European Crime Prevention Network

Theoretical Paper

Cybercrime

Cybercrime: A theoretical overview of the growing digital threat

In the framework of the project 'The development of the observatory function of the European Centre of Expertise on Crime Prevention within the EUCPN' - EUCPN Secretariat, February 2016, Brussels

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

Cybercrime: a theoretical overview of the growing digital threat

Abstract

This theoretical paper is published by the EUCPN Secretariat in connection with the theme of the Luxembourgian presidency which was cybercrime. Cybercrime is a global definition which characterizes many different criminal forms committed in the virtual world. This means the phenomenon covers a very wide scope of activities. This theoretical paper is written as an overview to help understand the definition of cybercrime and its forms. We concentrate on the variety of consequences as a result of the phenomenon. Moreover, this paper also has attention to the current European law and legislative actions against cybercrime.

Citation

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

Author

Cindy Verleysen, 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

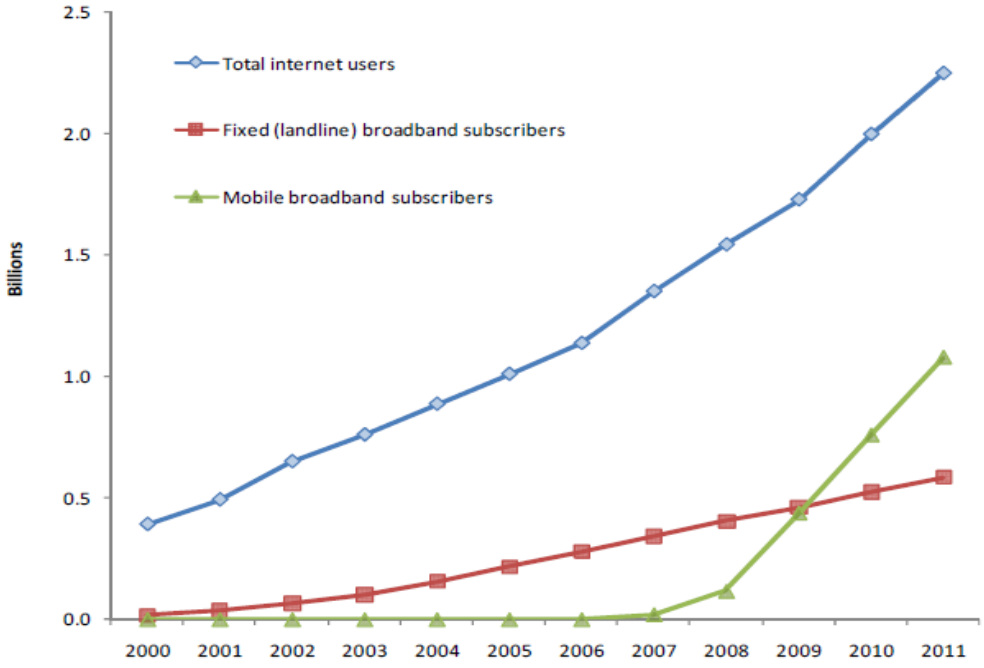
Content

1. Introduction

In 2011, at least 2,3 billion people, which is the equivalent of more than 1/3th of the world's total population, had access to the Internet. Over 60% of all Internet users are in developing countries, with 45% of all internet users below the age of 25 years.[1] Figure 1 gives us the evolution of the global internet connectivity since 2000.[2]

The 2014 Internet Organised Crime Threat Assessment (iOCTA) mentioned already more than 2,8 billion people using the Internet across the globe and over 10 billion Internet-facing devices in existence.[3] By the year 2017, it is estimated that mobile broadband subscriptions will approach 70% of the world's total population.[4]

Figure 1: The Global internet connectivity 2000-2011



Source: ITU World Telecommunication ICT Indicators 2012

[1] **United Nations Office on Drugs and Crime** (2013), '*Comprehensive Study on Cybercrime*', Vienna, February 2013. [https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf]
[2] **United Nations Office on Drugs and Crime** (2013), '*Comprehensive Study on Cybercrime*', Vienna, February 2013. [https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf]
[3] **Europol** (2014), '*The Internet Organised Threat Assessment (iOCTA) 2014',* The Hague, 2014.
[4] **United Nations Office on Drugs and Crime** (2013), '*Comprehensive Study on Cybercrime*', Vienna, February 2013. [https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf]

European societies are nowadays increasingly dependent on electronic networks and information systems. Over the last twenty years, the Internet - more broadly cyberspace has had a tremendous impact on all parts of our society. Our daily life, our fundamental rights, social interactions and economies depend on information and communication technology working seamlessly. 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 – most strikingly during the Arab Spring.5 Technology has become integral to virtually every sector of the global economy, including banking, communications and the electrical grid.

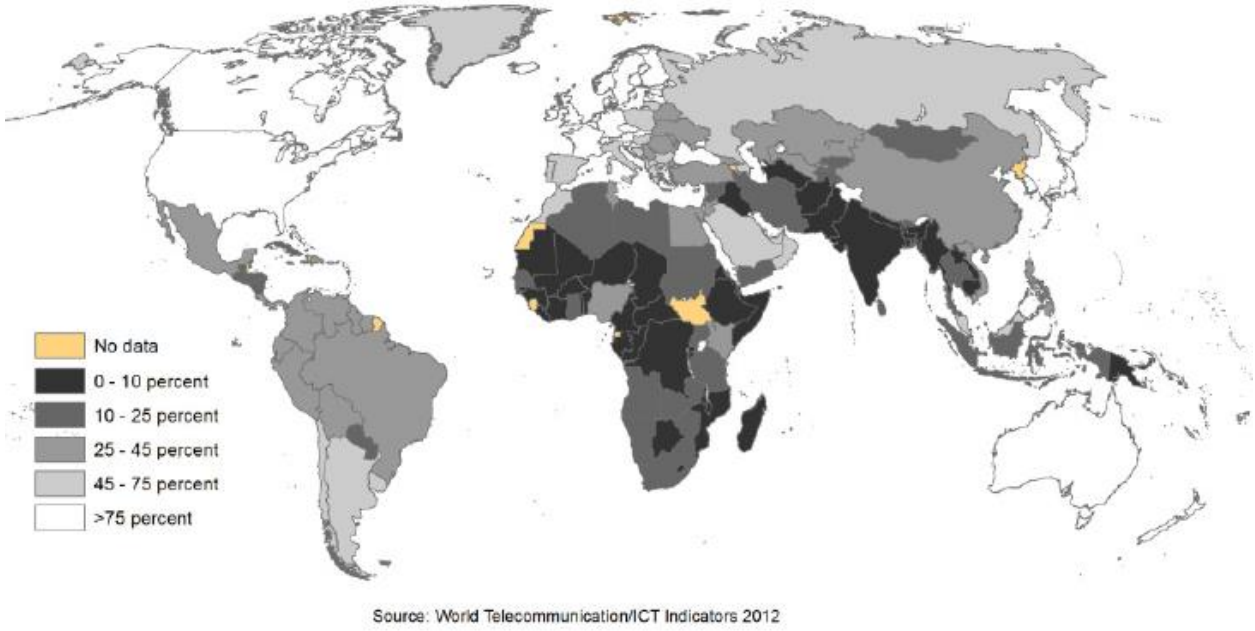


Figure 2: Percentage of Internet users (2011)
UNODC (2013), 'Comprehensive Study on Cybercrime', Vienna, February 2013.

While the digital world brings enormous benefits, it is also vulnerable. The promise of today's interconnected world is immeasurable. However, the benefits that stem from this promise, face real threats. These threats can have different origins - including criminal, politically motivated, terrorist or state-sponsored attacks as well as natural disasters and unintentional mistakes.[6] We have to be aware of the increasing amount of opportunities to commit crime facilitated, enabled or amplified by the Internet. For many people, being online is no longer the exception but the norm, often without the individual being aware. This creates a broader attack surface and multiple areas of peoples' lives for criminals to

[5] **European Commission** (2013), Joint Communication to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels: COM (2013) 01 final, 07 February 2013. [http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52013JC0001]

[6] **European Union** (2014), Cyber Security Strategy and Programs Handbook, Volume 1 Strategic Information and Regulations, p. 113.

exploit. Across the EU, more than one in ten Internet users has already become victim of online fraud[7].

Cybercrime is increasing in scale and impact, while there is a lack of reliable figures. Trends suggest considerable increases in scope, sophistication number and types of attacks, number of victims and economic damage. Cybersecurity incidents - intentional or accidental - are increasing at an alarming pace and could disrupt the supply of essential services we take for granted such as water, healthcare, electricity of mobile services etc. While the 'real' extent and economic impact of cybercrime is hard to quantify, scientists and officials agree that cybercrime is a huge and still growing problem. The impact of cybercrime is far-reaching. Nothing and no one is safe from cybercrime.

More than a million *people* worldwide are daily victims of cybercrime. Bank and credit card information can be stolen through emails that appear to come from the bank, sometimes online stores turn out not to exist at all and smartphones can be hacked. It can cost you a lot of money when cybercriminals apply for a loan or benefit in your name, but the personal impact is even bigger. Identity fraud can sometimes continue for years, which leads you into long legal procedures to prove you're a victim of identity fraud. Furthermore, the social media is a target: around 600.000 Facebook accounts have been harassed.

Cybercrime costs the *Government* and business world a lot of time and energy they would rather spend on other things. As technology increases between Governments that are caught up in international business, criminals have realized that this is an efficient method of making money. Cybercrime has been increasing since corporations have begun to use computers in the course of doing business. Cyberattacks on critical infrastructure can have severe consequences for business, government and society: Malicious software, malware, or botnets used for large-scale attacks on information and communications structures, can disrupt the delivery of vital goods or services. This type of attack can also maintain other viral infrastructures, such as transport or energy networks.

> ***"The world isn't run by weapons anymore, or energy, or money. It's run by ones and zeros – little bits of date – it's all electrons… There's a war out there, a world war. It's not about who has the most bullets. It's about who controls the information – what we see and hear, how we work, what we think. It's all about information."***
>
> Lines from the character 'Cosmos', in the movie Sneakers, MCA/Universal Pictures, 1992.

Computer crime is, after theft, the biggest criminal threat to *companies*. However companies still take this form of crime not seriously. One of the main consequences of cybercrime for a company is loss of income. This loss may be caused by an outside

[7] **European Commission** (2013), Joint Communication to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels: COM (2013) 01 final, 07 February 2013. [http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52013JC0001]

person who acquires sensitive financial information, using it to extract funds from an organization. Another major consequence of cybercrime is the time that is wasted when Information Technology personnel must dedicate a maximum part of their day handling such incidents. Rather than working on productive and creative measures for an organization, many Information Technology staff members spend a great percentage of their time handling security breaches and other problems related to cybercrime. Furthermore, in situations where customer records are compromised by a security contravene associated with cybercrime, a company's reputation can take a major blow. Customers whose credit cards or other monetary data gets grabbed, by hackers or other infiltrators, lose confidence in an organization and often take their business elsewhere. Finally, due to the safety measures that many companies must implement to neutralize cybercrime, there often is a pessimistic effect on employees' efficiency. This is because, due to many security reasons, employees must enter more passwords and execute other time-consuming acts in order to do their jobs. Every second wasted executing these acts is a second not spent working in an effective manner.

The cybercriminal economy as a whole is not precisely known, nevertheless the losses are thought to represent billions of euros per year. The scale of the problem is itself a threat to law enforcement response capability – with more than 150.000 viruses and other types of malicious codes in circulation and a million people that become victims of cybercrime every day. The world's attention on the fight and prevention of cybercrime has risen after annual figures shown almost 113 billion dollar worth of costs and has hit one million victims every day.[8] It is therefore compulsory that people, and especially children, should become more aware of the possible threat they face when life has become digitalized in every aspect.

For cyberspace to remain open and free, the same norms, principles and values that the EU upholds offline, should also apply online. Cyberspace should be protected from incidents, malicious activities and misuse. Governments have a significant role in ensuring a free and safe cyberspace. However, the private sector owns and operates significant parts of cyberspace, and so any initiative aiming to be successful in this area has to recognize its leading role.

Before we can focus on the prevention of cybercrime and how to combat this form of crime, we will explain cybercrime as a phenomenon. First we take a look of what we understand under 'cybercrime' and discuss some definitions on cybercrime. Furthermore we look at the different characteristics and motives of cybercrime and compare it with traditional crimes. Also we will dwell on cybercriminals. To end this chapter, we will give some information about the statistics on cybercrime.

Because cybercrime is such a large phenomenon, we will dwell a whole chapter on the classifications and common forms of cybercrime.

In the toolbox 'Cybercrime', we will focus on the legislative measures and policy of the EU and his Member States, the awareness and prevention projects and good practices.

[8] 2013 Norton Report, Dangerous liaisons. [https://www.symantec.com/content/en/us/about/presskits/b-norton-report-2013-infographic.en-us.pdf]

2. What is Cybercrime?

2.1 Definition

A primary problem for the analysis of cybercrime is the current absence of a consistent definition.[9] Cybercrime is a container-concept that holds many different crimes, performed in almost complete concealment by anonymous and creative offenders, in different contexts and in a continuous digitalizing era. The definition of cybercrime is extremely wide and can be interpreted in many different forms. The definitions of cybercrime have evolved experientially.[10] Cybercrime is a term that most people will still define as hacking or a virus. As of today, cybercrime has grown than just the latter: cybercrime is a pervasive threat for today's Internet dependent society. The definitions of cybercrime differ depending on the perception of both observer/protector and victim, and are partly a function of computer-related crimes geographic evolution.

'Definitions' of cybercrime mostly depend upon the purpose of using the term 'cybercrime'.[11] Therefore, cybercrime lacks a universal and consensual definition due to a missing definition of the term in national and international law.[12]

In our quest of finding a global definition of cybercrime, we came across many different interpretations. The most understandable interpretation states cybercrime to be *a crime that is enabled by, or that targets computers*. The understanding of the whole cybercrime-picture forces us into a more detailed research.

Firstly, the *10th United Nations Congress on the Prevention of Crime and the Treatment of Offenders* (2000) developed two definitions within a related workshop. They individually defined 'computer related crimes' and 'cybercrime', narrowing the latter to the 'involvement of a computer network' and mentioning 'specific crimes' in the definition.

A more common version by *Carter* states *'any activity in which computers or a network are a tool, target or a place of criminal activity*.'[13] This version would indirectly mean that a man would commit cybercrime if he hits a person to the head with a keyboard. Furthermore Kruse and Heiser mentioned that '*the computer may have been used in the commission of a crime, or it may be the target'.*[14] Following a definition provided by Casey, cybercrime refers to any crime that involves a computer and a network, where a

[9] **YAR, M. (2005),** *'The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory.'* European Journal of Criminology 2005; 2 ; 407

[10] **Gordon, S., Richard, F. (2006),** *'On the definition and classification of Cybercrime,' Journal in Computer Virology 2006, Volume 2, Issue 1, pp. 13-20.*

[11] *United Nations Office on Drugs and Crime* (2013), *'Comprehensive Study on Cybercrime',* Vienna, February 2013. [https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf]

[12] **Proteus Manual** (2015) *'Prevention, Information and support to victims of online identity theft*', 2015, Lisboa, APAV.

[13] **Carter, D.L.,** *'Computer Crime Categories: How Techno-Criminals Operate'.* FBI Law Enforcement Bulletin, 1995, Volume: 64, Issue 7, pp 21-27 [https://www.ncjrs.gov/pdffiles1/Digitization/156176NCJRS.pdf]

[14] **Warren, G. Kruse, Jay, G. Heiser**, (2001) *'Computer Forensics: Incident Response Essentials'.* Boston, MA: Addison-Wesley.

computer may or may not have played an instrumental part in the committing of the crime.[15]

In reading these definitions, it becomes clear that the term cybercrime actually refers to computer-related crime. However, some people consider computer crime to be a subdivision of cybercrime that warrants its own definition and understanding. Dr. Debarati Halder and Dr. K. Jaishankar define cybercrimes as: *"offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)"*.[16]

A working definition is offered by Thomas and Loader (2000), who conceptualized cybercrime as *'computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks'*.[17] The specificity of cybercrime is therefore held to reside in the newly instituted interactional environment in which it takes place, namely the 'virtual space' ('cyberspace') generated by the interconnection of computers into a worldwide network of information exchange, primarily the Internet. Within this definition it is possible to further classify cybercrime along a number of different lines. We can distinguish 'computer-assisted crimes' and 'computer-focused crimes.'[18]

With a much broader approach and the specificity of the area in which cybercrimes take place, in particular the Internet, the European commission defined a more comprehensible version: *'Cybercrimes can be defined as any crimes which are committed via the Internet'.* The EU-commission's definition on cybercrime can make its way to the Member States and harmonize the understanding of the phenomena 'cybercrime' into a uniform national law. With a global definition, law enforcements are able to form a global jurisprudence, which is obligatory in the fight against cybercrime. However, considering most definitions on the topic, the EU-commission's definition is too concise due to the fact it incorporates the Internet to be a necessary factor to commit cybercrime. Nonetheless, the EU-commission's definition prevents an overly complicated and expansive working definition by thriving to a clear understanding by mentioning all crimes using the internet (which automatically implements usage of a computer or a software-based device).

In our quest of searching a good definition on cybercrime, we noticed the discussion that keeps coming back: 'does cybercrime denote the emergence of a 'new' form of crime and/or criminality?

[15] **Moore, R.,** (2015) **'***Cybercrime: investigating high-technology computer crime',* Routledge, p. 4.
[16] **Halder, D., & Jaishankar, K.**, (2011) *'Cybercrime and the Victimization of Women: Laws, Rights, and Regulations,'* Hershey, PA, USA.
[17] **Yar, M.,** (2006) *'Cybercrime and society',* Sage Publications Inc., London, p. 9.
[18] **Castells, M.** (2002), *'The internet galaxy: Reflections on the internet, business and society',* Oxford: Oxford University Press.

2.2 *Cybercrime: a new form of crime?*

Some people suggest that the advent of 'virtual crimes' marks the establishment of a new and distinctive social environment with its own ontological and epistemological structures, interactional forms, roles and rules, limits and possibilities. Other people see 'cybercrime' as a case of familiar criminal activities pursued with some new tools and techniques. Grabosky[19] suggested that cybercrime was simply a case of 'old wine in new bottles'. If this was the case, cybercrime could be fruitfully explained, analysed and understood in terms of established criminological classifications.[20]

Like traditional crime, cybercrime has different facets and occurs in a wide variety of scenarios and environments. Apparently, there is no distinction between cyber and conventional crime. However, on a deep introspection we may say that there exists a fine line of demarcation between the conventional and cybercrime, which is appreciable. The demarcation lies in the involvement of the medium in cases of cybercrime. The sine qua non for cybercrime is that there should be an involvement, at any stage, of the virtual cyber medium.

On the other hand, combating cybercrime requires a different approach from the one traditionally taken in respect of most crimes, because of severity of cybercrime and the extent to which it has a greater potential for harm than traditional crime. In contrast to the off-line world where criminals need to be physically present at the crime scene and can commit one offence at a time, criminals in cyberspace do not need to be close to the crime scene, they do not have to travel to the target country, and can attack a large number of victims globally with a minimum of effort and risk through hiding their identity.[21] The information capabilities of the Internet change the nature of crime, as they provide cyber criminals with simple, cost effective and repeatable means of conducting rapid global-scale attacks, while remaining anonymous and/or unreachable for law enforcement.[22] Cybercrime opens new doors to criminals where they have the power to defraud entire institutions in ways that would not have been possible traditionally. Housing billions of gigabytes of sensitive information and valuable date, the Internet is very appealing to criminal organizations, who can act anonymously (and so remain more unpunished). Finally, one of the differences between cybercrime and traditional crime is the evidence of the offenses: traditional criminals usually leave traces of a crime, through fingerprints, physical evidences,... On the other hand, cybercriminals rely on the Internet via which they commit their crimes, and leaves little evidence.

This part leads us to an additional word of explanation on the unique characteristics of cybercrime.

[19] **Grabosky, P.N**., *(2001), 'Virtual criminality: Old wine in new bottles?'.* Social and Legal Studies (10:2), 243-249:243
[20] **YAR**, **M. (2005),** '*The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory,' European Journal of Criminology 2005; 2 ; 407*
[21] **Europol** (2014), The Internet Organised Threat Assessment (iOCTA) 2014, The Hague, 2014.
[22] **Clough, J. (2010),** '*Principles of cybercrime*', Cambridge University Press.

2.3 *The unique characteristics of cybercrime*

✓ *Internationality*

The virtual world does not feature any frontiers and the different legal systems apply according to the territorial competences of law enforcement agencies. The *borderless nature of cybercrime* makes it possible to commit crimes against governments, business and citizens in the EU from almost anywhere around the world. Compared to other, more traditional crime types, criminals who use the Internet for hacking computers, stealing data and emptying bank accounts are not hindered by logical constraints, such as travelling and transporting the looted goods. There is hardly any identifiable link between the criminals and the crime scenes.[23]

These crimes transcend jurisdictional boundaries, often involving multiple victims from different communities, states and countries. The geographic location of a victim is not a primary concern for perpetrators who target victims over the Internet. For example, pedophiles often travel hundreds of miles to different states and countries to engage in sexual acts with children they met over the Internet. Many of these cases involve local, state, federal, and international law enforcement entities in multiple jurisdictions.

Therefore it is important to note that access to the Internet is expected to increase significantly in the coming years.

✓ *The scalability*

The scalability results from the ease to replicate crimes on a massive scale due to the standardization of software and the possibility to reach millions of computers without any logistical constraints.[24]

✓ *Anonymity and pseudonimity*

Perpetrators feel very safe and can easily hide their real identity on the Internet. Physical contact between victim and perpetrator is not necessary to become a victim or for a crime to be committed.

The Internet also provides a source for repeated, long-term victimization of a victim that can last for years, often without the victim's knowledge. For example, once a victim's picture is displayed on the Internet, it can remain there forever. Images can stay on the Internet indefinitely without damage to the quality of the image.

Individuals who did not realize that they were actually victimized are one of the reasons that there is an under-reporting for this sort of crimes. Other reasons can be:

- Not perceiving that what had taken place was a crime, or did not think it is worth reporting
- Not knowing where to report the crime
- Thinking that the police cannot do anything

McGuire, M., Dowling, S., *"Cybercrime: a review of the evidence. Research Report 75. Summary of key findings and implications."* Home Office, October 2013.

[23] **EC3, Europol**, First Year Report, p. 26
[24] **EC3, Europol**, First Year Report, p. 26

Many victims of Internet crimes do not disclose their victimization or even realize that they have been victims of a crime. For example, whereas children who experience physical or sexual abuse may disclose the abuse to a friend, teacher, parent, many victims of Internet crimes remain anonymous until pictures or images are discovered by law enforcement during an investigation.

The presumed anonymity of Internet activities often provides a false sense of security and secrecy for both the perpetrator and the victim. There are different technologies and forums that criminal actors can take advantage of in order to anonymise themselves and facilitate criminal activity. The ease to hide comes from the use of hacked computers, stolen identities and from techniques to re-route traffic through numerous nodes while obfuscating the origin. Operating from or via countries in which the regime has limited competence or ambition to prevent and fight cybercrime is an effective way to hide. For example, the anonymity of the Internet is frequently misused for child sexual exploitation. Child abuse material is offered and exchanged via anonymous networks, but also through peer-to-peer networks and peer groups on social media.[25]

> It is true that individuals can use false identities to go online, but one of the more stunning and frequently overlooked features about networked technologies is that every move online can be tracked and the 'mouse droppings', leave a data trail behind. So we can say that this issue is not so much one of anonymity, but one of the investigators having the human and technological resources available to follow the digital trail.
>
> **Wall, D.S.,** (2008), *"Cybercrime, Media and Insecurity: the shaping of public perceptions of cybercrime",* International review of Law, Computers and technology, vol. 22.

Darknets offering a high degree of anonymity are increasingly hosting hidden services devoted to traditional types of crimes, like for example drug trade, selling stolen goods, weapons, compromised credit card details, forged documents, fake ID's and trafficking of human beings.[26]

- ✓ *Asymmetry*

Authors of internet crimes are mostly ahead of police and justice authorities by developing new modi operandi. Criminal entrepreneurs can operate relatively efficiently due to the innovation enabled by the Internet. This results in a strife between criminal developers and those who try to foil them. It is really hard protecting yourself against unknown vulnerabilities, which makes it hard to stay ahead of criminal actors. The law enforcement already had some limited success in penetrating technologies to identify and capture criminals, and/or has taken advantage of sloppy use of these technologies to find those who hide behind them.

However, the speed and capacity of cybercriminals to develop and guard what, how and where they do it in cyberspace should not be underestimated. Law enforcement experiences have already shown that cybercriminals are efficient in learning from police

[25] **EC3 Europol,** *First Year Report,* p. 26.
[26] **EC3 Europol,** The Internet Organised Crime Threat Assessment (iOcta) 2014, p.12.

operations and responding to these with improved software security and encryption, and mechanisms for conducting criminal activity.[27]

- ✓ *Low marginal cost of online activity*

The effort and resources required to commit a cybercrime are substantially less than for traditional crimes. In general, effort refers to the combination of mental energy and time necessary to implement the attack. If the demand for attack resources as greater, the target becomes less attractive. In contrast, like with cybercrimes, computers provide most of the effort and resources, by virtue of their tremendous speed of processing, rendering cyber targets attractive.[28]

- ✓ *Nature of criminal cooperation.* [29]

The nature of criminal cooperation via the internet has resulted in networks of criminals that amplify each other's criminal services. This applies in the area of cybercrime, but also other types of crime. A complete underground economy has developed, where all kinds of criminal products and services are traded such as drugs, weapons, stolen payment credentials, child abuse etc. As mentioned earlier, this is facilitated by anonymous payment systems, such as virtual currencies and hidden market places where the criminal services are offered. Especially for cybercrime this underground economy has a multiplying effect, because any kind of cybercrime can be procured by anyone even without any technical skills or instruments: password cracking, hacking, malware testing and many more.

1	Low marginal cost of online activity due to global reach	6	concrete regulatory measure
2	Lower risk of getting caught	7	Lack of reporting and standards
3	Catching by law and enforcement agency is less effective and more expensive	8	Difficulty in identification
4	New opportunity to do legal acts using technical architecture	9	Limited media coverage
5	Official investigation and criminal prosecution is rare; not very effective sentences	10	cyber crimes are done collectively and not by individual persons

Figure 3: Govil, J. (2007), 'Ramifications of Cyber Crime and Suggestive Preventive Measures'. IEEE, 43(4), 610-615

Govil [30] mentioned the following characteristics shown in Figure 3.

[27] **City of London (2015)**, '*The implications of economic cybercrime for policing,'* Research report City of London corporation, October, 2015.
[28] **Gosh, S., Turrini, E. (2011),** '*Cybercrimes: A Multidisciplinary Analysis', Springer, p.373*
[29] **EC3 Europol,** *First Year Report,* p. 27.

These characteristics make traditional law enforcement strategies, particular strategies based on identifying and apprehending perpetrators after they commit online crime, less effective and more expensive.

However, other characteristics of cyberspace provide at the same time new opportunities to control illegal acts. Unlike the physical world, in cyberspace certain readily identifiable third parties – such as Internet service providers, telecommunication providers, and victims themselves – have exclusive or shared technical control over the infrastructure through which most illegal online behavior is carried out. The characteristics provide new opportunities for innovative policy approaches to controlling undesirable behavior; including the use of technical architecture as a regulatory mechanism, the use of novel authorization and surveillance regimes to prevent or deter undesirable activity, and the use of data and activity logging to enhance persistence and recoverability of evidence, amongst others.

2.4 Motives for cybercrime

There are many reasons why people commit a cybercrime: recognition, quick money, to fight a cause (one thinks) he believes in, low marginal costs of online activity due to global reach, official investigation and criminal prosecution is rare, no concrete regulatory measure, lack of reporting and standards, difficulty in identification, limited media coverage and corporate cybercrimes are done collectively and not by individual persons.

- ✓ *Money*

Anyone who makes a financial profit from the crime - whether it is a bank employee who uses his computer access to divert funds from someone else's account to his own, an outsider who hacks into a company database to steal identities that he can sell to other criminals, or a professional "hacker for hire" who is paid by one company to steal the trade secrets of another. Almost anyone can be motivated by money – they are young, old, male, female, those from all socio-economic classes. Because the white collar criminal tends to be very different from the seasoned scam artist or the professional "digital hit man, it is better to break this category down further.

- ✓ *Emotion*

The most destructive cybercriminals often act out of emotion, whether anger/rage, revenge, "love" or despair. This category includes spurned lovers or spouses/ex-spouses (cyber-stalking, terroristic threats, email harassment, unauthorized access), disgruntled or fired employees (defacement of company web sites, denial of service attacks, stealing or destroying company data, exposure of confidential company information), dissatisfied customers, feuding neighbors, students angry about a bad grade, and so forth. This can even be someone who gets mad over a heated discussion on a web board or in a social networking group.

- ✓ *Sexual impulses*

[30] **Govil, J.** (2007). '*Ramifications of Cyber Crime and Suggestive Preventive Measures'. IEEE , 43*(4), 610-615.

Although this is related to emotion, this category is slightly different and includes some of the most violent of cybercriminals: serial rapists, sexual sadists (even serial killers) and pedophiles. Child pornographers can fit into this category or they may be merely exploiting the sexual impulses of others for profit, in which case they belong in the "money" category.

- ✓ *Politics or religion*

This category is also closely related to the "emotions" category, since people get very emotional about their political and religious beliefs and are willing to commit heinous crimes in the name of those beliefs. This is the most common motivator for cyberterrorists, but motivates many lesser crimes, as well.

- ✓ *Just for fun*

This motivation applies to teenagers (or even younger) and others who may hack into networks, share copyrighted music/movies, deface websites and so forth - not out of malicious intent or any financial benefit, but simply "just because they can". They may do it to prove their skills to their peers or to themselves, they may simply be curious, or they just may see it as a game. Although they do not intentionally do harm, their actions can cost companies money, cause individuals grief and tie up valuable law enforcement resources.

2.5 Cybercriminals

There are a range of motivations behind cybercrimes. The focus is largely around financial gain or can be a form of protest and/or criminal damage. For child exploitation, the motive is not always for profit. More unorthodox motivations for cybercrimes include intellectual curiosity or challenge, general maliciousness, revenge, gaining some respect or power in online communities, or even simply boredom.[31]

Cybercrime offenders no longer require complex skills or techniques, due to the advent and ready availability of malware toolkits. While some perpetrators may have completed advanced education, (especially in the computer science field) many known perpetrators do not have any specialized education. More than 80% of cybercrime acts are estimated to originate in some form of organized activity, with cybercrime black markets established on a cycle of malware creation, computer infection, botnet management, data sale, and 'cashing out' of financial information. Cybercrime often requires a high degree of organization to implement and may lend itself to small criminal groups, ad hoc networks or organized crime on a larger scale. The typology of perpetrators and active criminal groups mostly reflect patterns in the conventional world.

The demographic nature of perpetrators mirrors conventional crime in that young males are the majority, although the age profile is increasingly showing older individuals, particularly concerning child pornography offences.

[31] **Kirwan, G. and Power, A.** (2012) '*The Psychology of Cyber Crime,'* Hershey: IGI Global.

Different studies suggest that cybercrime perpetrators are most commonly aged between 18 and 30 years old. Other studies can differ somewhat, and indicate older perpetrator age groups. Nevertheless cybercrime perpetrators overall may be younger than criminal offenders in general. Cybercrime perpetrators are also mainly male.[32]

The profile of persons engaged in the computer-related production, distribution or possession of child pornography is different to that of cybercrime offenders in general. They are male and ranged in age from 15 to 73 years, with an average age of 41 years. Online offenders are more likely to be unemployed and marginally younger than offline offenders, but links nonetheless may exist. A part of online child pornography offenders, may also be involved in 'offline' abuse of children.

2.5.1 Categories

In the Journal of Alternative Perspectives in the Social Sciences, there have been made 4 categories of cybercriminals.[33]

- *Children and adolescents between the 6 – 18 years:* The simple reason for this type of delinquent behavior pattern in children is seen mostly due to the inquisitiveness to learn, know and explore things. Other reasons may be to prove themselves, to be outstanding amongst other children in their group.

  Furthermore the reasons may be psychological. In most literature you can find in this category the 'script-kiddies'.

- *Organised hackers:* These kinds of hackers are mostly organised to reach certain objectives together. The reason may be to accomplish political bias, fundamentalism, etc.
- *Professional hackers / crackers:* The work of professional hackers or crackers, is motivated by the color of money. These kinds of hackers are mostly hired to hack the site of rivals to receive credible, reliable and valuable information.
- *Discontented employees:* Those people have been either sacked by their employer or are dissatisfied with their employer. They normally hack the system of their employer to get some revenge.

A **script kiddie** or **skiddie** is an unskilled individual who uses scripts or programs developed by others to attack computer systems and networks and deface websites. It is generally assumed that script kiddies are juveniles who lack the ability to write sophisticated programs or exploits on their own and that their objective is to try to impress their friends or gain credit in computer-enthusiast communities. However, the term does not relate to the actual age of the participant, the term is generally considered to be pejorative.

[32] **United Nations Office on Drugs and Crime** (2013), *'Comprehensive Study on Cybercrime'*, Vienna, February 2013, [https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf]
[33] **Kamini, D**. (2011) *'Cybercrime in the Society: Problems and Preventions'*. Journal of Alternative Perspectives in the Social Sciences (2011) Vol 3, No 1, 240-259

Marcus Rogers identified 8 types of cyber-criminals, distinguished by their skill levels and motivations.

<table>
<tr>
<td>Novice
Limited computer and programming skills.
Rely on toolkits to conduct their attacks.
Can cause extensive damage to systems. since they don't understand how the attack works.
Looking for media attention.</td>
<td>Coders
Acts as mentors to the newbies. Write the scripts and automated tools that others use.
Motivated by a sense of power and prestige.
Dangerous – have hidden agendas, us Trojan horses.</td>
</tr>
<tr>
<td>Cyber-punks
Capable of writing their own software.
Have an understanding of the systems they are attacking.
Many are engaged in credit card number theft and telecommunications fraud.
Have a tendency to brag about their exploits.</td>
<td>Old guard hackers
Appear to have no criminal intent.
Alarming disrespect for personal property.
Appear to be interested in the intellectual endeavor.</td>
</tr>
<tr>
<td rowspan="2">Internals
Disgruntled employees or ex-employees
May be involved in technology-related jobs.
Aided by privileges they have or had been assigned as part of their job function.
Pose largest security problem.
Petty thieves
Include employees, contractors, consultants.
Computer literate.
Opportunistic: take advantage of poor internal security.
Motivated by greed or necessity to pay off other habits, such as drugs or gambling.</td>
<td>Professional criminals
Specialize in corporate espionage.
Guns for hire.
Highly motivated, highly trained, have access to state-of-the-art equipment.</td>
</tr>
<tr>
<td>Information warriors/cyber-terrorists
Increase in activity since the fall of many Eastern Bloc intelligence agencies.
Well-funded.
Mix political rhetoric with criminal activity. Political activist.
Possible emerging category.
Engage in hacktivism.</td>
</tr>
</table>

Figure 4: BEDNARZ., A. (2004) , 'Profiling cybercriminals: A promising but immature science in Networkworld'. [http://www.networkworld.com/article/2327820/lan-wan/profiling-cybercriminals--a-promising-but-immature-science.html]

Literature also mentions the following backgrounds that perpetrors can have:

- *Scammers, hacker groups: usually* work anonymously and create tools for hacking. They often hack computers for no criminal reason and are sometimes even hired by companies that want to test their security.
- *Phishers:* want personal information.
- *Political/religious/commercial groups.*
- *Insiders:* they may only be 20% of the threat, but produce 80% of the damage. These attackers are considered to be the highest risk. To make matters worse, they often reside within an organization.
- *Advanced Persistent Threat (APT) Agents:* responsible for highly targeted attacks carried out by extremely organized state-sponsored groups. Their technical skills are deep and they have access to vast computing resources.

2.6 Statistics on cybercrime

More than one million people are affected by cybercrime every day. Cybercrime costs the global economy more than €368 billion a year. Every day more than 150,000 viruses and other malicious codes circulate. Our digitalized societies are increasingly relying on electronic networks and information systems, however this has also created more opportunities for online fraud and forgery. Anyone, from individuals to companies and public authorities, can fall victim to schemes such as identity theft, fake bank websites or industrial espionage.

In general, cybercrime is increasing in scale and impact. While there is a lack of reliable figures, trends suggest considerable increases in scope, sophistication, number and types of attacks, number of victims and economic damage.

For many reasons, there are no reliable statistics on cybercrime. Cybercrime is a vast area and covers innumerable crimes and no common statistics system exists. Because of the difficulties arising when trying to define and identify cybercrime (see above), cross-national comparative statistics on cybercrime are much rarer than for other crime types.

The following indicative figures can be given to illustrate the scope of the problem:

- As an indicative example of the increased frequency of one particularly serious form of crime, the publication of child sexual abuse material, the UK-based Internet Watch Foundation has estimated that the number of sites with this type of illegal material has increased with 1 500 percent in the period 1997-2005.
- It has been estimated that 750 000 computers are infected through Botnets every year in Germany.
- The UK Financial Service Authority has estimated that the number of bank frauds through Phasing has increased with 8 000 percent in the last two years.

European Commission, The commission communication "towards a general policy on the fight against cyber crime"http://europa.eu/rapid/press-release_MEMO-07-199_en.htm#fn2 , 22 may 2007.

The increasing ubiquity of global connectivity presents a serious risk that rates of cybercrime will increase and are increasing. A range of cybercrime acts are increasing, such as computer-related

fraud and identity theft, computer-related production, distribution or possession of child pornography, phishing attempts and illegal access to computer systems, including hacking.

Criminological theories and socio-economic approaches offer several possible explanations for the growth of cybercrime. The increasing use of the Internet and ICT create new opportunities for offenders and facilitates the growth of crime. Another underlying development that contributes to driving cybercrime levels is the emergence of global connectivity in the context of world economic and demographic transformations. Socio-economic factors may play an important role in increases in cybercrime. Pressure on private sector enterprises to cut spending and to reduce staffing levels can lead to reductions in security and to opportunities for exploitation of ICT weaknesses.

Police-recorded crime statistics do not represent a sound basis for cross-national comparisons. About 75% of the countries view their systems of police statistics as insufficient for recording cybercrime. Police-recorded cybercrime rates are associated with levels of country development and specialized police capacity, more than underlying crime rates.

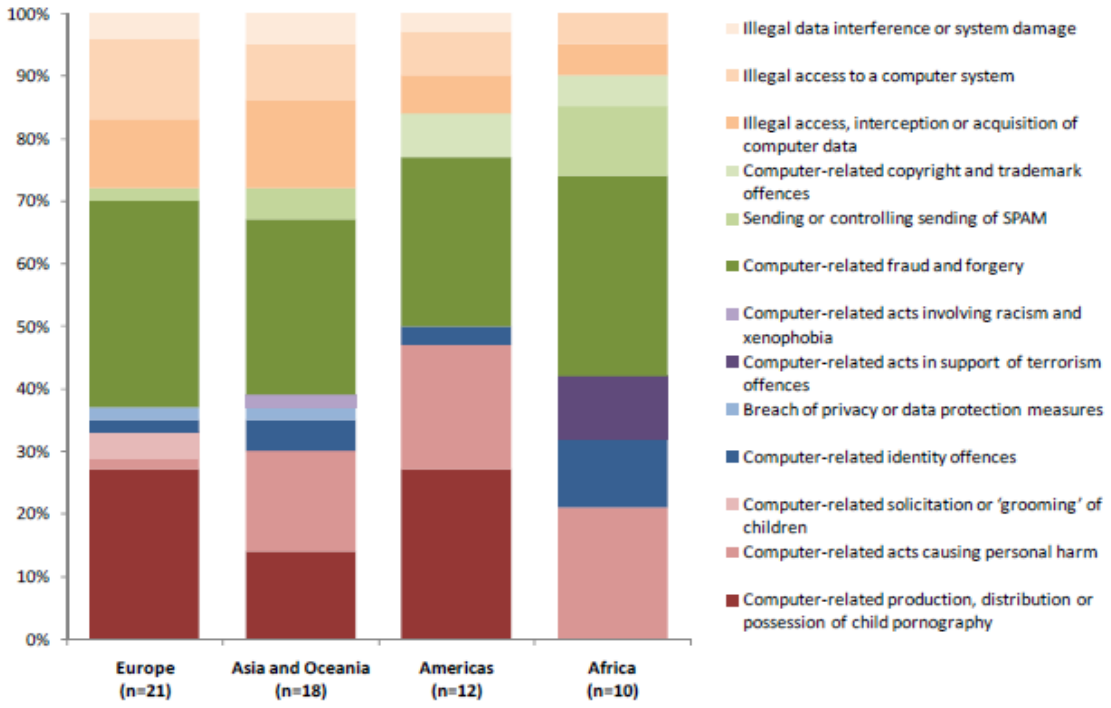


Figure 5: Most common cybercrime acts encountered by national police
Source: UNODC

There is evidence suggesting that cybercrime incidents are very rarely reported. This is especially the case when the criminal activity is directed towards companies: any report might be perceived as a security problem and lead to competition disadvantages.

Police data is under-reported for various reasons: fear of negative publicity, lack of incentive, perception that the police response will be ineffectual, no prospect of restitutionary damages and victims not realizing that they have been victimized.

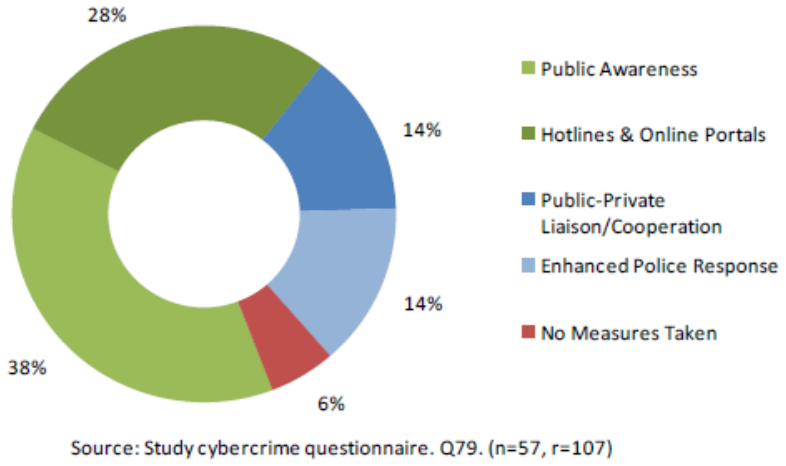


Figure 6: Measures taken to increase reporting cybercrime to police
Source: UNODC

Many countries have strategies and approaches to increase the reporting of cybercrime, as shown in figure 6.

Victimization surveys represent a more sound basis for comparison. They demonstrate that individual cybercrime victimization is significantly higher than for 'conventional' crime forms. Victimization rates for online credit card fraud, identity theft, responding to a phishing attempt, and experiencing unauthorized access to an email account, vary between 1 and 17% of the online population for 21 countries across the world, compared with typical burglary, robbery and car theft rates of fewer than 5 per cent for these same countries. Private sector enterprises in Europe report similar victimization rates – between 2 and 16 per cent – for acts such as data breach due to intrusion or phishing. Criminal tools of choice for these crimes, such as botnets[34], have global reach. More than one million unique IP addresses globally functioned as botnet command and control servers in 2011. Internet content also represented a significant concern for Governments. Material targeted for removal includes child pornography and hate speech, but also content related to defamation and government criticism, raising human rights law concerns in some cases.[35]

Finally, surveys have been done about the concerns of Internet users about cyber security. According to a Eurobarometer survey (2015) Europeans are highly concerned about cyber security. Under half of the EU citizens feel well informed about the risks of cybercrime, 89% of all internet users avoid disclosing personal information online, 85% agree that the risk of becoming a victim of cybercrime is increasing, 73% agree that they are concerned that their online personal information is not kept secure by websites and 67% agree that they are concerned that this information is not kept secure by public authorities. About 68% of the Internet users in the EU are concerned about experiencing identity theft and about discovering malicious software on their device. More than half are concerned about being the victim of bank card or online banking fraud, having their social media or email account hacked, scam emails or phone calls, online fraud and accidentally discovering child pornography online, not being able to access online services because of cyber-attacks, cyber extortion and accidentally encountering material which promotes racial hated or religious extremism.[36] One outcome of the cybercrime

[34] Botnet refers to a collection of compromised machines running programs under a common command. The criminal takes control over the whole collection of machines, without the knowledge of the owner/user of the individual computers, and use them to, for example, attack a specific information system.

[35] **United Nations Office on Drugs and Crime** (2013), Comprehensive Study on Cybercrime, Vienna, February 2013. [https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf]

[36] **European Commission** (2015), *Special Eurobarometer 423 cybersecurity report,* February 2015. [http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf]

communication 'towards a general policy on the fight against cybercrime' may be that more information on crime is collected and that the statistics have to be improved.

3. Categorization of cybercrime

3.1 Classifications of cybercrime

As mentioned before, cybercrime is a container-concept that holds many different crimes, performed in almost complete concealment by anonymous and creative offenders, in different contexts and in a continuous digitalizing era. While the term cybercrime is not amenable to a single description, the question arises whether cybercrime objectives, features or modus operandi can be identified in general terms, rather than by reference to a list of individual cybercrime acts.

One example of this approach is found in the Council of Europe Cybercrime Convention[37], which uses broad criminalization headings, including *'offences against the confidentiality, integrity and availability of computer data and systems,' 'computer-related offences', 'content-related offences and copyright-related offences'.* Figure 7 proposes acts that may constitute cybercrime, organized in 3 broad categories. The purpose of this list is to introduce a tentative set of acts that may be included in the term 'cybercrime', with a view to establishing a basis. This list was not intended to be exhaustive.

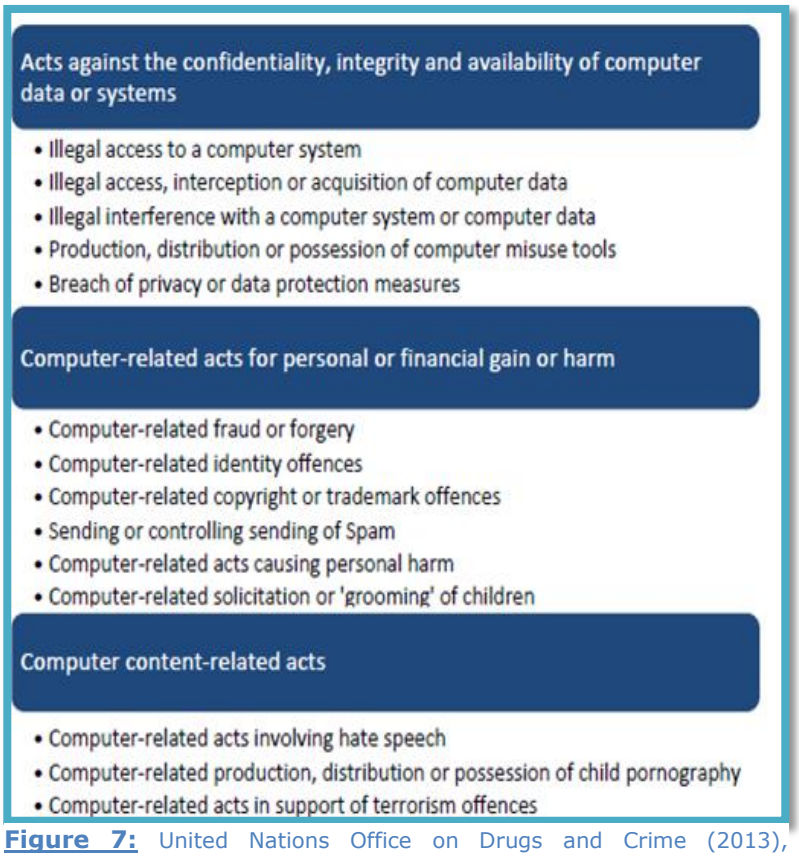


Figure 7: United Nations Office on Drugs and Crime (2013), Comprehensive Study on Cybercrime, Vienna, February 2013, retrieved from https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

The first category, *'offences against the confidentiality, integrity and availability of computer data and systems'*, have as object a computer system or computer data. Basic actions include unauthorized access, interception, acquisition or interference with a computer system or data. These acts may be committed using many different modus operandi. Illegal access to a computer system for example, may consist of the

[37] **Council of the European Union (2001),** Convention on Cybercrime, Budapest, 23 November 2001.

unauthorized use of a discovered password, or remote access using exploit software. The latter may also constitute interference with computer data and/or a computer system. Individual acts can thus show a degree of overlap across offence 'baskets'. This category also includes acts related to tools that can be used to carry out acts against computer systems or data. Finally this category includes criminal acts related to the (mis)handling of computer data in accordance with specified requirements.

The second category, *'computer-related acts for personal or financial gain or harm',* focuses on acts for which the use of a computer system is inherent to the modus operandi. The object of such acts differs. In the case of computer-related fraud, the object may be considered as the economic property targeted. In the case of computer-related copyright or trademark offences, the offence object may be considered as the protected intellectual property right. In the case of *'computer-related acts causing'* personal harm, such as the use of a computer system to harass, bully, threaten, stalk or to cause fear or intimidation of an individual, or 'grooming' of a child, the offence object may be regarded as the individual targeted. It is clear from these approaches that a number of general features could be used to describe cybercrime acts. One approach is to focus on *the material offence object* – that is, on the person, thing or value against which the offence is directed.[38] Another approach is to consider whether computer systems or *information system* form an integral part of the *modus operandi of the offence.*[39] Identifying possible cybercrime offence objects and modus operandi does not describe cybercrime acts in their entirety, but it can provide a number of useful general categories into which acts may be broadly classified.

Earlier, we mentioned the classification of the working definition (Thomas and Loader): The distinction of *'computer-assisted crimes'* - those crimes that pre-date the Internet but take on a new life in cyberspace, e.g. fraud, theft, money, laundering, sexual harassment, hate speech, pornography - and *'computer-focused crimes'* - those crimes that have emerged in tandem with the establishment of the Internet and could not exist apart from it, e.g. hacking, viral attacks, website defacement. This distinction may be socio-technically helpful, but has a limited criminological utility.

An alternative is to mobilize existing categories derived from criminal law into which their cyber-counterparts can be transposed. Wall (2001) subdivides cybercrime into four established legal categories:[40]

- *Cyber-trespass or hacking/cracking*: crossing boundaries into other people's property and/or causing damage, e.g. hacking, defacement, viruses
- *Cyber-deceptions and thefts*: stealing (money, property), e.g. credit card fraud, intellectual property violations (a.k.a. piracy)
- *Cyber-pornography*: activities that breach laws on obscenity and decency
- *Cyber-violence*: doing psychological harm to, or inciting physical harm against others, thereby breaching laws pertaining to the protection of the person, e.g. hate speech, stalking

[38] *Title 1 of the substantive criminal law chapter of the Council of Europe Cybercrime Convention, where the objects are computer data or computer systems.*
[39] *Title 2,3, 4 of the substantive criminal law chapter of the Council of Europe Cybercrime Convention.*
[40] **Wall, D**., **(2001),** *'Crime and the Internet: cybercrimes and cyberfears',* Routledge, London and New York.

This classification is helpful in relating cybercrime to existing conceptions of proscribed and harmful acts, however it does little in the way of isolating what might be qualitatively different or new about such offences and their commission when considered from a perspective that looks beyond a limited legalistic framework.

In literature, a simple classification can be found in three categories: crime against individuals, property and the government. Each category can use a variety of methods and the methods used vary from one criminal to another. Crimes against individuals can be in the form of cyber stalking, distributing pornography, grooming etc. Crimes against property are just like in the real world where criminals can steal and rob: in this case criminals can steal a person's bank details and siphon off money, misuse credit cards to make numerous purchases online, run scams to get naïve people to part with their earned money, use malicious software to gain access to an organization's website or disrupt the systems of the organization. Malicious software can damage software and hardware, just like vandals damage property in the offline world. At last we have the crimes against the government. Although this is not as common as the other two categories, crimes against a government are referred to as cyber terrorism. This category can cause panic amongst the civilian population. In this category, criminals hack government websites, military websites or circulate propaganda. Perpetrators can be terrorists, unfriendly governments or other nations.

Finally, on the website of the European Commission, it is mentioned that cybercrime can be classified in three broad definitions:

- *Crimes specific to the Internet:* such as attacks against information systems or phishing (e.g. fake bank websites to solicit passwords enabling access to victims' bank accounts)
- *Online fraud and forgery:* Large-scale fraud can be committed online through instruments such as identity theft, phishing, spam and malicious code
- *Illegal online content*: including child sexual abuse material, incitement to racial hatred, incitement to terrorist acts and glorification of violence, terrorism, racism and xenophobia.

3.2 Common forms of Cybercrime.[41]

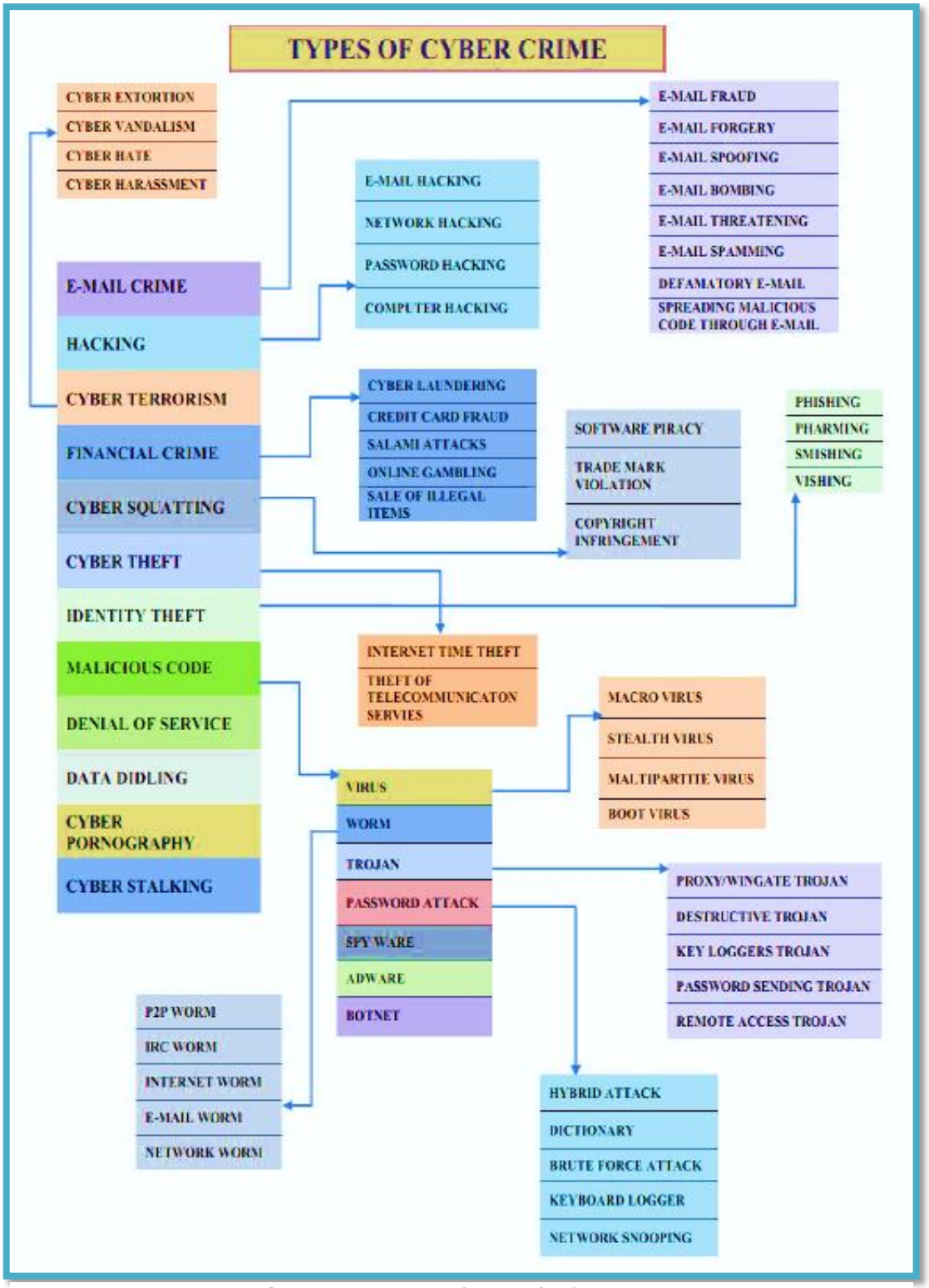


Figure 8: Common forms of cybercrime.
Source: AJEET SINGH POONIA, (2014), 'Cyber Crime: Challenges and its Classification International Journal of Emerging Trends & Technology'. Computer Science (IJETTCS) Volume 3, Issue 6.

[41] **AJEET SINGH POONIA,** (2014), *'Cyber Crime: Challenges and its Classification International Journal of Emerging Trends & Technology'* . Computer Science (IJETTCS) Volume 3, Issue 6.

3.2.1 Hacking

Hacking is a very vague concept. Even computer experts differ on the exact meaning of the word. Hacking is unauthorized intrusion into a computer system. Malicious intent is usually involved, with this intrusion. But also inadvertently connected to preserve voluntarily, and that connection is considered as hacking. Even the hacking of a computer system that is hardly protected, is punishable.

In the assessment of hacking, a distinction can be made between insiders and outsiders. Insiders are people that do have a certain access power, but exceed this power. They are only punishable if they hack to inflict harm, or deceptive intent to commit. This restriction does not apply to outsiders: they are always punishable, even if they crack a system 'with good intentions'.

Hacking can take place in different situations. Not infrequently, hackers use a vulnerability in a ICT system through which an automated workspace can be invaded. By hacking we understand also the intrusion of a system under a false capacity, for example with a stolen log-in name and password on a webmail service like Hotmail or Gmail. Hacking can also take place via a "brute force attack". This technique uses a large number of password variations tried out in succession until access to the automated workplace is gained. Another important method is infecting computers with a malicious software program (malware), which accesses through a 'back door' to the automated workplace. In this case, the malicious software called 'a Trojan horse'; quite appropriately, because the program stays unnoticed on the victim's computer.

- White hat hackers are the so-called 'good' hackers. The white hat hackers hack especially for the challenge and the thrill they get if they manage to break in at a (large) authority. White hat hackers often hack to see if there are leaks in the security of a website, so that it can be improved. They are not out to rob data or steal money.
- *Black hat hackers* are the most dangerous kind of hackers. They hack mainly for private gain. These people will try to break into the computer in order to earn money.
- *The grey hats* sit in between; they hack sometimes for private gain, and sometimes not. Just like white hats they find the challenge of hacking important, but sometimes they will also break into somewhere for their own gain.
- *Scriptkiddies:* These people are actually no real hackers, but people who penetrate a system through the use of a program that was created by others (a script). There are relatively more of these people, but they are easier to stop.

Hacking Eras & Generations:

From the early days of modern computing through to the 1970s, it was far more common for computer users to have the liberties that are provided by an ethic of open sharing and collaboration. So the first generation hackers (70's) were driven by need for knowledge. The 2nd generation (the early 80's) was driven by curiosity and need for knowledge. Later on (85-90) hacking became a trend. The 3th generation, in the 90's, was driven by addiction, curiosity, establishing networks, information sharing. Finally, the 4th generation (2000- ..) is driven by eagerness and

money. In this generation you can see that hacking meets with politics (cyber-hacktivism) or with the criminal world (cybercrime).

Hacktivism is the subversive use of computers and computer networks to promote a political agenda. The definition of hacktivism is controversial. Broadly a 'hacktivist' is someone who uses technology hacking to effect some social change. With roots in hacker culture and hacker ethics, its ends are often related to the free speech, human rights, or freedom of information movements.[42] Due to the variety of meanings of this term, hacktivism is sometimes ambiguous and there is significant disagreement over the kinds of activities and purposes it encompasses. Some definitions include acts of cyberterrorism, while others simply reaffirm the use of technological hacking to affect social change.[43] Depending on who uses the term, hacktivism can be a politically motivated technology hack, a constructive form of anarchic civil disobedience, or an undefined anti-systemic gesture. Hacktivists are ideologically motivated individuals that can dynamically form groups/subgroups, usually lacking a central organisation structure. Their main motivation is usually the defense of ideas that are sometimes manifested. Targets of hacktivists are selected in such a way, that media attention creates high visibility in order to successfully preform a cyber-attack... hacktivists may achieve severe impact.[44] Some people describing themselves as hacktivists have taken to defacing websites for political reasons, such as attacking and defacing government websites as well as websites of groups who oppose their ideology.

3.2.2 Spamming

Spamming is the mass sending of e-mails to people who have asked not to. An individual can be able to close down computer systems of companies or government organizations by automatically sending thousands of emails per day. Spammers send messages to thousands and even millions of recipients at the same time. Usually it concerns commercial messages with an erotic character. The mail servers of most Internet Service Providers (ISPs) refuse all mails that come from incorrect addresses. Many spammers use different shipping addresses, to stay anonymous and hide their address.

Spam messages are always sent through an electronic channel. You can receive them by e-mail, via a mobile phone (sms or mms), using the fax, by phone – when you receive a call from an automated call system, via social network websites, via another electronic channel. Furthermore, comment spam – advertising messages posted in the form of comments on websites (such as newssites, guestbooks, webblogs,…) are very common. Comments on websites are very popular and even more fun to read than the article itself. So spammers use that to put their advertisements on websites, in combination with links to advertising websites. A more dangerous form of spam is 'phishing' (see later). Finally there exist also 'splogs': a website that consists of only spam. This website has been created to advertise spam-products or to lead you to websites with spam. Splogs are blogs where the articles are fake, and are only created for search engine spamming.

[42] **Krapp, P.,** (2005), *'Terror and Play, or What was Hacktivism? Grey Room'.* MIT Press.
[43] **Ludlow, P.,** (2013), *'What is a 'Hacktivist'?'* The New York Times, January 2013.
[44] **ENISA**, *'Threat Landscape Report 2013, Overview of current and emerging cyber-threats.'*

Recently, a number of sites, including Amazon.com and Yahoo!, were overloaded willfully. This practice is not an offence itself, but can be extremely unpleasant. According to Google there are millions of spam Webpages created. They are actively engaged in fighting spam. Google distinguishes the following types of spam:

- *Cloaking and/or hidden redirects*: the website seems to be dealing with cloaking (show a different content to search engines than to users) or resolving users to a page other than that Google saw.
- *Hacked site:* some pages on the internet site may be hacked by a third party to show content or links with spam. Website owners should immediately take action to clean up their sites and to resolve any security problems.
- *Hidden text and/or excessive use of keywords:* On some pages, hidden text and/or excessive use of keywords can appear.
- *Parked domains* are placeholdersites with little unique content, so Google does not take them usually up on the search results.
- *Pure spam:* the site seems to use aggressive spam techniques, such as automatically generated nonsense, cloaking, content from other websites, repeated or serious, violations of Google's webmaster guidelines
- *Free hosts and dynamic DNS providers with lots of spam*: this site is hosted by a free hosting service or dynamic DNS provider with content which contains a lot of spam.
- *Limited content with little or no additional value*: the site seems to consist of pages of poor quality or superficial pages which do not offer a lot of additional value to the user.
- *Unnatural links of a site:* Google has detected on that site a pattern of unnatural, artificial, misleading or manipulative links detected.
- *Unnatural links to a site:* Google has a pattern of unnatural, artificial, misleading or manipulative links detected that refer to this site.
- *User-generated spam:* that site seems to obtain a user-generated content with a lot of spam. The problematic content may appear on forum pages, guest books or pages in user profiles.

3.2.3 Cyber pornography

Pornographic material is increasingly being spread via the internet. This also applies to texts and images relating to minors, the so-called 'child pornography'. Pedophiles use also the Internet. For a pedophile, the Internet is inexpensively and simple, because he does no longer have to invest in all kinds of material, such as photos and videos. Otherwise, the internet makes it easier for the police to detect and discover pedophiles. Pedophiles have two ways to make use of the internet: they pick up pedophile material of websites and they try to make contact with minors, through chat boxes under a false identity. Those chat boxes are very interesting for pedophiles, because they can ask undisturbed spicy questions without standing out, especially if they use a language which suits their target audience.

3.2.4 *Payment Fraud* [45]

Payment card transactions are the most widespread non-cash payment method used in the European Union. In 2012, the value of transactions made by debit and credit card issued within the Single Euro Payments Area amounted to 3,5 trillion €. In the same period, criminals acquired 1,33 billion € from payment card fraud (PCF). This is 38 cents lost to fraud for every 1000€ worth of transactions. But the real impact of PCF is far more substantial due to the other costs associated with the crime. Moreover, expenses can be expected in terms of insurance, fraud management and crime prevention costs.

Furthermore, a 2013 European Commission survey found that 35% of EU citizens interviewed had concerns about the security of online payments, which translates into a reluctance to use online transactions.

In 2012, 60% of the total payment card fraud value occurred when the card was not present (CNP) at the Transaction. In 2014, the number of online transactions is estimated to reach 34.8 billion worldwide, almost twice the number from 2010. CNP fraud is likely to grow proportionately with the increasing number and volume of online transactions.

Payment card fraud has developed into a true hybrid crime that can occur in both online and offline environments. Regardless of where it occurs, the fraud inevitably includes two phases: obtain the credit card details and monetise. This is facilitated by online forums who bring together buyers and sellers of compromised cards.

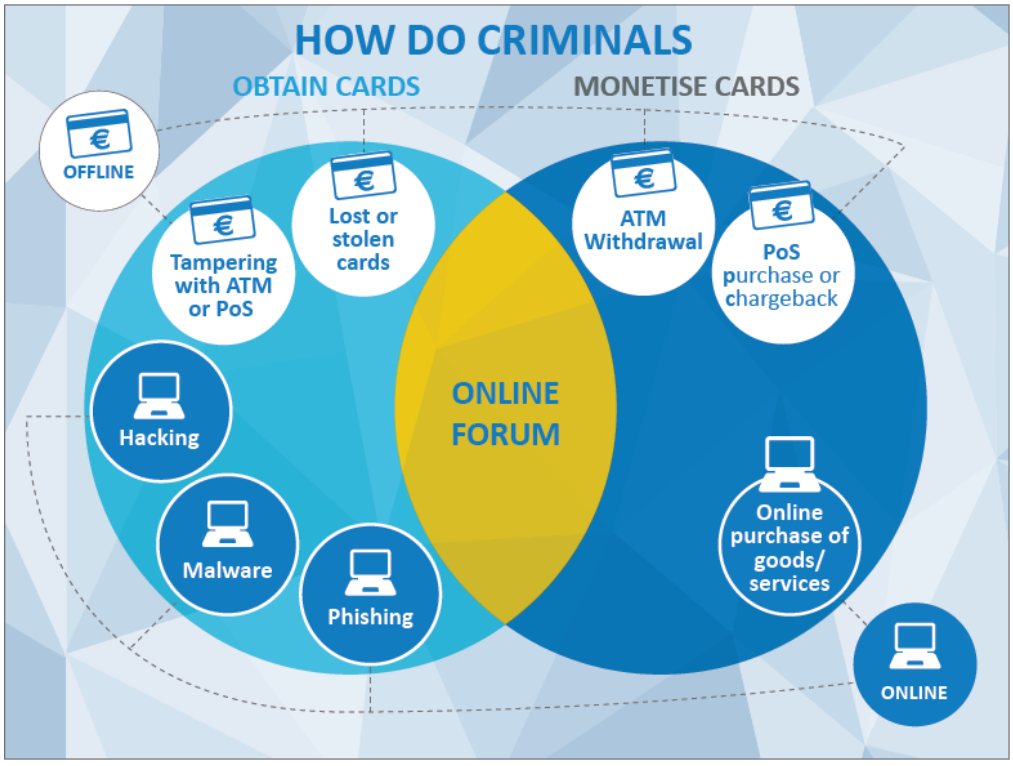


Figure 9: Payment Fraud
Source: Europol (2014), The Internet Organised Threat Assessment (iOCTA) 2014, The Hague, 2014.

Skimming, the extraction of card data from the magnetic strip of a payment card, continues to have a strong presence, especially across Member States in the Southern and Eastern part of the EU as well as in candidate and potential candidate countries.

[45] **Europol** (2014), The Internet Organised Threat Assessment (iOCTA) 2014, The Hague, 2014.

However, most European countries have already observed an increasing shift from skimming towards CNP. This trend is being replicated across the continent. The Internet has changed the way traditional crimes - such as skimming - work. Now, skimming components can be bought online and the price of a skimming set is so payable that even a single cashed out card may cover the cost of the investment.

3.2.5 Phishing

Phishing is a ruse designed to obtain information of the victim by using e-mails, webpages or letters that seem authentic documents from institutions/agencies. These messages carry the victim to provide information to shut down an account to respond quickly to a golden opportunity or to respond quickly to a gift.[46] The majority of phishing incidents start with potential victims receiving spam, luring them to websites attempting to elicit login credentials and other sensitive data from them, or hosting exploits designed to compromise the visitor's computer system.

Phishing is one of the most common types of cybercrime (in internet fraud and hacking). Despite the publicity generated by certain scams and prevention campaigns, the number of victims falling for phishing has increased across Europe. Particularly affected are elderly people who lack internet skills and who are generally more trusting and respectful of official-looking material than younger generations.

In figure 10 (see next page) you can see the different types of listed from a previous investigation into phishing at the Belgian Government.[47]

Deceptive Phishing[48]*:* we talk of deceptive phishing when the phisher sends out messages containing a list in order to persuade the victim to visit a certain site to change or to fill in data. In this category malware has not been used to forward information to the phisher (see Malware-based phishing).

- *Spoofing – Spam Based Phishing:* Phishing with email and spam is a common form of phishing. Often emailspoofing is used, which has falsified information of the sender. Most of the posts contain an urgent note that the user asks to enter information. This information is, according to the message, necessary to modify account information, in order to update account information and to check the accounts. Sometimes you will be asked to fill in a form to receive access to a new service via a link which you can find in the phishingmail.[49]
- *Instant Messaging Based phishing:* This method uses a message via an instant messaging channel (MSN, Facebook chat, ...) containing a link to a phishing site that has the same look as a legitimate website. If the user does not check the URL,

[46] **Workman, M.** (2008), *'Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security.' Journal of the American Society for Information Science and Technology*; Volume 59, Issue 4, pages 662–674, 15 February 2008.
[47] **Schoofs, P.,** (2014), '*Phishing bij de overheid in België.'* Masterproef Business Process Management and IT; Open Universiteit Heerlen.
[48] **Bergholz, A., De beer, J., Glahn, s., Moens, M.-F., Paass, G. & Strobel, S.,** (2010), *'New filtering approaches for pshishing email.' Journal of Computer security, 18(1), 7-35.*
[49] **Vishwanath, A., Herath, T., Chen, R., Wang, J. G. & Roa, H. R.**, (2011), '*Why do people get phished? Testing individual differences in pshishing vulnerability within an integrated, informative processing model'.* Decision Support Systems, 51(3), 576-586.

it can be difficult to see the difference between the fake and the legitimate website. Then the user will be asked to enter personal information on the webpage.[50]

- *Telephone phishing:* the phisher calls the user and asks for a certain action, such as giving a password or turning off the firewall on the computer. The goal is getting personal information or getting control over the victim's equipment. Telephone phishing is usually done with a fake caller ID.[51]
- *SmiShing:* this method uses a SMS message to lure the victim.[52]
- *Vishing:* takes advantage of the Voice Over Internet Protocol (VOIP) to contact victims and to trap them.[53]
- *Phishing via search engines:* Some phishing attacks use search engines where the user is referenced to websites that offer cheap products or services whenever he seeks something out in a search engine, such as Google. When the user attempts to purchase the product, whereby his credit card details are entered, this data will be collected by the phishing site.
- *Social media:* Social media sites (such as Facebook) could be exploited according to Symantec. Links would be posted on social media sites, whereby the victim is led to the site that aims to steal data.

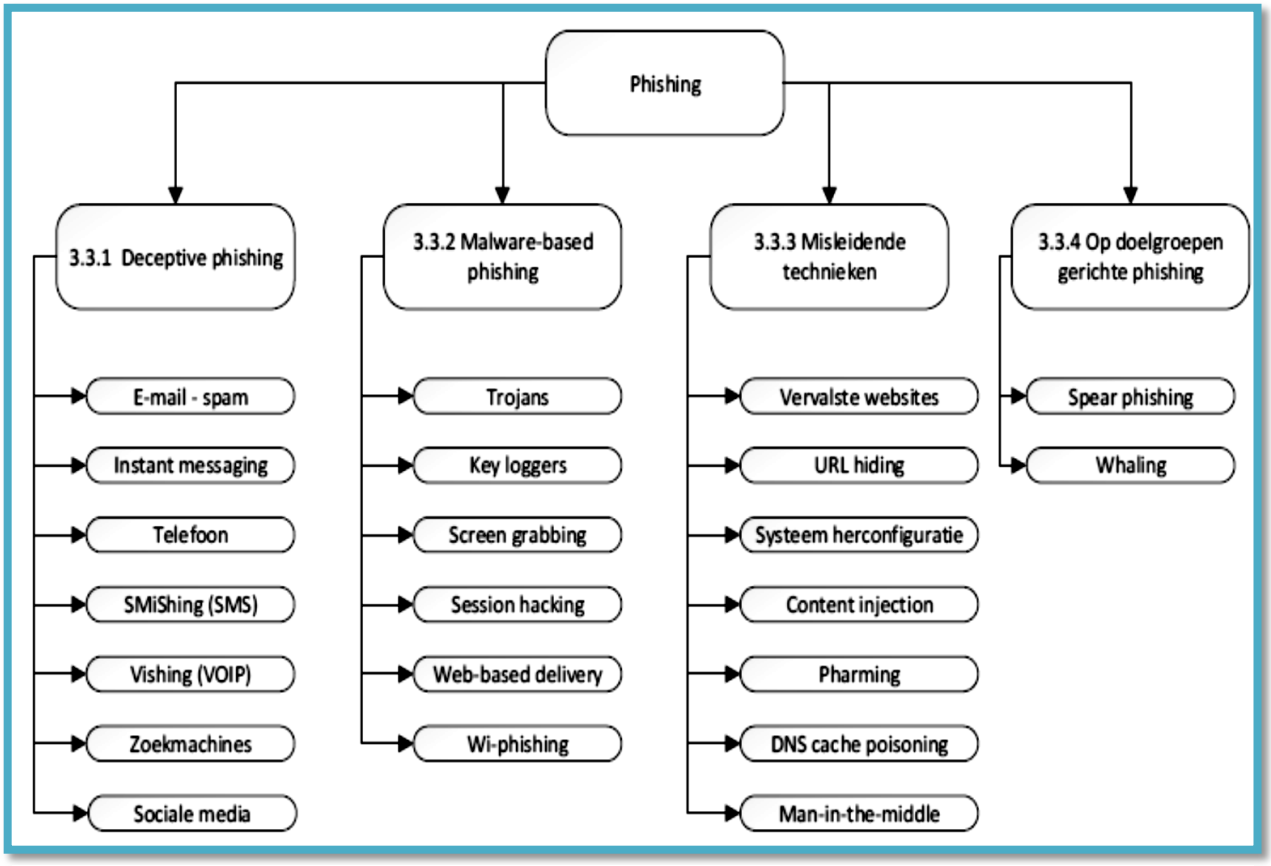


Figure 10: Different types of phishing
Schoofs, P., (2014), 'Phishing bij de overheid in België.' Masterproef Business Process Management and IT; Open Universiteit Heerlen.

[50] **Bose, I. & Leung, A. C. M.**, (2007*), 'unveiling the mask of phishing: threats, preventive, measures and responsibilities.'* Communications of the Association of InformationSystems, *19,* 544-566.
[51] **Bose, I. & Leung, A. C. M.**, (2007*), 'unveiling the mask of phishing: threats, preventive, measures and responsibilities.'* Communications of the Association of InformationSystems, *19,* 544-566.
[52] **Wall, D.S.,** (2008), 'Cybercrime, Media and Insecurity: the shaping of public perceptions of cybercrime'. International Review of Law, Computers and Technology, vol. 22, nos. 1-2, pp. 45–63 (ISSN 0965-528X).
[53] **Baron, L .,** (2006), *'Gone Vishing. Journal of Accountancy', 202(3), 15-15*

Malware-based Phishing: we talk of 'Malware-based phishing' when malicious software is used to nestle on the computer of the victim, with the objective to send confidential data of the victim to the hacker.[54]

- *Trojans:* a malicious computer program which misrepresents itself to appear useful, routine, or interesting in order to persuade a victim to install it. If installed or run with elevated privileges a Trojan will generally have unlimited access. What it does with this power depends on the motives of the attacker.
- *Key loggers:* A form of malware that captures and identifies every keystroke typed on a particular keyboard. All the typed information can be obtained by another person, even if the author modifies or deletes what was written, or if the character does not appear on the monitor, such as when entering a password. The input is sent to the hackers, who try to decipher all sorts of passwords and other types of information from all the input they get.[55]
- *Screen Grabbing:* some advanced phishing attacks make screenshots of the data who are entered, for example, in a web-based application. This type of malware is used to bypass the security of programs provided with anti-key loggers.[56]
- *Web-Based Delivery:* this form of malware-based phishing happens when the victim clicks on the link in the phishing message and is directed to a website. This website, when opened, will install a malware on the computer of the victim. Once the victim uses the computer to execute some transactions, the malware will forward the data to the phisher.[57]
- *Session hacking:* The phisher makes advantage of a web session controlmecanism. A simple 'session hacking' allows the phisher to use a sniffer to intercept relevant information, so that the offender can provide illegal access to the webserver itself.[58]
- *Wi-phishing:* installing a Wi-Fi access point in order that mobile users can connect automatically with their measurement to this access point. In the meantime malware will be installed on the appliance or the data from the mobile devices will be stolen. Because there are installed more and more free Wi-Fi access points in public places, it is easy for the phisher to use another name of the Wi-Fi network (SSID) to entice the user to their Wi-Fi accespoint.[59]

On target-specific phishing

- *Spear-phishing:* not the medium, but the victim is carefully chosen. The perpetrator tries to collect as much information as possible about the target and the misleading nature of the phishing message will become stronger and increase the success rate of the attack. Collecting the information is used to scan for vulnerabilities (e.g.

[54] **Bergholz, A., De beer, J., Glahn, s., Moens, M.-F., Paass, G. & Strobel, S.,** (2010), *'New filtering approaches for pshishing email.'* Journal of Computer security, 18(1), 7-35. Doi: 10.7813/2075- 4124.2013/5-6/A.30.
[55] **Gyorffy, J., Tappenden, A., & Miller, J.,** (2011), *'Token-based graphical password authentication.'* International Journal of Information Security, 10(6), 321-336.
[56] **Gunter, O., (2007),** *'The Phishing Guide: Understanding & Preventing Phishing Attacks.'* [http://www-935.ibm.com/services/us/iss/pdf/phishing-guide-wp.pdf]
[57] **Bose, I. & Leung, A. C. M.**, (2007*), 'unveiling the mask of phishing: threats, preventive, measures and responsibilities.'* Communications of the Association of InformationSystems, *19,* 544-566.
[58] **Mannan, M., & Oorschot, P. C.**, (2011), *'Leveraging personal devices for stronger password authentication from untrusted computers'.* Journal of Computer Security, 19(4), 703-750. doi: 10.3233/JCS-2010-0412.
[59] **Sinha, A., Haddad, I., Nightingale, T., Rushing, R., & Thomas, D.,** (2006), *'Wireless intrusion protection system using Distributed collaborative intelligence.'* Paper presented at the Performance, Computing and Communications Conference, 2006. IPCCC 2006. 25th IEEE International.

personal information on social media), hacking a customer's file or website in order to trick the victim.

- *Whaling:* can be regarded as a special form of spear-phishing, where the offender chooses companies, Governments or groups of high-level executives as target. The phisher tries to attack a small group of senior officials to rip off, so he can invest more time in the attack and refine his message to the highest success rate on to achieve success.[60]

3.2.6 *Child sexual exploitation online*

Child sex offenders commit criminal offences with an element of sexual activity or sexual contact with a minor, thereby violating established legal and moral codes with respect to sexual behaviour. Most child sex offenders are not part of any criminal network and usually operate alone, driven solely by their sexual interest in children. But this does not mean that offenders act in isolation from each other: they communicate among themselves within like-minded groups in cyberspace, using different online tools.

The most common method for perpetrators to exchange Child Abuse Material is Peer-to-Peer platforms, facilitated by the ease of access to this type of platforms and by the large amounts of Child Abuse Material available for free within this medium. The increase in mobile devices and apps, which enables constant connection to the online world by potential victims and offenders, is a facilitating factor.

✓ *Exploitation of children online* [61]

Child sex offenders use the Internet to meet like-minded persons, to have access to a wider pool of children, to share resources and their knowledge and to disseminate Child Abuse Material. Girls of white ethnicity, aged between 11 and 14 years old are the main

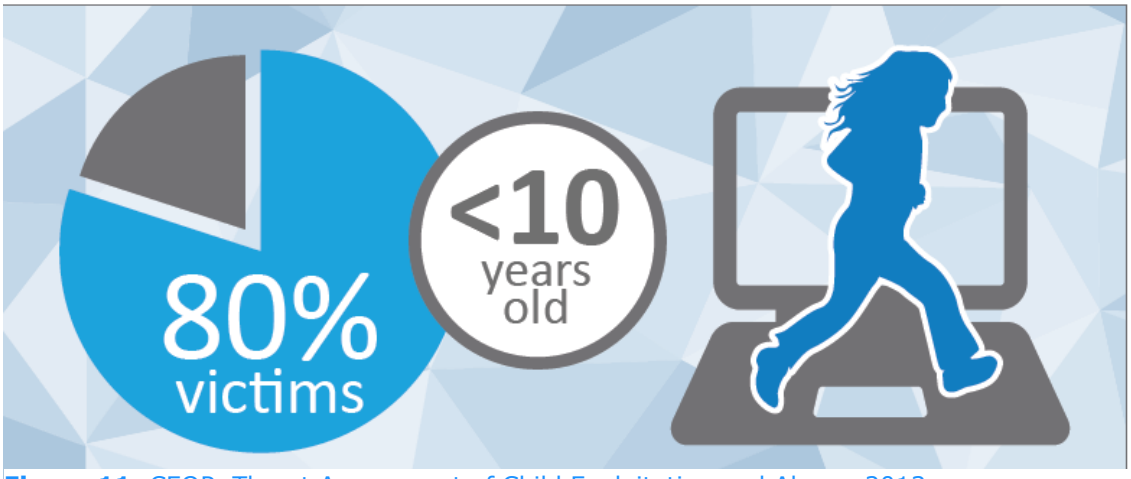


Figure 11: CEOP: Threat Assessment of Child Exploitation and Abuse, 2013

victims. However, information from the Internet Watch Foundation tells us - when considering web pages containing child abuse material - that the age of the victims is

[60] **Gunter, O., (2007),** *'The Phishing Guide: Understanding & Preventing Phishing Attacks.'* [http://www-935.ibm.com/services/us/iss/pdf/phishing-guide-wp.pdf]
[61] **Europol** (2014), The Internet Organised Threat Assessment (iOCTA) 2014, The Hague, 2014, p. 29.

even considerably lower: 80% of the victims are under 10 years old. Data of INHOPE, the International Association of Internet Hotlines, show an increase in infant victims of sexual abuse and in abuse of an extreme and sadistic nature.

- ✓ *Sextortion and grooming*

Many cases of sexual extortion are a consequence of 'sexting'. Sexting can be defined as the 'exchange of sexual messages or images', typically self-generated, sent via the Internet or a mobile phone. This exchange frequently occurs between young people consciously exchanging naked or sexualised images of themselves with one other. Technology can facilitate the further unwanted dissemination of these pictures, affecting the well-being of the originator, leading to harassment and bullying, online and off-line, self-harming and even suicide.[62]

Sextortion refers to the broad category of sexual exploitation in which abuse of power is the means of coercion, but it refers also to the category of sexual exploitation in which threatened release of sexual images or information is the means of coercion. Sextortion is a form of corruption in which people entrusted with power – such as government officials, judges, educators, law enforcement personnel,… – seek to extort sexual favors in exchange for something within their authority to grant or withhold.

Furthermore, sextortion refers to a form of sexual blackmail in which sexual information or images are used to extort sexual favors from the victim. Social media and text messages are often the source of the sexual material and the threatened means of sharing it with others. An example: people are extorted with a nude image of themselves they shared on the Internet through sexting. Afterwards, they are coerced into performing sexual acts with the person doing the extorting or are coerced into performing hardcore pornography.

- ✓ *Child Sexual exploitation online on the Darknet* [63]

Using the Darknet is increasingly popular among Europeans. A large number of perpetrators, the ones with a higher security awareness and technical knowledge, have established communities using hidden services on platforms. These platforms and their hidden services facilitate practically untraceable sexual exploitation of children by allowing the exchange of images and pictures anonymously through websites, private messages and email.

- ✓ *Live streaming of child abuse* [64]

The popularization of webcams and chat rooms that empower the streaming of live images and videos has led to their exploitation by child sexual abusers. Some applications allow users to upgrade their accounts by paying a fee, guaranteeing access to extended features, including broadcasts protected by passwords and extra layers of anonymity. While live streaming is common in sexual extortion cases, a trend has been detected concerning the abuse of children overseas, live in front of a camera. A session allows the perpetrator the chance to orchestrate and view the abuse of a child in real

[62] **EC3 Europol,** The Internet Organised Crime Threat Assessment (iOcta) 2014*, p.30*
[63] **EC3 Europol,** The Internet Organised Crime Threat Assessment (iOcta) 2014*, p.30*
[64] **EC3 Europol,** The Internet Organised Crime Threat Assessment (iOcta) 2014*,* p.32

time. The abused kids are from countries with deprived economies, for example Eastern Asia. In investigated cases, the financial profit is used to support the basic needs of the family or group involved. The potential to earn money, makes the crime of abuse via live streaming an attractive proposition. This live streaming of child abuse is likely to be a growing area. It is hard to detect and investigate, since the perpetrators do not usually store a copy of the streamed material.

3.2.7 Cyber Terrorism

Government officials and Information Technology security specialists have documented a significant increase in Internet problems and server scans since early 2001. There is a growing concern among federal officials that such intrusions are part of an organized exertion by cyberterrorists, foreign intelligence services, or other groups to map potential security holes in critical systems. A cyberterrorist is someone who intimidates or coerces a Government or organization to advance his or her political or social objectives by launching a computer-based attack against computers, networks, or the information stored on them.

Cyberterrorism, can be defined as an act of terrorism committed through the use of cyberspace or computer resources.[65] A simple propaganda on the Internet, that there will be bomb attacks during the holidays, can be considered as cyberterrorism. There are also hacking activities directed towards individuals, families, organized by groups within networks, tending to cause fear among people, demonstrate power, collecting information relevant for ruining peoples' lives, robberies, blackmailing,…

Cyber-terrorism can have a serious large-scale influence on significant numbers of people. It can weaken countries' economy greatly, thereby stripping them of its resources and making it more vulnerable to military attack. Cyber-terror also affects internet-based businesses. Like brick and mortar retailers and service providers, most websites that produce income (whether by advertising, monetary exchange for goods or paid services) could stand to lose money in the event of downtime created by cyber criminals. As internet-businesses have increasing economic importance to countries, what is normally cybercrime becomes more political and therefore "terror" related.

3.2.8 Racism and Holocaust denial

Racism, holocaust denial and files not free from racist statements or publications are punishable, also when they are distributed over the internet. This includes the concept of 'cyberhate'; which refers to expressions of hate on the internet. That hate is reflected in racism: the use of bullying (cyberbullying), insults or violence based on a person's skin color, race or ancestry. But also discrimination based on gender, sexual orientation, religion or philosophy of life falls under the concept of 'cyberhate'. Others vent their hate by anti-Semitism and Holocaust denial: the denial, minimize, justify or approve of genocide committed during the Second World War.

3.2.9 Cyberextortion

Cyberextortion is a crime involving an attack or threat of attack coupled with a demand

[65] **Parker D.,** (1983) '*Fighting Computer Crime',* U.S, Wiley.

for money to avert or stop the attack. Cyberextortion can take many forms. Originally, denial of service (DoS) attacks against corporate websites where the most common method of cyberextortion. The attacker might initiate a ping storm and telephone the president of the company, demanding that money be deposited to a bank account in a foreign country, in exchange for stopping the attack.

Lately, cybercriminals have developed ransomware which encrypts the victim's data. The victim receives an email that offers the private decryption key in exchange for a monetary payment in bitcoins. Unfortunately, as with other types of extortion, payment does not guarantee that further cyber-attacks will not be launched. Most cyberextortion efforts are initiated through malware in e-mail attachments or on compromised websites.

As the number of enterprises that rely on the Internet for their business has increased, opportunities for cyberextortionists have exploded too. According to some reports, most cyberextortion episodes go unreported, because victims do not want the publicity.

3.2.10 Cyberbullying

Cyberbullying is defined in legal glossaries as

- actions that use information and communication technologies to support deliberate, repeated, and hostile behavior by an individual or group, that is intended to harm another person or other persons.
- use of communication technologies for the intention of harming another person or other persons.
- use of Internet service and mobile technologies such as web pages and discussion groups as well as instant messaging or SMS text messaging with the intention of harming another person or other persons.

Cyberbullying can be seen as being distinguished from other forms of online behavior. Some see cyberbullying as a form of cyberstalking, which involves taking a more strategic approach than Internet trolling.[66]

In Internet slang, a troll, is a person who sows discord on the Internet by starting arguments or upsetting people, by posting inflammatory, extraneous, or off-topic messages in an online community, e.g. a newsgroup, forum, chat room or blog, with the deliberate intent of provoking readers into an emotional response or of otherwise disrupting normal on-topic discussion, often for their own amusement.

Examples of what constitutes cyberbullying include communications that seek to intimidate, control, manipulate, put down, falsely discredit, or humiliate the recipient. The actions are deliberate, repeated, and hostile behavior intended to harm another. A cyberbully may, but does not have to, know their target. A cyberbully may be anonymous and may solicit involvement of other people online who do not know the target. This is known as a 'digital pile-on'. Cyberbullying has been defined as 'when the Internet, cell phones or other devices are used to send or post text or images intended to hurt or embarrass another person'.

[66] **Bishop, J.** (2013). *'The effect of deindividuation of the Internet Troller on Criminal Procedure implementation: An interview with a Hater.'* International Journal of Cyber Criminology 7(1), pp. 28-48.

One speaks about cyber bullying when young people are represented on both sides . Cyber bullying takes place when a child or young person threatens another child or a young person is harassed, humiliated, annoyed, or embarrassed by using digital techniques. As soon as adults are involved, one speaks rather about stalking or harassment.

4 Conclusion

Although many people have a limited knowledge of 'cybercrime', this kind of crime has the serious potential for severe impact on our lives and society, because our society is becoming an information society, full of information exchange happening in "cyberspace". The Internet - and cyberspace - has a tremendous impact on all parts of our society. In a digital age, where online communication has become the norm, Internet users, governments and business face increased risks of becoming the targets of cyberattacks. Threats can have different origins, - including criminal, politically motivated, terrorist or state-sponsored attacks as well as natural disasters and unintentional mistakes. Over the past few years, the global cybercrime landscape has changed dramatically, with criminals employing more sophisticated technology and greater knowledge of cybersecurity.

Cybercrime is a borderless problem, consisting of criminal acts that are committed online by using electronic communication networks and information systems, including crimes specific to the Internet, online fraud and forgery and illegal online content. Because of the borderless characteristic of cybercrime, criminal investigations are more complicated for law enforcement authorities.

While the 'real' extent and economic impact is really hard to quantify, scientists and officials agree that cybercrime is a huge and still growing problem. The value of the cybercriminal economy as a whole is not precisely known, however the losses are enormous. In 2011, the estimate of global corporate losses alone stood at around 750 billion€ per year. The unprecedented scale of the problem threatened the ability of the authorities to respond – with more than 150,000 viruses and other types of malicious code in global circulation, and 148,000 computers compromised per day. At the same time, the authorities have more data on criminal activity at their disposal than ever before, and now have an opportunity to harness this information in ways which make intelligence development and investigation more streamlined and cost effective.

In order to combat cybercrime, the EU has implemented legislation and supported operational cooperation, as part of the ongoing EU Cybersecurity Strategy. Furthermore, several legislative actions were developed to contribute to the fight against cybercrime. These include for example a Directive against information systems, online offensive material, combating the sexual exploitation of children online and child pornography,… In addition to these EU initiatives, lots of projects and practices have been developed in various Member States. To learn more about those legislative actions, initiatives, projects and practices, you can read the EUCPN Toolbox 'Cybercrime', which is primarily written for local policy-makers and practitioners who may be confronted with these issues in their daily work.

5 Bibliography

AJEET SINGH POONIA, (2014), *'Cyber Crime: Challenges and its Classification International Journal of Emerging Trends & Technology'.* Computer Science (IJETTCS) Volume 3, Issue 6.

Baron, L ., (2006), *'Gone Vishing. Journal of Accountancy', 202(3), 15-15*

BEDNARZ., A. (2004) , 'Profiling cybercriminals: A promising but immature science in Networkworld'. [http://www.networkworld.com/article/2327820/lan-wan/profiling-cybercriminals--a-promising-but-immature-science.html]

Bergholz, A., De beer, J., Glahn, s., Moens, M.-F., Paass, G. & Strobel, S., (2010), 'New filtering approaches for pshishing email.' *Journal of Computer security, 18(1), 7-35.*

Bishop, J. (2013). *'The effect of deindividuation of the Internet Troller on Criminal Procedure implementation: An interview with a Hater.'* International Journal of Cyber Criminology 7(1), pp. 28-48.

Bose, I. & Leung, A. C. M., (2007*), 'unveiling the mask of phishing: threats, preventive, measures and responsibilities.'* Communications of the Association of InformationSystems, *19,* 544-566.

Carter, D.L., *Computer Crime Categories: How Techno-Criminals Operate,* FBI Law Enforcement Bulletin, 1995, Volume: 64, Issue 7, pp 21-27 [https://www.ncjrs.gov/pdffiles1/Digitization/156176NCJRS.pdf]

Castells, M. (2002), *'The internet galaxy: Reflections on the internet, business and society.'* Oxford: Oxford University Press.

City of London (2015), *The implications of economic cybercrime for policing",* Research report City of London corporation, October, 2015.

Clough, J. (2010), '*Principles of cybercrime'*. Cambridge University Press.

Council of the European Union (2001), Convention on Cybercrime, Budapest, 23 November 2001

EC3, Europol, 'First Year Report, p. 26

EC3 Europol, *The Internet Organised Crime Threat Assessment (iOcta) 2014*, p.12.

ENISA, *'Threat Landscape Report 2013, Overview of current and emerging cyber-threats.'*

European Commission (2013), Joint Communication to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels: COM (2013) 01 final, 07 February 2013. [http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52013JC0001]

European Commission (2015), Special Eurobarometer 423 cybersecurity report, February 2015. [http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf]

European Union (2014), Cyber Security Strategy and Programs Handbook, Volume 1 Strategic Information and Regulations, p. 113

Europol (2014), The Internet Organised Threat Assessment (iOCTA) 2014, The Hague, 2014.

Grabosky, P.N., *(2001), 'Virtual criminality: Old wine in new bottles?'.* Social and Legal Studies (10:2),243-249:243.

Gordon, S., Richard, F. (2006), *'On the definition and classification of Cybercrime,' Journal in Computer Virology 2006, Volume 2, Issue 1, pp. 13-20.*

Gosh, S., Turrini, E. (2011), '*Cybercrimes: A Multidisciplinary Analysis', Springer, p.373*

Govil, J. (2007). '*Ramifications of Cyber Crime and Suggestive Preventive Measures'*. *IEEE , 43*(4), 610-615

Gunter, O., (2007), *'The Phishing Guide: Understanding & Preventing Phishing Attacks.'* [http://www-935.ibm.com/services/us/iss/pdf/phishing-guide-wp.pdf]

Gyorffy, J., Tappenden, A., & Miller, J., (2011), *'Token-based graphical password authentication.'* International Journal of Information Security, 10(6), 321-336

Halder, D., & Jaishankar, K., (2011) '*Cybercrime and the Victimization of Women: Laws, Rights, and Regulations.'* Hershey, PA, USA.

Kamini, D. (2011) *'Cybercrime in the Society: Problems and Preventions'*. Journal of Alternative Perspectives in the Social Sciences (2011) Vol 3, No 1, 240-259

Kirwan, G. and Power, A. (2012) '*The Psychology of Cyber Crime.'* Hershey: IGI Global.

Krapp, P., (2005), *'Terror and Play, or What was Hacktivism? Grey Room'.* MIT Press.

Ludlow, P., (2013), *'What is a 'Hacktivist'?'* The New York Times. January 2013.

McGuire, M., Dowling, S., *"Cybercrime: a review of the evidence. Research Report 75. Summary of key findings and implications."* Home Office, October 2013.

Mannan, M., & Oorschot, P. C., (2011), *'Leveraging personal devices for stronger password authentication from untrusted computers'.* Journal of Computer Security, 19(4), 703-750. doi: 10.3233/JCS-2010-0412.

Moore, R., (2015) **'***Cybercrime: investigating high-technology computer crime',* Routledge, p. 4.

Parker D., (1983) '*Fighting Computer Crime',* U.S, Wiley.

Proteus Manual (2015) 'Prevention, Information and support to victims of online identity theft', 2015, Lisboa, APAV.

Riek, M., Böhme, R., '*Understanding the influence of cybercrime risk on the e-service adoption of European Internet users'. Proceedings of the 13th Workshop on the Econmics of Information Security (WEIS), The Pennsylvania State University, State College, Pennsylvania.*

Schoofs, P., (2014), *'Phishing bij de overheid in België.'* Masterproef Business Process Management and IT; Open Universiteit Heerlen.

Sinha, A., Haddad, I., Nightingale, T., Rushing, R., & Thomas, D., (2006), '*Wireless intrusion protection system using Distributed collaborative intelligence.'* Paper presented at the Performance, Computing and Communications Conference, 2006. IPCCC 2006. 25th IEEE International.

United Nations Office on Drugs and Crime (2013), Comprehensive Study on Cybercrime, Vienna, February 2013, retrieved from https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Vishwanath, A., Herath, T., Chen, R., Wang, J. G. & Roa, H. R., (2011), '*Why do people get phished? Testing individual differences in pshishing vulnerability within an integrated, informative processing model'.* Decision Support Systems, 51(3), 576-586. doi: 10.1016/j.dss.2011.03.002.

Wall, D., **(2001),** *'Crime and the Internet: cybercrimes and cyberfears',* Routledge, London and New York.

Wall, D.S., (2008), 'Cybercrime, Media and Insecurity: the shaping of public perceptions of cybercrime'. International Review of Law, Computers and Technology, vol. 22, nos. 1-2, pp. 45–63 (ISSN 0965-528X).

Workman, M. (2008), 'Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security.' *Journal of the American Society for Information Science and Technology*; Volume 59, Issue 4, pages 662–674, 15 February 2008.

Warren, G. Kruse, Jay, G. Heiser, (2001) '*Computer Forensics: Incident Response Essentials'.* Boston, MA: Addison-Wesley.

Yar, M., (2006) '*Cybercrime and society'.* Sage Publications Inc., London, p. 9

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

2013 Norton Report, Dangerous liaisons. [https://www.symantec.com/content/en/us/about/presskits/b-norton-report-2013-infographic.en-us.pdf]