European Crime Prevention Network

Theoretical Paper

Cyber Safety

Cyber Safety: A theoretical insight

In the framework of the project 'The implementation of the Multiannual Strategy of the EUCPN and the Informal network on the Administrative Approach' - EUCPN Secretariat, 2017, Brussels

With the financial support of the Prevention of and Fight against Crime Programme of the European Union
European Commission – Directorate-General Home Affairs

Cyber Safety: A theoretical Insight

Abstract

This paper is written by the EUCPN Secretariat following the topic of the Estonian Presidency of the Network, which is Cyber Safety. It gives a theoretical insight in what Cyber Safety is.
Furthermore, we take interest in what the exact object is of cybercrime and have a deeper look into two European policy priorities, namely cyber-attacks and payment fraud. Moreover, these priorities are the subject of the European Crime Prevention award. The goal of this paper is to add to the digital awareness of local policy-makers and practitioners on a theoretical level. A toolbox will follow with legislative measures, existing policies and best practices on this topic.

Citation

EUCPN (2017). Cyber Safety: A theoretical Insight. In: EUCPN Secretariat (eds.), *EUCPN Theoretical Paper Series,* European Crime Prevention Network: Brussels.

Legal Notice

The contents of this publication do not necessarily reflect the official opinions of any EU Member State or any agency or institution of the European Union or European Communities.

Authors

Jorne Vanhee, Research Officer EUCPN Secretariat
Cindy Verleysen, Senior Research Officer EUCPN Secretariat

EUCPN Secretariat
Waterloolaan / Bd. De Waterloo 76 1000 Brussels, Belgium
Phone: +32 2 557 33 30 Fax: +32 2 557 35 23
eucpn@ibz.eu – www.eucpn.org

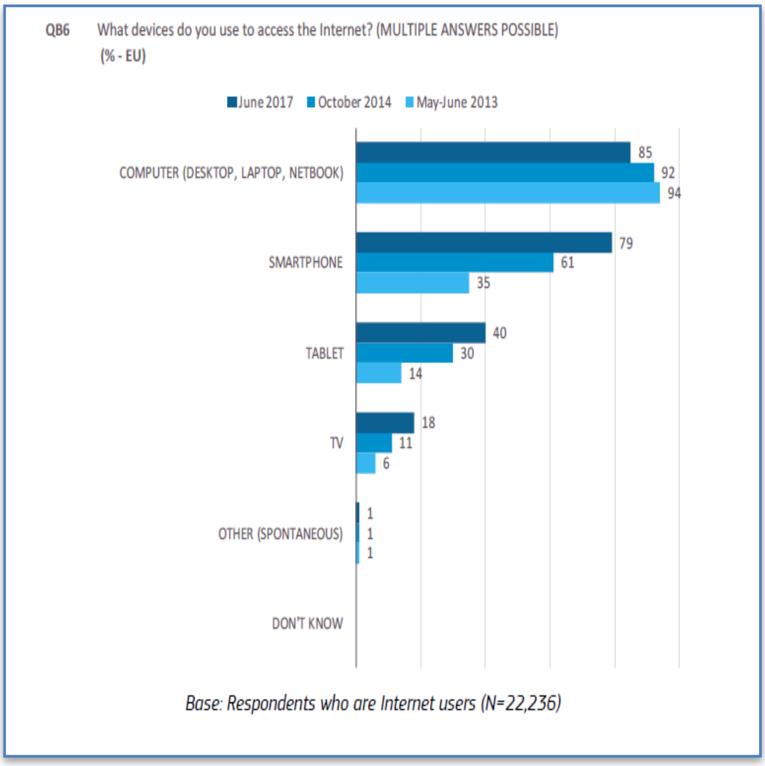
Content

1. Introduction

Cyberspace is increasingly forming an integral part of everyday life. The opening paragraph of the Cybersecurity Strategy of the European Union from 2013 depicts this idea:

> *"An open and free cyberspace has promoted political and social inclusion worldwide; it has broken down barriers between countries, communities and citizens, allowing interaction and sharing of information and ideas across the globe; it has provided a forum for freedom of expression and exercise of fundamental rights, and empowered people in their quest for democratic and more just societies"* (European Commission, 2013, p. 2)

Five years after the inception of this strategy, this is even more the case. 85% of the households in the European Union have access to the internet (EUROSTAT, 2017). The rise in use of smartphones and so-called smart devices is one of the main drivers behind this fourth industrial revolution. Space and time themselves become relative as one can now easily control the temperature of his house while being at work. Video chats enable us to communicate throughout the world, effectively bringing the world in the palm of our hand. Moreover, the Internet of Things (IoT) does not even need human help to operate as it almost solely depends on intercommunication of connected devices. Smartness of technology and the ability of these devices to interact with each other offer numerous application possibilities in a myriad of environments ranging from hospitals to roads, cars, airports, factories and even smart cities (Elmaghraby & Losavio, 2014; Fu, et al., 2017; Zhang, et al., 2017).



Source: European Commission, 2017, p.19

As society is digitalising, so is its crime; **the flipside of this digital coin** makes society however vulnerable to an extent not previously encountered (UNODC, 2013). Crime and its actors are very adaptive to this new environment (Skórzewska-Amberg, 2017; European Commission, 2013). Modern ICT devices and infrastructures are open for traditional types of criminal activities as well as new types of crime phenomena (Helfenstein & Saarliluoma, 2014). Cybercrime continues to grow and evolve (Europol, 2017c), but it is neither the scope nor interest of this paper to give a new overview of cybercrime. The European Crime Prevention Network published a thematic paper on this issue in 2015 (EUCPN, 2015). Cybercrime as a relatively new phenomenon was situated in the criminological debate whether cybercrime constitutes a new type of crime or if these crimes are just the continuation of traditional crimes with different means (EUCPN, 2015). As an annex, a brief summary of the previous paper is presented as well as some extra input. The point of view in this previous paper was the one of the perpetrator. Yet, the current study turns this view around and *starts from a potential victim's perspective*.

The paper at hand concentrates on **cyber safety**. In order to fully take advantage of cyberspace, it is necessary to be aware of and be able to recognise the risks to online safety (Council of the European Union, 2017). The exponential evolution of cyberspace and its components makes it difficult for individuals, organisations, businesses, policy makers and governmental institutions to maintain a clear understanding of these risks (Sommer & Brown, 2011). Being safe online and securing cyberspace are however one of the most important challenges of the 21th century (ENISA, 2016c). The opening statement from the Joint Communication to the European Parliament and the Council on 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU' (2017) makes this challenge concrete:

> *"Cybersecurity is critical to both our prosperity and our security. As our daily lives and economies become increasingly dependent on digital technologies, we become more and more exposed. Cybersecurity incidents are diversifying both in terms of who is responsible and what they seek to achieve. Malicious cyber activities not only threaten our economies and the drive to the Digital Single Market, but also the very functioning of our democracies, our freedoms and our values"* (European Commission , 2017, p. 2)

We will start by referring to the definitions on cyber safety in academic literature. As with cybercrime itself, the term does not go uncontested. What's more, we will dig deeper into the digital coin discussion. Anonymization is a perfect example of benefits for both sides of the user's spectrum and has beneficiary effects for users with good and malicious intentions. A second section will clarify the commodification of data and tries to show how this data is of interest for criminals. Thirdly, we will list up the types of threats to these data and focus more specifically on card fraud and cyber-attacks. A fourth section will explore preventive and security measures.

In the **toolbox** on Cyber Safety, a more practical focus will be maintained. Policy and legislative measures will be considered as well as good practices throughout the European Union. Policy-related definitions and agenda setting are discussed here as well. This thematic paper has a more academic point of view. As such, this paper aims to contribute to raising digital awareness of local policy-makers and practitioners on a theoretical level and to clarify what risks exist and against which threats protection is needed.

2. What does it mean to be safe online?

At first glance, safety and security are words that seem clear and precise, but depending on the context they might have different meanings. Even linguistically speaking, explaining the difference is a difficult task. In some languages there even is a single word for both safety and security, for example in Spanish (*Seguridad*) or Swedish (*Säkerhet*) (Piètre-Cambacédès & Chaudet, 2010). In Dutch, an active-passive distinction can be made between safety as the active situation and security as the securing actions to achieve this. In French the translation differs depending on the context. Piètre-Cambacédès & Chaudet (2010) show two different ways to distinct safety and security based on an extensive literature review.

1. System vs. Environment distinction: here security is concerned with environmental originating risks, potentially impacting the system. Safety however deals with the risks arising from the system, impacting the environment.
2. Malicious vs. Accidental distinction: security in this distinction deals with malicious risks and safety with accidental risks.

Based on both distinctions, one could argue that in the cyber context the environment is cyberspace and the system is the individual user and his point of access to cyberspace (distinction 1) and that malicious risks originate from this environment, more specifically cybercrime (distinction 2). As such, **cyber safety** could be described as *the perfect situation where individuals move through cyberspace – in space and time – where they safely and responsibly use Information and Communication Technologies* (ICT) (Third, Forrest-Lawrence, & Collier, 2014). We do not pretend to form an exhaustive and all-encompassing definition of cyber safety here. Rather a working definition is presented to guide us through theoretical issues. Nor does cyber safety apply directly to crimes as cyber bullying since the involvement of data is key when talking about cyber safety. Data corruption or dissemination for example could be a constituent part of cyber bullying, and it is exactly this part we are interested in here.

One of the ways of being safe online is the use of **encryption**. Services as WhatsApp, Jabber, Viber,… have increasingly adopted more thorough ways of encryption in order to ensure privacy. WhatsApp recently changed its encryption to end-to-end encryption providing better privacy protection. Inherent to these messaging systems is the asynchronous aspect. One must be able to send a message to another person, even if the latter is offline. This is a perfect example of the absence of time in cyberspace. Typically, the encrypted message is temporarily stored on a server while the receiver of the message is offline (Cohn-Gordon, Cremers, Garratt, Millican, & Milner, 2017). With end–to-end encryption, only the people within the chat can decrypt and read the messages in this type of encryption. The central server is no longer able to read these texts since only the people in the chat have the decryption key (Europol, 2016a). This allows users to communicate freely without the risk of being spied upon (Toldinas, Venckauskas, Grigaliunas, Damasevicius, & Jusas, 2015).

Another anonymization tool is the use of **e-currency** such as Bitcoins. E-currency is a medium to exchange money on the web and avoid being exposed (Gad, 2014). Bitcoins and others use a blockchain structure in order to provide almost absolute privacy (Dorri, Kanhere, Jurdak, & Gauravaram, 2017). Moreover, this solves what the inventor of Bitcoin and blockchain called the 'inherent weakness of the trust based model' (Nakamoto, 2008, p. 1). Commerce on the internet relies almost exclusively on financial institutions as trusted third parties to verify electronic payments. It is difficult for the user to avoid these parties as they mediate all transactions. What blockchain and consequently Bitcoin do, is taking out these mediating parties and replacing the trust-based system with a peer-to-peer network where trust is replaced with encryption (Nakamoto, 2008; EMCDDA & Europol, 2017).

Digital: bitcoin is based on only electronic records. There is no gold or other tangible asset supporting bitcoin.

Decentralised: the system managing bitcoin is decentralised through the use of a peer-to-peer network. Every member of the network has software that distributes the management of the currency.

Open source: the software needed to acquire and use bitcoin is free and available to anyone.

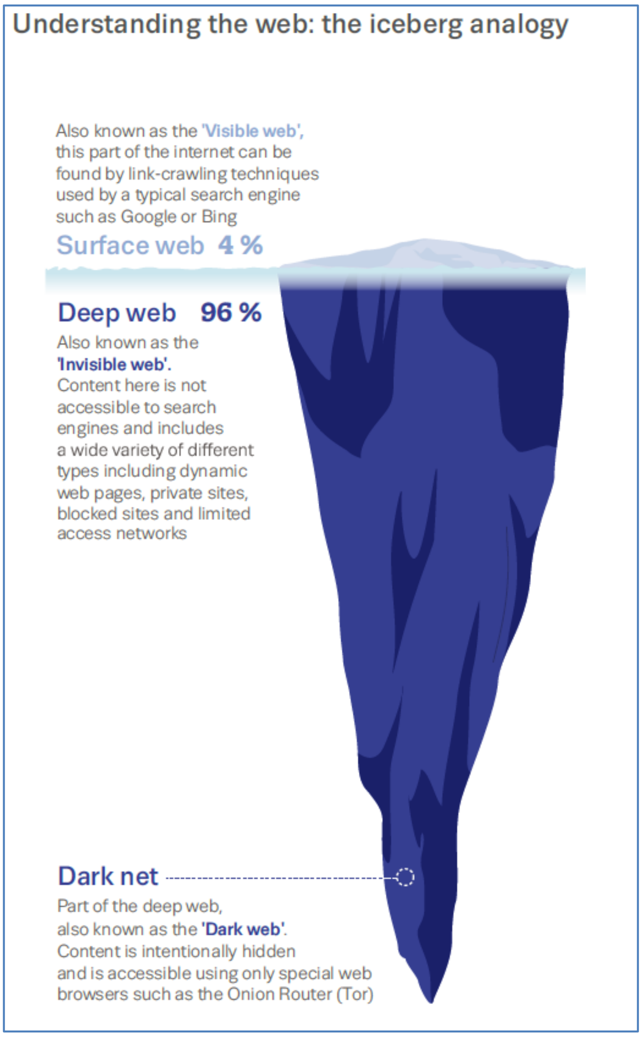
Public ledger: all bitcoin transactions are recorded in a public ledger called the blockchain, stored on the decentralised network. When a transaction is made with bitcoin, this is entered in the ledger, preventing the user from spending the bitcoin twice.

Generated through mining: new bitcoins can be generated through a process called mining, which enables the creation of a new blockchain

Source: EMCDDA & Europol (2017), Drugs and the Darknet: Perspectives for enforcement, research and policy, p23

Apart from anonymizing certain aspects of the user's action in cyberspace, it is possible to be entirely anonymous while online. TOR, Freenet or I2P are network services providing users protection from traffic analysis, which threatens personal freedom, privacy, confidential activities,… These networks enable anonymous and almost untraceable access to the internet and more specifically to what is known as the **Deep Web** (Gad, 2014; Europol, 2016a). This Deep Web is a part of the internet which is not accessible through normal browsers (e.g. Internet Explorer) or search engines (e.g. Google) (Berghel, 2017). These traditional services only scratch the Surface Web. TOR or The Onion Router is probably the most (in) famous anonymity network to access the Deep Web. It redirects the user's signals through nearly 6 000 servers, effectively concealing a user's location or usage from anyone conducting network surveillance or traffic analysis (Gad, 2014; Lacson & Jones, 2016; Spalevic & Ilic, 2017).

A subdivision of the Deep Web is called the Dark Net. This is traditionally presented with the use of an iceberg analogy. The Dark Net represents a certain amount of content of the Deep Web that is used for illegal activities such as selling drugs, illegal weapons, etc. (Sunde, 2016; Spalevic & Ilic, 2017; EMCDDA & Europol, 2017). It is not surprising that criminals have taken advantage of these networks. TOR is the perfect example of this perverse effect as it is a favourable tool within the cybercrime universe. Anonymization is of course of equal interest to criminals as they can easily conceal their identity, the hosting location of criminal websites, forums, markets,… (Europol, 2016a; Toldinas, Venckauskas, Grigaliunas, Damasevicius, & Jusas, 2015). A recent joint report by the European Monitoring Centre for Drugs and Drug Addiction and Europol (2017) estimates that 62 % of the darknet markets content is related to drugs, the other 38% goes to fraud and counterfeit, guides and tutorials, hacking and malware, firearms and explosives, and some other categories.



Understanding the web: the iceberg analogy

Also known as the 'Visible web', this part of the internet can be found by link-crawling techniques used by a typical search engine such as Google or Bing
Surface web 4 %
Deep web 96 %
Also known as the 'Invisible web'. Content here is not accessible to search engines and includes a wide variety of different types including dynamic web pages, private sites, blocked sites and limited access networks
Dark net
Part of the deep web, also known as the 'Dark web'. Content is intentionally hidden and is accessible using only special web browsers such as the Onion Router (Tor)

Source: EMCDDA & Europol (2016). EU Drug Markets Reports. In Depth Analysis, p.47

3. Data as a commodity

All actors of the current society increasingly rely on cyberspace (Council of the European Union, 2017). Conveniently, criminals have entered the cyber arena as well. ‘Society gets the crime it deserves’ is an all too familiar maxim. Cyberspace presents itself as a society or – perhaps more fitting – environment where crime seems to flourish (Helfenstein & Saarliluoma, 2014). It is clear that criminals have seen the benefits of data as a commodity and turned it into an opportunity. Indeed, data has become one of the most important commodities in contemporary society. Personal information roams freely on the internet. Social media can identify our networks and interests. Just as the world is in the palm of our hands, our privacy could be in the palms of a criminal.

Data has become a key commodity for criminals and new opportunities keep presenting themselves (Europol, 2017e). One of these opportunities is the development of the Internet of Things (IoT) and the ‘smartness’ of devices. Smart devices typically contain a large amount of sensitive personal data as they provide services to the user based on the gathered data (Arabo & Pranggono, 2013). Smartphones, smart TV’s, smart refrigerators, smart washing machines,… a lot of home and personal appliances have come to get connected to the internet and make peoples’ lives more convenient (Kang, Moon, & Park, 2017). The last couple of years have been characterized by a huge development and demand for seamless interconnectivity of smart devices (Arabo & Pranggono, 2013). The Internet of Things is the current pinnacle of this development where smart devices are connected with each other and with the individuals using them (Sunde, 2016). This creates the ability for physical objects, which were previously often unconnected and without computing power, and people to remotely interact and thereby creating a worldwide network of uniquely addressable interconnected ‘things’ (Toldinas, Venckauskas, Grigaliunas, Damasevicius, & Jusas, 2015; Stojkoska & Trivodaliev, 2016).

The IoT has led to the conception of smart environments. Smart homes are a perfect example (ENISA, 2015b). In interoperation with smart devices (e.g. the thermostat, light sensors, cameras, door locks,…), the smart home offers living conveniences for users taking their living patterns and its accumulated experience in consideration (Kang, Moon, & Park, 2017; Zeng, Mare, & Roesner, 2017; Stojkoska & Trivodaliev, 2016). The possibilities are endless and are making it possible for users to control their house regardless of space and time (Kang, Moon, & Park, 2017). You could be in the subway checking if you actually did lock your front door via the app on your smartphone (Sunde, 2016).

The smart home is not the only possible smart environment. A smart hospital for instance relies on optimized and automated processes based on the IoT to improve patient care procedures and introduced new capabilities to healthcare (Zhang, et al., 2017; ENISA, 2015a; ENISA, 2016e). Smart airports are another environment producing more seamless, secure and safe passenger experiences

(ENISA, 2016d). Smart cars provide drivers and passengers added-value services via connected infotainment systems such as hands-free telephone and messaging systems or adjusting the cars trajectory when unwillingly crossing the traffic lane due to absentmindedness (ENISA, 2016a; Elmaghraby & Losavio, 2014).

Needless to say that criminals are interested in these vast amounts of data (Arias, Ly, & Jin, 2017; Dorri, Kanhere, Jurdak, & Gauravaram, 2017; Yang, Wu, Yin, Li, & Zhao, 2017). Once they have access to this data, it can reveal sensitive information about a user's online and offline activities that are transmitted through the IoT (Apthorpe, Reisman, & Feamster, 217). The gathered data could help position a user's location for example (Sharma, Dixit, Pathik, & Sahu, 2017). It is clear that data is not 'just data' and represents another dimension. As such *data is the commodification of other online or offline objects or qualities*.

First and foremost, *privacy issues* are commodified into data (Zeng, Mare, & Roesner, 2017). A smartphone today is almost a personal assistant, containing loads of personal data such as your social network or your personal notes. Also having your home address in the GPS of your car could lead criminals to your address (Elmaghraby & Losavio, 2014). And even in your home, obtaining the data gathered from movements in your house is a severe breach of privacy concerns (Zeng, Mare, & Roesner, 2017). Patient records in smart hospitals contain the same privacy issues (ENISA, 2015a; ENISA, 2016e).

Another object that is commodified is *property*. To explain this, it is interesting to look at ransomware. In short, this malware encrypts data and only releases this data when a ransom is paid (cf. infra). In 2017 a ransomware called WannaCry infected around 300 000 systems. The data encrypted represented money, transaction orders, telephone records,… (ENISA, 2017; Europol, 2017c). This property commodification can best be seen in online banking applications. Once access is no longer secure, criminals can steal your money and for example immediately convert it to Bitcoins, anonymizing their identity (Bucko, 2017).

As such, almost anything can be commodified into data and consequently be taken advantage of by criminals. Even *time* itself can be of interest. Spamming for example is a very time consuming victimization but mostly harmless. Distributed Denial of Service (DDoS) however creates a moment in time where a server can no longer process all data and can tear down activities in this manner (Europol, 2016a). The data here represents the time needed for the server to process it.

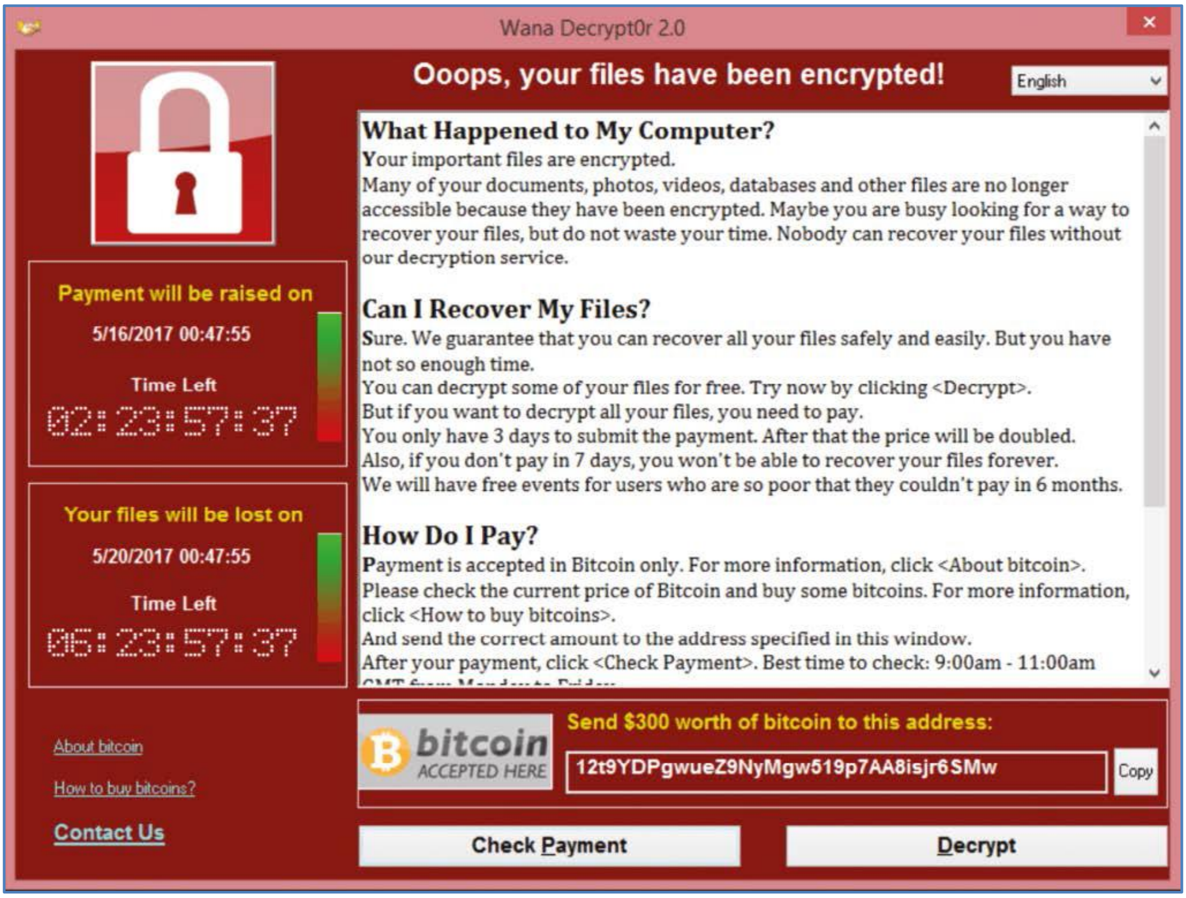
4. Threats to Cyber Safety

In order to contribute to ‘digital awareness’ we will draw attention to some of the used techniques and types of cybercrime. This however is not exhaustive. The reader is referred to the previous paper of EUCPN on cybercrime, a report by ENISA where an effort was made in 2016 to come up with a threat taxonomy and the Internet Organised Crime Threat Assessments by Europol (ENISA, 2016b; EUCPN, 2015; Europol, 2017c; Europol, 2016a). A focus will be put on *cyber-attacks*, such as malware and DDoS, and *payment fraud*.

Cyber-Attacks

Attacks in and on cyberspace are more often than not caused by **malware**. Malicious software or malware encompasses a wide range of products that enable perpetrators to gain unauthorised access to data (Rand Corporation, 2015; Europol, 2017c). According to the IOCTA of 2016, there are *two broad families of malware* (Europol, 2016a). One is *payload malware* where the goal is to obtain money or other valuable goods such as information, virtual or not. The other family exists of *enabling or facilitating malware*. Here a specific type of malware is used to spread or install other malware (Europol, 2016a).

Within the first family, ransomware is probably the most known and is a dominant concern for EU law enforcement (Europol, 2016a). In 2016 law enforcement agencies noted a 750% increase in ransomware families (Europol, 2017c). This type of malware infects computer systems as a virus (replicates through execution of a program), worm (replicates itself in a network) or Trojan horse (embedded within another installed program) and denies their users access unless upon paying a ransom (Rand Corporation, 2015; Europol, 2017b). This ransom could be in the form of money but can easily be information that is of interest to the attacker. Cryptoware is a specific type of ransomware where files are encrypted in order to deny the user access to his or her own files (Europol, 2017e).



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Source: Europol. (2017c). *Internet Organised Crime Threat Assessment (IOCTA)*. The Hague: Europol, p.26

Recently, Europe and the rest of the world were shook by a massive ransomware outburst. This WannaCry ransomware affected more than 150 countries and infected about 300 000 systems in May 2017 causing chaos due to its large scale of distribution and timing. The attackers timed the release of their malware right before the weekend, leaving businesses vulnerable for a few days. Moreover, the malware also targeted critical infrastructure, for example the UK's National Health Service (ENISA, 2017; Europol, 2017c). What's more is that these attacks are growing in sophistication. This makes it even more difficult to decrypt your hijacked files (Europol, 2016b). One month after WannaCry, (Not) Petya targeted 20 000 machines around the globe and was already a lot harder to 'crack' (Europol, 2017c).

Other payload malware are Remote Access Trojans (RAT). This type of malware is typically installed by other malware and gives almost complete control to the attacker (Europol, 2017b). RATs are also getting more custom-made, which makes it harder to identify the malware and their operators (Europol, 2017c). These other, *enabling malware* types are the second family containing exploit kits, droppers, spam,… (Europol, 2016a). Spam for example is the mass sending of emails or other electronic messages to people who did not ask for it (EUCPN, 2015). These can range from being harmless and ‘inbox-filling’ to advertising material or services leading the recipients to the real scams, malicious websites or containing malware (Zappa, 2014). Exploit kits are also part of this second family. These kits are software tools used to get other software on the victim’s system. They exploit security holes in the operating system (Rand Corporation, 2015; Johnson, 2013). Zero-day kits for example target security vulnerabilities in a system originating to the initial start of the system before the developers are aware of this problem.

A DoS is another key cyber-attack according to Europol (2016a). In a **Denial of Service** attack, the attacked system receives a lot of data in such a way that it can no longer respond to it and as such denying the service normally provided by the attacked system (Nagy & Mezei, 2016; Zappa, 2014). A DDoS or Distributed DoS is launched from multiple connected devices that are distributed across the internet (Nagy & Mezei, 2016). This type of cyber-attack is a favourable tactic of hacktivists as well (Rand Corporation, 2015). Anonymous for example launched several (D)DoS attacks against the Church of Scientology in 2008, or more recently against ISIS websites.

The multiple connected devices in a DDoS could be used as a botnet (Europol, 2016a). Here a network of malware infected devices is controlled by attackers (Arabo & Pranggono, 2013; Zappa, 2014). In October 2016 the Mirai botnet, consisting of connected IoT devices, launched an attack on Dyn, a company offering internet domain names. The attack affected internet access for the US’s west coast for about 2 hours. One month later, a variant of the network attacked Deutsche Telekom, resulting in a similar outcome. These networks provide criminals with immense computer capacity to conduct all kinds of cybercrime such as banking fraud, spam, DDoS attacks,… (Rand Corporation, 2015; Europol, 2017c).

A whole array of cyber-attacks is possible and potential criminals do not even need a high level of skill to pursue them. The Crime-as-a-Service model (see Annex, p.23) provides easy access to the tools and services that are required to carry out attacks, driving the digital underground economy in doing so (Europol, 2017e; Toldinas, Venckauskas, Grigaliunas, Damasevicius, & Jusas, 2015; Gad, 2014). Due to a division of labour in this underground, the model is booming. Malware could be sold or rented out, criminals could be payed to hack a certain account, money mules could be found to interrupt the money trail pointing to criminals, and even brokers exist to act as a trusted intermediary in criminal transactions… (Leukfeldt & Jansen, 2015; Gad, 2014; Europol, 2014). As a result, there is a huge disparity between the costs of attacks and the costs for both prevention and reparation (Europol, 2017c).

Payment fraud

The drive for trust with the blockchain system might also stem from the practices surrounding payment fraud on the web. There are different types of payment fraud. One is *card-present fraud* where the practice of skimming is most common (Europol, 2016a). Here, card data is extracted from the magnetic strip of a payment card by mechanical tools or malware installed on the ATM and is later on used online or offline (Europol, 2017e; EUCPN, 2015; Europol, 2017c). *E-commerce fraud* on the other hand consists of 66% of total card fraud practices (Europol, 2016a). This type of fraud intervenes in card-not-present transactions where the plastic card is not handed to the merchant or machine at the time of payment or transaction (Ali, Arief, Emms, & van Moorsel, 2017; Smart Card Alliance, 2014). In card-not-present fraud criminals use the card data to purchase products and services in an e-commerce setting, e.g. the Dark Net. In a majority of cases, the victims are unaware of this unauthorised use of their card which is still in their actual possession (Europol, 2017d). Automated card shops (ACS) offer fraudsters automated click-and-buy sites where they can search for cards. A large number of these are scam sites where criminals effectively 'rip off each other' (Europol, 2017c).

A common tactic to obtain the card data is by **phishing** (Europol, 2017a). This specific form of spamming takes advantage of the cyberspace effects on human behaviour (Agustina, 2015; Bhattacharyya, Jha, Tharakunnel, & Westland, 2011; Skórzewska-Amberg, 2017). The aim is to deceive the victim to obtain personal information (EUCPN, 2015; Jansen & Leukfeldt, 2016; Zappa, 2014). In the case of payment fraud, the goal is of course to gather the user credentials of the card (Choo, 2011). This can either be a massive scam or a more tailored attack which is called spear-phishing (EUCPN, 2015; Vishwakarma, 2017).

The problem for the fraudster stays however: he needs to move the victim into a mindset where he engages in an exploitive interaction (Burgard & Schlembach, 2013). Mostly, **social engineering** of the victim takes place in order to achieve this (Moreno-Fernández, Blanco, Garaizar, & Matute, 2017). Social engineering is a set of techniques that exploit human behaviour through deception, identity hiding or assuming a different identity. In other words, attackers exploit the weakest link in cyber security: the human (Europol, 2016a; Zappa, 2014; Europol, 2017c).

An example of assuming a different identity is CEO fraud. Here, the attacker could contact an employee speaking to him as if it was the CEO (Europol, 2016a). A preliminary investigation is done by the attacker to become acquainted with the firm and its structure, the CEO's linguistic characteristics,… in order to fulfil the scam (Uma & Padmavathi, 2013). A familiar manner in literature to explain the mechanisms underlying this is by the six principles of influence by Cialdini (Uebelacker & Quiel, 2014; Cialdini, 2009).

- Reciprocation: a social norm that obliges people to repay what another person provided us;
- Commitment and consistency : the urge to behave in compliance with what we already did and said;
- Social proof: the tendency to validate an action as positive when peers often engage in this specific action;
- Liking: not fulfilling a request for example is considered disrespectful. We want people to like us;
- Authority: Police ransomware uses this influence factor as it takes advantage of the perceived authority law enforcement has over people. Victims follow their orders more easily;
- Scarcity: people value certain things more as there are is less availability.

If we further elaborate on the CEO fraud, we can see how 'authority' is an obvious influencer, but also not being perceived as disrespectful ('liking'), 'consistency' and other factors come into play.

5. Prevention, security and the circular movement

One of the characteristics of cybercrime is the asymmetry aspect. Because of this, law enforcement struggles to keep up with the ever changing modi operandi of the perpetrators (EUCPN, 2015). We could almost say that - as is the case with drug traffic or illegal migration – a waterbed effect is in play. The moment the police for example are familiar with a certain malware, criminals already moved on to another and more sophisticated one. Add this to the difficulties arising from transposing traditional criminological theories (see Annex) and you have no real 'guidebook' to formulate prevention strategies. To be clear, what we mean by prevention here is prevention targeted at 'cyber victimization' and more specifically to threats to cyber safety.

According to Reyns, Randa and Henson (2016), the leading approach for prevention of cyber safety issues focusses on *reducing opportunities*. As it is difficult to perceive who will be victim and when it will happen, focusing on the moment it does happen seems almost the best option. This automatically leads us to *situational crime prevention* and circles back to Routine Activity Theory (cf. Annex). Situational crime prevention mainly tries to manipulate the situational characteristics that generate criminal opportunities (Jacques & Bonomo, 2017). **Cyber security** fits this idea perfectly. Although definitions differ on what cyber security exactly is, logically speaking it is the securing of cyberspace (Christou, 2017; Dewar, 2017; Carrapico & Barrinha, 2017; Rand Corporation, 2015; OECD, 2012; CEN/CENELEC Cyber Security Focus Group, 2017; RAND Corporation, 2016).

This securing is done by technologies and processes to protect computers, networks and data from unauthorized access, vulnerabilities and attacks by cyber criminals, hence taking away the situational characteristics for crime genesis (Aggarwal, Arora, Neha, & Poonam, 2014). Examples of these are installing firewall and other anti-virus software to counter harmful programs (Brenner & Clarke, 2005). However, these processes are not merely computational (Agustina, 2015). As stated earlier, unauthorized access can be staged by a process called 'social engineering'. Securing would then also mean being able to resist to this danger (Brenner & Clarke, 2005). The work of Miló LLinares (2012) is of specific interest here. This author transformed the 25 techniques of situational crime prevention of Cornish and Clarke (2003) to a cyber context. The table below shows his reinterpretation.

REDUCING ENVIRONMENT OF INCIDENCE	INCREASING PERCIEVED EFFORT	INCREASING PERCIEVED RISK	REDUCING PERCIEVED REWARDS	ELIMINATING EXCUSES
Don't introduce targets Separation of hard drives with and without access to system; Systems of parental control; Content filters; ActiveX security controls; No access to chat rooms *(grooming)*	**Control access to system** Firewall; Update operating systems; Passwords for system access; Passwords for access to web; Update passwords; Profiles on social networks	**Extend guardianship** Forum moderators; Echelon, Enfopol, Carnivore and Dark Web systems	**Hide targets** Use systems of encryption; Hide personal data on social networks; Don't use bank passwords; Perfect ecommerce systems	**Set rules** International legal harmonisation; "Netiquette"

Identify risk zones
Informational campaigns about risks;
Advise network of spam infections;
White and blacklists of web
and spam;
Identify bots
	Detect and impede the attack
	Antivirus;
	Antispyware;
	Antispam;
	systems of control for electronic banking
		Reduce anonymity
		Identify IPs;
		Registration on web forums;
		User identification systems;
		Biometric identification and authentication
			Remove targets
			Removable hard drives;
			Alternative payment systems (PayPal);
			Change web addresses, domains and other
				Set rules
				Web licence notifications: copyright and 'copyleft';
				Privacy notifications on social networks

Decontamination/residue cleanup Erase and destroy latent viruses; Bot disinfection	**Deflect offenders** Close networks; Request removal of illicit content; Flagging mechanisms on social networks; Denial of access to specific IPs.	**Strengthen formal surveillance** Control networks through proxy; Specialized teams for cyber crime persecution	**Remove benefits** Persecution of buyers of illicit content; persecution of money laundering	**Strengthen moral conscience** Raise consciousness about intellectual property; Morally enforce legitimate businesses

Separatation of targets
Internet2;
Creation of local security sub-networks
	Control tools/weapons
	Obligatory vigilance through IPPPS;
	Control data through RSS
		Assist natural surveillance
		Improve IP identification systems;
		Reconstruct architecture with defensive ends
			Disrupt markets
			Offer economic systems of file sharing (Spotify and others);
			Control direct file download sites
				Assist compliance
				New business models (Apple);
				Legal hacker competitions;
				Strengthen open software

Within criminology, there are however some well-known problems with situational crime prevention. One of the hardest critics is the blaming of the victim. This view is probably best formulated by blaming rape victims of inciting the perpetrator (Wortley, 2010). The RAT theory is disputed to be applicable to cyberspace. The same remark could be made regarding the critic 'blaming the victim'. Due to the different characteristics of cybercrime, who could blame the victim? The ubiquity of victims because of the anti-spatial and anti-temporal features of cyberspace leaves almost everyone open to victimization. This is shown for example in a study by Jansen and Leukfeldt (2016) where the value or visibility of a potential victim has no specific impact on being the subject of online banking fraud. Again, a counter example could be made with social engineering where victims could be blamed of naivety or thoughtlessness (Agustina, 2015).

To leave this discussion, it suffices to say that criminology and prevention strategies have a difficult time in cyberspace. In order to be able to devise grounded prevention and security it is however necessary to further examine the threats that need to be addressed and against what these threats are aimed for. Just as it is perhaps more interesting to characterize cybercrime rather than actually define it, the same might apply to elaborate on the objects that have to be secured and the threats to cyber safety.

Note that it is here that the *distinction between safety and security is blurred*. The reader may have noticed that **although cyber safety and cyber security are considered separately, security measures were proposed while describing safety.** To be anonymous on the web is considered safe use of ICT. In order to achieve this, anonymization is necessary. The act of encryption for example is such a security measure. The blockchain mechanism is a securing mechanism to bypass the trust issues existing in traditional online trade, rendering online payments 'safe'. **The distinction made in the working definition thus becomes irrelevant seeing this circular movement of safety and security in cyberspace**. This inextricable link between the two terms is why they are used variably throughout literature and policy (Wolf & Serpanos, 2017). Conversely, cybercriminals also use safety and security measures as illustrated in the following figure.

privacy, freedom of speech

hard to trace, privacy, cryptoware

replaces intermediary trust model

hard to trace, easier money laundering

privacy, freedom of speech

hard to trace, Dark Net, Crime-as-a-service

6. Conclusion

The main goal of this paper was to further draw on the picture of the cyber safety and security landscape and building on the previous cybercrime paper of the EUCPN. Firstly, we tried to define what is considered safe in cyberspace. Secondly, we took an interest in what actually composes the object of cybercrime. Putting the different definitions of cybercrime aside, it becomes clear that data is the encompassing object. Without degrading all cybercrime to data-theft, we saw that data is the commodification of other values such as privacy, property or even time. Data in this way is never 'just data'. Thirdly, two different threats to cyber safety and security where considered. Cyber-attacks were narrowed down to malware, DDoS attacks and botnets. Payment fraud was discussed in light of phishing and social engineering. However, the two types of threats do not rule each other out since malware for example can easily be hidden in phishing e-mails. A last section provided insight on preventing victimization online and securing cyberspace.

In conclusion, we can say that cyberspace is as much a **crime-generator** as a **crime-attractor** (Agustina, 2015). Different aspects of this environment have led to a rise in new or old crimes. This sets the scene for a very difficult policy and practitioner's field. Nonetheless, **safety and security in cyberspace will play a crucial role in the next couple of years with a society that is digitalizing in a massive pace**. A toolbox will be written on the policy and practice of this delicate subject.

Annex: The criminological definitional problem

As with many criminal phenomena, criminologists are discussing the definition of cybercrime. Defining often says more about the view of the one that is defining, rather than the actual phenomenon at hand. This is even more so the case when defining cybercrime. There are two very different views in this discussion. **The transformationist view** states that cybercrime is a totally new form of crime (EUCPN, 2015; Leukfeldt & Yar, 2016). Jaishankar, one of the founders of cyber criminology, is a fierce proponent of this view. He expresses the need for cyber theories that are apt to explain crime in cyberspace (Jaishankar, 2011). As such, cybercrime represents a new and distinctive format of crime, creating challenges to the prediction and prevention of it (UNODC, 2013). Even the prefix 'cyber' suggests that this phenomenon occurs in a space different from where humans normally interact (Sunde, 2016). Moreover, theoretical issues with traditional criminological theories arise. The usual suspects for example in many 'real life' theories are minorities, poorly educated offenders, originating from the lower classes, etc. Cybercriminals however tend to be well educated middle-class members (Diamond & Bachmann, 2015; Leukfeldt & Yar, 2016). It has led Jaishankar to theorize the 'space transition theory' which has as its prime assumption that people behave differently when they move from one space to another. For example, people with repressed criminal behaviour in physical space have, according to this theory, a propensity to commit crimes in cyberspace, crimes that they would never do due to their status and socio-economic position (Jaishankar, 2011).

On the other hand, **the continuist view** sees cybercrime merely as 'old wine in new bottles'. These proponents state that cybercrime is conventional crime going digital. The affected interests still remain the same. A fraudster is still a fraudster even if he does it online (Leukfeldt & Yar, 2016; Viano, 2017). The tools in achieving the goal of the crime changed, not the intrinsic crime (EUCPN, 2015).

Apart from defining cybercrime, it is perhaps more interesting to look at its characteristics as is done in the earlier EUCPN paper. The *international* and borderless aspect of cybercrimes is a first characteristic. This has a rather special effect since the criminal objects come to the criminal, leading to an increased availability of potential victims (Helfenstein & Saarliluoma, 2014). Moreover, due to the *scalability* of crimes, perpetrators can easily replicate crimes on a massive scale. A perfect example of this is phishing. *Anonymity* as a characteristic does not need much more explanation. As stated in the paper, as well as providing cyber safety to the typical user, the anonymization effect of the internet is of equal interest to the malevolent user. What's more, users could potentially be victimized without even knowing. Another characteristic, *asymmetry*, is something we find in other phenomena as well. Just as with the designer drug market, police and justice authorities are struggling to keep up with new modi operandi and products.

Low marginal cost of online activity is one of the reasons why cybercrime is so attractive. Computers and other programs almost do the dirty work for perpetrators, augmenting the perceived sense of safety and anonymity in the process. Lowering these costs even more is the *nature of criminal cooperation* in cyberspace. As a result of this a 'Crime-as-a-service' model has grown. Here cybercriminals share, rent or sell their malware, computing resources and hosting services to the lesser cyber adapt criminals (Gad, 2014). This model facilitates virtually any type of cybercrime by making it almost child's play (Toldinas, Venckauskas, Grigaliunas, Damasevicius, & Jusas, 2015). Add these characteristics to specific criminal motives as financial gain, emotion, sexual impulses, politics or religion and 'fun' together with an enormous availability of potential victims and you have the perfect recipe to apply the *Routine Activity Theory* to cybercrime. Or not?

Especially from a crime prevention perspective, the *Routine Activity Theory* (RAT) has had an enormous impact. And more often than not, RAT is at the centre of theoretical discussions about applicability to cyberspace (Leukfeldt & Yar, 2016). According to this theory crime risk increases upon a convergence of time and space of three factors: a motivated offender, a suitable target and absence of capable guardians (Jansen & Leukfeldt, 2016; UNODC, 2013; Reyns, Randa, & Henson, 2016). A literature review on nine empirical studies on RAT's applicability to cybercrime by Leukfeldt & Yar (2016) shows mixed results. Five studies have positive results, while six of them came to a negative conclusion. The same mixed results were shown by Ngo & Paternoster (2011) depending on the type of cybercrime.

Yar (2005) formulates criticism on RAT as a valid theory for cybercrime because of the ecological problem. The transposability of RAT to cyberspace requires that cyberspace has a similar spatio-temporal ontology as the physical world. As stated before, time and space are relative in cyberspace. Notions of place location and spatial separation are first of all non-existent in an environment that is anti-spatial. The imagery of having the world in your hand is exemplary here. Secondly, temporal structures are problematic as well. There are no particular points in time at which actors can be expected to be generally present or absent from the environment (Yar, 2005). Furthermore, suitable targets can be constructed by social engineering leaving victims to play a crucial role in their own victimization (Jansen & Leukfeldt, 2016). Cyberspace seems to foster attitudes of excessive trust, naivety or thoughtlessness which offenders happily take advantage of (Agustina, 2015).

Other theories are being tested as well. Social learning theories, where potential criminals learn from peers, are also noteworthy here. Especially on the Dark Net and applying this to the Crime-as-a-Service model promises to be very interesting (Diamond & Bachmann, 2015).

References

Aggarwal, P., Arora, P., Neha, & Poonam. (2014). Review on Cyber Crime and Security. *International Journal of Research in Engineering and Applied Sciences, 2*(1), 48-51.

Agustina, J. (2015). Understanding Cyber Victimization: Digital Architectures and the Disinhibition Effect. *International Journal of Cyber Criminology, 9*(1), 35-54.

Ali, M., Arief, B., Emms, M., & van Moorsel, A. (2017). Does The Online Card Payment Landscape Unwittingly Facilitate Fraud? *IEEE Security and Privacy*.

Apthorpe, N., Reisman, D., & Feamster, N. (217). *A Smart Home is No Castle: Privacy Vulnerabiliies of Encrypted IoT Traffic.*

Arabo, A., & Pranggono, B. (2013). Mobile Malware and Smart Device Security: Trends, Challenges and Solutions. *19th International Conference on Control Systems and Computer Science* (pp. 526-531). Bucharest: IEEE Computer Society.

Arias, O., Ly, K., & Jin, Y. (2017). Security and Privacy in IoT Era. In H. Yasuura, C. Kyung, Y. Liu, & Y. Lin, *Smart Sensors at the IoT Frontier* (pp. 351-378). Springer International Publishing.

Berghel, H. (2017). Which is More Dangerous- The Dark Web or the Deep State? *IEEE Computer Society, 50*(7), 86-91.

Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. (2011). Data mining for credit card fraud: A comparative study. *Decision Support Systems, 50*, 602-613.

Brenner, S., & Clarke, L. (2005). Distributed Security: Preventing Cybercrime. *The John Marshall Journal of Information Technology & Privacy Law, 23*(4), 659-710.

Bucko, J. (2017). Security of Smart Banking Applications in Slovakia. *Journal of Theoretical and Applied Electronic Commerce Research, 12*(1), 42-52.

Burgard, A., & Schlembach, C. (2013). Frames of Fraud: A Qualitative Analysis of the Structure and Process of Victimization on the Internet. *International Journal of Cyber Criminology, 7*(2), 112-124.

Carrapico, H., & Barrinha, A. (2017). The EU as a Coherent (Cyber)Security Actor? *Journal of Common Market Studies*, 1-19.

CEN/CENELEC Cyber Security Focus Group. (2017). *Definition of Cybersecurity.* CEN/CENELEC Cyber Security Focus Group,.

Choo, K. (2011). The cyber threat landscape: challenges and future research directions. *Computers & Security, 30*, 719-731.

Christou, G. (2017). The EU's Approach to Cybersecurity. *EU-Japan Security Cooperation: Challenges and Opportunities, 2017*(Spring/Summer), 1-13.

Cialdini, R. (2009). *Influence: the psychology of persuasion.*

Cohn-Gordon, K., Cremers, C., Garratt, L., Millican, J., & Milner, K. (2017). On Ends-to-Ends Encryption: asynchronous group messaging with strong security guarantees. *IACR Cryptology ePrint Archive*.

Cornish, D., & Clarke, R. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. In M. Smith, & C. D., *Theory for Practice in Situational Crime Prevention* (pp. 41-96). Monsey: Criminal Justice Press.

Council of the European Union. (2017). *Detailed Report on the Outcome of the Questionnaire (CM1124/17): Prevention and Cyber Awareness across the EU among its citizens and its SMEs .* Brussels.

Dewar, R. (2017). *Cyber security in the European Union: An historical institutionalist analysis of a 21st century security concern.* Glasgow: Glasgow University.

Diamond, B., & Bachmann, M. (2015). Out of the Beta Phase: obstacles, challenges, and promising paths in the study of cyber criminology. *International Journal of Cyber Criminology, 9*(1), 24-34.

Dorri, A., Kanhere, S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. *Pervasive Computing and Communications Workshops*, 618-623.

Elmaghraby, A., & Losavio, M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of Advanced Research, 5*, 491-497.

EMCDDA & Europol. (2016). *EU Drug Markets Reports. In Depth analysis.* Luxembourg: Publications Office of the European Union.

EMCDDA & Europol. (2017). *Drugs and the Darknet: Perspectives for enforcement, research and policy.* Luxembourg: Publications Office of the European Union.

ENISA. (2015a). *Security and Resilience in eHealth Infrastructures and Services.*

ENISA. (2015b). *Security and Resilience of Smart Home Environments.*

ENISA. (2016a). *Cyber Security and Resilience of Smart Cars.*

ENISA. (2016b). *ENISA Threat Taxonomy.*

ENISA. (2016c). *NCSS Good Practice Guide: Designing and Implementing National Cyber Security Strategies.* ENISA.

ENISA. (2016d). *Securing Smart Airports.*

ENISA. (2016e). *Smart Hospitals. Security and Resilience for Smart Health Service and Infrastructures.*

ENISA. (2017, May 15). *WannaCry Ransomware Outburst*. Retrieved from ENISA: https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst

EUCPN. (2015). Cybercrime: a theoretical overview of the growing digital threat. In EUCPN Secretariat, *EUCPN Theoretical Paper Series.* Brussels: European Crime Prevention Network.

European Commission . (2017). *Joint Communication to the European Parliament and the Council 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU'.* Brussels: European Commission.

European Commission. (2013). *Cybersecurity Strategy of the European Union: an open, safe and secure cyberspace.* Brussels: European Commission.

European Commission. (2015). *Special Eurobarometer: Cyber Security.* European Commission.

European Commission. (2017). *Special Eurobarometer: Europeans' attitudes towards cyber security.* European Union.

Europol. (2014). *Internet Organised Crime Threat Assessment (IOCTA).* The Hague: Europol.

Europol. (2016a). *Internet Organised Crime Threat Assessment (IOCTA).* The Hague: Europol.

Europol. (2016b). *Ransomware: What you need to know.* The Hague: Europol.

Europol. (2017a). *Banking Trojans: From Stone Age to Space Era.* The Hague: Europol.

Europol. (2017b). *Cybercrime*. Retrieved from Europol: https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime

Europol. (2017c). *Internet Organised Crime Threat Assessment (IOCTA).* The Hague: Europol.

Europol. (2017d). *Payment Fraud*. Retrieved from Europol: https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/forgery-of-money-and-means-of-payment/payment-fraud

Europol. (2017e). *Serious and Organised Crime Threat Assessment (SOCTA).* The Hague: Europol.

EUROSTAT. (2017, august 09). *Level of internet access-households*. Retrieved from Eurostat: http://ec.europa.eu/eurostat/tgm/graph.do?tab=graph&plugin=1&pcode=tin00134&language=en&toolbox=type

Fu, K., Drobnis, A., Morrisett, G., Mynatt, E., Patel, S., Poovendran, R., & Zorn, B. (2017). *Safety and Security for Intelligent Infrastructure.* National Science Foundation.

Gad, M. (2014). Crimeware Marketplaces and Their Facilitating Technologies. *Technology Innovation Management Review, 4*(11), 28-33.

Helfenstein, S., & Saarliluoma, P. (2014). How cyber breeds crime and criminals. *DigitalSec 2014 Proceedings: The International Conference on Digital Security and Forensics* (pp. 76-90). Wilmington: The Society of Digital Information and Wireless Communications.

Jacques, S., & Bonomo, E. (2017). Learning from the Offenders' Perspective on Crime Prevention. In B. Leclerc, & E. Savona, *Crime Prevention in the 21st Century* (pp. 9-18). Cham: Springer.

Jaishankar, K. (2011). *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior.* Florida: Taylor & Francis Group.

Jansen, J., & Leukfeldt, R. (2016). Phishing and Malware Attacks on Online Banking Customers in the Netherlands: A Qualitative Analysis of Factors Leading to Victimization. *International Journal of Cyber Criminology, 10*(1), 79-91.

Johnson, M. (2013). *Cyber Security: Threats and Solutions.* London: Ark Group.

Kang, W., Moon, S., & Park, J. (2017). An enhanced security framework for home appliances in smart home. *Human-Centric Computing and Information Sciences, 7*(6).

Lacson, W., & Jones, B. (2016). The 21st Century DarkNet Market: Lessons from the Fall of Silk Road. *International Journal of Cyber Criminology, 10*(1), 40-61.

Leukfeldt, E., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior, 37*(3), 263-280.

Leukfeldt, R., & Jansen, J. (2015). Cyber Criminal Networks and Money Mules: An Analysis of Low-Tech and High-Tech Fraud Attacks in the Netherlands. *International Journal of Cyber Criminology, 9*(2), 173-184.

Lin, I., & Liao, T. (2017). A survey of Blockchain Security Issues and Challenges. *International Journal of Network Security, 19*(5), 653-659.

Llinares, M. (2012). *El cibercrimen. Fenomenología y criminología de la delincuancia en el ciberespacio.* Madrid: Marcial Pons.

Moreno-Fernández, M., Blanco, F., Garaizar, P., & Matute, H. (2017). Fishing for phishers. Improving Internet users' sensitivity to visual deception cues to prevent electronic fraud. *Computers in Human Behavior*, 421-436.

Nagy, Z., & Mezei, K. (2016). The organised criminal phenomenon on the Internet. *Journal of Eastern-European Criminal Law, 2*, 137-149.

Nakamoto, S. (2008). Bitcoin: a peer-to-peer electronic cash system.

Ngo, F., & Paternoster, R. (2011). Cybercrime Victimization: An examination of Individual and Situational Level Factors. *International Journal of Cyber Criminology, 5*(1), 773-793.

No More Ransom Project. (2017). *Ransomware Q&A*. Retrieved from No More Ransom: https://www.nomoreransom.org/nl/ransomware-qa.html

OECD. (2012). *Cybersecurity policy making at a turning point.* OECD.

Piètre-Cambacédès, L., & Chaudet, C. (2010). The SEMA referential framework: avoiding ambiguities in the terms "'security" and "safety". *International Journal of Critical Infrastructure protection, 2010*(3), 55-66.

Rand Corporation. (2015). *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses.* Brussels: European Parliament.

RAND Corporation. (2016). *A focus on Cybersecurity.* Brussels: Rand Corportation.

Reyns, B., Randa, R., & Henson, B. (2016). Preventing Crime Online: identifying determinants of online preventive behaviors using structural equation modeling and canonical correlation analysis. *Crime Prevention and Community Safety: an international journal, 18*(1), 38-59.

Sharma, S., Dixit, S., Pathik, B., & Sahu, S. (2017). Review of Malware Data Classification and Detection in Smart Devices. *International Research Journal of Engineering and Technology, 4*(5), 202-209.

Skórzewska-Amberg. (2017). Global Threats But National Legislations- How to adapt to the New Cyberspace Society. In E. Viano, *Cybercrime, Organized crime and Societal Responses* (pp. 67-86). Cham: Springer.

Smart Card Alliance. (2014). *Card-Not-Present Fraud: A Primer on Trends and Authentication Processes.* New Jersey: Smart Card Alliance.

Sommer, P., & Brown, I. (2011). *Reducing Systemic Cybersecurity Risk.* OECD.

Spalevic, Z., & Ilic, M. (2017). The use of dark web for the purpose of illegal activity spreading. *Ekonomika, 63*(1), 73-82.

Stojkoska, B., & Trivodaliev, K. (2016). A review of Internet of Things for smart home: Challenges and solutions. *Journal of Cleaner Production*.

Sunde, I. (2016). A new thing under the sun?: Crime in the digitized society. *Research Seminar: New challenges in criminology: can old theories be used to explain or understand new crimes*, 60-79.

Third, A., Forrest-Lawrence, P., & Collier, A. (2014). *Addressing the cyber safety challenge: from risk to resilience.* Telstra Corporation.

Toldinas, J., Venckauskas, A., Grigaliunas, S., Damasevicius, R., & Jusas, V. (2015). The 3rd International Virtual Research Conference in Technical Disciplines. *Suitability of the digital forensic tools for investigation of cyber crime in the Internet of Things and Services* (pp. 86-97). Zilina: Publishing Institution of the University of Zilina .

Uebelacker, S., & Quiel, S. (2014). The social engineering personality framework. *Socio-Technical Aspects in Security and Trust (STATS)*, 22-30.

Uma, M., & Padmavathi, G. (2013). A Survey on Various Cyber Attacks and Their Classification. *International Journal of Network Security, 15*(5), 390-396.

UNODC. (2013). *Comprehensive Study on Cybercrime.* Vienna: UNODC.

Viano, E. (2017). Cybercrime: Definition, Typology and Criminalization. In E. Viano, *Cybercrime, Organized crime, and Societal Responses* (pp. 3-22). Cham: Springer.

Vishwakarma, P. (2017). Emerging Online Frauds: Detection and Their Possible Controlling Strategies in E-Business. *International Journal of Innovative Research in Engineering & Management, 4*(3), 655-657.

Wolf, M., & Serpanos, D. (2017). Safety and Security of Cyber-Physical and Internet-of-Things Systems. *Proceedings of the IEEE, 105*(6), 983-984.

Wortley, R. (2010). Critiques of situational crime prevention. In B. Fisher, & S. Lab, *Encyclopedia of Victimology and Crime Prevention.* Thousand Oaks: Sage.

Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A Survey on Security and Privacy Issues in Internet-of-Things. *IEEE Internet of Things Journal*.

Yar, M. (2005). The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory. *European Journal of Criminology, 2*(4), 407-427.

Zappa, F. (2014). *Cybercrime and the Risks for the Economy and Enterprises at the EU and Italian Level.* UNICRI.

Zeng, E., Mare, S., & Roesner, F. (2017). End User Security and Privacy Concerns with Smart Homes. *Proceedings of the Thirteenth Symposium on Usable Privacy and Security* (pp. 65-80). Santa Clara: USENIX.

Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., & Shen, X. (2017). Security and Privacy in Smart City Applications: Challenges and Solutions. *IEEE Communications Magazine*(January), 122-129.