The Hague, 11/01/2019

First report of the observatory function on encryption

EDOC#1014687
Version 1

Joint Report

Table of Contents

List of abbreviations

AES – Advanced Encryption Standard

AI – Artificial Intelligence

BPH – BulletProofHosting

CAV – Counter Anti-Virus

CEPS – Centre for European Policy Studies

CUIng – Criminal Use of Information Hiding

DES – Data Encryption Standard

E2EE – End-to-end encryption

EC3 – European Cybercrime Centre

ECC – Elliptic Curve Cryptography

EJCN – European Judicial Cybercrime Network

EDRi – European Digital Rights

EFF – Electronic Frontier Foundation

ENISA – European Union Agency for Network and Information Security

EU – European Union

FDE – Full Disk Encryption

GDDP – Government Disclosure Decision Process

HTTP – HyperText Transfer Protocol

IETF – Internet Engineering Task Force

IMSI – International Mobile Subscriber Identity

IOCTA – Internet Organised Crime Threat Assessment

IoT – Internet of Things

IT – Information Technology

J-CAT – Joint Cybercrime Action Taskforce

LIBE – Committee on Civil Liberties, Justice and Home Affairs

NCSC – National Cyber Security Centre

NIST – National Institute of Standards and Technology

NSA – National Security Agency

PGP – Pretty Good Privacy

QKD – Quantum Key Distribution

RSA – Rivest-Shamir-Adleman

SHA256 – Secure Hashing Algorithm 256

SSL – Secure Sockets Layer

TLS – Transport Layer Security

Tor – The Onion Router

VEP – Vulnerabilities Equities Process

VPN – Virtual Private Network

1 Executive summary

In contemporary society, encryption has become an integral characteristic of everyday life. Strong encryption is an imperative feature of protecting privacy and doing business. However, criminals also abuse encryption as part of their modus operandi. This is where the challenge for law enforcement, prosecution and policymakers commences.

As part of the measures outlined by the European Commission in the Eleventh progress report towards an effective and genuine Security Union to address the role of encryption in criminal investigations, Europol, in cooperation with Eurojust has established an observatory function to engage in a forward-looking analysis with respect to encryption. This is the first report published as part of the observatory function and has as its primary objective to provide an overview of the state of play. The purpose of the observatory function is to inform; to provide a useful and balanced resource for future decision-making, approached from a law enforcement and prosecutorial perspective. The primary audience, therefore, is policymakers.

First, the report provides a brief overview and historical background of encryption, as well as a description of what encryption is. Core concepts such as symmetric versus asymmetric encryption are explained to provide a basic understanding of how encryption works. Subsequently, we give a non-exhaustive overview of services and products that use encryption. The aim is to contextualise the sections on challenges introduced by criminal use of encryption by identifying these services. With the distinction between encryption used for data in transit and encryption used for data at rest in mind, anonymisation tools such as Tor and proxy services are described.

Next, we explore the challenges pertaining to encryption for law enforcement and prosecution. Since 2016, EC3's Decryption Platform has been used to support multiple investigations in various Europol-mandated crime areas, thus indicating the cross-crime nature of the challenges posed by encryption to today's law enforcement investigations. Discussions surrounding the challenges introduced with regard to encryption for law enforcement have an extensive history. We touch upon some of the main points that are being raised in the encryption debate.

Currently, official statistics on how much digital evidence is seized in criminal investigations, or on the number of investigations that require decryption of data are not available. To make the problem more tangible to the outside world, the sixth chapter includes some case examples.

As criminals increase their operational security in response to some successful law enforcement operations, it becomes progressively more difficult for law enforcement to gain

access to encrypted data in the context of investigations. We discuss a number of possible workarounds, including their advantages and disadvantages. Examples of such workarounds include guessing the key, which is both time and resource-intensive.

The last chapter aims to provide a preview of what developments are likely to emerge based on available research. These include the opportunities and challenges introduced by quantum computing, followed by an exploration of possible criminal use of Artificial Intelligence, 5G and steganography.

This report functions as an invitation to relevant stakeholders to provide their input with regard to the identification of future developments. It is clear that law enforcement is facing challenges because of criminal abuse of encryption. Through the observatory, a specific insight into new developments can be explored at greater length. This process should also be considered as two-way street where Europol and Eurojust should use the opportunity to provide their insights about the challenges they face in this area. Facing these challenges, it is essential to not only cooperate with other law enforcement agencies, but also with both the private sector and academia. In order for law enforcement to try to keep up with criminal activities, it is necessary to continue investing in training and capability.

2 Introduction

In contemporary society encryption has become an essential feature of everyday life for digital communication and storage for everyone, from citizens to businesses to government agencies. There is no doubt that encryption plays a key role in safeguarding the confidentiality and integrity of information in general and personal data in particular. Strong encryption is an essential feature of protecting privacy and doing business.

Simultaneously, encryption has also introduced challenges for law enforcement and the entire criminal justice chain. While these challenges surrounding encryption are not new, the developments with respect to digital technology have reinvigorated the debate in an unprecedented manner. The complexity of the encryption debate is palpable, as can be witnessed from the many studies and papers published by a variety of sources. As part of the measures outlined by the European Commission in the Eleventh progress report towards an effective and genuine Security Union to address the role of encryption in criminal investigations[i], Europol, in cooperation with Eurojust, has established an observatory function to engage in a forward looking analysis with respect to encryption[1].

This is the first report published as part of the observatory function and has as its primary objective to provide an overview of the state of play. At the same time, the report also aims to provide a preview of what developments are likely to come our way based on available research, which will be further elaborated in subsequent reports.

This document is meant to function as a source of reference in the ongoing debate, with a particular focus on how encryption and closely related developments can and do have an influence on law enforcement and prosecutorial activity. The purpose of the observatory function is not to directly become engaged in the policy debate but to inform it; to provide a useful and balanced resource for future decision-making, approached from a law enforcement and prosecutorial perspective. The primary audience, therefore, is policymakers. For the purposes of transparency, where possible we include the reference to the source, but certain information included in the report is based on in-house knowledge, expertise and experience.

[i] The other measures proposed by the Commission to support Member States on encryption are: to support Europol to further develop its decryption capability; establish a network of centres of encryption expertise; create a toolbox for legal and technical instruments; provide training for law enforcement authorities (supported by EUR 500 000 from the ISF – Police fund in 2018); and establish a structured dialogue with industry and civil society organisations.

3 Approach

As identified in the introduction, this is the first report of the observatory function and primarily serves to set the stage for the establishment of the function as well as future iterations of this report. As a result, this report is based on limited open source research and does not claim to provide a comprehensive overview. Where possible we indicate where readers can access sources that go more in-depth or provide a more elaborate overview. We have supplemented the report with internal expertise, from both Europol and Eurojust. The section on the legal landscape derives its information from a questionnaire disseminated to the EJCN and analysed by Eurojust. Moving forward, we wish to consult external experts in both the private and the public sector to further enhance future editions of the report and to also ensure its role in informing others.

In an attempt to determine the nature and scope of the problem, there is frequently a request for statistics to indicate how often law enforcement encounters challenges with respect to encryption in criminal investigations. The acquisition of such statistics is beyond the scope of this report. We have provided a limited number of case examples to serve as an illustration how the criminal abuse of encryption influences the work of law enforcement.

4 Brief historical background

Before going into the current state of affairs, we believe it is essential to include a brief reflection of the historical origins of encryption to contextualise the state of play and the challenges associated with it. This historical background also describes what encryption is to ensure a common understanding for the reader before moving forward.

Simply put, encryption refers to the process of transformation of information into a secure format to protect it from unwanted access or modifications by third parties, typically referred to as confidentiality and integrity. Having originally been used to prevent intercepted handwritten messages from being read, encryption has evolved over the last decades to protect digital data and is now a well-established research field, closely connected to computer science and mathematics.

The origins of cryptography can be traced back to around 1900 BC, to inscriptions carved into the wall of the main chamber of a tomb in Ancient Egypt[2]. Having replaced a number of ordinary hieroglyphic symbols with more unusual ones, the author did not aim to hide the message, but rather to add a degree of dignity worthy of signifying the sarcophagus of nobleman Khnumhotep II. Since these early beginnings, traces of the use of secret writings have been found on clay tablets to protect recipes in Mesopotamia (dating to around 1500 BC) to pass messages among spies in India, as well as in Ancient China where messages have been found to be transformed into ideographs for the sake of privacy[3].

As various methods of encryption have been used across centuries and civilisations since today's arguably most well-known historical cipher dates back to around 100 BC and the days of the Roman Republic. Wanting to securely pass secret messages to trusted recipients through untrusted messengers, Julius Caesar applied a simple substitution cipher to the Latin alphabet[4]. Accordingly, this type of encryption is today known as a Caesar Cipher. Since it keeps certain characteristics of the text to be encrypted such as the frequency distribution of the letters and word lengths, it is not particularly difficult to break it.

Plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Caesar Cipher	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

Table 1: Example of a Caesar cipher with a rotation of three places.

Plaintext	E	U	R	O	P	O	L
Caesar Cipher	B	R	O	L	M	L	I

Table 2: Example of encoding plaintext using the cipher above.

Fast forward to the 20th century, German engineer Arthur Scherbius invented the Enigma machine with the intention of selling it for commercial use. Further advancing breakthroughs in cryptology made use of rotary disks, the German military used the machine (1933-1945) to send coded transmissions with an encryption key which changed on a daily basis. The breaking of the Enigma machine was one of the most significant developments in the history of encryption and is said to have been a turning point in the Allies' efforts to win World War II.

After the end of World War II, and breakthroughs in commercial computing, IBM set up a 'crypto group' in the 1970s and designed a block cipher to protect customer data. The design, created with input from the United States National Security Agency (NSA), was chosen to be the U.S. Data Encryption Standard (DES) in 1976 and preceded a majority of modern-day encryption standards[5]. It was replaced in 2001 by the Advanced Encryption Standard (AES), a global standard used today as a specification for the encryption of electronic data.

5 Encryption: the basics

As noted in the introduction, the purpose of this document is to provide an overview of the state of play without making the report itself part of the ongoing debate on encryption. Therefore, this report includes an overview of current standards, anonymisation tools and encrypted communication services, meant to sketch the scene.

Before assessing current trends and upcoming developments in the area of encryption, it is worthwhile to take a closer look at some of the core concepts.

Term	Description
Encryption	The process of converting data, such as messages or pieces of information, in a way which prevents unauthorised access.
Decryption	The process of reversing encrypted data back to its initial state.
Plaintext	A readable, clear message.
Cipher	An algorithm performing encryption.
Ciphertext	The end result of the encryption process.
(cryptographic) Key	A string of bits, passphrase or similar which is used by the cipher to encrypt the plaintext.
Hash	An encrypted entity that encodes data in such a way that it cannot be decrypted or recovered.

Table 3: Overview of key terms related to encryption

5.1 Symmetric versus asymmetric encryption

In general, there are three main types of encryption: symmetric encryption and asymmetric encryption, as well as cryptographic hash functions. Symmetric encryption uses one and the same key to both, encrypt and decrypt data. For data to be encrypted and decrypted by the sender and recipient, respectively, the same encryption key is needed on both sides[6].

Given that there is only one key, it is vulnerable to attack and must be kept secret and its composition unpredictable. One of the most fundamental problems of encryption revolves around the challenges of key distribution and key management. The former refers to the question of how to establish secure communication by providing keys only to those who legitimately need them, whereas the latter poses the question of how to safely preserve large numbers of keys and how to make them available as needed. Asymmetric encryption

effectively overcomes these challenges. One of the most well-known and arguably historically most significant examples of symmetric encryption is the aforementioned DES.

While DES remained a global standard for over 20 years, it was eventually publicly broken in 1999 by distributed.net and the Electronic Frontier Foundation (EFF). As a result, it was subsequently withdrawn by the U.S. National Institute of Standards and Technology (NIST) as a standard for encryption[7]. DES' successor, the AES, was established by NIST through a public process in 2001 and subsequently adopted by the U.S. Government to protect classified information[8]. Today it is a global standard used as a specification for the encryption of electronic data. While asymmetric key cyphers are used to encrypt the session key, the symmetric AES cipher is commonly found in secure file transfer protocols (such as HTTPS) to encrypt the actual data and commands[9]. Other examples of symmetric key cryptography include Blowfish, and RC4, 5 and 6[10].

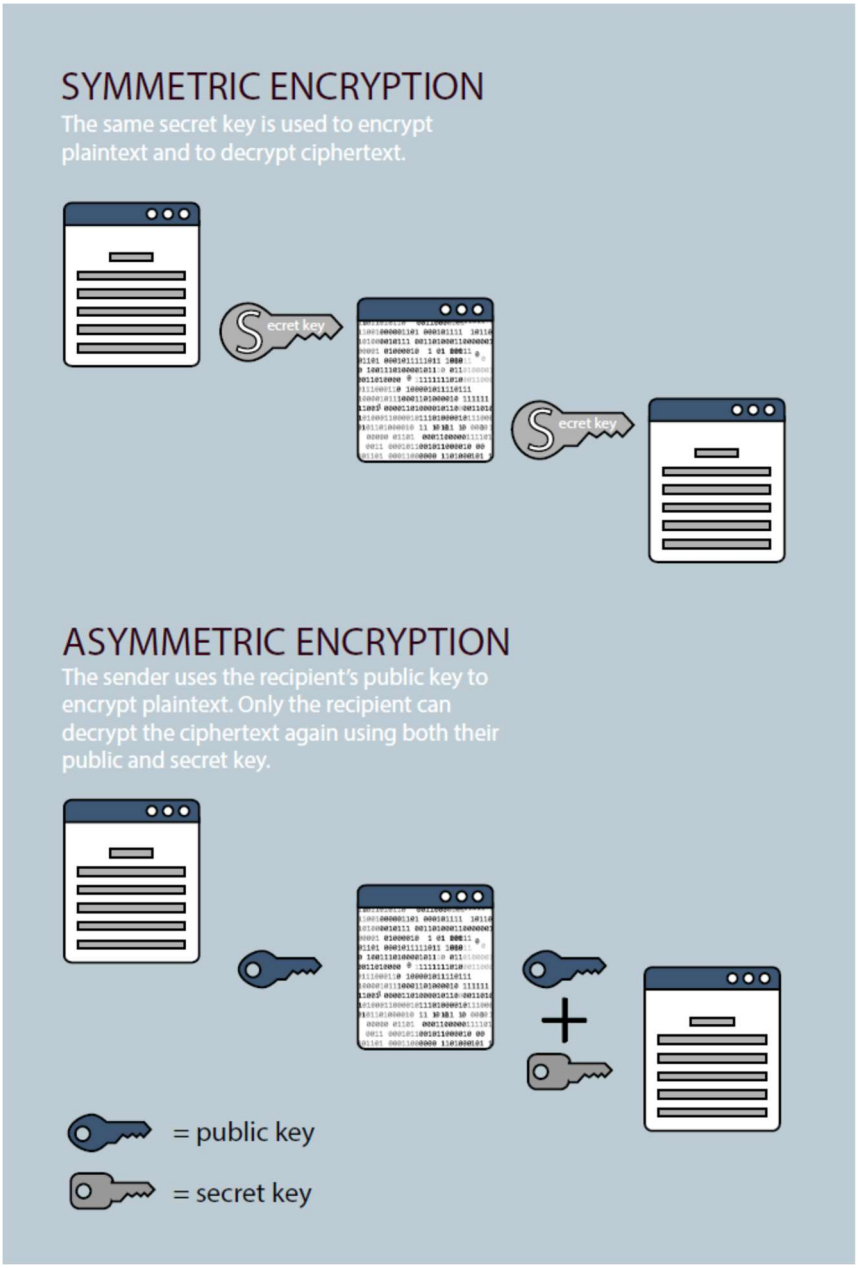

Figure 1: Overview of symmetric encryption versus asymmetric encryption

Asymmetric key encryption or public-key cryptography is based on the principle of not one key, but a combination of a public and a private key. A recipient's public key is, as the name states, publicly available and requires no security measures. It is used to encrypt a message sent to the recipient which then, in turn, can be decrypted by the same recipient's private key. Public-key cryptography is commonly used to secure electronic conversation on the internet and other open networked environments.

There are a variety of widely used asymmetric encryption standards. One of the first standards making use of public-key cryptography is Rivest-Shamir-Adleman (RSA), used for

Secure Sockets Layers (SSL) and Transport Layer Security (TLS) protocols and first published in 1978. Presently, RSA is the most used encryption algorithm worldwide, largely due to the facts that it provides a significant level of encryption with no known way to break it.

On the side of recent developments in asymmetric encryption, Elliptic Curve Cryptography (ECC) is being increasingly used and recognised as one of the most powerful and secure types of cryptography. Since ECC features a significantly more complex mathematical problem used in the algorithm to encrypt data, it would also require significantly higher computational power to break it. Arjen K. Lenstra, a Dutch mathematician, introduced the concept of 'Global Security', which can measure the energy required to break cryptographic algorithms. While breaking a 228-bit RSA key would require the equivalent energy necessary to boil a teaspoon of water, breaking a 228-bit elliptic curve key would require the energy to boil all the water on earth[11]. To reach the same level of security ECC provides with RSA, a key about ten times as long (2380 bits) would be needed[12]. While ECC is not only much more secure, it also uses smaller keys and is thus able to be run to encrypt data by smaller and less powerful devices such as mobile phones.

Asymmetric encryption is further widely used in email communication or, more recently; secure messaging apps such as WhatsApp or Telegram. OpenPGP is the most widely used email encryption standard. Having originally been derived from the Pretty Good Privacy (PGP) software, created by Phil Zimmermann, OpenPGP is defined as a Proposed Standard in RFC 4880[13] by the OpenPGP Working Group of the Internet Engineering Task Force (IETF)[14]. OpenPGP is a non-proprietary protocol relying on public key cryptography and is based on the original PGP software[15]. With regards to the end-to-end encryption of voice or video calls, as well as instant messaging conversations, the Signal Protocol has been implemented by some of the world's most used services, including WhatsApp, Facebook Messenger and Signal's own proprietary app. With its use of various well-established cryptographic algorithms and repeated resistance to various types of attacks, Signal Protocol is considered one of the most secure cryptographies currently in use.

It is worth pointing out that in this type of Transport Layer Security (TLS), asymmetric encryption is typically used to exchange the shared secret key which is then used by the much more efficient symmetric encryption methods for performance reasons. Asymmetric encryption algorithms are, then, used as part of the TLS dialogue to exchange the key into symmetric encryption algorithms such as AES.

5.2 Cryptographic hash functions

Cryptographic hash functions (also called message digests or one-way encryption) work differently compared to symmetric or asymmetric encryption in that they do not use a key to encrypt data[16]. Instead, cryptographic hash functions apply an algorithm to be run on files, passwords or other data to produce a checksum with a fixed length, which in turn can be used to verify the authenticity of the encrypted content. The hash value represents the digital fingerprint of the relevant data and ensures that it has not been tampered with (to include malware, for instance). The resulting checksums can be used to store encoded passwords on a server, provide the anonymity of persons or to authenticate a blockchain.

Plaintext	SHA256 Checksum
12345	5994471abb01112afcc18159f6cc74b4f511b99806da59b3caf5a9c173cacfc5
password	5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
Password	e7cf3ef4f17c3999a94f2c6f612e8a888e5b1026878e4e19398b23bd38ec221a
Europ0l_#%^@*$+EC3-fgijsegjegoj	4377d2d4315c70a2d45f07e06cff5bd18f6466c89e5b306c9ef41d3c4a87ee50

Table 4: Examples of checksums created with SHA256

As can be seen from the table above, the SHA256 (Secure Hashing Algorithm 256) cryptographic hash function consistently creates checksums of 64 character length, regardless of the length of the plaintext input. As such, the complete works of William Shakespeare (around 880 000 words), if encoded through SHA256, would result in a string of the same length as the input 'dog'. The change from 'password' to 'Password', for instance, creates a different output.

Cryptographic hash functions are impossible to reverse with currently known techniques and available technology. To translate a hash value back to its initial plaintext, it is not only necessary to know the algorithm which was used to create the checksum. Typical attacks use dictionaries or rainbow tables to guess passwords, as a potential hacker would otherwise have to cycle through a number of potential variations in order to derive, for instance, a password used in a website[ii]. In order to circumvent this possibility, many passwords undergo additional cryptographic hashing functions on their checksums or have salt (random data which guarantees a unique output) added, in order to further increase the difficulty.

[ii] While there is a probability that two different files will produce the same hash value, which is referred to as a random collision, the chances of this happening are negligibly small, even for billions of items. However, certain hash algorithms like MD5 or SHA-1 have known vulnerabilities that can be exploited to easily create hash collisions.

6 Products and services using encryption

The previous section provided a broad introduction to encryption to assist in the understanding of the remainder of the report for those unfamiliar with encryption. The focus was primarily on the standards and how encryption works in practice. The following section aims to provide a non-exhaustive overview of services and products that use encryption. By identifying these services, we aim to contextualise the subsequent sections on challenges introduced by encryption in criminal investigations. Important to note here is that the services and products we describe are generally used by all types of users. As a result, the inclusion of a particular service or product is done without prejudice.

From the outset, it is essential for the overall understanding of encryption and the subsequent discussion on the challenges for law enforcement with concern to criminal use, to distinguish between encryption used for data in transit and encryption used for data at rest.

Encryption for data in transit refers to the process of using encryption to secure information while it is being transferred from one device to another. Such encryption prevents an unauthorised third party from intercepting or modifying data—such as web traffic, text messages, content entered into a web form, or emails—as the data travels to its destination over the network. As such, the function of using encryption for data in transit is to protect the confidentiality and integrity of the content while facilitating authentication[17].

Encryption for data at rest focuses on securing the data while it is stored on a device or on the server of a provider. Such encryption can be used to protect a file or an entire disk.

6.1 Browsers – Darknet

Every time someone posts a comment, opens a website or makes a purchase, she leaves a certain footprint. While there are several ways to ‘discover’ those user footprints, a user’s IP address is one of the most evident and technically available ways. As a result, various anonymisation tools have been created which to a certain extent, mask the footprints of the user activities.

The Onion Router (Tor) is free, open-source software, which aims to increase anonymity and privacy. In order to achieve that, it creates a network of all software users and shares it with everybody. When a user connects to the internet via Tor, the software automatically creates a randomised path of different nodes, by ‘borrowing’ several other IP addresses for a session.

Each node has its own layer of encryption, which includes information about the next connection. As a result, it becomes difficult to track the original IP address, as it is being disguised by three or more intermediate encrypted IP addresses (see infographic overleaf).

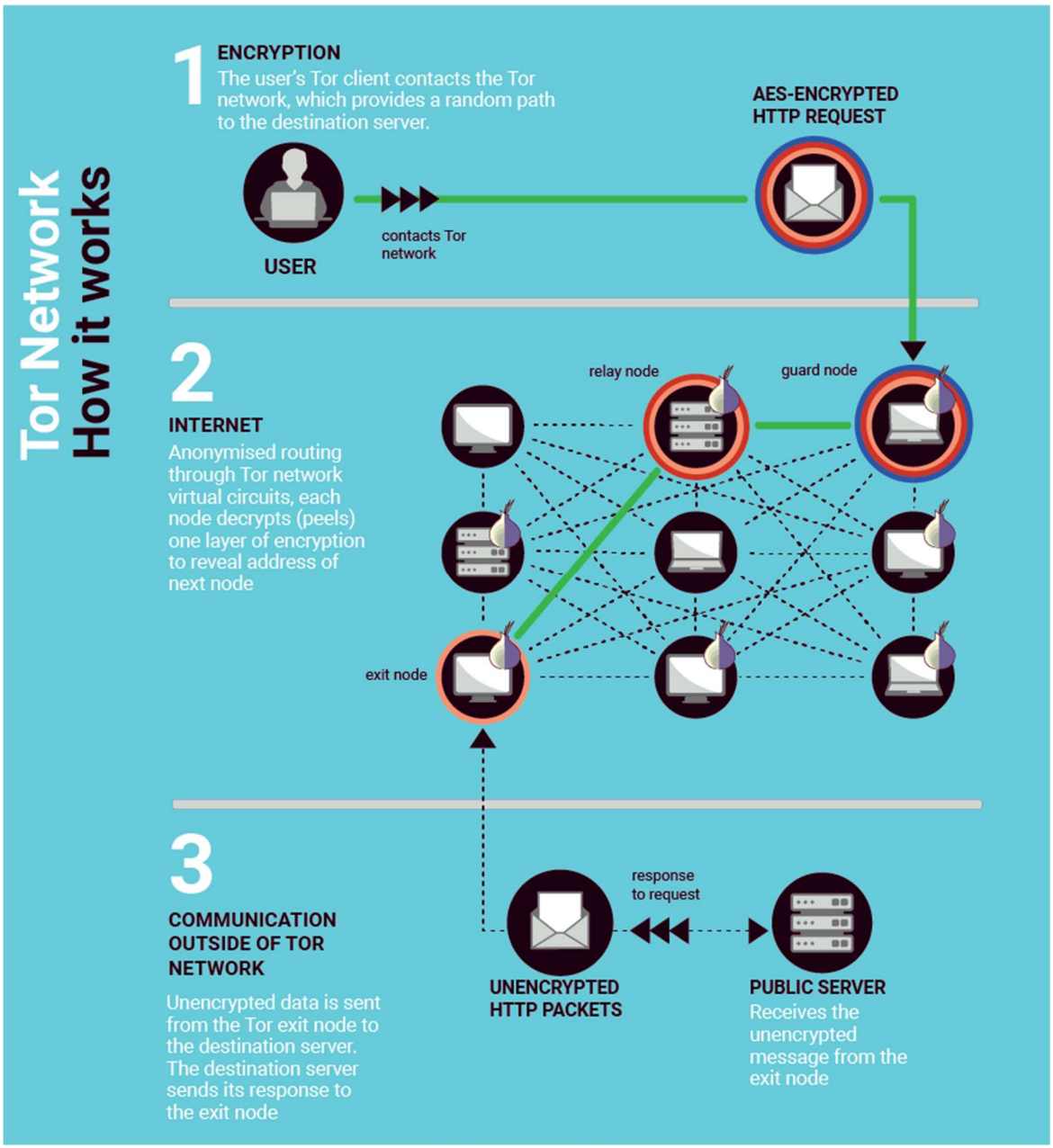

Figure 2: Tor network – how it works

A proxy service is a server that acts as a middleman in the information flow of internet traffic. With a proxy service, the internet activities appear to come from another location than the user's actual location. It also masks the IP address.

Two common proxy server protocols are HTTP and SOCKS. HTTP is the oldest type of proxy server, and it is designed solely for web-based traffic. The SOCKS proxy server protocol is an extension of the HTTP proxy system and is able to pass along any internet data[18].

A drawback of a proxy server is its configuration on an application basis, for example the web browser. Only the chosen application is connected to the proxy, and not the whole computer.

Most importantly, the largest disadvantage of proxy servers is their lack of encryption. It does not encrypt the traffic between the computer and the proxy server, which leaves the content of the data stream exposed. This is also the biggest difference between proxy servers and Virtual Private Networks (VPN).

VPNs are often cited as one of the most prominent encryption-fuelled anonymity tools. Its main purpose is to 'coat' a connection between a user's computer and a server, protecting the connection with the help of so-called VPN tunnel[19]. The encryption is created by private and public keys, where everybody has the public key and only the intended recipient the private one. The private key, in this case, belongs to the VPN, which receives its user's command, unlocks it with its private key and proceeds with it in a user-secure manner[20].

6.2 Use of encryption

End-to-end encryption (E2EE), as the name suggests, is a secure communication channel where only the intended receiver can interpret the data. In the messaging application, a text to-be-send is encrypted while it is still on the device and reaches the 'channel' already encrypted. Depending on the application used, the message will reach the cloud, where the encrypted piece of information will be stored until a receiver is available. When this message is delivered to the receivers' device, it is still in an encrypted form and will be decrypted using the right key.

Applications are now using 'forward secrecy', which grants a unique set of keys every time a new conversation is initiated, resulting in a difficult-to-compromise environment even if one of the keys is discovered[21]. As a result of such a unique and individual 'lock' on every message, the service providers face more technical difficulties to carry out the retrieval of the data, for example, in response to a warrant from law enforcement agencies.

6.2.1. Voice communications

Voice communication is becoming more internet-based so more operators want to offer this service with the option of encryption. This option is already made available by Silent Circle, the Swiss operator, by Signal – a well-known platform which started with encrypted messaging – and by other smaller players which are emerging.

When voice communication passes via internet, it not only becomes more difficult to identify voice data from the rest of the data traffic but it can also be encrypted. Messaging applications provide voice as an additional feature which makes it more difficult to detect among the other forms of data in the encrypted traffic[22].

6.2.2. Full Disk Encryption (FDE)

Full Disk Encryption (FDE) protects data that is at rest on a disk drive, as opposed to data that is in transit on a network, such as email. It is useful for small electronic devices vulnerable to theft or loss, such as laptops or phones. FDE is an increasingly widespread phenomenon, it is often installed by default on all major commercial operating systems, or as an option to protect personal data.

FDE prevents unauthorised users from accessing the data on the drive, for example by using a strong password. However, it only protects the data while the system is turned off. Once an authorised user logs in, the FDE is unlocked. Unless a user manually encrypts individual files as well, the data is exposed to anyone able to access the computer[23].

6.2.3. Emails

Messaging apps might not be convenient to securely transmit bulkier messages or even files. As a result, traditional products such as email services and file-sharing platforms have started offering additional layers of encryption, which could facilitate bigger information streams between people.

ProtonMail, with 1 million users[24], has been one of the most widely-known encrypted email services, based in Switzerland. While it shares many similarities with various messaging apps by using E2EE (for example, having no access to the encrypted information as a provider), it nevertheless stores encrypted information on its physical servers rather than in a cloud. To guarantee the encryption, ProtonMail uses several protocols, such as AES, RSA and OpenPGP. Additionally, it indicates that it uses SSL for another layer on top of the already existing E2EE, in order to avoid man-in-the-middle attacks. Due to the increasing demand, more and more

email providers are either incorporating email encryption to their current products or creating their own state-of-art encrypted services[iii].

6.2.4. File sharing

One of the leading platforms for sharing files – SecureDrop[iv] – is an open-source system, which is used to share documents, as well as to establish communication between parties. While it is generally known for being a platform for whistle-blowers and journalists, it could also be used to anonymise other criminal and non-criminal documental transactions, including various files, pictures, schemes and so on.

From a technological outlook, the SecureDrop system is comprised of a combination of four parts: servers, admins, senders and receivers. The communication and data transfer between these parts is executed through the Tor-application, creating additional security layers by using an anonymous computer environment such as the operating system. Tails and transferring information via USB keys to an air-gapped computer[v]. Firstly, a sender uploads her material on the application server, which is a public Tor Hidden Service and thus can be accessed only via Tor. Its system already provides E2EE and in addition, documents within SecureDrop's server are again encrypted with PGP standard. The receiver downloads the encrypted information and copies it to a USB key, which must be taken to an air-gapped system for decryption. As a result, decrypted information stays within an offline environment and protects it from being stolen and decrypted on a midway.

6.2.5. Self-destructing and anonymous applications

Besides the encryption feature of many communication products and services, another challenge is the self-destruction of evidence – whether images or messages – with respect to instant messaging applications, also called impermanent messaging. Several applications provide users with the ability to take a photo or send a message that self-destructs within seconds, which means the potential evidence evaporates before law enforcement could even have gained access to it. As Salmon (2018) describes within a broader context, "disappearing-

[iii] https://protonmail.com/

[iv] https://securedrop.org/

[v] https://docs.securedrop.org/en/release-0.8/overview.html

messaging apps may keep snoopers away—but they can also prevent us from preserving the past and finding justice in the future[25].”

7 The encryption challenge for law enforcement and prosecution

Offenders regularly use online anonymity and encryption tools to avoid detection, such as VPNs, Tor and Darknet forums, allowing them to operate in a relatively secure environment. There are two important reasons for this development. First, we are encountering a new generation of offenders who have grown up with technology and are therefore more familiar with and comfortable using IT. Second, most of these technologies have over time become much easier to use. Using anonymisation applications such as a VPN or Tor requires very little in the way of technical skill. Many social media applications now have standard E2EE, which means even offenders without any technical skills communicate with relative anonymity[26].

The encryption of criminal material is a cross-cutting challenge that affects all crime areas. Since 2016, 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, thus indicating the cross-crime nature of the challenges posed by encryption to today's law enforcement investigations.

From another perspective, there is also the argument of protecting victim rights and in preventing revictimisation. Through the inability of accessing digital evidence as a result of criminal usage of encryption, law enforcement officials find themselves obstructed in protecting victims from future victimisation. This is especially the case with respect to Child Sexual Exploitation but also applies to other forms of crime.

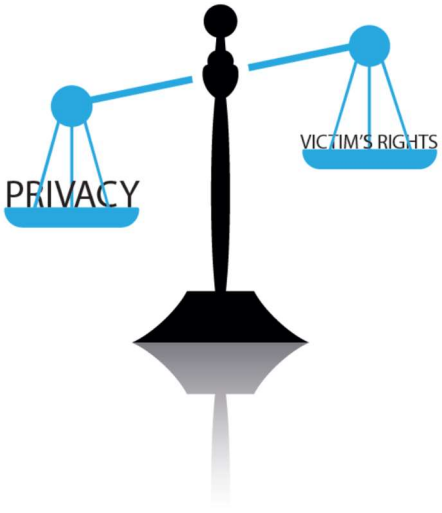

Figure 3 : Justice scale balancing privacy and victim's rights

7.1 Necessity of empirical evidence

Law enforcement units within Member States indicate that a significant and increasing percentage of cybercrime investigations involve the use of some form of encryption to protect relevant evidence in the form of data and communications. Due to its nuanced existence, official statistics on how much digital evidence is seized in criminal investigations, or on the number of investigations that require decryption of data are not available. Despite this, law enforcement agencies consider that the incidence of both is increasing[27]. As previously noted, the provision of reliable statistical data on this matter is beyond the scope of this report. This is a challenge unto itself, which places doubts as to the empirical reality in terms of the size of the problem[vi]. To make the problem more tangible for the outside world, this report contains a number of case examples to demonstrate the problem (see section 6.3).

7.2 EU legal landscape: existing legislation, legal challenges and observations

When addressing encryption in criminal investigations, the right balance needs to be struck between individual's rights, i.e. the right to privacy, and a State's responsibility to protect its citizens and thus to ensure that law enforcement agencies and judicial authorities can investigate and prosecute effectively. As a consequence, regulating this domain seems particularly delicate and difficult.

In the current legal landscape, very few Member States have specific legal provisions allowing law enforcement agencies and judicial authorities to bypass or attack encryption. Bypassing encryption can be done by requesting/ordering the unencrypted data or access key to be handed over; attacking or breaking the encryption would entail for example law enforcement agencies applying brute force, installing tools or lawful interception. If there are no specific legal provisions in force, Member States will often apply general legal provisions, aiming to effectively address encryption in criminal investigations[28]. Because of the application/interpretation by an analogy of general legal provisions, however, authorities can be confronted with legal obstacles in this respect (see below).

7.2.1. Legal obligation to hand over the data or encryption key

There are currently only a limited number of Member States which have a legal provision compelling the suspect to hand over the access key or (assist law enforcement agencies to

[vi] See for example Gill et al. (2018).

get access to) the data in an unencrypted format. Most of the Member States do not have such a provision, as it is considered irreconcilable with a person's right not to incriminate himself (*nemo tenetur* principle). On the other hand, with a few exceptions, most Member States do have specific or general legal provisions containing an obligation for third parties (persons and/or legal entities) to hand over the key or the unencrypted data. Although this legal obligation is considered useful, the penalties for non-compliance by third parties are considered too low or not proportionate to the penalty of the crime under investigation. Some countries incorporated into their law a disclosure obligation, particularly for online service providers. However, notwithstanding this legal obligation, Member States still encounter difficulties obtaining the requested data or access key from service providers, as they claim not to be able to comply with the request because they do not have access to the end-to-end encrypted data, which leaves the legal requirement void and service providers can as such remain unaccountable.

7.2.2. Attacking encryption using forensic tools or techniques

There are different ways in which law enforcement agencies can try to gain access to data by breaking encryption. It is generally understood that, if a key is legally found (finding/guessing the key) in the course of an investigation, it can generally be used for further investigation. Furthermore, Member States can also attempt to access a device through the use of forensic tools. Only a few Member States have specific legislation in this respect. All other countries apply general provisions to access a device, meaning the traditional rules on search and seizure. On the one hand, as such general rules do not contain any specific legal limitations with regard to the use of any of such tools, they leave a certain margin of possibilities for law enforcement agencies and thus there seem to be no legal limitations on what can be done with legally obtained devices. From this point of view, the application of the general rules is considered sufficient. On the other hand, practitioners do point out that specific provisions on the use of particular tools could be of added value as this would provide more legal clarity[29]. Such specific provisions should however not be too technically descriptive and detailed, in view of the evolving technological landscape. Also, given the difficulties encountered with end-to-end encryption, some practitioners do see a need for specific legislation in that area (cooperation with service providers).

Another way to bypass encryption is to remotely access a computer system (extended search or using a technical tool). In this case, only a few Member States apply specific legal provisions, whereas most of the Member States make use of the general legal provisions. In some countries this is not legally possible[30].

7.3 Case examples

There is little doubt that there is a strong desire to receive more empirical evidence from the side of law enforcement to illustrate the challenges they speak about with regard to encryption. Part of the problem in providing such empirical evidence is the restricted nature of operations. Another part of the problem is how to acquire this data since much of the challenge is the inability to gain access to encrypted data. The most illustrative examples therefore to indicate the challenge concern cases that had to be dropped, cases where considerable time and resources were required, or cases that could only be partially completed. The below is merely a sample of some of the problems we can share from Europol's perspective in our efforts to support the Member States in their investigations.

- In one specific cybercrime operation, criminals were suspected of developing, exploiting and distributing banking Trojans, as well as channelling and cashing-out the proceeds of their crimes. The analysis of a sample set of approximately 40 Million messages exchanged over a public online communication platform showed that 62% of the messages were encrypted. Therefore, there was a loss of crucial investigative opportunities in targeting high-level cybercriminals and their accomplices.
- In early 2015, the Joint Cybercrime Action Taskforce (J-CAT) and EC3 launched an umbrella investigation into BulletProofHosting (BPH) services misused by cybercriminals. BPH services are used to conceal malicious tools (malware components, exploit kits, etc.), to serve as botnet command centres, act as repositories of stolen information, or host sites used in phishing or other scams. Further to intensive data collection activities and mapping of the top priority services, different cases were opened to target these BPH services and the associated criminal activities. Due to encryption challenges, eight of these investigations were closed in 2016 as there were no possibilities to proceed any further. The last one is still on-going but not much progress has been made to date.
- In 2016, EC3 collaborated with Analysis Project (AP)[vii] Firearms in the investigation of a Darknet marketplace specialised in the illicit trade of weapons online. Due to the encryption challenges, trying to identify where the service was hosted in order to proceed with the investigation took months of work, which also involved the support of private sector partners, and in the meantime the criminals behind the marketplace closed it off in an exit scam. No further investigative action was possible.
- In 2017 Operation Neuland targeted suspected customers of a Counter Anti-Virus (CAV) platform and crypter service – two cybercriminal tools used for testing and

[vii] Analysis Projects (APs) are within the Europol Analysis System (an information processing system)and focus on certain crime areas from commodity-based, thematic or regional angles, e.g. drugs trafficking, Islamist terrorism, Italian organised crime.

clouding of malware samples to prevent security software solutions from recognising them as malicious. The data gathered generated multiple hits with a large number of other high-profile investigations thus underlying the growing reliance of the cybercriminals on such tools to conceal their illicit activities. In addition, there were more than five different cases under the J-CAT umbrella since 2016 which targeted different CAV services and had to be dropped due to encryption challenges.

- In 2017, two major law enforcement operations led to the takedown of two of the largest Darknet markets: AlphaBay and Hansa. AlphaBay was the largest criminal marketplace, utilising a hidden service on Tor to effectively mask user identities and server locations. Prior to its takedown, AlphaBay reached over 200 000 users and 40 000 vendors. There were over 250 000 listings for illegal drugs and toxic chemicals on AlphaBay, and over 100 000 listings for stolen and fraudulent identification documents and access devices, counterfeit goods, malware and other computer hacking tools, firearms, and fraudulent services. Hansa was the third largest criminal marketplace on the Dark Web, trading similarly high volumes in illicit drugs and other commodities. Compared to previous operations with similar objectives, law enforcement has noticed an increase in the operational security implemented by criminals, including the more wide-spread use of encryption. In fact, the criminal abuse of encryption was one the biggest challenges during this investigation[31].

7.4 Encryption debate summary

Discussions surrounding the challenges introduced with regard to encryption for law enforcement have an extensive history. Gill et al. (2018) speak of four decades of the encryption debate. The current debate commenced in 2011 and is generally referred to as the Going Dark debate. Hayes et al. (2015) describes how "the history of the 'crypto wars' is critical when examining the area of law enforcement and cybercrime today, including in the context of EU policy[32]."

Several sources provide comprehensive overviews of the encryption debate, including the historical background as well as the different arguments posed by the various stakeholders[viii]. All these overviews acknowledge the complexity of the debate and often lend their own

[viii] See for example Soesanto (2018); Horsman (2018); Gill et al. (2018); and the National Academies of Sciences, Engineering and Medicine (2018).

interpretation to the validity of argumentation offered by the different stakeholders[33]. We do not wish to duplicate their work herein, but merely wish to touch upon some of the main points that are being raised. With respect to criticism addressed at law enforcement, one of the main arguments is that despite the many calls for action and identification of the existence of a problem relating to encryption in criminal investigations, there is a little in terms of offering a concrete solution from the law enforcement side.

Critics argue that in the past the calls for actions identified more concrete solutions. The challenge is to approach the encryption challenge as a collective problem, as the criminal use of encryption prevents the criminal justice chain from identifying criminals. To identify solutions, law enforcement recognises a couple of requirements such as processing power as well as human expertise, but more innovative solutions can only come through cooperation with other partners.

Certain authors aim to introduce more constructive arguments despite the complexity of the debate. Soesanto (2018), for example, aims through his policy brief to "dislodge the encryption debate from its current endless loop on strong encryption versus backdoors and key escrow[34]." As he as well as many others recognise, the encryption debate is approached as a zero-sum game, which leaves no room for any middle ground. He specifically states this as well when he indicates that a middle ground is not a possibility.

Instead, he advocates a targeted approach as the only alternative. Such a targeted approach "…means that law enforcement and intelligence agencies need to have the resources, tools, and legal framework needed to hack into computers and mobile devices, obtain private encryption keys and data before it is encrypted, and have the technical and legal means to break into an encrypted device if they have physical access to it. This strategy will naturally necessitate that the agencies be well funded, well-staffed, and allowed to build up an arsenal of exploits to break into devices." The usage of exploits is controversial as shall be elaborated further on in the section on vulnerability disclosure, but must be included as part of any future discussion on options with respect to responses to the challenges as a result of criminal use of encryption or other tools.

The overarching challenge is the unification of these interests in a way to accommodate different needs.

7.5 Response to the challenges

How to respond to the challenges introduced by the criminal use of encryption is difficult in itself. A response requires various components; these include technology in the form of computational power, human resources and a clear legal framework. Increased computational power is merely a piece of the puzzle as the need for human resources, particularly forensic expertise, remains an essential ingredient in offering a response to the

challenge. Any response requires a particular resilience to criminal creativity. As criminals increase their operational security in response to some successful law enforcement operations, it becomes progressively more difficult for law enforcement to gain access to encrypted data in the context of investigations.

Kerr and Schneier (2017) identify six kinds of workarounds for encryption. These include find the key, guess the key, compel the key, exploit a flaw in the encryption software, access plaintext while the device is in use, and locate another plaintext copy. As the European Digital Rights (EDRi) notes, in principle, finding the key and guessing the key are ways to respond to the encryption challenges that do not lead to human rights problems[35].

7.5.1. Guessing the key

Guessing the key – the more realistic option compared to finding the key – is a challenging and above all a resource-intense endeavour. To give an idea of the level of resources required, it would take 2 500 years with current computational power to crack a key if a criminal used a certain form of encryption software. Increased computational power, through additional resources, may bring this down to 500 years. Yet, whether the total is 2 500 or 500 years, the length of time needed to guess the key of a criminal is still far too long.

To speed up this process, law enforcement uses contextual information about the perpetrator to make educated guesses about the more easily memorisable passwords that protect the keys. An important weakness in human-generated passwords is that they are not random. This leads to the selection of passwords that often have semantic meaning and contain recurrent internal structures. For example, when the password is required to include both letters and a minimum of one number, people often create a password beginning with letters and placing one number at the end[36].

Previous passwords are valuable information for making a guess about current passwords. People often reuse their passwords, either in their entirety or in another form. A technique to generate new passwords is to cut an existing password into small pieces and recombine them[37]. This approach is integrated into some passwords guessing tools, such as Hashcat.

People must be able to recall their passwords and a password with personal meaning is easier to remember[38]. Therefore, personal and social information about the user such as favourite books, hobbies and names of relatives is also valuable information for guessing passwords.

Contextual information about the perpetrator allows for a more targeted approach to gaining access and reducing the time needed to guess the key correctly. Notwithstanding, while this contextualisation helps to guess the key and enter into the device to collect the data, it is a process which requires both the technological tools, such as the computational power, as well as the human resources. The use of increased computational power alone is insufficient to carry out the attacks on keys based on the contextualised information. This process needs experts to determine how the information can be leveraged to gain access to the data.

To this end, whereas part of the process can be automated, a large part still needs to be carried out by experts.

7.5.2. Exploiting vulnerabilities

To exploit a flaw in the encryption scheme is a way to gain access without the key. It makes use of a weakness in the system, which can take several forms. The weakness can be a result of a mistake made by a system designer, but also a mathematical flaw in the encryption algorithm. Criminals, governments and others take advantage of these flaws. The success of exploiting a flaw to gain access is dependent on finding an unknown or an unpatched flaw in the software. If a weakness is made known, it is often quickly corrected by the software writers or vendors may offer a patch.

Flaws in software for which no patch or fix has been publicly released are also called zero days. The research community has heavily criticised exploitation by governments of zero-day vulnerabilities, with a delay in reporting the vulnerability to the software vendors. Critics argue that exploiting the flaw not only exposes the target of an investigation, but it leaves all users of the software vulnerable to malicious attacks[39]. Such criticism, however, can only apply to zero days since other vulnerabilities where a patch is available can still be taken advantage of if the user, in this case the criminal, has not made the effort to patch it.

Some flaws may be added on purpose to ensure entrance when needed. In some cases this is done by the software vendors themselves, but also by individuals with the intent of reducing security. These deliberate flaws are also called 'backdoors'. In the 1990s, some governments thought they could use backdoor schemes to allow exceptional access for law enforcement. However, the use of backdoors is no longer considered a viable option as a response to the criminal use of cryptography[40]. A flaw in the encryption would not only enable access to law enforcement, but it would also make systems vulnerable to criminals. Therefore, most governments have now abandoned plans of backdoor-access schemes.

How government agencies, from law enforcement to intelligence, treat vulnerabilities is a particularly relevant topic. In 2015, the European Union Agency for Network and Information Security (ENISA) stressed the need for transparency and openness when it comes to the use of flaws in software by law enforcement and intelligence agencies[41]. From a report by the

Centre for European Policy Studies (CEPS) on software vulnerability disclosure in Europe, it appears that most Member States do not yet have a clear legal framework on how to deal with vulnerabilities[42]. The only publicly available information[ix] on this subject is the Vulnerabilities Equities Process (VEP) in the US. The VEP aims to balance whether to disseminate vulnerability information to the vendor/supplier in the expectation that it will be patched or with temporarily restricting the knowledge of the vulnerability so that it can be used for national security and law enforcement.

The report stresses that it is critical for governments to have robust, accountable and transparent policies in place when it comes to disclosure. Only then can companies and users trust in the responsible management of vulnerabilities by governments. Therefore, the recommendation for EU governments is to implement a Government Disclosure Decision Process (GDDP) for vulnerability disclosure. A number of policies and practices are suggested, such as reviewing decisions to delay disclosure of a vulnerability and codifying the GDDP in law or other legally binding policy. ENISA can play an important role in assisting and advising Member States in implementing a GDDP.

Whereas an important distinction must be made between intelligence and law enforcement, for purposes of the broader discussion, especially at the policy level, it is worth taking note of a recent publication by the National Cyber Security Centre (NCSC) in the United Kingdom. In November 2018, the NCSC-UK introduced its equities process in which it describes how it treats identified vulnerabilities. As the Agency writes: “When we discover a previously unknown vulnerability, our starting position is to disclose it. We always perform a thorough review so we can understand whether there is an overwhelming national security benefit in retaining it[43].” While the retained vulnerability and the fact that it was retained must remain confidential, the NCSC UK aims to become more transparent in its approach to the process, and, as such, has published a decision tree as a means to make their approach more accessible[44].

7.5.3. Access plaintext

Another workaround for encryption is to access plaintext when the device is in use. As users cannot read ciphertext, the encrypted data must be decrypted to be read by them. This is a necessary vulnerability in security. A limitation of this workaround is that it usually only works

[ix] At the time of the CEPS publication.

in ‘real time’, with ongoing access to the device in use. Accessing plaintext can be as simple as physically obtaining the device while it is being used by the suspect.

The final kind of workaround is locating a plaintext copy. In this manner, encryption is not bypassed, but rather avoided altogether. An example is an unencrypted backup copy of a locked phone in a cloud storage service. To successfully locate and use a plaintext copy, four conditions must be met. The plaintext copy has to exist, the government must be able to locate it and must have the legal ability to acquire it and the unencrypted copy has to be sufficiently similar to the original to be an adequate substitute.

7.5.4. Key escrow

In the past, the United States and other national governments have proposed laws to assure the government access to encrypted data. Anyone using encryption would be required to file a copy of the encryption key with a trusted third party, like a government agency. The key could then be retrieved to decrypt the data if necessary. This system is also known as key escrow. However, there are several problems with this approach[45]. Firstly, there are practical issues with ensuring all users of encrypted data place their key in escrow. Another great challenge is securing the escrowed keys against attack by criminals. Any datastore could be compromised by hackers, and recent history has taught us that both governments and trusted third parties are not immune to these dangers. There is also a danger of intentional misuse internally or simple incompetence leading to a breach. In addition, most messaging platforms now use forward secrecy and have implemented E2EE. This makes the key unknown to anyone except the participants of the interaction.

7.6 Necessity, proportionality and the lack of less intrusive means

The use of techniques to bypass encryption by law enforcement brings with it certain risks pertaining to privacy. The fundamental right to privacy must be protected. This includes the fact that a limitation on the right to privacy must be subject to the principles of proportionality and necessity. As was stressed in the 2016 Joint Statement by ENISA and Europol, the use of intrusive investigative tools must be proportionate to the crime that was committed. Additionally, proportionality requires that the least intrusive tool is used to achieve the investigative object. This also means other less invasive tools are first exhausted, or deemed insufficient.

The requirement of necessity means that bypassing encryption should be limited to situations where they are “strictly and demonstrably necessary to achieve a legitimate aim[46].”

At the request of the European Parliament’s LIBE committee, a comparative analysis of legal frameworks and practices for hacking by law enforcement across six EU Member States and three non-EU countries was carried out. The application of the principles of necessity and

proportionality are important elements of Member State legal provisions. These include conditions before using hacking techniques ('ex-ante conditions'), such as judicial authorisation; ensuring hacking practices are appropriately targeted and limiting the duration of a hacking practice. Practices for after using hacking techniques ('ex-post mechanisms') include the notification of targets, the opportunity for effective remedy and provisions on removal of the hacking tool after use.

In many countries, a clear legal framework for lawful hacking still needs to be established. The challenge for policy-makers is finding a balance between privacy and confidentiality of the public's communications, and the safeguarding of national security. To ensure that the principles of proportionality and necessity are applied, further development of policies is necessary. In response to the lack of policies, the aforementioned study developed policy recommendations. For instance, they propose for Member States to "conduct a Privacy Impact Assessment when new laws are proposed to permit and govern the use of hacking techniques by law enforcement agencies. This Privacy Impact Assessment should focus on the necessity and proportionality of the use of hacking tools[47]." They also recommend for more training for national-level members of the judiciary on the principles of necessity and proportionality in relation to lawful hacking.

8 Looking forward

The previous sections discussed the current state of the encryption debate and the challenges and opportunities for law enforcement and prosecution. The following section aims to provide a preview of what developments are likely to come our way based on available research. These include quantum computing, artificial intelligence, 5G and steganography.

8.1 Quantum computing

One relevant development with respect to encryption concerns quantum computing. The awareness that quantum computing would be great at factoring large numbers has existed since the 1980s. The building of such quantum computers was not possible then. However, considerable progress has been made in recent years into producing a viable quantum computer. Forms of quantum computers are already being built by organisations such as Google and IBM[48]. Quantum computing has been heralded as the next great security risk, although opinions vary on the level of concern this should attract. Projections about how quickly the quantum computer will become a reality vary.

The advent of quantum computing will most likely introduce a revolution in computing, especially in information security and encryption. This is because many security standards used today depend on the complexity of tasks that classical computers simply cannot complete in any reasonable time. Given that quantum computers will overcome these limitations, it is easily expected that it will prompt a radical rethinking of cyber security. Practically usable quantum computers, however, are still decades away. Furthermore, quantum computers have their limitations. They could be used for certain types of problems such as integer factorisation or for problems related to discrete logarithm problems. However, there are encryption algorithms already in use that are considered to be 'quantum-safe', because they are based on a different mathematical approach. This is in accordance with Buchanan and Woodward (2017), who describe a range of alternative mathematical problems that appear to be quantum resistant[49].

Quantum computers are being developed right now by several state actors[50]. Their high value for these actors, coupled with the tremendous costs involved in quantum computers' development make the prospects of any immediate danger coming from non-state actors (such as criminals or terrorists) unlikely. However, states with this technology in their possession may use it to orchestrate far more sophisticated cyber-attacks or break encryption.

8.1.1. Breaking today's encryption standards with quantum computers

One of the principal effects of the application of quantum technology to cryptography is its ability to be used to break current encryption standards. Theoretically, this would grant the first actor with a quantum computer of necessary computing power with the ability to render current encryption standards in the area of asymmetric encryption obsolete.

In more technical terms, current public-key encryption relies on the difficulty of factoring and the difficulty of calculating elliptic curve discrete logarithms, making it impervious to being cracked by classical computers in a reasonable amount of time. For illustration, factoring RSA-768, a 232 decimal digits-long number used as a key in the eponymous encryption protocol took a collection of hundreds of computers two years to factorise[51]; more complex standards such as RSA-2048 still remain virtually uncrackable. However, it is estimated that a quantum computer of sufficient power (several thousand qubits, i.e. a quantum version of the classical binary bit) using Shor's algorithm would do the same task in mere seconds, making RSA-2048 and possibly also RSA-4096 simply insufficient for encryption[52].

While certainly a great opportunity, this also poses a serious security threat. The expectation is that the technology will not remain inaccessible for long and will proliferate quickly.

This is not an imminent threat. Currently, the most advanced quantum computer 'Bristlecone' by Google has only 72 qubits. This is rather far removed from the estimated 4-10 000 qubits necessary for any practical use in encryption and decryption[53]. A closer cooperation of different stakeholders of quantum computers will be required, in order to prepare and make the upcoming security standards resistant to the new technology; this has already been reflected in the advent of the post-quantum cryptography, an area of research focussing on development of cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks[54]. Much like the processes that led to the standardisation of AES (see 3), NIST (see 4.1) has called upon the public for assistance and has initiated a process to develop and standardise strategies for post-quantum algorithms.

8.1.2. Quantum encryption

The other opportunity stemming from the application of quantum technology is its use for encryption of communications, making them impervious to eavesdropping. At the heart of it stands Quantum Key Distribution (QKD), a principle that follows the traditional pattern of encryption by using keys shared by the communicants while taking advantage of the

principles of quantum mechanics (quantum indeterminacy and entanglement). The message is encoded in quantum states of unknown length (usually photons sent via optic cable) instead of standard bits; this is crucial because measuring a state in quantum mechanics necessarily and irreversibly alters it to some degree. In turn, this makes interception of the encrypted message by a third party almost impossible[x] as they would have to measure the key in some way, thus disturbing the whole system and notifying the communicants they are being eavesdropped upon.

Should this technology proliferate and be made available to private actors to be used to encrypt their communications, it would make their interception almost impossible. Still, the scheme described above incorporates quantum computing only in the key distribution stage and apart from that it still uses today's encryption protocols, making its decryption dependent only on the key interception.

8.2 Artificial Intelligence (AI)

The continuous evolution of developments with the anticipation of having artificial intelligence (AI) will also influence encryption, as well as its debate. While we often speak of AI, it is important to note that actually achieving artificial intelligence has yet to occur. However, many sub-categories of AI such as machine learning, natural language processing, deep learning, adversarial search algorithms, probabilistic decision-making, etc. are already well established with many practical applications. We encounter these applications on a daily basis, often without being aware of it being AI. Machine learning and natural language processing are used by virtual assistants such as Apple's Siri and Amazon's Alexa. Machine learning is also widely used by social media platforms to personalise your newsfeed or ad targeting. An example is the 'face recognition' feature on Facebook.

Similarly to quantum computers, presently, abuse of AI by criminals appears limited, as the technology is still under development. The technology may make communications almost immune to decryption, which may prove to be a challenge from the law enforcement perspective.

These claims are based on Google's 2016 experiment[55], where two neural networks were tasked with developing their own encryption protocols to encrypt messages they send between themselves; another third neural network was tasked with intercepting these messages and decrypting them. The longer the experiment ran, the more apparent it became that the two communicants became more adept at securing their communications by

[x] While in theory the process of QKD is immune to interception, its real-world application is not. See: https://www.technologyreview.com/s/418968/commercial-quantum-system-hacked/

developing new encryption protocols; conversely, the third network became gradually worse at successfully intercepting and decrypting the messages.

Linking it to the previous section on quantum computing, it is hypothesised that AI may be used to enhance encryption protocols by disposing of standardised encryption protocols and creating completely new and unknown algorithms and key for each communication session. As the QKD-centred scheme above shows, because brute-forcing the key in more advanced encryption protocols is an ineffective effort, intercepting the key is currently the main problem with decryption – after that, breaking the well-known standard protocol such as AES is a comparatively easier task. However, the experiment with Google's Brain project shows that future AI-developed, quantum-resistant encryption protocols may "be just as fluid as the key", making any decryption an immensely resource-costly endeavour, bordering on impossible[56].

Should this technology become accessible to criminals, it may considerably exacerbate today's threats. For example, using completely unique, AI-generated encryption protocols in ransomware would make law enforcement assistance in these incidents extremely difficult; effects of these protocols' application to criminals' communications or device encryption are very similar, complicating law enforcement assistance substantially.

8.3 5G

5G represents a new generation of communication technology, which in comparison with its predecessors – 1G, 2G, 3G and 4G – brags of a new quality of super-speed, reduced delay and ability to manage large amounts of simultaneous connections. Indeed, the technological promise behind 5G enables great opportunities for complex network structures and unseen capacities of multiple-sourced connections, especially important to the rise and application of the Internet of Things (IoT) industry: self-driving cars, smart homes and smart business infrastructures. 5G differs from the previous generations with regards to certain qualities, particularly its potential capability of high-speed data transmissions and simultaneous use of multiple data sources. But it also features a new encryption level, which could have direct consequences to criminal investigations.

For example, the long-term identifier (IMSI) is an important tool to trace and identify users behind particular subscriptions. Since 5G is still undergoing the standardisation process, it might become more difficult to preserve the same traceability methods as used in 3G or 4G. As an example, a unique identifier could be replaced by a temporary dynamic identifier, which

changes immediately after the session is over. It would work as an additional layer of encryption for the criminal activities, increasing workload and resources for law enforcement agencies.

Another challenge could be 5G's facilitated identity management, which would be divided into two separate parts: device and service identities. It is very likely, that traditionally used SIM cards will be unsuitable for upcoming devices, therefore the combination of device and service identities will be used to authenticate and authorise. These new types of identity management will have their own, separate layers of encryption; leading to new ways of identity manipulation and concealment.

8.4 Steganography

Steganography is the practice of hiding secret content and messages in otherwise non-secret mediums. Cybercriminals can also use these methods. For example, a perpetrator can conceal malware inside an ordinary image file to control servers[57]. In this way, the user is unaware of the existence of the malware and the perpetrator remains undetected.

Steganographic methods can be grouped in several ways according to different experts. Modern information hiding through steganography can be divided between covert data storage and covert data communication. Under covert data storage, we find the most well-known type of steganography – digital media steganography – and file/mass storage information hiding. Under covert data communication, we have network steganography and local and out-of-band channels[58].

According to Johnson and Katzenbeisser, digital media steganography can be broken down into six categories[59]:

- Methods that substitute redundant data in cover objects;
- Methods that embed data in a signal's transform space;
- Methods that utilise spread spectrum techniques;
- Methods that change statistical properties of a cover object;
- Methods that represent secret information by introducing a distortion into a signal;
- Methods that create cover objects only for carrying secret information.

Steganography has been used by criminals for quite some years now. Already in 2001/2002, several articles suggested that al Qaeda members used steganography to coordinate their actions. Around the same time, several Shadowz Brotherhood's members, a high-tech paedophile organisation who distributed child abuse material with the aid of steganography, were arrested[60]. Nevertheless, it is almost impossible to guess how widespread these information-hiding techniques are in the cybercriminal world.

Such as other encryption and anonymisation tools, steganographic applications are easily accessible and relatively easy to run and to use. There are even Android and iOS apps that are available for free[61], which further contributes to the challenges law enforcements agencies already face. Investigators face a two-step process, where they first need to discover whether any information hiding programme was installed and used, and if it was, what message was indeed hidden.

Steganography has been used by criminals for different purposes: as covert storage, which allows to hide secret data in such a way that no one besides the owner is authorised to discover its location and retrieve it; as a covert communication tool, used to make sure their exchanges are kept confidential; as a data exfiltration technique, through which cybercriminals steal confidential and sensitive data; and as covert malware communication, by equipping the malware with information hiding techniques to become stealthier while residing on the infected host. As an example, in late 2016 the Stegano Exploit Kit, originally created in 2014, reappeared in the form of malicious ads displayed on a variety of reputable news websites, each with millions of daily visitors. The ads, without requiring any interaction from the user, used either a clean image or its almost imperceptibly modified malicious evil twin to report information about the victim's machine to the attacker's remote server. Online games and gaming consoles are also being used to enable covert communication.

The Criminal Use of Information Hiding (CUIng) Initiative was launched in 2016, with the support of Europol's EC3, to combat criminal exploitation of information hiding techniques. Their aim is to raise awareness of information hiding techniques like steganography and the threat it can pose, to track its progress, work jointly with, and educate and train law enforcement agencies, companies, institutions, etc. on how to react to potential cybercriminals' information hiding exploitation[xi]. In January 2018 the first report of research performed within the CUIng initiative was published[62]. The second international workshop of CUIng was held at the ARES conference 2018.

[xi] http://cuing.org/

9 Conclusion

Encryption as a tool provides benefits for society as a whole. It is a fundamental part of how the internet works in a safe and productive way for the vast majority of users. Nevertheless, we have to highlight that criminals also abuse encryption as part of their modus operandi, in particular, to hide their activities. This is where the challenge for law enforcement and prosecution commences. As the use of encryption becomes more widespread and the encryption tools become more robust, the greater the difficulty to access data becomes.

As indicated in the introduction, this report is the first of its kind and primarily functions as a kick-off for future iterations as part of the establishment of the observatory function. While there is a brief overview of the background of encryption, more comprehensive resources are available for those who wish to derive a better and more in-depth understanding of encryption, its history and the many developments that have taken place.

In many ways, this report functions as an invitation to relevant stakeholders to provide their input with regard to the identification of future developments. This allows the observatory function to connect to some of the other measures introduced by the EC with respect to encryption. This comprehensive package of measures, particularly the stakeholder dialogue with industry, and the network of experts on encryption provide specific insight into new developments that can be explored at greater lengths through the observatory. This process should also be considered as a two-way street where Europol and Eurojust should use the opportunity to provide their insights about the challenges they face in this area. This also means the law enforcement and prosecutorial perspective must be expressed and heard in meetings and fora that connect to relevant developments, such as on the topic of 5G.

As a result, in addition to cooperation with other law enforcement agencies, it is also essential to build and maintain relationships with both the private sector and academia. Both are often nearer the cutting edge of technology and often, either through research or the course of their business, have access to data and expertise which law enforcement not only lacks but is often highly valuable to criminal investigations. While collaboration is essential, in order for law enforcement to try to keep up with criminal developments, it also needs continued investment in training, and capacity building, particularly in terms of technical and forensic capability. In view of efficient use of resources, sharing of tools and expertise at EU level would also be beneficial.

References

[1] European Commission, 'Eleventh progress report towards an effective and genuine Security Union', p. 10, 2017.

[2] Kahn, D., 'The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet', Scribner, 1996.

[3] Cohen, F., '2.1 - A Short History of Cryptography', 1990/1995.

[4] Churchouse, R.F., 'Codes and Ciphers: Julius Caesar, the Enigma, and the Internet', Cambridge: Cambridge University Press, 2001.

[5] SANS Institute InfoSec Reading Room, History of Encryption, 2001.

[6]Microsoft, 'Description of Symmetric and Asymmetric Encryption', https://support.microsoft.com/en-us/help/246071/description-of-symmetric-and-asymmetric-encryption

[7] Van De Zande, P., The Day DES Died, https://www.sans.org/reading-room/whitepapers/vpns/day-des-died-722, 2001.

[8] Federal Information Processing Standards Publication 197, Specification for the advanced encryption standard (AES), 2001.

[9] Abdullah, A. M., 'Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data', 2017.

[10] Villanueva, J. C., 'Symmetric vs Asymmetric Encryption', Jscape, https://www.jscape.com/blog/bid/84422/Symmetric-vs-Asymmetric-Encryption, 2015.

[11] Sullivan, N., 'A (relatively easy to understand) primer on elliptic curve cryptography', https://arstechnica.com/information-technology/2013/10/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/2/, 2013.

[12] Lenstra, A., K., Kleinjung, T., Thome, E., 'Universal security from bits and mips to pools, lakes and beyond', https://hal.inria.fr/hal-00925622/document, 2013.

[13] Callas, J., Donnerhacke, L., Finney, H., Shaw, D., Thayer, R., 'OpenPGP Message Format', https://tools.ietf.org/html/rfc4880, 2007.

[14] The Internet Engineering Task Force (IETF), 'Working Groups', https://www.ietf.org/how/wgs/

[15] OpenPGP, https://www.openpgp.org/about/, 2016.

[16] Northcutt, S., 'Security Laboratory: Cryptography in Business Series', https://www.sans.edu/cyber-research/security-laboratory/article/hash-functions.

[17] Gill, L., Israel, T., Parsons, C., 'Shining a light on the encryption debate: a Canadian field guide', Citizen Lab and the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic, 2018.

[18] Fitzpatrick, J., 'What's The Difference Between a VPN and a Proxy?', https://www.howtogeek.com/247190/whats-the-difference-between-a-vpn-and-a-proxy/, 2016.

[19] Athow, D., 'VPN Tunnel: What is it, how can it keep your Internet data secure', https://www.techradar.com/news/vpn-tunnels-explained-how-to-keep-your-Internet-data-secure, 2018.

[20] Walters, G., 'VPN Encryption Guide: Best VPNs With Strong Encryption Levels', 2017, https://www.addictivetips.com/vpn/vpn-encryption-guide/.

[21] Xolphin, 'Perfect Forward Secrecy', https://www.sslcertificaten.nl/support/Terminologie/Perfect_Forward_Secrecy.

[22] Woodward, A., 'End-to-end encryption tests SIGINT agencies', Jane's Intelligence Review, 2017.

[23] Zetter, K., 'Hacker Lexicon: What is Full Disk Encryption?', https://www.wired.com/2016/07/hacker-lexicon-full-disk-encryption/, 2016.

[24] Lewis, J., A., Zheng, D., E., Carter, W., A., 'The Effect of Encryption on lawful access to communications and data', Centre for strategic & international studies, 2017.

[25] Salmon, F., 'How Snapchat is Sending #Metoo Down the Memory Hole', https://www.wired.com/story/snapchat-sending-metoo-down-the-memory-hole/, 2018.

[26] Europol, 'Internet Organised Crime Threat Assessment 2018', 2018.

[27] National Academies of Sciences, Engineering and Medicine, 'Decrypting the Encryption Debate: A framework for decision makers', https://www.nap.edu/catalog/25010/decrypting-the-encryption-debate-a-framework-for-decision-makers, 2018.

[28] Eurojust, 'Cybercrime Judicial Monitor nr.4'

[29] Eurojust, 'Workshop on encryption', 2017

[30] Eurojust, 'Cybercrime Judicial Monitor nr.2', 2016.

[31] Europol, 'Massive blow to criminal Dark Web activities after globally coordinated operation', https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation, 2017.

[32] Hayes, B., Jeandesboz, J., Ragazzi, F., Simon, S., Mitsilegas, V., 'The law enforcement challenges of cybercrime: are we really playing catch-up?', Policy Department Citizens' Rights and Constitutional Affairs, European Parliament, 2015.

[33] Horsman, G., 'A call for the prohibition of encryption; panacea or problem?', https://tees.openrepository.com/tees/bitstream/10149/621677/2/621677.pdf, 2018.

[34] Soesanto, S., 'No middle ground: Moving on from the crypto wars', https://www.ecfr.eu/page/-/no_middle_ground_moving_on_from_the_crypto_wars.pdf, 2018.

[35] Kerr, O.S., Schneier, B., 'Encryption workarounds', https://www.schneier.com/academic/paperfiles/Encryption_Workarounds.pdf, 2018.

[36] Shay, R., Bauer, L., Christin, N., Cranor, L.F., Forget, A., Komanduri, S., Mazurek, M.L., Melicher, W., Segrett, S.M., Ur, B., 'A Spoonful of Sugar? The Impact of Guidance and Feedback on Password-Creation Behavior', http://cups.cs.cmu.edu/rshay/pubs/Feedback.pdf, 2015

[37] Coisel, I., Sanchez, I., Galbally, J., 'Divide, Recombine and Conquer: Syntactic Patterns-Reassembly Algorithm applied to Password Guessing Process', https://www.researchgate.net/publication/321663700, 2017.

[38] Cazier, J.A., Meldin, B.D., 'Password Security: An Empirical Investigation into E-Commerce Passwords and Their Crack Times', https://www.researchgate.net/publication/220450084_Password_Security_An_Empirical_Investigation_into_E-Commerce_Passwords_and_Their_Crack_Times, 2006.

[39] Koops, B.J. and Kosta, E., 'Looking for some light through the lens of "cryptowar" history: Policy options for law enforcement authorities against "going dark"', Computer Law & Security Review, 2018.

[40] ENISA and Europol, 'ENISA and Europol issue joint statement on lawful criminal investigation that respects 21st Century data protection', 2016.

[41] ENISA, 'Good Practice Guide on Vulnerability Disclosure: From challenges to recommendations', https://www.enisa.europa.eu/publications/vulnerability-disclosure, 2015.

[42] CEPS Task Force, 'Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges', https://www.ceps.eu/system/files/CEPS%20TFRonSVD%20with%20cover_0.pdf, 2018.

[43] GCHQ, 'GCHQ and the NCSC publish the UK Equities Process', https://www.gchq.gov.uk/news-article/dealing-vulnerabilities, 2018.

[44] GCHQ, 'The Equities Process', https://www.gchq.gov.uk/features/equities-process, 2018.

[45] Europol, 'Internet Organised Crime Threat Assessment 2015', 2015.

[46] Necessary & Proportionate: The International Principles on the Application of Human Rights to Communications Surveillance, https://necessaryandproportionate.org/files/2016/03/04/en_principles_2014.pdf, 2014.

[47] European Parliament Policy Department for Citizens' Rights and Constitutional Affairs, 'Legal Frameworks for Hacking by law Enforcement: Identification, Evaluation and Comparison of Practices', http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf, 2017.

[48] Europol, 'Internet Organised Crime Threat Assessment 2016', 2016.

[49] Buchanan, W., Woodward, A., 'Will quantum computers be the end of public key encryption?', https://www.tandfonline.com/doi/pdf/10.1080/23742917.2016.1226650?needAccess=true, 2017.

[50] Greenemeier, L., 'How Close Are We—Really—to Building a Quantum Computer?', https://www.scientificamerican.com/article/how-close-are-we-really-to-building-a-quantum-computer/, 2018.

[51] Kleinjung, T., Aoki, K., Franke, J., Lenstra, A., Thomé E., et al., 'Factorization of a 768-bit RSA modulus', https://hal.inria.fr/inria-00444693v2/document, 2010.

[52] Svore K., 'The Future is Quantum', Microsoft Research Podcast, https://www.microsoft.com/en-us/research/blog/future-is-quantum-with-dr-krysta-svore/, 2018.

[53] Moses, T., 'Quantum Computing and Cryptography', Entrust, https://www.entrust.com/wp-content/uploads/2013/05/WP_QuantumCrypto_Jan09.pdf, 2009.

[54] Chen, L., Jordan, S., Liu, Y., Moody, D., Peralta, R., Perlner, R., Smith-Tone, D., ,'Report on Post-Quantum Cryptography', National Institute of Standards and Technology, 2016.

[55] MIT Technology Review, 'Commercial Quantum Cryptography System' Hacked', https://www.technologyreview.com/s/418968/commercial-quantum-cryptography-system-hacked/, 2010.

[56] Abadi, M., Andersen, D., G., 'Learning to protect communications with adversarial neutral cryptography', 2016.

[57] CISOMAG, 'Cybercriminals using Steganography in their attacks: Researchers, https://www.cisomag.com/cybercriminals-using-steganography-attacks-researchers/, 2017.

[58] Mazurczyk, W, Wendzel, S., ,Information Hiding: Challenges for Forensic Experts, https://cacm.acm.org/magazines/2018/1/223894-information-hiding/fulltext, 2018.

[59] Johnson, N.F. and Katzenbeisser, S.C., 'A survey of steganographic techniques', Information Hiding, 2000.

[60] ESET Research, 'Readers of popular websites targeted by stealthy Stegano exploit kit hiding in pixels of malicious ads', https://www.welivesecurity.com/2016/12/06/readers-popular-websites-targeted-stealthy-stegano-exploit-kit-hiding-pixels-malicious-ads/, 2016.

[61] National Academies of Sciences, Engineering and Medicine, 'Decrypting the Encryption Debate: A framework for decision makers', https://www.nap.edu/catalog/25010/decrypting-the-encryption-debate-a-framework-for-decision-makers, 2018.

[62] Cabaj, K., Caviglione, L., Mazurczyk, W., Wendzel, S., Woodward A., Zander, S., 'The New Threats of Information Hiding: the Road Ahead', https://arxiv.org/ftp/arxiv/papers/1801/1801.00694.pdf, 2018.