Master's thesis

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

Tiril Ligaya Tinde

Cyber Threat Information Requirements for Strategic Decision-Making

Master's thesis in Information Security
Supervisor: Dr. Benjamin J. Knox
June 2022

NTNU
Kunnskap for en bedre verden

Tiril Ligaya Tinde

Cyber Threat Information Requirements for Strategic Decision-Making

Master's thesis in Information Security
Supervisor: Dr. Benjamin J. Knox
June 2022

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

NTNU

Kunnskap for en bedre verden

Acknowledgments

First and foremost, I would like to thank my main group of supervisors, Dr. Benjamin J. Knox, Dr. Ricardo G. Lugo, and Torvald F. Ask, for their invaluable advice and continuous encouragement during this MSc thesis project. They provided a perfect blend of knowledge and humor. I truly enjoyed taking part in the Advancing Cyber Defence by Improved Communication of Recognized Cyber Threat Situations (ACDICOM) project. I also thank Stefan Sütterlin and Torbjørn Kveberg for their mentorship during this project.
I am grateful to the research participants who so generously took time out of their schedules to contribute to this research project.
A special thank you to Hilde Bakke from the Faculty of Information Technology and Electrical Engineering at NTNU for answering my numerous phone calls and emails. Your guidance helped me navigate this master's degree program smoothly.
Lastly, the biggest thank you to my front-row people for their immeasurable support. I am forever grateful to you.

Abstract

A cyber threat situation involves high-stakes decision-making that relies on human communication where technical complexity and time sensitivity make communication in cyber threat situations challenging. Consequently, there is a need to establish the information requirements of strategic decision makers to improve the quality of cyber threat communication. This master's thesis aims to provide an overview of the information needed to make informed strategic decisions and non-technical considerations in a cyber threat situation. Moreover, the research project examines appropriate communication methods and information sharing frequencies in a cyber threat situation.

Cyber threat information requirements were investigated through exploratory research. A mixed-methods research design was used to establish the information requirements of strategic decision makers. A systematic literature review was carried out to determine the information needed to make strategic decisions and non-technical considerations based on existing literature. A questionnaire (n=43) and semi-structured interviews (n=3) were conducted to determine the information requirements according to decision makers and technical specialists from the public and private sectors. Collected data from the literature review, questionnaire, and interviews were compared using triangulation to enhance the credibility and validity of the research findings.

The findings indicate that information about organizational assets and the estimated impact of the cyber threat is crucial to a strategic decision maker. Furthermore, implemented and required measures to handle the situation are relevant. Information concerning the cyber threat actor's motivation and objectives also helps support decisions; technical information, such as indicators of compromise, is far less relevant. The findings suggest that cyber threat communication involving a strategic decision maker should be concise and formal, such as an executive summary. The findings also point at the strategic decision maker's preferences being the deciding factor of the most appropriate communication method. The severity of a cyber threat situation and an organization's characteristics affect the information requirements and sharing frequency. By applying a mixed research methodology, this thesis has developed a method for measuring cyber threat communication that has provided a novel and scientific understanding of its implications on strategic decision-making and recommendations for future research.

Sammendrag

I en cybertrusselsituasjon må informasjon utveksles på tvers av disiplinære og organisatoriske grenser for å støtte beslutningstakere på alle nivåer. Denne informasjonsutvekslingen er preget av teknisk kompleksitet og skjer ofte under stort tidspress. Kommunikasjon i cybertrusselssituasjoner er et fagområde som mangler evidensbasert forskning, spesielt dens påvirkning på strategiske beslutningsprosesser. For å bidra til den vitenskapelige forståelsen av kommunikasjon i cybertrusselsituasjoner etablerer denne masteroppgaven informasjonsbehovene til strategiske beslutningstakere i slike situasjoner. I tillegg undersøker oppgaven egnetheten av forskjellige kommunikasjonsmetoder samt hensiktsmessig hyppighet for informasjonsdeling.

Gjennom utforskende forskning og metodetriangulering belyser masteroppgaven problemstillingen. Forskningsdesignet besto av en systematisk litteraturstudie, en spørreundersøkelse (n=43) og semistrukturerte intervjuer (n=3). Forskningsutvalget besto av beslutningstakere og tekniske spesialister fra offentlig og privat sektor som har erfaring med cybertrusler. Forskningsresultatene tilsier at informasjon om organisasjonens verdier og den antatte effekten av cybertrusselen er svært viktig for en strategisk beslutningstaker. Videre er en strategisk beslutningstaker interessert i informasjon om de iverksatte samt nødvendige tiltakene for å håndtere situasjonen. Informasjon om cybertrusselsaktørens motivasjon og mål bidrar også til å støtte strategiske beslutninger. Teknisk informasjon, som kompromissindikatorer, er mindre relevant. Informasjonsutveksling i en cybertrusselsituasjon bør være kortfattet og formell, men det er hovedsakelig den strategiske beslutningstakerens preferanser som avgjør hvilke kommunikasjonsmetoder som er best egnet for situasjonen. Til slutt taler forskingen for at hyppigheten av informasjonsdeling er svært situasjons- og kontekstavhengig. Alvorlighetsgraden av situasjonen og organisasjonens forretningsområde påvirker også hvilken type informasjon og hvordan denne informasjonen bør formidles til en strategisk beslutningstaker.

Gjennom en blandet forskningsmetodikk har denne oppgaven utviklet en metode for å utforske kommunikasjon i cybertrusselsituasjoner. Dette har gitt en ny og vitenskapelig forståelse av kommunikasjonens implikasjoner på strategiske beslutninger samt anbefalinger for fremtidig forskning.

Contents

Figures

Tables

Abbreviations

AAR After-Action Review.

ACDICOM Advancing Cyber Defence by Improved Communication of Recognized Cyber Threat Situations.

ACM Association for Computing Machinery.

APTs Advanced Persistent Threats.

ARPANET Advanced Research Projects Agency Network.

CEO Chief Executive Officer.

CIA Confidentiality, Integrity, and Availability.

CISO Chief Information Security Officer.

COAs Courses of Action.

COP Common Operational Picture.

CSA Cyber Situational Awareness.

CSIR Computer Security Incident Response.

CSO Chief Security Officer.

CSV Comma Separated Values.

CTO Chief Technology Officer.

CVE Common Vulnerability Enumeration.

CYDETI Cyber Security Decision Making Informed by Cyber Threat Intelligence.

DoS Denial of Service.

ENISA European Union Agency for Cybersecurity.

FinTech Financial Technology.

GDP Gross Domestic Product.

ICT Information and Communications Technology.

IDS Intrusion Detection System.

IEC International Electrotechnical Commission.

IEEE Institute of Electrical and Electronics Engineers.

IMRaD Introduction, Methods, Results, and Discussion.

IoCs Indicators of Compromise.

IP Internet Protocol.

IPS Intrusion Prevention System.

ISMS Information Security Management System.

ISO International Organization for Standardization.

IT Information Technology.

M Mean.

NAF Norwegian Armed Forces.

NIS Norwegian Intelligence Service.

NIST National Institute of Standards and Technology.

NSD Norwegian Centre for Research Data.

NTNU Norwegian University of Science and Technology.

OSINT Open-Source Intelligence.

PCA Principal Component Analysis.

RQ Research Question.

SA Situational Awareness.

SD Standard Deviation.

SLR Systematic Literature Review.

SOC Security Operations Center.

SP Special Publication.

SSI Semi-Structured Interview.

TTPs Tactics, Techniques, and Procedures.

UiO University of Oslo.

WEF World Economic Forum.

Chapter 1

Introduction

First, the chapter presents the topic covered by the master's thesis and relevant keywords. The research problem and justification, motivation, and benefits of the research project are described next. Lastly, research questions are defined, followed by a description of planned contributions[1].

1.1 Topic covered by the project

Digital technologies are changing how we live, work, and govern; consequently, opportunities and challenges abound. According to World Economic Forum (WEF) [2], the COVID-19 pandemic has expedited automation and digitization, forcing us to adapt to new ways of working and advancing hybrid work as a future work model [3–5]. In 2019, WEF estimated that 60 percent of global GDP would be digitized by 2022 [6]. It is not unlikely that this is an underestimation seeing the recent accelerated digitalization. Digitalization helps make our world fairer and more just by improving connectivity, financial inclusion, and access to public services [7]. However, it also threatens privacy, erodes security, and fuels inequality [7]. For instance, a digital workplace extends an organization's attack surface to its employees' homes. Whether public or private, the organization becomes a target of cyber threats and part of a complex cyber threat landscape. In its latest threat landscape report, the European Union Agency for Cybersecurity (ENISA) stated that the cyber threat landscape has grown in sophistication, complexity, and impact through 2020 and 2021 [8]. ENISA recognizes that the COVID-19 pandemic has had a notable impact on the cyber threat landscape, seeing a rise in cyber attacks targeting organizations through their employees' home offices [8].

Furthermore, McAfee estimates that, between 2018 and 2020, the cost of global cybercrime reached over $1 trillion [9]. Cyber threat actors actively targeted the healthcare industry, academia, and governments during this period [10]. According to ENISA, cyber threat actors are increasingly motivated by financial

[1] Several sections in the *Introduction* chapter are extracted or adapted from the thesis research project proposal approved by NTNU in February 2022 [1].

gain [8]. In addition to economic consequences, cyber threats have political and social impacts. Digitalization enables online covert influence operations. These operations are closely related to information warfare and can sway decision-making processes by spreading disinformation. Consequences related to national security arise when cyber threat actors, such as state-sponsored actors, target critical infrastructures or conduct cyber warfare. These circumstances may cause social disruption to people's everyday life and potentially undermine their trust in central institutions and national authorities [11, 12]. Cyber threats can also induce individual psychological distress, such as anxiety, stress, or loss of confidence in technology [12].

In line with the United Nations in [7], we – governments, businesses, and individuals – have a responsibility for how we govern and handle digital technologies and transformation. The rapid technological advancement of cyberspace strengthens the need to gain a scientific understanding of the organization's and the individual's limitations in cyber threat situations [13]. This master's thesis examines cyber threat communication to support strategic leaders in their decision-making processes to take part in this responsibility.

1.2 Keywords

Cyber threat communication, cyber threat situation, cyber situational awareness, strategic communication.

1.3 Problem description

Considering the rise in cyber threats and their complexity [8], it is not unlikely that, at one point in time, most organizations will need to make high-stakes decisions regarding cyber-related issues. These issues often require that the organization as a whole is involved, from a technical specialist hands-on with technology to an executive-level decision maker required to make strategic decisions and non-technical considerations. A cyber threat situation implies high-stakes decision-making that relies on human communication. Human communication involves technical complexity, time sensitivity, and interdisciplinary factors, among other things [14]. Considering the vast amount of data flowing between information systems and the time it takes to process and analyze it, a decision maker can experience both a lack and an overload of information in a cyber threat situation. Human communication in a cyber threat situation is challenging and seriously impacts decision-making processes.

With most organizations being targeted by cyber threats [8], it is imperative to ensure efficient communication in a cyber threat situation. Communication is one of the critical aspects of supporting decision-making processes. In private and public sector organizations, decision makers need to have situational awareness to make informed decisions and non-technical considerations [15]. To establish

situational awareness, decision makers need to acquire an accurate perception and understanding of the cyber threat situation. In addition, they need to project future events to support decision processes. While the National Institute of Standards and Technology (NIST) provides cybersecurity standards and guidelines on an organizational level, it does not incorporate the challenges relating to cyber threat communication between individuals or organizations [16]. Furthermore, there is a lack of quantitative and experimental studies on cyber threat communication [14].

This master's thesis will use quantitative and qualitative research methods to identify the information needed to make strategic decisions and non-technical considerations in a cyber threat situation, tackling the *what* to communicate. The thesis will also examine communication methods that are most appropriate in cyber threat situations, addressing the *how* to communicate.

1.4 Justification, motivation, and benefits

As cyber threats are becoming more complex, there is an increasing need to study individuals' limitations regarding communication in cyber threat situations [13]. Identifying the information needed to make strategic decisions in a cyber threat situation can help improve a decision maker's situational awareness and, thus, high-stakes decision-making processes. Identifying this information can also reduce the time and effort spent on unnecessary preparation of content and method of delivery by technical specialists. In today's digital age, an understanding of cyber threat communication can benefit anyone utilizing digital technologies in everyday social, economic, and organizational activities. An improved understanding may reduce user errors and misunderstandings [8].

1.5 Research questions

To address the research problem described in Section 1.3, the master's thesis will answer the following research questions (RQs) in the context of a cyber threat situation:

RQ1 What information is needed to make strategic decisions and non-technical considerations based on literature?

RQ2 What information is needed to make strategic decisions and non-technical considerations according to decision makers and technical specialists?

RQ3 How does the information identified in the literature overlap with the opinions of decision makers and technical specialists?

1.6 Planned contributions

The contribution of this master's thesis will be evidence-based knowledge regarding the information needed to make informed strategic decisions and non-technical considerations in a cyber threat situation. In addition, the thesis will contribute with evidence-based knowledge concerning the communication methods deemed most appropriate to communicate cyber threat information to a strategic decision maker. A systematic literature review (SLR), a questionnaire, and semi-structured interviews (SSIs) will be conducted. The questionnaire will primarily collect quantitative data, and the SLR and SSIs will collect qualitative data. The data source is field experts with several years of experience with cyber threats, providing a decision maker's and a technical specialist's perspective. The results obtained from the three data collection methods will be triangulated to find consistencies or inconsistencies, ultimately forming the evidence-based knowledge.

The thesis is part of a collaboration with the ACDICOM project [13], a research project funded by The Research Council of Norway (project number 302941). ACDICOM intends to provide protocols and standards for the improved exchange of cyber threat information between individuals and organizations facing cyber threats. This contribution will lead to easier and more competent communication between individuals and organizations across industries, hierarchical layers, and professional backgrounds [16].

1.7 Thesis structure

The thesis is structured as follows:

Chapter 2 places the research project in an overall theoretical framework that relates to this master's degree program and contextualizes the project in a larger body of research.

Chapter 3 describes the research methodology and justifies the choices made to create the research design.

Chapter 4 presents the project's results and analysis of these.

Chapter 5 discusses the results in regards to the research questions and puts them into context. Additional findings are also discussed. Finally, the limitations of the research project are discussed.

Chapter 6 answers the research questions, summarizes the conducted research, and most important findings. Suggestions for future research are also presented.

Chapter 2

Background

This chapter places the research project in an overall theoretical framework that relates to this master's degree program and contextualizes the project in a larger body of research. It defines the most important cyber terms, such as cyber threats and cyber threat information. Additionally, the chapter describes cyber situational awareness and decision-making aspects relevant to the research problem[1].

2.1 From information security to cyber resilience

The topic of this master's thesis pertains to NTNU's master's degree program in information security and, specifically, to the program track that focuses on the management aspects of information security. Information security involves securing information technology (IT) services and structures to ensure the confidentiality, integrity, and availability of digital information. Confidentiality, integrity, and availability form the three pillars of information security and are referred to as the CIA triad [17]. Management of information security is the process of protecting an organization's assets from threats and vulnerabilities. This process is often carried out using an information security management system (ISMS). International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001 [18] is a leading information security standard that provides requirements and best practices for an ISMS.

In [19], Sharkov contextualizes information security in today's cyber domain (see Figure 2.1). The author expresses that information security was introduced several decades ago along with cybersecurity and information and communications technology (ICT) security. In fact, cybersecurity, or computer security, was a concept introduced in the 1970s through the Advanced Research Projects Agency Network (ARPANET), known as the first packet-switched network and prototype of the Internet [20, 21]. Computer security became highly relevant when researchers Bob Thomas and Ray Tomlinson created the first worm and antivirus software,

[1] Several sections in the *Background* chapter are extracted or adapted from the thesis research project proposal approved by NTNU in February 2022 [1].

CREEPER and Reaper, respectively, revealing flaws in the packet-switched network. Cybersecurity has evolved into a complex concept between the 1970s and today [2022], introducing new elements, such as Advanced Persistent Threats (APTs) and cyber warfare. Regardless of when information security and cybersecurity were first introduced, we need to recognize that, in this day and age, we are facing unknown, unforeseeable, and unexpected cyber threats that are beyond the aspects of information security. In order to keep up with the ever-evolving cyber domain, an organization needs to prepare for the *known knowns*, *known unknowns*, and *the unknown unknowns*; that is, an organization needs to embody practices from information security, cybersecurity, and cyber resilience. These concepts, the known knowns, known unknowns, and unknown unknowns, have their origins in the Johari window technique [22]. The Johari window was originally designed to illustrate interpersonal awareness, but it applies to many areas, including cyber.

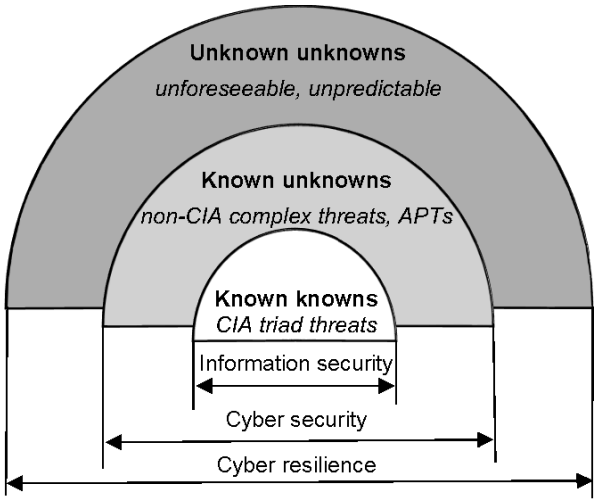


Figure 2.1: Cyber resilience: a holistic approach (Reprinted from [19, Fig. 1]).

Sharkov [19] explains that three aspects characterize cyber resilience:

1. An "[e]ffective protection and [adequately] comprehensive response to threats" [19, p. 5] should be in place. This can be understood as all involved parties, on all levels of management, should properly understand the cyber domain to act effectively and provide an adequately comprehensive response to the current situation. In other words, involved parties should have cyber situational awareness, as described later in this chapter.
2. An organization should maintain business continuity without harmful effects. The author may refer to avoiding shortcuts when securing assets seeing as suboptimal practices may negatively impact business continuity. Furthermore, routines must be in place, and measures must be available to limit or absorb the impact of harmful situations and thereby reduce their harmful

effect. This aspect is closely related to the third level of situational awareness discussed later in Section 2.3. The third level of situational awareness involves a strategic decision maker being able to predict future states and events in the cyber environment, which influences the routines and measures the organization chooses to have in place in case of an unexpected harmful situation

3. In the case of an unexpected harmful situation, an organization is expected to recover back to normal business operations promptly and timely. A holistic approach to cyber resilience, which embodies aspects of information security and cybersecurity, gives organizations a competitive advantage considering they are prepared for the known knowns and the unknown unknowns. Thus, business continuity is more likely to be maintained. Moreover, cyber resilience supports business sustainability and growth [19].

2.2 Cyber terminology

As most cyber terms have different definitions depending on their user and application, in this section, the definitions used in the context of this project are presented. Most definitions stem from NIST's Computer Security Resource Center's glossary[2], which assembles verbatim extractions from NIST cybersecurity final publications.

Cyber relates to information, communications, and computer networks [23].

Cyberspace is a complex and global domain – or environment – that results "from the interaction of people, software and services on the Internet [utilizing] technology devices and networks connected to it" [23, p. 41]. In this project, *cyberspace* is used interchangeably with the terms *cyber domain* and *cyber environment*.

Cyber domain See *Cyberspace*.

Cyber environment See *Cyberspace*.

Cyber attacks aim to disrupt, disable, destroy, or control an organization's information and communications networks, i.e., the organization's use of cyberspace. Cyber attacks may also aim to destroy the integrity of information, or perform unauthorized removal or movement of information, also called data exfiltration [1, 24].

Cyber incidents (or computer incidents) are occurrences that affect the confidentiality, integrity, or availability of information systems and the information residing therein [1, 24]. The difference between cyber incidents and cyber attacks lies in their scale and impact. A cyber incident is minor in scale and

[2]https://csrc.nist.gov/glossary

compromises the concepts of the CIA triad, whereas a cyber attack has a much broader scope and impact. A cyber attack may consist of several cyber incidents, among other things.

Cyber threat refers to any circumstance or event that has the potential to harmfully impact a state, an organization, organizational operations or assets, or individuals through modification, disclosure, or destruction of information, service unavailability, or authorized access to information or information systems [1, 24]. A cyber threat differs from a cyber attack and cyber incident because a threat encompasses the *potential* for harmful impact. In contrast, attacks or incidents are actions that have already taken place and, therefore, are less ambiguous than a threat [1].

Cyber threat actors are states, groups, or individuals who pose a cyber threat. They operate with malicious intent and aim to exploit vulnerabilities in cyberspace to gain unauthorized access to a victim's information system and the information therein [1, 25]. As illustrated in Figure 2.2, cyber threat actors are categorized based on their sophistication and motivation.

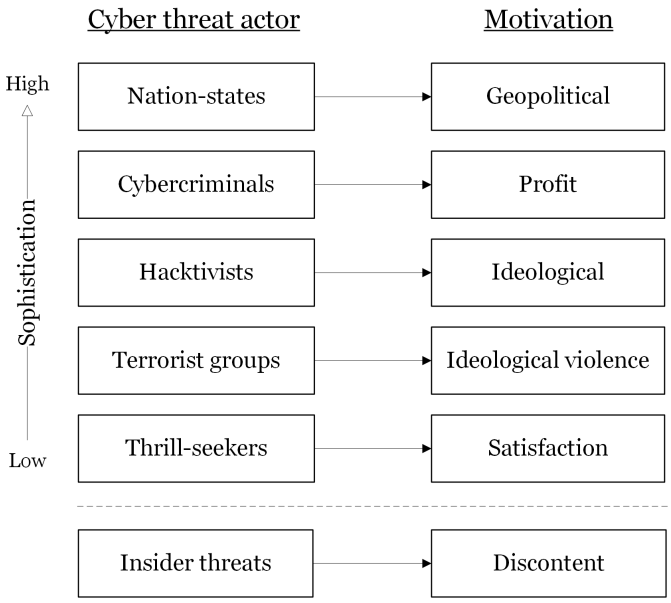


Figure 2.2: Cyber threat actors (Adapted from [25, Fig. 1]).

For example, nation-state actors generally have a geopolitical motivation behind their actions, whereas hacktivists aim to obtain ideological change. Nation-state actors and cybercriminals are among the most sophisticated cyber threat actors considering they have access to many resources and receive ample financial support. Consequently, they can develop, acquire, and employ sophisticated techniques and are often categorized as APTs. However, despite having access to a range of tools and techniques, a sophistic-

ated actor may choose to use less sophisticated techniques to, e.g., correlate their actions with less sophisticated actors, such as thrill-seekers or script kiddies[3].

Insider threats are kept separate from the sophistication scale in Figure 2.2 because their sophistication level varies on their technical background and system privileges in the organization they are associated with. An insider threat is a threat that an individual with authorized access to a system uses this access to harmfully impact an organization, e.g., by disclosing classified information or Denial of Service (DoS). Insider threats are often motivated to act based on discontent toward their organization [1, 25]. However, there is a difference between malicious insider threats and unintentional insider threats. The latter act unintentionally, meaning that the outcome of their actions was not intended to harm or damage the organization's systems. An example of this is human user errors that lead to misconfigured and, thus, vulnerable IT systems. In contrast, malicious insider threats act through deliberate actions that aim to to impact their organization in a harmful manner.

Cyber threat information is any information that assists an organization in identifying, assessing, and responding to cyber threats [27]. Cyber threat information contributes to acquiring cyber situational awareness (see Section 2.4) and can be used to inform decisions on all levels of management. In this project, the term *cyber threat information* also encompasses the terms *cyber threat data* and *cyber threat intelligence* for brevity. The reason is that data, information, and intelligence are often used interchangeably in research and organizations. Generally, cyber threat data refers to unprocessed and raw facts that are machine-readable, such as hash values and registry keys [28]; cyber threat intelligence refers to information that has been processed to provide an appropriate context for decision-making, for example, a report summarizing a cyber threat actor's possible courses of action (COAs) [27].

Cyber threat situation refers to a combination of circumstances or events indicating that an organization is experiencing a (or several) cyber threat(s). At this moment, most organizations are experiencing situations that involve cyber threats. To illustrate, in April 2022, cybersecurity authorities in Australia, Canada, New Zealand, the United Kingdom, and the United States released a joint advisory to warn "organizations that Russia's invasion of Ukraine could expose organizations both within and beyond the region to increased [cyber threats to critical infrastructure]" [29]. In other words, most organizations worldwide are currently facing a heightened cyber threat situation. A cyber threat situation varies in complexity and intensity depending on the level of sophistication of a cyber threat actor and

[3]A script kiddie is an "amateur who tries to illegally gain access to a computer system using programs (scripts) that others have written. Although they may have some programming skill, script kiddies do not have the experience to write their own programs that exploit vulnerabilities" [26].

whether the cyber threat is targeted toward an organization or not. A cyber threat situation differs from situations involving cyber attacks or incidents. The latter require that an organization respond to a specific event or occurrence, e.g., the unavailability of a business-critical service. In those situations, decision-making is often straightforward since the issue is clearly identified. Whereas in a cyber threat situation, nothing conclusive has taken place, making it challenging to identify what decision makers, particularly strategic ones, should be informed of regarding the ongoing cyber threat situation.

2.3 Situational awareness

Before defining Cyber Situational Awareness (CSA), one needs to understand the concept upon which it is built: Situational Awareness (SA), also referred to as Situation Awareness. Endsley provides a widely accepted definition of SA [15]:

> *Situational awareness is "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future"* [15, p. 36].

To make informed decisions in a given situation, it is essential that a decision maker *perceives* the environment, *comprehends* the meaning and significance of the situation, and is able to *project* how the situation may evolve [30]. These concepts, *perception*, *comprehension*, and *projection*, form the three levels of situational awareness (SA) [15]. In [15], Endsley argues that a variety of environments would benefit from acquiring and maintaining SA to support decision-making, mentioning dynamic and complex environments, such as aviation, military operations, and anesthesiology. These environments are characterized by constant state changes, numerous parameters, and time-sensitive settings; in these environments, a minor misconception of the situation may have fatal consequences. Further, attention and working memory are identified as human factors that limit a decision maker from perceiving and understanding a dynamic and complex situation [15]. To overcome these limitations, Endsley presents a mental model of SA in decision-making, illustrated in Figure 2.3. The model consists of three levels: (1) *Perception*, (2) *Comprehension*, and (3) *Projection*.

The first level of SA refers to a decision maker's perception of the elements in the environment. Their perception forms the basis for their SA [15]. If the information obtained at the first level of SA is incorrect, inaccurate, or unreliable, the decision maker forms an incorrect perception of the current state. A flawed perception affects the following levels of SA and, ultimately, the decisions based on this perception [15, 30]. In a study on the sources of SA errors in aviation, Jones and Endsley [30, 31] found that 76.3 percent of errors were caused by an incorrect perception of information, i.e., Level 1 of SA. In contrast, 20.3 percent

were Level 2 errors, and 3.4 percent were Level 3 errors. The study [31] showed that level 1 SA errors in a dynamic flight environment occurred when:

- Relevant information was unavailable,
- Information was difficult to detect, monitor, or distinguish,
- Conveyed information was misperceived, or
- Memory loss occurred.

Several aspects of this study's findings are applicable to other environments, such as the cyber environment. The reason is that decision makers in both environments face large quantities of information, rapid changes in state, and time-sensitive decision processes, among other things. Therefore, a step toward bettering Level 1 SA in a cyber environment is to identify relevant information and appropriately convey this to decision makers.

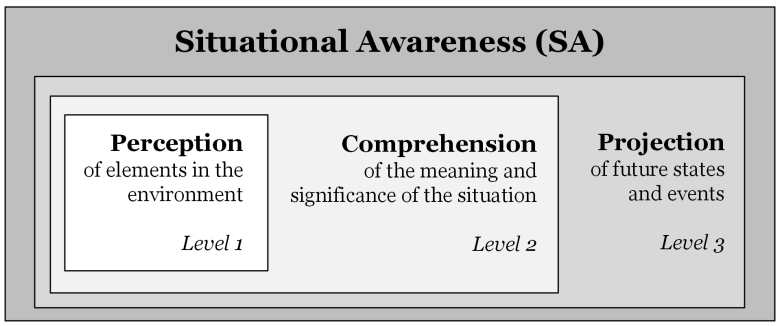


Figure 2.3: Situational Awareness (Adapted from [30, Fig. 1]) and [15, Fig. 1].

Level 2 SA involves comprehending, or understanding, the meaning, and significance of the situation. The comprehension is based on Level 1 elements. A decision maker uses these elements to form a holistic picture of the environment and comprehend the situation's meaning, significance, and involved elements. For example, a strategic decision maker must understand that receiving security warnings from different authorities, including national and private ones, regarding a cyber threat targeted toward their organization indicates something about their current cyber threat situation. In Level 2 SA, an inexperienced decision maker will likely have a different comprehension of the situation than an experienced decision maker [15].

The third level of SA refers to the ability to project future states and events in the environment. Endsley [15] specifies that Level 3 SA is limited to projecting future actions in the near future. Depending on their Level 2 SA, knowledge, and experience, the decision maker from the example above may project that their organization will likely be affected by the cyber threat in question. Based on this projection, the decision maker can decide on the most favorable course of action to ensure business continuity, whether producing an internal notice of the heightened cyber threat situation or establishing a crisis team to monitor the organization's systems more closely than usual.

2.4 Cyber situational awareness

In [30], Husàk et al. build upon Endsley's definition of SA to define CSA:

> *Cyber situational awareness is "the perception of the elements in the **cyber** environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future"* [30, p. 3]

Returning to the concept of CSA, several parallels can be drawn between CSA and SA; however, some specifics of the cyber environment need to be considered [30]. Compared to the environments studied by Endsley in [15], the cyber environment cannot be limited to a physical space, suggesting that the term *space* should be interpreted in light of limitless space. Considering that cyberspace has no borders, a decision maker should focus on the area of cyberspace that is most relevant to their organization to grasp the essence of the situation and avoid information overload.

Next, the perception of elements in the cyber environment differs from the perception of elements in other environments. For example, in a military operation in the physical domain (e.g., on land, at sea, or in the sky), a decision maker uses information obtained from physical observations and sensors to inform their decisions. However, in cyberspace, information derives mainly from sensors. It will rarely be physically possible to observe adversary actions in cyberspace. Data associated with hostile movements in cyberspace must be detected, processed, and analyzed to be human-readable. Only then can the elements, or information, from cyberspace be conveyed to a decision maker. While Level 1 SA in Endsley's model [15] is generally without interpretation or abstraction, Level 1 CSA would necessarily involve some interpretation, e.g., identifying associated cyber threat actors. Moreover, the relationship between the elements in cyberspace must be comprehended at Level 2 CSA [32].

Another specific of the cyber environment is the speed of changes and their impact in cyberspace, which are immensely higher than those of physical environments [32]. For example, an organization can have access to its cloud storage[4] in one moment and the next, a cyber threat actor has gained unauthorized access to the cloud and is denying the organization access until it pays a ransom. A sophisticated cyber threat actor can pose a severe threat to states, organizations, and individuals, using relatively few resources. As an example, Husák et al. [30] state that the launch of a cyber conflict can be scaled down to one single technical specialist with a unique set of skills.

A last specific to consider is the adversary's advantage in cyberspace [30]. A cyber threat actor can hide their affiliation behind their choice of tools, techniques, and technologies, making attribution extremely difficult. Responding to an unattributed cyber threat can be challenging because the organization is ignorant

[4] Cloud storage is a "backup and storage service on the Internet" [33].

of the type of adversary they are facing and hence, the adversary's sophistication level. In this situation, a decision maker must use their CSA to determine the organization's preparedness level. If their CSA is inaccurate, their decisions can have critical repercussions [30]. Other cyber threat actor advantages include the potentially limitless reach and impact of their actions and the wide range of vulnerabilities. Cyber threat actors are not limited to exploiting vulnerabilities in networks, software, and hardware; they can also take advantage of human weaknesses (i.e., social engineering) to achieve their objectives [30].

To summarize this section on CSA, cyber threat information should support a decision maker in acquiring CSA. As a result, the decision maker makes informed decisions based on an accurate Level 1 through Level 3 CSA.

2.5 Levels of management

There are typically three levels of management in an organization: *tactical*, *operational*, and *strategic*. The levels of management are depicted in Figure 2.4 and arranged following the Norwegian Armed Forces' (NAF) command hierarchy ([34, Fig. 1.1]). The sequence in this command hierarchy is commonly used in military and organizational contexts; however, it is not necessarily based on the NAF's figure in [34]. In some cases, the tactical and operational levels swap places; however, this thesis follows the sequence in Figure 2.4. Decision makers on different levels of management have different objectives and hence, distinct information requirements. Next, the characteristics of each management level in the context of a cyber threat situation are described.

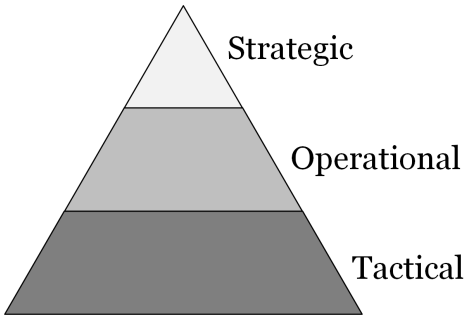


Figure 2.4: Levels of management (Adapted from [35]).

The tactical level focuses on the details of the situation, that is, the *what*. The details consist of IoCs, such as registry keys, timestamps, and hash values. Indicators of Compromise (IoCs) are used to create signatures for Intrusion Detection Systems (IDSs) or Intrusion Prevention Systems (IPSs), triage alerts, and support other responses [35]. Typically, the *what* is based on information from an organization's Security Operations Center (SOC). One could say that the tactical level represents the front line of an organization's cyberspace and its defense.

The operational level addresses the *how* and *where* the cyber threat may impact the organization [1]. On this level, one connects the details obtained from the tactical level with the needs of the broader and comprehensive strategic level. The *how* generally refers to the Tactics, Techniques, and Procedures (TTPs) of the cyber threat actor, that is, the behavior of the cyber threat actor; the *where* refers to determining where the cyber threat is posed in the organization's systems and information therein. Cyber threat analysis reports are usually produced on the operational level of an organization, where analysts employ the details from the tactical level to analyze the cyber threat landscape.

Lastly, the strategic level concerns the *who* and *why* related to the cyber threat situation [35]. The *who* refers to attributing the cyber threat to a cyber threat actor; the *why* refers to uncovering the reasons behind a specific cyber threat. Information that reaches the strategic level is built upon information and analyses from the lower levels of management. Strategic management typically consists of C-level or high-level executives. Information that addresses the *who* and *why* of the situation is used to inform strategic decisions, which include decisions related to business continuity planning, investment, human resources (HR), security requirements, and other long-term objectives.

2.6 Essential skills for strategic decision-making

The previous section on levels of management indicates that high-level executives are primarily concerned with information that supports their decision-making processes relating to the organization's long-term objectives. At the same time, to acquire an accurate CSA, we have learned that there may be a need to obtain other types of information to perceive and understand the cyber threat situation correctly. Considering that this master's thesis aims to identify the information needed to make strategic decisions and non-technical considerations, it will not attempt to define the needed information at this stage of the thesis, that is, before applying a research methodology. Instead, in this section, the six essential skills of a strategic decision maker, according to Schoemaker et al. [36], are described. The six skills are: *anticipate*, *challenge*, *interpret*, *decide*, *align*, and *learn*. The skills identified by Schoemaker et al. are based on research involving over 20,000 executives from various industries. When employed correctly and in conjunction, the skills support decision makers in thinking strategically and navigating the unknown. In the context of this master's thesis, the skills are used to interpret and evaluate the findings that emerge from the project's research. Following, each skill is described and exemplified.

Anticipate refers to being observant of peripheral threats, trends, and opportunities both inside and outside the organization. The ability to anticipate is comparable to Level 3 SA, that is, being able to project future states and events in the environment. To illustrate, Carías et al. [37] found that small and medium-sized enterprises (SMEs) that operationalize cyber resilience are

better equipped to anticipate, respond to, and recover from cyber incidents. As described earlier in the chapter, cyber resilience is a holistic approach to information security and cybersecurity that prepares an organization for the known knowns and the unknown unknowns. For a strategic decision maker to improve their ability to anticipate events in the cyber environment, it can be deducted from [37] that all levels of management in an organization should operationalize cyber resilience. This implies that decision makers on the tactical and operational level should consider both the expected and unexpected and ensure that relevant findings reach top-level management. In addition, high-level executives should proactively seek information that helps them prepare for the unexpected, whether attending conferences or talking to lower-level management [36], to ensure that their perception of the cyber environment is accurate, validating their Level 1 SA. An alternative means to anticipate future events is to develop multiple courses of action (COAs) [36], a technique often used in military operational planning [38]. Developing COAs encourages creative thinking and can help identify challenges and opportunities [38]. COAs are also based upon analysis and understanding of an adversary's most likely and most dangerous COA.

Challenge involves challenging own and others' points of view, reflecting on these, and then taking decisive action based thereon. A way of challenging points of view is to designate a devil's advocate [36]. In [39], Claver examined the applicability of a devil's advocate in cyber-related decisions. Drawing on experiences from the Israeli military in the 1970s and 2000s, Claver identifies lessons that may serve decision makers in today's cyber environment. The author argues that devil's advocacy can help address the imbalance that exists between an overwhelming amount of information and a lack of comprehension. In addition, it can help bridge the gap between the tactical, operational, and strategic levels. By designating a devil's advocate to review inputs, outputs, and processes on all levels of the organization, the devil's advocate can provide alternative analyses relevant to strategic management and act as an informed sparring partner to decision makers facing cyber-related issues. Lastly, challenging own and others' points of view can help stop groupthink, which is a known human decision-making bias [40].

Interpret refers to making sense of the information one is given before making decisions, rather than reflexively acting upon it. Through interpretation, a decision maker can recognize patterns, identify missing or incomplete information, and validate or reject own hypotheses. The ability to interpret, as described by Schoemaker et al. [36], is similar to the characteristics of Level 2 SA. To illustrate, in their comprehensive literature review on CSA [41], Franke and Brynielsson bring up the importance of converting large amounts of data into comprehensible information to help a decision maker acquire a high degree of SA and support decision-making processes. Although they refer to tactical decision support, information interpreted at

the tactical level will eventually reach the strategic level.

Decide involves making decisions informed by a robust and disciplined decision-making process. A decision-making process should balance precision with speed and help decision makers identify trade-offs and opportunities. As cyber threat situations involve many uncertainties, decision makers must rely on available information to inform their decisions. However, Schoemaker et al. [36] stress that a strategic decision maker must have the courage to request multiple approaches to solve the issue at hand and avoid getting prematurely locked into binary thinking (e.g., yes or no, go or no-go). Put differently, to make informed decisions, a decision maker must master balancing the need for more information with uncertainty.

Align implies establishing common ground with the entire organization and its stakeholders. Finding common ground requires communication, trust, and commitment between involved parties. Despite communication being critical to improving organizational alignment, few studies address communication in cyber threat situations, as shown by Ask et al. in [14]. Ask et al. reviewed studies on communication in cyber threat situations and found few studies that addressed the topic; most were correlational and exploratory, meaning that no experiments were conducted. This finding suggests that the ability to align in the context of a cyber threat situation is an unmastered skill. Knowing that cyber threat situations involve high-stakes decision-making in which a decision maker relies on, among other things, human communication to inform their decisions, organizational alignment becomes all the more critical.

Learn refers to promoting organizational learning and identifying the lessons learned from successes and nonsuccesses. In the cyber environment, high-level executives may lack technical understanding [35], strengthening the importance of creating a culture where learning is valued for the employees' sake and the decision maker. Learning culture means that a decision maker can ask questions without feeling judged and receive knowledgeable and reliable answers in return regardless of management level. A concrete way to improve the ability to learn is to conduct after-action reviews (AARs) and broadcast the resulting lessons to the organization [42].

Chapter 3

Methodology

This chapter describes how the research project was designed and justifies the research design choices made to help answer the research problem and questions defined in the Introduction *chapter. The chapter demonstrates an understanding of research design theories relevant to the research project and describes the method selection process. An in-depth description of the applied research design is provided to ensure that the study is reproducible*[1].

3.1 Considering methods

To answer the research questions defined in Section 1.5, there is an overarching methodological challenge to overcome. The challenge is that this master's thesis is conducting research on a topic with almost no established knowledge and methods for measuring and answering the research questions, such as validated theories or questionnaires. This leads to a need to create a new research design with new measurements for cyber threat information requirements. The following subsections address how the research project was designed while considering the quality and validity of the conducted research.

3.1.1 Enhancing credibility and generalizability

When considering research methods, an important aspect is to ensure the project's credibility. Credibility implies that other people agree that the project's design and methods are appropriate for the research problem, obtained results are reasonably accurate and reliable, and stated conclusions and recommendations are plausible [1, 43]. The term *internal validity* is often used when evaluating the credibility of the research. Internal validity is the extent to which the implementation of a research design leads to defensible conclusions [1, 43]. Two strategies that enhance the credibility of a research project are triangulation and respondent validation.

[1] Several sections in the *Methodology* chapter are extracted or adapted from the thesis research project proposal approved by NTNU in February 2022 [1].

Triangulation is a method that involves collecting and comparing multiple kinds of data, where the aim is to find consistencies or inconsistencies among them [1, 43]. In respondent validation, study participants are used to seek validation about conclusions and interpretations a researcher has drawn from collected data.

Another important aspect of research is generalizability. Generalizability involves the application of research findings, i.e., obtained results and drawn conclusions, to a population, for example, to other people, situations, or contexts. Generalizability can also signify that the research findings are applicable or transferable to similar situations or contexts, especially real-world ones. The term *external validity* is often used in this context. Using a representative sample and a real-world setting are two strategies for enhancing the generalizability of a research project. To enhance the credibility and generalizability of this research project, a triangulation method and a representative sample were employed as part of the research design [1, 43].

3.1.2 Quantitative and qualitative research

To answer the research questions, data needed to be collected and analyzed. Data collected in research is categorized as qualitative or quantitative, or both. Quantitative research brings forth numerical information or information that can easily be turned into numbers. Qualitative research yields descriptive and conceptual information that cannot be easily reduced to numbers. Cyber threat communication is a topic that has not been extensively studied. Consequently, involving both quantitative and qualitative aspects in this study is deemed advantageous as these aspects can complement each other. In other words, determining the information needed to make strategic decisions will benefit from qualitative and quantitative data. To draw defensible conclusions, there was a need to collect data from a representative sample and perform statistical analysis to determine which information is the most essential to communicate in a cyber threat situation. Accordingly, this research project used a triangulation of qualitative and quantitative methods, illustrated in Figure 3.1. The largest triangle with a dotted outline illustrates that the methods used in this research project had both quantitative and qualitative dimensions. For example, the questionnaire collected both quantitative and qualitative data.

3.1.3 Choice of methodology

To enhance the quality of this research project, a mixed-methods approach was chosen, i.e., conducting research that includes elements from both quantitative and qualitative research [1, 43]. Furthermore, triangulation ensured that the research findings were representative and reliable. In this project, the triangulation method uses multiple data sources to develop a comprehensive understanding of cyber threat information requirements for strategic decision-making. The first research question was answered through a literature review, and the second was

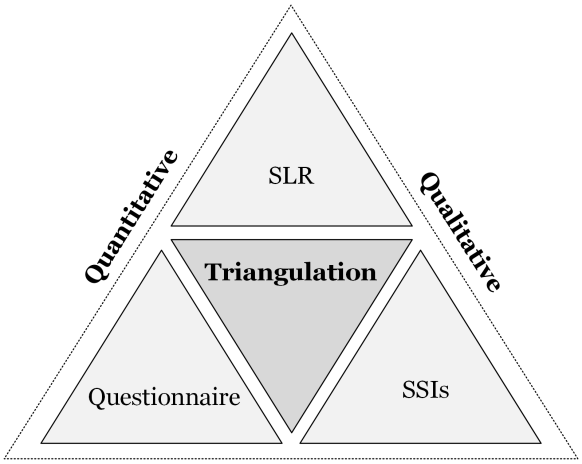


Figure 3.1: Triangulation method (Adapted from [44]).

through expert opinions. Finally, the third research question identified the consistencies and inconsistencies between the literature and expert opinions to produce evidence-based knowledge regarding a strategic decision maker's cyber threat information requirements.

A literature review and survey research were conducted to answer the research questions. The literature review laid the foundation for conducting the survey research and tied the thesis' findings to other theoretical understandings and a larger body of research [1, 43]. Survey research involves asking individuals questions, then analyzing and tabulating their responses to identify general patterns or trends in a population [43]. When conducting survey research, one must keep in mind that obtained results and drawn conclusions merely represent a fleeting moment in time. One would have to repeat the survey research over time to increase generalizability and draw valid conclusions over a more extended period. The survey research design consisted of a questionnaire and semi-structured interviews. The literature review and survey research findings were compared using triangulation to gain further insight. Triangulation helped determine which information is needed to make strategic decisions and non-technical considerations, ultimately addressing the research problem.

To summarize, this master's thesis combines qualitative research's flexibility and exploratory nature with the accuracy, reliability, and objectivity of quantitative research to conduct research in a field that lacks evidence-based knowledge and validated research methods [45].

3.2 Applied research methodology

The research methodology consisted of three parts, as depicted in Figure 3.2. First, a systematic literature review was conducted to answer RQ1 and form the questionnaire and semi-structured interview questions. The literature review also con-

tributed to the *Background* chapter and helped establish a foundation of knowledge on the topic. Second, two survey research techniques were carried out to collect data: a questionnaire and semi-structured interviews. This survey research design contributed to answering RQ2. Finally, the literature review and survey research findings contributed to answering RQ3.

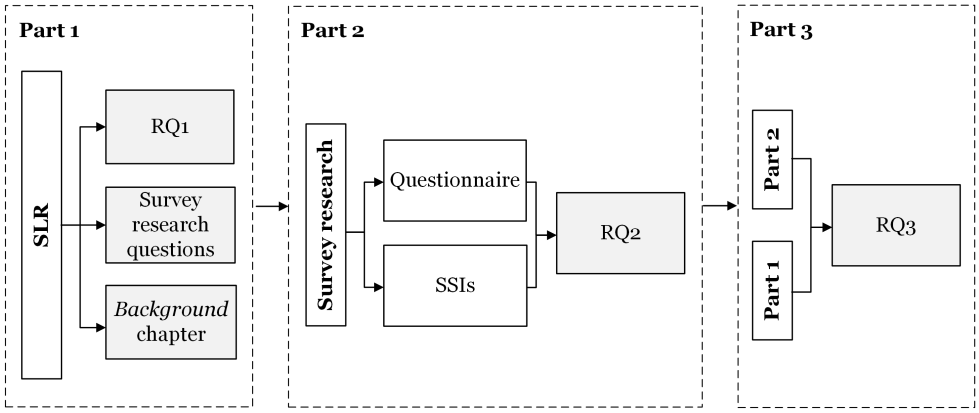


Figure 3.2: Overview of the research methodology (Adapted from [28]).

3.2.1 Literature review

The main purpose of the research project's literature review was to answer RQ1 from a qualitative perspective. A literature review is an assessment of existing knowledge on a specific topic. For this research project, a systematic literature review was carried out in accordance with Jesson et al. in [46]. An SLR follows an explicit and rigorous methodology and is a reproducible research method well-suited to address a specific research question. Jesson et al. describe a review process that consists of the following six phases: (1) *Scoping review*, (2) *Comprehensive review*, (3) *Quality assessment*, (4) *Data extraction*, (5) *Synthesis*, and (6) *Write up*. Due to the novelty and interdisciplinary nature of the field of research within which this project was conducted, a relevance assessment was added to the third phase, (3) *Quality assessment*. It was deemed appropriate to assess a paper's relevance to the research problem and, more specifically, to RQ1 while also assessing its quality. The literature review conducted for this project consisted of the six phases illustrated in Figure 3.3. The following paragraphs describe how each of the six phases was carried out.

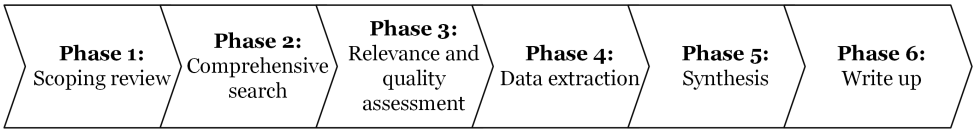


Figure 3.3: Systematic literature review (SLR) process.

Phase 1: Scoping review. In the first phase of the SLR, the aim was to get an overview of the research topic, identify knowledge gaps and discern how much relevant material was available. This phase began during the master thesis' project planning period, in conjunction with the NTNU course "IMT4205 Research Project Planning (Autumn 2021)"[2], where literature related to the thesis topic was identified [1]. During this first phase, keywords and Boolean search strings were identified and applied to databases and search engines to identify relevant types of literature, as shown in Table 3.1. Two search strings were used due to the first search string, "cyber threat information," yielding few to no initial search results, depending on the database and search engine (see Table 3.2). This could be due to a lack of research on this specific topic. The second search string encompasses the same topic as the first string but opens up to a broader range of wordings.

Table 3.1: Scoping review output.

Databases and search engines	ACM Digital Library IEEE Xplore Web of Science ScienceDirect Oria.no Google Scholar
Types of literature	Books/Book chapters Research articles Review papers Surveys Government publications Security reports
Keywords	Cyber threat Communication Cyber threat situation Cyber situation(al) awareness Strategic decision-making Strategic communication Decision-making Decision maker
Boolean search strings	String 1: "cyber threat communication" String 2: "cyber threat" AND "communication" AND "strategic" AND ("decision-making" OR "decision maker" OR "leadership" OR "leader")

[2]https://www.ntnu.edu/studies/courses/IMT4205#tab=omEmnet

Phase 2: Comprehensive search. The comprehensive search was carried out in March 2022 and consisted of searching all identified databases and search engines using the defined keywords and Boolean search strings from Table 3.1. The search strings were applied to the whole body text of publications. This includes, e.g., a paper's title, abstract, and full text. Considering that the scoping review yielded few to no initial search results for String 1, a broad application of the search strings was deemed appropriate to include publications whose title, keywords, or abstract did not include the topic of cyber threat communication. In addition, a search for grey literature was conducted, such as reports from organizations and government publications, by applying the search strings to the search engines Google and DuckDuckGo. Google was used to get personalized search results based on previous searches and interests, and DuckDuckGo for the opposite reason: to get depersonalized search results. The reference lists of highly relevant material were also searched, called a snowballing search [47]. The highly relevant material consisted mainly of papers published through the ACDICOM project. Tables 3.2 and 3.3 present the search results of the comprehensive search.

Table 3.2: Comprehensive search results of String 1.

Database/Search engine	Results
ACM Digital Library	0
IEEE Xplore	0
Web of Science	0
ScienceDirect	0
Oria.no	11
Google Scholar	5

Table 3.3: Comprehensive search results of String 2.

Database/Search engine	Results
ACM Digital Library	26
IEEE Xplore	4
Web of Science	2
ScienceDirect	208[3]
Oria.no	2 591
Google Scholar	7 010

Without limiting the comprehensive search to a specific period, most search results yielded papers published between 2014 and 2022, i.e., the year

[3]The ScienceDirect search was refined to articles published between 2018 and 2022 due to a high number of search results that comprised mostly of articles of no relevance to RQ1.

this research project was conducted. Except for ScienceDirect, the database searches yielded no results for papers published prior to 2014, likely due to a lack of research on cyber threat communication. It may also be that Franke and Brynielsson's systematic review of literature on cyber situational awareness published in 2014 [41], a thorough and highly cited paper, sparked a new focus on cyber threat communication in the research community as communication of cyber-related issues and cyber situational awareness are closely related topics. Due to a high number of search results from Oria.no and Google Scholar that comprised mostly of articles of no relevance to RQ1, search results for String 2 from these search engines were excluded. It was assessed that the search results from four major scientific databases, i.e., ACM Digital Library, IEEE Xplore, Web of Science, and ScienceDirect, would identify the most relevant papers related to the thesis topic. In total, this yielded 256 papers.

Phase 3: Relevance and quality assessment. The third phase involved cataloging and assessing the material from the comprehensive search. The material that came out of the comprehensive search consisted mainly of research articles and conference papers. Microsoft Excel was used to catalog and document the assessment process. The assessment process consisted of reading the title, keywords, abstract, introduction, and conclusion of each paper and rating the relevance of each element. The relevance assessment was an important and necessary step due to the large body of research with no direct relevance to the first research question or the overarching research problem. The relevance assessment helped ensure that included material would contribute to the project's research problem. The papers were evaluated against the following exclusion criteria:

- Papers that do not mention cyber threat information[4].
- Papers that do not mention decision-making or leadership.
- Papers with a technical focus on cyber threats.
- Papers that are written in languages other than English or Norwegian.
- Papers that are unavailable in full text.

The quality of each paper was also assessed by, e.g., verifying that it had been peer-reviewed and followed an IMRaD (Introduction, Methods, Results, and Discussion) structure. Based on this assessment, a paper was either included or excluded. Table 3.4 provides an overview of the checklist used to assess the relevance and quality of studies for this project.
After completing the quality and relevance assessment, 14 papers were included. These papers were taken on in the final three phases of the SLR. Table 4.1 provides an overview of the included publications according to type and research methodology.

[4]Different wordings of "cyber threat information" were not an excluding factor. For example, papers that mentioned "threat information" or "threat intelligence" were included.

Table 3.4: Quality and relevance assessment checklist.

Criteria	Assessment
Peer-reviewed	Yes / No
IMRaD structure	Yes / No
Title relevance	Low / Medium / High
Keywords relevance	Low / Medium / High
Abstract relevance	Low / Medium / High
Introduction relevance	Low / Medium / High
Conclusion relevance	Low / Medium / High
Research problem relevance	Low / Medium / High
RQ1 relevance	Low / Medium / High

Table 3.5: Overview of included material (Adapted from [14]).

	Methodology				
Publication type	Qualitative	Quantitative	Mixed	Other	Total
Conference paper	5	1	2		8
Journal article	1	1	1		3
Report template				1	1
Annual report				1	1
Guideline				1	1
Total	6	2	3	3	14

Phase 4: Data extraction. The full texts of the included material were read, and relevant data were extracted by highlighting and commenting on key aspects. The highlights and comments were helpful for the synthesis and write-up phases of the SLR.

Phase 5: Synthesis. In this phase, the data from each paper were synthesized. This phase helped identify connections between papers. Research gaps related to cyber threat communication were also identified. The identified research gaps helped form the questionnaire and the interview guide for the semi-structured interviews. For example, [27, 48, 49] were publications from the included material that had an influence in forming the questionnaire by providing examples of technical, management, and general information in a cyber threat situation.

Phase 6: Write-up. The final phase consisted of writing up the most relevant findings to this research project. The results helped answer RQ1, which are presented in Section 4.1. The SLR results also contributed to questions items in the questionnaire, the semi-structured interview guide, and the *Background* chapter.

3.2.2 Questionnaire

The questionnaire was designed according to Imperial College London's best practice in questionnaire design [50] and following Farnsworth's six-step process in [51]. The process consisted of the six steps shown in Figure 3.4. Next, a description of each step is provided.

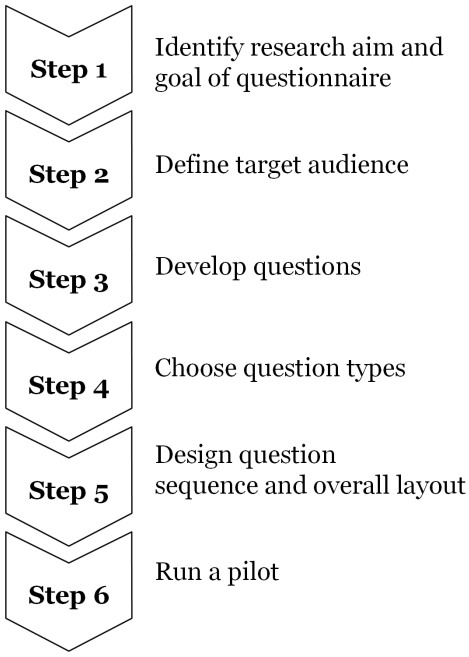


Figure 3.4: The six-step process of designing a questionnaire [51].

Step 1: Identify research aim and goal of questionnaire. In short, the research aimed to determine what information a strategic decision maker needs to make informed decisions and non-technical considerations in a cyber threat situation. The aim is described in more detail in Chapter 1. The questionnaire was a means to reach out to a representative sample and gather standardized information about opinions and preferences. The questionnaire primarily collected quantitative data. By analyzing the quantitative data, the results were used to draw conclusions across the studied population, that is, strategic decision makers. Additionally, due to the research's novelty, the questionnaire was also exploratory, meaning that the questionnaire collected both quantitative and qualitative data.

Step 2: Define target audience. To achieve the goal of the questionnaire, the project needed to collect data from individuals who had hands-on experience with cyber threats. Strategic decision makers in public and private sector organizations were the target audience. Decision makers at all levels, i.e., tactical, operational, and strategic decision makers, and technical experts,

were in the target audience. The reason being that individuals other than strategic decision makers may have important suggestions to what the latter should be informed of in a cyber threat situation. A sample size *n* of 30 questionnaire respondents ($n \geq 30$) was deemed sufficient as there was a limit to how many individuals with hands-on experience with cyber threats the project would be able to reach out to and that are also willing to participate in this study during this research project period. Convenience and snowball sampling were used to recruit research participants. Convenience sampling is a technique used to recruit the most convenient data sources [52], typically individuals in the researcher's professional or social network. To help further distribute the questionnaire, research participants were asked to assist in identifying potential participants, also called snowball sampling. Convenience and snowball sampling were necessary techniques for this project as the target audience was decision makers and technical specialists, which is not a random population. The questionnaire was open for submissions from all countries to increase the odds of reaching out to the target audience. The survey was not restricted to a specific country as cyber-related issues are largely borderless and universal issues. Using convenience and snowball sampling may introduce bias because the project reached out to individuals in a specific professional network, that is, the professional network of the thesis author. In turn, these individuals put the author in contact with their network(s) or forwarded the survey invitation on behalf of the author. The risk of this bias is assessed as acceptable as these individuals are among those who may benefit from the findings of this research project, and their opinions and experiences are highly relevant.

Step 3: Develop questions. The included material from the SLR and knowledge about the topic were used to develop the questions. The questions were developed in English as it is commonly used for technical terms, and the target audience was deemed familiar with using English for professional purposes. The questions' phrasing was kept simple to avoid any misinterpretations. Furthermore, the contents of each question were applicable to each respondent. Some question items were intentionally technical to avoid introducing bias regarding that a strategic decision maker may think that technical information is less important than other types of information. If that were the case, the project would want this opinion to emerge through the questionnaire's results. Additionally, each question was made sure to contribute to the research problem. Lastly, limiting the number of questions and having a specific intention behind each one prevented a time-consuming task for the respondent and questionnaire analysis.

Step 4: Choose question types. Most questions were formulated as closed-ended as the questionnaire intended to collect quantitative data. Most questions used a five-point rating scale, also known as a Likert scale, to evaluate respondents' opinions. The continuum of responses ranged from "not im-

portant" to "extremely important" and from "strongly disagree" to "strongly agree." One question used a four-point rating scale with responses ranging from "not appropriate" to "highly appropriate." The respondent also had the option to answer "no opinion" to each question item. An open-ended question was included at the end of the questionnaire to allow respondents to give answers and comments in their own words. Responding to this open-ended question was voluntary. The questions were formulated only to collect anonymous data, that is, data that cannot identify individuals in the data set or indirectly through background variables [53].

Step 5: Design question sequence and overall layout. In this step, the aim was to improve the overall flow and layout of the questionnaire using the questions formed in the previous step. The more important questions were placed earlier in the questionnaire to increase respondents' likelihood of answering these while focused and energized [50]. These included demographic questions and questions about what information is needed to make strategic decisions and non-technical considerations in a cyber threat situation, ultimately answering RQ1. Less important questions were those less related to RQ1, such as those related to cyber threat information sharing. The questionnaire was consequently divided into three sections:

- Background information
- Cyber threat information
- Cyber threat information sharing

According to Imperial College London in [50], it is best practice to place sensitive items, such as demographic questions, later in a questionnaire as respondents may feel more comfortable sharing sensitive information toward the end. However, this questionnaire's demographic questions were considered marginally sensitive, especially since the questionnaire is anonymous, and placed at the beginning of the questionnaire instead. The demographic questions were essential to the data analysis as these would allow to compare, e.g., the opinions of decision makers and technical specialists. Questions regarding age or gender were not included in the questionnaire. Excluding these aspects allowed the project findings to focus on other aspects of cyber threat communication, such as an individual's current position and years of experience with cyber threats. The questionnaire was developed using Nettskjema[5], NTNU's tool for online questionnaires. Nettskjema is developed and maintained by the University of Oslo (UiO) and recognized by Norwegian Centre for Research Data (NSD).

Step 6: Run a pilot. The questionnaire was reviewed over three rounds by the project's supervisors, who contributed with helpful feedback and suggestions for improvement. One of the supervisors, who would be the target

[5]https://nettskjema.no/

audience if it were not for their direct involvement in the research project, took the survey as a pilot participant. They helped understand their questionnaire experience and suggested widening the scope of the questionnaire by including questions on information sharing preferences. Due to the estimated small sample size, the pilot was run on a limited amount of people to ensure that the sample size would not drastically reduce. The final version of the questionnaire can be found in Appendix A.

After completing the six-step process described above, the questionnaire was ready to be distributed. The target audience was primarily contacted through e-mail, using a standardized survey invitation that called for participation. The invitation was standardized to avoid the time-consuming process of writing personalized e-mails to a large number of potential survey participants. The survey invitation was open for participation from all countries. The standardized invitation also allowed and encouraged recipients of the original invitation to forward it to relevant individuals. The survey invitation can be found in Appendix B.

The questionnaire was run once in conjunction with this master's thesis project during NTNU's spring semester of 2022. The questionnaire was open for submissions between March 28 and April 14, 2022, i.e., about three weeks after the first invitations were sent out.

Since the questionnaire was anonymous, there was no need to apply for permission from the Norwegian Centre for Research Data (NSD) to collect data. Nevertheless, a voluntary data management plan was created using a feature on NSD's website. The management plan described how the research data would be handled from the beginning to the end of this project. Creating the data management plan helped ensure that the data collected through the questionnaire was indeed anonymous.

The quantitative questionnaire data were analyzed using Excel version 2204 and IBM SPSS Statistics version 28.0.1.0. Excel was primarily used to convert the Nettskjema questionnaire data to a CSV (Comma Separated Values) format and perform descriptive analyses. SPSS was mainly used to perform statistical analyses. The qualitative questionnaire data, that is, the responses to the optional open-ended question included at the end of the questionnaire, were analyzed through a thematic analysis of reported comments. Thematic analysis is a systematic approach to analyzing qualitative data that entails identifying themes and interpreting these themes by searching for common patterns [54].

Validity and reliability of the questionnaire

In quantitative research, external validity is the extent to which the research findings can be generalized to other situations or contexts [1, 43]. The questionnaire collected quantitative data concerning cyber threat information and communication. To enhance the external validity of the questionnaire results, responses were collected from a representative target audience sample. Internal validity is the

extent to which the implementation of a research design leads to defensible conclusions. An appropriate statistical analysis of the data was applied, such as descriptive statistics and t-tests, to enhance the project findings' internal validity. To further enhance the validity, the thesis supervisors reviewed the questionnaire design before being distributed.

To evaluate the reliability of the project's quantitative data collection, the internal consistency was calculated by running Cronbach's alpha tests in SPSS. Internal consistency is the most commonly used form of reliability in research [52]. The questionnaire section concerning cyber threat information (see Appendix A, Cyber Threat Information: Part 1 and 2) yielded a Cronbach's alpha value of α=0.94. According to the rule of George and Mallery [55], $\alpha \geq 0.9$ signifies an excellent internal consistency. Nevertheless, a high Cronbach's alpha value, i.e., $\alpha \geq 0.9$, can also signify that some question items are redundant, that is, yielding the same information as other items. However, the risk is assessed as acceptable, and that defensible conclusions regarding the research problem can still be drawn. Further analysis can be done to identify the redundant question items and exclude these before rerunning the questionnaire. The questionnaire section concerning information sharing and communication methods (see Appendix A, Cyber Threat Information Sharing) yielded a Cronbach's alpha value of α=0.7. According to the rule of George and Mallery [55], $\alpha \geq 0.7$ signifies an acceptable internal consistency.

3.2.3 Semi-structured interviews

In this mixed-methods research project, the SSIs were used as an adjunct to supplement and validate the questionnaire results. Brinkmann and Kvale's seven stages of an interview inquiry in were [56] followed to plan and conduct the interviews. The seven stages are depicted in Figure 3.5. Next, the purpose of each stage and the activities carried out in each of these are described.

Stage 1: Thematizing. In this stage, the topic to be researched and the purpose of the interviews were defined, describing the *what* and *why* of conducting the interviews. This is an essential step before deciding on the how, that is, which method(s) to use to fulfill the interviews' purpose. The researched topic was cyber threat information for strategic decision-making. The purpose of conducting the interviews was primarily to validate the questionnaire results while being open to new input and aspects related to the topic from the interview subjects

Stage 2: Designing. This stage involved designing the actual interview and ensuring that the interviews produced the intended knowledge. The ethical implications of the interview were also considered at this stage. SSIs were conducted as these are deemed appropriate when the research question is exploratory, meaning that the research question has not previously been researched in depth [57, 58]. An SSI combines elements of structured and

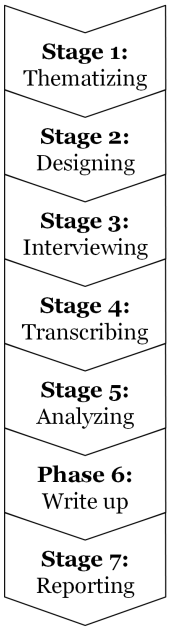


Figure 3.5: Seven stages of an interview inquiry [56].

unstructured interviews, making it flexible in design. A disadvantage of an SSI is that this flexibility in design can lessen its validity. Comparing responses between interviewees can be challenging as the interviews do not follow a fixed order or number of questions. However, for this project, the main purpose of the interviews was not to compare responses between interviewees but rather to validate questionnaire results, so this disadvantage is less relevant. A more relevant disadvantage is the difficulty of developing good SSI questions, as these call for a delicate balance between planning and spontaneity. The project leaned on published research, such as [28] and [59], handbooks, such as [60], and the project's supervisors to design an appropriate interview guide. The interview guide can be found in Appendix C. Once the interview guide was finalized, the NSD was notified of the processing of personal data in the context of this research project. The interview guide and a consent form for the interview subjects were included in the notification form submitted to NSD. The notification form was assessed and approved by NSD about two weeks after submitting it. The personal data included the name of the interview subject, online identifiers (e.g., e-mail address), sound recordings of the interview subject, and background data that can identify them. The personal data was used to facilitate communication with interview subjects and assure the quality of the audio transcriptions. The results and conclusions published in the master's thesis were anonymous, meaning they did not include any identifiable data.
In this stage, potential interview subjects were contacted, and interviews

were scheduled with three interview subjects. The interview subjects were acquaintances of the thesis author. This introduces several types of biases, such as friendliness bias and interviewer bias [61]. However, an advantage of being acquaintances is that common ground and trust likely exist between the interviewer and interviewee, providing a good starting point for an interview. Furthermore, a higher number of interview subjects would have been preferable as this would have improved the generalizability of the results. However, it was considered beneficial to interview three subjects rather than none. The three interview subjects had different backgrounds, which is advantageous to this study. They had different experiences with cyber threat communication and could contribute to different aspects of the topic.

Stage 3: Interviewing. The interviews were conducted in April 2022. They all followed the interview guide designed in the previous stage (see Appendix C). The COVID-19 pandemic has demonstrated that virtual meetings can be just as, if not more so, efficient as in-person meetings in many situations. For this reason, the interviews were conducted online using the video conferencing platform Zoom. Since these interviews were centered around a topic that did not involve disclosing sensitive information, such as personal data or classified information, conducting the interviews online would allow obtaining the intended knowledge. The interviews were recorded through Zoom to verify the quality of the transcription. Using an online video conferencing tool, such as Zoom, was convenient as it allowed the interviews to be recorded easily. In addition, there were no travel costs associated with conducting the interviews. System audio was also recorded as a backup solution if there was an issue with the Zoom recording. Recording the interviews also allowed the interviewer to be more present during the interviews since taking meticulous notes was no longer necessary.

Stage 4: Transcribing. In this stage, the interview material was prepared for analysis [56]. The interviews were transcribed from oral speech to written text using Microsoft Word's *Dictate from audio file* feature. At the time of this research project, the *Dictate from audio file* feature was only available through NTNU's Microsoft Office 365 online version. After an interview was transcribed, the transcription was sent to the corresponding interview subject for approval. Once the interview subject approved the transcription, associated interview recordings were deleted.

Stage 5: Analyzing. This stage aimed to analyze the interview material based on the topic and purpose formulated in Stage 1. Meaning condensation was used to analyze the interview material. Meaning condensation is a mode of interview analysis that focuses on the meaning and involves abridging the meanings expressed by the interview subject into shorter formulations [56]. A mode of interview analysis focused on meaning was chosen rather than language because the project was more concerned with what was said

than the meanings expressed in language. In addition, meaning condensation helped turn longer statements into briefer ones, making it easier to compare the interview material to the questionnaire results. Similar to the questionnaire qualitative data, the SSIs findings were also analyzed through a thematic analysis [54]. Accordingly, the SSIs findings are presented thematically in the *Results and analysis* chapter.

Stage 6: Verifying. This stage involved determining the interview findings' validity, reliability, and generalizability [56]. In the context of interviews, validity refers to "whether an interview study investigates what is intended to be investigated," according to Brinkmann and Kvale in [56, p. 41]. In this research project, the interviews were conducted in line with the purpose formulated in Stage 1, that is, to validate the questionnaire results. Reliability refers to how consistent findings are across the conducted interviews of a study. Since only three interviews were conducted in this research project, verifying how consistent the findings were across these three interviews did not prove to be valuable. Instead, the interview findings were used to verify the reliability of the questionnaire results. Lastly, generalizability refers to whether the findings are transferable to similar situations. The interview findings alone likely have low generalizability. However, using the interview findings to supplement the questionnaire results, the former strengthens the generalizability and reliability of the questionnaire results. The validity and reliability of the SSIs are further discussed in a following subsection.

Stage 7: Reporting. In the final stage of Brinkmann and Kvale's seven stages of an interview inquiry, the interview findings are communicated "in a form that lives up to scientific criteria, takes the ethical aspects [of the study] into consideration and results in a readable product." [56, p. 41]. As for the questionnaire participants, the interview subjects' identity was kept anonymous. Keeping the findings in this research project anonymous was used to encourage involved individuals to be as honest as possible in their answers and reflections. For example, an interview subject should ideally not be affected by what they think their employer expects them to communicate. The interview findings are reported in Chapter 4.

Validity and reliability of the SSIs

The interviews yielded qualitative data, and in qualitative research, ensuring validity and reliability is less straightforward than in quantitative research [62, 63]. In [62], Golafshani states that the quality of qualitative research is related to the generalizability of its results. Generalizability refers to whether the findings are transferable to similar situations. In this study, the interview findings alone likely have low generalizability; however, using the interview findings to supplement the literature review findings and questionnaire results, the former strengthens the generalizability and reliability of the overall research conducted in this mas-

ter's thesis. In addition, the interviews were not the primary data source, meaning that low generalizability is deemed acceptable considering that the interview findings were used as an adjunct to the triangulation method described in Subsection 3.1.3.

Using several data sources to address a research problem is called triangulation [62]. In this master's thesis, triangulation helped identify consistencies and inconsistencies among different data sources; however, triangulation can also lead to a rejection of hypotheses that qualitative research would have highlighted [62]. To ensure the internal validity of the qualitative research, the interviews were planned and conducted according to a recognized method, that is, Brinkmann and Kvale's seven stages of an interview inquiry [56]. In addition, the SSIs' findings were triangulated with findings from the literature review and questionnaire before addressing the research problem and drawing conclusions to ensure the external validity of the research findings.

Reliability refers to how consistent findings are across the conducted interviews of a study [45]. Considering that only three interviews were conducted in this research project, verifying how consistent the findings were across these three interviews did not prove to be valuable. Instead, the interview findings were used to verify the reliability of the questionnaire results.

Chapter 4

Results and analysis

The chapter begins by presenting the findings from the SLR. The SLR was conducted to answer RQ1, identifying the information needed to make strategic decisions and non-technical considerations based on literature. The findings are presented as summaries of the included material, comparing the contents of the different studies and identifying their limitations. The literature review findings are also tabulated to provide an overview of the results. Following, the questionnaire and SSIs results are presented and analyzed. The questionnaire and SSIs were conducted to answer RQ2, identifying the information needed to make strategic decisions and non-technical considerations according to decision makers and technical specialists. The questionnaire was the primary data collection method, and the SSIs were used as an adjunct to supplement and validate the questionnaire results.

4.1 Literature review

This section summarizes and compares the included material from the SLR. Significant findings are highlighted in bold. The findings from the literature review are also tabulated in Subsection 4.1.1.

Lack of research

As expected from initial literature searches and the scoping review, the literature review revealed a lack of material directly related to the project's research problem and, more specifically, RQ1. Nevertheless, a large amount of research material related to cyber threats and cyber information was available through the academic databases and search engines identified in Subsection 3.2.1. This body of research mainly covers how cyber threats and cyber incidents should be communicated, for example, by proposing tools, standards, and frameworks that describe how these can be communicated to decision makers more effectively and efficiently [27, 64, 65]. However, the research repeatedly fails to specify, and sometimes even address, what type of information should be used to support decision-making processes on the different levels of management [64, 66, 67]. Consequently, most of

the research articles and other types of material included in this literature review were not directly linked to the project's research problem or RQ1. By extracting sections from the included material that were either directly or indirectly relevant to the research problem, the project was able to identify information that could contribute to decision-making on a strategic level.

Cyber threat information according to NIST

In NIST Special Publication (SP) 800-150 "Guide to Cyber Threat Information Sharing" [27], Johnson et al. provide guidelines for cyber threat information sharing to support organizations' overall cybersecurity practices. The publication describes the basics of cyber threat information sharing and how to establish and participate in cyber threat information sharing. To describe the basics of this type of information sharing, the authors define several types of cyber threat information, such as the **types of systems being targeted, threat intelligence reports, TTPs, and IoCs** [27, p. iii]. The authors explain that several of these information types are available to or produced by most organizations. It is up to each organization to use the information, in the best possible way, as part of their cybersecurity efforts and to support decision-making on all levels. Through [27], NIST encourages organizations to engage in cyber threat information sharing, both in acquiring external information and sharing internally-produced information, as this enables organizations to expand knowledge and improve overall cybersecurity. In addition to the mentioned examples, Johnson et al. share other information elements that may be relevant to strategic decision-making in a cyber threat situation. These information elements can be found in Table 4.1, which presents the findings of the SLR. Compared to the rest of the material reviewed in the SLR, this NIST publication [27] provided the highest number of examples of cyber threat information.

In line with NIST in [27], [67] was another study that addressed cyber threat information sharing. Alkalabi et al. [67] studied the gap between developed and developing countries when it comes to cyber threat information sharing. Their motivation was that existing literature on cyber threat information sharing predominantly relates to developed countries. A reason for this could be that, in 2021, 85 of the top 100 cybersecurity universities in the world were located in developed countries [68]. These universities likely base the majority of their research on issues related to the country with which they are associated, both for economic reasons and convenience. E.g., data collection may be easier when one is physically and socioculturally closer to the research participants. In addition, if a university receives financial support from the government, this may affect the university's focus areas. Alkalabi et al. performed a case study in Saudi Arabia, i.e., a developing country according to [67], where they aimed to identify the barriers and incentives of cyber threat information sharing. The authors identified socio-cultural barriers and technological incentives as the most important factors. The main focus of the paper was information sharing; however, **attack indicators, TTPs, security**

alerts, threat intelligence reports, and best practices were given as examples of cyber threat information [67, p. 1]. These examples were taken from the NIST publication "Guide to Cyber Threat Information Sharing" [27]. Besides the reference to NIST SP 800-150, the research paper does not address what information cyber threat communication should contain to support decision-making. Rashid et al. [66], much like Alkalabi et al. [67], refer to the cyber information types defined in NIST's "Guide to Cyber Threat Information Sharing" and use these information elements as building blocks to create a model that measures the value created through cybersecurity information sharing. Neither [67] or [66] introduce cyber threat information types that are not mentioned in NIST's "Guide to Cyber Threat Information Sharing," nor do they specify what information types are more important than others to support decision-making in cyber threat situations. This literature review showed a visible pattern of studies published after NIST's "Guide to Cyber Threat Information Sharing" often using the latter as the only reference point to define and give examples of cyber threat information. Undoubtedly, NIST is renowned internationally for providing guidelines and frameworks of high quality and broad applicability. However, as this thesis aims to show, there is a benefit for both academia and industry to challenge the standards that have been set and especially attempt to adapt these to the management level in question.

Acquiring CSA

Despite introducing many cyber threat information types, NIST [27] does not specify what type of information an organization should use to support decision-making on a strategic level. This is where Varga et al. in [69] and [70] contribute with useful findings. In [69], Varga et al. examined the information needed for national-level stakeholders to acquire CSA. Typically, these stakeholders are responsible for making strategic decisions and considerations on a national level. Varga et al. explain that the information elements needed to acquire cyber situational awareness are included in a Common Operational Picture (COP), which the stakeholders use to support their decision-making processes. To explore the information elements needed to acquire CSA, Varga et al. distributed a survey to around twenty government officials and employees in the private sector who operate critical infrastructure. The results showed that it is important to have information about the **external events that led to a crisis, e.g., a heightened cyber threat situation or a cyber attack, and updated information about the internal state of the organization, e.g., the crisis' impact on business operations** [69, p. 777]. The majority of respondents also expressed the need for **a detailed description of events associated with the current situation** [69, p. 777]. This description should only be based on **verified information** [69, p. 777]. Other information elements that the respondents mentioned include **actions that have been carried out or planned for, the organization's information requirements, a communication plan with approved messages, an analysis of the causes and assessment of consequences related to the crisis, and the organ-**

ization's available resources [69, p. 777]. Most respondents thought that the COP provides an appropriate basis for making strategic decisions. To discuss the survey findings, Varga et al. compared the survey results to the seven aspects of cyber situational awareness of Barford et al. [32, pp. 3-4]:

1. "Be aware of the current situation."
2. "Be aware of the impact of the attack."
3. "Be aware of how situations evolve."
4. "Be aware of [adversary] behavior."
5. "Be aware of why and how the current situation is caused."
6. "Be aware of the *quality* (and trustworthiness) of the collected situation awareness information items and the knowledge-intelligence-decisions derived from these information items."
7. "Assess plausible futures of the current situation."

According to Barford et al., the questions "What has happened?" and "Why did it happen?" form the core of CSA [32, p. v]. Further, providing a satisfactory answer to "What should I do?" depends on the CSA of the decision maker [32, p. v]. In other words, a decision maker's CSA capability will determine whether they make informed or uninformed decisions. Varga et al. found that awareness of adversarial behavior was the only one of the seven aspects of CSA that the survey respondents did not mention [69, p. 779]. An explanation of this could be the context in which the data collection was conducted, as it was distributed in the context of a civilian crisis management exercise, which may not typically involve advanced cyber threats. In addition, only a third of the respondents (36 percent) had an IT-related role in their organization. This means that most survey respondents may have lacked an understanding of IT and cybersecurity, therefore, did not find that adversary behavior was worth mentioning. Moreover, in [69], Varga et al. found few significant differences between responses from public and private sector actors. This suggests that public and private sector actors have the same experiences and opinions on the information requirements for national-level cyber situational awareness.

In 2021, two years after publishing [69], Varga et al. published a new study [70] in which they distributed the same survey from [69] to employees in the Swedish financial sector to study this specific sector's CSA. The results from this study were consistent with [69]. Again, around a third of the respondents (15 of 42 respondents) had an IT or cyber-related role in their organization. In addition to the information identified in [69], the following also contributes to CSA: **unverified information (e.g., rumors and unprocessed open-source information), crisis management strategy, list of stakeholders and cooperating organizations, IoCs, and several types of prognoses, i.e., courses of actions (COAs)** [70, pp. 8-9].

Cybersecurity knowledge requirements

Another study that was relevant to this project's research problem was [71]. In [71], Garcia-Granados and Bahsi conducted a literature review and a survey to produce a list of topics that would serve as cybersecurity knowledge requirements for strategic decision makers. In the survey, Chief Technology Officers (CTOs), Chief Security Officers (CSOs), and Chief Information Security Officers (CISOs) were requested to determine what knowledge level a strategic decision maker should have within different topics in order to fulfill their strategic management responsibilities. The list included topics related to **APTs, disaster recovering planning, information security controls, risk assessment, and business continuity planning** [71, p. 6]. Although the authors did not specify what type of information each topic comprised, the topics helped deduce what type of information could be relevant in a cyber threat situation. For example, within the topic of APTs, information related to threat actors would be relevant. The findings in [71] also helped interpret this project's survey results as the survey participants in [71], i.e., decision makers with technical responsibilities, had similar roles to the individuals who participated in this research project. Assuming that CTOs and CISOs have a good technical understanding of cyber-related topics, their opinions and preferences regarding what cybersecurity knowledge they believe is important are likely affected by their level of understanding. This insight brought forth the importance of interpreting this project's results in light of the research participants' technical understanding.

Lessons learned from incident response

Thus far, this section has presented the literature that was most directly related to RQ1, that is, [27, 32, 69–71]. The following publications in this section primarily address cyber threat aspects less related to RQ1. However, to address their research topic, the publications contained insights deemed valuable to the project's research problem, sometimes even RQ1, hence why these publications are included in the literature review. A few of these studies conducted research related to cyber incidents, e.g., Spring and Illari in [65] and Knox's "Cyber Security Incident Report" [48]. As previously mentioned, cyber incidents and cyber threat situations have similarities. In [65], Spring and Illari reviewed computer security incident response (CSIR) standards and practical advice from ISO, Internet Engineering Task Force (IETF), Forum of Incident Response and Security Teams (FIRST), and the US intelligence community, focusing on the aspect of human decision-making in CSIR. Although their research focused on incidents and not cyber threat situations, there were parallels between the situations as they are both complex and composed of several elements. The authors suspected that "the structure of human decision-making is under-represented in available literature" [65, p. 2], which supports the project's observation on the lack of literature related to cyber threat communication, as described at the beginning of this section. Further, the authors experienced "an explosion of scope" [65, p. 2] as an immedi-

ate challenge to the literature review because the topic of incident response and decision-making has a broad application with many subparts. Further, they stated that "academic literature is not the only relevant source [of information about the topic]" [65, p. 2]; practitioners, or experts, are an additional and necessary source of information to capture the latest developments on the topic [65]. This statement supports the methodology choice of this master's thesis seeing as both literature and experts were consulted to address its research problem. Spring and Illari concluded that there is a lack of advice on "what information to report and how to communicate it to convince someone that the investigator [or analyst] should be believed" [65, p. 32]. The paper did not provide suggestions or references to other works regarding what information to report in incident response scenarios. For example, a template for cyber incident reporting, such as Knox's "Cyber Security Incident Report" [48], could have been referred to in [65] to exemplify the information that is important to collect and communicate in case of a cyber incident. Although [48] is yet unpublished (per May 2022), the report template contains several of the fields in Appendix B of NIST SP 800-61 Rev. 2 "Computer Security Incident Handling Guide" [49]. Examples of these fields are **summary of the incident, description of affected resources, and performed response actions** [49, pp. 58-59]. In addition to identifying types of information to answer RQ1, [48] and [49] contributed to the question items in the project's survey research. Inspired by [48] and [49], the questionnaire included question items that related to the **unit or individual responsible for threat management, classification level of the information, an executive summary**, as well as other information elements. Although an executive summary, or management summary, is not a specific type of information, it is known for being a concise summary of key points relevant to its readers, often high-level management. Its purpose is to summarize a longer report, so its reader becomes acquainted with a large body of material without reading the long report entirely. However, if the reader does not have a basic understanding of the topic in question, an executive summary may easily be misinterpreted and not understood at all.

CSA, cyber resilience, and the Johari window

As described in the *Background* chapter, CSA is an area of research relevant to this project. In order to acquire CSA, one relies on information to form a correct perception and comprehension of the current situation and project future states and events associated with the situation. In [19], Sharkov studied cyber resilience, a concept involving CSA aspects. The author presented a holistic approach to cyber resilience as a means to prepare for the unknown, unforeseeable, and unexpected cyber threats, also called *unknown unknowns*. Cyber resilience encompasses information security and cybersecurity practices, which address *known unknowns* (e.g., complex threats, APTs) and *known knowns* (i.e., threats related to the CIA triad). Figure 2.1 from [19] depicts the relationship between cyber resilience, cybersecurity, and information security. National situational awareness is an as-

pect of cyber resilience, and Sharkov argued the need for a holistic view of this. The holistic view of national situational awareness is referred to as the *national cyber picture*. A national cyber picture summarizes the status of cyberspace and ICT systems on a national level. Further, the author recognized the need to establish standardized information exchange protocols to maintain national situational awareness. The protocols should include standardized representations for **incidents, threat actors, and information that relates to these, such as campaigns, threat targets, TTPs, IoCs, observables, and COAs** [19, p. 4]. The national cyber picture is intended for information sharing at a national level, e.g., the national cyber situational center, and to coordinate actions between organizations within a nation. Sharkov explained that cyber resilience results from coordination on all levels of decision-making, that is, tactical, operational, and strategic. Lastly, Sharkov pointed out the importance of contextualizing the national cyber picture to have real value. Real value can be interpreted as having actionable information, that is, information that supports decision-making or problem-solving.

In [64], Aliyu et al. used concepts from the Johari window [22], similar to Sharkov in [19], to describe strategic decision-making in the context of cybersecurity. Aliyu et al. [64] proposed a cybersecurity decision-making informed by cyber threat intelligence (CYDETI) framework. Their motivation for proposing the framework is to address the challenges decision makers face when it comes to understanding the threat landscape in relation to business continuity. The CYDETI framework covers decision-making on all levels, from the technical (or tactical) to the strategic level. Undoubtedly, to support their strategic decision-making processes, executives rely on information. This information comes in the form of actionable intelligence from the operational level, which is based on technical information. In [64], this information includes **assets, attack vectors, threats, threat actors, vulnerabilities, likelihood, and impact** [64, Fig. 1]. Risk assessments, business continuity, and risk management are used to form the actionable intelligence shared with the strategic decision makers [64]. Aliyu et al. did not explicitly specify what information the actionable intelligence should contain.

Another study on CSA is [30], where Husák et al. reviewed CSA research and trends and propose an updated taxonomy of CSA. This research paper has previously been reviewed in the *Background* chapter. Relevant to this chapter is their statement regarding how automation has shifted from a technical specialist having an active role in searching for information to support a decision-making process to decision makers consuming information directly from automated systems and basing their decisions on this information [30]. Depending on how the information is presented and technical specialists' involvement in the process, the decision maker risks misinterpreting the cyber threat information and, consequently, making the wrong decisions. In their updated taxonomy of CSA, Husák et al. include the following information as relevant for strategic perception, i.e., the first level of situational awareness [15]: **asset management, risk management, incident response report, audit findings, policy review, open-source intelligence (OSINT), and cyber threat intelligence (CTI)** [30, Fig. 3]. Failing to perceive inform-

ation relevant to the situation correctly can form an incorrect picture. Moreover, an incorrect perception will further affect the comprehension and projection of the situation, that is, the second and third levels of situational awareness [15].

Technical understanding and decision-making

Kouremetis in [72] brings up the effect of a decision maker's technical understanding on strategic decision-making processes. Kouremetis analyzed Estonia's cybersecurity strategy, policy, and capabilities to assess the country's ability to mitigate and defend itself against threats in the cyber domain. Information about "**threats, trends and solutions**" [72, p. 408] related to these are mentioned as relevant to managing security incidents. The conducted research shows that Estonia's cybersecurity strategy is "coherent, organized and actionable" [72, p. 410]. The author argues that this is partly due to its small, young, and agile leadership force. In 2020, Estonia's population was around 1.3 million [73], making it one of NATO's least populated countries. Small population size may reduce the distance between strategic decision makers, both in the private and public sector, in the country. This, in turn, may streamline communication and decision-making. Also, Kouremetis suggests that a younger leadership force may be more prone to understanding cyber-related information and react quickly to related issues, considering that the technologies involved have been part of their private and professional lives for longer than an older leadership force [72]. These findings could be interesting to investigate in future research, that is, the relationship between informed and agile decision-making and a decision maker's characteristics, such as median age and population size.

Threat intelligence

The last research article included in the literature review was [74]. In [74], Brown et al. discuss the challenges that Threat Intelligence Management Platforms need to overcome to provide value to their end-users, high-level executives being one of them. A Threat Intelligence Management Platform manages cyber threat data and converts it to actionable intelligence (or information) that is delivered to different tools (e.g., machine learning tools that automate data analysis) and stakeholders (e.g., the board of directors of an organization). This management system category was introduced due to the information overload from internal collection and open-source and commercial sources. As discussed in the *Background* chapter, the terms *threat intelligence* and *threat information* are used synonymously in academia and industry. Brown et al. express that threat intelligence needs to be contextualized and adapted to its intended audience, which can also apply to threat information. As an example, Brown et al. state that strategic decision makers are interested in the **threat landscape, historical and predicted cyber trends, and business-related information** [74, p. 48]. Whereas tactical-level personnel, such as incident responders, are primarily interested in technical information, e.g., IoCs and relevant hash values. The authors express that technical information, such as

malware types associated with an attack, may be important to making business security decisions, which typically belong to the operational level of an organization [74, p. 48]. This suggests that, for technical information to be of value for high-level executives, it would need to be communicated through **reports that summarize essential information in a non-technical manner**, often called an executive summary.

In addition to reviewing research articles and cyber threat guidelines, other sources of information were consulted, such as unpublished literature and organizations' reports, to identify what cyber threat information is important to communicate to a strategic decision maker. Some of these have already contributed to the *Introduction* and *Background* chapters. However, to answer RQ1, DNB's threat assessment for 2021 [75] was reviewed as its contents are adapted for individuals that do not have a technical understanding of cyber threats, which may often be the case for high-level executives. DNB is Norway's largest financial services group, and by sharing its yearly threat assessment, DNB aims to spread awareness and better the understanding of cyber threats in the overall population. DNB's report [75] suggests that the following information is important to communicate to a strategic decision maker: **trends, threat actor motivation, threat assessment validity, description of threats for non-technical personnel**.

4.1.1 Results of literature review in tabulated format

Table 4.1 summarizes the findings from the SLR. Each cyber threat information type refers to the material in which it is mentioned. E.g., "Action(s) planned" was mentioned in [69] and [70]. As previously described, the SLR findings informed the development of the questionnaire (see *Methodology* chapter and Appendix A).

Table 4.1: Literature review results.

Category	Type of information
Technical	Action(s) planned [69, 70]
	Action(s) taken [69, 70]
	Affected systems and platforms [27, 48]
	Alert metadata [27]
	Aliases of associated threat actor(s) [27]
	Analysis of related causes [69]
	Associated attack(s) [27]
	Associated campaign(s) [19]
	Associated Common Vulnerability Enumeration (CVE) [27]
	Associated event(s) [70]
	Associated external event(s) [69]
	Associated incident(s) [19]
	Associated threat actor(s) [19, 64, 75]
	Associated threat(s) [48, 64, 72]

	Associated trend(s) [72, 74, 75]
	Attack vector(s) [64]
	Courses of action (COAs) [19, 70]
	Cyber kill chain analysis [48]
	Cyber threat landscape [74]
	Date of cyber threat [48]
	Detailed description of associated events [69]
	Incident response report [30]
	Indicators of compromise (IoCs) [19, 27, 67, 70]
	Individuals and/or organizations targeted by threat [19, 75]
	Information ownership [27]
	Information source(s) [27, 69]
	Malware samples [27]
	Mitigation options [27]
	Motives or intent of associated threat actor(s) [27]
	Observables [19, 27]
	Open-source intelligence (OSINT) [30]
	Recommended COAs [27]
	Response and mitigation strategies [27]
	Security alerts [27, 67]
	Sensor(s) (e.g, antivirus) [27]
	System artifacts [27]
	System(s) and/or information targeted by threat [27]
	System, network and/or application logs [27]
	Tactics, techniques, and procedures (TTPs) [19, 27, 67]
	Targeted vulnerability(ies) [27, 64]
	Threat affiliation(s) [27]
	Threat attribution [27]
	Threat intelligence report [27, 30, 67]
	Tool configurations [27]
	Unit/individual responsible for threat management [48]
Management	Approved messages for external and internal audiences [69, 70]
	Asset management [30, 64]
	Audit findings [30]
	Available internal resources [69]
	Business-related information [74]
	Classification level of information [48]
	Communications plan [69, 70]
	Crisis management [70]
	Information requirements [69]
	Information sharing policy [70]
	Internal state of the organization [69]
	List of cooperating organizations [70]
	List of stakeholders [70]

	Needs from technical personnel [75]
	Policy review [27, 30]
	Regulatory or legal requirements [27]
	Risk management [30]
	Risk tolerance [27]
	Sharing designations, e.g., the Traffic Light Protocol (TLP) [27]
	Status of national cyberspace [19]
	Status of national ICT systems [19]
General	Assessments of consequences [69]
	Best practices [27, 67]
	Brief overview [27]
	Estimated impact [27, 64]
	Executive summary [19, 27, 48, 74]
	Likelihood [64]
	Predicted consequences [70]
	Recommended measures [75]
	Severity rating [27]
	Standardized representations [19]
	Unverified information [70]
	Verified information [69, 70]

4.2 Questionnaire

This section presents the results from the questionnaire. Obtained data were primarily quantitative and are presented through tables and graphs. Qualitative data are presented through thematic summaries.

4.2.1 Questionnaire demographics

In total, 43 individuals participated in the survey. The majority of participants were based in Norway (86 percent), and (60.5 percent) worked in the public sector. Participants worked in different industries, the most common ones being military and defense (32.6 percent), IT (16.2 percent), and education (14 percent). Among the 43 participants, 14 (39.4 percent) were technical specialists and tactical decision makers, 9 (20.9 percent) were operational decision makers, and 9 were strategic decision makers. Other participants (n=8) included professors, advisors, and researchers. All participants stated that they had experience with cyber threats, and nearly half of the participants (46.5 percent) had over ten years of experience with cyber threats. Table 4.2 provides an overview of the questionnaire demographics.

Table 4.2: Overview of questionnaire demographics (Adapted from [28]).

Variable		Frequency	Percentage
Sector	Public	26	60.5%
	Private	16	37.2%
	Rather not say	1	2.3%
	Total	43	100%
Industry	Military and defense	14	32.6%
	IT	7	16.2%
	Education	6	14.0%
	Professional services	5	11.6%
	Finance and insurance	4	9.3%
	Telecommunications	3	7.0%
	Transport and logistics	2	4.7%
	Maritime	1	2.3%
	Rather not say	1	2.3%
	Total	43	100%
Country	Norway	37	86.0%
	Switzerland	2	4.7%
	Israel	1	2.3%
	Lithuania	1	2.3%
	United States	1	2.3%
	Rather not say	1	2.3%
	Total	43	100%
Current position	Technical specialist	17	39.6%
	Strategic decision maker	9	20.9%
	Operational decision maker	9	20.9%
	Other	8	18.6%
	Total	43	100%
Experience with cyber threats	0-3 years (Entry-level)	4	9.3%
	3-5 years (Intermediate)	11	25.6%
	6-9 years (Mid-level)	8	18.6%
	10 years (Senior/executive-level)	20	46.5%
	Total	43	100%

4.2.2 Cyber threat information

Participants were asked to rate the degree of importance of 65 types of information (see Appendix A). A 5-point Likert scale was used to rate the degree of importance: (5) *Extremely important*, (4) *Very important*, (3) *Important*, (2) *Less important*, (1) *Not important*, and (0) *No opinion*. Descriptive statistics were used to calculate the mean (M), also called the arithmetic average, to obtain the degree of importance of each information type. In addition, analyses were run to

compare the results of different groups. The groups that were compared included participants working in different sectors, i.e., public and private sector, and participants in different positions, i.e., strategic decision makers, operational decision makers, and technical specialists. The group of technical specialists included tactical decision makers. The analyses mainly showed consistencies among the different groups. The only notable inconsistency was the importance of informing a strategic decision maker about whether a threat is targeted or untargeted. Operational decision makers found this information more important than strategic decision makers and technical specialists. Other groups' responses were not compared due to the suboptimal sample size for running analyses. Considering that there were few inconsistencies among the groups, the results of the entire population sample (n=43) were analyzed as a whole, and conclusions were drawn based thereon.

According to literature review findings and knowledge of the topic, the types of information in the questionnaire were relevant to different levels of management in a cyber threat situation. It is expected that technical information is less important than non-technical information to a strategic decision maker. However, technical information, such as IoCs and CVEs, were not excluded from the questionnaire to avoid introducing this bias to the questionnaire. That being said, the questionnaire results indicate that technical information is less relevant for a strategic decision maker in a cyber threat situation (see Tables 4.6 and 4.5).

Table 4.3 presents the information that questionnaire participants think is *very important* to communicate to a strategic decision maker in a cyber threat situation, that is, the information types with a mean greater than or equal to 4.00 (M $\geq$ 4.00). According to questionnaire participants, it is very important to: share an executive summary with the strategic decision maker; notify them whether outside parties must be informed (e.g., national security authorities); and present suggested measures that require strategic commitment (e.g., costly cybersecurity investments).

Table 4.3: Very important information (M $\geq$ 4.00).

Type of information	M	SD[1]
Executive summary	4.35	1.19
Whether outside parties must be informed	4.26	1.07
Suggested measures	4.21	0.94
Risk assessment	4.19	1.03
Estimated impact	4.12	1.10
Brief overview	4.09	1.17
Whether threat is targeted or untargeted	4.07	1.03

[1]Standard deviation

An executive summary obtaining the highest degree of importance indicates that a strategic decision maker is less concerned about the details of the situation but more in need of the broader picture and information that directly relates to their area of responsibility. It can be argued that an executive summary is not a specific type of information. However, this result speaks of the level of detail that a strategic decision maker is, or rather, is not concerned with. The other information types in Table 4.3, such as risk assessment and estimated impact, also contribute to a general picture and assessment of the situation. In essence, a strategic decision maker is more concerned with being presented with information that directly supports their decision-making process or information that requires their commitment or support instead of receiving information that concerns the details of the cyber threat(s) the organization is facing. Considering that C-level executives are responsible for entire subject areas within an organization, if not the whole organization, they likely have a limited amount of time and attention to dedicate to the different subject areas. Unless the organization is experiencing a major cyber attack, this may imply that the C-level executives will have other subject areas to tend to. Lower-level management needs to prioritize what information they present to the organization's strategic decision makers. Table 4.3 can be used as a starting point to determine what a strategic decision maker thinks is most important to be informed of in a cyber threat situation.

Table 4.4 provides an overview of the information that questionnaire participants think is *important* to communicate to a strategic decision maker, that is, information types with a mean greater than or equal to 3.00 and less than 4.00 ($3.00 \leq M < 4.00$). This information includes the affected assets, the status of systems and platforms, and a timeline of the current threat situation. The former two information types are related to the organization's information security, whereas a timeline of the current threat situation concerns the ongoing threat situation. The latter indicates that participants think the timeline of the current threat situation can be used to support strategic decision-making processes.

Table 4.4: Important information ($3.00 \leq M < 4.00$).

Type of information	M	SD
Affected assets	3.98	1.20
Status of assets	3.95	1.27
Status of systems and platforms	3.93	1.28
Affected systems and platforms	3.91	1.15
Timeline of current threat situation	3.91	0.92
Motivation or objective of threat actor	3.88	1.00
Targeted assets	3.79	1.15
Targeted systems and platforms	3.79	1.17
Whether outside parties should be informed	3.77	1.09
Mitigation options	3.77	1.13
Requirements and needs of underlying units	3.70	1.08

Whether threat is targeting specific organizations or sectors	3.67	1.04
Length of time a threat is still considered valid	3.67	1.04
Implemented measures	3.67	0.97
Associated threat(s)	3.63	0.98
Sophistication level of threat actor	3.60	1.00
Vulnerability assessment	3.60	1.14
Information reliability	3.60	1.05
(Types of) individuals or organizations targeted by threat	3.53	1.05
Severity rating	3.49	1.10
Rules governing the use or sharing of threat information	3.49	1.32
Date or time a threat was identified	3.47	1.24
Associated attack(s)	3.47	1.08
Information source reliability	3.47	1.10
Associated incident(s)	3.37	1.00
Internal classification level of information	3.33	1.25
Associated trend(s)	3.28	0.93
Unit or function responsible for threat management	3.23	1.21
External/national classification level of information	3.23	1.43
Associated threat actor(s)	3.21	1.04
Information quality assessment	3.19	1.07
Planned measures	3.14	0.91
Involved third-party service provider(s)	3.14	1.17
General description of threats	3.09	1.21
General description of threat actors	3.09	0.97
Processed information based on internal data sources	3.05	0.90
Threat information suitable for sharing with outside parties	3.00	0.85

Table 4.5 provides an overview of the information that is *less important* to communicate to a strategic decision maker, according to the research participants. These information types have a mean greater than or equal to 2.00 and less than 3.00 ($2.00 \leq M < 3.00$) and are likely to have a lower value in a strategic decision-making process.

Table 4.5: Less important information ($2.00 \leq M < 3.00$).

Type of information	M	SD
Description of past threat situation(s)	2.91	0.89
Breaking news	2.86	1.34
Processed open-source information	2.84	0.81
Threat attribution	2.79	1.42
TTPs commonly used by threat actor	2.72	1.24
Timeline of past threat situation(s)	2.67	0.87
Groups or actors associated with an IoC	2.65	0.97
Unit from which the threat information originates	2.56	1.03

Automated or manual actions on target	2.56	1.30
Detailed description	2.28	0.98
Associated IoC(s)	2.28	1.20
Aliases of associated threat actor	2.23	1.11
Threat information source	2.19	0.82
Cyber kill chain-based analysis	2.12	1.00
Data flow visualization	2.12	0.98
Associated CVEs	2.09	1.39
Security alerts	2.05	1.07
Network visualization	2.05	0.95
Individual from which threat information originates	2.02	1.14

Finally, information that is *not important* to communicate to a strategic decision maker in a cyber threat situation is provided in Table 4.6. Tables 4.5 and 4.6 show that information types with a degree of importance (or mean) less than 2.00 are primarily technical in nature. These types of information are likely more relevant to lower-level management, such as operational decision makers and technical specialists. Furthermore, questionnaire participants think that information regarding the individual from which the threat information originates is not important or less important to communicate to a strategic decision maker. Network visualizations also received a low degree of importance (M=2.05), suggesting that the organization can refrain from presenting network visualizations in briefings or reports to top-level management. This result may also suggest that visualizations commonly shown to strategic decision makers need to be more appropriate to the situation and their receiver for these to have real value to decision-making processes.

Table 4.6: Not important information (M < 2.00).

Type of information	M	SD
Unprocessed open-source information	1.67	0.75
Tool configurations	1.65	0.84

4.2.3 Communication methods

In addition to identifying the information that is important to communicate to a strategic decision maker, the questionnaire addressed *how* cyber threat information should be communicated to the decision maker. Accordingly, participants were asked to rate the degree of appropriateness of 19 communication methods (see Appendix A). A 4-point Likert scale was used to rate the degree of appropriateness: (4) *Highly appropriate*, (3) *Appropriate*, (2) *Less appropriate*, (1) *Not appropriate*, and (0) *No opinion*.

The results are provided in Table 4.7 and Figure 4.1. Table 4.7 is structured to compare the means of opposite communication methods. For example, a short report obtained a mean of M=3.6, whereas a long report obtained M=2.21. This result indicates that participants think a short report is a more appropriate communication method to inform a strategic decision maker in a cyber threat situation. Furthermore, the results in Table 4.7 show that the following methods are appropriate ($M > 3$) to communicate cyber threat information to a strategic decision maker: short reports, face-to-face and digital meetings, visualizations, oral and written communication, and formal communication. There is a slight preference for face-to-face meetings over digital meetings, but both are deemed appropriate. Other communication channels are deemed less appropriate, such as phone calls or emails. The results show no preference between oral and written communication. However, there is a clear preference for formal communication over informal communication. To summarize, the cyber threat information communicated to a strategic decision maker needs to be concise and formal. This conclusion supports the finding that the most important cyber threat information is an executive summary, which is characterized as being short and formal. The graph in Figure 4.1 ranges the communications methods from most to least appropriate.

Table 4.7: Communication methods.

Communication method		M	SD
Report	Short report	3.60	0.49
	Long report	2.21	0.67
Meeting	Face-to-face meeting	3.56	0.55
	Digital meeting	3.30	0.77
Visuals	Visualizations	3.40	0.76
	Presentation with multiple slides	2.77	0.92
	One slide presentation	2.72	1.10
Mode	Oral communication	3.23	1.02
	Written communication	3.23	0.84
Style	Formal communication	3.21	0.83
	Informal communication	2.37	1.02
Channel	Phone call	2.84	0.84
	Email	2.58	0.85
	Instant messaging	2.14	0.86
	Company wiki	1.88	1.05
Length	5-15 minute meeting	2.81	1.24
	15-30 minute meeting	2.74	1.20
	30-60 minute meeting	2.28	1.20
	60 minute meeting	1.53	0.83

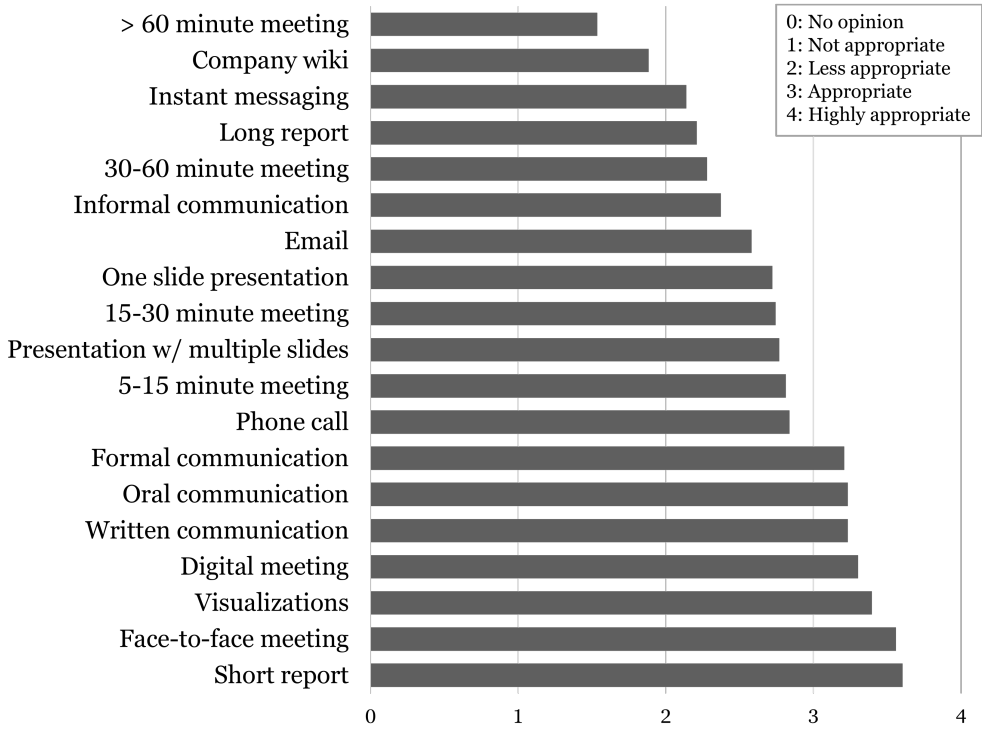


Figure 4.1: Communication methods.

4.2.4 Frequency of information sharing

Participants were asked to state how often they think cyber threat information should be shared with a strategic decision maker, in other words, the frequency of information sharing. Table 4.8 provides an overview of the responses regarding the frequency of information sharing. The question was posed as a multiple answer question, meaning that participants could choose several frequencies. In addition, participants had the option to provide a written answer, which 11 participants did. When asked how often cyber threat information should be shared with a strategic decision maker, *Weekly* (n=19) and *Monthly* (n=21) obtained the highest number of votes. Most responses stated that information should be shared depending on the situation, e.g., in case of a significant cyber threat or an incident. A few participants (n=4) stated that regular information sharing (e.g., weekly, monthly, or quarterly), combined with information sharing depending on the situation, is appropriate. Two participants stated that information should be available on-demand. However, this process would require many resources, both in terms of time and personnel. Further, it may have a low value to decision-making processes if the information is not adapted to its receiver(s).

Table 4.8: Frequency of information sharing (multiple answer question).

Frequency	n	Percentage
Hourly	0	0%
Daily	7	16.3%
Weekly	19	44.2%
Monthly	21	48.8%
Quarterly	9	20.9%
Semi-annually	1	2.3%
Annually	3	7%
Other	11	25.6%

Participants were also asked to determine whether they agreed or disagreed with the following two statements concerning information sharing:

Cyber threat information should be communicated at scheduled times.

——

Cyber threat information should be communicated continuously as it is uncovered.

A 5-point Likert scale was used to rate the degree of appropriateness: (5) *Strongly agree*, (4) *Agree*, (3) *Neutral*, (2) *Disagree*, (1) *Strongly disagree*, and (0) *No opinion*. The results showed a slight preference for communicating cyber threat information at scheduled times (M=4.14) instead of continuously as it is uncovered (M=3.74).

4.2.5 Additional comments from participants

This subsection presents the thematic analysis of the reported comments from the questionnaire, as described in the *Methodology* chapter. Fourteen out of 43 participants (32.6 percent) voluntarily contributed with a comment relevant to the topic addressed in the questionnaire. The option to provide an additional comment was placed at the very end of the questionnaire (see Appendix A) to allow participants to comment on all aspects of the questionnaire.

Situation-dependent. Nine out of 14 participants explicitly stated that cyber threat communication is situation-dependent. Quotations from research participants include: "*depends on the context of the cyber threat situation*", "*More than anything, I think the situation will affect what is "best," or deemed appropriate,*" and "*my answers depend on what context my company is in.*" This indicates that the situational context affects the content and format of the information. Factors that affect the situational context are the severity of the situation, sector, industry, hierarchical layers, internal procedures, organizational culture, and the individuals involved. Further, the severity of the situation triggers the need to inform or involve a strategic decision maker.

The participants' comments suggest that common protocols and standards for cyber threat communication, per ACDICOM's main objective [13, 16], will require a high degree of generalizability to be applicable across sectors, industries, and hierarchical layers.

Timely delivery. A strategic decision maker with over ten years of experience with cyber threats recognized the importance of the timely delivery of cyber threat information: "*What is important is that the strategic information is delivered timely.*" Further, they underlined that the information must be adapted to the level of knowledge of its receiver. Relevant parties should be informed of the receiver's level of knowledge in advance.

Information sharing frequency. Two technical specialists, one with entry-level experience and the other with intermediate experience, stated that information should be shared regularly when the cyber threat situation is less critical: "*There should be [continuous] information [in normal situations].*" When the situation is heightened, information should be shared more frequently or "*increased information [flow] during actual threats or incidents.*" Their comments support the finding in Subsection 4.2.4, that is, that regular information sharing combined with situation-dependent information sharing is appropriate. The technical specialist with entry-level experience specified that oral communication is appropriate if a decision is required at once. However, oral communication should always be documented in a written format to ensure traceability.

Decision-making is a collaborative effort. A strategic decision maker with over ten years of experience with cyber threats stated that strategic decision-making is not a solitary process and that "*it is as much about [their staff] and other advisors preparing decisions and taking [part] in decision-making.*" Most often, strategic decisions are informed by information from advisors. They specified that high-level decision-making should involve a wide range of contextual information regarding the cyber threat situation and the organization's operations: high-level decision-making "*should involve a wide range of contextual information on the threat and on own operations.*" The research participant's comment suggests that contextual information from the staff helps a strategic decision maker identify possibilities for business success while balancing the organization's initiative against the cyber threat(s).

Healthy organizational culture. A senior technical specialist addressed the importance of a healthy organizational culture for cyber threat communication. Critical information must be shared with the decision maker, regardless of whether it is "good news" or "bad news" for the organization, but "*it is equally important not to "blame the intern,*" suggesting that strategic decision makers should encourage honest communication since their decision-making processes rely on a wide range of contextual information. Refraining from sharing "bad news" with a strategic decision maker can affect the

decision maker's situational awareness and, thus the outcome of their decisions. These comments support the ability to align, as described by Schoemaker et al. [36] (see *Background* chapter).

Risk assessments. According to an entry-level operational decision maker, risk assessments are essential in keeping with the development of the cyber threat landscape: "*without risk assessment you will constantly be one step behind.*" Risk assessments involve identifying the organization's assets, vulnerabilities, and threats, among other things. This process and its output should help organizations balance their efforts in a cyber threat situation.

Save time and resources on custom formats. An operational decision maker with intermediate experience with cyber threats expressed that security incidents should be presented in the same format as other information related to the organization's operations: "*[security incidents] should be presented the same way as other [severe] operational issues.*" For example, suppose the C-level executives are presented with a monthly summary of the organization's areas of operation and business support. In that case, events that pertain to the cyber domain should follow the same format and frequency as other areas of operations within the organization. As described earlier, security incidents and cyber threats have similarities. The advantage of communicating cyber threat information in the same format and frequency as other information is that less time is spent developing and maintaining specific processes and tools for cyber threat information sharing.

4.3 Semi-structured interviews

This section presents the SSIs results. The SSIs yielded qualitative data that were analyzed using meaning condensation and thematic analysis, as described in the Methodology *chapter. The aim of the interviews was primarily to validate the questionnaire results.*

4.3.1 Demographics of interview subjects

The interviews were conducted in April 2022 and followed the interview guide in Appendix C. In total, three individuals were interviewed. The subjects were interviewed individually to establish a connection between interviewee and interviewer and help focus on one interview subject at a time. Norwegian was the preferred language, and accordingly, the interviews were conducted in Norwegian. Consequently, the interview findings have been translated from Norwegian to English to be presented in this thesis. There is a risk of translation errors, such as expressed statements having multiple meanings or language nuances being lost; however, the risk of translation errors is assessed as acceptable because the interview subjects' statements showed few ambiguities. The interviews lasted between

30 and 45 minutes each. The interview process is described in more detail in Subsection 3.2.3.

The first interview subject, referred to as Subject 1 (S1) in this thesis, was a strategic advisor from the IT industry with 3-5 years of experience with cyber threats. The second interview subject, referred to as Subject 2 (S2), was an operational decision maker in the financial technology (FinTech) industry with 6-9 years of experience with cyber threats. The final interview subject, referred to as Subject 3 (S3), was a senior strategic advisor working in the logistics industry. Table 4.9 provides an overview of the interview demographics.

Table 4.9: Demographics of interview subjects.

#[2]	Current position	Experience with cyber threats	Industry
1	Strategic advisor	3-5 years (Intermediate)	IT
2	Operational decision maker	6-9 years (Mid-level)	FinTech
3	Strategic advisor	10 years (Senior/executive-level)	Logistics

4.3.2 Findings from the interviews

The interviews were analyzed using meaning condensation. As described in the *Methodology* chapter, meaning condensation involves abridging the meanings expressed by the interview subject into shorter formulations [56]. Meaning condensation helped identify the essence of the subjects' answers and reflections and recurring themes between the three interviews. The interview findings are organized by theme.

Cyber threat information. To make informed decisions and non-technical considerations, the interview subjects expressed that a strategic decision maker relies on the following information: knowing the organization's assets, especially its most valuable assets, i.e., those that may need added protection, and estimated impact and consequences if the assets are compromised, e.g., if valuable data is stolen; a general description of the cyber threat situation, cyber threat, cyber threat actor; an assessment of the reasons for being targeted, e.g., the threat actor is interested in stealing classified information; implemented and available measures; and an action plan in case the cyber threat materializes.

All interview subjects stated that, in most cases, technical details are not relevant to the strategic decision makers (e.g., S2 stated that "*most of the technical details should be left out*"), particularly not relevant to the CEO and other C-level executives that are not responsible for security. S2 expressed that the technical details may be important to communicate to the CISO, the C-level executive responsible for the organization's information security management. According to S2, the CISO should have knowledge about

[2] In order interviewed.

the cyber threat actor's TTPs, how it operates from reconnaissance to actions on objectives, i.e., the stages of Lockheed Martin's Cyber Kill Chain[3], identified signatures and patterns relating to attacks that have been carried out against other organizations, to name a few examples. The CISO can use these technical details to establish situational awareness of their area of responsibility. However, a prerequisite for sharing technical information with the CISO is that they have a good technical understanding of the cyber domain.

Further, S1 placed cyber threat information in the context of the organization working as a whole, stating that cyber threat information involves all levels of management working together to understand the cyber threat situation, depending on which level the information is intended for. S1 also brought up the importance of having situational awareness to make informed decisions. They expressed that context establishment is the first step of acquiring situational awareness, implying that the decision maker should have a general understanding of the cyber threat situation.

Situation and context-dependent. A recurring theme of the three interviews was that the content and form of the communication are highly dependent on the cyber threat situation and the organizational context. To illustrate, S1 stated that "*[cyber threat communication] will vary greatly from case to case.*" The situation is affected by the severity of the cyber threat and the sophistication of the cyber threat actor, among other factors. The context is constituted by the organization's characteristics, e.g., industry and size. For example, suppose the organization relies on digital infrastructure to maintain its business operations, such as a cloud service provider. In that case, the organization may interpret the cyber threat as more severe than an organization that relies on elements from the physical domain, such as a restaurant. The three interview subjects expressed that strategic decision makers need to be oriented if the organization faces a heightened cyber threat situation. The orientation should address the broader picture of the situation and inform decision makers of the measures that have been implemented or can be implemented if the situation should evolve. According to the interview subjects, the situations in which top-level management must be informed or involved should be agreed upon in advance. If lower-level management assesses the threat as low or moderate, there may not be a need to involve top-level management.

Information sharing frequency. The interview subjects made it clear that the information sharing frequency should be agreed upon in advance. This is advantageous to the receiver and communicator because both parties will be prepared to receive or give information relating to the issue. S2 highlighted the importance of being mentally prepared to receive information.

[3]https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Suppose information is shared ad hoc or at irregular intervals. In that case, the strategic decision maker's attention may be absorbed in other business areas and not in a mental state of receiving new information concerning a complex topic.

According to the interview subjects, most organizations have established routines for information sharing. Information concerning the cyber threat landscape will be communicated to the strategic decision makers at fixed times. Generally, cybersecurity is addressed in conjunction with the organization's semi-annual or annual business review.

S2 thinks it should suffice to orient the C-level executives every six months if the threat is low or moderate. However, if the situation is heightened, executives should be oriented weekly or monthly, depending on the severity of the situation. In contrast, S3 answered that a weekly or monthly update of the cyber threat situation is more appropriate on a tactical and operational level. This answer suggests that strategic decision maker should be informed if the situation is particularly heightened, e.g., if the cyber threat materializes. In a moderate cyber threat situation, the strategic decision makers should be informed less frequently than monthly, possibly only semi-annually, during the business review.

Communication methods. According to the interview subjects, cyber threat information is typically delivered by personnel from the security department. Security personnel must ensure that the information is conveyed in an understandable manner to its receiver. The information should be put into the context of the organization's objectives. Additionally, technical jargon should be avoided. Nonetheless, S3 articulated that their experience is that security personnel are usually well-equipped to convey information in a clear and concise manner to top-level executives.

According to S1, oral communication is the most appropriate communication method because it allows the receiver to ask questions, which is advantageous if the receiver lacks knowledge of the topic. In addition, S1 expressed that using an example related to the physical domain makes it easier for a non-technical individual to understand concepts and elements in the cyber domain. For example, to explain the Log4j vulnerability[4] to somebody without a technical understanding, one could compare the vulnerability to being the same as giving their house key to a random stranger without being aware of it [77]. Further, S1 stated that information should pass through several hierarchical layers before reaching the C-level executives. This process helps distill the information down to its essence; however, the distillation can also lead to unintended negative consequences, such as unintentionally leaving out critical information.

Similar to S1, S2 expressed that a short and face-to-face meeting, preferably

[4]Log4j is a Java-based open-source logging library. The Log4j vulnerability came to light in December 2021 and allowed an adversary to load arbitrary Java code and take control over computers and systems [76, 77].

15-30 minutes, is the most appropriate way to communicate cyber threat information. The communicator should use a one-slide presentation with distilled information about the cyber threat situation to convey the information. This type of meeting makes it easier to know if the information is understood correctly. S2 also mentioned that a short report might be appropriate. However, they articulated that written reports make it challenging to know if the decision maker has interpreted the information accurately, hence why S2 expressed that oral communication is most appropriate.
In contrast to S1 and S2, S3 mentioned written communication as the most appropriate communication method and, more specifically, short reports (i.e., 1-3 pages) with condensed information about the organization's current cyber threat situation. This type of report is a useful supplement to business review meetings since a strategic decision maker can read the report before attending the meeting and, consequently, show up well prepared.

Similarities between public and private sectors. As described in Section 4.2, the questionnaire results mainly showed consistencies between participants' responses from the public and private sectors. The interview subjects were asked to comment on this finding. All three interview subjects concluded that cyber threat situations are essentially experienced the same way, regardless of whether the organization belongs to the public or private sector. An explanation of this is that most organizations use similar technologies, and cyber threats will therefore be the same. The interview subjects' reflections suggest that the cyber domain is universal and not limited by borders. Consequently, depending on their resources, all actors in the cyber domain, whether malicious or friendly, are subject to the same challenges and opportunities.
Additionally, S2 suggested that questionnaire respondents may have used the same references to cyber threats when responding to the questionnaire, such as email phishing and ransomware, which could lead to similar responses.

Technical specialists and decision makers in sync. As described in Section 4.2, the questionnaire results suggest that technical specialists and decision makers are aligned in cyber threat communication. The interview subjects were asked to comment on this finding. They interpreted the finding as meaning that technical specialists are well-trained in informing strategic decision makers, supporting S3's statement concerning security personnel being well-equipped to convey information clearly and concisely to top-level executives. Besides this reflection, the interview subjects did not provide further insight into this finding.

Personal preferences. Another recurring theme of the interviews was that cyber threat communication is highly dependent on the receiver's preferences: "*it depends on the decision maker*" (S1), "*[it] is evident [that it depends on the*

person] because it is very important to consider the recipient of the information" *(S2)*, and "*it will always be dependent on personal preferences*" (S3). All interview subjects appeared to have been in situations where different decision makers wanted the information communicated in different ways. For example, some decision makers process information more effectively when it is communicated orally, and they have the opportunity to ask questions. In contrast, other decision makers may prefer to read reports and dissect their contents in solitude. The interview subjects expressed that it is essential to know the receiver's preferred communication method to ensure that the conveyed information is received and understood accurately. The knowledge level of the strategic decision maker and their professional and personal interests may also significantly impact their perception of cyber-related issues, which makes it essential to know whom the information is intended for.

Chapter 5

Discussion

In this chapter, the results are discussed and contextualized with the research questions and research problem. Additional findings regarding communication methods and information sharing frequency are also discussed. Finally, the limitations of the research project are discussed.

5.1 Research question 1

In a cyber threat situation, what information is needed to make strategic decisions and non-technical considerations based on literature?

As addressed in Section 4.1, the literature review revealed a lack of material directly related to cyber threat communication on a strategic level, supporting the ACDICOM project's statement that there is a need for scientific understanding of the topic [13]. On the other hand, the lack of literature may suggest that there are valid reasons for not establishing common standards and guidelines for cyber threat communication. To illustrate, NIST does not provide a detailed description of how to implement its cybersecurity framework[1], such as specifying which technologies to use and defining the cybersecurity knowledge requirements of involved parties. NIST leaves these decisions and considerations up to the organization itself. A reason for this may be that implementing cybersecurity is highly dependent on the organization and individuals involved, which may also be the case for cyber threat communication. Nevertheless, a large amount of research material and gray literature relating to cybersecurity, CSA, and decision-making were available through academic databases and search engines. The SLR resulted in a lengthy list of information that may be relevant to a strategic decision maker facing a cyber threat situation. However, with literature as the only data source, determining a strategic decision maker's cyber threat information requirements proved difficult. It was challenging to determine what types of information were

[1] https://www.nist.gov/cyberframework

the most important to communicate to a strategic decision maker, e.g., technical information or general information. Additionally, considering that the different information types identified in the literature were only mentioned between one and four times, it was challenging to determine whether some information types were more important to communicate than others. To illustrate, Table 5.1 presents the information types most frequently mentioned in the literature: those mentioned between three and four times.

Table 5.1: Most mentioned information types in the literature.

Category	Type of information	Frequency[2]
General	Executive summary	4
Technical	IoCs	4
Technical	Associated threat actor(s)	3
Technical	Associated threat(s)	3
Technical	Associated trend(s)	3
Technical	TTPs	3
Technical	Threat intelligence report	3

Except for the executive summary, all the information types are technical in nature, e.g., IoCs and TTPs. Based on own experience with cyber threat communication, strategic decision makers appear to be less concerned with the technical details of a cyber threat situation. Instead, they appear to be more concerned with acquiring a general overview of the situation to help support their decision-making processes. This experience was neither confirmed nor rejected by the SLR findings seeing as the literature included a wide range of information types with no particular order of importance (see Table 4.1). By including additional sources of data to address the research problem, such as questionnaire and interview data, it became more apparent that strategic decision makers are indeed more concerned with a general overview of the cyber threat situation than the technical details.

Technical information appears to be the most important information category to communicate to a strategic decision maker in a cyber threat situation based solely on the literature. The paper of Brown et al. [74] was the only paper from the SLR suggesting that high-level executives are most interested in general information instead of technical information [74]. Brown et al. specified that, for technical information to be of value for strategic decision makers, it would need to be communicated through reports that summarize essential information in a non-technical manner. An executive summary was also mentioned in [19, 27, 48]. These insights did not come through clearly in the rest of the reviewed material. Nonetheless, the literature review produced a comprehensive list of cyber threat information that informed the questionnaire development.

Multiple papers from the included material referred to NIST's examples of cyber threat information in [27]. These examples were taken from either the abstract

[2]Number of mentions in the included material.

or the executive summary of [27], such as "indicators..., TTPs, security alerts, threat intelligence reports, and recommended security tool configurations" [27, p. iii]. Indeed, these are different types of cyber threat information; however, as NIST states in [27], these are only examples of cyber threat information, not a comprehensive list. Additionally, the information types are not sorted by degree of importance depending on whom the information is intended for. It is a concern if academia or industry limit themselves to examples of cyber threat information expressed in a summary or executive summary. The former may draw misguided or erroneous conclusions on cyber threat communication. As a first step to establishing common standards and guidelines for cyber threat communication, researchers and practitioners need to determine the contents of the communication, that is, determining the information requirements of decision makers on all levels of management. Only then should researchers and practitioners turn their attention to how this information should be communicated.

Based on the literature review findings, it is unclear what information is most required to make strategic decisions and non-technical considerations in a cyber threat situation. This is primarily due to a lack of research relating to cyber threat communication on a strategic level. Nevertheless, the information types presented in Table 5.2 suggest that, besides an executive summary, the most important information to communicate in a cyber threat situation is mainly technical information. However, the *Results and analysis* chapter, the questionnaire, and interview findings strongly suggest that the technical information types in Table 5.2 are less important to a strategic decision maker. This is further discussed in the following section.

Table 5.2: Information requirements based on the literature.

Category	Type of information[3]
General	Executive summary
Technical	IoCs
Technical	Associated threat actor(s)
Technical	Associated threat(s)
Technical	Associated trend(s)
Technical	TTPs
Technical	Threat intelligence report

5.2 Research question 2

In a cyber threat situation, what information is needed to make strategic decisions and non-technical considerations according to decision makers and technical specialists?

[3] In order of importance (based on frequency of mentions in the literature).

The questionnaire and interview findings were based on the opinions of decision makers and technical specialists. All of the research participants had experience with cyber threats, and consequently, they can be considered experts in the field. According to the research participants, a strategic decision maker requires information that provides an overview of the cyber threat situation. This information should relate to the organization's assets and business operations. The findings suggest that an executive summary encompasses the most important information requirements of strategic decision makers. This supports the insight provided by Brown et al. in [74]. According to the research participants, the executive summary should include information about the organization's assets, particularly those needing added protection, implemented and required measures, and the estimated impact and potential consequences of the cyber threat. Organizational assets are generally determined through a risk assessment. A risk assessment also identifies the organization's vulnerabilities and threats. Based on the findings, a risk assessment should be used to inform strategic decision-making processes. A few research participants stated that the strategic decision maker does not necessarily carry out the risk assessment themself, but they need to understand its implications. In addition, a strategic decision maker should be aware that cyber threat situations often entail uncertainties and may require a high level of risk acceptance. Lastly, the findings suggest that a strategic decision maker should be informed if outside parties, such as national security authorities, must be informed about the cyber threat situation.

Table 5.3 presents the cyber threat information requirements for strategic decision-making according to the research participants. As shown in Table 5.3, none of the information types are categorized as technical information. Although several of the information types could theoretically be categorized as technical information, the questionnaire and interview results strongly suggest that information intended for a strategic decision maker should address the general perspective of the situation, instead of the technical aspects of the situation. This insight did not come through clearly in the literature. To illustrate, in the studies of Varga et al. in [69, 70], most research participants expressed the need for a detailed description of events associated with the current situation. This finding should naturally be interpreted in light of the studies; however, there appears to be a discrepancy between literature related to cyber threat communication and expert opinions.

The questionnaire and interviews made it clear that *what* information and *how* it should be communicated depends on the cyber threat situation and the organization and individuals involved. This implies that research findings should be interpreted in light of the cyber threat situation at hand and whom the information is intended for. Considering that all research participants had experience with cyber threats, they likely have a good understanding of the cyber domain as a whole and may even have a technical background. Consequently, non-technical individuals may have different opinions on the information requirements than the project's

[4]In order of importance (based on reported comments).

Table 5.3: Information requirements according to research participants.

Category	Type of information[4]
General	Executive summary
Management	Status of assets
Management	Status of business operations
General	Implemented and required measures
General	Estimated impact and potential consequences
Management	Risk assessment
Management	Whether outside parties must be informed

research participants. Actively targeting strategic decision makers without a technical background or experience with cyber threats may yield different results and challenge the conclusions drawn in this thesis. However, being a strategic decision maker in the digital age demands an understanding of their organization's digital dependencies, as shown in [71]. Acquiring CSA, which is a correct perception, understanding, and projection of the cyber environment, and thus, the organization's digital dependencies, makes cyber threat communication more manageable and efficient [13]. An appropriate level of CSA can also support improved decision-making based upon realistic efficacy levels rather than dissonance at the strategic level.

5.3 Research question 3

How does the information identified in the literature overlap with the opinions of decision makers and technical specialists?

Some similarities were identified between the literature and the opinions of decision makers and technical specialists. For instance, all of the information included in the questionnaire was relevant to some degree in a cyber threat situation. The majority of the included information was based on literature, which indicates that the literature and expert opinions are somewhat aligned. However, few consistencies could be identified regarding the degree of importance of the different information types. The literature provided few indications regarding the information requirements for strategic decision-making. The literature searches conducted for the SLR showed that tactical and operational communication and decision-making during a cyber incident had been far more researched than cyber threat communication. This may be because cyber incidents are considered more concrete than cyber threats and, consequently, easier to respond to in a procedural and measurable way. As identified through this research, cyber threat situations require a deeper contextualized cognizance of cyberspace and how it relates to, for example, assets, business operations, and threat actor motivation. Additionally, lower-level management is typically more concerned with the details, which

means that technical information is more relevant to them than to upper-level management.

Furthermore, although cyber threats have been present for several decades, we have seen their sophistication and impact increase considerably over the last few years. It may be that strategic decision makers have not yet needed to make decisions in cyber threat situations. Consequently, research has not focused on cyber threat communication on the strategic level. This strengthens the need for a deeper contextualized cognizance of cyberspace on the strategic level. Strategic decision makers need to understand their organization's digital dependencies to make informed decisions and non-technical considerations in a cyber threat situation.

Another significant research finding was that the questionnaire and interview results point to the importance of considering the situation and context of the cyber threat situation and adapting the communication based thereon. These findings did not come through in the literature. This is likely due to the lack of research on cyber threat communication. Common standards and protocols for cyber threat communication should take into consideration the organization's business area, the severity of the situation, and the technical understanding and level of management of the individuals involved. The findings suggest that establishing cyber threat communication guidelines rather than standards and protocols may be more appropriate. For example, researchers can refer to NIST's guide in [27] for inspiration as to what a guide should include. However, adjustments will have to be made to produce a guide for cyber threat communication on the strategic level, considering that [27] does not explicitly cover this aspect.

Lastly, the findings indicate similarities between the public and private sectors regarding cyber threat communication. The questionnaire results did not show any significant differences between responses from the public and private sectors. According to the interview subjects, the public and private sectors are likely aligned because they experience the same cyber-related issues. This suggests that there may not be a need to limit future research to a particular sector, considering that both sectors experience the same cyber threats and are actors in the same cyber environment. The majority of the studies in the reviewed literature also included cross-sector samples, such as Alkalabi et al. in [67] and Varga et al. in [69]. In [69], Varga et al. found, similar to this research project, few significant differences between the responses of private and public sector actors. However, they did find differences between the actors' responses with different positions, such as regional crisis management actors and service providers. Varga et al. argue that actors in these positions have different focuses and objectives. Rerunning this research project's questionnaire with a larger sample size may lead to similar findings as in [69].

To summarize the three sections addressing RQ1, RQ2, and RQ3, Figure 5.1 provides the key findings of each research method: the SLR, questionnaire, and

SSIs. The SLR was the only research method that suggested that technical information is important to communicate to a strategic decision maker. The questionnaire made it clear that general and management information was more important than technical information. Finally, the key finding of the interviews was that cyber threat communication is highly dependent on the cyber threat situation and organizational context. This finding also came through in the questionnaire, mainly through the open-ended question. Figure 5.1 also shows that the SLR and questionnaire have a similar focus on cyber threat actors, including their objectives and motivation. The research methods identified similarities between the public and private sectors, as discussed earlier. In Figure 5.1, this is illustrated between the SLR and SSIs; however, this also came through the questionnaire findings. In common, the three research methods advance the executive summary as the most important element in strategic decision-making, supporting Brown et al. in [74].

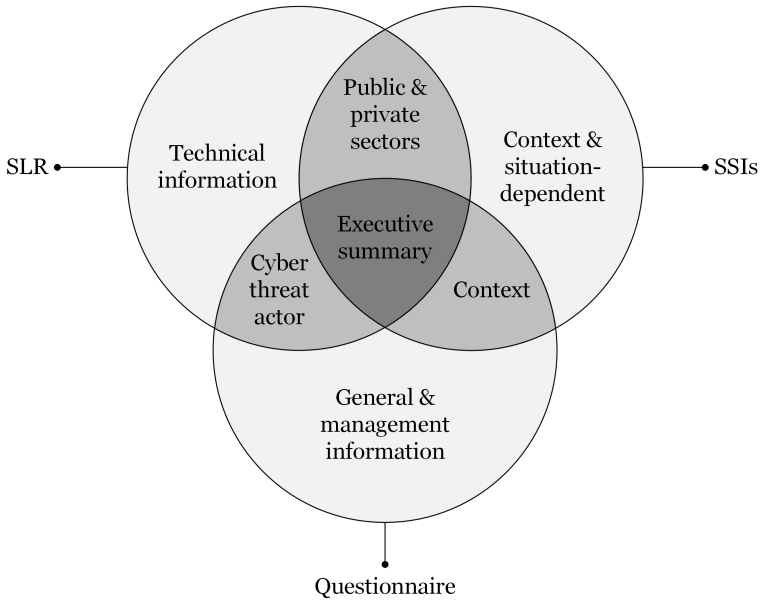


Figure 5.1: The relationships between RQ1, RQ2, and RQ3.

Figure 5.1 illustrates how the three research questions helped answer each other and address the overarching research problem through triangulation. The added value lies in using several research methods, in this case, three, to address a research problem. Furthermore, triangulation enhanced the validity of the research due to the different research methods yielding similar findings. For example, the questionnaire and SSIs suggested that cyber threat communication on the strategic level needs to be adapted to the situation and context.

5.4 Additional findings

In addition to answering the research questions, the research project contributed to findings concerning appropriate methods of communication in a cyber threat situation and the frequency of information sharing. In this section, the most significant findings are presented.

5.4.1 Communication methods

The findings of this research project show that cyber threat communication involving strategic decision makers should be short and formal, such as an executive summary or brief orientation. These findings are based on the opinions of experts in the field who are likely to have a good understanding of cyber-related issues. To further confirm the findings relating to appropriate methods of communication, one would need to repeat the research methodology on a broader sample that includes non-technical strategic decision makers and individuals without experience with cyber threats. Nevertheless, the study of Garcia-Granados and Bahsi in [71] proposes cybersecurity knowledge requirements for strategic decision makers, suggesting that the latter need to improve their cybersecurity knowledge to make informed decisions. In [78], Piccirilli and Tzabbar recommend providing cybersecurity education for top-level executives, supporting [71]. Providing cyber education for strategic decision makers can help ensure that their Level 1 SA is correct, which can positively impact their decision-making processes.

Considering that visualizations came out as the third most appropriate method of communication according to research participants (see Table 4.1), it is deemed appropriate to further research cyber threat communication methods. For example, the research of Kullman et al. in [79] on how visualizations can enhance the efficiency of cybersecurity analysts is relevant to this topic since efficient communication on other levels of management can enhance the quality of information conveyed to strategic decision makers, as the thesis' questionnaire and interview findings suggest.

5.4.2 Frequency of information sharing

There were a few inconsistencies in the results regarding the most appropriate frequency of information sharing. The majority of research participants think that cyber threat information should be shared weekly or monthly and more frequently in a heightened cyber threat situation. However, a few research participants think that strategic decision makers should only be informed if the cyber threat situation is significantly heightened.

There is a consensus about cyber threat communication taking place at scheduled times instead of ad hoc or irregular intervals. Nevertheless, the frequency of informing a strategic decision maker is situation and context-dependent.

5.5 Limitations

In this section, the research project's limitations are discussed. This section aims to reflect on the conducted research and discuss its validity and reliability. The scope of the thesis is discussed first.

5.5.1 Scope

The research in this master's thesis was conducted to identify the information needed to make strategic decisions and non-technical considerations in a cyber threat situation. As an extension of this, the research also addressed how the information should be communicated. Data collection, which included a literature review, a questionnaire, and interviews, was carried out between January and April 2022. The target population comprised decision makers and technical specialists in all sectors and industries worldwide. Convenience and snowball sampling were used to recruit research participants. These sampling methods were deemed appropriate considering that the target audience was limited to decision makers and technical specialists. In total, 43 individuals participated in the study. Participants were primarily based in Norway (86 percent). All participants stated that they had experience with cyber threats, which suggests they have a technical understanding of the cyber domain. The findings of this research can be generalized to similar populations, that is, decision makers and technical specialists with a technical understanding. Without repeating the research methodology with non-technical individuals, the findings may not be generalized to decision makers and technical specialists in all sectors and industries worldwide.

5.5.2 Literature review

The literature review carried out in this research project may have excluded or failed to uncover relevant material. For example, there may be unpublished knowledge because it was produced within organizations for their use only and without any interest in making the knowledge publicly available. There is a possibility that the knowledge in some of the papers included in the SLR has become outdated during this master's thesis project period. Additionally, although an SLR is characterized as yielding objective results, the reviewed material will undoubtedly be affected by its reviewer's bias and level of knowledge on the topic. Lastly, there may be shortcomings in generalizing the SLR findings. For example, if most studies were conducted in the United States, they may not be generalized to the Norwegian context. During the initial literature searches, there was an intention of acquiring literature that provided a broad overview of the topic, meaning studies that were conducted in different parts of the world. The literature review ended up including studies from Estonia [72], Saudi Arabia [67], and the United States [27], to name a few.

5.5.3 Questionnaire

The questionnaire was formed based on the literature review's information types and knowledge of the topic. Although 65 information types may form a comprehensive list, there is a possibility that the questionnaire was missing information types, for example, information relating to different types of tangible and intangible assets, such as reputation and digital infrastructure. By including these information types, the research project may have identified more inconsistencies between the sample groups, e.g., private sector participants are more interested in protecting their organization's reputation. Further, some question items may have been too technical in nature for non-technical individuals to perceive correctly. A strategic decision maker may not have heard about the Cyber Kill Chain, and consequently, they do not know how to rate its degree of importance. The "No opinion" option was included in the questionnaire to address this possible limitation. To yield quantitative data, the questionnaire consisted mainly of close-ended questions. A disadvantage of a close-ended question is that it limits the answer. To help counter this, the same questions from the questionnaire were asked but formulated as open-ended questions in the interviews.

The questionnaire section concerning cyber threat information yielded a high Cronbach's alpha value, implying that it had very high reliability. However, a high Cronbach's alpha value can also signify that some question items are redundant. Further analysis, e.g., performing principal component analysis (PCA) on the data set, can help identify redundant question items and exclude these before redistributing the questionnaire.

The questionnaire collected responses from 43 participants. The sample size is adequate to address the research problem; however, considering that the population extends out to all strategic decision makers in the world, it can be argued that the sample size is small. A revised version of the questionnaire can be distributed to a broader audience to draw further defensible conclusions and enhance validity.

5.5.4 Semi-structured interviews

Due to a small sample (n=3), the interview findings alone have low generalizability, meaning that the results can only be applied to a narrow population. Considering the low generalizability, the collected data and findings were not used as the primary data source to answer the research problem. Instead, the results obtained from the interviews were used as an adjunct to supplement and validate the questionnaire results and literature review findings. However, considering that cyber threats are a universal phenomenon, there is a possibility that the three interview subjects' opinions apply to a broader population. In addition, it could have been appropriate to conduct group interviews, seeing as the topic does not necessarily require confidentiality, and a group dynamic could provide some interesting insights. That being said, including the interview significantly contributed to the project by adding insight and informing how the research questions were

interpreted and answered.

Another possible weakness of the semi-structured interviews is the analysis technique used to interpret the interviews, i.e., meaning condensation. The technique helps turn longer statements into briefer ones, making identifying consistencies and inconsistencies among the three interviews easier. In addition, it helped compare the interview results to the questionnaire results and literature review findings. However, in condensing the statements expressed by the interview subjects, nuances may be lost in the process. Further, considering that the interviews were conducted in Norwegian and translated to English to convey the results in this thesis, nuances may also be lost in translation.

Lastly, by conducting interviews, different types of bias are inevitably introduced. Relevant examples include interviewer bias, similarity bias, and social desirability [61]. The interviews were recorded and transcribed instead of relying on memory and notes taken during the interviews, which may introduce bias and lose nuances.

Chapter 6

Conclusion

The master's thesis aimed to produce evidence-based knowledge regarding the information needed to make informed strategic decisions and non-technical considerations in a cyber threat situation. The evidence-based knowledge was produced based on three research methods: a literature review, a questionnaire, and interviews. The literature review and interviews yielded primarily qualitative data, and the questionnaire yielded quantitative data. Collected data were compared to identify consistencies and inconsistencies among them, using triangulation to enhance the credibility and validity of the research findings.

The research findings indicate that strategic decision makers require the following information to make informed decisions and non-technical considerations in a cyber threat situation:

- Organizational assets,
- Estimated impact and consequences,
- Implemented and required measures, and
- Cyber threat actor motivation and objectives.

An executive summary encompasses the most important information needed to support strategic decision-making. It should include the information stated above and a general and non-technical description of the cyber threat situation. The findings suggest that technical information relating to the cyber threat situation, such as IoCs and TTPs, should remain on the operational and tactical level of the organization as technical information appears to have a low value to a strategic decision-making process.

The research project also examined appropriate methods for cyber threat communication. The research findings suggest that cyber threat information communicated to strategic decision makers needs to be concise and formal. However, after interviewing three experts in the field, it was clear that the most appropriate way to communicate cyber threat information is highly dependent on its receiver, meaning that the decision maker's personal preference is the deciding factor for how cyber threat information should be communicated.

Lastly, the research project explored how often cyber threat information should

be shared with strategic decision makers. The results varied between informing strategic decision makers from weekly to annually. This finding suggests that cyber threat communication is highly situation and context-dependent.

6.1 Future research

This research project produced new evidence-based knowledge regarding cyber threat communication on the strategic level. Nevertheless, the topic is by no means fully explored and requires a further scientific understanding to improve the exchange of cyber threat information between individuals and organizations.

First, it would be useful to revise the project's questionnaire using participants' feedback and perform further analyses on the questionnaire data. For example, performing PCA can identify redundant question items. Excluding the latter will improve the reliability of the result if the questionnaire is redistributed.

Second, distributing the questionnaire to either a broader or narrower audience could lead to interesting findings. By broader, meaning a larger sample size, and narrower, meaning actively targeting non-technical strategic decision makers.

Third, the research project suggests studying cyber threat communication on other management levels, particularly on the operational level, considering that personnel on the operational level are typically responsible for conveying cyber threat information to the top-level executives. Additionally, looking specifically into the role of the CISO or CSO in a cyber threat situation could contribute to a deeper understanding of cyber threat communication.

Bibliography

[1] T. L. Tinde, "'An Evidence-Based Standard for Cyber Threat Communication," [MSc thesis project proposal],' IMT4205 – Research Project Planning (Autumn 2021), NTNU, unpublished paper, 2021.

[2] World Economic Forum (WEF), "*Global Gender Gap Report 2021*". *Weforum.org*, https://www3.weforum.org/docs/WEF_GGGR_2021.pdf, (Accessed on 13/11/2021), 2021.

[3] C. Nabe, "*Impact of COVID-19 on Cybersecurity*". *Deloitte.com*, https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html, (Accessed on 23/11/2021), n.d.

[4] J. Keane and T. Heiser, "*4 Strategies for Building a Hybrid Workplace that Works.*" *HBR.org*, https://hbr.org/2021/07/4-strategies-for-building-a-hybrid-workplace-that-works, (Accessed on 23/11/2021), 2021.

[5] D. Stevens, "*Hybrid Workplace: Designing A Long-Term Strategy For The Future Of Work.*" *Forbes.com*, https://www.forbes.com/sites/cisco-webex/2021/07/29/hybrid-workplace-designing-a-long-term-strategy-for-the-future-of-work/?sh=2133ff7a7fca, (Accessed on 23/11/2021), 2021.

[6] World Economic Forum (WEF), "*Our Shared Digital Future: Responsible Digital Transformation*" *(Board Briefing)*. *Weforum.org*, https://www3.weforum.org/docs/WEF_Responsible_Digital_Transformation.pdf, (Accessed on 13/11/2021), 2019.

[7] United Nations (UN), "*The Impact of Digital Technologies*". *UN.org*, https://www.un.org/sites/un2.un.org/files/un75_new_technologies.pdf, (Accessed on 13/11/2021), 2019.

[8] European Union Agency for Cybersecurity (ENISA), "*ENISA Threat Landscape 2021*". *ENISA.europa.eu*, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021, (Accessed on 23/11/2021), 2021.

[9] McAfee Corp., "*The Hidden Costs of Cybercrime*". *McAfee.com*, https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf, (Accessed on 24/11/2021), 2020.

[10] Cybersecurity and Infrastructure Security Agency (CISA), "*APT Groups Target Healthcare and Essential Services*". *US-CERT.CISA.gov*, https://us-cert.cisa.gov/ncas/alerts/AA20126A, (Accessed on 24/11/2021), 2020.

[11] Norwegian Intelligence Service (NIS), "*Focus 2021*". *Forsvaret.no*, https://www.forsvaret.no/aktuelt-og-presse/publikasjoner/fokus/rapporter/Fokus2021-highres.pdf, (Accessed on 25/11/2021), 2021.

[12] M. Bada and J. Nurse, '"The social and psychological impact of cyberattacks",' in *Emerging Cyber Threats and Cognitive Vulnerabilities*, Academic Press, 2020, pp. 73–92. DOI: https://doi.org/10.1016/B978-0-12-816203-3.00004-6.

[13] S. Sütterlin, B. Knox, S. Katsikas, O. Maennel, H. Bahsi, R. Lugo and K. Helkala, "*Advancing Cyber Defence by Improved Communication of Recognized Cyber Threat Situations (ACDICOM)*". *HIOF.no*, https://www.hiof.no/hvo/vlo/english/research/projects/acdicom/, (Accessed on 24/11/2021), 2021.

[14] T. F. Ask, R. G. Lugo, B. J. Knox and S. Sütterlin, 'Human-Human Communication in Cyber Threat Situations: A Systematic Review,' in *HCI International 2021 - Late Breaking Papers: Cognition, Inclusion, Learning, and Culture*, Cham: Springer International Publishing, 2021, pp. 21–43. DOI: https://doi.org/10.1007/978-3-030-90328-2_2.

[15] M. Endsley, 'Toward a theory of situation awareness in dynamic systems,' *Human Factors: The Journal of the Human Factors and Ergonomics Society*, vol. 37, pp. 32–64, 1995. DOI: 10.1518/001872095779049543.

[16] S. Sütterlin, B. Knox, S. Katsikas, O. Maennel, H. Bahsi, R. Lugo and K. Helkala, '"Advancing Cyber Defence by Improved Communication of Recognized Cyber Threat Situations (ACDICOM) (Researcher Project - SAMRISK)," unpublished.'

[17] J. Cawthra, M. Ekstrom, L. Lusty, J. Sexton, J. Sweetnam and A. Townsend, '"Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events" (SP 1800-25),' NIST, Gaithersburg, Maryland, Tech. Rep., 2020. DOI: https://doi.org/10.6028/NIST.SP.1800-25.

[18] International Organization for Standardization (ISO), *ISO/IEC 27001 — Information Security Management*, https://www.iso.org/isoiec-27001-information-security.html, (Accessed on 05/06/2022), 2013.

[19] G. Sharkov, 'From Cybersecurity to Collaborative Resiliency,' Vienna, Austria: Association for Computing Machinery (ACM), 2016, pp. 3–9. DOI: 10.1145/2994475.2994484.

[20] K. Chadd, "*The History of Cybersecurity.*" *Blog.avast.com*, https://blog.avast.com/history-of-cybersecurity-avast#the-1970s, (Accessed on 05/05/2022), 2020.

[21] D. Murphey, "*A history of information security.*" *IFSECGlobal.com*, https://www.ifsecglobal.com/cyber-security/a-history-of-information-security/, (Accessed on 05/05/2022), 2019.

[22] J. Luft and H. Ingham, 'The Johari Window: A Graphic Model of Interpersonal Awareness,' Proceedings of the Western Training Laboratory in Group Development, 1955.

[23] M. Hogan and E. Newton, 'Supplemental Information for the Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity (NISTIR 8074, Vol. 2),' 2015. DOI: 10.6028/nist.ir.8074v2.

[24] Joint Task Force Transformation Initiative (JTFTI), '"Guide for Conducting Risk Assessments" (SP 800-30, Rev. 1),' NIST, Gaithersburg, Maryland, Tech. Rep., 2012. DOI: 10.6028/NIST.SP.800-53r4.

[25] Canadian Centre for Cyber Security, "*Cyber threat and cyber threat actors*". *Cyber.gc.ca*, https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors, (Accessed on 04/12/2021), 2021.

[26] The Computer Language Company Inc., *Script kiddie - CLC Definition*, https://www.computerlanguage.com/results.php?definition=script+kiddie, (Accessed on 05/07/2022), 2022.

[27] C. Johnson, M. Badger, D. Waltermire, J. Snyder and C. Skorupka, "*Guide to Cyber Threat Information Sharing*" *(SP 800-150)*, Gaithersburg, Maryland, 2016. DOI: https://doi.org/10.6028/NIST.SP.800-150.

[28] A. Zibak, C. Sauerwein and A. C. Simpson, 'Threat Intelligence Quality Dimensions for Research and Practice,' *Digital Threats*, 2021, Just Accepted. DOI: 10.1145/3484202.

[29] Cybersecurity and Infrastructure Security Agency (CISA), "*Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure.*" *CISA.gov*, https://www.cisa.gov/uscert/ncas/alerts/aa22-110a, (Accessed on 05/06/2022), 2022.

[30] M. Husák, T. Jirsík 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*, Virtual Event, Ireland: ACM, 2020. DOI: 10.1145/3407023.3407062.

[31] D. Jones and M. Endsley, 'Sources of situation awareness errors in aviation,' *Aviation, space, and environmental medicine*, vol. 67, pp. 507–12, 1996.

[32] P. Barford, M. Dacier, T. G. Dietterich, M. Fredrikson, J. Giffin, S. Jajodia, S. Jha, J. Li, P. Liu, P. Ning, X. Ou, D. Song, L. Strater, V. Swarup, G. Tadda, C. Wang and J. Yen, 'Cyber SA: Situational Awareness for Cyber Defense,' in *Cyber Situational Awareness: Issues and Research*. Boston, MA: Springer US, 2010, pp. 3–13. DOI: 10.1007/978-1-4419-0140-8_1.

[33] The Computer Language Company Inc., *Cloud storage - CLC Definition*, https://www.computerlanguage.com/results.php?definition=cloud+storage, (Accessed on 05/07/2022), 2022.

[34] Forsvarsstaben [Norwegian Defence Staff], *Forsvarets fellesoperative doktrine (FFOD) 2019*, https://fhs.brage.unit.no/fhs-xmlui/bitstream/handle/11250/2631948/FFOD%202019%20.pdf, (Accessed on 05/08/2022), 2019.

[35] zvelo, Inc., "*The Strategic, Operational, & Tactical Levels of Cyber Threat Intelligence.*" *zvelo.com*, https://zvelo.com/strategic-operational-tactical-cyber-threat-intelligence/, (Accessed on 04/12/2021), 2021.

[36] P. Schoemaker, S. Krupp and S. Howland, "*Strategic leadership: The Essential Skills*". *HBR.org*, 2013.

[37] J. F. Carías, M. R. S. Borges, L. Labaka, S. Arrizabalaga and J. Hernantes, 'Systematic Approach to Cyber Resilience Operationalization in SMEs,' *IEEE Access*, vol. 8, pp. 174 200–174 221, 2020. DOI: 10.1109/ACCESS.2020.3026063.

[38] T. Heltberg and K. Dahl, 'Course of Action Development – Brainstorm or Brickstorm?' *Scandinavian Journal of Military Studies*, vol. 2, no. 1, pp. 165–177, 2019. DOI: https://doi.org/10.31374/sjms.30.

[39] A. Claver, 'Devil's advocacy and cyber space. In support of quality assurance and decision making,' *Journal of Intelligence History*, vol. 20, no. 1, pp. 88–102, 2021. DOI: 10.1080/16161262.2020.1864863.

[40] Y. Lee, "*Groupthink as a System of the Decision Making Process.*" *WP.NYU.edu*, https://wp.nyu.edu/steinhardt-appsych_opus/groupthink/, (Accessed on 05/04/2022), 2019.

[41] U. Franke and J. Brynielsson, '"Cyber situational awareness – A systematic review of the literature",' *Comput. Secur.*, vol. 46, pp. 18–31, 2014.

[42] B. Knox, '"Cyberpower Praxis: A Study of Ways to Improve Understanding and Governance in the Cyber Domain", Ph.D dissertation, NTNU, Norway,' 2020.

[43] P. Leedy, J. Ormrod and L. Johnson, *Practical research: Planning and Design*. Pearson, 2019.

[44] M. Alassafi, A. Alshdadi, R. Walters and G. Wills, 'A Framework for Critical Security Factors that Influence the Decision of Cloud Adoption by Saudi Government Agencies,' *Telematics and Informatics, Elsevier*, vol. 31, 2017. DOI: 10.1016/j.tele.2017.04.010.

[45] L. Given, *The SAGE Encyclopedia of Qualitative Research Methods*. Thousand Oaks, California: SAGE, 2008. DOI: 10.4135/9781412963909.

[46] J. Jesson, L. Matheson and F. Lacey, *Doing Your Literature Review: Traditional and Systematic Techniques*. SAGE, 2012.

[47] C. Wohlin, 'Guidelines for Snowballing in Systematic Literature Studies and a Replication in Software Engineering,' *Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering - EASE '14*, 2014. DOI: 10.1145/2601248.2601268.

[48] B. Knox, '"Cyber Security Incident Report",' unpublished report.

[49] P. Cichonski, T. Millar, T. Grance and K. Scarfone, "*Computer Security Incident Handling Guide*" *(SP 800-61 Rev. 2)*, Gaithersburg, Maryland, 2012. DOI: https://dx.doi.org/10.6028/NIST.SP.800-61r2.

[50] Imperial College London, "*Best practice in questionnaire design.*" *Imperial.ac.uk*, (Accessed on 13/04/2022). [Online]. Available: https://www.imperial.ac.uk/education-research/evaluation/tools-and-resources-for-evaluation/questionnaires/best-practice-in-questionnaire-design/.

[51] B. Farnsworth, '"How to Design a Questionnaire." iMotions.com,' *iMotions*, 2021, (Accessed on 13/04/2022). [Online]. Available: https://imotions.com/blog/design-a-questionnaire/.

[52] P. J. Lavrakas, 'Encyclopedia of Survey Research Methods,' *Sage Publications*, 2008. DOI: 10.4135/9781412963947.

[53] Norwegian Centre for Research Data (NSD), *Vocabulary*, (Accessed on 13/04/2022), 2022. [Online]. Available: https://www.nsd.no/en/data-protection-services/oppslagsverk-for-personvern-i-forskning/vocabulary/.

[54] A. Mills, G. Durepos and E. Wiebe, *Encyclopedia of Case Study Research*. Thousand Oaks, California: SAGE, 2010. DOI: 10.4135/9781412957397.

[55] D. George and P. Mallery, 'SPSS for Windows Step-by-Step: A Simple Guide and Reference, 14.0 update (7th Edition),' 2003.

[56] S. Brinkmann and S. Kvale, *Doing Interviews*, 2nd ed. 2018. DOI: 10.4135/9781529716665.

[57] T. George, "*Semi-Structured Interview: Definition, Guide & Examples.*" *Scribbr.com*, (Accessed on 13/04/2022), 2022. [Online]. Available: https://www.scribbr.com/methodology/semi-structured-interview/.

[58] T. George, "*Exploratory Research: Definition, Guide, & Examples.*" *Scribbr.com*, (Accessed on 13/04/2022), 2021. [Online]. Available: https://www.scribbr.com/methodology/exploratory-research/.

[59] J. Ulven, "*High level information security risk in higher education*", *M.S. thesis, Dept. of Info. Sec. and Coms. Tech., NTNU, Norway*, 2020.

[60] W. Adams, *Conducting Semi-Structured Interviews*. 2015. DOI: 10.1002/9781119171386.ch19.

[61] S. Shah, "*7 biases to avoid in qualitative research.*" *Editage.com*, https://www.editage.com/insights/7-biases-to-avoid-in-qualitative-research, (Accessed on 05/03/2022), 2019.

[62] N. Golafshani, 'Understanding Reliability and Validity in Qualitative Research,' *The Qualitative Report*, vol. 8, no. 4, pp. 597–606, 2003. DOI: https://doi.org/10.46743/2160-3715/2003.1870.

[63] J. M. Morse, M. Barrett, M. Mayan, K. Olson and J. Spiers, 'Verification Strategies for Establishing Reliability and Validity in Qualitative Research,' *International Journal of Qualitative Methods*, vol. 1, no. 2, pp. 13–22, 2002. DOI: 10.1177/160940690200100202.

[64] A. Aliyu, Y. He, I. Yevseyeva and C. Luo, 'Cyber Security Decision Making Informed by Cyber Threat Intelligence (CYDETI): IEEE CNS 20 Poster,' in *2020 IEEE Conference on Communications and Network Security (CNS)*, 2020, pp. 1–2. DOI: 10.1109/CNS48642.2020.9162162.

[65] J. M. Spring and P. Illari, 'Review of Human Decision-Making during Computer Security Incident Analysis,' *Digital Threats*, vol. 2, no. 2, 2021. DOI: 10.1145/3427787.

[66] Z. Rashid, U. Noor and J. Altmann, 'Economic model for evaluating the value creation through information sharing within the cybersecurity information sharing ecosystem,' *Future Generation Computer Systems*, vol. 124, pp. 436–466, 2021. DOI: https://doi.org/10.1016/j.future.2021.05.033.

[67] W. Alkalabi, L. Simpson and H. Morarji, 'Barriers and Incentives to Cybersecurity Threat Information Sharing in Developing Countries: A Case Study of Saudi Arabia,' ser. ACSW '21, Dunedin, New Zealand: ACM, 2021. DOI: 10.1145/3437378.3437391.

[68] EduRank, "*Best Universities for Cyber Security in the World.*" *EduRank.org*, (Accessed on 26/04/2022), 2021. [Online]. Available: https://edurank.org/cs/cybersecurity/.

[69] S. Varga, J. Brynielsson and U. Franke, '"Information Requirements for National Level Cyber Situational Awareness",' in *2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, 2018, pp. 774–781. DOI: 10.1109/ASONAM.2018.8508410.

[70] S. Varga, J. Brynielsson and U. Franke, 'Cyber-threat perception and risk management in the Swedish financial sector,' *Computers & Security*, vol. 105, p. 102 239, 2021. DOI: https://doi.org/10.1016/j.cose.2021.102239.

[71] F. Garcia-Granados and H. Bahsi, 'Cybersecurity Knowledge Requirements for Strategic Level Decision Makers,' 2020. DOI: 10.34190/ICCWS.20.102.

[72] M. Kouremetis, 'An Analysis of Estonia's Cyber Security Strategy, Policy and Capabilities (Case Study),' 14th European Conference on Cyber Warfare and Security (ECCWS), Univ Hertfordshire, Hatfield, England, July 02-03, 2015, 2015, pp. 404–412, ISBN: 978-1-910810-29-3.

[73] The World Bank Group, *Population, total - Estonia*, https://data.worldbank.org/indicator/SP.POP.TOTL?locations=EE, (Accessed on 04/28/2022), 2020.

[74] S. Brown, J. Gommers and O. Serrano, 'From Cyber Security Information Sharing to Threat Management,' in *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*, ser. WISCS '15, Denver, Colorado, USA: ACM, 2015, pp. 43–49. DOI: 10.1145/2808128.2808133.

[75] DNB, *Trusselvurdering 2021 [Threat assessment 2021]*, https://www.nsr-org.no/uploads/images/DNB-Arlig-Trusselvurdering_2021_Final_Lowres.pdf, (Accessed on 05/02/2022).

[76] A. Tan, *Top three questions about the Log4j vulnerability*, 2022. [Online]. Available: https://www.computerweekly.com/news/252512071/Top-three-questions-about-the-Log4j-vulnerability.

[77] Emy (@entropyqueen_), "*Explaining #log4j for non technical people...*" *Twitter.com*, (Accessed on 05/03/2022), 2022. [Online]. Available: https://twitter.com/entropyqueen_/status/1469606458597724161?s=20&t=PnYSvttr9ZeghaLF6fv8Yg.

[78] C. Piccirilli and D. Tzabbar, 'Management attention and cyber risk position,' *Organizational Dynamics*, p. 100 867, 2021. DOI: https://doi.org/10.1016/j.orgdyn.2021.100867.

[79] K. Kullman, L. Buchanan, A. Komlodi and D. Engel, 'Mental Model Mapping Method for Cybersecurity,' in *HCI*, 2020. DOI: https://doi.org/10.1007/978-3-030-50309-3_30.

Appendix A

Questionnaire

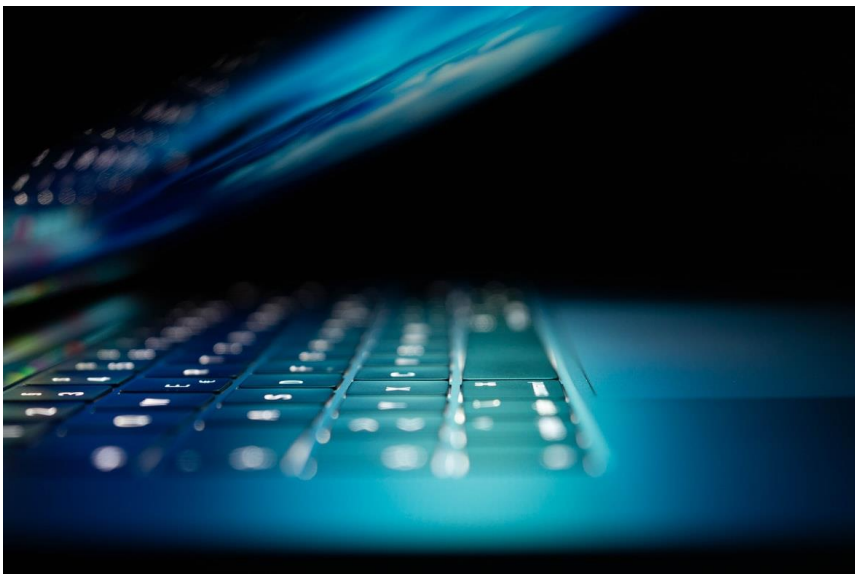
Cyber Threat Communication

Mandatory fields are marked with a star *

What information do you think is important to communicate to a strategic decision maker?

Concurrently with digitalization, cyber threats are increasing in terms of sophistication and impact, and their targets include nations, organizations and individuals. A cyber threat situation is an ongoing and complex state, and is represented based on a given context, such as a particular organization. A cyber threat situation is composed of cyber threats, attacks, trends, threat actors, and more.

In an organization, a strategic decision maker relies on information from different sources to make informed strategic decisions and non-technical considerations in line with the organization's vision, mission and long-term goals.



This survey aims to identify the information needed to make informed strategic decisions and non-technical considerations in a cyber threat situation. Its target audience includes decision makers and technical specialists at all organizational levels. The survey is part of a 30 ECTS master's thesis in Information Security at NTNU (Norwegian University of Science and Technology). Its findings will contribute to the ACDICOM (Advancing Cyber Defense by Improved Communication of Recognized Cyber Threat Situations) project. ACDICOM is funded by the Research Council of Norway (project number 302941).

The questionnaire will take approximately 10 minutes to complete.

Page break

Background information

Background information (or demographic information) allows us to describe the population represented in the research and helps us better analyze the data. In addition, the information allows us to compare opinions between different demographics. E.g., strategic decision makers stated X, whereas technical specialist stated Y.

Please use your current work situation as a basis for answering the questions.

Which sector do you work in? * (one answer per question)

- Public sector
- Private sector
- I prefer not to say
- Other (please state below)

Which industry do you work in? * (one answer per question)

- Education
- Finance and insurance
- IT
- Maritime
- Military and defense
- Professional services
- Telecommunications
- Transport and logistics
- I prefer not to say
- Other (please state below)

Which country do you work in? * (one answer per question)

If you work in multiple countries, state the country where you perform the majority of your work.

Select ...

What is your current position? * (one answer per question)

- Tactical decision maker
- Operational decision maker

- Strategic decision maker
- Technical specialist
- I prefer not to say
- Other (please state below)

How many years of experience do you have with cyber threats? * (one answer per question)

- 0-3 years (Entry-level)
- 3-5 years (Intermediate)
- 6-9 years (Mid-level)
- > 10 years (Senior or executive-level)
- I prefer not to say
- I have not worked with cyber threats

Page break

Cyber Threat Information: Part 1 of 2

For brevity, the questionnaire uses the terms:

- *threat* instead of "cyber threat",
- *attack* instead of "cyber attack",
- *IoC* instead of "indicator of compromise",
- *trend* instead of "cyber trend",
- *threat actor* instead of "cyber threat actor", and
- *TTP* instead of "tactics, techniques, and procedures".

In a cyber threat situation, what information do you think is important to communicate to a strategic decision maker? * (one answer per question)

Scale:

- Not important
- Less important
- Important
- Very important
- Extremely important
- No opinion

Types of information:

- Associated threat(s)
- Associated attack(s)
- Associated incident(s)
- Associated IoC(s)
- Associated trend(s)

- Associated threat actor(s)
- Associated Common Vulnerability Enumeration (CVE)
- Date or time a threat was identified
- Length of time a threat is still considered valid
- Description of past threat situation(s)
- Cyber kill chain-based analysis
- Threat attribution
- Motivation or objective of threat actor
- Sophistication level of threat actor
- Groups or actors associated with an IoC
- Aliases of associated threat actor
- TTP commonly used by threat actor
- Whether threat is targeted or untargeted
- (Types of) individuals or organizations targeted by threat
- Whether threat is associated with targeting specific organizations or sectors
- Automated or manual actions on target
- General description of threats
- General description of threat actors
- Affected systems and platforms
- Targeted systems and platforms
- Status of systems and platforms
- Affected assets
- Targeted assets
- Status of assets
- Risk assessment
- Vulnerability assessment
- Internal classification level of provided information
- External and/or national classification level of provided information
- Whether outside parties should be informed
- Whether outside parties must be informed (e.g., national authorities)
- Rules governing the use or sharing of threat information

Page break

Cyber Threat Information: Part 2 of 2

For brevity, the questionnaire uses the terms:

- *threat* instead of "cyber threat",
- *attack* instead of "cyber attack",
- *IoC* instead of "indicator of compromise",
- *trend* instead of "cyber trend",
- *threat actor* instead of "cyber threat actor", and
- *TTP* instead of "tactics, techniques, and procedures".

In a cyber threat situation, what information do you think is important to communicate to a strategic decision maker? * (one answer per question)

Scale:

- Not important
- Less important
- Important
- Very important
- Extremely important
- No opinion

Types of information:

- Threat information suitable for sharing with outside parties
- Timeline of current threat situation
- Timeline of past threat situation(s)
- Threat information source (e.g., sensors, antivirus)
- Executive summary
- Brief overview
- Detailed description
- Security alerts
- Tool configurations
- Estimated impact
- Severity rating
- Mitigation options
- Unit or function responsible for threat management
- Unit from which the threat information originates
- Individual from which the threat information originates
- Implemented measures
- Planned measures (does not require strategic commitment)
- Suggested measures (require strategic commitment)
- Requirements and needs of underlying units
- Breaking news
- Unprocessed open-source information
- Processed open-source information
- Processed information based on internal data sources (e.g., own sensor data)
- Involved third-party service provider(s)
- Information source reliability
- Information reliability
- Information quality assessment
- Network visualization
- Data flow visualization

Page break

Cyber Threat Information Sharing

How often do you think cyber threat information should be shared with a strategic decision maker? * (multiple answers per question)

- Hourly
- Daily
- Weekly
- Monthly
- Quarterly
- Semi-annually
- Annually
- Other (please state below)

To what extent do you agree with the following statements? * (one answer per question)

Scale:

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree
- No opinion

Statements:

- Cyber threat information should be communicated at scheduled times.
- Cyber threat information should be communicated continuously as it is uncovered.

In a cyber threat situation, what do you think are appropriate communication methods to inform a strategic decision maker? * (one answer per question)

Scale:

- Not appropriate
- Less appropriate
- Appropriate
- Highly appropriate
- No opinion

Communication methods:

- Written communication
- Oral communication
- Informal communication
- Formal communication
- Short report
- Long report
- Company wiki
- Email
- Instant messaging

- Phone call
- Face-to-face meeting
- Digital meeting
- 5-15 minute meeting
- 15-30 minute meeting
- 30-60 minute meeting
- > 60 minute meeting
- One slide presentation
- Presentation with multiple slides
- Visualizations (e.g., diagram, graphs)

Page break

Additional comments

Do you have any additional comments, questions, or concerns you would like to share?

Page break

Thank you for your time and answers! Click "Send" to submit.

References:

[1] C. S. Johnson, M. L. Badger, D. A. Waltermire, J. Snyder, and C. Skorupka, “Guide to Cyber Threat Information Sharing,” Oct. 2016, doi: 10.6028/nist.sp.800-150.

[2] S. Varga, J. Brynielsson and U. Franke, "Information Requirements for National Level Cyber Situational Awareness," *2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, 2018, pp. 774-781, doi: 10.1109/ASONAM.2018.8508410.

[3] B. Knox, "Cyber Security Incident Report," unpublished.

[4] “Trusselvurdering 2021.” DNB, Norway, 2021. Accessed: Mar. 15, 2022 [Online]. Available: https://www.dnb.no/portalfront/nedlast/no/om-oss/samfunnsansvar/2021/DNB_rlig_Trusselvurdering_2021_Final_Lowres.pdf.

By submitting this form, I consent to participate in this study. I understand that the data I provide can be used in ACDICOM-related research and because my participation is anonymous, I cannot withdraw consent once I have submitted my answers.

Appendix B

Survey invitation

What would you tell a strategic decision maker about cyber threats?

Dear participant,

My name is Tiril, and I am inviting you to participate in a survey about what executives need to know to make informed strategic decisions in a cyber threat situation. The target audience includes decision makers and technical specialists at all organizational levels. I also encourage individuals in other positions to participate, e.g., researchers and analysts.

The survey is part of my master's thesis in Information Security at the Norwegian University of Science and Technology (NTNU), which is supervised by Dr. Benjamin J. Knox, coordinator of the Cyber Defense research group at NTNU Center for Cyber and Information Security (CCIS). Its findings will contribute to the Advancing Cyber Defense by Improved Communication of Recognized Cyber Threat Situations (ACDICOM) project. ACDICOM is funded by the Research Council of Norway.

- The questionnaire takes approximately **10 minutes** to complete.
- Responses are **anonymous**.
- To participate, click on the following link: <*link to Nettskjema*>.
- Please complete the questionnaire by **Thursday, April 14, 2022**.

Do not hesitate to contact me at <*NTNU e-mail address*> if you have any questions and/or wish to be informed about the survey results (available June 2022).

Please forward this invitation to anyone you think should participate in the survey.

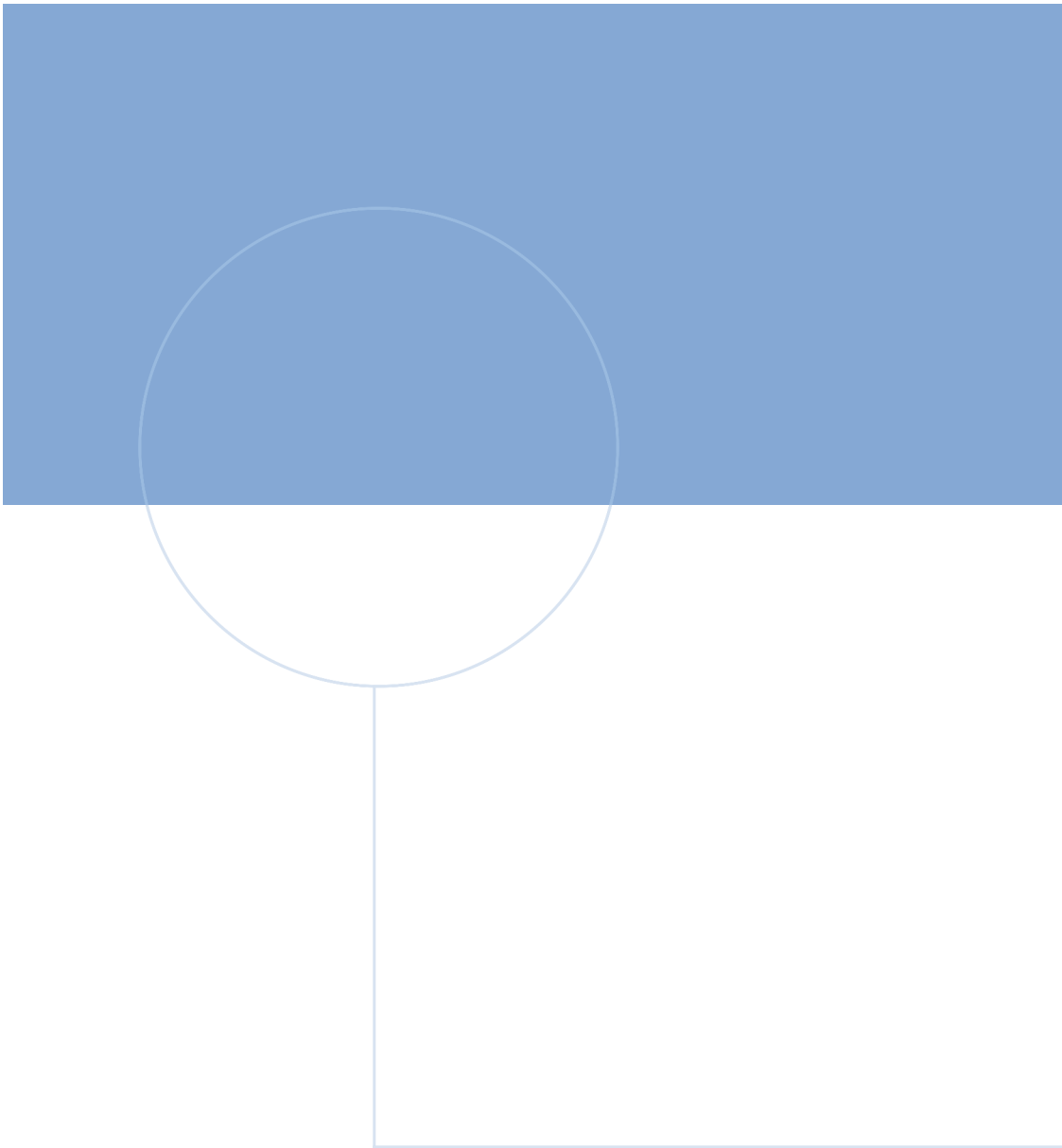
Thank you in advance for your time!

Sincerely,
Tiril Tinde

Appendix C

Interview guide

Themes	Comments and questions	Probes
Introduction	💬 Thank you for participating 💬 MSc thesis general info 💬 Interview objective + structure 💬 Consent agreement ➞ *Start audio recording*	
Background information	? Which sector and industry do you work in? ? What is your current position? ? How many years of experience do you have with cyber threats?	
Scenario	💬 Read scenario (See below) ? In this scenario, what information do you think is important to communicate to a strategic decision maker? ? …, how often should the strategic decision maker be informed of the situation? ? …, should information be communicated at scheduled times or continuously as it is uncovered? ? …, how should information be communicated to the strategic decision maker?	■ Nothing has happened yet, should the decision maker be involved/informed at all? ■ E.g., CEO with non-technical background ■ How to acquire CSA? ■ If executive summary is mentioned: what should it contain? ■ E.g., oral/written, short/long report
Interpretation of survey results	💬 Survey info + demographics 💬 Top 5-10 types of information 💬 What is your opinion on the following statements? They are based on the survey results. ? Information should be shared weekly, monthly, and in case of significant threats or incidents. Agree/disagree? ? Public and private sector reported the same degree of importance of the different types of information. Thoughts? ? Technical specialists decision makers (all levels) reported the same degree of importance of the different types of information. Thoughts? ? Does <u>everything</u> depend on the situation?	■ Cyberspace is universal ■ Same results if we compared Norway to other countries? ■ Technical specialists and decision makers appear to be in sync. Is that your experience as well? ■ Other factors: level of knowledge, personal preferences, etc. ■ Should today's strategic decision makers have a better technical understanding? If yes, why?
Additional comments	? Additional comments ➞ *End audio recording* 💬 Info about transcription process 💬 Thank you for participating 💬 Available for questions and comments	■ Any comments regarding the questionnaire or interview? ■ Anything I should know related to the MSc thesis topic?
Scenario (Adapted from NIST SP 800-150 [26]): *"A nation-state regularly targets [organizations in <participant's industry>] over several months. The attacks come in the form of targeted emails that carry malicious attachments containing a software exploit that, upon opening, launches malware on a victim's system. Systems that are successfully compromised by the malware are then reconfigured by the malware to contact command and control servers and other infrastructure operated by the actor to receive additional instructions, download other malware, and perform data exfiltration."*		



NTNU

Kunnskap for en bedre verden