Technically Advanced Finnish Cybercriminals by Finnish Court Data in 2015-2019

Technically Advanced Finnish Cybercriminals by Finnish Court Data in 2015-2019

Mikko Luomala
University of Vaasa
School of Technology and Innovations
Information Systems Science
mikko.luomala@uwasa.fi

Abstract

Cybercrime continues to evolve and be issue in global society. In this article, I examined the technically advanced characteristics of cybercrime, conducted by cybercriminals in Finland. The dataset of 365 court cases was examined from years 2015-2019. I investigated how technically advanced were cybercrimes. From the dataset 16 cases were discovered. I adopted interpretive approach, and the research methodology is qualitative. The results show that, the Finnish criminal justice system has processed some of the technically advanced cybercriminals, which have used their own tools for cybercrime which targets the computer systems. There were no cybercrimes, which included usage of artificial intelligence to aid the cybercrime. Between 2015-2019 there was no foreign government official convicted of any cybercrime in the dataset. The results show that the criminal justice system is capable of bringing a small number of cybercriminals to justice from the total amount of the cybercrimes.

Index terms: Cybercrime, Finland, Court data, Characteristics of cybercrime, CCSTC, Technically advanced cybercriminals

1. Introduction

Previously in 2021, we did study Finnish cybercriminality and what convictions criminal justice system has given to Finnish cybercriminals [1]. Also, we have studied what data protection violations has been occurred in Finland [2]. We also studied cybersecurity of the Finnish energy sector and how they fear of cybercrimes [3]. From the energy sector side, we learned that the Finnish energy sector fears wide spectrum of cyberattacks, which can be classified in the criminal justice system as cybercrimes. I started do research what type of cybercrimes are convicted on the Finnish courts [4]. In my previous study I developed the cybercrime classification scale of a technique of cybercrime (CCSTC) and we report it. The CCSTC concepts can be seen as a part of discussion about what criminal actions are cyber-dependent crimes or cyber-enabled crimes [5], and how advanced those cybercrimes can be.

There are studies on the trends of cybercrimes [6], legal studies for the definition of cybercrimes [7], and what cybercrimes are reported to the police [8]. There are gaps in how many so-called technically advanced cybercrimes end up in the courts and how we should describe the phenomenon of cybercriminality in a theoretical sense.

I this study, I try to examine what are technically advanced characteristics of cybercrime by Finnish cybercriminal between 2015-2019. We know that it is a myth that all cybercrimes are technically advanced [4]. According to a doctoral thesis conducted in the Netherlands in 2018,

technical characteristics of cybercrime committed by cybercriminals should be investigated more thoroughly in science [9, p. 206]. Digitalization has created new opportunities to commit crimes, which were in the past possible to commit [10, p. 37]. There are studies how sophisticated are cyberattacks [11], [12], [13], [14], but how many of these technically sophisticated cyberattacks end up for processing to a criminal justice system. Which cyberattacks are processed as a cybercrime in criminal justice system. I think there are gaps in the previous research and my previous research, which needs to be filled. We need to know can the criminal justice system catch advanced cybercriminals and if they can catch them, what type of advanced cybercrimes they have committed. I think we need to use qualitative approach, because there might not be huge number of cases which end up with a criminal justice system. The knowledge which this research produce will give indication that how many advanced cybercrimes will end in Finnish criminal justice and how advanced are so called high-tech cybercrimes.

Therefore, we need to examine what kind of technically advanced cybercrimes will end up with criminal justice. Therefore, my next research question is: (RQ) What kind of advanced cybercrimes have been convicted in Finland between 2015 and 2019?

2. Literature review

Narrative literature review is used for this article [15], to collect possible previous studies relating to technical advanced characteristics of cybercrimes. The literature is processed with discursive approach [16, p. 7]. The scope is to discover previous studies, which discuss about technologically advanced cyberattacks, which are classified as a cybercrime.

Definition relationships of a cybercrime, cyberattack and cyberwarfare

The cyberattacks are increased globally [12], which is hypothesized to be caused by continuous increase in the use of artificial intelligence (AI) and other advanced technologies [17]. Definitions of cyberattacks and cybercrimes seem to have some sort of overlap (Figure 1) [18], but their technicality has variation in how they are commenced to targets or victims [4]. Yuchong and Qinghui (2021) have defined relations of cybercrime, cyberwarfare and cyberattack. However, I have drawn a different picture to illustrate relationship of cyberattack to cybercrime and cyberwarfare (Figure 1).

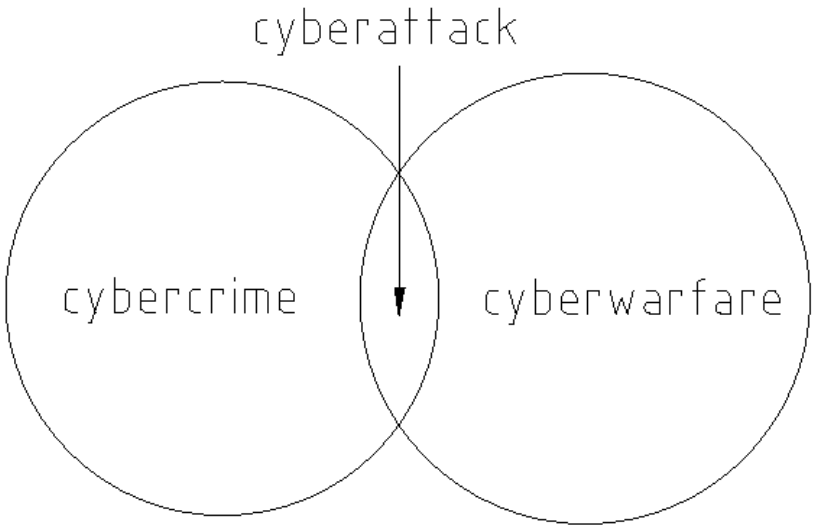


Fig. 1. Relations of cybercrime, cyberwarfare and cyberattack [19].
I used libreCAD to draw the figure from inspiration of previous researchers.

The Yuchong and Qinghui (2021) have drawn a different figure.

In Figure 1, I illustrate my interpretation from Yuchong and Qinghui (2021) relationship of cyberattack to cybercrime and cyberwarfare, that a cyberattack is technical phenomenon which occurs in information technology system. The users and different people will either make interpretation the cyberattack is either cybercrime (a police force, criminal justice view) or cyberwarfare (a military view). The Internet or nowadays the cyberworld offers little security, and this open environment allows anyone to become a cybercriminal; it is not the exclusive domain of criminal hacker [20, p. 2].

The classification and gradation discussion links to taxonomy discussion that how to classify different actions occurring in reality to either be an unlawfully or lawful, and what types of crimes and cybercrimes exits and how different criminal actions has some connection other crime definitions. Are there criminal actions which loosely connect to cybercrimes, but main objective is not do actual cybercrime.

Finnish criminologists write that cybercrime definitions is an umbrella term for different types of cybercrimes and criminal behaviour, and it is not legal definition for cybercriminality [10, p 402]. Wall (2007) classification system distinguishes between three generations:

> "The first generation of cybercrimes are traditional or ordinary crimes using computers - usually as a method of communication or to gather precursor information to assist in the organization of a crime." [21, p. 208]
>
> "The second generation of cybercrimes are hybrid cybercrimes, 'traditional' crimes for which network technology has created entirely new global opportunities. Take away the internet and the behaviour continues by other means, but not upon such a global scale or across such a wide span of jurisdictions and cultures." [21, p. 208]
>
> "The third generation of cybercrimes are true cybercrimes that are solely the product of the internet. Take away the internet and they vanish - the problem goes away. This last generation includes spamming, 'phishing' and 'pharming', and variations of online intellectual property piracy." [21, p. 208]

Alkaabi et al. (2010) defines two types of cybercrime in their taxonomy: type I crimes and type II crimes [22]. Type I crimes are actions where the computer is the target of a criminal activity and Type II crimes are actions where the computer is the tool to commit a crime [22]. Finnish criminologist and international criminologist discuss about cyber-enabled crimes and cyber-dependent crimes. The cyber-depended crimes have similar definition like Alkaabi et al. (2010) Type I crimes. The cyber-enabled crimes have similar definition like Alkaabi et al. (2010) Type II crimes. Luomala (2025) defines that there Type III crimes: "technical device or software as a target and aid for committing a crime" [4, p. 45] and it is extension for Alkaabi et al. (2010) taxonomy [4]. Please, see the Table 1 below.

Table 1. The classification and gradation of cybercrimes and link to traditional criminality.

Cybercrime [10, p 402]	
Type IV crimes	
	Type III [4]

		Cyber-dependent (Tietoverkkosidonnaiset): [23], [24], [25], [26]	**Cyber-enabled** (Tietoverkkoavusteiset): [27], [5]
		Finnish criminologist definition of cyber-dependent crimes (Tietotekniikkaan kohdistuvat rikokset) [10, p. 404–405]	**Finnish criminologist definition of cyber-enabled crimes** (Tietokoneavusteiset rikokset) [10, p. 405–406]
		Type I crimes [22]	**Type II crimes** [22]
Traditional crimes which have loose connection to cybercrimes	**The first generation of cybercrimes** [21, p. 208]	**The third generation of cybercrimes** [21, p. 208]	**The second generation of cybercrimes** [21, p. 208]

The Table 1 shows that it is own scientific discussion how make classification and gradation of cybercrimes. The demarcation problem becomes more visible, when different research interpretations are tried compare. Wall (2007) talks about three generation types of cybercrimes [21, p. 208]. The first generation is that someone just exploring information for making "crime", which raises the question that how much those so-called traditional crimes such as violence, drug manufacturing, extortion, financial crimes involve usage of technology? Because I have studied, some financial crimes even they are not classified a true cybercrime by Finnish criminal law, but they have an element to use technology to aid the crime [4]. For that reason, it would be reasonable update classification taxonomy and add line "Traditional crimes which have loose connection to cybercrimes" and update Alkaabi et al. (2010) and Luomala (2025) taxonomy by adding new extension of type IV crimes: traditional crime has loose connection to cybercriminal activity, where traditional crime includes also technical device or software as a target or aid for committing a crime.

History and evolution of cyberattacks and cybercrimes

Some of the cybercrimes are becoming more sophisticated and diverse with usage of technologies such as cryptocurrencies, machine learning and artificial intelligence (AI) [28]. Cybercrime covers a wide range of criminal cyberattacks, such as online extortion, cyber warfare, the spread of computer viruses or malware, Internet fraud, sending spam, phishing, scams, child pornography, and infringement of intellectual property rights [20], [29, p. 24]. Still, scholars are reporting that different types of advanced technologies such as AI-enabled malware, sophisticated cyber-attacks, vulnerability of Internet of things are proposing a threat against information systems (IT) and cybersecurity [30]. There is volution of cybercrimes [6]. From 1960s, issues on cybersecurity were relating to access control [6]. In the 1970s malware and access control become issue because of the pre-Internet connection called ARPA [6]. In the 1980s more different types of intrusions did become issue, when online services were exploited by dictionary attacks against weak passwords or default passwords [6]. Also, government level attackers started to make cyberattacks to gain sensitive information from foreign nations IT systems [6]. In the 1980s security controls were quite weak, antimalware software was started to develop, backups of the data were introduced, awareness training for users of information security issues relating to computer usage [6]. In the 1990s it was known as era of malwares [6]. Personal computers did become considerably common [6]. In the 1990s script

kids did use other persons malware codes to make their own malware attacks. This lead increased development of anti-malware software, firewalls, patch management of the software or operating systems, email filtration and begin of the emergence of incident response teams [6].

In the 2000s world was shifting towards to digitalization [6]. This was happening also in banking and money transactions sectors [6]. This created new opportunities for cybercrime, to commit online frauds and some of the cybercriminals did see opportunity to make real money by cybercrimes [6]. This era also advanced security controls, which lead to implementation of point-to-point encryption between connection (SSL/TLS) and implementation of two-factor authentication [6]. Those systems were enhanced with firewalls and fraud detection systems [6]. On that era also security standards such as PCI DSS were created to protect payment data [6].

In the 2010s the state-sponsored and state-backed attacks were common [6]. Governments did develop different types of cyberweapons [6]. Major criminal hacking groups were committing attacks against giants and corporations. In this era ransomware attacks have commenced and there were worldwide campaigns to steal data from information systems [6]. Because the cyberattacks were becoming more sophisticated, it led to development more advanced security controls such as zero trust architectures in information systems, threat intelligence sharing, advanced IDS/IPS [6]. Also red/blue team exercises and guidelines for targeted incidents were introduced against cyberattacks [6].

In the 2020s cybercrimes were becoming more sophisticated and cybercrimes magnitude has led to tread to use artificial intelligence augmented attacks, mass-scale financial scams and supply chain breaches [6]. Generative AI has made it possible to amplify cyber threats [6]. Generative AI gives opportunity to make scalable social engineering attack and automating attack vectors [6]. Generative AI is dual use item, because of its ability to be offensive and defensive [31]. Cybercrimes are diminishing trust and stability of financial industry [32]. In this era there is a need to create research framework which integrates technical aspects, psychological and social aspects [33]. In this era there is need to create multidisciplinary approach for issues of cybercrimes [31]. In this multidisciplinary approach we should combine regulatory changes, global cooperation, public education and combining AI-powered detection for countering evolving cybercrime threats [31]. Still, for example in South Africa cybercrimes related to usage of common technology to commit frauds [34]. In previous research, it has been discovered that cybercrime accumulates according to the technical characteristics of cybercrime used by the same perpetrator for the same perpetrator [9, p. 205]. This is because committing certain types of cybercrime requires specialized expertise [9, p. 205]. Which means that same perpetrator can be involved in many same types of cybercrimes.

Defining perpetrators of cyberattacks

Cyberattacks targeting critical infrastructure and socially significant institutions in countries such as the United States are challenging to distinguish from criminals, state actors, or cyber terrorists in the United States, because the armed forces that protect critical infrastructure are dealing with entities that are difficult to distinguish from natural persons who are criminals, or whether a cyber attacker is a state actor or simply a terrorist subject to terrorist legislation [35, p. 37]. Those identified as cyberterrorists want to present themselves as admirable figures who are fighting as "soldiers" against, for example, the United States of America [35, p. 37]. However, they are treated as common criminals under the US criminal justice system [35, p. 37]. Cyberterrorists also do not generally enjoy the protection afforded to combatants under Rule 106 of the Geneva Convention (1949) and international agreements, which is why they are not legally considered combatants [36, p. 31–110]. Instead, they are subject to each country's own criminal law, which makes them nothing more than criminals [36, p. 31–110]. In general, terrorist groups do not meet the legal requirements for combatant status, uniforms, the display of weapons, and the structure of a military organization, so

that they can be treated as legitimate combatants [35, p. 37–38]. However, those groups of terrorists may in practice have the capacity to cause catastrophic damage, so their terrorist objectives do not change the nature of the crimes they commit, and those terrorist acts are simply criminal acts [35, p. 38].

State sponsored cybercrimes

The Korean Defense Research Institute has conducted research on this topic and collected information from 30,000 North Korean refugees on the cybercriminal capabilities and methods of the North Korean state [37, p. 22]. The results of the study confirm claims circulating in the media about North Korea's ability to carry out state-sponsored cybercrimes targeting banks and virtual currency institutions [37, p. 33]. North Korea began conducting cyberattacks with simple denial-of-service attacks, which progressed to email and website hacking, and eventually to complex cyberattacks that can be referred to as advanced persistent threat [37, p. 21, 23].

3. Method

Aim of the research

The is to examine are there convicted cybercriminal from Finnish court data between 2015-2019 which have made cybercrime which higher that the CCSTC that one. The CCSTC is developed in previous research [4]. The purpose is to make description of the advanced cybercriminals and describe each case-by-case study approach, which is developed by Nuutila [38, p. 165-172]. From the case-by-case study approach, I try to explain juridical aspects of the cybercrime, the environment of the cybercrime and characteristics of the cybercrime.

Interpretive research methodology

This research uses an interpretive research method [39]. The court data is analysed with qualitative content analysis [40]. The tables and explanation are created with conventional content analysis [40], which is extended with Nuutila [38, p. 165-172] case-by-case study approach. Narrative literature review is used for this article [15], to collect possible previous studies relating to technical advanced characteristics of cybercrimes. The literature is processed with discursive approach [16, p. 7]. In the result section and the discussion section meta-synthesis approach is used to create new knowledge from empirical research data (court data) and from the results of the literature review [41]. Meta-synthesis is used to make comprehensive interpretation of the literature review to discover what aspects should be examined from more “advanced cybercriminals”. After that when the empirical data sets of the N=365 is examined, which are from 2015-2019. We can created table(s) of the more “advanced cybercriminals”.

Cybercrime scale metrics

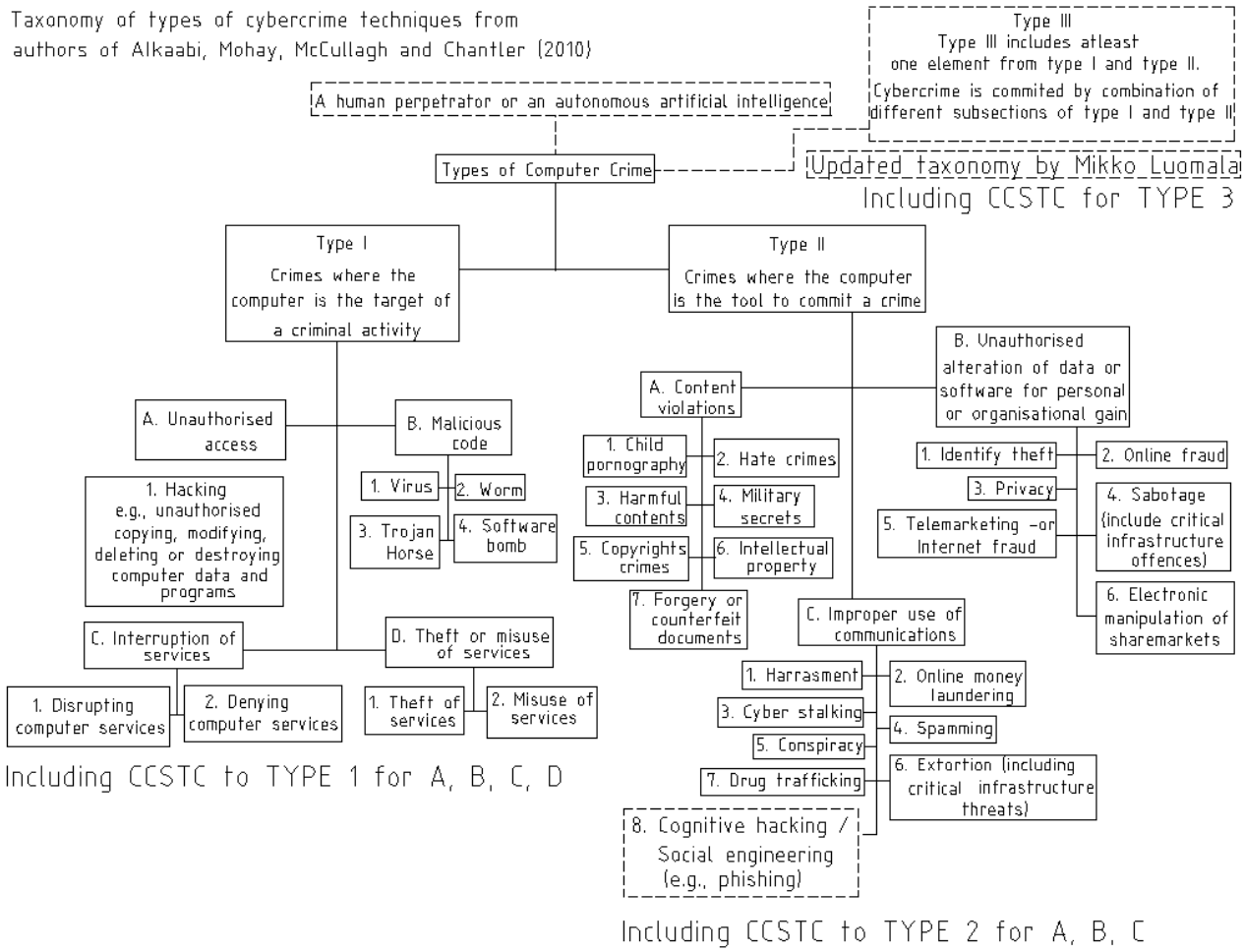
In this study, I will use the previous research [4] the cybercrime classification scale of a technique of cybercrime (CCSTC) for measuring more “advanced cybercrimes” from the research data. The CCSTC is extended with Nuutila’s [38, p. 165-172] case-by-case study approach. By doing this we can extended taxonomy of cybercriminality, show the evolution [42] of the cybercrime.

Research process and material

The research data is from Finnish Legal Register Centre. I was obtained by Jyri Paasonen. The research permission was handled at that time by Jyri Paasonen for the research data. The data set amount is N=365, which includes Finnish Criminal Code (39/1889) chapter 38 offences. One extra court document was requested from Western Uusimaa court.

Analysis

The court data N=365 was examined and it was done by naked eye observation method. The clauses from the documents where coded to an Excel file. The criterion of the CCSTC (Figure 2) was used to exclude cases which are not cybercrime, technique of cybercrime cannot be discovered from the court document and level one cybercrimes, which are regular usage of the computer, technology or software but offender has violated law.



Extension for Alkaabi et al., 2010 taxonomy by Mikko Luomala

The cybercrime classification scale of a technique of cybercrime (CCSTC).

Description of the definition of scoring of a technique of cybercrime

0 Not a cybercrime (no computer-related offence)

1 The cybercrime has been committed using technical techniques that are common to almost normal use of the technical system. Example to the explained in the text (logging in as if the victim would generally use the technical system or the act does not require narrow technical specialised knowledge, but can be learned by reading instructions, for example, resetting the password to the phone using the manufacturer's instructions).

2 The cybercriminal has used malware, or an algorithm created by another person.

3 The cybercriminal has written the malware or algorithm himself.

4 The cybercriminal has written the malware or algorithm and used the malware or algorithm created by another person (both).

5 No information on the technical modus operandi of the criminal act.

Fig. 2. The CCSTC is based on different definitions of researchers [22], [4].
The figure is from published research article of Luomala [4].
The figure was drawn with LibreCAD software.

Selection criterion was from the CCSTC the 2, 3 and 4. It led to selecting N=18 court cases (court documents). Please, see the Table 2 below.

Table 2. The cases which have technically advanced cybercrime (N=18) from N=365 court data dataset.

The CCSTC scoring number	The number of court cases relating to the CCSTC scoring number
Scoring number 2	1
Scoring number 3	15
Scoring number 4	2

Therefore, there are one cases where a cybercriminal has used malware, or an algorithm created by another person. Fifteen cases where a cybercriminal has written the malware or algorithm himself. Two cases where a cybercriminal has written the malware or algorithm and used the malware or algorithm created by another person (both). The content of the Table 2 will be examined in the results section. Duplicates will be filtered with simple python script, when the offender social security numbers are compared.

Ethical reflections

The Finnish law of *Act on the Publicity of Proceedings in General Courts* (370/2007) 1 § defines that court data is public. However, revealing information of individual deviance in the name of science possess social risks to the individual. To protect the identify of convicted individuals, I will not reveal them. It is part of ethics of a criminologist not to reveal identify of the research subjects [43, p. 42, 45], [44].

4. Results

I tried to explore whether there are any governmental officials or government sponsored cybercrime actors in the court dataset. There were five court documents and from those documents I was able to discover 6 different offenders, which were at the time of the crime as a public official. From Table 3 and by exploring a column of "Description of crime", we can see that most of the cybercrimes were a regular usage of the computer, where technology was an aid to commit a crime, which can be classified by other researchers cyber-enabled cybercrime [5], even though there are no hard barriers between cyber-depend crimes and cyber-enabled crimes [5]. I did not see any type III cybercrimes [4] from public officials, where technology would be itself a target and technology are aid for cybercrime. I did not discover that in the court dataset there would be any foreign government officials.

Table 3. The cases where cyber-offender is a public official (N=6).

Case	Reoffender* (yes or no)	Court level	Gender	Occupation	Description of crime	CCSTC	**	***
1	no	HO	female	public official	Opening unlawfully private mails of prisoners	0	0	1

2	no	KO	male	public official / police officer	Exploring unlawfully the police register	1	2	0
3	no	KO	female	public official / Social Insurance Institution of Finland	Exploring unlawfully registers of the social Insurance Institution of Finland	1	2	1
4	no	HO	male	public official	Exploring unlawfully register	5	4	1
5	no	HO	male	public official	Exploring unlawfully register	5	4	1
6	no	HO	male	public official	Exploring unlawfully register	5	4	1

*: I mean reoffending between time of 2015-2019 based on the N=365 court dataset

KO: District court [45], [46]

HO: Court of appeal [45], [46]

CCSTC: the cybercrime classification scale of a technique of cybercrime

** Pre-classification with Alkaabi et al. [22] metrics.[1]	None (Not a cybercrime): (0) / Computer as a target: (1) / Computer as a tool: (2) / computer as a target and computer as a tool: (3) / Cannot evaluate because tribunal documents are secret and methodology for criminal actions is not revealed or names of the victims: (4).
***:	Criminal charges dismissed = 0, a verdict was reached for the criminal charges = 1

Totally N=18 cases were discovered from the N=365 court dataset. There are two cybercrime offenders, which case progressed from district court to court of appeal. Two cases of the offenders from district court to court of appeal were interpreted as duplicates and only the court of appeal documents will be processed. Totally there is N=16 unique cybercrime offenders (Table 4).

Table 4. The cases which have technically advanced cybercrime (N=16).

Case	Reoffender* (yes or no)	Court level	Gender	Occupation	Occupation description	CCSTC	**
1	no	KO	male			3	2
2	no	HO	male			3	3
3	no	HO	male			3	3
4	no	KO	male			3	3
5	no	KO	male	A student	no information on the level of the education system	3	1
6	no	HO	male			3	1
7	no	KO	male			3	3
8	no	KO	male	A datanome student		4	3
9	no	KO	male	A student	No information on the student's grade level	3	3

[1] This measuring was used in pre-stage of the research, but the Alkaabi et al. metrics was developed during the research and coding the court data to have options of 0, 3 and 4. Alkaabi et al. (2010) used only “Computer as a target” or “Computer as a tool” classification.

10	no	KO	male	No information on the student's grade level	information about the student's level	3	3
11	no	KO	male	Management and administration in a company	electrical engineer	3	3
12	no	KO	male			3	3
13	no	KO	male			2	1
14	no	KO	male			3	3
15	no	KO	male			3	3
16	no	KO	male	School pupil, not gainfully employed		4	3

*: I mean reoffending between time of 2015-2019 based on the N=365 court dataset

KO: District court [45], [46]

HO: Court of appeal [45], [46]

CCSTC: the cybercrime classification scale of a technique of cybercrime

** Pre-classification with Alkaabi et al. [22] metrics.[2]	None (Not a cybercrime): (0) / Computer as a target: (1) / Computer as a tool: (2) / computer as a target and computer as a tool: (3) / Cannot evaluate because tribunal documents are secret and methodology for criminal actions is not revealed or names of the victims: (4).

Table 4 shows that from N=16 cases of 13 malware or algorithm to commit cybercrime was made, based on the CCSTC measurement. In one case (case 13) the cybercriminal used another person made malware or algorithm to commit the cybercrime. Also, in one case (case 16) the cybercriminal created own malware or algorithm and in addition used other person malware and algorithms to commit a cybercrime. All 16 cases technically advanced cybercriminals were males. In my observation, I did not find any evidence that artificial intelligence would be used to commit cybercrime by the offender between 2015-2019. Only two cases proceeded from district court to court of appeals.

In the 12 of cases the "technical device" was a target for the cybercrime and aid to commit a crime. Which means that the offenders commit cybercrime which targets the technology, and there are crimes where cybercrime is an aid to commit a crime. In the three of cases the technology was a target for crimes, which can be understood from engineering point of view "cybercrime". In one single case technology was an aid for crime.

In the court documents there was a minimal amount of data on what was the education level of the offenders. There were students, which education level was uncertain (not revealed in the documents), an electrical engineer which held some soft administrative position in a company and a datanome student. The datanome student seems to be studying in vocational education institution (EU second level education) and his studies related to information technology. In the Table 5, I am going to present the age of the perpetrators and victims of their cybercrimes.

[2] This measuring was used in pre-stage of the research, but the Alkaabi et al. metrics was developed during the research and coding the court data to have options of 0, 3 and 4. Alkaabi et al. (2010) used only "Computer as a target" or "Computer as a tool" classification.

Table 5. The ages of the perpetrators and victims of their cybercrimes (N=16).

Case	Age at the time of conviction	Total number of cybercrimes	Target of the cybercrime
1	41	1	To family and Social Services Office employee
2	39	1	To spouse
3	21	9	To companies, banks, and individuals
4	22	4	To businesses and banks
5	17	2	To the city and the education consortium
6	22	6	To Finnish authorities, municipalities, educational institutions, companies, and private individuals
7	23	5	To foundation, Social and Health Association, school, member of parliament, private individual
8	18	1	To a company
9	19	4	To businesses and individuals
10	27	3	To companies and individuals
11	42	1	To an individual
12	40	1	To an individual
13	19	5007	To individuals, authorities, companies, schools
14	26	2	To individuals
15	18	1	To the city
16	17	50704	To two foreign universities, a foreign association, a foreign company, and 50,700 computers around the world

In Table 5, we can see that none of the cybercriminals are over 50 years old. But that does not mean that in later their criminal carrier, they can be over 50 years old. In seems that technical advanced cybercrimes are either committed against individuals or multiple targets or in some cases thousands of the victims and organisations. However, we cannot generalise this from N=16 cases. In the Table 6, I am going to present the motives of perpetrators to commit cybercrimes.

Table 6. The motives of perpetrators to commit cybercrimes (N=16).

Case	The motive for committing the cybercrime
1	Reading private messages.
2	Reading emails and messages due to concerns about joint custody of children.
3	Testing systems, like-minded people spending time carrying out cyber attacks, interest in technology, joining forces to carry out denial-of-service attacks.
4	Like-minded people spend their time carrying out cyber attacks, participating in the practical implementation of denial-of-service attacks.
5	Teasing his teammates, trying out your offensive moves, wanting to attack the school,
6	Two deliberate DDOS attacks against private individuals, admits to having carried out denial-of-service attacks against authorities.
7	He told the district court that he wanted to study and explore the world of computers and therefore committed cybercrimes.
8	Interest and expertise in hacking and malicious software.
9	Let's see if data breach and fraud would succeed.

10	Revenge, because the victim had left the perpetrator (the defendant) and the breakup had been hard on him, as well as installing a keylogger on a shared computer owned by the defendant so that he could hack into the victim's social media accounts and email authentication.
11	Divorce and control over his own child (daughter), as well as the complexity of his life and greed for money, are also motives for the whole process.
12	The respondent wanted to monitor his daughter's phone calls due to divorce and to ensure that his daughter was being treated appropriately.
13	No information was found.
14	Interest in the victim's messages and monitoring of the former partner; the defendant and the victim had separated, and the defendant had taken the matter seriously and had been jealous, i.e., wanted to control the other person.
15	No information was found.
16	According to the investigating police, the act was clearly planned and carried out in such a way as to attract a lot of media attention. In this case, the aim was to make the stunt as visible as possible. The defendant says that it was mainly a matter of competing with other groups and thus showing off. The defendant's main goal was not to gain financial benefit, but rather to demonstrate his expertise in a certain reference group (interpretation of the district court).

As we can see that there are usually some personal motives behind the cybercrime. This reason is probable used to rationalise [47] their actions. I believe that like employees which infringe information security or nowadays cybersecurity policies of the company, goes thru similar rationalisation process [47]. Motivates shifted between different preparators relating to family issues, child custody issues, personal show off the technical skills of the perpetrator, social group internal issues to interest use technology to for hacking, which is view by the criminal justice system an act of crime. In the Table 7, I am trying to present the general information behind the cybercrimes, which may be influenced the perpetrator to commit cybercrimes.

Table 7. The general information of perpetrators to commit cybercrimes (N=16).

Case	General information
1	No general information was found.
2	No general information was found.
3	No general information was found.
4	No general information was found.
5	Individual do not have any income.
6	At the time of sentencing, the person had no secondary education or stable income. Just becoming independent.
7	Studied software and then visited various websites and information systems to explore.
8	The witness has assessed the perpetrator's skills in denial-of-service attacks and hacking as good. The perpetrator has also attempted to create malware, and material related to hacking was found in the perpetrator's possession. Among other things, the perpetrator has created malware himself.
9	The perpetrator's actions remained at the level of attempted fraud, but the data breach was successful thanks to a tool created by someone else.
10	The defendant had installed a keylogger program on the victim's computer, but did not use it to obtain the victim's login details, as he already knew them.
11	The respondent graduated as an electrical engineer in 2004. He works as a manager at a company that handles security and car parking systems, among other things. His area of expertise is more in management and administration than in technical matters. The defendant's computer skills are above average; he studied computer science at university in Iraq and has worked continuously with cameras and surveillance equipment. The plaintiff is not aware of any other means than spyware through which the defendant could have obtained information about the plaintiff's spouse and child.
12	No general information was found.

13	Writing malware (Trojan horse) and distributing it via a video service link to victims' computers from a download service, hijacking computers as part of an expanded denial-of-service attack network, and carrying out denial-of-service attacks.
14	No general information was found.
15	No general information was found.
16	Despite his young age, the defendant is an experienced computer programming enthusiast. The defendant has stated that he had become familiar with IRC chat rooms related to information security and technology several years before the alleged crimes, i.e., in his estimation, around 2010. He had gradually acquired knowledge and skills and got to know other people, even though he had not met them in person and knew very little about them. He had mainly engaged in theoretical discussions about data breaches online. The channel often discussed programming, and sometimes someone would copy a few lines of code and ask why it didn't work. On the discussion channels, he had also actively participated in hacking test servers in a controlled environment. This was called a "capture the flag" competition.

In Table 6, we can see that there are humane reasons behind the some of the criminal action. Then there is general information for what was reason to commit the cybercrime (Table 7). They have background story that they had either personal reasons to commit a cybercrime or there is interest in technology, which progressed in a group or other reasons to commit a cybercrime. In the Table 8, I am presenting the technical characteristics of cybercrime.

Table 8. The technical characteristics of cybercrime (N=16).

Case	**Technical characteristics of cybercrime (technical methods for the cybercrime)**
1	Spyware
2	SpyAgent
3	Dejabooter (DDOS), IP-killer (DDOS), HyperS (DDOS), Imminent monitor software and backdoor program which has a DDOS capabilities. Backdoor program for phishing bank credentials.
4	Hyper-S (DDOS), Booter (DDOS), RUDY (DDOS), Imminent monitor and backdoor program which has a DDOS capabilities.
5	Defiance Protocol software (DDOS), which was used for aiding and abetting in cybercrime.
6	Defiance Protocol software (DDOS).
7	Acunetix Web Vulnerability Scanner (vulnerability scanner), Havij 1.15 Pro (security testing tool, intrusion tool, and database theft tool).
8	booter.xyz ordered denial-of-service attacks.
9	Centry MBA tool
10	A key logger program that was acquired through Google and installed on the victim's computer.
11	Installation of the SuperSU root program, but the witness's statement shows, in the opinion of the district court, with sufficient reliability that the plaintiff's phone may have had spyware, even though no technical evidence of the program was found during the police search of the device. On the above grounds, the district court considers it technically possible that spyware was installed on the plaintiff's mobile phone, even though it was not detected in the police's subsequent investigation. The spyware program may have been Mspy. Although no spyware program was found on the plaintiff's mobile phone, there is ample circumstantial evidence in the case of the existence and use of spyware. The District Court considers that the complainant's statement, the supporting written evidence, the statement of witness A, and, in part, the defendant's own statement constitute sufficient evidence of the conduct described in the indictment against the defendant. On the basis of the above, the District Court finds that there is no reasonable doubt that the defendant installed spyware on the plaintiff's phone and thereby gained access to messages and their contents between the plaintiff and a third party. The defendant's actions meet the criteria for a violation of the confidentiality of communications.
12	Automatic Call Recorder

13	boot.php and windows-api/api-attack.php creating Trojan malware for him self and creating www.cyb3rium.net/cyber and nbooter.net portals.
14	The Best Keylogger
15	SQLi Dumper
16	Own malware (jews.exe, dragondildo.exe) zodiak bot program (wincpa.exe), servers, Acer Aspire computer, computer browser, python scripts (ap.py), command prompt, registered domains in the respondent's name (fkn.ddos.cat and loki. zf0.org), Skype (sharing of usernames)

If we look the Table 8. It is interesting to discover that some of the preparators has truly written they own malware, algorithms or created online service for the malwares (case 13, case 16). Thus, some of the preparators used some other person created tool or software for their cybercriminal activities. Some name of the tool suggested that they are created for cybersecurity testing, but they were used illegally with consent of the victims or justification from the law. That kind of action is very close to regular usage of the computer, but technology is used actions which violates the law. In previous study, we discovered that some cybercrimes are technically trivial [1], but they violate criminal code. For example, in the case 12, where "Automatic Call Recoder" was used to spy on victim. That could be classified as CCSTC scale as level one action, because the preparator is using a software for illegal actives, which do not have consent of the victim. But I end up classified to in CCSTC as level 3 cybercrime, because he installed the software and configured it. In addition, we have cybercriminal (case 16; Table 4) which create their own malware, software and also use other person tools and solutions for their cybercriminal actions. In the Table 9 I will explain, what was the court interpretation for what cybercrime did do actually or in technical sense.

Table 9. The court interpretation of what cybercrime actual did at technical level (N=16).

Case	Court Interpretation
1	Installing spyware and reading the victim's messages
2	Installing spyware and reading the victim's messages
3	Denial-of-service attacks against banks, extortion messages, unauthorized use of bank credentials, use of backdoor programs
4	Aiding and abetting denial-of-service attacks, denial-of-service attacks, and attempted extortion
5	
6	
7	Scanned pages and hacked into websites, stole a user ID database, carried out a denial-of-service attack using a tool, sent defamatory messages to websites, and wrote a defamatory message to a website using the victim's user ID.
8	Denial-of-service attack against an educational institution maintained by a company, possession of information network tools (passwords and email addresses belonging to others) and executable files (which turned out to be malware, e.g., a keylogger program), possession of material that violates a child's sexual integrity
9	
10	The defendant had installed spyware (key logger) on a shared computer that his former partner also used. He had logged in using the victim's user IDs, which he already knew, to the victim's social media accounts, e-mail accounts, university student accounts, and sports booking system, changed the victim's account passwords, sent messages in the victim's name using the accounts, and committed fraud using the victim's personal data to make online purchases. Installing spyware and reading the victim's messages
11	
12	The perpetrators knew each other. The defendant had installed the Automatic Call Recorder (Android) program on the victim's phone in order to listen to the victim's calls. It remained unclear whether the defendant listened to his daughter's calls, but the charge was still upheld.

13	Writing malware (Trojan horse) and distributing it via a video service link to victims' computers, which the victims had downloaded from a download service in good faith believing it to be safe, and hijacking computers as part of an expanded denial-of-service attack network and carrying out a denial-of-service attack.
14	The defendant had installed spyware on his own laptop, which was given to the victims to use, and was able to log into his former partner's Facebook and Hotmail email accounts. According to a police witness, the other victim's accounts had been accessed 202 times, but the exact number cannot be determined. The defendant had logged into his former partner's Facebook account and posted a threat against himself in the victim's name, as well as into the victim's H&M customer account. The District Court considers it contradictory whether the defendant obtained the victims' passwords and user IDs through a keylogger program or whether they were stored in a browser from which it is possible to access the victims' accounts. Some of the logins were made through an anonymous service on a computer used for logging in. The District Court considers that the program (The Best Keylogger) has been specifically developed to be suitable for eavesdropping on passwords or unauthorized interception of messages to prevent the IP address from being recorded.
15	By using the SQLi Dumper program, the defendant unlawfully gained access to files and data stored in the information system, i.e., user IDs, passwords, and email addresses. In count 2 of the indictment, the defendant published this information on a public discussion forum.
16	The defendant has committed eight crimes. He hacked into 50,700 computers using malware, some of which he created himself and some of which he obtained ready-made. The defendant, together with a criminal hacker group (Hack the Planet), hacked into 50,700 computers around the world. The defendant created a botnet (CFNET) from the hijacked computers together with the Hack the Planet group and has been developing the botnet. CFNET was used for denial-of-service attacks. The defendant manipulated the DNS addresses of the victims' websites and redirected traffic to another address. The defendant copied 7 GB of email traffic and messages for himself. The defendant carried out a single data breach into the database of an American company. The defendant had laundered criminal money obtained by cybercriminals through a bitcoin service. The defendant had passed on payment instrument details (credit card details). The defendant had used stolen credit cards to make purchases for himself from online stores.

In table 9, we can see that court made in some cases own interpretation what cybercrime did on in technical level, or how the preparator used technology to commit cybercrime. From the text we can interpret that preparators of cybercrime either use or/and create artefacts, which they need for committed cybercrime against technology or/and technology is an aid for criminal activity. From court document, we can see a little about the life path to crime and how the evolution of skills for committing a cybercrime have evolved. We can conclude that when we compare finish police statistic (Table 10) to this empirical snapshot (N=16), it is obvious that not all reported cybercrimes end up to court stage.

Table 10. The total amount of reported cybercrimes to Finnish Police in Finland. The number are from the article of "*Kyberrikokset tuomioistuimissa – tarkastelussa rikoslain 38 luvun mukaiset tieto- ja viestintärikokset*" [1, p. 982].

Year	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**
Total	717	976	986	1179	1275	1510	4455	5020	4854	5202

From the literature review of this study, we know that not all technical advanced cybercrime end to court system. This argument is established by comparing the literature review proposed advanced cybercrimes actual crimes which are processed in Finnish courts (Table 8). Based on the CCSTC metrics, I did not see any government official or foreign governments technical advanced cybercrimes in the empirical data between 2015-2019. All of this observation enhance that view the criminal justice system has this funnel effect: there is dark numbers of cybercrimes [48, p. 106], [49], which are not reported to the police, and cybercrime which are reported to the police, only narrowing amount of the end up to the court and it is not automatic that technically advanced cybercrime are processed in the court level.

Even I did discover that there are cybercrimes were malware were created and other software to commit cybercrime, and there were thousands of victims (case 16). From international literature review perspective, it can be argued that between 2015-2019 Finnish court system did not process those technical cybercrimes which can be portrayed as technical sophisticated high-tech cybercrimes. I did not observer any artificial intelligence assisted cybercrimes in the period of the 2015-2019. In the Table 11 I will the legal paragraph for the criminal offence and sentences.

Table 11. The criminal offense and sentences from the Finnish criminal code (39/1889)[3]

Case	Legal paragraph for the cybercriminal offence	Given sentences by the court
1	RL 34:9a endangerment of data processing, RL 38:3 Violation of the secrecy of communications	60 of unit fines
2	RL 38:4 Aggravated violation of the secrecy of communications	30 days of conditional imprisonment
3	RL 38:7a Interference with an information system (as a young offender and seven counts of the offence), RL 31:3 attempted extortion (as a young offender), RL 31:4 Attempted aggravated extortion (as a young offender), RL 34:9a Endangerment of data processing (as a young offender), RL 37:8 Means of payment fraud, RL 28:7 Unauthorised use (young offender), RL 36:1 Fraud (young offender)	1 year and 4 months of conditional imprisonment, 50 hours of ancillary community service, 1 year and 3 months of monitoring sentence
4	RL 38:7a Abetting to interference with an information system (as a young offender and two counts of the offence), RL 38:7a Interference with an information system (as a young offender), RL 31:4 Attempted aggravated extortion (as a young offender)	3 months of conditional imprisonment, 1 year and 3 months of monitoring sentence
5	RL 38:7a Interference with an information system (as a young offender), RL 38:7a Incitement interference with an information system (as a young offender)	Punishment is waived
6	RL 38:7a Interference with an information system (six counts of the offence)	90 of unit fines
7	RL 34:9b Possession of a data system offence device, RL 28:7 Unauthorised use (five counts of the offence), RL 38:7a Interference with an information system, RL 38:8 Unlawful access to an information system (four counts of the offence)	100 of unit fines
8	RL 38:7a Interference with an information system (as a young offender), RL 34:9b Possession of a data system offence device (as a young offender), RL 17:19 Possession of a sexually obscene image depicting a child (as a young offender)	45 of unit fines
9	RL 38:8 Abetting unlawful access to an information system (as a young offender), RL 36:1 Attempted fraud (young offender)	35 of unit fines
10	RL 28:7 Unauthorised use, RL 38:7a Interference with an information system, RL 36:1 Fraud	90 of unit fines
11	RL 38:3 Violation of the secrecy of communications	60 of unit fines
12	RL 38:3 Violation of the secrecy of communications	Punishment is waived
13	RL 38:8a 1500 counts of aggravated unlawful access to an information system, RL 38:7b Aggravated interference with an information system, RL 38:8a 3500 counts of aggravated unlawful access to an information system, RL 34:9a Endangerment of data processing	1 year of conditional imprisonment

[3] Unofficial translations of Finnish Criminal Code (39/1889): https://www.finlex.fi/en/legislation/translations/1889/eng/39-001

14	RL 38:8a aggravated unlawful access to an information system, RL 38:4 2 counts of Aggravated violation of the secrecy of communications	3 months of conditional imprisonment
15	RL 38:8 Unlawful access to an information system (as a young offender), RL 34:9a Endangerment of data processing (as a young offender)	30 days of conditional imprisonment
16	RL 38:8a 50700 counts of aggravated unlawful access to an information system, RL 38:5 Interference with communications (as a young offender), RL 38:4 Aggravated violation of the secrecy of communications (as a young offender), RL 38:8 Unlawful access to an information system (as a young offender)	2 years of conditional imprisonment

Abbreviation: *RL* means in Finnish "rikoslaki (39/1889)" and in English "Criminal code (39/1889)"

We can see from the Table 11 no unconditional imprisonment sentence was given for the technically advanced Finnish cybercriminals. If we look the criminal code and specially those cybercrimes which have prefix of aggravated. The courts did give either fines or conditional imprisonment for those actions. In addition, we can see that some of the cybercrimes are note listed in the Chapter 38 of Finnish Criminal code, but they are listed in other crime code chapters. When the technical technique for crime was done with the technology. This means that statutory definition for the different cybercrimes the interpretation by court to different criminal codes, which have neutrality for technique of the crime. This gives indication that cybercrimes can be part of "the traditional" crimes, because of the digitalisation.

Summarising the results

The sixteen cases show that there are indeed technological advanced cybercrimes. The number of the victims can be counted in ten thousand or in thousands. The perpetrators can have some sort of technical education, but not always. It was interesting that all perpetrators of the sixteen cases are men, but no females. The motivations to commit cybercrime varied either related to personal life issues such as divorce, revenge, teasing, interest to read private messages, learning how to use technology to do cyberattacks or showing off to their group that they can do a cybercrime. The tools for cybercrime were either some else made tools, or they own made tool or combination of both. It can be said that cybercrime is technologically advanced, if there are own malware or tools created. There was a cybercrime case where about 50704 victims, and cybercrime included actions where technology was a target to cybercrime and technology also was an aid to crime. It was done by creating own algorithms and using other tools for cybercrimes. This is advanced cybercrime. There was no unconditional imprisonment given for any of the offenders. There were either fines given, or the sentence was waived, or conditional imprisonment was given. There is one case where an ancillary community service was sentenced with conditional imprisonment and monitoring sentences.

From court documents, the defendants' and the court's interpretations of reasons to commit cybercrime varied. Individuals sometimes say their own emotional reasons to committing a cybercrime, and the courts make a legal interpretation where they just conclude that specific classification of criminal code. The court's perspective is to look at cases from their legal paradigm, and judges use descriptive language to interpret the actions of the perpetrators.

5. Discussion

My study shows that in international literature high-tech cybercrimes do not automatically end up in a criminal justice system. This empirical study gives answers to RQ that there is technically

advanced cybercriminal in Finland, when we measured the characteristics of cybercrime with the CCSTC metrics. It is technologically advanced cybercrime, if there are own malware or tools created. There was a case where number of victims was about 50704. One of the cases included actions where technology was a target to cybercrime and technology also was an aid to the crimes, and it included creating own algorithms and using other tools for cybercrimes. This raises question that how much cognitive hacking (Figure 2) there was, because cognitive hacking is becoming a growing and pervasive threat [50]? I did not see any artificial intelligence assisted with cybercrimes. However, that does not mean that they have not occurred. In These empirical observations raise new hypotheses that show how effective the criminal justice system is to detect and control technically advanced cybercriminals. In addition, can we start asking questions that are some other security controls such as private cybersecurity sector actual controls cybersecurity, cybercrime or even cyberwarfare issues?

It was also interesting to discover that in the dataset there are government officials which have done cybercrime [4], their technique for cybercrimes was not technically advanced, it was a regular usage of computer where public officials just violated data privacy by looking information which they should not explore (Table 3). It is also interesting to discover that between 2015-2019 there was no foreign government official convicted of any cybercrime in the dataset. It was interesting that all perpetrators of the sixteen cases are men, but no females. Some international research proposes that cybercrimes are usually done by male gender than female [51]. But this discussion needs taxonomy type discussion, because cyber-dependent crimes might be male dominated, because individuals which likes to create malwares, malicious code might only accept society persons which they share their values and gender [51]. In computer science there are lower number of females as students [52]. "*Females can be socialized to view computers as masculine, and thus less interested in choosing computer field. A meta-analysis has shown that gender difference on attitudes toward computers is largest in among high school students*" [53, p. 185]. In some technical orient societies females are treated differently than males and that may discourage them from continuing in society and the learning and sharing do not occur [53]. Therefore, this limits female individuals do not get opportunity to learn how technically advanced cybercrimes are done from male peers. However, this might change in future because nothing is certain than uncertain.

By looking at different tables, it can be interpreted that developing technologically advanced cybercrime is not tied to certain education, even though the interest in technology can be discovered in some cases. It was interesting to discover that all offenders were males. However, making generalization from that discovery we could make the ecological fallacy [54, p. 327] because it is commonly recognised that male gender makes most of the crimes [55]. By looking at victims which the advanced offenders have selected, in some cases motivation was revenge or some other personal issue where offender and victim know each other's (Table 5; Table 6). However, in cases where motivation was to try technology or take general revenge on society, the offenders just selected visible targets like companies and public institutions (Table 5; Table 6). Moreover, the judges of courts and offenders interpret differently what was motivation for cybercrime (Table 6; Table 7; Table 9).

In addition, looking at the tools or they own created algorithms or modules for cybercrimes, they are heterogeneous. There are different DDOS tools, spyware variation modules, keylogger, regular sound recording software and very specialized malware (Table 8). Also, the sentences of cybercrimes vary, it is either fine or non-mandatory imprisonment or some other rare ancillary community service and monitoring sentence (Table 11).

Therefore, the qualitative data shows and the qualitative analysis that their common nominators like ability to use technology for crime, when an emotional reason to commit such act is born in the mind, the victims are selected either personal agenda reasons for gaining control over other person or general frustration or upset feeling to the society. They might be in the court stage rationalization of their own actions, like when employees rationalize their violation of information security policy [56]. The basic discovery is that technological advanced cybercrimes are not just type I [4] cybercrimes

(cyber-dependent) [5], but also type II [4] cybercrimes (cyber-enabled) [5] where technology is aid for crime. In multiple cases, there was a hybrid form of type I and type II cybercrime, which gives indication that it is myth that technology is just crime against technology. This study show that type III cybercrime "computer as a target and computer as a tool" [4] is empirical true phenomena and classification.

Implications of results to science

This empirical study show that, yes indeed the criminal justice system does catch some technically advanced cybercriminals. However, based on the empirical data from 2015-2019 it not automatic that foreign government sponsored cybercriminals or other technologically high-tech cybercriminal would be detained. This study show that we need better taxonomies to understand life path of cybercrime and taxonomies to classify development skill of cybercrime. Without proper theories, metrics and taxonomies it is difficult create definitions to explaining this ccharacteristics of cybercrime. Those taxonomies are needed to supplement the funnel effect (Table 10; Table 3; Table 4), which happen in the criminal justice system. When we look at Table 10 and Tables 3-4, we can see that not all cybercrimes which are reported to the police end up in the courts. This is indeed a funnel effect that narrows the number of cybercrimes that end up in the criminal justice system, which creates abductive support for the development of the funnel theory of cybercrimes. Quality and technological advancement of the cybercrimes varied if we use the Luomala's CCSTC metrics. This study shows that there is indeed a funnel effect that narrows the number of cybercrimes that end up in the criminal justice system, which creates abductive support for the development of the funnel theory of cybercrimes. That is empirically important premises for developing future theories for science of criminology, cybercriminology and security studies.

Implications of results to practice

The practitioners of cybercrime prevention are interested how we can mitigate cybercrimes. We show the practitioners that the criminal justice system has limited capacity to detect cybercrimes and control them. Also, as we can see from the literature review the cybercrimes are one issue, which handled by the criminal justice system. We have cyber-attacks and cyberwarfare which relate to same phenomena of the cybersecurity issues. Different actors in the world participate detection and control of "cybersecurity issues", which are defined in different system either cybercrime, or cyberattack or cyberwarfare. From this study, it should be understood that n=16 analysis does not represent all world advanced cybercrimes; it only represents what the Finnish courts have processed between 2015 and 2019.

Limitations

This study dataset is from 2015-2019 and total amount cases is N=365. From the data set, I did select N=16 cases. We can carefully generalise this study results, but we need to understand that the data is 6 years old. This study is just a perspective on what has been ended in court proceedings, and it is not a holistic way of understanding all advanced cybercrimes. The previous criminological studies show that different human societies and professions have different interpretations of the amount of criminality [57, p. 9-10]. The reasons are just that they only know part of the criminality which they are detecting and processing. Every research has errors [43, p. 8]. This study is an interpretation of the documents of the courts. Some other researchers might interpret the same data differently [58].

Future directions for research

In future studies, we should study big data where might be dark figure of cybercrime and compare other nations court data to each other to create much more holistic picture what kind of technically advanced cybercrimes are processed in the courts. Also, we should create taxonomies which have development of the technical skill described in trends of cybercrime. Addition, the role of cognitive hacking and creating tools for cybercrime should be examined, because cognitive hacking is not a trivial action. Also, how usage of artificial intelligence is used in possible cybercrimes?

6. Conclusion

In 2015-2019 there was from N=365 dataset 16 technically advanced cybercrime cases. Those advanced cybercrime cases were discovered with the CCSTC metrics. In 2015-2019 it seems to be rare that technically advanced cybercrime ends up to the criminal justice system. Between 2015-2019 there was no foreign government official convicted of any cybercrime in the dataset, only a few Finnish public officials were convicted with a regular usage of computer for cybercrime in CCSTC 1 level. It is not automatic that advanced cybercrimes end up to courts. This study shows that there is indeed a funnel effect that narrows the number of cybercrimes that end up in the criminal justice system, which creates abductive support for the development of the funnel theory of cybercrimes.

Acknowledgements

I would like to give honourable regards to Jyri Paasonen from the University of Vaasa, School of Management, Public Law for the research data. I would also give regards for Tero Vartiainen for commenting this article. I would like to give regards for Jyri Naarmala for commenting this article and helping development of the Figure 1.

Funding

No funding has been received for this study.

References

[1] J. Paasonen, M. Aaltonen, and M. Luomala, “Kyberrikokset tuomioistuimissa – tarkastelussa rikoslain 38 luvun mukaiset tieto- ja viestintärikokset,” *Defensor Legis*, vol. 4, pp. 966–987, Dec. 2021, Accessed: Mar. 11, 2022. [Online]. Available: https://www.edilex.fi/defensor_legis/250670013

[2] J. Paasonen and M. Luomala, “Tietosuojan viranomaisvalvonnan ja seuraamusjärjestelmän kehitys — tarkastelussa tietosuojavaltuutetun ja seuraamuskollegion päätöksiä vuosilta 2018–2022,” *Defensor Legis*, no. 1, pp. 40–66, 2024, Accessed: Jul. 23, 2024. [Online]. Available: https://www.edilex.fi/defensor_legis/1001220003

[3] M. Luomala, T. Vartiainen, and J. Paasonen, “Suomen energia-alan kyberturvallisuuden tila vuonna 2021,” Vaasa, 2021. Accessed: Aug. 25, 2025. [Online]. Available: https://urn.fi/URN:ISBN:978-952-395-085-6

[4] M. Luomala, “A New Version of Cybercrime Taxonomy: Empirical Evidence from Finland,” *International Journal of Information Security and Cybercrime*, vol. 14, no. 1, pp. 37–62, Jun. 2025, doi: 10.19107/IJISC.2025.01.03.

[5] J. Lusthaus, T. J. Holt, M. Levi, E. Kleemans, and E. R. Leukfeldt, “The evolution of Nigerian cybercrime: Two case studies of UK-based offender networks,” *Eur. J. Criminol.*, vol. 22, no. 4, pp. 557–577, Jul. 2025, doi: 10.1177/14773708251329695.

[6] M. Abdullah, M. M. Nawaz, B. Saleem, M. Zahra, E. binte Ashfaq, and Z. Muhammad, “Evolution Cybercrime—Key Trends, Cybersecurity Threats, and Mitigation Strategies from Historical Data,” *Analytics*, vol. 4, no. 3, p. 25, Sep. 2025, doi: 10.3390/analytics4030025.

[7] G. Calcar, P. Sund, and M. Tolvanen, “Cybercrime, Law and Technology in Finland and Beyond,” Tampere, 2019. Accessed: Apr. 06, 2022. [Online]. Available: https://www.theseus.fi/bitstream/handle/10024/166377/POLAMK_rap133_web.pdf?sequence=2&isAllowed=y

[8] A. Graham, T. C. Kulig, and F. T. Cullen, “Willingness to report crime to the police: Traditional crime, cybercrime, and procedural justice,” *Policing: An International Journal*, vol. 43, no. 1, pp. 1–16, Apr. 2019, doi: 10.1108/PIJPSM-07-2019-0115.

[9] M. W. Kranenbarg, “Cyber-offenders versus traditional offenders - An empirical comparison ,” Doctoral thesis, Vrije Universiteit Amsterdam, Amsterdam, 2018. Accessed: May 31, 2022. [Online]. Available: https://research.vu.nl/en/publications/cyber-offenders-versus-traditional-offenders-an-empirical-compari

[10] J. K. A. Kivivuori, M. Aaltonen, M. J. Näsi, K. E.-M. Suonpää, and P. M. Danielsson, *Kriminologia: Rikollisuus ja kontrolli muuttuvassa yhteiskunnassa*. Suomi: Gaudeamus, 2018.

[11] Y. Li and Q. Liu, “A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments,” *Energy Reports*, vol. 7, pp. 8176–8186, Nov. 2021, doi: 10.1016/j.egyr.2021.08.126.

[12] A. Ali, M. Shah, M. Foster, and M. N. Alraja, “Cybercrime Resilience in the Era of Advanced Technologies: Evidence from the Financial Sector of a Developing Country,” *Computers*, vol. 14, no. 2, p. 38, Jan. 2025, doi: 10.3390/computers14020038.

[13] J. Nagathota, J. Kethar, and Ph. D. , S. P. Gochhayat, “Effects of Technology and Cybercrimes on Business and Social Media,” *Journal of Student Research*, vol. 12, no. 4, Nov. 2023, doi: 10.47611/jsr.v12i4.2284.

[14] L. K. C. Cotrina *et al.*, “Cyber Crimes: A Systematic Review of Evolution, Trends, and Research Approaches,” *Journal of Educational and Social Research*, vol. 14, no. 5, p. 96, Sep. 2024, doi: 10.36941/jesr-2024-0124.

[15] B. N. Green, C. D. Johnson, and A. Adams, “Writing narrative literature reviews for peer-reviewed journals: secrets of the trade,” *J. Chiropr. Med.*, vol. 5, no. 3, pp. 101–117, 2006, doi: 10.1016/S0899-3467(07)60142-6.

[16] A. Salminen, *Mikä kirjallisuuskatsaus? : johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin*, Toinen painos., vol. 62. Vaasan yliopisto, 2011. Accessed: Jan. 14, 2024. [Online]. Available: https://urn.fi/URN:ISBN:978-952-476-349-3

[17] IMF, “Global Financial Stability Report,” Washington, DC, USA, 2024. Accessed: Oct. 13, 2025. [Online]. Available: https://www.imf.org/en/Publications/GFSR/Issues/2024/10/22/global-financial-stability-report-october-2024

[18] J. Nagathota, J. Kethar, and Ph. D. , S. P. Gochhayat, “Effects of Technology and Cybercrimes on Business and Social Media,” *Journal of Student Research*, vol. 12, no. 4, Nov. 2023, doi: 10.47611/jsr.v12i4.2284.

[19] Y. Li and Q. Liu, “A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments,” *Energy Reports*, vol. 7, pp. 8176–8186, Nov. 2021, doi: 10.1016/j.egyr.2021.08.126.

[20] G. Higgins, *Cybercrime – An Introduction to an Emerging Phenomenon*, 1st ed. McGraw-Hill Companies , 2010.
[21] David. Wall, *Cybercrime : the transformation of crime in the information age*. Cambridge: Polity Press, 2007. Accessed: Jul. 17, 2026. [Online]. Available: https://discovered.ed.ac.uk/discovery/fulldisplay/alma9916181813502466/44UOE_INST:44UOE_VU2
[22] A. Alkaabi, G. Mohay, A. Mccullagh, and N. Chantler, "Dealing with the Problem of Cybercrime," in *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, Mar. 2010, pp. 1–18. doi: 10.1007/978-3-642-19513-6_1.
[23] M. Weulen Kranenbarg, "Cyber-Dependent Crime Versus Traditional Crime: Empirical Evidence for Clusters of Offenses and Related Motives," 2021, pp. 195–216. doi: 10.1007/978-3-030-60527-8_12.
[24] K.-L. Payne, A. Russell, R. Mills, K. Maras, D. Rai, and M. Brosnan, "Is There a Relationship Between Cyber-Dependent Crime, Autistic-Like Traits and Autism?," *J. Autism Dev. Disord.*, vol. 49, no. 10, pp. 4159–4169, Oct. 2019, doi: 10.1007/s10803-019-04119-5.
[25] E. R. Leukfeldt, R. J. (Raoul) Notté, and M. (Marijke) Malsch, "Exploring the Needs of Victims of Cyber-dependent and Cyber-enabled Crimes," *Vict. Offender.*, vol. 15, no. 1, pp. 60–77, Jan. 2020, doi: 10.1080/15564886.2019.1672229.
[26] D. Maimon and E. R. Louderback, "Cyber-Dependent Crimes: An Interdisciplinary Review," *Annu. Rev. Criminol.*, vol. 2, no. 1, pp. 191–216, 2019, doi: 10.1146/annurev-criminol-032317-092057.
[27] M. Watney, "Exploring Cyber Fraud within the South African Cybersecurity Legal Framework," in *European Conference on Information Warfare and Security, ECCWS*, 2024, pp. 628–634. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-105021464165&partnerID=40&md5=cba0703acf3a2b3aaded9bd253496ff8
[28] L. K. C. Cotrina *et al.*, "Cyber Crimes: A Systematic Review of Evolution, Trends, and Research Approaches," *Journal of Educational and Social Research*, vol. 14, no. 5, p. 96, Sep. 2024, doi: 10.36941/jesr-2024-0124.
[29] A. Kumari and S. Bhushan, "Cyber-crime the high-tech criminals and technology," *UGC Care Journal*, vol. 44, no. 1, pp. 24–28, Apr. 2022, Accessed: Oct. 15, 2025. [Online]. Available: https://www.researchgate.net/publication/358347560_CYBER-CRIME_THE_HIGH-TECH_CRIMINALS_AND_TECHNOLOGY
[30] W. S. Admass, Y. Y. Munaye, and A. A. Diro, "Cyber security: State of the art, challenges and future directions," *Cyber Security and Applications*, vol. 2, p. 100031, 2024, doi: 10.1016/j.csa.2023.100031.
[31] T. J. Luu and B. M. Samuel, "Exposing the Impact of GenAI for Cybercrime: An Investigation into the Dark Side," 2025. [Online]. Available: https://arxiv.org/abs/2505.23733
[32] O. E. Akinbowale, H. E. Klingelhöfer, and M. F. Zerihun, "Analysis of cyber-crime effects on the banking sector using the balanced score card: a survey of literature," *J. Financ. Crime*, vol. 27, no. 3, pp. 945–958, Oct. 2020, doi: 10.1108/JFC-03-2020-0037.
[33] L. K. C. Cotrina *et al.*, "Cyber Crimes: A Systematic Review of Evolution, Trends, and Research Approaches," *Journal of Educational and Social Research*, vol. 14, no. 5, p. 96, Sep. 2024, doi: 10.36941/jesr-2024-0124.
[34] L. Mpuru and C. Kgoale, "Recognizing the Evolving Cybercrime Threats in South Africa," *African Security*, pp. 1–25, Jun. 2025, doi: 10.1080/19392206.2025.2515302.
[35] P. B. Kraska, *Militarizing the American criminal justice system : the changing roles of the Armed Forces and the police*. Boston: Northeastern University Press, 2001. Accessed: Oct. 15, 2025. [Online]. Available:

https://onesearch.library.wwu.edu/discovery/fulldisplay/alma99100302440001451/01ALLIANCE_WWU:WWU
[36] Department of the air force, “International law-the conduct of armed conflict and air operations,” *AF PAMPHLET 110-31*, Washington DC, pp. 31–110, 1976. Accessed: Dec. 06, 2022. [Online]. Available: https://www.justsecurity.org/wp-content/uploads/2022/02/AFP-110-31-US-AIr-Force-INTERNATIONAL-LAW-THE-CONDUCT-OF-ARMED-CONFLICT-AND-AIR-OPERATIONS-just-security.pdf
[37] H. Boo, “AN ASSESSMENT OF NORTH KOREAN CYBER THREATS,” *J. East Asian Aff.*, vol. 31, no. 1, pp. 97–117, 2017, Accessed: May 08, 2022. [Online]. Available: http://www.jstor.org/stable/44321274
[38] A.-M. Nuutila, *Rikosoikeudellinen huolimattomuus*. Helsinki: Lakimiesliiton kustannus, 1996.
[39] G. Walsham, “Doing interpretive research,” *European Journal of Information Systems*, vol. 15, no. 3, pp. 320–330, Jun. 2006, doi: 10.1057/palgrave.ejis.3000589.
[40] H.-F. Hsieh and S. E. Shannon, “Three Approaches to Qualitative Content Analysis,” *Qual. Health Res.*, vol. 15, no. 9, pp. 1277–1288, 2005, doi: 10.1177/1049732305276687.
[41] Noah, “A systematic approach to the qualitative meta-synthesis,” *Issues In Information Systems*, vol. 18, no. 2, 2017, doi: 10.48009/2_iis_2017_196-205.
[42] R. C. Nickerson, U. Varshney, J. Muntermann, and H. Isaac, “Taxonomy development in information systems: Developing a taxonomy of mobile applications,” *ECIS 2009 Proceedings*, vol. 388, 2009.
[43] F. E. Hagan, *Research Methods in Criminal Justice and Criminology*, 6th ed. Boston, MA: Pearson education, Inc., 2003.
[44] J. D. Douglas, “Major Tactics of Investigative Research,” in *Focus: Unexplored Deviance*, C. H. Swanson, Ed., CT: Dushkin: Guilford, 1978, pp. 206–221.
[45] Tuomioistuinlaitos, “Courts.” Accessed: Mar. 19, 2026. [Online]. Available: https://tuomioistuimet.fi/en/index/tuomioistuinlaitos/tuomioistuimet.html
[46] K. J. Korpela, “A table of common abbreviations,” in *Handbook of Finnish, 2nd edition*, 2026. Accessed: Mar. 19, 2026. [Online]. Available: https://jkorpela.fi/finnish/all.html
[47] Siponen and Vance, “Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations,” *MIS Quarterly*, vol. 34, no. 3, p. 487, 2010, doi: 10.2307/25750688.
[48] E. A. Khodzhaeva, “Estimating Validity of Official Crime Statistics via Victimization Surveys (RCVS 2018, 2021): Case of Online Property Crime,” *The monitoring of public opinion economic and social changes*, no. 1, Mar. 2024, doi: 10.14515/monitoring.2024.1.2438.
[49] J. Curtis and G. Oxburgh, “Understanding cybercrime in ‘real world’ policing and law enforcement,” *The Police Journal: Theory, Practice and Principles*, p. 0032258X2211075, Jun. 2022, doi: 10.1177/0032258X221107584.
[50] R. Adefabi *et al.*, “Cognitive Hacking and Social Engineering in Healthcare: Exploiting Human Behaviour,” *European Conference on Cyber Warfare and Security*, vol. 24, no. 1, pp. 1–8, Jun. 2025, doi: 10.34190/eccws.24.1.3337.
[51] A. Hutchings and Y. T. Chua, “Gendering cybercrime,” in *Cybercrime Through an Interdisciplinary Lens* , T. Holt, Ed., Routledge, 2016. doi: 10.4324/9781315618456.
[52] J. M. Cohoon, “Toward improving female retention in the computer science major,” *Commun. ACM*, vol. 44, no. 5, pp. 108–114, May 2001, doi: 10.1145/374308.374367.
[53] B. E. Whitley, “Gender differences in computer-related attitudes and behavior: A meta-analysis,” *Comput. Human Behav.*, vol. 13, no. 1, pp. 1–22, Jan. 1997, doi: 10.1016/S0747-5632(96)00026-X.

[54] F. Hagan, *Research Methods in Criminal Justice and Criminology*, 10th ed. Hoboken: Pearson, 2018. Accessed: Apr. 07, 2024. [Online]. Available: https://www.pearson.com/en-us/subject-catalog/p/research-methods-in-criminal-justice-and-criminology/P200000001159/9780137409020

[55] C. M. Rennison, "A New Look at the Gender Gap in Offending," *Women Crim. Justice*, vol. 19, no. 3, pp. 171–190, Jul. 2009, doi: 10.1080/08974450903001461.

[56] M. Siponen and A. Vance, "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly*, vol. 34, no. 3, p. 487, 2010, doi: 10.2307/25750688.

[57] Anttila and P. Törnudd, *Kriminologia ja kriminaalipolitiikka*, 1st ed. Juva: Suomalaisen Lakimiesyhdistyksen julkaisuja, B-sarja, ISSN 0356-7214; n:o 194.WSOY, 1983.

[58] B. Gyawali and V. Prasad, "Same Data; Different Interpretations," *Journal of Clinical Oncology*, vol. 34, no. 31, pp. 3729–3732, Nov. 2016, doi: 10.1200/JCO.2016.68.2021.