# Cyber governance

## Investigating conceptualization of cybercrime and actors and tasks in cyber governance

A Thesis submitted to the Faculty of Behavioural, Management and Social Sciences

Psychology of Conflict, Risk and Safety

University of Twente

Commissioned by Saxion University of Applied Sciences

By Elsa Foppen

# Cyber governance

## Investigating conceptualization of cybercrime and actors and tasks in cyber governance

A Thesis submitted to the Faculty of Behavioural, Management and Social Sciences
Psychology of Conflict, Risk and Safety
University of Twente

Commissioned by Saxion University of Applied Sciences

By Elsa Foppen

**Graduation Committee**

First Supervisor: Dr. M. Stel
Second Supervisor: Dr. Ir. P. W. de Vries
External Supervisor: Dr. R. Spithoven

**Acknowledgements**

After the bachelor forensic investigation and this master's in psychology of conflict, risk and safety, my college years end with this thesis. I would like to start to thank my supervisor Dr. Mariëlle Stel for her support and guidance. She helped me by somewhat tempering my perfectionism. Without her I would have been working on this study for years! Her feedback helped me to continue, and it was valuable in improving the report. In addition, I would like to thank dr. ir. P.W. de Vries, my second supervisor. Furthermore, I would like to thank Dr. Remco Spithoven for the trust he placed in me when he provided the opportunity to conduct this research. I would like to say thank you to Michelle Walter for providing feedback and to Marjolein Klaver, Myrthe Hoevers and Lisanne Broshuis for being there. We all experience studying and writing a thesis during a pandemic, and it was great to vent about all struggles. Or just do an escape room with you to relax!

Finally, I would like to thank everyone close to me. My dear boyfriend, Bert, for shutting down my laptop and let me relax. Manja Buijen because she is always there for me. When I do not know how everything will work out, she always knows how to give me the power and energy to put my shoulder to the wheel. Without Annika von Heijden, my working hours would have been a lot less enjoyable. Many times, we had a Teams session of several hours to work "together" from home.

Thanks to everyone!

Elsa Foppen

**Abstract (ENG)**

Digitization entails a number of risks such as security breaches. To limit the risks of cybercrime and reduce victimization cyber resilience is needed. Since, people underestimate the risks of cybercrime, it is not expected that they are able to perform self-protective behavior in the near future. So, other actors need to increase awareness about cyber risks, improve cybersecurity and thereby reduce the number of cybercrime victims. Before these actors (cyber governance) can strengthen cyber resilience, it is necessary to conduct research into the conceptualization of cybercrime, the actors involved in cyber governance and the tasks of these actors. To address these topics, two systematic literature reviews were conducted. The results showed that cybercrime is conceptualized as all acts and behaviors that the legislator has made punishable, and norm-exceeding behaviors for which information and communication technology (ICT) is used. The actors involved in cyber governance are the private sector, government, individuals, educational institutes, law enforcement agencies, telecommunication and internet service providers and insurance companies are currently involved in cyber governance to foster cyber resilience. These actors perform tasks in the prevention, preparation, and suppression phase of cybercrime. Three gaps have been found in the literature that require further research. Overviews of actors and tasks in cyber governance in specific countries are missing in the scientific literature. Furthermore, scientific literature provides a definition of cybercrime, but it is unknown to what extent this conceptualization covers definitions from actors in cyber governance. Finally, the focus on integral collaboration in cyber governance is absent in the literature.

**Abstract (NL)**

De toenemende digitalisering brengt een aantal risico's met zich mee. Een voorbeeld van een risico is bijvoorbeeld het lekken van data. Om de risico's van cybercrime te beperken en slachtofferschap terug te dringen wordt er gestreefd naar cyberweerbaarheid. Doordat mensen de risico's van cybercriminaliteit onderschatten wordt niet verwacht dat zij op korte termijn in staat zijn om zelfbeschermend gedrag uit te voeren. Daarom is het de taak van andere actoren om het risicobewustzijn van cybercriminaliteit te vergroten, de cybersecurity te verbeteren en daarmee het aantal slachtoffers van cybercrime terug te dringen. Voordat deze actoren in staat zijn om de cyberweerbaarheid te vergroten is het van belang dat er onderzoek wordt gedaan naar de conceptualisering van cybercriminaliteit, de actoren betrokken in cybergovernance en de taken van deze actoren. Hiervoor zijn twee systematische literatuuronderzoeken uitgevoerd. De resultaten laten zien dat cybercrime gedefinieerd wordt als alle handelingen en gedragingen die bij wet strafbaar zijn, en norm overschrijdend gedrag, waarbij informatie en communicatietechnologieën (ICT) worden gebruikt. De actoren die betrokken zijn in cyber governance zijn de private sector, overheid, individuen, onderwijsinstellingen, politie, telecommunicatie en internet serviceproviders en verzekeringsmaatschappijen. Deze actoren voeren taken uit in de preventie, preparatie en repressie fase van cybercriminaliteit. Er zijn drie hiaten in de wetenschappelijke literatuur gevonden waarnaar vervolgonderzoek uitgevoerd dient te worden. Er is geen overzicht van actoren en taken in de governance van cybercriminaliteit in een specifiek land aanwezig in de wetenschappelijke literatuur. Verder is het onbekend in welke mate cybercriminaliteit in de wetenschappelijke literatuur en door de actoren in cyber governance hetzelfde worden geconceptualiseerd. Ten slotte ontbreekt de focus op integrale samenwerking in de governance van cybercriminaliteit in de literatuur.

## Index

## Introduction

Digitization entails a number of risks such as security breaches, business continuity during a cyber incident and the lack of analogous alternatives regarding digital vital processes and systems. Data from CBS (2020) shows that the number of cybercrime victims increases, despite the decline of traditional crime in the past years (CBS, 2020). Furthermore, the willingness to report victimization of cybercrime declines (CBS, 2020, Bernasco & Weijer, 2016). This indicates that the actual number of cybercrime victims is even higher than suggested by CBS. These trends are visualized in figure 1. The damage caused by cybercrime in The Netherlands is estimated at 10 billion euros per year (Deloitte, 2017). This alarming increase in cybercrime it not only observed in The Netherlands, but it is a worldwide problem (Monteith et al., 2021).

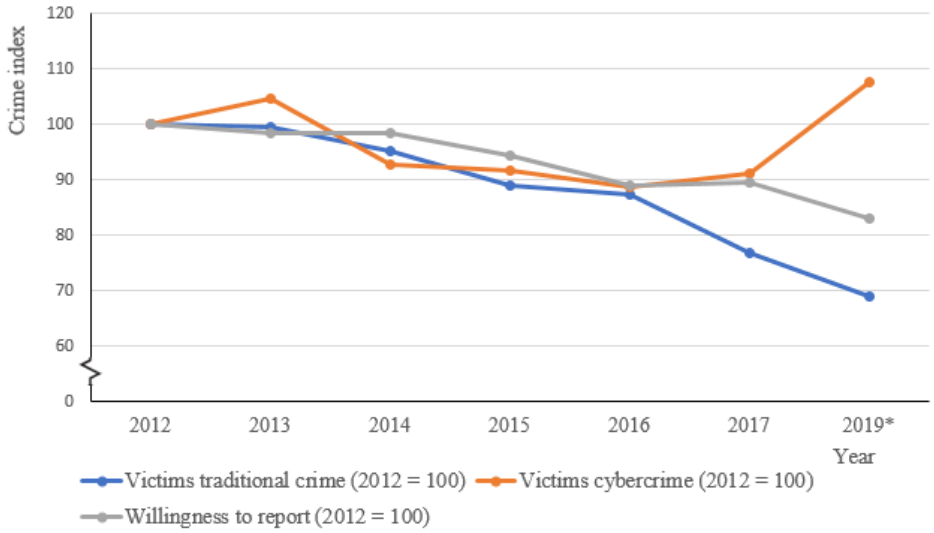


*Figure 1.* Development of traditional crime, cybercrime and the willingness to report in the period 2012-2019 whereby data of 2018 is missing, because no measurement was conducted.

*Preliminary figures registered crime.

Due to the simultaneous increase in cybercrime and decrease in traditional crime, it seems as if there is a link between both forms of crime. In this spirit the cybercrime hypothesis was formulated which assumes that the international crime drop was caused by the replacement of crime from the offline world to the online world (Farrel & Birks, 2018). To date, insufficient evidence has been found to support the cybercrime hypothesis (Farrel & Birks, 2018; Tcherni et al., 2016). Criminology, therefore, assumes that the rise in cybercrime and the decline in traditional crime are two separate phenomena that can be explained by changes in opportunities

(Spithoven, 2020). Due to the rapid digitalization of society without protection in the online world and improved protection against traditional (offline) crime, opportunity structures for criminals changed. The changed opportunity structure led to an increase in cybercrime and a decrease in traditional crime (Spithoven, 2020).

Another reason for the increase of cybercrime can be found at characteristics of the victims of cybercrime. In general, people tend to believe that they are not vulnerable for risks (of cybercrime), while they overestimate the risks (of cybercrime) for others (Misana-ter Huurne, et al., 2020; Weinstein, 1989). This, so-called optimistic bias prevents people from performing self-protective behavior. Since cybercrime is a relatively new phenomenon and the optimistic bias also applies, this lack of self-protective behavior results in almost no security which leads to opportunities for criminals in cybercrime.

To reduce cybercrime, societies want to achieve cyber-resilience. Cyber-resilience is the combination of risk awareness among potential victims and the ability to take self-protective measures to reduce individual victimization risks (Spithoven, 2020). However, due to the lack of awareness about cybercrime risks and the presence of the optimistic bias, it is not expected that individuals are able to perform self-protective behavior in the near future. That is why other actors need to increase awareness about cyber risks, improve cybersecurity and thereby reduce the number of cybercrime victims. The activities, aimed at decreasing cybercrime, that all actors together conduct can be summarized into the concept cyber governance.

To achieve cyber resilience, it is necessary to gain knowledge about the current conceptualization of cybercrime and organisation of cyber governance. The definition of cybercrime lies on the basis of cyber governance. When different actors collaborate to foster cyber resilience, it is necessary that they all have the same understanding of cybercrime. As Ostrom (in Carr & Lesniewska, 2020, p. 400) state "a common language framework is needed" to "avoid the spectre of the Tower of Babel." So therefore, the first question will be *"what is cybercrime?"* In addition, it is important to know which actors are now involved in cyber governance and what tasks they perform. The second question of this study is therefore *"which actors are currently involved in the governance of cybercrime according to the literature?"* and the third question is *"what tasks do actors have in the governance of cybercrime according to the literature?"*

The methodology and results of the literature study into the conceptualization of cybercrime (question 1) are discussed in chapter 1. Furthermore, the methodology and results

of the literature study into the current state of art regarding cyber governance (question 2 and 3) are discussed in chapter 2.

## Study 1: literature study into conceptualization of cybercrime

### Methodology

To investigate the research question "what is cybercrime?" a systematic literature study has been conducted. The PRISMA guidelines (guidelines (Preferred Reporting Items for Systematic reviews and Meta-Analyses) were followed during the search process. In this section the search strategy, inclusion criteria and data extraction strategy are discussed.

**Search strategy.** A search string was formulated. Words from two categories were combined by an "AND" function to search for all possible combinations of the words (see figure 2). By using * the library is searched for all literature that contain the word before the symbol. A pilot study was conducted to study in which libraries the number of relevant hits were maximized and whether the Dutch or English search string optimized the amount of relevant literature. The following search strings were searched for in the pilot study:

1. (Defin* OR Characteristics OR Framework OR Conceptualization OR "What is" OR Understanding) AND (Cybercrime OR "Online crime" OR "ICT Crime" OR "Computer crime")
2. (Defin* OR Kenmerk* OR Karakteristiek* OR Framework OR conceptualiser* OR "wat is") AND (cybercrim* OR "online crim*" OR "ICT crim*" OR "computer crim*")

It turned out that both the Dutch and English search string yielded only publications in the English language whereby the English search string yielded the most relevant results. That is why this systematic literature study is based on the English search string only. Furthermore, the libraries "Science Direct" and "Worldcat.org." provided the most relevant hits.

**Inclusion criteria.** A number of inclusion criteria were formulated for this review. When literature met all criteria, it was included in the review. The criteria are elaborated below.

***Geographics.*** Since cybercrime is a global phenomenon, it is expected that it is defined around the globe and thus the international literature can be used to answer the research question.

***Language.*** Due to the readability of the literature, only Dutch and English written literature is included in this review. Since the search string yielded no Dutch written results, only English written literature is included.

***Peer-review.*** This review will consider only peer-reviewed literature.

***Publication date.*** Cybercrime is a relatively new phenomenon and that is why only recent literature (past five years) is included in this review.

**Data extraction.** In order to select relevant publications that can answer the question "what is cybercrime?", the search results were screened. They were examined for the presence of the word's "definition", "defined" and "cyber." A hit was coded irrelevant when these words were not present in the publication. When one of the words were present, the passage was read to determine whether a definition of cybercrime was given. If no definition was given, the hit was still coded as irrelevant. The results of this screening process were not, as planned recorded in the data extractions form (Appendix A), but in an Excel file. The excel file was used because it provides more structure compared to the data extraction forms. The Excel sheet included all relevant items from the data extraction form and therefore an overview was created of all literature, all (ir)relevant literature, the reasons for irrelevance and the definitions of cybercrime provided by the studies[1].

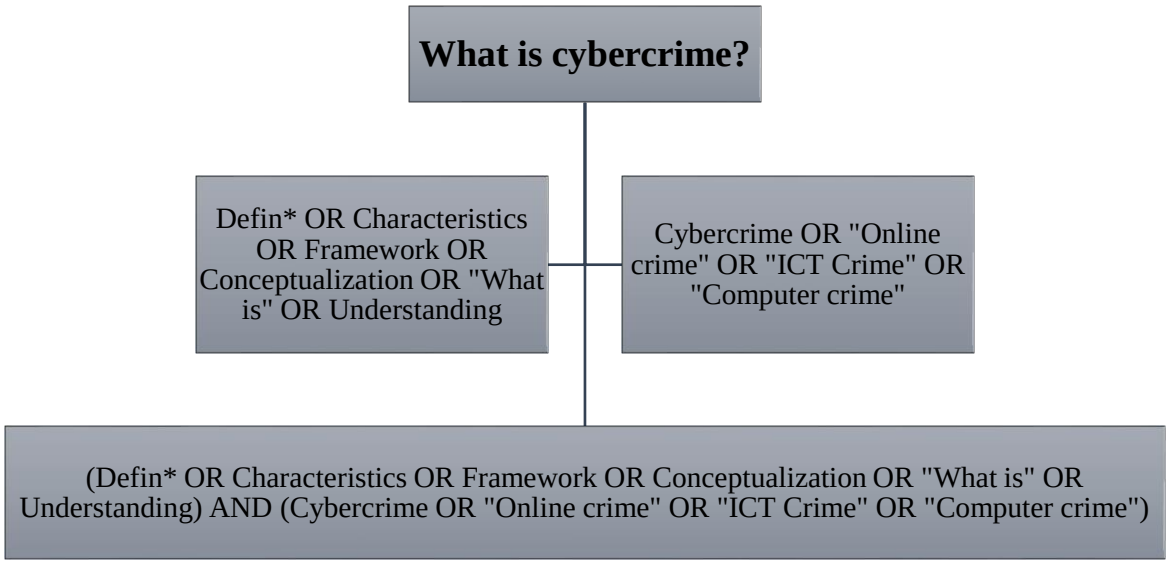


*Figure 2.* Schematic overview of the creation of a search string. Starting with the research question on which the categories are based. The relevant words in the categories are eventually combined into a search string.

## Results

This chapter discusses the findings of the systematic literature review into the conceptualization of cybercrime. This section starts with general information about the systematic literature review. It continues with the definitions of cybercrime and these definitions are further defined in the last part of this chapter.

**General information.** The search string for research question one resulted initially in

2.547 hits. After applying the inclusion criteria 299 articles remained. Twelve duplicate publications were excluded from the analysis. Resulting in 287 hits that have been reviewed on the words “definition”, “defined” and “cyber.” This ultimately resulted in 91 publications that define cybercrime (figure 3).

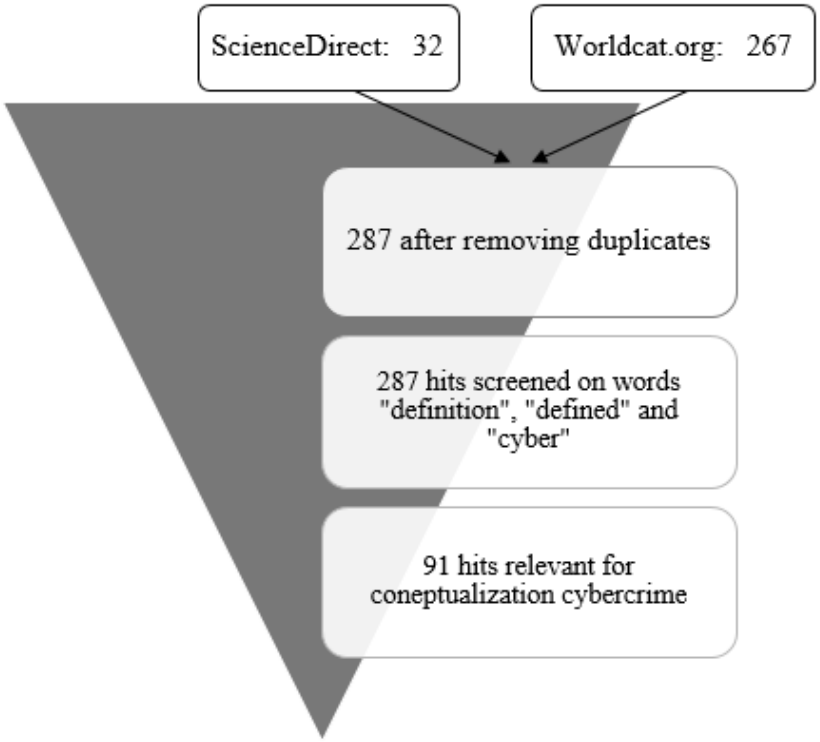


*Figure 3.* Screening process of literature.

**Cybercrime defined.** Cybercrime comprises crimes committed in cyberspace or crimes facilitated by (computer) technology (Hert, Parlar & Sajfert, 2018; Holt, Burruss & Bossler, 2016; Leukfeldt, Lavorgna & Kleemans, 2016; Payne, Hawkins & Xin, 2018; Payne, May & Hadzhidimova, 2018; Paquet-Clouston, Décary-Hétu & Bilodeau, 2017; Shamsi, Zeadally, Sheikh and Flowers, 2016; Shukan, Abdizhami, Ospanova & Abdakimova, 2019). This could for example concern fraud via an online platform or the intrusion and disruption of computer networks. The main concepts of cybercrime, “cyberspace” and “(computer) technology, are not defined in the literature. Various devices, ICT, networks, computer(networks), internet(networks), information and data systems, hardware devices, telephone lines and mobile networks, are included in the definitions of cybercrime (see for an overview appendix B). It is therefore likely that these devices are represented in the collective name cyberspace and (computer) technology. According to Payne and colleagues (2018), a characteristic of cyberspace is that it is not restricted to physical boundaries. It is therefore

possible that a Dutch computer network is intruded and disrupted from abroad.

Several authors make a distinction between (1) cyberspace as the target of a crime and (2) cyberspace as the means of an offense (Cai, Du, Xin & Chang, 2018; Lazarus, 2019; Donaldsa & Osei-Bryson, 2019; Garret, Mallia & Anthony, 2019; Leukfeldt, Kleemans, Kruisbergen & Roks, 2019; Rashkovski, Naumovski & Naumovski, 2015; Shaji, Sachin Dev & Brindha, 2018). The definition of cybercrime tuns into a framework that consists of different forms of cybercrime, due to this distinction. Ibrahim (2016) indicates this difference with the terms "cybercrime", meaning offenses committed with computers, and "computer crime", meaning computers as the targets of offenses. The category "computer integrity crimes" is added to this list by Leppänen and Kankaanranta (2017). This category describes situations where cyberspace is the means and target of a criminal event.

**Cybercrime further defined.** In addition to defining the word "cybercrime", in the above-mentioned publications light is shed on (1) the origin of the crime, (2) the technique used and (3) the motivation of the delinquent.

***The origin of the crime*.** With the rise of cybercrime, existing traditional crimes have moved to the digital world, but also completely new forms of crimes arose. Traditional forms of crimes that shifted to cyberspace (e.g. fraud) are indicated with the term cyber-enabled/computer-assisted crime, while new forms of crimes (e.g. hacking) are specified by the concept cyber-dependent/computer-focused crime (Leppänen and Kankaanranta, 2017; Lazarus, 2019; Payne et al., 2019; Donalds & Osei-Bryson, 2019; Ibrahim, 2016; Payne et al., 2020; Levi et al., 2016; Alali et al., 2018; Leukfeldt et al., 2019). In contrast to the division between cyber-enabled/computer-assisted crime and cyber-dependent/computer-focused crime, which focuses on the means originally used for a crime, the categories "techno-centric" and "people-centric" cybercrimes are about the power of the cyber element versus the human element in the offense (Ibrahim, 2016). For example, cyber vandalism, hacking and phishing are classified as techno-centric crimes while cyberbullying, cyberstalking and pornography are attributed to people-centric cybercrimes.

At first sight, the distinction between cyber-enabled and cyber-dependent crime appears to be based solely on the origin of the crime (before or after digitization). It is, however, not unlikely that cyber-enabled and cyber-dependent crime also focuses on the power of the cyber element versus the human element. In traditional forms of crime, it is likely that more social engineering is used as the target of the crime is mainly humans. Cyber-dependent crimes should then comprise the more technical forms of cybercrime since a digital device is often targeted.

***Cybercrime as a technique.*** Part of the publications (n = 42) do not provide the

definition of cybercrime, but only give a definition of a specific technique (e.g. phishing or hacking) of cybercrime. Appendix C gives an overview of the techniques and their definitions found in this literature study. A derogation is made by Shamsi and colleagues (2016). They categorize cybercrime techniques into: (1) social engineering, (2) hacking-based cybercrimes and (3) espionage-based cybercrimes. Social engineering concerns crime in which victims are deceived in order to extract sensitive information (Shamsi et al., 2016). By hacking-based cybercrime, the perpetrator uses weaknesses in a system to gain access or cause disruption (Shamsi et al., 2016). Finally, espionage-based crime uses espionage techniques to obtain confidential information which can be used to gain access or initiate other criminal activities (Shamsi et al., 2016). It appears that several methods underly the above-mentioned techniques. Methods that can be used for phishing are for example: brand spoofing, domain, and spear phishing (Mukhopadhya, Chatterjee, Bagchi, Kirs & Shukla, 2017). This stratification is visualized in figure 4.

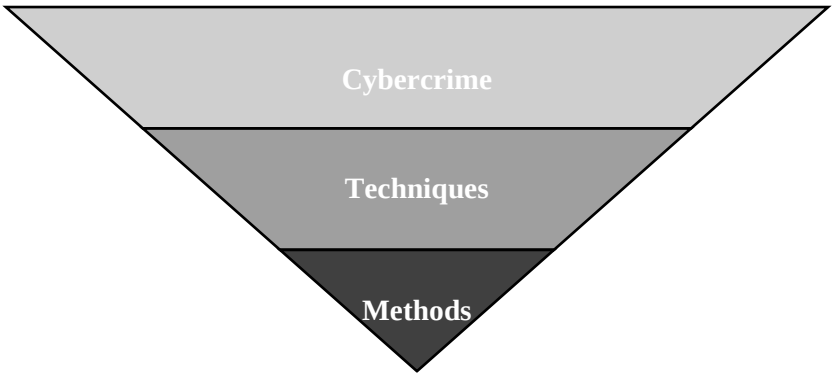


*Figure 4.* Stratification of cybercrime when defined by the underlying techniques and methods.

***Cybercrime and motivation.*** Only few researchers take the role of motivation into account (Leukfeldt, Lavorgna, et al., 2016; Levi et al., 2016). They distinguish an economic perspective (socioeconomic) and crimes intended to harm (psychosocial), often motivated by ideology, passion and revenge. The Tripartite Cybercrime Framework (TCF) adds another category and thus distinguish three broad motives: socioeconomic, psychosocial, and geopolitical cybercrimes (Lazarus, 2019; Ibrahim, 2016). Socioeconomic cybercrimes involve crimes via the computer or the internet with the aim of financial gain by, for example, false pretense or impersonation. Psychosocial cybercrimes are crimes via the computer or the internet which are mainly psychologically driven such as cyberstalking or cyberbullying. Finally, geopolitical cybercrimes include offenses via the computer or the internet that “are

fundamentally political in nature and involve agents of the state and/or industrial representatives" (Lazarus, 2019).

**Discussion**

The definitions of cybercrime that are provided by studies differ in content and specificity of the content. A possible explanation for this result is that research into cybercrime is conducted from different disciplines. For example, when a research focuses on technical security, cybercrime is defined from technology, whereas criminologist, for example, also takes the role of motivation into consideration. Definitions also differ from very short, "all crimes that involve the use of computer technology (Paquet-Clouston, Décary-Hétu & Bilodeau, 2017, p. 1)" to extensive:

> Cybercrimes are considered global crimes; they transcend geographical boundaries and can be perpetuated from anywhere against any individual and any technology. … the term is generally used to cover/describe a wide variety of illegal crimes or what is considered illicit conduct by individuals/groups against computers, computer-related and other devices, information technology networks; or traditional crimes, as well as actions targeting individuals, supported by the use of the Internet and/ or technology. (Donaldsa & Osei-Bryson, 2019, p. 1)

Although there are differences in content, specificity of content and extensiveness of definitions, it has been shown that there is unanimity about the fact that cybercrime is an umbrella term for many different crimes committed in cyberspace or crimes facilitated by (computer) technology. When cybercrime is defined further it appears that definitions are specified to (1) the origin of the crime, (2) the technique used and (3) the motivation of the delinquent. Since, cybercrime is defined as an umbrella term for many different crimes and specific techniques are defined separately, also renewed forms of cybercrime are included in the broad definition. This is an advantage because it keeps up with the rapidly developing technology and continuous emergence of new cybercrime techniques. New techniques can simply be added to the list, with their own name and definition.

**Solution for the unknown.** Because main concepts of cybercrime are not defined in the literature there is still a lot of uncertainty about the definition of cybercrime. As a result, question one (what is cybercrime?) can only be answered at a high abstract level. But cybercrime has high correlations with traditional crime (Șinca, 2015). So maybe the approach of defining traditional crime can be used to define and explain cybercrime. The similarities are

obvious: whereas cybercrime is about different types of crimes in cyberspace, traditional crime is about different types of crimes in the physical world. These similarities are best to explain with an example. To achieve a certain goal (obtain legitimate users' confidential or sensitive credentials) a specific technique can be used (phishing). The perpetrator subsequently can use different methods (brand spoofing, domain or spear phishing) each of which is defined separately. The same stratification is applied in traditional crime: to achieve a certain goal (obtain financial gains) a specific technique can be used (burglary) whereby the perpetrator can use different methods to enter the house (breaking a window versus using a crowbar during a burglary).

Due to the link between cybercrime and traditional crime a new definition can be made. There are three components that have to be considered when cybercrime is defined. Firstly, the literature shows that cybercrime is an umbrella term for different types of crime and therefore it has to be defined as a broad umbrella term. Secondly, the concept "crime" has its own definition that is independent from the medium in which the crime takes place. The definition of crime is provided in the Dutch law, and it is stated that crime consists of all acts and behaviors (both action and inaction) that the legislator has made punishable (Meijer, van den Braak & Choenni, 2020). This definition of crime is the first component that have to be included in the definition of cybercrime. However, crime develops faster than legislation. It is, for example, possible that violation of the standards is not yet legally a crime, while it is a problem in the digital world (Spithoven, 2020). That is why it was decided to include, besides "all acts and behaviors that the legislator has made punishable," "norm-exceeding behavior" in the definition of cybercrime. Thirdly, literature shows that cybercrime is a type of crime that is conducted in cyberspace (Hert, Parlar & Sajfert, 2018; Holt, Burruss & Bossler, 2016; Leukfeldt, Lavorgna & Kleemans, 2016). Therefore, the medium in which the crime is carried out, cyberspace, is included in the definition of cybercrime as well. The three components together define cybercrime and answer the first question of this study:

*"Cybercrimes are, all acts and behaviors that the legislator has made punishable, and norm-exceeding behaviors for which information and communication technology (ICT) is used."*

**Further research.** As far as known, is this the first systematic literature review into the conceptualization of cybercrime. It is an addition to existing literature as it provides the state of art regarding the conceptualization and definition of cybercrime. In this review, there was systematically searched for relevant literature whereby the PRISMA guidelines were taken into

consideration. The process as described in the PRISMA guidelines has improved the quality of this systematic literature study. The PRISMA guidelines increased the transparency of this study.

There are however four limitations that have to be considered by interpretation of the results. Firstly, 91 publications included a definition of cybercrime, but there is also a significant number of publications (almost 70%) that do not define cybercrime. Because these publications are excluded from this study, the proposed definition is based on a relatively small sample whereby it is unclear how majority of studies approach cybercrime. It is therefore recommended to study how articles, that do not provide a definition, approach cybercrime. Secondly, the proposed definition is not assessed against the literature or against definitions of actors in cyber governance and it is therefore unknown to what extent the proposed definition covers existing definitions and definitions from actors in cyber governance. By performing a review against the literature and by studying policy documents of actors, it can be established to what extent the proposed definition of cybercrime meets all aspects included in existing definitions. Third, a correlation between cybercrime and traditional crime is assumed. However, research shows that in addition to similarities (Șinca, 2015), differences (Weulen Kranenbarg, 2018) between cybercrime and traditional crime exist. A comparative study into cybercrime and traditional crime can provide more knowledge about the similarities and differences between cybercrime and traditional crime. Finally, the main concepts of cybercrime, "cyberspace" and "(computer) technology" are not defined in the literature. As a consequence, it is unknown which devices and technologies are represented in the collective names. A literature study into the conceptualization of cyberspace and (computer) technology can clarify this.

Although, the conceptualization of cybercrime does not have to deviate from traditional crime, it is likely that the governance of cybercrime and traditional crime does differ from each other. Actors in the security domain have their own specialties regarding crime. Specific knowledge is needed about the medium in which the crime takes place (digital versus physical world) to be able to tackle it. To gain more knowledge into the current organization of cyber governance, the next chapter discusses the state of art literature related to cyber governance.

## Study 2: literature study into the governance of cybercrime

### Methodology

To investigate the research question "which actors are currently involved in the governance of cybercrime and what tasks do actors have according to the literature?" a systematic literature study has been conducted. Based on the PRISMA guidelines (Preferred Reporting Items for Systematic reviews and Meta-Analyses), relevant literature was searched for. In this section the search strategy, inclusion criteria and data extraction strategy are discussed.

**Search strategy.** A search string was formulated. Words from two categories were combined by an "AND" function to search for all possible combinations of the words (see figure 5). By using * the library is searched for all literature that contain the word before the symbol. A pilot study was conducted to study in which libraries the number of relevant hits were maximized and whether the Dutch or English search string optimized the amount of relevant literature. The following search strings were searched for in the pilot study:

1. (Govern* OR Responsib* OR Organization) AND ("Cyber resilience" OR Cybersecurity OR Cybercrime OR "Online crime" OR "ICT crime" OR "Computer crime")
2. (Govern* OR Verantwoordelijk* OR Organisatie) AND (Cyberweerbaar* OR Cybersecurity OR Cybercrim* OR "Online crim*" OR "ICT crim*" OR "Computer crim*")

It turned out that both, the Dutch and English search string yielded only English written publications whereby the English search string yielded the most relevant results. That is why this review is based on the English search string. Furthermore, the libraries "Science Direct" and "Worldcat.org" provided the most relevant hits.

**Inclusion criteria.** A number of inclusion criteria were formulated for this review. When literature met all criteria, it was included in the review. The criteria are elaborated below.

***Geographic's.*** Since cybercrime is a global phenomenon, it is expected that cyber governance is a research topic worldwide and that the international literature can be used to answer the research question.

***Language.*** Due to the readability of the literature, only Dutch and English written literature is included in this review. Since the search string yielded no Dutch written results, only English written literature is included.

***Peer-review.*** This review will consider only peer-reviewed literature.

***Publication date.*** Cybercrime is a relatively new phenomenon and thus cyber governance is still nascent. That is why only recent literature (past two years) is included in this review.

**Data extraction.** In order to select relevant publications that give information about the governance of cybercrime, the publications were screened. Firstly, the title was read to determine whether the study was, was not or was possibly relevant. Attention has been paid to the presence of words that indicate tasks and activities relating to cyber resilience or words that indicate actors. Related to tasks and activities it concerns words such as "governance," "job(s)," "task(s)", but also sentences as "building cyber security awareness." Regarding the actors it concerns words as "education institutions" and "governments." When the publication could provide an answer to the research question because of the first selection, the abstract was read to determine whether actors involved in cyber governance or tasks in cyber governance were mentioned. When no actors or tasks were mentioned in the abstract, the publication was coded as irrelevant. When actors or tasks were discussed in the abstract, the publication was coded as relevant and read entirely. Relevant parts of the study were marked. The results of this screening process were not, as planned recorded in the data extraction forms, but in an Excel file. The excel file was used because it provides more structure compared to the data extraction forms. The Excel sheet included all relevant items from the data extraction form and therefore an overview was created of all literature, all (ir)relevant literature, the reasons for irrelevance and the outcomes of the study[2].

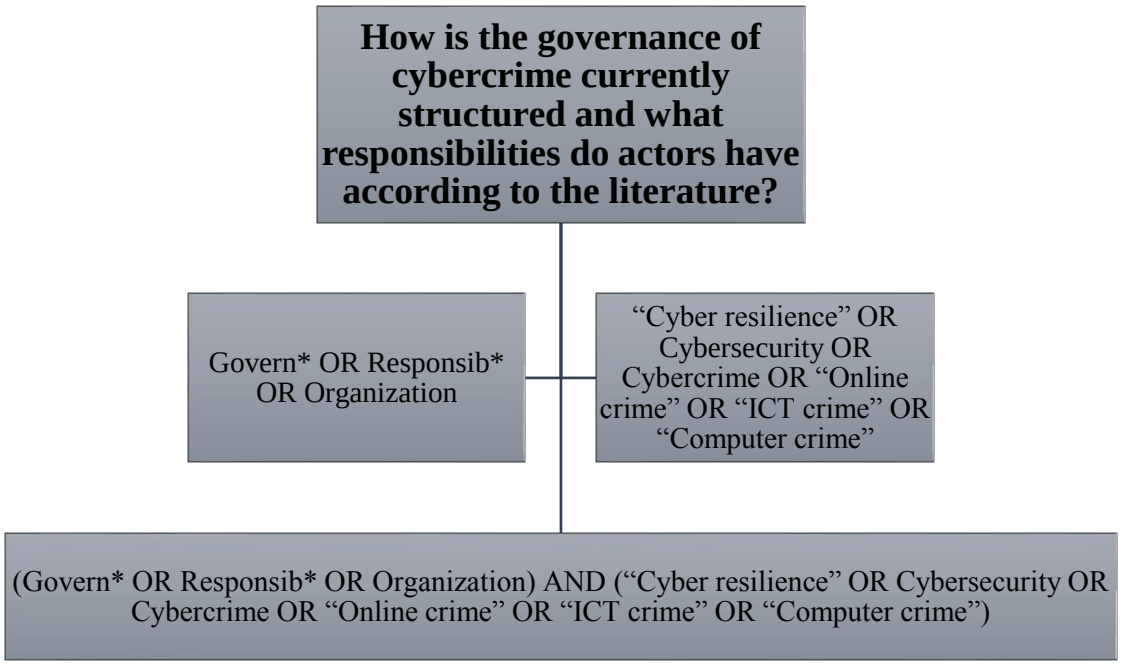


*Figure 5.* Schematic overview of the creation of a search string. Starting with the research question on which the categories are based. The relevant words in the categories are eventually combined into a search string.

## Results

**General information.** The search string for this research question resulted initially in 6.594 hits. After applying the inclusion criteria 334 articles remained. Thirty-five duplicate publications were excluded from the analysis which ultimately resulted in 299 hits that have been assessed on discussing cyber governance. Based on the title and abstract it was decided whether the study was not or possibly relevant for this literature review. After reading all the possible relevant articles, 39 publications remained that contained information about the governance of cybercrime (figure 6).

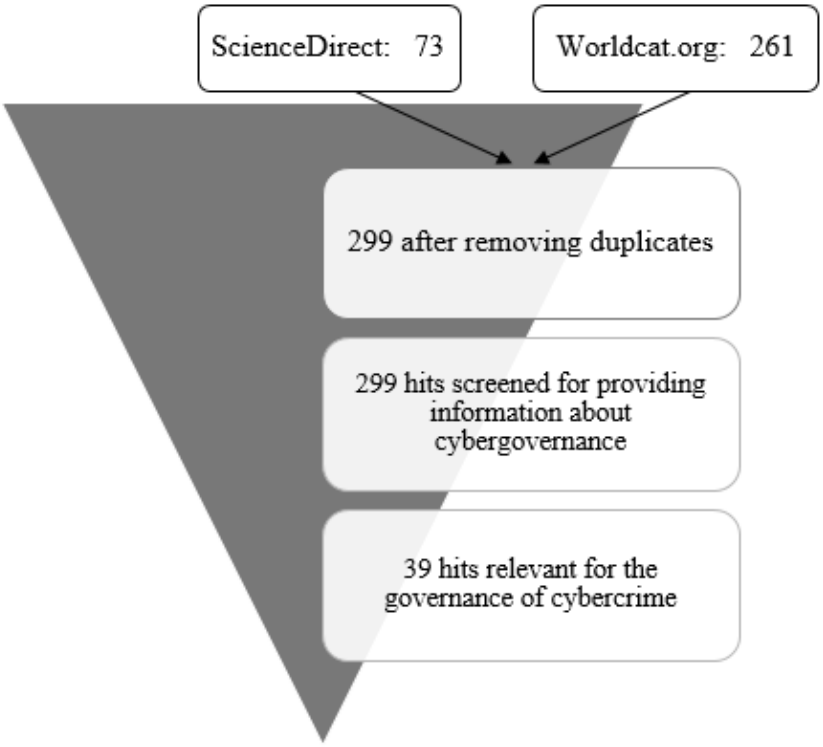


*Figure 6.* Screening process of literature.

**Actors in cyber governance and their tasks.** The literature research has shown that seven actors are involved in the governance of cybercrime: (1) private sector (n=18), (2) government (n=14), (3) individuals (n=7), (4) educational institutes (n=5), (5) law enforcement agencies (n=3), (6) telecommunication and internet service providers (n=2) and (7) insurance companies (n=2). Table 1 provide an overview of the actors and their tasks.

**Table 1**

*Actors and Tasks in cyber governance.*

| Actor | Task |
|---|---|
| Private sector | 1. Technical security |

| | |
|---|---|
| | 2. Security policies<br>3. Awareness raising (e-mails, websites, and trainings)<br>4. Audits and assessments<br>5. Cyber crisis plans<br>6. Support law enforcement agencies<br>7. Promote international norms<br>8. Counter misinformation and inauthentic posts<br>9. Closes terrorists' feeds |
| Government | 1. Laws<br>2. Performing periodic cybersecurity status reports<br>3. Cybersecurity compliance exercises and audits<br>4. Research and development<br>5. Working groups<br>6. Support employees, citizens and SME's<br>7. Technical security<br>8. Awareness raising (trainings) |
| Individuals | 1. Technical security<br>2. Behavioral security<br>3. Report cyber incidents. |
| Educational institutes | 1. Research into cybersecurity<br>2. Training |
| Law enforcement agencies | 1. Investigate cybercrimes |
| Telecommunication and internet service providers | 1. Monitor their network<br>2. Block harmful content<br>3. Protect user base |
| Insurance companies | 1. Enforcement authority<br>2. Cyber-resilience<br>3. Support clients<br>4. Monitor and warn for cyber incidents |

***Private sector.*** The literature results of eleven articles regarding tasks in cyber governance for the private sector shows that companies (1) implement technical measures, (2) create cybersecurity incident response teams that draw up security policies, (3) awareness raising, (4) conduct audits and assessments, (5) draw up cyber crisis plans, (6) support law enforcement agencies, (7) promote international norms, (8) counter misinformation and inauthentic posts and (9) closes terrorists' feeds.

The first task mentioned is implementing technical measures to protect companies' ICT infrastructure (Bahuguna, Bisht & Pande, 2019; Baillon et al., 2019; Fracalossi de Moraes, 2020; Lopez et al., 2020; Renaud et al., 2020; Van der Kleij, Wijn & Hof, 2020). In addition to technical measures, organizations focus on cyber secure behavior of their employees

(Baillon et al., 2019; Van der Kleij et al., 2020). That is why the second task that the private sector is engaged in is drawing up and implementing information security policies (Bahuguna et al., 2019; Baillon et al., 2019; Lee, 2020; Van der Kleij et al., 2020). These policies are implemented by cybersecurity incident response teams to describe the appropriate behaviour of employees and their responsibilities in the prevention of security incidents. To increase employees' knowledge of cyber risks and cyber security, the third activity that the private sector initiate is the distribution of awareness campaigns via websites, e-mails, or trainings. (Bahuguna et al., 2019; Baillon et al., 2019; Lee, 2020; Renaud et al., 2020; Van der Kleij et al., 2020). The goal of these awareness campaigns is strengthening the understanding of employees about why and how they have to comply with information security policies. The fourth task mentioned is the performance of audits and assessments, aimed at identifying vulnerabilities or determining whether a company complies with a standard (Bahuguna et al., 2019; Bahuguna, Bisht & Pande, 2020). ICT systems are, for example, searched for weaknesses by penetration-testing (Hatfield, 2019). After such a test, a report is drawn up with information about whether and how the tester was able to breach the security barriers, accompanied with recommendations to strengthen the vulnerabilities founded. Composing a Cyber Crisis Management Plan (CCMP) or an Incident Response Plan is the fifth task that organizations conduct (Bahuguna et al., 2019; Lopez et al., 2020). These plans can provide support when a cyber incident has taken place, since it focusses on cyber-resilience by discussing incidence response capabilities and strategies.

The previously described responsibilities of the private sector mainly aim at protecting companies own ICT infrastructure and at acting appropriately when a cyber incident occur, however the private sector can also be part of a collaboration to prevent cybercrime. Therefore, the sixth task of the private sector is providing information to law enforcement agencies to help them with the investigation of cybercrimes (Holt et al., 2020). A seventh, more specific, task for the private sector that is mentioned in the literature is the promotion of international norms by Microsoft and Siemens (Georgieva, 2019). Countering misinformation and inauthentic posting by Facebook and closing terrorists' feeds by Twitter are mentioned as the eighth and ninth task of the private sector (Reverson & Savage, 2020). The private sector thus has a total of nine tasks that they are performing in the prevention, preparation, and suppression phase of cybercrime.

***Government.*** Tasks of the government, as described in eleven studies are (1) drawing up and supervising of laws, (2) performing periodic cybersecurity status reports, (3) initiating cybersecurity compliance exercises and audits, (4) promoting research and development in

cybersecurity, (5) setting up working groups in the field of cybercrime, (6) support employees, citizens and SME's and (7) deploying technical measures.

The government's first and most entrusted task is to draw up and introduce laws and norms (Ebert, 2020; Maurer, 2019) that can be deployed "for enforcing cybersecurity requirements by countries or sectors" (Bahuguna et al., 2020, p. 255). Supervisory entities are established to periodically assess compliance to regulations (Bahuguna et al., 2020). In addition to forcing companies in the private sector to comply with certain cybersecurity standards, laws can be about penalties for cybercrimes (Ebert, 2020; Lee, 2020; Lei, 2019; Nielsen et al., 2020; Ronaldson, 2019).

As the second task, periodic cybersecurity status reports are performed (Bahuguna et al., 2020). These reports are drawn up by Computer Security Incident Response Teams (CSIRT) and Information Sharing and Analysis Centers (ISAC) and are aimed at identifying national trends in cyber incidents, targeted attacks and vulnerabilities exploited. The third task mentioned is the performance of audits and assessments (Bahuguna et al., 2020; Ebert, 2020; Haddad & Binder, 2019). These tools are used to identify vulnerabilities and to assess cybersecurity efforts at the national level.

In the fourth place, the government promote research and development in cybersecurity (Bahuguna et al., 2019; Calderaro & Craig, 2020). It cannot be deduced from the literature with what intention the government is promoting research and development. It does appear that the production of scientific and technical knowledge contributes to country's cyber capacity in the sense of technical protection and policy development (Calderaro & Craig, 2020). Fifthly, the Austrian government initiate projects and bring together experts with the aim "to enhance the security and resilience of Austrian infrastructures and services in cyber space" (Haddad & Binder, 2019, p. 122). With that, the Austrian government is the driving force behind building awareness and confidence in society regarding cybersecurity (Haddad & Binder, 2019).

Supporting employees, citizens and SME's is the sixth task of the government (Haddad & Binder, 2019; Renaud et al., 2020). Trainings are provided by the government to increase knowledge about cyber risks and cyber security among employees (Renaud et al., 2020). In addition to supporting its own staff, SME's and citizens are assisted by making financial resources available and by offering training. This is aimed at promoting digital awareness and practical knowledge so that unskilled citizen and labor force become digital skilled subjects (Haddad & Binder, 2019). The final task of the government is protecting its own ICT infrastructure for which they implement technical tools. The government thus has a total of seven tasks that they are performing in the prevention phase of cybercrime. The government is

involved in the direct (implementing technical measures) and indirect (stimulating research to obtain more knowledge) prevention of cybercrime.

***Individuals.*** The literature results of seven articles shows that individuals have to (1) take technical security measures, (2) take behavioral security measures and (3) report cyber incidents.

The first two tasks that individuals have, taking technical and behavioral measures, are aimed at improving cybersecurity (Armstrong, in Billingsley, 2019; Haddad & Binder, 2019; Renaud et al., 2020; Reverson & Savage, 2020; Van der Kleij, Wijn & Hof, 2020). They, for example, need to, (I) lock their screen when they leave the computer, (II) encrypt sensitive information before mailing it to external recipients, (III) share sensitive information only with authorized entities and (IV) verify recipient e-mail addresses before sending e-mails (Van der Kleij, Wijn & Hof, 2020). The third task it that individuals need to report (information about) cyber incidents (Holt et al., 2020; Renaud et al., 2020). So, individuals have a total of three tasks that they are performing in the prevention and suppression phase of cybercrime.

***Educational institutes***. Results from five studies show that educational institutes are involved in the governance of cybercrime in two ways: (1) conducting research into cybersecurity and cyber risks and (2) offering training.

With regard to the first task of educational institutes, the literature state that they are an important actor in conducting research (de Moraes, 2020; Norris et al., 2019). It is unclear what type of research is currently conducted and what the aim of these studies are. Secondly, educational institutes are offering training to students to accomplish digitally educated citizens and to train cyber-experts for the future (Chang & Coppel, 2020; Yang, 2019). Educational institutes thus have two tasks that they are performing in the prevention phase of cybercrime.

***Law enforcement agencies***. The investigation of cybercrimes is according to three studies the main and only task of law enforcement agencies (Holt et al., 2020). They have to find evidence for criminal activities (Fidalgo, Alegre, Fernández-Robles & González-Castro, 2019). In Taiwan, a distinction is made between the National Police Agency (NPA) and the Investigation Bureau (MJIB) (Wang, Hsieh, Chang, Jiang & Dallier, 2020). The NPA is concerned with everyday policing and therefore interacts with the general public, while the MJIB conducts several national major crime investigations yearly (e.g., counter-terrorism, white collar crime and cybercrime). In large-scale cybercrime investigations this means that the MJIB is mainly concerned with computer forensics and the NPA focus on broadcasting suspects' information to the public, track and seis stolen goods and arrest suspects. Thus, law enforcement agencies have one task in the suppression phase of cybercrime.

***Telecommunication and internet service providers.*** The literature results of two articles regarding tasks of telecommunication and internet service providers shows that they (1) monitor their network, (2) block harmful content from the internet and (3) protect their user base.

The first task conducted by telecommunication and internet service providers is the monitoring of their network to observe abnormal behavior (Parfenov, Zabrodina, Torchin & Parfenov, 2019). Second, internet service providers block harmful content from the internet when reported (Holt, Cale, Leclerc & Drew, 2020). Protection of telecommunication and internet service providers' own user base is the third task (Holt, Cale, Leclerc & Drew, 2020). It should be noted that telecommunication and internet service providers are under certain circumstances mandatory by law to protect their user base and to comply with subpoenas and legal requests. So, it is required by law in some circumstances, but it is unclear what is meant by "some circumstances" and thereby when this task is actually performed. So, telecommunication and internet service providers have a total of three tasks that they are performing in the prevention and suppression phase of cybercrime.

***Insurance companies.*** Tasks of insurance companies, as described in three studies are (1) being an enforcement authority, (2) fostering cyber-resilience, (3) offering support and (4) monitoring and warn for cyber incidents. Regarding the first task, Herr (2019) states that insurance companies are an enforcement authority because it sets baseline standards for their clients. Second, the availability of cybercrime insurances in general, is seen as "a first approach to cyber-resilience (…) as coverage to disruption-derived losses through insurance" (Sepúlveda Estay, Sahay, Barfod and Jensen, 2020, p. 1). Finally, insurance companies offer support in the area of security controls, risk assessment practices and they even monitor the network and warn for cyber incidents in some cases (Sepúlveda Estay, 2020). Insurance companies thus have a total of four tasks that they are performing in the prevention phase of cybercrime.

## Discussion

The two questions of the second study can be answered based on the literature. In answer to question two "which actors are currently involved in the governance of cybercrime according to the literature?" a total of seven actors where found who all have tasks in the governance of cybercrime: (1) private sector, (2) government, (3) individuals, (4) educational institutes, (5) law enforcement agencies, (6) telecommunication and internet service providers and (7) insurance companies. They all have specific tasks which are presented in table 1 (results section). This table provides an answer to question three ""what tasks do actors have in the

governance of cybercrime according to the literature?" The seven actors perform tasks in the prevention, preparation, and suppression phase of cybercrime.

**Gaps in cybergovernance.** Despite the above findings, four gaps have been identified in the scientific literature into cyber governance: (1) list of actors in cyber governance is not complete, (2) unclear to what extent tasks are (sufficiently) conducted by actors, (3) the seven actors are not equally investigated and (4) little is known about the effects when government does not intervene.

First, even though international publications were included in this systematic literature review to optimize the number of relevant hits, it seems that the list of actors is not complete. Prominent actors such as the public prosecutor's office are not included. Practical application research consisting of interviews is thus needed to complement the list. Second, the literature study has shown that there is a dichotomy in the literature about tasks in cyber governance. On the one hand, there is literature describing which tasks are already conducted by actors (table 1 in the results section). On the other hand, there is literature suggesting which tasks actors should be doing (table 2). The current situation and the recommendations relate, in many cases, to the same tasks and that makes it unclear whether the task is (sufficiently) conducted. Practical application research consisting of policy document analyses and interviews can be conducted on one actor from cybergovernance to establish to what extent tasks are performed. This extra research also provides insight into the scope of tasks, as this cannot clearly be deduced from literature. The specificity in which studies describe tasks of actors differ from general, implementing technical measures, to specific, penetration-testing.

**Table 2**

*Recommendations to Actors in Cyber Governance.*

| Actor | Task |
|---|---|
| Private sector | 1. Technical security[3]<br>2. Security policies[4]<br>3. Awareness raising[5] (programs and trainings)<br>4. Audits and assessments[6]<br>5. Incident reporting[7]<br>6. Stipulation of insurance policies[8] |
| Government | 1. (Supervision of) laws[9]<br>2. Policy planning[10]<br>3. Incident reporting[11]<br>4. Awareness raising among individual citizens and employees[12]<br>5. Technical security[13] |

| | |
|---|---|
| | 6. Working groups[14] |
| Individuals | 1. Technical security[15]<br>2. Behavioral security[16]<br>3. Report cyber incidents[17] |
| Educational institutes | 1. Research into cybersecurity[18] |
| Law enforcement agencies | 1. Develop transparent communication and intelligence sharing channels[19] |
| Telecommunication and internet service providers | 1. Influence behavior of clientele[20]<br>2. Support law enforcement agencies[21] |
| Manufacturers | 1. Controllers of data collected in their products/systems[22]<br>2. Collect and process minimum amount of data[23]<br>3. Deliver protected products and communication tools[24] |
| *Actor unknown* | 1. Prevent secondary victimization[25] |

Third, the seven actors are not equally extensive investigated on their tasks in cyber governance and therefore the reliability of the tasks for law enforcement agencies, telecommunication and internet service providers, and insurance companies are not certain. The private sector and government are relatively often the subject of studies, while law enforcement agencies, telecommunication and internet service providers and insurance companies are somewhat underrepresented. The government has a clear duty of care, and it is therefore not surprising that a great deal of responsibility is placed on the government and that they are relatively often subject of investigation. By contrast, the expectations of the private sector may not be based on a duty of care, but the private sector is an important owner of data and the producer of ICT products. They are the basis of ICT networks and products and therefore have a major impact on cybersecurity. This could explain why they are studied most often. Follow-up research, for example case studies, into tasks of actors that are underrepresented in the literature is needed to increase the reliability of the data found in this research. Finally, one publication has been found that approach cybercrime completely different compared to the other studies (Lee, 2019). The government should wait and see, because the internet and thereby cybercrime is a relative new phenomenon that is still nascent. As there is just one article that recommend this approach, little is known about the effects when government does not intervene. Follow up research can show whether there are countries that use this approach and what the effect of this approach is on the development of cybercrime.

In addition to the gaps in the scientific literature about cyber governance, two limitations of this specific study have to be mentioned. First, the absence of a second researcher

involved in the selection of publications and quality assessment may influence the internal validity of this study. The internal validity is about the extent to which valid conclusion can be drawn from the literature studied (Kleemans, Korf & Staring, 2008). The internal validity of this study could have been maximized by avoiding systematic errors. Involving a second researcher in the quality assessment of the publications could have contributed to this. Third, due to time constraints, it was decided to include studies published in the last two years only (instead of last five years[26]). Consequently, the number of hits in Worldcat.org and ScienceDirect were not optimized, and thus relevant literature may have been missed. However, as far as known, this is the first systematic literature review into the governance of cybercrime. It is an addition to existing literature as it provides the state of art cyber governance. In this systematic literature review, there was searched for relevant literature whereby the PRISMA guidelines were taken into consideration. The selection process as described in the PRISMA guidelines has improved the quality of this systematic literature study. The PRISMA guidelines increased the transparency of this study. There are however also six limitations that have to be considered.

## General discussion

Digitization entails a number of risks such as security breaches and business continuity. To limit these risks, societies want to achieve cyber-resilience. Cyber-resilience is the combination of risk awareness among potential victims and the ability to take self-protective measures to reduce individual victimization risks. Achieving cyber resilience is hindered by the optimistic bias. Since people tend to believe that they are not vulnerable for risks of cybercrime, it is not expected that they are themselves able to take effective precautions in the near future. That is why other actors need to increase awareness about cyber risks, improve cybersecurity and thereby reduce the number of cybercrime victims. To achieve cyber resilience, it is necessary to gain knowledge about the current conceptualization of cybercrime and organisation of cyber governance. Therefore, this study addressed the conceptualization of cybercrime and the organisation of cyber governance.

To be able to organize the governance of cybercrime, it should be known how cybercrime is defined. Therefore, the first sub question was *"what is cybercrime?"* Synthesized from the literature study, cybercrime can be conceptualized as all acts and behaviors that the legislator has made punishable, and norm-exceeding behaviors for which information and communication technology (ICT) is used. Furthermore, it is of importance to know which actors are currently involved in cyber governance. Therefore, the second sub question was

*"which actors are currently involved in the governance of cybercrime according to the literature?"* Seven actors are found in the literature with a task in cybergovernance: (1) private sector, (2) government, (3) individuals, (4) educational institutes, (5) law enforcement agencies, (6) telecommunication and internet service providers and (7) insurance companies. Thirdly, it is important to know which tasks these actors currently have. The third sub question was therefore *"what tasks do actors have in the governance of cybercrime according to the literature?"* The seven actors involved in cyber governance perform tasks in the prevention, preparation, and suppression phase of cybercrime. A more detailed overview of tasks is given in table 1 (results section study 2).

**The full perspective.** Although, the research questions have been answered based on the literature, three key gaps in the scientific literature are observed: (1) absence of an overview of actors and tasks in cyber governance in a specific country, (2) absence of studies into the conceptualization of cybercrime according to actors in cyber governance and (3) absence of focus on integral collaboration in cyber governance.

Concerning the first gap, no publications have been found that provides an overview of all actors and tasks in cyber governance in a specific country[27]. Because cultural differences are expected to influence, for example, the extent to which government intervene in private lives of its citizens, the organization of cyber governance may differ per country. Unless the borderless character of cybercrime, cyber governance seems to be a local affair. Practical application research consisting of interviews with actors from cyber governance are thus needed to provide knowledge about actors and their tasks in cyber governance in a specific country. Interviews with the seven actors found in this study can be used to gain knowledge about the organisation of cyber governance in a specific country. The snowball method can be applied to reach, still unknown actors in cyber governance, via the known actors. Policy analyses can provide information about the tasks that these actors are performing.

Second, no study has been found into the conceptualization of cybercrime by actors in cyber governance. It is therefore unknown to what extent the definition of cybercrime according to scientific literature covers definitions from actors in cyber governance. This should be addressed, since a common definition between actors is a must to improve clear communication, responsibilities, and tasks to foster cyber resilience. Therefore, practise-oriented research is needed into the conceptualization of cybercrime by actors involved in cyber governance.

Concerning the third gap, it is of great importance to focus on integral collaboration in cyber governance. All actors in cyber governance contribute independently to achieving cyber

resilience, but it is the integral collaboration of actors that contributes to the effectiveness in achieving cyber resilience by cyber governance. There is just one task observed in the literature with a focus on cooperation, the support of law enforcement agencies by the private sector. And as far as known, no research is conducted into the entire spectrum of actors in cyber governance. Integral collaboration in cyber governance is thus understudied and therefore it is recommended to conduct further research into the entire spectrum of actors. Interviews and traditional focus groups with the actors involved in cyber governance can be used to gain knowledge about integral collaboration in cyber governance. This can, for instance, provide insight into the actors that currently collaborate and into the tasks on which actors collaborate.

As far as known, this is the first systematic literature review into the conceptualization of cybercrime and cyber governance. As little research into the conceptualization of cybercrime has been carried out, there is a gap in knowledge concerning the conceptualization of cybercrime in practice. Also, much is still unknown about the organisation of cyber governance, while this knowledge is desperately needed to achieve cyber resilience and prevent cybercrime. For example, an overview of actors and tasks in cyber governance in specific countries is needed and more research with a focus on integral collaboration in cyber governance have to be conducted. Despite the fact that much is still unknown about cyber governance, this study is an important step in achieving cyber-resilience. However, more needs to be done to bring a cyber-resilient world a step closer (Cyber Security Raad, 2021).

## References

Abraham, C., Chatterjee, D., & Sims, R. R. (2019). *Muddling through cybersecurity: Insights from the U.S. healthcare industry. Business Horizons,* 62(4), 539–548. doi:10.1016/j.bushor.2019.03.010

Adewole, K. S., Anuar, N. B., Kamsin, A., & Sangaiah, A. K. (2017). *SMSAD: a framework for spam message and spam account detection. Multimedia Tools and Applications,* 78(4), 3925–3960. doi:10.1007/s11042-017-5018-x

Alali, M., Almogren, A., Hassan, M. M., Rassan, I. A. L., & Bhuiyan, M. Z. A. (2018). *Improving risk assessment model of cyber security using fuzzy logic inference system. Computers & Security,* 74, 323–339. doi:10.1016/j.cose.2017.09.011

Ali, S. T., McCorry, P., Lee, P. H.-J., & Hao, F. (2017*). ZombieCoin 2.0: managing next-generation botnets using Bitcoin. International Journal of Information Security*, 17(4), 411–422. doi:10.1007/s10207-017-0379-8

Alieyan, K., ALmomani, A., Manasrah, A., & Kadhum, M. M. (2015). *A survey of botnet detection based on DNS. Neural Computing and Applications*, 28(7), 1541–1558. doi:10.1007/s00521-015-2128-0

Álvarez-García, D., Barreiro-Collazo, A., Núñez, J. C., & Dobarro, A. (2016). *Validity and reliability of the Cyber-aggression Questionnaire for Adolescents (CYBA). The European Journal of Psychology Applied to Legal Context*, 8(2), 69–77. doi:10.1016/j.ejpal.2016.02.003

Anagnostopoulos, M., Kambourakis, G., & Gritzalis, S. (2015). *New facets of mobile botnet: architecture and evaluation. International Journal of Information Security*, 15(5), 455–473. doi:10.1007/s10207-015-0310-0

Baek, H., Nicholson, J. A., Higgins, G. E., & Losavio, M. M. (2018). *Parental Indifference and Children's Digital Piracy in South Korea: Mediation Effects of Low Self-Control and Misconception. Asian Journal of Criminology*, 13(4), 293–309. doi:10.1007/s11417-018-9271-3

Bahtiyar, Ş. (2016). *Anatomy of targeted attacks with smart malware. Security and Communication Networks*, 9(18), 6215–6226. doi:10.1002/sec.1767

Bahuguna, A., Bisht, R. K., & Pande, J. (2019). *Assessing cybersecurity maturity of organizations: An empirical investigation in the Indian context. Information Security Journal: A Global Perspective*, 28(6), 164–177. doi:10.1080/19393555.2019.1689318

Bahuguna, A., Bisht, R. K., & Pande, J. (2020*). Country-level cybersecurity posture assessment:Study and analysis of practices. Information Security Journal: A Global Perspective*, 29(5), 250–266. doi:10.1080/19393555.2020.1767239

Baillon, A., de Bruin, J., Emirmahmutoglu, A., van de Veer, E., & van Dijk, B. (2019). *Informing, simulating experience, or both: A field experiment on phishing risks. PLOS ONE*, 14(12), e0224216. doi:10.1371/journal.pone.0224216

Barbon, S., Igawa, R. A., & Bogaz Zarpelão, B. (2016). *Authorship verification applied to detection of compromised accounts on online social networks. Multimedia Tools and Applications*, 76(3), 3213–3233. doi:10.1007/s11042-016-3899-8

Bartholomae, F. (2017). *Cybercrime and cloud computing. A game theoretic network model. Managerial and Decision Economics*, 39(3), 297–305. doi:10.1002/mde.2904

Battaglio, R. P., & Hall, J. L. (2019). *Ordo Ab Chao? Complexity and Its Implications. Public Administration Review*, 79(6), 807–809. doi:10.1111/puar.13128

Bernasco, W. & Weijer, S. van de. (2016). *Aangifte- en meldingsbereidheid. Trends en determinanten*. Amsterdam: Nederlands Studiecentrum Criminaliteit en Rechtshandhaving. Retrieved May 11, 2020, from http://www.wimbernasco.nl/Manuscripts/Nederlands/TK%20Bijlage%20Aangifte%20en%20meldingsbereidheid%20Trends%20en%20determinanten.pdf

Bhushan, K., & Gupta, B. B. (2017). *A novel approach to defend multimedia flash crowd in cloud environment. Multimedia Tools and Applications*, 77(4), 4609–4639. doi:10.1007/s11042-017-4742-6

Billingsley, L. (2019). *Cybersmart: Protect the Patient, Protect the Data. Journal of Radiology Nursing*, 38(4), 261–263. doi:10.1016/j.jradnu.2019.09.010

Bressers, H., Bressers, N., & Larrue, C. (Eds.). (2016). *Governance for Drought Resilience.* doi:10.1007/978-3-319-29671-5

Broadhead, S. (2018). *The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments. Computer Law & Security Review*, 34(6), 1180–1196. doi:10.1016/j.clsr.2018.08.005

Calderaro, A., & Craig, A. J. S. (2020). *Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building. Third World Quarterly*, 41(6), 917–938. doi:10.1080/01436597.2020.1729729

Carr, M., & Lesniewska, F. (2020). *Internet of Things, cybersecurity and governing wicked problems: learning from climate change governance. International Relations*, 34(3), 391–412. doi:10.1177/0047117820948247

Carrapico, H., & Barrinha, A. (2017). *The EU as a Coherent (Cyber)Security Actor? JCMS: Journal of Common Market Studies*, 55(6), 1254–1272. doi:10.1111/jcms.12575

Cai, T., Du, L., Xin, Y., & Chang, L. Y. C. (2018). *Characteristics of cybercrimes: evidence from Chinese judgment documents. Police Practice and Research*, 19(6), 582–595. doi:10.1080/15614263.2018.1507895

CBS. (2020, March, 2). *Minder traditionele criminaliteit, meer cybercrime.* Retrieved April 23, 2020, from https://www.cbs.nl/nl-nl/nieuws/2020/10/minder-traditionele-criminaliteit- meer-cybercrime

CCV. (2020, 7 september). *Ondernemers onderschatten risico's cybercrime*. Centrum voor Criminaliteitspreventie en Veiligheid (CCV). https://hetccv.nl/nieuws/ondernemers-onderschatten-risicos-cybercrime/

Chang, L. Y. C., & Coppel, N. (2020). *Building cyber security awareness in a developing country: Lessons from Myanmar. Computers & Security*, 97, 101959. doi:10.1016/j.cose.2020.101959

Cheng, L., Liu, F., & Yao, D. D. (2017). *Enterprise data breach: causes, challenges, prevention, and future directions. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 7(5), e1211. doi:10.1002/widm.1211

Conway, G., & Hadlington, L. (2018). *How Do Undergraduate Students Construct Their View of Cybercrime? Exploring Definitions of Cybercrime, Perceptions of Online Risk and Victimization. Policing: A Journal of Policy and Practice*. doi:10.1093/police/pay098

Costa, P., Montenegro, R., Pereira, T., & Pinto, P. (2019). *The Security Challenges Emerging from the Technological Developments. Mobile Networks and Applications*, 24(6), 2032–2037. doi:10.1007/s11036-018-01208-0

Croke, L. (2020). *Protecting your organization from e-mail phishing and ransomware attacks . AORN Journal*, 112(4). doi:10.1002/aorn.13229

Crossler, R. E., Bélanger, F., & Ormond, D. (2017). *The quest for complete security: An empirical analysis of users' multi-layered protection from security threats. Information Systems Frontiers*, 21(2), 343–357. doi:10.1007/s10796-017-9755-1

Cyber Security Raad. (2021, april). *Adviesrapport integrale aanpak cyberweerbaarheid. Een integrale aanpak om de open, vrije en welvarende Nederlandse samenleving structureel cyberweerbaar te maken en (digitale) kansen te verzilveren.* https://www.cybersecurityraad.nl/documenten/adviezen/2021/04/06/csr-adviesrapport-integrale-aanpak-cyberweerbaarheid

De Corte, C. E., & Van Kenhove, P. (2015). *One Sail Fits All? A Psychographic Segmentation of Digital Pirates. Journal of Business Ethics*, 143(3), 441–465. doi:10.1007/s10551-015-2789-8

De Hert, P., Parlan, C., & Sajfert, J. (2018). *The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist transborder access to electronic evidence promoted via soft law. Computer Law & Security Review*, 34(2), 327-336 https://doi.org/10.1016/j.clsr.2018.01.003

De Kimpe, L., Ponnet, K., Walrave, M., Snaphaan, T., Pauwels, L., & Hardyns, W. (2020). *Help, I need somebody: Examining the antecedents of social support seeking among cybercrime victims. Computers in Human Behavior*, 108, 106310. doi:10.1016/j.chb.2020.106310

Deschamps, R., & McNutt, K. (2016). *Cyberbullying: What's the problem? Canadian Public Administration*, 59(1), 45–71. https://doi.org/10.1111/capa.12159.

Deloitte (2017). *Cyber Value at Risk in The Netherlands 2017.* Amsterdam: Deloitte.

Dodel, M., & Mesch, G. (2018). *Inequality in digital skills and the adoption of online safety behaviors. Information, Communication & Society*, 21(5), 712–728. doi:10.1080/1369118x.2018.1428652

Donalds, C., & Osei-Bryson, K. M. (2019). *Toward a cybercrime classification ontology: A knowledge-based approach. Computers in Human Behavior*, 92, 403–418. doi:10.1016/j.chb.2018.11.039

Dupont, B. (2016). *Bots, cops, and corporations: on the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime. Crime, Law and Social Change*, 67(1), 97–116. doi:10.1007/s10611-016-9649-z

Dushi, D. (2018). *Challenges of protecting children from sexual abuse and exploitation on the internet: the case of Kosovo. International Review of Law, Computers & Technology*, 32(1), 80–98. doi:10.1080/13600869.2018.1431871

Ebert, H. (2020). *Hacked IT superpower: how India secures its cyberspace as a rising digital democracy. India Review*, 19(4), 376–413. doi:10.1080/14736489.2020.1797317

Farrel, G., & Birks, D. (2018). *Did cybercrime cause the crime drop? Crime Science*, 7(1). doi:10.1186/s40163-018-0082-8

Fidalgo, E., Alegre, E., Fernández-Robles, L., & González-Castro, V. (2019). *Classifying suspicious content in tor darknet through Semantic Attention Keypoint Filtering. Digital Investigation*, 30, 12–22. doi:10.1016/j.diin.2019.05.004

Fracalossi de Moraes, R. (2020). *Whither Security Cooperation in the BRICS? Between the Protection of Norms and Domestic Politics Dynamics. SSRN Electronic Journal.* doi:10.2139/ssrn.3632389

Garrett, B., Mallia, E., & Anthony, J. (2019). *Public perceptions of Internet-based health scams, and factors that promote engagement with them. Health & Social Care in the Community*. doi:10.1111/hsc.12772

Georgieva, I. (2019). *The unexpected norm-setters: Intelligence agencies in cyberspace. Contemporary Security Policy*, 41(1), 33–54. doi:10.1080/13523260.2019.1677389

Gosine, A. (2020). *Industrial Control Systems: Cyber Policies and Strategies. Journal AWWA*,112(6), 48–54. doi:10.1002/awwa.1518

Haddad, C., & Binder, C. (2019). *Governing through cybersecurity: national policy strategies, globalized (in-)security and sociotechnical visions of the digital society. Österreichische Zeitschrift Für Soziologie*, 44(S1), 115–134. doi:10.1007/s11614-019- 00350-7

Hatfield, J. M. (2019). *Virtuous human hacking: The ethics of social engineering in penetration-testing. Computers & Security*, 83, 354–366. doi:10.1016/j.cose.2019.02.012

Herr, T. (2019). *Cyber insurance and private governance: The enforcement power of markets.Regulation & Governance*, 15(1), 98–114. doi:10.1111/rego.12266

Holt, T. J. (2017). *On the Value of Honeypots to Produce Policy Recommendations. Criminology & Public Policy*, 16(3), 739–747. doi:10.1111/1745-9133.12315

Holt, T. J., Burruss, G. W., & Bossler, A. M. (2016). *Assessing the Macro-Level Correlates of Malware Infections Using a Routine Activities Framework. International Journal of Offender Therapy and Comparative Criminology*, 62(6), 1720–1741. doi:10.1177/0306624x16679162

Holt, T. J., Cale, J., Leclerc, B., & Drew, J. (2020). *Assessing the challenges affecting the investigative methods to combat online child exploitation material offenses. Aggression and Violent Behavior*, 55, 101464. doi:10.1016/j.avb.2020.101464

Hong, J., Park, S., Kim, S.-W., Kim, D., & Kim, W. (2017). *Classifying malwares for identification of author groups. Concurrency and Computation: Practice and Experience*, 30(3), e4197. doi:10.1002/cpe.4197

Huda, S., Abawajy, J., Abdollahian, M., Islam, R., & Yearwood, J. (2016). *A fast malware feature selection approach using a hybrid of multi-linear and stepwise binary logistic regression. Concurrency and Computation: Practice and Experience*, 29(23), e3912. doi:10.1002/cpe.3912

Ibrahim, S. (2016). *Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. International Journal of Law, Crime and Justice*, 47, 44–57 . doi:10.1016/j.ijlcj.2016.07.002

Kaakinen, M., Räsänen, P., Näsi, M., Minkkinen, J., Keipi, T., & Oksanen, A. (2017). *Social capital and online hate production: A four country survey. Crime, Law and Social Change*, 69(1), 25–39. doi:10.1007/s10611-017-9764-5

Kleemans, E. R., Korf, D. J., & Staring, R. (2008). *Mensen van vlees en bloed: kwalitatief onderzoek in de criminologie. Tijdschrift voor criminologie*, 51(4), 1.

Weulen Kranenbarg, M. (2018). *Cyber-offenders versus traditional offenders: An empirical comparison*. http://dare.ubvu.vu.nl/handle/1871/55530

Kumar, A., & Sachdeva, N. (2019). *Cyberbullying detection on social multimedia using soft computing techniques: a meta-analysis. Multimedia Tools and Applications*, 78(17), 23973–24010. doi:10.1007/s11042-019-7234-z

Lazarus, S. (2019). *Just married: the synergy between feminist criminology and the Tripartite Cybercrime Framework. International Social Science Journal*. doi:10.1111/issj.12201

Lee, G. (2019). *What roles should the government play in fostering the advancement of the internet of things? Telecommunications Policy*, 43(5), 434–444. doi:10.1016/j.telpol.2018.12.002

Lee, I. (2020). *Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. Future Internet*, 12(9), 157. doi:10.3390/fi12090157

Lei, H. (2019). *Modern information warfare: analysis and policy recommendations. Foresight*, 21(4), 508–522. doi:10.1108/fs-06-2018-0064

Leppänen, A., & Kankaanranta, T. (2017). *Cybercrime investigation in Finland. Journal of Scandinavian Studies in Criminology and Crime Prevention*, 18(2), 157–175. doi:10.1080/14043858.2017.1385231

Leukfeldt, R. (2018). *De 'human' factor in cybersecurity*: *Intreerede.* Den Haag: Haagse Hogeschool.

Leukfeldt, E. R., & Holt, T. J. (2019). *Examining the Social Organization Practices of Cybercriminals in the Netherlands Online and Offline. International Journal of Offender Therapy and Comparative Criminology*, 64(5), 522–538. doi:10.1177/0306624x19895886

Leukfeldt, E. R., Kleemans, E. R., Kruisbergen, E. W., & Roks, R. A. (2019). *Criminal networks in a digitised world: on the nexus of borderless opportunities and local embeddedness. Trends in Organized Crime*, 22(3), 324–345. doi:10.1007/s12117-019-09366-7

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2016). *A typology of cybercriminal networks: from low-tech all-rounders to high-tech specialists. Crime, Law and Social Change*, 67(1), 21–37. doi:10.1007/s10611-016-9662-2

Leukfeldt, R., Kleemans, E., & Stol, W. (2017). *The Use of Online Crime Markets by Cybercriminal Networks: A View From Within. American Behavioral Scientist*, 61(11), 1387–1402. doi:10.1177/0002764217734267

Leukfeldt, E. R., Lavorgna, A., & Kleemans, E. R. (2016). *Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime. European Journal on Criminal Policy and Research* , 23(3), 287–300. doi:10.1007/s10610-016-9332-z

Leukfeldt, E. R., & Yar, M. (2016). *Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. Deviant Behavior*, 37(3), 263–280. doi:10.1080 /01639625.2015.1012409

Levi, M., Doig, A., Gundur, R., Wall, D., & Williams, M. (2016). *Cyberfraud and the implications for effective risk-based responses: themes from UK research. Crime, Law and Social Change*, 67(1), 77–96. doi:10.1007/s10611-016-9648-0

Liao, R., Balasinorwala, S., & Raghav Rao, H. (2017). *Computer assisted frauds: An examination of offender and offense characteristics in relation to arrests. Information Systems Frontiers*, 19(3), 443–455. doi:10.1007/s10796-017-9752-4

Lilley, C. M. (2016). *The Role of Technology in Managing People Who Have Been Convicted of Internet Child Abuse Image Offences. Child Abuse Review*, 25(5), 386–398. doi:10.1002/car.2444

Lopez, M. A., Lombardo, J. M., López, M., Alba, C. M., Velasco, S., Braojos, M. A., & Fuentes-García, M. (2020). *Intelligent Detection and Recovery from Cyberattacks for Small and Medium-Sized Enterprises. International Journal of Interactive Multimedia and Artificial Intelligence*, 6(3), 55. doi:10.9781/ijimai.2020.08.003

Lowry, P. B., Zhang, J., Wang, C., & Siponen, M. (2016). *Why Do Adults Engage in Cyberbullying on Social Media? An Integration of Online Disinhibition and Deindividuation Effects with the Social Structure and Social Learning Model. Information Systems Research*, 27(4), 962–986. doi:10.1287/isre.2016.0671

Luna, R., Rhine, E., Myhra, M., Sullivan, R., & Kruse, C. S. (2016). *Cyber threats to health information systems: A systematic review. Technology and Health Care*, 24(1), 1–9. doi:10.3233/thc-151102

Lusinga, S., & Kyobe, M. (2017). *Testing a Typology of Mobile Phone Victimisation Using Cluster Analysis. The Electronic Journal of Information Systems in Developing Countries*, 78(1), 1–36. doi:10.1002/j.1681-4835.2017.tb00574.x

Marcum, C. D., & Higgins, G. E. (2019). *Examining the Effectiveness of Academic Scholarship on the Fight Against Cyberbullying and Cyberstalking. American Journal of Criminal Justice*, 44(4), 645–655. doi:10.1007/s12103-019-09482-8

Marcum, C. D., Higgins, G. E., & Nicholson, J. (2016). *I'm Watching You: Cyberstalking Behaviors of University Students in Romantic Relationships. American Journal of Criminal Justice*, 42(2), 373–388. doi:10.1007/s12103-016-9358-2

Maurer, T. (2019). *A Dose of Realism: The Contestation and Politics of Cyber Norms. Hague Journal on the Rule of Law*, 12(2), 283–305. doi:10.1007/s40803-019-00129-8

McGlynn, C., Rackley, E., & Houghton, R. (2017). *Beyond "Revenge Porn": The Continuum of Image-Based Sexual Abuse. Feminist Legal Studies*, 25(1), 25–46. doi:10.1007/s10691-017-9343-2

Megira, S., Pangesti, A. R., & Wibowo, F. W. (2018). *Malware Analysis and Detection Using Reverse Engineering Technique. Journal of Physics: Conference Series*, 1140, 012042. doi:10.1088/1742-6596/1140/1/012042

Meijer, R. F., Braak, S. W. van den., & Choenni, R. (2020). *Criminaliteit en rechtshandhaving 2019: ontwikkelingen en samenhangen* (Cahier 2020-16). Wetenschappelijk Onderzoek- en Documentatiecentrum. https://www.rijksoverheid.nl /documenten/ rapporten /2020/10/27/tk-bijlage-criminaliteit-en-rechtshandhaving-2019

Misana-ter Huurne, E., Van Houten, Y., Spithoven, R., Notté, R., & Leukfeldt, R. (2020, februari). *Cyberweerbaarheid: risicobewustzijn en zelfbeschermend gedrag rondom cybercriminaliteit onder jongeren en mkb-ers.* Saxion. https://www.saxion.nl/binaries /content/assets/onderzoek/areas--living/maatschappelijke-veiligheid/saxion--haagse-hogeschool---cyberweerbaarheid.-risicobewustzijn-en-zelfbeschermend-gedrag-rondom-cybercrime-onder-jongeren-en-mkb-ers..pdf

Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glenn, T. (2021). *Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry. Current Psychiatry Reports*, 23(4). doi:10.1007/s11920-021-01228-w

Mukhopadhyay, A., Chatterjee, S., Bagchi, K. K., Kirs, P. J., & Shukla, G. K. (2017). *Cyber Risk Assessment and Mitigation (CRAM) Framework Using Logit and Probit Models*

*for Cyber Insurance. Information Systems Frontiers*, 21(5), 997–1018. doi:10.1007/s10796-017-9808-5

Munnichs, G., Kouw, M., & Kool, L. (2017). *Een nooit gelopen race – Over cyberdreigingen en versterking van weerbaarheid. Rathenau Instituut.*

Nielsen, J. C., Kautzner, J., Casado-Arroyo, R., Burri, H., Callens, S., Cowie, M. R., & Fraser , A. G. (2020). *Remote monitoring of cardiac implanted electronic devices: legal requirements and ethical principles - ESC Regulatory Affairs Committee/EHRA joint task force report. EP Europace*, 22(11), 1742–1758. doi:10.1093/europace/euaa168

Norris, D. F., Mateczun, L., Joshi, A., & Finin, T. (2019). *Cyberattacks at the Grass Roots: American Local Governments and the Need for High Levels of Cybersecurity. Public Administration Review*, 79(6), 895–904. doi:10.1111/puar.13028

O'Malley, R. L., & Holt, K. M. (2020). *Cyber Sextortion: An Exploratory Analysis of Different Perpetrators Engaging in a Similar Crime. Journal of Interpersonal Violence*, 088626052090918. doi:10.1177/0886260520909186

Paoli, L., Visschers, J., & Verstraete, C. (2018). *The impact of cybercrime on businesses: a novel conceptual framework and its application to Belgium. Crime, Law and Social Change*, 70(4), 397–420. doi:10.1007/s10611-018-9774-y

Paquet-Clouston, M., Décary-Hétu, D., & Bilodeau, O. (2017). *Cybercrime is whose responsibility? A case study of an online behaviour system in crime. Global Crime*, 19(1), 1–21. doi:10.1080/17440572.2017.1411807

Parfenov, D., Zabrodina, L., Torchin, V., & Parfenov, A. (2019). *Approaches to find vulnerabilities and security in the digital production networks. Journal of Physics: Conference Series*, 1399, 022061. doi:10.1088/1742-6596/1399/2/022061

Payne, B. K., Hawkins, B., & Xin, C. (2018). *Using Labeling Theory as a Guide to Examine the Patterns, Characteristics, and Sanctions Given to Cybercrimes. American Journal of Criminal Justice*, 44(2), 230–247. doi:10.1007/s12103-018-9457-3

Payne, D., & Kennett-Hensel, P. A. (2017). *Combatting Identity Theft: A Proposed Ethical Policy Statement and Best Practices. Business and Society Review*, 122(3), 393–420. doi:10.1111/basr.12121

Payne, K., Maras, K. L., Russell, A. J., Brosnan, M. J., & Mills, R. (2020). *Self-reported motivations for engaging or declining to engage in cyber-dependent offending and the role of autistic traits. Research in Developmental Disabilities,* 104, 103681. doi:10.1016/j.ridd.2020.103681

Payne, B., May, D. C., & Hadzhidimova, L. (2018). *America's most wanted criminals: comparing cybercriminals and traditional criminals. Criminal Justice Studies*, 32(1), 1–15. doi:10.1080/1478601x.2018.1532420

Payne, K.-L., Russell, A., Mills, R., Maras, K., Rai, D., & Brosnan, M. (2019). *Is There a Relationship Between Cyber-Dependent Crime, Autistic-Like Traits and Autism? Journal of Autism and Developmental Disorders*, 49(10), 4159–4169. doi:10.1007/s 10803-019-04119-5

Pereira, F., & Matos, M. (2015). *Cyber-Stalking Victimization: What Predicts Fear Among Portuguese Adolescents? European Journal on Criminal Policy and Research*, 22(2), 253–270. doi:10.1007/s10610-015-9285-7

Pektaş, A., & Acarman, T. (2018). *Botnet detection based on network flow summary and deep learning. International Journal of Network Management*, 28(6), e2039. doi:10.1002/nem.2039

Pektaş, A., & Acarman, T. (2018). *Deep learning to detect botnet via network flow summaries. Neural Computing and Applications*, 31(11), 8021–8033. doi:10.1007/s00521-018-3595-x

Rashkovski, D., Naumovski, V., & Naumovski, G. (2015). *Cybercrime Tendencies and Legislation in the Republic of Macedonia. European Journal on Criminal Policy and Research*, 22(1), 127–151. doi:10.1007/s10610-015-9277-7

Ravindran, S., Moorthy, V. & Venkataraman, R., 2019. *An Approach to Secure Software Defined Network against Botnet Attack. Journal of Physics: Conference Series*, 1362, p.012127. Available at: http://dx.doi.org/10.1088/1742-6596/1362/1/012127.

Renaud, K., Orgeron, C., Warkentin, M., & French, P. E. (2020). *Cyber Security Responsibilization: An Evaluation of the Intervention Approaches Adopted by the Five Eyes Countries and China. Public Administration Review*, 80(4), 577–589. doi:10.1111/puar.13210

Reveron, D. S., & Savage, J. E. (2020). *Cybersecurity Convergence: Digital Human and National Security. Orbis*, 64(4), 555–570. doi:10.1016/j.orbis.2020.08.005

Ronaldson, N. (2019). *Hacking: the naked age cybercrime, clapper & standing, and the debate between state and federal data breach notification laws. Northwestern Journal of Technology and Intellectual Property*, 16, 305

Sardi, A., Rizzi, A., Sorano, E., & Guerrieri, A. (2020). *Cyber Risk in Health Facilities: A Systematic Literature Review. Sustainability*, 12(17), 7002. doi:10.3390/su12177002

Saridakis, G., Benson, V., Ezingeard, J.-N., & Tennakoon, H. (2016). *Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. Technological Forecasting and Social Change*, 102, 320–330. doi:10.1016/j.techfore.2015.08.012

Sepúlveda Estay, D. A., Sahay, R., Barfod, M. B., & Jensen, C. D. (2020). *A systematic review of cyber-resilience assessment frameworks. Computers & Security*, 97, 101996. doi:10.1016/j.cose.2020.101996

Sergi, A. (2016). *National Security vs Criminal law. Perspectives, Doubts and Concerns on the Criminalisation of Organised Crime in England and Wales. European Journal on Criminal Policy and Research*, 22(4), 713–729. doi:10.1007/s10610-016-9304-3

Shah, S., Shah, B., Amin, A., Al-Obeidat, F., Chow, F., Moreira, F. J. L., & Anwar, S. (2019). *Compromised user credentials detection in a digital enterprise using behavioral analytics. Future Generation Computer Systems*, 93, 407–417. doi:10.1016/j.future.2018.09.064

Shaji, R. S., Sachin Dev, V., & Brindha, T. (2018). *A methodological review on attack and defense strategies in cyber warfare. Wireless Networks*, 25(6), 3323–3334. doi:10.1007/s11276-018-1724-1

Shamsi, J. A., Zeadally, S., Sheikh, F., & Flowers, A. (2016). *Attribution in cyberspace: techniques and legal implications. Security and Communication Networks*, 9(15), 2886–2900. doi:10.1002/sec.1485

Shillair, R., Cotten, S. R., Tsai, H.-Y. S., Alhabash, S., LaRose, R., & Rifon, N. J. (2015). *Online safety begins with you and me: Convincing Internet users to protect themselves. Computers in Human Behavior*, 48, 199–207. doi:10.1016/j.chb.2015.01.046

Shukan, A., Abdizhami, A., Ospanova, G., & Abdakimova, D. (2019). *Crime control in the sphere of information technologies in the Republic of Turkey. Digital Investigation*, 30, 94–100. doi:10.1016/j.diin.2019.07.005

Șinca, G. M. (2015). *Cybercriminology transition from traditional criminal techniques to cybercrime. Agora International Journal of Juridical Sciences*, 9(1), 63–70. doi:10.15837/aijjs.v9i1.1910

Spithoven, R. (2020). *Verbonden risico's. Maatschappelijke veiligheid in de black box society* (1). The Hague, The Netherlands: Boom criminology Den Haag.

Tcherni, M., Davies, A., Lopes, G., & Lizotte, A. (2016). *The Dark Figure of Online Property Crime: Is Cyberspace Hiding a Crime Wave? Justice Quarterly*, 33(5), 890–911. doi:10.1080/07418825.2014.994658

TNO. (n.d.). *Cybersecurity: het belang van integrale oplossingen*. Retrieved April 23, 2020, from https://www.tno.nl/nl/aandachtsgebieden/defensie-veiligheid/roadmaps/nationale-veiligheid/cybersecurity-het-belang-van-integrale-oplossingen/

Vaczi, D., & Szadeczky, T. (2019). *A Threat for the Trains: Ransomware as a New Risk. Interdisciplinary Description of Complex Systems*, 17(1), 1–6. doi:10.7906/indecs.17.1.1

van der Kleij, R., de Bruin, I., van 'T Hoff-de Goede, S., Ancher, M., & Leukfeldt, R. (2019, 4 maart). *Cybercriminaliteit leeft niet onder retailers*. Centrum voor Criminaliteitspreventie en Veiligheid (CCV). https://ccv-secondant.nl/platform/article/cybercriminaliteit-leeft-niet-onder-retailers

Van der Kleij, R., Wijn, R., & Hof, T. (2020). *An application and empirical test of the Capability Opportunity Motivation-Behaviour model to data leakage prevention in financial organizations. Computers & Security*, 97, 101970. doi:10.1016/j.cose.2020.101970

van ’t Zelfde, W. (2017, 2 maart). *“Burgers beveiligen data onvoldoende tegen cybercriminaliteit”*. Trouw. https://www.trouw.nl/nieuws/burgers-beveiligen-data-onvoldoende-tegen-cybercriminaliteit~b05f7f48/

Visu, P., Lakshmanan, L., Murugananthan, V., & Cruz, M. V. (2019). *Software-defined forensic framework for malware disaster management in Internet of Thing devices for extreme surveillance. Computer Communications*, 147, 14–20. doi:10.1016/j.comcom.2019.08.013

Wang, S.-Y. K., Hsieh, M.-L., Chang, C. K.-M., Jiang, P.-S., & Dallier, D. J. (2020). *Collaboration between Law Enforcement Agencies in Combating Cybercrime: Implications of a Taiwanese Case Study about ATM Hacking. International Journal of Offender Therapy and Comparative Criminology*, 65(4), 390–408. doi:10.1177/0306624x20952391

Weinstein, N. D. (1989). *Effects of personal experience on self-protective behavior. Psychological Bulletin*, 105(1), 31–50. doi:10.1037/0033-2909.105.1.31

Westlake, B. G., & Bouchard, M. (2016). *Liking and hyperlinking: Community detection in online child sexual exploitation networks. Social Science Research*, 59, 23–36. doi:10.1016/j.ssresearch.2016.04.010

Willison, R., Warkentin, M., & Johnston, A. C. (2016). *Examining employee computer abuse intentions: insights from justice, deterrence and neutralization perspectives. Information Systems Journal*, 28(2), 266–293. doi:10.1111/isj.12129

Yang, S. C. (2019). *A curriculum model for cybersecurity master’s program: A survey of AACSB-accredited business schools in the United States. Journal of Education for Business*, 94(8), 520–530. doi:10.1080/08832323.2019.1590296

## Footnotes

[1]The excel file with all relevant literature can be requested by the author via mail: e.foppen@saxion.nl.

[2]The excel file with all relevant literature can be requested by the author via mail: e.foppen@saxion.nl.

[3] Bahuguna et al., 2019; Lee, 2020

[4] Bahuguna et al., 2019; Chang & Coppel, 2020; Croke, 2020

[5] Bahuguna et al., 2019; Chang & Coppel, 2020; Costa et al., 2019; Croke, 2020; Sardi et al., 2020; Vaczi & Szadeczky, 2019; Wang et al., 2020

[6] Bahuguna et al., 2019; Croke, 2020; Gosine, 2020; Lee, 2020; Sardi et al., 2020

[7] Chang & Coppel, 2020

[8] Sardi et al., 2020

[9] Bahuguna et al., 2020; Chang & Coppel, 2020; Lee, 2020

[10] Chang & Coppel, 2020

[11] Chang & Coppel, 2020

[12] Chang & Coppel, 2020; Norris, Mateczun, Joshi & Finin, 2019; Renaud et al., 2020

[13] Norris et al., 2019

[14] Lee, 2019

[15] Armstrong, in Billingsley, 2019; Haddad & Binder, 2019; Renaud et al., 2020; Reverson & Savage, 2020; Van der Kleij, Wijn & Hof, 2020

[16] Armstrong, in Billingsley, 2019; Haddad & Binder, 2019; Renaud et al., 2020; Reverson & Savage, 2020; Van der Kleij, Wijn & Hof, 2020

[17] Holt et al., 2020; Renaud et al., 2020

[18] Haddad & Binder, 2019

[19] Wang et al., 2020

[20] Holt er al., 2020

[21] Holt er al., 2020

[22] Nielsen et al., 2020

[23] Nielsen et al., 2020

[24] Nielsen et al., 2020

[25] de Kimpe et al., 2020

[26] The search string yielded 334 hits in the past two years and 820 hits in the past five years.

[27] At the start of this study, it was planned to conduct interviews with actors from Dutch practise. In this way a comparison could be made between cyber governance in The Netherlands and abroad. Based on this comparison, recommendations could have been made about the Dutch governance of cybercrime. However, the corona pandemic has caused an

enormous increase in cybercrime and that is why the professionals did not have enough time to participate in this research. This caused delays and it was therefore ultimately decided to focus this study only on the literature and to study the situation in The Netherlands when professionals are more accessible again.

# Appendices

## Appendix A: data extraction form literature review into conceptualization cybercrime

---

**Data extraction form "what is cybercrime?"**

---

**Study Title……..**

**Reviewer…….**

**Date…….**

**Keywords……...**

**Concerns research question 1 / 2 / 3**

| | |
|---|---|
| **First author** | |
| **Year of publication** | |
| **Country of publication** | |
| **Publication type** | Journal/Abstract/Other… |

| **Inclusion criteria** | **Criteria met?** |
|---|---|
| Language……... | Yes / No |
| Publication date…… | Yes / No |

Include study ☐ Exclude study ☐

**Reason for exclusion……...**

**……..**

**……..**

**Method and results**

| | |
|---|---|
| **Research question / goal** | |
| **Type of publication** | |
| | |
| **Definition cybercrime** | |
| **Types of cybercrime offenses included in definition** | |

**Appendix B: devices mentioned in literature to indicate cyberspace or (computer) technology**

| Components of cyberspace | Article |
|---|---|
| **Computer (networks)** | Payne, Russell, Mills, Maras, Rai & Brosnan, 2019; Cai, Du, Xin & Chang, 2018; Rashkoviski, Naumovski & Naumovski, 2015; Ibrahim, 2016; Broadhead, 2018; Payne, Hawkins & Xin, 2018; Payne, Maras, Russell, Brosnan & Mills, 2020; Carrapico & Barrinha, 2017; Shamsi, Zeadally, Sheikh and Flowers, 2016; Garrett, Mallia & Anthony, 2019 |
| **Internet networks** | Lazarus, 2019; Payne, Russell, Mills, Maras, Rai & Brosnan, 2019; Rashkoviski, Naumovski & Naumovski, 2015; Ibrahim, 2016; Holt, Burruss & Bossler, 2016; Sergi, 2016; Payne, Maras, Russell, Brosnan & Mills, 2020 |
| **ICT** | Lazarus, 2019; Broadhead, 2018; Carrapico & Barrinha, 2017; Rashkoviski, Naumovski & Naumovski, 2015; Leukfeldt & Yar, 2016 |
| **Information and data systems** | Cai, Du, Xin & Chang, 2018 |
| **Hardware devices or a network** | Shamsi, Zeadally, Sheikh and Flowers, 2016 |
| **Telephone lines or mobile networks** | Rashkoviski, Naumovski & Naumovski, 2015 |

## Appendix C: Techniques used in cybercrimes

| Title of publication | Authors | Publication year | Definition |
|---|---|---|---|
| **Phishing** | | | |
| Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime | Leukfeldt, Lavorgna & Kleemans | 2016 | A scalable act of deception whereby impersonation is used to obtain information from a target using digital means such as email. |
| The Use of Online Crime Markets by Cybercriminal Networks: A View From Within | Leukfeldt, Kleemans & Stol | 2017 | The process aimed at retrieving users' personal information by criminals posing as a trusted authority and thereby using digital means, such as email. |
| Computer assisted frauds: An examination of offender and offense characteristics in relation to arrests | Liao, Balasinorwala & Raghav Rao | 2017 | The act of sending fake messages to the victim, often in the disguise of bank notifications or emails promising monetary gains and romantic relationship, luring the victim into handing over sensitive information such as account number and password, or install malware on the victim's system |
| Cyber Risk Assessment and Mitigation (CRAM) Framework Using Logit and Probit Models for Cyber Insurance. | Mukhopadhyay, A., Chatterjee, S., Bagchi, K. K., Kirs, P. J., & Shukla | 2017 | Phishing is an approach for gaining information by duping the user |
| Examining the Social Organization Practices of Cybercriminals in the Netherlands Online and Offline. | Leukfeldt & Holt | 2019 | The process of deception, that is, impersonation, to retrieve personal information to get access to online bank accounts or credit card credentials |
| A typology of cybercriminal networks: from low-tech all-rounders to high-tech specialists. | Leukfeldt, Kleemans & Stol | 2016 | Process aimed at retrieving users' personal information by criminals who, by using digital means such as e-mail, pose as a trusted authority |
| Improving risk assessment model of cyber security using fuzzy logic inference system. | Alali, Almogren, Hassan, Rassan & Bhuiyan | 2018 | The criminal act of trying to direct access sensitive details such as credit card information, username and passwords |
| **Malware** | | | |

| | | | |
|---|---|---|---|
| Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime | Leukfeldt, Lavorgna & Kleemans | 2016 | Programs used to compromise computer systems and steal information. |
| Inequality in digital skills and the adoption of online safety behaviors | Dodel & Mesch | 2018 | Malicious software (malware) is a term used to describe different kinds of software that threaten the functionality, integrity and/or security of a device or network. |
| Software-defined forensic framework for malware disaster management in Internet of Thing devices for extreme surveillance | Visu, Lakshmanan, Murugananthan & Cruz | 2019 | Malware are the malicious software which often gain access to computer and cause damage to the in Internet of Thing (IoT) devices, without the knowledge of legitimate user |
| Assessing the Macro-Level Correlates of Malware Infections Using a Routine Activities Framework | Holt, Burruss & Bossler | 2016 | Software which can automate an attack process, acquire sensitive information, or interrupt critical system resources |
| Malware Analysis and Detection Using Reverse Engineering Technique. | Megira, Pangesti & Wibowo | 2018 | Any program or file that intentionally designed to harm, infiltrate or damage a computer, server or computer network<br><br>A malicious code that can disable or disrupt the operation of a system, allowing hackers to gain access to confidential and sensitive information and to spy on the computer and the owner of the computer itself |
| Anatomy of targeted attacks with smart malware. | Bahtiyar | 2016 | Malicious software that is used to harm a computer system intentionally or obtain sensitive information without permissions of owners |
| A fast malware feature selection approach using a hybrid of multi-linear and stepwise binary logistic regression. | Huda, Abawajy, Abdollahian, Islam & Yearwood | 2016 | A piece of malicious code that is specifically designed to perform illicit action on data, hosts or networks which is evolving as an epidemic in the digital world<br><br>Malware penetrates the computer network, breaks the secrecy and integrity policies of the data and steals confidential information, changes the control flow and functionality of a computer system |
| Classifying malwares for identification of author groups. | Hong, Park, Kim & Kim | 2017 | Software specifically designed to accomplish malicious tasks such as eavesdropping of private information, hijacking system control, and even destroying computer systems |
| Improving risk assessment model of cyber security using fuzzy logic inference system. | Alali, Almogren, Hassan, Rassan & Bhuiyan | 2018 | Taxonomy of software that takes the charge of a personal computer to distribute an infection to other social networks or devices |
| **Cyberbullying** | | | |

| | | | |
|---|---|---|---|
| Cyberbullying: what's the problem? | Deschamps & McNutt | 2016 | Bullying by electronic means that occurs through the use of technology, including computers or other electronic devices, social networks, text messaging, instant messaging websites or e-mail.<br><br>Cyberbullying means any electronic communication through the use of technology including, without limiting the generality of the foregoing, computers, other electronic devices, social networks, text messaging, instant messaging, websites and electronic mail, typically repeated or with continuing effect, that is intended or ought reasonably (to) be expected to cause fear, intimidation, humiliation, distress or other damage or harm to another person's health, emotional wellbeing, self-esteem of reputation, and includes assisting or encouraging such communication in any way.<br><br>Using the internet or other information or communication technologies, such as e-mail messages or text messages sent by cell phone or pager, to support deliberate, repeated and hostile behavior by an individual or group that is intended to harm someone else<br><br>Emotional, psychological or social bullying that occurs using technology to forward or spread hurtful messages and/or images through email, texting, social media or other forms of electronic communication. Cyberbullying is simply a different setting for bullying.<br><br>Bullying behavior which is carried out through an internet service such as email, chat room, blog, discussion group or instant messaging. It can also include bullying through mobile phone technologies and new internet technologies in the future. |
| Just married: the synergy between feminist criminology and the Tripartite Cybercrime Framework | Lazarus | 2019 | Bullying is an intentional, aggressive behavior, carried out repeatedly against a victim, whereas with cyberbullying, the power imbalance between bully and victim and the repetitiveness of the behavior typically involved in traditional bullying are often missing from the equation |
| Why Do Adults Engage in Cyberbullying on Social Media? An Integration of Online Disinhibition and Deindividuation Effects with the Social Structure and Social Learning Model. | Lowry, Zhang, Wang & Siponen | 2016 | Cyberbullying generally refers to deliberate and hostile behavior intended to harm people using the internet by leveraging the imbalance of power between bullies and victims |

| | | | |
|---|---|---|---|
| Cyberbullying detection on social multimedia using soft computing techniques: a meta-analysis. | Kumar & Sachdeva | 2019 | Bully someone in the digital realm<br><br>Bullying an individual or a group of individuals using Internet, mobiles or any other electronic device by sending inappropriate textual or non-textual multimedia message in order to hurt or cause embarrassment |
| Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. | Saridakis, Benson, Ezingeard & Tennakoon | 2016 | The use of e-mails, instant messaging and websites to inflict repeated harm wilfully on a person |
| Testing a Typology of Mobile Phone Victimisation Using Cluster Analysis. | Lusinga & Kyobe | 2017 | The exposure to negative actions (aggressive behavior or intentional harm-doing) which are done repeatedly and over time in a relationship where there is an imbalance of strength. Bullying can be conventional or cyber-based<br><br>Form of aggression committed using electronic means such as the internet, mobile technology and computers |
| **Spamming** | | | |
| SMSAD: a framework for spam message and spam account detection | Adewole, Anuar, Kamsin & Sangaiah | 2019 | Spamming is a method of spreading bulk unsolicited content usually for the purpose of advertisements, promoting pornographic websites, fake weight loss, bogus donations, fake news, online task scams, and a host of other malicious intents, which are perpetrated by spammers. |
| Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals | Ibrahim | 2016 | Mass-produced, unsolicited bulk messages |
| Authorship verification applied to detection of compromised accounts on online social networks | Barbon,Igawa & Bogaz Zarpelão | 2016 | Considering a spam any message containing a link to a fraudulent site with malicious content |
| Anatomy of targeted attacks with smart malware. | Bahtiyar | 2016 | One purpose of spams is to obtain personal information of users |
| Examining the Effectiveness of Academic Scholarship on the Fight Against Cyberbullying and Cyberstalking. | Marcum & Higgins | 2019 | Willful and repeated harm inflicted through the use of computers, cell phones, and electronic devices |
| Improving risk assessment model of cyber security using fuzzy logic inference system. | Alali, Almogren, Hassan, Rassan & Bhuiyan | 2018 | Stray emails sent out of the recipient's consent |
| **Online harassment** | | | |
| Just married: the synergy between feminist criminology and the Tripartite Cybercrime Framework | Lazarus | 2019 | Online harassment can be defined as the act of aggressively pressuring, intimidating, distressing or spread denigrating rumours about others |

| | | | |
|---|---|---|---|
| Computer assisted frauds: An examination of offender and offense characteristics in relation to arrests | Liao, Balasinorwala & Raghav Rao | 2017 | It includes online stalking, cyber bullying and spreading of inappropriate materials |
| Why Do Adults Engage in Cyberbullying on Social Media? An Integration of Online Disinhibition and Deindividuation Effects with the Social Structure and Social Learning Model. | Lowry, Zhang, Wang & Siponen | 2016 | Repeated or one-off malicious internet behaviors that are unsolicited but noticed by victims, which are intended to upset, disturb, or threaten other people. |
| **Cyber-fraud** | | | |
| Just married: the synergy between feminist criminology and the Tripartite Cybercrime Framework | Lazarus | 2019 | Cyber-fraud refers to the computer or/and internet-mediated acquisition of financial benefits by false pretence, impersonation, manipulation, counterfeiting, forgery or any other fraudulent representation of |
| **Revenge porn** | | | |
| Just married: the synergy between feminist criminology and the Tripartite Cybercrime Framework | Lazarus | 2019 | Revenge porn is defined as non-consensual sharing of sexually explicit images (including photographs) and/or videos, with an underlying motivation linked to revenge |
| Beyond "Revenge Porn": The Continuum of Image-Based Sexual Abuse. | McGlynn, Rackley & Houghton | 2017 | Non-cionsensual distribution of private, sexual images by a malicious ex-partner |
| **Child pornography** | | | |
| Liking and hyperlinking: Community detection in online child sexual exploitation networks | Westlake & Bouchard | 2016 | Child pornography includes "… any written material, visual representation or audio recording" of a person "under the age of eighteen years and is engaged in or is depicted as engaged in explicit sexual activity" |
| Challenges of protecting children from sexual abuse and exploitation on the internet: the case of Kosovo. | Dushi | 2018 | The provision criminalizes production, offering, distribution, production and even possession of child pornography when these are done electronically, though a computer system |
| **Cyber sextortion** | | | |
| Cyber Sextortion: An Exploratory Analysis of Different Perpetrators Engaging in a Similar Crime | O'Malley & Holt | 2020 | Cyber sextortion is part of a larger continuum of image-based sexual abuse (IBSA), which includes crimes such as revenge pornography and nonconsensual sexting, in which explicit images are used for harm |
| The Role of Technology in Managing People Who Have Been Convicted of Internet Child Abuse Image Offences. | Lilley | 2016 | A range of behaviors including viewing child abuse images, contact with like0minded offenders and the sexual grooming of children |
| **Cyberstalking** | | | |
| Just married: the synergy between feminist criminology and the Tripartite Cybercrime Framework | Lazarus | 2019 | Cyberstalking or "cyber dating abuse" can be defined as the use of the internet and other technological devices to monitor or harass another person in a threatening way |

| | | | |
|---|---|---|---|
| Cyber-Stalking Victimization: What Predicts Fear Among Portuguese Adolescents? | Pereira & Matos | 2015 | A set of repeated and planned stalking behaviors in which a person imposes inappropriate and unwanted forms of communication, contact or an intention to approach in virtual space |
| Why Do Adults Engage in Cyberbullying on Social Media? An Integration of Online Disinhibition and Deindividuation Effects with the Social Structure and Social Learning Model. | Lowry, Zhang, Wang & Siponen | 2016 | Series of repeated intrusive behaviors performed via the internet such as gathering private information or direct communication, that are intended to convey implicit and explicit threats and thus induce fear in online victims |
| I'm Watching You: Cyberstalking Behaviors of University Students in Romantic Relationship | Marcum, Higgins & Nicholson | 2016 | An adapted definition of physical stalking as applied to technology and electronic devices<br><br>The use of the internet and other technological devices to monitor or harass another person in a threatening way |
| **Digital piracy** | | | |
| Just married: the synergy between feminist criminology and the Tripartite Cybercrime Framework | Lazarus | 2019 | While digital piracy involves the illegal uploading or downloading of computer files, and software, offenders generally victimize creative artists, and their respective industries, whose creative works they acquire without paying for them |
| Parental Indifference and Children's Digital Piracy in South Korea: Mediation Effects of Low Self-Control and Misconception. | Baek, Nicholson, Higgins & Losavio | 2018 | Illegal downloading without payment of copyrighted software and media files on the internet |
| One Sail Fits All? A Psychographic Segmentation of Digital Pirates. | De Corte & Van Kenhove | 2015 | Illegal procurement of infringed copyrighted digital media files by (Bit)Torrent downloading via P2P networks |
| **Identity theft** | | | |
| Computer assisted frauds: An examination of offender and offense characteristics in relation to arrests | Liao, Balasinorwala & Raghav Rao | 2017 | It can include personal information, credit card, phone number and email addresses, which were then used in payment frauds, loan frauds ant other financial services |
| Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals | Ibrahim | 2016 | Unauthorized use of citctim's personally identifying information to commit fraud |
| Cyber Risk Assessment and Mitigation (CRAM) Framework Using Logit and Probit Models for Cyber Insurance. | Mukhopadhya, Chatterjee, Bagchi, Kirs & Shukla | 2017 | In an identity theft, the attacker uses techniques such as hacking, phishing, and pharming to obtain critical personal data (e.g., social security number, date of birth, mother's maiden name) or financial information (e.g., PIN numbers) or passwords, and uses the information to gain entry to bank accounts or for other financial gain. |

| | | | |
|---|---|---|---|
| Combatting Identity Theft: A Proposed Ethical Policy Statement and Best Practices. | Payne & Kennett-Hensel | 2017 | The unauthorized use or attempted use of an existing account, such as a credit or debit card, checking, savings, telephone, online or insurance account (Harrell and Langdon 2013, p. 1).<br><br>The use of personal information to open a new account, such as a credit or debit card, telephone, checking, savings, loan, or mortgage account (ibid, p. 2).<br><br>The "misuse of personal information for a fraudulent purpose, such as getting medical care, a task, or government benefits; renting an apartment or house; providing false information to law enforcement when charged with a crime or traffic violation (ibid, p. 2). |
| Cyber threats to health information systems: A systematic review. | Luna, Rhine, Myhra, Sullivan & Kruse | 2016 | Occurs when a person "knowingly transfers, possesses or uses, without lawful authority, a means of identification of another person with the intent to commit.. a violation of Federal law, or [an act] that constitutes a felony under any applicable State or local law |
| The quest for complete security: An empirical analysis of users' multi-layered protection from security threats. | Crossler, Bélanger & Ormond | 2017 | Having personal information taken by someone without permission |
| **Hacking** | | | |
| Computer assisted frauds: An examination of offender and offense characteristics in relation to arrests | Liao, Balasinorwala & Raghav Rao | 2017 | The specific action of using computer technology to illegally gain access to secured systems with the purpose of causing damage or stealing information |
| Cybercrime and cloud computing. A game theoretic network model | Bartholomae | 2017 | The term hacker is used to refer to people who either break into systems for which they have no authorization or intentionally overstep their bounds on systems for which they do have legitimate access |
| On the Value of Honeypots to Produce Policy Recommendations. | Holt | 2017 | The legal, legitimate use of knowledge of computers and networking to affect a piece of hardware or software, as well as the illicit application of such information |
| **Online hate** | | | |
| Social capital and online hate production: A four country survey | Kaakinen, Räsänen, Näsi, Minkkinen, Keipi & Oksanen | 2017 | Online hate involves the dissemination of racist or xenophobic content and acts that threaten or degrade indivdiuals or social groups |
| **DDos attacks** | | | |

| | | | |
|---|---|---|---|
| | | | DDos attacks work by flooding a web server or other Internet resource with more request that can be completed in millisecond intervals. The server cannot handle any additional requests, leading it to be unavailable to legitimate users for a certain period |
| Cyber Risk Assessment and Mitigation (CRAM) Framework Using Logit and Probit Models for Cyber Insurance. | Mukhopadhya, Chatterjee, Bagchi, Kirs & Shukla | 2017 | DoS attacks flood a router with malicious requests and shut out real customers from accessing services |
| A novel approach to defend multimedia flash crowd in cloud environment. | Bhushan & Gupta | 2017 | Attempt to disrupt the services of the authorized customers either by exhausting the bandwidth of the network or by exhausting the server resources |
| Cyber threats to health information systems: A systematic review. | Luna, Rhine, Myhra, Sullivan & Kruse | 2016 | Type of attack on a network designed to bring the network to its knees by flooding it with useless traffic |
| **Employee computer abuse** | | | |
| Examining employee computer abuse intentions: insight from justice, deterrence and neutralization perspectives | Willison, Warkentin & Johnston | 2016 | The unauthorized and deliberate misuse of computers and other forms of information technology of the local organization information systems by individuals' with inside access |
| **Botnet** | | | |
| Bots, cops, and corporations: on the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime | Dupont | 2016 | Networks of computers infected by malicious software that allows a criminal or "botmaster" to simultaneously control thousands, if not millions, of machines |
| Assessing the Macro-Level Correlates of Malware Infections Using a Routine Activities Framework | Holt, Burruss & Bossler | 2016 | Botnet malware remotely controls a network of multiple infected computers to coordinate attacks or to send spam |
| A survey of botnet detection based on DNS. | Alieyan, Almomani, Manasrah & Kadhum | 2015 | A group of compromised hosts running malicious software program for malicious purposes<br><br>A software program that manipulates computers for malicious purposes |
| New facets of mobile botnet: architecture and evaluation. | Anagnostopoulos, Kambourakis & Gritzalis | 2015 | A network consisting of infected and compromised computers, called bots, zombies or slaves, which are controlled by an attacker … botnets could be used for launching DDoS Attacks, sending spam emails on a massive scale, identity theft, distributing malware or even copyrighted material, and so forth |
| Anatomy of targeted attacks with smart malware. | Bahtiyar | 2016 | A set of infected computer systems that are controlled remotely by a third party |
| Deep learning to detect botnet via network flow summaries. | Pektas & Acarman | 2018 | The network of bots, which are compromised computer systems or devices on the internet |

| | | | |
|---|---|---|---|
| ZombieCoin 2.0: managing next-generation botnets using Bitcoin. | Ali, McCorry, Lee & Hao | 2017 | Networks of compromised machines, individually referred to as bots or zombies, and controlled remotely by a malicious entity known as the botmaster. They were originally developed as tools for vandalism and to showcase hacking skills and have evolved into sophisticated platforms geared towards financial gain and cyberwarfare |
| Botnet detection based on network flow summary and deep learning. | Pektas & Acarman | 2018 | A number of computers or devices managed on the internet to perform unintended malicious activities without the authorization of the sys |
| An Approach to Secure Software Defined Network against Botnet Attack. | Ravindran, Moorthy & Venkataraman | 2019 | Large swarm of computers that are connected to perform a number of repetitive tasks requested by the cybercriminals |
| **Cyberterrorism** | | | |
| Cyber threats to health information systems: A systematic review. | Luna, Rhine, Myhra, Sullivan & Kruse | 2016 | The convergence of terrorism and cyberspace directed towards a computer or network of information. This attack or breach steals information to damage or cause fear to an individual or group |
| **Cybersquatting** | | | |
| Cyber threats to health information systems: A systematic review. | Luna, Rhine, Myhra, Sullivan & Kruse | 2016 | When a person other than the owner of a well-known trademark registers that trademark as an Internet domain name and then attempts to profit from it either by ransoming the domain name back to the trademark owner or by using the domain name to divert business from the trademark owner to the owner of the domain name |
| **Data breach/loss** | | | |
| Cyber threats to health information systems: A systematic review. | Luna, Rhine, Myhra, Sullivan & Kruse | 2016 | The acquisition, access, use or disclosure of unsecured data, in a manner not permitted |
| The quest for complete security: An empirical analysis of users' multi-layered protection from security threats. | Crossler, Bélanger & Ormond | 2017 | Losing access to data or information stored electronically |
| **Cyber-aggression** | | | |
| Validity and reliability of the Cyber-aggression Questionnaire for Adolescents (CYBA). | Álvarez-García, Barreiro-Collazo, Núñez & Dobarro | 2016 | Intentionally harm, offend or hurt other adolescents |
| **Computer performance degradation** | | | |
| The quest for complete security: An empirical analysis of users' multi-layered protection from security threats**.** | Crossler, Bélanger & Ormond | 2017 | Having the computer noticeably slowing down when running programs |

**Appendix D: data extraction form literature review into actors and tasks in cyber governance**

---

**Data extraction form "which actors are currently involved in the governance of cybercrime?" and "what tasks do actors have in the governance of cybercrime?"**

---

**Study Title……..**

**Reviewer…….**

**Date…….**

**Keywords……...**

**Concerns research question 1 / 2 / 3**

| | |
|---|---|
| **First author** | |
| **Year of publication** | |
| **Country of publication** | |
| **Publication type** | Journal/Abstract/Other… |

| **Inclusion criteria** | **Criteria met?** |
|---|---|
| Language……... | Yes / No |
| Publication date…… | Yes / No |

Include study ☐ Exclude study ☐

**Reason for exclusion……...**

**……..**

**.**

……..

**Method and results**

| | |
|---|---|
| **Research question / goal** | |
| **Type of publication** | |
| | |
| **Actors included in study** | |
| **Place of actors in safety chain** | ☐Proaction<br>☐Prevention<br>☐Preparation<br>☐Repression<br>☐After care |
| **Responsibilities actors** | |