UiA University of Agder

IS-507-1 MASTER'S THESIS CYBER SECURITY

Unveiling the Potential of Open-Source Intelligence (OSINT) for Enhanced Cybersecurity Posture

A study on OSINT implementation and utilization within organizations and recommendations for increased leverage of OSINT's advantages

JOHANNA SOFIE SLINDE

SUPERVISOR

Professor Jaziar Radianti, University of Agder

University of Agder, 2023

Faculty of Social Sciences

Department of Information Systems

Master

Obligatorisk egenerklæring

Den enkelte student er selv ansvarlig for å sette seg inn i hva som er lovlige hjelpemidler, retningslinjer for bruk av disse og regler om kildebruk. Erklæringen skal bevisstgjøre studentene på deres ansvar og hvilke konsekvenser fusk kan medføre. Manglende erklæring fritar ikke studentene fra sitt ansvar.

1.	Jeg erklærer herved at min besvarelse er mitt eget arbeid, og at jeg ikke har brukt andre kilder eller har mottatt annen hjelp enn det som er nevnt i besvarelsen.	Ja
2.	**Jeg erklærer videre at denne besvarelsen:** • Ikke har vært brukt til annen eksamen ved annen avdeling/universitet/høgskole innenlands eller utenlands. • Ikke refererer til andres arbeid uten at det er oppgitt. • Ikke refererer til eget tidligere arbeid uten at det er oppgitt. • Har alle referansene oppgitt i litteraturlisten. • Ikke er en kopi, duplikat eller avskrift av andres arbeid eller besvarelse.	Ja
3.	Jeg er kjent med at brudd på ovennevnte er å betrakte som fusk og kan medføre annullering av eksamen og utestengelse fra universiteter og høgskoler i Norge, jf. Universitets- og høgskoleloven §§4-7 og 4-8 og Forskrift om eksamen §§ 31.	Ja
4.	Jeg er kjent med at alle innleverte oppgaver kan bli plagiatkontrollert.	Ja
5.	Jeg er kjent med at Universitetet i Agder vil behandle alle saker hvor det forligger mistanke om fusk etter høgskolens retningslinjer for behandling av saker om fusk.	Ja
6.	Jeg har satt meg inn i regler og retningslinjer i bruk av kilder og referanser på biblioteket sine nettsider.	Ja

Publiseringsavtale

Fullmakt til elektronisk publisering av oppgaven. Forfatter(ne) har opphavsrett til oppgaven. Det betyr blant annet enerett til å gjøre verket tilgjengelig for allmennheten (Åndsverkloven. §2).
Oppgaver som er unntatt offentlighet eller taushetsbelagt/konfidensiell vil ikke bli publisert.

Jeg gir herved Universitetet i Agder en vederlagsfri rett til å gjøre oppgaven tilgjengelig for elektronisk publisering:	Ja
Er oppgaven båndlagt (konfidensiell)?	Nei
Er oppgaven unntatt offentlighet?	Nei

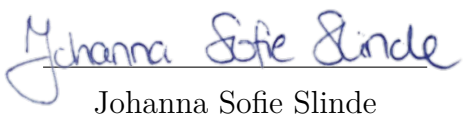
Acknowledgements

This thesis completes my master's degree in cybersecurity management at the University of Agder (UiA). Throughout my courses in the cybersecurity program, I became conscious of the discrepancy between the efforts employed by cyber adversaries to target their victims and the efforts made by organizations to defend against them. As a result, I delved into cyber threat intelligence and open-source intelligence, aiming to understand how organizations can leverage analyzed information for enhanced protection against relevant cyber threats and increase their understanding of the surrounding threat landscape.

I want to thank several people for helping me conduct this thesis. Firstly, thanks to the people involved from Deloitte Cyber Risk Advisory for providing me with theoretical guidance and support and for connecting me with relevant interview candidates. Secondly, I want to acknowledge the contributions of all interview participants, which have provided me with essential empirical evidence for this thesis. Thirdly, a thank you to my fellow students for a great two years studying together throughout the master's program.

Last but certainly not least, I sincerely thank my supervisor Professor Jaziar Radianti from the Department of Information Systems at the University of Agder. Your academic knowledge and experience have helped me immensely through this journey. Thank you for your continuous encouragement.

Kristiansand,
1st of June 2023



Johanna Sofie Slinde

Abstract

Never before has it been more important to increase internal cybersecurity posture to prevent malicious activity, and organizations are forced to mobilize their resources to prepare for tomorrow's threats. Throughout the past few years, the usage of open-source intelligence (OSINT) has made its way from the military landscape into public, private, and commercial organizations. Using OSINT, organizations can tailor their countermeasures to the tactical, operational, and strategic procedures of potential cyber threat actors by benefiting from the knowledge within openly available sources. Leveraging the enormous information sharing on online platforms using OSINT also requires organizations to navigate the increasing information overload. Nevertheless, many are using ad hoc and unstructured approaches, contradicting the systematic fundamentals of the intelligence profession. Therefore, this study investigated how organizations can implement and use OSINT to improve cybersecurity posture using OSINT's advantages. A semi-systematic literature review (SSLR) highlighted a scant focus on organizational aspects of OSINT, whereas the focus has primarily relied on technical considerations. Interviews with nine representatives of different private, public, and commercial organizations helped understanding how each applied OSINT to extract as much value as possible from the CTI capability. During data collection and analysis, this thesis adopts the intelligence cycle, a well-known cyclic representation of the intelligence acquisition process. The thesis extends the theory by integrating several intelligence cycle theories and offers a more dynamic and comprehensive representation of the intelligence process. Through an inductive conceptual framework (ICF), the thesis highlights how OSINT can become a valuable tool to ensure organizations encounter the cyber threat landscape by considering relevant information about threat actors. The study emphasizes the significance of establishing an understandable definition of OSINT within one's organization and identifying intelligence requirements aligned with available resources. Determining the organization's motivation, prioritizing dialogue and feedback, and continuously evaluating the intelligence requirements are essential to leveraging OSINT's advantages. This new framework is one of the main contributions of this thesis, visualizing how the research findings all contribute to a coherent utilization of OSINT as a cybersecurity-enhancing tool. By guiding organizations through the entire intelligence cycle, they will likely experience a greater understanding of their own capabilities and potential cyber attackers.

List of Abbreviations

APT	Advanced persistent threat
CDC	Cyber defense center
CERT	Computer emergency response team
CSA	Cyber situational awareness
C-suite	An organization's top management positions (e.g., CEO, CFO, CISO)
CTI	Cyber threat intelligence
DCF	Deductive conceptual framework
GEOINT	Geospatial intelligence
HUMINT	Human intelligence
ICF	Inductive conceptual framework
IMINT	Image intelligence
IoCs	Indicators of Compromise
IR	Intelligence requirement
MASINT	Measurement and signature intelligence
OSINF	Open source information
OSINT	Open source intelligence
QRC	Qualitative research cycle
SIGINT	Signal intelligence
SIR	Specified intelligence requirement
SOC	Security operations center
SSLR	Semi-systematic literature review
TTPs	Tactics, techniques, and procedures

Table 1: Abbreviations

Contents

List of Figures

List of Tables

1 | Introduction

> If you know your enemies and know yourself, you will not be imperiled in a hundred battles; if you do not know your enemies but do know yourself, you will win one and lose one; if you do not know your enemies nor yourself, you will be imperiled in every single battle.
>
> *Sun Tzu, The Art of War*

Although living over 2400 years ago, the lesson from Sun Tzu is still applicable today. However, the enemies these days are not knights in shining armor, nor are the battles fought with swords and shields. Having made our way into the information age – where every human has access to one or several connected devices – the battles are fought in the cyber domain every day, all the time. Being a 24/7 available service, the Internet has become a battlefield that requires everyone to show precaution to avoid being harmed by users with malicious intentions. The importance is highlighted by the National Security Authority in Norway (NSM, *Nasjonal sikkerhertsmyndighet*), which detected a drastic increase in the number of attempted compromises against Norwegian organizations during the first half of 2022 (National Security Authority, 2022). Simultaneously, discoveries show a significant disparity between advanced persistent threats (APTs) capabilities and organizations' ability to protect and defend themselves against them (Microsoft Corporation, 2021). Sun Tzu states that the key to winning battles is knowing oneself and one's enemies, which in the cyber domain translates to adopting cybersecurity measures to meet relevant threats with tailored countermeasures (Shin & Lowry, 2020). By implementing cyber threat intelligence (CTI), organizations can gain knowledge of tactical (what), operational (how and where), and strategic (who and why) information (FireEye Inc., 2019), aiding them in facing cyber threats.

A method of obtaining CTI is through publicly available sources, called open-source intelligence (OSINT). By leveraging open sources, OSINT enables organizations to learn about adversaries' tactics, techniques, and procedures (TTPs) to make informed decisions to strengthen their cybersecurity. Using intelligence has been especially important within military organizations due to the need to navigate in obscure environments. When OSINT was first proposed is

unknown, but in modern years, it entered during World War II as used by the US Army to monitor publicly available information to aid their military operations (Hassan & Hijazi, 2018). Today, information is shared much faster through our interconnected world, where a large part of the information shared is publicly available. OSINT is an intelligence capability that benefits from the enormous sharing of online information as one can address security threats emerging within cyberspace before causing damage (Hwang et al., 2022; Pastor-Galindo et al., 2020). By applying timely, accurate, and ingestible threat intelligence, organizations can apply real-time acquired information to their benefit by implementing tailored countermeasures (Hwang et al., 2022).

However, collecting information from open sources can be complex and challenging. The enormous amounts of information create an overload of information, upon which information also is spread to mislead, requiring intelligence analysts to examine the reliability of the information source carefully (Pastor-Galindo et al., 2020). Moreover, the knowledge gathered from OSINT must be sufficiently implemented within the organization to provide value and increase cybersecurity. Despite the growing trend of organizations adopting CTI as an essential element of their cybersecurity initiatives, many continue to follow an ad-hoc approach towards outlining their internal CTI requirements (Brown & Stirparo, 2022). Being successfully implemented, OSINT can be a valuable resource for organizations within their decision-making processes by providing knowledge of today's world and what it might look like tomorrow.

Since intelligence originates from the military domain, it has benefited from the strict structures and hierarchy within military organizations. With everyone having defined roles, the planning, collection, analysis, and dissemination of acquired intelligence flow naturally within such organizations. With an increasing amount of commercial, private, and public organizations developing their CTI capabilities and processes (Brown & Stirparo, 2022), they must find their way of collecting and leveraging OSINT and handling the following challenges. There is limited knowledge of how organizations should use threat intelligence processes to strengthen their cybersecurity posture (Kotsias et al., 2022). According to theory, intelligence processes must be structured, targeted, and tailored to achieve actionable intelligence (Pawliński et al., 2014). Meanwhile, surveys indicate that many use ad hoc and unstructured approaches (Brown & Stirparo, 2022). With the vision of how OSINT can benefit an organization and its cybersecurity posture, this thesis aims to investigate this area further through the following research questions (RQs):

RQ1: "How can organizations plan and implement Open Source Intelligence (OSINT) to enhance their cybersecurity posture?"

RQ2: "Which factors are critical for successful OSINT utilization in order to leverage its advantages and encounter its challenges?"

With these two research questions, the thesis aims to understand how organizations structure

their usage of OSINT as a CTI capability within their organizations to both leverage the value of OSINT and encounter its challenges. As intelligence processes are complex, extracting some essential factors that are especially important to consider for successful OSINT utilization is desired. As a result, the goal is to enhance an organization's cybersecurity posture, i.e., its overall readiness and defense against cyber threats.

1.1 Rationale and Motivation

As the amount of available data and information on the Internet increases daily, so does the frequency of cyberattacks. In their newest report (National Security Authority, 2023), NSM emphasizes the importance of organizations gaining accurate situational awareness through threat intelligence to increase their cybersecurity posture, meeting the increased risk of cyber-attacks. There is a constant battle between the defenders and the attackers, where both parties want to be ahead of the other. By implementing OSINT – considered one of the most valuable tools in the arsenal of online investigators and intelligence analysts (Gibson, 2016) – organizations can be carried through a shift from reactive to proactive within their cybersecurity posture (Kotsias et al., 2022). If used correctly and efficiently, OSINT can provide organizations with valuable threat information to support decision-making, influencing their overall cyber posture.

Upon examining previous research for implementing OSINT effectively in non-military organizations, it became clear that recent research within the cyber intelligence field has focused less on organizational processes and more on technical implementations. Whereas it was thought that only larger organizations with dedicated and robust cyber-teams utilized threat intelligence, a survey from SANS Institute (Brown & Stirparo, 2022) shows that the number of smaller organizations adopting CTI increases. With more than 200 organizations participating in the study, over 51% responding they use a combination of in-house and third-party services for the CTI function, indicating the increased importance of focusing on adopting CTI and synthesizing information to ensure organizational value. The lack of focus on behavioral and administrative aspects of threat intelligence implementations, despite CTI's and OSINT's raised popularity, is also remarked by Shin and Lowry (2020). Consequently, there is limited knowledge regarding how OSINT should be implemented within an organization, as much of our knowledge exists from its implementation within military and governmental institutions. Within intelligence studies, the intelligence cycle is used to describe the stages required from the initial intelligence request to the dissemination of an intelligence product. Due to the differences in objectives, resources, experience, and knowledge among organizations, the construction of the intelligence cycle describing intelligence implementation and planning might not be accurate and reflect intelligence processes in practice (Hulnick, 2006). Organizations must realize methods and approaches to gradually advance their OSINT capability by aligning acquired information with the organization's business context to provide actionable intelligence (Shin & Lowry, 2020).

Studying intelligence processes within organizations is complex, and only the tip of the iceberg is touched during this thesis. Nevertheless, Shin and Lowry (2020), among others, encourages researchers not to shy away from the complexity of threat intelligence but grab the opportunity to address both findings and new issues. Referred to as a "not yet exploited goldmine" by Pastor-Galindo et al. (2020), OSINT has considerable value to provide organizations.

1.2 Research Approach

The research questions have been examined through a qualitative research approach by adopting the qualitative research cycle (QRC) (Figure 4.1) by Hennink et al. (2020). The cyclic representation of the qualitative research methodology accurately represented how the research could be conducted and opened the possibility of adapting parts of the research as it developed. Furthermore, the QRC provided academic depth to the research and aided in assessing the research quality through the study. Assessing literature and theory is emphasized in the QRC, and it was decided to carry out a semi-systematic literature review (SSLR) – following the guide by Okoli and Schabram (2010) and recommendations by Snyder (2019) – to gather relevant material regarding the implementation of OSINT within organizations concerning cybersecurity matters. Previous research was used to gain knowledge of the current state-of-the-art within OSINT usage.

Moreover, extracting perspectives regarding researchers' views of OSINT's advantages and disadvantages was emphasized, which would aid in understanding organizations' potential motivational aspects and challenges upon implementation and usage. These aspects were considered crucial in answering the research questions regarding OSINT implementation and the key factors to success. The SSLR identified six proposed intelligence cycles, symbolizing the researchers' visualizations of how OSINT implementation within an organization. Following the QRC, a deductive conceptual framework was created after the completion of the SSLR, which summarized the key points and relation between the literature reviewed. For data collection, conducting semi-structured interviews with nine intelligence practitioners gave empirical evidence for the research. By conducting interviews, the aim was to understand the steps within the practitioners' intelligence processes within their respective organizations and address the perceived value and potential challenges encountered in their daily operations. The deductive conceptual framework was used both when creating an interview guide and during data analysis. Knowledge from previous research gathered during the SSLR was applied upon analyzing the empirical findings, resulting in a discussion assessing this thesis' research questions.

1.3 Delimitations

It is essential to note the delimitations regarding this thesis as it provides information as to why the thesis is constructed as it is and what the thesis aims at targeting. Firstly, OSINT

has many different use cases – in which three of which are presented in Section 3.1.2 – which makes it important to remark that this thesis discusses the implementation and usage of OSINT within organizations for cybersecurity-enhancing purposes. Thus, aspects related to OSINT usage for business intelligence, social opinion, marketing purposes, and such is outside the scope of this thesis.

Secondly, RQ1 refers to the organizational aspects of how OSINT implementation provides cybersecurity-enhancing value. The hypothesis relates to the perception of how OSINT can aid in increasing people's understanding of the threat landscape. A correct understanding of one's cyber adversaries and cyber threats can facilitate the implementation of tailored countermeasures, thus, enhancing the overall cybersecurity posture by being prepared for threats relevant to one's organization. As the semi-structured interviews lead to the empirical evidence, the perception of *enhanced cybersecurity posture* is based on subjective interpretation of qualitative content, not quantitative measurements.

Lastly, there are many aspects one can discuss concerning the usage of OSINT, for instance, different ethical considerations and GDPR compliance considerations upon using social media as an information source. Although these are important concepts to consider, such considerations are not covered within this thesis as the focus is on the process and actions taken to ensure that OSINT provides value for cyber defense within the organization.

1.4 Thesis Overview

The thesis is structured as follows: **Chapter 1** provides an introduction to the thesis where the research area and problem will be clarified, in addition to the research gap to which the thesis aims to contribute; **Chapter 2** explains the theoretical background related to the intelligence profession and how threat intelligence applies to the cybersecurity field. The concept of OSINT will be further explained and defined here; **Chapter 3** maps out and describes the theory on CTI and OSINT found through a semi-systematic literature review and concludes with the research gap this thesis addresses; **Chapter 4** describes the thesis' research approach. Justification and explanation of the chosen methods – the qualitative research method and the semi-systemized literature review – are presented. The deductive conceptual framework is presented as used both during data collection and data analysis; **Chapter 5** presents the empirical findings from nine interviews using the structure of the inductive conceptual framework; **Chapter 6** discusses and analyses the empirical findings in the light of the theory provided in Chapters 3 and 4, and highlights the significant findings related to the research questions and the construction of the inductive conceptual framework. The chapter ends by presenting the inductive conceptual framework; **Chapter 7** presents the thesis' conclusions and its contribution to the industry. Limitations are also discussed, together with recommendations for potential future research.

2 | Theoretical Background

> Intelligence is an activity that has to perform three functions. Information has to be acquired; it has to be analyzed and interpreted; it has to be put into the hands of those who use it.
>
> Professor F. H. Hinsley (cited in UK Ministry of Defence (2011)

Some might associate *intelligence* with spies with trench coats and black hats, with secret identities sitting in parks with newspapers with holes for their eyes to see through. Or uniformed personnel walking around with piles of documents stamped with SECRET in big red letters. As with many other professions, intelligence has modernized throughout the years and become a profession not only applicable to governmental or military institutions but also to other types of organizations and private businesses which perceive a potential threat danger. Shortly speaking, the intelligence profession can be explained as in the quote at the beginning of this chapter. Nevertheless, the intelligence profession is complex; hence, this chapter aims to clarify it further. Terms like cyber threat intelligence and open-source intelligence will be introduced and explained in detail to provide the thesis with sufficient theory for the subsequent chapters.

2.1 What Intelligence Is

Being referred to as the world's second oldest profession, writings about intelligence date back all the way to the Old Testament (Stenslie et al., 2019a). Trying to predict our neighbors' and enemies' actions by discovering their secrets is something humans have done for thousands of years. It could be said that intelligence is the answer to the human endeavor of trying to foresee potential threats and create countermeasures for averting them (Forsvaret, 2021). For that reason, the field of intelligence has played a crucial role in military conflicts in the form of espionage, where it has been applied in the making of strategic decisions. Having background information before making important decisions was advantageous then, and is still, as the world is progressing and changing rapidly. Intelligence is often associated with secrecy, as it is kept secret and away from the public for it to remain valuable for its possessor.

Defining intelligence is not an easy task as its definition often depends on by whom and where it is used. For example, a military entity will have a different need and understanding of intelligence than a commercial organization. Despite the different definitions, it is important that the definition is understood by the people involved in where it is used and that it makes sense for their work. For simplicity, one could say that intelligence is information; however, not all information is intelligence (Liska, 2014, p. 22). Thus, the definition of intelligence depends on where it is applied and the understanding of the difference between *information* and *intelligence*.

2.1.1 Data, Information, and Intelligence

According to *Forsvarets Etterretningsdoktrine* (English: The Norwegian Armed Forces' Intelligence Doctrine) (Forsvaret, 2021, p. 25) data, information, and intelligence are all related concepts but provide the end user with varying degrees of value. Figure 2.1 visualizes the process from data to intelligence, where the value for the intelligence user increases from left to right. The initial result from the collection is called *data* and must be interpreted and processed by professionals with knowledge within the area. Then, the interpreted data becomes information and can be used by people from outside the field. Finally, information becomes intelligence when it is analyzed and evaluated by professionals. At this stage, the intelligence has normally become a product, e.g., a report, which states something about the probability of the analyzed information becoming a reality and its potential consequences. Through its way from being just information to intelligence, the content has become *actionable*, which is an essential attribute of intelligence as a product. By being actionable it is meant the information is now accurate, relevant, timely, complete, and ingestible for its receiver (Pawliński et al., 2014). If not analyzed into intelligence and made actionable, the retrieved information may become unmanageable for the receiver as one lacks understanding of how to put it into context and make the value of it (Yusof et al., 2018).

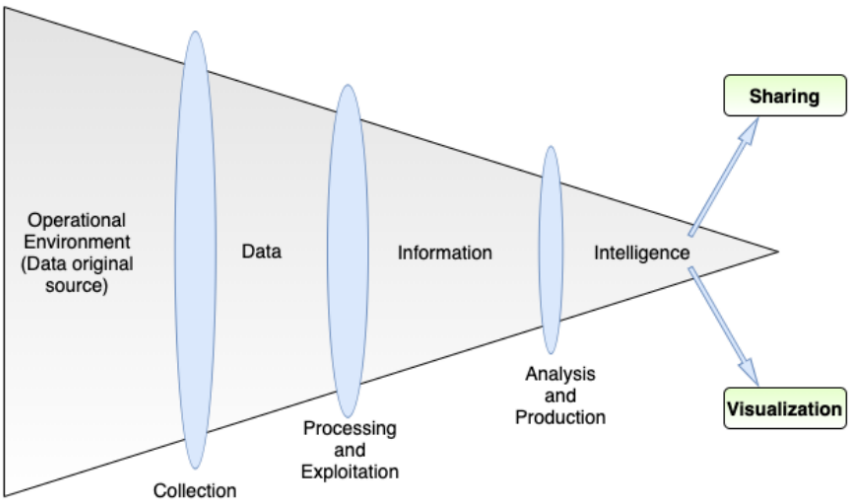


Figure 2.1: The relation between data, information and intelligence (Amaro et al., 2022, p. 3)

To illustrate the differences, Hassan and Hijazi (2018) presents the following example of how to distinguish between data, information, and knowledge (intelligence):

- Data is facts describing something, e.g., "The price of gold is $1,2/ounce."
- Information is interpreted data, e.g., "The price of gold has fallen from $1,2/ounce to $1,1/ounce within the last week".
- Knowledge (intelligence) is information in combination with experience and insight aiding to make decisions in the future, taking experienced situations into consideration, e.g., "The price of oil is interlinked with the price of gold, meaning if the gold prices fall, the oil prices falls as well".

2.1.2 Definition of Intelligence

The distinction between information and intelligence is often visible in the definition of intelligence. Since intelligence originates from military institutions, several military and governmental sources have been thoroughly examined to understand its definition. As a NATO member, the Norwegian Armed Forces have adopted NATO's definition of intelligence (Forsvaret, 2021). NATO defines intelligence as:

> "The product resulting from the directed collection and processing of information regarding the environment and the capabilities and intentions of actors, in order to identify threats and offer opportunities for exploitation by decision-makers." (NATO, 2019, p. 68)

To compare, the Norwegian Police have applied the following definition of intelligence in their report *Politiets Etterretningsdoktrine* (English: The Norwegian Police's Intelligence Doctrine):

> "Intelligence is a controlled process, consisting of systematic collection, analysis, and assessment of information about individuals, groups, and phenomena to form a basis for decisions." (Politiet, 2020, p. 18)

The term intelligence is used both for the organization, the activity and the knowledge one possesses (Kent (1949) cited in Stenslie et al., 2019a), thus; one does often distinguish if one is speaking about intelligence as a process or a product. The two abovementioned definitions do well illustrate the different meanings and definitions one is making of intelligence depending on where it is applied. While one of them focuses on the intelligence product, the other emphasizes the process. As this thesis discusses intelligence both in terms of being a process and a final product supporting decision-making, the following definition is applied:

> "Intelligence is the umbrella term referring to the range of activities – from planning and information collection to the analysis and dissemination – conducted in secret and aimed at maintaining or enhancing relative security by providing forewarning of threats or potential threats in a manner that allows for the timely implementation

> of a preventive policy or strategy, including, where deemed desirable, convert activities." (Gill & Phythian (2012) cited in Liska (2014, p. 22)).

This more detailed definition of intelligence also includes the aspect of being preventive, which is especially important when applying intelligence into the cyber field, more elaborated in Section 2.2.

2.2 Cyber Threat Intelligence (CTI)

Upon the rise of the Internet in the 1990s, communication shifted from the physical space to the digital space, and people were no longer bound by time and space to communicate with each other. Simultaneously as new doors opened for information sharing through digital tools came also the possibility of misusing these methods to perform criminal actions. In recent years one has witnessed a drastic shift in how cyber attacks are performed, from people experimenting with their cyber skills – popularly called *script kiddies* – to organized criminals and even nation states (Kotsias et al., 2022). The increased frequency of cyberattacks and the severity they can cause both business continuity and people's safety, implies the importance of being prepared for the worst. Similar to how military forces have gathered detailed information on their adversaries in order to stay prepared, organizations can use threat intelligence to gather an understanding of potential cyber threat actors. These are actors that have the capability, intent, and opportunity to exploit a vulnerability present in the victim's environment, with the motivation to reach an asset and, subsequently, cause a risk to the organization (NIST, 2022).

With the definition of intelligence from Section 2.1.2 in mind, the term cyber threat intelligence (CTI) can be understood as analyzed, processed, and disseminated information about cyber threats which advises decision-makers in courses of action (Ettinger et al., 2019). The adaption of CTI can enable organizations to enhance their awareness of the constantly evolving threat landscape, with the objective of identifying and averting threats prior to an attack. In addition to being considered a crucial tool in both preparing and detecting potential cyber risks, CTI can also aid in the creation of situation awareness among stakeholders (Brown & Lee, 2019; Wagner et al., 2019). The attributes of intelligence re-enter here – accuracy, relevance, timeliness, completeness, and ingestible – as CTI is not simply an indicator of a previous cyber attack, the attributes must be present for it to be actionable (Bromiley, 2016).

Theoretically, CTI can be divided into three levels depending on the type of information the intelligence is communicating. The levels provide the intelligence receiver with information on *what* the adversary does during its attacks, *how* and *where* the attacks are performed, and *who* they are and their motives. In more detail, Bamford et al. (2013) explains the three levels in the following way:

- **The strategic level** determines the adversary's motives and objectives for carrying out the attack.

- **The operational level** describes the adversary's planning and the intelligence they have collected themselves to prepare for an attack. Here, the capabilities are being made to prepare for the tactical operation.
- **The tactical level** is where the action happens in terms of infiltration and exploitation of vulnerabilities. This level describes their tactics, techniques, and procedures (TTPs), which can be examined to clearly understand how an actor behaves during an attack (NIST, 2022).

By adopting information from all these three levels, Omand (2019, p. 34) describes how threat intelligence can aid decision-makers in four main ways: increase situational awareness; explain the situation (why and how); predict and evaluate future events; alert on important future development. Hence, the utilization of CTI can aid an organization in gaining a coherent understanding of the threat landscape and consequently implement tailored technical countermeasures based on that information. Besides the technical perspective, CTI can also provide *strategic* decision-making support. From the strategic perspective, CTI can provide organizations with direction and set objectives, including enhancing the shared understanding of cyber threats (Borum et al., 2015). While the technical CTI tends to regard short time frames and hands-on information in technical considerations, the strategic CTI is often focused on longer time frames and produced for leaders and executives (Borum et al., 2015). The strategic perspective will provide information on trends, analytics, and sector-specific information, which can support decision-making in the long run. Such decisions can involve risk management and the advancement of an organization's objectives where knowledge about the organization's vulnerable resources and assets are especially important to consider (Borum et al., 2015).

2.3 Open-Source Intelligence (OSINT)

Having described how intelligence differs from regular information and data, it is necessary to map out the different capabilities from which intelligence can originate. From a military perspective, one usually differs between information retrieved from human sources (HUMINT) and from technical sources (Stenslie et al., 2019b). Using technical sources, one can interpret information from signals (SIGINT), images (IMINT), measurement and signatures (MASINT), geographics (GEOINT), and open sources (OSINT), among others. These capabilities are formally known as *intelligence disciplines*.

Beginning an intelligence process starts by identifying the knowledge one wants to obtain, called an intelligence requirement (IR). This is a requirement for any kind of information needed by someone to develop an understanding of a situation (UK Ministry of Defence, 2011). The IR can arise due to knowledge gaps or requests from intelligence users (Forsvaret, 2021). Depending on the IR, the intelligence producer collecting the information must choose the discipline best suited (Liska, 2014, p. 24). In the 1990s, OSINT much evolved around the

translation of foreign-press publications, but as the world has digitized, OSINT has changed to benefit from the wide spread of available information (Pastor-Galindo et al., 2020; Williams & Blum, 2018). Within the cyber domain, information from open sources has long been acknowledged as a valuable resource when preparing oneself against cyber attacks (Williams & Blum, 2018). As the usage of social media and online resources has increased over the last few years, open sources have become a mecca of potentially useful information.

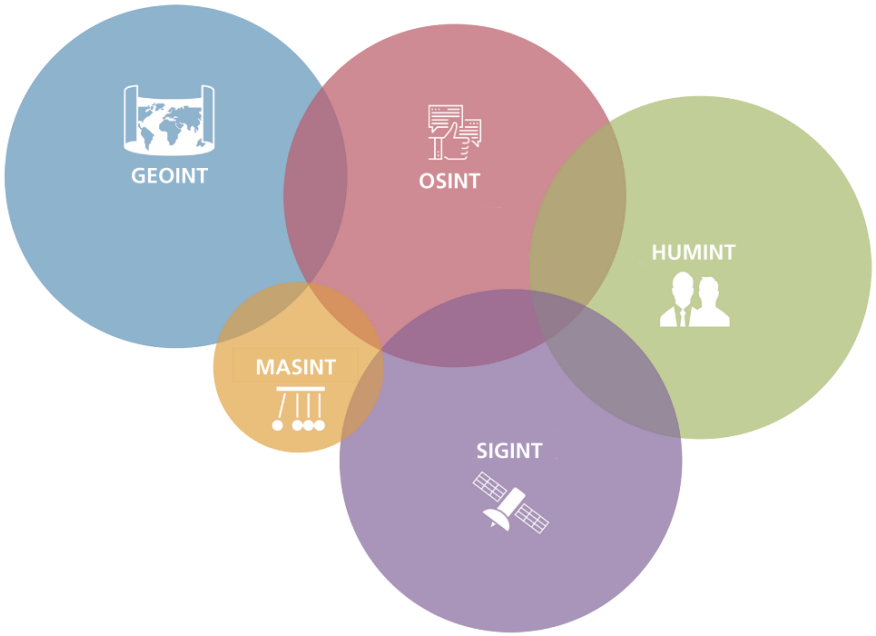


Figure 2.2: The overlapping of intelligence disciplines (Williams & Blum, 2018, p. 9)

Due to its variety of users – from military institutions to technical operations centers and larger corporations – the definition of OSINT varies accordingly. Shortly described, OSINT is a type of intelligence derived from open sources, as can be understood by its compounded words (Open Source INTelligence). However, the discussion arises in defining what is meant by *open sources*. Pastor-Galindo et al. (2020, p. 10282) defines open source information (OSIF) to be information from "[...] mass media, social networks, forums and blogs, public government data, publications, or commercial data", while Williams and Blum (2018, p. 10) states that "OSIF is material that can be lawfully obtained through request, purchase, or observation by a member of the public". Within this thesis, a combination of the two is used as the definition of OSINT, thus; OSINT is material obtained legally from openly available sources, either through manual or automatic methods, through either internal systems, or via third-party vendors. Nevertheless, it is important to notice the distinction between OSINT and OSINF, as OSINF is information – when seen in isolation – provides no significant intelligence value.

As OSINT is, in fact, a discipline gathering information from various sources, it would be correct to visualize the terms as overlapping. Figure 2.2 represents the thoughts of Williams and Blum (2018) on how the disciplines are connected, which provides an interesting angle in

the debate on the definition and sense of OSINT as both a product and process. Williams and Blum (2018) argues that our understanding of OSINT as a discipline affects how the final intelligence product is treated, whether a single-source or an all-source product, influencing how the intelligence discipline is prioritized.

2.4 The Intelligence Cycle

As earlier described in this chapter, the primary goal of both intelligence in general and OSINT specifically is to provide its users with an increased understanding of the threat landscape, thereby, potential threats and their TTPs. From the initial requirement of intelligence is raised until an intelligence product is complete, numerous steps are required. For that purpose, the intelligence cycle is often used to visualize the efforts that lie behind an intelligence product. The cyclic representation is used to visualize how obtained intelligence products often reproduce new IRs (Forsvaret, 2021). Even though referred to as a *process* – which often gives associations with work performed in routines and without reflection – the intelligence process must be adaptable and usable for various scenarios, and hence very *dynamic* (UK Ministry of Defence, 2011). Depending on factors like the stakeholders, scenarios, IRs, and the time perspective, among others, the intelligence process will vary. Usually, there are many different cycles operating in parallel at different speeds and levels; hence it is a continuous and dynamic process (UK Ministry of Defence, 2011).

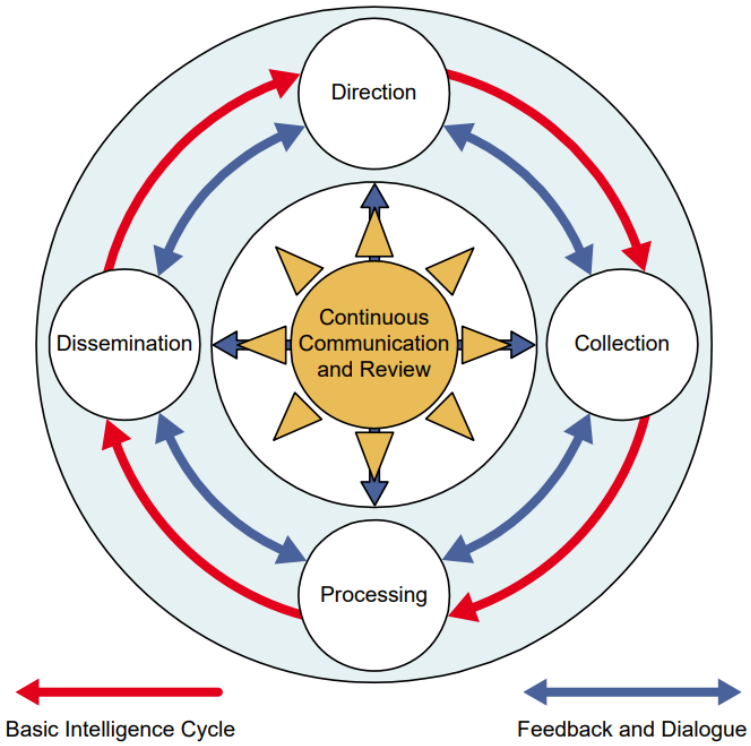


Figure 2.3: An example of the intelligence cycle from UK Ministry of Defence (2011, p. 54)

Although different variations exist, the intelligence cycle usually consists of at least four

stages: planning, collection, analysis, and dissemination. Figure 2.3 shows an example of how the four stages are organized according to each other and how each of the stages is essential for the final intelligence product to be of value for its receivers and users. Comparing the intelligence cycle to the previously introduced relation between data, information, and intelligence (Figure 2.1), the contruction is recognizable. The stages do not necessarily happen sequentially, and they may overlap each other depending on by whom and where it is adapted. Subsequently, it is especially important to prioritize communication and feedback during the process (Forsvaret, 2021), visualized in Figure 2.3 through both the center circle and the blue arrows in between the stages.

Adapting the definitions and descriptions from both the Norwegian Armed Forces (2021) and UK Ministry of Defence (2011), the four main stages can be understood as follows:

Planning

The planning stage lays the directions for the upcoming stages and ensures that all involved instances are on the same page regarding the process forward. An intelligence process should start with an intelligence requester having an IR. During this stage, the requester needs to establish a dialogue with someone who can provide the intelligence, being either an internal or external part of the organization. The initial IRs are often very generic; for instance: "How well-prepared are we against cyber-attacks considering our current countermeasures?". For intelligence analysts to answer this requirement, they are in need to divide it into smaller specified IRs (SIR). For example, SIRs related to this initial requirement could be "What are the threat actors relevant for our organization?", "What are the indicators of compromise (IoCs) related to cyberattacks relevant for our sector/industry?", and "How are our current security measures aligned with TTPs used by relevant threat actors?". The requirements which cannot be answered based on current possessed knowledge determine the data and information that needs to be collected during the subsequent stage (Forsvaret, 2021).

Vandepeer (2018) emphasizes the importance of question-asking during this stage of the intelligence cycle as it provides it shapes the analytic endeavor and creates the foundation for the remaining parts of the process. According to him, questions should be asked both ways between the decision-makers and the intelligence analysts. Decision-makers are naturally asking the questions they would like an answer to from the analysts; at the same time, the analysts have to make sure the question and the broader context are understood correctly. Also, questions highlight what we do not know, preventing analysts and decision-makers from working with assumptions (Vandepeer, 2018). Thus, question-asking is a valuable tool to identify knowledge gaps (what we do not know) and concretize the decision-makers' demands.

Collection

Having determined the requirements and identified knowledge gaps, the data collection can start. It is during this stage that the different intelligence disciplines – for instance, OSINT,

IMINT, HUMINT – are expressed in terms of *how* the data is obtained. Discussing OSINT, open sources will be examined in order to extract data that could be relevant to fulfill the IR. Both automated and manual processes are used during this stage to identify information sources, cross-check information and summarize findings (Pastor-Galindo et al., 2020).

Analysis

The data and information obtained during the collection must be analyzed and evaluated, which will apply the attributes differentiating information from intelligence (explained in Section 2.1.1). The stage requires intelligence analysts to evaluate the reliability and accuracy of the information, compare information and produce intelligence products. Depending on the IR, the evaluation could determine the tactical, operational, and strategic aspects of a potential threat actor. During analysis, the information must be evaluated in terms of its reliability. As this is the final stage before dissemination, the intelligence product should be associated with a sensitivity grade, such as a color from the Traffic Light Protocol (TLP). The sensitivity grade determines how the intelligence can be communicated and to whom, depending on its content.

Dissemination

Dissemination can be described as "the timely conveyance of intelligence, in an appropriate form and by any suitable means, to those who need it" (UK Ministry of Defence, 2011, p. 52), meaning the intelligence created must be communicated to the requester using a suitable method. Additionally, intelligence products should be marked with a probability degree describing the amount of probability associated with the product. The probability degree should consider both the quality of the actual intelligence product and the sources it builds upon. It is essential for the decision-makers to understand the amount of trust that should be given the intelligence product to make rightful decisions (Haugorm, 2019, p. 154). Furthermore, the intelligence product must be "in an appropriate form", meaning it must be presented such that it is both understood and usable for its receivers. For the intelligence product to serve as decision-making support, it is crucial that the product is understood and remembered correctly by the receiver (Haugorm, 2019, p. 153). To ensure correct and sufficient dissemination according to these requirements, the analyst can adapt the structure and content of the intelligence product. The intelligence product should be structured with the most important parts first, often the main conclusion or a short summary, followed by an extensive part complementing the conclusion (Haugorm, 2019, p. 153). Regarding the content, it should be adapted to suit the receiver's level of knowledge regarding that subject and contain any necessary background information.

Feedback becomes especially important approaching the dissemination stage. It is necessary for the intelligence provider to understand whether the requester is satisfied with the final product. Although reaching the end of the cycle, the process might have created new IRs, forcing the cycle to repeat itself once more (Haugorm, 2019, p. 24).

3 | Related Literature and Research

Having understood the purpose of OSINT and how it can be applied to cybersecurity in Chapter 2, this chapter presents an overview of previous studies and literature related to OSINT and cybersecurity. Relevant literature and research were collected using a semi-systematic literature review (SSLR) to reach the various research conducted within the field of OSINT. The utilization of SSLR made it possible to detect repeating themes and concepts in the literature, as well as other theoretical perspectives (Snyder, 2019), providing valuable knowledge in studying the research questions. The overall methodology of SSLR, including keyword search and literature synthesizing, is explained in detail in Section 4.3, together with the remaining research methods used in this thesis.

During the SSLR, 129 unique records were identified through database searches. After a thorough screening process, 21 studies were extracted, including six studies using alternative methods. A comprehensive list of the extracted papers is presented in Appendix A. One of the six additional studies was a literature review by Pai Yogish and Krishna Prasad (2021) to study OSINT's application in next-generation cyber security. Several of the retrieved articles in this chapter, for instance, Gibson et al. (2016) and Williams and Blum (2018), were first discovered in this literature review.

Through the SSLR, the focus lies on mapping the state-of-the-art of OSINT today from an organizational perspective, thereby elaborating on OSINT's role within CTI and how OSINT can be applied in organizations to enhance cybersecurity. It was considered relevant to highlight both advantages and challenges of OSINT to provide a nuanced and realistic representation of OSINT as a cybersecurity-enhancing tool. Moreover, the literature review would aid me as a researcher in embedding the thesis in the research field and understanding where my work could provide new knowledge (Hennink et al., 2020, p. 33). The chapter starts by mapping out the findings of the SLR using a concept-oriented approach and ends by identifying the research gaps discovered in where this thesis can be placed.

3.1 How Researchers Define OSINT as a Discipline

Analyzing the retrieved articles, it soon became apparent that researchers are debating on the definition of OSINT and, thereby, what OSINT as a concept means. Even within the

Intelligence Community, which has been involved with OSINT for over 50 years, the definition of OSINT is still being debated as the rise of social media has complicated the situation both in terms of methods and sources (Williams & Blum, 2018). Hence, the following section provides insight into how researchers have viewed OSINT and its application to cybersecurity over the last few years and how this can aid in a broader understanding of how OSINT can provide value. Despite being minor differences in the definition of OSINT among all the authors, it visualizes the difficulty of understanding the concept in terms of organizational cybersecurity and how to best implement it, as the perception of a concept is naturally reflected by examining how it is defined.

3.1.1 Definitions of OSINT

As elaborated in Chapter 2, the definition of intelligence and OSINT vary in terms of where it is applied and for what purpose. Similarly, it was discovered that the definition varied greatly in the retrieved papers. One can distinguish between the authors describing OSINT as a product and those describing it as a process. Some authors define OSINT as simply being publicly available information and emphasize that it must be required using legal methods, i.e., without privacy or copyright violations (Hassan & Hijazi, 2018). Williams and Blum (2018) similarly defines OSINT as an intelligence product but underlines that OSINT is collected, exploited, and disseminated public information assessed on time to suit a selected audience for a specific purpose, i.e., the IR.

Others define OSINT to be something more than just an information product, but explain it as being a process consisting of both collection, processing, and correlation of data from open sources that will aid in expanding the knowledge about the target, and thereby continuously getting closer to the final goal (Melshiyan & Dushkin, 2022; Pastor-Galindo et al., 2020). Similarly, Abdullah et al. (2021) refers to a NATO definition that emphasizes that OSINT is "[...] material that has been purposely found, discriminated against, distilled, and disseminated [...] to resolve a problem". Both definitions are clear examples of how OSINT should be guided by a goal or a problem – IR – it is entitled to solve. The definition of an IR is an essential part of intelligence processes as it is the fundamental ground for all involved in the process to understand what the OSINT is supposed to bring to the organization in the first place.

Some of the definitions touch upon whether leaked documents should be considered OSINT or not. One definition found in the literature defines that OSINT must originate from "[...] open sources and publicly available data from unclassified, non-secret sources" (Fleisher,2008; Koops et al.,2013 cited in Tabatabaei and Wells (2016, p. 214)), hence; specifying that OSINT could never originate from leaked documents. On the contrary, Hassan and Hijazi (2018) states that, in fact, OSINT can be considered to include leaked documents, like the documents from WikiLeaks, and that this category of OSINT is considered nOSINT. The paper by Tabatabaei and Wells (2016) defines that OSINT must originate from "[...] open

sources and publicly available data from unclassified, non-secret sources". Hassan and Hijazi (2018) means this is nOSINT and that intelligence considers all sources regardless of their legal accessibility.

For the rest of this thesis, the definition from Section 2.3 is applied. However, the numerous definitions and descriptions of what OSINT is and is not among the retrieved papers underline the importance of defining OSINT within one's organization. How one defines OSINT will likely also be reflected in how it is being adopted into the organization, thereby influencing how the organization extracts value from it.

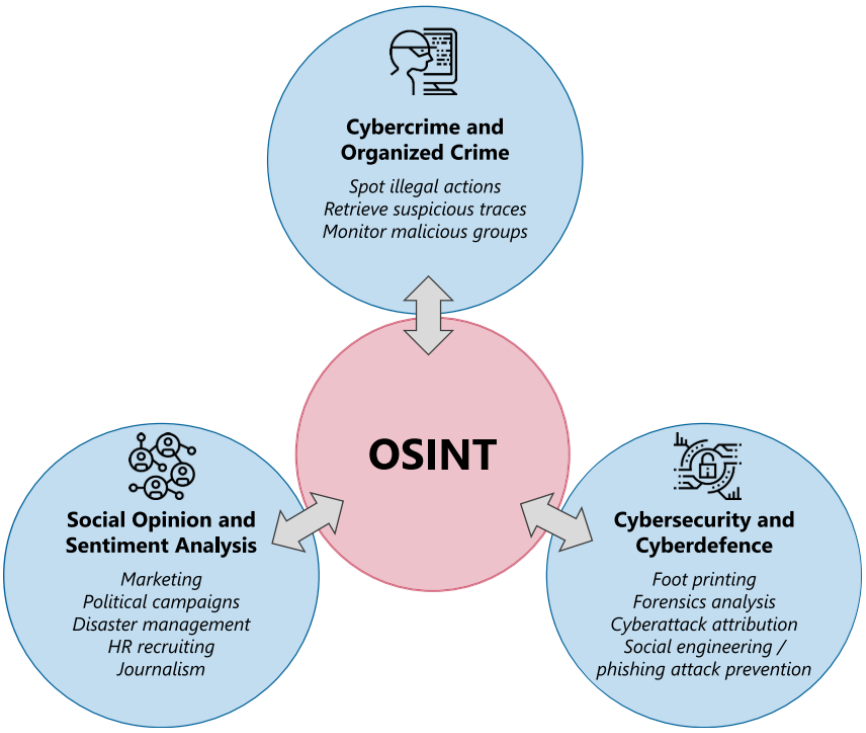


Figure 3.1: OSINT use cases presented by Pastor-Galindo et al. (2020, p. 10283)

3.1.2 Utilization of OSINT

Contributing to the comprehension of OSINT theory and how it can provide value for its users, Pastor-Galindo et al. (2020) identifies three prominent use cases of OSINT. Presented in Figure 3.1, the differentiation by Pastor-Galindo et al. can aid in understanding the various ways OSINT can be applied and underlines the importance of distinguishing between the use cases. Pastor-Galindo et al. choose to differentiate between OSINT for cybercrime and organized crime and cybersecurity and cyber defense. Whereas the former refers to OSINT usage for detecting criminal intentions and illegal actions on the Internet (also known as digital forensics), the latter relates its usage during analysis and correlations of cyber attack attempts and to increase cybersecurity posture. The third use case refers to using online services to detect social opinions of, for instance, one's organization, trademark, or service,

which will aid in marketing settings. This third use case is out of scope for this thesis, which also underlines the importance of distinguishing between OSINT use cases during the literature review.

3.2 Motivation for Applying OSINT

Recalling the definitions from Section 2.1.2, intelligence acquisition happens due to an objective directed by someone who requires that information. Thus, the organization should consider the underlying motivation before implementing an intelligence capability. The importance of considering the motivational choice was emphasized during the SSLR as many researchers stated the advantages and incentives of using OSINT for cyber defense. A summary of the motivational aspects discussed in this section is presented in Table 3.1.

Motivational factors	Challenges
Gain knowledge about the cyber threat landscape	Without suited mechanisms, knowledge, and experience, one can encounter information overload
Increase situational awareness and support decision-making processes	False information is shared, and information must be carefully analyzed to determine reliability and validity
Aid in the creation of tailored security countermeasures to prevent cyber incidents	The information shared is unstructured, and it can be challenging to see the whole picture

Table 3.1: Summary of motivational factors and challenges with OSINT identified through the literature review

Improve knowledge of the cyber threat landscape As modern warfare has moved much from the physical to digital space, malicious actions performed within cyberspace can cause direct physical consequences for those victimized. Due to the enormous consequences one can face, it is beneficial for organizations to improve their knowledge about cybersecurity to increase resilience. The number one benefit of OSINT is, as the name states, that it is freely open and available to everyone with an Internet connection. Consisting of immeasurable amounts of data and increasing daily, OSINT as an information retrieval capability greatly benefits from the constant expansion of the Internet (Pastor-Galindo et al., 2020). Using OSINT can thus provide organizations with information on many cyber-related themes covering numerous organizational sectors. As organizations constantly search for the best way to mitigate cyberattacks potentially damaging their daily operations, extracting information about cyber adversaries through publicly available information is considered a fundamental approach (Tabatabaei & Wells, 2016). Thus, organizations are encouraged to take advantage of OSINT's availability and acquire the necessary skills to retrieve information through open sources (Hayes & Cappa, 2018).

As one can understand, using open source in the creation of intelligence can aid an organization in creating an accurate picture of the cyber landscape regarding an attacker's motives, strategy, and techniques. The skills and knowledge retrieved from OSINT can serve a purpose to organizations in mainly two ways, according to the literature: it can aid organizations in protecting themselves against cyber-attacks and in detecting abnormalities by possessing skills and knowledge.

Enhance preparedness Tundis et al. (2022) claims that by accessing openly available information, organizations can gather a more coherent understanding of the threat landscape and the techniques and tools used by cyber adversaries. The importance of this is backed by Crowe et al. (2021), which emphasizes the need to constantly gain knowledge about the threat landscape in the never-ending race between threats and defenders. As described in Section 2.2, knowledge from CTI about cyber adversaries can be divided into three levels: tactical (what); operational (how, where); and strategic (who, why). The implementation and utilization of OSINT within organizations can aid in approaching all these three levels by providing information such as who initiated the attack, the motive, the tools used, consequences, and resources involved (Lande & Shnurko-Tabakova, 2019). Gaining a coherent understanding is a powerful tool against cybercrime, not only because it aids in identifying current vulnerabilities in one's organization but also because it increases the ability to prepare and protect against potential threats. Using OSINT can provide organizations with relevant and accurate information on cyber adversaries, aiding in creating a thorough understanding of the current cyber situation.

Provide cyber situational awareness During a potential cyber attack, time is precious, and decisions must be made with the deepest precaution. In such cases, a correct situational understanding becomes handy and can aid in making the best decisions. Having generated an understanding before a potential cyber attack can be valuable, as in the heat of the moment, there is a constant race between the defenders and the threats where knowledge becomes valuable (Crowe et al., 2021). Connected with the ability to be prepared for a potential cyber attack, Crowe et al. (2021, p. 233) introduces the concept *cyber situational awareness as* (CSA) as "[...] collecting and analyzing data from various sources to provide security analysts with precise information for decision-making about potential security threats". CSA is a subset of situational awareness (SA), whose original definition was made by Endsley (1988). According to Endsley, SA refers to the ability to consider the elements in the current situation, comprehend it, and thereby use the gained knowledge to project future status. In a cyber context, CSA can be understood as cyber defenders' ability to use pre-gained knowledge to make suited decisions (Crowe et al., 2021). Having experience with how early warning signs detected through OSINT can develop into actual cyber incidents can then aid in formulating and integrating sufficient countermeasures before the warning signs escalate. Understanding the importance of obtaining cyber situational awareness for decision-making underlines the

importance of using accurate and relevant information when gathering knowledge on the cybersecurity threat landscape. Instead of implementing countermeasures for every thinkable vulnerability, one can use CTI, and thereby OSINT, to support decision-making, improving the defense capabilities (Tundis et al., 2022).

Shift from reactive to proactive In their efforts to encounter the many cyber threats, organizational security has focused on enhancing readiness. Shin and Lowry (2020) argues that this approach is not suited to dealing with the increasing sophistication of cyber-attacks and compares it to the prevention paradigm by Baskerville et al. (2014), which assumes that threats are persistent and measurable and that there is a persistent relationship between threats and controls. Adopting this defense approach makes organizational security reactive and static when facing dynamic and sophisticated threats and threat actors. Thus, Shin and Lowry (2020) argues that organizations must instead change to meet Baskerville et al. (2014)'s response paradigm, aiding them in becoming more reactive and adopting countermeasures to meet the dynamic threats. Through the change from reactive to proactive, OSINT can be applied to access information that can aid the organization in acquiring intelligence to support strategic decisions. Gibson (2016) emphasizes that also OSINT can be applied either reactive or proactive: either a cyber incident is being identified, and the intelligence process starts to gather more information about the incident, or the intelligence product has revealed interesting information about a potential cyber incident and guides the subsequent investigation.

Detect abnormalities As discussed earlier, using OSINT within an organization can aid in obtaining a better CSA of the situation surrounding the organization. Not only would increasing CSA aid the organization in implementing suitable security measures, but it would also aid in detecting early signs of abnormalities within the organization's digital systems. Due to the wide variety of cyber attackers and their methods, gaining knowledge about the threat situation before a potential attack is very beneficial (Crowe et al., 2021) as one can identify and recognize the attack patterns and tools used by known perpetrators. By using open sources to gather information about potential early signs of an attack, the security professionals are using their obtained CSA to understand easier the abnormalities which could signify a cyber incident Tundis et al. (2022). That could be information like potential threat campaigns or new vulnerabilities which threat actors could exploit. Using OSINT would also benefit digital forensics during a cyber attack, providing valuable knowledge in detecting and tracking the threat actor's routes within the compromised system (Qusef & Alkilani, 2022).

3.3 Potential Challenges

The retrieved papers point to several challenges or disadvantages of using OSINT, which will likely influence the amount of value extracted by its consumer. Of the challenges mentioned

in the literature, the aspect of information overload, information reliability, dealing with unstructured information, connecting information, and considering time sensitivity was repeated and are subsequently presented here. A summary of the challenges discussed in this section is shown in Table 3.1.

Information overload One of the major challenges of using OSINT is the possibility of information overload due to the rapidly increasing publication of available information online. Aided by the rise of social media during the beginning of the 2000s, it has been a massive increase in information sharing among individuals online. The information which before was published by trustworthy newspapers or institutions is now being shared uncontrollably by everyone. The changed nature of information sharing has made both the collection and analysis of information more challenging as the trustworthiness and reliability of information can no longer be taken for granted (Tabatabaei & Wells, 2016). Glassman and Kang (2012) presents the rise of Wikipedia – being one of the most used online encyclopedias – as an example of how peoples' interaction with online information sharing makes us question the reliability of the information, as fluid and non-exhaustive information is hard to trust. A lot has happened since Glassman's reflections over ten years ago, and the evaluation of information reliability has not become less important than it was then.

Information reliability Evaluating information reliability is critical to intelligence, as an organization's security could be at risk. Using open source information for intelligence purposes, assessing its authority and trustworthiness is essential for successful usage (Pastor-Galindo et al., 2020). However, the analysis can be time-consuming as the intelligence analyst spends significant time on data wrangling, meaning collecting the correct data, converting it, fusing it, extracting and aggregating information (Gibson, 2016). As correct information is mixed with incorrect information, determining the reliability of information is a time-consuming process (Hwang et al., 2022). Hence, effective methods should be applied as the information must be verified thoroughly by defined methods to determine trustworthiness (Hassan & Hijazi, 2018).

Researchers propose various strategies for encountering the challenge of information reliability. One method is adopting automated tools to facilitate the evaluation process where information streams are provided to the consumer with an increased probability of reliability based on it being compared to several information sources (Hassan & Hijazi, 2018). Despite using automated tools for information comparison, the information should still be analyzed using human efforts. This could be done by applying methods of source criticism, describing how some sources are considered to have higher credibility than others due to the source's origin (Gibson et al., 2016). For instance, one assigns more credibility to information published by well-known newspapers than information shared by an anonymous Twitter account Pastor-Galindo et al. (2020).

One could also use manual methods by accessing multiple sites to gather insight. A study by

Alves et al. (2020) confirms that one should use several information sources as they are likely to complement each other and ensure that the receiver is covering a larger area compared to only using one source.

Unstructured information Until this point, information has been discussed as a whole, but assessing information within OSINT can take many different forms. Gibson et al. (2016) discusses the challenge of assessing and analyzing the information to understand the whole picture, as understanding the relationships between actions and threat actors and identifying methods can be time-consuming. Information can be text from social media, news media, literature, or other publications, as gray literature (Williams & Blum, 2018). The vast differentiation between the information form causes a challenge in structuring it, as information on the Internet is very disorganized (Pastor-Galindo et al., 2020). Consequently, the unstructured data may yield unreliable results using automated processes and algorithms (Johnsen & Franke, 2019). Johnsen and Franke (2019) suggests the usage of exhaustive data cleaning until reaching a state where one is left with a result containing coherent topics and information. Data filtering processes remain challenging for OSINT practitioners as it is both a time-consuming and crucial part of the information collection (Hwang et al., 2022).

3.4 Comparing OSINT Intelligence Models

Understanding the challenges of OSINT from Section 3.3, turning data into actionable intelligence can be a complex task. Due to the steps essential to transforming data to intelligence, many visualize the intelligence process through different models. During the literature review process, six different representations of intelligence processes and cycle variations were found, some tailored explicitly to OSINT and some framing CTI more generally. Similar for all is their presence in articles relating to the usage of OSINT, so the cycles are interpreted as being relevant when discussing OSINT processes. Table 3.2 summarizes and compare the models in terms of their structure and included stages, whereas they are presented in their entirety in Appendix B. Due to their compositions' varying shapes and construction and with various amounts of additional information, the table only extracts the information regarding their primary design for comparison. Comparing the models – focusing on their overall composition and non-technical aspects – revealed what the authors evaluated as crucial steps that should be included for successful OSINT leverage.

Naming of the stages In the model by Williams and Blum (2018), the stages originally known as *analysis* and *dissemination* have consciously been renamed to *exploitation* and *production* to differentiate the model from all-source production to OSINT production. Gibson (2016) has also included additional steps to the usual four steps, that being *processing* and *feedback*. In the description of her model, Gibson explains how most of the information extracted from open sources exists in various forms – as also discussed in Section 3.3 – and;

Figure	First step(s)	Second step	Third step	Fourth step	Last step(s)
Figure B.1 by Hwang et al. (2022)	Identify sources of purpose	Data collection (active harvesting, passive harvesting)	Processing	Analysis	Reporting
Figure B.2 by Tabatabaei and Wells (2016)	N/A	Data collection	Data enrichment	Data analysis	Dissemination
Figure B.3 by Williams and Blum (2018)	N/A	Collection (acquisition and retention)	Processing (translation and aggregation)	Exploitation (contextualizing and authentication)	Production (Dissemination and classification)
Figure B.4 by Gibson (2016)	Direction	Collection	Processing	Analysis	Dissemination/ Feedback
Figure B.5 by Samtani et al. (2020)	Intelligence planning and strategy	Data Collection and aggregation	N/A	Threat Analytics	Intelligence usage and dissemination
Figure B.6 by Lee and Shon (2016)	Establishment of OSINT plan & Preparation of OSINT	Collecting information from open sources	N/A	Generating security intelligence	N/A

Table 3.2: Comparison of intelligence models from the SSLR. The models can be viewed in Appendix B.

hence, requires much time to be processed. Aspects such as the semantics of the language, spelling errors, and synonyms need to be considered during the analysis.

Static or dynamic The paper by Williams and Blum (2018) discusses the lack of a defined methodology for OSINT and presents their take on the OSINT operations cycle. It is emphasized how *processsing* and *exploitation* not necessarily happens sequentially, as visualized in the model, but in parallel. The distinction between how the process often is represented (static) and how it is performed (dynamic) is one of the main challenges of modeling the OSINT process, as reflected by Williams and Blum. Despite the more dynamic model presented by Lee and Shon (2016) and the linear model by Hwang et al. (2022), the four other models are designed as cycles where all steps are sequentially following each other. The cyclic representations embrace the circular process of intelligence where one is constantly looking for new information that can aid in understanding the threat landscape and support decision-making. Hwang et al. (2022) have adopted a dynamic twist to their model by adding an arrow from *analysis* to *data collection*, symbolizing the potential need to retrieve additional information when needed.

Technical or organizational focus The cycles represent the researchers' perceptions of the necessary focus during OSINT application and usage. The model presented by Gibson (2016) has sacrificed an entire step to focus on the feedback session, where the intelligence collected through the previous steps is evaluated against the original IR determined in the

direction step. Gibson (2016, p. 71) states that an intelligence cycle should move "[...] from the identification of the intelligence required through the data collection and analysis phases to the feedback phase, where the intelligence collected is measured against the initial requirements, and consequently new requirements are identified". Emphasizing the continuity of the intelligence cycle, the *feedback* stage provides additional guidance regarding the next cycle iteration (Gibson, 2016). Tabatabaei and Wells (2016) does also include *feedback*, but the model lacks explanation regarding the motivation for including this stage, compared to the information provided by Gibson (2016).

Establishing IRs As visualized in column "First step" in Table 3.2, four of six models start by establishing the IRs before moving on to the collection phase. The stage before *collection* operates under many names across the different models: intelligence planning, strategy, direction, and the establishment of OSINT plan. Still, the emphasized need to establish a direction for the upcoming OSINT process is common for them all. As described in the model by Samtani et al. (2020), the planning stage should include identifying the organization's assets and vulnerabilities, which would aid in establishing the IRs. Having a clear idea of the IRs would facilitate the performance of the upcoming stages, as visualized in the model by Lee and Shon (2016), which has included an arrow between establishing an OSINT plan and preparing OSINT.

Evaluating existing knowledge Through the six models, the model presented by Lee and Shon (2016) is the only one describing the usage of an intelligence repository (knowledge base) where already established knowledge is gathered. The model visualizes how newly acquired knowledge would be added to the intelligence repository after it has been analyzed and how the repository is continuously updated. The paper by Lee and Shon (2016) lacks to describe how the intelligence repository is administrated and examples of how such an intelligence repository could look in terms of software solutions or platforms. Regardless of the lack of description of practical implementation, the usage of an intelligence repository is a unique visualization of how the intelligence process can be modeled.

3.5 Adopting CTI into a Commercial Organization

There was a lack of research papers describing adopting an OSINT capability in a non-military organization to enhance its cybersecurity posture. Due to the desire to adopt findings from an actual case study, reflections and results from a study conducted on CTI implementation within a commercial organization have been included. As OSINT, within the cybersecurity context, is an intelligence capability within CTI, the findings can also be adopted into the OSINT context for this thesis. Within the study, Kotsias et al. (2022) discovered four major problems with the current usage of CTI within the organization: "CTI was difficult to consume from the recipients' perspective (Problem 1); CTI did not reach all recipients, e.g., executive consumers (Problem 2); CTI had operational utility, but lacked strategic utility

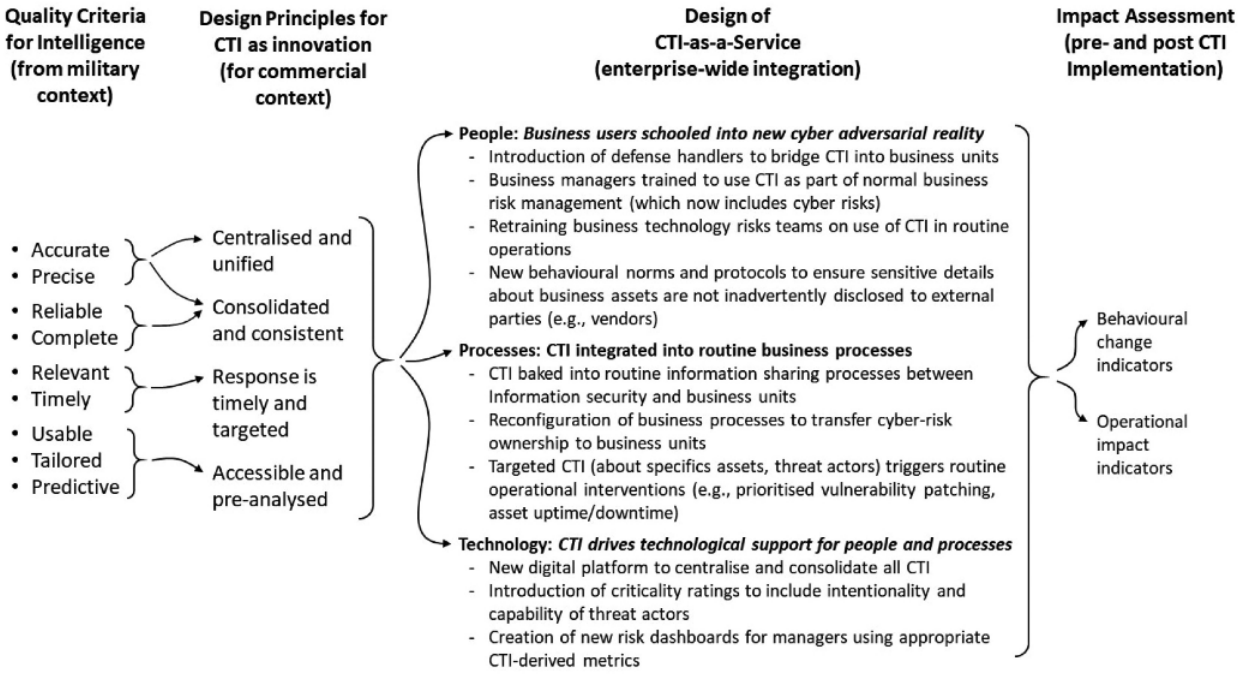


Figure 3.2: The design principles of CTI-as-a-service from Kotsias et al. (2022, p. 9)

(Problem 3); and, CTI consumption was driven by obligation, not as a business imperative (Problem 4)" (Kotsias et al., 2022, p. 8). The study resulted in the design principles of CTI-as-a-service, presented in Figure 3.2. The design principles embrace the quality criteria of intelligence from the military context (as described in Chapter 2) but adopt them into the commercial context by adding the design principles in the second column from the right. Kotsias et al. specifies how the design principles must be specified, systematized, and standardized to contain the military principles in the first column.

Stating how military organizations have long understood the importance of acquiring threat intelligence to increase their defense mechanisms, Kotsias et al. demonstrates how the military disciplines can indeed be integrated into a non-military organization. Kotsias et al. (2022, p. 10) describes that "[...] without CTI, the firm is unaware of the who, what, when, how, and why of the attack and the threat actors. As a result, their response can only be reactive, and they must assume the worst-case scenario.". Findings from the study showed how *mutual understanding*, *trust*, and *respect* were central aspects during the implementation of CTI to provide an organizational relationship, e.g., by the usage of briefings and communication. For instance, Kotsias et al. observed that the environment using CTI must accept and understand it as a prerequisite for CTI to provide value. As cyber adversaries are hard to get hold of, the practitioners within the organization struggled to understand how to apply CTI information into action and respond to speculative or weak signals. The fear of crying wolf by acting on a false alarm was high as it largely affected the relationship between the business and IT.

Despite not discussing the aspects regarding using open sources for intelligence purposes, findings from Kotsias et al. (2022) are highly applicable to this thesis. The study shows

how military intelligence concepts also can be applied in other types of organizations with adoptions tailored to a non-military context. The adaptation of CTI did provide significantly increased value within the organization in terms of increased situational awareness among the employees and proactive defense behavior.

3.6 Summary of Literature Findings and Research Gaps

To summarize, the conduction of the SSLR aided in detecting the themes discussed within the research landscape of OSINT as a CTI capability. Using OSINT can aid an organization in adopting countermeasures against relevant threat actors tailored to the TTPs they use to gain access to an organization's systems and cause potential damage. But, as elaborated in this chapter, in implementing an OSINT process, an organization will likely encounter several challenges that can prevent them from leveraging value from OSINT as a cybersecurity-enhancing tool. The most common topics in the literature are:

- **Definitions:** It was discovered a variety of OSINT definitions among the papers, emphasizing how OSINT is indeed understood and used differently among practitioners.
- **Implementation and usage:** During the search for literature, it was found that most papers concentrated on the implementation and usage of OSINT from a technical perspective, focusing on third-party vendors and architectural considerations.
- **Advantages and challenges of OSINT:** Across many papers, both advantages and disadvantages of OSINT were elaborated on. Still, there needed to be a description of how OSINT should be implemented to ensure that the benefits were indeed being leveraged.
- **Organizational focus:** In the search to understand the acquisition of OSINT from an organizational perspective, several intelligence models were compared to learn how the OSINT process should be structured. Few of the models contained exhaustive information regarding how the intelligence process should be performed from an organizational point of view.

The SSLR also identified some research gaps by not describing the self-reflection and consideration the organizations must perform during the process to ensure coherence in using OSINT. Shin and Lowry (2020) remarks on this specific research gap, that regardless of CTI's raised popularity, there has been a lack of focus on the behavioral and organizational aspects of CTI implementation. This can also be carried over to the usage of OSINT, being treated as a subsection of the CTI umbrella. Hence, this thesis aims to explore how OSINT should be implemented – from an organizational process point of view – to ensure that the highlighted advantages are being transferred into the organization and that they are experiencing an enhanced cybersecurity posture.

4 | Research Methodology

This chapter explains this thesis' several complementary research methods and approaches. As the conduction of the thesis followed the qualitative research cycle (QRC) from Hennink et al. (2020), this chapter is organized accordingly. The presents the thesis research design, data collection, and analysis. Moreover, the chapter describes the method for literature review and presents the deductive conceptual framework derived from literature and theory. Lastly, limitations and ethical considerations are discussed.

4.1 Research Approach

Before creating the research question for this thesis, the study's objectives were mapped out. The objectives were twofold:

- I wanted to understand how OSINT is currently used within non-military institutions and study how the utilization aligned with intelligence theory regarding implementation, planning, and utilization.
- I wanted to use the knowledge gathered from theory and the empirical evidence to map out my understanding of how the discovered concepts were interrelated and how an organization's approach to the concepts would affect the leveraged value of OSINT as a CTI capability.

The objectives of this study were both exploratory and descriptive: the state-of-the-art of OSINT within cybersecurity had to be understood before being able to understand how OSINT should be used to gain value according to theory and data collection through interviews.

When deciding upon the research approach for this thesis, two things became clear during that process: firstly, it was essential to understand people's honest thoughts, feelings, and experiences with using OSINT within the organization; and secondly, asking follow-up questions to gather an exhaustive understanding of their answers was needed. Thus, I decided to use a qualitative research method. The definition by Hennink et al. (2020) of qualitative research was considered well fitting for this study:

> "[...] qualitative research is an approach that allows you to examine people's experiences in detail by using a specific set of research methods such as in-depth

> interviews, focus group discussion, observation, content analysis, visual methods, and life histories or biographies. [...] Perhaps one of the most distinctive features of qualitative research is that the approach allows you to identify issues from the perspective of your study participants [...]." (Hennink et al., 2020, p. 10)

Hence, using a qualitative research approach would allow for gathering more detailed information on each participant compared to a quantitative research approach. Moreover, a qualitative approach is suitable for examining research questions formulated with *why* or *how* as the approach seeks to understand more complex issues, processes, and people's behavior (Hennink et al., 2020, pp. 10–16).

4.2 Research Design

Before presenting the research design and methodologies used in this thesis, defining the two concepts and underlining their different meanings within a research process is essential. While *methodology* can be referred to as the principles, procedures, and practices that guide the research, *research design* can be seen as the overall description of how the research question is to be addressed (Kazdin, 1992, 2003a cited in Marczyk et al., 2005). Hence, the research design is presented to visually and textually describe the process followed throughout the research process. For this matter, the qualitative research cycle (QRC) presented by Hennink et al. in their book on qualitative research methods (Hennink et al., 2020) was adopted. The cycle, viewed in Figure 4.1, is divided into smaller cycles – components – describing the three main parts of a research plan: the design, the data collection, and the analysis. Using the QRC throughout the creation of the thesis provided theoretical guidance and academic weight to the decisions made along the way.

As one is planning and designing a research study, many decisions follow, thus; influencing both previous and future plans. The cyclic representation by Hennink et al. through the QRC is found by me to be an understandable and accurate representation of how the process can be both systematic and dynamic at the same time. Nearly in all types of research, the researcher returns to earlier parts of the process to perform modifications to ensure the final product is coherent throughout all its parts. As an example, the research question of this particular thesis has been modified continuously through the process as new knowledge and discoveries have been adopted. Not only is the adjustment of the research question necessary for the thesis to stay coherent, but it also visualizes the continuous learning process of writing a thesis as one participates in a steep learning curve.

Moreover, the QRC aids in assessing the quality of the qualitative research process in this thesis through three principles: coherence, inductive and deductive reasoning, and reflexivity (Hennink et al., 2020, p. 323). Firstly, coherence is assessed by ensuring that all tasks performed during the process are interlinked and aiding in the answering of the overall research question. Secondly, deductive reasoning is implemented to ensure the data collection

is guided based on theoretical concepts and shaped into inductive inferences. Thirdly, reflexivity is assessed by being transparent in the research process, including adjustments and actions taken to provide data quality and a sound research result.

The QRC in Figure 4.1 will be used throughout the entire thesis as a guideline for the research process. Thus, it will be referenced when approaching new components and the corresponding tasks. Overall, the tasks of the design cycle are described in Chapter 1 and 3; the data collection cycle in Chapter 4; and the analytic cycle in Chapter 5 and 6.

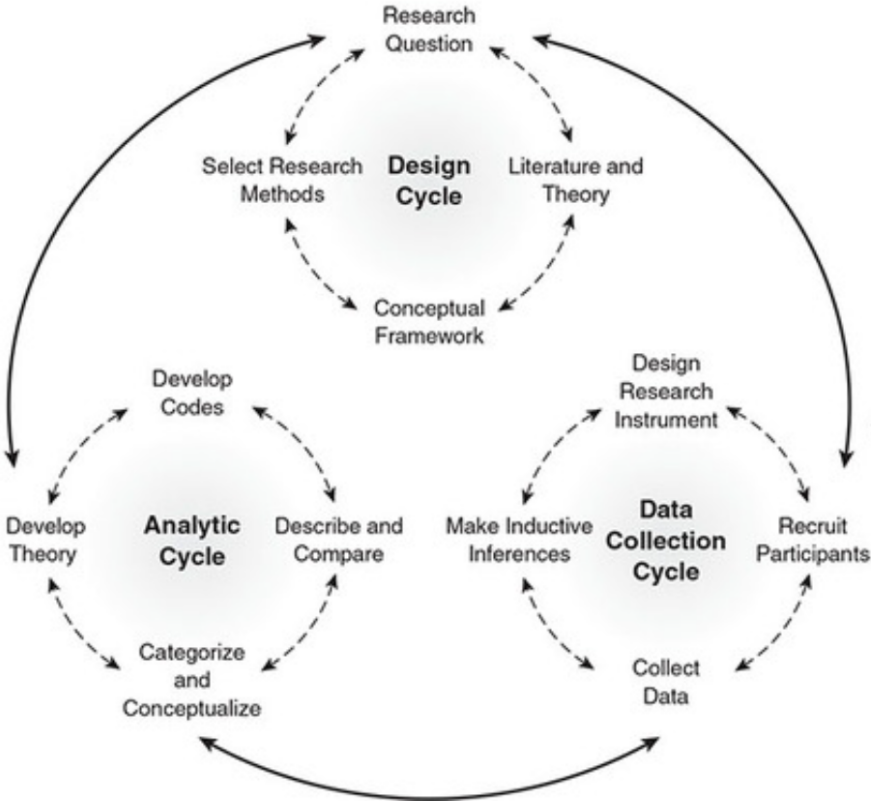


Figure 4.1: The qualitative research cycle (QRC) by Hennink et al. (2020, p. 4)

4.3 Semi-Systematic Literature Review (SSLR)

Figure 4.1 shows the importance of considering literature and theory upon approaching new research areas. Likewise, in this thesis, it was necessary to study existing research to discover the state-of-the-art within the field of OSINT (Rowe, 2014). By collecting and analyzing relevant research, one can study prior knowledge, compare findings and identify potential research gaps, which aids in providing the theoretical foundation of the thesis. Hence, a literature review was conducted to contribute to the development of the theoretical foundation and conceptual framework (Chapter 2), the research findings (Chapter 5), and the discussion (Chapter 6).

Rowe (2014, p. 243) describes a literature review as a process that "[...] synthesizes past

knowledge on a topic or domain of interest, identifies important biases and knowledge gaps in the literature, and proposes corresponding future research directions". As the literature review aimed to map out the different perspectives of prior research, in addition to conceptualizing and synthesizing the state-of-the-art, I chose to conduct a semi-systematic literature review (SSLR). Being similar to a traditional systematic literature review (SLR), the SSLR is well-suited when the discipline has been studied by various groups of researchers across various fields over time, which hinders the conduction of a complete systematic process (Snyder, 2019). That is to say, as it is simply challenging to cover all potential relevant titles for a complex and diverse field such as OSINT, – being tackled in both cyber and non-cyber-related fields by both military, governmental, private, and public institutions – the SSLR approach aided in synthesizing the current state of knowledge and understand the overall themes and perspectives (Snyder, 2019).

As with any other systematic literature review process, the SSLR should follow a strategy. Snyder (2019) emphasizes that since the SSLR covers large concepts across research fields, the process must be transparent in order for readers to evaluate the methods used to carry out the final result. Moreover, a systematic approach would also ensure diversity in sources consulted (Webster & Watson, 2002) and allow other researchers to reproduce our analysis (Okoli & Schabram, 2010). Therefore, it was necessary to adopt an SLR framework to ensure the quality of the literature review throughout the whole process. Scholars have proposed various approaches and procedures for the conduction of SLR. However, I adopted a systematic guide for literature review within the information systems research proposed by Okoli and Schabram (2010). The guide has eight essential steps with a corresponding explanation from the beginning of the review process until the end. The eight steps of Okoli & Schabram's guide are:

1. *Purpose of the literature review:* Identify the purpose and goals of the review.
2. *Protocol and training:* A detailed procedure for conducting the review.
3. *Searching for the literature:* A detailed description of the literature search and justifications.
4. *Practical screen:* Equal to 'screening for inclusion,' i.e., which literature was included in the review and why.
5. *Quality appraisal:* Equal to 'screening for exclusion,' i.e., which literature was excluded and why.
6. *Data extraction:* Description of how relevant data were extracted from the literature.
7. *Synthesis of studies*: Combining the facts from the literature into a systematic presentation.
8. *Writing the review:* Reporting the literature review process in sufficient detail.

The eight steps are categorized into four categories: planning, selection, extraction, and exclusion – which correlate to the chart describing the actual process of this particular review in Figure 4.2. Steps 1 and 2 are already explained in this chapter's introduction and the present section; hence the remaining parts of Section 4.3 will describe the conduction of the literature review from steps 3 to 7.

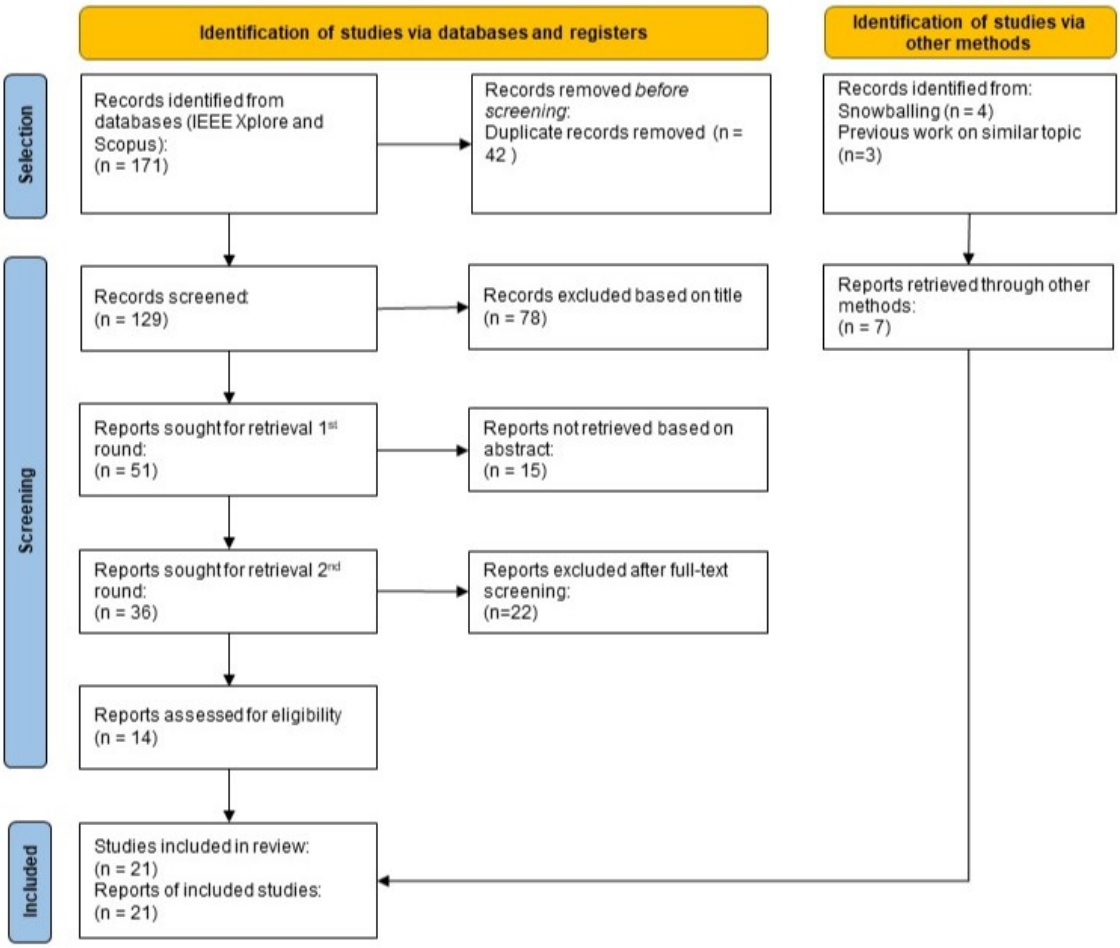


Figure 4.2: PRISMA flow diagram, adopted from Page et al. (2021), visualizing the SSLR process

Searching for the literature During the literature search, I used digital libraries to create customized search queries to be executed in the database searches. The literature search began with several test searches to understand the amount of available literature and how broad or narrow the search query should be to receive a sufficient amount of records. I tried several online databases before using Scopus and IEEE Xplore as my two primary online databases in the literature search. AIS eLibrary, a major database within information systems research, was also used but did not return any usable articles discussing OSINT.

The boolean operators *AND* and *OR* were used to target more records using related words. As can be seen from the search queries below, the words *osint*, *open source intelligence*, and *open source information* were used to target records concentrating on this particular type of threat intelligence. Further, *cyber defense*, *cyber security*, *information security*, and

cybersecurity were used to ensure that the article concerned OSINT within cyber use cases (and not business intelligence, further elaborated in Section 3.1.2). By using these keywords actively within the search queries, I was assured that the articles retrieved concerned the use cases I was interested in.

The two search queries used during the literature search were:

IEEE Xplore: (("All Metadata":osint OR "All Metadata":"open source intelligence" OR "All Metadata ":"open source information") AND ("All Metadata":"cyber defense" OR "All Metadata":"cyber security" OR "All Metadata":"information security" OR "All Metadata": cybersecurity))

Scopus: (TITLE-ABS-KEY (osint OR "open source intelligence" OR "open source information") AND TITLE-ABS-KEY ("cyber defense" OR "cyber security" OR cybersecurity OR "information security"))

The result from the literature search performing the two above searches can be viewed in Figure 4.2, which maps out the entire search process. 171 records were retrieved through database searches and screened further.

Practical screen After performing the searches, all retrieved records were examined to determine their relevance using a systematic approach. This was particularly necessary as the two queries generated a total of 171 records to be examined. Subsequently, it was necessary to construct a set of rules for inclusion describing the criteria of whether a record was considered relevant or not. The criteria must be broad enough to include sufficient records but also narrow enough to include records that will help answer the research question (Okoli & Schabram, 2010).

After removing duplicates, I applied the following inclusion criteria during the examination of titles and abstracts:

- Articles describing the use, advantages, and/or challenges of using OSINT in a cyber context.
- Articles written in English.
- Articles being available and accessible online.
- Articles published within the last ten years (2013-2023). In cases where the article is particularly relevant (e.g., its main focus is OSINT in usage within non-military organizations or discusses interesting aspects of the intelligence cycle), it will be included despite its publishing date.
- Articles published in a scientific journal or proceedings of a scientific conference.

Regarding the articles' publishing date, I chose to include articles published within the last ten years to capture possible evolution or notable changes that happened over the years. As

the intelligence profession is an old profession, yet relatively new within the cybersecurity area, it was considered necessary to include everything available discussing OSINT and CTI and organizational processes over the last ten years.

Applying the inclusion criteria, 93 (= 78 irrelevant titles + 15 irrelevant abstracts) records were excluded and not considered further in the literature review.

Quality appraisal A full-text screening was performed after sorting the records by title and abstract using the practical screening criteria. Okoli and Schabram describes that the quality appraisal serves two primary purposes: to sort out the articles that do not meet the reviewer's standard and to score the methodological standard of the articles, as the quality of the final literature review depends very much on the quality of the included articles. Thus, the quality appraisal call for stricter criteria for which records to be included and which to be discarded. The process was performed by conducting a full-text screen where the record's introduction, discussion, and conclusion were the center of attention. The following exclusion criteria were applied:

- Articles concerning developing mathematical processes or technical procedures for using OSINT in a cyber context were excluded.
- Articles containing little to no explanation or elaboration of OSINT in cyber from a process or methodological perspective were excluded.

Simultaneously, as full-text screening, cited sources were examined if being mentioned in a particularly relevant part of the record. It was also remarked if relevant records from the literature search were cited in other articles with interesting and relevant topics. The technique of using a record's references and citations is referred to as backward and forward snowballing (Wohlin, 2014), where additional records are identified through these two techniques – and is an excellent technique to use in addition to regular database search (Wohlin, 2014). Following the process through Figure 4.2, the 36 remaining reports after the practical screen resulted in 14 after the full-text screening. Moreover, four studies were included based on the snowballing method, and three were included as additional studies.

Data extraction and synthesis of literature The process of extracting relevant material from each paper happened simultaneously with synthesizing the papers to create a coherent sense out of them. After performing the quality appraisal, 14 papers remained, all listed in Appendix A. These were imported into the analytic tool Nvivo, where the relevant parts of each article were coded using the codebook presented in Table 4.1. I created the codebook by knowledge acquired from the theory background from Chapter 2 and by adding additional codes as new, interesting aspects were discovered during reading. The coding helped in providing a concept-centric approach, which would serve as a basis for the presentation of the literature retrieved. The concept-centric view would prevent the literature presentation from

Codes	Files	References
Challenges	1	1
Connecting Dots	2	2
Data Filtering	4	4
Data Reliability	4	5
Data Reliability Method	1	2
Information Overload	6	9
Private Data	2	2
Time Sensitive	2	2
Definition OSINT	14	25
Method	0	0
Information Relevance	3	6
Intelligence Requirement	2	2
Proactive Or Reactive	2	2
Motivation	8	12
Available And Not Classified	1	1
Decision Making Support	1	1
Increase Cyber Defense	8	13
Info About Mal.actors	5	8
Info From Non-Mal.actors	2	3
Quality Of Info	1	1
Security Audit	2	3
Statistics Of Usage	1	1
Time-Saving	2	2
Volume Of Info	1	1
Process	3	3
Intelligence Cycle	7	11
Analysis	1	1
Dissemination	1	1
Organizational	1	1
Tools	2	2
Motivation	1	1
Twitter	4	5
Research Gap	1	3
Theories	2	2

Table 4.1: Codebook used during data extraction and synthesis of the literature. Codes marked in *italic* are sub-codes of their respective proceeding code.

only summarizing the record's content but rather compare the articles' different approaches to the concepts highlighted (Webster & Watson, 2002)

4.4 Deductive Conceptual Framework (DCF)

Following the QRC (Figure 4.1), a deductive conceptual framework (DCF) was created prior to the empirical data collection. The DCF is an aggregation of comparing the intelligence models presented in Section 3.4 and the theoretical background from Chapter 2. The DCF describes the essential steps at each stage to leverage value from an OSINT capability for cybersecurity-enhancing purposes. By visualizing the expected relationships between the concepts related to the intelligence process, the DCF provides focus and structure to the

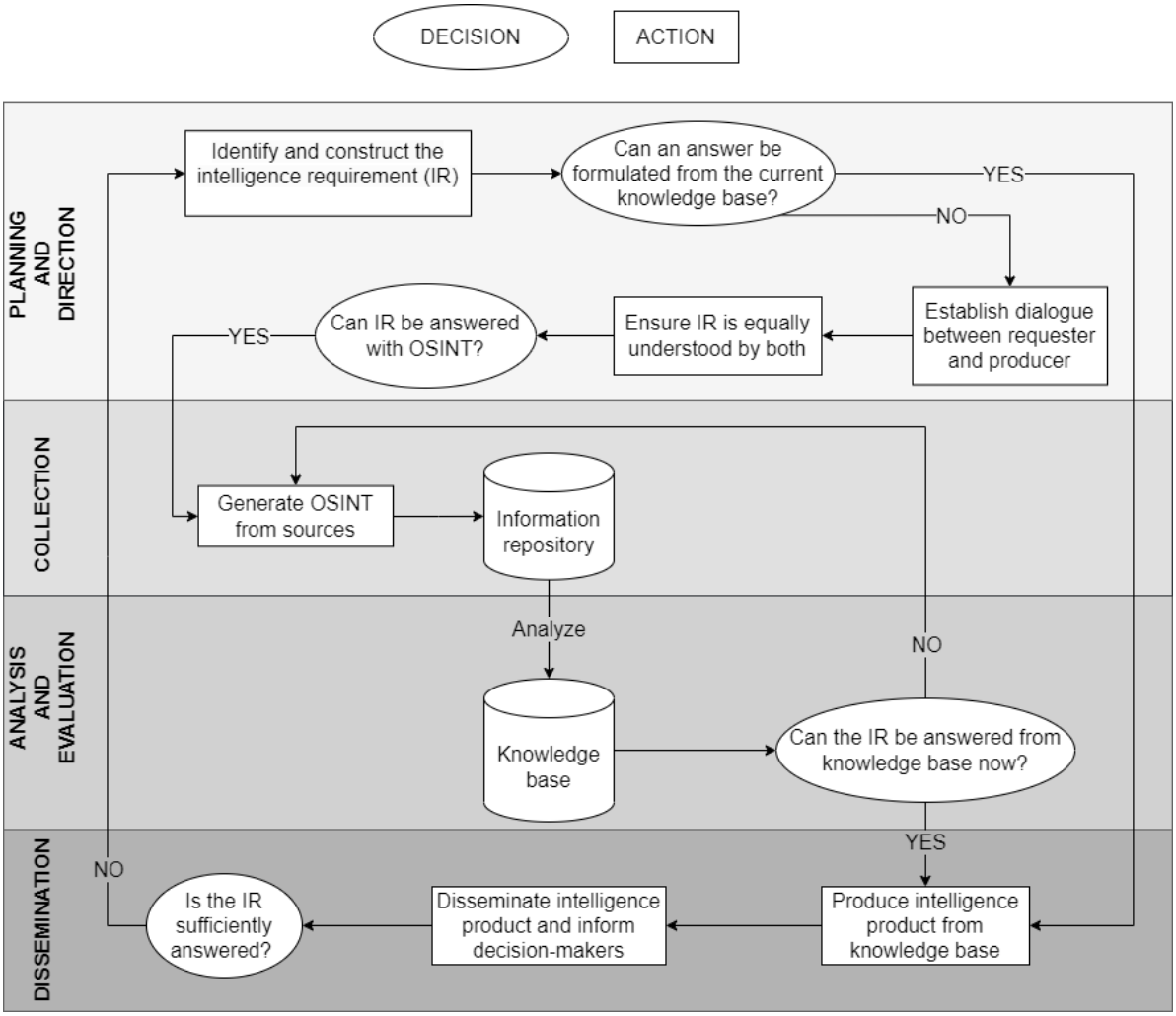


Figure 4.3: The deductive conceptual framework (DCF) created based on theory and literature

study by ensuring all concepts are explored during data collection. The model was shown in the interviews to validate the framework´s accuracy in capturing OSINT processes in the interviewees' respective organizations. Moreover, the framework was also used during data analysis to relate concepts from the transcribed interviews, e.g., different methods to perform information analysis during the stage *analysis and evaluation*.

Like many of the other models presented in Section 3.4, Figure 4.4 contains the four main stages *planning and direction*, *collection*, *analysis and evaluation*, and *dissemination*. As four of six explored intelligence models emphasized the importance of identifying the intelligence purpose and establishing an OSINT plan, the DCF begins by constructing the IR to guide the intelligence process. Further, dialogue should be established to ensure the intelligence requester and the producer understand the IR equally. As described in Section 2.3, as the different intelligence disciplines serve different purposes, one must evaluate whether OSINT is the correct discipline for that particular IR. As this framework is constructed to examine OSINT usage, a no-option is consciously left out here. Continuing from the established IR,

the DCF emphasizes the evaluation of possessed knowledge from a knowledge base, as in the intelligence model 6 by Lee and Shon (2016) (Figure B.6) and material by Forsvaret (2021). As included in both model 1 (Figure B.1) and the earlier mentioned model 6, it should be evaluated whether the analyzed information (current knowledge base) contains sufficient amounts of information or whether a new round of information collection is required. Lastly, the DCF has emphasized the necessary stages of dissemination, as all six models included variations of dissemination methods. Through the DCF, the reader is guided through the different decisions and actions needed at each stage in an OSINT process. By ensuring the intelligence product is aligned with the IR, an organization obtains material containing information that can guide them to make advocated decisions based.

4.5 Data Collection

Several qualitative data collection methods exist to derive empirical evidence for the thesis, such as interviews or observations (Marczyk et al., 2005, p. 117). As the research question aims to discover the processes of using OSINT for cybersecurity purposes in organizations, the empirical material had to be derived from multiple informants. Thus, in-depth interviews were chosen as the data collection method since being suitable when a researcher wants to obtain detailed information about a topic or ask open-ended questions (Oates, 2006, p. 187). Hennink et al., 2020, p. 116 states that in-depth interviews should contain the following:

- An interview guide as a research instrument to prompt the data collection
- A trusted relationship between the interviewer and the interviewee
- Questions asked openly and emphatically, motivating the interviewee to tell their story in an insightful way

The rest of the section describes how the abovementioned aspects were addressed during the data collection to ensure that the retrieved data was sufficient for assessing the research question.

4.5.1 Interview Methodology

As an interview's effect depends on its structure (Marczyk et al., 2005, p. 117), an interview guide was prepared beforehand containing the questions and aspects that needed to be covered during the session. The interview guide aimed to guide me as a researcher to elicit knowledge from the different participants. Following the recommendations from Hennink et al. (2020) on an interview guide's structure, the guide consisted of an introduction, opening, key, and closing questions. The interview guide is found in Appendix E.

The interview was designed as a semi-structured interview where the guide ensured that the same themes were covered in all interviews. The semi-structured approach allowed me as an interviewer to ask follow-up questions based on the interviewees' responses to clarify

or extend the interviewee's replies (Kvale, 2007a). As described in Section 4.4, the DCF was used to guide the data collection. Constructing the interview guide in accordance with the DCF assured me that the four main components of the intelligence cycle – planning, collection, analysis, and dissemination – were discussed during the interviews. The concepts were grouped due to where they overlap, and questions were formed within each group. Relevant theories, both from the systematic literature review and specific theories on the threat intelligence cycle, were used to construct the particular questions. Moreover, the framework ensured that the concepts were discussed in a logical order to prevent confusion and potentially damaged data quality (Hennink et al., 2020; Kallio et al., 2016). Hence, the DCF aided in covering the theoretical concepts needed in addition to administering the interview session.

If desired, the interviewees were offered access to the guide prior to the interview to allow them to prepare themselves. Although sharing the interview guide could influence the authenticity of the interviewee's answers to the questions, it was done due to the secrecy associated with sharing an organization's threat intelligence processes and methods. As a result, the interviewees could be assured the interview was not touching upon confidential information.

The interviewees also received and signed a consent agreement based on the template from Norsk institutt for forskningsdata (NSD; English: Norwegian Centre for Research Data), included in Appendix D. This document contained detailed information concerning the purpose of the study, why I wanted them to participate, and how the study would be performed. The document also informed the interviewees that the interview would be sound-recorded and transcribed afterward. As I would process the interviewee's personal information – like their full name, organization, and personal expressions – the document also stated the privacy concerns like the storage and usage of personal data. Through the consent agreement document, and in addition to being transparent with the purpose of the study, at the beginning of the interview, the interviewee was reminded about the thesis's scope and purpose.

As seen from 4.1, the data collection is a cyclic process where findings from one interview can be used in the following ones. When time allowed, the interviews were transcribed soon after their conduction to make inductive inferences for the following interviews. Following the guidelines from Hennink et al. (2020, p. 118), the interview guide remained essentially the same throughout all the interviews to provide consistency. However, small changes were made as I gained more knowledge during the process. I did, for example, include anonymous statements from previous interviews to ask the current interviewee about his/her opinion. In that way, I could retrieve more comparable data material, which was interesting to include in the discussion. Sometimes it also helped the interviewee understand my question by providing examples of how previous interviewees had answered, but it was done with the precaution of receiving only yes/no answers. Hence, follow-up questions asking for argumentation on why or why not my example was applicable was always in my mind during these situations.

4.5.2 Recruitment of Interview Participants

Before starting the recruitment of participants, I defined the eligibility criteria of the potential participants. I considered there to be mainly two requirements to ensure the relevance of the participants for the study:

1. The interviewee must be representing a non-military organization, e.g., not from the Norwegian Armed Forces, as a part of the study was to examine non-military organizations' usage of OSINT for cybersecurity.
2. The organization must collect information from open sources for cybersecurity purposes and not for business intelligence purposes.

Participants were required through connections at Deloitte Cyber Risk Advisory and by contacting individuals through email and LinkedIn. During the interviews, I also applied the snowballing method by asking the interviewees if they knew about additional relevant interview candidates for my thesis. By leveraging the interview participants' network within the intelligence field, I could recruit additional participants from outside my reach.

Table 4.2 presents the resulting group of interview participants. In compliance with the consent agreement presented in Section 4.5.1, all information about the participants has been anonymized to ensure their integrity. Therefore, in Table 4.2, each participant has been provided with general and unidentifiable information about their role, years in that role, and the size of their organization to provide some background information. The size of the organization is determined using *small* (up to 49 employees), *medium* (50 to 249 employees), or *large* (250 or more employees).

Pseudonym	Role	YIR (YOE)	Org. size
CTI_consultant	CTI analyst with team lead responsibility	0,5 (6)	Large
CTI_analyst_1	CTI analyst	4,5 (N/D)	Small
CTI_analyst_2	CTI analyst	12 (12)	Small
CTI_analyst_3	Principal analyst in information technology	1 (6)	Large
CTI_analyst_4	Security incident coordinator	2,5 (6,5)	Large
Cybersec_manager_1	Cybersecurity Operations Manager	0,5 (6)	Large
Cybersec_manager_2	Cybersecurity Manager with responsibility for CTI at a strategic level	1 (10)	Large
CISO_1	Cybersecurity manager with personnel responsibility (CISO)	3 (8)	Large
CISO_2	CISO	24 (N/D)	Large

Table 4.2: Overview of the interview participants. YIR refers to *years in role* and YOE to *years of experience*.

4.6 Data Analysis

The data analysis process involves the development of codes, description and comparison, categorization, conceptualization, and theory development. Although described as a cyclic process within the figure, Hennink et al. (2020, p. 202) emphasizes that the processes are closely interlinked and usually performed simultaneously and at different stages during the analysis. The following section will describe how the beforementioned steps were conducted in this thesis.

4.6.1 Transcription Materials

An essential part of preparing data for analysis is converting the data from verbal to textual form as it aids in capturing the participants' words and expressions (Hennink et al., 2020, p. 213), which is used as empirical evidence in the thesis discussion. As the purpose of the data analysis influences the type of transcript being conducted (Hennink et al., 2020, p. 213), it was essential to consider the thesis' purpose again at this stage. All interviews were recorded with the interviewee's consent. Seven out of nine interviews were conducted in Norwegian, and I chose to leave the transcription in the original language as it aids in preserving the accuracy and correctness of the transcripts (Hennink et al., 2020, p. 217). Upon using quotations in Chapter 5, each quote was translated to English with great discretion to prevent important content from being lost or misinterpreted upon translation.

4.6.2 Coding of Transcripts

Having transformed the interviews into a textual form, it was necessary to code the transcripts to capture the essence and concepts presented by the interviewees systematically. The codebook, presented in Table C.1 in Appendix C, was created based on an example provided by Hennink et al. (2020, p. 219). Dividing the transcripts into smaller meaningful parts also proved to be practical as dealing with long transcripts can make it challenging when comparing results across interview objects (Hennink et al., 2020, p. 118). The coding was conducted by using the qualitative data analysis tool NVivo as this is a tool specifically fit for coding qualitative data and a tool I was already familiarized with. As each transcript was carefully read, I was looking for text segments that could aid me in answering the research question and coding these segments according to the codebook. The four stages from the DCF (Figure 4.3) were used during this process as the identified text segments were linked to the stage to which they belonged.

In Table C.1, each code is marked by the strategy used, being either deductive or inductive. Deductive codes were created prior to the careful reading of the transcripts and were based on theory aspects from the interview guide. Upon reading the transcripts in more detail and starting the coding process, codes were developed inductively from the data sets. For instance, reflecting upon the participants' responses and their underlying meaning and

noticing connections and repetition in answers were actively used when coding the transcripts. As coding transcripts is an evolving process, the codebook proved to be a valuable tool for keeping track of all the codes and their meanings.

4.6.3 Evaluating Data Quality

While gathering data, it is crucial to consider its quality, which can be achieved by evaluating the data's validity and reliability (Grønmo, 2016, p. 261). As the collected data is used to answer the research question, these three factors are considered crucial for the final analysis and conclusion to be sound and successful (Grønmo, 2016, p. 237).

The principle of communicative validity was applied to evaluate the data's validity. This type of validity applies the usage of dialog and communication between the researcher and relevant partners to assess the data's relevance to the research question (Grønmo, 2016, p. 255). Discussing with both internal and external supervisors aided greatly in evaluating potential strengths and weaknesses in the collected material. As a representative unit of the interview, objects were used for data collection – in which all had relevant experience concerning OSINT and CTI – the validity of the data collection was evaluated as satisfactory.

As there are no standardized methods for evaluating data reliability in qualitative studies compared to quantitative studies (Grønmo, 2016, pp. 248–249), I used alternative methods. Grønmo describes how one in qualitative studies can evaluate the data's stability to consider the reliability. Thus, reading and evaluating the transcripts more than once was wishful to ensure that I noticed all important and relevant aspects. Turning back to earlier read transcripts made it possible to notice aspects one had ignored earlier based on newly obtained knowledge from other transcripts. Moreover, the reliability of the data material was evaluated based on the trustworthiness of the interview units in terms of their experience and communicated knowledge. As many of the units have been in cybersecurity and threat intelligence profession for several years, their contribution to the study was considered reliable.

It requires a great deal of knowledge and experience to be a good interviewer who brings out the best in their interviewees in such a demanding setting as an interview can be. As more interviews were conducted, my experience also increased. The focus was on asking good questions to extract as much useful knowledge from the interviewees as possible. As my knowledge increased in parallel with the execution of interviews, I improved an interviewer throughout the process. The conduction of pilot interviews could have aided me in growing more confident prior to the actual interviews and familiarizing myself with the interview guide quality (Hennink et al., 2020, p. 125), but it was not prioritized due to time limitations.

4.7 Limitations and Ethical Considerations

When conducting a research project, it is essential to consider challenges that can influence both the process and the result. Both limited amount of time and restricted access to

interview candidates are common challenges encountered by researchers (Kvale, 2007b). Studies involving direct human interaction through interviews and asking the participants to share their stories voluntarily should consider the ethical issues researchers may encounter (Orb et al., 2001). Being aware of these challenges in advance and thereby being able to identify them as they occurred aided me as a researcher in reflecting on how they influenced my study. Ergo, this section will reflect on the aspects that have – or may have – influenced my thesis.

4.7.1 Limitations During Data Collection

There were several challenges to consider during the data collection process, which limited the study to various degrees. Having some experience from earlier small research projects, I considered recruiting interview participants a challenge as my network and ability to reach out to competent participants were limited. Despite starting the recruiting process early, it proved to be challenging to reach out to relevant personnel. During this process, several approaches were tried, both by reaching out to various organizations through their contact email and by directly contacting individuals on LinkedId, where the latter proved to be the most successful solution. Nevertheless, the number of respondents was lower than expected when planning the study. Since conducting a qualitative study with semi-structured interviews is a time-consuming process (Queirós et al., 2017), I decided to be satisfied with the recruited participants to follow my progress plan. Due to the number of participants, I was conscious about recruiting people from different sectors, organizations, and experiences to gain as much diverse information as possible and prevent biases.

As the data collection happened only through semi-structured interviews, the collection depended much on my abilities as an interviewer. I had to establish a context in which the interviewees understood the purpose of their study participation and felt comfortable sharing information with me. As the interviews were semi-structured, I also had to be flexible regarding the order of my questions to follow the interviewee's responses. Examining the transcripts during the coding process explained in Section 4.6.2, it became clear that some of the interviewees elaborated very much on my question rather than directly answering it. Perhaps linked to my interview experience, the indirect answers to my questions meant that I had to interpret their meaning using inductive methods.

4.7.2 Ethical Considerations

As the study relied on the recruitment of participants – which included them being willing to share their thoughts about the research topic with me through an interview – it was essential to seek consent from the participants before the data collection. Through email correspondence, I provided all interviewees with two information documents: one from NSD (Appendix D) containing detailed information about the study's purpose and conduction and one containing the interview questions. The participants could consider the significance

of their participation in the study and if they were willing to contribute (Hennink et al., 2020, p. 74) by receiving adequate and detailed information in the document. Even though signing the consent form in the NSD document, they were not obliged to participate in the interview and could withdraw their consent whenever they wanted. Information from the earlier shared documents was repeated during the interview session to ensure the information reached the participants. For example, the participants were informed prior to starting the recording of that Teams call – to make them aware that the recording had started – and they were ensured that their contribution would be anonymized upon transcription to protect their identities. Additionally, I allowed all participants to access the transcription material afterward if desired. Communicating the transparency of the study's process to the participants, both before, during, and after its conducting, was a conscious act to ensure research ethics.

Conducting studies within cybersecurity and intelligence can be challenging as participants are conscious about not sharing organization-sensitive information. Within CTI, this could include information on their specific IRs and detailed procedures during information harvesting. Consequently, as this type of detailed information was irrelevant to the thesis and due to respect for my participants, I deliberately formulated my questions to avoid putting my participants in an uncomfortable situation. For instance, when asking about their IR processes, I explicitly stated that I was not interested in the content of the IR but rather in the process of their creation.

5 | Empirical Findings

> There are known knowns; there are things we know we know. We also know there are known unknowns; that is to say, we know there are some things we do not know. But there are also unknown unknowns – the ones we don't know we don't know.
>
> *Donald Rumsfeld*

The empirical findings were gathered by interviewing nine intelligence practitioners from different organizations, which after that were analyzed according to the methods described in Chapter 4. This chapter presents the empirical findings by following the DCF (Figure 4.3), guiding the data collection and analysis. Within each step of the framework, the data analysis will highlight the similarities and differences to understand better the reasons for the participants' current OSINT processes. The discovered similarities and differences will aid in answering how organizations can effectively plan and implement OSINT to enhance cybersecurity posture (RQ1) by being interpreted according to theory and literature in Chapter 6. These findings, in addition to the interviewees' descriptions of motivational aspects and challenges, will also aid in identifying critical factors for successful OSINT utilization (RQ2). The chapter ends by providing a table of summary (Table 5.2) for each interviewee and their respective OSINT utilization.

5.1 Interviewees' Definitions of OSINT

After a few interviews, it became clear that the interviewees had different perceptions of what the term *OSINT* meant to them. Since the definition of intelligence, including OSINT, depends on where and by whom it is applied (Section 2.1), it was decided to start asking the interviewees about their definitions. The answers would reveal if they answered based on their personal understanding of the term or if the organization had established a definition for their employees. Upon being asked the question, *Cybersec_manager_1* answered:

> "[...] my perception of OSINT is open-source threat intelligence. So more around kind of news stories and kind of IoCs [indicators of compromise] that have been released into the wild, those sorts of things, not so much threat hunting and TTPs

and tactics and that sort of thing."

Interpreting the answer, the interviewee demonstrates a technical-oriented understanding of what OSINT brings to their organization. On the contrary, both *CTI_analyst_1* and *CTI_analyst_4* describe how open sources cannot be used to write detection rules based on discovered IoCs as these technical indicators change constantly.

Two of the interviewees, *CTI_consultant_1* and *Cybersec_manager_2* , bring up the question of what is included in "open sources" and if information that is being paid for or shared in closed information channels is considered open sources. *CTI_consultant* perceive information originating from paid sources not to be a part of OSINT and continues:

> "OSINT, I would define it as - well, isn't it somewhat defined in the word itself - yes, it's that, it's sources that are available online or accessible to everyone."

The definition by *CTI_consultant* thus describes OSINT as an information source, not an intelligence product, contradicting intelligence theory. Similarly, *Cybersec_manager_2* speaks of OSINT as an information source:

> "[...] and what is OSINT? Is there a separation between what I can find openly online or is information being sent and shared in information channels between organizations and businesses? That I do not consider as OSINT."

Common for all the answers was that the definition of OSINT depended much on the interviewees' personal opinions, as neither answered with confidence as if their organization had taken a stand on the matter. As the definition of OSINT depends on where it is applied and for what purpose, it was not surprising that the answers differed between the ones using OSINT for purely technical reasons and those using it for more strategic purposes.

5.2 Current OSINT Processes

Following the DCF, this section presents the empirical evidence related to each of the four stages. Although the interview findings showing the processes among the interviewees are not equally structured, the content has been interpreted through the view of the DCF to provide a systematized dissemination of the material. As the interviewees described their OSINT processes, similarities and differences became visible.

5.2.1 Planning and Direction

Intelligence requirements (IRs) There were significant variations in how the interviewees determined their organizations' respective IRs during the planning stage, and the findings show several reasons for that. It was discovered that some of the organizations using OSINT to purely detect zero-day vulnerabilities, and for that reason, did not see the need for specified IRs as they had control over their technical systems regarding versions running and the

types of services they had. As stated by *CISO_1* when being asked about the process of determining IRs:

> "You could say that we don't have an overall process for that, but like, everything is managed through our management system. We have the management built upon ISO27001, but kind of made for us [...]. But in regards to answering specifically to that question, it is more like vulnerability stuff, or like, towards the services."

Similarly, *Cybersec_manager_1* acknowledges not having a defined process either, as they are "[...] just looking for things to block". Furthermore, the interviewee states:

> "[...] the point to raise here is that it's not really thought of by people outside of cyber [...]. It's very kept inside of our bubble, you know, you've not got the CFO sitting there thinking about what's going on in cyber intelligence. They're thinking about their own things"

One can understand the cyber department within the organization of *Cybersec_manager_1* being highly isolated from the other department in terms of sharing cybersecurity information.

CTI_Analyst_2 describes a compound situation with defined and undefined IRs. Due to being a small organization, the structure of the intelligence cycle can seem too "bureaucratic", meaning the daily practice is more dynamic.

> "[...] so the ones addressing the requirements and the ones looking for the information are often the same person. Oftentimes, it is me or a colleague that realizes that there is a requirement. So, there isn't a formalized process, like, 'we have to do *this*, let's go through the formalized intelligence process to identify it.' [...] So, it's much more [...] dynamic than the formal intelligence process."

On the contrary, some of the interviewees described situations where they would get a specific request, as stated by *Cybersec_manager_2*:

> "So, the guy being the risk manager is requesting, like, 'what are the biggest threats right now?', and then we'll collect statistics from open-source and, like, compare to get a solid foundation enough to be able to state like 'yes, okay, so we think *these* are the biggest threats right now'. So, he'll make the requirements, [...] and then I'll collect what I can find [...]. "

Also, *CTI_analyst_4* describes situations where they would produce intelligence after a request from the risk department within the organization, then using a more ad-hoc approach. Shall one understand *CTI_analyst_3*, building an environment where the decision-makers are requesting IRs takes time and resources, as the decision-makers must understand the value the intelligence team is delivering before they will request anything:

> "[...] I feel like, okay, it took *at least* a year, a year and a half maybe, until we got to a spot where we were like 'wow, this team is really like delivering quality intelligence,

> that's unique, and that really fulfills the client's intelligence requirements'.[...]. As soon as they [CISO, CEO etc.] started requesting information from us, then we knew okay, we had to build a reputation for ourselves as a trusted advisor"

Ergo, one can summarize the different approaches regarding the process of defining IRs into two different groups: the situations where the CTI analysts are defining the IRs themselves based on trends they are witnessing; and the situations where people from the C-suite or other decision-makers are specifically asking for intelligence on a specific matter. Interpreting the situations describing the latter, findings showed that these situations were often equally unstructured and that the intelligence requests happened occasionally and were not due to a structured process. Moreover, these situations also required the intelligence requester to trust the quality and value of the products delivered by the intelligence team.

Knowledge base The usage of a knowledge base – a place where knowledge (i.e., previously created intelligence) is stored – was hardly practiced among the participants. The empirical findings showed various explanations concerning why. The organizations where few people were involved in the collection stage did not need a knowledge base where things were stored as they knew most of it based on experience. As *CISO_1* explains:

> "[...] There's a lot that's just in people's heads, and even technical people are often not very good at documenting things. Often, you have a lot of experience and knowledge, but you don't know how to use it or put it into a system to help others."

According to this quote, one can imagine how the usage of a knowledge base could have made *CISO_1*'s organization less dependent on individuals being present in the analysis of a particular piece of information, as the knowledge base could have contained people's learnings from previous cases. By actively using a knowledge base, pieces of information could have been given new meanings and provide value as an attribute in making the intelligence product. Working at the strategic level alone, *Cybersec_manager_2* also explained how the usage of a knowledge base seems exhaustive in their position but admitted that it could have benefited the daily routine:

> "At the strategic level at least, it is usually just me, at least at group level, and – so, it could be that, at our different business areas, there are contacts I should've had more relation to, which could've had a knowledge base that I should've had access to."

Hence, learnings from *CISO_1* and *Cybersec_manager_2* reveal that there might be an undiscovered value within their OSINT utilization due to the absence of structuring already possessed knowledge within the organization. According to *CTI_analyst_2*, the knowledge base is much connected to the organization's level of maturity. Similarly, as stated above, *CTI_analyst_2* refers to much of the gathered knowledge just being left in people's heads as

one is hardly producing formal intelligence products:

> "[...] in my opinion from experience in Norway, very few are mature enough to start having a formal process when working with intelligence or information [...]."

Overall, the discussions regarding the knowledge base showed that the intelligence theory from how intelligence is originally created is somewhat exhaustive in some organizations. The small size of the workforce, unawareness of how to store knowledge or highly dynamic daily routines were reasons found that can make people or organizations neglect the usage of a knowledge base.

5.2.2 Collection

Proactive or reactive approach The interviewees' descriptions showed that there are various approaches regarding the collection phase. *Cybersec_manager_1* using OSINT for mainly technical reasons, e.g., detecting IoCs and blocking traffic, describes how they have an ad-hoc approach to using OSINT. If something interesting is detected, the team will address it and try to solve it internally. Not having created specified IRs, the collection phase is thereby guided by individuals and their perception of "interesting". Also *CISO_2* mentioned their approach being reactive and shared a concrete example of the consequences of their current approach:

> "[...], for example, last week, there was a major vulnerability in Outlook that we should have seen coming much earlier. The consequences of that were that we had to start the IRT team to patch it in the middle of the night. And that leads to a lot of wear and tear on the personnel. It also leads to WEA [working environment act] violations, that is, violations of rest regulations and such things. And it generates a lot of overtime. If we had been a little more proactive, we would have acted earlier on these types of things."

The causes of the consequences mentioned in the above quote are most likely multiple, like the amount of knowledge, experience, and resources available; nevertheless, having a defined procedure for data collection during the intelligence process could have led them to discover the incident earlier. At least if one shall understand *CTI_analyst_1*:

> "The longer you've worked [with intelligence] the more mature you become, or if you're from the intelligence environment and have an intelligence background [the Armed Forces], you have an increased focus on 'yes, this is good, this is what has happened today and what's happening now, we'd like to know more of what *can* happen'."

On the other side, the descriptions by *CISO_1*, *CTI_analyst_1* and *CTI_analyst_4* shows a clear process of how the collection phase is carried through. As *CTI_analyst_1* described:

> "We take the information that we collect internally from our colleagues in the

> CDC, the SOC, and the CERT, we complement that with OSINT, plus kind of also like business understanding, and then merge that together and then send it up to the business. ”

All three described how OSINT often complements information from other sources. Using multiple sources of information during the data collection has aided them in pursuing the IR as one can then cover a larger area. Nevertheless, the interviewees emphasized the importance of communicating with each other while utilizing multiple sources to ensure distribution of important information.

Information sources and channels Findings showed variations regarding how information from open sources was retrieved. Whereas some interviewees described using primarily open sources and thus included the usage of multiple information sources, others used OSINT mainly as enrichment to already gained information and used fewer information sources. The information sources mentioned through the interviews were media, social media, governmental sources, network/partner channels, and third-party services. The latter was used by many to facilitate the retrieval of information by subscribing to streams provided by a paid vendor or a free platform. As described in Section 5.2.3, using information from third parties does not necessarily imply the information is filtered in terms of information relevance and reliability, but it facilitates the collection stage. Both *CTI_analyst_4* and *Cybersec_manager_2* used the information provided by the third parties to retrieve statistics that complemented their threat intelligence products. Using a third-party vendor aids the team in being proactive, according to *CTI_analyst_3*:

> “[...], like right now our efforts are manual, they’re ad hoc, which is to say okay if I know what to look for, then I can look here. [...] I can look for known unknowns, right? If I know that I don’t know a thing. But there’s a whole bunch of unknown unknowns that are missing us because we don’t have, kind of, proactive alert set. So that’s where it kind of these open source intelligence platforms, these vendors, come in because they monitor proactively”

The interviewee refers to the quote by Donald Rumsfeld presented at the beginning of this chapter. Using third-party vendors (e.g., AlienVault) aid the interviewees in gaining knowledge of the things they are unable to detect themselves, as one must know where to look for them. In addition to using third parties, some interviewees also described using information shared in closed networks (e.g., between companies within the same sector) for similar purposes. Both *CTI_analyst_4* and *Cybersec_manager_2* describe these channels as important for information sharing but acknowledges that these channels are not entirely open-source as the information could be confidential.

The encrypted messaging platform Telegram was used by both *CISO_2*, *CTI_analyst_4* and *Cybersec_manager_2* to retrieve information from potential threat actors by being members of specific chat groups. However, *CTI_analyst_4* describes the information from

these channels can be considered as "gray zone" open source information. Likewise, Twitter was also used by some interviewees to gain knowledge of early indicators. It varied if the usage of Twitter was a part of the organization's OSINT process or if it was a choice taken by the analysts themselves to access potential information. *CTI_consultant* described the usage of Twitter as follows:

> "Twitter is where you'll get the early warning signals, right? But it's not like I'll bring a Twitter post to the customer meeting, unless it's – like, usually, you're not in such a rush, you've time to wait for one of these news websites or more serious actors to pick it up, but it's very useful for those early warning signs."

Hence, *CTI_consultant* had experienced the benefits of using Twitter to get the early signs, which could direct the attention when more information appeared in trusted sources.

One can understand that multiple tools and methods are used during the collection stage to retrieve sufficient data or information. The interviewees described that open sources were not always used independently during this stage. By merging information from open and closed sources, the information could complement one another and bring forward new perspectives. In such a way, the information from open sources can become of increased value.

5.2.3 Analysis and Evaluation

One of the main challenges of OSINT is the overwhelming amount of information available in open sources – mentioned both by the interviewees and in the literature – one has to adopt some method to distinguish between relevant and irrelevant information and between reliable and unreliable information. All of the interviewees agreed to the need to apply methods to sort the information to suit their needs and requirements. Even though many of them were using third-party vendors of threat intelligence, the information was hardly sorted enough beforehand, so sorting was always needed.

Information relevance The interviewees described different methods for determining information relevance upon using open sources. Both *CTI_consultant* and *CTI_analyst_3* emphasize the importance of cooperating with colleagues with different backgrounds and who have different knowledge regarding the business to aid in determining information relevance. *CTI_consultant* highlights physical meetings with colleagues as a method they are using to aid them in determining information relevance for their customers. The interviewee emphasizes that often, some piece of information is relevant to some and not to others and that it brings value to discuss the findings with others:

> "[...] it can be dangerous to sit all by yourself and take all these decisions alone within your own head, right, so it's healthy to speak out about it and discuss it.[...] I can miss something because I think that nobody uses this [technology], but in fact, customer x is using this a lot, right, so suddenly it becomes very relevant"

Thus, communicating with colleagues can prevent individuals from making biased decisions on information relevance. Through conversation, the information relevance can be discussed with multiple perspectives present. Additionally, *CTI_analyst_3* explains:

> "[...] for example, one thing that kept coming is that there is this Russian dark web forum that we came across which kept having references to the company that I worked at but it was totally innocuous, so we didn't report it up because we touched based with the business and they said 'yes, they're talking about this but they're not planning for an attack, [...]'. So, I see that our key role is to act as that filter as well because you only want to report things that are actual threats and that are relevant to the business. "

The interviewee indicates the importance of putting everything into a business context. If the collected information could be related to the business context, it becomes easier to visualize the potential impact of the finding and how it should be approached.

Information reliability Although agreeing on the importance of evaluating the reliability of the information from open sources, the interviewees had different opinions regarding the amount of effort put into the evaluation. This was again highly linked to the objective. Interviewees using open sources to supplement information from closed sources, such as *Cybersec_manager_2* and *CTI_analyst_4*, used limited time evaluating information reliability. Conversely, the interviewees using third parties to gather open-source information explain putting that much effort into information reliability by considering the information's source, place, and actual content.

Regarding the evaluation of the source, many interviewees mentioned that they usually have a set of sources that are trusted more than others. That could be sourced from nation-states, peers, or other more recognized organizations. Both *CTI_analyst_1* and *CTI_analyst_2* mention that information sources having an extreme political view makes them more skeptical. The latter explains:

> "Of course, there are certain places on the Internet where it's [...] very politically oriented in one direction, and very far out on the right. Yes, but then we have to take that into consideration when we look at both information and the source versus one that may not be as politically motivated. [...], so we look at both the source and the information and what it provides. Actually, the most important thing is to examine whether we can find the same information from different independent sources. Yes, then it has a much higher value compared to only finding the information from, like, an obscure Twitter account created two weeks ago."

Furthermore, *CTI_analyst_2* is not the only one mentioning the usage of multiple sources as an indicator of information reliability. For instance, *CISO_1* explained having made a choice

of using multiple third parties to evaluate the content against one another. As discussed in Section 3.3, if multiple sources state the same information – corroborative reporting – the reliability increases. Using this method showed to be very normal among the interviewees, but *CTI_analyst_3* emphasized that there are some pitfalls of using this method:

> "And then of course the number one question that you need to look into is, are we talking about two independent streams and reporting, or is the circular reporting? [...] okay, it's six people saying this thing, but actually, they're just kind of mirroring each other. Um, because that happens all the time, so you need to be worried about that."

Evaluating multiple sources of information was highlighted by the interviewees as a major method in determining information reliability. The interviewees agreed on the importance of evaluating their sources but there were put different amounts of effort into this operation. The more usage of information from open sources in their intelligence process, the more effort was laid into evaluating the trustworthiness.

5.2.4 Dissemination

Adapting the content Upon communicating the intelligence internally, the interviewees mainly used two methods: written reports and physical meetings. Interviewees described that written reports often were delivered according to a pre-defined frequency (e.e., bi-weekly) or upon special requests. Several interviewees emphasized that the written intelligence material had to be adapted for it to be *ingestible* to the receiver. This brings several of the interviewees into a dilemma as often the distribution lists of the written report could include everything from the CEO to highly technical people. Naturally, these people need the information formulated in different ways. *CTI_consultant* states that this often leads to the CTI report being something in the middle: not technical enough for the IT department and not business-oriented enough for the C-suite. To solve that problem, *CTI_analyst_3* described that the intelligence product should rather be distributed to a smaller section of people and tailored to them. One of the adjustments made was the introduction of an action list:

> "[...] we developed a bit of a framework to make sure that we classify our reports as, like, *actionable*, *corroborative*, or *background* because I immediately want the clients to know, 'okay, is this something which requires action from me?'"

According to the system presented by *CTI_analyst_3*, *actionable* means the report contains intelligence that requires action from the reader and how the problems should be approached; *corroborative* means reports describing how the intelligence team had discovered things being stated by the larger intelligence companies in their reports; *background* means the report is just providing background information to enhance the reader's situational awareness. The intelligence team would mark each report or document with either of the three categories for

the receiver to know how to handle the information.

The interviewees further describe how an intelligence report to people outside the cyber department should be kept within 2-3 pages and contain figures, tables, and graphics to make the material more ingestible to the receiver. A physical meeting is recommended to follow up on any potential questions by the reader. A physical dissemination method is also great for the intelligence team, as they can get an instant feeling of how the material is received and ask any potential questions on the spot according to *Cybersec_manager_2*.

Building internal trustworthiness Some of the interviewees brought up an interesting aspect during the discussion of dissemination methods regarding the dilemma of *when* and *what* to communicate to stakeholders. *CTI_analayst_3* elaborated on how their team was very conscious about the type of intelligence they communicated as to its quality and decision-support potential:

> "There's a lot of skepticism about threat intelligence teams, [...] I've seen intelligence teams that have been criticized or derided, and then with the one person used the slogan "yesterday's news reported tomorrow". [...]. So I'm very conscious of that, [...] we need to really focus on making sure that we're seen as delivering unique value. [...] As a security team or as an Intel team, the number one value you're trying to protect is your reputation so that when you say something is an issue, people read it, and they'll act upon it because they know that you wouldn't be crying wolf."

Also, *CISO_1* used the "crying wolf" analogy upon describing the dilemma of whether or not to communicate findings to people outside the threat intelligence team. Both emphasize the importance of well-formulated dissemination to ensure that the information communicated is not scaring the receivers but rather informing them about a cyber threat concern. As stated by *CTI_analyst_3*:

> "If you're talking to people that don't work in security, the easiest thing to do is to just scare them [...]. Like being scared as a waste of time. My role isn't to scare people. My role is to make sure that people feel, especially decision-makers, feel empowered to make more secure decisions."

Hence, the interviewees did show consciousness concerning both *how*, *when*, and to *whom* the threat intelligence information was disseminated. Although mass-producing threat intelligence reports could be the "easiest" task, the interviewees largely agreed that physical meetings with intelligence receivers were a better dissemination method compared to reports as they could often be distributed too broadly and thereby lose their value.

Feedback and communication In order for the intelligence team to develop useful and valuable intelligence, they need feedback from the requester. Findings showed that the

amount of feedback mainly depended on the dissemination method and if feedback was requested. Dissemination meetings make it easier for the receivers to express their thoughts regarding the intelligence product immediately with minimal effort as they are physically present. According to *Cybersec_manager_2*, the physical meetings are to be preferred:

> "I find it valuable both for myself and also for the recipients because it gives them the opportunity to ask questions and request more information. And, more – yes, it provides much more than just sending out a report internally."

Nevertheless, the same interviewee describes that feedback is not explicitly requested within the meetings, only that it is a "positive consequence" of being physically together. The interviewee also shared that there had never been any misunderstandings upon being delivered an IR; hence, one could interpret the frequency of physical meetings to mitigate the risk of misinterpretation during both the planning and dissemination stage.

Although physical meetings facilitate receiving feedback, it is not a direct consequence and depends much on the people attending. Due to people's different perceptions of the need for asking questions and raising feedback on an intelligence product, *CTI_analyst_1* emphasizes being conscious of the fact that feedback must be specifically requested. One of the possible methods is to arrange meetings once a year with the requester to ask whether the intelligence team had delivered satisfactory CTI during the last year. *CTI_analyst_3* explained how the yearly meetings gave positive results:

> "I think it's also good when we have that session after one year where we looked at, okay, what are the things that we did, then having a bit of more of a formal conversation. So instead of going to the client after each report [...]. [...] Then, in my experience, that tends to be a more fruitful conversation. You get more out of it [...]."

The intelligence process, being a continuous cycle, would then automatically start over as the conclusion of the meeting would lay the foundation for the next IRs. Hence, being provided feedback would ensure that the intelligence process is continuously improved and that the team is delivering valuable intelligence.

5.3 Interviewees' Views on OSINT

Discussing the motivational factors and challenges mentioned by the interviewees in applying OSINT within their cybersecurity operations was interesting for several reasons. Detaining their motivational factors would aid in understanding their intelligence processes as someone's aim of collecting intelligence is influencing their processes and methods. Moreover, this part of the interview would reveal similarities and differences regarding the motivational factors identified through the SSLR. A summary of the practitioners' view can be seen in Table 5.1.

Motivational factors	Challenges
Being proactive	Information overload consisting of mis- and disinformation and exaggerated information
Enhance understanding of the threat landscape and possible threat actors	Must interpret weak signals
Support decision-making	Much of the information is not specified enough

Table 5.1: Summary of motivational factors and challenges with OSINT identified through the empirical findings

5.3.1 Motivational Factors

Support decision-making Since originating from military organizations, one of the main purposes of using intelligence is to aid in making informed decisions. By providing decision-makers with analyzed information in such situations, the goal is to enhance the awareness of the situation and minimize insecurity toward potential consequences. Several of the interviewees share this perception and motivation of what OSINT could bring them. One of them, *CTI_analyst_3*, describes one of the main motivational factors being the enhancement of situational awareness among decision-makers within the organization. This being a large organization, the interviewee is especially aware of sharing information that perhaps the security team possesses but which can aid other people in the organization as well:

> "So, to make sure that we don't get into a situation where, let's say, the CSO, or the CISO or the head of the Information Security Centre, makes some sort of decision, and then, in the corner and in the CDC [Cyber Defense Centre] someone says: 'Well, why didn't they take *this* into account? Don't they know x, y and z?'"

During the first couple of months in 2023, the debate started on whether the social media platform *TikTok* should be banned from mobile devices used in service. *Cybersec_manager_2* was in the middle of this decision and had to gather information on the subject to support the organization's decision-makers. Hired as the organization's CTI-responsible on a strategic level, *Cybersec_manager_2* underlines how the increased material on *TikTok*'s security issues have supported their decision-making:

> "So, it's absolutely useful for the decision-makers to have a person that – to have someone to turn to when things happen in the world, [...]. [...] sharing information and using information, even if it's from open sources or from peers, it makes us, I would say, better equipped to know where to set the focus and the strategy."

Also, *CISO_1* remarks how OSINT has aided them in situations where making the right decision at the correct time have been especially challenging. After the Russian invasion of Ukraine in 2022, organizations have pulled out of Russia to show their distance from Russian politics. The organization of *CISO_1* had Russian-located offices, which had been kept off

the table from the start. Having pulled out of Russia now, the interviewee describes how the decision-makers made use of the information they had retrieved through open sources:

> "[...] we took advantage of the information in order to make better decisions. [...] it is clear that it is also important to consider these things [the cyber threat landscape] if selling a part of the business, dividing a business, or such things."

At least several interviewees have the best ambitions and motivation for applying intelligence to enhance thoughtful decision-making. As this process is closely interlinked with *how* the intelligence is delivered, this aspect is elaborated more in Section 5.2.4. However, interpreting the responses of *Cybersec_manager_1* reveals another focus compared to several of the others. The respective organization's motivation is mainly to block unwanted traffic and detect IoCs, so the ability to provide strategic decision-making is deficient. Upon being asked how the information they possess is communicated within the organization, *Cybersec_manager_1* answers:

> "I think it just, I think it just stays in cyber, but I'd imagine [CISO] would probably do some sort of presentation to the higher leadership team of that kind of information. But I know that they don't get the report and read it, and those sorts of things."

Thus, one can understand that the focus on what OSINT intends to serve the organization is highly related to the organization's ability to apply intelligence as a foundation in technical and strategic decision-making.

Being proactive and understanding the threat landscape One of the interviewees' main factors being brought up frequently regarding motivational factors was the ability to be, or become, proactive in the battle against cyber threats. Understanding the threat landscape by detecting threats and applying change before it affects the organization is seen as a great advantage as it is becoming increasingly complex.

> "So, you have to –at least it you are supposed to be a bit proactive, which is smart in most contexts – you are dependent on identifying what's moving, how the threat landscape develops and try to predict to the best extent possible, to establish proactive security measures for customers and ourselves." *CTI_consultant_1*

The interviewees' responses show different approaches to the proactive part of OSINT and CTI in general. Some answer based on a thought or a hope of it aiding them into becoming proactive, whereas others answer based on personal experience. Having several years of experience within the field, *CTI_analyst_3* describes how OSINT collection historically has been performed in an ad-hoc way and then often – as a consequence of the ad-hoc approach – the approach has been more reactive than proactive. This was the situation in the organization prior to implementing OSINT, as *CTI_analyst_3* describes:

> "But, basically, before we got into the OSINT tool, we would be aware of things when they happened, when they were usually quite bad. So, I was like: 'okay, ****, either something happened or something is just about to happen', and it was kind of like a house on fire. Okay, incident response, but the OSINT tool really opened our aperture to the range of threats that we face and really made us aware of things which were – really challenged us in terms of processes because we would get a ping to say 'okay, this thing happened on the dark web, it's not a house on fire, there's no like – but it's also nothing'."

Overall, the interviewees are highly ambitious and positively perceive what OSINT as a CTI capability can provide for the organization. They believe that by being proactive and utilizing these tools, they can demonstrate control of the threat landscape towards the rest of the C-suite within the organization, which is a desirable outcome.

Access valuable information The two aforementioned motivational factors can be understood as the bi-effects of extracting information from open sources. That is to say; open sources provide access to valuable information about the threat landscape, which can support decision-making. If having the resources, experience, or knowledge, open sources can provide a broad specter of information in massive amounts. Both *CTI_analyst_2* and *CTI_consultant* elaborates on how they are using Twitter to get notification about the early signs of a cyber incident, which thereby guides their interest to dig into that track if being relevant. Moreover, *CTI_analyst_2* argues that one of the advantages of using open sources to retrieve threat information is the fact that it is open, that is to say, it can be freely distributed to everyone as it is not classified:

> "In the last, maybe 5-6 years, the information that is freely available has been so good that I would say maybe 99% of the information we use comes from open sources. [...] For us, there has certainly been a significant increase in quality – we can use open sources as the main basis for everything we do, and then we supplement with a few closed sources for the last piece - that's how it should be."

As with all other information online, the interviewees emphasized the importance of being conscious of what one gathers and trusts as the amount of published misinformation increases simultaneously with the amount of usable information. The aspect of misinformation is further elaborated in Section 5.3.2.

5.3.2 Perceived Challenges

Information overload The increased usage of connected devices and online services have influenced how one shares information and what is shared. Consequently, distinguishing between information and dis- or misinformation can be a tough task requiring both resources and knowledge. Thus, using open sources can be challenging due to information overload, i.e., being overwhelmed by the amount of information about a topic or a situation. One of

the interviewees experiencing information overload is *CTI_analyst_2*:

> "[...], there has been a drive to push out information as early as possible when something is seen, and the quality often suffers. There is a lot more noise. This is not only because there are many newcomers who start working in cybersecurity and produce low-quality things due to their lack of experience, but also because large companies in this quest to be the first to publish something, publish poor information."

In addition to dealing with potentially exaggerated information – causing the wrong perception of a potential cyber threat – there is also the need to filter regarding information reliability. *CISO_1* mentioned that, especially during cyber attacks, the information can be overwhelming as many people are sharing information at once. *Cybersec_manager_2* had experienced dealing with disinformation, i.e., wrongful information being published to deceive. In the aftermath of the war in Ukraine, several actors claimed to be the source of several attacks, whereas they took the blame for someone else's attack. Dealing with disinformation is a difficult task:

> "That's perhaps what I find difficult, and when the actors additionally claim responsibility for an attack that they haven't actually carried out but find exciting enough to say they have, [...]. But it's also enough to take this into consideration, like, 'they claim [to be responsible], but it doesn't necessarily have to be true'."

As can be understood, exaggerated information, misinformation, and disinformation are all concepts contributing to the overall information overload which OSINT analysts need to navigate in their seek for valuable threat information.

Weak signals Often, the information retrieved can be perceived as vague by analysts. *CTI_analyst_3* how much of the job involves interpreting and analyzing information. Questions like how the organization should treat an identified risk and choose the correct countermeasure arise often.

> "[...] that's when you're actually talking about intelligence because intelligence is about weak signals that may or may not reach through some sort of end result, [...], like, there's a slight chance that something might happen and the overwhelming chance that it won't, but you still need to kind of think through that problem. "

Interpreting information – which finds its place in the analysis and evaluation stage in the intelligence cycle – requires considering just that: weak signals that might cause some kind of effect. Dealing with weak signals can be exhausting and is a significant challenge in doing threat intelligence based on open sources.

Information is sometimes too generic As the information used in OSINT originates from open sources, some of the interviewees mentioned the challenge of it being too generic. Espe-

cially the interviewees working on the technical side of intelligence within their organization, like *CTI_analyst_4*, stated that OSINT often leads to information not being tailored enough to their sector. Furthermore, the interviewee mentioned that the IoCs found in open sources change quickly, which means that OSINT could not be used to write detection rules:

> "So, we use it to some extent, we take – we retrieve and use open sources to interpret and analyze our logs. That we do, but usually, the information is poorer than the information we get from our [network] partners."

CISO_1 mentioned a similar challenge. Being CISO in a global company, not all the information being published by Norwegian state organizations (e.g., the yearly report by The Norwegian Security Authority) was considered relevant. Consequently, the interviewee said that most of the information from open sources was used to create situational awareness and understand the threat landscape.

5.4 Summary of Findings

Interviewee	Main motivation	Type of usage	Process
CISO_1	Discover vulnerabilities within technical systems, also sometimes to support decision-making	Technical and a bit strategic	Unstructured on paper but follows the intelligence cycle in practice
CISO_2	Become proactive and detect vulnerabilities and incidents before they become a great danger	Technical and strategic	Somewhat unstructured. Defined process under development.
CTI_analyst_1	Provide intelligence to support their members	Technical, tactical, and strategic	Dynamic
CTI_analyst_2	Provide intelligence to support their members	Technical, tactical, and strategic	Dynamic
CTI_analyst_3	Address the gap between the technical and the business in terms of cybersecurity	Technical and strategic	At the beginning of development
CTI_analyst_4	Be proactive and aware of the threat landscape	Technical and strategic	Structured
Cybersec_ manager_1	Block unwanted traffic, detect vulnerabilities	Technical	Somewhat structured
Cybersec_ manager_2	Provide intelligence to support decision-makers at other business areas	Strategic	A single person. Somewhat structured
CTI_consultant	Provide support to decision-makers	Strategic	Somewhat structured

Table 5.2: Summary of empirical findings

In addition to walking through the four steps in detail, the interviewees were also asked to what extent the deductive conceptual framework did represent their current OSINT process. The answers from the interviewees revealed that the material – the structure of the intelligence cycle – was known, but that practice often deviates from theory. For instance, *CTI_analyst_2*

answered that in their daily operations and monitoring, the processes are much more dynamic than the framework presents, as tasks are not necessarily performed in the order presented by the intelligence cycle. Nevertheless, the interviewee added that a more formal process is followed when producing larger products, e.g., exhaustive reports, compared to day-to-day monitoring. Also, the other interviewees confirm that the four stages describe the overall workflow but admit that the process is often undefined within the organization. According to *CISO_1*, having a defined and acknowledged process within the organization could have facilitated the communication between stakeholders:

> "In the communication process that we plan to establish, we want to have the theory in place so that everyone agrees on how everything is communicated in relation to all stakeholders."

Interpreting the responses from the interviewees shows that the structured understanding of how the four stages fit into the intelligence process is hardly present in practice. At the same time, having a defined structure would aid in communicating the intelligence process to internal and external stakeholders and ensure that everybody is on the same track. *CTI_analyst_2* shared some thoughts regarding a possible reason for the deviation between theory and practice upon being shown the deductive conceptual framework:

> "For many, it is based on personal experience and what they remember, and they may produce less formally from the sources than they should. [...], if you talked about cyber threat intelligence five years ago, for many people, it was just IPs and domains. That wasn't actually what the intelligence community would consider intelligence."

The above quote can aid in understanding the reasons and results of the various usage and understanding of CTI processes, and then also how OSINT as an intelligence capability fits into the cybersecurity domain. Going through the interviewees' intelligence processes showed how the usage of OSINT among the nine different interviewees varies to a great extent. As can be seen from Table 5.2, both motivation, type of usage, and the process deviates between the interviewees. Reading the table sets all the interviewees' responses into a context as to their current processes and how they leverage OSINT's advantages while encountering the challenges. The answers regarding the accuracy of the deductive conceptual framework revealed that although they are familiar with the intelligence cycle, their intelligence processes are not directly transferable to the deductive conceptual framework.

6 | Discussion

This thesis aims to understand how organizations can plan and implement OSINT to enhance their cybersecurity posture and, by that, also understand the factors critical for successful utilization leveraging OSINT's potential value and advantages. The review of published research on OSINT related to the cybersecurity field in Chapter 3 and the researchers' viewpoints regarding OSINT as a CTI capability, including motivational factors for its application and potential challenges one can encounter, have contributed to the knowledge on the role and positions of OSINT in organizations today. Most importantly, the chapter compared different intelligence cycles/models describing how OSINT can be applied to an organization. Furthermore, Chapter 5 presented the empirical findings according to the construction of the deductive conceptual framework (Figure 4.3). The four stages *planning*, *collection*, *analysis and evaluation*, and *dissemination* were used to highlight the significant findings across all nine interviews. Subsequently, the following chapter discusses the implications of findings from the literature and the interviews to provide additional views on organizational intelligence processes. An inductive conceptual framework (ICF) is presented as the interpretation of the deductive conceptual framework in combination with the empirical findings.

An important finding was ascertained during the analysis of the empirical findings, influencing the discussion of the two research questions. As described in Section 2.1.2, the intelligence profession originates from military institutions. Still, it has slowly entered the cyber domain as digital warfare has increased in frequency. From the theory, one must acquire intelligence per one or several IRs, guiding the collection, analysis, and dissemination to stay relevant and provide decision-making support. The interviews made it clear that understanding what intelligence and OSINT can bring to an organization varied greatly. It seems like the elements ensuring information becomes intelligent – being timely, accurate, ingestible, and complete – are often not in the cyber domain's main focus. For instance, some interviewees argued that the data and information acquired from open sources often were too generic and, thus, difficult to render relevant to the organization (Section 5.3.2). Reviewing Figure 2.1, which explains the correlation between data, information, and intelligence, it is the analyst's job to process and analyze the data and information in such a way that it becomes intelligence. By putting pieces of information together, generic information can become actionable intelligence with some effort. One can argue that this particular example of a challenge perceived by

some interviewees emphasizes the different perception of *intelligence*, compared to military instances. That is to say, while implementing intelligence capabilities within non-military organizations, some of the most essential attributes are neglected, thereby influencing the organization's ability to leverage the value of what OSINT is supposed to provide. Thus, this thesis points to three steps that should be considered during the implementation and planning of OSINT (RQ1), followed by factors ensuring the actual utilization of OSINT leverages its values as described in intelligence theory and research (RQ2). The discussion offers a view of how one may understand the connection between the four stages of the intelligence cycle and how the approach to each affects the remaining parts of the process in terms of potential leveraged value.

6.1 Inductive Conceptual Framework (ICF)

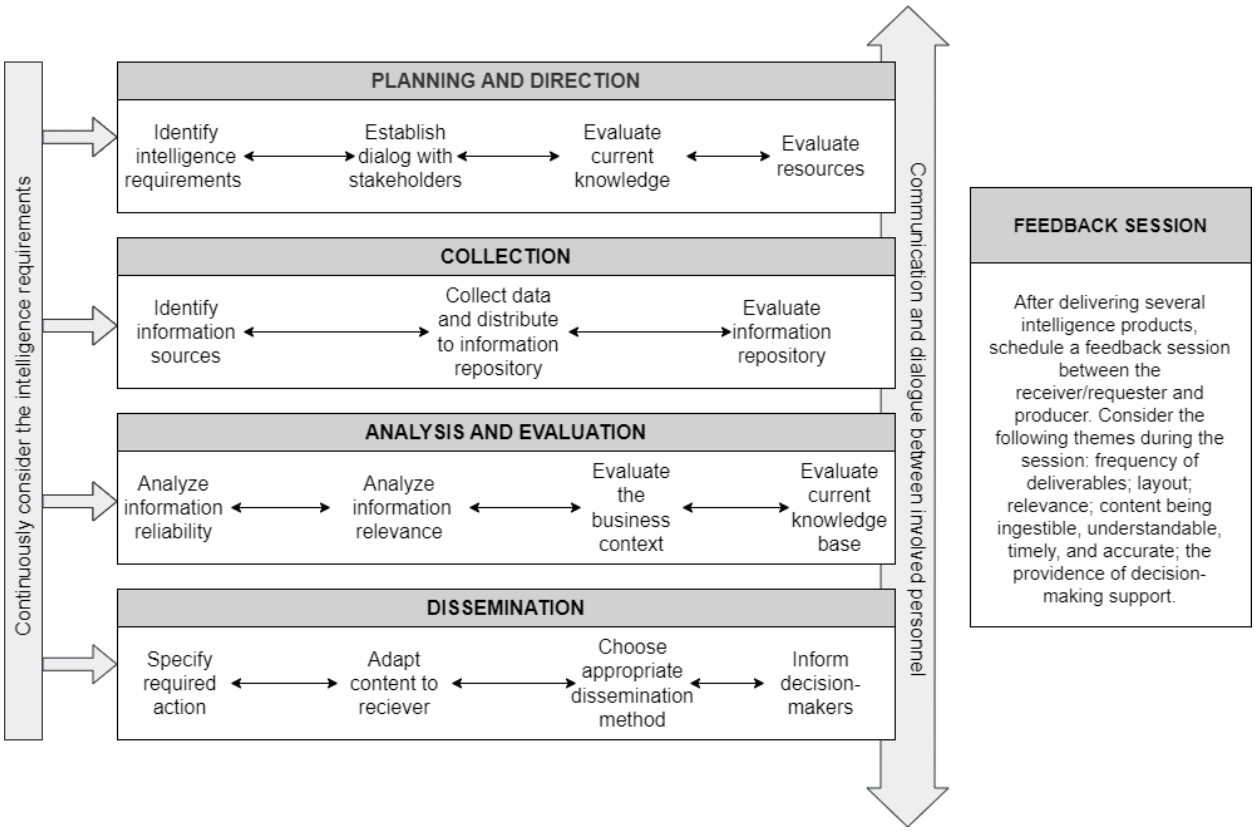


Figure 6.1: The inductive conceptual framework (ICF) for research on OSINT processes within organizations

Figure 6.1 presents the ICF, which contains central elements from the intelligence models discussed in Section 3.4 and the empirical findings from the interviews from Chapter 5. By combining elements from theory, literature, and empirical evidence, the framework summarizes the discussion related to the research questions by mapping out the relation between the discovered concepts (Hennink et al., 2020, p. 38). This chapter will discuss and link interpretations and findings to the framework along the way, but the main ideas can be

explained as follows:

- The four stages are placed vertically, similar to the model by Hwang et al. (2022) (Figure B.1), which symbolizes that the stages can (and do often) happen in parallel, not sequentially as modeled by many others.
- Double-sided arrows within the stages represent how one should return to previous steps to re-think earlier decisions. The process is not fixed, and changes must be welcomed as one gathers new knowledge during the process.
- The bar on the left visualizes the importance of constantly remembering and considering the initial objectives of the current intelligence process. The IRs will guide the process through each stage, ensuring the final intelligence product fulfills the objective.
- The vertical arrow and the box on the right visualize communication's role during the process. Continuous dialogue (the arrow) and scheduled feedback sessions (the box) can aid the intelligence team in many ways, i.e., by making enhanced intelligence products and ensuring the dissemination is tailored to the receivers.

Despite aiming to visualize the essentials steps found for an organization to leverage value from an open-source intelligence process taking multiple considerations into account, it must be noted that intelligence acquisition is a complex process, hence; the framework is not exhaustive but aims to emphasize the findings from working with this thesis. Intelligence processes must be tailored to the ones involved, meaning it is necessary to make changes to the structure for it to suit one's organization. Nevertheless, the framework will work as a guideline describing steps that should be included in the intelligence process from an organizational perspective.

6.2 Planning and Implementation of OSINT

This section will focus on the choices and methods applied prior to and during the *planning* stage within the intelligence cycle to understand how organizations can plan and implement OSINT to enhance their cybersecurity posture (RQ1). Since the planning stage is a central piece of the intelligence process (Section 2.4), choices taken here will influence the resulting intelligence product(s) and to what extent they will aid in enhancing the organization's cybersecurity posture.

A series of questions were asked to prompt them to describe their current processes to evaluate the effect of the current planning and implementation methods among the interviewees. The objective was to understand the advantages and disadvantages of the current methods and how they align with existing theory and research. Upon comparing the answers provided by the interviewees, it became evident that only a few of the described processes fit into any of the intelligence models discussed in Section 3.4. While the intelligence models typically present the stages of *planning*, *collection*, *analysis*, and *dissemination* in a sequential manner,

the interviewees explained that their everyday routines did not necessarily conform to this static representation of the process. Neither the DCF (Figure 4.3) accurately captured their processes, according to the interviewees. Analyzing the empirical findings from all interviews and considering all four stages, several aspects were identified and deemed relevant to the discrepancy between Figure 4.3 and the reality described by the interviewees:

- Whereas intelligence theory explains how a requester identifies IRs during the *planning* stage, this was hardly the case among several of the interviewees. On the contrary, the practitioners/intelligence analysts themselves were often the ones to set the requirements alongside conducting the collection of information.
- The interviewees described the usage of CTI as decision-support as rarely considered by individuals outside the cyber department. Consequently, the acquisition of OSINT often depends on the intelligence team's perception of intelligence relevant to the organization, and the dissemination methods are not customized for the intelligence receiver.
- Individual knowledge and experience among intelligence analysts highly influenced the processes. As the interviewees described how knowledge often remained in people's heads, the daily operations were often informal and based on the analysts' perception of what to consider as important tasks. This also showed during the planning stage, where using a knowledge base or active question-asking, like "What do we know?", was inconsistent. Concurrently, some mentioned that sharing knowledge and information between analysts can aid in determining information relevance and reliability.
- In the cases where intelligence products were utilized by people outside the cyber department, building trustworthiness between the requester and producer was considered necessary among several interviewees to avoid crying wolf and causing fear. The relationship between the requester and receiver has not been given attention in the intelligence process's visualizations. However, it was an important concern among some interviewees as this affected their methods and how they communicated their intelligence.

The rest of this section uses these findings to conclude RQ1.

6.2.1 Step 1: Define OSINT within the Organization

Both findings from the interviews (Section 5.1) and the literature review (Section 3.1.1) showed how the definition of OSINT depends on where it is applied and by whom. Whereas the definitions from the literature concentrated on whether to define OSINT as a process, product, or both, the empirical findings showed how the interviewees were most concerned about what to consider as *open sources*. Discovering multiple understandings of OSINT as an intelligence discipline was not surprising, but the discussions around OSINT definitions revealed something else. From the intelligence theory (Section 2.1.2), despite the definition adopted, it must be sound and clear among the people utilizing it. When asked how they

defined open-source intelligence, the responses from the interviewees gave an impression that the definition where based on personal perception. The impression was based on two things: none of the interviewees mentioned having an organizational definition upon being asked to define OSINT and the confidence in their answers. Although it might be considered a minor problem, the numerous personal definitions could propagate to more significant problems reaching the other stages of the intelligence cycle. For instance, some interviewees considered OSINT an information source, not an intelligence capability. Not considering OSINT to contain strategic, operational, and technical information will entail the result of lacking those attributes (Section 2.2). Moreover, an organization should determine whether they consider leaked, openly available documents as OSINT. The trustworthiness and legality of the information source can affect the resulting intelligence product's classification and determine how it can be distributed. Therefore, the initial step in planning and implementing OSINT is for the organization to establish a clear definition of OSINT and ensure that all relevant stakeholders are well-informed.

6.2.2 Step 2: Identify Objectives

Section 3.1.2 described how Pastor-Galindo et al. (2020) distinguished between three different use cases regarding OSINT utilization: cybercrime and organized crime; social opinion and sentiment analysis; and cybersecurity and cyberdefense. Despite all interviewees applying OSINT for cybersecurity purposes, the interviewees shared different perceptions of OSINT's usage within the cybersecurity context. The empirical findings show that their different understandings influence the implementation of OSINT within their respective organizations. As seen in Table 5.2, some used OSINT purely to get hold of newly discovered vulnerabilities and their existence within their systems, while others also distributed their findings to other business areas. While Kotsias et al. (2022) referred to the lack of intelligence products reaching all recipients as a problem (3.5, Problem 2), an interesting discovery is the question of who is determining the recipients and the alignment with the motivation for implementing an intelligence capability. During their study, Kotsias et al. discovered that the acquired CTI provided useful knowledge for decision-makers outside the cybersecurity function and was thus distributed to these stakeholders. The findings from this thesis append the attribute of *motivation* to the research findings from Kotsias et al. and the importance of considering motivation upon implementing and planning an intelligence process.

Recall that the definition of intelligence and CTI (Chapter 2) suggests intelligence must be implemented to serve an objective (IR) and collected, analyzed, and disseminated in accordance with that objective. At first, *Cybersec_manager_1*'s description of their internal usage of threat intelligence where not in accordance with how theory describes the implementation and usage. Through the conversation with *Cybersec_manager_1*, it became clear that their internal objective was the discovery of vulnerabilities and blocking unwanted traffic; hence, the remaining parts of the intelligence cycle (collection, analysis, dissemination)

were implemented accordingly. Nevertheless, one could argue that this organization is an open-source information user (OSINF), not OSINT (presented in Section 2.3). Still, the point remains the same: the motivational factors and process are highly connected. As the objective does not require exhaustive treatment of the information before it is applicable and can be put into a business context for *Cybersec_manager_1*'s organization, the process, formally known as the intelligence cycle, is lacking but not in spite of the current objective. On the contrary, many of the other interviewees, like *CISO_1*, *Cybersec_manager_2* and *CTI_analyst_4*, had intelligence processes where the four stages were more visible. Moreover, their objectives for using OSINT were also strategic, in addition to being technical. That implied an increased focus on the phases succeeding *collection* as the acquired information had to be put into context to have strategic intelligence value.

The interviewees acknowledged the challenges of using open sources for information retrieval (Section 5.3.2), such as information overload and dealing with generic information. The empirical findings did not show any direct connection between the perception of challenges and the amount of structure put into OSINT implementations. However, according to intelligence theory, the IR should be determined during the planning stage to guide intelligence acquisition. Thus, with a clear objective of what the intelligence process is supposed to provide, tackling the challenges can become easier as the objective is determined. Thus, during the second step, it is recommended that the organization identifies and determines its objectives for implementing OSINT, as this will lay the foundation of how the process will be structured later.

6.2.3 Step 3: Align Objectives to Resources

Although not mentioned as a prerequisite in the studied intelligence theory, the interviewees' experiences demonstrate the importance of adapting the intelligence objective to available resources and building internal capability over time. Section 3.3 demonstrated the challenges of using OSINT, including the time required during analysis when determining information reliability. The interviewees acknowledged these challenges. While emphasizing the significant amount of time required to build a solid intelligence capability within the organization, *CTI_analyst_3* also stated the importance of internal trustworthiness. By focusing on developing the intelligence capability over time, the team gained recognition within the organization as a trusted and reliable source of threat intelligence tailored to the business context. As the team's maturity grew, so did their ambitions and objectives. *CISO_1* shared the fear of crying wolf by reacting to weak signals or wrongful information. The reflections by the two interviewees confirm the research findings by Kotsias et al. (2022) who emphasized *trust* being a central aspect of implementing an intelligence capability. *CTI_analyst_1*, with many years of experience, also noted how maturity contributes to creating valuable intelligence from the acquired information. Building trust between the teams receiving and producing the intelligence can increase the organization's leveraged value (Kotsias et al.,

2022), similar to that experienced by several of the interviewees.

Shall one understand the interviewees, encountering the challenges of creating intelligence from open sources (Section 5.3.2) is both time- and resource-consuming but necessary to leverage value. Despite using third-party vendors to acquire threat information, an intelligence team must still be able to sort relevant information from irrelevant information within the increasing sea of information. Being a complex profession, leveraging the advantages requires many people involved during all the stages of the intelligence process. Based on the empirical findings, the third step to accomplish an OSINT process that leads to enhanced cybersecurity posture within the organization is to ensure the objectives are aligned with available resources. Starting slow and steady with manageable objectives with the available workforce is thus recommended to maintain what intelligence is supposed to bring an organization (Section 2.1.2) while encountering the challenges.

6.3 Factors Critical for Successful OSINT Utilization

Analyzing the empirical findings suggests several factors critical for successful OSINT utilization. The following section presents the factors found and how they relate to previous research.

6.3.1 Understand How Motivation and Process are Connected

Analyzing the empirical findings reveals how the organizations' objective of OSINT utilization affected their processes. The dissemination especially depended on the intelligence objective. Interviewees using OSINT for strategic purposes focused more on the dissemination phase than those who did not. For instance, *Cybersec_manager_1* did not disseminate any of the findings other than assuming the department leader read some of the findings every now and then. Additionally, the interviewee also remarked that the usage of threat intelligence was not thought of by people from outside the cyber department within the organization. As a result, the acquired intelligence stays within the cyber department, and putting effort into disseminating their findings was not considered necessary.

Moreover, within the organization of *CTI_consultant*, the motivation was to share the intelligence products with as many as possible as it was thought to provide value. On the contrary, the wide distribution resulted in the creation of vague intelligence products not being tailored to their receivers. The former interviewee describes a process adapted to current usage, which has changed in the case of changed motivation. The latter describes a situation where process and motivation are currently not aligned. Both scenarios support the suggestion by Kotsias et al. (2022) to emphasize *responsive*, *timely*, and *targted* intelligence products for an increased likelihood of it being reached and understood by non-cyber employees (as visualized in Figure 3.2). Confirming the suggestion, interviewees like *Cybersec_manager_2* and *CTI_analyst_3* were conscious about how the intelligence was disseminated as one of

their motivational factors were to support decision-makers outside the cyber department. One can argue that the process carried out by *Cybersec_manager_1*'s organization prevents it from leveraging some of OSINT's potential value, like increased CSA and the support of decision-making, as the intelligence is not distributed to business areas outside the cyber department.

In the ICF (Figure 6.1), the findings marked out in this section are visualized through the left bar containing the text: "Continuously consider the IRs". Having an arrow to each of the four stages, this bar emphasizes the discussion from this section in two ways. Firstly, the IRs set by the organization affect each stage regarding how they are carried out regarding focus areas. Secondly, the IRs should not be forgotten when the organization moves from planning to collection. Therefore, the IRs have an indirect impact on the stages. Still, they must also be taken into account directly at each stage to ensure that the final intelligence product is valuable to the organization. This aligns with the definition of CTI as a product that meets the IRs in order to support decision-making (Section 2.2).

6.3.2 Focus on Dialogue and Feedback

The aspect of communication between stakeholders during the intelligence process is often neglected within the visualization of the intelligence cycle, as became clear during the analysis of the six intelligence cycles/models in Section 3.4. Despite its absence within the theoretical descriptions, interpreting the empirical findings reveals a great advantage of prioritizing communication during intelligence. Interviewees who used OSINT for strategic decision-making and thus disseminated it to decision-makers outside the cyber department were also the ones prioritizing building a solid connection between the intelligence analysts and the receivers. For instance, as described by *CTI_analyst_3* in Section 5.2.4, this interviewee was especially conscious of sharing information and adapting the content to the receiver. This was also the same interviewee describing how one of the strongest motivational factors for their OSINT usage was to support decision-making. The relation between intelligence dissemination and one's ability to apply intelligence to support decision-making backs the theory by Haugorm (2019). In the opposite corner, one has *Cybersec_manager_1*, which was the interviewee describing how the intelligence team's objective concentrated on using OSINT for detecting IoCs and blocking IPs and, subsequently, did not disseminate the intelligence products to other departments of the organization. As a result, *Cybersec_manager_1*'s organization could not leverage OSINT's capability of providing strategic decision-making support as it is neither thought of nor prioritized at the current stage. Interpreting the findings demonstrate how one can leverage the advantage of OSINT providing strategic decision-making support by prioritizing communication in two areas: the dialogue between stakeholders; and feedback sessions.

Dialogue In the ICF, the aspect of dialogue is visualized through the vertical arrow containing the following text: "Communication and dialogue between involved personnel".

As an organization passes through the stages of the intelligence process, from planning all the way to dissemination, dialogue should be prioritized continuously to ensure it accomplishes the objective of the intelligence process. Establishing contact points for dialogue would facilitate the possibility of question-asking, which is a valuable resource, especially during the planning stage (Vandepeer, 2018). Interviewees like *Cybersec_manager_2* describe how having a solid connection with the risk manager makes it easier to understand the person's needs and demands and mitigates the risk of misunderstandings during the handover of new intelligence requests. Moreover, having a clear vision of the IR is beneficial upon reaching the analysis as information must be interpreted and put into the business context suiting the IR. Frequent dialogue also aids in creating a clear picture of what intelligence analysts actually do and how they are able to aid the organization in terms of enhancing cybersecurity posture. This can prevent the analysts and decision makers from having unrealistic expectations of each other by knowing each other's roles better. As a result, it can become easier to deliver intelligence products of value at the time needed for the decision-maker. Nevertheless, from a socio-organizational perspective, one should not underestimate the time required to build such a trusted relationship as noted by *CTI_analyst_3*. Therefore, dialogue has been given much attention in the ICF to emphasize both the value it can bring to the intelligence process and underline the importance of prioritizing it during all stages.

Feedback sessions The interviews revealed that feedback was often given due to a physical presentation of the intelligence product rather than being explicitly demanded. Physical presentations minimized the distance between the analyst and the receiver, resulting in multiple positive results, as mentioned by *Cybersec_manager_2*. It allowed the analysts to receive comments on their work and let the receiver share thoughts regarding the content and how it was understood. Such dissemination methods are essential in ensuring that the intelligence product is rightfully understood by its receivers to provide decision-making support, which is one of OSINT's primary purposes. Within the intelligence models proposed by scholars (Section 3.4), only Figure B.4, proposed by Gibson (2016), and Figure B.2, by Tabatabaei and Wells (2016), have included feedback as a part of the process. In both models, the feedback is placed at the end of dissemination and prior to planning/collection. The empirical findings support this placement. However, neither Gibson (2016) nor Tabatabaei and Wells (2016) describes how the feedback should be done, and the empirical findings also show a lack of systematized feedback processes. Although feedback was often described as infrequent and ad-hoc, the interviewees underlined how it aided them as intelligence practitioners in understanding how intelligence products could be useful to the receivers and how the content was interpreted. Feedback was especially appreciated when the intelligence product was delivered as a written report due to the absence of physical contact. Among the interviewees delivering written reports, there was shown great consciousness regarding adopting the layout, content, and length. They had experienced that long, exhaustive reports were rarely read nor understood sufficiently, confirming Haugorm (2019)'s theory regarding

the requirements of disseminating intelligence products correctly (Section 2.4).

Intelligence theory often describes how the decision-makers should identify IRs during the planning and direction stage and pass these on to the intelligence analyst. During the interviews, it became evident that the IR was equally often identified by the intelligence analysts themselves rather than the decision-makers. Several factors contribute to this, including a potential lack of interest among employees outside the cyber department, a significant level of trust in the intelligence analysts' expertise in recognizing relevant information, or possibly a combination of these reasons. *CTI_analyst_3* meant it was unrealistic that decision-makers without much cybersecurity experience were able to define IRs from their analysts from the start. They could not understand what requirements to set during the initial meetings. Thus, the interviewee described how the first intelligence products should be delivered based on the analysts' perspective of the organization's needs until the decision-makers could understand how OSINT, or CTI in general, could provide decision-making support. Intelligence theory from military institutions implies that the decision-maker has some knowledge of the area from which they seek intelligence, as this person identifies the intelligence needs. However, the empirical findings suggest that this approach is not as applicable within non-military organizations, as familiarity with the cyber domain outside of cyber departments is naturally less widespread. Therefore, *CTI_analyst_3*'s suggestions consider the need for decision-makers to enhance their understanding of how OSINT can provide value before they can articulate specific IRs. After the analysts have disseminated a certain amount of intelligence products, a feedback session should be scheduled to harvest information on how the products have been used, understood, and of value by their receivers. The experiences from *CTI_analyst_3* support the theory from Haugorm (2019) regarding the importance of communication as a tool to guide the subsequent iterations of the intelligence cycle. In that way, the feedback session would lay the foundation for upcoming processes and provide both the analysts and the receiver with examples of what did and did not work.

6.3.3 Consider the Business Context

As open sources can be accessed from anywhere at any time, the concept of OSINT may have suffered from people underestimating the attributes necessary for it to become *intelligence*. As presented in Section 2.1.1, information must be accurate, relevant, timely, complete, and ingestible for its receivers to be considered intelligence. To achieve the necessary attributes, synchronizing information from the tactical, operational, and strategic levels aids in providing a holistic picture of the situation (Bamford et al., 2013), thereby providing cyber situational awareness. Achieving this proactive approach to the cyber threat landscape was mentioned by many of the interviewees upon being asked about their motivational aspects for OSINT utilization (Section 5.3.1). Implementing tailored countermeasures was considered by the interviewees as a valuable method of continuously enhancing their cybersecurity posture as the threat landscape evolved. This unifies with the response paradigm from Baskerville et al.

(2014), referred to by Shin and Lowry (2020), which argues how the proactive approach is better suited to meet dynamic and sophisticated cyber threats, thereby embracing the fact that dynamic approaches must meet dynamic threats.

However, upon discussing the interviewees' approach to the information collection, some – for instance *Cybersec_manager_1* and *CTI_analyst_2* – described their approaches as "ad hoc", interpreted as if information retrieval happened based on what the intelligence analysts considered important at that exact moment based on previous experience. Not to say that this approach will not lead to usable intelligence, but by interpreting the interviewee's responses, one can consider there to be a relation between an ad-hoc approach and perceived OSINT value. The key to linking these concepts together is to consider the business context. *CTI_analyst_3* mentioned the importance of business context upon dissemination as the business context would aid non-cyber people to understand how the intelligence information applies to the organization. One can assume that the same procedure can be valuable during collection and analysis upon ensuring the information is kept relevant and in accordance with the IR. In combination with the three steps discussed in Section 6.2, constantly considering the business context could aid in adopting the response paradigm by Baskerville et al. (2014), meanwhile also encountering the challenges of information overload and information reliability.

6.4 Study Limitations

There are several limitations that are important to remark on in light of the provided discussion. Firstly, this study only included interviews with intelligence practitioners – representing the intelligence providers – and not decision-makers or other people from other business areas – representing the intelligence receivers. Consequently, the thoughts shared during the interviews are only telling half of the story, i.e., the intelligence practitioners' perception of OSINT's value, usage, and challenges. Although the interviews with the practitioners have provided a valuable contribution to the study, it could have benefited from including interviews with the people receiving the intelligence products in such cases where the products were distributed outside the cyber department.

Secondly, the empirical findings have both been collected and analyzed using the four main stages of the intelligence cycle as a theoretical basis. Using other frameworks could have led to a different result or added other perspectives to the discussion. For instance, frameworks focusing on the effects of structured processes within organizations could have been applied in this thesis and provide different findings. Hence, this study is highly influenced by the construction of the intelligence cycle.

7 | Conclusion

"If you know your enemies and know yourself, you will not be imperiled in a hundred battles" Sun Tzu stated a long time ago. With these famous words in mind, this study has investigated how OSINT can be used within organizations to gain knowledge of cybersecurity adversaries to implement tailored security measures and subsequently enhance the cybersecurity posture. Two research questions were formulated to encounter the research objective: how can OSINT be planned and implemented within organizations to enhance cybersecurity posture (RQ1), and which factors are critical for successful OSINT utilization to leverage its advantages and encounter its challenges (RQ2). The research questions were examined using the qualitative research methodology (Figure 4.1) by Hennink et al. (2020), which ensured academic guidance and the implementation of necessary methodological requirements. The qualitative research approach provided the study with valuable knowledge from intelligence practitioners with experience in OSINT utilization for cybersecurity purposes.

Theory from the intelligence profession was gathered to describe the origin of OSINT and how it can provide value within organizational cybersecurity. As intelligence originates from the military profession, sources such as Forsvaret (2021) and UK Ministry of Defence (2011) were actively used to determine the foundational purpose of intelligence acquisition. Using intelligence theory from military institutions was a deliberate choice to provide the thesis with acknowledged sources on how the profession defines intelligence processes and necessary factors for successful utilization. The theoretical foundation from these sources provided definitions and descriptions of related concepts, guiding the subsequent SSLR. Synthesizing retrieved papers revealed that a strong focus on technical implementation had overshadowed an organizational focus on OSINT. The SSLR confirmed various understandings of what OSINT is and how it can aid cybersecurity. Researchers highlighted several advantages of OSINT, such as enabling reactive measures against cyber adversaries and enhancing the situational understanding of the cyber threat landscape. Followed by the many challenges OSINT users can experience, six of the examined research papers provided a model describing the OSINT process from the researchers' perspective (see Appendix B). These findings, along with the insights from the case study by Kotsias et al. (2022), laid the theoretical foundation of this thesis on OSINT utilization within organizations. By comparing the intelligence models and the theoretical background resulting, a deductive conceptual framework (DCF, Figure 4.3) was created, summarizing the understanding of OSINT implementation and

usage.

The thesis concludes each of the research questions as follows:

RQ1: "How can organizations plan and implement open-source intelligence (OSINT) to enhance their cybersecurity posture?"

The discussion on RQ1 in Section 6.2 highlights the deviations between the DCF and the empirical findings through three steps. *Firstly*, it is essential to determine the objective of OSINT implementation. The analysis of the research findings reveals that uncertainty and different perceptions regarding OSINT's purpose can influence the implementation. For instance, some consider OSINT as pure information, whereas others emphasize its role as being decision-making support. Thus, findings suggest that the individuals involved with OSINT usage – both receivers and providers – must synchronize their understanding of OSINT as an intelligence discipline and what it can provide the organization. *Secondly*, the objective of OSINT utilization, in terms of intelligence requirements (IRs), must be determined carefully by facilitating collaboration among strategic decision-makers, cybersecurity specialists, and intelligence analysts. The collaborative effort ensures a comprehensive understanding of each other's needs. Depending on the purpose of OSINT, whether it is to enhance situational awareness about the threat landscape, provide indicators of compromise, or support strategic decision-making, the intelligence process will be influenced accordingly. *Thirdly*, the defined objectives must align with available resources, such as knowledge, capacity, and time. Arting with more than one can handle from the beginning can overwhelm the organization with information, making it challenging to derive relevant intelligence and implement tailored cybersecurity measures. However, by gradually developing the OSINT capacity and focusing on a few objectives aligned with available resources, organizations can provide value to the intelligence receivers. Establishing a reputation as a trusted intelligence provider allows for an appropriate increase in capacity over time.

RQ2: "Which factors are critical for successful OSINT utilization in order to leverage its advantages and encounter its challenges?"

The data analysis found three essential factors that can aid an organization in leveraging the advantages while encountering the challenges of OSINT. *Firstly*, the objectives identified during the implementation and planning influence the construction of the intelligence process. Organizations with strategic objectives for OSINT tend to focus more on the entire intelligence process, including disseminating intelligence to decision-makers outside the cyber department. Responsive, timely, and targeted intelligence products can increase the likelihood of being reached and understood by non-cyber employees. *Secondly*, although barely emphasized within the literature, prioritizing communication throughout the process proved very valuable, according to the interviewees. Establishing a dialogue with the intelligence receiver and producer can clarify needs and expectations early and aid the analyst during the collection, analysis, and dissemination. In the cases where the analysts themselves specify the IR,

communication becomes essential during dissemination. Adapting the intelligence product to the receiver's needs, knowledge level, and original intelligence objective is essential. Communication must be present during the process as *dialogue* and after dissemination as *feedback* to ensure continuous development. *Thirdly*, organizations must emphasize the business context to ensure the intelligence stays relevant through the process. By building a systemized approach around the objective, OSINT can put the organization in a proactive cybersecurity posture.

7.1 Key Findings

When comparing the empirical evidence with the theoretical background of military institutions, findings indicate that many of the essential attributes of intelligence are overlooked during the transition from military to commercial usage. Findings related to the two research questions show that although organizations use open sources to obtain intelligence for cybersecurity purposes within organizations today, the usage deviates to some extent from the intelligence profession. Where theory describes how a decision-maker should request intelligence from the analyst, this does not work in practice within the cyber domain as cybersecurity as a practice still needs to be matured within organizations. Although many have opened their eyes to the importance of focusing on cybersecurity enhancement, the empirical evidence highlighted the difficulty for people outside the cyber department to apply threat intelligence to their daily operations. As a result, they cannot request IRs due to limited knowledge, and intelligence analysts are trusted to acquire intelligence relevant to the organization as they have cyber expertise. For analysts, defining relevant IRs requires insight into the business context, which is often possessed by top management. Practitioners must distinguish between information and intelligence, understanding that OSINT results from a thorough analysis. Adapting the mindset from the theoretical foundation would aid organizations in leveraging the value of OSINT by acknowledging its original form. By recognizing the complexity of OSINT implementation, planning, and utilization, organizations can leverage their full potential to their benefit within the ever-changing cyber threat landscape.

As visualized through the inductive conceptual framework (ICF, Figure 6.1), awareness of the essential parts of the intelligence process can aid organizations in using intelligence as a powerful tool that can be built upon as they mature. By acquisition of intelligence through open sources, organizations can adopt a proactive approach by enhancing awareness of the threat landscape and encountering threats by implementing tailored countermeasures. However, findings emphasize the importance of defining OSINT within one's organization, understanding its attributes, and using this knowledge to define clear objectives aligned with the organization's resources. Moreover, awareness of the critical factors for successful OSINT utilization, including motivation, process adaptation, and communication/feedback, can enhance the leveraged value derived from OSINT. Adapting as much as possible from these sources into the private, public, and commercial context upon OSINT utilization is considered

beneficial to preserve intelligence's original form. With these findings, organizations can be guided into OSINT adaptation which embraces the non-military environment while conserving the attributes necessary to leverage OSINT's values for cybersecurity purposes.

7.2 Study Contribution

This thesis unveils the potential of OSINT as being a valuable tool to enhance cybersecurity posture in organizations' cybersecurity workforce. As the SSLR highlighted a gap concerning studies on OSINT utilization from an organizational perspective, this study contributes new knowledge of OSINT utilization within non-military organizations and how the implementation aligns with intelligence theory. The usage of DCF aided in gathering the essence of intelligence theory and literature, ensuring relevant concepts were explored during data collection and data analysis. Moreover, the established understanding of the intelligence process aided in analyzing the empirical evidence and evaluating its accuracy through the interviewees' descriptions.

The discussion of RQ1 and RQ2 has resulted in the ICF depicted in Figure 6.1. By extending theory from the intelligence profession and the SSLR, the ICF contributes to research by presenting an alternative view of the intelligence processes. The study acknowledges the presence of all four intelligence stages during OSINT acquisition but emphasizes them happening simultaneously rather than sequentially. The ICF marks this discovery by visualizing *planning and direction*, *collection*, *analysis and evaluation*, and *dissemination* as parallel components. By abandoning the sequential perspective, the ICF highlights the dynamic nature of OSINT acquisition and encourages organizations to adapt the elements of the intelligence process to suit their specific requirements. Furthermore, the framework emphasizes the significance of continually evaluating the reasons for utilizing OSINT, achieved by prioritizing communication through both continuous dialogue and scheduled feedback. The findings visualized through the ICF contribute to a new perspective on intelligence processes and the stages essential for leveraging OSINT's advantages.

7.3 Recommendations for Further Research

Due to limited knowledge of OSINT within organizations, future research can provide valuable contributions to enhance understanding of how it should be utilized depending on variables such as organization size, industrial sector, and perceived cyber threat. As mentioned in the thesis delimitation in Section 1.3, the research depended on the interviewees' perception of the usage, being people from the cyber and intelligence departments within their organizations. Concurrently, being based on subjective interpretations, the study could have benefited from a comparable point of view from intelligence requesters or receivers with a non-cyber or -intelligence background. By applying multiple views, future research can test the ICF and potentially discover additional aspects regarding organizational aspects within OSINT

processes. For instance, using observations, researchers can examine current intelligence processes within different organizations and derive comparable results by acquiring knowledge of how OSINT implementation and utilization differ among organizations. With new angles, the relevance and accuracy of the ICF can be tested, for instance, to investigate the effect of systematization on cybersecurity processes.

Furthermore, as this thesis aimed at understanding OSINT within organizations, literature related explicitly to OSINT was extracted during the SSLR. As the research gap showed a lack of focus regarding organizational considerations of OSINT, the provided intelligence models from scholars within OSINT papers were used to interpret their thoughts on organizations' OSINT utilization. Future researchers could apply more studies on CTI implementation (in addition to Kotsias et al. (2022)) to explore further the differences between adopting a general CTI capability versus a pure OSINT capability within an organization to enhance the cybersecurity posture.

Bibliography

Abdullah, A., Laghari, S. A., Jaisan, A., & Karuppayah, S. (2021). OSINT Explorer: A Tool Recommender Framework for OSINT Sources. https://doi.org/10.1007/978-981-16-8059-5{_}24

Alves, F., Andongabo, A., Gashi, I., Ferreira, P. M., & Bessani, A. (2020). Follow the Blue Bird: A Study on Threat Data Published on Twitter. https://doi.org/10.1007/978-3-030-58951-6{_}11

Amaro, L. J. B., Azevedo, B. W. P., de Mendonca, F. L. L., Giozza, W. F., Albuquerque, R. d. O., & Villalba, L. J. G. (2022). Methodological Framework to Collect, Process, Analyze and Visualize Cyber Threat Intelligence Data. *Applied Sciences 2022, Vol. 12, Page 1205*, *12*(3), 1205. https://doi.org/10.3390/APP12031205

Bamford, G., Felker, J., & Mattern, T. (2013). *Operational Level Of Intelligence* (tech. rep.). Intelligence and National Security Alliance. https://www.nist.gov/system/files/documents/2017/06/08/20131213_charles_alsup_insa_part3.pdf

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information and Management*, *51*(1), 138–151. https://doi.org/10.1016/J.IM.2013.11.004

Borum, R., Felker, J., Kern, S., Dennesen, K., & Feyes, T. (2015). Strategic cyber intelligence. *Information and Computer Security*, *23*(3), 317–332. https://doi.org/10.1108/ICS-09-2014-0064

Bromiley, M. (2016). Threat Intelligence: What It Is, and How to Use It Effectively. www.gartner.com/doc/2487216/definition-threat-intelligence

Brown, R., & Lee, R. M. (2019). The Evolution of Cyber Threat Intelligence (CTI): 2019 SANS CTI Survey. *SANS Whitepaper*. www.sans.org/reading-room/whitepapers/analyst/cyber-threat-intelligence-uses-successes-failures-2017-cti-survey-37677,

Brown, R., & Stirparo, P. (2022). *SANS 2022 Cyber Threat Intelligence Survey* (tech. rep.). SANS. www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack

Crowe, S., Pournouri, S., & Ibbotson, G. (2021). Use of Classification Techniques to Predict Targets of Cyber Attacks for Improving Cyber Situational Awareness During the COVID-19 Pandemic. https://doi.org/10.1007/978-3-030-72120-6{_}9

Endsley, M. R. (1988). Situation Awareness in Aircraft Systems: Symposium Abstract. *Proceedings of the Human Factors Society Annual Meeting*, *32*(2), 97–101. https://doi.org/10.1177/154193128803200220

Ettinger, J., Barmer, H., Kane, J., Evans, H., Brandon, E., Gupta, R., DeCapria, D., & Mellinger, A. (2019). *Cyber Intelligence Tradecraft Report: The State of Cyber Intelligence Practices in the United States* (tech. rep.). Carnegie Mellon University. Pittsburgh. https://resources.sei.cmu.edu/asset_files/EducationalMaterial/2019_011_001_546699.pdf

FireEye Inc. (2019). Threat Intelligence Foundations. https://www.fireeye.com/solutions/cyber-threat-intelligence/

Forsvaret. (2021). *Forsvarets etterretningsdoktrine* (tech. rep.). https://www.etterretningstjenesten.no/publikasjoner/etterretningsdoktrinen/Etterretningsdoktrine_2021_Web_LoRes_02.pdf/_/attachment/inline/633b7840-43de-42af-bb89-243d81076208:edd1367bd55a434b4489162637336d7d632d42a0/Etterretningsdoktrine_2021%20-%20Web_LoRes%2002%20(PROD).pdf

Gibson, H. (2016). Acquisition and Preparation of Data for OSINT Investigations. https://doi.org/10.1007/978-3-319-47671-1{_}6

Gibson, H., Ramwell, S., & Day, T. (2016). Analysis, interpretation and validation of open source data. *Advanced Sciences and Technologies for Security Applications*, 95–110. https://doi.org/10.1007/978-3-319-47671-1{_}7/FIGURES/1

Glassman, M., & Kang, M. J. (2012). Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). *Computers in Human Behavior*, *28*(2), 673–682. https://doi.org/10.1016/j.chb.2011.11.014

Grønmo, S. (2016). *Samfunnsvitenskapelige metoder* (2nd ed.). Fagbokforlaget.

Hassan, N. A., & Hijazi, R. (2018). The Evolution of Open Source Intelligence. In *Open source intelligence methods and tools* (pp. 1–20). Apress. https://doi.org/10.1007/978-1-4842-3213-2{_}1

Haugorm, L. (2019). Å fange oppdrasgivers oppmerksomhet. In S. Stenslie, L. Haugorm, & B. H. Vaage (Eds.), *Etterretningsanalyse i den digitale tid* (1st ed., pp. 151–177). Fagbokforlaget.

Hayes, D. R., & Cappa, F. (2018). Open-source intelligence for risk assessment. *Business Horizons*, *61*(5), 689–697. https://doi.org/10.1016/j.bushor.2018.02.001

Hennink, M., Hutter, I., & Bailey, A. (2020). *Qualitative research methods* (2nd ed.). SAGE Publications, Ltd. https://akademika.vitalsource.com/books/9781473924352

Hulnick, A. S. (2006). Intelligence and National Security What's wrong with the Intelligence Cycle. *Intelligence and National Security*, *21*(6), 959–979. https://doi.org/10.1080/02684520601046291

Hwang, Y.-W., Lee, I.-Y., Kim, H., Lee, H., & Kim, D. (2022). Current Status and Security Trend of OSINT (Y. Huo, Ed.). *Wireless Communications and Mobile Computing*, *2022*, 1–14. https://doi.org/10.1155/2022/1290129

Johnsen, J. W., & Franke, K. (2019). The impact of preprocessing in natural language for open source intelligence and criminal investigation. *2019 IEEE International Conference on Big Data (Big Data)*, 4248–4254. https://doi.org/10.1109/BigData47090.2019.9006006

Kallio, H., Pietilä, A.-M., Johnson, M., & Kangasgniemi, M. (2016). Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. *Journal of Advanced Nursing*, *72*(12), 2954–2965. https://doi.org/10.1111/jan.13031

Kotsias, J., Ahmad, A., & Scheepers, R. (2022). Adopting and Integrating Cyber-Threat Intelligence in a Commercial Organisation. *European Journal of Information Systems*. https://doi.org/10.1080/0960085X.2022.2088414

Kvale, S. (2007a). Introduction to Interview Research. In *Doing interviews* (pp. 2–10). SAGE Publications, Ltd. https://doi.org/10.4135/9781849208963

Kvale, S. (2007b). Planning An Interview Study. In *Doing interviews* (pp. 35–50). SAGE Publications, Ltd. https://doi.org/10.4135/9781849208963

Lande, D., & Shnurko-Tabakova, E. (2019). OSINT as a part of cyber defense system. *Theoretical and Applied Cybersecurity*, *1*(1). https://doi.org/10.20535/TACS.2664-29132019.1.169091

Lee, S., & Shon, T. (2016). Open source intelligence base cyber threat inspection framework for critical infrastructures. *2016 Future Technologies Conference (FTC)*, 1030–1033. https://doi.org/10.1109/FTC.2016.7821730

Liska, A. (2014). *Building an Intelligence-Led Security Program* (T. Gallo, Ed.). Syngress.

Marczyk, G., DeMatteo, D., & Festinger, D. (2005). *Essentials of Research Design and Methodology*. John Wiley & Sons, Inc.

Melshiyan, M. A., & Dushkin, A. V. (2022). Information Security Audit Using Open Source Intelligence Methods. *2022 Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus)*, 379–382. https://doi.org/10.1109/ElConRus54750.2022.9755530

Microsoft Corporation. (2021). *Microsoft Digital Defense Report* (tech. rep.). Microsoft. https://info.microsoft.com/ww-landing-Microsoft-Digital-Defense-Report-Gate.html

National Security Authority. (2022). *Nasjonalt digitalt risikobilde 2022* (tech. rep.). Nasjonal sikkerhetsmyndighet. Oslo. https://nsm.no/getfile.php/1312007-1664785983/NSM/Filer/Dokumenter/Rapporter/NDIG2022_online.pdf

National Security Authority. (2023). *Sikkerhetsfaglig råd Et motstandsdyktig Norge* (tech. rep.). https://nsm.no/getfile.php/1312994-1683615611/NSM/Filer/Dokumenter/Rapporter/Sikkerhetsfaglig%20r%C3%A5d%20-%20Et%20motstandsdyktig%20Norge.pdf

NATO. (2019). NATO Glossary of Terms and Definitions (English and French). https://www.coemed.org/files/stanags/05_AAP/AAP-06_2019_EF.pdf

NIST. (2022). Glossary | Computer Security Resource Center. https://csrc.nist.gov/glossary

Oates, B. J. (2006). *Researching Information Systems and Computing*. SAGE Publications Ltd.

Okoli, C., & Schabram, K. (2010). A Guide to Conducting a Systematic Literature Review of Information Systems Research. *Sprouts: Working Papers on Information Systems*, *10*(26). http://sprouts.aisnet.org/10-26

Omand, D. (2019). Et historisk tilbakeblikk. In S. Stenslie, L. Haugorm, & B. H. Vaage (Eds.), *Etterretningsanalyse i den digitale tid* (pp. 33–50). Fagbokforlaget.

Orb, A., Eisenhauer, L., & Wynaden, D. (2001). Ethics in Qualitative Research. *Journal of Nursing Scholarship*, *33*(1), 93–96. https://doi.org/10.1111/j.1547-5069.2001.00093.x

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., ... Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *Journal of Clinical Epidemiology*, *134*, 178–189. https://doi.org/10.1016/J.JCLINEPI.2021.03.001

Pai Yogish, U., & Krishna Prasad, K. (2021). Open Source Intelligence and its Applications in Next Generation Cyber Security - A Literature Review. *International Journal of Applied Engineering and Management Letters*, *5*(2), 1–25. https://doi.org/10.47992/IJAEML.2581.7000.0100

Pastor-Galindo, J., Nespoli, P., Gomez Marmol, F., & Martinez Perez, G. (2020). The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends. *IEEE Access*, *8*, 10282–10304. https://doi.org/10.1109/ACCESS.2020.2965257

Pawliński, P., Jaroszewski, P., Kijewski, P., Siewierski, Ł., Jacewicz, P., Zielony, P., & Żuber, R. (2014). *Actionable information for security incident response.* (tech. rep.). European Union Agency for Network and Information Security (ENISA). Publications Office. https://doi.org/10.2824/38111

Politiet. (2020). *Etterretningsdoktrine for Politiet* (tech. rep.). Politidirektoratet.

Queirós, A., Faria, D., & Almeida, F. (2017). STRENGTHS AND LIMITATIONS OF QUALITATIVE AND QUANTITATIVE RESEARCH METHODS. *European Journal of Education Studies*, *3*(9), 369–387. https://doi.org/10.5281/zenodo.887089

Qusef, A., & Alkilani, H. (2022). The effect of ISO/IEC 27001 standard over open-source intelligence. *PeerJ Computer Science*, *8*, e810. https://doi.org/10.7717/peerj-cs.810

Rowe, F. (2014). What literature review is not: diversity, boundaries and recommendations. *European Journal of Information Systems*, *23*(3), 241–255. https://doi.org/10.1057/ejis.2014.7

Samtani, S., Abate, M., Benjamin, V., & Li, W. (2020). Cybersecurity as an Industry: A Cyber Threat Intelligence Perspective. In *The palgrave handbook of international cybercrime and cyberdeviance* (pp. 1–20). Springer International Publishing. https://doi.org/10.1007/978-3-319-90307-1{_}8-1

Shin, B., & Lowry, P. B. (2020). A review and theoretical explanation of the 'Cyberthreat-Intelligence (CTI) capability' that needs to be fostered in information security practitioners and how this can be accomplished. *Computers and Security*, *92*. https://doi.org/10.1016/J.COSE.2020.101761

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333–339. https://doi.org/10.1016/J.JBUSRES.2019.07.039

Stenslie, S., Haugorm, L., & Vaage, B. H. (2019a). *Etterretningsanalyse i den digitale tid.* Fagbokforlaget.

Stenslie, S., Haugorm, L., & Vaage, B. H. (2019b). Innledning. In S. Stenslie, L. Haugorm, & B. H. Vaage (Eds.), *Etterretningsanalyse i den digitale tid* (pp. 19–31). Fagbokforlaget.

Tabatabaei, F., & Wells, D. (2016). OSINT in the Context of Cyber-Security. In B. Akhgar, O. Bayerl, & F. Sampson (Eds.), *Open source intelligence investigation: Advanced sciences and*

technologies for security applications. (pp. 213–231). Springer. https://doi.org/10.1007/978-3-319-47671-1{_}14

Tundis, A., Ruppert, S., & Mühlhäuser, M. (2022). A Feature-driven Method for Automating the Assessment of OSINT Cyber Threat Sources. *Computers and Security*, *113*. https://doi.org/10.1016/J.COSE.2021.102576

UK Ministry of Defence. (2011). *Understanding and Intelligence Support to Joint Operations (JDP 2-00)* (tech. rep.).

Vandepeer, C. (2018). Intelligence and Knowledge Development: What are the questions intelligence analysts ask? *Intelligence and National Security*, *33*(6), 1–19. https://doi.org/10.1080/02684527.2018.1454029

Wagner, T. D., Mahbub, K., Palomar, E., & Abdallah, A. E. (2019). Cyber threat intelligence sharing: Survey and research directions. *Computers & Security*, *87*, 101589. https://doi.org/10.1016/J.COSE.2019.101589

Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*, *26*(2), 13–23. http://www.jstor.org/stable/4132319

Williams, H. J., & Blum, I. (2018). *Defining second generation Open Source Intelligence (OSINT) for the defense enterprise.* Rand Corporation.

Wohlin, C. (2014). Guidelines for Snowballing in Systematic Literature Studies and a Replication in Software Engineering. *Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering.* https://doi.org/10.1145/2601248.2601268

Yusof, R., Abu, S., Selamat, S. R., & Ariffin, A. (2018). Cyber Threat Intelligence-Issue and Challenges. *Indonesian Journal of Electrical Engineering and Computer Science*, *10*(1), 371–379. https://doi.org/10.11591/ijeecs.v10.i1.pp371-379

Appendices

A Paper overview from SSLR

Authors	Year	Title
Abdullah, A., Langhari, S., Jaisal, A. et al.	2021	OSINT Explorer: A Tool Recommender Framework for OSINT Sources
Alves, F., Andongabo, A., Gashi, I. et al.	2020	Follow the Blue Bird: A Study on Threat Data Published on Twitter
Crowe, S., Pournouri, S. & Ibbotson, G.	2021	Use of Classification Techniques to Predict Targets of Cyber Attacks for Improving Situational Awareness During the Covid-19 Pandemic
Gibson, H.	2016	Acquisition and Preparation of Data for OSINT Investigations
Gibson, H., Ramwell, S. & Day, T.	2016	Analysis, Interpretation and Validation of Open Source Data
Hassan, N. & Hijazi, R.	2018	The Evolution of Open Source Intelligence
Hayes, D. & Cappa, F.	2018	Open-source Intelligence for Risk Assessment
Hwang, Y., Lee, I., Kim, H. et al.	2022	Current Status and Security Trend of OSINT
Johnsen, J. & Franke, K.	2019	The Impact of Preprocessing in Natural Language for Open Source Intelligence and Criminal Investigation
Kotsias, J., Ahmad, A. & Scheepers, R.	2022	Adopting and Integrating Cyber-Threat Intelligence in a Commercial Organization
Lande, D.	2019	OSINT as a Part of a Cyber Defense System
Lee, S. & Shon, T.	2016	Open Source Intelligence Base Cyber Threat Inspection Framework for Critical Infrastructures
Melshiyan, M. & Dushkin, A.	2022	Information Security Audit Using Open Source Intelligence Methods
Pastor-Galindo, J., Nespoli, P., Gomez Marmol, F. et al.	2020	The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges, and Future Trends
Qusef, A. & Alkilani, H.	2022	The Effect of ISO/IEC 27001 Standard over Open-Source Intelligence
Samtani, S., Abate, M., Benjamin, V. et al.	2020	Cybersecurity as an Industry: A Cyber Threat Intelligence Perspective

Shin, B. & Lowry, P.	2020	A Review and Theoretical Explanation of the 'Cyberthreat-Intelligence (CTI) Capability' That Needs to be Fostered in Information Security Practitioners and How This Can Be Accomplished
Tabatabaei, F. & Wells, D.	2016	OSINT in the Context of Cyber-Security
Tundis, A., Rupport, S. & Mühlhäuser, M.	2022	A Feature-Driven Method for Automating the Assessment of OSINT Cyber Threat Sources
Williams, H & Blum, I.	2018	Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise
Yogish Pai, U. & Krishna Prasad, K.	2021	Open Source Intelligence and its Application in Next Generation Cyber-Security - A Literature Review

Table A.1: Retrieved articles sorted by author (A-Z)

B Intelligence cycles from SSLR

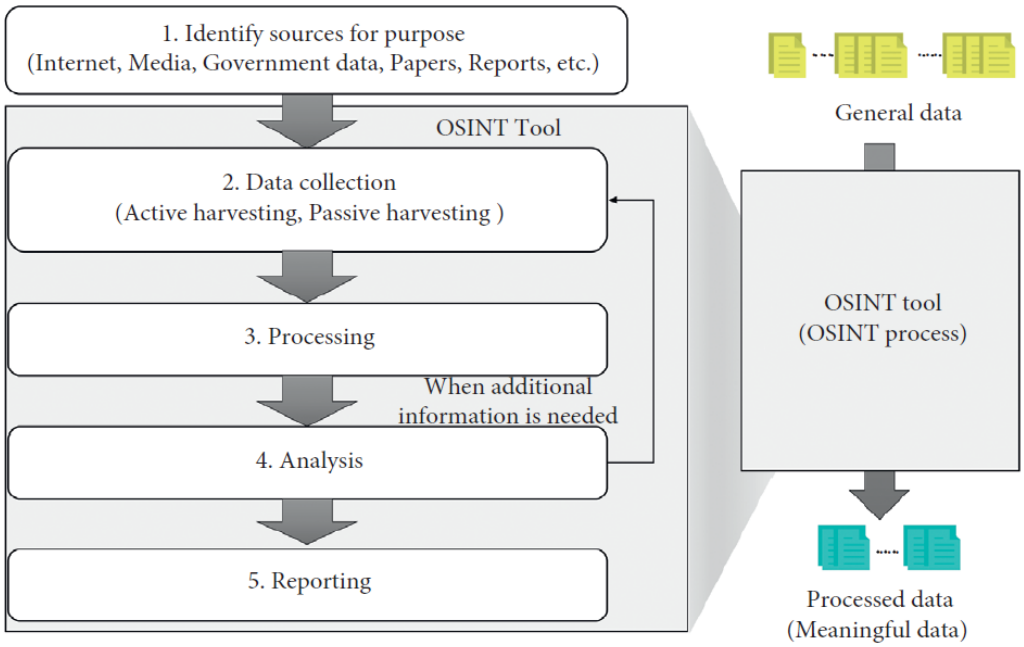


Figure B.1: Model 1(Hwang et al., 2022, p. 3)

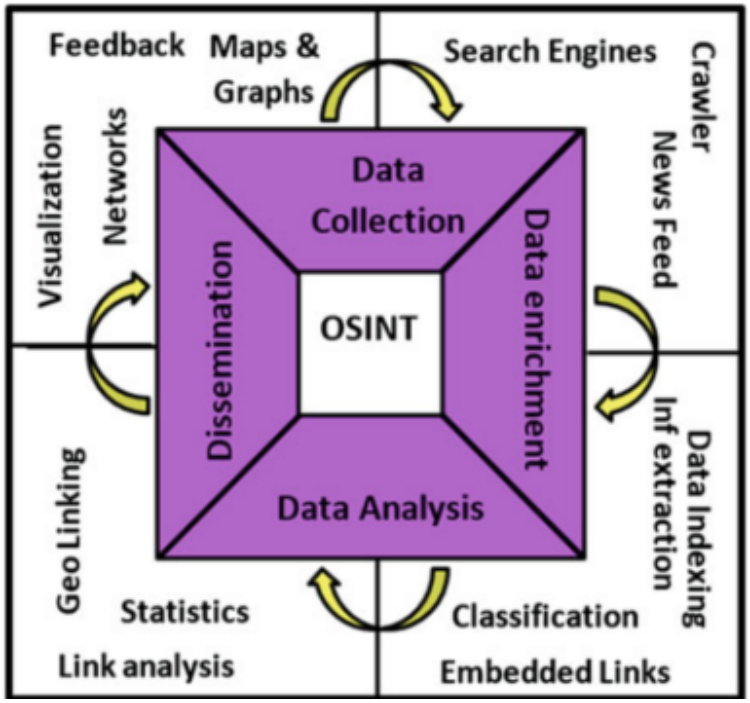


Figure B.2: Model 2 (Tabatabaei & Wells, 2016, p. 215)

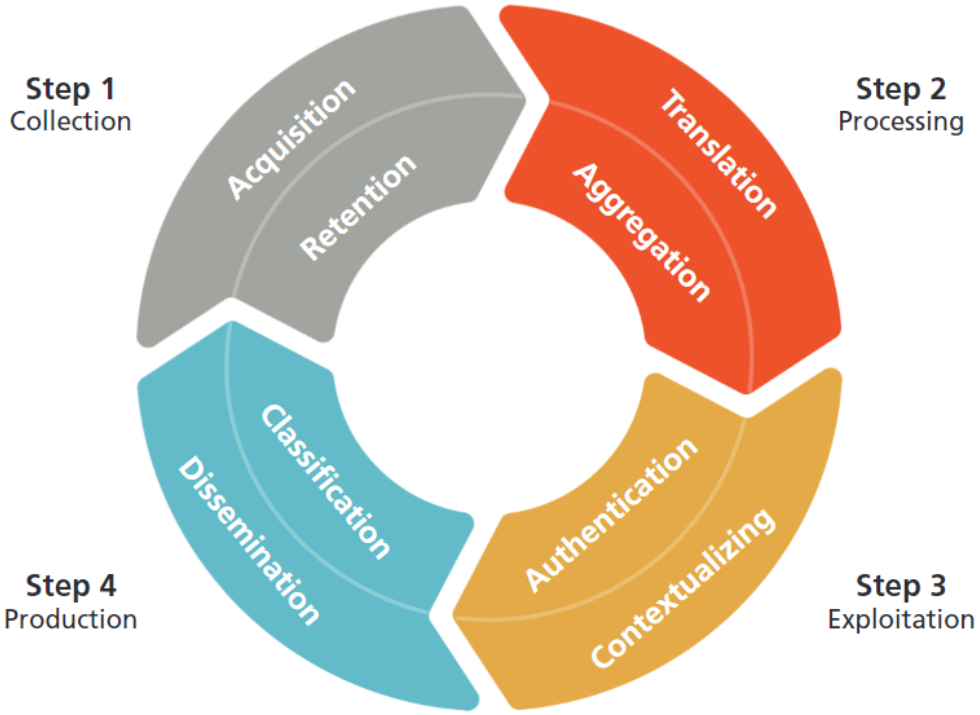


Figure B.3: Model 3 (Williams & Blum, 2018, p. 13)

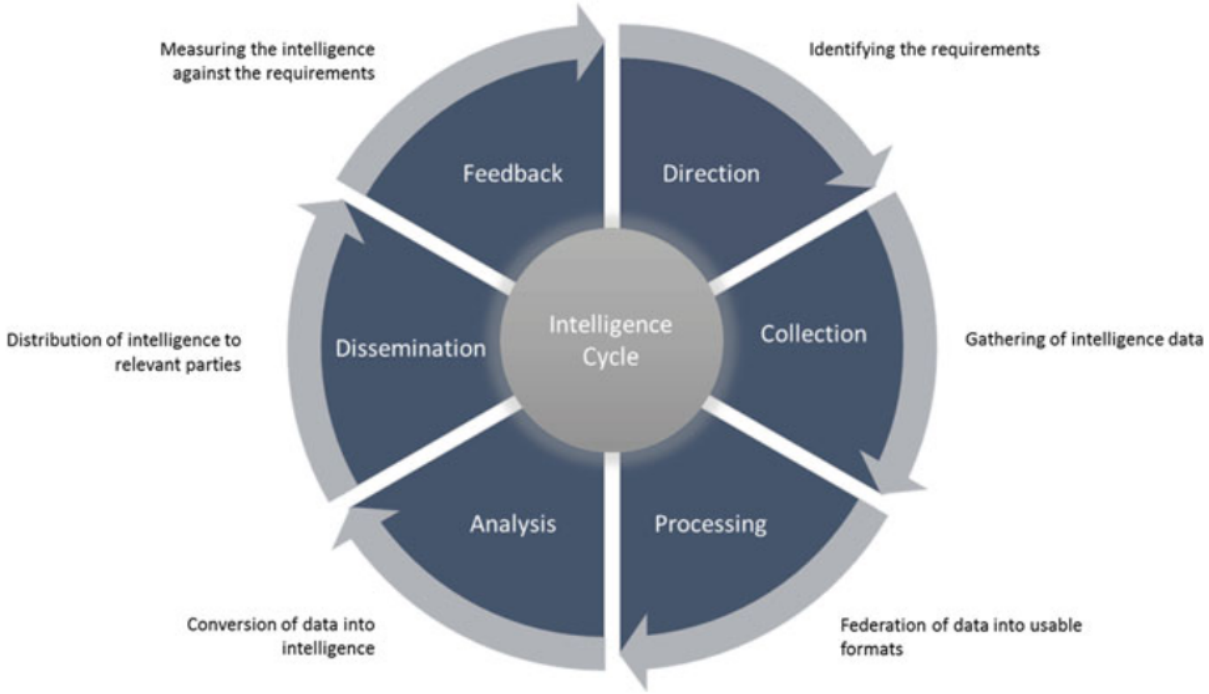


Figure B.4: Model 4 (Gibson, 2016, p. 72)

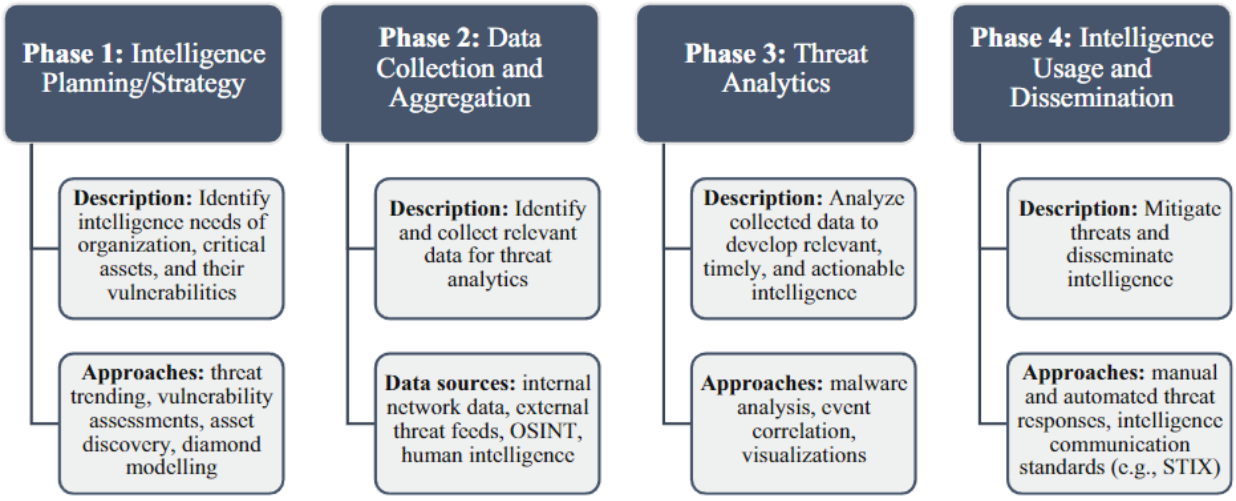


Figure B.5: Model 5 (Samtani et al., 2020, p. 3)

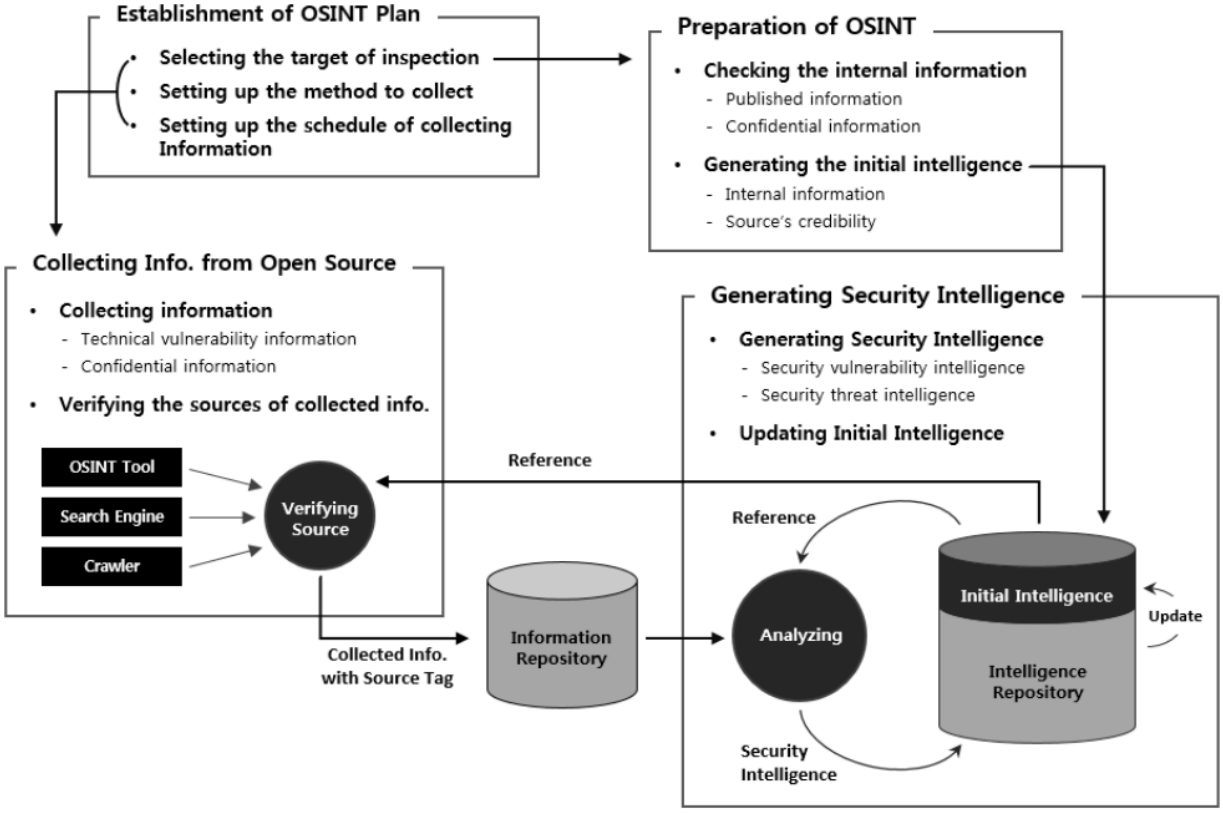


Figure B.6: Model 6 (Lee & Shon, 2016, p. 1031)

C Codebook for coding trancripts

A table representation of the codebook for the interview transcripts. Codes in *italic* are subcodes of the previous code, also marked by indenting. The two columns at the right indicate the number of files being referenced with that code and the number of total references across all files. Codes with zero files or references do not indicate that they were irrelevant but that the content was coded with a more specified subcode.

Code	Strategy used	Description	Files	Ref.
Analysis	Deductive	How is information analyzed?	3	3
Relevance	Deductive	How is the collected information kept relevant?	7	16
Reliability	Deductive	How is the reliability of information evaluated?	8	24
Collection	Deductive	How is OSINT collected?	0	0
Procedure	Deductive	How is the process of the collection? Ex. reactive, proactive, ad-hoc, systematic etc.	2	6
Proactive	Deductive	Collection method	4	11
Reactive	Deductive	Collection method	4	8
Tools	Deductive	How is OSINT collected?	1	1
Gov. org	Inductive	Through governmental sources	3	4
Media	Inductive	Through media	2	2
Network	Inductive	Through network and co-workers	6	17
Telegram	Inductive	Through the social media app Telegram	3	3
Third-party	Inductive	Through a third-party provider	8	20
Twitter	Inductive	Through Twitter	2	5
Dissemination	Deductive	How is OSINT disseminated?	0	0
Information sharing external	Deductive	How is the intelligence shared externally?	5	9
Information quality	Inductive	Information quality is influenced by external sharing	1	1
Understand information relevance	Inductive	Information relevance is influenced by external sharing	1	1

Information sharing internal	Deductive	How is the intelligence shared internally?	6	24
Adapt the content	Deductive	Thoughts on the adaption of content	8	20
Feedback	Deductive	Thoughts on feedback	8	10
Trustworthiness	Inductive	Thoughts on the importance of trustworthiness	2	6
DCF feedback	Deductive	Feedback from the interviewees on the deductive conceptual framework	5	7
Planning	Deductive	How is the usage of OSINT planned prior to collection?	1	2
Communication	Deductive	Focus on the communication between consumer and analyst	6	16
Evaluation of OSINT	Deductive	How is OSINT evaluated as being the correct intelligence capability for the intelligence requirement(s)?	4	7
Intelligence requirements	Deductive	Are intelligence requirements made? How?	7	14
Analyst initiative	Inductive	By the analyst's initiative	3	7
Requests from leaders	Inductive	By request from leaders/C-suite/decision-makers	6	9
Knowledge base	Deductive	Is a knowledge base/information repository used? How?	5	5
Products	Deductive	Tools/products used during planning	2	2
Unknown unknown	Inductive	Thoughts on "unknown unknowns"	1	2
Usage of OSINT	Deductive	General information regarding the usage of OSINT	1	1
Challenges	Deductive	Thoughts on challenges of using OSINT	2	3
Information overload	Deductive	Challenge	6	11
Not specified enough	Deductive	Challenge	3	4
Weak signals	Inductive	Challenge	1	1

Definition of OSINT	Deductive	Thoughts on the definition of OSINT	4	7
Duration	Deductive	How long has the organization used OSINT?	3	3
High maturity	Inductive	Segments that reflect on the interviewee's maturity towards the usage of CTI/OSINT in terms of their own capabilities, and what CTI/OSINT can provide of value	6	12
Lack of knowledge	Inductive		1	1
Low maturity	Inductive	Segments that reflect on the interviewee's maturity towards the usage of CTI/OSINT in terms of their own capabilities, and what CTI/OSINT can provide of value	3	11
Motivation	Deductive	Why did they start using OSINT?	6	8
Being proactive	Deductive	Motivational factors	4	16
Decision-making support	Deductive	Motivational factors	6	17
Define threat landscape	Deductive	Motivational factors	6	15
Information access	Deductive	Motivational factors	4	8
Organization of workforce	Deductive	Size of workforce dedicated to work with OSINT	5	7
Situational awareness	Inductive	Thoughts on how OSINT influences situational awareness	9	20
Size of workforce	Deductive	How many are prioritized to work with OSINT	6	8
Time horizon	Deductive	The time horizon in which CTI is aimed to provide value	4	5

Table C.1: Codebook for interview transcript analysis

D Consent Form for Interviewees

Are you interested in taking part in the research project

"A framework for the use of open source intelligence in organizations for cyber defense" ?

You are invited to participate in a research project where the main purpose is to develop a framework that tries to standardize the process of information extraction when using open-source intelligence (OSINT) for cyber defence within an organization. In this document, you will find further information about the project's purpose and what participating in the study will entail for you.

Purpose of the project
The project is a 30-credit master's thesis to be conducted in the spring of 2023.

The research question of the thesis is as follows: "How can one understand the current processes of using open-source intelligence for cyber defense within organizations?"

The purpose of the master's thesis is to develop a framework that explains and/or standardizes how organizations can use OSINT as a resource for security work in the company. The framework will be based on information and input from both theory and conversations with interviewees. It is desirable to conduct interviews with individuals from companies where OSINT is currently used to gain a better understanding of how information is gathered through open sources and how this affects the company's security work. It will also be relevant to discuss the company's current process(es) for collecting OSINT, the advantages the company experiences through the use of OSINT and highlight any challenges. Since relevant information for the company is essential for security work, it is particularly interesting to highlight how the company ensures that the collection includes relevant information, and not incorrect or misleading information, and how this assessment is made in the company.

Which institution is responsible for the research project?
University of Agder (Norway) – Faculty of Social Sciences is responsible for the project (data controller).

Why are you being asked to participate?
I wish to invite you to participate in this project because you are employed in a company where OSINT is currently used for security work and/or have knowledge/experience from the use of OSINT that is valuable for this master's thesis.

Recruitment of participants is done through personal networks and acquaintances, as well as by asking already recruited participants for suggestions for other participants who may be relevant for the project.

What does participation involve for you?
If you chose to participate in this project, it will involve that you participate in an online interview through Teams. Sound and video will be recorded through the record functionality in Teams. In the interview, we will go through the themes and questions elaborated in the project's purpose and in the shared interview guide containing the questions. The interview is set to last a maximum of 50 minutes.

Participation is voluntary
Participation in the project is voluntary. If you chose to participate, you can withdraw your consent at

any time without giving a reason. All information about you will then be made anonymous. There will be no negative consequences for you if you chose not to participate or later decide to withdraw.

Your personal privacy – how we will store and use your personal data
We will only use your personal data for the purpose(s) specified here and we will process your personal data in accordance with data protection legislation (the GDPR).

- Only I, Johanna Sofie Slinde, and my supervisor, Jaziar Radianti, will have access to the data collected.
- To ensure that unauthorized personnel do not gain access to personal information, audio and video recordings will only be stored on a locked OneDrive managed by the University of Agder. The recordings will be deleted as soon as they are transcribed. The transcribed document will also be stored only on the aforementioned OneDrive.
- Name, gender, job title, company, and other identifiable information will be anonymized and replaced with a code stored in a separate name list separated from other data after transcription. This ensures that you as a participant will not be able to be identified during the publication of the master's thesis.

What will happen to your personal data at the end of the research project?
The planned end date of the project is mid-summer 2023. Sound- and video recordings will be deleted as soon as all material is transcribed during the spring 2023. As the project ends, the documents containing the transcriptions will also be deleted.

What gives us the right to process your personal data?
We will process your personal data based on your consent.

Based on an agreement with *University of Agder (Norway) – Faculty of Social Sciences*, The Data Protection Services of Sikt – Norwegian Agency for Shared Services in Education and Research has assessed that the processing of personal data in this project meets requirements in data protection legislation.

Your rights
So long as you can be identified in the collected data, you have the right to:

- access the personal data that is being processed about you
- request that your personal data is deleted
- request that incorrect personal data about you is corrected/rectified
- receive a copy of your personal data (data portability), and
- send a complaint to the Norwegian Data Protection Authority regarding the processing of your personal data

Where can I find out more?
If you have questions about the project, or want to exercise your rights, contact:

- *University of Agder, Faculty of Social Sciences* via supervisor Jaziar Radianti, jaziar.radianti@uia.no

- *University of Agder, Faculty of Social Sciences via student Johanna Sofie Slinde, johannass@uia.no*
- Our Data Protection Officer: *Trond Hauso, personvernombud@uia.no*

If you have questions about how data protection has been assessed in this project by Sikt, contact:

- email: (personverntjenester@sikt.no) or by telephone: +47 73 98 40 40.

Yours sincerely,

Jaziar Radianti	*Johanna Sofie Slinde*
(Supervisor)	(Student)

Consent form

I have received and understood information about the project *A framework for the use of open source intelligence in organizations for cyber defense* and have been given the opportunity to ask questions. I give consent:

- ☐ to participate in *an interview*

I give consent for my personal data to be processed until the end of the project.

(Signed by participant, date)

E Interview Guide

Intervjuguide

Masteroppgave i cybersikkerhetsledelse ved Universitetet i Agder (UiA), våren 2023

Student: Johanna Sofie Slinde

Veileder: Jaziar Radianti

Tusen takk for at du ønsker å delta i dette intervjuet for min masteroppgave «Et rammeverk for bruk av frikildeetterretning i norske organisasjoner for cyberforsvar». Hensikten med intervjuet er å kartlegge hvordan du og din bedrift drar nytte av OSINT for å styrke deres cyberforsvar. Funn fra intervjuet vil være med på å konstruere et rammeverk/model som beskriver hvordan bedrifter kan dra nytte av OSINT for cybersikkerhetsarbeid, med fokus på hvilke handlinger og valg som er spesielt viktig for at bruken av OSINT skal få størst mulig verdi for bedriften.

Spørsmålene i dette dokumentet vil bli brukt for som utgangspunkt for intervjuet, og det er ønskelig at samtalen holdes rundt disse temaene som belyses. Estimert tid for intervjuet er 50 minutter.

Intervjuet vil bli tatt opp via båndopptaker (fysisk interjvu) eller via Teams sin opptaksfunksjon (digitalt intervju). Utfyllende informasjon om hvordan personopplysninger håndteres og oppbevares finnes i dokumentet «Informasjonsskriv_samtykke». All informasjon vil bli anonymisert ved publisering i masteroppgaven.

Del 1: (Kort) Generell informasjon om deg og din arbeidsplass' forhold til OSINT

1. Kan du fortelle litt om din rolle og arbeidserfaring i organisasjonen/bedriften?
2. Hvordan definerer du OSINT/frikildeetterretning?
3. Hvor lang er din erfaring med bruk av OSINT som innhentingskapabilitet og som en del av sikkerhetsarbeidet i bedrifter?
4. Jeg vet at dere bruker data og informasjon innhentet fra åpne kilder som en del av deres cyberforsvar. Kan du fortelle noe om hvor lenge dere har drevet med innhenting fra åpne kilder?
    a. Hvorfor begynte dere med det på det tidspunktet?
    b. Hva var motivasjonen?
5. Hvor stor andel av deres cyber-avdeling er prioritert til å jobbe innenfor dette området, sammenlignet med andre avdelinger hos dere innen cyber (f. eks sammenlignet med andelen som jobber med testing, patching etc.)?
    a. Har det vært noe økning i det siste med tanke på økt frekvens av alvorlige cyberangrep mot alle typer bedrifter de siste årene?

Del 2: Prosess – Styring og innhenting

1. I din organisasjon, har dere klare prosesser for opprettelsen av nye etterretningsbehov?
    a. Hvordan er dialogen innad i organisasjonen i denne prosessen – hvem snakker med hvem?
    b. Hvordan kommer dere vanligvis frem til et eller flere bestemte etterretningsbehov?
2. Etter at et etterretningsbehov er opprettet – kan du fortelle om prosessen videre frem til analyse av innhentet informasjon?

a. Hvordan vurderer dere om OSINT er rett innhentingskapabilitet for etterretningsbehovet?
b. Noen tanker om forholdet mellom «bestiller» og «analytiker» - hvor og hvordan mye fokuseres det på lik forståelse av etterretningsbehovet?

Del 3: Prosess – Analyse, vurdering og formidling

1. For at informasjonen som uthentes skal ha etterretningsverdi må den også ha en relevans for bedriften – hvordan sørger dere for at informasjonen som uthentes holdes relevant for dere igjennom hele prosessen?
    a. Hvordan vurderer dere relevant informasjon fra irrelevant informasjon?
2. Hvordan forsikrer dere dere om at informasjonen som er uthentet kan stoles på? Hva er prosessen for informasjonsvalidering?
3. Etter at dere er forsikret om at informasjonen er relevant og validert, hvordan distribueres denne informasjonen videre i organisasjonen?
    a. Deler dere informasjonen også til andre organisasjoner?
        i. Hvordan
        ii. Hvem

Johanna presenterer et eksempel på en etterretningssyklus (sammensatt av ulike versjoner fra litteraturen)

Etter at vi nå overordnet har gjennomgått hvordan en etterretningssyklus kan se ut – hvordan vil du si at denne syklusen passer inn i det du nettopp har beskrevet?

Del 4: Verdien av frikildeetterretning

1. Hva anser du som største verdien din organisasjon/bedrift kan trekke ut av OSINT?
2. Har du eller din organisasjon opplevd noen mindre positive eller negative konsekvenser av å benytte seg av OSINT?
    a. Hvis ja – kan du forteller litt mer om det?
    b. Hvis nei – kan du tenke deg til en mindre positiv eller negativ situasjon som kunne oppstått?
3. Sammenlignet med andre måter bedriften deres forbereder seg på cyberangrep på (sårbarhetstesting, ROS-analyser, oppdatering av systemer og generell sikkerhetsbevisstgjøring blant ansatte etc.) – anser du OSINT som en dårligere, like bra eller bedre måte å forberede seg mot cyberangrep på?
    a. Hvorfor?
4. Å innhente informasjon om trussellandskapet kan gjøre organisasjonen bedre forberedt på trusler en kan forvente – hvilken effekt har bruken av OSINT hatt for din organisasjons/bedrifts situasjonsbevissthet innen cyberområdet?
    a. Har du noen tanker om situasjonsbevisstheten har blitt bedre etter at frikildeetterretning ble benyttet?