Master's thesis

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

Jarl Goksør

Cyber Threat Intelligence

Impact and Utility

Master's thesis in Experience-based Master in Information Security
Supervisor: Sokratis Katsikas
May 2024

NTNU
Norwegian University of
Science and Technology

Jarl Goksør

Cyber Threat Intelligence

Impact and Utility

Master's thesis in Experience-based Master in Information Security
Supervisor: Sokratis Katsikas
May 2024

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Norwegian University of
Science and Technology

Abstract

Today's cyber threat landscape is characterized by immense volume, entropy, and opportunistic actors, forcing defenders to prioritize finite resources. For this purpose, Cyber Threat Intelligence (CTI) is an increasingly popular cybersecurity function, which aim to reduce knowledge asymmetry, guide defensive efforts, and improve decision making.

With a few exceptions, existing research have mostly focused on various quality factors, without exploring its real impact and utility. This thesis aimed to bridge that gap, by investigating *how CTI provides utility for organizations*. The problem statement is answered by looking at CTI's effect on security posture and on decision making processes, as well as by examining CTI utility factors and organizations' ability to exploit CTI's potential. A qualitative research design was selected to gain insight into the causal processes and outcomes of CTI in real private and public sector organizations.

The research suggests CTI has an overall positive impact, primarily through early warning leading to more proactive and efficient defense operations. Moreover, strategic level insights inform investment decisions and complement risk assessments. Yet on both accounts, many struggle with substantiating this impact and attributing specific security improvements or decisions solely to CTI. Even where clear causal links between CTI and decisions exist, assessing actual outcomes remains challenging.

The most important utility factor was found to be relevance, understood in this context as added value in the shape of analytical output or unique collection. Analytical tradecraft is also a defining feature of CTI. Arguably, some services being sold as CTI lack this property, which risks diluting CTI as a discipline. In this context, poor professionalism and accuracy in the CTI industry also risk undermining trust, another key utility factor.

Lastly, there is a significant disparity among end users' ability to exploit CTI. Organizations with mature cybersecurity programs are better able to direct and specify requirements, and are more aware of how and where it has effect and what is required to extract net value.

The findings of this study suggests that CTI indeed holds potential as a strategic asset. But realizing this potential requires organizational commitment, a mature cybersecurity program, and a refined understanding of CTI's capabilities and limitations as well as of their own requirements.

Sammendrag

Dagens cybertrussellandskap kjennetegnes av et enormt volum, entropi og opportunistiske aktører, som tvinger forsvarere til å prioritere begrensede ressurser. For dette formålet er Cyber Threat Intelligence (CTI) en stadig mer populær funksjon, hvis mål er å redusere kunnskapsasymmetri, veilede forsvarstiltak og forbedre beslutningstaking.

Med noen få unntak har eksisterende forskning primært fokusert på ulike kvalitetsaspekter, uten å utforske den reelle innvirkningen og nytteverdien. Denne masteravhandlingen satt som mål å tette dette gapet ved å undersøke hvorledes CTI gir nytte for brukerorganisasjoner. Problemstillingen blir besvart ved å betrakte CTIs innvirkning på beslutningsprosesser og på sikkerheten totalt, samt ved å undersøke CTIs kvalitetsfaktorer og organisasjoners evne til å utnytte CTIs potensiale. En kvalitativ forskningsmetode ble valgt for å få innsikt i årsakssammenhenger og resultater av CTI i reelle private og offentlige virksomheter.

Studien indikerer at CTI har en generelt positiv innvirkning, primært gjennom tidlig varsling som fører til mer proaktive og effektive forsvarstiltak. Strategiske vurderinger kan understøtte investeringsbeslutninger og risikovurderinger. Likevel sliter mange med å begrunne denne innvirkningen og tilskrive spesifikke sikkerhetsforbedringer eller beslutninger utelukkende til CTI. Selv der klare årsakssammenhenger mellom CTI og beslutninger eksisterer, er det utfordrende å vurdere reelle resultater av beslutningene.

Den viktigste kvalitetsfaktoren er relevans, forstått i denne sammenheng som merverdi i form av analyse eller unik innhenting. Analytisk håndverk er også en definerende egenskap ved CTI. Noen tjenester som selges som CTI mangler denne egenskapen, hvilket risikerer å utvanne CTI som disiplin. I denne sammenhengen risikerer også dårlig profesjonalitet og unøyaktighet i CTI-bransjen å undergrave tillit, en annen nøkkelfaktor.

Til slutt er det en betydelig forskjell i sluttbrukernes evne til å utnytte CTI. Organisasjoner med modne cybersikkerhetsprogrammer er bedre i stand til å styre og spesifisere krav, og er mer bevisste på hvordan og hvor det har effekt og hva som kreves for å oppnå netto nytteverdi av tjenestene.

Studien antyder at CTI innehar potensial som en strategisk rssurs. Men å realisere dette potensialet krever at organisatorisk satsing, et modent cybersikkerhetsprogram, og god forståelse for CTIs evner og begrensninger så vel som forståelse for deres egne behov.

Contents

Figures

Tables

Acronyms

CERT Computer Emergency Response Team. 49

CISO Chief Information Security Officer. 45

CTI Cyber Threat Intelligence. 1

EBITDA Earnings before interest, taxes, depreciation, and amortization. 45

GRC Governance, Risk, and Compliance. 48

IR Intelligence/Information Requirement. 10

IRM Intelligence Requirements Management. 10, 60

MISP Malware Information Sharing Platform. 49

NIST National Institute of Standards and Technology. 1

ROI Return on Investment. 46

SOC Security Operations Center. 40

Chapter 1

Introduction

Digitization has increasingly permeated society in almost every realm, spanning economic, military, public, and private sectors. This has created vast opportunity, but also vulnerabilities that are exploited to our detriment every day.

The threat landscape has changed significantly over the last decade. As the digital economy grows, and every aspect of public and private life is increasingly digitized, both incentives and opportunities for malicious actors in cyber space have grown in tandem. Fortunately, the downsides of digitization is not lost on the public, as demonstrated by surging focus and spending on cyber defense measures. For instance, bank JP Morgan Chase spends around 600 million USD yearly and employs over 3000 in cyber security [1].

As such, information security has emerged as a vital activity, as opposed to an afterthought which was often the case in the nascent days of digitization. Although spending and awareness has gone up, there is a common understanding that threat actors are always one step ahead of defenders, constantly evolving their methods and tactics as vulnerabilities are fixed or effective security processes are implemented. Attaining completely secure systems while also maintaining usability is infeasible. Thus, defenders must evaluate their own assets and liabilities, and prioritize defensive efforts accordingly.

Cyber Threat Intelligence (CTI) is an increasingly popular method of guiding defensive efforts. NIST defines threat intelligence as:

> Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes [2].

CTI aims to elucidate the threat landscape and reduce the knowledge asymmetry between attackers and defenders. CTI is ideally tailored according to specific customer requirements, and encompasses both a product and a process. Consequently, its effective exploitation is demanding, meaning it is mostly reserved for larger organizations with dedicated security budgets. These aspects will be discussed extensively throughout this thesis.[1]

[1]Note that a project plan was conducted at NTNU prior to this thesis [3]. While substantially

1.1 Keywords

Security and Privacy Protection, Information Security, Information Technology and Systems, Threat Intelligence, CTI

1.2 Planned Contribution

The importance of information security has created an entire industry of experts and services, one of which is centered around CTI. Given the commercial aspect of CTI, the industry is incentivized to sell those services, which necessitates impartial scrutiny and research into its validity. The impact and efficiency of process-oriented solutions can be difficult to substantiate. While CTI certainly make sense conceptually, it is prudent to assess why or how it provides value, and under what circumstances. If CTI's purpose is to improve decision making processes with regard to an organization's defensive posture, this author argues that the decision maker's initial information requirement should be how CTI can deliver exactly that, and whether adopting a CTI service is suitable for their organization. Some research has been conducted on CTI, as detailed in Section 2.2. Mostly this research is focused on various quality factors and best practices, but generally the benefits of CTI are seen as given. Meanwhile, little research has been done on how CTI affects an organizations cyber security posture in practice, and not the least how it affects organizational processes and decision making.

This thesis aims to reduce this knowledge gap by conducting a qualitative examination of real life accounts centering on these very questions. By investigating a sample of current practice through the prism of theoretical frameworks and expert guidelines, this work can hopefully inform future and current adopters on what factors have significance for an effective CTI program.

1.3 Research Questions

The overall problem statement is as follows:

How does Cyber Threat Intelligence provide utility for organizations?

The problem statement will be answered through the following research questions:

- RQ1: What effect does CTI have on organizations' security posture?
- RQ2: How does CTI affect stakeholder's decision making processes?
- RQ3: What factors determine CTI utility?
- RQ4: How are organizations able to exploit CTI?

changed since then, the general concept remains the similar. As such, elements of the introduction chapter are carried over from said plan.

RQ1 aims to answer how CTI impacts organizations' security by examining what tangible outcomes can be traced to CTI, to the extent respondents possess that visibility. Do they see an overall benefit? What changes are made based on CTI? Further, a core tenet of CTI is its function as decision support. RQ2 will detail how CTI affects the more abstract realm of decision making processes relevant to information security. RQ3 will look closely at what factors intrinsic to CTI are perceived to determine utility value. In other words, what features of CTI are important for users? Lastly, since CTI is process oriented it requires a certain level of organizational involvement to exploit. RQ4 will examine to what extent the surveyed organizations possess the required ability or willingness to extract its potential.

1.4 Thesis Outline

The structure of this thesis is as follows:

- Chapter 1 Introduction
- Chapter 2 Background and Related Work - Details the theoretical framework for CTI and Intelligence in general,. This including best practices, principles, use cases, and discussions of the most significant aspects of the CTI process. The results of the literature review is also included in this chapter.
- Chapter 3 Methodology - Discusses methods considered and what were choices made on data collection and analysis.
- Chapter 4 Results - Presents the results of the data collection, structured by themes that were identified during analysis.
- Chapter 5 Discussion - The results are discussed in with regard to the theory chapter, answering the research questions. Includes partial conclusions for each question for greater clarity and readability.
- Chapter 6 Conclusion

Chapter 2

Background and Related Work

This chapter provides background information on Cyber Threat Intelligence. It details key definitions and concepts, as well as theoretical frameworks explaining the state of the art for CTI today. This will serve as an important baseline when analyzing the empirical data in chapters 4 and 5. Finally, the chapter also presents the literature study for this thesis.

2.1 Cyber Threat Intelligence

CTI is a relatively new phenomenon, emerging as a discipline the last 10-15 years in conjunction with society's rapid digitization and subsequent focus on cybersecurity. Meanwhile, many principles and processes on which CTI rely have their origin from the deep historical roots of the Intelligence domain in general. As such, CTI is not simply another stand alone cybersecurity system, and should not be thought of as an add-on to an existing cyber defensive suite, but rather as a permeating organizational function that guides cybersecurity efforts and more.

The concept of 'Intelligence' can have many meanings. It can refer to the process or act of conducting Intelligence work, the resulting products, or even an Intelligence unit itself [4]. Here we will focus on the former two: The Intelligence process and its organizational implications, and Intelligence products and their utility. It should be noted that this thesis does not aim to discuss Intelligence as an academic discipline or explore its various points of contention, of which there are many. Still, any understanding or analysis of CTI is arguably incomplete without some foundational knowledge on Intelligence in general.

Before continuing, it is useful to explore some core terms and definitions. Commonly, the literature points to distinctions between *data*, *information*, and *Intelligence*. Unsurprisingly, no consensus or authoritative definition exist. In essence, the difference can be summarized as the degree of processing, organization, and contextual meaning (see Figure 2.1 for an illustration).

Meanwhile, the term 'Cyber Threat Intelligence' warrants a precise definition. Crowdstrike, a commercial cybersecurity firm uses the following:

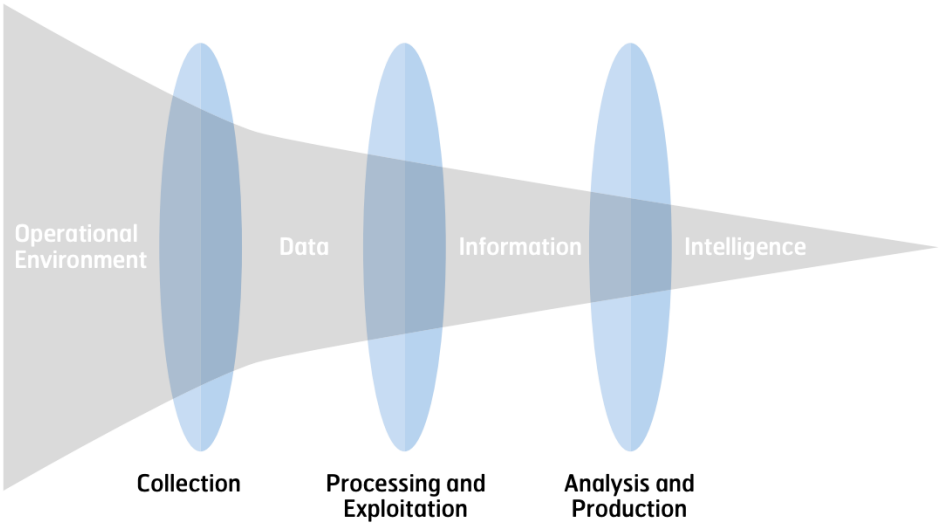


Figure 2.1: Relationship between data, information, and Intelligence [5]

> *Threat Intelligence is data that is collected, processed, and analyzed* ***to understand a threat actor's motives, targets, and attack behaviors****. Threat Intelligence enables us to make faster, more informed, data-backed* ***security decisions and change their behavior*** *from reactive to proactive in the fight against threat actors [6].*

A similar sounding definition by NIST is included in chapter 1. It can be useful to view these alongside the broadly adopted NATO-definition of Intelligence:

> *Intelligence is the product resulting from the* ***directed*** *collection and processing of information regarding the operating environment and the capabilities and intentions of actors, in order to identify threats and* ***offer opportunities for exploitation*** *by decision-makers [4].*

Two major points are highlighted in each definition. The first alludes that Intelligence is purposeful: Collection and analysis is done with a clear objective. The NATO-definition is even more succinct, saying that the product results from a *directed* effort. The dialogue with, and direction from, stakeholders, is a defining feature of Intelligence work, and arguably has great bearing on utility.

The second point is stated explicitly in both definitions, and summarizes the purpose of Intelligence: Change decision maker behaviour and create opportunity to exploit the situation for a more favorable outcome. In other terms, Intelligence has value when it improves decision making, whether decisions actually change or if it provides more confidence in current trajectory and posture.

2.1.1 Purpose and Usefulness

The purpose of Intelligence and CTI has been touched upon in section 2.1, with the definitions capturing it reasonably well. But such a foundational subject call for more elaboration. Kovacs [7] discussed the use of Intelligence, focusing on the age-old issue of tying purpose with a measure of usefulness. To being with, he criticizes much of the Intelligence literature for omitting or downplaying usage and the user perspective. While recognizing that much Intelligence work will never be used, he nevertheless argues:

> [...] since Intelligence is not an end unto itself, he intended use of the intelligence should be a guiding principle in all stages of intelligence work [...] When this is not so, we end up with intelligence agencies producing intelligence for other agencies or for the sake of intelligence. They go through collecting, evaluating, analyzing, writing reports and shipping them out - scarcely knowing nor caring about who reads them and to what purpose

Moreover, Kovacs acknowledges that evaluating Intelligence usage is both theoretically and practically difficult. While many authoritative figures attempt to judge Intelligence by various criteria such as accuracy and timeliness (see also subsection 2.1.6 and section 2.2), Kovacs posit that these attributes do not really give any indication of how 'useful' the Intelligence is. Instead, he suggests that we distinguish between 'usability' (encompassing said attributes), and 'usefulness' [1]. The former is a measure of *potential*, while the latter is a measurement of *actual* effectiveness. Ultimately, this effectiveness is related to stakeholder action. As military Intelligence expert R.V Jones put it:

> The test of good intelligence services is not merely that you were right, it is that you persuaded your operational or research staff to take the correct measures. [...] The ultimate object of intelligence is to enable action to be optimized [7]

Consequently, effectiveness is an attribute extrinsic to the Intelligence product, and one that can only be evaluated, still with great difficulty, post-facto.

Expanding on output as a measure, Professor Ernest May suggest another aspect to consider:

> A better test than either accuracy or acceptability may be simply whether assessments address the right question: that is, the question right answers to which could be useful guides to action [7]

Distilling these arguments we're left with three aspects that will have bearing on this thesis:

[1] Throughout this thesis we use 'utility' instead of Kovacs' 'usability', as it was found to be more appropriate. Ultimately, both terms convey the same meaning: Intrinsic properties of CTI.

1. Stakeholder action as a measurement of utility
2. Dissemination and communication is crucial to achieve effect
3. The importance of user involvement in the Intelligence process to ensure that the right questions are addressed

These considerations will be explored further in the discussion section.

2.1.2 CTI: Users and Use Cases

Larger organizations, having more valuable assets and business processes, will typically require more sophisticated security programs. Likewise, even smaller organizations can have outsized cybersecurity liabilities if their business case depends on trust or particularly valuable digital resources. Ultimately, security investments in any organization is a result of risk appetite and available resources. This begs the question: Who can benefit from CTI?

The UK National Cyber Security Centre (NCSC) has advised governmental entities on the possible adoption of Threat Intelligence led security programs, in a 2019 white paper[8]. With many governmental departments having nascent CTI programs or considering their establishment, NCSC suggests some fundamental conditions to be met before proceeding:

1. CTI programs are likely valuable only for users that already has a **mature** cybersecurity posture. As a rule of thumb, NCSC recommended that organisations should only make significant CTI investments after achieving or being on a realistic roadmap to completing all of their other recommended cybersecurity standards. Furthermore, even mature organisations should only establish Threat Intelligence programs if they have the capacity, capability, and intent to actually utilize it. This entails not only the technical aspects: System owners must be empowered to act on Threat Intelligence for it to have meaning.
2. Resources will always be scarce in any organization, and CTI is a broad field. Since many service vendors, products, and customers are immature, proper strategising and piloting is important to both explore requirements and to discover what functions and use cases are important for a particular organisation.

Section 2.1 detailed CTI as a concept and provided some definitions. As those descriptions lean towards the abstract, a reference to more practical use cases is useful. Again, the NCSC provides some good examples that are worth citing verbatim (see Figure 2.2). The rightmost column, 'Intelligence Required', can indeed be considered Intelligence products on its own. However, I argue that the true purpose of Threat Intelligence is not achieved until these products are utilized towards the ends described under 'Objective'.

Use Case	Objective	Intelligence Required
Validate Alarms/Events	Validate alarms/events and decide which to escalate to the incident response team for remediation.	Threat data: data connecting individual indicators, threat actors, techniques, etc.
Enhance Automated Response	Automate the triage process of investigations by helping Security Information and Event Management (SIEM) and analytics tools correctly prioritise alarms and events presented to the CTI lead/analyst.	Threat data: threat indicators and severity ratings, linked to attacks targeting specific industries, applications, etc.
Inform Departmental Risk Profession	Enhance the security assurance and risk management process with contextual content from intelligence gathering	Threat data: threat indicators and severity ratings, linked to attacks targeting specific industries, applications, etc.
Prioritise Vulnerabilities	Create a metric for evaluating vulnerabilities, by measuring the overlap between the problems which can be fixed and those with the most impact, given the time and resource available.	Vulnerability data: CVEs linked to attacks against specific industries, CVE's linked to specific threat actors, etc.
Support Threat Hunting	Proactively uncover hidden attacks on a department's network, related to current incidents, or threats targeting the department.	Threat data: indicators with links to context regarding campaigns, threat actors, techniques, history and targets.
Contain and Remediate Attacks	Disrupt attacker communications/ command and control, remove malware.	Threat data: intelligence knowledge base including data on techniques, history and targets of various threat actor groups.
Anti-Phishing	Enhance existing mail protection capabilities by enriching detection datasets with indicators.	Threat data: indicators with links to context regarding campaigns, threat actors, techniques, history and targets.

Figure 2.2: NCSC CTI Use Cases [8]

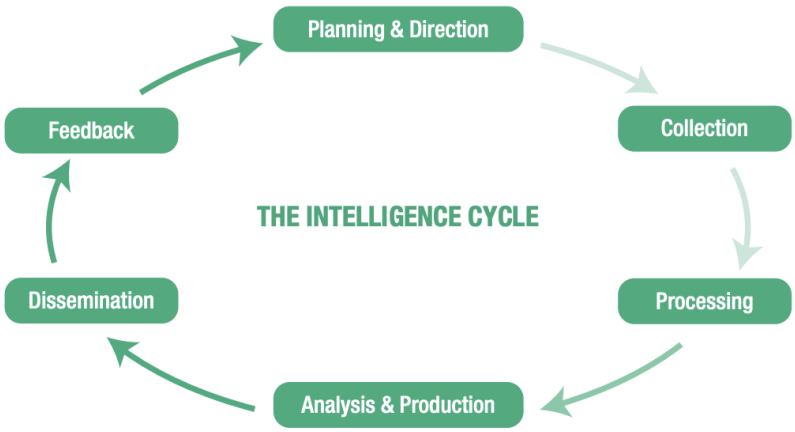


Figure 2.3: The Intelligence Cycle [9]

2.1.3 The Intelligence Cycle

To understand CTI on a conceptual level, we should first look at the 'Intelligence Cycle', which (nominally) depicts the Intelligence process. The cycle looks similar regardless of subject matter, field, theme, or so-called Intelligence discipline (e.g. Signals Intelligence, Human Intelligence, Open Source Intelligence). While CTI is not a traditional Intelligence discipline per se, instead encompassing various open and secret collection methods, the salience of the Intelligence cycle still holds true. Note that despite the name, it is seldom cyclical in nature. In reality most steps or activities, while tightly interdependent, are conducted continuously and in parallel, and is never really 'completed'. Nonetheless, the Intelligence cycle is still useful in depicting the components that together constitute Intelligence work.

The cycle comes in many forms, but almost always includes the four steps of *planning*, *collection*, *analysis*, and *dissemination*. Figure 2.3 shows a slightly higher granularity of six steps, but for the short elaboration below we will merge into four [9].

1. **Planning and direction**
   This is the domain of arguably one of the most important and defining aspects of Intelligence: Information/Intelligence Requirements (IR). The mission direction is determined, ideally based on a thorough and continuous dialogue with stakeholders. Here the CTI unit prioritizes their efforts; what vulnerabilities are most critical for the organization; what threats and threat actors are most important; what information is actually needed by information security functions; what means can be used to answer those requirements. Many of these questions could be derived from an overall risk assessment. Finally, planning should also account for available resources, in terms of both analytical capacity and collection capability. One should also be familiar with the related term Intelligence Requirements Management

(IRM), which in addition to the IR process also highlights the importance of managing collection resources as an integrated task.

2. **Collection and processing**
   Once IRs and the overall direction is determined, collection can commence. Collection can be conducted by many means, and data types can vary greatly depending on use case. For example, CTI units may rely on several open or commercially available repositories containing updated Threat Intelligence on specific threats, vulnerabilities, adversary TTPs, signatures, or ongoing attacks campaigns. Many CTI-units may also have sensors within their own networks, or be privy to data streams from the sensors of larger public organizations or even Intelligence agencies.
   Data and information must be structured and organized, so as to enable further analysis. This step is often referred to as processing, and many CTI units may rely on commercial tools such as Threat Intelligence Platforms (TIP). Often an under appreciated step outside of analyst circles, effective processing is crucial to extract maximum Intelligence value from limited analytical capacity, and also to avoid circular reporting or false positives in data streams.
3. **Analysis and Production**
   Simply put, the analysis step is where data and information is turned into Intelligence. Herein, human analysts, advanced analytical tools, or usually a combination of the two, bring all processed information together to create insights or knowledge that can answer questions derived from the IR process. Analysts may also identify knowledge gaps: Lack of information that can be gathered by new collection, or new threats that previously had not been considered. The outcome of this step will be products that enable stakeholders and decision makers to improve their defensive posture, as ideally the CTI-products will be tailored towards the specific threats facing the organization.
4. **Dissemination and Feedback**
   The dissemination step is rather self-explanatory. 'Finished' CTI products are created in accordance with recipient needs and expectations. Format and type of contextualization will differ based on the consumer: For instance, 'raw' Intelligence may be continuously shared with other technical consumers in a STIX format, while a c-suite reader may only be interested in higher levels of abstraction focusing on what is relevant for their particular level and function. The importance of effective communication cannot be overstated. If the purpose of CTI is to elicit behavioral change or offer opportunities for exploitation, CTI products must be formed and communicated in a manner that easily conveys its utility.

2.1.4 Requirements-Driven CTI

Subsection 2.1.3 briefly described the 'Planning and Direction' part of CTI. However, the topic deserves some further elaboration to highlight its centrality to an effective CTI program. First we will refer to how planning is discussed in the 'traditional' Intelligence realm. The Norwegian Intelligence Service doctrine describes IRs as a component fundamental to the entire Intelligence process, the direction of which is the responsibility of leadership, but requires participation and input from all parts of the organization[4]. Importantly, precise IRs are predicated on:

1. Knowledge of what decisions are to be supported
2. What context the decision maker operates in
3. The decision makers' specific requirements for the delivery or completion of said IRs.

In other words, out-of-the-box solutions are unlikely to yield satisfactory results, apart from standardized collection streams that feed into *parts* of the overall solution. Moreover, the doctrine points out that another major advantage to a proper planning and direction process pertains to resource management. The IR development phase is also an opportunity for the organization to evaluate its own data and information base: Do we already have the necessary information to answer these IRs, or is additional collection needed? Good maintenance of the knowledge base can avoid superfluous human efforts, and not the least unnecessary acquisition of costly data streams.

From the CTI-specific domain, cybersecurity firm Mandiant suggested that firms should pursue 'requirements driven CTI', in a 2023 white paper [10]. The foundational argument is similar to that of the doctrine cited above: CTI is a means to empowering stakeholders, and understanding and producing on their requirements are therefore fundamental to delivering value in a resource-constrained environment. Continuing this argument, the paper contends that the introduction of any security program or framework presents a clear opportunity cost. Thus, while some may see this as an additional administrative process affecting a stretched security unit negatively, the argument for completing the effort is precisely *because of* resource limitations: Focusing on requirements benefits prioritization decisions and sets realistic expectations for different stakeholder needs. Clear requirements also provide the necessary focus for CTI teams under high workload. For example, security incidents may spawn myriad questions and demands for action from various stakeholders. Understanding the foundational requirements and priorities beforehand can reduce overhead and provide the necessary space to deal with the situation at hand.

Perhaps more powerful is an illustration of the opposite: What can a dearth of developed IRs result in? In Figure 2.4, Mandiant lists some common CTI pitfalls.

Pitfall	Description	Examples
Product-driven intelligence	The topics, format, and cadence of intelligence products are developed through habit and without consideration of whether it is useful or consumed by stakeholders—i.e., a CTI program that produces certain intelligence products because they have always done so.	• A quarterly industry threat report that is never read by stakeholders. • A weekly threat activity email report that does not fit with the security operation center's internal workflow (i.e., preference to consume intelligence via security platforms and/or via Slack).
Analyst-driven intelligence	Outputs focused on what analysts are interested in or perceive to be important. Leads to reports that do not consider stakeholder needs or the organization's threat profile.	• Extensive reporting on geopolitical developments within Iran and their impact on the cyber threat landscape for an organization that is rarely targeted by Iranian threat actors. • Majority of analyst time spent producing strategic reports within an organization that has predominantly tactical and operational CTI stakeholders.
Event-driven intelligence	Reactive and ad hoc reporting based on what is trending in the news without connection to the impact or why it matters to an organization.	• In-depth reporting on software vulnerabilities gaining attention in industry news which are not present on the organization's network. • Frequent reporting on destructive campaigns targeting industrial control systems for organizations with limited cyber-physical networks.

Figure 2.4: Common CTI pitfalls [10]

2.1.5 Intelligence Analysis as a Discipline

Recall from the definitions in section 2.1, that Intelligence products are distinguished from 'mere' information by a certain degree of analytical effort, among other characteristics. As this distinction will be important for the discussion part of the thesis, the topic of analysis warrants some more detail. Throughout the last few decades, Intelligence analysis has emerged as its a field of study on its own, often receiving an uptick after what has been considered major Intelligence blunders such as the Yom Kippur war or 9/11. Central to Intelligence analysis lies an adherence to scientific norms and principles, to the extent possible [4]. For instance, much focus should be put on having an reflective and transparent relationship to the analytical methods in play, such as induction, deduction, or abduction, and on actively addressing biases and logical fallacies. Proper analysis is also about providing structure in order to identify behaviors, patterns, and methods in the underlying data. Some popular formats within CTI include Open IOC, MITRE ATT%CK, and STIX [9].

Figure 2.5 depicts a cyber attack by with a combination of STIX and ATT%CK. By connecting the various components of cyber incidents in this manner, you can enable yourself or other defenders to take proactive actions against similar attacks, or get a head start in mitigating incidents that involve one or several of the same components. This type of illustration is a great example of the type of value-added context that makes Intelligence from varied information pieces.

Further structured analytical techniques (SAT) may be employed, such as scenario building, alternative competing hypotheses, SWOT/TOWS, or mind maps and decision trees [4]. Some are intended for more abstract and complex problem sets, while others may not be suitable in a day-to-day cyber context. Regardless, at a foundational level using SATs is intended to pull thought processes and analysis residing in the human mind into broad daylight. Together with focus on scientific principles and effort to counter biases, structured and rigorous analysis can serve myriad purposes:

- Enable collaboration
- Avoid circular reporting
- Enable traceability
- Encourage critical thinking
- Highlight assumptions and gaps
- Highlight uncertainty, confidence and probability scales
- Clearly communicate differences between reported information and analytical assessments

The analytical methods and techniques described here are not expected to be employed concurrently or exhaustively for a product to qualify as Intelligence. After all, Intelligence is also a process, the analysis of which rests on many smaller components such as collected raw data and information. But when discussing CTI overall, at least some form of structure or added context should be part of the package to step beyond the pure information sharing domain.

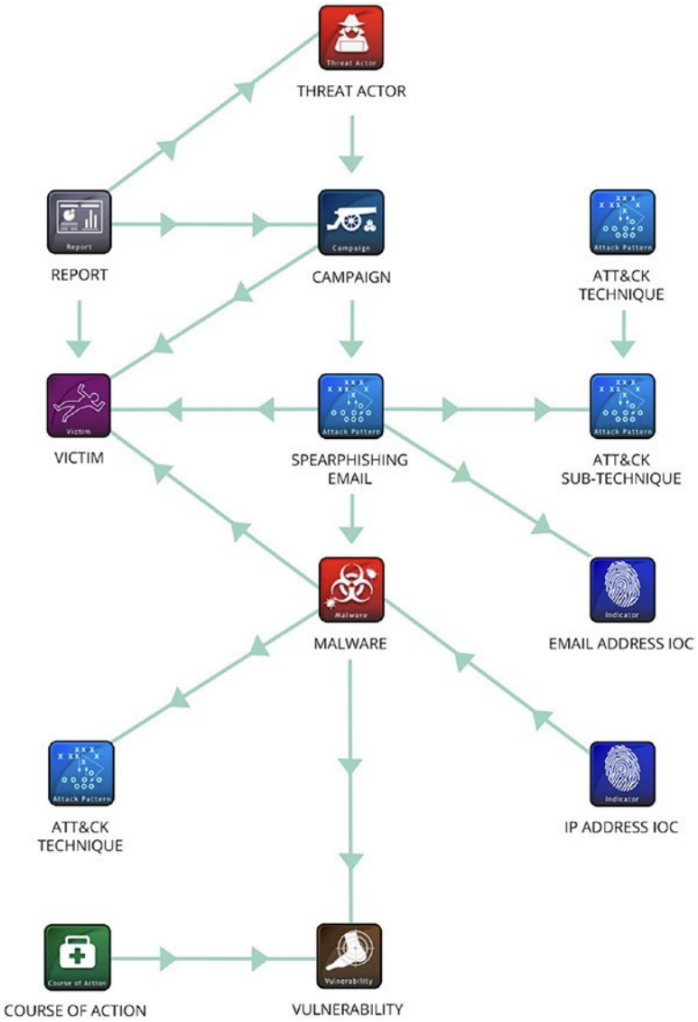


Figure 2.5: Structured illustration of a cyber attack[9]

2.1.6 Principles

In the field of Intelligence, numerous principles have been posited and developed by various organizations. Knowledge of such principles can be useful when studying and evaluating CTI quality and utility factors, as they will likely be familiar for many practitioners. One example of a set of CTI principles is the CROSSCAT-V model, recommended by entities such as Verisign and the UK Payment industry [5]:

- **Centralised Control**:
  A single point of control for Intelligence team simplifies interactions and eliminates duplication of effort.
- **Responsiveness**:
  The team must answer the question the customer asked, not the question the Intelligence team wishes to answer.
- **Objectivity**:
  An Intelligence team should not pick sides, no matter how emotive a subject.
- **Source and Methods Protection:**
  Sources of information (both human and non-human), an organization's technical capabilities and its operational methodologies are the lifeblood of an Intelligence team and must be protected.
- **Systematic Exploitation**:
  Intelligence is a methodological practice of research and review, using multiple sources and agencies.
- **Continuous Review:**
  Intelligence has a shelf life, and the Intelligence team must carry out a periodic review of their product to ensure it remains relevant.
- **Accessibility**:
  An Intelligence team must constantly balance the risk of its product falling into the wrong hands with the need for the customer to access that product.
- **Timeliness**:
  Delivering Intelligence products to customers in a timely fashion is central to the Intelligence function.
- **Vision**:
  The Intelligence team must consider possibilities that are not immediately obvious. Often, the vision of an Intelligence analyst, combined with the moral courage to voice an unconventional theory in an open forum, can make the difference between operational failure and mission success.

Albeit with other words, the principles quoted above correspond well with those of the traditional Intelligence field, as well as quality dimensions suggested by other industry experts (see section 2.2). Although adherence to such principles may not always be achieved in full, they nonetheless represent fundamentals that should strongly influence any proper CTI ecosystem.

2.2 Related research

This section provides summaries of relevant literature with regard to the research questions posited in section 1.3. The literature review was mostly conducted as part of a project plan preceding this thesis [3]. Consequently, substantial parts of this section have been carried over from said project plan, with some minor changes to reflect revisions to thesis direction and research questions. A few additional papers were also discovered after project plan completion. These are added starting here.

Some studies have examined the quality dimensions of Threat Intelligence. Zibak et. al [11] have conducted two of the most relevant studies for this thesis to build upon (primarily significant for RQ3). The first cited how both research and practice within CTI lack a common understanding of what factors influence the success of CTI management platforms, and attempted to capture success factors through an extended version of the Delone & Mclean information system success model [11]. The model prescribes the following success factors:

- Content quality
- System quality
- Service quality
- Perceived trust
- Use
- User satisfaction
- Net benefit

According to the authors, theirs was probably the first attempt to empirically validate the success of CTI management models. The empirical evidence as seen through the prism of the model indicated that content quality and perceived trust in the platform were the most significant success factors. The limitations mentioned in the study are relevant for this thesis. For instance, voluntary participation inevitably results in selection bias. Carefully selecting respondents in a specific sector can provide some further granularity and detail, or a larger and more random sample can be sought for greater external validity. Another limitation is that some hypothesized relationships, such as that between service or system quality and use of the CTI system, are left unsupported. In this author's view, besides the *net benefit* factor, the model to little extent capture detailed *tangible* information of how a CTI platform is used, e.g. measures taken by users stemming from Threat Intelligence that resulted in actual thwarting or mitigation of real attacks.

In the second study, Zibak et. al [12] looked closer at the quality dimensions for both research and practice. Much research has highlighted how data quality issues is the most common barrier to effective Threat Intelligence, without closer investigation or even defining quality requirements. Further, most researchers either adopt an intuitive (expert opinion or common sense) or theoretical approach to data quality, which largely omits the stakeholder's view. User perspective is cru-

cial, as data quality in its most basic form can be defined "as data that are fit for use by data consumers".

Through a combination of systematic literature review and structured interviews using the Delphi method, a 'quality model' was developed that captured the following properties as important for Threat Intelligence quality:

- Accuracy
- Actionability
- Interoperability
- Provenance
- Relevance
- Reliability
- Timeliness

Where experts gave particular importance to Relevance, Actionability, and Timeliness. Yet, stakeholders are still to develop or even identify suitable metrics to measure these properties. Making the assumption that quality is related to effectiveness, a measurement could entail tracking decisions made on the basis of Threat Intelligence, the impact of which could be specific control changes to an organization's security posture.

Lastly, one interesting bit of information with significance to RQ4, is the trend that smaller organisations without the resources to tailor their own CTI, rely on Intelligence management solutions that benefit from analytics from the larger community.

Schaberreiter et. al [13] also looked at the quality dimensions of CTI, with specific aim at addressing the challenge of effectively sharing cyber threat information by assessing the quality of the information provided by different sources and determining the level of trust that can be placed in those sources. The study involved collecting data from various CTI sources and evaluated them based on a set of quality parameters, including accuracy, relevance, timeliness, completeness, and credibility. The authors also identified trust indicators, such as reputation, expertise, and track record.

Overall, the study provides valuable insights into the complex process of evaluating the quality and trustworthiness of CTI sources, which can help improve the effectiveness of cyber threat information sharing and enhancing cybersecurity efforts. While the study does not connect assessed quality with any perceived or measured change to decision maker's calculations, it is still noteworthy due to its attempt at capturing quality in quantitative manner. Also relevant for RQ3.

As exemplified above, significant research has been done on CTI models aimed at improving processes. Mavroeidis & Bromander [14] argue that the infosec community lack an standardization that cover the complete spectrum of Threat Intelligence, with vaguely defined terminology, lack of formalized representation and presentation, and lack of coherent relationships between different abstraction layers. Since CTI is dependent on effective information sharing where someone's detection results in another's prevention, the authors argue that a common multi-

layered ontology is necessary to better capitalize on the vast amounts of heterogeneous data sources available. Partially relevant for RQ3 and RQ4.

Sauerwein et.al [15] conducted an exploratory analysis on CTI platforms, in which they emphasized the importance of *actionable* Intelligence as opposed to mere threat data. While it does not directly answer any of the research questions, it still has partial relevance for RQ3 as it highlights an important aspect of utility with regard to CTI.

In [16] challenges and issues that organizations face in achieving cyber situational awareness (CSA) for network security are addressed. The authors discuss the importance of CSA for network security and the need for a clear taxonomy to define the different types of CSA information. They also identify the challenges in achieving CSA, such as the volume and diversity of data sources, the complexity of data processing, and the need for accurate and timely analysis. The article offers solutions to these challenges, including the use of machine learning and artificial Intelligence techniques, integration of multiple data sources, and collaboration between different organizations.

The article provides insight into the types of information needed to achieve CSA, including Threat Intelligence, vulnerability information, and network activity data, which can have relevance when addressing RQ1 and RQ3.

[17] explores the possibilities and limitations of using Cyber Threat Intelligence (CTI) in energy systems. It discusses the challenges of implementing CTI in energy systems, including the difficulty of obtaining relevant information, and the lack of common standards for sharing information. The authors argue that CTI can be an effective tool for improving security in energy systems, but only if it is used in conjunction with other security measures and processes. They also suggest that the effectiveness of CTI in preventing certain types of cyber threats may be limited, particularly in the case of sophisticated attacks that use multiple vectors. As it describes the viewpoint of a particular sector and the limitations it faces, the article is relevant for RQ1 and RQ3.

A noteworthy study was conducted by Xu et.al [18], which has relevance for RQ1. The article proposes a Vine copula model for predicting the effectiveness of cyber defense early-warning. The model is designed to capture the dependence structure between different types of cyber events and to assess the effectiveness of early-warning systems. The authors apply the model to a dataset of cyber incidents and demonstrate its usefulness in predicting the likelihood of future incidents. Thus, the article provides insights into how statistical models can be used to analyze cyber threat data and predict future events. The findings suggest that early-warning systems can be effective in preventing cyber incidents, and that models like the Vine copula model can be useful in assessing the effectiveness of such systems.

In [19], a case study was performed on a large international financial institution to explore how CTI is implemented and used in the organization. The methodology was that of a 'clinical research process', conducted by 'researcher-practitioners' who possessed both deep theoretical knowledge of the field while

also being deeply immersed in the organization of study. This study was unique, as it was the only one identified where a researcher-practitioner had the opportunity to observe, participate in, direct, and assess the impact on an organization's security posture **before and after the adoption of CTI**. Although it was infeasible to replicate anything similar for this master thesis, the insights gained are invaluable input to the construction of it's methodology.

Several findings have potential value. Firstly, it was assessed that the adoption of CTI had significantly improved the cyber security situation by:

- improving alignment between the activities of cyber-defence and cyber-attack
- reducing the success rate and impact of attacks as they were thwarted higher up in the kill-chain
- improving efficiency and focus of cyber defence operations against cyber-attacks

Furthermore, these points are not only observations, but represent an attempt to measure CTI-impact qualitatively by surveying all layers of stakeholders within the organization. Referring to the fundamental function of CTI - that it enables the user to better 'engineer' defensive measures - the study attempted to capture this logic by measuring cybersecurity performance in the following way: Reactive and undirected defensive behaviour indicates low performance, while proactive and directed behaviour translates to high performance. Thus, indicators of performance are those that show transformed behaviour among users, such as time spent higher up in the kill-chain as opposed to putting out fires.

Secondly, it was revealed that there were issues in 'consuming' CTI. For instance, the survey found that CTI had operational utility, but lacked strategic utility. Specifically, CTI did not really reach executive levels (who were also more sceptical of its utility to begin with), and for some levels CTI consumption were driven by obligation rather than business imperative. Methods were devised to improve those findings. They will not be detailed in this review, but the issues are included to highlight potential hurdles and limitations of CTI at various levels of an organization. Finally, the authors observed reluctance among stakeholders in acting on CTI related to resourceful adversaries, such as state actors or APTs. Such CTI were perceived to be speculative in nature, incurring great cost against threats that were invisible or hard to defend against.

In summary, the study addressed RQ1-4 in a novel manner directly relevant to this master thesis. The most obvious limitation is its reliability, as it was only conducted on a single organization. As mentioned, replicating a pre/post-adoption study for another or even multiple organizations is infeasible, but its framing and construction provide useful input for anyone investigating a similar problem set.

The SANS institute has regularly conducted surveys that attempt to "track the evolution of CTI as a mechanism for prevention, detection, and response", the last one completed in 2019 [20]. The survey had 585 respondents across a variety of industries, the largest portion coming from cyber security service providers, fin-

Area of Improvement	Level of Improvement Noted			
	None	Measureable	Significant	Overall
Improving visibility into threats and attack methodologies impacting our environment	3.3%	47.3%	43.3%	90.6%
Revealing vulnerabilities where new security measures should be implemented	8.2%	51.4%	32.7%	84.1%
More accurate risk analysis	6.9%	49.0%	31.8%	80.8%
Reducing time to identify and respond to incidents	6.5%	52.7%	27.8%	80.4%
Prioritization of efforts and resource utilization	9.8%	48.2%	31.0%	79.2%
Detecting unknown threats	12.2%	47.8%	29.8%	77.6%
Improving accuracy (fewer false positives)	11.0%	51.8%	24.9%	76.7%
Locating the source of events impacting our enterprise	10.6%	53.5%	22.0%	75.5%
Measurably reducing the impact of incidents	11.8%	54.3%	19.6%	73.9%
Reducing exposure of sensitive data	10.6%	53.1%	20.8%	73.9%
Preventing breaches	13.5%	44.5%	25.3%	69.8%
Preventing business outage	23.7%	37.6%	13.9%	51.4%

Figure 2.6: Usefulness of CTI [20]

ance, government, and technology. Asking questions about perceived CTI usage and value, the presence of structured IRs, collection sources, staffing, and processing, the survey has direct relevance for most research questions of this thesis. In that regard, one of the most interesting questions pertains to the usefulness of CTI: How it supports and improves existing security programs across different categories (Figure 2.6).

The top ranked areas of improvement capture the core purpose of CTI: Analyzed information about adversary intents and capabilities that enable defenders to adapt their security posture and prepare for more effective incident handling. It should be noted that the survey captures respondents' *perceptions* of utility. It is conceivable in that regard that answers may be influenced by a framing effect from both the questionnaire itself, as well as by how CTI is defined and promoted. Some comments on specific use cases were also made by respondents, which approach the elusive tangible outcomes that this thesis hopes to touch upon. For example, one respondent spoke of how exchanging samples and analyses with fellow CTI practitioners had enabled them to proactively block traffic from infrastructures that were used for ransomware campaigns months later.

Overall assessment of the literature review

Searching existing literature yielded few research articles that directly answered the problem statement and research questions. But this was assumed from the initial exploratory phase: lack of existing research that focused on CTI utility and impact or effect was what inspired the topic selection to begin with. As detailed in this section, most of the studies partially relevant to this thesis focused on various quality aspects of CTI (RQ3). They include processual and organizational issues, taxonomy and standardisation, and ontology. Outside of the articles detailed in this section, a significant amount of CTI research is focused on sharing.

By far the most relevant and interesting studies were [19], [11], and [12], which all were significant for the direction and construction of this thesis.

Chapter 3

Methodology

This chapter will explain the research process and design, and the choice of methodology employed to to answer the problem statement and research questions. The data collection process, its theoretical basis, as well as the subsequent analysis will also be detailed.

3.1 The Research Process

This section presents the overall research process. The following subsections will elaborate on method selection and implementation, data collection, and analytical approach.

Thomas [21] distinguishes between *research methods* and *research methodology*. The former pertains to research techniques, data collection methods, evaluation of research results and so forth, i.e. techniques that are employed throughout the implementation phase. On the other hand, the latter term also encompasses the science and philosophy behind these methods, and is relevant also during the planning phase. Hence, the logic behind method selection should be considered with care.

The research process can be summarized by the following steps [21]:

1. Identify the research problem
2. Review of literature
3. Develop the objectives
4. Decide the research design
5. Formulate the research protocol
6. Get approval from competent authorities
7. Conduct the research work and collect data
8. Analysis of data
9. Interpretation of data
10. Preparation of the thesis/report
11. Presentation of results
12. Publication of reports

Roughly speaking, this can be divided into the following phases:

- Research planning
- Data collection
- Analysis and interpretation
- Report writing

Much of the research planning phase was completed as part of a preliminary 'project planning' course at NTNU during the Spring of 2023 [3], although changes were made to the methodology as well as adjustments to the problem description and research questions. In practice, the other phases can not really be delineated into a neat waterfall process. For instance, a successful data collection phase depends on thoroughly selected and researched methodology, as well as a sound understanding of the topic's theoretical basis.

3.2 Method Selection

This master thesis aims to examine practical usage and effect of CTI within organizations. As discussed and defined in the research questions, effect in this context is measured as information that leads to changes in decision makers' calculations and subsequent changes in defensive posture. Such effects are not easily captured by quantitative measures. In general, quantitative methods are useful when attempting to measure independent, objective, and discrete entities[22]. Factors such as cost, error rates, user satisfaction, or even attacks thwarted can reasonably be measured by quantitative methods *in isolation*. This is challenging because CTI is not a stand alone security system as such, but instead informs and directs both humans and programs in a larger cyber security system. Moreover, in a real life setting the external environment is naturally uncontrollable, complicating measurements as it his difficult to discern whether a given level of detected malicious activity can be attributed to a particular system or to external factors.

One interesting approach, detailed in section 2.2, involved researchers being deployed at an organization's cyber security center both before and after the adoption of a CTI platform. Although a highly relevant and valid study, the methodology was deemed unfeasible for this thesis due to time, opportunity, and lack of access. Given these factors, this thesis will rely on qualitative research methods.

3.2.1 Qualitative Research Design

The primary objective of qualitative research is to gain insights into specific issues or situations by exploring the perspectives and behaviors of individuals within those contexts, as well as the overall environment in which they operate [22]. To achieve this, qualitative research is carried out in natural settings, relying on textual instead of numerical data. Qualitative data are primarily sourced from observations, interviews, and documents, and their analysis involves a range of systematic techniques. This approach is suitable for comprehending causal pro-

cesses: The goal of qualitative research is to understand phenomena from a participant's viewpoint in its own social or institutional context. Such meaning can largely be lost when quantified and aggregated. Importantly, qualitative methods are predominantly inductive, with hypotheses emerging as the study progresses to account for the evolving understanding of the setting and its inhabitants.

Kaplan and Maxwell [22] provide five main reasons for using qualitative methods in evaluating computer systems:

1. Understanding how a system's users perceive and evaluate that system and what meanings the system has for them
2. Understanding the influence of social and organizational context on systems use
3. Investigating causal processes
4. Providing formative evaluation that is aimed at improving a program under development, rather than assessing an existing one
5. Increasing the utilization of evaluation results

At least the first three reasons are very much inline with the general problem statement and research questions of this thesis. Within the philosophy of causation, many argue that a key strength of qualitative research is its ability to examine the context of causal processes [23], particularly by providing evidence for *how* interventions have lead to outcomes under specific circumstances. Thus, they challenge the idea that universal 'context-independent' conclusions, typically provided by e.g. randomized controlled trials, are immediately applicable in different contexts. This notion is especially valid when studying phenomena like policy interventions and processes, highlighting the suitability of qualitative methods for this thesis.

3.2.2 Descriptive Research

Research can broadly be divided into two categories: *Descriptive or exploratory research* and *analytical or explanatory research* [21]. The former attempts to describe and identify current state of affairs, while the latter goes into the *why*. Examples of analytical research designs include experimental research, quasi-experimental research, or correlational studies. On the other hand, descriptive studies entail designs such as case studies, cross-sectional studies, or observational studies.

Typically, descriptive research methods are not employed to establish causality per se, or *cause and effect*. While the reasoning for qualitative methods (3.2.1) mentions the investigation of causal processes, the nuance warrants explanation, especially since the problem statement and research questions target the *effect* of a system and its corresponding processes. Actual cause and effect studies usually fall within the domain of experimental research, where the crux of the method involves manipulating *causal variables*, while keeping other variables as constant as possible [21]. In the research design for this thesis, no researcher-imposed interventions, controls, or treatments are involved. But this does not mean that descriptive research is strictly limited to detailing a current state, ignoring causal

explanations. Rather, descriptive research can be suitable when examining causal processes in their own context, as discussed above. The specific descriptive research method selected for this thesis is that of *in-depth interviews*, which will be detailed in section 3.4.

Research method and design also has bearing on the overall problem statement, and vice versa, and is thus worth repeating at this stage:

How does Cyber Threat Intelligence provide utility for organizations?

3.3 Literature Review

A literature review is crucial for research projects as it enhances understanding of the subject, shapes the research problem, and highlights what has been done and to what extent [21]. A well conducted literature review is important in order to discover peer methodologies, potential pitfalls, and broadening knowledge. The objectives include understanding the current state of the art, identifying key works, pinpointing knowledge gaps, and relating new findings to previous ones. A comprehensive review is essential, especially in the context of a thesis, which requires covering all related research works.

This section briefly describes methodology for the literature review, the results of which can be found in section 2.2. Note that the literature review was mostly conducted as part of a project plan preceding this thesis [3]. To find relevant literature, systematic searches were conducted in digital libraries and databases accessible for NTNU students. The following resources were used: IEEE Digital Library, JSTOR, ACM Digital Library.

Search queries were made for the primary research question and all sub questions. After many iterations and refinements, the queries used are as follows:

- SQ1: ("cyber threat intelligence") AND ("effectiveness" OR "quality")
- SQ2: ("cyber threat intelligence") AND ("limitations" OR "failure" OR "challenges")

Table 3.1 provides an overview of the results. In cases where searches yielded too many results to be reasonably treated, either a few dozen articles were evaluated or until a satisfactory selection was identified. In addition to the sources found directly through searching, several relevant sources were also identified through the bibliography sections of relevant articles. Due to the rapid development of CTI specifically and ICT generally, the results were delimited to the time period between 2012-2023.

Not all identified results are described in the literature review below, but rather a selection which in this author's view are descriptive for the width of research relevant for this thesis.

Search query	Search engine	Results (#) / Relevant sources (#)	Source and related RQ	Date of search
SQ1	ACM	123 / 3	[13]: RQ1 [15]: RQ1/2 [12] 2: RQ1 / 4	01 May
SQ1	IEEE	40 / 1	[14]: RQ4	08 May
SQ1	JSTOR	75 / 0		08 May
SQ2	ACM	142/1	[16]: N/A	08 May
SQ2	IEEE	41/1	[17]: RQ3/4	08 May
SQ2	JSTOR	69/1	[18]: N/A	09 May

Table 3.1

3.4 Data Collection

3.4.1 In-Depth Interviews

For the reasons discussed in section 3.2, a qualitative research methodology through in-depth interviews was chosen for this study. We can distinguish between different types of interviews, based on degrees of openness. For instance [21]:

1. **Structured Interviews:** In structured interviews, an interview schedule is used for a standardized, low-variation interview, yielding data suitable for statistical analysis.
2. **Unstructured Interviews:** Unstructured interviews involve informal, open-ended conversations, focusing on the respondent's opinions, often termed open-ended or in-depth interviewing.
3. **Semi-structured Interviews:** Semi-structured interviews utilize a question guide with open-ended questions, promoting relaxed, conversational settings and flexibility in question phrasing and probing.

The semi-structured interview was selected in order to both allow for some uniformity, opening for comparison across research subjects, as well as maintaining enough flexibility to explore the research questions in-depth.

Theory

Johnson and Rowlands [24] describes the goals and purposes of in-depth interviewing with focus on the interpersonal dynamics at play. As implied by the name, in-depth interviewing seeks ´deep´ knowledge on a subject, knowledge that is obtained from real participants in the subject or phenomenon of study. The sought-after insights extend beyond surface level knowledge or conventional interpretations of the research topic: The researcher aims to uncover information that is normally unavailable or hidden from ordinary view. According to DiCicco-Bloom and Crabtree [25] semi-structured interviews are the most widely used interview

format, and is often the sole data source in qualitative research projects. Within this format, the primary research question should have a specific focus, ensuring that a relatively uniform group shares common experiences on the subject. While the main research question can often serve as the initial interview query, it's typical to create an additional set of 5 to 10 specific questions to explore various facets of the research matter more comprehensively.

DiCicco-Bloom and Crabtree [25] also highlights the importance of establishing rapport with the interview subject. In essence, rapport is built on trust and a deep respect for the interviewee and the information they provide. It serves as the foundation for creating a secure and welcoming setting where the interviewee can openly share their genuine personal experiences and perspectives. Stages of rapport can be described as:

- Apprehension
- Exploration
- Cooperation
- Participation

In summary, the apprehension phase is often characterised by uncertainty and slight unease with the situation. At this stage the goal is to allow for space and get the subject talking, by starting with broad, open-ended, and non-threatening questions that reflect the overall nature of the research. Further, the exploration phase involves the interviewee engaging in a detailed description, fostering learning, listening, and bonding. In the co-operative phase, participants feel comfortable, free from fear, and gain satisfaction from the interview process. The interviewer can clarify points, and the interviewee may correct them as they jointly interpret the interviewee's world. This phase may also address sensitive questions initially avoided. If the interpersonal dynamics allow and the interview is of sufficient length, the final participation stage may occur, in which the interviewee themselves take a larger role in steering the conversation.

Another important consideration is how questions are formulated. Unsurprisingly, the literature on qualitative methods and interviews highlight the importance of open questions to achieve real depth, as opposed to closed yes/no type questions. While seemingly simple, it can be deceptively hard to achieve as closed questions are an ingrained part of regular social interactions [26]. When ad-hoc formulating questions, as is a central feature of the semi-structured interview, it can be useful to be aware of the concept of *content mapping* and *content mining*. The former are meant to expand the research territory, create opportunity, and identify paths that are worth exploring further. On the other hand, content mining means exploring the identified dimensions and eliciting the interviewee's feelings and opinions in order to obtains his in-depth perspectives [26]. When mining for insight, the researcher should sometimes go to lengths of iterative probing that are unnatural to regular conversation. The methodology calls for sometimes banal questions in order to exhaustively explore interesting aspects. Doing this may also require the researcher to ignore and even suppress their own knowledge to avoid

assuming comprehension, as the subject (which is the actual data source) may ultimately reveal an unexpected reasoning for their perceptions and attitudes.

If we imagine this concept as a classical decision tree in which branches are both added and finalized, we realize that both open and closed questions have their place in an in-depth interview. The point is rather to be aware when one or the other is appropriate, and trying to avoid closing potentially valuable branches or wasting time creating twigs.

Challenges and Pitfalls

When it comes to the relationships or roles within an interview context, informants or research subjects can be viewed as educators, while interviewers can be seen as learners. Johnson and Rowlands [24] argue that an important issue to consider is the knowledge of researchers and their relationship and prior experience with the research topic. If the researcher lacks prior knowledge and experience in the interview topics, the interviews may become instructional, with experienced individuals guiding the novice interviewer. Such interviews often exhibit uneven quality, primarily revealing the novice's lack of understanding rather than shedding light on the subject of study. Novices may also have difficulties seeing nuances, and may be less adept at steering conversations towards the most valuable information. Some studies observe that the majority of such studies are worthless as empirical data [24]. Meanwhile, novices are more likely to lack historical baggage and hardened assumptions about the topic. Their outsider status can also elicit different responses from interview subjects, compared to that of an insider who's stature may constitute a mental barrier. On the other hand, researchers with prior experience and knowledge likely spend less time at the surface level, are better able to grasp layered meanings and identify what information is truly noteworthy, and overall may be more adept at studying phenomena to which they have access. While we can certainly assess our own knowledge level or status within the subject field, accurately gauging how these interpersonal dynamics play out prior to the interview setting is impossible. However, we can try mitigating potential issues by being reasonably aware of the dynamics that develop between two people in a given setting.

Finally, it is important to be cognizant of the clear distinction between the data collection setting and analysis [26, pp.144]. Attention should be dedicated to listening, responding, and steering the conversation, while not falling for the temptation to interpret or make analytical constructs.

3.4.2 Sampling method and recruitment

Sampling is a fundamental part of data collection for any research project, as it is seldom practical or efficient to study an entire population. Quantitative sampling methods, and in particular random or probability sampling, is often lauded as the best method to reduce sampling error and produce results that can be generalized across the population. The process is rigorous and well-defined, but unsuitable for

qualitative studies for a number of reasons [27]. For instance, random sampling is usually done for studies seeking to answer a predetermined hypothesis and provide generalized results, which is not the aim of exploratory studies in general or this study in particular. Further, achieving a truly representative sample is only possible if the research characteristics are normally distributed: "Cyber Security personnel with experience in CTI" is not a common trait across the general populace. Thus, since in-depth interviews aim to uncover common perceptions within a specific group, the sample should exhibit a reasonable degree of uniformity and possess significant traits relevant to the research questions. Marshall [27] describes three broad categories for sampling in qualitative studies:

1. Convenience sample - The selection of the most accessible subjects. It is the least costly method in terms of time and effort. While most qualitative sampling, including this study, includes a certain element of convenience, some more thought and direction must be applied in order to increase data quality.
2. Judgment sample / purposeful sample - The most common sampling method for qualitative studies, in which units are selected based on who are assessed to provide the most productive data. Some base knowledge on the subject area is required to make sound judgements. Within purposeful sampling, researchers can choose to strive for a broad range of subjects (maximum variation sample), outliers (deviant sample), or people with specific expertise (key informant sample).
3. Theoretical sample - Constructing interpretive theories from emerging data, and iteratively adjust new samples based on new knowledge and refinement of said theories.

Commonly, purposeful sampling is the preferred method for recruiting participants for in-depth interviews [25], and is the method selected for this thesis. Furthermore, the concepts of *maximum variation sample* and *key informant sample* have guided recruitment. In practice, the structured and consistent utilization of CTI (in-house or external) is reserved for companies or organizations above a certain size and budget, typically those with dedicated cyber security teams. Although the sample size is numerically small, effort has been made to ensure participation from various actors in both public organizations and from different private sectors. Additionally, while the field is narrow and required expertise is highly specialized, the author has sought participants from different levels and positions in the decision chain, such as technical practitioners and managers. This approach was deemed important to capture a range of perspectives and potential differences in perceived value.

Sample Size

Sample size in qualitative studies is a debated subject. Some attempts have been made to establish numerical requirements, but this has been challenging as qualitative theorists have arrived at different conclusions. For example, different re-

searchers have suggested 6, 6-12, 5-25, or 2-10 participants as sample sizes in which thematic redundancy normally occurs [28]. Currently, it is common to look at the concept of theoretical saturation as a guide to predetermined sample sizes.

Guest *et al.* [29] conducted a study on theoretical saturation, piggybacking on another qualitative study using semi-structured open-ended interviews, sampled through a non-probabilistic purposeful method. Saturation is defined as the point in which no new themes or information are observed in the incoming data. Using theme identification in a code book structure as the guiding measurement for saturation, the authors found that complete thematic discovery was almost entirely achieved after 12 interviews. Of a total of 114 codes identified, 80 of them had been found after only 6. Their analysis also showed that the most important themes were identified early, and those themes were prevalent throughout the entire collection. This fairly low range presupposes a sample consisting of carefully selected, high quality subjects from a relatively homogeneous group, as is the case for this study. While hedging against categorical numbers, the study nonetheless concludes that 12 interviews should suffice in most cases.

3.4.3 Reliability and Validity

Within academic research, reliability and validity are central terms in the pursuit to ensure scientific rigour. As reliability and validity has its origin in positivist quantitative methodology, many researchers question its direct applicability for the naturalistic perspective and qualitative methods such as in-depth interviewing [30]. As such, the discord warrants some discussion to highlight how the terms are understood in the context of this thesis. Firstly, according to the Merriam Webster dictionary, reliability in science is defined as:

> the extent to which an experiment, test, or measuring procedure yields the same results on repeated trials [31]

Golafshani [30] summarized attitudes on both sides of the argument. On one hand, some researchers posit that reliability is irrelevant and even misleading in qualitative inquiry, as reliability issues concern measurements that may be all but impossible to apply on qualitatively collected data. For example, test-retest methods may sensitize respondents to the questions, or reflection could have taken place in between, yielding variations in answers. The interpersonal dynamics in an interview setting is also very difficult to control and adjust for. The other side argue the term's relevance not in the traditional definition stated above, but rather in a nuanced understanding as qualities such as *credibility*, *neutrality*, *consistency*, and *dependability*. Without immersing into further definitions, an assessment of these terms can summarize them as the pursuit of integrity in handling the collected data. Thus, a key focal point was that information provided in the data collection was processed in its original form as expressed by interviewees. Instead of relying on the author's note taking abilities, this was ensured by automatically

transcribing interviews and collating the information in the NVivo software. Additionally, interviews were recorded to make up for inaccuracies in the automatic transcriptions.

Opinions on validity in qualitative research also differ greatly. Again, some researchers argue that the concept as it is normally understood is not applicable, while others suggest that it is dependent on researchers' own perceptions and the paradigms in which they operate. Consequently, many researchers adopt their own concepts of validity or intersperse it with other related terms[30]. One definition describes validity in qualitative research as the 'appropriateness of tools, processes, and data', and focuses on the consistency between research questions, methodology design, sampling, and analysis [32]. In even simpler terms, this can be summarized as the *relevance* of collected and analyzed data, in line with the ubiquitous definition of internal validity. Choices for all of the above points have been addressed in this chapter thus far, and will not be further elaborated. This leaves external validity, which is whether conclusions drawn are transferable to samples or contexts outside this particular study. For external validity we refer to the theory section on CTI, and conclude that due to the common epistemology and origin of threat intelligence, the results will likely be applicable on other populations at least within the anglosphere and larger western world.

3.4.4 Ethical Considerations

The data collection and handling of was carried out in accordance with the guidelines stipulated by the Norwegian Personal Data Act [33]. The research project was registered and approved through Sikt (NSD), and informed consent was obtained by all interviewees. No sensitive personal information was collected, as defined by the Personal Data Act. But since the topic intended to go into details on organizational and technical aspects of cybersecurity, information on which could be valuable for malicious actors, respondents were anonymized. This approach was selected to encourage honest and open discussions without risking repercussions for participants. Consent was given to include position and sector in the final product, but these characteristics were only used in a few instances relevant to the thesis (see also section 4.1).

3.5 Data Analysis

Within qualitative interviewing the most common analytical approaches are *content analysis* or *thematic analysis* [34]. With different subcategories and various interpretations and definitions, the exact distinction between the two methods can be murky. At center of both methods lies *coding*, the systematic collation of data, although they somewhat differ in coding approach as well as in a few other key aspects, which can be summarized as follows [35] [36].

1. Content Analysis:

- Focus: Content analysis is primarily concerned with the objective and systematic examination of the content of communication, such as text, images, or audio.
- Coding: It involves coding the data into categories or themes based on predefined criteria. The aim is often to quantify and analyze the frequency of specific words, phrases, or themes within the data.
- Objectivity: Content analysis tends to be more objective, as it relies on explicit coding rules and predefined categories.
- Research Questions: It is often used to answer research questions related to the frequency and distribution of certain words or themes in a given set of data.

2. Thematic Analysis:

    - Focus: Thematic analysis, on the other hand, focuses on identifying, analyzing, and reporting patterns (themes) within the data. It is more interpretive and aims to uncover the underlying meanings and patterns present in the data.
    - Coding: Thematic analysis involves inductive coding, meaning that codes and themes emerge from the data rather than being predefined. Researchers immerse themselves in the data to identify patterns and themes.
    - Flexibility: Thematic analysis is more flexible and allows for a more nuanced exploration of the data, capturing both explicit and implicit meanings.
    - Research Questions: It is often used when the goal is to gain a rich understanding of the experiences, perspectives, or meanings embedded in the data.

While content analysis may be more structured and quantitative, focusing on the explicit content and frequencies of specific elements, thematic analysis is more flexible, qualitative, and interpretive, aiming to uncover deeper meanings and patterns within the data. Unsurprisingly, the fluidity and varying definitions between methods have also resulted in the development of hybrid approaches that combine inductive and deductively developed codes [37]. Other notable methods include *grounded theory*, which emphasises theory generation directly from the data.

This research project is descriptive in nature, and does not aim to elucidate existing or develop new theories. Thus, the thematic approach was chosen to allow for emerging patterns as interviews proceeded, although some initial codification was conducted around research questions. The codification and subsequent analysis was done using the NVivo software , which enables easy identification and categorization of themes.

Chapter 4

Results

The results from the data collection is organized into five major themes which emerged throughout the analysis:

1. Effect on Decision Making (4.2)
2. Stakeholder Involvement: Direction, Steering, Feedback (4.3)
3. Impact on Security Situation (4.4)
4. Utility Factors (4.5)
5. Impediments and Improvements (4.6)

4.1 Sample

The sample consists of 10 participants from the following sectors:

- Finance
- Health
- Defense
- Cyber Security Firms and Consultancies
- Telecom

All organizations surveyed were situated in Norway, although most were internationally involved or were part of cross-border collaborative environments. All interviewees had significant experience (> 5 years) within both information security and CTI, and held a variety of positions within both analysis and middle management. A majority of the sample also had backgrounds from the military or had received professional Intelligence training at one stage in their careers, although only one was still employed in the defense sector. Since anonymization was a crucial prerequisite for this study (as detailed in subsection 3.4.4), the sample demographics will not be described in further detail. Importantly, how interviewees are referred to will change slightly throughout this chapter. Although they consented to sector and position being referred to, it is only interesting or relevant for the thesis in a few instances. Since some themes may be more sensitive than others, the characterizations are used sparingly.

4.2 Effect on Decision Making

4.2.1 Summary

This section details interviewees' opinions and experiences on how CTI affects decision making. Whereas any effect or change made by a person could theoretically be described as a 'decision', this section focuses more on the abstract and processual aspects higher up in the cycle, as opposed to the more tangible and technical effects detailed in section 4.4.

The value of early warning emerged as a significant theme, with many expressing its organizational impact and the positive effect it could have on timely incident response and prioritizing resources. Related was also the value on advising early in any process, even before certain systems were established and operational. Most subjects also raised points related to infosec maturity, suggesting that CTI benefits and impact on decision making was largely determined by the maturity of both the infosec programs overall as well as leadership involvement and understanding. Another point being made was CTI's contribution to aspects such as actor intentions, which were not really captured by technical day-to-day operations. This supported decisions higher up in organizations, for example as part of risk assessments and investments.

4.2.2 Details

A senior security consultant in a cyber security firm maintained that from their experience, very few if any organizations utilized Intelligence in their decision making processes at the strategic level or within the C-suite, with the exception of defense and security related sectors.

> Yet in the market, some do provide CTI products and services within 'geopolitical analysis' and the like. How many companies actually need those and are able to use them? Sure, they provide added context on why the security picture has changed and so forth, which may be interesting and nice to know. But only rarely does it hold practical value for e.g. investment decisions. I would be quite wary of spending much money on these elevated risk or threat analyses if I represented a regular company or organization in Norway.

On the other hand, they were aware of instances in which investment decisions had been made, not solely based on, but informed by CTI. In one case, CTI had contributed to a heightened threat perception that was crucial to the decision to invest in a particular capability. In that instance there was an interesting dynamic as the decision was driven forward by the larger and more mature parent organization, who exhibited a higher and more updated threat perception than that of the smaller distributed operational teams. This point was reiterated by a technical CTI analyst from the same firm:

> Some deliveries have been instrumental for customers' budget approvals, especially when we've made serial reports highlighting attack trends or methods against certain types of targets.

When it comes to decision making and decision support, the senior security consultant also raised an important point about definitions.

> When people are talking about CTI, I consider a lot of it to actually be threat research or vulnerability hunting, and testing of that to hone and develop defensive systems [such as enrichment for endpoint detection and response systems]. This isn't what I'm normally used to [as opposed to the stricter definition of CTI as decision support]. You can say what you about that, but it's important to note.

A security leader in the public sector spoke of 'sharper' incident management as a tangible effect on the decision making process. With more advance warning, it was possible to get a head start on deciding to perform counter measures before an incident had properly materialized, reducing the overall consequence. Similar views on the effect of early warning were also expressed by several others in this study.

Continuing, the same interviewee highlighted CTI contribution to risk assessments as a major boon. Risk assessments were described as a function of impact and probability. While impact was relatively easy for a product or system owner to assess, calculating probability was unsurprisingly a much harder task. 'Regular' cyber security systems and functions usually capture the 'what' and 'how' of cyber attacks as they occur, albeit in a somewhat reactive manner. Meanwhile, some types of CTI also ventured into the 'who' and 'why', which could be useful building blocks for probability assessments. As such, the interviewee lauded 'actor knowledge' as an important facet of CTI from their point of view. Having knowledge on the threat actor landscape, their capabilities, and who they typically target, was an important contribution when prioritizing the organization's limited resources.

This perception was in contrast with that of a security coordinator in the same organization, who worked less in the strategic and leadership domain and more towards the operational and tactical levels. From their perspective, actor knowledge was currently of less importance:

> It's certainly 'cool' to know that it's this or that Chinese or Russian actor, but currently there is not much we can do about it. We don't really have the ability to adapt specifically according to whether it's APT X, APT Y, or some ransomware group - for us it's all about the tactics and tools employed against us. I can certainly see how you can exploit this knowledge and counter a specific actor, knowing their goals, before they've played out their moves. But at the end of the day we're not at that maturity level yet.

A senior analyst from a different sector, also focusing more towards the strategic level, brought up points on probability and risk assessments similar to that of

the security leader above. They stated that their products on threat landscape and actors had enabled end users to conduct better probability assessments, contributing to a more substantiated overall risk picture and a baseline risk score that could guide their efforts. Furthermore, they confirmed that there were indeed instances where end users had changed security posture based on CTI they delivered (i.e. decision support in the strict definition). Due to sensitivity concerns, they were unable to elaborate in detail on the exact measures taken, but suggested that these [strategic level] effects were more likely due to the totality over time rather than singular products or reports as were constantly the case on the tactical level. As for strategic level effects, they also explained that the impact they now enjoyed were the results of a maturity process over time in which leadership now better understood how to utilize and actively steer the CTI function.

Lastly, a middle manager in the public sector pointed to the 'advisory' part of their mission as a way in which their CTI directly influence decision makers. Specifically, they highlighted how they were often solicited to advise on new establishments (e.g. new physical sites or investments in major digital assets). Providing recommendations at an early stage were an effective way to provide impactful decision support.

4.3 Stakeholder Involvement: Direction, Steering, Feedback

4.3.1 Summary

A crucial step of CTI as a concept, this turned out to be a considerable talking point throughout most interviews. This section captures subjects' experience of the 'Planning and Direction' part of the Intelligence cycle (see subsection 2.1.3). It is divided in two: The first is direction and steering, which essentially pertains to the quality and extent of IR development and level of stakeholder involvement. The second details to what extent they utilize feedback loops to measure, adjust, and improve CTI.

The extent and level of structure to stakeholder dialogue varied greatly among interview subjects. Some organizations report of opaque end user requirements, with specifications and Intelligence dialogues at a generic level. Often, end users were reported as unable to properly specify their needs. Other organizations tell of structured dialogue processes that effectively capture stakeholder requirements. But even in cases where direction and steering is considered a distinct and well developed part of the CTI product, considerable effort is spent to reach desired effects as perspectives and priorities often differ among different stakeholders.

A mixed picture also emerged on the topic of feedback and measurements. Some organizations had defined processes for capturing feedback as part of the CTI framework. Only one organization reported they employed quantitative measurements (surveys), while most organization at least had qualitative methods as part of continuous dialogue processes between stakeholders. Lastly, a few re-

spondents cited feedback and measurement as lacking and an obvious point of improvement. Regardless of maturity, none reported to have complete satisfactory routines and methods.

4.3.2 Direction and Steering

A middle manager from an organization serving myriad public and private sector customers, noted that communication and coordination was mixed, depending on level. On one hand, the overall mission direction did involve stakeholder requirements from a strategic perspective, resulting in specific tasks that guided their work. But when it came to the needs and requirements of actual end users that utilize these products in some form for their situational awareness or security posture, it was described as "quite opaque", adding that some end users were also unaware of their own requirements.

A senior security consultant in a cyber security firm reported that the Intelligence dialogue with customers was often at a quite 'generic level'. Seldom did they experience that customers specified tailored CTI products to fill in knowledge gaps - this really only occurred with the largest organizations with the most mature security programs. For most customers purchasing CTI services, the initial dialogue would often be something akin to:

> We are aware that information security is important, and the threat is increasing. We suspect that we haven't assessed this properly the last 10 years, can you advise us on what we need to do?

In a few instances at the other end of the spectrum, they would have customers with a level of specificity to their IRs and knowledge gaps which necessitated engineer to engineer dialogue to develop service requirements.

A technical CTI analyst from the same firm painted roughly the same picture when it came to stakeholder involvement. Elaborating further, they reported that customers did not always have the ability to specify their requirements. Stakeholder dialogues were conducted to help customers develop IRs, focusing on helping them find subjects that not only "*sounded exciting or interesting, but actually created meaningful value for the customers*". Again, a few customers had highly developed security programs and a good grasp of their gaps and requirements. Differentiating between the two categories were often done by maturity assessments, using NIST frameworks, sometimes at customers' demand.

A middle manager in the private sector described a quite well developed process for stakeholder involvement. In general, there were overarching procedures to capture end user intel requirements as part of the operational cycle. At the strategic level, it was slightly less explicit. While such an intel dialogue was not clearly expressed in SLAs, it was still an integral part of the on-boarding process where aspects of the offered services were directly linked to CTI. Moreover, they employed continuous development processes as part of component life cycle management, that aimed to capture changes in focus and requirement in order to improve the CTI service.

A senior advisor in a public organization serving multiple recipients, demonstrated advanced doctrinal knowledge and processual understanding of CTI. They highlighted planning, direction, and stakeholder dialogue as a crucial component of a successful CTI program. Elaborating on the Intelligence dialogue aspect, they explained that customer expectations had to be centre stage, seeing that satisfying their specific needs is a prerequisite to maintain necessary funding and deliver value. Such a realization should be a given, bordering on banal, but their unprompted and strong emphasis on this point separated them from other interviewees. Achieving the desired level of stakeholder involvement was demanding, requiring them to dedicate both time and effort. Understanding stakeholder needs and reaching a common understanding was not straight forward either. Often they would attempt to interpret stakeholders from another angle:

> I don't really are what they ask, I care more what they're gonna use it for. "What's going on with actor X these days?" That is not really your question. What you're actually asking is what can hit you tomorrow, and whether your posture allows you to detect and respond to it. And if not, what do we need to change and at what cost.

Also, they added that decision makers rarely knew exactly what they needed: Not as in they are unaware that they need information on various threats, but that they were often unable to specify how and where CTI fit into those needs, complicating the task of achieving common understanding on what exactly the CTI unit can deliver. It was noted that the dialogue had significantly improved over the years, but as their stakeholders' job ultimately revolved around risk analysis, they had to adapt their communication accordingly when discussing Intelligence process. Thus, considerable emphasis was put on stakeholder analysis.

This level of cognizance to stakeholders' actual needs were also reflected in the dissemination phase. Rather than reporting on threat actors' 'technical' behaviour, which was adequately covered by other security functions, they focused on delivering a narrative through 'unified kill chain': Why are they a threat to your organization specifically and what's their motivation and intentions - aspects that fit into overall risk assessments. Importantly, the Intelligence dialogue was part of a planned process, structured to capture both customer satisfaction with existing deliveries as well as direction and changes going forward. Moreover, they stressed the importance of educating technical CTI practitioners on customer demands. This was exemplified by making sure that technical practitioners always were critical of where they spent their efforts: "*Although this analytical lead is interesting, is this what the customer actually needs?*".

A security leader in another public sector organization detailed their nascent implementation effort of CTI throughout their information security system. Still in its infancy, the leader realized the program was far from complete, but nonetheless highlighted Intelligence dialogue as a crucial step in realizing the value of CTI. So far they had started exploring IR development internally by improving dialogue between Security Operations Center (SOC), security leaders, and not

least C-suite level which previously had not opined much on the direction and requirements within information security. This process had not yet translated into a real Intelligence dialogue with CTI providers.

A security coordinator at the operational level of the same organization, described the Intelligence dialogue with their CTI-unit as "*without a formal dialogue process*". Being 'operationally integrated' and physically close, most of the dialogue and collaboration between various security components (such as SOC, and CERT which provided the CTI), happened through informal processes and organically through working on the same digital platforms.

4.3.3 Feedback and Measurements

One interviewee elaborated on customer feedback as an integral part of the Intelligence dialogue. Within their organization, feedback was a component of the structured steering process. Although feedback and metrics were a distinct step at the end of the Intel cycle, they were adamant that the groundwork for obtaining useful feedback must be laid already at the beginning of the cycle when developing IRs. Further, while actual metrics on relevance were both useful and interesting, they emphasised their reliance on dialogue with recipients to capture how products were actually used. Often recipients could elaborate on how CTI products changed or reinforced decisions, and what aspects had contributed to that utility. A similar process was also reported by another interviewee, stating that "*[customer feedback] normally happens within the product development life cycle, and it's included as one of the integral components of particular products*".

Another interviewee from the same sector also reported good processes for stakeholder feedback, through both qualitative and quantitative means. Their surveys measured perceptions across different roles, for various security products including non-CTI (e.g. anti-fraud, incidence handling). Results on perceived CTI utility (and other products) were mixed. The interviewee hypothesized that some respondents rated products according to their primary role and interest, thus creating a somewhat distorted picture, but this was opaque due to survey design (anonymity). Regardless, they noted that on aggregate both qualitative and quantitative surveys painted roughly the same picture. Yet, even through these structured processes including interviews, customers were generally unable to tie decisions or changes in posture to specific Intelligence items.

One interviewee spoke of feedback sessions throughout the delivery being defined in their framework, as a method of capturing satisfaction and adjustments. These did not include quantitative measurements, but relied on open discussions with customers on a group level or with specific stakeholders.

An interviewee in the private sector with a mature CTI program, reported simply that feedback and measurements was included as one of the integral components of particular products within the product development cycle.

Yet, some respondents explained that specific feedback on products were lacking, citing no real structure or attempt to capture fine grained details on delivery

satisfaction. This was particularly the case for one public entity who provided strategic products to many recipients, often without a direct relationship between producer and end user. Others described a similar status: Some ad-hoc feedback was conducted, but as the CTI program matured they intended to improve by creating a real process for feedback and measurements.

4.4 Impact on Security Situation

4.4.1 Summary

This subsection goes into detail on how organizations experience CTI impact on their security situation, i.e. the more tangible and direct effects it has both on handling of technical incidents and on methodology and approach. Interviewees were unable to provide detailed accounts on methods and capabilities, but offered general explanations on overall effectiveness and impact.

Most interviewees were aware of instances in which CTI had resulted in tangible benefits such as mitigation, disruption, or reduced impact from cyber attacks, with all examples cited within the operational or tactical levels. Generally, the cases discussed involved counter measures as a result of some form of early warning, often with complementary collection and understanding of the target environment as enabling factors. Others cited benefits of CTI as a multiplier to different security services, and as a service that aided prioritization and reinforced other efforts. Additionally, Intelligence methodology and analytical mindset was also lauded as an improvement to security programs. Finally, some also mentioned TI-based testing as a boon to security, usually mentioned as part of regulatory requirements in certain sectors.

4.4.2 Details

A middle manager from a public sector organization detailed how their CTI had contributed directly in improving security among numerous end users. Their impact ranged from preventing attacks completely from materializing, to reducing damage potential by enabling customers to e.g. avoid privilege escalation and further infection of their systems. An important aspect was CTI ability to separate signal from noise, sharpening priorities on what attacks warrants particular effort.

A senior advisor confirmed that their products and services had directly impacted customers' security in several ways, often as a result of them bridging collection gaps of end user organizations. Examples included them observing threat actors attempting to sell access to victim networks to other threat actors, and providing early warning on emerging campaigns that included Intelligence on TTPs and potential targets. These points were reiterated by another analyst from the same sector, who explained how timely Intelligence on specific threats had directly resulted in the disruption of cyber attacks. Notably, both subjects mentioned how these instances were analyzed in the context of frameworks such as

the 'Unified Kill Chain'.

A middle manager in the private sector highlighted optimization as a particular benefit. In that context, CTI was described as value added, a multiplier for organizational progresses as well as for particular services and products. Perhaps the largest impact in this regard was on incident detection, where CTI was a clear multiplier especially when considering low maturity products and early stage advisory (similar sentiments were also brought up by other interviewees, in that CTI could often reinforce or provide additional assurance on other efforts). Also, they confirmed that CTI had indeed contributed to stopping or mitigating specific events 'within SOC operations', although they could not provide more detail.

A security coordinator described practical effects on their security posture. Working mostly towards the operational side, they spoke of how they had made configuration changes to various systems as a result of CTI detailing emerging threats with specific TTPs. Examples included vulnerable software that had been used by threat actors to conduct other nefarious activity, as well as new types of multi-factor resistant phishing. Importantly, the fact that CTI could inform on what others in the same sector were experiencing, which were often organizations with a similar technology stack, made it a pertinent basis on which to perform counter measures.

Two interviewees from a cyber security firm discussed a mixed picture on how their contribution had impacted customer defensive efforts. On one hand, it was very difficult to directly attribute their CTI to any changed security posture or heightened level of security. Metrics, transparency, and insight into what measures are effective were often lacking (even within an organization), a point repeated by many other interviewees. In fact, none could corroborate any overall trend of heightened security attributed to CTI. On the other hand, certain products and efforts had a demonstrable impact. For example, through a mix of their own threat discovery, collection, analysis, and knowledge on customer assets and priorities, they would advise and report on emerging or even ongoing attacks. Yet, also here it was often difficult to pinpoint CTI in itself as the determining factor:

> Technical personnel, incidence response, and the CTI units are intertwined. [In this particular case] the CTI people were deeply involved in the process, although to be strict this falls within the incident response domain. The lines are quite blurred.

Notably, the quote above illustrate how the subject of definitions and delineations between security functions elicited different opinions throughout interviews, with others describing incident response support as a core function of CTI.

Several interviewees also pointed to analytical methodology as having an effect on how infosec teams conducted their work, although none were able to tie this directly to any improvement in security. Rather, methodology improvements from the CTI field was described as having led to reduction in analytical bias and hasty conclusions, as well as improved communication and dissemination. One security leader even described the improvement in analysis as the largest impact

of their nascent CTI program so far, as analysts became more trained in critical thinking and structured analysis techniques.

Another way in which some organizations experience changes in security posture, is through TI-based testing. This is especially prevalent in the finance sector, where EU frameworks and regulations such as TIBER (Threat Intelligence-Based Ethical Red-teaming) and DORA (Digital Operational Resilience Act) mandate CTI-based penetration testing and ethical hacking. The general idea is to use CTI as a basis to emulate threat actor TTPs, which can discover not only relevant vulnerabilities, but also what critical assets and functions are present on the host system which may be of particular interest for adversaries.

4.5 Utility Factors

4.5.1 Summary

Interviewees expressed their opinions on what factors they deemed most important for the utility of CTI. Many communicated *relevance* as a major factor: Threat Intelligence must be tailored to the recipient's specific mission and threat landscape. It should also complement existing efforts, i.e. provide unique value, which also speaks to the importance of collection. Respondents also pointed out the importance of *usability* (understood as ease of operationalizing) and *dissemination*. CTI must be conveyed in a precise and efficient manner which aid stakeholder action. On the more technical or tactical side, it must also facilitate automation, integration, and efficient data flow. Some interviewees also highlighted users' own ability to exploit CTI (i.e. maturity) as the most crucial utility factor.

4.5.2 Details

A middle manager noted their ability to provide indicators with **context** as a major utility factor (i.e. enrichments). Largely due to the nature of their mission and the collection abilities that came with it, they had the ability to collect and collate additional context from seed indicators upon request from a given party, which gave a significant advantage in the CTI cycle, providing analyzed Intelligence products as a result. Additionally, they experienced that their organization's standing and reputation in itself was an important factor among their consumers. Due to operational constraints such as classification, their organization was sometimes unable to provide all context and details that end users desired, as described in the first point. But knowing its origin, end users would normally weigh the information heavily and act on it. As such, professional **credibility** and **trust** could be understood as utility factors.

A technical CTI analyst pointed out several factors that were emphasized by customers during the Intelligence dialogue and feedback processes. **Relevance** was repeatedly stressed. In their context, it usually meant that CTI products must deliver unique value that end users could not readily obtain from common media

sources. **Tailored** was another word often used to describe the same quality. For the analysts, tailored was also a term used as guideline to promote and ensure that customer requirements were always front and center when considering to share information or analytical products. The interviewee also promoted **dissemination method** as a utility factor. End users would cite not only the content of the CTI, but how it was delivered as a determining factor. E.g. the Intelligence should be conveyed in a manner that is both succinct and detailed enough, where in some cases an additional oral walk-through was sought after. Also, with respect to 'tactical deliveries' (e.g. indicators), **automation** and **efficient data flow** processes were considered crucial utility factors. As a CTI producer, the interviewee also pointed out precise and comprehensive IRs as a utility factor on its own. In that regard, they suggested that there should be room for producers to be somewhat demanding of customers in order for the latter to extract full utility from CTI.

A related point was made by a senior advisor from the same organization. They referred not specifically to any quality dimension, method, or content to the actual CTI product as a utility factor, but focused more on user organizations' own ability to exploit Threat Intelligence. The same point was also raised by a project manager for a consultancy within cybersecurity. According to them, the single most important factor determining utility from CTI was the recipient's resources and ability to receive, process, and understand what significance CTI holds for their mission. Moreover, this ability must permeate the organization: Roles and functions that receive, process, analyze, convey, and implement must be at a sufficient level to be able to exploit CTI. Last but not least, the leadership that actually allocate the money and resources for this ability must also be convinced that it holds value for it to make sense on an organizational level.

A different perspective on these considerations was made by a CISO at a consultancy, with significant background and experience within CTI. Having reviewed the infosec approach of the entire company, and deliberated the adoption of CTI, they had opted **against** investing in any specific CTI services. A few reasons were provided. For instance, they had recognized that the organization was not mature enough to effectively exploit any advantage CTI may pose. Furthermore, their 'technical security' level was considered excellent: Ostensibly, they had good overall control of their systems and networks with little indication of abnormalities or attacks beyond an expected baseline which was well manageable. Also, their business and accompanying assets were not considered particularly targeted as opposed to other more exposed sectors. Lastly, they tied these assessments with their business perspective. As a listed company, they were guided by EBITDA measures, one component of which is overall staff levels. Security was primarily seen as an expense, thus a risk based approach meant that they always struck a balance between security investments and potential losses. Additionally, the business culture was described as being permeated by an extensive focus on compliance and standards: Mostly related to core business, but also within infosec such as ISO 27001. This meant that an investment in a CTI was not prioritized as other

measures were assessed to give greater ROI at this moment. However, they noted that this decision was for investing in CTI as a standalone function or service. On a strategic level they did indeed utilize open source reports such as those of the three Norwegian secret services when assessing larger trends and the overall threat environment.

Aforementioned factors such as relevance and automation were also pointed out by other respondents. For example, a security coordinator opined that CTI products on the operational level must be effectively and succinctly communicated, i.e. they should be clear on exactly why the recipient must care about this issue. At the technical or tactical level, deliveries should ideally be accompanied by indicators that can automatically be ingested in their detection systems.

One interviewee highlighted their unique **collection capabilities** as an important utility factor. Du to the specific mandate bestowed upon their mission (by regulatory bodies and participant organizations), they were allowed to store data for longer than usual. The same circumstances also allowed them to share more data and Intelligence with partnering organizations across borders. Both aspects gave an obvious analytical edge: A collaborative environment with more unique data from myriad sensors and sources, enabled sharing of **timely** and **relevant** CTI to end users that had clear utility and effect on their defensive posture. The same arguments were also raised by a lead analyst from the same sector, stating that timeliness and relevance as the most important factors. When it came to relevance, they further defined that as "*ideally capturing 4W (who, what, where, why)*".

Finally, a security middle manager in the private sector highlighted **maintenance** and **integration** as the most prevalent utility factors.

> There are lots of sources for CTI, that must be practically deployed. You have various data such as event inputs, penetration testing, indicators and so forth, and at the end of the day CTI can also be bought, of various quality. This must be integrated and maintained at an organizational level into a common inference engine to make sense of it. Putting all this together within the organizational pipeline, maintaining it, and create real *actionable Intelligence*, I think that is one of the most important things. This is the very tricky bit, but also the bit that makes it useful right? Otherwise it's just one more pile of data.

4.6 Impediments and Improvements

4.6.1 Summary

This section details interview subjects' view on impediments to effective utilization of CTI, as well as their take on how to improve various features. The most common theme among almost all subjects was infosec maturity. Their accounts focused on two aspects: The first pertains to end users' ability to understand what

CTI can deliver and how to integrate and exploit it in both security and business processes. The second focuses more on the professionalism and ability of CTI purveyors. Another prominent issue was managing and exploiting the vast amount of data, information, and Intelligence, with many highlighting automation and AI solutions as crucial to extracting more value out of CTI. Other issues include the difficulty of measuring impact, as well as challenges with communicating analytical products in an effective manner.

4.6.2 Details

Maturity was a major theme throughout interviews, cited by most as a key impediment for full exploitation of CTI. Generally, maturity was described along two pillars: The first pertained to the size, resources, sophistication, and professionalism of an organization's cyber security system. The second pillar was more abstract, relating to an organization's ability to comprehend and utilize CTI in the decision making process, an exercise that could extend beyond dedicated security functions.

For instance, one senior analyst lamented how Intelligence as a concept was poorly understood:

> Very few understand what Intelligence really is and what an Intelligence function can contribute with. We´ve worked strenuously the last few years at getting them [decision makers] away from the latest Twitter feed or media headlines, into looking more long term at how to best utilize us. [...] This has especially been the case at the strategic level, educating users that our function is not providing indicators, but rather elucidating threat landscapes to support good decision making.

A corresponding point was raised by another interviewee, who called for greater reflection from the customer side on why they really wanted CTI and for what purpose. In their experience there was a lot of hype and buzzwords surrounding CTI, which they suggested may have driven some of the demand. This final point was an experience shared by other interviewees, with one suggesting it even damaged the profession:

> There is so much jargon circulated, to the extent that it's hurting our reputation. Some are seemingly making things up. Those who understand what these terms really entail get a bit dejected when some unfitting buzzword gets thrown around. This is an issue because to be understood and heard you rely on a maintaining a certain standing and respect.

Related, the senior analyst also argued that low maturity wasn't only a challenge at the 'user' side. Various reports, blogs, official documents, and books on CTI were described as inadequate on some accounts. For example, descriptions of what the Intelligence cycle entails, although common, were superficial and failed

to properly detail stakeholder discourse and the importance of exploring CTIs purpose, function, and utility.

Continuing the thread of raising understanding of CTI among stakeholders, another senior analyst suggested integrating risk assessments with threat assessments. Increasing the understanding on both sides would bring concrete benefits: Technical CTI analysts should gain a better understanding of risk management work by Governance, Risk, and Compliance (GRC) consultants and vice versa. The same point was raised by a different analyst, who suggested that they could increase the value and impact of CTI by integrating it in other products such as risk assessments or vulnerability assessments. Such efforts could also alleviate another issue: As many end users were not mature enough to make purposeful use of CTI, integrating parts of e.g. threat assessments in other services could make it more digestible. Moreover, another interviewee pointed to knowledge gaps between different security functions in the organization. Their issue was not necessarily related to poor understanding of CTI as a concept and how to effectively utilize it. Instead they lamented that the perception resulting from CTI at the strategic and operational level did not really seep through to the technical side such as the SOC, leaving them with unrealized potential.

Still on the topic of maturity, a security leader provided a candid assessment of their nascent CTI effort. While they recognized their maturity level was currently low, they saw opportunities going forward both in terms of how to employ certain capabilities and how to exploit CTI processually.

> We have started to utilize all these data sensors and now manage to aggregate and collate them. The platform [named technology] is also starting to be able to highlight the connection between all these sources. [...] But for the time being, we have lots of information, but not much in terms of Intelligence. The analysis, extracting the Intelligence product from it, we're not really there yet. [...] And we've been discussing the procurement of these other platforms and CTI sources. If we do that, will we get Intelligence or just another information source to aggregate?

Going forward, they explained that stakeholders needed to comprehend how to utilize CTI, and most important how it can create real value, in order to construct something viable. This would require building knowledge, competency and awareness, and not least how to integrate CTI in various processes throughout the organization. Other subjects also opined along the same lines, pointing to how CTI must be incorporated in business processes to extract its full value and purpose. One interviewee argued that while this was a well established practice within e.g. defense (from which Intelligence originates), their experience was that organizations in the civilian sector were not set up to facilitate or absorb it in the same way. With these issues in mind, the security leader also noted that in their experience CTI vendors could be clearer on these aspects of CTI when 'selling' their services and products.

Several interviewees pointed to automation, AI, and further optimization as a pertinent path to extracting more value from CTI. Seldom was data availability an issue: Where specific data or information were lacking, access could usually be bought or systems could be adapted to detect what was sought after. On the contrary, data glut was a commonly cited issue. For example, one senior advisor spoke of the need to construct an AI-assisted data lake. Conceivably, this could reduce the amount of noise and irrelevant data produced by various sensors, aiding analytical efforts and purposeful output. Further, collation could be improved vastly, which in turn would improve analysis by enabling a more powerful interface against well-sourced and sorted basic Intelligence. Pilot projects were indeed under way, both commercially and within respondents' organizations, but similar to AI broadly in most other industries net benefit was still some way off. On the topic of automation, many also brought up the value of Malware Information Sharing Platform (MISP). Uptake varied between sectors: Those who already had adopted it lauded its importance - after all, effective sharing is a key tenet of Intelligence - while those considering it viewed it as low hanging fruit. While sharing in itself was a repeated theme throughout interviews - most found data and information availability to be sufficient - one interviewee brought it up as an area needing improvement. Specifically, they found sharing of some Intelligence to be inadequate, especially between certain trust groups, CERTs, and other interest groups within industries that could benefit greatly from increased sharing and transparency.

As detailed in subsection 4.3.3, the state of feedback and measurements on CTI effectiveness and target realization was often lacking. This point was also a recurring theme among interviewees as an issue that could have a major impact if improved.

Finally, communication or dissemination was mentioned by several subjects as a crucial part of CTI, and as an area that was ripe for refinement. For example, one analyst spoke of how there was often a disconnect between conveyors and receivers, with CTI personnel failing to communicate at the level relevant to users, or even failing adapt their focus and knowledge to the environment and circumstances at hand.

Chapter 5

Discussion

In this chapter, the results will be discussed against theory and previous research detailed in chapter 2. The chapter is structured according to the research questions.

Problem statement:

> *How does Cyber Threat Intelligence provide utility for organizations?*

Research questions:

- RQ1: What effect does CTI have on organizations' security posture?
- RQ2: How does CTI affect stakeholder's decision making processes?
- RQ3: What factors determine CTI utility?
- RQ4: How are organizations able to exploit CTI?

5.1 RQ1 - What effect does CTI have on organizations' security posture?

In the context of this research question, 'security posture' means an organization's ability to detect, respond, and recover necessary function in the face of cyber attacks against IT systems and information assets under the responsibility of said organization.

When planning this thesis, one initial goal was to uncover and describe detailed actions that had been made as a result of specific CTI products. Motivation for this goal was the notoriously difficult challenge of assessing the usefulness of Intelligence (see subsection 2.1.1), which will also be discussed in section 5.2. One way of 'bypassing' the issue of examining opaque decision making processes, can be to look directly at changes being made. This may be easier within CTI than with other realms of Intelligence, since changes made often be more concrete: Networks and firewalls are configured, vulnerabilities are patched and so forth. Yet no interviewees were able to elaborate in detail on what actual changes had been made, for source and method protection reasons. Meanwhile, they were willing to provide generalized descriptions of how CTI had directly contributed

to isolated security improvements. All examples provided were on an operational or tactical level, with disruption, mitigation, or impact reduction as achieved effects. Furthermore, measures taken were often cited as a result of early warning, a common sub-function of Intelligence that is proven effective in preventing cyber incidents [18].

It should be repeated that when we look at 'changes made' as an indicator of usefulness, even when those changes are relayed by interviewees as definite links between CTI and security changes, it still only functions as a proxy indicator in lieu of a proper measurement regime. Measurements will also be treated in section 5.4, but a short discussion on its challenge is useful here. To reiterate from the introduction and problem statement, capturing the effect of organizational processes, as CTI partially can be considered, is quite challenging. For CTI, there are at least two main issues. The first is what to measure: Conceivably, we could find a way to gauge the level of malicious cyber activity against an organization, which is likely quite feasible through the monitoring activity of e.g. SOC operations. But that leaves the significant issue of false negatives: Actual compromisations are what matters, and successful ones are by definition usually not detected. Looking at impact on business processes in terms of monetary or operational loss could be another metric, but since impact on that scale is relatively rare any statistics would be very eschewed, in addition to the issue of isolating the enabler or the cause of the compromise. As a corollary to the last point, some subjects spoke of the difficulty of pinpointing CTI as a determining factor, especially with regards to the blurred lines between CTI and other security functions. The second issue concerns the actual live environment that is cyber space: We simply cannot control the variables of the evolving threat landscape, IT systems, and human motivational factors, seriously complicating the efforts of separating correlation from causation. In essence, this sort of exercise is practically infeasible for most organizations. Hence, if we return to CTI theory (2.1) and its definition:

> Threat Intelligence enables us to make faster, more informed, data-backed security decisions and change their behavior from reactive to proactive in the fight against threat actors

I contend that the focus on **decisions** (5.2) and **action** are both feasible and adequate methods of evaluating CTI usefulness.

With this in mind, it is interesting to revisit the perhaps most relevant study from the literature review (2.2). [19] This study was also qualitative, but with the added benefit that the authors had the opportunity to conduct a pre/post-adoption study as practitioner/researchers in a real organization that implemented CTI. The proximity and familiarity with the subject organization enabled as close to control of one part of the environment as practically possible. One finding was that the adoption of CTI had significantly improved the cyber security situation by "*reducing the success rate and impact of attacks as they were thwarted higher up in the kill chain*". In essence, this finding correlates with the benefits of early warning - with the effects of disruption, mitigation, and impact reduction - that were reported in

the data. When it comes to the 'kill chain', it was only explicitly mentioned by two interviewees. But several more mentioned structured analytical techniques and improved analytical mindset as having an impact on the human aspect of the cybersecurity posture. This factor can also be seen in conjunction with structure and focus in general, with interviewees highlighting CTI as a multiplier enabling both process and product to be optimized, and as a service that aid prioritization and reinforces other efforts. Again, another potential value identified by said study was "*improving efficiency and focus of cyber defense operations*".

One final point from that study was that, while arguing that there is no direct causal link between CTI implementation and cyber security performance, they attempted to capture performance by applying the following logic: Reactive and undirected defensive behaviour indicates low performance, while proactive and directed behaviour translates to high performance [19]. The notable difference between that study and this thesis, is that the former examined *behavioral transformation* between two states. This was supported by evidence, such as Incidence Management Records and Risk and Problem Ticketing Records. Naturally, no such evidence could be made available for this author. What we are left with is the testaments from the sample population, many of which point to advanced behaviors in the latter category, suggesting that while not a demonstrable causal contributor, they at least strongly indicate that CTI contribute to an improved cyber security posture. Finally, it should be mentioned that the cases reviewed were successful examples. As we will discuss throughout this chapter, the possibility for CTI to deliver tangible security outcomes such as these depend on several other factors.

5.1.1 Partial Conclusion

Within the sample population, all subjects with sufficient insight asserted that CTI made a positive contribution to the security posture of their own organization or that of end users. Meanwhile, substantiating causal links remains elusive, and isolating the effect of CTI from other security services is challenging. This is why discussions focused on 'changes made' as a vessel to agnostically capture CTI impact. In conclusion, when it comes to successful instances, the effects reported fell within two realms: The impact of cyber attacks were reduced by mitigation occurring at an earlier stage, and the efficiency, structure, and focus of defense operations were improved.

5.2 RQ2 - How does CTI affect stakeholder's decision making processes?

One of the core tenets of CTI is aiding and improving decision making. Reiterating from the definitions:

> [...] Threat Intelligence enables us to make faster, more informed, data- backed security decisions and change their behavior from re-

> active to proactive [6] and [...] in order to identify threats and offer opportunities for exploitation by decision-makers [4]

As such, when considering how CTI provide utility, we should examine how it affects decision making processes.

Firstly, on this topic many subjects highlighted the value of early warning. This was thoroughly covered in section 5.1, but in this context interviewees also spoke of the organizational aspect. For example, for many advanced warning created the opportunity to deliberate more in depth, on a more informed foundation, whether and when to allocate precious resources to perform counter measures.

Some also spoke of the role of CTI in early advisory, brought in to counsel new establishments before going live. Related is also CTI contribution to investments and budget approvals, with many respondents confirming their awareness of such instances. Details were scarce for security reasons, but one elaborated on an interesting dynamic of intra-organizational difference in receptiveness, where the ultimate (positive) investment decision was made by a more mature part of the organization. Within this topic, subjects also spoke of the positive impact of serial reports and how a totality over time had probably enabled the effects they saw in this realm. As a side note, these accounts also speak to the importance of effective communication and dissemination methods, where products are adapted in a manner that conveys their meaning and utility. When it comes to CTI influencing investment decisions, we are clearly discussing 'strategic level effects'. Here some terminology should be addressed. As one interviewee put it succinctly:

> Very few if any organizations utilize Intelligence in their decision making processes at the strategic level or within the C-suite, with the exception of defense and security related sectors [...] Yet in the market, some do provide CTI products and services within 'geopolitical analysis' and the like. How many companies actually need those and are able to use them?

Indeed, within the Intel world, 'strategic intelligence' is usually used to describe the types of products mentioned above, with grand complexities and long term trends among nation states. Importantly, this should be separated from strategic as an adjective in the dictionary, where CTI to support investment decisions can certainly be classified as something "done as part of a plan that is meant to achieve a particular purpose" [38].

CTI as a component in risk management was another prominent topic, one also listed by the UK NCSC as a common use case (Figure 2.2). Specifically, interviewees spoke of how in some cases CTI products complemented risk assessments efforts by focusing on actor descriptions and their intentions, which aided the difficult task of assessing probability when taking into account your own assets and exposure. As such, this Intelligence led to a more substantiated risk picture, and a baseline risk score on which further infosec decisions could be made. These accounts correspond with one of the findings from Kotsias *et al.* [19]:

> Organisations should realise that possibilistic cyber-risks are inherently unpredictable and there is no determinate relationship between investment in security safeguards and reduction in risk exposure. To address possibilistic cyber-risks, organisations must introduce two new externally focused constructs, i.e., cyber-threat actors' intentionality and capability into their risk calculus.

By possibilistic, it is meant to meant that threat actors must be viewed as innovative and highly unpredictable. Under this paradigm cyber attacks are dynamic, and their associated risks cannot be quantified in advanced, hence the utility of actor knowledge as proposed by said interviewees. It is noteworthy how the strong value of actor knowledge as proposed by one security leader was not shared by one in the same organization that worked more at the operational level. By their own account, much was still to be done i terms of adapting the organization to operationalize new capabilities. Without running too far with a single data point, this discrepancy hints at how demanding it can be to extract value from CTI, which will be discussed further in section 5.4.

The different examples discussed so far, clearly demonstrate that CTI does indeed contribute to supporting decision making under the right circumstances, partially confirming the research question. But what about the outcome? The problem statement focuses on utility, necessitating an improved outcome. Recall from subsection 2.1.1, that effectiveness is an attribute extrinsic to the Intelligence product, which can only be evaluated retroactively. None of the sample population, even among leadership, expressed that they possessed the required insight or granularity to assess actual outcomes, an exception being incidence response where decisions to employ counter-measures result in some tangible event being mitigated. Although not an explicit talking point during interviews, this author claims that mechanisms to evaluate decision making processes are rarely employed in real life, beyond post mortem assessments after crisis. This invariably creates blind spots and complicates the effort to judge abstract problems, especially when it comes to CTI as a strategic level advisory.

5.2.1 Partial Conclusion

The analysis reveals several key insights into how CTI influences decision-making. For instance it is evident that CTI through early warning facilitates more informed and proactive decision making, which is in line with how CTI is defined as well as best practices described in the literature. At a higher organizational level, CTI can also assist in investment decisions by providing strategic-level insights, although this appears to depend on receptiveness and maturity of the receiver, as well as how effectively the Intelligence is conveyed. Further, CTI complements risk assessment efforts by contributing to a more nuanced understanding of cyber security risks, enabling organizations to make informed decisions on security safeguards. Despite the potential benefits, operationalizing and extracting value from intelligence capabilities remains difficult. While CTI demonstrably influence decision

making as intended, challenges persists in evaluating actual outcomes.

5.3 RQ3 What Factors Determine CTI Utility?

In RQ1 and RQ2, we discussed how CTI affects user organizations through two means: Changes made and influence on decision making. Together these constitute this thesis' operationalization of one part of how Kovacs [7] describe how Intelligence is used. The second part pertains to what Kovacs describe as 'usability' (referred to in this thesis as utility). As described in subsection 2.1.6 and section 2.2, there are myriad schemes developed over the decades that detail utility factors commonly cited throughout the profession and larger industry. These factors and principles were deliberately not made explicit when discussing the topic during interviews, in order to avoid framing the conversation. This approach also support one of the aims of the problem statement which is capturing real experience and practice from normative theory. When it comes to utility factors, they can be viewed from two perspectives: That pertaining to the user organization (5.4), and that of the CTI service and product. This section will discuss the latter.

One of the most common themes brought up was how CTI must be **relevant** for it to be usable. We can consider relevance to consist of two components. The first is the property of being *tailored* as it was put by one interviewee, which means that it must answer specifically to customer requirements. This property is equally dependent on the user organization itself, and will be discussed further in section 5.4. The second component is intrinsic to the CTI product, and applies to whether it can deliver **unique** value which cannot be easily obtained elsewhere. In turn, we can further split this component in two: Added value as a result of analysis, and as a result of unique collection. These properties are crucial as they go into the very core definition of what can be considered CTI and what is mere information or data.

For instance, the property of added value as a result of an analytical process was mentioned in one way or another by several interviewees. Some referred to it as *enrichments* or *contextualization*. This described the ability to provide additional context through collation and subsequent analysis, with one exemplifying the process by pointing to how they could ingest 'seed indicators' on request and return analyzed CTI products. Other adjectives were put forth when describing the analytical part of CTI, such as automation, efficient data flow, maintenance, and integration. Analysis is a core property of 'regular' Intelligence, but may be even more important in CTI, especially at the tactical and operational level as alluded to above. For example, Oosthoek and Doerr [39] maintain that the volume and velocity of cyber threats make the absence of rigorous analytical methodology even more visible. While applying structured analysis (as taught in Intelligence studies) on thousands of artifacts is unfeasible, the lack of an overarching analytical process can lead to analysis paralysis. Furthermore, they contend that while machine learning is being applied successfully to much of the collation process, it is yet far

from able to capture the tacit knowledge or intuition of human analysts. The proposed solution is more process, not technology. Accordingly, a number of subjects were emphatic on the importance of analysis in the CTI cycle, expressing their apprehension of introducing even more unstructured, unexploitable information that overwhelmed security personnel. As one interviewee put it:

> [...]Putting all this together within the organizational pipeline, maintaining it, and create real **actionable** Intelligence, I think that is one of the most important things. This is the very tricky bit, but also the bit that makes it useful right? Otherwise it's just one more pile of data.

Recalling from the CTI definition (2.1), Threat Intelligence is data that is collected, **processed**, and **analyzed**. Within the sample, some lamented that in the commercial space, CTI sometimes encompassed other services they considered to be outside the scope of Threat Intelligence. Moreover, there was also a prevalence of jargon and buzzwords surrounding CTI. One could reasonably question whether strict adherence to definitions really matter, as long as the service has an impact and customers are pleased. But at least one subject was adamant that lack of professionalism negatively impacted their reputation and respect, an important factor to another much cited utility factor concerning effective communication and dissemination. Another subject even asserted that their credibility and trust directly impacted end users' degree of action. In fact, empirical evidence from other studies highlight 'perceived trust' as a significant success factor [11][13], suggesting that these issues should not be ignored by CTI professionals.

Continuing with the topic of unique value, collection is also an important facet which warrants discussion. Several interviewees brought up their unique access as a significant utility factor, in which they were able to provide Intelligence end users could not obtain from other commercial sources. Proceeding with the debate of what CTI actually constitutes, a pertinent question is whether unique collection capabilities is a prerequisite in that regard. As discussed in chapter 2, definitions often point to the relationship between user and producer (Intelligence dialogue), and a certain level of analysis. But if we take a reductive attitude, many services can be said to "provide thoughtful answers to specific questions". As such, within traditional Intelligence there is often a focus on the secret aspect of operations and collection as a defining future to separate Intelligence activity from that of e.g. think tanks [40]. But this is obviously not applicable in the realm of commercial operations such as that of Business Intelligence or CTI. Indeed, an important caveat to the statements above is that those mentioning access as a key factor were in that position due to specific regulatory and operational environment. Thus, in this author's view it is not reasonable to demand unique collection or access as a litmus test of CTI. Instead, CTI professionals are better off striving for relevance and added value by responding to requirements in a comprehensive, efficient, and systematic manner.

Finally, timeliness was proposed by many as a critical to CTI's utility, which is both an established principle (see subsection 2.1.6) and a common quality factor

[11]. Ultimately, other factors mentioned such as automation and efficient data flow partially underpins timeliness, speaking to its centrality to an effective and usable CTI service. Closely related to early warning, its effects are sufficiently discussed in sections 5.1 and 5.2.

5.3.1 Partial Conclusion

Utility factors describe what features of CTI products are most important for users, as opposed to *how* they are put to use or towards what *effect*. Relevance was identified as the most prevalent factor according to this study, considered to consist of two components in this context: Added value as a result of analysis, and as a result of unique collection. Although both properties are demonstrably important and effectual, it is unreasonable to expect the latter from most commercial CTI operations. On the other hand, analytical tradecraft, also encompassing other properties such as integration, contextualization, efficiency, and timeliness, are seen as key components of a usable CTI service. As such, a central part of the very definition of CTI is found to be a crucial utility factor. Thus, observing definitions is not only an academic exercise. Failing adherence to core features of CTI is also detrimental to professionalism and trust, which in turn affects the ability to communicate and influence decision making.

5.4 RQ4 Are Organizations Able to Exploit CTI?

This section will discuss to what extent user organizations are able to exploit the potential value that lies in having a CTI program. The discussion will also include perspectives on what CTI professionals experience as major challenges.

A significant portion of the sample population highlighted end users' own ability to exploit CTI as perhaps the most important determining factor when assessing how it provides utility for organizations. The prevalent term used to describe these abilities is 'maturity', or more specifically 'cyber security maturity'. In this regard, the recommendations of the UK NCSC is worth repeating [8]:

> [...] organisations should only make significant CTI investments after achieving or being on a realistic roadmap to completing all of their other recommended cyber security standards. Furthermore, even mature organisations should only establish Threat Intelligence programs if they have the capacity, capability, and intent to actually utilize it. This entails not only the technical aspects: System owners must be empowered to act on Threat Intelligence for it to have meaning.

From this recommendation we can unpack two facets:

1. Overall cyber security standards
2. Ability and intent to utilize

On the first point, we can consider 'cyber security standards' as synonymous with 'maturity'. Since *formal* standards and maturity levels were not explicit discussion points during interviews, no judgement can be made on adherence to this recommendation (or others) from the sample population. Granted, a few subjects brought up the subject. For example, interviewees from a cyber security firm reported to have maturity assessments as an integral part of their customer relationship, using the NIST framework for cyber security maturity. Through this exercise they could set realistic expectations and calibrate the level of guidance provided early in the process.

Although formal standards were not explicitly discussed it was clear that maturity as a property was prevalent in security professionals' minds, with most discussion pertaining to the second facet. For instance, organizational receptiveness and comprehension was a frequently raised talking point. With a few exceptions, the overall understanding of CTI was reportedly inadequate, where CTI professionals spent considerable time educating stakeholders on the potential contributions of an Intelligence function. Very few viewed it in terms of decision support, with some reporting that a perception of CTI as a merely a source indicators prevailed. Hence, there seems to exist a conception of CTI as being another cyber security function that runs in the background with minimal input from the larger organization, indicating that the traditional view on cyber security as something being handled by IT still persists to a degree. A few factors have likely contributed to this view. One pertains to an industry which to some degree is characterized by weak methodology, buzzwords and jargon, driven by profit incentives (see also section 5.3). As Oosthoek and Doerr [39] put it:

> The marketing of CTI-related products and services is an increasingly important revenue-generating asset for many cybersecurity vendors with roots in the production of firewall and antivirus offerings. They have re-branded the commodity activity of providing a blacklist into a "CTI" operation [...]

In this regard, it is likely that the prerequisites for a valuable CTI program are either not known or clearly communicated at an early stage, as expressed by some in this survey. Another factor, perhaps ironically, may come from increased infosec awareness. The upshot of governmental information campaigns combined with a host of high profile security incident, have left organizations more willing to invest in infosec. Consequently, organizations search for improvements and find a receptive market, but often don't possess the maturity needed to understand what they need or take advantage of solutions offered. As one interviewee paraphrased from customer dialogues:

> We are aware that information security is important, and the threat is increasing. We suspect that we haven't assessed this properly the last 10 years, can you advise us on what we need to do?

It is certainly unrealistic, and probably unnecessary, to expect all decision makers and stakeholders to comprehend the finer nuances of Threat Intelligence

and infosec at large. But understanding Intelligence on a conceptual level is still crucial for those who are tasked with operationalizing its potential value through the process of developing requirements. Requirements-driven CTI is not merely jargon put forth by a Mandiant, a commercial vendor [10]. In fact it is fundamental to the entire Intelligence process, requiring some form of input from most parts of the organization [4]. Thus, the extent to which organizations are able to conduct a proper IRM process can be viewed as a gauge of maturity level, and consequently as an indicator of how well they are able to exploit CTI. Broad organizational involvement in the IRM process may seem both daunting and demanding, but stakeholder analysis has precedence in other parts of information security. For example, it is central to all parts of the ISO27001 standard for information security management [41]. This includes risk management, an area highlighted as a beneficiary of CTI by many in this survey, as well as a typical stakeholder according to Mandiant's paper on requirements-driven CTI. In fact, some suggested integrating CTI in more established processes as a way of raising understanding and easing its adoption.

When it comes to the state of the art of stakeholder involvement, responses in this survey were mixed. At one end of the spectrum there were reports of highly developed, comprehensive, and structured processes with some aiming to capture a broad set of stakeholder requirements and focusing on adapting communication, product, and dissemination to various recipients. At the other end of the spectrum were reports of end users unable to specify their requirements or comprehending where CTI fit into the overall infosec regime. Also, even with a clear understanding of the overall purpose and function, some mentioned that operationalizing CTI could be challenging, leaving them with unrealized potential.

Related, feedback and measurements is an important facet of the IRM process, as it enables both adjustment of existing requirements as well as the development of new ones. It should be noted that none reported to have completely satisfactory feedback systems and routines, with most highlighting the issue as an area they wished to improve. As discussed in section 5.1, this is a notoriously difficult subject, with proposed methodologies still in its infancy [42]. Also, the issue is more difficult at higher levels of abstraction: UK National Cyber Security Centre (NCSC) [8] suggests strategic products are the most challenging to create effective metrics and measurement for as the value of products is often both opaque and delayed. The data also indicates this to be the case, where a number of interviewees lauded qualitative dialogue to be crucial in capturing impact at higher levels.

On this topic we see similar results to that of stakeholder involvement with the same distribution: Organizations reporting to have well developed IRM processes also reported to have more structured feedback and measurement. Analyzing the data further, we find a larger picture emerging. From the sample, the top three respondents in terms of IRM process development also stand out as being surer of CTI impact: Their accounts on CTI effects and outcomes are characterized by being clearer, more detailed, and more confident compared to the rest of the population who are marked by more reservations and caveats. Whether this is due to

actual CTI impact and usefulness being stronger, or a result of better insight and granularity is unknown. But the theory certainly suggests a correlation between high maturity levels, as these accounts indicate, and ability to exploit the potential of CTI.

If the evidence points to high maturity having a positive impact on extracting value from CTI, it is less clear how the opposite has an effect. Recall Mandiant's common CTI pitfalls, describing event-driven, analyst-driven, and product-driven Intelligence as possible consequences of poorly developed IRs (Figure 2.4). Several interviewees self-report low maturity levels. While generally cognizant of ongoing challenges, none brought up such issues specifically. Conceivably, these pitfalls do not emerge or are identified until some time has passed, and low maturity organizations with long-running CTI programs do not occur in the sample population.

Meanwhile, in one interesting case from the data we can see how the two facets of NCSC's recommendation were deliberated fully. A seasoned CTI veteran now occupying the role of CISO had opted not to adopt a CTI service after careful consideration, citing a few different reasons. Firstly, they assessed that their organization was not mature enough to effectively exploit the potential advantages of CTI. Secondly, they focused on fully implementing an ISO standard infosec management system, in line with what they referred to as the 'extensive compliance culture' of the organization. Thirdly, they considered their overall technical security level to be excellent, and the threat environment to be favorable with a low probability of sophisticated targeting. Tying all these factors together, they referred to the overall business perspective where security was primarily seen as an expense, and within current risk assessments CTI could not be justified from an ROI position. The second and third points are instructive. Baskerville (2005, as cited in Kotsias *et al.* [19]), argued that this approach was outdated almost two decades ago:

> [...]the prevailing prevention paradigm assumes risks can be anticipated, measured, and quantifiably mitigated in advance using cybersecurity controls. This paradigm renders risk management a problem of compliance, rooted in the probabilities of known attacks

Instead, as Kotsias *et al.* [19] also concluded, a possibilistic methodology is required in cyber defense to account for the entropy in today's threat landscape, to which Threat Intelligence is the proposed answer. As such, the approach discussed in the case above can reasonably argued to be complacent. Yet in this authors view, while the proposed possibilistic approach which conceptually rests on CTI may be theoretically advisable, it faces some key constraints at many organizations. Even if we assume that the proposal is made with a certain size and budget in mind, we must still contend with the second facet of the NCSC recommendation which entails '*ability and intent to utilize*'. In this perspective, maturity considerations should take precedence, leaving the adoption of CTI as a recommended option only for the most advanced infosec programs. Besides the maturity reflections

already discussed, another corollary to this position could be heard from in this survey. Several respondents expressed concerns of introducing yet another data or information source, saturating the information space without the proper processing ability.

Regardless of what one consider to be the prudent choice, this case illustrates how opposing infosec recommendations call for a self-reflective view on needs and maturity that many firms seem not to realize.

5.4.1 Partial Conclusion

To a large degree, the ability to exploit and extract real value from CTI rests on an organization's cyber security maturity level. The status quo reveals a significant disparity with many challenges. A number of organizations appear to struggle with understanding CTI's potential contributions, what is required to implement it successfully, and whether they really need it. The CTI industry also bears responsibility. In some cases it is marked by inaccuracies and a lack of professional rigor, but still find a receptive audience in today's climate of cyber insecurity. Consequently, a perception persists of CTI as a background function rather than a strategic asset.

An organization's ability to conduct an IRM process is both an indicator of overall maturity, as well as its ability to successfully exploit CTI. Doing so properly entails capturing the needs of all relevant stakeholders and adapting CTI production accordingly. Feedback loops and measurements are closely related, as it guides and improves on the requirement process. Accurately measuring impact is incredibly difficult, especially at higher levels of abstractions. Both pillars of stakeholder involvement see substantial spread in the survey, but organizations at the advanced end of the spectrum exhibit signs of extracting greater value from CTI compared with less mature organizations. As most are positive to CTI's overall contribution, it is impossible to point to a threshold where the ROI is favorable. But seeing that barriers of entry are quite high, organizations probably do well with a self-reflective view and adopting the entire process if committing to CTI.

5.5 Limitations and Future Research

The methodology chosen for this thesis was that of semi-structured interviews, coupled with a thematic analysis approach. Both are quite fluid and flexible, which comes with some advantages and disadvantages. For example, since semi-structured interviews allowed for emerging paths to be explored ad hoc, no two interviews were exactly similar. This means that particular topics were only discussed with a few subjects, although that was almost certainly related to the variation in the sample. Regardless, I'm confident that all of the primary aspects of the topic were sufficiently explored with all subjects. Furthermore, a feature of the methodology is that only subjective experiences were captured and subsequently discussed

withing theoretical frameworks. While considered infeasible for this thesis, an improvement on the methodology could include evidence from logs or records to correlate and further investigate expert opinions and accounts.

A major discussion point throughout this thesis is the inherent difficulty in measuring the real impact of CTI, especially with regards to decision support which can be opaque and diffuse even to decision makers themselves. In the project management world some utilize decision tracking software to improve notoriety and visibility. Finding candidates with CTI programs that also employ these could present an opportunity for more avant-garde research, although gaining entry would likely propose a major challenge in itself.

Chapter 6

Conclusion

The investigation into the utility of Cyber Threat Intelligence (CTI) has revealed a nuanced landscape where its impact is discernible yet challenging to measure definitively. Across the spectrum of research questions, several key themes emerge, shedding light on both the potentials and limitations of CTI.

Firstly, the sample suggest a causal link between CTI and changes made to organizations' security postures. Moreover, respondents assert that CTI has an overall positive contribution to security, predominantly manifesting its value through early threat detection, leading to more efficient and focused defense operations. However, attributing specific security improvements solely to CTI proves challenging amidst the broader array of security measures in place.

In terms of its influence on decision-making processes, CTI emerges as a catalyst for informed and proactive decision-making, particularly through early warning capabilities. Strategic-level insights provided by CTI can also inform investment decisions and complement risk assessment efforts, but operationalizing these insights at lower levels remains difficult. Meanwhile, even where causal links between CTI and decision making are reported, assessing whether actual outcomes improve remains a formidable challenge, highlighting the difficulty of judging impact on organizational processes. The issue appears most pertinent with strategic level CTI, the overall utility and efficacy of which remains most indeterminate throughout this study.

When it comes to CTI utility factors, relevance emerged as the major determinant. Relevance can be understood as added value, either as a result of analysis or unique collection. Analytical tradecraft is also closely related to or encompasses other features such as integration, contextualization, efficiency, and timeliness. A defining feature of CTI, its importance cannot be overstated. Arguably, without an analytical component it cannot be called Threat Intelligence, and in this regard the study found some CTI services to be questionable. In some ways, its absence risks undermining professionalism and trust, which in turn affects the ability to communicate and influence decision making.

Finally, the ability of organizations to exploit CTI is closely intertwined with their cybersecurity maturity level. In this regard, there is significant disparity

among end users. While CTI holds promise as a strategic asset, many organizations struggle with understanding its potential contributions and implementing it effectively. Moreover, the CTI industry itself faces challenges of professional rigor, contributing to a perception of CTI as a background function rather than a strategic enabler. Ability to engage stakeholders through a proper Intelligence Requirement Management (IRM) process is an indicator of maturity and well as of the potential to exploit CTI. Organizations with well established IRM processes exhibit greater ability to extract value from CTI.

In conclusion, while CTI offers tangible benefits in enhancing security postures, informing decision-making, and mitigating cyber threats, realizing its full potential requires organizational commitment, cybersecurity maturity, and a refined understanding of CTI's capabilities and limitations as well as of their own requirements. As such, potential adopters would be well advised to reflect on these relatively high barriers of entry before justifying the investment. Moving forward, fostering collaboration between stakeholders, enhancing analytical capabilities, and promoting industry professionalism are essential steps in maximizing the utility of CTI within organizations.

Bibliography

[1] K. Zetter, *Hacking wall street*, Jul. 2021. [Online]. Available: https://www.nytimes.com/2021/07/03/business/dealbook/hacking-wall-street.html.

[2] National Institute of Standards and Technology, *Threat Intelligence*, https://csrc.nist.gov/glossary/term/threat_intelligence, [Online; accessed 6-May-2024], 2024.

[3] J. Goksør, *Effectiveness of cyber threat intelligence*, Project report in TTM4502, May 2023.

[4] E. Kristoffersen, 'Forsvarets etterretningsdoktrine,' Norwegian Armed Forces, Oslo, Tech. Rep., Jan. 2021, p. 57. [Online]. Available: 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.

[5] C. Rice, *Cyber threat intelligence research paper*, Accessed: January 18, 2024, 2014. [Online]. Available: https://www.foo.be/docs/informations-sharing/Payments%20UK%20Cyber%20Threat%20Intelligence%20Research%20Paper.pdf.

[6] K. Baker. 'What Is Threat Intelligence.' (2023), [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/ (visited on 06/05/2024).

[7] A. Kovacs, 'Using intelligence,' *Intelligence and National Security*, vol. 12, no. 4, pp. 145–164, 1997. DOI: 10.1080/02684529708432452. [Online]. Available: https://doi.org/10.1080/02684529708432452.

[8] UK National Cyber Security Centre (NCSC), 'Cyber threat intelligence in government: A guide for decision makers & analysts,' UK National Cyber Security Centre, Tech. Rep., Mar. 2019.

[9] A. Roberts, *Cyber Threat Intelligence: The No-Nonsense Guide for CISOs and Security Managers*, eng, 1st ed. Berkeley, CA: Apress L. P, 2021, ISBN: 9781484272190.

[10] J. Collier, S. Ronis, I. Lane and R. Simpson, *A requirements-driven approach to cyber threat intelligence*, https://mandiant.widen.net/s/nvnljhtpjg/requirement-driven-approach-to-cti-white-paper, Mandiant, 2023.

[11] A. Zibak, C. Sauerwein and A. Simpson, 'A success model for cyber threat intelligence management platforms,' *Computers and Security*, vol. 111, p. 102 466, 2021, ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2021.102466. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S016740482100290X.

[12] A. Zibak, C. Sauerwein and A. C. Simpson, 'Threat intelligence quality dimensions for research and practice,' *Digital Threats*, vol. 3, no. 4, Mar. 2022, ISSN: 2692-1626. DOI: 10.1145/3484202. [Online]. Available: https://doi.org/10.1145/3484202.

[13] T. Schaberreiter, V. Kupfersberger, K. Rantos, A. Spyros, A. Papanikolaou, C. Ilioudis and G. Quirchmayr, 'A quantitative evaluation of trust in the quality of cyber threat intelligence sources,' ser. ARES '19, Canterbury, CA, United Kingdom: Association for Computing Machinery, 2019, ISBN: 9781450371643. DOI: 10.1145/3339252.3342112. [Online]. Available: https://doi.org/10.1145/3339252.3342112.

[14] V. Mavroeidis and S. Bromander, 'Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence,' in *2017 European Intelligence and Security Informatics Conference (EISIC)*, 2017, pp. 91–98. DOI: 10.1109/EISIC.2017.20.

[15] C. Sauerwein, D. Fischer, M. Rubsamen, G. Rosenberger, D. Stelzer and R. Breu, 'From threat data to actionable intelligence: An exploratory analysis of the intelligence cycle implementation in cyber threat intelligence sharing platforms,' in *Proceedings of the 16th International Conference on Availability, Reliability and Security*, ser. ARES 21, Vienna, Austria: Association for Computing Machinery, 2021, ISBN: 9781450390514. DOI: 10.1145/3465481.3470048. [Online]. Available: https://doi.org/10.1145/3465481.3470048.

[16] M. Husák, T. Jirsik and S. J. Yang, 'Sok: Contemporary issues and challenges to enable cyber situational awareness for network security,' in *Proceedings of the 15th International Conference on Availability, Reliability and Security*, ser. ARES '20, Virtual Event, Ireland: Association for Computing Machinery, 2020, ISBN: 9781450388337. DOI: 10.1145/3407023.3407062. [Online]. Available: https://doi.org/10.1145/3407023.3407062.

[17] C. Krasznay and G. Gyebnár, 'Possibilities and limitations of cyber threat intelligence in energy systems,' in *2021 13th International Conference on Cyber Conflict (CyCon)*, 2021, pp. 171–188. DOI: 10.23919/CyCon51939.2021.9468289.

[18] M. Xu, L. Hua and S. Xu, 'A vine copula model for predicting the effectiveness of cyber defense early-warning,' *Technometrics*, vol. 59, no. 4, pp. 508–520, 2017, ISSN: 00401706, 15372723. [Online]. Available: http://www.jstor.org/stable/44869216 (visited on 09/05/2023).

[19] J. Kotsias, A. Ahmad and R. Scheepers, 'Adopting and integrating cyber-threat intelligence in a commercial organisation,' *European Journal of Information Systems*, vol. 32, no. 1, pp. 35–51, 2023. DOI: 10.1080/0960085X.2022.2088414. eprint: https://doi.org/10.1080/0960085X.2022.2088414. [Online]. Available: https://doi.org/10.1080/0960085X.2022.2088414.

[20] R. Brown and R. M. Lee, 'The evolution of cyber threat intelligence (cti): 2019 sans cti survey,' *SANS Institute. Available online: https://www. sans. org/white-papers/38790/(accessed on 12 July 2021)*, 2019.

[21] C. G. Thomas, *Research Methodology and Scientific Writing*. Mar. 2021, ISBN: ISBN 978-3-030-64864-0. DOI: 10.1007/978-3-030-64865-7.

[22] B. Kaplan and J. A. Maxwell, 'Qualitative research methods for evaluating computer information systems,' in *Evaluating the Organizational Impact of Healthcare Information Systems*, J. G. Anderson and C. E. Aydin, Eds. New York, NY: Springer New York, 2005, pp. 30–55, ISBN: 978-0-387-30329-1. DOI: 10.1007/0-387-30329-4_2. [Online]. Available: https://doi.org/10.1007/0-387-30329-4_2.

[23] J. Maxwell, *Causality in Qualitative Research*. London: SAGE Publications, Inc., 2019. DOI: 10.4135/9781526421036856899. [Online]. Available: https://methods-sagepub-com-christuniversity.knimbus.com/foundations/causality-in-qualitative-research.

[24] J. Johnson and T. Rowlands, 'The interpersonal dynamics of in-depth interviewing,' in *The SAGE Handbook of Interview Research: The Complexity of the Craft*, 2nd ed., SAGE Publications, Inc., 2012, pp. 99–114. DOI: 10.4135/9781452218403.

[25] B. DiCicco-Bloom and B. F. Crabtree, 'The qualitative research interview,' *Medical Education*, vol. 40, pp. 314–321, 2006. DOI: 10.1111/j.1365-2929.2006.02418.x.

[26] R. Legard, J. Keegan and K. Ward, 'In-depth interviews,' *Qualitative research practice: A guide for social science students and researchers*, vol. 6, no. 1, pp. 138–169, 2003.

[27] M. N. Marshall, 'Sampling for qualitative research,' *Family practice*, vol. 13, no. 6, pp. 522–526, 1996.

[28] B. Beitin, 'Interview and sampling: How many and whom,' in *The SAGE Handbook of Interview Research: The Complexity of the Craft*, 2nd ed., SAGE Publications, Inc., 2012, pp. 243–254. DOI: 10.4135/9781452218403.

[29] G. Guest, A. Bunce and L. Johnson, 'How many interviews are enough? an experiment with data saturation and variability,' *Field methods*, vol. 18, no. 1, pp. 59–82, 2006.

[30] N. Golafshani, 'Understanding reliability and validity in qualitative research,' *The qualitative report*, vol. 8, no. 4, pp. 597–607, 2003.

[31] Merriam-Webster. 'Reliability.' (2024), [Online]. Available: https://www.merriam-webster.com/dictionary/reliability (visited on 06/05/2024).

[32] L. Leung, 'Validity, reliability, and generalizability in qualitative research,' *Journal of Family Medicine and Primary Care*, vol. 4, no. 3, pp. 324–327, Jul. 2015. DOI: 10.4103/2249-4863.161306.

[33] Personopplysningsloven, *Lov om behandling av personopplysninger (personopplysningsloven)*, https://lovdata.no/dokument/NL/lov/2018-06-15-38/KAPITTEL_gdpr-7-3KAPITTEL_gdpr-7-3, 2018.

[34] J. Morse, 'The implications of interview type and structure in mixed-method designs,' in *The SAGE Handbook of Interview Research: The Complexity of the Craft*, 2nd ed., SAGE Publications, Inc., 2012, pp. 193–205. DOI: 10.4135/9781452218403.

[35] M. Vaismoradi, H. Turunen and T. Bondas, 'Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study,' *Nursing & Health Sciences*, vol. 15, no. 3, pp. 398–405, 2013. DOI: https://doi.org/10.1111/nhs.12048. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1111/nhs.12048.

[36] N. Humble and P. Mozelius, 'Content analysis or thematic analysis: Similarities, differences and applications in qualitative research,' in *European Conference on Research Methodology for Business and Management Studies*, vol. 21, 2022, pp. 76–81.

[37] J. Fereday and E. Muir-Cochrane, 'Demonstrating rigor using thematic analysis: A hybrid approach of inductive and deductive coding and theme development,' *International Journal of Qualitative Methods*, vol. 5, no. 1, pp. 80–92, 2006. DOI: 10.1177/160940690600500107.

[38] Oxford Learner's Dictionaries. 'Strategic.' (), [Online]. Available: https://www.oxfordlearnersdictionaries.com/definition/english/strategic (visited on 06/05/2024).

[39] K. Oosthoek and C. Doerr, 'Cyber threat intelligence: A product without a process?' *International Journal of Intelligence and CounterIntelligence*, vol. 34, no. 2, pp. 300–315, 2021. DOI: 10.1080/08850607.2020.1780062.

[40] M. Stout and M. Warner, 'Intelligence is as intelligence does,' *Intelligence and National Security*, vol. 33, no. 4, pp. 517–526, 2018. DOI: 10.1080/02684527.2018.1452593. eprint: https://doi.org/10.1080/02684527.2018.1452593. [Online]. Available: https://doi.org/10.1080/02684527.2018.1452593.

[41] International Organization for Standardization, *ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems - Requirements*, Geneva, Switzerland: International Organization for Standardization, 2013.

[42] D. Schlette, F. Böhm, M. Caselli *et al.*, 'Measuring and visualizing cyber threat intelligence quality,' *International Journal of Information Security*, vol. 20, pp. 21–38, 2021. DOI: 10.1007/s10207-020-00490-y. [Online]. Available: https://doi.org/10.1007/s10207-020-00490-y.

Appendix A

Interview Guide

Some respondents may be purveyors or practitioners on behalf of customers, or as part of a public system. Questions will be adapted accordingly. Further, the questions below are not exclusive nor exhaustive, but meant to be used as a guide for what major areas should be covered.

Introduction Present the overall aim of thesis and the research questions. Explain anonymity measures, sign Information Letter (consent).

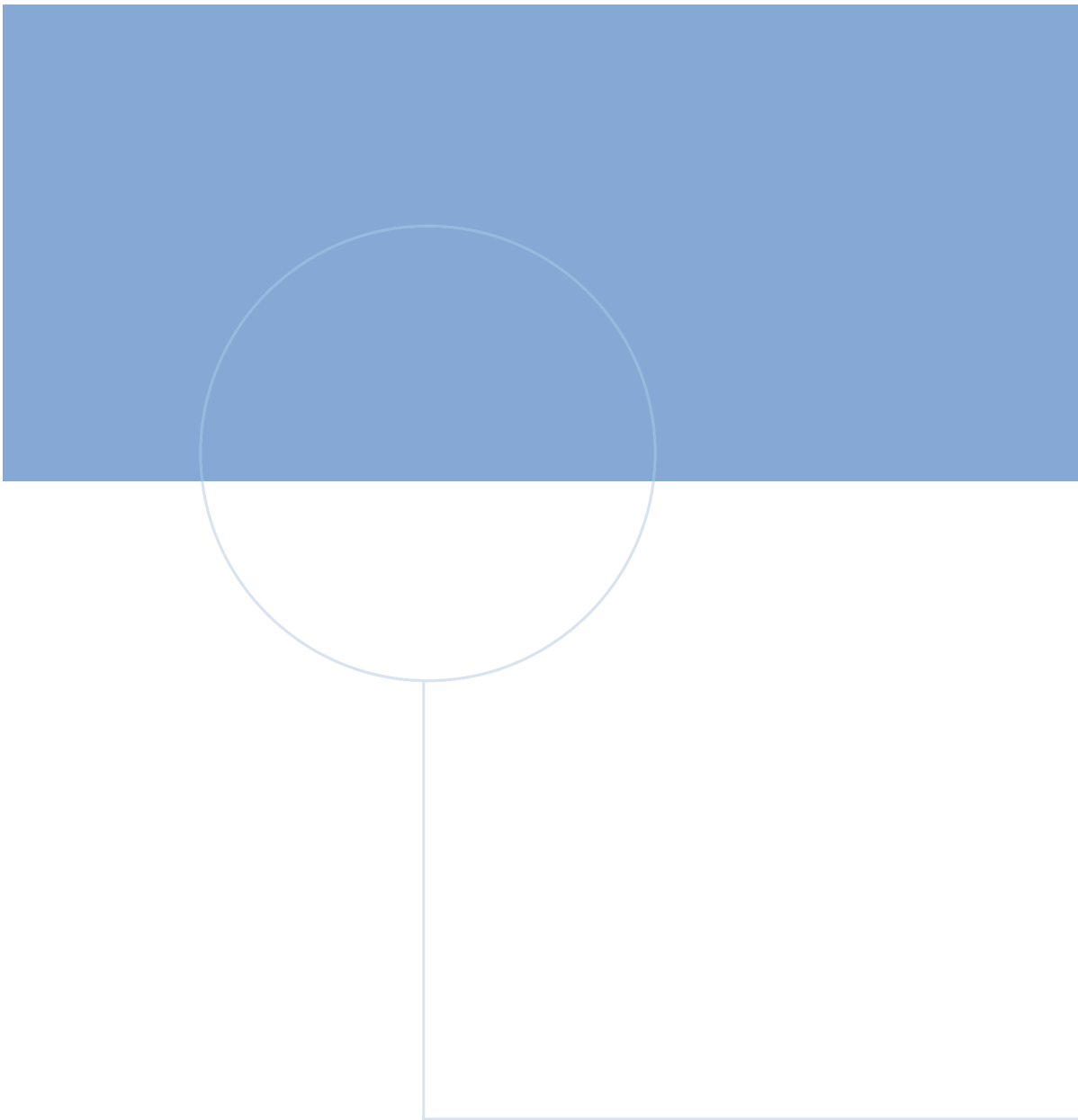
Part 1: Context The first part establishes context on the Interview Object (IO) and the Organization's CTI and Infosec approach.

1. The IO's experience in the field
    a. Years/positions as a cyber security professional and CTI practitioner
    b. Years/positions with *other* roles than cyber security
2. The IO's current position and role within
    a. Infosec in the organization, broadly
    b. CTI specifically
3. Describe your current responsibilities
4. The Organization
    a. Sector
    b. Approximate size and budget
    c. Partnerships - Is the organization part of a larger system?

Part 2: CTI Platform and Effectiveness This part of the interview explores the actual research questions

1. What CTI platform is used? Commercial? Bespoke?
2. How long has the organization used CTI?
3. What parts of the organization receives information derived through CTI?

4. Do other stakeholders and decision makers outside of the InfoSec unit receive information from CTI? How is that information disseminated?
5. Do you perceive an overall benefit from using CTI? Why or why not?
    a. Is this perception shared in the organization?
6. Since adopting CTI, how has the overall Infosec situation evolved?
    a. Can the change be substantiated, and if so, how?
7. Have your organization stopped, mitigated, or disrupted attacks based on CTI information?
    a. What type of threats to your organization are captured by CTI?
    b. What facet or type of information has contributed to this outcome?
8. Does your organization change security posture based on CTI information?
    a. What does that entail?
    b. What facet or type of information has contributed to this outcome?
    c. Who makes that decision?



NTNU

Norwegian University of
Science and Technology