Eivind Nes Fossum

Intelligence for cybercrime prevention: A study of stakeholders' needs for actionable intelligence

December 2022

Master's thesis
2022
Eivind Nes Fossum

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Information Security and Communication Technology

NTNU
Norwegian University of Science and Technology

NTNU
Norwegian University of
Science and Technology

Intelligence for cybercrime prevention: A study of stakeholders' needs for actionable intelligence

Eivind Nes Fossum

Experience-based Master in Information Security
Submission date: December 2022
Supervisor: Stewart Kowalski
Co-supervisor: Ivar Kjærem

Norwegian University of Science and Technology
Department of Information Security and Communication Technology

Abstract

In an ever-increasing digitized society, the need for protective and mitigative measures against cyber-attacks seems more important than ever. Cybercrime has risen to become a threat not only to businesses, but also to national interests, citizens, and critical infrastructure. Cyber-attacks are often categorized as criminal actions, which implies that the police are the ones mandated to protect, investigate, and prevent them from occurring. But recent reports indicate that Norwegian police does not have the capacity or capabilities to do so, and there seem to be room for improvement in regards of how the police are approaching and handling their work within the cybercrime environment.

This research examines the possibilities for the police to improve their policing by leveraging means and methods from other professionals working with cyber security and cyber threat intelligence. The objective is to research how the police can work more intelligence-led, thus make better grounds for decision-making, both within the police and for other stakeholders. The goals of doing so could be to improve mitigation, prevention, and the investigation of cybercrime.

For this research, selected individuals from cyber security agencies and the police are interviewed to examine their perspectives on methods and techniques used, and their intelligence-led procedures. Further, the research seeks to examine how they perceive the police's position in the cybercrime environment, and to gain more knowledge of their roles and information-needs, as possible stakeholders of police information and intelligence.

There are seven individuals interviewed, and these interviews are thematically analysed, coded, and presented in two main themes. These themes are grounds for a socio-technical analysis, in which causes for police's position with cybercrime is presented, together with identified opportunities for the police to utilize. These causes and opportunities are further being used for an SBC-modelling, where concrete measures are proposes and mapped to all categories of the socio-technical stack.

The proposed measures are suggestions, and in no means exhaustive. However, to try to implement some of the proposed measures could affect the police's work positively. Goals achieved through the measures could be a shift in focus with the police from working reactive, to increased knowledge-based policing, by contextualizing, enrich, and analytical structuring of technical data, where sharing and dissemination of intelligence is of great importance.

Sammendrag

I et stadig mer digitalisert samfunn er det et økende behov for å forhindre og forebygge dataangrep. Datakriminalitet er i dag ikke bare en trussel mot bedrifter, men også for nasjonale interesser, innbyggere og kritisk infrastruktur. Mange av dataangrepene kan kategoriseres som kriminelle handlinger og faller derfor under politiets mandat til å beskytte, forebygge og etterforske. Men nyere rapporter indikerer at det er manglende kapasitet og kompetanse i norsk politi, og det synes derfor å være muligheter for forbedring av politiets virke innen datakriminalitet og digitale trusler.

Denne masteroppgaven undersøker mulighetene politiet har for å forbedre sitt virke ved å undersøke metodikker og teknikker benyttet innen cybersikkerhet og cybertrusseletterretning. Målet er å belyse hvordan politiet skal kunne jobbe mer kunnskapsbasert og etterretningsstyrt innen datakriminalitet, som igjen kan danne bedre grunnlag for beslutningstaking, både innad i politiet, men også utenfor etaten. Resultatet ved å jobbe på denne måten kan være et politi som er bedre rustet til å forhindre, forebygge, og etterforske datakriminalitet.

Utvalgte personer innen cybersikkerhet, cybertrusseletterretning og fra politiet er intervjuet, for å undersøke deres perspektiver på metoder og teknikker de benytter seg av, samt hvordan de selv jobber etterretningsstyrt. Det er i tillegg et mål å undersøke hvordan disse deltakerne oppfatter politiets posisjon innen datakriminalitet og digitale trusler. Dette er fordi flere av deltakerne representerer et utvalg av mulige mottakere av informasjon og cyberetterretning fra politiet, slik at kjennskap til deres informasjonsbehov vil kunne danne bedre grunnlag for politiets etterretningsprosesser.

Det er intervjuet syv personer, og intervjuene er tematisk analysert, kodet og presentert ut ifra to hovedtemaer. Disse temaene danner grunnlag for en sosio-teknisk analyse, der årsaker for politiets mangelfulle innsats innen datakriminalitet blir belyst. I tillegg belyses også muligheter for politiet til å kunne forbedre sin innsats. Både årsakene og mulighetene danner videre grunnlag for en SBC-modellering, der konkrete tiltak presenteres og knyttes til de ulke nivåene i den sosio-tekniske modellen.

De presenterte tiltakene er å anse som forslag, og er ikke uttømmende. Men motivasjonen for å forsøke å gjennomføre flere av disse tiltakene er at det kan gi en positiv påvirkning på måten politiet håndterer og tilnærmer seg arbeidet innen datakriminalitet. Målet med å gjennomføre tiltakene kan være et skifte i politiet fra å jobbe primært reaktivt, til mer kunnskapsbasert og etterretningsstyrt ved å berike, kontekstualisere, samt analytisk strukturere teknisk data, der deling og videreformidling av etterretningsinformasjon anses som viktig.

Preface

This thesis ends 3,5 years as a part-time student at NTNU. It has not been easy to combine work, school, and family-life, but I am grateful to have been given the opportunity to attend the program, and I now look forward to spending a little less time in front of the computer.

I would like to thank NTNU and PHS for making such a great master's program, to Håvard who approved my application of attending, to all interviewees in this research, my torn ACL that forced me to change work practices, to Frederick for proofreading and in general being a good guy, and to Odin for introducing me to digital forensics and this master's program back in the day.

I would also thank my supervisor Stewart for the guidance in this process.

And a special thanks to my wife and my two little boys who means the world to me, for your patience, understanding, and support.

Table of Contents

List of Figures

List of Tables

Glossary

ACH[1]	A methodology for evaluating multiple competing hypotheses for observed data
Analyst Notebook	A Tool for data analysis
Argus	Threat detection platform
Course of action matrix	A model to categorize the course of action from the Cyber Kill Chain
Detection rules (Sigma/YARA)	Rules for identifying malware or other files by looking for certain characteristics
Hansken	A digital forensic tool
iBase	A database solution for capturing, controlling, and analysing multi-source data
IP	The principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries. Often denominated as an IP address, which is a client or servers' address on a network
JA3	Cryptographic fingerprint for identifying malicious encrypted traffic
Jira	A project managing system
Mandiant	A cyber security company
MISP[1]	A threat intelligence sharing platform
Pyramid of pain	A conceptual model to use for cyber threat intelligence in cyber threat detection operations
Reddit	An Online community service
Registry files[1]	A database that contains information, settings and options for programs and hardware installed on Microsoft Windows operating systems
Sentinel	A security analytics platform
Styx	An intelligence platform driven by artificial intelligence
Twitter	Micro blog service and social media platform
Virus Total	An online service that analyses suspicious files and URLs to detect types of malware and malicious content
O-day exploit	An unknown exploit that leaves no opportunities for detection

[1] See list of abbreviations

List of Abbreviations

ACH[2]	Analysis of Competing Hypotheses
API	Application Programming Interface
APT	Advanced Persistence Threat
C2	Command and Control
CEO	Chief Executive Officer
CERT	Computer Emergency Report Team
CISO	Chief Information Security Officer
CTA	Cyber Threat Actor
CTI	Cyber Threat Intelligence
DDoS	Distributed Denial of Service Attack
DNS	Domain Name System
ELYS	Etterlysningsregister
ENISA	The European Agency for Network and Information Security
FCKS	Felles Cyberkoordineringssenter
IALEIA	International Association of LE Intelligence Analysts
ICT	Information and Communications Technology
ILP	Intelligence-led Policing
IOC	Indicators of Compromise
IOCTA	Internet Organized Crime Threat Assessment
IR	Incident Response
ISS	Information Systems Security
IT	Information Technology
LE	Law Enforcement
MISP[2]	Malware Information Sharing Platform
NC3	Nasjonalt Cyberkrimsenter (Kripos)
NCDBS	Norwegian Computer and Data Breach Survey
NCFI	Nordic Computer Forensic Investigators
NCSC	Nasjonalt Sikkerhetssenter (NSM)
NSM	Nasjonal Sikkerhetsmyndighet
OAG	The Office of the Auditor General of Norway
OSINT	Open-Source Intelligence
PIR	Priority Intelligence Requirements
PO	Politiets Operasjonslogg
PST	Politiets Sikkerhetstjeneste
SAM (registry file)[2]	Secure Account Manager
SAT	Structured Analytic Tools
SIR	Specific Intelligence Needs
SSH	Secure Shell
SSP	Det sentrale straffe- og personopplysningsregister
Strasak	Straffesaksregisteret
TTP	Techniques Tactics and Procedures
VDI	Varslingssystem for Digital Infrastruktur

[2] See list of glossaries

1 Introduction

In an ever-increasingly digitized society, the chances of becoming a (digital) victim of a crime for citizen, business and government agencies is increasing. Many cybercrime incidents are not reported to the police, and those reported are seldom investigated. Reports (Riksrevisjonen, 2021) suggest that the efforts of the police in handling cybercrimes and prevent them from happening is insufficient.

To work more knowledge-based to prevent crimes from occurring is one of the police's main goals (Politidirektoratet, 2017a). Knowledge-based crime prevention requires that decision-making should be supported by intelligence and knowledge. The environment of cybercrime is characterized by technical indicators and complex data where contextualization, structuring and enrichment of the information is key. It demands analytical skills, technical understanding, and structured methods for this data to be transformed to actionable intelligence. However, given the current situation based on the number of reported cybercrime (Næringslivets Sikkerhetsråd, 2022), there might not be sufficient data for the police to analyse.

The process of working intelligence-led is a well-known practice for private cyber-security companies, where they often refer to intelligence as cyber threat intelligence (CTI). This research is an attempt to collect information from personnel working with CTI and gather experiences and knowledge which could influence how the police could be working to reach their objectives of knowledge-based crime prevention.

1.1 Motivation and background

A report from The Office of the Auditor General of Norway (OAG) (Riksrevisjonen, 2021), outlines a number of shortcomings in regard to how the Norwegian police are investigating ICT[3]- related crime. The report concluded lack of competence and cooperation within investigation of cybercrime, lack of a general overview of cybercrime and insufficiently prioritizing or solving "pure" cybercrime cases. At the same time, a report from National Security Agency (NSM, 2021) stated that their cyber security centre had a significant growth in level of activity in the digital environment compared to earlier years.

Further, the report from the Police Directorate (Politidirektoratet, 2021) assesses it as "highly likely" that Norwegian businesses will be victims of cyberattacks involving ransomware, seen in relation to increased number of incidents the last years and the possibilities of high profit for the criminals. They also mention in the same sentence that attribution and prosecution are highly complex.

The conclusion drawn from these reports is that there are a rising numbers of cyber incidents/attacks towards Norwegian interests, and that the police are currently not achieving their statuary responsibility, which is manifested in the Norwegian Police Act §2 (Justis- og beredskapsdepartementet, 1995). In section 1 of the Police Act, it states that the police shall protect all legal activities, person, property, maintaining peace and order and everything that threatens the general societal security. The following section 2 and 3

[3] The term "ICT crime" is in the report (Riksrevisjonen, 2021) described as "data breach and unauthorized handling of access data". "ICT-crime" is referred to as "cybercrime" in this thesis.

states that the police shall prevent crime and other violations against public order and security, and detect, stop, and investigate criminal activity according to law.

The motivation for this thesis comes from my own experiences in investigating cybercrime cases and handling cybercrime-related information. The objective of this research is to get more knowledge and conduct research on how the police can increase their capabilities, capacities, and efforts in handling cybercrime, and find causes and possibilities for improvement.

1.2 Research problem

The Norwegian police has formalized intelligence in The Intelligence Doctrine for Norwegian Police (Politidirektoratet, 2020), where it states that intelligence shall provide information to decision makers in order for them to make qualified future decisions, and it should contain assessments regarding expected development of society or special actors. It further says that the information must be analysed in context with other information to provide insight and understanding to reduce insecurity to make qualified decisions regarding future events. The process ends with an intelligence product, where actionable intelligence is elucidated and disseminated. This product should help make decisions both on strategic-, operational-, and tactical level, in which measures in the areas of preparedness, prevention and investigation, should be conducted. The goal is to work more intelligence-led, and to focus on a more knowledge-based decision-making-process, regarding persons, groups and phenomenon's that creates or may create crime (Politidirektoratet, 2020).

This research means to elucidate how the police can leverage the use of intelligence-led measures to handle the increasingly vast landscape of cyber-crime, where standard investigative measures clearly have failed to provide a sense of security. The intelligence-led police work can resemble preventive police work, which is why the SBC (Kowalski, 1993) socio-technical control systems model is used to present and structure possible measures. As mentioned in beginning of this chapter, OAG (Riksrevisjonen, 2021) reports that police capabilities and efforts are not keeping up with the challenges they are facing, and new technology demands new means and methods to fight it, especially when measuring the cyber-threat landscape in which intelligence may be applied.

The police's stakeholders are potentially many, and on the tactical and operational level within the police, the need for information could come from the police investigators, analysts, or investigation-leaders, where swift decision-making and testing hypothesis is an essential part of the job. On a more strategic level the need for information typically comes from policymakers and police leaders. Stakeholders from outside the police could be private or governmental businesses in which the intelligence is meant to support decision-making and to conduct preventive measures. These are i.e., personnel either from national agencies or cyber security companies, where the provided intelligence should be somewhat actionable. On a tactical and operational level, this could typically be personnel working with CTI or incident response (IR). It was therefore sought to conduct interviews on personnel either from CTI or IR, both to gather information on their means of work and to examine their perception of the police, where the intention is to help the police make better grounds for decisions for them.

Some frameworks used by other intelligence agencies and intrusion detection teams, being the Diamond Model of intrusion detection, Cyber Kill Chain and MITRE ATT&CK, will also be an important issue of this thesis. These are frameworks that are not commonly used in the Norwegian Police today, neither by investigators nor intelligence analysts, but maybe they should be as a part of the police's goals to work more intelligence-led.

1.3 Research question

The main research question in this research:

- How can intelligence-led policing support the objectives to process and prevent cybercrime efficiently?

1.4 Target group

This thesis is targeted towards police personnel, either working with cybercrime, or wanting to learn more about this area. It is not meant for investigators exclusively, as it is equally relevant for investigation leaders, police attorneys or decision-makers higher up in the organization. The methods and tools described here are in close relation with digital forensics, intelligence, and structured analytical processes, in which personnel working with those areas could be the ones finding this thesis the most interesting.

An important effect of using intelligence is to reduce uncertainty and increase competence, which is transferable to cybercrime and policing where the subject is assessed by many to be too complex and technical to grasp. This research may provide some useful information for those having needs for it.

1.5 Delimitation and limitation

This research's primary goal is to provide an overview of the area and not exhaustively examine what CTI or IR are, or to map all techniques, tools, and methods used. The goal is to examine if there are elements in their processes that may be applicable for the police to use, and how they work intelligence-led to achieve their objectives. And even though digital forensics is important in processing cybercrime, there is a delimitation in regards of digital forensics tools or hardware. Another goal of this research is to address the police's positioning in the cybercrime environment and draw attention to possible areas due for improvement.

The limitation is to focus on actionable intelligence, and how utilization of intelligence-led policing can help the police to reach their end state, thus increasing mitigation and resilience in society. One important aspect of intelligence-led policing is to support decision-making, and this research focuses on decision-making on the tactical and operational level, as opposed to the strategic level.

There is also a limitation regarding the number of participants in this research. As mentioned in 3.3.1, this research methodology is phenomenological in nature, which depends upon a small and carefully selected sample of participants. A typical sample is 5 to 25 individuals, and they should all had direct experience with the phenomenon being studied (Leedy and Ormrod, 2015). For this research, 7 individuals have been carefully selected based on their profession and knowledge of the subjects being studied.

1.6 Thesis outline

Chapter 2 describes the state of current Norwegian policing in relation to cybercrime, together with relevant theory. The police's methodologies are also described, such as investigation versus intelligence, and preventive policing. There is also outlined a description of traditional intelligence procedures, CTI, and descriptions of methods and frameworks. Chapter 3 presents the research methodology, the researcher's background and biases, and quality assurance. Chapter 4 describes the data collection and analysis of the interviews. The result from the analysis is described in chapter 5, where the socio-technical systems analysis and SBC-modelling are presented, together with strengths and weaknesses of the study. The conclusion is presented in chapter 6, and lastly, chapter 7 presents outlines and perspectives on future research.

2 Background

Cybercrime is a frequently used term and can be differentiated between "cyber-dependent crime", also referred to as "pure cybercrime", and "cyber-enabled crime" (Interpol, 2021). This research will only cover "cyber depended crime", such as sophisticated attacks by using a computer against computer hardware, software or networks (Årnes, 2020). The cybercriminals, also referred to as cyber threat actor (CTA), is a participant (person or group) in an action or process that is characterized by malice or hostile action (intending harm) using computer, devices, systems, or networks. The CTAs are further classified into one of five groups based on their motivations and affiliations (Cisecurity, 2022): cybercriminals, insiders, nation-state, hacktivists and terrorist organizations. Cybersecurity makes it intake by executing measures to avoid unauthorized access or attacks from these groups, and this research seeks to find out if some of these measures are applicable to how the police handles cybercrime.

2.1 Norwegian cybercrime environment

Cyber-attacks and digital threats towards Norway and Norwegian interests are increasing, and the Norwegian Police Security Service (PST) states that digital threats are the number one threat towards Norwegian interests (PST, 2021). In relation to this, private companies do what they can to deter and prevent attacks from happening, and some private and governmental agencies are trying to attribute these attacks for intelligence purposes, as shown in the report from PST (PST, 2021), where the attack against the Norwegian Parliament (and other institutions) in the fall of 2020 was attributed to the Russian hacker group APT-28, also known as "Fancy Bear".

In the report from National Cyber Crime Centre (NSCS) (NSM, 2021) it mentions that preventive measures are important to reduce digital risk, and with the level of severity that cyber operations brings, the urgency to implement risk-reducing measures increases. Many of these cyber operations can be labelled as crimes, such as system breach, theft, extortion, and damages to the systems. The investigative responsibility resides with the police, independently of area of criminality, with reference to The Norwegian Criminal Procedure Act §223: "criminal acts are reported to the police" (Justis- og beredskapsdepartementet, 1981). The police are the ones mandated to, according to the Norwegian Police Act (Justis- og beredskapsdepartementet, 1995), prevent, uncover and stop crime and to investigate it, and the criminal proceedings shall contribute to reduce crime by uncover criminal offenses and solve cases, thus convict and sanction offenders adequately (Riksadvokaten, 2019). Unfortunately, threats and cyber incidents/attacks seen in Norway over the past years is not proportionate to the level of reported and successfully investigated cybercrime cases.

The report from OAG (Riksrevisjonen, 2021) states that the ambitions and capacities of National Cyber Crime Centre (NC3) are to investigate one-two serious cybercrime cases each year, and simultaneously assist the other police districts. This means that the investigative responsibility resides with the districts. The consequences of this are low capacity of pure ICT related cases, resulting in closure of criminal cases. The cases are large, too complex, and resource-demanding for the districts to investigate. But the same report also illustrates how intelligence-led policing is beneficial in handling pure ICT-related crime, by saying that to efficiently prevent and use crime-reducing measures, it implies knowledge-based policing that emphasizes analysis and intelligence (Riksrevisjonen, 2021). This is both stated in the Intelligence Doctrine for Norwegian Police (Politidirektoratet, 2020), in The Local Police Reform (Justis- og beredskapsdepartementet,

2014) and in Politimeldingen (Justis-og beredskapsdepartementet, 2019). Despite the governmental anchoring of this ideology, the report (Riksrevisjonen, 2021) states that the ICT-area suffer from a blurry definition of the term ICT-crime, limited overview in regard to reported ICT-crime, vast area of unrecorded police-reporting's and lack of intelligence and systematic increasing of knowledge. And one of the trending cyberattacks the last years are ransomware attacks, evidently described in the Police Threat Assessment (Politidirektoratet, 2021); "it seems highly likely that computer breaches with ransomware will be conducted towards Norwegian businesses", and "there is a chance that businesses with societal critical functions will be victims of successful ransomware attacks".

The report called Norwegian Computer and Data Breach Survey (NCDBS) (Næringslivets Sikkerhetsråd, 2022), states that only 12% report attacks and/or unwanted incidents to the police. This report is based on 2500 interviews from Norwegian private (2234) and governmental (266) businesses, where attempt of computer breach/hacking, phishing, and actual computer breach/hacking were the most common incidents. Respectively 10%, 9% and 3 % of the businesses had experienced this. On the positive side, 3% said they had been victims of ransomware attacks, and subsequently 26% had reported this to the police, which is a good development. But in regards of the relatively low number of victims, the actual reported cases might not be that many.

OAG (Riksrevisjonen, 2021) counted the number of reported ICT cases to the police in 2018, and found 296 345 cases in total, but only 461 of these could be classified as pure ICT cases, meaning cyber-dependent crimes. This is a low number and should be viewed with moderation, because the only two penal codes (Justis- og beredskapsdepartementet, 2021) used that were suitable for extraction from the penal case registry was § 201: Unjustified handling of access data, etc. and § 204: Burglary of computer systems, and the fact that the number is from 2018, meaning the number might be higher today. Other relevant penal provisions contains both ICT-related crime and other types of crime, which makes the final number hard to estimate (Riksrevisjonen, 2021).

Recent surveys, as mentioned in the report from OAG (Riksrevisjonen, 2021), indicates that businesses and citizens have a lower degree of trust in the police`s capabilities in terms of ICT-crime compared to other crimes, which is why it is not reported to the police (Riksrevisjonen, 2021). The report also states that both corporations and private individuals are contacting private operators as opposed to the police when they are victims of ICT-related crime.

However, the report NCDBS (Næringslivets Sikkerhetsråd, 2022) states that only 2% and 1% of business reports incidents to sector CERTs (or similar) or NorCERT (NSM), and 5% reports incidents to other authorities. In the analysis of the data in the same report, it clearly states that the low grade of reporting to government agencies are unfortunate, especially since the actual reporting of incidents may provide valuable information regarding ongoing attacks, or methods to protect towards them. The report points at the ignorance that resides amongst the various businesses in relation to what the government can provide, with reference to the "National Strategy for Digital Security" (Departementene, 2019), where the establishment of national centers such as NC3 and NCSC are mentioned.

NSMs VDI sensor network (NSM, 2020b) should be mentioned here, which is a warning system for digital infrastructure. The members are a secret, but NSM collects metadata from network sensors to discover cyberoperations. By doing so NSM are better prepared to gain situational awareness in the national cyber landscape. The data is then systemized, automized and structured to enable alarming of structured data, where warnings and detection mechanisms can be issued if a cyber incident were to occur. This system must be taken into consideration of the low numbers of both reporting to NSM and to the police,

because there might be a mutual understanding between the offended business and NSM, where further reporting seems unnecessary.

Kripos and NC3 has ambitions to investigate only one-two large cases per year (Riksrevisjonen, 2021), where the legality is anchored in The Norwegian Prosecution Instruction (Justis- og beredskapsdepartementet, 1986) §37-3, saying that the National Criminal Investigation Service (Kripos) can investigate severe ICT-crime, and selection of cases happens from either a principal character, the demands of an extensive international cooperation, not residing in any specific police district, or is especially competence- or technology demanding. By looking at these criteria, a great number of cybercrime incidents could fit the legal threshold of being investigated by Kripos, but this is not the case. Due to capacity the investigative responsibility belongs to the districts, but they seem unable to handle cybercrime cases (Riksrevisjonen, 2021). To work intelligence-led, thus preventive, might be the remedy for this problem. But to do so, the two dependent variables of increased police reporting and police efforts, must be addressed for the police to have better grounds for decision-making, where the effects are more preventive policing.

2.2 Global cybercrime environment

The global threat environment has in 2022, according to NSMs report National Digital Risk Assessment (NSM, 2022), moved from a pandemic to war in Europe, and the security policy situation has changed dramatically in a short period of time. The digital risk picture is characterized by ever-increasing complexity in systems and technologies. The vulnerabilities in society becomes more demanding to detect due to constantly more complex digital value chains. The same report stated that the different types of cyber-attacks had statistically been more targeted towards three societal areas, being technology businesses, science, and development, and against public administration. There are however few of these cyberattacks being reported to the police.

According to a report (Cybercrime Magazine, 2021), if measured as a country, then cybercrime would be the world´s third-largest economy after the U.S. and China and is predicted to inflict damages totalling $6 trillion USD globally in 2021. It is expected to grow 15% per year, reaching $10,5 trillion USD by 2025, and will be more profitable than the global trade of all major illegal drugs combined.

Every year Europol publishes the Internet Organized Crime Threat Assessment (IOCTA) (Europol EC3, 2021), which is a strategic product mainly for law enforcement. The IOCTA describes evolving threats and key developments in cybercrime, and recommendations from Europol. The key findings in the report are new multi-layered extortion methods from ransomware affiliate programs, mobile malware with two-factor authentication disruption, and DDoS for ransom where criminals are using known APT names to scare their targets into complying with ransom demands. Some of the recommendations that are presented in the report are a stronger focus on prevention, where national governments should make businesses of all sizes aware of the risk of falling victim to cybercrime and offer practical guidelines in securing their networks. Other recommendations are streamline information sharing and to enhance awareness campaigns, and to enhance insight into ransomware attacks to facilitate effectiveness of criminal investigation, and to encourage reporting to the police. The IOCTA further says that to combat advancing threats, police officers need to be able to have timely access to data and recommend making it mandatory for major cyber incidents affecting critical sectors or essential service providers of a suspected criminal nature, to be reported to the police.

2.3 Police's room for maneuver

The Norwegian Police Act §2 (Justis- og beredskapsdepartementet, 1995) describes the tasks of the police, and states that "The police shall prevent crime and other violations of the public order and security, uncover, stop criminal activity and pursue criminal offenses". The means to achieve this is mainly by working reactive (investigation) and proactive (prevention).

Two of the approaches to handle cybercrime are through investigation and the collection and distribution intelligence, which are tightly sown together through the concept of knowledge-based police work. This is clearly stated in the Police preparedness system (Politiet, 2020b), which stipulates that police emergency preparedness shall follow the principle of knowledge-based police work, which implies systematic and methodical collection of relevant information and knowledge (both experience-based and theoretical). This information, through its analyses, aims to hit strategical and operative decisions regarding preventive and reactive measures, thus combining intelligence and knowledge-based policing with analytical and scientific knowledge.

But there is a problem in relation to the intelligence process, being there is not enough data to fix the problem efficiently because individuals and business are hesitant in reporting incidents to the police, as shown in the report NCDBS (Næringslivets Sikkerhetsråd, 2022). Consequently, the police do not have the intelligence to do intelligence-led police work. The survey also stated that it was the smallest companies with less than 100 employees that were most reluctant to report incidents, not necessarily to the Police, but other authorities such as NSM. These numbers shows that there is large under-reporting of ICT-incidents to the Police, as well to other authorities, especially amongst smaller business.

There have been measures taken to improve the competence and feasibility regarding cybercrime, such as the newly developed NC3 in Norway (Politiet, 2021a), and the latest guidelines from the Attorney General (Riksadvokaten, 2019). The guidelines state that police efforts against serious computer-attacks, breaches and other ICT-crime must be intensified, and that this type of crime is increasing, but fewer are being prosecuted. Further, the guidelines add that these cases demand high technical competence, and a higher level of cooperation between the police districts, Kripos, private businesses and international relations, must be emphasized.

So clearly, there is room for improvement for the police in handling cybercrime, an area which seems to be increasingly more threatening towards national interests, security of both business and citizens, and yet something the society is become more reliant upon. This security is today primarily covered by private security companies, other national agencies (such as NSM), and the sector-wise response environments (SRM). These institutes do not have the same areas of responsibility and possibilities as the police, but they are providing security and does preventive measures, as well as investigating and producing intelligence.

However, one major difference is that private companies monetize from doing this, but equally the quality of their work is what may leverage them in being competitive. The costs of security services could result in smaller companies being vulnerable towards cyber-attacks, both in terms of social security awareness and in the actual protection of its assets. But for the police, the tools, methods, and techniques used by private companies could be worth adapting into its own organization. These security companies are market-leaders in what they do, and even though the end-state and goals are somewhat different, the means and measures to reach them have similarities.

For the police to be unable to reach its objectives is the same as failing to keep the citizens safe, or for businesses to feel a sense of security. Omand describes security as a state of confidence on the part that normal life can continue, despite the dangers to individuals, families, and business (Omand, 2011), and how intelligence can be used as a means to achieve this. He further discusses the value of anticipation, together with risk assessment, preventive work, to be able to see emerging trends and work strategically is of great importance for achieving end state being public security, or to maintain normality. In the ever-increasing digitized society, this seems more relevant than ever. The way to achieve this, according to Omand, is to use intelligence to reduce the risk, through cooperation to pursue (stop the attacks), prevent, protect, and prepare, also known as the 4Ps. Ultimately, this is much the same as what private security companies are offering to their clients and stakeholders, where risk management, risk assessments and understanding threats are key components to reduce the victimization rate.

2.3.1 Investigation

Investigation can be defined as: "a systematic examination, with the purpose of identifying or verifying facts. A key objective during an investigation is to identify key facts related to a crime or incident" (N. Sunde, 2020a). Investigation is of one of the core tasks for the police and prosecution (Politidirektoratet, 2016), which is stated in the Prosecution Act §226 (Justis- og beredskapsdepartementet, 1981). This paragraph states that investigation is purpose-driven and is to be regarded as an investigation if the purpose is fully, or partially, one of these criteria: "to provide the necessary information for the decision on the question of indictment, and to serve as preparation for the further processing of the case by the court". The superior goals for the criminal case chain are to "secure a targeted and efficient criminal proceeding of high quality which preserves the rule of law and human rights" (Riksadvokaten, 2016).

There are however some challenges in cybercrime investigation, such as application of tactics, the technical complexity of the data, and regularly operating between inconsistent legal frameworks in international investigations (Lemieux and Bales, 2012)

In a circular letter from the Attorney General (Riksadvokaten, 2019), ICT-related crime is specifically mentioned, and describes it as criminal actions which includes the use of ICT-tools or services, or is directly pointed towards technology, infrastructure or computer systems. The letter further states that clarification of ICT-crime cases is of upmost importance, and that police´s effort on serious computer attacks/breaches and other ICT-crimes shall be intensified. And to uncover more punishable offences, it seems necessary to facilitate increased cooperation's between the police districts, and to emphasize the importance of international cooperation (Riksadvokaten, 2019).

The vision of an intensification of ICT-investigation is stated in the ICT-crime Strategy from Ministry of Justice and Public Security (Justis-og beredskapsdepartementet, 2015), where it says that Norway must be safe and secure, equipped to handle future crisis, prevent, deter, provide safety, solve cases and prosecute ICT-crime. Lastly, the document states that those who execute ICT-related crime shall not be able to prepare or conduct crimes without there being a significant risk of being caught and prosecuted.

The police, despite low reporting, (Næringslivets Sikkerhetsråd, 2022), are continuing to encourage to report crime, as investigation and prosecution may produce both individual- and general preventive effects (I. M. Sunde, 2020), emphasized by the new feature in 2021 to submit tips through the Police`s web page (Politiet, 2021b). In order to report a crime, the victim has to deliver this in person at the local police office, and only then is the police in position to investigate (I. M. Sunde, 2020), meaning the incoming tips are suited for intelligence use. This is also emphasized on the actual tips page, stating: "the police

want tips regarding computer crime and fraud in order to gain more knowledge regarding the crime phenomenon and to be able to strengthen the preventive and crime fighting police work" (Politiet, 2021b).

A key component in any cyber investigation is digital forensics, where digital evidence is processed according to well defined scientific processes in order to establish facts (Årnes, 2020). These facts can further be utilized in a court of law or used for intelligence purposes. The digital forensic process follows the principles of evidence integrity and chain of custody, where the first aims at preserving the evidence in its original form without any intentional or unintentional changes (Sunde, 2017), referring to (Casey, 2011; Hamremoen, 2016; Flaglien, 2018), whereas the latter means that every contact with the physical and digital evidence should be accounted for to prove authenticity and integrity (Sunde, 2017), referring to (Kruse and Heiser, 2002; Casey, 2011; Flaglien, 2018). To conduct the actual digital forensics, investigative measure conducted beforehand is necessary, often referred to as "coercive measures", such as online computer search, surveillance, interception of electronic communication, or measures of physical kind such as house search and seizure of computer equipment. The competence to authorize coercive measures lies with the court and, whereas the public prosecutor has the authority to forward a request for this measure (I. M. Sunde, 2020).

These coercive measures cannot be applied outside of the investigation, emphasizing the need for reporting from business and citizens to be able to enlighten the criminal activity.

There are several phases in the digital forensic process, but for the purpose for this research, only the analysis phase will be highlighted. This is the phase where the objective is to identify relevant information suitable for hypothesis-testing, and to establish credibility (N. Sunde, 2020a). Sunde further states that investigative technical competence is necessary to identify which digital artefacts may be searched for to answer the information requirement, and hence, test the investigative hypothesis. But in a cybercrime investigation, there are several other aspects besides the digital forensics process, because it requires a wide range of technical and non-technical professional disciplines and investigative skills (Hunton, 2010, 2011; Lemieux and Bales, 2012). In Lemieux and Bales research based on interviews of police investigators, it was evident that regardless of technical complexity of the investigation, the traditional crime investigation techniques were considered a necessity. This statement was supported by the human element in crime solving, meaning there is always a human element regardless of technologically advancement of the computer crime case.

The end state, or goals, of an investigation could also be arguable, as shown in Lemieux and Bales' research (Lemieux and Bales, 2012). This research consisted of interviews of police personnel in cybercrime, and some investigators perception of investigative success has direct effects on selection of cases to investigate, where success was defined by numbers of arrests and prosecutions. Hence, investigators are more likely to go for "easy" arrests, in greater numbers. However, the same research discovered that the participants from a national security standpoint perceived success differently, where the success of an investigation was measured by the possibility of gaining counterintelligence from a cyber threat, especially for cases of a national security matter.

2.3.2 Intelligence

The first Intelligence Doctrine for Norwegian police was published in 2014 (Politidirektoratet, 2020), and the newest update of the doctrine was published in December 2020. This doctrine provides the framework for how intelligence work is conducted in the Police. The objective for intelligence is to deliver strategic, operational, and tactical support for decision making for prioritization and guidance, with the foundation

being data put in context. The process, as described in the Doctrine, consists of four sub-phases, where the outcome of the process is intelligence, which starts with leaders setting the direction, as seen in Figure 1.

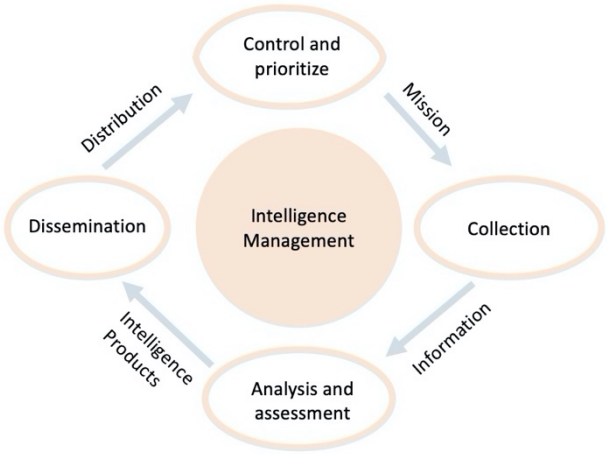

Figure 1: Intelligence Process described in the Intelligence Doctrine (Politidirektoratet, 2020)

- Control and prioritization: formulate the intelligence needs
- Collection: data being collected to provide answers to intelligence needs
- Analyse and assessment: information transformed to intelligence
- Dissemination: Disseminate and distribute intelligence products to the client

The first part of the process is to establish who needs intelligence about what, based on overall prioritizations, prior intelligence work, or the leaders desire for decision support. The outcome of this sub-phase is to formulate a collection plan which is a structured overview showing how each single need for information is answered out. The collection sub-phase is split in human-based and technical collection, and the goal is to formulate this data to information, making it understandable and put it in context where it is available for analysis. In the analysis and assessment sub-phase, the collected material is processed, analysed, interpreted, and transformed into support for decision making. The most basic form for analysis is to describe and assess the current state: what is going on where, who is involved, why and how is it happening?

To be suitable for decision making it should also be predicable and should describe what the expected development is and when will it occur. The last sub-phase is dissemination and distribution of the product to the client and potentially other receivers. A mutual understanding of the message is important, and there are three principles that should be sought after: disseminate timely, the message must be relevant, and it should be presented clearly. Intelligence should generate a basis for decision making on all levels (strategic, operational, and tactical), where leaders are conducting suitable measures.

The intelligence terminology has to be defined contextual, since its increasingly being used by several actors within different sectors (Moen, 2020). To illustrate both the value and limitations within the various sectors, intelligence may be defined by purpose: "the most basic purpose of intelligence is to improve the quality of decision-making by reducing ignorance" (Omand, 2011). In policing, the objective is to develop a deep understanding of a crime problem, in which information has to be placed in context and arranged in ways that allow decision-makers to draw meaning and inferences form the collective wisdom available (Ratcliffe, 2016). According to Moen, one important note in using intelligence in policing is that, traditionally, the intelligence production is both produced and used

internally by the police; thus, it is police-leaders using the intelligence for grounds for decision-making (Rønn, 2016; Moen, 2020).

The structural emergence of intelligence in the Norwegian Police came in 2014, with the implementation of the Intelligence Doctrine (Politidirektoratet, 2020). This doctrine refer to the Police Act §2 (Justis- og beredskapsdepartementet, 1995) as the foundation of its relevance, which says that "..the police, through preventive, enforcing and assisting activities, shall be a part of society's overall efforts to promote and consolidate citizens' legal security, security and general welfare in general", and "This means that the police must protect people, property and public goods as well as protect legal activities and maintain public order and security". The Intelligence Doctrine uses the Police Act §2 as the foundations for its objectives by stating: "To solve these tasks the police need, and police leaders in particular, decision support in the shape of knowledge regarding problems and dangers that threaten the values to be protected".

This is also clearly manifested in the Norwegian Guidelines for the Police Emergency Preparedness (Politiet, 2020b), stating that the police activities must follow the principles of knowledge-based policing, which implies systematic and methodical collection of relevant information and knowledge (both experience-based and theoretical). When knowledge-based policing and intelligence is combined with analytical and scientific knowledge, preventive and reactive measures can be implemented based on strategic and operative decisions (Politiet, 2020b). The proactive perspective is also elucidated in Plan and Rammeskriv (Politidirektoratet, 2017a), where one of four main strategic visions for Norwegian Police towards 2025 is to be ahead of the crime, where one of the means are to use intelligence and knowledge in decision-making.

In order to be proactive, one has to connect intelligence to the risk-terminology, as mentioned in (Politidirektoratet, 2018), and cited from Aas in (Aas, 2020). She further cites Hestehave (Hestehave, 2018), when she debates that the police over several years have tried to cope with crime "smarter", through i.e., problem oriented-, intelligence-based, and hot-spot policing in terms of violence in close relations. Aas states that the understanding of risk must be elucidated to understand how the policing is, or can be, towards this kind of violence, and this can very well also be applicable to risk in the cyber environment. This is where the applications of principles in risk management to public security may seem relevant, where taking managed risk to achieve desired objectives is the goal. In order to reduce the risk, businesses follow the principles of the Chinese General Sun Tzu of "knowing yourself and knowing the enemy", meaning identifying, examining, and understanding the threats facing the organization´s information assets (Whitman, 2019). The "assets" in which the government is obliged to protect is the national security and protection of its citizens, where the citizens can continue with their normal life, despite the dangers to individuals, families, or businesses. The public must have a state of confidence in the security authorities´ ability to make risk judgements in order to live a normal life, and according to Omand, risk avoidance is here not an option, but good risk managing is (Omand, 2011).

There is a difference between knowledge and intelligence, where knowledge is to generate an understanding and intelligence is to generate action (de Lint, O'Connor and Cotter, 2007; Ratcliffe, 2016) Intelligence is information compiled, analysed and/or disseminated in an effort to anticipate, prevent or monitor criminal activity (United States of Department and Justice, 2012; Ratcliffe, 2016) Knowledge on the other hand, can fuel insight and understanding, but has to be structured in a way that can help decision makers develop policy (Ratcliffe, 2016). The goal of using intelligence is therefore to produce a sense of knowledge suitable for decision, where hierarchy and governance is central elements (Ratcliffe, 2016; Gundhus, 2018; Vestby, 2018; Bahonjic, 2021). This approach will ensure that intelligence products are ordered by persons suitable for decision-making based on

the product. The value of the product is limited if not used to make decisions (Bahonjic, 2021), cited from (Politidirektoratet, 2020), hence the emphasis on actionable intelligence in this research. The process of making information, which is knowledge in raw form, to something useful is through evaluation, being a process of considering the information regarding its context through its source and reliability, where the outcome is intelligence. This intelligence is further analysed to produce products to support decision making, which is mentioned in the manual from United Nations (UNODC, 2011). This manual also states what is applicable for cybercrime intelligence, namely that the potential vast sets of data and large volumes of available intelligence, makes the analysis process more applicable to further analysis for meaningful results to be obtained.

This classic form of intelligence analysis is based on induction, which is grounded on a belief that a logical inference exists between the conclusion and the historical precedents (Hatlebrekke, 2021). In taking a logical approach to inference development, the analyst must avoid logical errors, which may lead to false inferences. Fallacies of omission and false assumptions are the two general classes of logical errors. When applying inductive logic, the facts are examined, but it goes beyond those facts, where reasoning is used to work from the parts to the whole (UNODC, 2011). Hatlebrekke argues that this inductive method is restrictive and reductive, since the analyst is unable to detect and identify threats occurring in new variations and hence outside of the inductive premises. The essence, according to Hatlebrekke, is therefore to judge and elucidate how classical threats may occur in new contextual variations, by identify the similarities and differences between the past and the future. Accordingly, the standard inductive intelligence method may hamper this (Hatlebrekke, 2021), where the criminal investigators and analysts are interested in those cases in which, if the premises are true, the inference is also probably true (UNODC, 2011). In the event of a perpetrator attacking under false flag, an inductive intelligence process where the inferences are based on the premises, may lead to false assumptions and as such hamper the decision-making.

In cybercrime intelligence, what the analysts are basically doing is analysing an intrusion, which in IR is an important part of the post-incident activity. Thus, the principles of IR and especially intelligence-driven IR seem applicable to use for the police, both in investigation and intelligence work. There are two intrusion analysis models that have caught attention the last decades, namely the Kill Chain and the Diamond Model of Intrusion Analysis, and these can complement each other to give more depth when analysing (Nese, 2018). For the police, these models can benefit what Hatlebrekke argues in regards of standard inductive reasoning as mentioned above (Hatlebrekke, 2021), where fallacies may occur. To exemplify, the Diamond Model, with support of the Kill Chain, looks at each relevant "cyber" event and breaks it into four vertices or nodes. Ultimately, activity groups and threads are generated, by correlating nodes from events across incidents or knowledge of infrastructure or capabilities prior to them being used operationally (Papaioannou, 2021). In this manner, threats can be assessed by identify its similarities and differences and find new contextual variations, thus fulfilling what Hatlebrekke demonstrates in regards of the importance of using creativity and imagination in intelligence production (Hatlebrekke, 2021).

2.3.3 Intelligence versus investigation

The two approaches (investigation and intelligence) have similarities, such as collecting information and analyse it, and they are both used to support decision makers involved in societal cyber defence. But they are separated by the purpose, as discussed in Hustveit's master thesis (Hustveit, 2017). Here he points out that the investigative purpose is that analysed data is used as evidence in penal cases and trials, and the requirements is that criminal acts must be proven guilty beyond reasonable doubt for conviction. Intelligence on the other hand serves the purpose of informing future events, thus never proving

something. Instead, intelligence is provided with various grades of probability to be transparent of the underlying insecurity of information. In this way the consumers of intelligence can make their own assessments (Politidirektoratet, 2021). Hustveit points out another important divergence between investigation and intelligence: responsibility. The intelligence resides with the Justice Department, whereas investigation is allocated with prosecution where the attorney general (Riksadvokaten) oversees the investigation. Thus, one can say that the Norwegian justice system is based on a "two-track system", divided by the responsibility (Roy Røsberg, 2020), and the intelligence process operates on both tracks, separated by different regulations setting the premises for collection, storing and disseminating information (Politidirektoratet, 2020). The Attorney General (Riksadvokaten, 1999) said that it is the purpose of information collection that defines whether it is an investigation or intelligence process, which in term dictates the methods allowed to be used.

Coercive methods may first be applied when it is an investigation, and paves ways for a much broader field of information collection as opposed to an intelligence process. These coercive methods are based on the rules of e.g., the procedural law, whereas the legal frameworks for intelligence process is subject to rules concerning data protection (I. M. Sunde, 2020). The surplus material harvested from investigations could therefore hypothetically be of great value, due to its legislative grounds in which the material was collected in the first place, meaning intelligence activities may be conducted in both tracks; within and outside an investigation (Politidirektoratet, 2020). This is also emphasized in Hustveits master thesis (Hustveit, 2017), where all the intelligence operators answered that it was the surplus information that investigation best could support the intelligence process with.

Further, to separate the collected information (both planned and un-planned collection) in either investigation or intelligence track, the prosecution lawyer must, in timely manner, have access to the information to allocate the process correctly. If the information collection is planned and the policy makers has no intension of investigate further, e.g., to elucidate threat actors, OSINT etc., then no involvement from the prosecution lawyer is needed. If there is a possibility of the opposite, the prosecution lawyer has to assess if the information collection process slides into an investigation (Politidirektoratet, 2020). This will underline the need for the collected information to be consecutively registered and systematically structured and made understandable for prosecution lawyers with the probability of less technical skills than the analyst.

The intelligence platform used by Norwegian police today is called Indicia, which serves the purpose to prevent crime, unveil and stop crime and ensure safety (Justis- og beredskapsdepartementet, 2013), and the prosecuting authority has access to read the content (Politidirektoratet, 2020), according to the Police Register Regulation §47-8, cf. §8-2 nr.2, cf. the Police Register Act §21 (Justis-og beredskapsdepartementet, 2010; Justis- og beredskapsdepartementet, 2013). The Police Directorate regulation from 2006 (Politidirektoratet, 2006) concludes that personal information is deleted from Indicia after five years, unless new information is in the time frame is registered. As stated by Bjelland (Bjelland, 2020), personal information is data than can tell us something about an individual´s identity, street address, computer equipment, the organizations to which s/he belongs to etc., meaning that cyber investigation and information collection entails the processing of personal data (I. M. Sunde, 2020), regardless of a successful attribution or not.

Since Indicia was introduced in 2007, its main purpose is to serve as an intelligence register, where various police programs (PO, ELYS, Strasak, SSP) are integrated to ensure a holistic intelligence process (Politidirektoratet, 2006). Worth noticing is that it was intentionally not built for a specific field of criminality, and that the cybercrime landscape

has changed since 2007, meaning its intentional use might not be suited for cybercrime information. In regards of usage, Hustveits master thesis points out that it is time consuming for both the investigators and intelligence analysts to manually register information in Indicia, and the mutual consensus in the police is that "if information is not registered in Indicia, it does not exist", and that Indicia is "…Norways biggest fairy tale book, due to the amount of information that never is being touched. Until recently, this was the case. This generates a demoralization within the investigation environments" (Hustveit, 2017).

If one looks at the technical complexity inherent in intelligence from cybercrime and how the intelligence analysts describe the process in using this platform, then the indications points to that Indicia might not be the best analytical tool to use for cybercrime intelligence. However, this is the statutory platform used for police intelligence even though it might not seem sustainable for cybercrime information. Further, this is a mutual platform for both tactical analysts, intelligence analysts and investigators to work simultaneous on and indicators can be shared, before the processing and contextualization of data is done in respective analyst-specific tools, such as Analyst Notebook and iBase.

This emphasizes the analytical-centered intelligence process, where the analyst has an early involvement in regards of information collection, but also to have an overview of existing data to be able to find information gaps and to have a more controlled and active process of information collection. For cybercrime intelligence and its technical nature, this demands more knowledge from the analyst as opposed to "standard" intelligence work. And consequently, it will demand more from the technical and tactical investigator, where having an analytical mindset and to have a holistically perspective on the data is of great importance. Norwegian police separate intelligence analysts from tactical/strategic analysts, and investigators, meaning there must be a well-balanced system between them to avoid knowledge-gaps. If not, vital knowledge will remain locked up inside the heads of investigators and analysts, only retained when it is useful (Ratcliffe, 2016)

2.3.4 Hypotheses

Hypotheses is something that is applicable to both intelligence and investigation. A method focused on hypothesis testing is implemented as the best current practice (Fahsing and Bjerknes, 2017; Politidirektoratet, 2017b; Riksadvokaten, 2018; N. Sunde, 2020b) In the introductory phase in the intelligence process in the police, alternative hypothesis is generated to clarify the objective of the mission, which decision to be supported, and the testing of these is meant to provide a foundation for formulating information needs (Politidirektoratet, 2020). For the army, establishment and maintenance of situational awareness is based upon partly analysis and assessments of prior events, making it a foundation to generate hypothesis regarding future events. The results of these hypothesis testing's are an important contribution to fulfil the other roles in the intelligence process (Forsvaret, 2021). The use of hypothesis also understates the fallacy of being too induction-centered in the intelligence process, as mentioned by Hatlebrekke (Hatlebrekke, 2021), where he states that intelligence institutions must seek to foresee possible contextual threat combinations, and it is this duality that intelligence institutions should attempt to understand and elucidate. This is further mentioned in the Norwegian Intelligence Doctrine, where it says that it is appropriate to use alternative hypothesis, since this might provide more options for clarifications, increase objectivity and will elucidate various development possibilities (Politidirektoratet, 2020).

2.3.5 Intelligence-led policing

A systematically production and use of intelligence is a means for the police to plan and prioritize preventive measures to reduce crime (Politiet, 2020b), and the police shall work preventive within all areas, either under the police-umbrella or in cooperation with others

(Justis-og beredskapsdepartementet, 2014) and the objective is to be proactive to avoid negative events and actions (Myhre Lie, 2011; Aas, 2020). Bjørgo describes proactive means as barriers, in which several barriers to stop crime from occurring are needed in some cases. And these barriers are what can be described as proactive mechanisms, where the mechanism may provide an effect, such as crime-reducing (Bjørgo, 2015). One of these mechanisms is intelligence-led policing (ILP), which may be referred to as a management model and data driven movement, thus provide more objective grounds for deciding priorities and resource allocation with emphasize on sharing, collaboration, analysis, and intelligence (Ratcliffe, 2016).

The grounds for ILP came originally from a program called CompStat around 1980, where the fundamentals were policing from experiences (lessons learned) from previous experimentations, including a scientific analysis of crime problems, an emphasis on creative and sustained approaches to solving the crime problems, and strict management accountability (Bratton and Malinowski, 2008; Bureau of Justice Assistance, 2012) ILP made its appearance in the US prior to the 9/11 attacks, based on a concept from the British National Intelligence Model (National Criminal Intelligence Service, 2000), where understanding multijurisdictional crime threats, relying on proactive information sharing (internally and externally with other agencies) was used to develop a pathway toward solving the crime problems (Bureau of Justice Assistance, 2012). ILP was designed to challenge the dominant reactive, and response-based policing models where the operations dictates the intelligence gathering priorities. This is opposed to the ILP model, where the intelligence drives the operations, including a more holistic perspective that may prevent crime across a wide spectre (Ratcliffe, 2016). However, there submerges a problem for cybercrime intelligence, namely the potential of too much information, and the problematic venture of turning this into actionable intelligence. Ratcliffe describes this as being information rich, but knowledge poor (ibid). The large amount of data is however symbolic to the path we see in cybercrime policing, where the objective is no longer to determine the criminal responsibility but to reduce the uncertainty through risk management. The investigation relies on intelligence, where investigation provides data through case studies, and the intelligence apprehends data globally through a broader data collection (Barlatier, 2020).

To work with ILP in cybercrime demands more technical skills, and Omand points out that the government should try to anticipate future risk to prevent risk from arising, and to mitigate their effects through reducing vulnerability and increase the preparedness, especially within areas such as science and technology. In these areas the range of accessible information has been extended, the number of decisions to be had has increased, and information needs to be disseminated at a higher pace (Omand, 2011). Therefore, the standard intelligence wheel as shown in Figure 1 is insufficient for cybercrime intelligence because the different sub-phase happens simultaneously. To notify the clients in a timely manner, the process cannot happen sequentially, which demands more from each analyst then in the standard intelligence cycle (Steffensen, 2021). The intelligence process is now more analytic-centric as opposed to collection-centric (Harr Vaage and Sundal, 2019), where the analyst is central in different phases from the development of information needs, collection, processing, and dissemination of intelligence.

Thus, new techniques seem applicable, such as using the Diamond Model and MITRE ATT&CK framework. These new techniques can help reaching objectives for cyber-crime intelligence, such as disseminating the meaning of the information, and consequences of provided information, rather than provide the clients with technical data without any substance to it. However, one important challenge of cybercrime intelligence is to explain technical information which can be transformed to actionable intelligence. In standard

intelligence work the idea of presenting the 6Ws: what, why, where, who, when, and which is not that applicable for cyber-crime, where the questions are more based on the actual meaning. More appropriate questions therefore might be: So, what? What does this mean? Who cares? Who cares/to whom is this important for? (Steffensen, 2021).

So how does the police work intelligence-led in cybercrime? There is not an abundance of theory related to this, meaning ordinary intelligence-led procedures must be considered. At the very core of intelligence-led policing is criminal intelligence, which has multiple descriptions, but the one from International Association of Law Enforcement Intelligence Analysts (ALEIA), published by the United States of Department and Justice, is favourable:

> The evaluation of information and its comparison to other information to determine the meaning of the data in reference to a criminal investigation or assessment, which is further elaborated in terms of crime pattern analysis: a process that looks for links between crimes and other incidents to reveal similarities and differences that can be used to predict and prevent future criminal activity (United States of Department and Justice, 2012).

The actual indicators and entities have to be given a meaning and context, where placing them in a database to provide context and assessment by an analyst or officer seem reasonable (Davenport and Prusak, 1997).

However, as emphasized by Davenport, the assessed and contextual data must be categorized according to systems designed by intelligence professionals. This is where it might seem applicable to acquire inspiration from private information security agencies making use of threat intelligence platforms. If used by the police, the dissemination process might be a problem, since the information could be harder to transfer without some common unit of measurement that makes sense to both the transmitter and the receiver (Ratcliffe, 2016), making the dissemination process both a problem and a solution. However, by using common frameworks like the MITREATT&CK may help develop a mutual understanding of the content, and the classified data could be de-classified thus disseminated by utilizing MITRE ATT&CK matrixes. This process further underlines how the cybercrime police processes has become more analysts driven.

2.4 Cyber threat intelligence

What relates most to cybercrime intelligence is what in information security is called Cyber Threat Intelligence (CTI), where the focus is on others covert activity. CTI can help an investigator or forensic analyst identify and understand important evidence in the context of information gathered from other sources (Årnes, 2020) In the paper Extracting Cyber Threat Intelligence From Hacker Forums, CTI is described as a proactive approach, since it involves analysing data from multiple diverse sources, and identifies any indicator that can inform in advance about potential cyber threats, including their intent, resources, and methods (Deliu, Leichter and Nguyen, 2017; Papaioannou, 2021). Another definition defines threat intelligence as information that can aid decisions, with the aim of preventing an attack or decreasing the time taken to discover an attack. Intelligence can also be information that, instead of aiding specific decisions, helps to illuminate the risk landscape (Chismon and Ruks, 2015). One important thing to remember that separates CTI from police cyber intelligence products, is the price of the product. As stated in (ibid):

> At the more cynical end of the spectrum, it's been suggested that threat intelligence is at a threshold where it could become either useful, or simply antivirus signatures by another name… and at a higher price.

The police are not producing these intelligence products for profit, but rather to reach the end state of providing security and fight crime. Accordingly, the products should be deemed more reliable and trustworthy for the stakeholders. By having this perspective there are however elements and methods from the private information security industry that the

police may benefit from. The paper from Barlatier (Barlatier, 2020) describes how principles from prevention of cyber threats from private companies might be adapted to the police's handling of cybercrime, both in terms of intelligence and investigation. The risk anticipation and the mitigation of threats is at the core of information systems security, where the objective through its measures is taking a proactive approach to intelligence based on multi-source collection helping to understand, to track the threats, and to be able to attribute. This approach is opposed to the prior objective where monitoring, investigating, and repressing cyber-malware was the key measures in private industry (ibid).

This perspective might benefit all levels of intelligence: help decision-makers develop countermeasures on the tactical level, adapt the company's information systems security at the operational level, and enable managers to take measures of the risks linked to technical technology at a strategic level. This might be fundamentally intelligence-based hence transferable to police processes since its logical structures resembles the investigation phase by recreating the past. Thus, accumulated knowledge in this area developed by the private sector could benefit the law enforcement agencies.

2.4.1 The levels of cyber threat intelligence and the stakeholders

This section describes the different levels of CTI, and how the principles from CTI may be transferable to traditional intelligence, which here means cybercrime intelligence.

There are different goals on the different levels of CTI, where each goal can be described as: Tactical; How (technical aspects), Operational; What (understanding the attackers high level architecture and the attacker profile), and Strategic; Who and Why (understanding who is responsible for the attack) (Rid and Buchanan, 2015). According to MWR Security (Chismon and Ruks, 2015) there are four levels: strategic, operational, tactical and technical, as seen in Figure 2. But the CTI company Threat Connect (Papaioannou, 2021) only operates with two levels, strategic and operational. All four will be elaborated below.

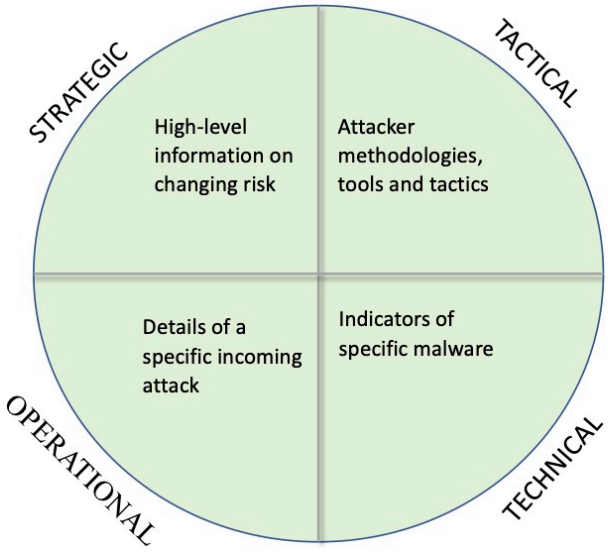

Figure 2: 4 levels of CTI. Influenced by(Chismon and Ruks, 2015)

Strategic

CTI illuminates how exposed an organization is to threats, and how those threats can be seen in relation to current and future financial risks, reputational risks, and continuity

operations. CTI products can be risk assessments, intelligence summaries and adversary profiles or assessments (Papaioannou, 2021).

For cybercrime intelligence in the police, this is the level in which most of the intelligence products are allocated, with references to the National Threat Assessment from PST (PST, 2021), and the Police Threat Assessment from Norwegian National Police Directorate (Politidirektoratet, 2021). These are both mainly strategic products and refers to cybercrime with little or few technical details. In the master thesis from Bahonjic (Bahonjic, 2021), he points out that the Police Threat Assessment, as a strategic product, is meant to provide guidance to which threats that should be prioritized in the preventive police work. This is further based on the idea that the Norwegian Police are focusing on working increasingly more knowledge based (Gundhus, 2013). Bahonjic found that the threats described in the Police Threat Assessment was assessed on "structured analytical techniques", which gives a constructed picture of order and systematic work, which terminologically hides as much information as it provides.

With the lack of technical details regarding cyber threats, the intelligence products from Norwegian Police are for decision making on a higher level, thus being strategic. And as mentioned in the paper from Deliu, Leichter and Nguyen (Deliu, Leichter and Nguyen, 2017), the motives and intent of threats changes less frequently as opposed to its TTPs (Tactics, Techniques, and Procedures). This means that strategic intelligence usually has a longer lifetime.

Operational

CTI on this level identifies threat indicators that increase detection capability and provide warnings of attacks or potential attacks. Intelligence products can be vendor feeds, open-source feeds of indicators, blog posts with indicators, and tactical reporting indicating attacks, capabilities, and infrastructure of adversaries (Papaioannou, 2021). At its core, the operational level provides information about specific impending attacks, and is consumed by security managers and incident responders (Nese, 2018).

MWR Security (Chismon and Ruks, 2015), as mentioned by (Deliu, Leichter and Nguyen, 2017), defined this as information about the nature of an incoming attack, and the identity and capabilities of the attacker. MWR Security also stated that this kind of information is difficult to collect for non-government organizations such as private security firms, as its collection demands legal permission (ibid). This makes it more relevant for the police if the dissemination of the intelligence also follows the same juridical requirements. Some of the examples mentioned in (Deliu, Leichter and Nguyen, 2017) are information about the vulnerabilities that different threat actors are exploiting, the methods and tools they use in each phase of the Cyber Kill Chain, and the communication manners between different threat actors. The operational intelligence can cover the scope from a simple IP-address to more complex indicators extracted from thorough investigations (ibid).

Tactical

This level contains intelligence on how threat actors behave, what their operations look like and what attack vectors are leveraged (Nese, 2018). This is often referred to as TTPs, and within private intelligence agencies this level is consumed by the security operation centre personnel and incident responders to ensure that their defences, alerting and investigation are prepared for current tactics (Chismon and Ruks, 2015). The outcome, or intelligence products, should be used for decision-making in terms of finding appropriate tactical approaches to solve a problem, where organizing defence and foresee the opponents' actions and dispositions is central elements. The goal should be to defeat an enemy in battle, where the essential element for tactical success is knowledge of the enemy and your own units, and being able to influence both (Johnsen, 2020). Tactical threat

intelligence is often acquired by reading white papers or the technical press, communicating with peers or purchase intelligence from other agencies.

According to (Politidirektoratet, 2020), tactical decision can be supported by intelligence for operational goals. Both in terms of the police's core tasks, such as prevention, security, criminal prosecution as well as different assistance functions. The decision made by the stakeholders should set a direction of how tasks should be solved, with a short time span. And as opposed to the yearly publishes from Norwegian police, this tactical intelligence should be disseminated more rapidly, and used actively when investigating, conducting structured intelligence analysis, or to guide the digital forensic analysis processes.

Technical

Chisom and Ruks describes this is as simple indicators, such as IP-addresses or hashes of malicious files, which has a short lifetime as attacker can easily change them, making this type of intelligence appropriate to be disseminated automatically (Chismon and Ruks, 2015). However, Nese argues that this should be referred to as "data", as opposed to "Technical Threat Intelligence", since the indicators is often provided without much context other than it is suspected to be related to malicious activity. This makes is difficult for security personnel to act on associated alarms and notifications, when the context is missing (Nese, 2018).

On this level the stakeholders in the police are the ones handling technical indicators and conducting digital forensic analysis. The core tasks here is to contextualize and enrichen the indicators, which will help decide which new hypotheses to be made, or to reject other hypotheses. The decision on this level is primarily done by the personnel handling the technical data.

2.5 The need for actionable cyber intelligence

By making information actionable, one must extract timely information, that can be immediately acted on from vast amounts of all data types flowing in, as reported from ENISA (ENISA, 2014). The same report further describes the importance of rapidly detect and understand incidents and vulnerabilities, and to address them before they are exploited. Sir David Omands all-risk intelligence cycle is good example to illustrate the need for actionable intelligence, where "action-on" has been added to his intelligence cycle, seen in Figure 3. This is done to emphasize the need for operational intelligence in modern times, where the use of intelligence is needed to support security operations in real time, or near real time, described as "action this day" (Omand, 2011). He does not specifically introduce the use of this cycle for cybercrime threat intelligence, but the basic principles are applicable. Further, the cycle shows how each phase is affected by user interaction, where the analyst is participating on all phases of the intelligence process.

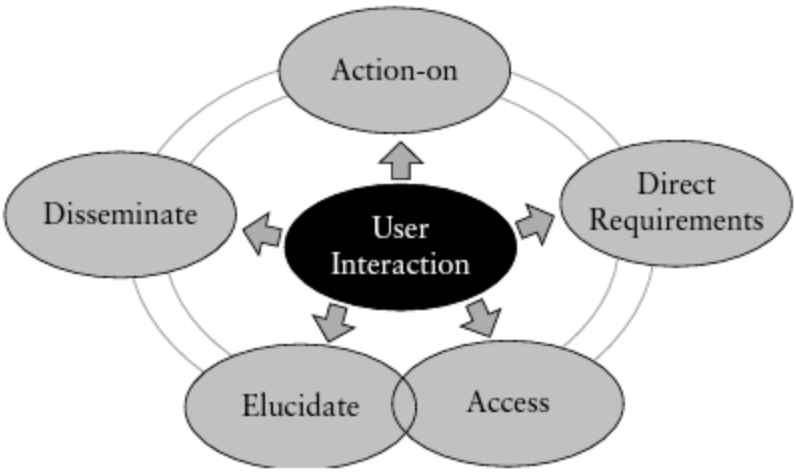

Figure 3: David Omands all-risk intelligence cycle (Omand, 2011)

But for the analyst to assess and be capable to extract the actionable intelligence, s/he must know the material and have a deeper understanding, and ENISA (ENISA, 2014) also points out that this analyst should also be involved in identifying how and what data to be collected in the first place, and that the actual scope of what is considered actionable will vary between stakeholders. There are however five criteria for information being actionable, as shown from ENISA (ibid):

- Relevance: it must be applicable to the recipient`s area of responsibility
- Timeliness: the actionable information must be timely
- Accuracy: the consumer must be confident that the information is verified and free of errors
- Completeness: provide value to the recipient in the context of the information readily available to the recipient
- Ingestibility: formats and transfer protocols used for data sharing

In policing, the initial handlers of seized evidence and other digital artefacts, is the digital forensic investigators, which suggests that the investigator could also function as an intelligence analyst. This person, depending on the degree of involvement in the case, should know the background and what she is looking for in the seized material, or in the received information. For the analyst some of the information that might be considered actionable are simple atomic indicators such as IP-addresses or e-mail addresses, or more complex analysis based on the digital investigation process, which includes vulnerability identifiers, indicators of compromise and attacker`s modus operandi (ENISA, 2014).

This new analyst centered approach to cyber intelligence demands the understanding and technical skills to fully grasp the technicality inherent in the data, both from the collectors of the data and intelligence analysts, or a merging of these roles for cybercrime intelligence. This demands emphasize on training, personal development and a mutual understanding of the possibilities and delimitations of the digital forensic investigators, as well as how the intelligence process works (Harr Vaage and Sundal, 2019). Harr Vaage and Sundal also says that this is not only an individual responsibility, but it has to be a task for the organization to develop a culture where this interdisciplinarity is both natural and wanted, and to work better together they have to learn each other's subject. (Harr Vaage and Sundal, 2019).

For the police, this implies that both investigators, analysts and intelligence analysts should work closer together, and be more integrated in each other's work. As an example, the criminal analysts (strategic and operational) in the Norwegian police are offered structured analytical courses, which enables them to use tools such as iBase and Analyst Notebook. But only a selected few are chosen to be given this course, meaning the capacity of the analysts are limited. Presumably, a technical digital forensic investigator could benefit from utilizing structured analytical processes when conducting digital forensic analysis. This is as opposed to request for assistance from the analyst-team, which from experience can be difficult to grant and hard to implement.

In terms of the actionable cyber intelligence and its productions in Norwegian police, the report from OAG (Riksrevisjonen, 2021) refers to a statement from NC3 that they do not have the capacity to collect intelligence for pure cybercrime, and that they are using all their capacity to provide assistance and investigate own cases. A result of this is lack of necessary information to conduct efficient, crime-fighting measures on this area. But they are trying to build capacity to produce own cybercrime threat assessments and intelligence based on knowledge to Norwegian context (Riksrevisjonen, 2021). Worth mentioning, is that this is not requested form either Justice Department or the Police Directorate from NC3. Nonetheless, in the report from PST (PST, 2021), cybercrime is mentioned on two pages, but the relevance of content being suited for decision making in the cyber environment is debatable, since it is merely mentioning the dangers of ransomware and how the pandemic has elucidated the vulnerabilities of public businesses with critical societal functions. That being said, NC3 are contributing to a mutual understanding of the threat landscape and sharing of relevant information to FCKS (Felles Cyberkoordineringssenter), where the participants are connected to the NCSC at NSM, which contributes to knowledge sharing for cyber threats in a public-private frame (Riksrevisjonen, 2021).

Also worth mentioning is a campaign ran by NC3 in 2020 which was dissemination of surplus information from a cybercrime penal case, where a large number of exfiltrated credentials was found in seized material, and warnings was issued based on identification process, as well as measures for how to avoid further damage (Politiet, 2020a). The dissemination process was based on phone warnings, together with a newly established and purposely build web page to establish grounds for credibility. Further, in February 2022, Kripos and Økokrim conducted a massive preventive operation, (Økokrim, 2022) where 170 businesses were given early warnings, and 28 possible cyber-attacks was estimated to have been prevented. The disseminated information was detailed to the point to where precise measures could be implemented to mitigate possible attempts of fraud. The background for this operation was one penal case and analysis of additional collected information from multiple other sources, which made it possible to reveal the criminals´ technique. The head of NC3, Olav Skard, said in a statement that:

> ...the primary strategy for the police is to prevent crime, and when we are able to prevent all these businesses to be victims for fraud, this gives out strategy positive effect (ibid).

The information that was disseminated on both these examples can be categorized as actionable intelligence, since the information described mitigation techniques and how to remove attack paths (Chismon and Ruks, 2015).

Ratcliffe (Ratcliffe, 2016) also has some perspectives on actionable intelligence, with references to John Grieve (Harfield and Maren Eline, 2008) former Director of Intelligence for the Metropolitian Police (UK), where it was argued that intelligence is information designed for action where the emphasis is on action. Ratcliffe (Ratcliffe, 2016) also elaborated what the difference between information and intelligence is, and he presented two thoughts regarding this. *Firstly*, it depends whether some action results come from the

decision makers interaction with the info, where the distinction rests with the consequence of the decision. *Secondly*, it ignores the value of intelligence to fuel non-action. Ratcliffe explains this by questioning if there is a need for intelligence to inform triage processes so that lower grade threats can be put aside through prioritizations processes. According to Andersen (Andersen, 2019) all the possible hypothesis that might explain the incident should be identified and tested, as a strategy and principle in the investigation process.

Ratcliffe (Ratcliffe, 2016) argues the same for the value of intelligence to fuel non-action, that it might strengthen the testing of hypothesis, in which intelligence frameworks could be beneficial to use, such as the Diamond Model of intrusion detection. In this model, each element of an intrusion event generates its own hypotheses which require evidence to strengthen, weaken or change the hypothesis by pivoting. To have success in this pivoting process, much relies on the analyst´s ability to understand the relationship between indicators and how they can successfully exploit a data element and data sources (Caltagirone, Pendergast and Betz, 2013). This also emphasizes the analysts-centric perspective, and how knowledge and technical competence is important in the intelligence process and to discover related, though important, elements in the data sets.

2.6 Structured analysis and avoiding biases

Within cyber intelligence there are some central terms worth noticing, such as CTI as mentioned above, activity groups and/or intrusion sets seen in correlation with attribution, capabilities such as TTPs describing the modus operandi, command and control (C2) describing parts of the threat actor's infrastructure, exfiltration from compromised systems and indicators often mentioned as indicators of compromise (IoC) (Steffensen, 2021). These are data that must be structured and analysed to be used for decision-making, and the process from information to intelligence products is known to be critical to cognitive biases. Some of these biases are the confirmation bias where the analytical process is influenced by the analysts' own beliefs and mirror imaging where there is a risk of believing that the criminal, or adversary, would do as yourself would do (Omand, 2011).

Another aspect of importance, since we are dealing with highly technical data, is the bias of assumption overruling evidence, where it might be easy to take shortcuts to assume something, where the analysts' knowledge might be insufficient. These biases might lead to intelligence failure which is essentially a misunderstanding of the situation, and could lead stakeholders of the intelligence to take inappropriate and counterproductive actions to its own interests (Shulsky and Schmitt, 2002; Hatlebrekke, 2021) Hatlebrekke claims that intelligence failures is found in human cognitive propensities, and the remedy is vastly formalized and made explicit in the analytical phase, supporting the idea of a more analytical-centered approach towards intelligence (Harr Vaage and Sundal, 2019; Steffensen, 2021). However, there are various methods and techniques used in intelligence agencies to avoid cognitive biases and intelligence failures, in which the police could benefit from using when structuring and finding meaning in the acquired data sets. These methods and techniques are further elaborated below.

If the police are to make use of these methods and techniques, the influence must come from intelligence-driven computer network defence and its risk management strategy. They address the threat component of a risk, with analysis of adversaries, their capabilities, objectives, doctrine, and limitations. A key component is to perceive the intrusions as phased progressions (Hutchins, Cloppert and Amin, 2011). The police are not analysing intrusion literally when conducting either cybercrime investigation or intelligence analysis, but its analytical principles, being important of the post-incident activities, seem applicable for the police. As mentioned above, two of the most common models over the past decade is the Diamond Model of Intrusion Analysis and Cyber Kill Chain, which compliments each

other to provide more depth when analysing intrusions (Nese, 2018). One way to work could be to use the Cyber Kill Chain for structuring data in single events, and the Diamond Model to group several compromises and identify patterns. The sharing of communications, as well as a being a database, is the MITRE ATT&CK framework. MITRE's framework illustrates the different phases of an attack, and external professionals and partners often tend to use this framework to see how MITRE is separating TTPs in computer incidents (Steffensen, 2021).

2.7 Methods and frameworks for intelligence analysis and intrusion detection

2.7.1 The Diamond Model of intrusion detection

The idea behind this model is that in order to attribute, one can not only focus on technical indicators, but has to see non-technical context in order to preserve the essential and complex relationships (Caltagirone, 2016). To describe intrusion activity four core features of an antagonistic event has to be in place: an adversary using a capability delivered over an infrastructure in order to target a victim and produce an outcome (Cook *et al.*, 2017). As opposed to Kill Chain, this model can see more complex relationships, but these two models can be complimented. There is also an Extended Diamond Model, which includes social-political and technology features. This is primarily to unveil the relationship between the adversary and victim, because there always are. As an example, one can see how long the adversary has been inside the computer systems to perceive the degree of persistence, which can tell us something about the motivation and capabilities. Further, one can by implement socio-political aspects find info about the adversary 's decision making, through psychology, victimology, and political agenda (ibid). However, the social-political approach does not lead directly to new elements or indicators, but by looking at the expected relationship between adversary-victim one can hypothesize who might be the next victim, and who might be attacking this victim (Papaioannou, 2021). The paper from Papaioannou exemplifies this by saying that organizations in one country might be targeted by a rival country, a company from one country may be attacked by a rival country with which it is at war. This example further emphasizes the need for collaboration within the Norwegian private and governmental agencies.

The main objective by using this model is to help the analyst find the adversary 's next step, and to help us ask the correct questions on the data, develop hypothesis, which in turn can help decision making and improve the cyber defence. The advantage of using the Diamond Model is how the operator can analytically pivot between the connected points, also called the core features, on the diamond to reach other connected points, meaning common capabilities being used in different intrusion events can be correlated and identified (Cook *et al.*, 2017).

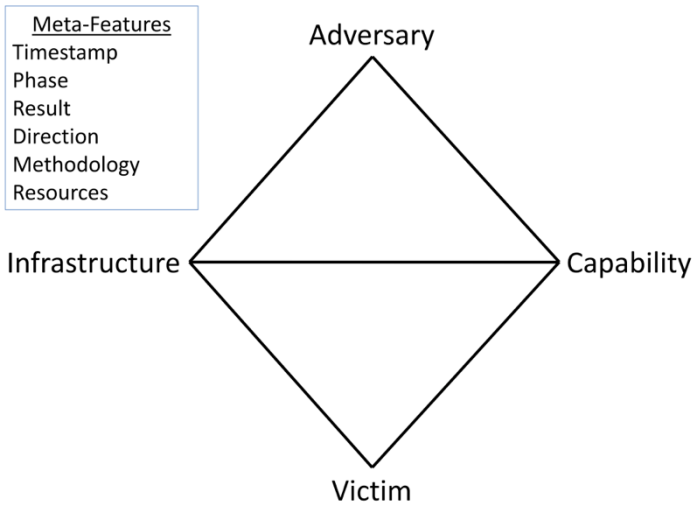

Figure 4: The Diamond Model of intrusion detection (Caltagirone, Pendergast and Betz, 2013)

The Diamond Model, illustrated in Figure 4, can be used by having four different perspectives: the victim-centered, the infrastructure-centered, the capability-centered, and the adversary-centered approach. These approaches are beneficial to utilize to make hypothesis, and the "hunt" may begin (Caltagirone, 2016). The meta-features are listed as well, and while not core features, they are still important in high-order analysis, grouping, and planning functions. Further, social-political and technology features can be added, in a model called the Extended Diamond Model, shown in Figure 5.

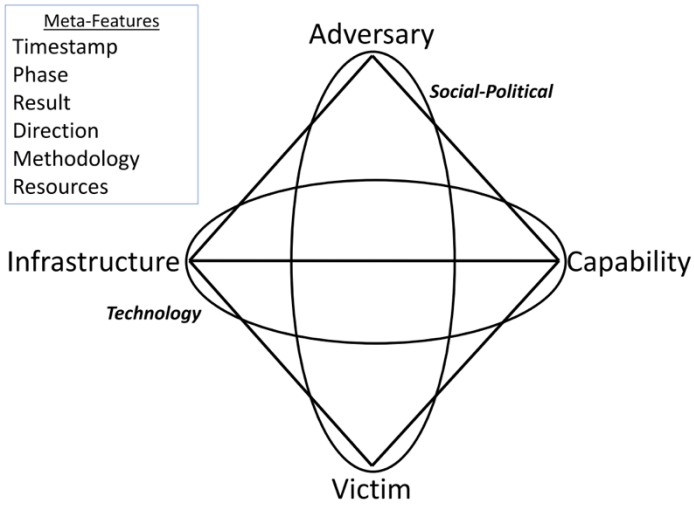

Figure 5: The Extended Diamond Model (Caltagirone, Pendergast and Betz, 2013)

The socio-political meta-feature in Figure 5 implies that there is always a relationship between the adversary and the victim, whilst the technology meta-feature represents the technology connecting and enabling the capability and infrastructure to operate.

The grouping and creation of activity threads are a process of finding correlations between events, both horizontally and vertically as shown in Figure 6.

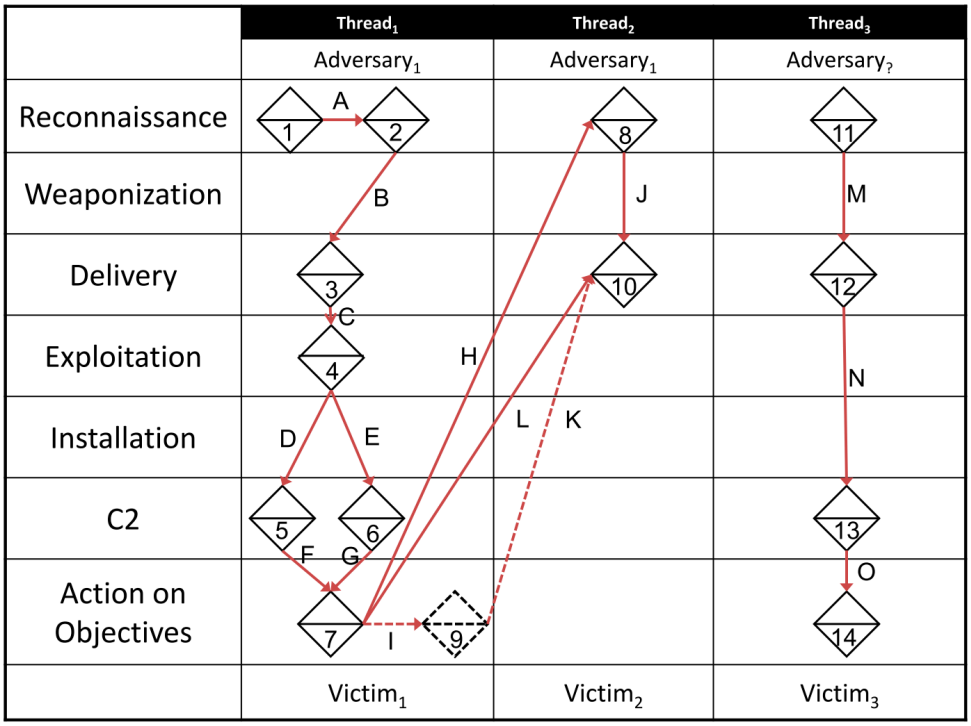

Figure 6: Activity threads in the Diamond Model (Caltagirone, Pendergast and Betz, 2013)

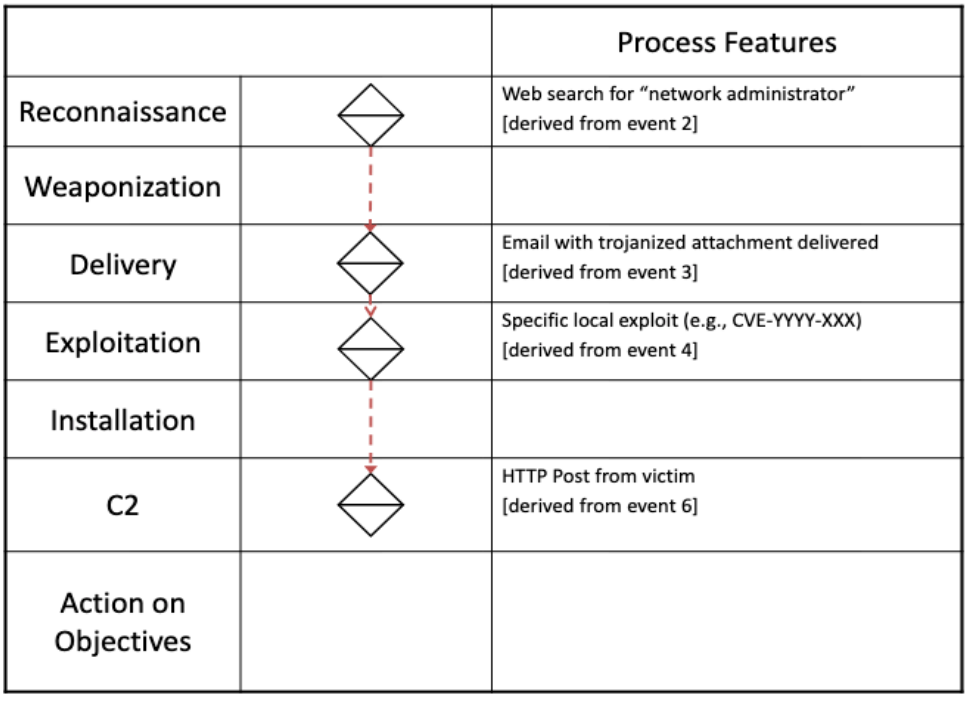

Figure 7: Process Feature in the Diamond Model (Caltagirone, Pendergast and Betz, 2013)

In Figure 6 one can see how Diamond events are being linked together vertically within a single victim, and horizontally across victims. The solid lines represent actual elements of information supported by evidence, whilst the dotted lines represent hypothesized elements. (Caltagirone, Pendergast and Betz, 2013). On the left-hand side in Figure 6 and Figure 7, are the steps in the Cyber Kill Chain to illustrate the phases of an attack. Activity

grouping is used to solve a variety of problems, and by placing events in activity groups, and as phase-based model where the process feature represents an event, knowledge gaps can be more easily identified, which makes a great foundation for making hypotheses.

For the police, Diamond Model can be used to discover new activity, see correlations, synthesize new information and pursue the adversary over time, all while maintaining the needs for communication and integrity. An intelligence product can be created that can be understood, without having in-depth knowledge of how the indicators works or why they are related, which also can be actionable and make grounds for further decision making. The downside of using this model is that it is time consuming and demands a certain amount of effort and resources to fully use the models' capabilities, and there must be a certain amount of data available. And as this research emphasizes, the police might lack both the data, capacities, and resources.

2.7.2 Cyber Kill Chain

This model sees cyber intrusions as phased progressions, not single events (Hutchins, Cloppert and Amin, 2011), and it is used to analyse the adversary, their capabilities, objectives, doctrine and limitations. The idea is that a cyberattack must follow a set of steps, or chains, and any deficiency will interrupt the entire process. The simplified chains are reconnaissance, weaponization, delivery, exploitation, installation, command and control and action on objectives. The outcome of using this model on digital evidence is to measure the performance of the adversary, and effectiveness of the actions to get a better understanding of the adversary. Another outcome is to reconstruct the intrusion, where the objective is to fully understand the attack, in every phase, to mitigate and gain leverage on future attacks, also the unsuccessful ones. The last outcome by using this model is doing campaign analysis, where the strategic objective is to compare multiple intrusion kill chain analyses. This is done to find key indicators, detect "how they operate", rather than "what" they do, to determine the patterns and behaviours of the intruders, their tactics, techniques, and procedures.

In the same paper (Hutchins, Cloppert and Amin, 2011), a case study is shown. Here are three different cyber incidents described, where the similarity in the different phases is shown. The Kill Chain analysis shows the same indicators prior to the exploitation phase, where the last incident used a 0-day exploit. All three incidents were mitigated before the last stage of the Kill Chain, actions on objectives, but they would not have seen the resemblance in the incidents if it was analysed post-compromise. In an investigation setting, it will be possible to make use of the whole Kill Chain process since incidents are only reported to the police after actions on objectives. This case study also shows that even though a 0-day exploit is used, we might hypothesize that this might be a highly sophisticated threat actor, which it most likely is, but the prior indicator in other cases can cast light on interesting artefacts in earlier stages of attacks.

As mentioned in 2.7.1., and shown in Figure 6 and Figure 7, the Cyber Kill Chain works perfectly with the Diamond Model.

2.7.3 MITRE ATT&CK

MITRE ATT&CK stands for MITRE Adversarial Tactics, Techniques and Common Know-ledge (ATT&CK). This is a framework includes a knowledge database for cyber adversary behaviour and indicators, which is useful in intrusion analysis and preparing a proper cyber defence. This framework goes into significantly more depth on how each stage of the cyber-attack is conducted as opposed to the Kill Chain framework, and MITRE ATT&CK is regularly updated with industry to keep up with the latest techniques. But MITRE can be implemented into the Kill Chain framework as a supplement.

The MITRE ATT&CK framework contains of a matrix where a set of adversarial techniques are presented, and these are categorized as tactics in the matrix. As with the Kill Chain, these tactics are presented linearly from the point of reconnaissance to the end of the attack, where the adversarial objective is met. Adversary tactics are categorized in 14 stages, as opposed to 7 for Kill Chain (Trellix, 2021): Reconnaissance, resource development, initial access, execution, persistence, privilege escalation, defence evasion, credential access, discovery, lateral movement, collection, command and control, exfiltration, impact. Table 1 illustrates these 14 tactics with a short explanation of their goals.

There are several ways to use this framework, depending on your objectives. In an investigative setting the best way to use this framework is by behavioural analytics development, where the framework can simplify and organize patterns of suspicious activity deemed malicious. Another benefit is to use the framework for CTI enrichment, where intelligence can be used towards the investigation. This is mainly information about the threat actor and its threats, and one can determine if compromised system could relate to an advanced persistent threat (APT), and common behaviours across multiple threat actors.

ID	**Tactic**	**Goal (The adversary is trying to)**
TA0043	Reconnaissance	Collect data to plan future malicious activities.
TA0042	Resource Development	Identify resources to support malicious operations
TA0001	Initial Access	Gain first access to your network
TA0002	Execution	Execute malicious code
TA0003	Persistance	Maintain their foothold
TA0004	Privilege Escalation	Get access to higher-level permissions
TA0005	Defense Evasion	Evade defenses to avoid being detected
TA0006	Credential Access	Acquire account names and passwords
TA0007	Discovery	Investigate your environment
TA0008	Lateral Movement	Move through your environment
TA0009	Collection	Collect data relevant to their goal
TA0011	Command and Control	Control compromised systems and communicated with them
TA0010	Exfiltration	Steal collected data
TA0040	Impact	Alter, corrupt, or destroy your systems and data

Table 1: 14 tactics presented with MITRE ATT&CK (Picussecurity, 2022)

3 Methodology

3.1 Introduction

The theoretical framework and choice of methodology will be discussed and described in this chapter, together with a presentation of the conducted interviews, and the analysis of the transcriptions. A qualitative methodical approach was used in this research to collect data on cybersecurity intelligence practices and needs among cyber security intelligence stakeholders.

3.2 Research methodology

There has been little research on how the police are conducting their cyber-dependent crime, which is defined as any crime that can only be committed using computers, computers networks or other forms of ICT (Europol EC3, 2017). Hence, the similarities and possible areas of cooperation between private enterprises and governmental handling of cybercrime is a somewhat unexplored area of research, apart from the surveys in NCDBS (Næringslivets Sikkerhetsråd, 2022) and the report from OAG (Riksrevisjonen, 2021). An important objective of the research is to explore on the experiences, tools, analytical approaches, and various perspectives from the individuals that are daily working with either IR or CTI, to see if this could be applicable for the police. For this research, a qualitative approach with semi-structured interviews of selected individuals were conducted. The interviews were analysed and broken down in categories and themes by using a thematic analysis approach. To best find possible measures and new procedures for the police to prevent cybercrime from happening, a socio-technical systems approach was conducted towards the results of the thematic analysis. Finally, the SBC-model was utilized to identify the measures.

3.2.1 Qualitative methodology

The qualitative methodology differs from quantitative that requires rigidity of data (Gunzenhauser and Gerstl-Pepin, 2006; Sloan and Bowe, 2014) and the qualitative seek to portray a world in which reality is socially constructed, complex and ever changing (Glesne, 1999). Another benefit of using a qualitative approach, according to Tjora (Tjora, 2021), is the possibility it provides of being curious of the "normality" and the meaning of routines and habits, such as how other professionals are handling cybercrime and their views on the police on the same subject. As such, a qualitative approach seem applicable, as it is based on recognition of the subjective, experimental, lifeworld of human beings and description of their experiences in depth (Glesne, 1999; Sloan and Bowe, 2014). Within qualitative theoretical approach there is a distinction between deductive and inductive approach, where the former often derives from a general rule to explain single events, which are often quantitative. The latter is when one assumes or develops general contexts from the observation of single events (Tjora, 2021), an approach often used in qualitative research. For this thesis, an inductive approach is chosen, and semi-structured interviews are used to collect the data.

3.2.2 Socio-technical system

Technology creates both possibilities and challenges, and the intersection of the two sets, social and technical insecurity, can be referred to as IT insecurity gap (Kowalski, 1994). This terminology is based upon the dynamics of technology and social change. According to Steinmetz, there are different premises for a crime to occur; the offender must have the opportunity to commit a crime, and this crime presupposes a potential perpetrator, a suitable victim or object, and inadequate protection of the victim or object (Steinmetz, 1982; Kowalski, 1993). In the socio-technical system approach, conceptual barriers in the

shape of social and technical may help separate a potential victim of computer crime from a potential perpetrator, and Kowalski describes this system with sub-categories, shown in Table 2.

SOCIAL	- Culture: represent the collection of values from individuals - Structure: represent the distribution of power within a system
TECHNICAL	- Machines: represent the technical artifacts used in the system - Method: represent the different techniques applies to the technical artifacts

Table 2: Socio-technical system with subcategories

For the system to be considered secure, these four sub-categories must be in equilibrium. If one sub-category is changed without consideration to the other sub-categories, it might take the system out of balance and introduce threats (Røger, 2019).

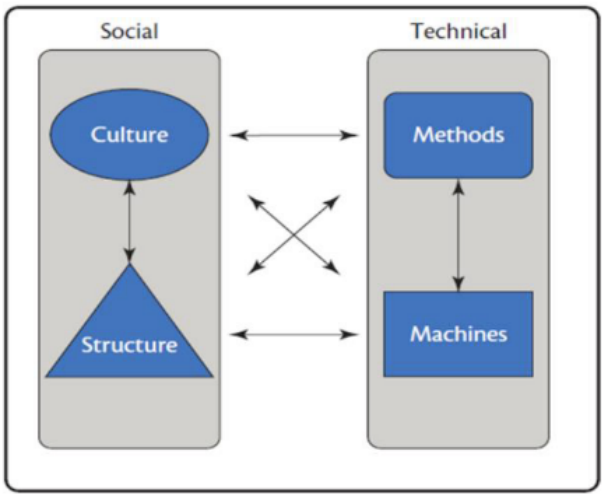

Figure 8: Socio-technical system model (Kowalski, 1994)

Figure 8 shows the social and technical components broken down into sub-categories. The arrows indicate multiple interchanges between the categories, and a change in the machines used in the system can not only affect the methods used in the system, but also the structure and culture (Kowalski, 1994). Kowalski further says that the underlying principle driving these interchanges is homeostasis or balance. Thus, cyber security can be seen as a continuous socio-technical process, combining human actors' interactions and behaviour with technical assets. This means that for cyber security to be effective, it requires both technical systems and people to act securely (Selebø, 2022).

For the police, a dysfunctional socio-technical system could be where new tools and methods are introduced without the sufficient knowledge to use them properly. Or that highly technical intelligence from crime cases and other information is not explained or understood properly by decision-makers. The results of both scenarios could i.e., be failure to disseminate critical information to the public and businesses, or to have the wrong grounds for deciding which cases to investigate next. The social-technical approach thus

seems appropriate because the measures consist of both technical and social aspects that can help the police to be better equipped to prevent cybercrime.

3.2.3 SBC Model

The Security by Consensus (SBC) model (Kowalski, 1993) is a theoretical framework to support IT crime prevention, build upon the socio-technical system represented by preventive barriers. Inadequate protection can be classified according to the two classes of barriers or protection mechanisms: inadequate social protection or inadequate technical protection. These two barriers can further be divided into six levels, as shown in Figure 9.

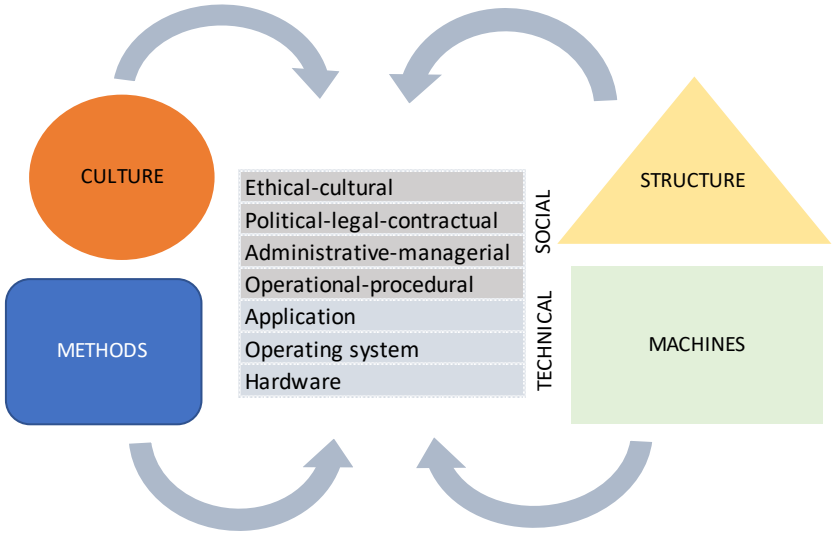

Figure 9: The SBC Model

Figure 9 illustrates how measures from either the culture, methods, structure, or machines category are proposed into the framework and traversed through the different levels. Potential insufficiencies on each level are mapped out that hampers the level to be a complete stack of integrated levels (Schumann, 2021). By doing this mapping, certain enablers in both social and technical sub-categories are elucidated (Røger, 2019). An example could be to introduce two-factor authentications for all employees.

The different sub-categories of the model are described in 3.2.2

The SBC model's main intentions are to find the root-causes of a problem, and to serve as an abstract model of system's problems at different levels (Kianpour, 2021). One example is to use the model to examine inadequate protection mechanisms of a cyberattack. There is however another way of using this model, as illustrated in Schumann's research (Schumann, 2021) where he uses the model to map appropriate measures on the different levels in his socio-technical analysis. The same methodology is used for this research, where identified measures from the thematic analysis is mapped in an SBC model, and proposed measures are illustrated and linked to either culture, structure, methods, or machines in the police.

3.2.4 Background and biases

A bias in a research study is any influence, condition, or set of conditions that singly or in combination distort the data obtained or conclusions drawn (Leedy and Ormrod, 2015).

The researcher has worked as a police officer for many years and was working as a digital forensic investigator with cybercrime when this research was commenced. Hence, the state of cybercrime within the Norwegian police is relatively known, and the research topic was selected based on a motivation to increase Norwegian police efforts and capacities in handling, processing, and preventing cybercrime.

This background has thus influenced the research topic, as well as the interpretations made during the process of interviewing and the analysis. The decisions of selecting relevant data from the analysis was also influenced by the researcher's background. This could also trigger the response bias, where the interviewees answered what they thought the interviewer wanted to hear or felt demanded to provide certain answers.

3.2.5 Strengths and weaknesses of the study

The profession as a technical investigator has contributed to identifying what could be feasible for the police when identifying possible measures, and when analysing the interviews from personnel working in the private industry. However, by not having in-depth knowledge of how private industry handles intelligence or IR, there is always the risk of the Hawthorne effect (Leedy and Ormrod, 2015) where the participants change their behaviour by participating in the research. As a result, the participants might seek to give a perception of a better work performance than they would perform in reality (Sunde, 2017).

In regards of the SBC-modelling, as seen in 3.2.3, it should also be mentioned that the participants were specifically asked questions regarding the methods and frameworks of the Diamond Model, MITRE ATT&CK, and the Cyber Kill Chain, which occupies three proposed measures. However, the answers from the participants indicated that they are frequently used, or influenced by, in the private CTI community, thus appropriate to propose as measures.

Another weakness of the study is that the interviews were conducted in Norwegian and translated to English during transcription by the researcher. To ensure reliability, the interviews were recorded both on video and on additional sound, and unclear pronunciations or expressions were marked in the transcription and eliminated if not possible to translate correctly.

Lastly, there is a possible weakness in the research that all participants are male. Ideally, this research could have been more gender balanced.

3.3 Research procedure and data material

3.3.1 Sampling procedure

This research project is phenomenological in nature and attempts to understand the participants' perceptions, perspectives, lived experiences and meanings (Kafle, 2013), relative to a cyber intelligence process within the police. The sampling strategy was a purposive sampling, where participants were chosen based on certain prespecified characteristics relevant to the research problem (Leedy and Ormrod, 2015), such as either working with CTI, IR or other relevant security positions. The author contacted governmental agencies and private businesses with a description of the research topic. The request was issued out to specific agencies and businesses that the researcher knew worked with areas in which could enrich the research data. Some requests remained unanswered, but in the end the author selected 5 individuals from private cyber security businesses and 1 from a CERT working with CTI. Three of the individuals from the private sector was selected based on the snowball-effect (Creswell, 2007).

The last participant is a police intelligence analyst that the researcher knew worked with cybercrime intelligence, thus relevant for this research.

The participants are listed below, and the abbreviations are used in the following thematic analysis.

Participant 1: Corporate security manager in a private firm. Former police officer
Participant 2: Security Director in a private firm. Specializes in intelligence
Participant 3: Works with CTI for a Computer Emergency Response Team (CERT)
Participant 4: Works with cyber intelligence in the police
Participant 5: Works with CTI for a private firm. Former police officer
Participant 6: Works with CTI and IR for a private firm
Participant 7: Works with CTI and IR for a private firm

Table 3: Participants in the study

3.3.2 Semi-structured interview

As opposed to structured interviews, where the researcher asks certain questions and nothing more, the semi-structured interview is more individually tailored to get a clarification or probe a person's reasoning (Leedy and Ormrod, 2015). This form of interview is often used in the social sciences for qualitative research purposes, and it is focused on a core topic to provide a general structure. This also allows for discovery, with space to follow topical trajectories as the conversation unfolds (Magaldi and Berler, 2020). There were issued an interview guide (Appendix A) prior to the interviews, which contained open questions in which the participants were allowed to elaborate.

3.3.3 Data analysis

Thematic analysis was used as an approach for the analysis, which is both a strategy and a tool that provides a rich, detailed, and complex account of the data (Braun and Clarke, 2006; Ho, Chiang and Leung, 2017), where the method includes identifying and reporting patterns (themes) within the data (Braun and Clarke, 2006). The idea in thematic analysis is to recover the theme or themes that are embodied and dramatized in the evolving meanings and imagery of the work (van Manen, 1997; Ho, Chiang and Leung, 2017). There are two approaches to thematic analysis, being theoretical and inductive thematic analysis, where the theoretical utilizes a particular theoretical framework for the analysis. The inductive is data-driven, with no attempt to fit the data into a pre-existing theoretical framework, or into a researcher's analytical preconception (Hsieh and Shannon, 2005; Braun and Clarke, 2006; Ho, Chiang and Leung, 2017).

However, there are flexibility amongst these approaches, as described by Anderson et.al (Anderson *et al.*, 2014). Anderson mentions how the researcher may apply a method to data, and still make their epistemological assumptions explicit, claiming the researcher must be clear about what they are doing and why, and to include the often omitted "how" they did their analysis (Braun and Clarke, 2006). Braun and Clarke also claim that a thematic analysis has limited interpretative power beyond mere description if it is not used within an existing theoretical framework that anchors the analytic claims that are made. For this research an inductive thematic analysis was chosen together with the theoretical frameworks of socio-technical systems and SBC-modelling.

There are however some pitfalls in using such a flexible method, because it allows for a wide range of analytic options, it may be difficult for the analyst to decide what aspects of their data to focus on (Braun and Clarke, 2006). The pitfalls are tried mitigated by using a solid interview guide and utilizing the socio-technical systems approach to identify causes and opportunities, together with an SBC-modelling for presentation of measures.

In thematic analysis there are certain phases to follow, as described by Braun and Clarke (Braun and Clarke, 2006) revolving around getting to know the material thoroughly and generating codes and themes from it. The goal is to find patterns of meaning and issues of potential interest in the data, where the endpoint is the reporting of the content and meaning of patterns (themes) in the data. This is not a technique that is unique for thematic analysis, as it relates to the constant comparative method, being a known technique in qualitative research where the researcher moves back and forth in the data looking for patterns or dynamics in the phenomenon being investigated (Leedy and Ormrod, 2015). However, the guide to conducting a thematic analysis presented by Braun and Clarke (Braun and Clarke, 2006) was appealing, which is the reason the researcher ended up using this form of analysis. In thematic analysis these are the steps to follow: familiarizing yourself with the data; generate initial codes; searching for themes; reviewing themes; defining and naming; producing the report.

The material was familiarized during the actual interviews, which was further reinforced through the transcriptions of them. The transcription was time consuming and written manually after unsuccessful attempts to automate it. The next step was to code the interviews based on what was deemed interesting and relevant to the objectives latent in my research questions. The coding was conducted in Excel, where different parts of each interview was given a code, and sometimes the same statements was given multiple codes. This process ended up with 166 codes, which later was analysed and taken into consideration on how different codes may be combined to form overarching themes. The result were 10 sub-themes and 2 main themes, as shown in Figure 10.

For this thesis, the research area is somewhat under-researched, and a rich thematic description is used, to make the reader aware of the important themes (Anderson *et al.*, 2014). The two main themes will form the foundation on how the socio-technical systems approach are utilized to try to answer the research question. The whole process of generating codes and themes participated in identifying both similarities and differences in how the police and private industry are working, and to compare them to one another. The two research questions were not introduced to the process until after the thematic analysis was done, as this can be a pitfall during the thematic analysis (Braun and Clarke, 2006; Hustveit, 2017) The questions were however extensively used when identifying causes and possibilities from the thematic analysis.

3.4 Quality assurance

3.4.1 Validity

To have validity in the research means that the project can yield accurate, meaningful, and credible results, in which defensible conclusions can be drawn. The internal validity for qualitative research means to minimize alternative explanations for the results obtained (Leedy and Ormrod, 2015). This research has used different theoretical methods to ensure that the final conclusions are as accurate and trustworthy as possible. Firstly, thematic analysis was used to break the interviews down in codes and themes. Secondly, a socio-technical systems approach was utilized to find causes and possibilities, and thirdly, SBC-modelling was used as framework to identify possible measures. The socio-technical systems approach can especially increase the internal validity, where the intent of using it was to identify possible cause-and-effect relationships. However, to ensure the internal validity further, some precautions could have been taken to eliminate other possible explanations, such as interviewing individuals from the different socio-technical levels, as used in Kowalski's socio-technical system approach (Kowalski, 1994). The levels of interest in this research are the level above (prosecution members, policymakers, and leaders),

level in focus (analysts and investigators) and level below (victims, citizens, and costumers). By doing so, the outcome could have been more nuanced and valid.

The external validity is whether or not the result of the study is true for other cases, such as different people, places or times (Volden, 2019). For qualitative research, this means that the research is generalizable to the world "out there" (Leedy and Ormrod, 2015). To ensure external validity, Leedy and Ormrod mentions some strategies to follow to ensure validity: Firstly, the researcher should acknowledge personal biases, which has been addressed here in 3.2.4 and 3.2.5. Secondly, the researcher could spend extensive time in the field, and i.e., study a particular phenomenon. This master's thesis is experienced-based, hence the research should to some extend be based upon experiences. The researchers background, as mentioned in 3.2.4, implies understanding and knowledge of the researched area, as well as a perception of weaknesses and rooms for improvement. Thirdly, the researcher can use a thick description of the researched areas to allow the readers to draw their own conclusions from the data presented. In this case, the interviews were transcribed, and all the content of the transcriptions were used in the future coding and making of the categories. All categories are explained under chapter 5, thus enabling the reader to make their own conclusions. The thick description is also mentioned in 3.3.3, but there referred to as rich thematic description (Anderson *et al.*, 2014).

3.4.2 Reliability

To have reliability in research means to reduce errors and biases, such as applying standardized methods and correct criteria (Volden, 2019). Creswell (Creswell, 2007) mentions one strategy aiming at having good integrity when collecting data in qualitative research. This strategy is also in line with the importance of consistency and the trustworthiness of the research results, as mentioned by Sunde. (Sunde, 2017; Kvale and Brinkmann, 2019). The consistency and trustworthiness should also apply when transcribing the interviews and during the analysis of the collected data.

These aspects were addressed in this research where the interviews were conducted online, with both videorecording and additional sound recording. The interviews were then transcribed, and a thematic analysis was applied for coding and identification of themes. The application of the socio-technical systems analysis will contribute to strengthening the reliability, as well as using the SBC-modelling for identifying the measures.

The weaknesses are that the interviews were translated during transcription by the researcher. One way to possible bypass this would have been to conduct the interviews in English. Another potential weakness is that the coding and socio-technical analysis was conducted solely by the researcher. Ideally, these processes could have been conducted with a peer, but this was not a feasible option for this research.

3.4.3 Ethical and legal

The participants in a qualitative study should be protected from harm, must be voluntary and well-informed, have the right to privacy and be given appropriate credit where credit is due (Leedy and Ormrod, 2015). Prior to conducting the interviews, all participants were provided a consent form, which described the study, the ethical considerations of participating, and that they could withdraw their consent at any time. This was signed by the participants before the interviews began. The consent form is annexed in this thesis (Appendix B).

The participants' personal data was stored appropriately according to applicable rules, and before the data collection began, the author applied to NSD (Norsk Senter for Forskningsdata) for approval. This form is annexed in this thesis (Appendix C).

The interviews were anonymized during the transcription, and each participant was given a number, see pkt. 3.3.1.

The participant's spent around one hour of their time for the participation, and the identified measures presented in this thesis might be overwhelming, and hard to implement. The question is therefore if the benefit is greater than the cost for both these measures and the participants. By looking at the external validity, the benefit of increasing the police's ability to prevent cybercrime, would help towards a more resilient and secure society. And if the interaction and cooperation between the private business and the police strengthens during this process, this could benefit both parties, as well a better sense of security for the citizens and the societal critical assets.

4 Data Analysis

This chapter presents the findings of the interviews and the following thematic analysis of them. The structure of this presentation is to separate them in the two main themes and discuss each subject. The two main themes were separated in a police-theme and an intelligence-theme.

As mentioned in 3.3.3, there was identified 10 sub-themes which was broken down to 2 main themes. These themes are "police and cybercrime", and "cyber threat intelligence and processes", since these were the two main topics covered in the interviews. And by separating the further analysis in these two themes, the research question could thus be more elucidated, since it deals with both the police, and how policing in cybercrime can be supported by methods and techniques from cyber threat intelligence.

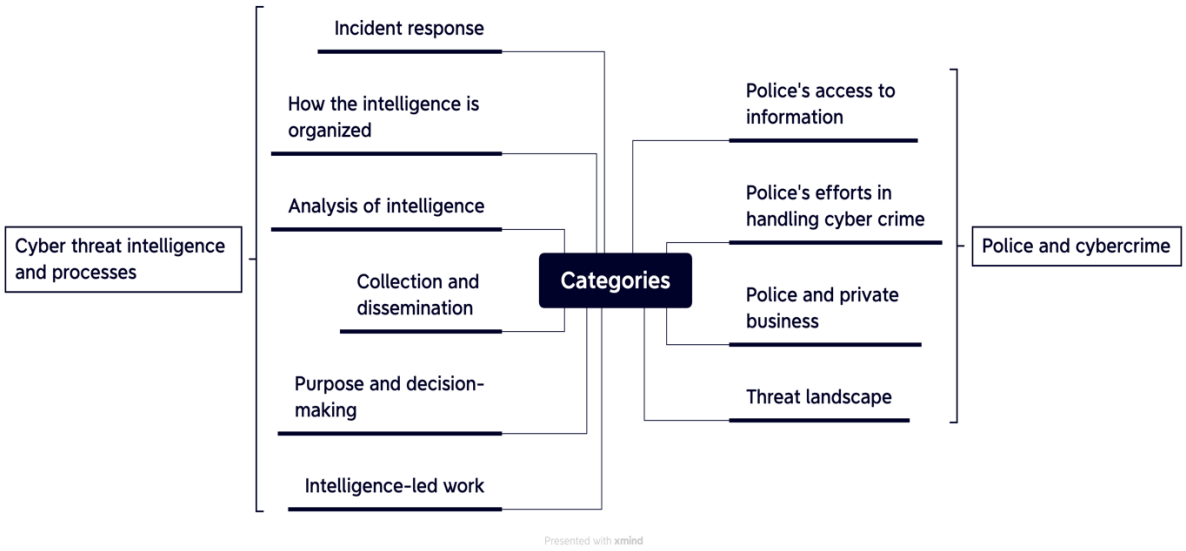

Figure 10: Thematic analysis categories and themes

4.1 Police and cybercrime

4.1.1 Police's access to information

The increasing number of under-reporting of cybercrime was one of P1's main concerns, and if this continued, the outcome might be that the police are not getting information regarding cyber criminality. This might lead to insufficient capacities, less resources to use and not enough economical funding.

P4 said that based on the number from NCDBS in 2020 (Næringslivets Sikkerhetsråd, 2020), this indicated vast under-reporting to the police, meaning it was hard to work intelligence-led, and this would cause an overall low confidence. However, as mentioned by P1, the problem might be inherent with the police also, where they were aware of the problem, but did not dare to touch it.

In regards of cybercrime and the police-reporting of them, there were a broad agreement that this was a process more demanding than useful. P1 said that all criminal actions that happens in private business should be reported and said the reason for this was for the police to have a more accurate and sufficient statistical basis needed to assign resources and economical funds to fight cybercrime, and to see the crime-development. P1 also stated the following:

> it might seem useless and a waste of time to report crimes to the police, but it could be, down the line, your case making the big difference enable something to become a large investigation, and someone is being arrested in the other end, having to face the consequences of their actions. (P1)

In regards of the actual reporting, P5 concluded that the efforts in collecting correct information and consult the company to report it, had not been worth it, because the apparatus to receive it at the police was inadequate. The experience was that nothing really happened after one had filed a report, and for P6 would a simplified possibility of reporting make the companies report incidents more frequently. P6 gave an example that this could in the shape of a desk the offended party could contact, explaining to the person on the desk what the problem was, and simultaneously ask if this was something the police would investigate. If no, then the police could have said that they still wanted information regarding the result of the internal handling of this incident.

According to P5, much of the responsibility laid with the police:

> In a very simple way, if you have proper knowledge, the costumers will return. This is about creating good experiences, and see the potential in a crisis, and to help where you can. And if you communicate thoroughly, also regarding the limitations. Because it's not just that things will magically be solved because you try, but that you can become better at talking.I think that is the first step, to have a well thought out dialogue and then include feedback to the victim in a good way. It must start there to increase reporting. (P5)

A simplified reporting routine was mentioned by several of the interviewees, such as when P7 commented that that the process of reporting had to be easier, especially knowing that most cases are dropped, or just collected and nothing more happens, other than having the statistics. P7 further said that several of their clients had critical infrastructure, meaning they had other means of reporting, primarily to NSM, since the clients now were participating in NSM's approval for IR. Therefore, P7 and the team were filling out a monthly one pager to NSM with information on what had happened lately. P7 didn't know if the police received any of this from NSM.

P6 thought that it was primarily extra work to call the police when an incident had happened, and that if the police would have a more agile way of saying: "we are actually going to act on this, and we wish to be involved", then the police might have appeared less like an anchor in the process:

> What if it would actually be valuable to reach out to the police for help? (P6)

The security services offered by P6's team were expensive, and smaller business could not afford this. A ransomware-attack could be the end of for these smaller businesses, and that there should be a place for them to call for help in the case of a cyber-attack, which should be from the government.

P5 had experienced that there really hadn't been an apparatus ready at the police to receive information from them or the offended company. On the other hand, from P5's own police experience, this was quite the challenge for many police districts inexperienced with cybercrime. The police were supposed to handle many types of crimes, and P5 had experienced that computer crime cases ended up with the group for environmental crime, being littering and forestry, or financial investigation where only one person worked. P5

further said that it had been difficult for local police to have knowledge about cybercrime and to have a certain understanding of the phenomena. There had not been a template or guide to follow for local police, such as it is in burglary, rape, and fire, thus there was need for a "playbook", an encyclopaedia, or at least something the police could use for support and to look up where to seek for further help.

4.1.2 Police's efforts to handle cyber crime

There were many and different opinions regarding this subject, and some of the statements and quotes here could also have been placed under chapter 4.1.1., because a consequence, or effect, of the capabilities of the police could be less flow of information. There were a mutual understanding and opinion amongst the interviewees that the police were unable to handle cybercrime sufficiently, and they all presented various possible reasons and remedies for this. Some of the elements that stood out was the governance of the police, lack of resources, limited access to information and legislation issues. But they also gave the police credit for some of the recent arrests and investigations.

P1 suggested that the issue of police capabilities must be raised high on a political level, and maybe influence and elucidate the scope of the problem. If the police had nothing to negotiate with it can be difficult. P1 also mentioned the jurisdictions, both the international and domestic, because this was border-less crime, which made it difficult for Norwegian legislation.

In regards of the transnational perspective, P4 and P3 mentioned that many threat actors operated from abroad, meaning it hampered the preventative perspective. P3 proposed that more cooperation with international organizations, collect information and facilitate to understand the threat and risk, may enable arrests of the criminals:

> To find them is hard, but not that hard if you put the right resources in. (P3)

But to do so, according to P3, the correct mandates must be in place, both politically and in intelligence to find the perpetrators.

P1 said that the legislation ought to be revised, such as the Criminal Procedure Act with regards of coercive measures, storage of data etc., and that legal development is not keeping up the technological development:

> I often feel that we protect criminal acts too much, and that we are afraid to share information. (P1)

According to P2, there were now often private business doing the police's job, and said that the police should be making more arrests and be proud about it:

> It must be evident that it is frightful to be a cybercriminal. Confiscate money, take the luxury yachts away from the market and get rid of all of them expensive cars. (P2)

The prevention of cybercrime was also mentioned by P2, and how an early contained situation from the police could be effectful, such as preventing stolen data from being sold with the rest of the criminal underground. As an example, P2 mentioned a ransomware case where sensitive data was exfiltrated and could be found on the criminal's extortion sites. This data contained sensitive data regarding children welfare cases, and that the children were the real victims in the ransomware case, and in need of protection. The political consequences for the offended governmental business or the staff was unimportant, and that the police should dare to act strongly:

> When they put lives in danger, they should know that the consequences are not only bad publicity on Twitter, but a pair of handcuffs and jail time. These guys can take actual lives. (P2)

The police had good intentions, P1 said, but were held down by lack of resources, economic issues, and not keeping up with the technological pace. Unfortunately, this issue would not be helped, nor solved, when competent police people are hired by private companies either, because the economic terms are better there.

P5 introduced a centralized register governed by the government, a database where Norwegian companies, or that operates from Norway, had to share anonymized data from security incidents, as a type of national MISP (Malware Information Sharing Platform) or similar. P5 said that this could be a part of the police's mandate in justice preparedness, where the data from incidents are placed in the database, and either the police, or others by providing anonymized access and search possibilities, could search and use it to increase their understanding and get manageable information from it.

However, as mentioned from P4, the police were unable to investigate themselves out of this problem, hence the focus could be more on intelligence. Accordingly, P4 said that NC3 were mandated to investigate 2-3 cases each year, but P4 did not believe the police would overcome the problem this way. P4 suggested that to focus more on intelligence the two-part purpose had be taken into consideration: to use intelligence for case selection, and more importantly: use intelligence for preventive measures. The police's capacities on traditional intelligence and crime analysis could be utilized towards cyber intelligence, P4 said, because the personnel working in these areas in Norwegian police did so with high quality. By doing this, according to P4, it could provide a more dynamic organization, where police forces could be placed where it was needed.

In regards of intelligence versus investigation, P4 mentioned that the police had to cooperate better, and the important issue was that things were conducted correctly, meaning guidance from a methodical attorney that could help when they moved from intelligence to an investigation. This shift in the process was driven by the Criminal Justice Act, which deployed a whole other set of rights etc., for the involved parties. In regards of using information from investigation towards intelligence, P4 had this comment:

> I think that you must have opportunities for intelligence people to work and have access to the information and be able to help extract things. (P4)

There was also a unity amongst the interviewees that the police truly had good intentions in the environment of cybercrime, but that they were hampered with lack of resources and personnel, limited economical funding's, issues with jurisdictions, not enough political leverage, and low level of competence both on decision makers and ground personnel in the police. These elements combined, P1 said, has made people lose their faith in the police in the battle against cybercrime.

In P4's mind, the technical competence made it problematic in two ways:

> You first have to understand the content of incoming information, and then you have to translate this as an intelligence analyst to decision makers. (P4)

Further, P3 said that there had not been that many technologists in the police, but rather competent investigation personnel which might not have had a proper technical understanding. And from own experience, the technical level of police personnel in antifraud cases was high, but low in cybercrime cases. When P3 started in the job in 2018 and reached out to the police for help, it was like throwing the case information into a black hole, and it was a struck of luck if there were anyone who knew what this meant upon receiving the information. This was a bit better now with the build-up of NC3, according to P3.

P2 said that their company would always be friendly with the police, and give them access to cases, if the investigator and the police attorney had a certain degree of

understanding what they are doing and were able to ask the right questions. Then they can gladly coach the police if they need, and they had also hired a former police officer because they needed someone that understood the human "police API". P2 mentioned that the police's "Næringslivskontakt"[4] had been amazing, meaning this person had shown a great understanding of policing and had functioned as a gateway to protect the inner dynamics.

P4 lastly mentioned the mandate to keep the citizens safe, and how the threat landscape was complex, and how it was evident that the police had repetitive challenges with the borders toward the mandate of the Security Services on a national level in Norway and the police

4.1.3 Police and private business

P1 was disappointed when hearing about the private businesses' experience of the police, where expectations did not meet reality. And the fact that private business hired police officers was becoming a vicious circle, because everyone in the private business were trying to get the best competent people and use a lot of money and resources to do so. They saw themselves having to secure their own business when there is no help from the police, and P1's company was experiencing that it was hard to find the right people for their jobs. Everyone was headhunting, and the police couldn't keep up with the pace, P1 said, and said this in relation of being a former police officer:

> This is what causes me to have the constant conflict with myself: should I stay in private business, or should I stay in the police? If you don't have that experience, or that inherent thing in you, then it's quite clear and the choice is easy: you choose higher salary if you are assessed really competent by the private sector. (P1)

P4 saw this a bit differently, when saying that if someone from the police travelled to the private business this might be a strength for the company, but also for the police. Because then they could work more preventative, and the former police personnel could receive the police`s assessments and generate actions for the company.

In P2's mind, there weren´t many good digital forensics analysts in Norway, and P2 would like to hire many to their own company. But by doing so, the police would be drained for forensic personnel, and P2 didn't want to ruin things for the police. But P2 thought the police had to make police work more attractive and display their achievements. If not, the police would decay.

P2 further said that there was a mutual consensus amongst the biggest private companies to not hire competent personnel from the newly established NC3, but rather let NC3 grow strong peacefully and show its efficiency before they (private businesses) tried to hire them with proper salaries. On the other hand, if people went from P2's business to the police conducting useful societal affairs, this would be great P2 said. But for this to happen, the salary, terms and visibility and everything else had to be in place.

It was a broad consensus from the participants working in private business to cooperate with the police, and P1 said that they were more than happy to collect logs, put together the evidence, analyse IP-addresses and measures prior to reporting it to the police. The collected material and analyses could also work as leverage when talking to the police, to make the police prioritize the case.

According to P1, a few cases with good cooperation with the police per year, would have helped. The outcome didn't have to be positive, but just by showing their will to talk and

[4] Police personnel whose function is to ensure good local cooperation between police, business, security authorities and other actors in society (Politiet, 2022).

join and participate internally and to our partners. P6 mentioned how things had gotten better in private business during last 3 years, where they simply were not allowed to report incidents to the police because the leaders were afraid of being on the front page of national newspapers if they talked with them. This has gotten better now, but there is still a resistance towards free interaction with the police.

P2 meant that the key is to be more transparent, and for the police to remove the silk gloves, and mentioned the successful investigation done by NC3 and cooperating agencies (E24, 2021) of the Hydro-attack in 2019, and how the cybercriminal group ReVil (Reuters, 2022) was taken down by U.S. request:

> The criminals don't deserve to be treated nicely. Move in with more force, remove the silk gloves. The cyber-security community cheered when we saw REvil was taken by the Americans and the police. And the case that NC3 did with the Hydro case, we just said "yes-yes!", and it was amazing. It was joy and cheering. It should cost to do crime, and it should not be worth it to buy a gamer-world-reality for you to spawn a new person and keep on with your crime. (P2)

P3 were more than glad to help the police, and in return, they would like to have gotten feedback on case development, such as: we have not prosecuted the perpetrator, but thanks for your help." The challenge was however if some of them had to testify in court based on the provided information, meaning all personal information was presented to the participants. Thus, P3 hoped that they could find a solution where innocent people was not dragged into something just by doing the right thing.

And this elucidated another point, where the burden of proof fell in the hand of the private business in criminal cases. As P6 said:

> This means that you, in private business, must spend a lot of time with the police to make them capable of understanding and to secure their interest in the case. (P6)

Some sectors had more resources to do this than others, P6 said, such as finance, meaning they were wrongfully getting more attention than other sectors. Further, P6 said that there was too much responsibility placed on private business to conduct the police work.

On the other hand, P2 said they do have other possibilities than the police, where private business can operate in any country with a legitim need to be present there, by talking the language and with a trustworthy backstory. That was a massive capacity, P2 said. However, they were afraid to be perceived as an intelligence service because they were not, and P2 said:

> We are providing self-protection and are forced to do so because of the lack of police resources in the world. (P2)

There were also differences in how daily affairs was conducted in the private business versus the police, where P3 said that there were solid connections with their business and police. But P3's business was mainly handling cyber and the organization of cyber, whereas the police handle reported cases, which were often a clear mismatch. P3 specified that this was the ordinary police, not the specialized unit NC3, in which they cooperate great with and share a lot of information.

In regards of the technical aspect of it, P5 said that the analysis courses P5 has taken in private business could very well correspond with the former work as an investigator in computer crime cases. In P5's mind there were a lot of parallels to operational criminal analysis and the job of monitoring incidents over time, being able to extract IOC's, find the human aspect of the incident and try to connect it to a threat actor, tools, and find similarities towards other cases. They also did endpoint digital forensics and triage, together with Kill Chain and Diamond Model for their technical analysis, and tried to find

the links between the endpoint, C2, infrastructure, capacity of victim. This process could fit in a cyber-crime investigation, or to create a framework for investigation and cybercrime, P5 commented.

4.1.4 Cyber-threat landscape

In general, the consensus amongst the participants was that the cyber threat landscape was complex and severe, especially for economical crime. Within ransomware there had been a professionalization lately, where organized crime is a very high manifest threat towards Norway, the state of Norway and for the companies that operates within our borders. However, Norway was not any different from the rest of the world. There also seemed to be a sense of naivety amongst companies, especially the smaller ones:

> Several of our companies we purchase claim they are too small to be victims of cyber-attacks. This is not correct according to our data: every company is a target. (P2)

The naivety did not only occur amongst companies, but also within the citizens, where P2 said that the people in Norway was used to a certain degree of security, and to trust the authority. This was regardless of how the authorities made good or bad decisions; citizens still trust them. With naivety there could be a limited feeling of wanting to protect yourself, and arguments of why one should be protected against cyber threats are few, P2 said.

P2 further said that even though we had a high threat picture, our consciousness remained low:

> We feel safe but are not conscious on how the threat actors are operating. (P2)

P5 emphasized to focus more on the active counterparts, what motives them and to examine the nature of the threat actors. These seemed to be economical motivated, hence they had to cause damage or disturb someone to get paid, P5 said. P5 further said that the cyber threat landscape is characterized by a decreased threshold to conduct cyber-attacks, because it has become easier:

> If an attacker is qualified on one part of the capacity, a capacity that is needed to conduct a certain cyber-attack, this capacity can be sold, meaning that the person doesn't have to complete the entire criminal action. These cyber-attacks makes it hard to understand, and hard to defend against. (P5)

However, P3 said that the focus was on organized crime and actual people being the threat actors, but often these people are bought to deliver services for national states, or national states interfere with organized crime campaigns, false flagging that the attacks come from organized crime, not a state actor. As P5 said, these nation state actors are not economically motivated, but more towards getting access to information, acquiring various power positions to influence a country on a broader term, such as infiltrate critical infrastructure to cause an effect.

P6 stated that a large part of his job was to keep track of the technical changes in the threat landscape, and how the threat actors were ever changing to keep up with new technology:

> As an example, a few years ago all malware was binary files, compiled .exe files or DLL files. Today there are only documents, and this will change again. When Windows turns off their scripting language in some of their products, the threat actors has to change. And with change, the threat actor will find new ways to operate. (P6)

To have both detection and capability to both analyse and examine was something P5 spend a lot of time on, to be able to see what lied in the horizon.

P2 also pointed out that some of the companies were not keeping up with technology and the threat landscape, such as when a company had bought firewalls and other basic remedies for protection, claiming this was sufficient. Or that the company trusted their employees. P2 said they had 14.000 employees in the company and were not able to trust every single one of them.

The report NCDBS (Næringslivets Sikkerhetsråd, 2020) was also discussed. P3 pointed out that most of the responders, approximately 80%, to this survey was business with 5-11 employees. The businesses with 150 employees or more had a low score in terms of participating in this survey, meaning there could be a skewed distribution of responders and type of responders. P3 worked with some of the bigger companies and said that incident and events are reported and tracked all the time, but not necessarily to the police, nor to the Norwegian Financial Supervisory Authority either, because they were not interested if there had been 150.000 cyber-attack attempts the last year. P3 further said there were a opposite pole, in regards of the responders in the survey, and what value they presented.

4.2 Cyber threat intelligence and processes

4.2.1 Incident response

To work intelligence-driven was important for P6's company, where intelligence was used for improvement and to ensure they had detection, was prepared for threat handling and IR, where hypothesis-making played an important role. P6 also mentioned the distinction between CTI and IR, but both genres resided in an infinite loop, and many of their analysts worked with both:

> As an analyst you are involved in all processes, from defining tasks, collection, perform analysis and dissemination. (P6)

P6 also described how they handled an event, by starting with identifying IOC's and the machines the threat actor had been on. Later, they would examine what the threat actor had done on the machine, such as to find out if data was prepared for exfiltration, how much data was residing in the Active Directory, etc. The results of these examinations were presented in a conclusion from the IR team, and said:

> When we are working with IR, this is hypothesis-based, and we use some intelligence methodology to prioritize the tasks in an event. If you have several hypotheses and try to identify what to prioritize from technical investigation steps, you want to prioritize those tasks deemed to be most significant. (P6)

P6 also placed data in ACH (Analysis of Competing Hypotheses) matrices, and by doing so they were able to check the data's integrity, credibility, and relevance, which resulted in either approval or denying certain hypotheses. This process was also based on experience from similar incidents and information from threat intel partners.

It was primarily a CTI analyst or IR analyst doing the excavation work, i.e., from an alarm on a third point, P7 stated. These analysts started immediately to populate data, where tools such as the Diamond Model was useful both for triage, overview of data, and to identify data-gaps. They also used MITRE ATT&CK framework together with their own textualization, to examine the different stages of an attack, where investigative methods also were used, and according to P6, a lot of technical work had to be done to be able to conclude something.

However, P6 mentioned how they found many of the same techniques in different stages of an attack, which meant that it was hard to conclude when the same techniques were found both in stage 3 and 7. Thus, they had created detection signatures in logs or

information collected from a system by doing digital forensics, followed by the making of a dashboard connected to a database where they were searching for techniques. One example of this was when they tried to find out if an attacker had moved from one system to another, or if the attacker had been able to run commands to another system. Hence, the had created signatures for techniques that would enable this activity, such as SSH (Secure Shell) or Remote Powershell. Digital forensic images were dumped in the database, and they used the dashboard for searching, such as searching for indications of lateral movement:

> In this manner, we can triage the data and say something about the probability that a threat actor has done something we have seen before, in a couple of hours. (P6)

By doing this, P6 and the team saved a lot of time as opposed examining images manually and utilized less experienced personnel to conduct this automated triage. This process could be called intelligence-driven, where the information need was that they had to enable more junior analysts to contribute towards larger incidents. More experienced staff had spent a lot of time identifying techniques in the dashboard, and when the dashboards were provided to enable more and less experienced personnel in the IR, was a good example of the intelligence wheel.

The process of IR was also a moment where private business often met the police, according to P5. In these types of events, the handlers of the incident, being private or police, was often limited by time and high pressure, meaning that these events were not the best prerequisite to establish a relationship, as opposed to establish it during peaceful times. However, some of the IR reports from private business were often sent to the police as attachments to the written complaints. P4 had been the receiver of some of these reports and said that they use SAT (Structured Analytic Tools), such as the Diamond Model, to support the reading and locate knowledge gaps in these IR reports.

4.2.2 How the intelligence is organized

On the strategic level, P5 said they had a longer perspective towards the decision-makers, such as CISO's (Chief Information Security Officer), board members, CEO (Chief Executive Officer), and those who did investments etc. The provided intel could help them make the right choices and prioritize the organizations resources in the best way, in the right order,

P7 mentioned how they produced strategic intelligence on an ad-hoc basis, and that this level was vague because it was hard to measure compared to operational intelligence. P6 said their strategic intelligence was compliance-driven, where the stakeholders had to be given a report due to demands from supervisory authority. P6 was not sure it these reports gave the effect they wanted.

P7 tried to keep it on the operational level in their daily work, such as handling indicators and detections. P6 stated the same, and that this was also where developed signatures for detection and worked with detection.

Most of P3's day-to-day intelligence work resided on technical and tactical level, meaning on the operational side. The tools used was many and varied, such as Virus Total, the use of flow data and Analyst Notebook.

On the tactical level, P6 typically created a MITREATT&CK map that said something about techniques used. P5 said that on the technical level, being day-week perspective up to monthly-quarterly perspective, was when they talked to system administrators, SOC-staff, or technical staff at the company. These are people that understood MITRE ATT&CK, which measures and lookups they had to do to find the mentioned TTPs.

P4 said that the intelligence production in the police had to be on all levels, both to write quick warnings on national level. However, these warnings were somewhat strategic, and if produced by a specialized unit, it still had to be used by a police business contact, and personnel working with preventive policing on all levels in Norwegian Police. Further, P4 stated that possible case selections based on intelligence were something that resided on the operational level, and P4 saw a great potential there, also down to police district level.

4.2.3 Analysis of intelligence

Most of the participants used the standard intelligence wheel with its four steps to a certain degree, but P3 had added two steps: program leadership prior to production, and the measuring of value from the provided intelligence:

> Because everything relates to value. If we don't deliver value, the whole process is meaningless. (P3)

Most participants also tried to work hypothesis-based, and ACH was mentioned by a few. P3 said that they worked with intelligence from two perspectives. Firstly, they had the technical perspective, where they used the Diamond Model and Kill Chain together, which didn't include that much intelligence theory. Secondly, they used what they learned from the SANS course on Threat Intelligence, which was more based on structured analysis techniques.

P6 mentioned how they worked with intelligence semi-structured from a perspective like the police's intelligence doctrine. They tried to identify information needs prior to collecting information, followed by analysis and dissemination. This was a continuously ongoing process, where the clients were updated and provided with new advice whenever changes occurred, P6 said. The client's need was also guiding the intelligence process, according to P7. And in cases where they had a good assignment dialogue the client could give the intelligence team their PIR's (priority intelligence requirements) and SIR's (specific intelligence needs), which controlled the needs for collection.

The use of intelligence platform for intelligence was something many of the participants used, such as MISP and others. These platforms were used and controlled by the intelligence personnel, and other could access it based on their needs for it. P3 said they used MISP for indicator-sharing, and that these indicators had been assessed by a human, meaning IP-addresses such as 8.8.8.8 did not appear, which would have blocked all traffic from Google. P5 said they used Argus platform to keep track of their data, as well as passive DNS databases based on their monitoring work. P7 also mentioned how they used MISP and Sentinel, and another response platform that had built-in MITRE ATT&CK techniques.

Some of the structured analysis techniques mentioned was the Diamond Model with Kill Chain, as mentioned above by P3, and P3 gave this short process description: They often got indicators, such as an IP-address, together with information about the incident. The objective was then to figure out where in the Kill Chain they were, such as the exfiltration stage or an actual breach. They would then conduct analysis and try to fill the Diamond Model. However, in many cases there were several actors in the system simultaneously, meaning they would have to use several Diamond Models and a timeline to find the threat actor's TTPs. The TTPs gave a description of the whole process. And by using the Kill Chain and Diamond Model they could pin-point their collection, which saved them time being few analysists set to serve many clients. As an example, if an endpoint had been breached, one result of using the Diamond Model was that they were able to see that two infrastructures had participated in this breach, as opposed to seemingly only one threat actor.

P7 also used Diamond Model to structure ongoing activity, such as if a client has experienced spear phishing. They could then use information from this to define an activity group in the Diamond Model and Kill Chain, and even though they didn't have much information, they could track it over a period. Thus, the Diamond Model could be used in the initial triage, making it an analytical support tool. They also used MITRE ATT&CK to map the different techniques used, such as vulnerabilities and malwares.

P5 used MITRE ATT&CK to be able to communicate with the clients, since the mapping of the techniques provided a mutual understanding of the techniques used. P4 called MITRE ATT&CK a tool for categorization, but that it was critical to use it as a foundation. According to P6, if you had information on how the threat actor operated, they made a MITRE ATT&CK map which described the techniques used. However, this also came with a high degree of uncertainty, because most reports that described the threat actors only showed how the indicators of compromise were, and sometimes the first lateral movements. But by using a heat-map, they were able to organize and grade the techniques, and they could map them towards detection.

P6 also said that there is a difference between techniques and procedures, meaning procedures is what they could detect, whilst the techniques only described the data access needed to detect procedures. Thus, they did not have detection on pure techniques, and P6 emphasized the importance of having the knowledge that a technique is not discovered because you don't have the data access.

P4 also mentioned MITRE ATT&CK, and saw this more as a tool for categorizing, and that there were different tools already used by the private business that the police also should use, such as in reports with technical indicators. P4 also saw the structured analytical techniques as important:

> Because in the end it is all about structuring the data, write it and contextualize it, in which others can comment on it and improve it. (P4)

4.2.4 Collection and dissemination

P1 and P5 said they both bought and collected their own intelligence, and P5 said they were a quite large costumer of Mandiant which provided them with CTI, as well as their own massive amount of data from their sensor networks and clients.

P4 explained how they collected information from the police registrars, such as surplus information from investigations or the intelligence register, or through open sources. P7 got a lot of information from open sources, both in terms of indicators, threat moderation, ongoing campaigns, typically found on Twitter and Reddit, together with free information from the major cyber security companies.

P2 used various scraping-tools on different extortion-sites, enabling them to find the extortionists, and it was a good incentive when the term "Norway" appeared. They also searched the darkweb for credentials to utilize prevention of ransomware attacks.

Threat hunting was mentioned by several, and through this practice they could gather information, i.e., from their sensor networks. If they had knowledge gaps, they would go hunt for information to fill them, thus enabling them to still decode, detect and extract relevant information from certain malicious software, or penetration-testing tools.

P3 benefitted by having the customer's data, which no other had. Other companies delivered what they could find on open sources etc., whilst they had the actual data knowledge regarding the incidents and activities from their members. That was "the real gold", as P3 described it. This data was normally collected through their API with an

interface connected to the clients' networks, where alarms and triggers were collected to conduct their own investigations and analysis.

P1 emphasized the importance of sharing information to get information back, and that their organization had a policy of sharing after securing their own business first. The sharing of information happened both in formal and informal channels. Some examples of internal sharing were through dedicated sharing platforms, security awareness programs and security letters. Sharing of information internally was under continuously scrutiny and development. The external sharing happened based on subjective selection of information.

P6 mentioned how the process of sharing could be described as an onion, where more high value competence was shared the farther you got into the onion. The outer part of the onion was described as the ones knowing what security was, whereas the inner were the ones attending conferences and had an informal tone to one another, but with a very high degree of trust. P6 also said that they had to share information, or else nobody would help them in return, and that everyone in the company was aware of the importance of cooperating and sharing information with others.

P3 used forums to share information with other sectors and partners, and said that the sharing and mutual understanding of threats were important:

> If a company protects itself from something today, the whole sector will protect itself tomorrow. (P3)

P3 also said that it was the biggest companies most at risk of being victims of cyber-attacks, but that it was in these companies' interest to secure the smaller as this would pressurize the whole sector. P3's team had close strategic and operational contact with all the client's incident operators, to discuss trends, emerging threats, and to do assessments.

On cross of sectors, P7, P3 and P5 said they shared information with other sectors and described NCSC at NSM as a strong cooperative partner and. NSM was described as the right place to contact to be provided early warnings of upcoming threats. P5 and the team first and foremost wanted to protect their customers, but at the same they were dependent on sharing understanding and experiences with others. They had to learn from events, and share indicators, and cooperate with other strategic partners.

MISP was also used for sharing information according to P7, and if their clients had MISP this made sharing of technical data easy. P3 used MISP for assessments of indicators, as well as a sharing platform. However, the best way to share in P3's opinion, was the informal one-to-one sharing, where they could take a phone call to someone known and discuss how to solve it. To build informal relations was something P3 valued highly, as opposed to reaching out to major organizations.

There were however some challenging aspects with information-sharing, and P6 said that to not be able to identify unique information, since the source of information was many, was one of them. P5 mentioned how the company could have restrictions in regards of what to share, due to the clients wishes. The classification could also be an issue, and P4 talked about how to be able to protect sources and methods, but still be able to share. P4 further stated that the challenge was the ability to communicate likelihood and confidents, but not hurt the work of fighting crime.

P3 said that they did cooperate with the police/NC3, central banks, secret services etc., and that one the biggest challenges for secret services now were how they wanted to share but did not know how. P3 further mentioned how there were a political decision describing how NSM should increase sharing, but P3 had yet not seen the effects of this. P5 said they aimed to cooperate more with police, and that they wanted to imply the police more integrated in their IR work.

P5 mentioned how they were in the process of creating a formal agreement with NC3, where they were supposed to meet quarterly to share experiences and discus common interests. The purpose was to be better prepared in times of emergency. P7 explained that because they were a managed service provider, thus not a member of SRM, this complicated the bilateral cooperation with the police and the army. In P7's day-to-day work, there were little or no cooperation with the police, since it was not their responsibility to report incidents onward to the police, as this was the client's responsibility. But P7 also said that if NC3 was more intelligence based as opposed to being a police organization, this would made sharing easier thus very relevant for their company. By doing so according to P7, their clients and themselves could use relevant intelligence for detection and block traffic for protection.

P7 understood that doing detection was out of scope for the police but known indicators that could strike other targets in Norway would have been relevant to share. P1 said that to have had a national hub for intelligence sharing would be useful, where small business could send their information needs, and pass this along for other to answer out.

Quick dissemination was mentioned by P2, where high-quality intelligence could be disseminated quickly, without too much bureaucracy and other elements hampering the process:

> The information must be disseminated quickly. Based on good intelligence, police officers can go hunting, applying the subject by arresting people based on high-value intelligence, proper information, and solid analysis. And to conduct simple targeting-practices as police officers. (P2)

P2's company had applied dissemination as an own subject, where they used CTI in together with the life cycle, meaning that the process of intelligence had to end up in something. Thus, they made weekly news reports based on their intelligence and assessments. P2 also emphasized in the importance of dissemination intelligence timely and in the client's language. They used Jira to disseminate the technical information and for communication within the team.

P4 thought that the police's dissemination of intelligence had to be done quickly to be utilized for preventive measures, at the stakeholders, such as citizens and businesses. However, businesses often got their intelligence from private security companies, and questioned:

> What data do the police have to contribute with, that the other ones don't have? Maybe the job must be cultivated. Instead of getting lots of new people who are good at open sources and gathering, the police could focus on your own data base, and what can be shared from it, and to make others more skilled. (P4)

4.2.5 Purpose and decision making

P1 explained how their company spent much money and resources on intelligence to become more proactive, where the support for decision-making was important and questioned:

> What can you do, and how can you use this to prepare for future events? (P1)

According to P1, the essential work was to make analysis of trends and developments, and examine how they worked towards their goals, and which measures they had to have to be better prepared. P3 said this in regards of intelligence and its purpose:

> I believe that intelligence has a lot to deliver, and that it will also be incorporated more into the entire organizational stack, not just down in cyber, but through the cyber risk department - and all the way up to management. Because ultimately, it is risk that will make decisions, and point out; these are the risks, these are the measures we have at these prices and take

> this amount of time, and what is the risk appetite based on that threat and the vulnerability we have. The threat is what we deliver, and that is what they must protect themselves against. (P3)

P2 said that to understand the operational pattern was important for preparation to understand the modus operandi. If they understood this, they could handle it, and this was why they highly prioritized intelligence.

The purpose of using cyber intelligence was both to be used for case selection, especially if NC3 were only to conduct a few yearly investigations, and for preventive policing, P4 said.

For P6, the main purpose of intelligence was to use it for preparedness and detection and said that intelligence controlled the technical investments and competence needs, where they strived to turnover data to knowledge and used that knowledge to make the right choices. They further conducted a semi-structured assessment for verification of data. For P7, it was purposeful to use intelligence to provide info on the threat landscape, which included info on campaigns, used vulnerabilities, malware, and new attack vectors.

As for the clients and their decisions, P3 said that they made sure the data they got from their clients was washed, organized, and analysed, and made intelligence which were returned to support decision-making.

P4 said that the intelligence product from the police had to be based on a needs-analysis with the decision-maker:

> Which decisions will be taken and based on this you can say you need this product and based on that you will need this amount of personnel, and they will work this way, with these functions on the assignment. (P4)

The main objective with cyber intelligence is to provide early warnings, according to P4, but this was not always easy because it was difficult to be able to tell the Police Director, "this could we very big", or "this comes next week". There was also a paradox in providing early warnings from the police, and not necessarily to the leaders, but to the private enterprises. Because private enterprises also got info from other private agencies, which did have their own interest in it, plus more resources and data than the police. P4 said:

> So, you have this question, and possibility: what do we have in the police which the others don't have that we can contribute with? (P4)

Knowing your stakeholders was also a subject in which many of the respondents had opinions on, where there was a mutual consensus that the goal was to provide protection for their clients. And to do so, they had to know their clients and their needs. P3 said that they conducted a stakeholder-analysis and asked the questions:

> Who are they, what do they care about, what resources do we have, which analysis do have to do, which products/services can this turn into, what are the criteria of success, how do we measure it what is the maturity scale we shall reside on, and how do we develop it in the coming years? (P3)

P5 explained the use of standard intelligence wheel to know the stakeholders needs, where they began with plan and preparation, followed by asking the clients about their needs. P7 helped their stakeholders to form a threat landscape based on their values, possible threat actors, and the vulnerability. P7's company provided what they called a "vulnerability-assessment-as-a-service" to their clients, in which the clients could be provided with intelligence both on threats, threat actors, and technical details such as i.e., a list of 15 vulnerabilities known to have been used by several ransomware-gangs. They could then provide a tool which scanned their clients' servers, thus helped the clients decide which

security measures to conduct. This was an easy example of how intelligence is actionable, P7 said, and they could provide this service to their clients uninvited because they had a solid assignment description with their clients. According to P7, the provided security also benefited their own business, because possible vulnerabilities at their client would look badly for them as provider of security.

P7 further said that they strived to make the stakeholders happy, and that the provided intelligence was experienced as high value for the clients. This all resolved back to the data that P7, and the team had, where the intelligence product should be supported by empirical data. This meant that they worked from an ethical compass as opposed to produce politicized intelligence to please the stakeholders. However, this was not same as tailoring the intelligence based on the client's values or threat image, and they were not trying to monetize from the intelligence, since the clients were already a paying costumer. Hence, P7 just had to deliver a proper intelligence product.

The effect the intelligence had could be seen with the customers when they made protective decisions, bought technology, changed the way they worked, or conducted their own threat hunting procedures based on their reports, P3 said. P3's team measured this effect both quantitatively and qualitatively, where the provided intelligence was both enforceable and traceable, thus they could make empirical data from measuring the provided intelligence. P5 said that the effect they often saw, was how their intelligence helped the clients from prioritizing how to use money, and to improve the holistic impression of security within the business.

4.2.6 Intelligence-led work

Every one of the participants agreed upon the importance of learning from knowledge, information and prevent incidents from happening. P4 said that the police were inherently reactional based, and measured on investigation, arrears etc., as opposed to the preventive work, which was hard to do. P4 mentioned that §2 of the Police Act did however make a point towards preventive work and the importance to use it for cybercrime, but it became a democratic challenge if Norway as a nation wanted to utilize it:

> We are struggling with the fact that we may not only have to professionalize the subject of intelligence and learn the technical aspects of cyber, but we also have to turn the police into becoming more of an intelligence organization than it is today. (P4)

P5 mentioned the importance to formulize the experiences turned to knowledge, which may not provide results tomorrow, but further down the line. Further, P6 said that to have knowledge-based approach towards both detection and IR could help a threat not becoming a crisis. The more knowledge they could use, the more prepared they were, thus less consequence for the client.

To work intelligence-based was defining for P7's company, where they wanted to do measure, secure, and give recommendations based on their client's threat image. P7 further said that to manage the expectations of the customer was important, where the intelligence analyst could collect different information from a certain event, and then make a narrative which was properly sourced and say: "what have we really seen now?" and make proper assessments on the information. This was something the clients really appreciated and made the intelligence actionable where the client's expectations were managed and measures was based on well-founded information, P7 said.

And what was concerned as actionable intelligence was something the participants had different views on, where P1 said that if they received information regarding something that may hit them or others, this had to be shared. And to be provided information timely enough to act on it, was something P2 said was actionable intelligence, and preferably

before something occurred. P3 said they got feedback from the clients and asked them which measures they conducted based on the intelligence. By doing so, they could better understand the intelligence needs, in which they could adapt and produce better intelligence for them. P3 also mentioned instances where they had delivered intelligence which led to a legal indictment.

P6 gave me an example where their intelligence stopped a ransomware-attack based on actionable intelligence, where warnings enabled the client to mitigate and minimize the consequences. IOCs could also be actionable intelligence, P6 said, but their effects could be increased if the IOCs could be turned to signatures, such as Yara-rules or detection-rules, enabling them to discover what is not known thus move further up in the Pyramid of Pain stack. See Figure 11.

> Things that make the threat actor have to change their behavior are the best, because it requires a lot from the other party to do something more. (P6)

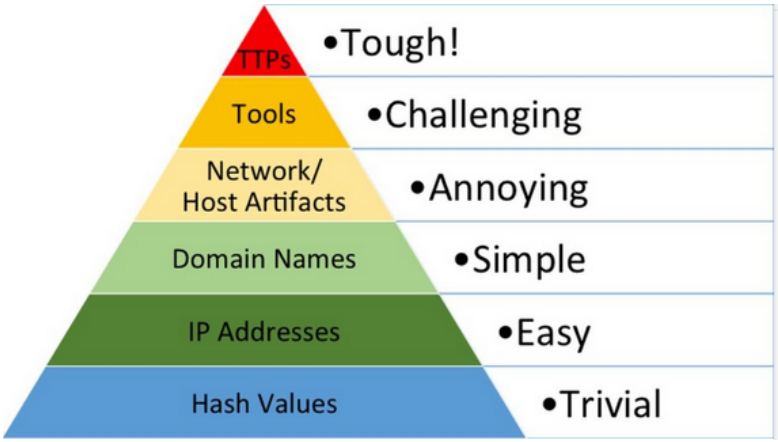

Figure 11: Pyramid of Pain (Drake, 2022)

P6 said that the highest intelligence value was when the threat actor changed their modus operandi, and the lowest value was IP-addresses and domains, meaning short validity value equalled little value, because it was easy for the threat actor to change. To change the malware, methods and set of codes demanded more:

> Newly compiled versions of the same malware, given that we have detection for the malware, helps me. But if a new malware or a new way of doing things appears, this demands something completely different for us to make a detection on and demands even more for the threat actor to change. (P6)

P7 mentioned 3 elements regarded as actionable. Firstly, IOCs could be actionable intelligence, and said that for something to be actionable, it had to be used for something, where indicators, even though they are short-lived, could be actionable. Secondly, platforms such as MISP and Sentinel were actionable. MISP was used for automatization of new indicators, which in turn was disseminated through Sentinel, and provided the information to clients in real-time. This made it very actionable and enabled them to check if new indicators had given any effects to their clients or not and created hits or alarmed them for as long as they assessed it to be relevant. It was the same for detection-rules, and to implement this for their clients. This was actionable because they were more secure after implementing this detection than before doing it. Thirdly, intelligence reports that assessed a threat, either about an actor, a campaign, or malware which were placed in context and said something about: "is this something that we should care about/not care about", was actionable information. Lastly, P7 mentioned how information from the police

could be actionable for them, i.e., if the police shared two IP-addresses, then P7' s company could place these IP-addresses in block to not hit their clients. Or if P7' s company got an alarm on these two IP-addresses, such as if they were observed on an endpoint, they would get an alarm and they could conduct an IR and act on it.

A creation of a database for the police would support the first steps of a course of action matrix from Lockheed Martin, P5 said, where the two first D' s were to discover and detect. These were passive modes of action and could be done without any interaction from a counterpart. By using these two steps, enabled the possibility to discover: has this happened before? It could also detect: How do we stop this from happening again? P5 said that just by using the first step you could get an immediate contextualization, and a joint national database would support these two steps, and that it could possibly enable everyone to act when a given thing occurred:

> Because if you have that data, you can look back at past events and get context when new things appear, and you can try to build different ways to prevent them in the future by utilizing rules, Sigma/Yara technical prevention, or being able to construct more humanly comprehensible models. Discover and detect are something you can build a long-term strategy on. (P5)

5 Discussion

5.1 Social-technical systems analysis

The objective of the socio-technical systems analysis with its proposed candidates, and the proposed measures from SBC-modelling, is to outline answers to the research question, and to achieve the overarching preventive objective of the police. In the thematic analysis of the interviews, two main themes were found, which were elaborated above. Each theme has been analysed to find socio-technical causes, or opportunities, shown as candidates in a modified Ishikawa (Ishikawa, 1985) diagram below. The Ishikawa diagram's main purpose is to illustrate a cause-effect relationship, where one side of the diagram illustrates the different causes, and the effect-side which illustrates the problem, or final effect (Schumann, 2021). For this purpose, the different levels of the socio-technical stack are presented as causes, or opportunities. This procedure is chosen because the intention of the analysis is to both identify causes of why the police are not achieving their objectives, and which opportunities for improvement were found that could affect identification of the proposed measures. These opportunities and causes are meant to provide grounds for measures for the police to better enable them to process and handle cybercrime, which is presented through SBC-modelling.

The candidates proposed through the socio-technical analysis, should cover all levels in the stack (culture, structure, methods, and machines), and the selection of them is grounded on perceived importance and relevance for the research problem. The proposed measures from SBC-modelling are based on the candidates from the social-technical analysis and are consequently implemented to cover the different levels of the socio-technical stack. This is shown in Table 4.

The socio-technical systems approach is elaborated in 3.2.2.

The abbreviation LE for law enforcement is used in Figure 12, Figure 13, Table 4, and Table 5.

5.1.1 Police and cybercrime socio-technical analysis

As seen in Figure 12, a large part of the candidates is located at the socio-level. One of the reasons is that the approach for this research and the interviews were somewhat phenomenological, and that this theme did not cover the technical aspects to a large degree.

The social-culture and structure candidates revolve around the relationship between private business and the police, perceptions of individual perspectives and structures within the police, such as:

- LE personnel are attractive for private business
- Private business lacks faith in LE
- Disadvantageous to report to the police from private businesses
- Burden of proof relies with private business

All candidates from the social culture/structure could contribute to the selection of measures, and if one uses the candidate "Lack of competence of LE personnel" as an example, the generic measure could be to educate more police personnel. An even though the measure origins from an individual perception, the measure itself could apply to different sub-categories of the socio-technical stack.

Technical-methods are candidates of how methods are used on technical artifacts. A prerequisite for the technical-method candidates is an existing technical platform in which

the possible measures can be utilized upon. The only technical-machines candidate found was the lack of a national database for intelligence in Norwegian police. If this candidate were to be operationalized as a measure, it would probably depend on a unique technical artifact.

There are however some of these causes/opportunities that are not feasible to implement generically, such as the social-structural candidate "lack of consequences for the criminals". The penal systems cannot easily be adapted in terms of sentences, but the implemented measures may cause an effect regarding arrests as results from a cybercrime investigation, which again could have public preventive effects.

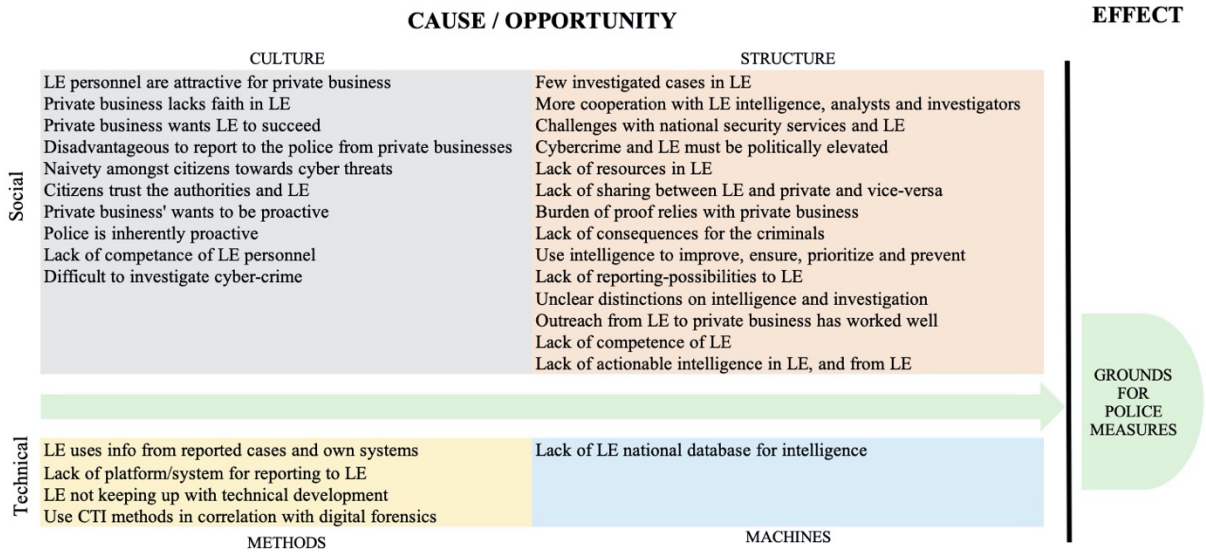

Figure 12: Police and cybercrime socio-technical analysis

5.1.2 Cyber threat intelligence and processes

As opposed to the social-technical analysis of police and cybercrime, there are more candidates mapped to technical-methods, as illustrated in Figure 13. These are methods that describes technical frameworks, methods, analytical/intelligence tools mentioned by the interviewees, which needs technical artifacts to be utilized. Again, a prerequisite is that the technical artifacts are present and inherent within the police. There are two candidates found on technical-machines, and one of them is an API in which intelligence-personnel can collect information from. If this were to be transferable for the police, it resembles the candidate proposed in Figure 12; a national database for intelligence, where the measure is a decentralized intelligence database for the police, governed by NC3. The other technical-machine candidate is the opportunity of implementing a central storage network for cybercrime, where the effects of implementation could be to enable cross-analysis of seizures, and sufficient data to conduct threat-hunting on.

The social-culture and structure candidates provides insights of how CTI, intelligence-led work and decision-making are perceived and conducted by the participants. Some of the social-structure candidates, such as "intelligence for preparedness and detection", cannot be directly transferred to policing since detection of malicious activity in the network is not a part of the police's work. However, the methods and routines used for detection can be utilized by the police. A good example of this is to use signatures and rules for automation of digital forensics triage, as mentioned by P6 in 4.2.1.

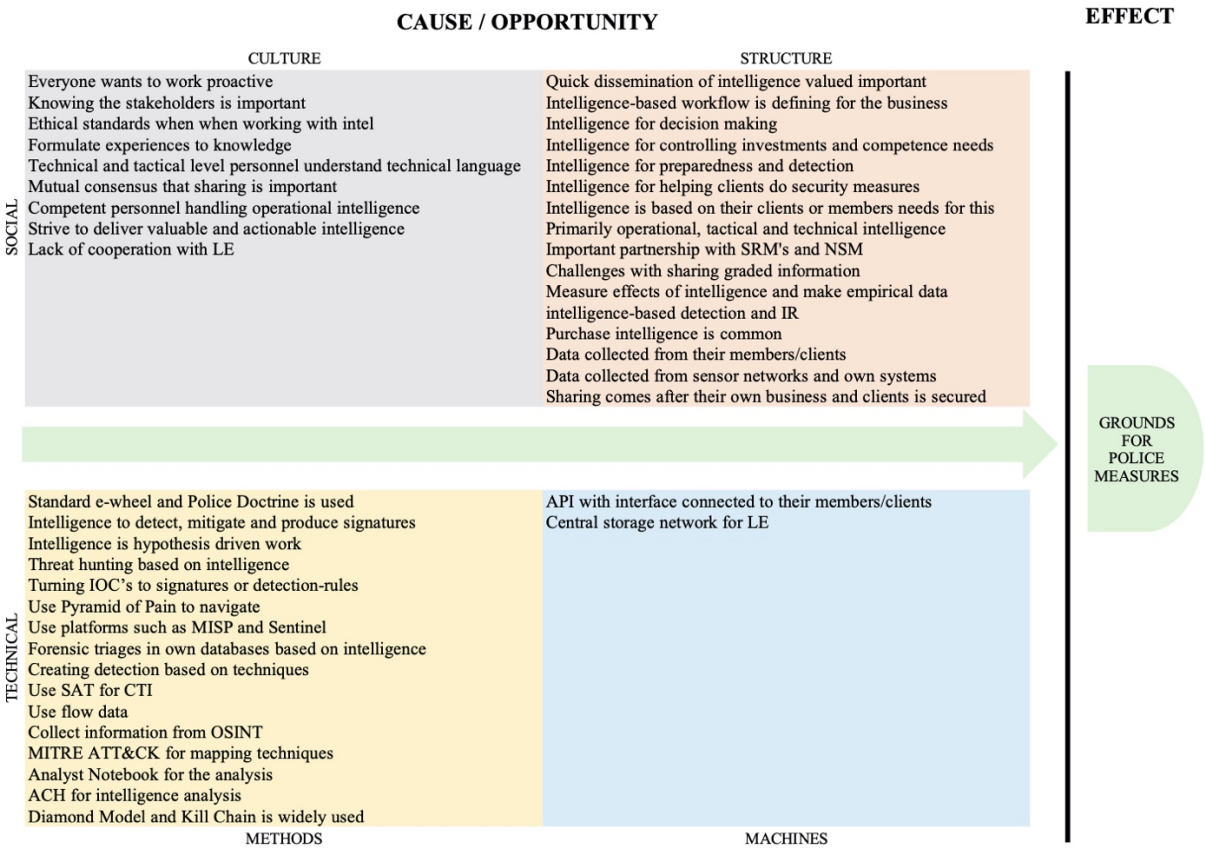

Figure 13: Cyber threat intelligence and processes socio-technical analysis

5.2 SBC Modeling

The proposed measures in Table 4 are based on the categories from the socio-technical analysis, as seen in Figure 12 and Figure 13. The proposed measures from the SBC-modelling are in no means exhaustive, as they are based on the socio-technical analysis and assessed by the research whether they are feasible for the Norwegian police. Thus, they should be treated as suggestions.

Table 4 also illustrates how measures are mapped to causes/opportunities in the socio-technical sub-categories, where measures could have effects on several of them. One example is the effects of implementing the measure of "improvement of sharing actionable intelligence within LE". This measure could have effects in terms of how police investigators and intelligence analysts are conducting their day-to-day work, as well as how the organization are structured to enable this improved sharing. Eventually, the sharing must be done somewhere, and if done digitized, this could affect the methods in which sharing is conducted on.

The different levels in the SBC-model are used for proposing measures, and the levels are described below. The descriptions are influenced by the research from Kianpour (Kianpour, 2021), but adapted for this research's purposes.

5.2.1 Social

Ethical/cultural: social behaviour, norms, capabilities, and knowledge found amongst police personnel and organizations. Examples are to implement increased situational awareness (SA) amongst personnel and organization. Effects of this is more knowledge and insight, which provides better grounds for ILP. Some of these measures could be implemented and anchored structural, such as the measures of promoting the police's needs and work, by having increased presence in cyber security forums, liaison-positions towards other sectors, etc.

Political/legal/contractual: systems of rules to regulate behaviour, insurance that legal considerations are cared for, and compliance with regulations. For the police these are measures that relates to what might leverage political and decisions, or that could better organize sharing of intelligence within the legal framework. An example of this is to "establish quantification of produced intelligence for statistical purposes", where the results indirectly could give grounds for the police to be provided increased capacity and budget.

And some of the measures are perhaps not feasible in the short run, or at all, such as "improvement of wages". But it still a measure that could give positive effects in keeping the police staff and make policework more attractive.

Administrative/managerial: management is the administration of the organization and includes the activities of strategy-planning and coordination of efforts of the internal and external actors, to accomplish the objectivities through the application of available resources. For the police these are measures from i.e., police staff and leaders, or on the more strategic level of decision-making, such as the Police Directory. Examples are "improve the outreach to private business", where the measure can be administratively decided to be effectuated, based on available budget, and needs for this capacity.

Operational/procedural: operations and procedures describe the tasks that needs to be executed to harvest value from assets owned by the organization. For the police, this is typically the actual processes of doing investigation or other analysis. As an example, the measure "establish threat-hunting as a part of working intelligence led", means that the analyst or investigator adapts, or implement this way of identifying new threats, as opposed to standard investigative methods or means to collect information for cyber intelligence. A prerequisite is that intelligence-led policing is already implemented from a strategic decision-making perspective.

5.2.2 Technical

Application, operating system, and hardware: This is the sum of techniques, tools, and processes, such as physical devices, frameworks, methods, and applications to accomplish the organizational objectives. For this research, to map measures on operating systems and hardware is out of scope, as seen on Table 4. Some of the application-measures are not application, but techniques and methods, and knowledge of them. One example is to "introduce the Diamond Model to find patterns in crime-cases and data", where different strategic tools and techniques can be applied, such as Microsoft Excel or Analyst Notebook. The common denominator for the measures presented here is that they are all mapped towards methods in the socio-technical levels, meaning that each implemented measure could provide methodological effects. I.e., the effect of implementing ACH for hypothesis-testing is to make more qualified decisions of where to collect additional information, or to whom the intelligence should be disseminated to.

		MEASURES	CAUSES/ OPPORTUNITIES: Culture	Structure	Methods	Machines
Technical	Hardware					
	Operating System					
	Application	Introduce an intelligence platform for IOCs and TTPs governed by NC3		x	x	x
		Introduce a central storage network to be used for analysis		x	x	x
		Establish automation of digital forensic analysis by using knowledge-databases for triages		x	x	x
		Introduce ACH for hypothesis making		x	x	
		Introduce Pyramide of pain for cyber threat intelligence		x	x	
		Introduce the Diamond Model to find patterns in crime-cases and data		x	x	
		Establish the use of Cyber Kill Chain to structure data in single events		x	x	
		Introduce MITRE ATT&CK to map techniques and find possible TTPs		x	x	
Social	Operational-procedural	Introduce threat-hunting	x	x	x	
		Establish access to the intelligence platform to all police districts	x	x	x	x
		Improve the collection and acquisition of information	x		x	
		Establish more focus on intelligence-led policing and dissemination of information	x	x	x	
		Improve cooperation with criminal analysts, cybercrime investigators and digital forensic personnel	x	x	x	
		Establish a more integrated workflow between police districts and NC3	x	x	x	
		Establish a more analyst-centered approach when processing cybercrime data	x		x	
		Establish cyber threat intelligence with cybercrime LE investigators and analysts	x	x	x	x
		Ensure that intelligence personnel work closely with the investigators	x	x		
	Administrative-Managerial	Ensure that measures have effect		x	x	
		Improve knowledge of cybercrime with leaders and decision-makers		x		
		Establish procedures for proper registration of cybercrime cases		x	x	
		Establish procedures for police districts to collect IOCs		x	x	
		Improve methods for gaining experience and evaluation	x	x	x	
		Establish SOCs in every police district to locally govern the LE intelligence platform		x	x	
		Improve the outreach with the private industry		x		
		Improve sharing of actionable intelligence within LE	x	x	x	
		Improve sharing of actionable intelligence outside LE	x	x	x	
		Coordinate purchasing and administration of software and tools for intelligence-led policing		x		
		Establish user-testing and training for new tools and frameworks		x	x	
		Ensure that the LE investigators have sufficient knowledge of structured analytical thinking	x	x		
		Improve technical training for LE personnel	x	x		
		Establish a closer relationship with cyber intelligence communities, private and national		x		
	Political-Legal-Contractual	Establish intelligence-led policing for cybercrime	x	x	x	x
		Establish quantification of produced intelligence for statistical purposes		x	x	
		Ensure that data used for intelligence is in accordance with current laws		x		
		More clarification of routines and responsibility of cybercrime intelligence and investigation		x		
		Improve juridical possibilities i.e., using coercive methods for intelligence purposes		x		
		Improvement of wages with LE enforcement staff		x		
		Establish a tighter relationship with LE officer and prosecuting authority	x	x		
		Establish better procedures of registering modus operandi and IOCs in criminal records		x	x	
		Improve how to share and use graded information		x	x	
		Strengthen the national coordination of handling cyber-crime		x	x	
		Enrich classified information with non-classified data to enable dissemination	x	x		
	Ethical-Cultural	Establish SA on cybercrime and threat landscape	x	x		
		Establish better understanding of the benefits of intelligence-led policing	x			
		Change the culture to understand the importance of having a continuously incoming flow of data	x			
		Establish a better understanding of the importance of indicators and the contextualization of them	x			
		Establish a better understanding of the importance of using structured analytical techniques for cybercrime	x			
		Promote the work being done by LE	x	x		
		Promote why LE need help to fight cybercrime	x	x		
		Establish security culture and why LE is important in this culture	x	x		
		Improve the citizens trust in LE	x			
		Promote to protect the citizens and core functions in Norway	x			

Table 4: SBC modelling with measures mapped to socio-technical categories

5.2.3 SBC summary

Table 5 is a summary of the measures and mapping to causes/opportunities from the socio-technical analysis. This is influenced by what was presented in Schumann's master's thesis (Schumann, 2021). He states in his thesis that the presented causes and measures and its placements in the SBC-model, can be a matter of discussion. This also applies for this SBC-modelling, but even though some may be placed incorrectly, the presented measures still provide some useful insight.

For this research, 52 measures were proposed on the different levels within the socio-technical groups, where 44 relates to the social group, and 8 is on the technical group. This means there is an abundance of social measures, as opposed to measures on the hardware and software, but this was calculated since this research was delimited by focusing on these aspects. There are however some interesting methods and frameworks mentioned in technical-application category, which can be applied as methods without buying new expensive equipment, thus change the structure of how the analysis of information is conducted.

As for social measures, these are respectively 9 measures on operational-procedural level, 14 on administrative-managerial level, 11 political-legal-contractual level, and 10 on ethical-cultural. They apply to many different sub-categories in the social-technical stack, and there are 3 measures that cover all four causes/opportunities, which indicates their importance and are elaborated below:

Firstly, it is to provide access to an intelligence database for all police districts in Norway. This may cause an effect on needed equipment to operate it, it could change the way the cybercrime information is processed locally, thus effects on routines and structures, which could eventually affect how the individual investigators, or intelligence analysts, are perceiving cybercrime intelligence:

Secondly, the measure of implementing CTI also covers all four causes/opportunities. If it were to be implemented, this could imply an upgrade on police national networks and (intelligence)databases, it would change the way information from an intrusion in relation to cybercrime is processed and handled, thus change in methods. Further, this way of working must be rooted managerial, meaning end-state must be agreed upon, where i.e., to produce measurable actionable intelligence defines success or not. This process would also affect how the individuals working with cybercrime conducts their work, where the aim is to contextualize and find deeper meaning in the available information. Examples of this is to establish threat hunting by using CTI as a formal procedure.

Thirdly, to establish ILP for handling and processing cybercrime also applies for all four categories. This is the overarching objective in many ways, and to operationalize this measure may provide effects on all four categories. This measure is mapped under the political-legal-contractual, since an implementation must be anchored and decided within the correct legal frameworks, and strategically decided. If ILP were more integrated in cybercrime policing in Norway, this could affect the machines, and imply more automated intelligence or digital forensic processing, and it could influence technical methods used. Further, it would have an effect in the structures within the various police sections or agencies, and the individuals may have to re-arrange their normal ways of handling and processing cybercrime-related data. ILP goes together with the measure of implementing CTI.

		Measures	Applies to number of causes / opportunities	Total causes / opportunities applied	Total measures
Technical	Hardware		0	0	0
	Operating System		0	0	0
			0	0	0
	Application	Introduce an intelligence platform for IOCs and TTPs governed by NC3	3	19	8
		Introduce a central storage network to be used for analysis	3		
		Establish automation of digital forensic analysis by using knowledge-databases for triages	3		
		Introduce ACH for hypothesis making	2		
		Introduce Pyramide of pain for cyber threat intelligence	2		
		Introduce the Diamond Model to find patterns in crime-cases and data	2		
		Establish the use of Cyber Kill Chain to structure data in single events	2		
		Introduce MITRE ATT&CK to map techniques and find possible TTPs	2		
Social	Operational- procedural	Introduce threat-hunting	3	26	9
		Establish access to the intelligence platform to all police districts	4		
		Improve the collection and acquisition of information	2		
		Establish more focus on intelligence-led policing and dissemination of information	3		
		Improve cooperation with criminal analysts, cybercrime investigators and digital forensic personnel	3		
		Establish a more integrated workflow between police districts and NC3	3		
		Establish a more analyst-centered approach when processing cybercrime data	2		
		Establish operational CTI with cybercrime investigators and intel-personnel	4		
		Ensure that intelligence personnel work closely with the investigators	2		
	Administrative-Managerial	Ensure that measures have effect	2	27	14
		Improve knowledge of cybercrime with leaders and decision-makers	1		
		Establish procedures for proper registration of cybercrime cases	2		
		Establish procedures for police districts to collect IOCs	2		
		Improve methods for gaining experience and evaluation	3		
		Establish SOCs in every police district to locally govern the LE intelligence platform	2		
		Improve the outreach with the private industry	1		
		Improve sharing of actionable intelligence within LE	3		
		Improve sharing of actionable intelligence outside LE	3		
		Coordinate purchasing and administration of software and tools for intelligence-led policing	1		
		Establish user-testing and training for new tools and frameworks	2		
		Ensure that the LE investigators have sufficient knowledge of structured analytical thinking	2		
		Improve technical training for LE personnel	2		
		Establish a closer relationship with cyber intelligence communities, private and national	1		
	Political-Legal-Contractual	Establish intelligence-led policing for cybercrime	4	20	11
		Establish quantification of produced intelligence for statistical purposes	2		
		Ensure that data used for intelligence is in accordance with current laws	1		
		More clarification of routines and responsibility of cybercrime intelligence and investigation	1		
		Improve juridical possibilities i.e., using coercive methods for intelligence purposes	1		
		Improvement of wages with LE enforcement staff	1		
		Establish a tighter relationship with LE officer and prosecuting authority	2		
		Establish better procedures of registering modus operandi and IOCs in criminal records	2		
		Improve how to share and use graded information	2		
		Strengthen the national coordination of handling cyber-crime	2		
		Enrich classified information with non-classified data to enable dissemination	2		
	Ethical-Cultural	Establish SA on cybercrime and threat landscape	2	14	10
		Establish better understanding of the benefits of intelligence-led policing	1		
		Change the culture to understand the importance of having a continuously incoming flow of data	1		
		Establish a better understanding of the importance of indicators and the contextualization of them	1		
		Establish a better understanding of the importance of using structured analytical techniques for cybercrime	1		
		Promote the work being done by LE	2		
		Promote why LE need help to fight cybercrime	2		
		Establish security culture and why LE is important in this culture	2		
		Improve the citizens trust in LE	1		
		Promote to protect the citizens and core functions in Norway	1		

Table 5: SBC-modelling with measures and socio-technical numbering

5.2.4 How can socio-technical system be balanced?

If the implemented socio-technical measures are in imbalance, they are inherently inefficient and ineffective (Kowalski, 1994). In Table 4 and Table 5, the social-technical measures are listed and mapped to their socio-technical sub-category. But each of these measures must be balanced to the rest of the socio-technical model, as shown in Table 6. If not, the implementation of the measures would be contradictory and quite pointless in a socio-technical model, since the systems requires balance to work properly (Borhaug, 2019)

Each measure relies on each other for the system to be balanced. If one investigator decides to single-handedly be creative with new methods and techniques, then this could negatively affect the culture and contradict the aims of the investigation. However, there should be room for creativity within the police, but the process of doing so has to in balance with the rest of the organization. Table 6 is inspired by the table presented in Borhaug's research (Borhaug, 2019).

Methods→	←Culture
Must be usable and functionable	Must have understanding and competence
Culture→	←Structure
Must be organized and cooperative	Must be adaptable and understandable
Structure→	←Machines
Must have resources and capacity	Must have access
Machines→	←Methods
Must be usable and functionable	Must be implementable
Methods→	←Structure
Must be tested and learned	Must provide support and delimitations
Culture→	←Machines
Must have capability and skills	Must be manageable

Table 6: Balanced socio-technical system

6 Conclusion

The process of conducting a socio-technical analysis of the interviews was to seek to proposal answers to my research question:

- How can intelligence-led policing support the objectives to process and prevent cybercrime efficiently?

The findings in this thesis aim to provide insight in how a more intelligence-led approach can be applied by the police. The essence in ILP is to reduce crime, where proactive mechanisms should reduce the cybercrime rate. The process is data-driven with emphasizes on sharing, collaboration, analysis and intelligence (Ratcliffe, 2016) There haven't been many empirical studies on how ILP has been conducted under the cybercrime-umbrella, which is why the researcher has reached out to the private industry to study how they are practicing this.

The essence of the interviews is that the intelligence-based ways of operating their business is valued highly and seem necessary to provide security, to help construct a threat environment picture, and remain profitable. There also seem to be a consensus in the security industry that all parties within the security industry, as well as governmental agencies, will benefit from reducing the risk, share vital information to stay proactive and collectively increase resilience.

As mentioned, all measures should be assessed as proposals, and some of the measures are perhaps also in correlation to one another. And the purpose of this research is not that by implementing all measures, the police's quality, efficiency, capacity, and competence will immediately increase. But the measures could be worth examining further, and they can be grounds for further research, as showed in chapter 7.

How can intelligence-led policing support the objectives to process and prevent cybercrime efficiently?

The Norwegian Police Act §2 states clearly that prevention and investigation is one of the police's core functions. Some effects from doing these jobs thoroughly are to protect and secure the citizens, business, national interests, and critical infrastructure. Together with prosecution, the build-up of a more resilient and less insecure society are also important effects. The measures and procedures from the police should participate in making it difficult and risky for the threat-actor to reach their goals and make them re-think their offensive operation and tactical decisions. The end-state is not to eliminate the risk completely, but to reduce the risk to the point where the police's efforts are deemed sufficient. Ultimately, working intelligence based is about reducing uncertainty, where knowledge, sharing information and analytical approaches are the keywords.

However, what is deemed sufficient or not is impossible to answer, as there are many extraneous variables to consider. Traditionally this has been issued by quantifying efforts, such as numbers of cars stopped, number of successfully investigated cases etc. But quantification and measuring preventive measures, or the ILP, is far more difficult. Because ultimately, to be able to measure the effects of intelligence and ILP, is of great importance. A lack of effect should make the analysts and investigators re-evaluate the process and discuss with the decision makers and learn from the process.

The outreach, called "Næringslivskontakt"[4] (Politiet, 2022), from the police to private business was also something that was positively mentioned in the interviews. To further increase police presence in private sector is often underestimated, where the informal contact and networking can play an important role when it comes to understanding threat environment, for the private business to understand police's role, and gain trust with private business. This may also lead to increased flow of information from private business to the police if they have a person functioning as a pipeline to the police. To have this increased presence may also help the reporting numbers, where trained police personnel can encourage and guide them in the initial phase of the event, and the private business knows they have one person to talk to, as opposed to calling the police central for instructions or help.

The use of a common intelligence platform for the police may also help quantify, measure, and share the information. These platforms, such as MISP or STYX, typically handle IOCs, allows mapping of TTPs, and enables the possibility to share information swiftly. Some even uses machine-learning models to understand the context and relationship between the data and the assessed risk (*STYX Intel*, 2022). Ideally, a platform should be governed by a special police unit, such as NC3, but every police district should be able to use it. As such, local police can receive information, either from reported cases or through other incoming information. The police officer receiving this information does not have to be very technical skilled but should be able to outsource elements in the information that may be used for intelligence purposes, such as IOCs. This decentralized process allows for a much better flow of potential actionable information, as the process of finding links and connections to the implemented information happens automatically. This process also allows for actionable information to be shared rapidly on an operational, or technical level, thus fulfilling some elements of ILP.

But to use a platform in the police and make use of its features, there must be incoming information, and private businesses are hesitant to report crimes. A simplified way for people and businesses to report cases could reduce this hesitancy. As examples, it could be useful to be able to report crime cases online, with embedded areas where the reporting party could insert IOCs, possible TTPs, MITRE ATT&CK techniques etc., which would make the registration easier. However, the vague lines between cyber dependent crime and cyber enabled crime enables the possibility of having an abundance of information, where fraud, scam and online-abuse categorizes as the latter. However, the benefit of having too much information seem to exceed the cost of abundance, where the initial assessment done by a specialized police officer can categorize and label modus operandi more correctly. And ultimately, most cybercrime cases are most likely going to be dismissed, but with a more proper, and more frequently reporting, the information is gathered, enabling the police to work more knowledge based.

There are however some caveats by using a platform, especially with information from cybercrime cases, namely the deployment of laws and regulation, such as GDPR and the Criminal Procedure Act (Justis- og beredskapsdepartementet, 1981). A possible implementation of platforms must therefore be scrutinized by policymakers and juridical teams, especially in relation to store data for intelligence purposes and sharing of these. The utilization of such a platform might pave ways to "wash" data from penal cases, and other graded sources of information, where the enriching, structuring and contextualized output might be something that can be shared, used, and considered actionable intelligence. Another caveat is that to be able to extract possible useful information from investigation or reported cases demands police investigators or operational analysts with high technical skills. As stated in the report from OAG (Riksrevisjonen, 2021), and also mentioned in the interviews, there is a lack of highly technical competent digital forensic investigators, and the best ones are often attractive for the private market. If we are to

introduce the analyst centred approach towards digital forensics, this might be too much to ask for.

Another option is to train and help more operational police analysts with technical skillset or increased understanding of cybercrime, and which possibilities a digital forensic analysis may produce. The process of doing this will enable police analysts, with structured analytical skillsets, to be more integrated in how information from cybercrime cases is handled, and how to make the best use of it. If the police are fortunate to have good police educated digital forensic personnel, with analytical mindsets, there must be made a proper effort to keep them within the police, when their capabilities and skills is regarded highly valuable for the police efforts in handling cybercrime.

NSM was mentioned by several of the participants as an important cooperating party. NSM has its own warning system for digital infrastructure (VDI) (NSM, 2020b). The Police could benefit from increasing its cooperation with NSM, and harvest experiences and knowledge of how they are handling data from this VDI-network, which platform is being used, how it is used, how the automation of information happens, and how this network with data is integrated with current laws and regulations. Further, NSM also has capabilities to analyze data and generate actionable intelligence both from the VDI-sensors, but also from data from the different CERTs working together in SRM, which is a great place to share information, experiences, trends, and indicators. These factors combined, regards it as it useful to have a semi-integrated platform with NSM, where both the Police could contribute on the correct legal terms, and the Police could have access to data from the CERT and VDI community. Quick lookups on known indicators and JA3-hashes could thus provide swift replies and guide the direction of where to search from more info, see if the indicators are a part of a bigger campaign, or are known to be related to a certain threat actor. There is a formalized cooperation today with Joint Cyber Coordination Center (FCKS) (NSM, 2020a), where the parties are Kripos, PST, National Intelligence Service and NSM. But the purpose of FCKS is to quickly clarify the principal responsible party to handle and follow up on the cyber event, together with producing strategic analytical products to support governmental response. This means that there may not be too much integration of operational and technical intelligence with no contextualized or verified technical information.

The stakeholders addressing the intelligence needs in cybercrime policing could potentially be many, and it differentiates based on which level the intelligence process resides on. If the intelligence need is on a more strategic level, the stakeholder claiming its needs would therefore typically be policymakers, police leaders and the Norwegian Police Directory. On an operational level, the stakeholders might be investigation leaders and analysts. Ultimately, the main stakeholders for the police in cybercrime is citizens, protectors of businesses, national interests, critical infrastructure, and the different value chains in society that are dependent on technology to function. A well functioned and balanced society will be more resilient towards threat actors. If we think of stakeholders need for actionable intelligence, we will have to address the intelligence in which actions can be based upon, and decisions made.

For many stakeholders the need for actionable intelligence is relied upon the threat environment and understanding the risk, where the threat-part is the most important risk component in intelligence-led response. And to understand, differentiate, and properly respond to threats, it is helpful to divide this concept into three components: intent, opportunity, and capability (SANS, 2015). And by combining information on a threat with observation of activity, one can more specifically analyse further seized data, do a better selection of the next case to investigate, and connect the discovered TTPs to a threat actor. As an example, if the investigation reveals that the adversaries are intent on stealing data from a certain business sector, there are reasons to believe that the intent is not

opportunistic, and it may be relevant to warn other businesses in the same sector. This non-opportunistic intent of the adversary together with its capabilities may also reveal if this is an APT, often a nation-state actor, which could be actionable and useful information on a more strategic and political level.

The standard intelligence process seems to be used by most of the interviewees, where they emphasized on the importance of knowing the stakeholder and findings their needs for intelligence, as well as the importance of trying to measure the effects of provided intelligence.

The principles of intelligence-driven intrusion detection are the process of identifying and developing intelligence during, and after, an incident and using the feedback to faster identify the compromise of new systems. This process also employs mechanisms, both automated and manually, to identify TTPs, and the best TTPs to identify are those associated with specific goals the adversary is trying to achieve (SANS, 2015): Initial compromise, establish foothold/maintained presence, lateral movement, data collection and data exfiltration. In traditionally standard forensic analysis, the investigator does not always know what to look for, especially in cybercrime cases. If principles of CTI and threat hunting is employed in the process, the investigator will know more of what to look for. One example is automated scanning for compromises by employing indicators from threat intelligence, where the aim could be to search for a specific process, file, registry key, or activity on a system. This methodology could even be used to find new intrusions and move up the kill chain detection earlier (SANS, 2015). The basic principles for CTI, is described as a proactive approach since it involves analysing data from multiple diverse sources and identifies any indicator that can inform in advance about potential cyber threats, including their intent, resources, and methods (Deliu, Leichter and Nguyen, 2017; Papaioannou, 2021). This can enable the police investigator or forensic analyst to identify and understand important evidence in the context of information gathered from other sources (Årnes, 2020).

The aim of the research is not to copy all the principles from CTI or intrusion detection, but to find out if some elements of it could be transferable for the police. Even though the end states and stakeholders are perhaps different, the processes and methods have similarities. Such as the creation of a knowledge database for digital forensics and quick lookups on IOCs, JA3 hashes, signatures etc., which would have been useful for the police. From the interviews, P6 described a method where they made signatures of internal movement in the system, such as techniques indicating lateral movements, and placed these signatures in a database. Several digital forensic images could be placed in this database, enabling them to search for techniques that indicates lateral movement. This is a triage process making the investigator say something about the probability that a threat actor has done something they have seen before, all within a couple of hours. This could potentially save a lot of time as opposed to manually conduct a digital forensic analysis and give actionable answers and guide the investigation process in the right direction. If such a knowledge database were to be used, it could consequently also be shared with the rest of the police. Such a system and infrastructure could have spared tremendous amount of time and efforts from local police and facilitate for a better organizational technical relationship and understanding within the police. Technically, far less skills are demanded to only acquire the data and make digital forensic copies of it.

The main problem has been the analysis, and the holistically technical overview and competence an investigator must have to conduct a thorough digital forensic analysis in a cybercrime case. But to dump images into a database could resolve this issue, at least in the initial phase of the investigation. However, this demands that there is proper infrastructure in place, such as a well-functioning network for sharing seized data, and to conduct analysis regardless of which police districts the investigator is at. By having such

an infrastructure, police officers from NC3 could also travel to local police on requests, and conduct the analysis on premises, and vice versa.

One potential issue of using such a database for triage is that is must be forensically sound for the police, meaning to follow the correct chain of custody. If the data in the knowledge database origins from the police, there should not be a problem. But if data is received from private businesses, this might be a problem. Because in private industry, the focus of a forensically sound process is not prioritized, where the end state, goals and demands are somewhat different. The problem emerges when report or data are shared with the police. The discussion of which tools, frameworks and databases that are forensically sound is out of scope for this thesis, but to have knowledge and understanding of this issue is useful. Because to have insight, and technical understanding, and to be able to find knowledge gaps in the received data is of importance. If knowledge gaps are found, such as lack of actual data or reports to proper validate the conclusion from the report, this can be addressed to the IR team in the private security company, where documentation (if stored) can be shared with the police. If the investigator and police attorney is pleased with the results, the criminal case can continue, knowing that the analysed data is handled forensically sound. However, if the data is used for intelligence purposes, the demands for a forensically process decreases. But to know which data, or reported case, leads to an investigation is difficult to predict, meaning to have a closer relationship with IR teams with a mutual understanding of each other's limitations, capabilities, and routines is relevant, hence the need for additional cooperation with the private security industry.

In terms of the digital forensic analysis, Kripos has now started to use the Tool Hansken for big data, in which multiple digital forensic images can be placed, processed and analysed (Politiforum, 2018). It is out of the scope for this thesis to deeply discuss digital forensic tools and frameworks, but Hansken should be mentioned. This tool is built upon a more open software, enabling the investigators to utilize own scripts for searches and triages across forensic images. This tool may therefore be a good way to perform triages on before the artifacts and indicators are used for further intelligence-led analysis by the means of other relevant tools and frameworks.

And there are many tools and methods mentioned in this thesis, but there is however someone that stands out, such as the Diamond Model in relation with Kill Chain to be able to structure the intelligence work and find new correlations and links. The ACH-model in correlation with Diamond Model as also something that might be useful for the police, especially since hypothesis-making is so incorporated within the police. MITRE ATT&CK is also assessed to be important by the interviewees, with emphasis to be able to map techniques and have a common language. By using this, technical reports may be more understandable for police leaders, and decision-makers further up the system in the investigation, or intelligence process. And the sharing and receiving of information may also be less troublesome by deploying this framework.

Another important aspect of working intelligence-led is threat hunting, which was mentioned during the interviews. Diamond Model is known to work perfectly for threat hunting, and the relationship of hunt for threats and develop hypothesis, as most police personnel is known to, are quite similar. In threat hunting these four questions are important to understand and build strategies upon: What are you hunting? Where will you find it? How will you find it? When will you find it? (Caltagirone, 2016). These four questions should address the basis of hypothesis-making: to answer the "Why", and hunters must build and test many hypotheses at once. As an example, the investigators or analyst's hypothesis that the adversary has used command line interface, then the examination should cover logging processes of executions of command-line. Or if the hypothesis is regarding credential dumping, which is the process of obtaining account login and password information and used for lateral movement end more accesses. Then the examination, or

hunt, should cover command execution and hunt for commands that invoke AuditID or the Security Accounts Manager (SAM). Hence, the SAM-registry files should also be examined (MITRE, 2022). Each failed hypothesis can lead to a failed hunt.

To use the Diamond Model for intelligence-led examinations also enables the investigator, or analyst, to have an analytical mindset towards the technical side of the digital forensic process. Since the model utilized four approaches, all these can deploy new hypothesis: infrastructure, capability, victim, and adversary. To exemplify, the victim approach is used, since this may be important for the police in terms of preventive policing. Some hypotheses are thus relevant to organize and structure the hunt. Initially, we hypothesize that several adversaries target a specific victim, and that the adversary deliver their capabilities via email, which could answer the question "Why". The goal of the hunt can answer the "What", such as having a goal to collect intelligence on adversary attacks in the email delivery phase. The "Where" and "How", can address our victim-centred approach, where we wish to gain visibility into the victim email and apply tools which illuminate likely malicious elements. "When" could be for how long we wish to examine the email (Caltagirone, 2016). However, to hunt demands patience and discipline. But the idea if having more structured, analytically and intelligence driven approaches to both the digital forensic process, and technical analysis might be a good idea for the police.

In terms of level of intelligence, the structuring and contextualization of operational, tactical, and technical indicators are what seems to be most actionable, especially on a short-term basis. At this level the indicators are important, which can be described as any information that objectively describes an intrusion. Indicators can further be subdivided into three types: **Atomic** (cannot be broken down into smaller pieces, i.e., IP-address), **computed** (derived from data involved in an incident, i.e., hash value), and **behavioural** (collection of computed and atomic indicators). Behavioural indicators are often subject to qualification by quantity and possibly combinatorial logic (Hutchins, Cloppert and Amin, 2011). The tools, techniques and methods mentioned in this research advocate these behavioural indicators, that can be revealed through forensic analysis and collaboration. This can lead to findings of additional indicators. One way to systematically search for indicators is to deploy Kill Chain, and use this as a basis for the investigation, or collection of intelligence. Also, the Diamond Model integrates its phased approach and complements Kill Chain by broadening the perspective which provides needed granularity and the expression of complex relationships amongst intrusion activity (Caltagirone, Pendergast and Betz, 2013).

Another important aspect by learning from private businesses and other intelligence agencies is the technical skills and training. The Norwegian Police Academy with the NCFI program (Nordic Computer Forensic Investigators) (PHS, 2022), offers courses in both digital forensics and cybercrime investigation. On regards of the researchers own experiences, these courses are valuable, relevant, and not least, they are free for police personnel. However, these courses might also be supplemented with other relevant courses, although most private courses are costly. But as an effort to both increase knowledge, and retain own employees, perhaps these courses should be prioritized to a higher degree. One should also utilize in-house competence for governmental agencies, such as facilitate a closer relationship, not only for sharing information, but also for sharing experiences and knowledge. Norway has many agencies that work towards the same cyber-related goals, such as NSM and The Norwegian Cyber Defence.

7 Further Research

Measuring

One of the participants, P3, mentioned how they measured the produced cyber intelligence both quantitative and qualitative. By doing so, they ensured that the produced intelligence was both enforceable and traceable, meaning they could make empirical data from measuring the effects. This was their way to validate that the cyber intelligence was actionable and had effects. The way NCDBS are producing their yearly report (Næringslivets Sikkerhetsråd, 2022) is partly based on interviews, but still provides great insight in how the police are assessed from outsiders. Something similar could be done in the police, such as surveys or short interviews of decision makers, where the outcome could form the bases for where to direct the production of intelligence. You would then have empirical data of the state today, and their intelligence needs. This can further be measured and quantified and used as basis to allocate resources and funding.

Another interesting approach is to implement some of the proposed measures to the police, as seen in Table 4, and measure the effects afterwards. This could be done both quantitatively and qualitatively which in terms could be measured and generate empirical data. The results could yield better grounds for debating whether new ideas, methods and models is appropriate or feasible for the police to use, and it would strengthen the validity of this master's thesis.

There was conducted research in 2020 from The Norwegian Institute of Public Health, called Target management in the police's preventive work (Langøien, Nøkleby and Jacobsen, 2020), which did the research on behalf of the Norwegian Police Directory. The research problem was to study target management of the police's preventive work aimed towards sexual offences and radicalization, and this research might be a good source to gain more knowledge on how to conduct preventive measures in cybercrime policing, and how to measure it. The main conclusion from the report is that there were challenges in relation to what are being measured and how the indicators are registered, since the police are incident-driven and measured by completed offences. Examples are lack of knowledge, lack of resources, inconsistencies between strategies and goal formulations, a mutual understanding of preventative policing, and the importance of cooperation between actors in the preventive work. Further, the report concluded that indications of measurements should be assessed upon productivity as opposed to results, done by qualitative indicators. This report could be taken advantage of for further research for how to conduct preventive policing strategically and tactically with cybercrime, and how to statistically measure efforts.

Work intelligence-led

Regardless of methods, tools or procedures, a consensus amongst the participants is the need for cooperation to work intelligence-led. Lemieux and Bales performed research on proactive investigations models in 2012 (Lemieux and Bales, 2012), and their take on the research was to interview police cybercrime investigators from three different agencies in USA, where the aim was to seek how they worked intelligence-led. The main conclusions were that the investigators worked on a case-by-case basis, where the starting point to investigations was based on reporting and complaints. They also saw indications of that

police personnel were currently not using proactive, intelligence-led type measures to handle cybercrime, even though the characteristics of cyber threats are compliant with the main objectives of ILP (Lemieux and Bales, 2012). This research also stated that FBI and Secret Service had established extensive partnership with private businesses for sharing intelligence and crime prevention. The research from Lemieux and Bales could be scrutinized further, and additional research can be conducted, especially if Norwegian police are going to formalize ILP with cybercrime.

Knowledge database

There is also emphasis on knowledge databases in this research, in which digital forensic images could be dumped and triaged based on automation of IOCs and signatures, as mentioned by P6 in 4.2.1. The results from this triage could be to compare with the results from traditional digital forensics analysis and see quantitatively which artefacts and indicators were found by the different methods. One could also add another perspective, as illustrated in the master's thesis project description from the researcher (Fossum, 2021), where a traditional digital forensic analysis process is measured and compared with an analysis using models and frameworks, such as the Diamond Model and MITRE ATT&CK. A prerequisite is that the participants are given the same digital forensic image, but they can use different means to reach a conclusion.

In terms of knowledge bases and automation of triaging digital forensic images, one necessary condition is that the knowledge base has content in which the images can be compared against. And to produce and generate rules and signatures is perhaps a delimitation for the police, because this demands capacity in which Norwegian police does not have abundances of. Hence, rules and signatures might have to be purchased, or borrowed from other security or intelligence agencies. It could therefore be interesting to examine which methods that could work in correlation with the police's objectives, and to measure and research with detection rules or signatures that may be applicable for cybercrime investigation. Two of the most common signatures or set of rules are Sigma and YARA, which respectively can detect anomalies by monitoring log events to find signs of suspicious activity (Sigma) and identifying and classifying malware samples using IOCs (YARA) (Ax, 2022).

Knowledgebases and different methods and frameworks can be used as a solid base for threat hunting. Additionally, to triage forensic images in a database can also be categorized as threat hunting, since the goal is to look for potential threats. But the process could be operationalized as a formal procedure for preventing and mitigating cybercrime, and one area of research is to examine how a threat hunting procedure might be designed for police purposes. The process of threat hunting is very much intelligence-led, driven by actionable intelligence and hypotheses. The Diamond Model purpose fits well with processes of threat hunting, where the four distinctive features can be used as grounds for hunting procedures: adversary, victim, infrastructure, and capability (Caltagirone, 2016).

Threat hunting

In research conducted on threat hunting (Liliengren and Löwenadler, 2018), they compared threat hunting to a forensic investigation. One part that differs forensic investigation from threat hunting is that the former tries to obtain evidence of malicious actions on exploited systems, whereas the latter tries to determine how certain systems can be exploited. The analytical mindset is similar, but they found that forensic investigation has more reliable, repeatable, and well-documented methods for procedures. And there has been done research in Norway on digital forensic processes, such as the latest doctoral thesis from Sunde (Sunde, 2022), and the thesis' from

Heitmann (Heitmann, 2019) and Borhaug (Borhaug, 2019). They all aim to research how the digital forensic processes, methods and challenges are within the police. Some of this empirical data, together with additional standardized methods and frameworks, could form the basis of a solid procedural practice of conducting threat hunting in the police. Because threat hunting has clear resemblances to CTI, where a threat hunter might see CTI as a start for hunting, and not an end result (Liliengren and Löwenadler, 2018).

Sharing

The importance of cooperation and sharing of information was something all participants agreed upon, and it is also an important element of intelligence-led policing. However, the formality of doing so for the police is a somewhat unexplored area and could be researched additionally. The caveat of sharing for the police is how to keep it within the correct juridical framework, which channels to utilize for sharing of information, and how the information should be classified as.

8 References

Aas, M. (2020) *Risikoanalyse som ferskvare*. Universitetet i Oslo.

Andersen, S. (2019) 'Technical Report: A preliminary Process Model for Investigation', *SocArXiv.* doi: 10.31235/osf.io/z4wma.

Anderson, C. A. *et al.* (2014) 'Using thematic analysis in psychology', *Psychiatric Quarterly*, 0887(1), pp. 37–41. Available at: http://www.ncbi.nlm.nih.gov/pubmed/11752478.

Årnes, A. (2020) 'Introduction', in Årnes, A. (ed.) *Cyber Investigations*. Unpublished book.

Ax, S. (2022) *Sigma rules explained: When and how to use them to log events*. Available at: https://www.csoonline.com/article/3663691/sigma-rules-explained-when-and-how-to-use-them-to-log-events.html (Accessed: 22 November 2022).

Bahonjic, D. (2021) *Etterretning og virkelighetskonstruksjoner*. Politihøgskolen.

Barlatier, J. (2020) 'Criminal Investigation and Criminal Intelligence: Example of Adaptation in the Prevention and Repression of Cybercrime', 8, p. 99. doi: 10.3390/risks8030099.

Bjelland (2020) 'Internet Investigations', in Årnes, A. (ed.) *Cyber Investigations*. Unpublished book.

Bjørgo, T. (2015) *Forebygging av kriminalitet*. Universitetsforlaget.

Borhaug, T. S. (2019) *The Paradox of Automation in Digital Forensics*. NTNU.

Bratton, W. J. and Malinowski, S. W. (2008) 'Police Performance Management in Practice: Taking COMPSTAT to the Next Level', *Policing: A Journal of Policy and Practice*, 2(3), pp. 259–265. doi: 10.1093/police/pan036.

Braun, V. and Clarke, V. (2006) 'Using thematic analysis in psychology', *Qualitative Research in Psychology*, 3(2), pp. 77–101. doi: 10.1191/1478088706qp063oa.

Bureau of Justice Assistance (2012) 'Reducing Crime Through Intelligence-Led Policing'. Available at: https://www.bja.gov/Publications/ReducingCrimeThroughILP.pdf%5Cnpapers3://publication/uuid/FD0A64DD-B695-4FE0-86E1-0CD19585CD6B.

Caltagirone, S. (2016) *Building Threat Hunting Strategies with the Diamond Model*. Available at: https://www.activeresponse.org/building-threat-hunting-strategy-with-the-diamond-model/ (Accessed: 10 December 2022).

Caltagirone, S., Pendergast, A. and Betz, C. (2013) 'The Diamond Model of Intrusion Analysis', *Threat Connect*, 298(0704), pp. 1–61. Available at: http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA586960%5Cnhttps://www.threatconnect.com/wp-content/uploads/ThreatConnect-The-Diamond-Model-of-Intrusion-Analysis.pdf.

Casey, E. (2011) *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Elsevier Science. Available at: https://books.google.bi/books?id=lUnMz_WDJ8AC.

Chismon, D. and Ruks, M. (2015) 'Threat Intelligence: Collecting, Analysing, Evaluating', *Cert-Uk*, p. 36. Available at: https://www.cpni.gov.uk/Documents/Publications/2015/23-

March-2015-MWR_Threat_Intelligence_whitepaper-2015.pdf.

Cisecurity (2022) *Election Security Spotlight – Cyber Threat Actors*. Available at: https://www.cisecurity.org/spotlight/cybersecurity-spotlight-cyber-threat-actors/ (Accessed: 9 December 2021).

Cook, A. *et al.* (2017) 'The industrial control system cyber defence triage process', *Computers and Security*, 70, pp. 467–481. doi: 10.1016/j.cose.2017.07.009.

Creswell, J. (2007) *Qualitative inquiry and research design: Choosing among five approaches*. 2nd edn. Thousand Oaks, CA: Sage Publications, Inc.

Cybercrime Magazine (2021) *Cybercrime To Cost The World $10.5 Trillion Annually By 2025*. Available at: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ (Accessed: 12 December 2021).

Davenport, T. H. and Prusak, L. (1997) *Information Ecology: Mastering the Information and Knowledge Environment*. 1st edn. USA: Oxford University Press, Inc.

Deliu, I., Leichter, C. and Nguyen, H. T. (2017) *Extracting Cyber Threat Intelligence From Hacker Forums*. NTNU.

Departementene (2019) *Nasjonal strategi for digital sikkerhet*.

Drake, V. (2022) *The Pyramid of Pain and Cyber Threat Intelligence*. Available at: https://flashpoint.io/blog/the-pyramid-of-pain-and-cyber-threat-intelligence/ (Accessed: 10 December 2022).

E24 (2021) *Her slår politiet til mot mistenkte Hydro-hackere*. Available at: https://e24.no/naeringsliv/i/MLdEyr/her-slaar-politiet-til-mot-mistenkte-hydro-hackere (Accessed: 10 December 2022).

ENISA (2014) *Actionable Information for Security Incident Response*.

Europol EC3 (2017) *IOCTA 2017*. doi: 10.2813/55735.

Europol EC3 (2021) *IOCTA 2021*. doi: 10.2813/113799.

Fahsing, I. A. and Bjerknes, O. T. (2017) *Etterforskning Prinsipper, metoder og praksis*.

Flaglien, A. O. (2018) 'The digital forensics process', in Årnes, A. (ed.) *Digital Forensics*. Gjøvik: John Wiley and Sons Ltd.

Forsvaret (2021) *Forsvarets etterretningsdoktrine*.

Fossum, E. N. (2021) *Intrusion Analysis of Ransomware in Cybercrime Cases*.

Glesne, C. E. (1999) *Becoming Qualitative Researchers: An Introduction*. 2nd edn. New York: Longman.

Gundhus, H. O. . (2013) 'Experience or knowledge?: Perspectives on new knowledge regimes and control of police professionalism', *Policing: A Journal of Policy and Practice*.

Gundhus, H. O. I. (2018) 'Smart politiarbeid? Når skillene mellom etterretning, forebygging og etterforskning viskes ut', in Rønne, A. and Stevnsborg, H. (eds) *Ret smart: Om smart teknologi og regulering.* Jurist- og Økonomforbudets forlag.

Gunzenhauser, M. G. and Gerstl-Pepin, C. I. (2006) 'Engaging Graduate Education: A Pedagogy for Epistemological and Theoretical Diversity.', *Review of Higher Education: Journal of the Association for the Study of Higher Education*, 29, pp. 319–346. doi: 10.1353/rhe.2006.0008.

Hamremoen, E. (2016) *Kriminalteknikk: første enhet på åstedet*. 2nd edn. Gyldendal.

Harfield, C. and Maren Eline, K. (2008) 'Intelligence, knowledge and the reconfiguration

of policing', in Harfield, C. et al. (eds) *The Handbook of Intelligent Policing: Consilience, Crime Control and Community Safety*. Oxford: Oxford University Press, pp. 239–253.

Harr Vaage, B. and Sundal, K. M. (2019) 'Mot en analysesentrisk etterretningsprosess', in Stenslie, S., Haugom, L., and Harr Vaage, B. (eds) *Etterretningsanalyse i den digitale tid*. Fagbokforlaget, p. 222.

Hatlebrekke, K. A. (2021) *The Problem of Secret Intelligence*. Edinburgh University Press (Intelligence, surveillance and secret warfare). Available at: https://books.google.no/books?id=iI15zQEACAAJ.

Heitmann, O. (2019) *Digital investigation: The malnourished child in the Norwegian police family?* NTNU.

Hestehave, N. (2018) *Proaktiv kriminalitetsbekæmpelse for politifolk*. Edited by N. R. Fyfe, H. O. Gundhus, and K. Vrist Rønn. Routledge.

Ho, K. H., Chiang, V. C. and Leung, D. (2017) 'Hermeneutic phenomenological analysis: the "possibility" beyond "actuality" in thematic analysis', *Journal of Advanced Nursing*, 73(7), pp. 1757–1766. doi: 10.1111/jan.13255.

Hsieh, H.-F. and Shannon, S. (2005) 'Three Approaches to Qualitative Content Analysis', *Qualitative health research*, 15, pp. 1277–1288. doi: 10.1177/1049732305276687.

Hunton, P. (2010) 'Cyber Crime and Security: A New Model of Law Enforcement Investigation', *Policing: A Journal of Policy and Practice*, 4(4), pp. 385–395. doi: 10.1093/police/paq038.

Hunton, P. (2011) 'The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation', *Computer Law & Security Review*, 27(1), pp. 61–67. doi: https://doi.org/10.1016/j.clsr.2010.11.001.

Hustveit, R. A. (2017) *Etterretning vs. etterforskning*. Politihøgskolen.

Hutchins, E., Cloppert, M. and Amin, R. (2011) 'Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains', *6th International Conference on Information Warfare and Security, ICIW 2011*, (July 2005), pp. 113–125.

Interpol (2021) 'Interpol (2021) National Cybercrime Strategy Guidebook'. Available at: https://www.interpol.int/content/download/16455/file/National Cybercrime Strategy Guidebook.pdf.

Ishikawa, K. (1985) *What is total quality control? : the Japanese way*. Englewood Cliffs, N.J. : Prentice-Hall.

Johnsen, R. (2020) *Cyber defense tactics: Defending our way of living*. Unpublished.

Justis- og beredskapsdepartementet (1981) *Straffeprosessloven*. Norway. Available at: https://lovdata.no/dokument/NL/lov/1981-05-22-25 (Accessed: 14 September 2021).

Justis- og beredskapsdepartementet (1986) *Påtaleinstruksen*. Norway. Available at: https://lovdata.no/dokument/SF/forskrift/1985-06-28-1679/KAPITTEL_6-6#§37-3 (Accessed: 2 December 2021).

Justis- og beredskapsdepartementet (1995) *Politiloven*. Norway. Available at: https://lovdata.no/dokument/NL/lov/1995-08-04-53 (Accessed: 10 September 2021).

Justis- og beredskapsdepartementet (2013) *Politiregisterforskriften*. Norway. Available at: https://lovdata.no/dokument/SF/forskrift/2013-09-20-1097 (Accessed: 16 December 2021).

Justis- og beredskapsdepartementet (2014) 'Prop. 61 LS: Proposisjon til Stortinget

(forslag til lovvedtak og stortingsvedtak) Endringer i politiloven mv. (trygghet i hverdagen-naerpolitireformen)'.

Justis- og beredskapsdepartementet (2021) *Straffeloven*, *Straffeloven*. Norway: Justis- og beredskapsdepartementet. Available at: https://lovdata.no/dokument/NL/lov/2005-05-20-28?q=straffeloven (Accessed: 21 November 2021).

Justis-og beredskapsdepartementet (2010) *Politiregisterloven*. Norway. Available at: https://lovdata.no/dokument/NL/lov/2010-05-28-16?q=politiregisterloven (Accessed: 16 December 2021).

Justis-og beredskapsdepartementet (2014) 'Proposisjon til Stortinget (Prop. 61 LS)'.

Justis-og beredskapsdepartementet (2015) *Justis-og beredskapsdepartementets strategi for å bekjempe IKT-kriminalitet*.

Justis-og beredskapsdepartementet (2019) *Politimeldingen – et politi for fremtiden (Meld. St. 29)*. Available at: www.regjeringen.no (Accessed: 29 November 2021).

Kafle, N. P. (2013) 'Hermeneutic phenomenological research method simplified', *Bodhi: An Interdisciplinary Journal*, 5(1), pp. 181–200. doi: 10.3126/bodhi.v5i1.8053.

Kianpour, M. (2021) 'Socio-Technical Root Cause Analysis of Cyber-enabled Theft of the U.S. Intellectual Property - The Case of APT41'. Available at: https://uscode.house.gov/browse/prelim@title18/part1/chapter37&.

Kowalski, S. (1994) *IT Insecurity: A Multi-discipline Inquiry PhD thesis*. Univ Stockholm and Royal Inst Technology.

Kowalski, S. J. (1993) 'Reporting ICT crimes: SBC as a conceptual framework'.

Kruse, W. G. and Heiser, J. G. (2002) *Computer Forensics: Incident Response Essentials*. Addison-Wesley. Available at: https://books.google.no/books?id=nNpQAAAAMAAJ.

Kvale, S. and Brinkmann, S. (2019) *InterViews*. København: Hans Reitzel.

Langøien, L. J., Nøkleby, H. and Jacobsen, P. S. (2020) *Målstyring i politiets forebyggende arbeid: en systematisk kartleggingsoversikt*.

Leedy, P. D. and Ormrod, J. E. (2015) *Practical Research*. 11th edn. Harlow: Pearson Education Limited.

Lemieux, F. and Bales, B. (2012) 'Cyber Crime and Intelligence-led Policing: In Search of a Proactive Investigation Model', *Technocrime, Policing and Surveillance*, (January 2012).

Liliengren, T. and Löwenadler, P. (2018) *Threat hunting, definition and framework*. Halmstad University.

de Lint, W., O'Connor, D. and Cotter, R. (2007) 'Controlling the flow: Security, exclusivity, and criminal intelligence in Ontario', *International Journal of the Sociology of Law*, 35(1), pp. 41–58. doi: 10.1016/j.ijsl.2007.01.001.

Magaldi, D. and Berler, M. (2020) 'Semi-structured Interviews', in Zeigler-Hill, V. and Shackelford, T. K. (eds) *Encyclopedia of Personality and Individual Differences*. Cham: Springer International Publishing, pp. 4825–4830. doi: 10.1007/978-3-319-24612-3_857.

van Manen, M. (1997) *Researching lived experience: Human science for an action sensitive pedagogy*. 2nd editio. Left Coast Press Inc.

Mitre (2022) *OS Credential Dumping*. Available at: https://attack.mitre.org/techniques/T1003/ (Accessed: 1 December 2022).

Moen, R. (2020) *Anbefalinger i politiets etterretningsprodukter – et dilemma*, *Nordic*

Journal of Studies in Policing. Universitetsforlaget. doi: 10.18261/ISSN.2703-7045-2020-03-02.

Myhre Lie, E. (2011) *I forkant – kriminalitetsforebyggende politiarbeid*. Oslo: Gyldendal Akademisk.

Næringslivets Sikkerhetsråd (2020) *Mørketallsundersøkelsen*.

Næringslivets Sikkerhetsråd (2022) *Mørketallsundersøkelsen*.

National Criminal Intelligence Service (2000) 'National Intelligence Model'.

Nese, A. (2018) *Improving Security Posture by Learning from Intrusions*. NTNU. Available at: https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/2562796/19083_FULLTEXT.pdf?sequence=1.

NSM (2020a) *Nasjonalt cybersikkerhetssenter og nasjonale tekniske sikkerhetstiltak*. Available at: https://nsm.no/hold-deg-oppdatert/meninger/nasjonalt-cybersikkerhetssenter-og-nasjonale-tekniske-sikkerhetstiltak (Accessed: 1 December 2022).

NSM (2020b) *Varslingssystem for digital infrastruktur (VDI)*. Available at: https://nsm.no/tjenester/varslingssystem-vdi/ (Accessed: 25 November 2022).

NSM (2021) *Nasjonalt digitalt risikobilde 2021*. Available at: https://nsm.no/aktuelt/nasjonalt-digitalt-risikobilde-2021.

NSM (2022) *Nasjonalt digitalt risikobilde 2022*. Available at: https://nsm.no/getfile.php/1312007-1664785983/NSM/Filer/Dokumenter/Rapporter/NDIG2022_online.pdf.

Økokrim (2022) *Stor forebyggende aksjon mot datakriminalitet: Over 170 bedrifter varslet og 28 angrep avverget*, *Pressemelding*. Available at: https://www.okokrim.no/stor-forebyggende-aksjon-mot-datakriminalitet-over-170-bedrifter-varslet-og-28-angrep-avverget.6505227-549344.html (Accessed: 1 April 2022).

Omand, D. (2011) *Securing the State*. New York: C Hurst & Co Publishers Ltd.

Papaioannou, F. (2021) 'Threat Intelligence Platforms evaluation'. Available at: https://dione.lib.unipi.gr/xmlui/handle/unipi/13346.

PHS (2022) *Nordic Computer Forensic Investigators*. Available at: https://www.politihogskolen.no/en/post-graduate/nordic-computer-forensic-investigators/ (Accessed: 20 November 2022).

Picussecurity (2022) *MITRE ATT&CK Framework BEGINNERS GUIDE*. Available at: https://www.picussecurity.com/mitre-attack-framework-beginners-guide (Accessed: 10 December 2022).

Politidirektoratet (2006) 'POD rundskriv 2006/010 pkt 4.', pp. 1–4.

Politidirektoratet (2016) 'Handlingsplan for løft av etterforskningsfeltet'.

Politidirektoratet (2017a) *Plan-og rammeskriv versjon 1.0*.

Politidirektoratet (2017b) *Retningslinjer for bruk av etterforskningsplan. Versjonnummer 1.0.*

Politidirektoratet (2018) 'Kriminalitetsforebygging som politiets primaerstrategi 2018-2020'.

Politidirektoratet (2020) *ETTERRETNINGSDOKTRINE FOR POLITIET*.

Politidirektoratet (2021) *Politiets trusselvurdering*.

Politiet (2020a) *Informasjon til de som er utsatt for skadevare*. Available at: https://www.politiet.no/om/organisasjonen/sarorganene/kripos/kripos-hovedarbeidsomrader/nasjonalt-cyberkrimsenter/informasjon-til-de-som-er-utsatt-for-skadevare/ (Accessed: 22 December 2021).

Politiet (2020b) 'PBS I Retningslinjer for politiets beredskap'. Available at: www.politiet.no (Accessed: 8 October 2021).

Politiet (2021a) *Nasjonalt cyberkrimsenter*. Available at: https://www.politiet.no/om/organisasjonen/sarorganene/kripos/kripos-hovedarbeidsomrader/nasjonalt-cyberkrimsenter/ (Accessed: 25 November 2021).

Politiet (2021b) *Tips politiet*. Available at: https://tips.politiet.no/web/ (Accessed: 16 December 2021).

Politiet (2022) *Næringslivskontakter i politiet*. Available at: https://www.politiet.no/kontakt-politiet/naringslivskontakter/ (Accessed: 12 December 2022).

Politiforum (2018) *Nederlansk big-data-program analyserer store mengder data på rekordtid. Nå anbefaler Kripos at norsk politi får ta det i bruk.* Available at: https://www.politiforum.no/datakriminalitet-dataverktoy-hansken/nederlansk-big-data-program-analyserer-store-mengder-data-pa-rekordtid-na-anbefaler-kripos-at-norsk-politi-far-ta-det-i-bruk/145541 (Accessed: 25 November 2022).

PST (2021) *Nasjonal Trusselvurdering 2021*.

Ratcliffe, J. H. (2016) *Intelligence-Led Policing*. Taylor & Francis. Available at: https://books.google.no/books?id=Anz7CwAAQBAJ.

Reuters (2022) *Russia takes down REvil hacking group at U.S. request - FSB*. Available at: https://www.reuters.com/technology/russia-arrests-dismantles-revil-hacking-group-us-request-report-2022-01-14/ (Accessed: 10 December 2022).

Rid, T. and Buchanan, B. (2015) 'Attributing Cyber Attacks', *Journal of Strategic Studies*, 38, pp. 4–37. doi: 10.1080/01402390.2014.977382.

Riksadvokaten (1999) *Rundskriv nr 3 for 1999*.

Riksadvokaten (2016) *Mål og prioriteringer for straffesaksbehandling i 2016 - Politiet og statsadvokatene*.

Riksadvokaten (2018) *Kvalitetskrav til straffesaksbehandlingen i politiet og ved statsadvokatembetene mv.* Available at: https://www.riksadvokaten.no/wp-content/uploads/2019/02/Kvalitetsrundskrivetrevidertfebruar19.pdf.

Riksadvokaten (2019) *Mål og prioriteringer for straffesaksbehandlingen i 2019*.

Riksrevisjonen (2021) *Riksrevisjonens undersøkelse av politiets innsats mot kriminalitet ved bruk av IKT*.

Røger, O. G. (2019) 'An root cause analysis of VISMA security breach 2018'. Not published.

Rønn, K. V. (2016) *Efterretningsstudier*. 1.udgave. samfundsliteratur.dk.

Roy Røsberg, A. (2020) *'The abductive organised crime detective'*. Politihøgskolen.

SANS (2015) 'FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics'. SANS.

Schumann, R. (2021) *The Norwegian Infection-Tracing App analyzed from a Socio-technical Perspective*. NTNU.

Selebø, B. E. (2022) *Develop best practice within exercise control management Content*.

Shulsky and Schmitt (2002) *Silent Warfare: Understanding the World of Intelligence*. Washington, D.C.: Brassey's, Inc.

Sloan, A. and Bowe, B. (2014) 'Phenomenology and hermeneutic phenomenology: the philosophy, the methodologies, and using hermeneutic phenomenology to investigate lecturers' experiences of curriculum design', *Qual Quant*, 48, pp. 1291–1303. doi: 10.1007/s11135-013-9835-3.

Steffensen, T. (2021) 'Leveranse fagspesialisering cyberetterretningsanalyse'. Not published.

Steinmetz, C. H. D. (1982) 'A First Step towards Victimological Risk Analysis. A conceptual model for the prevention of "petty" crime', in, pp. 55–87.

STYX Intel (2022). Available at: https://styxintel.com/ (Accessed: 5 December 2022).

Sunde, I. M. (2020) 'Cyber law', in Årnes, A. (ed.) *Cyber Investigations*. Unpublished book.

Sunde, N. (2017) *Non-technical Sources of Errors When Handling Digital Evidence within a Criminal Investigation*. NTNU.

Sunde, N. (2020a) 'Cyber Investigations', in Årnes, A. (ed.). Unpublished book.

Sunde, N. (2020b) 'Structured Hypothesis Development in Criminal Investigation-A method aimed at providing a broad and objective starting point for a criminal investigation'.

Sunde, N. (2022) *Constructing digital evidence*. University of Oslo.

Tjora, A. H. (2021) *Kvalitative forskningsmetoder i praksis*. 4th edn. Gyldendal.

Trellix (2021) *What Is the MITRE ATT&CK Framework?* Available at: https://www.trellix.com/en-us/security-awareness/cybersecurity/what-is-mitre-attack-framework.html (Accessed: 13 September 2021).

United States of Department and Justice (2012) 'Law Enforcement Analytic Standards'.

UNODC (2011) *Criminal Intelligence: Manual for Analysts*. Available at: www.unodc.org (Accessed: 20 October 2021).

Vestby, A. (2018) 'Policy making without politics: Overstating objectivity in intelligence-led policing', in *Moral issues in intelligence-led policing*. Routledge.

Volden, F. (2019) *IMT4110 Scientific Methodology and Communication*, *Lectures in 2019*.

Whitman, M. (2019) *Management of information security*. Boston, MA: Cengage Learning.

9 Appendices

Appendix A: Interview guide

Appendix B: Consent form

Appendix C: NSD approval

Appendix A:

Intervjuguide – Master`s Thesis: **"Intelligence for Cyber Crime: The study of stakeholders needs for actionable intelligence"**

NB: Husk å underskrive på samtykkeskjema!

Formalia

Utdanning, erfaring med etterretning og hendelseshåndtering, erfaring med digitale trusler.

Beskrive egen rolle

- Beskrive sin rolle i prosessen med håndtering av digitale trusler og/eller til bruken av etterretning

Digitale trusler, samarbeid, etterretning og forebyggende politiarbeid er fokusområder i dette intervjuet

- Hva tenker du om det digitale trusselbildet i Norge i dag?
- Hvordan bruker dere etterretning mot datakrim i egen bedrift?
- Hvilken betydning har etterretning for deres forsvare mot dataangrep?
    - evt. hvorfor er det ikke en sentral del?
- Hva tenker du om forebyggende arbeid mot å forhindre datakrim?

Bruken av etterretning og informasjon

- Hvilken informasjon har dere behov for slik at dere best mulig skal kunne utføre jobben deres på en trygg måte?
    - Hva er den beste måten å motta slik informasjon på?
    - Hva tenker du er den beste måten å videreformidle dette på?
- Hvordan struktureres etterretningsjobben i egen bedrift?
    - Hvor innhentes informasjon fra?
        - Hvor viktig er hendelseshåndtering?
        - Hvordan blir denne informasjonen prosessert videre?
    - Hvilke(n) etterretningsprosess(er) benytter dere?
        - Hvorfor benytter dere denne/disse?
- Det gode eksempelet
    - Fortell om en sak med positivt utfall etter en etterretningsjobb
    - Hva kunne vært gjort annerledes i denne saken?
- Det dårlige eksempelet
    - Hva var det som gjorde at dette ikke fungerte?
    - Var det noe som fungerte slik det skulle?
- Kunnskapsbasert arbeid
    - Hvordan benyttes etterretning for å jobbe kunnskapsbasert?
    - Har du sett gode resultater av dette?
    - Har du sett negative resultater av dette?
- Beslutningstakerne
    - For hvem blir etterretningsprodukt utarbeidet for?
    - Hvilken effekt ser du av beslutninger som blir tatt på bakgrunn av etterretningsprodukt?

Samarbeid

- Har dere noe samarbeid når det gjelder informasjonsdeling og/eller formidling av etterretning?
    - Hvilke samarbeidspartnere har dere?
    - Evt. hvilke samarbeidspartnere er ikke til stede, og hvorfor vil du ha et samarbeid med disse?
    - Hvilke utfordringer mener du det foreligger i samarbeidsprosessen?

    - Beskrive samarbeidet med politiet
        - Hvordan tenker du at denne kunne blitt bedre?
- Videreformidling av etterretning
    - Hvilke etterretningsprodukt blir mottatt og faktisk benyttet?
    - Hvilke etterretningsprodukt blir videreformidlet fra din bedrift?

Etterretningsanalyse

- Hvordan analyseres og bearbeides informasjonen?
- Hvilke analyseverktøy blir benyttet?
    - Hvorfor brukes disse?
        - Negative erfaringer?
        - Positive erfaringer?
- Hvis dette ikke framkommer i forrige spørsmål:
    - Erfaringer med bruk av Diamant-modellen?
    - Erfaringer med bruk av Mitre Atta&ck?
    - Erfaringer med bruk av Cyber Kill Chain?
- Hvem bruker verktøyene?
    - Hvordan fungerer samarbeidet mellom den som benytter verktøyet og beslutningstakere?
- Hvilken rolle har analytikeren i deres arbeid?

Beskyttelse mot dataangrep

- Fortell om hvilken strategi din bedrift har mot dataangrep
- Hva er hovedmålet hvis bedriften skulle blitt utsatt for et angrep?
- Hva tenker du om politiets rolle før og etter et evt. angrep?

Politiets rolle og bekjempelse av datakriminalitet

- Fortell om hva du tenker om hvorvidt hendelser og datainnbrudd burde rapporteres til politiet, evt. hvorfor det ikke burde rapporteres
- Hvordan oppleves politiets rolle blant kolleger i egen bedrift, og/eller i andre bedrifter?
- Hvilket samarbeid har du hatt med politiet i forbindelse med digitale trusler?
    - Hvis ikke, er det noe du kunne tenke deg å samarbeide nærmere om?

Muligheter i kampen mot digitale trusler og dataangrep

- Hvilke muligheter mener du det finnes i bruken av etterretning og bygge et bedre forsvar mot digitale trusler og dataangrep?
- Hvilke muligheter ser du for deg at politiet kan ha i forbindelse med håndteringen av digitale trusler, datakriminalitet og det forebyggende arbeidet?

Appendix B:

Forespørsel om deltakelse i forskningsprosjekt

Masteroppgave: "Intelligence for cybercrime: The study of the need for actionable intelligence"

Bakgrunn og formål:

Det har den siste tiden kommet en rapport på politiets manglende evne til å håndtere datakriminalitet (Riksrevisjonens undersøkelse av politiets innsats mot kriminalitet ved bruk av IKT), i tillegg til at mange bedrifter vegrer seg for å rapportere inn mulig straffbare forhold som omhandler datakrim inn til politiet (Næringslivets Sikkerhetsråds Mørketallsundersøkelse). Det er ofte bedrifter selv, eller innleide sikkerhetsselskaper som håndterer digitale trusler/hendelser, ofte uten politiets involvering. Et resultat av dette er at politiet ikke tilstrekkelig nok oppnår sine mål som er stadfestet i politilovens §2, å forebygge, avdekke og stanse kriminell virksomhet og forfølge straffbare forhold.

I min masterstudie forsøker jeg å se nærmere på hvordan politiet kan oppnå sine målsetninger, og hvordan politiet kan dra nytte av, og anvende, etterretningsstyrt politiarbeid innen datakriminalitet for å oppnå dette. Målet vil være økt situasjonsforståelse, bedre beslutningsgrunnlag og økende grad av kunnskapsbasert politiarbeid. Et av de mer konkrete tiltakene som et ledd i dette er å anvende analytiske verktøy som Diamond Model for Intrusion Analysis, samt sosio-tekniske rammeverk for innhenting og formidling. I den anledning har jeg et ønske om å undersøke hvordan etterretnings- og sikkerhetsmiljøer håndterer sitt etterretningsstyrte arbeid, samt om hvordan privat sektor og politi kan dra nytte av hverandre. I tillegg ønsker jeg å høre med mellomstore bedrifter som ikke har sitt eget sikkerhetsmiljø om hvordan de opplever både trusselbildet, politiets involvering og bruken av etterretning.

Hva innebærer deltakelse i studien?

Alle personopplysninger vil bli behandlet konfidensielt. Det er kun jeg som har tilgang til personopplysningene, og disse vil lagres adskilt fra intervjudataene. Intervjuene vil danne grunnlag for analysen som presenteres i rapporten (masteroppgaven). Deltakerens navn vil ikke bli brukt i rapporten, og det vil heller ikke bli gitt inngående beskrivelser av person eller arbeid som vil kunne identifisere deltakerne. Dersom opplysninger om bakgrunn blir benyttet i tilknytning til sitater, vil du få anledning til å lese gjennom dette.

Prosjektet skal etter planen avsluttes 01.06.22, og personopplysninger blir slettet når endelig sensur på masteroppgaven er klar (september/oktober 2022).

Frivillig deltakelse

Det er frivillig å delta i studien, og du kan når som helst trekke ditt samtykke uten å oppgi noen grunn. Dersom du trekker deg, vil alle opplysninger om deg bli anonymisert. Ta gjerne kontakt med meg, Eivind Nes Fossum, telefonnummer 97529081. Veileder er Stewart Kowalski, telefonnummer 95434212, professor ved NTNU, Institutt for informasjonssikkerhet og kommunikasjonsteknologi. Studien er meldt til Personvernombudet for forskning, NSD - Norsk senter for forskningsdata AS.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger
Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

Samtykke til deltakelse i studien

Jeg har mottatt og forstått informasjon om prosjektet: *"*Intelligence for cybercrime: The study of the need for actionable intelligence*"*, og har fått anledning til å stille spørsmål. Jeg samtykker til:

- □ å delta i intervju
- □ at mine personopplysninger lagres 6 måneder etter sensur for å sikre etterprøvbarhet.
- □ at det benyttes direkte sitater kommet frem i intervjuet.
- □ ved benyttelse av direkte sitater ønsker jeg å lese gjennom disse før publisering

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet

---

(Signert av prosjektdeltaker, dato)

Appendix C:

Sikt

Meldeskjema / Masteroppgave - erfaringsbasert master i informasjonssikkerhet ve... / Vurdering

Vurdering av behandling av personopplysninger

Referansenummer	Vurderingstype	Dato
516562	Standard	09.12.2022

Prosjekttittel
Masteroppgave - erfaringsbasert master i informasjonssikkerhet ved NTNU

Behandlingsansvarlig institusjon
Norges teknisk-naturvitenskapelige universitet / Fakultet for informasjonsteknologi og elektroteknikk (IE) / Institutt for informasjonssikkerhet og kommunikasjonsteknologi

Prosjektansvarlig
Stewart Kowalski

Student
Eivind Nes Fossum

Prosjektperiode
16.08.2021 - 15.12.2022

Kategorier personopplysninger
Alminnelige

Lovlig grunnlag
Samtykke (Personvernforordningen art. 6 nr. 1 bokstav a)

Behandlingen av personopplysningene er lovlig så fremt den gjennomføres som oppgitt i meldeskjemaet. Det lovlige grunnlaget gjelder til 15.12.2022.

Meldeskjema

Kommentar

Bekreftelse på status

Personverntjenester har vurdert endringen i prosjektsluttdato.

Vi har registrert 15.12.2022 som ny sluttdato for behandling av personopplysninger.

Vi vil følge opp ved ny planlagt avslutning for å avklare om behandlingen av personopplysningene er avsluttet/pågår i tråd med den behandlingen som er dokumentert.

Kontaktperson: Anne Marie Try Laundal
Lykke til videre med prosjektet!