A qualitative exploration of the challenges the Danish police face in dealing with cybercrime

MAGNUS TIN MAYLAND
A qualitative exploration of the challenges the Danish police face in dealing with cybercrime

MAGNUS TIN MAYLAND

Mayland, T, M. A qualitative exploration of the challenges the Danish police face in dealing with cybercrime. Degree project in Criminology 30 Credits. Malmö University: Faculty of Health and Society, Department of Criminology, 2019.

Abstract
Cybercrimes have been rapidly increasing over the past decade becoming more sophisticated and increasing victimization, resulting in an increased load of the police in the effort to prevent and stop these crimes. This study explores the challenges the Danish police encounter facing cybercrime and their approach to preventing it. The data were collected through interviewing individuals on a managing level in two different departments dealing with cybercrime within the Danish police force. The data were analyzed thematically to identify key issues. The main challenges found being; the time frame the police has to act upon in reference to the nature of the data, the culture that exists on the internet and distinguishing jokes from threats, the effortlessness of criminals justifying once actions, and the visible presence of the police on the internet. The primary focus of prevention to deal with some of these issues is moving towards creating a healthy network between the police and the private sector, in an effort to create a shared responsibility and a forum of which information can be shared to create a possible united front towards cybercrime.

Keywords: Cybercrime, data-sharing, justification, responsibility, visibility
Table of content

INTRODUCTION ................................................................................................................. 3
Defining cybercrime ................................................................................................. 3
Challenges of cybercrime ....................................................................................... 3
Aim .......................................................................................................................... 5

METHOD ....................................................................................................................... 5
Interview .................................................................................................................. 6
Participants .............................................................................................................. 6
LCIK .......................................................................................................................... 6
NC3 ........................................................................................................................... 7
Analysis .................................................................................................................... 7
Ethics ......................................................................................................................... 7

RESULTS ...................................................................................................................... 7
Data ............................................................................................................................ 8
Culture ....................................................................................................................... 10
Justification of cybercrime ..................................................................................... 10
Prevention ................................................................................................................ 11

DISCUSSION .............................................................................................................. 13
Responsibility .......................................................................................................... 13
Data sharing ............................................................................................................. 14
Limitations ............................................................................................................... 15

CONCLUSION ............................................................................................................ 16

REFERENCES .......................................................................................................... 17

APPENDIX ................................................................................................................ 20
INTRODUCTION

In today’s digital age, where more and more applications are created to support us in our daily endeavors in life and digital systems are progressively having more control over our infrastructures, a new digital world has been born. This has given plenty of new opportunities for its users, but also new opportunities for these users to be exploited by criminals in the form of cybercrimes.

Cybercrimes have been on the rise in recent years, and from 2009-2016, the Danish police saw an increase of three-hundred fifty percent in it-related economic crimes alone (Politiet. 2019). This is an alarming increase and adding to its eeriness both police and independent studies have found that cybercrimes are largely under-reported by both private individuals and companies (Leppänen, A et al. 2016; Politiet. 2017). This development has instilled some fear in the public, and seventy-eight percent of the public feels distressed about the risk of having their payment details or other information stolen and misused (Politiet. 2019). These issues are also worrying in the context that Denmark is the leading country in the I-DESI report (The International Digital Economy and Society Index) which measures the digital economy performance of countries (European Commission. 2018). The Danish police, therefore, face an enormous task in dealing with this increase in cybercrime and public distress.

Defining cybercrime
To explore the field of cybercrime, we first need to understand what the term covers. In everyday language, cybercrime will often lead one’s thoughts towards hacking and malware, but cybercrime covers a much broader range of crimes, ranging from digital piracy to child abuse and sexual exploitation. It reaches far and wide, in both the types of crimes and the physical distances. One frequently used way of defining cybercrime, is by dividing it into two categories ‘cyber-dependent’ and ‘cyber-enabled’ (Hadlington L et al. 2018). Cyber-dependent meaning crimes that can only happen through the use of computers or similar technology, this would be such things as hacking, cyber espionage, and malware attacks. Cyber-enabled, on the other hand, is traditional crimes which are now moving to cyberspace, changing its structure and perhaps enhancing and increasing the speed of the crimes, an example of this could be fraud (ibid.). The Danish police use the same definitions of cybercrime, but adds one more category to the list, ‘cyber-enabling of criminal content.’ This category relates to cyber-enabled but focuses on the content which is uploaded or expressed, such as sexual assault of children (Politiet. 2017). This definition and its categories stretch over a large body of crimes, showing that the police are now facing a “second” world of which they must protect its citizens and enforce the laws.

Challenges of cybercrime
The challenges of cybercrime have started to see exploration from different researchers, with many different angles and perspectives. One of such studies is from Cameron S. D. Brown (2015), who did extensive research on the limits of the criminal justice process, legal loopholes and enabling technologies which facilitate and complicates the process of preventing cybercrime. Brown does this from an Australian perspective and shows through a fictive example the issues that common law presents for investigating and prosecuting cybercrime. Furthermore, even if these legal issues would be fixed, the broader criminal justice system is faced by an important task of communicating a shared
understanding regarding technical skills, knowledge, and roles performed during investigation and prosecution (Brown, S.D Cameron. 2015). This issue is also highlighted by Hadlington, Lumsden, Black, and Ferra (2018) who did a qualitative study in the UK of police officers experiences, challenges, and perceptions of cybercrime. They found that police officers, have difficulties in defining cybercrime and had frustrations in relations to lack of knowledge and the power to deal with cybercrime (ibid.). Furthermore, they had difficulties in keeping up with the rapid development of cybercrime and its new methods in contrast to the length of investigations as well as training within the area of cybercrime (ibid.).

The challenges of cybercrime from a police perspective is explored by Yvonne Jewkes and Majid Yar (2008) as well. They examine the challenges with certain types of cybercrimes such as child pornography, hate crimes, electronic theft, invasion of privacy, and more, taking basis in the UK. Finding challenges such as but not limited to the sheer volume of material that is generated, legislation problems within and between countries, under-reporting, limited resources and police culture (ibid.). They illustrate that we are just only beginning to figure out how to police the internet and create better results, that we still face many challenges which need to be solved and it might not only be the police we rely on but a shared responsibility of several actors (ibid.).

Routine activity theory and its three requirements for crime; likely offender, suitable target and absent guardian, is another perspective to cybercrime that has been discussed in research (Cohen, L. & Felson, M. 1979). Routine activity theory is discussed as part of the background for cybercrime by Leppänen, Kiravuo, and Kajantie (2016). They give examples of how the internet and our technologies offer plentiful of suitable targets with absent guardians, which likely offenders could attack and the fact that the internet is global only increases the pool of likely offenders. Routine activity theory is also explored from the perspective of the suitable target themselves acting as capable guardians by Graham and Triplett (2016). They did this by looking at the digital literacy of individuals and comparing it to the number of phishing emails they got and how they responded to them. They found that with higher digital literacy, individuals respond to receiving more phishing emails as well as responding less to them. Secondly, they found that social position also affects the number of phishing emails individuals receive as with higher income and education, the likelihood of being a part or reliant on different computer networks increases (ibid.). Routine activity theory has further been tested through quantitative methods in a cybercrime environment by Leukfeldt and Yar (2016), who tested routine activity theory with six different cybercrimes with several variables. They found visibility to play a role. However, the results were mixed across the different types of crimes giving an inconclusive conclusion as to whether routine activity theory is fully applicable.

Graham and Triplett’s research is very much complimented by Bele, Dimec, Rozman, and Jemecs (2014) article on raising awareness for children and teenagers as a means of preventing and protecting against cybercrime. They suggest that implementing educational modules targeting youngster, as a first step towards creating an information security culture (Bele, J.L et al. 2014). This focus on awareness is however not only seen pushed towards young people but also the global business world. Various articles and studies suggest and push for a higher priority of cybersecurity and cooperation between the private and government
sector. (Brown, 2015; Eddolls 2016; Leppänen et al., 2016; Stanciu, & Tinca. 2017). This is because cybercrime is still under-reported, and companies possess a considerable amount of data for the police to use and to uncover these dark numbers. The police can therefore not face this threat alone, as they are often not the first capable guardian the cybercriminals face, but rather the companies themselves their systems, employees, and private individuals themselves.

**Aim**

The increase in cybercrime and the constant development of technologies presenting new opportunities for cybercriminals to exploit shows the importance of focusing on understanding it and preventing it. This is further supported by Hutchings and Holts (2018) study about the difficulties of researching cybercrime, they say, and I quote:

> *Taken as a whole, this study demonstrates the need for future scholars to continue to use qualitative methodologies to better understand the evolution of cybercriminality. The depth of information that can be developed from robust interview protocols can improve our understanding of practices of actors, their motivations, and decision-making processes.* – (Hutchings & Holt 2018 p. 19)

This study aims to explore the Danish police’s perspective and approach to cybercrime on a management level. The research will use semi-constructed interviews to delve into the world of the police and examine the challenges and processes they face. The overarching research question is as such:

- What are the obstacles in doing police work and researching cybercrime, and how do the police approach prevention of the matter?

The following structure of the thesis will be as follows: The next section will consist of a description of the methodologies used in gathering the data as well as analyzing it. This will be followed by the results of the study, describing the experiences of the police and their perspective. The thesis will then end with a discussion and analysis of the results in regard to the background material.

**METHOD**

The data used in this qualitative study consist of interviews gathered on a management level within the police. The purpose of the interviews is to explore the perspective of the Danish police on cybercrime and identify the challenges they are facing in combating it. The inspiration for the method of this study was taken from two similar studies on cybercrime. One is exploring the perspective of Finland through expert interviews and the other exploring the challenges that police officer face with cybercrime (Hadlington, L et al 2018; Leppänen, A. et al 2016).
Interview

A total of two interviews were conducted with a total of three participants. One interview had two participants being interviewed from two different departments of the national center for cybercrime. The number of interviews is low, but the participants are key individuals that cover and have the insight into the overall structure and aims of the different police cybercrime departments, therefore keeping the data quality reasonable with the aim in mind. The validity and reliability of the data are supported by the coherence of the answers as there were no significant discrepancies in their answers and descriptions, giving the impression that it was the overall perspective of the Danish police. Having two people being interviewed at once can have its merits and demerits. The respondents can be uncomfortable with the other being there and not be as open or as confident in their responses. However, it can also open for more in-depth discussions as their knowledge supplement each other and cover each other’s shortcomings. In this case, the reason for having two participants was a choice done by the participants because of a time issue. The interviews lasted for about an hour each. The questions formulated were mostly made to get descriptions of the situations they were facing and how they handled them and not their personal opinion. Thus, having key individuals as respondents, was more important than having a multitude of interviews.

To help conduct and streamline the interviews, *Interview: introduction til et håndværk* by Steiner Kvale and Svend Brinkmann (2009) were used. The chosen method for conducting the interviews was the semi-structured approach to ensure that the interviews and the questions, would not limit or direct the perspective of the participants and therefore stay as accurate to their perspective as possible, but keep it within the intended theme. To conduct the interviews and ensure that they met the quality needed for academic purposes an interview guide (see appendix 1) was constructed using Steiner and Brinkmann’s guidelines for the qualitative interview (Steiner, Brinkmann. 2009). Furthermore, in creating the interview guide and during the interview, Steiner’s and Brinkmann’s quality criteria has been kept in mind to create the best possible scenario for further analysis. The interviews have been recorded and later transcribed for use in the analysis phase.

Participants

The participants were chosen and contacted by email, based on networking and research about the structure and departments of the Danish police to find the best suited and available informants on a managing level. The participants were from two different departments of the police. One was from LCIK (Landsdækkende Center mod It-relateret økonomisk Kriminalitet) the national center for it-related economical crime and the other with two participants were from the national center for cybercrime (NC3), both in managing positions with a focus on different types of cybercrime.

LCIK

LCIK is a centralized department, stationed in Valby near Copenhagen. The task of this unit is to handle all of the preliminary investigation surrounding it-related economic crimes across Denmark. The center was created as the police saw a need for centralizing the investigation of these types of crimes. The investigations of these crimes were too prolonged, as the victims of these crimes were scattered nationwide and the reports to the individual precincts and jurisdictions made it challenging to collect and find connections in a timely manner, as well as the
crime scene, was no longer within a precinct area but instead on the internet. The initiative to create LCIK was therefore launched in November 2017, and LCIK was ready for its first reports 3. December 2018 (Madsen, J. 2019).

NC3
NC3 is another centralized department of the police which takes care of cybercrime in general or crimes where computers or other gadgets have been used and needs to be examined for evidence and information. This department does a sort of IT-forensic work and is therefore in touch with many kinds of crimes, from child pornography, national hacking, terror, to economic crimes in some cases (PET. 2019).

Analysis
The interviews have been analyzed using a thematic approach, like Braun and Clark (2006) suggests, using their steps of familiarization, generation of code, creating themes, reviewing and refining (ibid.). The different themes formed from the transcribed material have been grouped to create four overarching themes, which contain sub-themes (see table 1 in the results section). These themes intend to keep the results within a frame, as the broadness of the study could course confusion as well as damage the focus of the study by straying in too many directions. Quotes from the respondents are furthermore provided when found appropriate to illustrate situations and challenges in their own words. One thing that could have been helpful and improve the overall results and analysis, would be follow up interviews digging into the generated themes to get a deeper understanding and opinion of those.

Ethics
This thesis does not touch upon any sensitive personal data of individuals and instead moves in the sphere of general opinions, strategies, and views of the police. However, the anonymity of the people who have been interviewed and if they wish to stay anonymous is essential to keep in mind. This has been cleared with all participants of the study. Furthermore, there is ethical importance in the handling of the recorded data and the transcriptions of it, as for it not to be misused. The intent is to destroy this data after the end of the thesis so others cannot use it in any wrong manners. Quoting the interviewees is also essential to consider, and when doing so, the quote and the interpretation of it should always be sent and approved by the individual before it is used in the thesis.

RESULTS
The analysis of the data revealed four initial overarching themes with several additional sub-themes, which is as shown in table 1. Each of the sub-themes is discussed in the context of its relating overarching theme. The following text will consist of the findings within each of the overarching themes following the structure from the table; data, culture, justification, and prevention.
Table 1 – Generated themes

<table>
<thead>
<tr>
<th>Themes</th>
<th>Data</th>
<th>Culture</th>
<th>Justification</th>
<th>Prevention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sub-themes</td>
<td>Data quality</td>
<td>Traditions</td>
<td>Moral</td>
<td>Police visibility</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Evanescent data</td>
<td>Technology</td>
<td>Distance to</td>
<td>Priority</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>others</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Statistics</td>
<td>Hobbies</td>
<td>Capable</td>
<td>Resources</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>guardian</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time</td>
<td>Internet and the way we</td>
<td>Finding</td>
<td>Responsibility</td>
<td></td>
</tr>
<tr>
<td></td>
<td>speak</td>
<td>others with</td>
<td>Private sector</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>similar</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>interest</td>
<td>Learning</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>process</td>
<td></td>
</tr>
</tbody>
</table>

Data

Data were an ongoing theme in both interviews, as would naturally happen when dealing with digital information and the internet in general. All the interviewees mentioned how data is both a problem solver and an obstacle at the same time. The data itself is not so much an obstacle, but the nature of it is. What is meant by this, is that useful quality data can give the police a tremendous insight into where the most crimes are conducted in terms of websites and geographical location of the perpetrator, what demographics do the most frequent victims have and what is the profile of the perpetrator? These are just some of the things that the police hope to create with a good quality dataset. Getting this kind of data is, however, a challenge. One of the reasons for this challenge is highlighted through the interviews as the temporary nature of the data.

Now we have a form of crime where the crime scene is located online. We have some perpetrators sitting and scamming a lot of people in a very short time. Those victimized are scattered throughout the country. The victims report in 12 different police circles. Before you get to see coherence, find out where the perpetrator is and send the information to the right police jurisdiction a lot of time passes.

How the data is evanescent is different from situations. One of the main ways it is evanescent is through the theme of time, as seen in the quote. Time plays a crucial role in collecting the data, as it needs to be done fast, or the data might be deleted by the criminals themselves, the platforms such as Facebook on which the crime happened, or through victims not giving the proper information when reporting, resulting in the police not being able to investigate the case properly. The first case of criminals deleting or hiding the data themselves is mostly seen in the more organized types of crime. Within the economic sphere, this is crimes such as CEO fraud, where the money is trafficked outside of the country in which the crime is committed and hidden on accounts or elsewhere, where the police cannot trace, get jurisdiction or legal right to pursue it.

It moves fast, especially when we talk about money and these CEO frauds, as soon as they are out of country it becomes difficult to regain.
Within the NC3 however, this can be of many types, child pornography being one of them and here the data can be hidden in many ways through methods such as the dark web, and networks where the police will have much difficulty in accessing. Time is crucial in these situations, getting the information and reacting to it as quick as possible, before the data, the perpetrator or the money is out of the country and out of reach is of utmost importance to solve such cases. The issues with companies and platforms such as Facebook deleting the data can be seen in many forms of cybercrime, and the reasons for time being a factor for the evanescent data is multiple. The companies can have regulations, allowing them only to store certain types of data for a short time period, such as fourteen days. It might be data that are against their policies, such as graphic content or of other substance, that pushes them to delete it. This creates a race against time for the police from the moment they get a report. The police might be tracking the data and having a different approach to investigating, where the platform deleting the data is quite a hassle for them. Another issue that is raised, is the willingness of the companies to cooperate with the police, as they would not like to be seen as being in too much in bed with police. This would especially be highlighted in the case of Snowden, and how big American companies freely delivered information to the police. Another case is if it is a user of the platform that reports a crime, they might not be in control of the data and the platform not aware of the report. Examples that ties to this, is how it worked before LCIK and its report system arrived. Here victims would write an e-mail to the police, and it would go as such:

```
Hi police I’ve been scammed. Then we have to write back. Hi Magnus, okay, who are you? At the moment, we only have your name and your email address. Can we have some personal information? Also, how have you been scammed? Do you have any documentation?
```

As shown, this would create a very time costly process which would produce sparse quality data which were little of use. This has however changed with the new type of report system for it-related economic crimes, where specific data is required and asked for during the report, enabling the police to categories, track and react much quicker.

Another way the data can be of poor quality is through the statistics and how they are collected. With the nature of cybercrime, a perpetrator can commit hundreds of scams in a short period which can cause statistics to explode, and dependent on how it is categorized, can skew the perspective of the beholder as seen:

```
...and there was a huge increase, I think it was in Copenhagen, but if you do not know the background for the numbers then you can just say try to listen. Yes, there is a huge increase between the 15-18 year old’s but that is because we have single 15 year old who have 1400 charges...
```

The police are therefore facing a task of categorizing and specifying all of these reports into different categories to get a better perspective of where effort is needed and what is urgent. Simultaneously, it is of utmost importance for them to know the background of their data and have a large body of it. For as for now in the short time LCIK has existed the typical perpetrator would be a 40-year-old
woman as she has the most charges of all the charges filed in this limited window of time.

**Culture**

Culture was another overarching theme that was raised throughout the interviews, as both a partial explanation as to why the focus of cybercrime might seem late, but also an explanation as to the obstacles the police now face.

As to explanations of why the focus on cybercrime might seems late, as LCIK was only just released in December the 3rd 2018, the traditions of the police is brought up in perspective to economic crime.

...then there has been that economic crime traditionally in the old days, was something with a lot of binders and something that whew this is hard. It has also been articulated as hard and been lying and collected a bit of dust.

In the past, investigating economic crimes have been mostly backtracking, meaning that a crime has happened, and every step of the crime had to be discovered and examined. This backtracking would then include a bunch of binders, accounting, curators, and numbers, making it difficult for investigators to understand and difficult to handle. Economical investigations have therefore always been articulated as complicated and with the added layers of the internet, with IP-addresses, deep and dark web, it only became more difficult. Add to this that life has always been prioritized over money, meaning that most investigators were experienced within gangs, narcotics, and murders, being transferred to economic crimes did not help its reputation as being complicated.

The culture of the internet and the rapidly developing technologies and apps such as Uber, Airbnb, etc. have not made the job of the police any easier. These technologies might not have been developed with criminal misuse in mind, resulting in them having several exploits in them at early stages for criminals to use, resulting in much work for the police in learning and gathering information on how to deal with each of these. This is time-consuming and piles on the abilities and understanding the police need to have to solve such crimes. The sharing culture of the internet and its social media adds on to this. An example brought up is the case in Denmark, where more than a 1000 young people, were charged with sharing child pornography because of a video floating around with two 15-year-olds having sex. The intent of these young people was never to share child pornography, but it nonetheless happened, and it cannot be removed from the internet. The same goes for the language that is used on the internet, where the meaning of a text can be difficult to construe for the police. For example, a young girl posting she would be the next school shooter as she hates the system and ending that sentence with a LOL (laughing out loud). Are the police to take this serious or not? They must, considering the possible consequences if they do not. Resulting in many resources used on cases like these.

**Justification of cybercrime**

The moral barrier and how it has changed from committing crimes in the real world to cybercrimes was the third overarching theme that was discussed during the interviews. This was mainly focused on the justification of the actions done in cybercrime.
There was no dispute in the interviewee’s thoughts about the moral barrier and how it has been lowered for committing cybercrime. The reason for this is put on the aspect, that it is much easier to justify one’s actions on the internet. The reasons brought up were, that it is much easier to find like-minded people on the internet, “so if many others do it, its fine for me to do it.” The distance to the victims was also seen as a significant contributor to justification. People do not risk meeting their victims on the street the next day or looking them into the eyes when committing the crime. They can turn off their screens, and it is gone. It is possible to sit in Africa and try to scam people in Denmark and believe, “they have lots of money, it will not hurt,” and this is not contested in the criminal act itself. The small amount of feedback they have received from a criminal as well, is also: …it is so easy! Why shouldn’t I do it? The feeling that I am not scamming any person particularly, it is just a system I am scamming, leading back to the distancing from the victim. The culture and language of the internet are also brought up, as it can be rather harsh, creating a larger accept of harsh language and it does not hurt as much, which could be paralleled to a larger acceptance of crime or misbehavior. In cases of child pornography, where people are only watching and paying for a service, they might see themselves as having nothing to do with it, they did not touch anybody, and the crime happened on the other side of the world. They might even believe they are helping, as they are paying for the children to have food and shelter.

Another critical point that is brought up is routine activity theory, and the three elements needed for a crime to happen, a suitable target, likely offender and the absence of a capable guardian. Especially the last one is emphasized, as the internet does not provide this guardian in the same sense as the real world. The police are not present in the same way, and there are no neighbor or other actors to interfere in the same way.

Prevention
Prevention was the last, and the central overarching theme throughout the interviews, this will of course be natural, as that is the job of the police in dealing with prevention. The indication from the interviews was that the focus was mostly on the primary and tertiary aspects of prevention (Lab, S. P 2010). As prevention is the natural job of the police, the prevention theme will also have crossovers with the rest of the themes.

Starting with the tertiary, most of the information coming from LCIK as they are newly started and had a better opportunity to explain what they are going through now to improve. However, exact methods cannot be disclosed or allow for much transparency.

In the tertiary area of prevention, the police mainly focus on how to better catch and charge the criminals. LCIK is currently in a phase of experimentation, trying to find out what cases to pursue, what charges stick and what evidence to have, to create a basis from which they can develop their procedures and methods to better them. In creating this basis, much data is needed to be collected to create the best possible foundation for pressing charges. When cybercrime is happening across borders, the data collection is filing letters rogatory to foreign national courts and figure out which nations respond, and which do not, being in dialog with companies who report cybercrimes and sharing data with them, all of this to map
out what they are facing and what needs improvement. This can be a resource heavy challenge, and in the light that lives a favored over economics, finding those resources can be difficult.

…but it has also been hard to sit as a leader on something that is always being given low priority and employees who actually wants to, but then they are suddenly transferred, so the plan you had no longer holds.

However, this has changed, LCIK has been granted secured resources, meaning that what they have in their disposal cannot be redistributed to other branches of the police. The goal of this mapping and data collection is to have a preliminary charge percentage of 50% at the exit of 2019, from every case that is sent out from LCIK.

The primary area of crime prevention is much more transparent as it is widely public information and campaigns that are used with the aim of preventing crime before it happens.

In this area the police use several methods, one of them being spawned from their co-creation initiatives, where apps and websites have been created to give the public a better insight into how to manage themselves on the internet. Furthermore these apps can be used as so:

…Then we can make warnings via the app. For example, we can say that, we are now seeing these types of emails, and then tell people don’t be fooled by them. So, we are trying to push that.

The media is also heavily used as both an informing but also scaring tactic. An example that is presented by the NC3 is the case with the 1000 young people mentioned earlier. In this case, the police used many resources into making this case very publicly known, to spawn a discussion about the sharing of such videos, and to show themselves visible on the internet as well as showing there are consequences of doing so. Internally, they create these strategy packages, which different jurisdiction can use and adapt to their local area, as a way of informing the public and preventing cybercrime from happening.

One issue they raise that they are facing is their visibility on the internet and their difficulties in being presented as a capable guardian. This issues adds another reason as to why they want to use the media to bring forth the excellent success stories of the police, to let the public know the police are out there and watching, and which is why the police are happy when a person uses LCIK as threat, which is seen in some cases:

…if you do not send the package, the police have the new LCIK task force and I am not afraid to report to them. Great! Only three months old and we are used. So, there are some people who know we are here and that we make a difference.

Data sharing is also an essential part of the primary prevention as well as the tertiary and was a big theme going through the interviews as a must do practice for creating the best form of prevention.
One of the things we should look at now is data sharing. Data sharing between companies too. There are reports which is one thing but then there is intelligence which is something else. And, among other things, I know that the banks are holding on to a lot of information.

As seen, the reason for this is that especially banks hold much information about economic crimes done through cybercrime. The reason for this is when a citizen sees a charge on their credit card that does not belong there, or they were conned for their money, they report it to the bank. The bank gives the money back to the citizen's bank account and then does a charge-back to the company that withdrew the money in the first place. This results in many such cases, never reaching the police. Creating a sizeable dark number, and a vast pool of valuable information for the police. Furthermore, the data sharing and dialog is there to close exploits that might be within individual companies for cybercriminals to exploit as well as getting companies to rethink criminal exploits into their development of practices and technologies.

**DISCUSSION**

This study leads us to show that the police faces a copious amount of challenges on a daily bases when dealing with cybercrime. The main challenges being; the time frame the police has to act upon in reference to the nature of the data, the culture that exists on the internet and distinguishing jokes from threats, the effortlessness of criminals justifying once actions, and the visible presence of the police on the internet. Furthermore, the primary focus on prevention seems to be creating a robust network between the police and the private sector, where information can be shared to create a possible united front towards cybercrime.

In the following section, the main findings will be discussed and insights into what possible issues that form around these challenge.

**Responsibility**

The issue of police visibility in cyberspace and their capabilities to act as a capable guarding is rather interesting in case of showing how the police and their job is depicted in public. What is meant by this, is in the real world the police are expected to act and be there when something criminal happens, but an interesting point brought by Yvonne Jewkes and Majid Yar (2008), is that the same expectation is not there in cyberspace. They write that there is a broad agreement that it is the ISP’s (internet service providers) and users’ primary responsibility to clean up cyberspace (ibid.). If this is true, what are the effects then on how the offenders perceive the followed consequences? This could very well add to the justification of the offender’s actions, as it is not the police they are facing. The previously mentioned research by Graham and Triplett (2016) on the users as capable guardians becomes even more important as their role is suddenly seen as the prime capable guardian. However, do they have a responsibility, and how much? Offline the responsibility is to lock the house when leaving, but after that, the individual is not to blame if someone break-in to their house. This responsibility might be skewed in cyberspace. The lack of police presence and the
user-driven nature might create such things as vigilantism, as Trottier (2017) examines. This vigilantism can cross privacy violations and laws, creating a heavier workload for the police (ibid.). This can be problematic if it is primarily the user’s job to clean up cyberspace. Is what they do then a sort of vigilantism or not, what are the boundaries? Are the police now also needed to judge right vigilantism from wrong? This leads to the culture of the internet and the issues the police have with such things as language. Language and the culture of different communities a very much user-driven, but how are the police going to interpret all these communities? Is it possible?

What to keep in mind is that it is all very much dependent on which types of crime we are talking about and far from all apply to these issues. Nevertheless, they do exist. One interesting point from Yvonne Jewkes and Majid Yar (2008) is that there might be a need for a change in how society views the police. At the moment there exists a particular view of what a police officer is, this being a sort of hero, being out in public, action happening and that sort of things, and not a desk job (ibid.). These things are depicted in the media and will be the expectation of new police officers, but maybe this should be changed to fit the new paradigm of cybercrime, to create a better and stronger front towards it with new recruits (ibid.). This would be very well supported by the findings of Hadlington, Lumsden, Black, and Ferra (2018) and the frustrations they found in police officers dealing with cybercrime. Parts of these issues might be covered by the increased insight and integration the police will hopefully have with their data sharing plans. This is however, to be seen.

**Data sharing**

The issue with getting the data in time and the approach to prevention by data sharing does touch upon some of the same issues. These are the issues of what is morally right to store for companies and for how long. The police would of course like to have as comprehensive a dataset as possible as that would give them a much better basis for investigating cybercrimes, but is the users of such companies platforms or services okay with such detailed data and for how long would it be okay to store it? There is always the risk of such a database being breached by hackers, and that risk only increases if the data is there permanently. That is not a comfortable feeling for most users, which is why we in the EU and Denmark have implemented laws such as the GDPR (General Data Protection Regulation) and PDL (persondåtaloven) which creates guidelines for companies conduct with data and gives the citizen certain rights when it comes to personal data (Datatilsynet 2019; European Union. 2019). Laws are a complicating factor as well as Cameron S.D. Brown (2015) shows in his research. What can be used as evidence during prosecution and what kind of data does a defendant have access to, to prove themselves innocent? The playing fields should be even in such cases, and how do laws affect this? Too much access can violate privacy rights and create a surveillance society and what can we as citizens accept as surveillance, what risks are we willing to take and how much privacy are we willing to give up for security? What is the barrier between mass surveillance and data sharing? These questions were very much brought up after the Snowden leaks and are heavily discussed by Bauman, Z. *et al.* (2014), mass surveillance can quickly turn every citizen into a suspect, which I do believe would not be of interest to the government or the police. All these questions can quickly get one to think of George Orwell’s novel 1984 (Orwell, G. 1949). This is, however, not the intention, and one must remember that what information is needed and shared can
be very dependent on which crimes the police are investigating. Another perspective on data sharing one could imagine, is that creating a broader culture of data sharing with the police and between companies, the issue with under-reporting might disappear as reporting and sharing would be much more natural.

Nevertheless, it seems like data sharing with companies is the way the police are moving forward to better prevent and investigate crime. This is also what has been pushed for or concluded in other research, which suggests that it is the right move (Brown. 2015; Eddolls 2016; Leppänen et al. 2016; Stanciu & Tinca. 2017). This strategy is also starting to see used in the private sector in Denmark, specifically the critical sectors such as; energy, health, finance, tele, and shipping (Energi-, Forsynings- og Klimaministeriet. 2018; Finanstilsynet. 2018; Sundhedssektoren. 2018; Søfartsstyrelsen. 2018; Telesektoren. 2018). These sectors have made a cyber alliance where within they help each other and share data on threats and cyberattacks to combat hacking and other forms of cyber attacks they might be vulnerable to. This shows that the private sector is also stepping in to take share in the responsibility and act as a capable guardian.

Capable guardian has been mentioned quite a bit as there is a larger question as to who and how regarding the internet. The study by Leukfeldt and Yar (2016) showed that the concept of a capable guardian did not fit with all types of cybercrime and had mixed results. However, I think it is not as much a question of who the capable guardian is, but more a question of who is to stand responsible. The answer to that question seems to be everyone, and that is starting to be seen by this engagement in data sharing from both the private and public sector. This is also the conclusion in other studies (Jewkes, Y. Yar, M. 2008; Williams, M. 2007). With these initiatives taken by the private and public sector and laws implemented such as the GDPR, it seems like a sort of corporate digital responsibility is introduced that will only grow with the development of new technologies.

**Limitations**

This study and its research aim are rather broad, and it does cause some issues and limitations. The broadness stems from a few choices and situations. First is the choice of creating an exploratory examination of the Danish police and in a state where a newly open center (LCIK) has not yet settled their dataset and a still in an exploring and experimenting stage. This results in specifics not always being available, but it does give a great insight into the preliminary aim and the obstacles of the upstart of such center. The fact that it is only two interviews with three people in total and at a management level does also limit the perspectives given and the opportunity for disagreements. When done from a management level, it limits the pool of people to interview, and the opinions and statements given might not be the reality lived further out the chain dealing with cybercrime. These perspectives could be essential disagreements that are limited from the study by only having the management level. The management level does, however, give a broad insight into the organization as a whole and gives a better understanding as to why certain decisions were made. The method of semi-structured interviews does also add to the breadthness of the subject. Though there are questions to theme the interview and steer it in directions, it still opens for a lot of different discussion in general, compared to a structured interview. The structured interview could potentially dig more in-depth, but that would require the interviewer to know precisely what questions to ask, if he does not, it could be
limiting to the gain of information. With the new upstart in mind and that LCIK is in a sort of explorative phase, it is therefore argued that the semi-constructed interviews were the right way to go for exploring their aim and difficulties. The generalizability of the study is also very limited, both because the amount of data points is minimal, but also because it explores in a Danish perspective with Danish laws and structure, which might not be the same in other countries.

Even with these limitations, this study gives an insight into the developments that are happening on cybercrime within the police and that it shows that what has been pushed for in other research is starting to happen within Denmark. This study lies as preliminary insight into the world of cybercrime as seen from the Danish police and gives grounds for further research as LCIK and NC3 develop, and data sharing becomes more prominent as a prevention method. Furthermore, exploration of the different actors working with cybercrime at different levels within the police is suggested, to be able to dig into potential practical issues and opinions that would give different perspectives of the issues that lie ahead.

**CONCLUSION**

This research aimed to identify the challenges the Danish police face in dealing with cybercrime, as well as how they go about prevention of the matter. Based on the qualitative analysis the main challenges found were; the evanescent nature of the data, the culture of the internet, identifying threats from jokes, the justification of cybercrime, and the visible presence of the police on the internet and how the lack of it affects prevention and their position as a capable guardian. The study furthermore adds that the way of dealing with most of these issues for now, is through data sharing and creating a healthy network between the police and the private sector, sharing the responsibility and dealing with cybercrime on multiple fronts. There are limitations to this study as listed, main one being the low amount of qualitative data, which does limit the overall generalizability of the study. The method used could have benefitted from follow up interviews or investigation more perspectives from for example the private sector. However, this study does demonstrate the increased amount of cybercrime we are facing, and it raises a lot of questions as to how, who, as well as ethical questions of privacy vs security. The field of cybercrime would greatly benefit in exploring and researching on how different elements such as police visibility, justification, responsibility, and internet culture interacts and affects cybercrime and how methods such as data sharing will affect not only cybercrime but our online life and its privacy.
REFERENCES


APPENDIX

Interview/meeting guide

The approach and theory to this interview will take grounds in “Steiner Kvaløs - En introduktion til et håndværk”. The twelve aspects will be in mind and especially the first five, life world, meaning, qualitative, descriptive and specificity will be in focus. The objective of the meeting and interviews is to get an insight into the police perspective on cybercrime and have it as descriptive and precise as possible to be able to analyze it and compare it to literature and the private perspective. The goal is to dig as deep as possible in an explorative way, as research on this field is new and what can be expected is unknown.

Overarching research questions

- How does the background of the common criminal compare to someone who does crime on the internet?
- What are the potential obstacles in doing research of internet crime through the internet?
- How can the background information of internet criminals, be used in prevention matters?
- What tendencies does the police see in the movement from common crime to cybercrime?
- What are the main cybercrime areas?
- What is the approach to prevention?
- Is there a moral change from common to cybercrime? (is it more morally right to do cybercrime)?

<table>
<thead>
<tr>
<th>Briefing</th>
<th></th>
<th>Master student criminology. Magnus Mayland. Malmö University. Bachelor in technoantropology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Presentation of the project and the interviewer</td>
<td>Who am i?</td>
<td>Look at short about the project</td>
</tr>
<tr>
<td></td>
<td>What is the project about?</td>
<td>The goal with the interview is to get the interviewee’s perspective on Cybercrime in a Danish perspective, the issues with preventing it, studying it etc. and the development from common to</td>
</tr>
<tr>
<td></td>
<td>What is the goal of the interview?</td>
<td></td>
</tr>
<tr>
<td>The framework for the interview</td>
<td>Time</td>
<td>The interview will be between 30-60 minutes long.</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Tell the interviewee that the interview will be recorded on a Dictaphone</td>
<td>Anonymity</td>
<td>The interview and its data will be treated confidentially and will be destroyed at the end of the thesis after the exam. Everything used from the interview will be anonymized so it won't lead back to the interviewee at any point.</td>
</tr>
<tr>
<td>Short info</td>
<td></td>
<td>If there is anything you have doubts about or do not understand during the interview you are free to ask at any point. I want to let you know that your participation is voluntarily and that you can always withdraw your consent. You can opt out of answering any question.</td>
</tr>
<tr>
<td>Presentation of the interviewee</td>
<td>The interviewee presents themselves</td>
<td>Do you want to present yourself? (name, age, profession, position etc.)</td>
</tr>
<tr>
<td>Themes for the interview</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------</td>
<td>-----------------</td>
</tr>
<tr>
<td><strong>Background</strong></td>
<td>How does the background of the common criminal compare to someone who does crime on the internet?</td>
<td>Do you touch upon the criminal’s background or have any insight on if it’s a career switch from common criminals or new people who start cybercrime?</td>
</tr>
<tr>
<td></td>
<td>How can the background information of internet criminals, be used in prevention matters?</td>
<td>Do you see a pattern in the criminals committing cybercrime?</td>
</tr>
<tr>
<td></td>
<td>What tendencies does the police see in the movement from common crime to cybercrime?</td>
<td>Is it done within or a cross boarders in Denmark?</td>
</tr>
<tr>
<td></td>
<td>What are the potential obstacles in doing research/prevention of internet crime through the internet?</td>
<td>How much is done within borders in Denmark?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Are there any age tendencies?</td>
</tr>
<tr>
<td><strong>Issues</strong></td>
<td></td>
<td><strong>What are the obstacles facing police in preventing and investigating and are some unique to cybercrime? • Does cybercrime become more difficult or easier to investigate and stop? (who is leading the race?)</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Are there ethical issues in cybercrime investigation? (personal data, what are you allowed, what are you not, rights, etc.)</strong></td>
</tr>
<tr>
<td><strong>Moral</strong></td>
<td>Is there a moral change from common to cybercrime? (is it more morally right to do cybercrime)?</td>
<td></td>
</tr>
</tbody>
</table>
| Prevention | • What are the main cybercrime areas?  
• What is the approach to prevention? | • What can the police do about prevention compared to private companies and private individuals?  
• How can prevention online be compared to prevention offline?  
• The police's presence/visibility on the internet compared to the real world? |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Debriefing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reaching the end of the interview</td>
<td><strong>Information</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>You are welcome to be send the final product if interested. If you have any more comments or questions you think of later, you are welcome to send them to me on <a href="mailto:m.mayland@hotmail.com">m.mayland@hotmail.com</a>. You are at any point welcome to withdraw anything said during this interview, and if I use any quotes these will be send to you beforehand to be confirmed and allowed by you.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Thank you for your help</td>
<td></td>
</tr>
</tbody>
</table>