never total due to the required randomness of the reduction function.

[33] https://link.springer.com/chapter/10.1007/978-3-540-45146-4_36
[34] Source : https://commons.wikimedia.org/wiki/File:Rainbow_table1.svg
[35] Source: https://fr.wikipedia.org/wiki/Rainbow_table#/media/Fichier:Simple_rainbow_search.svg

When a salt is used by a service, the salt must be appended to the input as well at the building time of the rainbow table. This reduces drastically the size of the password space to keep a practical processing time for the pre-computing step. For example, if building a rainbow table for hash function inputs of up to 8 characters is considered feasible, but the salt is 3 characters, then the resulting space is limited to passwords of up to 5 characters. In this type of scenarios, rainbow tables are no longer relevant, as it usually becomes more efficient to conduct directly an exhaustive search.

4.4 ON-CLIENT (BROWSER) PASSWORD POLICY CHECKING MECHANISMS

Part of the challenge surrounding encryption refers to a matter of governance. Parallel to technological developments are policies introduced and decisions made by technology companies, which influence the ability of law enforcement to access user data for the purposes of criminal investigations.

This includes newly introduced password policies, where companies now use large quantities of passwords from leaked sites as a reference database for bad passwords, for instance in domain password policies (DPP) or in browser password field (BPF) checks.[36] The user technically cannot use a 'bad password' anymore. This means that passwords of suspects become more difficult to guess and detect. This is a security measure, which enhances the level of protection for users, but unfortunately also a measure, which criminals benefit from, as law enforcement attempts to decrypt the criminal's passwords also becomes more difficult.

Google, for instance, alerts Chrome browser users of weak or compromised passwords linking their password policies to a reference database called ''have I been pwned'' (HIBP)[37]. Google performs the checks in real time as Chrome users visit a password protected website. Bad passwords will trigger a red dialogue box alerting users to take action to better protect their account. The new policy integrates a feature previously only available via a Google Chrome browser extension called Password Checkup.[38] However, the password checking feature is now integrated into Google Accounts and no longer requires the browser extension. Users who allow their Google Chrome browser to store passwords for sites will receive an alert, but if a user declines to have the Chrome browser "save" their password for a specific site, there is no red flag that the password is weak or compromised when visiting the site.[39]

The "password problem" has worried the security industry for years. Poor quality passwords greatly amplifying many of the major issues that afflict the cybersecurity landscape. To deal with this issue, the HIBP service, for consumers wanting to know if their user names and passwords have been compromised in a data breach, has been launched.[40] To benefit from this service, other browsers have sought to test and implement similar solutions, such as Mozilla's Firefox Monitor, which leverages a partnership with Cloudflare and HIBP (Firefox Monitor relies on HIBP's API endpoints) to create a HIBP duplicate to bring the service to a larger audience.[41] Firefox Monitor users can see the details on sites and other sources of breaches and the types of personal data exposed in each breach, and receive recommendations on what to do in the case of a data breach. Mozilla announced it is also considering a service to notify people when new breaches are found to include their personal data.[42]

The importance of these developments cannot be underestimated. They are integral to safeguarding the security of electronic communications networks and services, and privacy of electronic data and fundamental rights of all users, and limit the success of attacks to gain access to personal and corporate devices. Further thinking is required to identify feasible alternative solutions that preserve law enforcement's ability to detect, investigate and prosecute criminals effectively, whilst protecting the privacy and security of communications.

4.5 ODOH-OBLIVIOUS DNS OVER HTTPS

As presented in the last Observatory Function report, the Domain Name System (DNS) is one of the most important databases in the internet infrastructure. Increased concern over the monitoring of DNS traffic (Figure 4) has led to standardisation of modern DNS resolution protocols that make use of encryption, one of them being DNS over HTTPs (DoH) (Figure 5).

Many Web applications, among them Internet browsers like Mozilla Firefox, have started to deploy DoH. Historically, the default DNS provider was automatically assigned by the network operator (i.e. the user's Internet Service Provider [ISP]), or a system administrator within enterprise environments, or could be personally selected by the end-

[36] https://threatpost.com/google-adds-password-checkup-feature-to-chrome-browser/148838/
[37] HIBP offers a free service for consumers wanting to know if their user names and passwords have been compromised in a data breach.
[38] https://threatpost.com/google-adds-password-checkup-feature-to-chrome-browser/148838/
[39] https://threatpost.com/google-adds-password-checkup-feature-to-chrome-browser/148838/
[40] https://threatpost.com/troy-hunt-sell-have-i-been-pwnd/145565/
[41] https://threatpost.com/troy-hunt-sell-have-i-been-pwnd/145565/
[42] https://threatpost.com/troy-hunt-sell-have-i-been-pwnd/145565/

user following a few configuration steps. Now, DoH allows browsers and other applications to send DNS queries directly to their chosen DNS resolver via Https.[43]

More recently, in a second move, companies such as Cloudflare and Apple, announced a new proposed DNS standard that separates IP addresses from queries, preventing an entity from seeing both at the same time. The protocol is being called Oblivious DNS over HTTPS (Figure 6), or ODoH, and is available on open source.[44] The overall aim of ODoH is to decouple client proxies from resolvers. ODoH adds a layer of encryption around the DNS query and sends it through a proxy server, which acts as a go-between the internet user and the website they want to visit. Because the DNS query is encrypted, the proxy cannot see what is being sent, but rather acts as a shield to prevent the DNS resolver from seeing who sent the query to begin with.[45] Open sources indicate that the actual implementation of this protocol may take some years, but companies like Firefox stressed their interest in experimenting with oDoH already now.[46]

While addressing the security problems of DNS is very welcome, the implementation of DoH or oDoH by private companies raises some further concerns. Despite the anticipated benefits of DoH, a number of challenges and concerns were raised, including user privacy, network security and access to criminal data.[47] For instance, one of the main objectives of deploying DoH is to increase users' privacy by encrypting the communication between the user's device and the resolver, making DNS traffic monitoring and intercepting more challenging. This is a significant benefit and securing DNS communication and traffic is important, but researchers claim that DNS monitoring will just be moved from ISP level to application level. As a result, over-the-top providers will gain access to massive amounts of user data, which can then be monetised.

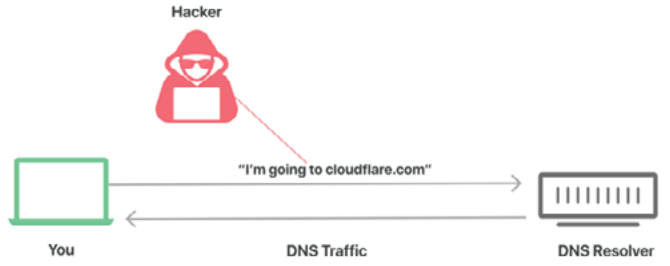

Figure 5 Traditional DNS requests[48]

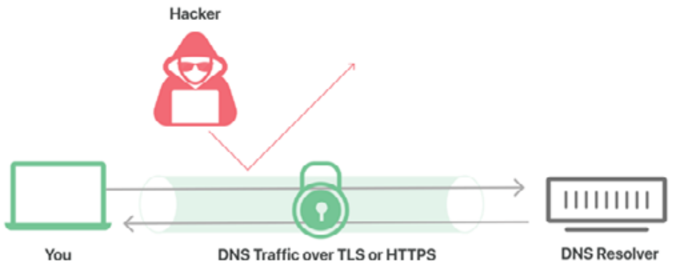

Figure 6 DoH requests[49]

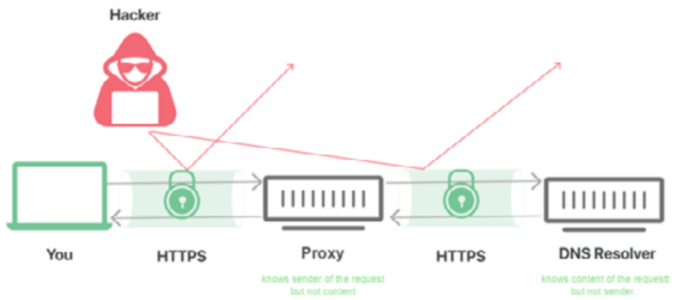
Hacker
You
HTTPS
Proxy
knows sender of the request but not content
HTTPS
DNS Resolver
knows content of the request but not sender.

Figure 7 ODoH requests

As queries to the DNS will be encrypted, interception will be more complicated for law enforcement as well, and countries hosting the majority of the DoH service providers will receive the vast majority of the internet DNS lookups, in contrast to the previous national decentralisation of these sensitive queries. As a consequence of this, most of the oDoH-related investigations will involve international legal requests to those jurisdictions. The oDoH provider is likely to have a privacy policy in place, which will make it even more difficult for law enforcement to receive the necessary information for crime investigations.

[43] 2nd Observatory Function report
[44] http://www.circleid.com/posts/20201209-new-privacy-focused-dns-protocol-called-oblivious-released/
[45] https://www.schneier.com/blog/archives/2020/12/oblivious-dns-over-https.html
[46] https://www.zdnet.com/article/oblivious-doh-cloudflare-supports-a-new-privacy-security-focused-dns-standard/
[47] https://www.zdnet.com/article/dns-over-https-causes-more-problems-than-it-solves-experts-say/
[48] Source : https://www.cloudflare.com/es-la/learning/dns/dns-over-tls/
[49] Source: https://www.cloudflare.com/es-la/learning/dns/dns-over-tls/

4.6 QUANTUM COMPUTING

4.6.1. UPCOMING OPPORTUNITIES AND CHALLENGES

The First report of the Observatory Function already highlighted the impact that the progress made in quantum computing will have on encryption and more generally on cryptography. One of the statements in the previous report underlines that we are still decades away from a usable quantum computer. In the meantime, Google has published a research article in Nature[50] in which they claim to have reached quantum supremacy for the first time for calculating a mathematical problem[51]. The following section aims to update and complement the information already provided in the first observatory.

Quantum computers experience progress and the quantum volume[52] continues to grow. As an example, IBM has announced the development of a 127 qubits machine for 2021 and a 1.000 qubits machine for 2023[53]. The machine used by Google for the experiments published in Nature is a 53-qubits device. The quantum processor, called Sycamore, took around 3 minutes to produce results that would have taken 10.000 years on the most advanced supercomputer. The achievement of quantum supremacy by Google is disputed among the community and is not the point of this report. What remains valid is that a usable quantum computer that would affect cryptography is not there yet and, while it will probably come sooner than later, it remains hard to predict when this will occur.

Technical box 3:

What Quantum computers might be capable of and what they will not

Cryptography is not solely about encryption and can offer many properties other than confidentiality, such as authentication, integrity and non-repudiation. Depending on the manner the security keys are handled and shared, cryptography is divided in two main groups, symmetric and asymmetric cryptography. In addition to these two families, cryptographically secure hash functions constitute a third group, mostly used as a functional building block of many cryptosystems (e.g. digital signatures). We regroup below the currently known quantum attacks that might affect typical cryptography. Note that the development of quantum algorithms is still a new and experimental field of research. There is no guarantee that in the future no other approaches could be developed, which would further impact cryptography.

- Asymmetric cryptography: the most well-known quantum algorithm impacting asymmetric cryptosystems is Shor's algorithm. This algorithm can find a solution to the factorisation problem and the discrete logarithm problem on which current asymmetric cryptographic standards, such as RSA and ECC, rely. The complexity of the Shor's algorithm is polynomial while there is no known polynomial algorithm[54] able to factorise a number with a classic computer.
- Symmetric cryptography: quantum computing is not considered as a major threat to this family of cryptographic functions. Thanks to a better search algorithm, i.e. Grover's algorithm, a quadratic speed-up is expected. In other words, while AES-128 is considered to bring a security level of 128 bits against classical computer, it only brings a security level of 64 bits against quantum computer. Doubling the size of the key is therefore sufficient to maintain an equivalent level of security.
- Hash Functions: one expected security property of hash functions is the collision resistance. In other words, it is difficult to find two inputs leading to the same output. Brassard et al.[55] have described a quantum birthday attack relying on Grover's search algorithm making the search for a collision faster. Many of the currently used hash functions would be impacted by such an attack. Nevertheless, SHA-2 and SHA-3 are still considered as quantum safe thanks to their longer input.

[50] https://www.nature.com/articles/s41586-019-1666-5

[51] A similar claim has been announced in December 2020 in a Science article

[52] Following IBM definition, the quantum volume is a metric considering the number of qubits of a computer but additionally how good the error correction is and the capacity of parallelism.

[53] https://www.sciencemag.org/news/2020/09/ibm-promises-1000-qubit-quantum-computer-milestone-2023

[54] A recent research article has been published in 2021 presenting a polynomial algorithm able to factorize large numbers claiming that it "destroys the RSA cryptosystem". The results presented in the article still need to be validated.

[55] https://doi.org/10.1145/261342.261346

4.6.2. A STANDARDISATION EFFORT INITIATED

As described in technical box 3 , most cryptographic standards will be impacted by the capacity of expected quantum computers. In accordance to this statement, standardisation institutions have initiated measures to address the upcoming security risks.

The US NIST[56] initiated in 2017 a series of post-quantum cryptography competitions similar to those organised for the advanced encryption standard (AES) for symmetric cryptography and SHA-3 for hash functions. Sixty-nine candidates have been selected for the first round. The NISTIR 8309 report[57] presents the result of the second round where the twenty-six successful candidates from the first round have been analysed. This report marks the end of the second round and the beginning of the third and last round for which fifteen candidates have been selected and divided into two categories focusing on i) Public-key Encryption and Key-establishment Algorithms ii) Digital Signature Algorithms. The proposed candidates will address difficult mathematical problems (e.g. lattice-based, multivariate-based or code-based cryptography) that, up to the current knowledge, cannot be practically solved by either classical or quantum computers.

The European Telecommunications Standards Institute (ETSI) has established a Quantum-Safe Cryptography (QSC) working group[58] which "aims to assess and make recommendations for quantum-safe cryptographic primitives, protocols and implementation considerations, taking into consideration both the current state of academic cryptography research and quantum algorithm research, as well as industrial requirements for real-world deployment." The working group has released in August 2020 the technical report TR 103 619[59] containing migration strategies from a non-quantum safe cryptographic state to a fully quantum safe cryptographic state. In February 2021, ETSI organised the Quantum Safe Cryptography Technical Event[60], during which, one day was dedicated to the standardization initiatives worldwide, such as the NIST offering previously described.

Post-quantum cryptography is not necessarily the end of the game for successful decryption. The coming standards shall be resistant to known attacks, either quantum or classical, yet quantum computers will offer new possibilities. As an example, it is possible to record encrypted communications that cannot be decrypted today but that could be in the future. While underlining the need to do the quantum migration recommended by ETSI, this might represent the opportunity to close cold cases. Furthermore, quantum computing could eventually offer new tools and methods for cryptanalysis and decryption that are not yet known. It can consequently be beneficial for law enforcers to invest resources in quantum programming facilities to start building expertise in quantum capabilities.

[56] https://www.nist.gov/
[57] https://csrc.nist.gov/publications/detail/nistir/8309/final
[58] https://www.etsi.org/technologies/quantum-safe-cryptography
[59] https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf
[60] https://www.etsi.org/events/1870-etsi-quantum-safe-cryptography-technical-event

4.7 CONCLUSION

The need for law enforcement to gather digital evidence from devices used by criminals is essential to conduct criminal investigations, but the answers to these challenges are complex and vary within EU jurisdictions. As the previous Observatory Function reports and this chapter have demonstrated, encryption as a tool provides benefits for society as a whole. It is a fundamental part of a safe and productive internet environment for the vast majority of users. Nonetheless, it is important to emphasize and highlight potential criminal abuse of encryption by organised crime groups as part of their modus operandi. This is where the challenge for law enforcement and prosecution commences.

The new encryption challenges faced by law enforcement include higher obstacles when conducting reverse engineering, particularly due to encrypted hardware combined with encrypted software or DNS traffic. At the same time, new security policies introduced by private companies increase the iteration count and provide stronger protection tools. An increased iteration count leads to slower processing and a lower success rate for law enforcement decryption during criminal investigations. As seen in the examples above, criminals already take advantage of encrypted communication on mobile devices that are designed for a criminal target group. On the other hand, technology companies in their attempts to improve user and cyber security, introduce new policies and services that lead, even if inadvertently, to higher protection of criminal activity and additional difficulties for law enforcement in conducting criminal investigations.

While, law enforcement and the judiciary work towards solutions that take into consideration the protection of fundamental rights and security of society as a whole, encryption technology and tools become more robust and develop at such a pace that legislation cannot always keep up. Resulting in greater difficulty for law enforcement to lawfully access digital evidence. While the debate about how to approach encryption-related challenges continues, technological developments also progress.

5. ENCROCHAT CASE: AN EXAMPLE OF GOOD PRACTICE

French authorities first detected the use of EncroChat services in 2017, with regular discoveries of these phones in operations against organised crime groups. EncroChat was operating from servers in France and provided encrypted digital communication to users worldwide. By early 2020, EncroChat had a very high share of users presumably engaged in criminal activity. Law enforcement frequently seized these devices as evidence in investigations, but standard forensic extraction devices were not able to overcome EncroChat's device security measures.

Given the global use of this communication tool, French authorities decided to open a case at Eurojust, towards the Netherlands in 2019. Eurojust facilitated the creation of a JIT between France and the Netherlands in April 2020, with the participation of Europol.

Eventually, it was possible for French authorities, based on the French legal provisions[61], and following intense research and development efforts to bypass the technical obstacles and circumvent encryption to obtain access to the users' communications.[62] The JIT made it possible to intercept, share and analyse messages that were exchanged between criminals to plan serious crimes.

Throughout the investigation, the JIT members organised five coordination meetings at Eurojust to ensure coordination between all involved parties, identify parallel or linked investigations, facilitate information exchange, decide on the most suitable framework for cooperation and solve potential conflicts of jurisdiction.

Europol has been actively involved in the investigations led by France and the Netherlands since 2018. The agency supported the JIT by promoting and arranging international cooperation, providing extensive technical coordination and analytical support for the visualisation and exploitation of the intercepted data, financial support, and a secured platform for the exchange of information between the countries involved. Law enforcement monitored and analysed in real time during a three month period, millions of messages. Criminal business providers realised and communicated to all users that devices had been compromised in June 2020, officially shutting down the network[63].

Over 100 million intercepted text messages exchanged by tens of thousands of users, mostly based in Europe, triggered a significant number of investigations mostly concerning drugs trafficking and connected criminal activities such as violent crimes, money laundering and corruption. The international dimension of criminal networks and high level of connectivity between organised crime groups is undeniable. Criminal markets appear fluid and competitive and criminal services are easily available in criminal networks. The amount of EncroChat users intercepted while carrying out their illicit businesses together with the high subscription fee paid for the service, show clearly how encrypted communication channels played a crucial role in this networked and dynamic criminal scene.

Further developments in the investigations led to organising the processing of the data gathered. The data was in the first instance shared with the Netherlands through the JIT. Other countries that wanted to obtain decrypted data from EncroChat, to use it as evidence in their own investigations, requested it from France via an EIO or MLA request. Decrypted data and information has been supplied to hundreds of ongoing investigations, providing insights and access to new evidence and resulting in the disruption of criminal activities including large-scale drug trafficking, money laundering and other forms of serious and violent crime, such as murder, extortion, robbery, grievous assault and hostage taking. At the same time, the available data is triggering a very large number of new criminal investigations into organised crime across the European continent and beyond.

EncroChat was a legally incorporated service provider offering encrypted software and hardware solutions for secure communication, with servers based in France. The service included the use of a dedicated mobile phone: a

[61] Article 706-102-1 Criminal Procedure Code
[62] For more information on the French investigation, see here
[63] Europol, Press Release: Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe, 2 July 2020

specifically set Android device where only the EncroChat communication application was installed. All functions considered a vulnerability in terms of traceability, such as GPS, microphone and USB port, were disabled. The dual operating system hid the encrypted interface and any association between SIM card, device and user was removed. Additional security measures were put in place as a countermeasure to potential interception or compromising of the device. These features included the remote deletion of all data with the assistance of a reseller or helpdesk, the remote deletion of messages on the recipient end and the immediate deletion of all data through the insertion of a specific PIN code or by inserting the wrong password[64] a number of times.

The company was advertising the service guaranteeing full communication anonymity following a payment of a one-off sum of around EUR 1 000 for the purchase of the device and a monthly subscription. The purchase of the device and subscription were channelled through an international network of trusted resellers and a 24/7 helpdesk support was included in the fee[65].

[64] Europol, Press Release: Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe, 2 July 2020
[65] Europol, Press Release: Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe, 2 July 2020

6. POLICY DEVELOPMENTS INFLUENCING AND SHAPING THE DEBATE ON ENCRYPTION

This section of the report follows up on a number of elements raised in the second report, which briefly outlined the progression of the encryption debate. It aims to provide a snapshot of some of the most recent ongoing policy developments relating to the criminal use of encryption and its implications for criminal investigations. This chapter complements the other parts of the report through factual information on the developments taking place in specific key countries and regions. It introduces a third viewpoint that when aligned with the legal and technical considerations can provide readers with a more complete picture of a number of key equities in the discussion on encryption. As this is the first instance where the policy angle is being included, a decision has been taken to only focus on policy developments that purely relate to encryption. Subsequent reports may consider a broader perspective to inform readers about policy developments that are ancillary to the efforts on encryption.

6.1 INTRODUCTION TO THE POLICY DEBATE

As alluded to several times in this and the previous report the importance of encryption technology is considerable. It is at the heart of digital security, making it part of our daily lives. It is an important tool for the protection of fundamental rights, including privacy, confidentiality of communications and personal data[66], a key component in keeping intellectual property secure[67], and to provide a secure means of communication for journalists, dissidents and vulnerable groups[68]. More broadly, the European Commission's 2020 Cybersecurity Strategy references the need for encryption in ultra-secure communications infrastructures, as a means of protecting critical communication and data assets and in the development of cyber defence capabilities[69].

This importance has to be balanced with the use of encryption by criminals which has become more commonplace, extending its use to various crime areas, including child sexual abuse, and other forms of serious and organised crime[70]. This new reality creates more strain on already limited resources and challenges law enforcement's capability to gain lawful access to evidence needed to proceed with criminal investigations and prosecution[71].

Concurrently, there is a legitimate expectation that rules apply online as they do offline, as the EU has committed to ensure. People in the EU are becoming increasingly worried about security online[72], as well as about rising exposure to hate speech, other abusive and criminal behaviour, and use of encryption[73] as a weapon in the form of ransomware[74]. Law enforcement continue to argue that important parts of the digital world are "going dark", and there is a need for reliable and sufficiently rapid and scalable ways to access plaintext (decrypted data and messages)[75].

Key stakeholders, including civil society and data protection organisations, a number of cryptography experts and the big tech industry have signalled their concern. They take the position that certain actions, such as setting out regulation that mandates lawful access to decrypted data, would pose unacceptable risks to cybersecurity, privacy and fundamental rights and in the longer term hamper

[66] Existing European Union legislation specifically refers to the use of encryption as a possible measure to ensure an appropriate level of security for the protection of the fundamental rights and strengthening cybersecurity: Article 32(1a), 34(3a), 6(4e), recital (83) of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC; recital (60), article 31(3a) of the Law Enforcement Directive; recital (20) in conjunction with article 4 of the ePrivacy Directive 2002/58/EC; recital (40) of Regulation (EU) 2019/881 (Cybersecurity Act).

[67] From the report on Cybersecurity in the European Digital Single Market

[68] *Moving the encryption policy conversation forward*. Report by Carnegie endowment for international peace encryption working group

[69] The EU's Cybersecurity Strategy for the digital Decade JOIN(2020) 18 final

[70] These concerns have been recorded in the Internet Crime Threat Assessments (iOCTA) issued in October 2020

[71] For more extensive information on the legal and technological challenges posed by encryption, please refer to the previous two observatory reports on encryption.

[72] Europeans' attitudes towards cyber security. Special Eurobarometer survey of 6 June 2020

[73] Internet Organised Crime Threat Assessment 2020: cyber-dependent crime.

[74] Since the start of the No More Ransom initiative, there have been 4.2 million visitors from 188 countries to the decryption tool repository. It is estimated that this tool has stopped $632 million in ransom demands from ending in criminals' pockets

[75] Decrypting the Encryption Debate: A Framework for Decision Makers. Consensus study report by the National Academics of sciences, engineering and medicine.

innovation both in encryption technologies and more broadly in technology that relies on encryption. Additionally, critics point out that the use of connected smart electronic devices has resulted in a richness of generally unencrypted metadata that law enforcement could possibly rely on to a larger extent in criminal investigations.

The challenge for law enforcement remains obtaining information-in-clear, or information that can be read and processed in an appropriate format, where law enforcement have the means to do so e.g. a warrant to access that information for investigatory purposes. The use of encryption, particularly end-to-end encryption results in decreased or no visibility for companies, limiting their ability to detect harmful and illegal conduct and material, and their ability to provide information that can support investigations and prosecution of criminals.

Law enforcement report that encryption has pervaded the vast majority of their caseload, notwithstanding the lacunae in statistics about the impact of encryption on investigations, as the lack of visibility due to encryption makes it difficult to quantify the extent of the problem. Assessing the effects that regulation would have on this landscape is equally difficult. One may only speculate about the reactionary behaviours of criminals, including whether they would turn to noncompliant encryption service providers, if the government required companies to provide lawful access solutions.

These different concerns have resulted in tensions that, with the exception of a few key efforts, have fuelled a complicated debate. It has remained mostly theoretical and over-simplistic, characterised by 'privacy' and 'security' advocates positioned at opposite ends of the spectrum, requesting absolutist approaches[76]. Policy-makers are left with the onerous task of reconciling the various dimensions of security, from cyber and terrorist threats to fundamental rights, privacy and data protection.

6.2 DEVELOPMENTS WITHIN THE EUROPEAN UNION

Like many other governments around the world, the EU is confronted with multiple perspectives on issues relating to encryption. Encryption linked to criminal investigations was propelled to the top of the political agenda following the spate of terrorist attacks that hit Europe between 2014-2016[77]. EU Member States called for solutions to allow law enforcement and other competent authorities to gain lawful access to digital evidence, without prohibiting or weakening encryption, and in full respect of privacy and fair trial guarantees consistent with applicable law[78] at the EU Member States' Justice and Home Affairs (JHA) Ministerial meeting of December 2016. Heads of States or Governments reiterated this call in June 2017[79] to ensure that competent authorities were not stalled by lack of visibility to vital data in the face of future attacks.

In response, the Commission proposed, in its 11th progress report towards an effective and genuine Security Union[80], a set of six practical measures to support law enforcement and the judiciary when they encounter encryption in criminal investigations. The focus of these measures was on data "at rest", that is, data stored in encrypted devices and hard drives. The measures proposed constituted funding and coordination efforts. The Commission also committed to further internal reflection to attempt to address the more complex aspects of encryption, such as e2ee in electronic communications applications.

Germany revisited the topic of encryption during its term of the Presidency to the Council of the EU at the second half of 2020. The Presidency led discussion in the Council that resulted in the adoption of a resolution[81] on encryption on the 24th November 2020. This marked the first instance that a common EU-wide position has been set out on the topic, which considers the importance of encryption, recognises the challenges and proposes concrete action in collaboration with industry. The resolution seeks to address encryption in its broadest sense, covering different aspects

[76] One key effort worth mentioning in this regard, is the work carried out by the Carnegie Endowment for International Peace, which set up an encryption working group to discuss ways to promote a more pragmatic and constructive debate on the benefits and challenges of the increasing use of encryption. The group suggested potential ways to evaluate the societal impact, including both benefits and risks, of any proposed approaches to try to address the deadlock over law enforcement access to encrypted data. The group focused on mobile phone device encryption, detailing specific approaches to evaluate proposals focusing on law enforcement's access to encrypted mobile phones.

[77] Europe saw a rise in Islamic terrorist incidents between 2014-2016. These include the Jewish Museum of Belgium shootings in May 2014, the 2015 November Paris attacks and July 2016 Nice truck attack, the Brussels bombings of March 2016 and the Ataturk Airport Attack in June 2016.

[78] The issue of encryption was discussed during the Justice and Home Affairs (JHA) Council meeting of December 2016

[79] Refer to the European Council conclusions on security and defence adopted in June 2017

[80] Eleventh progress report towards an effective and genuine Security Union, COM/2017/608 final

[81] https://press-releases/2020/12/14/encryption-council-adopts-resolution-on-security-through-encryption-and-security-despite-encryption/

and use cases. The adoption of the resolution created momentum for work in the Council and set out a number of expectations that should be handled by subsequent presidencies in advancing this file.

ENCRYPTION AND THE FIGHT AGAINST CHILD SEXUAL ABUSE

The exponential developments of technology including encrypted communications, social media platforms and other openly accessible communication services shas made it easier for perpetrators to contact, groom and sexually abuse children, and produce, share, livestream and obtain child abuse material. Encrypted communications have made it easier for child sex offenders to hide their criminal activities criminal activity, evading both electronic service providers and law enforcement. These trends have resulted in a sharp increase in online child sexual abuse, whichhas been made worse during the COVID-19 pandemic. Children are spending more time than before online and at home, possibly unsupervised and at increased risk of coming into contact with predators[82].

In 2020, The UK Internet Watch Foundation found that every three minutes a web page showed a child being sexually abused[83]. The National Center for Missing and Exploited Children (NCMEC) in the US received almost 22 million reports in 2020 alone[84] of instances of CSA detected by online service providers. These reports include images and videos but also situations that pose an imminent danger to children, such as arrangements to physically meet and abuse a child, and have been instrumental in saving victims from ongoing situations of abuse. Electronic service providers made up the majority of reports received (21.7milliion) with around 20 million of these reports originating from Facebook and its different social media and electronic communications platforms (Messenger, Instagram and WhatsApp)[85].

Facebook's announcement to roll-out e2ee across all of its messaging platforms, as part of their privacy-focused vision for social networking[86] was met with outrage by child safety organisations[87]. The announcement also resulted in governments calling on Facebook to maintain lawful access for law enforcement to the content of communications and ensure the safety of Facebook users and the wider public including children online[88]. Once encryption is implemented, as much as 2/3 of these reports submitted by Facebook could be lost, as current detection tools used by companies do not work on e2ee communications.

In an effort to overcome this problem, in 2020, the Commission, together with industry, cryptography experts, members of civil society organisations and competent authorities, conducted an expert process to identify technical solutions that may help companies to specifically detect child sexual abuse in e2ee electronic communications[89].

6.3 DEVELOPMENTS OUTSIDE OF THE EUROPEAN UNION

A similar evolution to the debate within the EU is mirrored more broadly. A number of prominent third countries and country alliances have weighed in on the issue of lawful access by law enforcement authorities to encrypted material. This third report of the observatory function on encryption will focus on developments in the United States, and Australia, and provide some insight into the collective work of the Five Eyes Partnership. Light is being shone on these particular strands due to the timeliness of developments, their links to the progression of the policy debate within the EU, and the likelihood that these developments may be reflected in the discussion on encryption within the EU.

6.3.1. ENCRYPTION AND THE FIVE EYES COUNTRY PARTNERSHIP

Australia, Canada, New Zealand, the United Kingdom and the United States have been vocal about the need to address the challenges created by criminals' use of encryption, highlighting it as security challenges common to all[90]. On 11 October 2020, the Five Eyes countries, together with the Governments of Japan and India published an international statement[91] setting out the impact on public safety of e2ee that precludes lawful

[82] WePROTECT Global Alliance, World Childhood Foundation, Unicef, UNDOC, WHO, ITU, End Violence Against Children and UNESCO, COVID-19 and its implications for protecting children online.
[83] Internet Watch Foundation, 2020 Annual report,
[84] 2020 reports by electronic service providers (ESP) to NCMEC
[85] https://www.missingkids.org/content/dam/missingkids/gethelp/2019-reports-by-esp.pdf
[86] https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/
[87] End-to-end encryption: Ignoring abuse won't stop it: NCMEC's statement on Facebook's decision to roll out e2ee in all it's messaging platforms.
[88] Open letter to Facebook
[89] EU Strategy for a more effective fight against child sexual abuse COM(2020) 607 final.
[90] Five Country Ministerial 2017: Joint Communiqué
[91] International Statement: End-to-end Encryption and Public Safety

access to the content of communications. The statement aimed to generate greater public awareness of the issues and encourage technology companies to step up their engagement on issues of public safety in relation to how their products are designed and deployed.

This effort follows the joint Australia, UK and US open letter to Facebook of 4 October 2019, and responds to the trend of online communication platforms to include e2ee on their services, and indeed other industry services and hardware that come built-in with encryption measures that preclude, by virtue of their design, access by law enforcement when this is lawfully authorized and proportionate.

The international statement attracted plenty of controversy. In an open letter[92] responding to the statement, The Internet Society, Global Partners Digital, and the Centre for Democracy and Technology (CDT), all members of the Steering Committee of the Global encryption Coalition[93], called it an "ill-considered attempt to undermine use of end-to-end encrypted communications". They warned that pursuing such a course of action would result in devastating consequences to the security of people and countries worldwide.

The Five Countries are also concerned about the impact of end-to-end encryption on the ability of companies to fulfil their voluntary commitments to take action to protect children online. In 2020, the Five Countries launched the Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse (the Voluntary Principles) which were developed with the companies Facebook, Google, Microsoft, Twitter, Roblox and Snap, NGOs and academia, and provide a high-level best practice framework for online platforms and services to combat child sexual abuse. The Voluntary Principles outline 11 ways for companies to take action against online child sexual abuse. In particular, encryption could prevent companies from fulfilling their commitments under the Voluntary Principles to prevent and identify child sexual abuse material and report it to law enforcement.

6.3.2. FOCUS ON AUSTRALIA. THE ACCESS AND ASSISTANCE ACT

In late 2018, the Australian Federal Parliament enacted significant changes to existing electronic surveillance legislation. The Telecommunications and Other legislation Amendment (Assistance and Access) Act 2018 (Cth) (TOLA)[94] addresses the impact of technological obstacles to national security and law enforcement investigations, such as the use of encrypted communications and devices.

Specifically, the legislation:

- Establishes a framework for Australian agencies to request or compel assistance from communications providers in their investigations and operations.
- Establishes new 'computer access warrants' for law enforcement
- Strengthens agencies' existing search and seizures powers for computers (including all mobile devices) to access unencrypted data

TOLA introduced a technologically neutral industry assistance framework that established a structure for Australian agencies and industry to collaborate on addressing technological obstacles to investigations into serious crime and threats to national security.

The framework allows:

- Agencies to request voluntary assistance from providers with a technical assistance request (TAR),
- Agencies to require assistance from providers with a technical assistance notice (TAN) where the provider is already capable of giving the required assistance, and
- The Australian Attorney-General, with the approval of the Minister for Communications, may require a provider to develop a new capability with a technical capability notice (TCN), where the provider is not already able to offer that type of assistance.

Robust safeguards and oversight arrangements ensure that any technical assistance being sought is reasonable and proportionate, practicable and technically feasible and does not fundamentally weaken cybersecurity.

USE OF THE FRAMEWORK AND IMPACT ON INDUSTRY

Industry criticism of TOLA has focused on the perceived impact the industry assistance framework has had on the competitiveness of the communications and technology industry. However, TOLA does not impose any standing obligations on industry, and does not require companies to change the way in which they conduct their business operations in Australia. The framework is designed to ensure agencies can operate in light of new and emerging technologies, without imposing an undue burden on

[92] CDT, GPD and Internet Society respond to new statement from Five Eyes Alliance.
[93] The Global Encryption Coalition brings together entities to promote and defend encryption in key countries and multilateral gatherings where it is under threat.
[94] Lawful access to telecommunications. The assistance and Access Act 2018.

providers, and without compromising the competitiveness and reputation of industry's products and services.

Since TOLA came into force on 9 December 2018, Australian agencies have used the industry assistance framework in a targeted fashion to resolve technical issues impeding the investigation of transnational, serious and organise crime, cybercrime and serious crimes against the person, as well as on matters of national security, in cooperation with industry.

By 30 June 2020, 18 voluntary TARs had been used by law enforcement agencies. No compulsory TANs or TCNs were issued during the reporting period[95]. Additionally the Australian Security Intelligence Organisation (ASIO) reported making use of the industry assistance framework[96]

The reported figures indicate that Australian agencies are taking a collaborative approach with industry in the utilisation of the industry assistance framework by seeking voluntary assistance in the first instance to engender support and cooperation.

REVIEW OF TOLA

The Federal Parliamentary Joint Committee on Intelligence and Security (PJCIS)[97] was due to complete its third review of TOLA on 30 September 2020, however as of April 2021 the Committee has not yet published its report[98]. PJCIS referred some aspects of TOLA to the Independent National Security Legislation Monitor (INSLM)[99], the review of which was completed on 9 July 2020[100].

The INSLM found that TOLA is likely to be necessary and proportionate, subject to the implementation of the INSLM's central recommendations, which include:

- Establishing a new division of the Administrative Appeals Tribunal[101] to approve the issuing of compulsory technical assistance and technical capability notices,
- Raising the offence threshold so that, generally, an agency cannot obtain industry assistance for offences punishable by less than three years' imprisonment,
- Narrowing ASIO's voluntary assistance powers.

The Australian Government will consider the findings of both the INSLM and the PJCIS and when the PJCIS publishes its review of TOLA.

OPERATIONAL EXAMPLES OF THE POWERS IN ACTION

Australian Federal Police- Cybercrime- Remote Access Trojan malware[102]

This matter involved an investigation into the possession and use of "Imminent Monitor – Remote Access Trojan" (IM-RAT) malicious software (malware). The malware allowed remote and secret control over a victim's computer and other devices, to access and view files, record keystrokes and activate the computer's web camera.

A statistically high percentage of Australian-based purchasers of IM-RAT (14.2%) are named as respondents on domestic violence orders, and one of the purchasers is registered on the Child Sex Offender Register.

Without these powers, the Australian Federal Police (AFP) would have been unable to proactively investigate and capture relevant data and evidence stored in Australian and other participating countries, or identify victims and prosecute users of this malware. The TOLA powers also enabled the AFP, and partners, to identify and stop other serious crimes, including computer misuse, fraud, dealings in the proceeds of crime, narcotics and sexual offences.

An overt search warrant would have alerted the criminals using this malware, precluding further identification, disruption and prosecution on ancillary offending being facilitated by the malware. A traditional search warrant would only yield a limited subset of the customer database (noting the purchase may be made in cryptocurrency and untraceable), and this would not have assisted proactive or the targeting of investigations on the users of the malware.

OUTCOMES:

As at 30 November 2019 in relation to this investigation[103]:

- 85 warrants had been executed internationally
- 434 devices have been seized (laptops, phones, servers etc.)

[95] Telecommunications (Interception and Access) Act 1979". Annual Report 2018-19.
[96] ASIO must include classified statistics pursuant to their use of the industry assistance framework in their annual report presented to the Australian Minister for Home Affairs. This report is not published.
[97] The PJCIS' functions include building bipartisan support for national security legislation by reviewing national security bills introduced to Parliament and ensuring national security legislation remains necessary, proportionate and effective by conducting statutory reviews.
[98] Review of the amendments made by the Telecommunications and Other legislation Amendments (Assistance and Access) Act 2018.
[99] The INSLM independently reviews the operation, effectiveness and implications of national security and counter terrorism laws, and consider whether the laws contain appropriate protections for individual rights, remain proportionate to terrorism or national security threats, and remain necessary.
[100] Trust but Verify. A report Concerning the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 and related matters*
[101] The Administrative Appeals Tribunal (AAT) provides independent merits review of a wide range of administrative decisions made by the Australian Government. AAT members have a role in issuing electronic surveillance warrants to law enforcement agencies under Commonwealth legislation.
[102] Example sourced from Australian Federal Police Submission to the Parliamentary Joint Committee on Intelligence and Security Review of the Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018 (TOLA) of 6 August 2020.
[103] This case was supported by Europol and Eurojust;

- 13 people have been arrested (none yet in Australia)
- The website selling the malware has been taken down.

Cybercrime DDOS attack on government infrastructure[104]

The AFP used TOLA powers during an eight-month investigation into the use of a carriage service to make threats, identify data sets of compromised personal information, inform Australian government and public telecommunications infrastructure of cyber vulnerabilities and compromise and prevent online fraud. This was a parallel investigation to a State police operation investigating dedicated denial of service attacks against their own telephone infrastructure.

TOLA powers were of significant benefit in this investigation, as they enabled the AFP to obtain evidence from multiple electronic systems used by the alleged offender to commit a variety of offences. Information obtained using TOLA powers also identified further avenues of police enquiry, filled significant evidentiary gaps in relation to the alleged offending, and better-directed police resources in relation to this investigation. A significant proportion of material obtained using TOLA powers is relied on in a brief of evidence in relation to the accused.

OUTCOMES:

- Two men were charged on 14 June 2019 with offences including:
- Unauthorised access to data held on a computer;
- Using a carriage service to make a threat or cause serious harm;
- Dishonestly obtaining or dealing with personal financial information;
- Sabotage; and firearm offences

6.3.3. EFFORTS IN THE UNITED STATES

Following the 2016 San Bernardino legal dispute between Apple and the Federal Bureau of Investigations (FBI) over access to an encrypted iPhone, then Attorney General Barr made action on encryption one of his key priorities. AG Barr spoke about the importance of preserving lawful access to encrypted communications for law enforcement[105] and called out service providers, device manufacturers and application developers for developing and deploying technology that does allow for lawful access by law enforcement agencies under the appropriate safeguards.

He points to the need to balance the individual's right to privacy and the public's right to security in efforts that do away with online "law free" zones[106] that tip the scales against public safety by preventing effective law enforcement efforts, and sets clear comparisons between lawful access in the offline and online environments, and the need to preserve both equally. If this scrutiny is not retained in the online environment, it will further incentivise criminals to expand the scope of their activities online. In order to stop online communications from "going dark" Barr called firstly for collaborative efforts with industry and the private sector, but did not exclude the possibility of legislation.

THE EARN IT ACT AND LAWFUL ACCESS TO ENCRYPTED DATA ACT

Further to the calls for more balanced approaches Senators introduced two bills: the EARN IT Act (Eliminating Abusive and Rampant Neglect of interactive Technologies Act)[107] and the Lawful Access to Encrypted Data Act[108] in Congress. The EARN It Act is meant to combat online child sexual abuse through an amendment to Section 230, introduced as part of an amendment with the 1996 Communications Decency Act (CDA) to the Communications Act of 1934. The intent of Section 230 is to treat ISPs as a conduit for distribution, rather than content publishers, thus absolving them from responsibility over content they distribute.

The amendment under consideration would establish a National Commission on Online Child Sexual Exploitation Prevention, the purpose of which would be to develop and regularly update a manual of recommended best practices that assist ISPs to prevent, reduce and respond to online CSA. The bill also introduces two changes to Section 230(C)(2)'s liability, allowing any state to bring a lawsuit against an ISP if they fail to deal with CSA on their services, or if they allow e2ee on their services without means for lawful access. Finally the bill replaces the wording "child pornography" in existing laws with the more accurate "child sexual abuse material".

[103] This case was supported by Europol and Eurojust;

[104] Example sourced from Australian Federal Police Submission to the Parliamentary Joint Committee on Intelligence and Security Review of the Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018 (TOLA) of 6 August 2020.

[105] Keynote address at the International Conference on Cyber Security of 23 July 2019

[106] *Lawless Spaces: Warrant-proof encryption and its impact on child exploitation cases*. Event organised by the US Department of Justice on 4 October 2019

[107] https://www.congress.gov/bill/116th-congress/senate-bill/3398/text

[108] https://www.congress.gov/bill/116th-congress/senate-bill/4051/text

The Act was welcomed by child protection advocates, including NCMEC who praised the piece of legislation for recognizing the impact of online child sexual abuse and for providing a roadmap to support ESPs to adopt consistent best practices[109] and also opposed by a number of organisations[110]. This bill was introduced to the 116th session of Congress on 2 July 2020 but did not receive a vote and 'died' when the 116th Congress cycle ended on 3 January 2021.

The Lawful Access to Encrypted Data Act has a broader objective and aims to cover national security interests and better protect safety and security across the US by ending the use of "warrant-proof" encryption technology by bad actors and terrorists. The bill would update several pieces of legislation[111] through targeted amendments. The bill covers data-at-rest (stored on encrypted devices), data-in-motion (lawful interception) and data stored remotely (e.g. Cloud Services).

This proposal would be applicable to a large swath of industry including; device manufacturers, providers of remote computing services, operating system providers, application developers and providers of pen register and trap and trace devices (surveillance devices that capture phone numbers dialled on outgoing and incoming telephone calls respectively). In its conceptualisation, the bill shares some similarities with the Australian Access and Assistance Act. Companies would receive 'assistance capability directives' that oblige them to provide assistance and a first report within 30 days to the Attorney General of the technical capabilities that are needed to implement the court order and timeline for the development and deployment of the capability.

Companies, within the same 30 days may submit a petition to modify or set aside the directive. The directive would be put aside if the entity proves that it does not meet the intended requirements, it is technically impossible to obtain the data being requested or that the request was made unlawfully. The bill also covers aspects of compensation to cover some expenses incurred by entities in complying with the directives and foresees a waiver from civil liability for companies.

In order to better support and underpin the core objectives of this legislation the bill proposes setting up a Prize Competition to incentivise research into creation of secure products and services that provide for lawful access. Title VII of the bill frames the importance of encryption-related training programmes for law enforcement, and the need for consistent use of clear standards for securing and minimising the amount of data collected by law enforcement.

It proposes the comprehensive collection of statistics though a master database that tracks investigations in the US where, despite having a warrant for lawful access to digital evidence, no clear-text information could be obtained due to encryption. And finally looking at ways to streamline international coordination through baseline standards and practices for lawful access. Similarly to the Earn It Act, the bill that was introduced in Congress on 23 June 2020 received not vote and 'died' with the ending of the 116th Congress cycle.

6.3.4. CONCLUSION

It is important to recognise that ensuring that law enforcement has the right capabilities to do their jobs effectively is a multi-faceted issue, and that encryption should be considered in the broader context of law enforcement's capabilities and needs. Other difficulties such as obtaining timely access to evidence in full compliance with court orders and other legal processes, as well as having adequate legal and policy tools e.g. mutual legal assistance treaties, the right personnel and resource levels and policies, are all important investments. Investments in these areas could offset some of the impact on law enforcement from inaccessible encrypted data.

As the policy efforts surrounding encryption continue to move forward, the broader political debate that key stakeholders are engaging in remains divisive. The work achieved so far has not managed to re-calibrate the debate from a zero-sum approach to a discussion that clearly presents the choices and trade-offs that are required to safeguard the security and fundamental rights of citizens, including children and other vulnerable categories of society.

[109] NCMEC letter of support to the EARN IT Act of 2020

[110] In an open letter to the senate 25 organisations expressed strong concerns over the bill, noting it would fall short of reaching its goal to protect children whilst potentially exposing all citizen's data to security breaches by undermining encryption. The Electronic Frontier Foundation called it a direct threat to free speech and expression, whilst Human Rights Watch suggested that the bill could be construed as proposing a choice between protecting children versus other fundamental rights.

[111] The bill looks at introducing updates , most prominently to the US Communications Assistance for Law Enforcement Act (CALEA), The Foreign Intelligence Surveillance Act (FISA).

7. CONCLUSION

The Internet has become central to global economic activity, politics and security and has led to changes in the types of threats faced by civilians and States. In order to match and overcome these threats, technology continues to evolve, including by making unrecoverable encryption more readily available and easy to obtain and deploy. Encryption has become an essential component to safeguarding fundamental rights, digital sovereignty and innovation. This dependency on the use of the Internet and adjunct technologies is even more pronounced now, as the world continues to adapt to the constraints brought about by the COVID-19 pandemic. Unfortunately, encryption is not only used for legitimate purposes. Criminals continue to find more creative ways to leverage the latest technologies in order to evade law enforcement.

A clear example of this is the EncroChat case explored in the report. In this instance encryption protocols were exploited to create a service offered to criminals to safeguard their communications. However, criminals have also been making use of off-the-shelf solutions and in the case of tech-savvy criminal communities building and deploying home-grown solutions. This has led to calls from law enforcement and the judiciary for proportionate and adequate tools to obtain lawful access to electronic evidence so that it can be used to move investigations forward. Accompanying such tools with proper safeguards, including requirements of necessity and proportionality will ensure that the obtained electronic evidence will be admissible in court. Proportionate lawful access also safeguards other equally important fundamental rights apart from privacy and secrecy of communications, such as the right to security, and the protection of citizens, by preventing, detecting and prosecuting crimes. Balancing these rights is important.

This has left policy makers with a seemingly impossible task. A number of EU Member States have unilaterally introduced specific provisions in their national criminal law regimes to try and mitigate the difficulty and most recently the Council of the EU adopted a Resolution on encryption that has created further momentum for action. Other regions and countries are grappling with similar dilemmas and in some cases have gone on to propose and adopt specific initiatives to try and manage all the issues at hand.

Whatever decisions are taken and whether regions and countries move on with enacting specific initiatives, the overarching issues relating to access to data brought about by technological development will remain present. A strategic approach may be required that looks at the broader concepts of policing and criminal justice in the current reality. Such an approach should also aim at assessing whether law enforcement agencies and the judiciary is well equipped to carry out their duties in the digital age.

EUROPOL EUROJUST