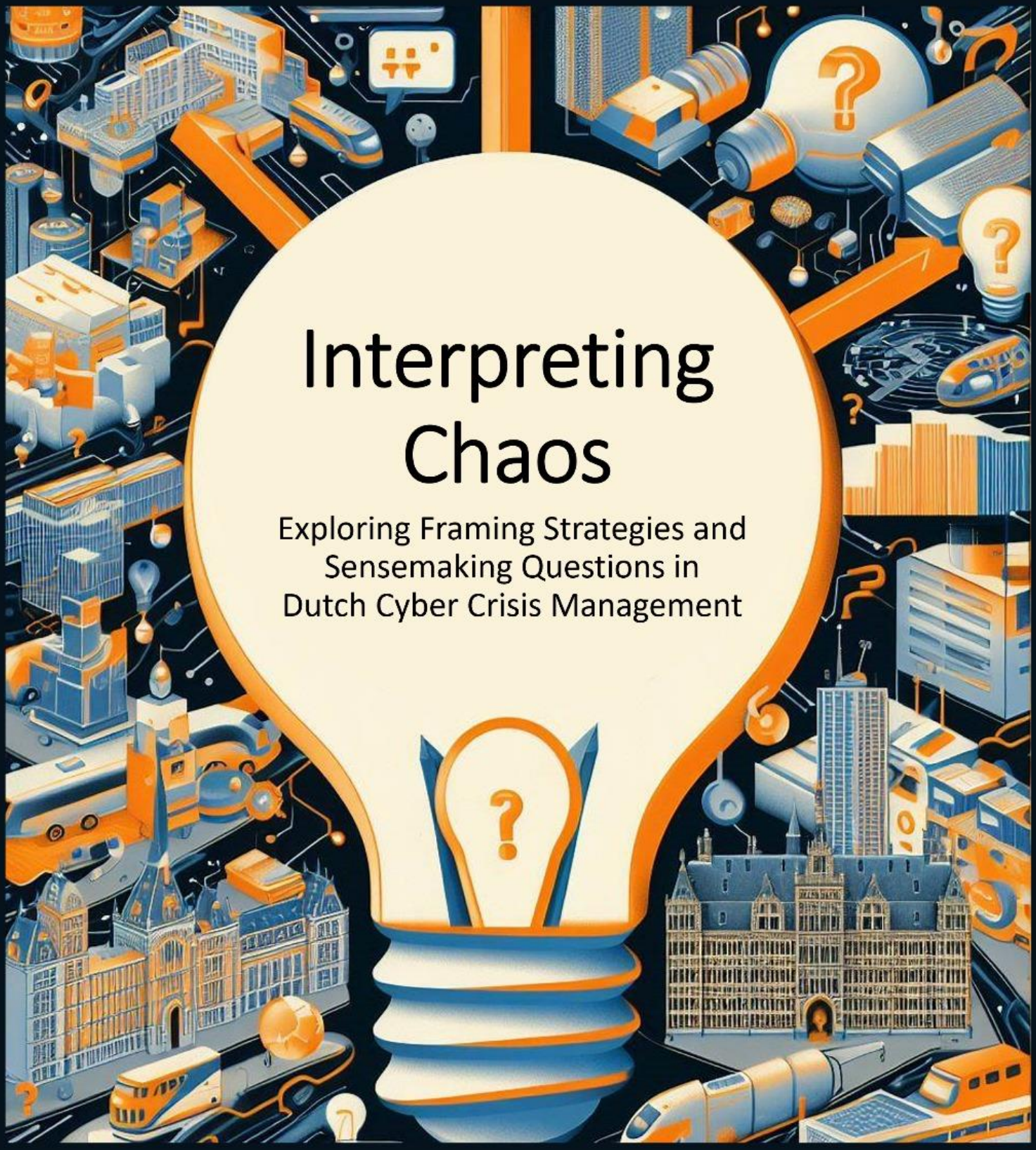
Interpreting Chaos: Exploring Framing Strategies and Sensemaking Questions in Dutch Cyber Crisis Management

Aansorgh-Bok, Maaike



Interpreting Chaos

Exploring Framing Strategies and Sensemaking Questions in Dutch Cyber Crisis Management

Maaike Aansorgh-Bok

Submitted in partial fulfilment of the requirements for the degree of Executive Master Cyber Security

Thesis supervisors:
dr. Cristina del Real, Universiteit Leiden
prof. dr. Sanneke Kuipers, Universiteit Leiden

Universiteit Leiden
The Netherlands

Interpreting Chaos: Exploring Framing Strategies and Sensemaking Questions in Dutch Cyber Crisis Management

Maaike Aansorgh-Bok

Supervised by
dr. Cristina del Real
prof. dr. Sanneke Kuipers

Submitted in partial fulfilment of the requirements for the degree of
Executive Master Cyber Security

Institute of Security and Global Affairs
Faculty of Governance and Global Affairs
Leiden University, The Netherlands

The Hague, January 2024

Picture on front page generated by Microsoft Copilot based on thesis title

Abstract

Cyber crisis management is a relatively new and under researched topic in scientific literature. Most research on cyber crises is focused on defining it and developing exercises. But to make sense of a cyber crisis has not been thoroughly examined. The current study aims to explore how incident response (IR) and crisis response (CR) teams in governmental (GOV) and critical infrastructure (CI) organizations make sense of a cyber crisis, in the context of a Dutch national cyber exercise, "ISIDOOR IV". Through a questionnaire, observers of participating teams were asked to indicate how these teams show behavior related to the Data/Frame theory (Klein, 2010) and on the questions they ask in relation to situational, identity-oriented, and action-oriented sensemaking (Kalkman, 2019). In interviews, experts were asked to indicate challenges in sensemaking and suggest how sensemaking in teams, organizations and between organizations can be improved. This study revealed that IR and CR teams within GOV and CI organizations utilize framing strategies derived from the Data/Frame theory, with a particular focus on Identifying a frame. Behavior on other steps in the framework appears less pronounced. Especially Questioning a frame seems to pose challenges. The study demonstrated that IR and CR teams in GOV and CI organizations ask sensemaking questions. Particularly noteworthy are the high scores observed in Information sharing. And finally, the questionnaire and interviews provided insight into what the challenges to sensemaking in cyber crises are, and what can be improved on team, organizational and inter-organizational level when it comes to sensemaking.

Keywords: cyber crisis management, framing, sensemaking.

Preface

As a crisis manager, I am accustomed to dealing with uncertainty. I enjoy bringing order out of (what seems like) chaos and minimizing the societal impact of an energy disruption, no matter how significant. The physical aspects of the causes and effects associated with a scaled-up gas or power outage, I can sketch out for you effortlessly. I can talk for hours about cascading effects and what they means to society, also because I believe they don't always receive the attention they deserve. When I am alerted, based on experience, I can fairly well assess the visible and tangible effects and where the disruption's effects "cross the borders" to be handled by other crisis organizations. But a cyber crisis is a different story.

Just before I started this Executive Master's program on Cyber Security, a serious vulnerability was found In Apache Log4J, which kept organizations around the globe busy during the Christmas holidays. This incident was an eye-opener, because it was not treated as a crisis by my organization, but could indeed have been described as one when looking back on it. It sparked the creation of a separate crisis response plan for digital disruptions with a cyber component, which I coordinated as a liaison between our IT and OT organization, CISO Office and crisis organization. The finished product consisted of a description of the crisis organization structure, escalation criteria and possible scenario's, but in hindsight never spoke of how to make sense of a cyber crisis. In the second year of the Executive Master's program, this became more apparent and sparked my interest in the behavioral side of cyber crises. Especially how teams make sense of a cyber crisis caught my attention, as during exercises I noticed that not all teams were able to grasp this 'not our core business' type of crisis and found it hard to wrap their head around all this information about mostly ones and zeros. Making sense of a cyber crisis seemed harder to do than making sense of a 'regular' crisis. This led me to the starting phase of the product that lies before you now, my Master's thesis on making sense of a cyber crisis.

I'd like to thank my supervisor dr. Cristina del Real for her continuous support during the writing process. Even though the process sometimes resembled managing a crisis, you kept me focused on the finish line. Next to that, I'd like to thank my second reader prof. dr. Sanneke Kuipers for being available as a second reader, even though that was not self-evident being in a different chair. Your crisis governance expertise is very valuable to me. This program has also been a blast thanks to my peers, and I'd especially like to thank Kim, Nynke and Maarten for their input, laughs and (crisis😊) support. I also want to thank my colleagues for making it possible for me to spend Fridays in Den Haag and allowing me to expand my horizon. Henk, Sebastiaan, Wesley, Sebastien and Maaike, thank you so much! Of course I'd also like to thank all the participants for filling out the questionnaire and the interviewees for their valuable insights.

And last, but certainly not least, I'd like to thank my wife for her patience and continuous support during these two years. Your sacrifices, whether big or small, have not gone unnoticed and I certainly could not have done this without you as my rock! I'm looking forward to spending more time together and with our daughter and son.

Maaike Aansorgh-Bok
Lent, January 26, 2024

Table of contents

1. Introduction

In the heart of a bustling workplace, a frigid Thursday unfolded just days before Christmas. The routine hum of productivity came to an abrupt pause as distant sirens pierced the air. Curiosity drew the employees' attention to a nearby house, now engulfed in flames. Through the office windows, they witnessed the chilling spectacle. Flames painted the wintry sky with hues of orange and red, casting an eerie glow. The biting air carried the acrid scent of burning wood and memories, a bitter reminder of the unfolding tragedy. The wail of sirens harmonized with the chaos. Peering through blinds, they observed the stark contrast between the cold night outside and the intense heat within, a poignant reminder of life's fragile nature.

In the newspaper the next day, a photograph painted a clear picture of what had happened the day before. The article that accompanied it recounted the harrowing details of the blaze that had consumed the home. The article spoke of courageous firefighters battling the intense flames in freezing temperatures and the devastating loss of cherished possessions and memories, on this Thursday just before Christmas. You could almost relive it.

People have always told each other stories. To describe a situation, to make contact with others, to form a collective identity, to persuade or inspire others. But also to make sense of the world around them and help them understand chaotic situations.

Imagine now that the story above was about a cyber crisis that happened on the Thursday before Christmas. Would the details of it paint as clear a picture as the fire? Would the smell of it be described so vividly? Would it be as easy for people to see it before them in their minds? Would it be as easy to tell others about what happened? Would the picture in the newspaper show courageous Incident Responders fighting a digital fire?

Probably not.

1.1 Problem statement

In the context of crisis management, research has been conducted on handling conventional crises, which are more tangible in terms of cause and (physical) consequences. These crises can be articulated easily, possessing clear beginnings and endings. Decades of practical experience and research have been accumulated to make sense of and manage crises of this type effectively. In recent decades however, a new type of crisis, namely the cyber crisis, has emerged. With, amongst others, specific characteristics such as intangibility, interconnectedness, and transboundary nature, it represents a distinct new crisis category which we will dive deeper into in the contextualization section of the literature review.

The features of interconnectedness, intangibility, and transboundary nature differentiate a cyber crisis from conventional crises with a more physical character, posing distinct challenges in comprehending the situation. Due to the increased interconnectivity of systems and networks since the fourth industrial revolution took place, chain-related problems can arise, amplifying the impact, particularly in society. The non-temporal and non-spatial nature of a cyber crisis introduces uncertainty regarding its origin, when the crisis started and ended, and the actions of the actors involved. The transboundary and interconnected nature of cyber crises increase the likelihood that it affects not only individual organizations, but also inflicts harm through cyberspace, impacting society as a whole, as seen in recent years with for example ransomware

attacks (e.g. Wannacry (Milmo, 2022)) and hacks on critical infrastructure (e.g. Ukraine (Slowik, 2018; Whitehead et al., 2017).

This paints the picture of the problem we are facing today: to be able to fight a digital fire, to be able to mitigate a cyber crisis, and to be able to coordinate actions between teams and organizations first we need to make sense of the crisis at hand. Because cyber crises are intangible, cyber-physical systems are interconnected and cyberspace gives a transboundary nature to these types of crises, it's especially important for an organization in critical infrastructure or government to be able to make sense of it. So, how do these types of organizations approach sensemaking in the context of a cyber crisis?

1.2 The current study

To comprehend a crisis situation, it is crucial to make sense of it. So, despite the characteristics of a cyber crisis that make it different from a conventional crisis, how do organizations make sense of a cyber crisis? Investigating the behavior of crisis teams in terms of sensemaking, specifically in how they formulate sensemaking questions and frame the situation, can shed light on this topic. The sensemaking and framing processes in the context of a cyber crisis have not been explored, highlighting the need for further investigation.

1.2.1 Context

In the Netherlands, the overseeing of national cyber security policy is done by the Ministry of Justice and Security (Nationaal Coördinator Terrorismebestrijding en Veiligheid, 2022). The goal is to prepare both governmental organizations and organizations with vital processes for a cyber crisis by promoting collaboration between the private sector, academic institutions, and governmental organizations. The Dutch National Cyber Security Center (NCSC), is part of the Ministry of Justice and Security and has a legal basis within the Network and Information Systems security Act (WBNI, the Dutch translation of the NIS-Directive) (Nationaal Cyber Security Centrum, 2019). NCSC's tasks are to be a national CERT, cooperate with partners and function as a "single point of truth" in collecting, interpreting and sharing information during cyber incidents and crisis situations.

Public and private sectors in vital processes (Ministerie van Justitie en Veiligheid, 2023) share information between each other on cyber threats and incidents. Voluntary sectoral Information Sharing and Analysis Centers (ISACs) facilitate this and the intelligence services and Dutch High Tech Crime units also participate regularly (Boeke, 2018). The basis for this information sharing is trust and equality.

Regarding cyber crisis management, the National Crisis Plan Digital (Ministerie van Justitie en Veiligheid, 2022b) provides the frameworks for effective cooperation between government organizations, vital providers and non-vital sectors. In the plan, the characteristics of a digital crisis are mentioned, amongst others the interconnectedness of systems, transboundary nature and the intangibility in terms of the source of the incident (Ministerie van Justitie en Veiligheid, 2022b).

If a cyber crisis occurs, the National Coordinator on Terrorism and Safety (NCTV) can activate the National crisis structure through the National Crisis Center (NCC). Next to that, the NCSC coordinates the operational side of cyber crisis management. The information flows are complicated, as shown in the National Crisis Plan Digital (Ministerie van Justitie en Veiligheid, 2022b). In essence, the left side describes the parties that are dealing with the cyber crisis itself, and the right side describes the generic national crisis structure, which is further explained in the National Crisis Management Manual (Ministerie van Justitie en Veiligheid, 2022a).

One way the central government prepares the organizations with vital processes is by organizing a national cyber crisis called “ISIDOOR”. This exercise focuses on coordination and cooperation between national and sectoral organizations in the Netherlands. The goal of the exercise is to practice the crisis procedures as mentioned in the National Crisis Plan Digital Nationwide Crisis Response plan for digital crises (Ministerie van Justitie en Veiligheid, 2022b), the National Playbook Crisis Management (Ministerie van Justitie en Veiligheid, 2022a) and the Network and Information Systems security Act (WBNI) (Ministerie van Economische Zaken en Klimaat, 2018). The exercise aims to promote information sharing, cooperation between vital sectors and government and hopes to strengthen this.

1.2.2 Scope

The scope of this study is governmental organizations and critical infrastructure organizations in the Netherlands, who participated in the national cyber exercise “ISIDOOR IV” in November 2023.

This exercise presents three opportunities as a playground for research. First, it comprises a precisely defined target demographic, and second, all participants engage in the exercise with a uniform foundational scenario, enhancing comparability between our defined groups of interest: governmental organizations and organizations in critical infrastructure. Finally, the exercise takes place during multiple days, which makes it a more realistic exercise to observe than the regular exercises individual organizations execute and usually look like a pressure cooker for 1,5 to 3 hours. As Northwave for example have researched in their whitepaper on the mental impact of ransomware attacks, “on average it takes about 23 days to get most of the systems up and running again” (Northwave, 2022, p. 11).

1.2.3 Research question

The current study specifically focuses on incident response and crisis response teams in government and critical infrastructure organizations, by looking at the following aspects: framing behavior and sense-making questions asked in these teams. Therefore, the current study has the following main research question:

MRQ: “How do incident response and crisis response teams of organizations in critical infrastructure and governmental organizations use framing and sensemaking behavior to make sense of a (national) cyber crisis in the Netherlands?”

To be able to answer the main question, the concepts of sensemaking and framing in the context of crisis management will be elaborated on in a literature review. This provides the framework for a behavioral observation of incident response and crisis response teams participating in the “ISIDOOR IV” exercise. This observation will shed light on the actual observed behavior of crisis teams with regards to framing, and sensemaking questions asked by looking at the following sub questions.

SQ1: "What framing behaviors do incident response and crisis response teams of organizations in critical infrastructure and governmental organizations demonstrate when framing and making sense of a national cyber crisis, including how they identify, question, reframe, and elaborate on frames?”

SQ2: "How do crisis teams utilize questioning strategies to understand and navigate a national cyber crisis, considering situational sensemaking, identity-oriented sensemaking, and action-oriented sensemaking?"

SQ3: "What are the challenges and necessary improvements with regards to making sense of a (national) cyber crisis?"

The sub questions are answered by asking observers of participating crisis teams to fill out an online questionnaire that focuses on the team behavior that can be observed.
The questionnaire provides an outcome to discuss with experts in the field of Cyber Incident Response and Cyber Crisis Response. In short interviews, they will provide insight into the broader question on how organizations make sense of a cyber crisis, what the main challenges are in their view and what can be done to advance sensemaking in cyber crises in the future.

1.3 Justification

1.3.1 Scientific relevance

Sensemaking theory has been applied to many organizational challenges, as well as to crises, but it has not yet been researched in the context of a national cyber crisis like "ISIDOOR IV". Framing theory has also been researched in many different conditions, but not yet on the behavioral characteristics of a crisis team during a national cyber crisis exercise like "ISIDOOR IV". Most exercises focus on the triggering of a cyber-resilience plan, people's capability of managing a crisis ("to have the right people with the right training in the right place at the right time with the right information and able to make the right decisions" (Mils Hills, 2016, p. 122) or specific technical aspects like in simulations on pen testing or DDoS attacks. The type of exercise that is usually done is a desktop exercise, as they are relatively effective in developing capabilities (Mils Hills, 2016) and are easy to organize. Also, they don't interfere with actual critical processes, but only simulate disruptions. "ISIDOOR IV" can be categorized as a desktop exercise as well, but a very large one considering the number of organizations that take part.

The application of sensemaking and framing theories to a cyber context will provide theoretical basis for explaining why some teams are more successful than others in making sense of crises. This will provide insight and a first description on how organizations apply framing and sensemaking within the context of a national cyber crisis as exercised during "ISIDOOR IV".

1.3.2 Societal relevance

Cyberspace is a backbone for not only social, but also for vital processes in society. Therefore, it's vital to protect, and knowing how to make sense of a cyber crisis is essential for being able to get to the right decisions and actions that need to be made.

In the latest Risk and crisis barometer of Autumn 2023 (Nationaal Coördinator Terrorismebestrijding en Veiligheid, 2023), it is shown that Dutch people consider it very likely that cyber threats pose threat to national security. The survey also indicates that people don't consider themselves having a lot of knowledge about cyber threats, but they also indicate that more and more citizens are concerned about cyber threats. The stopping of vital processes and cyber threats are among the top 3 events Dutch citizens consider the most severe in impact.

Next to that, it's relevant to study how crisis teams make sense of a cyber crisis, as cybersecurity and cyber crises are a young field of research. It's often said that it's not a question of if your organization will be hit by a cyber crisis, but when. As former FBI-director Robert Mueller said: "I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again" (Mueller III, 2012). Or, as the Netherlands Scientific Council for Government Policy (WRR) phrased it in 2019, it's not the question *if* but *when* society will be confronted with the consequences of a large-scale cyber-attack" (Schrijvers et al., 2021).

This means that organizations need to have their incident response and crisis response in order, to effectively manage the cyber crisis. And to be able to do this, sensemaking and framing of the situation are essential.

2 Literature review

In this chapter, we provide contextualization on the topics of cyber crises and the characteristics (intangibility, interconnectedness and transboundary nature) that make it difficult to make sense of a cyber crisis. Afterwards, we provide a theoretical framework for our current study, based on the concepts of sensemaking and framing.

2.1 Contextualization

To understand the context on the topic of this thesis, it is important to elaborate on the concept of cyber crises and the characteristics that make it hard to make sense of a cyber crisis: intangibility, interconnectedness of systems and the transboundary nature.

2.1.1 Cyber crises

The topic of cyber crises doesn't get much attention in literature. In 2017, Kuipers and Welsh reviewed three journals on the crisis types they publish on in the period of 1983-2016. Cyber crisis was among the crisis types that receive the least attention (Kuipers & Welsh, 2017). They summarize their findings by stating that "the literature on crises and disasters remains focused around 'classic' natural disaster types and our ability to prepare and respond to the threat they pose" and note for example the lack of attention for system interconnectedness and cyber dependence (Kuipers & Welsh, 2017, pp. 279–280). Prevezianou (Prevezianou, 2021) states that security and crisis management scholars are excited to dive into the topic of cyber crises, but also have a little "fear of falling" (Prevezianou, 2021, p. 52), due to lack of familiarity with the topic. As the author describes it, it is necessary to start "building the necessary bridge between the technical aspect and the crisis management aspect" (Prevezianou, 2021, p. 52), because while we have been addressing significant cyber-related events for an extended period, there has been a notable lack of exploration into the term "crisis" within the cyber domain. Simultaneously, commonly used terms like "disruption," "incident," or "attack" have gained widespread usage. In a world in which systems and networks are interconnected, this means there is quite a large research gap, and as Prevezianou states it, "a lack of understanding of the new threats could result in us managing them the same way as other conventional threats and, thus, follow a "one size fits all" logic." (Prevezianou, 2021, p. 56).

Although there are several authors trying to define cyber crises, at the moment the academic world lags behind when it comes to researching the understanding of and capabilities for dealing with cyber crises (Kuipers & Welsh, 2017) and definitions of cyber crises are scarce (Backman, 2021). There are however a few definitions that help us understand the concept more.

For example, Prevezianou (Prevezianou, 2021) defines a cyber crisis within the transboundary crisis framework as follows. “A cyber crisis is a situation during which damage to or exploitation of a “vital cyber asset” can cause serious damage or disruption to critical societal functions, such as critical infrastructure, routine operations, reputational damage and economic damage, threaten fundamental societal values, or, in extreme cases, endanger human lives” (Prevezianou, 2021, p. 65). This definition highlights the fact that a cyber-attack can inflict harm on individuals and considers the magnitude and potentially far-reaching consequences of a cyber crisis. Simply put, this means that a cyber crisis is a lot to handle, especially if the full range of effects takes place. This is hardly doable for organizations and even countries.

Another definition is provided by Backman, a cyber crisis is “IT disruptions that has the potential to severely limit or eliminate the functionality of key societal services or critical infrastructure, which must be dealt with urgently under conditions of deep uncertainty in order to avoid physical, financial and/or reputation damage” (Backman, 2021, p. 432). This definition also highlights potential impact on society and states that it is necessary to deal with it immediately. Backman also places the definition of a cyber crisis in a transboundary context.

In the Dutch Cybersecurity Strategy 2022-2028 (Nationaal Coördinator Terrorismebestrijding en Veiligheid, 2022), a cyber incident is defined as “a (connected set of) events or activities that could lead to disruption one or more (digital) processes. This includes both a cyber-attack (deliberate activity by an actor who is aimed at disrupting one or more digital processes with digital means) as failure as a result of incidental example natural or technical causes or human errors” (Nationaal Coördinator Terrorismebestrijding en Veiligheid, 2022, p. 53). This definition is similar to the two provided by Prevezianou and Backman, but next to *intentional* attacks also includes disruption due to *incidental* and *accidental* failures. This connects well with the Harm-model approach of Van den Berg and Kuipers (van den Berg & Kuipers, 2022) we will touch upon later and offers a more comprehensive interpretation of a cyber crisis in our opinion.

2.1.2 Intangibility

Intangible concepts lack a concrete or physical form, making them difficult to grasp or quantify through the senses. The idea, quality, or aspect cannot easily be perceived, touched, or measured physically. Understanding intangible concepts requires a level of abstraction and interpretation, relying on, for example, (shared) language or symbols to make sense of and communicate their meaning. While intangible concepts may not have a physical form, they play a crucial role in shaping human experiences, values, and perspectives. The cyber crisis itself is also intangible in the sense that it can change during time (van den Berg & Kuipers, 2022). This means they can go from a creeping crisis (undetected vulnerability), to a full-blown materialized crisis (ransomware note on a laptop) with impact on operational processes. And even if the effect is physical, it might be unknown who the attackers were (van den Berg & Kuipers, 2022).

A cyber crisis is less visible and tangible than its conventional counterpart, both in terms of causes (within cyberspace) and effects or harm done (harm within and outside of cyberspace) (van den Berg & Kuipers, 2022), making it challenging for individuals to form a clear understanding. Without a clear understanding of what is going on, it is hard to make sense of the crisis at hand, impacting not only the situational awareness needed, but also hinders the decision-making process.

2.1.3 Interconnectedness

The interconnectedness of the digital and physical worlds plays a role. The Fourth Industrial Revolution, which the World Economic forum defines as "the advent of 'cyber-physical systems' involving entirely new capabilities for people and machines" (Davis, 2016), is an example of a seemingly chaotic situation with implications we are still trying to understand and shape. As Klaus Schwab wrote, the sheer speed of this revolution "has an impact on human identities, communities, and political structures" (Schwab, 2023) and we need to structure it and give it purpose. Every industrial revolution up until now has brought both risk and opportunity and the fourth is no different. The risks in terms of cyber security threats, misinformation and the socio-technical aspects have been described before (Mils Hills, 2016).

Charles Perrow (Perrow, 1999) is famous for demonstrating how seemingly insignificant events can spiral out of control within complex and tightly interconnected systems. His Normal Accidents theory names three conditions that render it likely for a system to be susceptible to a normal accident. The systems have to be complex, tightly coupled and have catastrophic potential. A cyber crisis ticks all three boxes. Cyber systems, especially within critical infrastructure, are an example because they embody inherent complexity through diverse interconnected components, technologies and dynamic threats. They demonstrate tight coupling, because changes or malfunctions in one part can quickly affect interconnected components, facilitating the rapid spread of incidents through the network. And finally, they pose catastrophic potential with far-reaching consequences resulting from minor security oversights or vulnerabilities leading to cascading effects.

As the physical and digital world have become interconnected so much in the last few decades, it's important to have an integrated view on safety and security. As for example the cyber-attacks on the Ukraine power system (Whitehead et al., 2017), and on the Colonial Pipeline (Hale, 2021) have shown, operational processes can indeed be disrupted, and interests of safety and security come together as harm is inflicted on society through cyberspace (van den Berg & Kuipers, 2022). This means that the topics of safety and security are increasingly interconnected as well and ask for an alignment of safety science and security studies, as Van den Berg and Kuipers propose (van den Berg et al., 2021).

Van den Berg and Kuipers also note in a different article, "incidents that start in cyberspace may have spill-over effects causing harm in the physical world" (van den Berg & Kuipers, 2022, p. 12). Their proposed harm model show that incidents that start in cyberspace, can have spillover effects on the physical world. It is this interconnectedness of the digital and physical worlds that can lead to digital disruption, potentially disrupting society as a whole, which illustrates the need for thorough preparation.

2.1.4 Transboundary nature

Transboundary crises are not new (Boin, 2019), but they vary from crises that are confined within specific borders. Various scholars have written on the topic and provide a description of a transboundary crisis. Ansell et al. (Ansell et al., 2010) for example describe the characteristics of a transboundary crisis on three dimensions: 1) *political boundaries*, in which both vertical and horizontal coordination is required to manage the crisis; 2) *functional boundaries*, in which crises cross functional boundaries, for example between public and private parties and 3) *time boundaries*, in which a crisis has no clear beginning or end, or require a very long response, or trigger effects that don't happen in the same timeframe. Kuipers and Boin write in European Civil Security Governance, "transboundary crises typically affect multiple jurisdictions and challenge authorities at multiple levels of government […], require public-private cooperation, undermine

the functioning of multiple policy sectors and critical infrastructures, escalate in unforeseen directions, exploiting linkages between functional and geographical domains" (Bossong & Hegemann, 2015, p. 193). In this description they don't mention the time boundaries, which is a factor that is relevant when we look at transboundary cyber crises.

Cyberspace is not physically boundarized as countries or municipalities are, it is transboundary in nature (Ansell et al., 2010) (Boin, 2009), in both time and place. If a cybercriminal in one country starts an attack with one click of a mouse, the damage can be done in another country. As Van den Berg and Kuipers argue, "this makes cyber security crises fundamentally different from, let's say, an upcoming weather event or a kinetic attack with a long-range missile" (van den Berg & Kuipers, 2022, p. 14). It's harder to see what's coming and where it's coming from, there is no time delay between start of the attack and impact and therefore it's harder to mitigate the consequences of or prepare adequately for a cyber-attack before impact, as they argue. Next to that, setting it apart from the fire story as described before in this chapter, it might take weeks or months to find out who was responsible for the attack, and solving it. Cyber crises in this way also transcend the boundaries of two fields of study: safety science and security studies, as a security threat (e.g. ransomware attack) can escalate a safety issue (delaying critical care to patients) as for example in the Wannacry ransomware attack (van den Berg et al., 2021).

To conclude this conceptualization, we will briefly summarize. Cyber crises are a relatively new type of crisis, with characteristics that make it hard to make sense of. Cyber crises are intangible due to their digital nature, are interconnected as a result of complex dependencies in information systems, and are transboundary, affecting entities across geographical and political borders in the global cyberspace. The transboundary nature of cyberspace also means that the consequences of a cyber crisis can impact individuals, organizations, and even nations beyond the borders of the initial incident location, adding to the complexity and challenge of managing such crises. Making sense of this type of crisis, with these characteristics is a critical, but challenging, task in dealing with a cyber crisis.

In the next chapter we will zoom in on the topic of sensemaking, to illustrate why sensemaking is indeed a critical task and how sensemaking questions can help crisis teams to advance their understanding of a crisis, cyber related or not. Then we will focus on a specific part of sensemaking, which is the ability to create a frame as a base for handling a crisis.

3 Conceptual framework

In crisis management, the initiation of all processes starts with the cognitive activity of sense-making. What's going on and how does this affect us are the first questions asked in crisis teams. To be able to answer the sub questions and the main research question, we need to dive deeper into the concepts of sensemaking and framing. To do this, in this theoretical framework we examine both sensemaking and framing research in relation to crisis management and generate hypotheses based on this literature to use for our study.

The goal of our study is to explore if sensemaking and framing behavior is visible in incident response and crisis response teams in Dutch government and critical infrastructure organizations. First, we will explain what sensemaking in general is, provide a brief history and how this concept applies to crisis management. Next, we will elaborate on the topic of framing and zoom in on how the Data/Frame theory can help us measure team sensemaking by looking at framing behavior. And finally, we'll zoom into the three types of questions crisis team should ask themselves when faced with a crisis. These are questions on situational sensemaking, identity-oriented sensemaking and action-oriented sensemaking.

3.1 Sensemaking

3.1.1 History of sensemaking

To start our literature review on sensemaking off, there is not yet one all-encompassing definition of sensemaking. As Maitlis and Christianson brilliantly summarized in their excellent review including a history of sensemaking (Maitlis & Christianson, 2014), sensemaking as a concept already exists since the 1920's, and in the 1960's it became a separate field of study. One of the most influential scholars in the field was Karl Weick, who researched sensemaking in the context of organizations. In the 1970's sensemaking as a social construct of reality was researched and methods were developed further.

In the 1980s, organizational behavior and strategic management research shifted towards a cognitive focus in sensemaking. Scientists investigated how people try to understand things when their expectations are not met and how they make sense of the information in their surroundings. Additionally, studies revealed that actions taken during sensemaking could change the immediate environment and even influence the course of events or lead to crises.

In the 1990s, research on sensemaking became more specialized, with Weick's book, 'Sensemaking in Organizations' (Weick, 1995) marking a crucial development. This work provided a theoretical framework for understanding key aspects of sensemaking. He wrote there are seven characteristics that "set sensemaking apart from other explanatory processes such as understanding, interpretation, and attribution" (Weick, 1995, p. 17). These seven characteristics are that sensemaking as a process is 1) grounded in identity construction, 2) retrospective, 3) enactive of sensible environments, 4) social, 5) ongoing, 6) focused on and by extracted cues and 7) driven by plausibility rather than accuracy (Weick, 1995, p. 17). Next to that, in the 1990's scholars used case studies of critical events to explore sensemaking during crises and its application afterward to explain such situations. The role of language in sensemaking became a focus, and research expanded to encompass various organizational contexts, linking sensemaking to outcomes like culture, social influence, and strategic change. This period saw a deepening and broadening of sensemaking research across different dimensions (Maitlis & Christianson, 2014) and includes Karl Weick's organization perspective and the role of language.

Since 2000, there has been a growing emphasis on understanding the social aspects of sensemaking processes. Research has expanded into exploring the relationships between sensemaking and language, narrative, and discursive practices. The study of sensemaking has extended to diverse settings, bridged different levels of analysis, and started exploring its embodied and sociomaterial aspects, challenging the previous focus on cognitive and discursive elements (Maitlis & Christianson, 2014).

One of these settings, sensemaking in crisis management, gained more attention after the year 2000. Especially after the formal establishment of the safety regions in the Netherlands in 2010, we also see more research on the topic of distributed sensemaking. Wolbers (Wolbers, 2022), Boersma & Wolbers (Boersma & Wolbers, 2021), Treurniet & Wolbers (Treurniet & Wolbers, 2021) and Mills and Weatherbee (Mills & Weatherbee, 2006) are examples of authors that have contributed a lot to this field.

Distributed sensemaking is a relevant topic especially when multiple organizations have to work together to manage the effects of a crisis. In the context of "ISIDOOR IV", this is also applicable. Due to the nature of our current study and the timeframe available, it is however impossible to take this specific topic further. Still, within the questionnaire we have developed (see methodology chapter), we do ask some questions related to distributed sensemaking, to gauge if this is a topic for future research related to our study.

3.1.2 Defining sensemaking

This long history of sensemaking has led to a variety of definitions on the topic. Maitlis and Christianson (Maitlis & Christianson, 2014) have created a table in their review article with various definitions of sensemaking by various authors in the field. In these definitions, the history of sensemaking is reflected. Some definitions focus more on the cognitive aspects, others focus more on the social aspects of sensemaking. For the purpose of the current study, which looks at team sensemaking, the social aspect is essential. Maitlis and Christianson propose an integrated definition, by defining sensemaking as "a process, prompted by violated expectations, that involves attending to and bracketing cues in the environment, creating intersubjective meaning through cycles of interpretation and action, and thereby enacting a more ordered environment from which further cues can be drawn" (Maitlis & Christianson, 2014, p. 67). This definition implies that sensemaking is dynamic, triggered by unexpected situations, in which actions are needed based on a collective understanding, with the goal of creating order in a chaotic situation.

3.1.3 Sensemaking in crisis situations

Sensemaking, as a procedure of comprehending a situation that lacks clarity, is crucial for the proficient and successful management of crises (Weick, 1993), (Maitlis & Christianson, 2014). In this paragraph we look at the application of sensemaking to crisis situations and why it is a relevant concept to study, also with regard to our topic of cyber crises.

Research on crisis sensemaking can be categorized into two main streams, according to Maitlis and Sonenshein (Maitlis & Sonenshein, 2010). The first focuses on the unfolding of sensemaking during crises across various contexts, mainly. The second strand examines how sense is retrospectively made of crises, often utilizing public inquiry reports and documents to construct an account of the events, reasons behind them, and accountability. In both strands, the authors identified three main themes, showing individual, collective and institutional influences on sensemaking (Maitlis & Sonenshein, 2010). In the collective sensemaking studies, they identify various challenges that teams for example face when they try to get to a common understanding and collective action in crisis situations. In fact, they argue that sensemaking can "both aid and hinder adaptation in environments that are dynamic and unpredictable" (Maitlis & Sonenshein, 2010, p. 561). Being a social construction process, in crisis situations a shared meaning is very important, but only if collectives "update and doubt" their sensemaking Maitlis and Sonenshein state. Updating makes sure that a current state of awareness is revised when new information is received, and doubting motivates people to continuously generate fresh understandings. Because, they argue, "one never makes finite sense of a situation because things are always changing" (Maitlis & Sonenshein, 2010, p. 565). Still, groupthink (Janis, 1982) and conformity (Asch, 1956) can get in the way of doubting and updating sensemaking. This means that it is important for people to share their minds on the sense they make of the crisis, so the social process of comparing these interpretations in the team can start and work towards a shared sense made of the situation.

In the literature reviewed, we find different reasons why sensemaking is an important factor in crisis situations and therefore relevant to study, also in the context of cyber crises.

Sensemaking in crisis situations is difficult. Crisis situations are usually low probability situations that can have a large impact, with consequences for the core business of an organization (Weick, 1988). To prevent a crisis from escalating it is imperative to make sense of the situation and take action, but this is difficult because of the low probability and the fact that the action taken also has an effect on the crisis situation itself, changing it as the crisis unfolds (Weick, 1988), (Weick, 1995), (Weick, 1993). The continuous process of sensemaking is necessary to step

by step get more understanding of what's happening and how our actions impact the crisis situation itself.

Sensemaking is the first of five critical tasks of leadership in crisis. Boin et. al. (Boin et al., 2016) identify five critical tasks when it comes to leadership in crisis: sensemaking, decision making, meaning making, terminating and learning. Sensemaking is the first critical task for a reason: if you can't make sense of a vague, ambivalent and contradictory situation, it is impossible to make the appropriate decisions, explain to people what is going on, determine when to end crisis mode and learn from the crisis. Boin et.al. state that it is "virtually impossible to predict with any sort of precision when and where a crisis will strike" (Boin et al., 2016, p. 19). In hindsight people can however explain what the trigger of the crisis was. Next to that, they argue that "it is possible to grasp the dynamics of a crisis once it becomes manifest and unfolds" (Boin et al., 2016, p. 19). This means that effective sensemaking can help to assess crisis situations and what needs to happen next.

Sensemaking enables decision-making in crisis situations. As sensemaking is a process and not an end state, it can produce (temporary) end states like situational awareness, or collective understanding of the situation (Klein et al., 2010). A successful sensemaking process enables decision-making during crises. It is related to situational awareness as described by Endsley (Endsley, 1995), but differs in that situational awareness is a state. In the process of sensemaking, it is possible to arrive at the state of situational awareness multiple times and this is usually written down in a common operational picture.

Boin et. al. (Boin et al., 2016) name a few different factors that can improve sensemaking in crisis situations (Boin et al., 2016). An early-warning system can help to spot slight disruptions that might escalate, being alert to issues that might compromise the information flow, trying to minimize blind spots by using the principle of managed diversity to scan and interpret their surroundings. But also enable the organization to put all the information pieces together in a swift way. This can be done by getting different organizations to share information and interact with each other, but also by organizing the information management process. And last but not least, it is necessary to stay alert to the point where stress wears you down, as it disables or impairs personal sense making capabilities. Maitlis and Sonenshein (Maitlis & Sonenshein, 2010) suggest that updating and doubting sensemaking is important to keep adapting to a changing situation like a crisis. These factors will be explored further in the next section on framing.

3.1.4 Team sensemaking in crisis situations

As we established in the previous paragraphs on sensemaking, it is not only an individual process, but also a collective process. This collective process comes back in the sensemaking behavior of a crisis team. Together, all team members try to find a frame for the situation at hand, based on internal and external expert input and the environmental image of the crisis, to make sense of the crisis. This sensemaking process is then input for their situational awareness, decisions and actions they have to take, which in turn have their impact on the crisis situation, triggering the sensemaking process once again. This is an ongoing process, see the figure below.

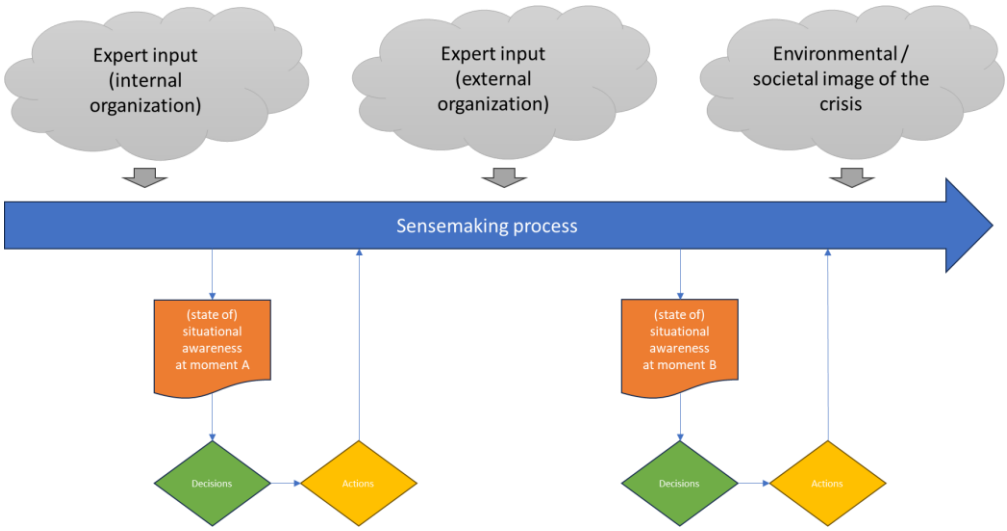


Figure 1 - The sensemaking process as viewed by the author

In their article on team sensemaking, Klein et al. (Klein et al., 2010) write that the team sensemaking process resembles the situation assessment part of the adaptive cycle of Burke's model of input-throughput-output of team adaptation (Burke et al., 2006). In this thesis, we won't dive further into the team adaptation model of Burke, but focus on the framing part of Klein's model. Klein et al. have argued that "team sensemaking is, in many ways, more critical than individual sensemaking" (Klein et al., 2010, p. 306). They define team sensemaking as "the process by which a team manages and coordinates its efforts to explain the current situation and to anticipate future situations, typically under uncertain or ambiguous conditions" (Klein et al., 2010, p. 306). This perfectly suits the context of a (cyber) crisis. The coordination and management of the team focuses on data seeking, data synthesizing and data dissemination. This also includes the negotiation of the inferences of the data, which leads to teams adjusting their frame or reframing, as new data is collected and analyzed. This is difficult to do, because team sensemaking poses coordination requirements and can break down if it doesn't meet emergent requirements. Klein also argues that research into team sensemaking is needed for improvements in practice.

"Sensemaking is seen as a reciprocal process of using data to identify a frame and using the available frame to determine what counts as data" (Klein et al., 2010, p. 307). This is different than going from data to information to knowledge and to understanding in regular waterfall type of information processing they write. The notable difference is that sensemaking leads to the end state of a frame that fits the situation (Klein et al., 2010).

To summarize, sensemaking is an important topic to research in relation to crisis management. Sensemaking is difficult, it is a critical task in crisis leadership and it enables decision-making, but updating and doubting are relevant factors to consider (Maitlis & Sonenshein, 2010), especially when we examine team sensemaking. To connect general and crisis (team) sensemaking with our study, in the following sections we zoom into the topic of framing.

3.2 Framing

Within the realm of social sciences, framing refers to a collection of concepts and theoretical viewpoints that explore how reality is structured, interpreted and communicated about by individuals and collectives. In this section we will examine the definition of framing and look at framing in crisis situations.

3.2.1 Defining framing

As Weick already wrote in 1995, “sensemaking involves placing stimuli into some kind of *framework*” and this enables people to "grasp, comprehend, interpret, attribute meaning, make projections, and predict events”. (Weick, 1995, p. 4). Framing is therefore a part of sensemaking. By identifying a frame, individuals and teams can build a narrative for the crisis, to base their actions on. A clear frame helps the process of sensemaking and in effect it helps to create situational awareness and enables decision making.

Klein et al. (Klein et al., 2006a), in their first part of a two part article on ‘making sense of sensemaking’, come to the verdict that “sensemaking is a motivated, continuous effort to understand connections (which can be among people, places, and events) in order to anticipate their trajectories and act effectively” (Klein et al., 2006a). In the second part they posit the Data/Frame theory, in which they state that “the basis sensemaking act is data-frame symbiosis” (Klein et al., 2006b, p. 88). A frame, they state, is a “perspective, viewpoint or framework” (Klein et al., 2006b, p. 88) used to make sense of something.

Our perspectives or narratives play a crucial role in defining what we consider as data. Sensemaking often revolves around the connection between data and the frames or narratives we hold. The Data/Frame theory of Klein et. al, as pictured below, explains how this process works by identifying emergent sensemaking strategies (Klein et al., 2010).

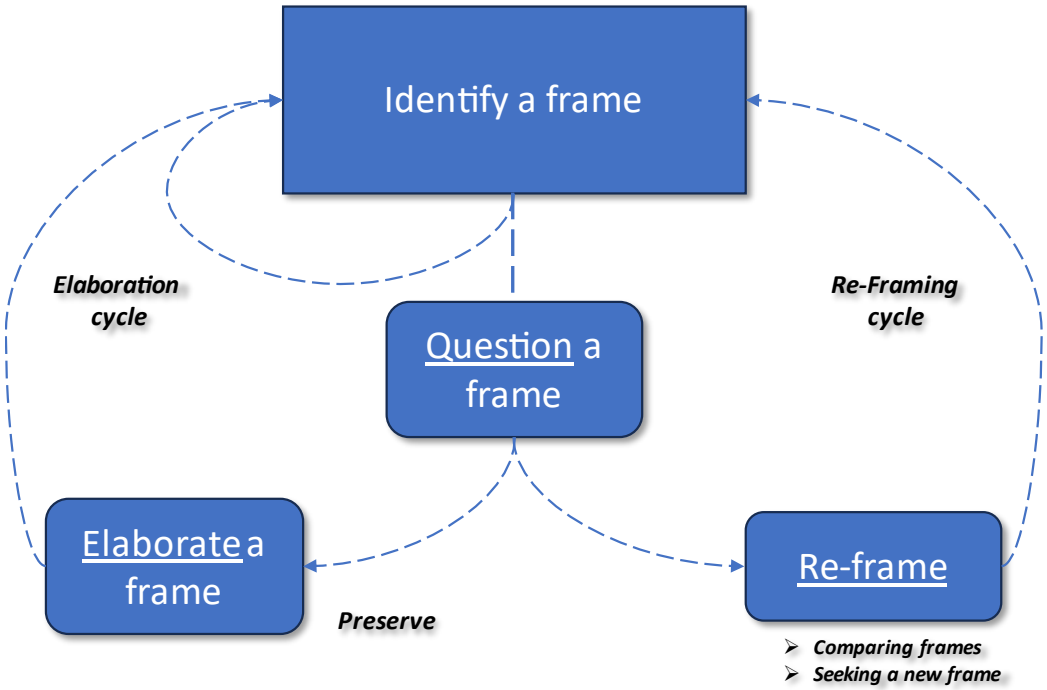


Figure 2 - The Data/Frame model (adapted from Klein, 2010)

The model of the Data/Frame theory starts with **identifying a frame**, by putting relevant data together to construct a frame, and also use this frame to gather and manage relevant data. Next, **questioning a frame** includes the tracking of anomalies, detecting inconsistencies and judging whether the data still indicate that the frame is correct or needs attention. This questioning process is usually triggered or accompanied by emotions like surprise and confusion. After questioning a frame, there are two possible cycles. The Elaboration cycle consists of **elaborating a frame** by specifically looking for missing data to craft a minor modification to the frame without altering its main features or discard irrelevant data and explain away the anomalies. Another reaction involves a more substantial change in the frame, known as the re-framing cycle. The

Reframe cycle consists of **reframing by comparing frames** and **seeking a new frame**. This can entail altering the existing frame, proposing alternative frames, and making choices between them. In extreme cases where no acceptable frames exist, sensemaking requires constructing an entirely new frame. These parts of the Data/frame theory will be elaborated on in more detail in the theoretical framework.

3.2.2 Framing in crisis situations

Klein et. al. (Klein et al., 2006b) indicate that the Data/Frame theory is both backward looking and explanatory, as well as forward looking and anticipatory. This is relevant for a crisis situation, as this connects the previous experiences of team members to the present situation and enables them to look forward into the crisis to anticipate what they can expect. This helps to identify a relevant frame for the current crisis and make sense of the situation at hand.

To be able to conduct team sensemaking in crisis situations, Klein et. al. (Klein et al., 2010) argue it's also important for a team to manage the emergent sensemaking requirements, which include data synthesis (putting all the pieces together), seeking data (coordinate on a shared intent on what data to look for), monitoring data quality (look for inconsistencies), resolving disputes, dissemination (when and what), and overhead and coordination costs (establishing and sustaining common ground) (Klein et al., 2010).

In crisis teams in the Netherlands, data synthesizers are usually the leaders of the crisis teams. They should be able to explain what kind of data they are looking for and make sure it's clear to the data seekers. In Dutch crisis teams the data seekers are usually the Information Managers, together with their information coordinators. If it's not clear what data needs to be searched for and why, it is possible that data seekers ignore or discard data that they think is irrelevant. To be able to gauge data quality, the information managers need to be alert to inconsistencies they might find. If there is a dispute, or a disagreement on how to clarify a situation, the team needs to have a strategy to deal with that. Usually in Dutch crisis teams this will be done in a collaborative way to reach consensus ("polderen"), but it is also possible to make just-in-time revisions or resolve the dispute by using hierarchical authority. After a frame is constructed and the common ground is established in a common operational picture, Dutch crisis teams in the public sector usually use the National Crisis Management System (LCMS) to disseminate their frame. Organizations in the private sector are getting on the bandwagon of LCMS as well, but also use other types of (internal) systems to support their crisis decision making process. These practices don't always connect well.

Overhead and coordination costs indicate how efficient a team can be in building, maintaining and repairing common ground and these are essential aspects to avoid losing this common ground. Because if the common ground is lost, decision-making will also break down (Klein et al., 2010). While these sensemaking requirements are important, we will not focus on those in our current study, but zoom in on framing behavior instead.

To summarize, while sensemaking as described by Weick and framing as described by Klein may have different emphases and perspectives, they share commonalities in their focus on the cognitive processes individuals use to interpret and make sense of information. Both concepts contribute to our understanding of decision-making and behavior in complex and uncertain environments and are particularly relevant within crisis contexts. We will next examine how teams use framing and sensemaking behavior to grasp an understanding of a crisis situation.

3.3 Theoretical framework for our study

The theoretical framework of the current study consists of two parts. The first part is about framing behavior that can be observed in teams during a crisis. The Data/Frame theory of Klein et al. (Klein et al., 2010) is the scientific basis for this behavior. The second part is about sensemaking questions that teams ask during a crisis meeting and if the teams show behavior on situational sensemaking, identity-oriented sensemaking and action-oriented sensemaking. The scientific basis for this part is the research conducted by Kalkman (Kalkman, 2019) on sensemaking questions asked in crisis response teams. These two frameworks are particularly valuable for addressing our specific sub-questions on the behavior that crisis teams show in a cyber crisis.

3.3.1 Observing framing behavior using the Data/Frame theory

As mentioned before in the section on framing, as part of the Data/Frame theory, Klein et. al. identify what they call emergent sensemaking strategies (Klein et al., 2010) in relation to team sensemaking behavioral markers. These behavioral markers indicate that team sensemaking is going on and can be observed in teams. Below we will elaborate on the different steps of the framework and show the behavioral markers we can use to identify if this framing behavior is present in a team.

Identifying a frame

Teams can employ different strategies to identify a frame and they are related to the team authority structure. Teams can use a bureaucratic strategy, for example by defining rules for data classification. They can use a collaborative strategy, in which te team comes to a consensus about what frame to use. And there is a hierarchical strategy, in which a leader of a team officially announces the frame.

In a cyber crisis, there are different teams working together to manage the source of the crisis and the effects. There might be differences between Incident Response teams and Crisis Response teams with regards to the team authority structure and the behavior they show on identifying a frame. Observable behavioral markers for identifying a frame are listed in the table below.

Table 1 - Behavioral markers for identifying a frame (as described by Klein et al.)

Team sensemaking strategy	Behavioral markers
Identifying a frame	Team formulates criteria or rules used to identify the frame
	A team member announces what the frame is
	Team collaborates to identify the frame

Questioning a frame

Teams can express their doubt about a frame, and this is a crucial task. To facilitate this, teams can use a number of techniques. These include designating a Devil's Advocate with the specific role of raising doubts or establish criteria for sounding alarms. This is especially relevant in cyber crises, because the situation may change suddenly and repeatedly based on findings in forensic research. There might be differences between IR and CR teams with regards to the behavior they show on questioning a frame. Observable behavioral markers for questioning a frame are listed in the table below.

Table 2 - Behavioral markers for questioning a frame (as described by Klein et al.)

Team sensemaking strategy	Behavioral markers
Questioning a frame	Appoint a team member to play devil's advocate and raise doubts about the suitability of a frame
	Team creates rules or tripwired to alert them that the frame may be unsuitable
	Team members voice and discuss what might go wrong using the current frame

Re-framing: comparing frames

When teams face multiple plausible explanations, they can utilize methods like voting, consensus-building, autocratic decision-making by the leader, rule-based approaches, or conflict resolution to settle on a single explanation. In a cyber crisis, it is important to be able to make sense of information that is non-conclusive for one specific frame, to make sure that crisis processes are not delayed. Observable behavioral markers for re-framing: comparing frames are listed in the table below.

Table 3 - Behavioral markers for re-framing: comparing frames (as described by Klein et al.)

Team sensemaking strategy	Behavioral markers
Re-framing: comparing frames	Team compares frames and votes for one
	Team forges consensus on which frame is most appropriate
	Leader announces, which frame is most appropriate

Re-framing: creating a new frame

It is hard for teams to create a new frame. Strategies to do this when someone offers a new frame is to adopt, modify or reject the new frame. Next to that, the team has the option to work together in crafting a narrative. Alternatively, team members can contribute data, opinions on data credibility, and speculate on connections and causal beliefs. The responsibility of combining these perspectives can either be assigned to the team leader or one of the team members.

During cyber crises, being able to create a new frame when the current frame is no longer valid, is an important task of a crisis team. There might be a difference in how IR and CR teams handle this, as the level of information they have might differ. There might also be differences between GOV and CI organizations, because the focus of their tasks is different. Observable behavioral markers for creating a new frame are listed in the table below.

Table 4 - Behavioral markers for re-framing: creating a new frame (as described by Klein et al.)

Team sensemaking strategy	Behavioral markers
Re-framing: creating a new frame	Individual suggests a frame and it is adopted, modified or rejected as the team compares frames
	Team speculates on data and suggests causal beliefs; leader or a team member combines viewpoints into a frame
	Team collaborates to synthesize competing frames

Elaborating a frame

After questioning the frame, a possible approach involves maintaining the existing frame, typically by providing explanations for the anomaly. Sensemaking might lead to either disregarding anomalies as minor or making minor adjustments to the frame without changing its core elements. In a cyber crisis, as new information comes in, this needs to be placed in and compared to the existing frame after questioning. There might be a difference between IR and CR teams in witnessing this behavior, as IR teams are more forensics and data-driven than CR teams, leading to less discussion on the frame. Observable behavioral markers for elaborating a frame are listed in the table below.

Table 5 - Behavioral markers for elaborating a frame (as described by Klein et al.)

Team sensemaking strategy	Behavioral markers
Elaborating a frame	Team discusses and rejects anomalous data as transiens signals or otherwise insignificant
	The team's data synthesizers direct the activities of the data collectors to seek new data to verify the frame
	The team's data synthesizers and data collectors collaborate to discover new relationships that preserve or extend the frame

To summarize, based on the Data/Frame theory we've identified behavioral markers for studying team sensemaking strategies. In the following section we'll continue to identify the behavioral markers for observing sensemaking questions asked in teams.

3.3.2 Observing sensemaking questions asked in crisis response teams

In the following paragraphs, we will briefly summarize how Kalkman defines the three types of sensemaking questions asked in teams and the behavior that can be observed in teams. This leads to working propositions we can check with the data collection and analysis of our current study.

Kalkman (Kalkman, 2019) problematizes current crisis sensemaking research, by arguing that they tend to look only at how crisis responders make sense of their surroundings, implying that situational sensemaking is enough to manage the response to the crisis. Instead, Kalkman argues that, based on his study in six terrorism response crisis exercises in Dutch crisis teams, it is also necessary to look at an identity-oriented and action-oriented types of sensemaking (Kalkman, 2019). This means that next to making sense of their immediate surroundings, it is important to take personal and team identity in consideration, as well as scripts and actions and what other organizations do and what their role in the crisis is. The three types of sensemaking questions asked in teams he suggests are elaborated below.

What connects Kalkman's view to the Data/Frame theory of Klein and to Weick's sensemaking, is that Kalkman also argues in his recent book 'Frontline Crisis Response' (Kalkman, 2023), that "if any crisis understanding is plausible and preliminary at best, responders should often act as if their operating frame is correct, while actively trying to seek indications for the opposite" (Kalkman, 2023, p. 46). Adding to that, Kalkman also specifically mentions the act of doubting sensemaking (Kalkman, 2023) as important aspect, synonymous to questioning a frame in the Data/Frame theory. This means that to be able to get a good crisis understanding based on sensemaking in a crisis team, it is necessary to keep asking yourself as a team if the current information is still plausible congruent with the identified frame. If not, it is necessary to take actions to re-frame or elaborate a frame.

According to Kalkman, when faced with a crisis, responders have to make sense of their surroundings to understand its origins, characteristics, and consequences (Kalkman, 2019). This is congruent with how other sensemaking scholars apply this to a crisis situation. Crisis sensemaking plays a crucial role in directing the execution of the response. This means that it is important to look at three types of sensemaking questions to be asked in teams: on **situational sensemaking** (what is happening in this crisis?), on **identity-oriented sensemaking** (who am I in this crisis?) and on **action-oriented sensemaking** (how do my actions matter in this crisis?).

In the next sections we will dive deeper into these three types of sensemaking questions and how they matter for our current study. We will briefly summarize what the three sensemaking questions entail and the behavior that can be observed in teams. This leads to hypotheses we can investigate with the data collection and analysis of our current study.

3.3.2.1 Situational sensemaking

Situational sensemaking consist of two parts: collecting and sharing information as a sensemaking process to reach a state of shared awareness, and afterwards negotiating this information into an agreement on how to understand this crisis information.

Information sharing commences with team members sharing information on the crisis with each other. The team members then present their information as factual and objectively as possible and attempt to create a shared image of the crisis. In this stage, the sensemaking is still relatively incomplete and will be completer and more adjusted as new information comes in.

Understanding crisis information entails making sense of the crisis' nature, causes and potential future risks. Next to that, it also examines what this means for the organization itself and which other organizations are involved. This last part, on knowing what your position is as a team within an organization and in the network of organizations working together, is what we would call network understanding. In cyber crises, this is an essential part of situational sensemaking, as a cyber crisis is complex and has a transboundary nature. The organizations you work together with may have essential information that your organization or team might need to manage the cyber crisis. Observable behavioral markers for situational sensemaking are listed in the table below.

Table 6 - Behavioral markers for situational sensemaking (based on Kalkman)

Situational sensemaking	**Behavioral markers**
Information sharing	Team members share information about the cyber crisis with each other.
	Team members present their information as factually and objectively as possible.
	The team can create a shared common understanding of the cyber crisis.
Crisis understanding	The team understands the nature of the cyber crisis.
	The team understands the cause of the cyber crisis.
	The team understands the potential future risks of the cyber crisis.
	The team understands the consequences of the cyber crisis for their own organization.
Network understanding	The team knows which other teams are involved within their own organization.
	The team knows which other organizations are involved outside their own organization.
	The team uses information from other organizations to refine or supplement their own understanding of the cyber crisis

3.3.2.2 Identity-oriented sensemaking

The question "who am I in this crisis?" is key for the part of identity-oriented sensemaking. Team members have an individual role they predominantly play in the team, and this influences the way they make sense of a crisis. In a group, the team identity is important, as it influences the way the team members together make sense of the crisis.

The individual identities Kalkman mentions are that of organizational liaison, representing a part of an organization, that of team member, with emphasis on the common goal of the team to resolve the crisis as soon and as best as possible. And finally, the role of professional/expert, in which team members, irrespective of their formal roles give a professional interpretation of the situation. Kalkman suggests that "the data demonstrate that the chosen identity guides the crisis understanding, while the crisis understanding can, in turn, guide the role one assumes. […] This serves to show that identity and crisis sensemaking mutually influence each other" (Kalkman, 2019, p. 655). There might be differences between IR and CR teams, as we expect IR teams to consist primarily of professionals/experts and CR teams primarily of organizational liaisons and team members.

The collective identity of the team is shown when the team members ask themselves what the situation at hand means to them as a team. This team role is the basis for creating a shared analysis and common operational picture of the situation and creating a plan. There might be

differences between IR and CR teams on this collective identity, as we expect that IR teams have their tasks defined more strictly and focused on cyber, as opposed to CR teams, who usually take an all-hazard generic approach based on the BOB decision making process.

Next to that, Kalkman suggests: "if this team identity remains unclear instead, an understanding of the crisis situation remains meaningless" (Kalkman, 2019, p. 655), and probably will lead to discussion on the crisis understanding and possible actions. If team identity is clear, this enables collective sensemaking. Observable behavioral markers for identity-oriented sensemaking are listed in the table below.

Table 7 - Behavioral markers for identity-oriented sensemaking (based on Kalkman)

Identity-oriented sensemaking	Behavioral markers
Individual role	Organizational liaison: represents a department within the organization
	Team member: is primarily a member of the team
	Professional/expert: is an expert in a specific subject
Team role	The team knows what their own role is in this cyber crisis
Team identity	The team has a collective identity. Team members identify with the team as a whole and have a sense of a common purpose, feeling connected to each other
	The team focuses on their own level of operation (operational, tactical, strategic)
	The team reaches a collective conclusion for which they are convened

3.3.2.3 Action-oriented sensemaking

Kalkman argues that it is important for a team to "be aware of the implications of the actions that they take" (Kalkman, 2019, p. 656), because these actions have an effect on the crisis itself. This is done in two ways, by using scripted actions like plans and procedures and by looking at the consequences of actions before implementing them.

Scripted actions like crisis plans and procedures aid crisis sensemaking, but how they are understood also influences the amount of aid they bring. A script never truly reflects the crisis at hand, this means that a generic plan always needs to be applied to the specific situation. We expect that in our study IR teams will show more behavior in using scripted actions than CR teams, as their tasks are more strictly defined.

Actions taken during a crisis influence the crisis itself and change its reality. Kalkman calls this "actions and enactment" (Kalkman, 2019). This needs sensemaking in itself, to be able to gauge the effect of certain actions on the crisis environment. We expect that in our study there might be a difference in IR teams and CR teams, as we expect that CR teams show more behavior in taking into account what other teams and organizations do in the cyber crisis. Observable behavioral markers for action-oriented sensemaking are listed in the table below.

Table 8 - Behavioral markers for action-oriented sensemaking (based on Kalkman)

Action-oriented sensemaking	Behavioral markers
Scripted actions	The team refers to or utilizes existing plans, procedures, etc.
	The team agrees on which existing plans/procedures, etc. are applicable
	The team debates conflicting plans/procedures
Actions and enactment	The team refers back to previous actions in a new meeting
	The team applies the results of previous actions to a new sense-making process
	The team takes into account what other teams (within the own organization) have done
	The team takes into account what other organizations have done

To summarize, based on the sensemaking questions asked in crisis teams by Kalkman, we've identified behavioral markers for studying team sensemaking behavior on situational sensemaking, identity-oriented sensemaking and action-oriented sensemaking. In the following

section we'll continue to summarize the hypotheses we have generated for our current study, based on the theoretical framework.

3.4 Hypotheses for our study

3.4.1 Hypotheses based on the Data/Frame theory

For the purpose of our study, we will focus on measuring the behavioral markers in team sensemaking. These can, according to Klein et al. (Klein et al., 2010), be studied under controlled conditions, or under more natural circumstances like observations of exercises like "ISIDOOR IV".

Klein et al. (Klein et al., 2010) offer several hypotheses we can examine when observing the behavioral markers of framing, providing us with literature based expectations for the in our study. We will convert these into hypotheses fitted to our current study and investigate them based on the methodology as described in the next chapter. The hypotheses cover the topics of individual roles in crisis teams, and the ability to question a frame. The hypotheses based on the Data/Frame theory are listed in the table below.

Table 9 - Hypotheses for our current study based on the Data/Frame theory (Klein et al., 2010)

Hypotheses based on Data/Frame theory	**Hypotheses for our current study**
Teams composed of highly experienced members will be more likely to question a frame than teams composed of less experienced members.	H1: Teams composed predominantly of professionals/experts will be more likely to show behavior on questioning a frame than teams composed of organizational liaisons and team members.
Teams composed of less experienced members will be more likely to accept the data provided and to explain away anomalies than teams composed of highly experienced members.	H2: Teams composed of predominantly organizational liaisons or team members will be more likely to elaborate on a frame by discussing and rejecting anomalous data as transient signals or otherwise insignificant.
Teams are unlikely to question a frame	H3: Teams are unlikely to question a frame

3.4.2 Hypotheses based on sensemaking questions asked in crisis response teams

Based on the literature on sensemaking questions asked in crisis teams, we use the following hypotheses and study them based on the methodology as described in the next chapter. The hypotheses as stated in the table below provide us with literature-based expectations for the findings in the current study on identity-oriented sensemaking and action-oriented sensemaking.

The hypotheses cover the topics of individual roles in crisis teams, team-identity and the use of scripted actions. Based on the findings of Kalkman, there are no specific hypotheses identified on situational sensemaking.

Table 10 - Hypotheses based on sensemaking questions asked in crisis response teams

Identity-oriented sensemaking	**Hypotheses for our current study**
The individual role team members assume influences the crisis understanding.	H4: teams comprised of professionals/experts show more behavior related to Crisis Understanding than teams comprised predominantly of organizational liaisons and team members
If team identity is unclear, this influences crisis understanding and actions.	H5: teams showing behavior of having a shared identity, focus on their own level of operation and coming to a shared conclusion of why they sit at the crisis table, show more behavior that indicates Crisis Understanding and Actions and Enactment
If team identity is unclear, this influences questioning a frame (Klein).	H6: teams showing behavior of having a shared identity, focus on their own level of operation and coming to a shared conclusion of why they sit at the crisis table, also show more behavior on Questioning a frame.

If team identity is clear, this influences identifying a frame	H7: teams showing behavior of having a shared identity, focus on their own level of operation and coming to a shared conclusion of why they sit at the crisis table, show more behavior on Identifying a frame
If team identity is clear, this influences the creating of a common operational picture	H8: teams showing behavior of having a shared identity, focus on their own level of operation and coming to a shared conclusion of why they sit at the crisis table, also show more behavior on being able to create a common operational picture of the cyber crisis.
Action-oriented sensemaking	**Hypotheses for our current study**
The use of scripted actions influences crisis understanding	H9: teams showing behavior that indicates they use or refer to existing plans and procedures, also show more behavior related to Crisis Understanding

In the next chapter, we will provide the method we used to collect and analyze data to render results for our research questions, taking the hypotheses above into account.

4 Method

This chapter discusses the design and methods used to generate an answer to the main research question and sub questions, based on the theoretical framework of the literature review. It starts with describing the scope of the research, and follows with the research design, methods and data analysis. It concludes with the limitations of the current study.

The goal of this research is to explore how incident response and crisis response teams use framing and sensemaking behavior to make sense of a national cyber crisis. As cyber crisis management is currently an under-researched topic, by using the context of a national cyber crisis exercise, this research can function as a benchmark or starting point for future research on cyber crisis management.

4.1 Scope of our study

The scope of this research is organizations in governmental and critical infrastructure organizations in the Netherlands. The cross-sectional study was carried out in November 2023, when the national cyber exercise "ISIDOOR IV" took place. This section will provide background on the exercise itself, explaining the context.

"ISIDOOR" is the largest national cyber crisis exercise in the Netherlands. In "ISIDOOR IV", more than 120 organizations in public and private sectors participated, with over 3000 individual participants spread over 12 different sectors (Nationaal Cyber Security Centrum, 2023). Although the evaluation is still ongoing at the time of writing this thesis, it is clear that the ISIDOOR exercises in general provide broad awareness of cyber crises impacting society physically, even though a cyber crisis is largely invisible, transboundary and effects spread quickly (Nationaal Cyber Security Centrum, 2023). This exercise also shows that to improve coordination and collaboration during a national cyber crisis, all these organizations knowing each other helps to be able to address the societal issues that can come from a large-scale cyber-attack when it really happens.

The setup of the exercise was three-fold. The main exercise takes place on three consecutive days in November and trains all participating organizations at the same time, sub-exercises that can be arranged by organizations themselves, and a specific exercise for central government, which focuses on the Interdepartmental Crisis Management Committee (ICCB). The scenario is developed as a main script that every organization follows, a sectoral script that takes the injects of the main script and develops it further for a specific sector and finally an organizational specific script if organizations need specific injects they want to train.

The general storyline encompasses a supply-chain attack by a fictitious state actor on a fictitious organization, which provides fictitious monitoring software to various organizations in

governmental and vital sectors. The state actor has been acquiring a critical position in the supply chain. The first day focuses on the operational/technical level, providing participating organizations with technical injects to chew on. The second day the threat grows, as organizations are required to scale up to their tactical crisis teams. The third day the scenario comes to an apotheosis, and the threats now affect everyone. This requires the individual organizations to scale up their strategic crisis teams and the national government will scale up their national crisis structure.

The scenario of a supply chain attack was chosen because there is an increase in hackers cooperating and applying long term strategies to influence a supply-chain (Nationaal Cyber Security Centrum, 2023). The chosen scenario also has the potential to indirectly disturb the functioning of vital processes in the Netherlands. This means the scenario provides enough impact to play on all levels of the crisis structure, from operational to political/strategical level.

4.2 Research design and methods used

Answering the main research question requires the combination of different types of research, as only data gathering through a questionnaire is not enough to describe how organizations make sense of a cyber crisis. Therefore, a mixed-methods study is conducted, to be able to both quantify the framing and sensemaking questioning behavior that is visible in teams, as well as provide a more qualitative in-depth view on this subject. This methodological triangulation (Flick, 2018) allows for putting the findings in context and provides richer data to analyze and draw conclusions from. The table below describes the purpose, approach, data collection and expected products of the study in an implementation matrix (Fetters, 2020).

Table 11 - Implementation matrix for our study

Purpose	Approach	Data collection	Products
To understand the background on cyber crises and cyber crisis management	Literature review	Search terms on "cyber AND crisis" "cyber AND crisis management" Snowball sampling	Brief overview of background on cyber crises and organization of cyber crisis management in the Netherlands
To identify relevant focus for the conducted study	Literature review	Search terms on "sensemaking OR sense making OR sense-making" "team sensemaking" "data/frame theory" Snowball sampling	Theoretical framework of sensemaking, the Data/Frame theory and sensemaking questions asked in teams.
To understand the behavior of crisis teams in relation to the Data/Frame theory	Questionnaire	N = 27	Overview of results on framing behavior observed in teams, in order to answer sub research question 1 Differences between GOV and CI groups Differences between IR and CR teams
To understand the behavior of crisis teams in relation to Sensemaking questions asked in crisis teams	Questionnaire	N = 27	Overview of results on sensemaking questions asked in teams, in order to answer sub research question 2 Differences between GOV and CI groups Differences between IR and CR teams
To understand how participants in the questionnaire view sensemaking in teams can be improved	Analysis via Gioia method	Q1: N = 19 Q2: N = 15 Q3: N = 18	Overview of results on open-ended questions how participants think sensemaking in teams, between teams and between organizations can be improved in the context of the ISIDOOR IV exercise.

To organize the results from the questionnaire and interpreting differences between GOV and CI groups and IR and CR groups	Descriptive statistics Correlations Mann-Whitney tests to compare two groups Kruskall-Wallis tests to compare more than two goups	N = 27	Overview or relevant results in terms of the research question and sub research questions 1 and 2.
To assess from a broader perspective how sensemaking in teams can be improved	Semi-structured interviews with experts on cyber incident response and cyber crisis response	N = 5	Overview of results on how experts think sensemaking of cyber crises can be improved in the Netherlands (sub research question 3)

First, a literature review was conducted, which focused on exploring the concepts of sensemaking, framing and how cyber crisis management is currently organized in the Netherlands. Based on this review, frameworks for sensemaking and framing were selected to design a questionnaire, which was distributed via Qualtrics within the group of participating organizations in the Dutch national cyber crisis exercise "ISIDOOR IV". Results were analyzed in SPSS and used to describe how participating teams during the exercise demonstrated framing and sensemaking questioning behavior during the exercise and compare differences between groups. Finally, interviews were held with experts in crisis management and incident response, to deepen the insights of the questionnaire results, using the Gioia Method (Gioia et al., 2013). Below the two main methods will be explained in more detail.

4.2.1 Questionnaire

The questionnaire was developed on the basis of two existing concepts that have been used in a crisis management context, framing and sensemaking. These concepts have been researched before, but not in a specific cyber crisis context. Also, the context of a national cyber exercise as large as "ISIDOOR IV", with 120 organizations in 12 both public and private sectors participating, has not been the focus of a study before.

By using a questionnaire, it's possible to standardize questions among pool of respondents that is too big to observe directly (Bhattacherjee, 2019), which enables comparison between groups of respondents (Young, 2015). A questionnaire is also useful to describe a phenomenon and look at relationships between variables (Young, 2015) (Bhattacherjee, 2019). It is suitable for descriptive and exploratory research.

Downsides of using a questionnaire are that it might be harder to find out what the deeper motivations behind an answer are. It's also possible that respondents do not finish the questionnaire completely (Lavrakas, 2008), for example when the list of questions is too long. And because we use an observer role to fill out the questionnaire, it might suffer from respondent bias if the observer doesn't have enough knowledge about the group they are observing (Bhattacherjee, 2019).

4.2.1.1 Inclusion and exclusion criteria

The respondents were observers of crisis teams participating in the exercise. Respondents were selected in organizations participating in national cyber exercise "ISIDOOR IV". The population contained 120 public and private organizations in 12 different sectors. Most organizations

participated with more than one crisis team, which made it possible for organizations to fill out one questionnaire per team participating.
In total 54 respondents started the questionnaire, of which 51 respondents consented to participating. Three respondents did not consent to participate and were guided to the end of the questionnaire. These responses were removed.

In the questionnaire, a pre-check question was added after the consent form, to make sure that only in "ISIDOOR IV" participating organizations would fill out the survey. Out of the 51 responses that did consent to participate, two indicated their organization did not participate in "ISIDOOR IV" and five of them did not answer this question at all. These responses were removed as well. This left 44 responses that consented to participate in the survey and were organizations that actually participated in "ISIDOOR IV". Eleven of them did not answer any further question and were excluded for that reason, which means there were in total 33 usable responses. These responses were used in the analysis. 26 of them were completely filled out, and seven of them were partly filled out, but still usable in (parts of) the analysis. This can be due to survey fatigue (Lavrakas, 2008) or simply forgetting the survey after starting it and/or being interrupted. Next to that, incorrect or more than 60% incomplete questionnaires were excluded, finalizing the number of usable questionnaires at 27, of which one was not completely filled out.

4.2.1.2 Sample

This paragraph shows the description of the participants. The main descriptives use all recorded responses (n=33), the descriptives that go more into the details or organizations only use the 26 (fully finished) or 27 (26 fully finished and 1 partly finished) responses. The n-number the analysis is based on is therefore always indicated.

The responding organizations (N = 33) were distributed over 10 different sectors. Most responses came from the Energy sector (21,2%), followed by Central Government (15,2%) and Telecom (15,2%).

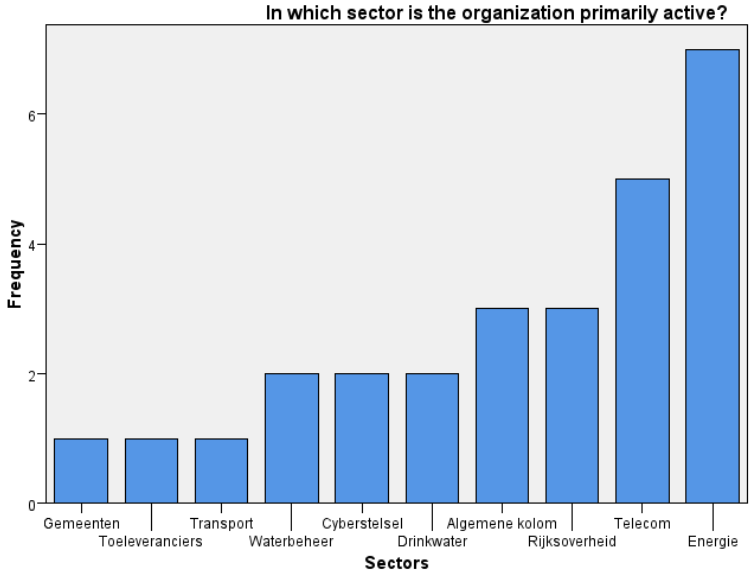


Figure 3 - Overview of participating sectors

The distribution in governmental versus critical infrastructure organizations (N = 33) was 33,3% government, and 57,6% critical infrastructure. 9,1% of the organizations represented in the survey indicated they were neither part of government nor critical infrastructure. The

responding organizations (*N* = 26) were mostly large organizations, consisting of 5000 or more employees (42,3%) or between 1000 and 4999 employees (23,1%).

Out of the organizations that took part (*N* = 26), 50% indicated their organization is part of an Information Sharing and Analysis Center (ISAC), and 38,5% indicated their organization is part of a sectoral CERT/CSIRT.

Incident response

Of the participating organizations 88,5% (*N* = 26) has an in-house incident response team, of which 34,8% (*N* = 26) use an incident response model like NIST, SANS or F3EAD. More than half of these organizations (52,2%; *N* = 26) indicate they use other ways to prepare their incident response.

When comparing the use of incident response models across all respondents (*N* = 26), NIST is used most (19,2%), and SANS comes in second (11,5%). The F3EAD model is not selected once. This can indicate organizations are not familiar the model.

15,4% of the respondents indicated their organization doesn't use an incident response model at all. More than half of the respondents (53,8%) don't know if their organization uses an incident response model or referred to '*Anders, namelijk*'. These (*N* = 5) indicated in the explanation box that they use incident response plans, (regional) crisis plans or refer to the national crisis structure.

Crisis response

Of the respondents (*N* = 26), 80,8% indicate their organization has a crisis organization that is a separate entity from the regular, standing organization. Half of the respondents (50%) indicate that their organization uses the netcentric way of working during a crisis. 30,8% responded that they use a hierarchical way of working and 7,7% use an opportunistic way of working.

When zooming in on the organization's vision on information management during a crisis, we find that 38,5% look at this from an information warehouse perspective, and 34,6% from a trading zone perspective. If we look at the organizations that use the netcentric way of working during crises, 61,5% of them look at crisis information management from an information warehouse perspective. This is in line with the current way of looking at a common operational picture, which lies at the heart of netcentric operations. Of the organizations that use the hierarchical way of working during crises, 50% indicate that they look at crisis information management from a trading zone perspective.

Teams observed

Taking into account all 27 respondents who answered the team related questions, 40,7% observed an IR team and 51,9% observed a CR team. Zooming in on the CR teams, 25,9% was a tactical team, 18,5% a strategic team and 7,4% a political team. 'Anders, namelijk' was selected twice (7,4%) and in the open question to explain this choice, one of the respondents indicated that the whole of operational/technical teams within their organization was observed, and the other respondent indicated that the team observed was a tactical-strategic team.

The analysis showed that the formal goal of the team observed was for the most part (55,6%) focused on Crisis Response. Incident response came in second at 22,2% and Incident Handling was mentioned 14,8%. 'Anders, namelijk' was selected twice (7,4%) and in the open question to explain this choice, one of the respondents indicated the formal role of the team was "to make strategic decisions" and the other respondent indicated the formal role of the team was

"to mainly test the incident response plan, but also look at communication, stakeholder management etc.".

4.2.1.3 Data collection strategy

To reach the desired population, the researcher contacted the National Cyber Security Center (NCSC-NL) as organizer of the exercise for assistance a few months in advance. The following arrangements were made. The organizer acts as liaison between the researcher and the respondents. The researcher then provides the NCSC with information (e-mail with instructions and ethical information brochure, see appendix) for two groups. The first group consisted of exercise leaders of participating organizations. They need to know that this research is taking place, why it's done and what I need from their organization (that is: monitoring that observers of their crisis teams fill out the questionnaire). The second group consists of observers of crisis teams of participating organizations. They need to know what they need to do (that is: fill out the questionnaire)

Before the exercise started on Monday November 13th, both groups are to be informed through the organizer. During and after the exercise, multiple reminders will be sent out to the participating organizations via organizer.

Starting Monday November 13th, the questionnaire opened at 8:00hrs and observers could fill out the questionnaire either during the exercise or thereafter. The questionnaire closed on December 5th at 17:00hrs.

Crisis! Setbacks in the strategy

Reaching the participating organizations proved to be challenging, as "ISIDOOR IV" is an exercise that needs to remain under the radar. This is partly because not all of the organizations that participate in the exercise want to make it known that they are participating, and partly because the organizers want to keep the communication about the exercise under their control.

Before the exercise took place, researcher reached out to the organizers to ask them to collaborate with me in reaching out to the participants. About a week before the exercise started organizers agreed on sending a prepared e-mail as described above to the participating exercise leaders and the observers of the participating organizations. This was cancelled four days before the exercise started and replaced by referring to the research in the newsletter to the exercise leaders. The researcher prepared a short message for the newsletter and in the end the newsletter aired without the message in it.

On the first day of the exercise, the researcher arranged with the organizer's contact person that he would send out a message with the link to the questionnaire to the Signal group of sectoral exercise leaders. He agreed to do this on all three exercise days. In the end, this was only done on Monday and Wednesday.

Also, the organizer's contact person agreed on publishing the link to the questionnaire in the newsletter to the exercise leaders on the Monday after the exercise. In the end, the newsletter was published on the Thursday after the exercise had ended.

This led the researcher to do two things. First, the researcher e-mailed the participating organizations she had in her own network, asking for their co-operation and sending the questionnaire also to their contacts. Second, the researcher published a total of three LinkedIn posts (see appendix), on November 23rd, November 29th and December 5th, asking observers of participating organizations' teams to fill out the questionnaire.

Before November 23rd, there were only two responses. After the e-mails and the LinkedIn posts aired, the responses went up drastically. This shows that it was necessary to use a different strategy than collecting responses through the organizers.

The LinkedIn posts were removed on December 6th, as the deadline for filling out the questionnaire was December 5th.

4.2.1.4 Measurements

The core of the questionnaire was built around the concepts of team sensemaking behavioral markers as described by Klein et al. (Klein et al., 2010) and sensemaking questions asked in crisis response teams as described by Kalkman (Kalkman, 2019). The behavioral markers as described in the sections on the theoretical framework were translated into questions for the observers of crisis teams that participated in "ISIDOOR IV". This led to the operationalization of the framing behavioral markers and sensemaking questions behavioral markers. Next to these observations, questions on organizational demographics and relevant crisis management related topics were asked, to be able to compare different groups. The full questionnaire can be found in the appendix.

4.2.2 Semi-structured interviews

After the questionnaire, semi-structured interviews with experts were held to be able to place the results of the questionnaire in a broader context of cyber crisis management in the Netherlands and to elaborate on challenges and necessary developments to further the area of cyber crisis management. Interviews can provide more depth of information about a phenomenon, leading to a greater understanding how the participants view this phenomenon (Billups, 2021). Because they are interactive, it's possible to ask interviewees to clarify responses and offer insights that might not be captured in alternative methods.

4.2.2.1 Sample

The interviews were held with two types of experts (N = 5). The first group contained experts with a main focus on crisis management consultancy (N = 3), who have from that perspective developed their work into the field of cyber crisis management. The second group contained experts with a main focus on incident response consultancy (N = 2), who have from that perspective developed their work into the field of cyber crisis management. This was done to prevent a single viewpoint from clouding the analysis and conclusion. All interviewees were part of organizations that have a long-standing reputation in incident response and crisis response consultancy. In the table below an overview of the interviewees is given.

Table 12 - Overview of interviewees

Expert group 1 – crisis management view	
Organization	Interviewee
AON Global Risk Consulting	*Hoofd Risk & Resilience AON Global Risk Consulting (CR1)*
COT	*Directeur COT Instituut voor Veiligheids- en Crisismanagement (CR2)*
Berenschot	*Managing consultant (Strategisch) adviseur en Project- en programmamanager Digitale Veiligheid (CR 3)*

Expert group 2 – incident response view	
Organization	Interviewee
Fox-IT	*Sr. Business Security Consultant Practice lead crisis readiness (IR1)*
Northwave	*Operational lead cyber resilience (IR2)*

4.2.2.2 Data collection strategy

The interview respondents were sourced by contacting people in the organizations that were connected to the researcher. These contact persons were asked which persons in their organization were working on the topic of cyber crisis management. The prospective interviewees were then approached to participate in the study via e-mail. All of them responded positively to the subject of the research and agreed to participate.

4.2.2.3 Measurements

The interviews were conducted in a semi-structured way, providing the interviewees with the same three main interview questions as described in the table below. The interview questions were asked in Dutch, as the interviewees were Dutch-speaking. A translation of the questions into English is provided in the table as well.

Table 13 - Interview questions

Interview question 1	Hoe geven de organisaties waar je mee werkt betekenis/duiding aan een cyber crisis? Welk gedrag laten zijn zien met betrekking tot framing? Welke soort duidingsvragen stellen zij? *How do the organizations you work with give meaning/interpretation to a cyber crisis? What behaviors do they exhibit in terms of framing? What kind of interpretation questions do they ask?*
Interview question 2	Welke uitdagingen zie je op het gebied van betekenis/duiding geven aan een cyber crisis? Waar komt dat door? *What challenges do you see in providing meaning/interpretation to a cyber crisis? What causes these challenges?*
Interview question 3	Hoe zou betekenis/duiding geven aan een cyber crisis kunnen worden verbeterd? Op team/organisatie/inter-organisatie niveau? *How could providing meaning/interpretation to a cyber crisis be improved? At the team/organization/inter-organization level?*

The first interview question was asked to gather additional data to the questionnaire on framing and sensemaking questions. The second and third question were aimed at answering SQ3.

The interviews were held in the period of 8-15 December and took place digitally. All interviews lasted between 30 and 75 minutes. The interviews were held digitally, and the researcher made use of Microsoft Teams to record the interviews and have them automatically transcribed. The transcription of each interview and the notes that were taken during the interview were combined to a summary per interview. These summaries were sent to the interviewees to review and correct if necessary. The reviewed summaries were used for further analysis. The full interview protocol can be found in the Appendix.

4.3 Data analysis

4.3.1 Questionnaire

The responses from the questionnaire were analyzed by using SPSS to make descriptive analyses and correlations. Because of the number of responses, due to the specific target group and limited cooperation of the organizer of the exercise, it was not possible to do regular statistical tests, as the sample didn't have a normal distribution. Instead, the researcher used the Mann-Whitney and Kruskall-Wallis non-parametric tests.

For analysis purposes, a number of new variables were created. These included totals for the questions on framing behavior and sensemaking questions asked. Next to that, new variables were created to be able to establish groups for comparison. See the table below for an overview.

Table 14 - variables created on framing behavior

Variables created on framing behavior	Purpose
F_ID_Total_Selected	Ability to identify a frame total score on all items (max = 3)
F_Q_Total_Selected:	Ability to question a frame total score on all items (max = 3)
F_Com_Total_Selected:	Ability to compare frames total score on all items (max = 4)
F_Crea_Total_Selected:	Ability to create a new frame total score on all items (max = 3)
F_Ela_Total_Selected:	Ability to elaborate on a frame total score on all items (max = 3)
Framing_Total:	total score of all items within framing behavior (max = 16)

The variable Comparing_frames 4 was removed, as it resembled too much Comparing_frames 1. Also, it was never chosen.

Table 15 - variables created on sensemaking questions asked

Variables created on sensemaking questions asked	Purpose
SitSens_IS_Tota_Selected l:	total score on all items (max = 3)
SitSens_CU_Total_Selected:	total score on all items (max = 4)
SitSens_NU_Total_Selected:	total score on all items (max = 3)
SitSens_Total_Selected:	total score on all SitSens items (max = 10)
IDSens_Team_id_total_Selected:	total score on all items (max = 3)
ActSens_SA_total_Selected:	total score on all items (max = 3)
ActSens_AE_Total_Selected	total score on all items (max = 4)

In our study, we want to compare differences between certain groups. We are interested in establishing if there are differences between governmental organizations (GOV) and critical infrastructure organizations (CI) on the one hand and if there are differences between incident response teams (IR teams) and crisis response teams (CR teams).

Governmental organizations in our study are local, regional and national government organizations. Critical infrastructure organizations in our study are defined by using the vital processes framework of the NCTV (Ministerie van Justitie en Veiligheid, 2023).

IR teams are teams that have a capability to "rapidly detect incidents, minimize loss and destruction, mitigate the weaknesses that were exploited, and restore IT services" as defined by NIST (Cichonski et al., 2012). CR teams are teams that have a capability to manage the effects of a crisis, both internal to the business continuity of the organization and external to the organization by employing stakeholder management and crisis communications. These teams can be formed on operational, tactical and strategic level.

In governmental organizations, a political level is added that focuses on "coordination of and decision-making with an urgency of the whole of the measures, facilities, regulations and perspectives for action that the central government takes in collaboration with those involved public and private partners in a situation where the national security is or may be at risk or in the event of a different situation, which has a major impact on the society exists or may exist" (Ministerie van Justitie en Veiligheid, 2022a).

The variable 'GOV or CI' was created to be able to compare organizations in government and critical infrastructures. The measures were defined based on the answers participants gave on the "In which sector are you active?" question. These were checked with the formal definition of the current vital processes in the Netherlands, as communicated by the NCTV (Ministerie van Justitie en Veiligheid, 2023) and based on the sectoral categorization NCSC has made for the "ISIDOOR IV" exercise. This led to the definition of three variables: 'government', 'critical infrastructure' and 'other'. See the table below how the distribution over the groups was made.

Table 16 - Variable to compare government and critical infrastructure organizations

Variable name: Gov or CI		
GOV	**CI**	**Other**
Algemene kolom	Energie	Cyberstelsel
Rijksoverheid	Telecom	MKB
Gemeenten	Transport	Attributie & opsporing
	Haven	Zorg
	Luchtvaart	Anders, namelijk
	Drinkwater	
	Waterbeheer	
	Chemie	
	Nucleair	
	Financiën	

The variable 'IR or CR team' was created to be able to compare Incident Response teams that focus on a technical and operational level, to Crisis Response teams, which focus more on the tactical, strategic and political level. The measures were based on the variable 'Type of team observed'. See the table below how the distribution over the groups was made.

Table 17 - Variable to compare IR and CR teams

Variable name: IR or CR team		
IR	**CR**	**Other**
Technical/operational	Tactical	Anders, namelijk
	Strategic	
	Political	

When zooming in the predominant role of the team members, we found that IR teams mostly consisted of Professionals/experts (90,9%; $N = 11$) and CR teams mostly consisted of Team members (42,9%; $N = 14$) and Organizational Liaisons (35,7%; $N = 14$). This indicates that CR teams are more varied in the roles they have at the table than IR teams.

The variable 'Uses IR model' was created to be able to compare organizations that use an IR model to those that do not use an IR model or don't know if it's used. The new variable was based on the variable IR_model. This led to 3 values: 'yes', 'no' and 'other'. 'Yes' contained the answers 'SANS', 'NIST' and 'F3EAD', 'No' consisted of the answer 'no' and 'Other' consisted of the answer 'Ik weet het niet' and 'Anders, namelijk'. See the table below how the distribution over the groups was made.

Table 18 - Variable to determine if any type or IR model is used

Variable name: Uses IR model		
Yes	**No**	**Other**
SANS	No	Anders, namelijk
NIST		Ik weet het niet
F3EAD		

4.3.2 Semi-structured interviews

The responses from the interviews were analyzed by first using Microsoft Teams to automatically transcribe the recordings. This, together with the notes that were taken during the interviews, was summarized and sent out for review by the interviewees. After this review, the summaries were analyzed through the Gioia Method, which allows us to develop rigorous qualitative data analysis

(Gioia et al., 2013). The basis for the Gioia Method lies in a well-specified, but general research question, the use of multiple data sources and semi-structured interviews (Gioia et al., 2013).

The Gioia method provides a structured way to analyze qualitative data, and fits in the constructivist approach of doing research (Gioia et al., 2013). It also fits the perspective of sensemaking, which is a constructivist concept as well, in which people use their thoughts and actions to explain their surroundings to make sense of a situation. And finally, as Gioia et al. state "we [as researchers] are pretty knowledgeable people too" and are able to find patterns in data and arrange them into concepts and relevant relationships and terms (Gioia et al., 2013, p. 17).

The Gioia Method works from analyzing the interviews and coming up with a number of first order concepts. These are arranged into second order themes and those will lead to the conceptual level of aggregate dimensions. The authors call this a data structure, which enables a researcher to think in terms of theoretical concepts, instead of methodologically "to see those transcripts and notes as more than page after page of work" (Gioia et al., 2013, p. 21).

With the data structure prepared, it's possible to come to a grounded theory model which shows the dynamic relationships between concepts that describe the subject. In the results chapter, the findings of te survey study and interviews will be combined to answer the main research question and sub-questions.

4.4 Reliability and validity

4.4.1 Reliability

Reliability and validity are critical considerations in assessing the quality of research that has been carried out. Reliability refers to the consistency of the measurement tool, indicating the extent to which the research produces consistent results over time or across different conditions. A reliable questionnaire should for example generate similar outcomes when administered under similar circumstances and tells you something about the reproducibility of a measurement.

Reliability for the questionnaire in this research was reached by using existing measures for both concepts of framing behavior and sensemaking questions.

Reliability for the interviews in this research was reached by partly using the same questions that were also asked as open-ended questions in the questionnaire. This helps to compare the views of participating organizations to the views of the experts that were interviewed. The interviews were conducted in the same consistent way.

4.4.2 Validity

Validity is about how accurately the chosen method measures what it intends to measure. Content validity ensures that the questionnaire adequately covers all relevant aspects of the construct, while criterion-related validity assesses the correlation between the questionnaire and an external criterion. Construct validity, the most complex type, explores the theoretical underpinnings of the measured construct.

For the questionnaire, construct validity in this research was assessed by using existing measures for both concepts of framing behavior and sensemaking questions. These concepts come from existing theory and knowledge and in the questionnaire exactly described behaviors and questions are used.

Content validity for the questionnaire in this research was assessed by zooming in on the framing and sensemaking subjects in the literature review, allowing the researcher to pinpoint a

specific topic on these subjects. Due to the scope and timeline of the research, other aspects of sensemaking, like for example distributed sensemaking, were excluded.

Criterion related validity was not possible to be assessed due to the scope of the research. There is no other questionnaire available on this topic that is considered a gold standard and could be used as a comparison.

4.5 Limitations

In the questionnaire, there was a potential for response bias, where respondents may have provided socially desirable responses or inaccurately represent their true opinions and behaviors. This has been mitigated as much as possible by asking observers to rate if certain behavior was seen in a team.

Surveys can lack depth in understanding complex phenomena, due to the limitation for participants to elaborate on their responses. This has been mitigated by adding interviews as a second research method.

The fact that the sample of the survey is small, is a limitation that jeopardizes the generalizability of the study. Therefor the data-analysis has produced mainly descriptive results and results on non-parametric tests. This limitation has been mitigated by adding a second research method in the form of semi-structured interviews.

5 Results

In this chapter, the results of the questionnaire and semi-structured interviews are presented. They will follow the structure of the sub research questions and conclude with the findings on the main research question. Before elaborating on the main findings in relation to the research questions, the questions are shown, as well as an overview of the hypotheses based on the literature review.

In this study, we've formulated a main exploratory research question (MRQ) and three sub-questions (SQ), as repeated in the table below. The answer to the MRQ will be provided by looking at two SQ's focusing on a part of the main research question. The third SQ is formulated to explore possible challenges and necessary improvements on sensemaking in the context of a national cyber crisis.

Table 19 - Overview of research questions

	Research question
MRQ	*How do incident response and crisis response teams of organizations in critical infrastructure and governmental organizations use framing and sensemaking behavior to make sense of a (national) cyber crisis in the Netherlands?".*
SQ1	*What framing behaviors do incident response and crisis response teams of organizations in critical infrastructure and governmental organizations demonstrate when framing and making sense of a national cyber crisis, including how they identify, question, reframe, and elaborate on frames?"*
SQ2	*"How do crisis teams utilize questioning strategies to understand and navigate a national cyber crisis, considering situational sensemaking, identity-oriented sensemaking, and action-oriented sensemaking?"*
SQ3	*"What are the challenges and necessary improvements with regards to making sense of a (national) cyber crisis?"*

The hypotheses we've found in the literature review are listed again in the sections on results. We will report the findings on them in both the questionnaire results and the interview results. The comparison between the groups of GOV and CI organizations and between IR and CR teams are added as well. In the following sections, the results on the questionnaire and the semi-structured interviews are presented.

5.1 Results on questionnaire

The questionnaire was live on Qualtrics between November 13th and December 5th, 2023. In the dataset, the cases are selected to be able to compare the group of government organizations (GOV) with critical infrastructure organizations (CI) and Incident Response teams (IR) with Crisis Response teams (CR). In the comparison, we look at the totals of the framing behaviors to see if there are any noticeable differences. We also examine the correlations between the concepts.

In this section we will present the outcomes of the questions on the Data/Frame theory and the outcomes of the Sensemaking Questions Asked in Crisis Response Teams. After providing an overview of the relevant results, correlations and hypotheses we will indicate other relevant results we've found.

5.1.1 Results on Data/Frame theory

The findings on the Data/Frame theory give an overview of how the sample, including the groups we've defined, show framing behavior based on the Data/Frame theory.
To examine if respondents have observed at least one of the indicators of framing behavior, we use the totals of the concepts, as indicated in the table below. This will give us an overview of the differences between the defined groups in terms of the behavior they show on the framing concepts.

Table 20 - Percentages indicating at least one of the underlying aspects was selected

	General		**GOV**		**CI**		**IR**		**CR**	
Concept	N	%	N	%	N	%	N	%	N	%
Identifying a frame	27	96,3	7	100,0	17	100,0	11	100,0	14	92,9
Questioning a frame	27	37,0	7	42,9	17	41,2	11	18,2	14	42,9
Re-frame by comparing frames	27	55,6	7	42,9	17	64,7	11	36,4	14	64,3
Re-frame by seeking a new frame	27	40,7	7	42,9	17	47,1	11	45,5	14	28,6
Elaborate a frame	27	63,0	7	71,4	17	58,8	11	54,5	14	71,4

To examine where we can find the possible differences between groups, the following table shows the results of the behaviors that were measured per question.

Table 21 - Results on framing behavior per question

		General		**GOV**		**CI**		**IR**		**CR**	
Concept	Behavior	*N*	%	*N*	%	*N*	%	*N*	%	*N*	%
Identifying a frame	The team has formulated criteria or rules to identify the frame.	27	55,6	7	71,4	17	52,9	11	72,7	14	50,0
	A team member announced what the frame is.	27	51,9	7	57,1	17	52,9	11	36,4	14	57,1
	The team collaborates to identify the frame.	27	63,0	7	57,1	17	76,5	11	54,5	14	64,3
Questioning a frame	The team selects a team member to take on the role of the devil's advocate and express doubts about the suitability of the frame.	27	7,4	7	14,3	17	5,9	11	9,1	14	7,1
	The team establishes rules or criteria to alert them that the frame may not be suitable.	27	7,4	7	14,3	17	5,9	11	9,1	14	0,0
	Team members express and discuss potential issues with the current frame.	27	33,3	7	42,9	17	35,3	11	18,2	14	42,9
	The team compares frames and ultimately decides to vote for one.	27	3,7	7	0,0	17	5,9	11	9,1	14	0,0

Re-frame by comparing frames	The team reaches a consensus on which frame is most suitable.	27	37,0	7	28,6	17	47,1	11	27,3	14	50,0
	The team chairperson announces which frame is deemed most appropriate.	27	29,6	7	28,6	17	29,4	11	27,3	14	21,4
Re-frame by seeking a new frame	A team member proposes a frame, and it is either adopted, modified, or rejected as the team compares frames.	27	18,5	7	14,3	17	23,5	11	27,3	14	14,3
	The team speculates about data and suggests causal beliefs (beliefs someone holds about the causal relationships between events); the team chairperson or a team member combines these viewpoints into a frame.	27	33,3	7	28,6	17	41,2	11	45,5	14	14,3
	The team collaborates to assemble competing frames.	27	11,1	7	28,6	17	5,9	11	18,2	14	7,1
Elaborate a frame	The team discusses and dismisses deviations in the data as transient signals or otherwise insignificant.	27	7,4	7	0,0	17	11,8	11	9,1	14	7,1
	The team's data processors (e.g., information officers) direct the activities of data collectors (other teams or individuals outside the team) to search for new data to verify the frame.	27	59,3	7	71,4	17	52,9	11	54,5	14	64,3
	The team's data processors and data collectors work together to discover new relationships that maintain or expand the frame.	27	37,0	7	42,9	17	29,4	11	45,5	14	28,6

5.1.1.1 Relevant results on framing behavior

The above results indicate that nearly all types of teams showed behavior on Identifying a frame (96,3%; *N* = 27). This means that in most cases, teams were able to identify a frame that fit the cyber crisis at hand. In the interviews, this is supported by the statement that framing is visible on tactical and strategic levels (IR1), behavior on identifying a frame is always visible (IR2). Identifying a frame is enabled by exercising (IR2), asking the right questions (IR2) and having affinity with the digital domain (IR2).

What stands out is that the results on showing behavior on Questioning a frame were much lower when looking at the totals. **This means the results support H3** and indicates that questioning a frame might be harder for teams to do. The respondents indicated that the teams showed less behavior on the question if the team appoints a devil's advocate role and the question on if the team establishes rules or criteria to alert them that the frame may not be suitable. If we look at the interviews for support on these findings, we see a difference. As some interview respondents indicated, behavior on questioning a frame is always visible (IR2) and goes well (IR2).

Especially in the IR group (18,2%, *N* = 11), the rates of questioning a frame were low. **This means the results do not support H1**. The interview respondents did indicate that framing between IR and CR teams is different (CR3), and that IR teams frame based on knowledge and experience (CR3).

5.1.1.2 Comparing groups

There were noticeable differences between the GOV and CI groups and IR and CR groups on framing behavior, but Mann-Whitney U tests indicated that these were not significant. This might be due to the small sample size. Below an overview of the comparisons between the groups and possible explanations of why these results were found is given.

GOV versus CI

Both GOV (100,0%; *N* = 7) and CI group (100,0%; *N* = 17) score high on behavior showing they identify a frame. There are no noticeable differences on questioning a frame and re-framing by seeking a new frame.

When we look at the findings in the CI group, we see that Re-framing: comparing frames is observed more in the CI group (64,7%; *N* = 17) than in the GOV group (42,9%; *N* = 7). This is the case for all questions within Re-framing: comparing frames. Especially on the question on the team coming to a consensus of which frame is most appropriate, the CI group (47,1%; *N* = 17) shows more behavior than the GOV (28,6%; *N* = 7) group. Based on these findings it is unclear why.

The GOV group score a little higher (71,4%; *N* = 7) on elaborate a frame than the CI group (58,8%; *N* = 17). This is especially so on the question on the team's data processors directing the activities of data collectors to search for new data to verify the frame (GOV 71,4%; *N* = 7 and CI 52,9%; *N* = 17) and the question on the team's data processors and data collectors working together to discover new relationships that maintain or expand the frame (GOV 42,9%; *N* = 7 and CI 29,4%; *N* = 17). This might be due to the vision on information management.

IR versus CR

We find that IR teams show behavior that demonstrates they identify a frame. This was selected 100,0% (*N* = 11). This was selected 92,2% (*N* = 14) in the CR group, this is a little lower than in the IR teams.

Questioning the frame behavior was quite low in IR teams at 18,2% (*N* = 11) when compared to the CR teams (42,9%, *N* = 14). This might be due to the fact that CR teams are more used to ask what the crisis at hand means to them, because they us the BOB-process to guide them through their meetings. This is supported by the interviewee's, who indicated that in a mature organization, CR teams go through all framing steps as these are hidden in meeting structure (BOB-process) (CR3).

Behavior observed on Re-framing: comparing frames was observed a lot less in IR teams (36,4%; *N* = 11) than in CR teams (64,3%; *N* = 14). This was mostly due to the scores on the question on the team coming to consensus on which frame is the most appropriate. CR teams showed a lot more behavior on that particular aspect than IR teams. This might be explained by the focus of the teams, in which the IR teams focus more on forensic evidence, indicating that there is not much to discuss on in terms of consensus. Insights from recovery and forensics can cause the frame to be adjusted a few times in the first days in IR teams (IR2), which supports this explanation.

Re-framing: selecting a new frame behavior was observed slightly more in IR teams (45,5%; *N* = 11) than in CR teams (28,6%; *N* = 14). The differences were true for all questions on this aspect. This might be explained by the focus of the teams as well, in which the CR teams work on a tactical level and depend less on the raw data of the forensics process, but focus on the effects of the cyber crisis. Interview respondents indicated that asking the right questions supports readjusting a frame (IR2) and that openness to readjusting a frame is essential, based on insights from the IR team (IR2).

Behavior observed on Elaborating on a frame was also seen more in CR teams (71,4%; *N* = 14) than in IR teams (54,5%, *N* = 11). When zooming in on the question about the team discussing and dismissing deviations in the data as transient signals or otherwise insignificant, the difference between IR (9,1%, *N* = 11) and CR (7,1%; *N* = 14) teams is a lot less visible. **This renders H2 inconclusive**. An explanation of this finding might be that there is a disbalance in

the questions asked by CR teams to IR teams on what information they need to elaborate on a frame, and IR teams work together better to find out new relations that keep or elaborate the frame.

5.1.1.3 Correlations on framing behavior

Correlations between concepts were measured using the Pearson-correlation. There is a significant strong positive correlation (r = .532; p = .004; N = 27) between the concepts of Questioning the frame and Comparing frames in general. This means that if the score on questioning a frame increases, the score on Reframing: comparing frames also increases. Although we can't say test if this correlation can have a causal relationship, due to the small sample size, we can say that these variables are related. It is possible that other variables can play a role in this correlation as well, which needs to be examined in future research.

The significant positive relation between Questioning the frame and Comparing frames is also found in the IR teams (r = .624; p = .040; N = 11) and GOV group (r = 1.000; p = < .001; N = 7) and is found to be stronger.

There is a significant strong positive correlation between the concepts of Questioning a frame and Elaborating on a frame in the CR group (r = .548; p = .043; N = 14). This means that if the score on Questioning a frame increases, the score on Elaborating on a frame also increases.

5.1.1.4 Results on open-ended questions

The questionnaire contained an open-ended question if there was anything else the observers noticed about the team on the topic of framing. The responses (N = 6) varied. Four of the responses were relevant to the framing behavior observed. Two of the respondents (OEF1, OEF2) mentioned specifically that the observed teams, both on operational and strategic level, didn't *consciously* identify a frame, but concentrated on events, consequences and actions. The observers indicated that this might have been due to the team members who naturally jump quickly from the imagination phase ('*beeldvorming'*) to actions ('*besluitvorming'*), without paying attention to the judgement phase ('*oordeelsvorming'*) in which framing has a place.

One respondent (OEF6) indicated that the frame was constructed by a specific role. A similar comment was made by another respondent (OEF5) who indicated that much of what is discussed during the crisis team meeting had been prepared by a scenario team that is separate from the crisis team. Framing had mostly been done by that team.

5.1.1.5 Summary

In summary, there are differences between the groups in terms of framing behavior, but they are not significant. The results do suggest a significant, positive correlation between Questioning the frame and Comparing frames in the general and IR group, and between Questioning the frame and Elaborating a frame in the CR group.

In the literature review, we've identified three hypotheses in relation to framing behavior, and checked whether they could be supported or not. This is summarized in the table below.

Table 22 – Support for hypotheses based on literature review

Hypotheses based on Data/Frame theory	Supported or not?
H1: Teams composed predominantly of professionals/experts (IR teams) will be more likely to show behavior on questioning a frame than teams composed of organizational liaisons and team members (CR teams).	**Not supported**

H2: Teams composed of predominantly organizational liaisons or team members (CR teams) will be more likely to elaborate on a frame by discussing and rejecting anomalous data as transient signals or otherwise insignificant.	**Inconclusive**
H3: Teams (general) are unlikely to question a frame	**Supported**

If we examine SQ 1, we can conclude that in general all underlaying concepts of framing behavior are demonstrated in teams, but not every concept in the same amount, as shown in the figure below.

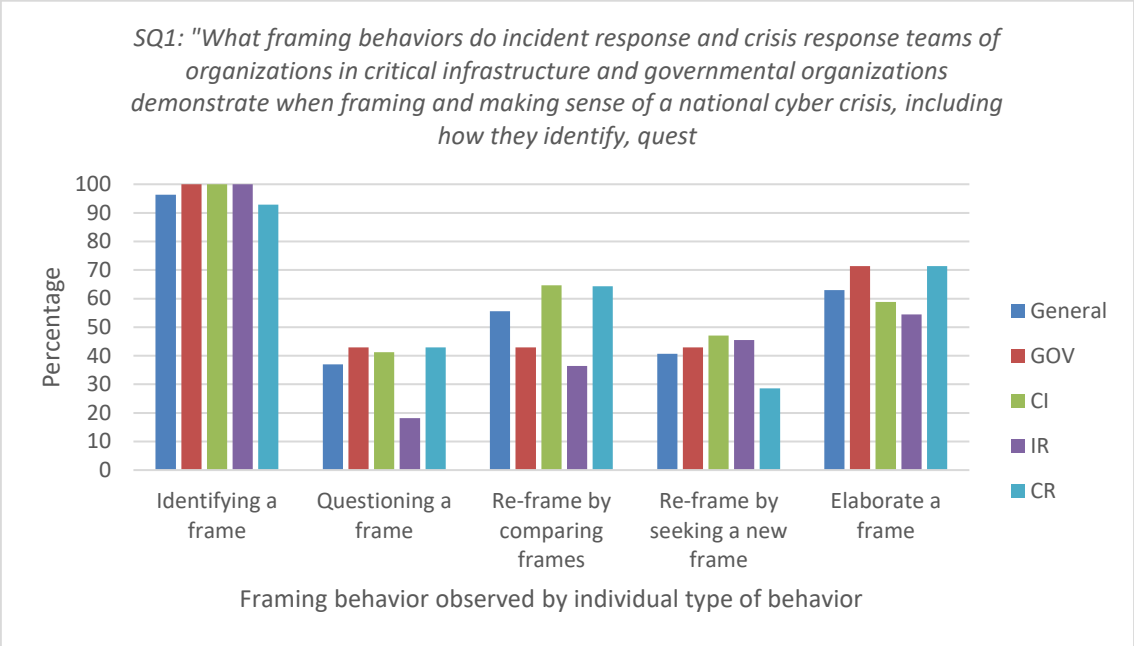


Figure 4 - Answer on sub-question 1

Identifying a frame is done by almost all observed teams, but the other behaviors are observed considerably less and vary between groups. The behavior on questioning a frame is observed the least in general, but in IR teams this behavior is absent most of the time. There are noticeable differences between GOV and CI teams on Re-framing by comparing frames and Elaborating a frame, none of which are significant.

5.1.2 Results on Sensemaking questions asked in crisis response teams

In this section, the results on Sensemaking questions asked in teams are presented. They zoom in on the three concepts of sensemaking as described by Kalkman: situational sensemaking, identity-oriented sensemaking and action-oriented sensemaking. First, the results of the general group are presented, followed by the results of the GOV vs CI group and the IR vs CR teams' group. The findings on the Sensemaking questions asked in crisis response teams give an overview of how the sample, including the groups we've defined, utilize questioning strategies to understand and navigate a national cyber crisis, considering situational sensemaking, identity-oriented sensemaking, and action-oriented sensemaking and enable us to answer SQ2.

To examine if respondents have observed at least one of the indicators of sensemaking questions, we use the totals of the concepts, as indicated in the table below. This will give us an overview of the differences between the defined groups in terms of the behavior they show on the sensemaking questions concepts.

Table 23 - Percentages indicating at least one of the underlying concepts was selected

		General		GOV		CI		IR		CR	
Dimension	**Concept**	**N**	**%**	**N**	**%**	**N**	**%**	**N**	**%**	**N**	**%**
Situational sensemaking	Information sharing	27	100,0	7	100,0	17	100,0	11	100,0	14	100,0
	Crisis understanding	27	96,3	7	85,7	17	100,0	11	100,0	14	92,9
	Network understanding	27	81,5	7	85,7	17	76,5	11	63,6	14	92,9
Identity-oriented sensemaking	Team identity	27	96,3	7	100,0	17	94,1	11	90,9	14	100,0
Action-oriented sensemaking	Scripted actions	27	81,5	7	100,0	17	76,5	11	90,9	14	78,6
	Actions and enactment	27	96,3	7	100,0	17	94,1	11	90,9	14	100,0

To examine where we can find the possible differences between groups, the following table shows the results of the behaviors that were measured per question.

Table 24 - Results on sensemaking questions asked in crisis response teams per question

Dimension: Situational sensemaking		**General**		**GOV**		**CI**		**IR**		**CR**	
Concept	**Behavior**	**N**	**%**	**N**	**%**	**N**	**%**	**N**	**%**	**N**	**%**
Information sharing	The team members share information about the cyber crisis with each other.	27	100,0	7	100,0	17	100,0	11	100,0	14	100,0
	The team members present their information as factually and objectively as possible.	27	70,4	7	85,7	17	64,7	11	72,7	14	71,4
	The team can create a shared common understanding of the cyber crisis.	27	85,2	7	85,7	17	82,4	11	63,6	14	100,0
Crisis understanding	The team understands the nature of the cyber crisis.	27	88,9	7	71,4	17	100,0	11	100,0	14	78,6
	The team understands the cause of the cyber crisis.	27	48,1	7	42,9	17	52,9	11	81,8	14	14,3
	The team understands the potential future risks of the cyber crisis.	27	63,0	7	71,4	17	64,7	11	54,5	14	64,3
	The team understands the consequences of the cyber crisis for their own organization.	27	81,5	7	85,7	17	82,4	11	72,7	14	85,7
Network understanding	The team knows which other teams are involved within their own organization.	27	66,7	7	42,9	17	76,5	11	45,5	14	78,6
	The team knows which other organizations are involved outside their own organization.	27	48,1	7	57,1	17	41,2	11	27,3	14	57,1
	The team uses information from other organizations to refine or supplement their own understanding of the cyber crisis.	27	66,7	7	85,7	17	52,9	11	45,5	14	85,7

Dimension: Identity-oriented sensemaking		**General**		**GOV**		**CI**		**IR**		**CR**	
Concept	**Behavior**	**N**	**%**	**N**	**%**	**N**	**%**	**N**	**%**	**N**	**%**
Individual role	Organizational liaison: represents a department within the organization.	27	22,2	7	28,6	17	17,6	11	0,0	14	35,7
	Team member: is a primary member of the team.	27	25,9	7	0,0	17	35,3	11	9,1	14	42,9
	Professional/expert: is an expert in a specific subject.	27	51,9	7	71,4	17	47,1	11	90,9	14	21,4
Team role	The team knows what their own role is in this cyber crisis.	27	81,5	7	71,4	17	88,2	11	81,8	14	78,6
Team Identity	The team has a shared identity. The team members identify with the team as a whole	27	66,7	7	71,4	17	70,6	11	100,0	14	71,4

	and have a sense of a common purpose, feeling connected to each other.										
	The team focuses on their own level of operation (operational, tactical, strategic).	27	77,8	7	71,4	17	88,2	11	72,7	14	78,6
	The team reaches a collective conclusion for which they are sitting at the table.	27	55,6	7	71,4	17	52,9	11	27,3	14	78,6
Dimension: action-oriented sensemaking		**General**		**GOV**		**CI**		**IR**		**CR**	
Concept	**Behavior**	**N**	**%**	**N**	**%**	**N**	**%**	**N**	**%**	**N**	**%**
Scripted actions	The team refers to or utilizes existing plans, procedures, etc.	27	70,4	7	85,7	17	70,6	11	72,7	14	71,4
	The team agrees on which existing plans/procedures, etc. are applicable.	27	55,6	7	71,4	17	52,9	11	45,5	14	64,3
	The team debates conflicting plans/procedures.	27	22,2	7	14,3	17	23,5	11	45,5	14	7,1
Actions and enactment	The team refers back to previous actions in a new meeting.	27	81,5	7	57,1	17	88,2	11	63,6	14	92,9
	The team applies the results of previous actions to a new meaningful process.	27	59,3	7	57,1	17	64,7	11	36,4	14	71,4
	The team takes into account what other teams (within their own organization) have done.	27	81,5	7	85,7	17	82,4	11	72,7	14	85,7
	The team takes into account what other organizations have done.	27	66,7	7	71,4	17	64,7	11	54,5	14	71,4

5.1.2.1 Relevant results on sensemaking questions asked in teams

The above results indicate that in general all types of teams showed a lot of behavior on the dimensions of Situational sensemaking, Identity-oriented sensemaking and Action-oriented sensemaking. This is not a surprise, as the respondents have observed crisis teams, and these are the types of questions that are asked in crisis response teams. However, if we zoom in on the different groups, there are differences to be seen as we'll discuss below.

5.1.2.2 Comparing groups

There were noticeable differences between the GOV and CI groups and IR and CR groups on sensemaking questions asked, and Mann-Whitney U tests indicated that some of these outcomes were significant. Below an overview of the comparisons between the groups and possible explanations of why these significant results were found is given.

GOV and CI groups

There was no significant difference found between GOV and CI groups. An interesting result however was found in the concept of Crisis Understanding, on the question if the team understands the nature of the cyber crisis. The result of the CI group (100,0%; $N = 17$) was a lot higher than the result of the GOV group (71,4%; $N = 7$), although this was not significant ($U = 42.500$, $p = .076$).

IR and CR groups

In the IR teams versus CR teams, there were several significant findings in all three dimensions on sensemaking questions asked in teams. Below we will examine them per dimension. On the question of the team debating on conflicting plans/procedures, an interesting result was found that the results of the IR team group (45,5%; $N = 11$) were almost significantly higher ($U = 47.500$, $p = .056$) than the results of the CR team group (7,1%; $N = 14$). This means that IR teams were observed to debate more on conflicting plans and procedures. A possible explanation might be

that on an operational level, the plans and procedures are more detailed, which can lead to more discussion.

Situational sensemaking

On creating a shared common operational picture of the cyber crisis, it was found that the results of the CR team group were significantly higher than the results of the IR team group (U = 49.000, p = .026). This means that it is no coincidence that the CR team group scored higher (100,0%; N = 14) on being able to create a shared image of the cyber crisis (63,6%; N = 11). As CR teams usually use the BOB-process as guidance for their crisis meetings, the underlying aspects of creating a shared image are hidden in the meeting structure already, making it easier to get to a shared understanding. This finding is also supported by the interviews, as one interviewee stated that situational awareness among operational teams is low and difficult to train (CR2).

On understanding the cause of the cyber crisis, it was found that the results of the IR team group (81,8%; N = 11) were significantly higher (U = 25.000, p = .001) than the results of the CR team (14,3%; N = 14) group. This means that it is no coincidence that the IR team group scores higher on understanding the cause of the cyber crisis. This might be explained by the fact that IR teams consist predominantly of Professionals/experts (90,9%; N = 11) who have a more thorough understanding of cyber security in general than members of CR teams. This is also supported by an interviewee stating that crisis understanding by specialists/professionals is high (CR3).

If we look at the differences of IR teams (100,0%; N = 11) and CR teams (92,9%; N = 14) overall on the concept of Crisis understanding, the results do not differ a lot. If we zoom in on the different questions asked, we see that IR teams score higher on understanding the nature and cause of the cyber crisis, and CR teams score higher on understanding the effects of the cyber crisis for their own organization and understanding the potential future risks of the cyber crisis. **H4 is therefore inconclusive.** This is mainly due to the formulation of the hypothesis, which is in retrospect too broad.

Overall, the results indicate that CR teams are more frequently observed than IR teams on the concept of network understanding. However not significant, this is not a strange outcome, as CR teams focus more on their surroundings within and outside of their organization and IR teams focus more on fixing the problem at hand and doing technical and forensic research.

Identity-oriented sensemaking

On the role individual team members predominantly assume in their teams, it was found that the differences between IR team group and CR team group were significant (U = 21.000, p = < .001). This is also significant when looking at the individual types of teams (H(4) = 11.334, p = .009). This means that it is not a coincidence that in IR teams the role of individual team members is predominantly that of Professional/expert (90,0%; N = 11) and that in CR teams the predominant role is a combination of Organizational liaison (35,7%; N = 14) and Team member (42,9%; N = 14). This is a logical outcome when we look at the goal of the teams. IR teams focus more on the operational level, technical problem and solutions (as indicated as well by interviewee IR1), in which experts are needed to understand the cause and nature of the cyber crisis. CR teams on the other hand focus more on the tactical and strategic level, focusing on business impact and impact external to the organizations (IR1), indicating that there is a higher need for Organizational

liaisons who can make sense of the effects of the cyber crisis on the organization, and team members that support the decision-making process.

On coming to a shared conclusion of why they are at the crisis table, it was found that the results of the CR team group were significantly higher than the results of the IR team group ($U = 37.500$, $p = .017$). This is also significant when looking at the individual types of teams ($H(4) = 10.861$, $p = .014$). This means that it is not a coincidence that CR teams score higher (78,6%; $N = 14$) on reaching a shared conclusion on why they sit at the crisis table than IR teams (27,3%; $N = 11$). This can be explained again by the BOB-process that is used to structure the crisis team meetings. One of the steps is establishing what the team is here for.

Action-oriented sensemaking

On action-oriented sensemaking, no significant findings were found. This can be due to the fact that not every organization uses plans and scripts, as indicated in the interviews (IR2). Some operational teams use quick reference cards for specific scenario's (IR1). Another interviewee indicated that tactical and strategic teams need reassurance on that there are plans available to guide management on operational and tactical level (IR1), but scenarios described in playbooks don't always have to be the same in the cyber crisis reality (CR3).

There were two open-ended questions asked on which other teams within the organization a team takes into consideration, and which other organizations a team takes into consideration. The results are shown in the tables below.

Table 25 - Other teams within organization taken into consideration

Operational teams ($N = 7$)	**Tactical teams ($N = 7$)**	**Strategic, political and other teams ($N = 9$)**
Tactical teams (3x)	Operational teams (4x)	Operational teams (6x)
Strategic teams (2x)	Strategic teams (3x)	Tactical teams
Regular organization	Regular organization	Communication (2x)
Communication	Communication (3x)	CSIRT
	None	Various (not specified)
		Relevant ministries
		Sector

Operational teams ($N = 7$) mainly take the tactical and strategic teams within their organization into consideration. Tactical teams ($N = 7$) mainly take the operational, strategic and communication teams within their organization into consideration. Strategic, political and other teams ($N = 9$) mainly take the operational and communication teams within their organization into consideration. This might be explained by the crisis management organizational structure.

Table 26 - Other organizations taken into consideration

Operational teams ($N = 8$)	**Tactical teams ($N = 7$)**	**Strategic, political and other teams ($N = 9$)**
None	NCSC (3x)	Sector (3x)
NCSC	Sector (4x)	Relevant ministries (3x)
Contractors	Other CISO's	NCSC (3x)
Sector	LOCC (2x)	Police
Sectoral CERT	NKC	NRN
Various (not specified)	NCC	Intelligence services
Source experts (Sysmetrics)	Sectoral ISAC	Various (not specified)
	Sectoral CERT	Contractors
	Customers	Customers
		CERT
		None

Operational teams (N = 87) mainly take sectoral organizations and NCSC into consideration. This might be because they want to find out if other organizations within the sector are having the same issues and try to collaborate on finding a solution. Tactical teams (N = 7) mainly take NCSC, sectoral organizations and Landelijk Operationeel Coordinatie Centrum (LOCC) into consideration, this might be explained by their focus on the effects of the cyber crisis and the need for coordination with other organizations on managing those effects and sharing relevant information.
Strategic, political and other teams (N = 9) mainly take the sectoral, NCSC and relevant ministries into consideration. This is logical due to their level of operation.

5.1.2.3 Other significant results

If we look at the total sample, there are more significant results to identify. We will describe them below.

Type of team observed

When examining the results between types of teams (operational, tactical, strategic, political and other), we see they significantly differ on five specific concepts. On the concept of understanding the nature of the cyber crisis, a significant difference was found (H = 17.643, p = .010, df = 4) between teams. Operational, strategic and other teams are more observed to show the most behavior on this concept than tactical and political teams.

On the concept of understanding the cause of the crisis, a significant difference was found (H = 15.060, p = < .001, df = 4) between teams. Operational teams are more observed to show the most behavior on this concept than tactical, strategic and political teams. This can be explained by the formal goal of the operational teams to do Incident Response.

On the concept of the team knowing which other organizations are involved in the cyber crisis, a significant difference was found (H = 8.988, p = .043, df = 4) between teams. Political teams are the most observed on this concept than any other team. This is not a surprise, given the inter-organizational level these teams operate on.

Differences between sectors

A Kruskall-Wallis test indicated that teams in the Gemeenten, Telecom and Transport sectors show significantly more behavior on understanding the cause of the cyber crisis (H(9) = 14.061, p = .046). The data also indicate that teams in the Algemene kolom, Cyberstelsel, Drinking water and Transport sectors show significantly more behavior on understanding which other teams are involved in their own organization (H(9) = 14.919, p = .036).

Use of crisis management system

We were interested in what the results of using a crisis management system would have on sensemaking questions observed in teams and ran a Kruskal-Wallis test to test this. As it turned out, organizations using either LCMS or another CMS showed the most behavior on the team identity concept of reaching a collective conclusion for which they are sitting at the table. This was a **significant result** (H(3) = 10.455, p = .004). Teams using either LCMS or another CMS

also showed the most behavior on agreeing on which existing plans and procedures apply to the current cyber crisis. This was a significant result (H(3) = 7.155, p = .039).

Use of IR model

We were also interested if the use of an IR model would show differences on sensemaking questions asked in teams. A Kruskal-Wallis test indicated that teams using the NIST IR model significantly scored higher on understanding the cause of the cyber crisis (H(4) = 10.921, p = .015) and debating on conflicting plans/procedures (H(4) = 12.271, p = .009).

5.1.2.4 Correlations on hypotheses based on literature review

To find out if the hypotheses related to sensemaking questions asked are supported or not by our findings, we use a correlation analysis.

For teams showing behavior of having a shared identity, there was no correlation found with Crisis understanding and Actions and Enactment, rendering **H5a unsupported**, and Identifying a frame, meaning **H7a was not supported as well**. These concepts are not related in our study. There was nearly a significant moderately positive correlation found between teams showing behavior of having a shared identity and behavior of Questioning the frame (r = .380; p = .051; N = 27) and of the team being able to create a common operational picture (r = .369; p = .059; N = 27), which we will consider **H6a and H8a to be inconclusive**. Further research might elaborate on this possible correlation.

No significant correlations were found between with teams showing a focus on their own level of operation and Crisis Understanding and Actions and Enactment, which means **H5b is not supported**, Questioning a frame, which means **H6b is unsupported**, Identifying a frame, which means **H7b is not supported** and the ability to create a common operational picture of the cyber crisis, which means **H8b is not supported** as well. These concepts are not related in our study.

No significant correlations were found between teams showing behavior of coming to a shared conclusion of why they sit at the crisis table and Crisis Understanding and Actions and Enactment, which means **H5c is not supported**, Questioning a frame, which means **H6c is unsupported**, Identifying a frame, which means **H7c is not supported** and the ability to create a common operational picture of the cyber crisis, which means **H8c is not supported** as well. These concepts are not related in our study.

There is also no evidence for a significant correlation between teams showing behavior that indicates they use or refer to existing plans and procedures and Crisis Understanding, **which means H9 is not supported**. These concepts are not related in our study.

5.1.2.5 Summary

To summarize, as we see in the figure below, teams in all groups show behavior on situational, identity-oriented and action-oriented sensemaking to understand and navigate a national cyber crisis, therewith answering SQ2. The concept of network understanding received the lowest scores in comparison to the other concepts, especially in IR teams. This indicates that it is necessary to keep practicing in national cyber crises, to raise this level, as network understanding is essential for inter-organizational sensemaking.

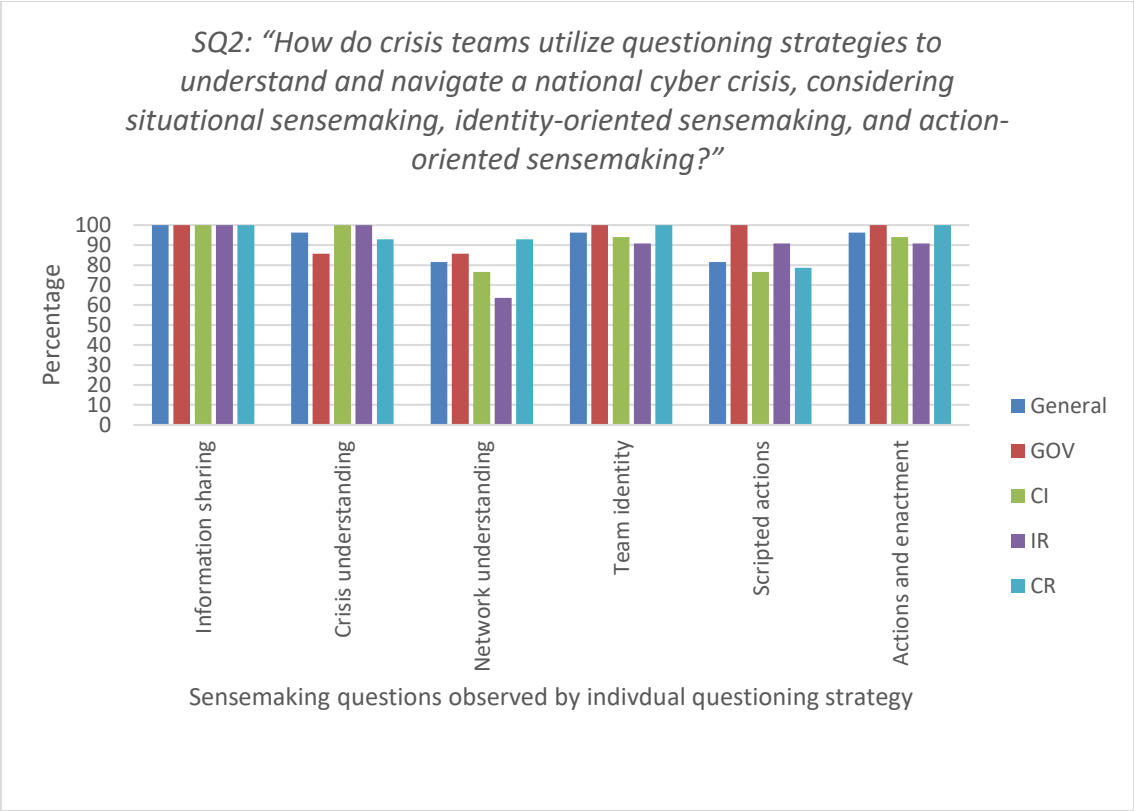


Figure 5 - Results on SQ2

There was no significant difference found between GOV and CI groups. In the IR teams versus CR teams, there were several significant findings in all three dimensions on sensemaking questions asked in teams. Next to looking at the overall concepts, we've also used Kruskal-Wallis tests to examine specific questions like type of team observed, differences between sectors, use of crisis management systems and use of IR model.

In the following table an overview is given of the proving or disproving of the hypotheses based on the literature review. Three hypotheses (H4, H6a and H8a) are deemed inconclusive, as they did show a positive correlation, but had a p-value just above .05. This means further research is necessary to be able to get to a conclusive answer on the correlation between these variables, preferably with a larger sample. The other hypotheses were disproved.

Table 27 - Results on hypotheses based on literature review

Hypotheses on Identity-oriented sensemaking	**Supported or not?**
H4: teams comprised of professionals/experts (IR teams) show more behavior related to Crisis Understanding than teams comprised predominantly of organizational liaisons and team members (CR teams)	**Inconclusive**
H5a: teams showing behavior of having a shared identity, show more behavior that indicates Crisis Understanding and Actions and Enactment	**Unsupported**
H5b: teams showing behavior of focus on their own level of operation, show more behavior that indicates Crisis Understanding and Actions and Enactment	**Unsupported**
H5c: teams showing behavior of coming to a shared conclusion of why they sit at the crisis table, show more behavior that indicates Crisis Understanding and Actions and Enactment	**Unsupported**
H6a: teams showing behavior of having a shared identity, also show more behavior on Questioning a frame.	**Inconclusive**
H6b: teams showing behavior of having a focus on their own level of operation, also show more behavior on Questioning a frame.	**Unsupported**
H6c: teams showing behavior of why they sit at the crisis table, also show more behavior on Questioning a frame.	**Unsupported**
H7a: teams showing behavior of having a shared identity, show more behavior on Identifying a frame	**Unsupported**

H7b: teams showing behavior of focus on their own level of, show more behavior on Identifying a frame	**Unsupported**
H7c: teams showing behavior of why they sit at the crisis table, show more behavior on Identifying a frame	**Unsupported**
H8a: teams showing behavior of having a shared identity, also show more behavior on being able to create a common operational picture of the cyber crisis.	**Inconclusive**
H8b: teams showing behavior of focus on their own level of operation, also show more behavior on being able to create a common operational picture of the cyber crisis.	**Unsupported**
H8c: teams showing behavior of why they sit at the crisis table, also show more behavior on being able to create a common operational picture of the cyber crisis.	**Unsupported**
Hypotheses on Action-oriented sensemaking	
H9: teams showing behavior that indicates they use or refer to existing plans and procedures, also show more behavior related to Crisis Understanding	**Unsupported**

In the next section, we will give an overview of the findings on the open-ended questions in the questionnaire. The results on the questions on how to improve sensemaking on team, organizational and inter-organizational level will be compared with the results of the same questions in the semi-structured interviews.

5.2 Results on open-ended questions of questionnaire

In this section, the results of the open-ended questions about improving sensemaking in cyber crisis situations are presented. There were three open-ended questions, which asked how respondents would improve sensemaking of a cyber crisis at the **team level**, **organizational level** and **between organizations**. The following paragraphs will summarize the answers. For analysis purposes, the questions were treated as if they were interview questions and analyzed by using the Gioia Method's coding scheme of first order concepts and second order themes to finally reach aggregated dimensions. These dimensions give us insight into the topics that respondents consider important for improving sensemaking on either team, organizational or inter-organizational level. The completed data structures as a result of the steps in the Gioia Method are presented as well. Conclusions on SQ3 relating challenges to and improvements on sensemaking in teams, organizations and between organizations will be presented in the section on the results of the interviews.

5.2.1 Improving sensemaking of a cyber crisis on team level

The visual data structure below represents the results of the open-ended question (N = 19) on how sensemaking of a cyber crisis can be improved at team level.

There are five aggregate dimensions found, being preparation, information management, crisis processes, plans and procedures, communication and effects and scenarios.

This means that respondents consider improvement on a broad spectrum: starting with the preparation phase which contains not only training, exercising and sharing knowledge before an incident occurs, but also attention for role separation in terms of clear mandates and making sure that one role does not have to be present in two separate teams. Another aspect on preparation respondents notice, but considered during a crisis, is that of personally preparing yourself before entering a crisis team meeting, by making sure all analyses are done before entering the meeting.

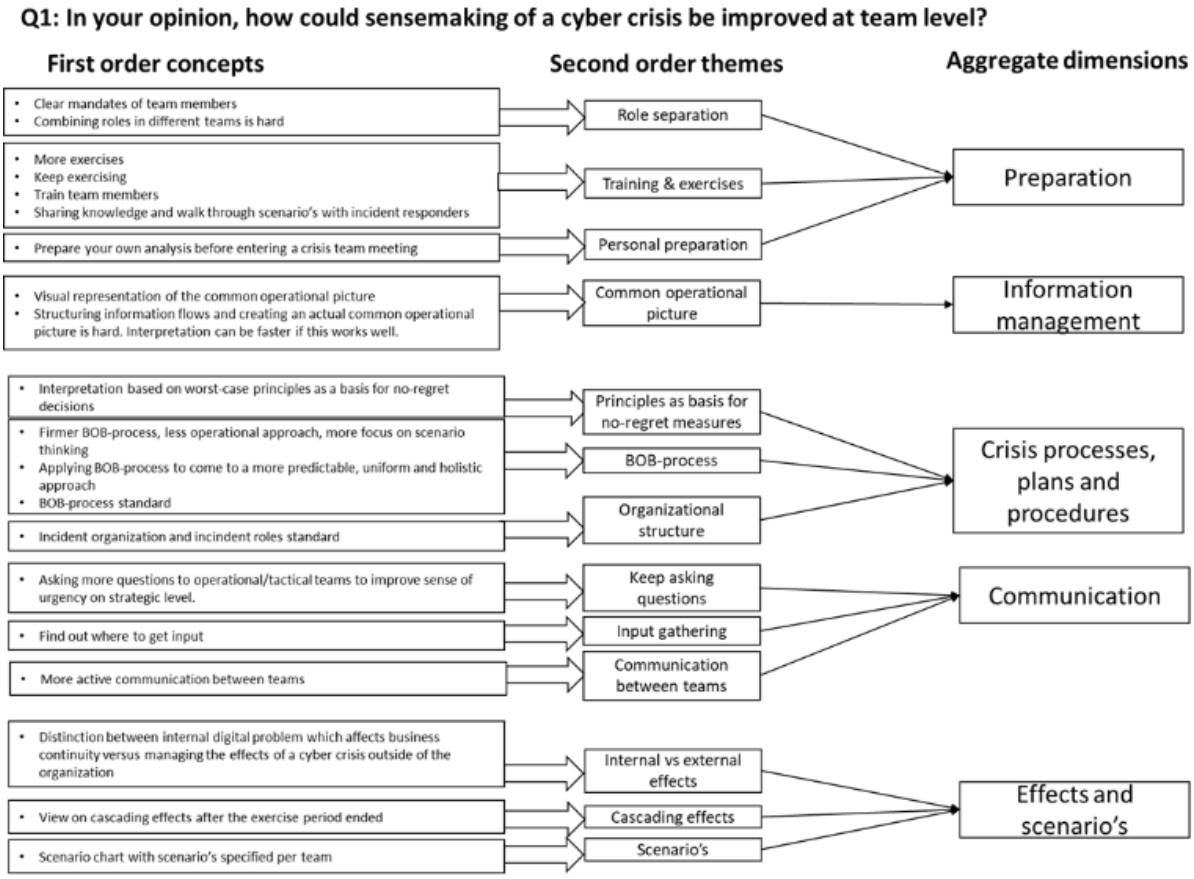


Figure 6 - Data structure on improving sensemaking of a cyber crisis on team level

Crisis processes, plans and procedures are a next step in making sure an organization is able to improve team sensemaking. A clear and standardized organizational structure and a firmly rooted decision-making process (BOB-process) ensure that sensemaking has its place in the crisis meetings. Placing this into context with predefined (worst-case) principles as a basis for sensemaking, makes sure that no-regret measures are taken.

Moving to the cyber crisis situation itself, we see that three dimensions are key. It is important to have a broad overview of what can happen to their organization, and this can be seen in the second order themes as well. An overview of internal vs external effects helps focusing the teams effort into business continuity aspects or into managing the effects of a cyber crisis outside of their organization. For this, a broad spectrum of scenario charts specified per team can be defined beforehand to help understand and make sense of the situation at hand. Another aspect respondents mention is that of bringing in a view of cascading effects that occur after the exercise period has ended, to help focus on a longer-term view inside the team.

And to bring all this information together, to be able to make a common operational picture (COP) of the cyber crisis as a periodic snapshot of the sensemaking process, the respondents suggest the following on the information management dimension. Make a visual representation of the COP that is available to everyone who works on the crisis and structure the information flows. Sensemaking will benefit from this in terms of speed.

And last but not least, communication is essential to improve sensemaking at team level. As we have seen in the results of the questionnaire, the team members can have different individual roles and therefore a different level of understanding a cyber crisis. This means it's important to keep asking questions, find out where to get relevant input and keep in touch with

all teams working on the cyber crisis. This improves sensemaking at team level and also aids in creating the right sense of urgency on a strategic level.

5.2.2 Improving sensemaking of a cyber crisis on organizational level

The visual data structure below represents the results of the open-ended question (N = 15) on how sensemaking of a cyber crisis can be improved at organizational level.

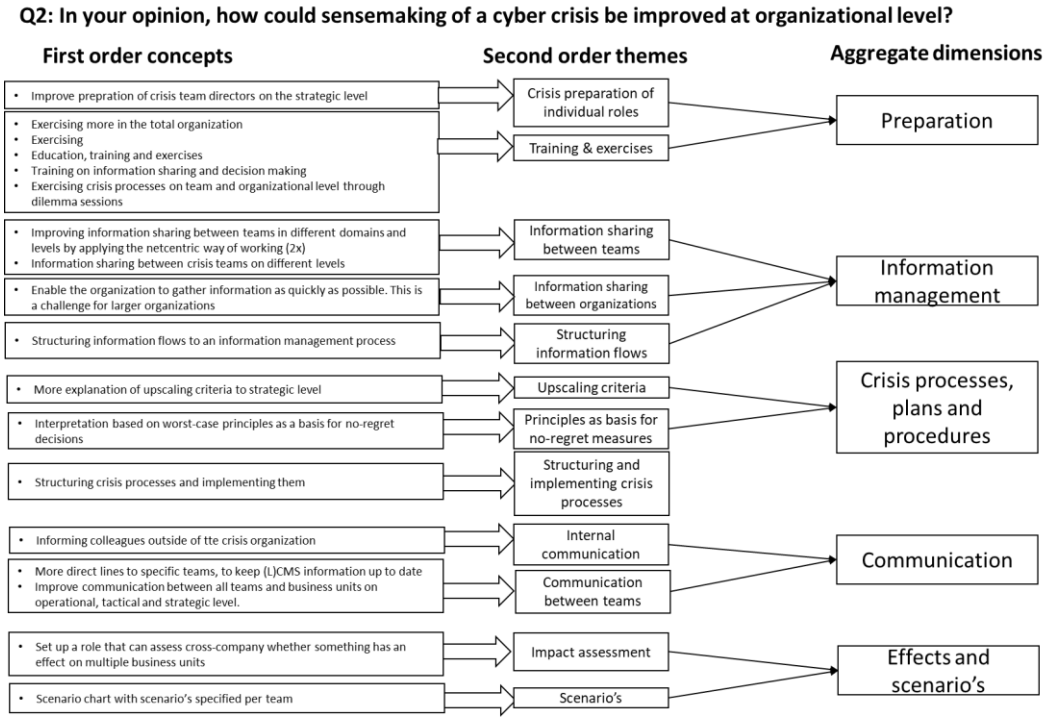


Figure 7 - Data structure on improving sensemaking of a cyber crisis on organizational level

The same 5 aggregate dimensions are found as in the first question, being preparation, information management, crisis processes, plans and procedures, communication and effects and scenario's. The second order themes and first order concepts vary. Again, we see a broad spectrum of possible improvements, from preparation phase to actual cyber crisis management.

On the dimension of preparation, respondents indicate that next to education, training and exercises, it is important to improve the preparation of crisis team directors on the strategic level. This is not specified further.

On the information management dimension, we see that structuring information flows is mentioned, but next to that the main improvement points are on information sharing between teams and between organizations. Implementing the netcentric way of working to improve information sharing between teams is mentioned twice. Information sharing between organizations can be improved by enabling organizations to gather information as quickly as possible. This was especially mentioned in the context of a national organization that needs to get information from the regional level.

The dimension of communication again shows that improvements can be made on more direct lines between teams and business units on all levels. Next to that, the importance of internal communication is mentioned, regarding informing colleagues outside of the crisis organization about what's going on.

5.2.3 Improving sensemaking of a cyber crisis on inter-organizational level

The visual data structure below represents the results of the open-ended question (N = 18) on how sensemaking of a cyber crisis can be improved between organizations.

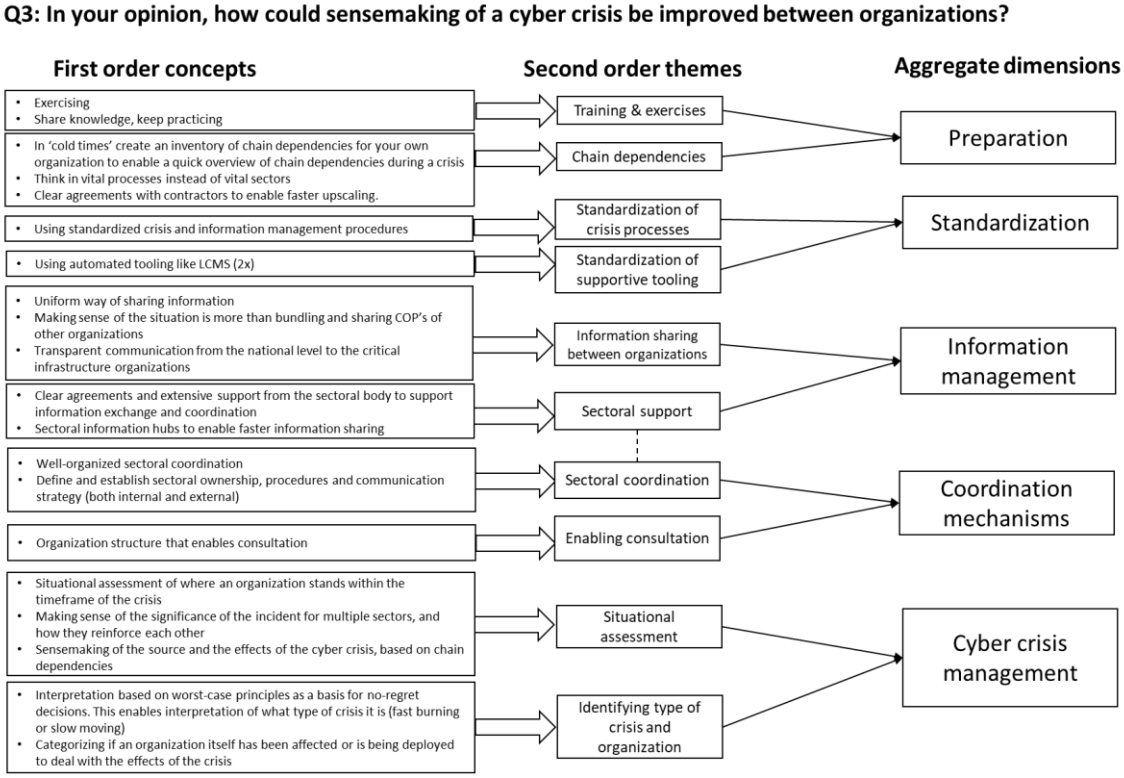


Figure 8 - Data structure on improving sensemaking of a cyber crisis on inter-organizational level

The aggregate dimensions on improving sensemaking between organizations are partly the dimensions that have been named in the previous two sections, preparation and information management. There are however three new aggregate dimensions found, being standardization, coordination mechanisms and cyber crisis management.

In the dimension of preparation, again training and exercise is mentioned to enable knowledge sharing and keep practicing with cyber scenario's. Besides that, there is a second order theme identified named chain dependencies, as multiple respondents have indicated that in this specific scenario (and most likely this is applicable to other types of cyber crises as well), it is important to create an inventory of chain dependencies before a cyber crisis hits, to be able to generate a quick overview during the crisis. It is also deemed important to have clear agreements with contractors to enable faster upscaling. And finally, it is noted that thinking in vital processes instead of vital sectors is important to get a better overview of the possible impact and cascading effects.

On the dimension of standardization, the respondents name standardization of crisis processes and information management procedures and standardization of supportive tooling like for example a crisis management system.

On the dimension of information management, there is once again attention for information sharing between organizations, like we have observed in the previous two questions. There is a call for a uniform way of sharing information, which connects with the standardization of crisis processes as well. Also, respondents deem it important to note that sensemaking is more than just bundling information and sharing common operational pictures from other organizations. Next to that, the importance of transparent communication between national

government and critical infrastructure organizations is noted. Another topic that is mentioned is about sectoral information hubs that could enable faster information sharing between organizations and the importance of clear agreements and need for support from the sectoral bodies to enable information exchange and coordination.

This sectoral coordination connects to another aggregate dimension: coordination mechanisms. Respondents indicate that it is important to have well-organized sectoral coordination and a well-defined and established sectoral ownership, so cyber crisis procedures and cyber communication strategy can also be synchronized. Another theme is that of enabling consultation. Organization structures should enable this.

The last aggregate dimension found is named cyber crisis management, as this one contains themes and concepts that are specific for cyber crises. A situational assessment is deemed important by respondents and specifically mentions where the organization stands within the timeframe of the crisis. There can be a difference between organizations in this case, as several organizations might already experience effects of the cyber-attack and some may not, or not yet. Another factor to consider here is the significance of the incident for multiple sectors and how cascading effects might develop. Sensemaking of the sources and effects of the cyber crisis based on the prepared chain dependencies is also mentioned by respondents. Identifying the type of crisis and organization is the last theme. This includes respondents mentioning that it is important to be able to gauge if a cyber crisis renders a fast burning or slow-moving situation and categorizing if an organization is affected itself, or is being deployed to deal with the effects of the crisis.

5.3 Results on interviews

In the interviews with experts, we focus on answering SQ3: "What are the challenges and necessary improvements with regards to making sense of a (national) cyber crisis?"

We start analyzing the interview data by working our way from raw data of the interview summaries to first order concepts to second order themes and finishing at aggregate dimensions. With these dimensions, we created a data structure of the themes we will present the results of in this chapter.

In 5 interviews, the summaries were coded into 189 initial codes. Within these, we have identified 118 first order themes, which we categorized to 25 second order themes by using axial coding (Gioia et al., 2013). Further analysis led us to finding 8 aggregate dimensions. We will present the most relevant results in terms of our research questions.

5.3.1 Challenges

If we look at the aggregated dimension of challenges that impact sensemaking, there are five second order themes identified in the interviews, as shown in the figure below.

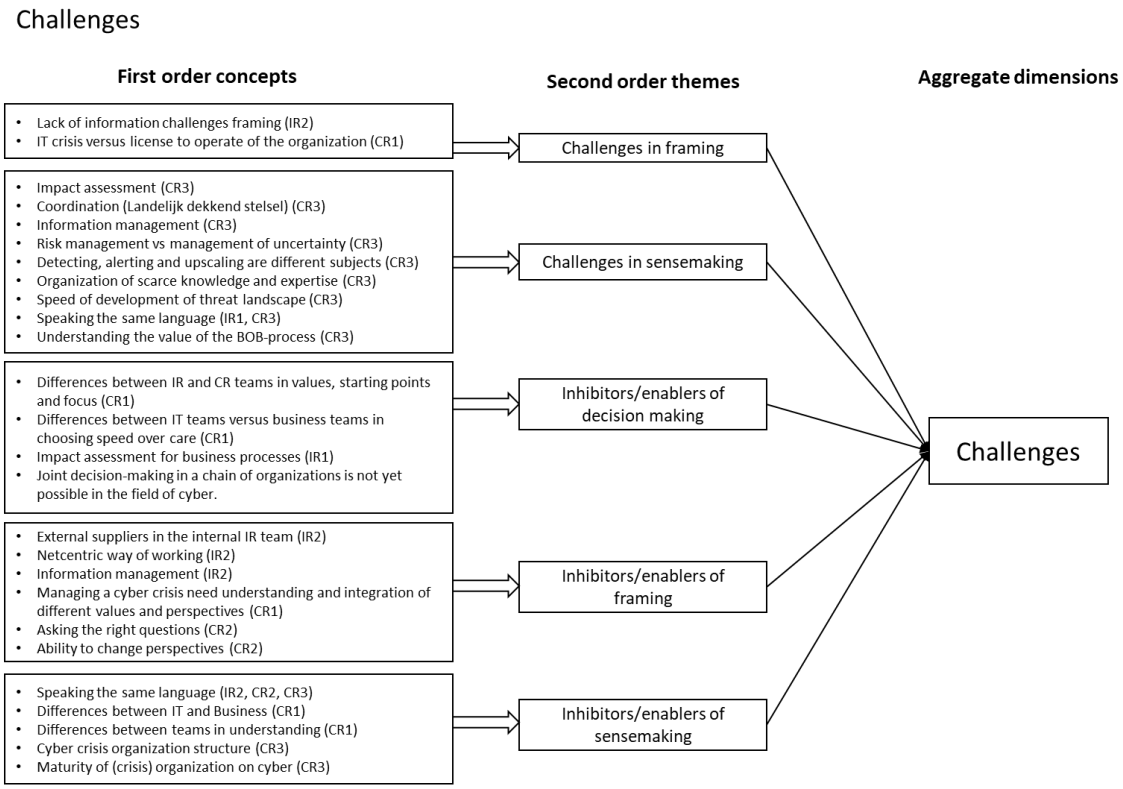


Figure 9 - Interview results on challenges that impact sensemaking

5.3.1.1 Challenges in framing

There are two specific challenges to framing, as the respondents indicated. First of all, a lack of information challenges framing (IR2). This is mostly due to the fact that in the first few days of a cyber crisis, not a lot of information is available. Another challenge is that it's not always clear for organizations if the cyber crisis is 'just' an IT crisis, or a possible threat to the license to operate of the organizations (CR1).

5.3.1.2 Challenges in sensemaking

Challenges in sensemaking that are mentioned include connecting the business to the various crisis teams, in order to facilitate making an impact assessment (CR3). This impact assessment should be based on Business Impact Analyses, critical processes described, the vital interests to protect and with an eye for the context (CR3). Ensuring that the right information is on the right table at the right time is a challenge of information management (CR3). This has to be a coordinated process, as dealing with uncertainty in the workings of a piece of software is a challenge (CR3). Coordination in the face of the expanding 'Landelijk Dekkend Stelsel' (National Coverage System) (Ministerie van Justitie en Veiligheid, 2021) on cybersecurity, in which the NCSC acts as a single point of information helps with that (CR3).

Another challenge is the preparation of risk management in an organization (CR3): what level of certainty or uncertainty do you still find acceptable? And how can you quantify that in the light of risks in the field of cyber security?

When we zoom in on possibilities to detect, alert and notify, respondent (CR3) indicates that this is about interpreting an initial report of a vulnerability and ensuring that the right people

are alerted in the right places and receive the right information to make a decision. Notification criteria and upscaling criteria are both necessary to have, but serve a different purpose (CR3). Notification criteria serve to notify individuals or teams that something is going on. This is especially important for a strategic crisis team, which often wants to know what's going on, to prevent them from being questioned by the outside world about an incident or vulnerability they are not yet aware of (CR3). An example of this is if the plug mandate ('stekkermandaat') has been applied. This is done preferably as low as possible in the organization, but the strategic team needs to be informed about it. Upscaling criteria are more of a checklist (CR3) in which, in the context of business continuity, a number of criteria are formulated that exceed a certain value (for example the recovery time objective), because repairs cannot be made within the stated agreements and therefore must be scaled up. Scaling up itself ideally takes place in multiple layers, for example from operational to tactical to strategic level (CR3).

Respondents also indicated that the speed of development of the threat landscape is a challenge to sensemaking (CR3). The threat landscape is evolving, and new attack techniques are continuously invented. This also makes a cyber crisis different from classic disasters (CR3). Speaking the same language (IR1) to translate the operational view to business impact and proposed measures and the organization of scarce knowledge (CR3) are named as challenges in this light.

During a crisis, the BOB-process is standard, but understanding the value of it proves to be a challenge (CR3). Sometimes, more technically oriented people have the feeling that a game is being played in a crisis team at a process level, which prevents them from making any progress in terms of content (CR3).

5.3.1.3 Inhibitors/enablers of decision making

According to the respondents, inhibitors of decision making in cyber crises are differences between IR and CR teams in terms of values, starting points and focus (CR1) and differences between IT and Business teams in choosing speed over care (CR1). Operational IR teams and tactical/strategic CR teams adhere to different values and starting points, this inhibits joint decision making on choosing for speed or care, while at the same time IT departments want to analyze thoroughly, but business departments are more likely to choose speed over care, because of the impact on services. These two worlds collide during a cyber crisis and the team's frame determines whether the organization chooses speed or care (CR1).

The judgment phase in which the impact of compromised systems (including scope of compromise) is connected to the effects on the business processes can enable decision making on a strategic level (IR1), as long as they are made beforehand. And finally, respondents (CR3) indicate that joint decision-making in a chain of organizations is not yet possible in the field of cyber. Maybe in a few decades, but this needs more development still.

5.3.1.4 Inhibitors/enablers of framing

Respondents indicated that an inhibitors of framing was that external suppliers are not always available in the internal IR teams (IR2). This inhibits framing, because it is then harder to understand what's going on, impairing the ability to identify a relevant frame.

Enablers of framing that are named are the netcentric way of working (IR2) to help construct a common operational picture across all levels of crisis teams, next to indicating what your 'single point of truth' is in the information management field (IR2). That enables identifying a frame. A cyber crisis is not only an IT challenge, but also an organizational crisis. Managing it needs the

understanding and integration of different values and perspectives (CR1), this also means asking the right questions.

One respondent (CR3) indicated that a good way to trigger framing behavior is to ask teams the question “imagine that in 3 months you are sitting at the table with Jinek, and you are telling the story of this cyber crisis . And then start your sentence with: ‘as we said from the beginning, this is a […] and that's why we acted this way’.” (CR3). This helps to provide the team with a more longer-term view, and thinking about where the effects occur instead of starting with the solution to the IT problem. One respondent (CR3) also indicated that this changing of perspectives is done better by CI organizations than for example hospitals and municipalities.

5.3.1.5 Inhibitors/enablers of sensemaking

During a cyber crisis, two groups that don't match come together (CR1): the IT and security world with their own language and responders who ‘own’ the problem. And the rest of the organization and the board who look at the crisis from a perspective of business impact, primary process, external stakeholders, and reputation. Still, these groups together have the responsibility to manage both the source and the effects of the cyber crisis. In this case, not speaking the same language is regarded as an inhibitor of sensemaking by various respondents (IR2, CR2, CR3), although these respondents do not agree on whether this is still a problem.

One respondent (IR2) indicated that sometimes teams don't speak each other's language, but usually they do and are able to translate this to IR and CR. Another (CR2) indicated that language barriers between IR and CR have largely disappeared, which also became visible during ISIDOOR. Everyone now understands what ransomware is, while previously it was a kind of abracadabra of technicians. The mystique of a cyber crisis seems to slowly disappear. It's still really complicated, but understandable. One respondent (CR2) had a great analogy: “I only need to know that the gearbox is broken, I don't need to know how the gearbox works”.

Another inhibitor of sensemaking is that teams don’t always have the same understanding. IT professionals often underestimate the problem at hand and especially its strategic implications. Directors and directors are often IT laypersons and overestimate the technical possibilities available to solve an IT problem (CR1). This means that speaking the same language is indeed important.

What enables sensemaking is ensuring the maturity of the (crisis) organization on cyber (CR3), preferably with a multi-year training program, and a solid crisis organization structure (CR3) that organizes the triangle of the generic crisis structure, incident response and business who need to be involved at the same time (CR3).

5.3.2 Improving sensemaking of a cyber crisis

Zooming in on the aggregate dimension of improving sensemaking, the second order themes are based on the improving of sensemaking of a cyber crisis on team, organizational and inter-organizational level. This is shown in the data structure below. The results of the interviews on improving sensemaking are presented in the next paragraphs.

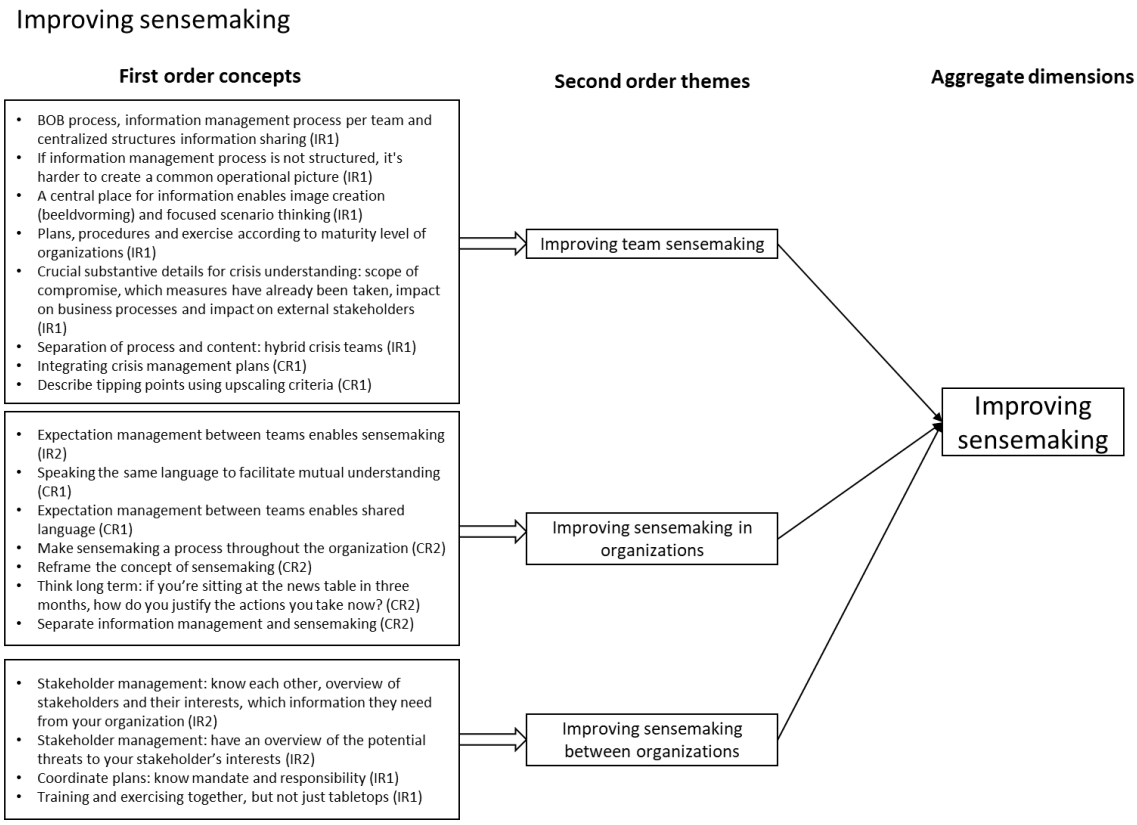


Figure 10 - Improving sensemaking of a cyber crisis data structure

5.3.2.1 Improving sensemaking of a cyber crisis on team level

On team level, sensemaking can be improved by a solid crisis organization structure and processes, which include the BOB-process (IR1), information management (IR1) to ensure the forming of a common operational picture and enable this by providing a central place for information (IR1). Next to that, in the teams there should be a separation of process and content (IR1), in which a permanent core of process roles (chairperson, secretary/log keeper, information manager, crisis management advisor) is formed, and a more flexible layer is added, suited to what the crisis needs. For cyber these should be cyber experts, not fire experts (IR1). Crisis understanding is also improved by taking into account the crucial substantive details during the crisis (IR1), which include the scope of compromise, which measures have already been taken, impact on business processes and impact on external stakeholders. Crisis plans and procedures should be integrated (CR1) and practiced according to the maturity level of the organization (IR1).

5.3.2.2 Improving sensemaking of a cyber crisis on organizational level

Improving sensemaking on organizational level can be done by starting with expectation management, in which the different teams in an organization come together to express their expectations towards one another, learn to speak each other's language and understand each other's working methods (CR1, IR2). This enables sensemaking, because otherwise "your IR team and CR team will both run, but in different directions" (IR2).

Sensemaking should also be a process throughout the whole organization, to formulate goals and principles (CR2), focusing on long term thinking (CR2). A separation between information management (collecting, validating and sharing information) and sensemaking

(interpreting and giving meaning to information) helps as well (CR2). As sensemaking is a strategic choice and is preferably done through the strategic layers (CR2). It's a question of framing an incident as big or small that is the strategic choice here, and the tactical or operational layer can advise on this (CR2).

And maybe, we should reframe the concept of sensemaking and call it framing or storytelling (CR2).

5.3.2.3 Improving sensemaking of a cyber crisis on inter-organizational level

Between organizations, sensemaking can be improved by stakeholder management, and having an overview of the interests of your stakeholders, which information they need from you, and an overview of how a cyber crisis can potentially threaten their interests (IR2). This enables sensemaking during a crisis (IR2). Make sure that you know the organizations in your network, grow with each other in this network and build trust (IR2).

Next to that, make sure to coordinate plans so that organizations can respond to each other and know what everyone's mandate and responsibility is (IR1). These plans can continue to be trained and exercised on together, but make sure there are not just tabletop exercises like ISIDOOR is (IR1).

5.3.3 Other relevant results

In the interviews, there were other relevant results that are worth mentioning. The respondents have indicated a **definition for incident handling** as a connecting process between IR and CR teams. Incident handling is part of the total response to a cyber crisis, where a team focuses on fixing the problem, a team/person focuses on explaining what that means for the rest of the organization and then you have another team that can make decisions accordingly. How this is set up depends on how large the organization is (CR2). Incident handling is considered a linking pin role, by a SOC team leader, CISO, director or manager IT or external partner (CR3, IR2, IR1). For this role, the following competence is needed: building bridges between technical experts and directors (CR2, IR1). If the role is implemented correctly, it can enable situational awareness in operational teams by translating the operational problems from an information-driven to a risk-driven approach (CR2).

Another relevant result is the view of the experts on the **differences between a cyber crisis and a regular crisis**. All respondents agree that a cyber crisis is different from a regular, physical crisis (IR1, IR2, CR1, CR2, CR3). In a regular crisis, you know what's going on (IR2), it's happening now (CR1), and the impact is visible quickly, because it's physically visible (IR2, CR1). There is a clear beginning and end ('under control' moment) (CR1) and it's easier to specify in words (CR2).

One respondent (CR1) calls a cyber crisis the next socially disruptive scenario (CR1) and states there are four manifestations of a cyber crisis (CR1): 1) a large-scale and long-term failure of IT systems, 2) a large-scale data breach of personal data, 3) a data breach of business-sensitive information and 4) data integrity (manipulation). Another respondent emphasizes that pace and unfamiliarity make a difference: in a cyber crisis it takes some time to gain good insights (IR2). Especially in the first days, a 'fog of war' is experience, as there are many more questions than information available to answer them (IR2). A summary of the cyber crisis characteristics the respondents have mentioned is provided in the table below.

Table 28 - Overview of cyber crisis characteristics

Themes	Responses
Invisible	First image only after a few days based on forensic investigation, making the crisis itself less visible (IR2)
	It can remain invisible for a long time (CR1)
	Invisible (unlike a dike breach) (CR3)
Intangible	Less tangible (IR2)
	In the initial phase, you don't know exactly what it is, how long it will last, what the recovery period will be, what it precisely affects, and what the costs will be (CR2)
	Incomprehensible (CR3)
	It's useful to have some knowledge of the content to make sense of it: along which axes can you be affected? What do the BIV criteria mean? What type of measures can you take? (CR3)
Transboundary	It may have been ongoing for days/weeks/months already (CR1)
	It's difficult to determine when it's over (CR1)
	The spread presents a residual risk: for example, you not only lose data but also remain vulnerable in other areas (CR2)
	The speed at which the crisis develops (CR3)
Uncertain	Ambiguous (IR2)
	Interests less clear (IR2)
	A cyber crisis thus has more uncertainties and dilemmas than a regular crisis (CR1)
	It can impact many of your processes, creating more uncertainty in cause, perception, and resolution (CR2)
	Uncertainty about motives (CR2)
	Unclear with what priority processes can be restored, making it difficult to determine who should be informed (CR2)
Interconnected	Interconnectedness of systems, dependence on generic components (CR3)
	In a cyber/IT problem, executives don't always fully understand what's happening "under the hood" (CR2)
	Dependent on well-established logging (IR2)
Malicious intent	Cyber crises are often deliberate attacks to blackmail or disable you (CR2)
	A number of unique decisions to be made regarding negotiating with cybercriminals, whether to pay or not (CR3)
Legal perspective	The legal perspective is much larger (IR2)

These finding support the claims we made in the introduction and literature review that intangibility, interconnectedness and transboundary nature are important aspects that set a cyber crisis apart from a regular crisis.

Next to cyber crisis characteristics, there is also a difference to be seen in crisis processes. **Crisis communication** for example has other aspects to consider during a cyber crisis (IR2): in the first three days there is not a lot to communicate, but after that questions are asked about specific aspects like forensics, privacy aspects, what has been hit and what is the perspective for action? It is imperative to think about cyber crisis communication beforehand and know how to position crisis communication in a CR context (IR2).

And last but not least, a **cyber crisis has different organizational characteristics**. At the moment cyber crisis management is still at a low level in terms of maturity, both socially and within organizations (CR1). Many organizations still have an inward focus on the technical side of the problem (CR2), and IR teams and CR teams have a different way of looking at the cyber crisis (IR2). Organizations need to move from seeing cyber crisis as an IT continuity problem to seeing cyber crises as a general continuity problem (CR2). The main focus has to be on offering alternatives to disrupted services and good crisis communication (CR2).

5.3.4 Summary

To summarize, the interviews have provided a more in-depth view on the topic and have also supported the results of the questionnaire. The results have provided an answer to SQ3: “What are the challenges and necessary improvements with regards to making sense of a (national) cyber crisis?”

In terms of challenges, the interview respondents have named challenges in framing and sensemaking, inhibitors/enablers of decision-making, framing and sensemaking. Differences between teams, differences in viewpoints of what a cyber crisis is, speaking the same language, asking the right questions and the maturity of a (crisis) organization were named.

If we compare the answers to the open-ended questions of the questionnaire on improving sensemaking to the interview questions on improving sensemaking, we can see that there are similarities and differences in answers.

Similarities on improving sensemaking in teams are found in the topics of information management, crisis process, plans and procedures, organizational processes and the distinction between IT problem versus a continuity problem. Differences were seen in terms of perspective, where the interview respondents were able to highlight key processes from a broader point of view and the questionnaire respondents provided more details on how specific tools for example can aid sensemaking in teams.

Similarities on improving sensemaking in organizations contained information management, structuring crisis processes. Differences were found again in terms of perspective, in which the questionnaire respondents focused mainly on the processes that can be improved, and the interview respondents focused more on facilitating the interpersonal connections and long-term view.

On improving sensemaking between organizations, similarities were seen in terms of the importance of exercising and knowing chain dependencies, stakeholders and information sharing between organizations. Differences were found in the perspective of the interview respondents who focused mainly on stakeholder management and coordinating plans in general, and the questionnaire respondents focusing on the sectoral coordination and support and sharing information between organizations.

Next to that, the interviews have provided other relevant results like providing a definition for Incident Handling and providing cyber crisis characteristics.

5.3.5 Answering the Main Research Question

With the result on the three sub-questions presented, we can formulate an answer to our MRQ: "How do incident response and crisis response teams of organizations in critical infrastructure and governmental organizations use framing and sensemaking behavior to make sense of a (national) cyber crisis in the Netherlands?"

This study has shown that IR and CR teams in GOV and CI organizations use framing strategies from the Data/Frame theory, particularly they show behavior on Identifying a frame. The other steps in the framework are less visible in behavior, especially Questioning a frame seems to be hard.

This study has also shown that IR and CR teams in GOV and CI organizations make use of sensemaking questions on situational, identity-oriented and action-oriented sensemaking. The scores were especially high on Information sharing.

The questionnaire and interviews have also provided insight into what the challenges are to sensemaking in cyber crises, and what can be improved on team, organizational and inter-organizational level when it comes to sensemaking.

6 Conclusion and discussion

In this chapter, we give a short conclusion on the study, and we discuss the results of this study in terms of relations to literature and theoretical frameworks and look at implications for policy

and practice. Furthermore, we will describe its limitations and give thoughts on future research in this field.

6.1 Conclusion

A cyber crisis is society's next socially disruptive scenario, as one of the interviewees stated. This study aimed to find out how incident response and crisis response teams in governmental organizations and critical infrastructure organizations make sense of such a scenario, in the context of a national cyber crisis. It has explored a field of study that has not been explored much before and added insights on how teams show framing behavior and asking sensemaking questions.

The method used was innovative in that it reached a larger sample by using a questionnaire in which observers of crisis teams could indicate if they saw certain behaviors in the teams they observed in a larger exercise, as opposed to conducting a smaller study with observations on single exercises done by the researcher. This means that although the sample is small, it has been possible to make comparisons between different teams and organizations, because they have used the same basis scenario in the ISIDOOR exercise.

The research questions were answered (see section 5.3.5) by conducting a survey among participating organizations in national cyber crisis exercise "ISIDOOR IV", and semi-structured interviews with experts on incident response and crisis response.

The results of the questionnaire provided insights into behavior on framing and sensemaking questions asked, which we will review in the discussion. The results on the interviews showed the challenges teams have to deal with when they face a cyber crisis, which showed challenges and inhibitors/enablers in framing and sensemaking, but also inhibitors and enablers of decision making. The differences between teams are the main reason for that. The results on the interviews also showed the necessary improvements that need to be made for the future to improve sensemaking in teams, between teams and between organizations. The results also showed that experts agree that a cyber crisis is indeed different from a regular crisis, amongst others on the concepts of intangibility, interconnectedness and transboundary nature. And experts have provided more insight into the concept of incident handling, cyber crisis communication and the organizational characteristics with regard to a cyber crisis. The study results will be discussed below, followed by implications for practice and future research.

6.2 Discussion on the expectations based on the Data/Frame theory

There were three hypotheses based on the Data/Frame theory (Klein et al., 2010) we will reflect on below. We'll zoom in to the results of the hypotheses, argue why the outcomes were congruent with our expectations or not and give pointers for reconducting the study.

First, teams composed of professionals/experts do not show more behavior on questioning a frame than teams composed of organizational liaisons and team members. This hypothesis (H1) was drafted to see if there was a difference between IR and CR teams in terms of questioning a frame. This hypothesis was unsupported by the data of our study, which might have been due to the translation of 'highly experienced members' to 'professionals/experts', and 'less experienced members' to 'organizational liaisons and team members'. The level of expertise as used for the hypothesis in the literature was not measured with the same connotation as was written in the H1 hypothesis, which measured the individual role. In future research this may be examined more in detail, to measure the correct construct.

The same goes for H2, as it also connected level of expertise to individual role, although the results did almost show a significant difference here. If we look at the level of experience with

regards to cyber crises, this may not be a completely incorrect construct after all, because IR teams usually do have more in-depth experience with the cause and nature of a cyber incident and use forensic evidence to support their frame. This indicates why IR teams will be more likely to accept the data provided than CR teams.

The final hypothesis based on the Data/Frame theory was that teams are unlikely to question a frame. This was not translated for our study and was supported clearly by the data we found. We did wonder why it was hard for teams to question a frame, and the open-ended questions did not shed much light on this. The only explanation we can offer is that the framing process might be done more subconsciously, as reported by respondents, and this might make it harder for observers to identify the behavioral aspects we've shown them. In future research this can be managed by controlling the observation part more, to get more consistent results across the whole sample.

The results suggested a significant, positive correlation between Questioning the frame and Comparing frames in the general and IR group, and between Questioning the frame and Elaborating a frame in the CR group. Based on the Data/Frame theory, we would have expected to find correlations between all parts of the framing process, but this was not the case. A smaller sample might have been the reason for this, although another explanation might be that the teams are not accustomed to consciously go through these steps one by one, and therefore the correlations are not shown. It would be interesting to find out if the correlations found also imply cause and effect relationships. Further research with a larger sample and more in-depth method might elaborate on this. In the broader literature on sensemaking, it is shown that sensemaking is difficult (Weick, 1988, 1993, 1995), it is a critical task in crisis leadership (Boin et al., 2016) and it enables decision-making (Endsley, 1995), but updating and doubting are relevant factors to consider (Maitlis & Sonenshein, 2010), especially when we examine team sensemaking. The findings on H3 are supported by the arguments for updating and doubting being relevant factors in team sensemaking.

6.3 Discussion on the expectations based on the sensemaking questions

There were nine hypotheses formulated on identity-oriented sensemaking and action-oriented sensemaking. In the results they were split up in sub-hypotheses to examine if they were supported by the data of our study or not. These hypotheses were based on the literature on sensemaking questions asked in crisis response teams. The findings suggested that the support of only three of these hypotheses was inconclusive (H4, H6a and H8a), and the rest of the hypotheses were not supported by our data.

The hypothesis H4 on teams comprised of professionals/experts (IR teams), showing more behavior related to Crisis Understanding than CR teams, was almost significant. A larger sample might have helped to get a better result. Still, if we dive into the results of the individual behaviors related to crisis understanding, the results showed that IR teams score higher on understanding the nature and cause of the cyber crisis, and CR teams score higher on understanding the effects of the cyber crisis for their own organization and understanding the potential future risks of the cyber crisis. This is actually to be expected based on their roles, so the hypothesis should have been formulated narrower to find supporting evidence.

The nearly significant moderate positive correlation found between teams showing behavior of having a shared identity and behavior of Questioning the frame (H6a) and of the team being able to create a common operational picture (H8a) was an interesting result. Further research might elaborate on this possible correlation, but the findings are supported by the

literature in the sense that if team identity is clear, the role they have guides the analysis of the crisis (Kalkman, 2019).

6.4 Discussion on the challenges of and improving sensemaking

We found that the observer group that answered the open-ended questions on improving sensemaking in teams, between teams and between organizations differed in their answer from the expert group that was interviewed. The answers of the observers were very practical in nature, which can be explained by the scope of their view. Their perspective was their own organization, which could lead to a variety of answers, that sometimes contradicted. The answers of the experts were given from a different perspective, namely that of a broader experience with different types of organizations. This means that the answers were more on a conceptual level already.

When we compare the differences between a regular crisis and a cyber crisis, as indicated by the experts, with the reviewed literature, we see a coherent picture. The literature supports the concepts of intangibility, interconnectedness and transboundary nature of a cyber crisis that is also mentioned by the experts. The visibility, uncertainty, malicious intent and specific legal perspective were added by the experts.

6.5 Implications for policy and practice

Other findings of our study were not based on literature, but nonetheless interesting for practical implications. The following implications for policy and practices are proposed.

First, the concept of network understanding received the lowest scores in comparison to the other concepts, especially in IR teams. This indicates that it is necessary to keep **practicing** in national cyber crises, to raise this level, as network understanding is essential for inter-organizational sensemaking.

Second, the CR group scored significantly higher on creating a shared common operational picture of the cyber crisis than the IR group. This indicates an implication for practice, as it is necessary to provide **training** to IR teams on how to create a common operational picture. This will most likely help CR teams to score higher on showing behavior with regard to understanding the nature and cause of the cyber crisis. This can be investigated further in the future.

Third, the CR group also scored higher than the IR group on network understanding. This implies that the **connection between the IR teams and other teams** inside and outside of the organization can be improved. Providing IR teams with a team member with the role of stakeholder management or situational awareness could help with this, so the technical experts can focus on what they do best.

Fourth, the CR group also show significantly more behavior on coming to a shared conclusion of why they are at the crisis table than the IR group. As we mentioned, this might be due to the fact that the decision-making model BOB as a basis for team meetings, implicitly tackles this question. IR teams might benefit from **using this BOB process** as a basis for their team meetings as well.

Fifth, the significant differences found in the concept of type of team observed show resemblance to the findings on crisis understanding as mentioned above. One thing that stood out was that political teams showed significantly more behavior on knowing which other organizations are involved in the cyber crisis. This is explained by their role in a national cyber crisis, but also implies that there is work to do for the other types of teams in this respect. Further **exercising and training** on this might improve this network awareness.

Sixth, between sectors several significances differences were found on understanding the cause of the cyber crisis and on understanding which other teams are involved in their own organization that could not be explained directly but need further investigation.

Seventh, another practical implication is given by looking into the **use of crisis management system**. It was found that teams using either LCMS or another CMS showed the most behavior on agreeing on which existing plans and procedures apply to the current cyber crisis. This might be due to the fact that a CMS is usually also a place to gather all the relevant documents. This can be prepared before a cyber crisis starts, and managed by an information manager during a cyber crisis and might be interesting for other organizations not using a CMS to explore.

Eighth, the results of this study show that when looking at framing behavior, there is still a lot to be improved. Teams are able to identify a frame, but especially questioning a frame proved to be complicated. That is a problem, as the re-framing cycle and the elaboration cycle start after questioning a frame. If the **process of framing can be improved**, this enables better sensemaking and decision-making during a cyber crisis. Development of training and exercises specifically aimed at improving behavior of questioning a frame could help to achieve this.

And finally, in practice, the results of this study mean that there is now an overview of improvements of team, organizational and inter-organizational sensemaking. These can be presented to sectoral bodies, governments and other organizations, so they **can jointly prepare** for better framing and sensemaking during a national cyber crisis. This could also be added to the National Crisis Plan Digital and plans of individual organizations, as a practical checklist.

6.6 Limitations

The most relevant limitation of this study is that the sample of the questionnaire has been smaller than initially aimed for. Challenges in the data collection have hampered the collection of enough data to conduct statistical tests based on a normal distribution. This means that the generalization of this study to a broader population is limited.

Another limitation is that this study has only focused on two topics relating sensemaking: framing behavior as the very start of the sensemaking process and sensemaking questions asked in crisis response teams. Of course, the sensemaking process consists of many more aspects and they also need to be investigated in a cyber crisis context. Due to time available and scope this was not possible for this thesis.

A third limitation is that observers may not have registered implicit behavior, as it was not visible, and we specifically asked to indicate visible behavior on framing and sensemaking questions asked. This means that our results might be flawed in this respect.

And finally, the researcher has not personally observed the teams that participated in the study. This means it was not possible to standardize the input of the different observers on the questionnaire, which could lead to different interpretations of the questions by the actual observers.

6.7 Future research

The goal of this research was to explore how incident response and crisis response teams use framing and sensemaking behavior to make sense of a national cyber crisis. As cyber crisis management is currently an under-researched topic, by using the context of a national cyber crisis exercise, this research can function as a benchmark or starting point for future research on cyber crisis management. The following suggestions arise.

First, future research based on our study is recommended to be done in a more controlled setting, as to be able to control for more external variables like for example varying observers or conducting the research either completely separate from an organizing team or having an organizing team fully invested. Also, this study could be repeated in a *regular* national crisis exercise and compared, to find out if there are differences in sensemaking between cyber crises and regular crisis.

Second, to be able to conduct team sensemaking in crisis situations, Klein et. al. (Klein et al., 2010) argue it's also important for a team to manage the emergent sensemaking *requirements*, which include data synthesis (putting all the pieces together), seeking data (coordinate on a shared intent on what data to look for), monitoring data quality (look for inconsistencies), resolving disputes, dissemination (when and what), and overhead and coordination costs (establishing and sustaining common ground). This has not been the scope of our study, due to limited time available in the master's thesis process and needs further research in the context of a cyber crisis.

Third, further research on the basis of our results is also recommended on cyber crisis communication, as the experts mention that there are other aspects to consider than in a regular crisis. These aspects should be clear, as this helps organizations think about their cyber crisis communication strategy.

Fourth, further research is recommended on the organizational characteristics of a cyber crisis. Especially on changing the inward focus on the technical issue to seeing a cyber crisis as a general continuity problem. The use of the NIST IR model seemed to indicate in our study that this leads to higher understanding of the cause of the cyber crisis and debating on conflicting plans/procedures. This relation could not be explained by the literature we reviewed, but might be explored in future research. And finally, future research should also focus on establishing why questioning a frame is difficult and what can be done to improve this ability.

And finally, apart from what we've studied, an interesting research direction could be to examine the concept of distributed sensemaking, in relation to cyber crises, as this might influence the steps of framing. And finally, future research can focus on the implications for policy and practice, to get a more hands-on perspective on framing behavior and sensemaking questions asked in cyber incident response and crisis response teams, in order to improve cyber crisis management.

After discussing the findings in relation to literature, policy and practice, we conclude with the statement that further development of a cyber crisis management field of research is highly recommended.

References

This reference list is produced by Zotero.

Ansell, C., Boin, A., & Keller, A. (2010). Managing Transboundary Crises: Identifying the Building Blocks of an Effective Response System. *Journal of Contingencies and Crisis Management*, *18*(4), 195–207. https://doi.org/10.1111/j.1468-5973.2010.00620.x

Asch, S. E. (1956). Studies of independence and conformity: I. A minority of one against a unanimous majority. *Psychological Monographs: General and Applied*, *70*(9), 1–70. https://doi.org/10.1037/h0093718

Backman, S. (2021). Conceptualizing cyber crises. *Journal of Contingencies and Crisis Management*, *29*(4), 429–438. https://doi.org/10.1111/1468-5973.12347

Bhattacherjee, A. (2019). *Social Science Research: Principles, Methods and Practices (Revised edition)*. https://usq.pressbooks.pub/socialscienceresearch/

Billups, F. D. (2021). *Qualitative Data Collection Tools: Design, Development, and Applications*. SAGE Publications, Inc. https://doi.org/10.4135/9781071878699

Boeke, S. (2018). National cyber crisis management: Different European approaches. *Governance*, *31*(3), 449–464. https://doi.org/10.1111/gove.12309

Boersma, K., & Wolbers, J. (2021). Foundations of Responsive Crisis Management: Institutional Design and Information. In K. Boersma & J. Wolbers, *Oxford Research Encyclopedia of Politics*. Oxford University Press. https://doi.org/10.1093/acrefore/9780190228637.013.1610

Boin, A. (2009). The New World of Crises and Crisis Management: Implications for Policymaking and Research. *Review of Policy Research*, *26*(4), 367–377. https://doi.org/10.1111/j.1541-1338.2009.00389.x

Boin, A. (2019). The Transboundary Crisis: Why we are unprepared and the road ahead. *Journal of Contingencies and Crisis Management*, *27*(1), 94–99. https://doi.org/10.1111/1468-5973.12241

Boin, A., ‘T Hart, P., Stern, E., & Sundelius, B. (2016). *The Politics of Crisis Management: Public Leadership under Pressure* (2nd ed.). Cambridge University Press. https://doi.org/10.1017/9781316339756

Bossong, R., & Hegemann, H. (Eds.). (2015). *European civil security governance: Diversity and cooperation in crisis and disaster management*. Palgrave Macmillan.

Burke, C. S., Stagl, K. C., Salas, E., Pierce, L., & Kendall, D. (2006). Understanding team adaptation: A conceptual analysis and model. *Journal of Applied Psychology, 91*(6), 1189–1207. https://doi.org/10.1037/0021-9010.91.6.1189

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology* (NIST SP 800-61r2; p. NIST SP 800-61r2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2

Davis, N. (2016, January 19). *What is the fourth industrial revolution?* World Economic Forum. https://www.weforum.org/agenda/2016/01/what-is-the-fourth-industrial-revolution/

Endsley, M. R. (1995). Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *37*(1), 32–64. https://doi.org/10.1518/001872095779049543

Fetters, M. D. (2020). *The Mixed Methods Research Workbook: Activities for Designing, Implementing, and Publishing Projects*. SAGE Publications, Inc. https://doi.org/10.4135/9781071909713

Flick, U. (2018). *Doing Triangulation and Mixed Methods*. SAGE Publications Ltd. https://doi.org/10.4135/9781529716634

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology. *Organizational Research Methods, 16*(1), 15–31. https://doi.org/10.1177/1094428112452151

Hale, G. (2021). *Colonial Pipeline Attack Started in IT Systems, Highlights SCADA System Vulnerability*. https://www.isa.org/intech-home/2021/june-2021/departments/industry-update#pipe

Janis, I. L. (1982). *Groupthink: Psychological studies of policy decisions and fiascoes* (2nd ed). Houghton Mifflin.

Kalkman, J. P. (2019). Sensemaking questions in crisis response teams. *Disaster Prevention and Management: An International Journal*, *28*(5), 649–660. https://doi.org/10.1108/DPM-08-2018-0282

Kalkman, J. P. (2023). *Frontline Crisis Response: Operational Dilemmas in Emergency Services, Armed Forces, and Humanitarian Organizations* (1st ed.). Cambridge University Press. https://doi.org/10.1017/9781009262170

Klein, G., Moon, B., & Hoffman, R. R. (2006a). Making Sense of Sensemaking 1: Alternative Perspectives. *IEEE Intelligent Systems*, *21*(4), 70–73. https://doi.org/10.1109/MIS.2006.75

Klein, G., Wiggins, S., & Dominguez, C. O. (2010). Team sensemaking. *Theoretical Issues in Ergonomics Science*, *11*(4), 304–320. https://doi.org/10.1080/14639221003729177

Klein, Moon, & Hoffman. (2006b). Making Sense of Sensemaking 2: A Macrocognitive Model. *IEEE Intelligent Systems*, *21*(5), 88–92. https://doi.org/10.1109/MIS.2006.100

Kuipers, S., & Welsh, N. H. (2017). Taxonomy of the Crisis and Disaster Literature: Themes and Types in 34 Years of Research. *Risk, Hazards & Crisis in Public Policy*, *8*(4), 272–283. https://doi.org/10.1002/rhc3.12123

Lavrakas, P. (2008). *Encyclopedia of Survey Research Methods*. Sage Publications, Inc. https://doi.org/10.4135/9781412963947

Maitlis, S., & Christianson, M. (2014). Sensemaking in Organizations: Taking Stock and Moving Forward. *Academy of Management Annals*, *8*(1), 57–125. https://doi.org/10.5465/19416520.2014.873177

Maitlis, S., & Sonenshein, S. (2010). Sensemaking in Crisis and Change: Inspiration and Insights From Weick (1988). *Journal of Management Studies*, *47*(3), 551–580. https://doi.org/10.1111/j.1467-6486.2010.00908.x

Mills, J., & Weatherbee, T. (2006). Hurricanes Hardly Happen: Sensemaking as a Framework for Understanding Organizational Disasters. *Culture and Organization, 12*, 265–279. https://doi.org/10.1080/14759550600871485

Milmo, D. (2022, August 11). NHS ransomware attack: What happened and how bad is it? *The Guardian*. https://www.theguardian.com/technology/2022/aug/11/nhs-ransomware-attack-what-happened-and-how-bad-is-it

Mils Hills. (2016). *Why Cyber Security Is a Socio-Technical Challenge: New Concepts and Practical Measures to Enhance Detection*. Nova.

Ministerie van Economische Zaken en Klimaat. (2018, September). *Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) voor Digitale dienstverleners*.

Ministerie van Justitie en Veiligheid. (2021, June 8). *Landelijk dekkend stelsel—Nationaal Coördinator Terrorismebestrijding en Veiligheid*. Ministerie van Justitie en Veiligheid. https://www.nctv.nl/onderwerpen/landelijk-dekkend-stelsel

Ministerie van Justitie en Veiligheid. (2022a, December 6). *Nationaal Handboek Crisisbeheersing*. https://www.rijksoverheid.nl/documenten/rapporten/2022/12/06/tk-bijlage-2-nationaal-handboek-crisisbeheersing

Ministerie van Justitie en Veiligheid. (2022b, December 23). *Landelijk Crisisplan Digitaal (LCP)—Publicatie—Nationaal Coördinator Terrorismebestrijding en Veiligheid*. https://www.nctv.nl/documenten/publicaties/2022/12/23/landelijk-crisisplan-digitaal

Ministerie van Justitie en Veiligheid. (2023, November 6). *Overzicht vitale processen—Vitale infrastructuur—Nationaal Coördinator Terrorismebestrijding en Veiligheid* [Onderwerp]. Ministerie van Justitie en Veiligheid. https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen

Mueller III, R. S. (2012, March 1). *Combating Threats in the Cyber World: Outsmarting Terrorists, Hackers, and Spies*. RSA Cyber Security Conference, San Francisco, CA. https://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies

Nationaal Coördinator Terrorismebestrijding en Veiligheid. (2023). *Risico en Crisisbarometer najaar 2023*.

Nationaal Coördinator Terrorismebestrijding en Veiligheid. (2022). *Nederlandse Cybersecuritystrategie 2022-2028*.

Nationaal Cyber Security Centrum. (2019, March 14). *Wettelijke taak—Over het NCSC - Nationaal Cyber Security Centrum* [Webpagina]. Nationaal Cyber Security Centrum. https://www.ncsc.nl/over-ncsc/wettelijke-taak

Nationaal Cyber Security Centrum. (2023, December 8). *Cyberoefening ISIDOOR 2023: "Cybercrisis leek ver van mijn bed" - Nieuwsbericht - Nationaal Cyber Security Centrum* [Nieuwsbericht]. Nationaal Cyber Security Centrum. https://www.ncsc.nl/actueel/nieuws/2023/december/8/isidoor

Northwave. (2022). *Whitepaper—After the crisis comes the blow*. https://northwave-cybersecurity.com/whitepapers-articles/after-the-crisis-comes-the-blow

Perrow, C. (1999). *Normal accidents: Living with high-risk technologies*. Princeton University Press.

Prevezianou, M. F. (2021). Beyond Ones and Zeros: Conceptualizing Cyber Crises. *Risk, Hazards & Crisis in Public Policy*, *12*(1), 51–72. https://doi.org/10.1002/rhc3.12204

Schrijvers, E., Prins, C., & Passchier, R. (2021). *Preparing for Digital Disruption*. Springer International Publishing. https://doi.org/10.1007/978-3-030-77838-5

Schwab, K. (2023, May 31). *The Fourth Industrial Revolution*. Encyclopædia Britannica. https://www.britannica.com/topic/The-Fourth-Industrial-Revolution-2119734

Slowik, J. (2018). *Anatomy of an attack: Detecting and defeating CRASHOVERRIDE*.

Treurniet, W., & Wolbers, J. (2021). Codifying a crisis: Progressing from information sharing to distributed decision-making. *Journal of Contingencies and Crisis Management*, *29*(1), 23–35. https://doi.org/10.1111/1468-5973.12323

van den Berg, B., & Kuipers, S. (2022). Vulnerabilities and Cyberspace: A New Kind of Crises. In B. van den Berg & S. Kuipers, *Oxford Research Encyclopedia of Politics*. Oxford University Press. https://doi.org/10.1093/acrefore/9780190228637.013.1604

van den Berg, B., Prins, R., & Kuipers, S. (2021). Assessing Contemporary Crises: Aligning Safety Science and Security Studies. In B. van den Berg, R. Prins, & S. Kuipers, *Oxford Research Encyclopedia of Politics*. Oxford University Press. https://doi.org/10.1093/acrefore/9780190228637.013.1733

Weick, K. E. (1988). Enacted sensemaking in crisis situations. *Journal of Management Studies*, *25*(4), 305–317. https://doi.org/10.1111/j.1467-6486.1988.tb00039.x

Weick, K. E. (1993). The Collapse of Sensemaking in Organizations: The Mann Gulch Disaster. *Administrative Science Quarterly*, *38*(4), 628. https://doi.org/10.2307/2393339

Weick, K. E. (1995). *Sensemaking in Organizations*,. Sage Publications, Thousand Oaks, CA.

Whitehead, D. E., Owens, K., Gammel, D., & Smith, J. (2017). Ukraine cyber-induced power outage: Analysis and practical mitigation strategies. *2017 70th Annual Conference for Protective Relay Engineers (CPRE)*, 1–8. https://doi.org/10.1109/CPRE.2017.8090056

Wolbers, J. (2022). Understanding distributed sensemaking in crisis management: The case of the Utrecht terrorist attack. *Journal of Contingencies and Crisis Management*, *30*(4), 401–411. https://doi.org/10.1111/1468-5973.12382

Young, T. J. (2015). Questionnaires and Surveys. In Z. Hua (Ed.), *Research Methods in Intercultural Communication* (1st ed., pp. 163–180). Wiley. https://doi.org/10.1002/9781119166283.ch11

List of figures

List of tables

Appendix – E-mail with instructions

Oefenleiders / Exercise leaders

[English below]

Geachte heer/mevrouw,

Mijn naam is Maaike Aansorgh-Bok, ik werk bij netbeheerder Alliander en daarnaast studeer ik Cyber Security aan de Universiteit Leiden. Op dit moment ben ik voor mijn studie bezig met een afstudeer onderzoek, waar ik graag uw hulp bij zou willen inroepen.

Het onderzoek
Ik doe onderzoek naar hoe crisisteams van organisaties in de kritische infrastructuur en overheid duiding geven aan een cyber crisis. Met andere woorden, hoe komen deze crisisteams, op operationeel, tactisch en strategisch niveau, tot een gezamenlijk beeld van de crisis en wat dit betekent? Welke factoren spelen daar een rol in? De context van ISIDOOR is daar bij uitstek geschikt voor, omdat alle deelnemende organisaties in de basis hetzelfde scenario hanteren. Dit maakt de vergelijkbaarheid groot.

Het onderzoek doe ik op basis van de literatuur rondom het concept 'sensemaking', geïntroduceerd door Karl Weick. Ook in de crisismanagement wereld is dit concept bekend, zeker in relatie tot bijvoorbeeld onderzoeken rondom netcentrisch werken. Om het concept in relatie tot cyber crises te kunnen onderzoeken zou ik graag binnen jullie crisisteams de waarnemers een vragenlijst mee willen geven die kan worden ingevuld tijdens ISIDOOR. Deze vragenlijst bevat naast observatievragen voor de teams ook een aantal algemenere vragen over de organisatie. Op die manier kunnen organisaties met elkaar vergeleken worden.

Verwerking van gegevens
Er worden geen vragen gesteld over persoonsgegevens, tenzij de invuller graag persoonlijke terugkoppeling wil ontvangen over de resultaten. Ik vraag daarnaast in de vragenlijst ook naar de naam van de organisatie. Met die informatie kan ik waarnemingen uit verschillende teams van één organisatie met elkaar vergelijken. Na ontvangst van de reacties zal ik de namen van de organisaties coderen en verder weglaten.

Alle reacties op dit onderzoek zullen dus geanonimiseerd worden en strikt vertrouwelijk worden behandeld. De antwoorden zullen niet worden gedeeld met derden en zullen uitsluitend worden gebruikt voor het doel van dit onderzoek. Geen van de verstrekte informatie kan worden herleid tot de identiteit van de invuller. Bij het invullen van de vragenlijst wordt ook nog expliciet om toestemming gevraagd voor het verwerken van de antwoorden en bijbehorende gegevens. Uiteraard is het ook mogelijk om op elk moment af te zien van deelname. In de bijlage vind u een uitgebreidere informatiebrochure met een overzicht van de gegevensverwerking en de toestemmingsverklaring die bij de vragenlijst zit.

Vragen?
Als u naar aanleiding van deze mail vragen hebt over de enquête, het onderzoek, of iets anders, aarzel dan niet om contact met mij op te nemen via e-mail op [e-mail address]. U kunt ook contact opnemen met mijn scriptiebegeleider Cristina del Real via [e-mail address].

Alvast hartelijk dank voor uw medewerking!

Met vriendelijke groet,

Maaike Aansorgh-Bok
[e-mail address]

[English version for exercise leaders]

Dear Sir/Madam,

My name is Maaike Aansorgh-Bok, and I work at regional grid operator of electricity and gas Alliander. Additionally, I am pursuing a master's degree in Cyber Security at Leiden University. I am currently conducting a research project for my thesis and I would like to request your assistance.

The research
I am studying how crisis teams in critical infrastructure organizations and government agencies make sense of a cyber crisis. In other words, I am exploring how these crisis teams develop a shared understanding of the crisis at operational, tactical, and strategic levels, and what this understanding entails. I am particularly interested in the factors that influence this process. The context of ISIDOOR is ideal for my research, as all participating organizations are operating within the same scenario, ensuring comparability.

I am basing my research on the concept of 'sensemaking' introduced by Karl Weick, which is also well-known in the field of crisis management, especially in relation to studies on netcentric operations. To study this concept in the context of cyber crises, I would like to distribute a questionnaire to the observers within your crisis teams during the ISIDOOR exercise. This questionnaire includes observation questions for the teams as well as some general questions about the organization. This approach will allow for comparisons between different organizations.

Data Processing
The questionnaire does not request any personal information, unless the respondent wishes to receive personal feedback on the results. I also ask for the organization's name in the questionnaire. With this information, I can compare observations from different teams within the same organization. Upon receiving responses, I will code and anonymize the names of the organizations, omitting any identifying details.

All responses to this research will be anonymized and treated with strict confidentiality. The answers will not be shared with third parties and will only be used for the purpose of this research. None of the provided information can be traced back to the identity of the respondent. The questionnaire also explicitly requests consent for processing the answers and related data. Of course, participants can choose to withdraw from the study at any time. Please find attached a detailed information brochure outlining the data processing and the consent form that accompanies the questionnaire.

Questions?
If you have any questions regarding this email, the survey, the research, or anything else, please do not hesitate to contact me via email at [e-mail address]. You can also contact my thesis supervisor Cristina del Real at [e-mail address].

Thank you in advance for your cooperation!

Kind regards,

Maaike Aansorgh-Bok
[e-mail address]

Observers

[English below]

Geachte heer/mevrouw,

Mijn naam is Maaike Aansorgh-Bok, ik werk bij netbeheerder Alliander en daarnaast studeer ik Cyber Security aan de Universiteit Leiden. Op dit moment ben ik voor mijn studie bezig met een afstudeer onderzoek, waar ik graag uw hulp bij zou willen inroepen.

Het onderzoek
Ik doe onderzoek naar hoe crisisteams van organisaties in de kritische infrastructuur en overheid duiding geven aan een cyber crisis. Met andere woorden, hoe komen deze crisisteams, op operationeel, tactisch en strategisch niveau, tot een gezamenlijk beeld van de crisis en wat dit betekent? Welke factoren spelen daar een rol in? De context van ISIDOOR is daar bij uitstek geschikt voor, omdat alle deelnemende organisaties in de basis hetzelfde scenario hanteren. Dit maakt de vergelijkbaarheid groot.

Het onderzoek doe ik op basis van de literatuur rondom het concept 'sensemaking', geïntroduceerd door Karl Weick. Ook in de crisismanagement wereld is dit concept bekend, zeker in relatie tot bijvoorbeeld onderzoeken rondom netcentrisch werken. Om het concept in relatie tot cyber crises te kunnen onderzoeken zou ik graag binnen jullie crisisteams de waarnemers een vragenlijst mee willen geven die kan worden ingevuld tijdens ISIDOOR. Deze vragenlijst bevat naast observatievragen voor de teams ook een aantal algemenere vragen over de organisatie. Op die manier kunnen organisaties met elkaar vergeleken worden.

Wat vraag ik van u?
U bent tijdens de ISIDOOR oefening observator van een crisisteam binnen uw organisatie. Graag vraag ik u om *tijdens of direct na afloop* van de oefening voor het crisisteam dat u hebt geobserveerd een vragenlijst in te vullen met daarin vragen over hoe het crisisteam duiding heeft gegeven aan de crisis in het ISIDOOR scenario. De vragen die ik stel gaan over de volgende onderwerpen: demografische vragen over de organisatie, de inrichting van incident response en crisis response. Daarnaast teamgerichte vragen over wat voor soort team u heeft geobserveerd en hoe zij duiding geven aan de crisis.

De link naar deze vragenlijst ontvangt u uiterlijk maandagochtend 13 november via NCSC.

Verwerking van gegevens
Er worden geen vragen gesteld over persoonsgegevens, tenzij de invuller graag persoonlijke terugkoppeling wil ontvangen over de resultaten. Ik vraag daarnaast in de vragenlijst ook naar de naam van de organisatie. Met die informatie kan ik waarnemingen uit verschillende teams van één organisatie met elkaar vergelijken. Na ontvangst van de reacties zal ik de namen van de organisaties coderen en verder weglaten.

Alle reacties op dit onderzoek zullen dus geanonimiseerd worden en strikt vertrouwelijk worden behandeld. De antwoorden zullen niet worden gedeeld met derden en zullen uitsluitend worden gebruikt voor het doel van dit onderzoek. Geen van de verstrekte informatie kan worden herleid tot de identiteit van de invuller. Bij het invullen van de vragenlijst wordt ook nog expliciet om toestemming gevraagd voor het verwerken van de antwoorden en bijbehorende gegevens. Uiteraard is het ook mogelijk om op elk moment af te zien van deelname. In de bijlage vind u een uitgebreidere informatiebrochure met een overzicht van de gegevensverwerking en de toestemmingsverklaring die bij de vragenlijst zit.

Vragen?
Als u naar aanleiding van deze mail vragen hebt over de enquête, het onderzoek, of iets anders, aarzel dan niet om contact met mij op te nemen via e-mail op [e-mail address]. U kunt ook contact opnemen met mijn scriptiebegeleider Cristina del Real via [e-mail address].

Alvast hartelijk dank voor uw medewerking!

Met vriendelijke groet,

Maaike Aansorgh-Bok
[e-mail address]

[English version for observers]

Dear Sir/Madam,

My name is Maaike Aansorgh-Bok, and I work at regional grid operator of electricity and gas Alliander. Additionally, I am pursuing a master's degree in Cyber Security at Leiden University. I am currently conducting a research project for my thesis and I would like to request your assistance.

The research
I am studying how crisis teams in critical infrastructure organizations and government agencies make sense of a cyber crisis. In other words, I am exploring how these crisis teams develop a shared understanding of the crisis at operational, tactical, and strategic levels, and what this understanding entails. I am particularly interested in the factors that influence this process. The context of ISIDOOR is ideal for my research, as all participating organizations are operating within the same scenario, ensuring comparability.

I am basing my research on the concept of 'sensemaking' introduced by Karl Weick, which is also well-known in the field of crisis management, especially in relation to studies on netcentric operations. To study this concept in the context of cyber crises, I would like to distribute a questionnaire to the observers within your crisis teams during the ISIDOOR exercise. This questionnaire includes observation questions for the teams as well as some general questions about the organization. This approach will allow for comparisons between different organizations.

What am I asking from you?
During the ISIDOOR exercise, you will be an observer of a crisis team within your organization. I kindly request you to fill out a questionnaire for the crisis team you have observed, either *during or immediately after the exercise*. The questionnaire contains questions about how the crisis team made sense of the crisis in the ISIDOOR scenario. The questions I will ask cover the following topics: demographic questions about the organization, the setup of incident response and crisis response, as well as team-specific questions about the type of team you observed and how they made sense of the crisis.

<u>You will receive the link to this questionnaire no later than Monday morning, November 13th, via NCSC.</u>

Data Processing
The questionnaire does not request any personal information, unless the respondent wishes to receive personal feedback on the results. I also ask for the organization's name in the questionnaire. With this information, I can compare observations from different teams within the same organization. Upon receiving responses, I will code and anonymize the names of the organizations, omitting any identifying details.

All responses to this research will be anonymized and treated with strict confidentiality. The answers will not be shared with third parties and will only be used for the purpose of this research. None of the provided information can be traced back to the identity of the respondent. The questionnaire also explicitly requests consent for processing the answers and related data. Of course, participants can choose to withdraw from the study at any time. Please find attached a detailed information brochure outlining the data processing and the consent form that accompanies the questionnaire.

Questions?
If you have any questions regarding this email, the survey, the research, or anything else, please do not hesitate to contact me via email at [e-mail address]. You can also contact my thesis supervisor Cristina del Real at [e-mail address].

Thank you in advance for your cooperation!

Kind regards,

Maaike Aansorgh-Bok
[e-mail address]

Appendix - Ethical information brochure

Informatiebrochure en toestemmingsverklaring (English below)

Duiding geven aan cyber crises

Inleiding

Ik ben Maaike Aansorgh-Bok en ik doe onderzoek voor mijn master thesis voor de opleiding Cyber Security aan de Universiteit Leiden. Het onderzoek dat ik doe is gericht op het beschrijven van hoe organisaties duiding geven aan een cyber crisis. Ik voer dit onderzoek uit op een onafhankelijke manier en word hiervoor niet betaald.

Hieronder leg ik het onderzoek uit. Als u iets niet begrijpt, of vragen heeft, dan kunt u die uiteraard aan mij stellen.

Als u wilt meedoen aan het onderzoek, en dat zou ik erg op prijs stellen, dan kunt u dit via de toestemmingsverklaring bij de vragenlijst aangeven.

Waar gaat het onderzoek over?

Het doel van het onderzoek is om inzichtelijk te maken hoe organisaties in de kritische infrastructuur en bij overheden duiding geven aan een nationale cyber crisis. Met andere woorden, hoe komen deze crisisteams, op operationeel, tactisch en strategisch niveau, tot een gezamenlijk beeld van de crisis en wat dit betekent? Welke factoren spelen daar een rol in?

Ik vraag u om mee te doen omdat uw organisatie deelneemt aan ISIDOOR IV, de nationale cyber crisis oefening die wordt georganiseerd door het Nationaal Cyber Security Centrum (NCSC) en de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). De context van ISIDOOR is bij uitstek geschikt voor dit onderzoek, omdat alle deelnemende organisaties in de basis hetzelfde scenario hanteren. Dit maakt de vergelijkbaarheid groot.

Wat kunt u verwachten?

Het onderzoek wordt gedaan middels het invullen van een vragenlijst door waarnemers van crisisteams uit deelnemende organisaties. Dit kunnen crisisteams zijn op operationeel/technisch niveau, maar ook op tactisch of strategisch niveau. Voor sommige organisaties kunnen zelfs op al de genoemde niveaus crisisteams actief zijn. Per actief crisisteam dient een vragenlijst te worden ingevuld door een waarnemer van het betreffende crisisteam. U krijgt de link naar de online vragenlijst per e-mail toegestuurd door NCSC.

Aan het eind van de vragenlijst is er gelegenheid om algemene opmerkingen achter te laten.

U kiest zelf of u meedoet

Deelnemen aan dit onderzoek is geheel vrijwillig. Niet deelnemen heeft geen invloed op uw werk of werk gerelateerde beoordelingen of rapporten. U kunt op ieder moment en zonder uitleg stoppen.

Welke gegevens heb ik van u en uw organisatie nodig?

Ik sla uw (zakelijke) e-mail adres op als u aangeeft dat u op de hoogte wilt worden gesteld van de uitkomsten van het onderzoek. Dit wordt los van de antwoorden op de vragenlijst opgeslagen. Verder sla ik geen persoonlijke gegevens op.

Voor het onderzoek heb ik wel gegevens nodig van uw organisatie. Dit gaat om de volgende gegevens:

- De naam van u organisatie: deze informatie heb ik nodig om de antwoorden van verschillende teams binnen uw organisatie met elkaar te kunnen koppelen en vergelijken. Na ontvangst van alle data wordt de naam van de organisatie vervangen door een code, waardoor de antwoorden niet meer te herleiden zijn naar uw organisatie.
- Algemene demografische gegevens van uw organisatie, zodat ik uw organisatie kan vergelijken met andere organisaties in bijvoorbeeld dezelfde sector.

Hoe lang bewaar ik uw gegevens?

De gegevens worden minimaal 10 jaar bewaard. Ik bewaar de gegevens zodat andere onderzoekers de mogelijkheid hebben om te controleren of het onderzoek juist is uitgevoerd.

(Een deel van) de gegevens die ik over uw organisatie verzamel, kan in (geanonimiseerde) vorm nuttig zijn voor bijvoorbeeld onderwijsdoeleinden en voor toekomstig onderzoek, ook op heel andere onderzoeksterreinen. Mijn thesis zal openbaar beschikbaar zijn. Ik zorg ervoor dat de resultaten niet naar uw organisatie te herleiden zijn.

Wat gebeurt er met de resultaten van het onderzoek?

U kunt aangeven of u de resultaten wilt ontvangen. Daarnaast worden de resultaten via het publiceren van mijn thesis op de thesis website van de Universiteit Leiden openbaar, zodat andere geïnteresseerden kennis kunnen nemen van het onderzoek.

Heeft u vragen over het onderzoek?

Heeft u vragen over het onderzoek of uw privacy rechten, zoals inzage, wijziging, verwijdering of aanpassing van uw gegevens, neem dan contact op met mij, Maaike Aansorgh-Bok via [e-mail address]. U kunt ook contact opnemen met mijn scriptiebegeleider Cristina del Real via [e-mail address].

Spijt van uw deelname?

Het kan zijn dat u spijt krijgt van uw deelname. Geef dit aan of neem hiervoor contact met mij op. Ik verwijder dan uw gegevens. Soms is het nodig om gegevens te bewaren zodat bijvoorbeeld de integriteit van het onderzoek getoetst kan worden.

<u>Toestemmingsverklaring (wordt via de vragenlijst uitgevraagd)</u>

Ik heb de informatiebrief gelezen. Ik begrijp waar het onderzoek over gaat en dat er gegevens van mijn organisatie worden verzameld. Als ik persoonlijk terugkoppeling wil van het onderzoek begrijp ik dat mijn e-mail adres wordt geregistreerd. Dit gebeurt los van de antwoorden op de vragenlijst.

Ook kon ik vragen stellen. Mijn vragen zijn voldoende beantwoord.

Door dit formulier te ondertekenen

1. geef ik toestemming voor deelname aan dit onderzoek
2. geef ik toestemming voor het verwerken van mijn e-mailadres indien ik persoonlijk terugkoppeling wil over de resultaten;
3. bevestig ik dat ik ten minste 18 jaar oud ben; en
4. geef ik aan dat ik begrijp dat deelname aan dit onderzoek geheel vrijwillig is en ieder moment kan stoppen.
5. geef ik aan dat ik begrijp dat de gegevens over mijn organisatie zullen worden geanonimiseerd met het oog op publicatie, en verder gebruik voor onderwijs en onderzoek.

Kruis hieronder de hokjes aan als u hier toestemming voor geeft.

Verplicht voor deelname aan het onderzoek,

Gegevens over mijn organisatie

- ☐ Ik geef toestemming voor het gebruik van de naam van mijn organisatie om gegevens van verschillende crisisteams binnen mijn organisatie aan elkaar te kunnen koppelen.

Optioneel,

- ☐ Ik word graag op de hoogte gehouden van de resultaten van het onderzoek en geef toestemming voor het verwerken van mijn e-mail adres voor dit doel.

Information Brochure and Consent Form

Making sense of Cyber Crises

Introduction

I am Maaike Aansorgh-Bok, conducting research for my master's thesis in Cyber Security at Leiden University. My research focuses on describing how organizations make sense of a cyber crisis. I am conducting this research independently and without financial compensation. Below, I explain the research. If you have any questions or if something is unclear, feel free to ask. If you wish to participate in the research, which I would greatly appreciate, you can indicate your willingness at the end of this form.

What is the Research About?

The aim of this research is to understand how organizations in critical infrastructure and government sectors make sense of a national cyber crisis. In other words, how do these crisis teams, at operational, tactical, and strategic levels, develop a shared understanding of the crisis and its implications? What factors come into play? I am conducting this research independently and without payment.

I invite your organization to participate because your organization is involved in ISIDOOR IV, the national cyber crisis exercise organized by the National Cyber Security Centre (NCSC) and the National Coordinator for Counterterrorism and Security (NCTV). The context of ISIDOOR is particularly suitable for this research, as all participating organizations are operating within the same scenario, ensuring high comparability.

What to Expect?

The research involves completing a questionnaire by observers from crisis teams in participating organizations. These crisis teams can operate at operational/technical, tactical, or strategic levels. Some organizations may have active crisis teams at all these levels. For each active crisis team an observer of this crisis team is required to fill out a questionnaire. You will receive the link to the online questionnaire via email from NCSC. At the end of the questionnaire, there is an opportunity to leave general comments.

Voluntary Participation

Participation in this research is entirely voluntary. Choosing not to participate will not impact your work, work-related evaluations, or reports. You can stop participating at any time without providing an explanation.

Data Collection

I will store your (business) email address if you indicate that you want to be informed about the research outcomes. This information will be stored separately from the questionnaire responses. I do not store any other personal data. For the research, I need the following information about your organization:

- Your organization's name: I need this information to link and compare answers from different teams within your organization. Upon receiving all the data, the name of the organization will be replaced with a code, ensuring that the responses cannot be traced back to your organization.
- General demographic data of your organization, to compare your organization with others, such as those in the same sector.

Data Retention

The data will be retained for a minimum of 10 years. I will keep the data so that other researchers can verify the correctness of the research. Some (or all) of the data collected about your organization may be useful for education purposes and future research in various fields. My thesis will be publicly available, and I will ensure that the results cannot be traced back to your organization.

Use of Research Results

You can choose whether you want to receive the research results. Additionally, the results will be made public through the publication of my thesis on the Leiden University student repository website, allowing other interested parties to learn about the research.

Questions about the Research?

If you have any questions about the research or your privacy rights, such as access, modification, deletion, or adjustment of your data, please contact me via [e-mail address]. You can also contact my thesis supervisor Cristina del Real at [e-mail address].

Regretting Your Participation?

If you regret your participation, please inform me, and I will delete your personal data. Sometimes, it is necessary to retain data to ensure the integrity of the research.

Consent Form (will be signable in the questionnaire)

I have read the information brochure. I understand the purpose of the research and that data from my organization will be collected. If I want personal feedback from the research, I understand that my email address will be stored separately from the questionnaire responses.

I had the opportunity to ask questions, and my questions have been answered satisfactorily.

By signing this form:

- ☐ I consent to participate in this research.
- ☐ I consent to the processing of my email address if I want personal feedback about the results.
- ☐ I confirm that I am at least 18 years old.
- ☐ I understand that participation in this research is entirely voluntary and that I can stop at any time.
- ☐ I understand that the data about my organization will be anonymized for publication and for further use in education and research.

Please check the boxes below to indicate your consent.

Required for Participation in the Research

Organization Data

- ☐ I consent to the use of my organization's name to link data from different crisis teams within my organization.

Optional

- ☐ I would like to be informed about the research results and consent to the processing of my email address for this purpose.

Original post: 23 november 2023

Maaike Aansorgh • U
(Cyber)crisismanagement & informatie gestuurde besluitvorming
1 w •

Heeft jouw organisatie ook meegedaan aan de nationale cyber crisis oefening ISIDOOR IV? Dan ben ik op zoek naar jou!

In de afstudeerfase van de Executive MSc Cyber Security Leiden University die ik volg aan de Universiteit Leiden doe ik onderzoek naar hoe crisisteams van kritische infrastructuur organisaties en overheden 'chocola maken' van een cyber crisis. Om daar eerste inzichten in te kunnen geven, heb ik een vragenlijst opgesteld, zie de link hieronder. Ik stel hierin vragen over het gedrag van crisisteams waar het gaat om duiding geven aan de cyber crisis.

Ben jij of is jouw organisatie betrokken geweest bij deze oefening?
Dan zou je me heel erg helpen als je deze vragenlijst wil laten invullen door de waarnemers/observatoren van de crisisteams op technisch/operationeel, tactisch en strategisch niveau die binnen jouw organisatie hebben meegedaan. Dat kunnen dus ook Incident Response teams of (sectorale) CERT's/CSIRT's zijn!

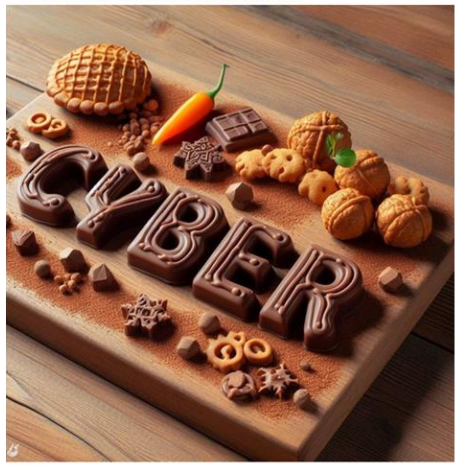
De link naar de vragenlijst: https://lnkd.in/ehSrPTdk

De vragenlijst staat open tot 5 december 17:00u en kost je ongeveer 15 minuten om in te vullen. Geef jij mij een mooi Sinterklaas cadeau? 😉

Heb je vragen? Laat het me dan even weten via een privé bericht of mail naar m.bok.2@umail.leidenuniv.nl

Delen is lief!

#ISIDOOR #CYBER #CRISIS #ONDERZOEK #OEFENING



Martin Molema ing. Msc. en 48 anderen 16 commentaren • 17 reposts

https://www.linkedin.com/posts/maaikebok_isidoor-cyber-crisis-activity-7133377884911464448-xVGq?utm_source=share&utm_medium=member_desktop

Reminder 1: 29 november 2023

Maaike Aansorgh • U
(Cyber)crisismanagement & informatie gestuurde besluitvorming
1 w • Bewerkt •

Heeft jouw organisatie ook meegedaan aan de nationale cyber crisis oefening ISIDOOR?
Lees dan dit bericht en let goed op hoor!

📘 Ben jij een organisatie die mee heeft gedaan?
Vul dan mijn vragenlijst in heel spontaan!

🍫 Het gaat over hoe je chocola maakt van cybercrises
Dat heeft echt aandacht nodig, nogal wiedes!

❓ Sensemaking en framing, hoe doet een team dat?
In de literatuur wel beschreven, maar in praktijk nog een gat.

☑️ Er zijn al aardig wat responses met waardevolle informatie
Toch heb ik er méér nodig, kom op met jullie participatie!

🔍 De doelgroep zijn de waarnemers van deze teams.
Zij kennen het gedrag dat ik graag terug zou zien.

⏰ Op 5 december om 17:00 is de finale deadline.
Hieronder de link, als je 'm invult zal ik blij zijn 😁

https://lnkd.in/ehSrPTdk

❤️ Ik vind het heel fijn als je deze post deelt,
dan komt-ie ook in jouw netwerk en tsjonge, dat scheelt!

ℹ️ Meer informatie, dat zoek je allicht.
Dat is ook te vinden via mijn vorige bericht:
https://lnkd.in/ehxziiCA

#ISIDOOR #CYBER #CRISIS #ONDERZOEK #OEFENING
#VITALEINFRA #OVERHEID #AFSTUDEREN

PS: ik doe dit afstudeeronderzoek voor de Executive MSc Cyber Security Leiden University aan de Universiteit Leiden en volg deze opleiding naast mijn baan als crisismanager bij Alliander / Liander.

https://www.linkedin.com/posts/maaikebok_isidoor-cyber-crisis-activity-7135571226768347136-gf50?utm_source=share&utm_medium=member_desktop

Reminder 2: 5 december 2023

Maaike Aansorgh • U
(Cyber)crisismanagement & informatie gestuurde besluitvorming
1 d • Bewerkt •

LAATSTE KANS! Heeft jouw organisatie ook meegedaan aan de nationale cyber crisis oefening ISIDOOR?

💂 Grijp dan nu de laatste kans om mee te doen aan mijn afstudeeronderzoek over hoe organisaties "chocola maken" van een cyber crisis.

👉 Ik ben op zoek naar observatoren/waarnemers van incident response teams en crisis teams van deelnemende organisaties, die mijn vragenlijst kunnen invullen die je vindt via deze link: https://lnkd.in/ehSrPTdk

🎯 In de vragenlijst stel ik vragen over het zichtbare gedrag van deze teams waar het gaat om duiding/betekenis geven aan de cyber crisis. De antwoorden worden anoniem verwerkt en helpen inzicht te geven in hoe we dit in Nederland doen!

⏰ Dit is echt je laatste kans om mee te helpen! De vragenlijst staat open tot 5 december 17:00u en kost je ongeveer 15 minuten om in te vullen.

❓ Heb je vragen? Laat het me dan even weten via een privé bericht of mail naar m.bok.2@umail.leidenuniv.nl

Delen is lief!!

#ISIDOOR #CYBER #CRISIS #ONDERZOEK #OEFENING
#VITALEINFRA #OVERHEID #AFSTUDEREN

PS: ik doe dit afstudeeronderzoek voor de Executive MSc Cyber Security Leiden University aan de Universiteit Leiden en volg deze opleiding naast mijn baan als crisismanager bij Alliander / Liander.

https://www.linkedin.com/posts/maaikebok_isidoor-cyber-crisis-activity-7137752574681600000-FxEy

Appendix – Full questionnaire

ISIDOOR

Enquêteflow

Standard: Introductie (1 Question)
Standard: Check (1 Question)
Standard: Section 1. Team demographics (5 Questions)
Standard: Section 2. Observations of team sensemaking behavioral markers (3 Questions)
Standard: Section 3. Observations of situational sensemaking (3 Questions)
Standard: Section 4. Observations of identity-oriented sensemaking (5 Questions)
Standard: Section 5. Observations of action-oriented sensemaking (4 Questions)
Standard: Section 6. Your organisation (11 Questions)
Standard: Section 7. Own observations (5 Questions)
Standard: Thanks (1 Question)

Pagina-einde

Start van blok: Introductie

Introductie

Dank u voor uw deelname aan dit onderzoek!

Mijn naam is Maaike Aansorgh-Bok en ik voer een enquête uit over cybercrisismanagement voor mijn masteropleiding Cyber Security aan de Universiteit Leiden. Het invullen van deze enquête kost u ongeveer 15 minuten.

Doel van het onderzoek

Ik doe onderzoek naar hoe crisisteams van organisaties in de kritische infrastructuur en overheid duiding geven aan een nationale cyber crisis. Met andere woorden, hoe komen deze crisisteams, op operationeel, tactisch en strategisch niveau, tot een gezamenlijk beeld van de crisis en wat dit betekent? De context van ISIDOOR is daar bij uitstek geschikt voor, omdat alle deelnemende organisaties in de basis hetzelfde scenario hanteren. Dit maakt de vergelijkbaarheid groot.

Wat wordt er gevraagd?

Per geobserveerd team wordt één volledige vragenlijst ingevuld. Dus als er meerdere teams uit de organisatie meedoen, dan graag ook meerdere keren deze vragenlijst invullen.

U kiest zelf of u meedoet

Deelnemen aan dit onderzoek is geheel vrijwillig. Niet deelnemen heeft geen invloed

op uw werk of werk gerelateerde beoordelingen of rapporten. U kunt op ieder moment en zonder uitleg stoppen.

Welke gegevens heb ik van u en uw organisatie nodig?

Ik sla uw (zakelijke) e-mail adres op als u aangeeft dat u op de hoogte wilt worden gesteld van de uitkomsten van het onderzoek. Dit wordt los van de antwoorden op de vragenlijst opgeslagen. Verder sla ik geen persoonlijke gegevens op.

Voor het onderzoek heb ik wel gegevens nodig van uw organisatie. Dit gaat om de volgende gegevens: De naam van uw organisatie: deze informatie heb ik nodig om de antwoorden van verschillende teams binnen uw organisatie met elkaar te kunnen koppelen en vergelijken. Na ontvangst van alle data wordt de naam van de organisatie vervangen door een code, waardoor de antwoorden niet meer te herleiden zijn naar uw organisatie. Algemene demografische gegevens van uw organisatie, zodat ik uw organisatie kan vergelijken met andere organisaties in bijvoorbeeld dezelfde sector.

Alle reacties op dit onderzoek zullen dus geanonimiseerd worden en strikt vertrouwelijk worden behandeld. De antwoorden zullen niet worden gedeeld met derden en zullen uitsluitend worden gebruikt voor het doel van dit onderzoek. Geen van de verstrekte informatie kan worden herleid tot de identiteit van de invuller.

Heeft u vragen over het onderzoek?

Heeft u vragen over het onderzoek of uw privacy rechten, zoals inzage, wijziging, verwijdering of aanpassing van uw gegevens, neem dan contact op met mij, Maaike Aansorgh-Bok via [e-mail address].

U kunt ook contact opnemen met mijn scriptiebegeleider Cristina del Real via [e-mail address].

Bij voorbaat dank voor uw deelname!

Toestemmingsformulier

Ik heb de informatiebrief gelezen. Ik begrijp waar het onderzoek over gaat en dat er gegevens van mijn organisatie worden verzameld. Als ik persoonlijk terugkoppeling wil van het onderzoek begrijp ik dat mijn e-mail adres wordt geregistreerd aan het einde van de vragenlijst. Dit gebeurt los van de antwoorden op de vragenlijst.

Ook kon ik vragen stellen. Mijn vragen zijn voldoende beantwoord.

Door dit formulier te ondertekenen:

1. geef ik toestemming voor deelname aan dit onderzoek
2. geef ik toestemming voor het verwerken van mijn e-mailadres indien ik persoonlijk terugkoppeling wil over de resultaten;
3. bevestig ik dat ik ten minste 18 jaar oud ben; en
4. geef ik aan dat ik begrijp dat deelname aan dit onderzoek geheel vrijwillig is en ieder moment kan stoppen.
5. geef ik aan dat ik begrijp dat de gegevens over mijn organisatie zullen worden geanonimiseerd met het oog op publicatie, en verder gebruik voor onderwijs en onderzoek.

Kruis hieronder de hokjes aan als u hier toestemming voor geeft.

Verplicht voor deelname aan het onderzoek: gegevens over mijn organisatie Ik geef toestemming voor het gebruik van de naam van mijn organisatie om gegevens van verschillende crisisteams binnen mijn organisatie aan elkaar te kunnen koppelen.

Optioneel: eigen e-mail adres Ik word graag op de hoogte gehouden van de resultaten van het onderzoek en geef toestemming voor het verwerken van mijn e-mail adres voor dit doel.

○ Ik geef toestemming voor het gebruik van de naam van mijn organisatie om gegevens van verschillende crisisteams binnen mijn organisatie aan elkaar te kunnen koppelen. (1)

○ Ik stem hier niet mee in, ik wens niet deel te nemen (2)

Ga naar: Einde enquête Als Introductie = 2

Pagina-einde

Einde blok: Introductie

Start van blok: Check

Check participation Voordat we beginnen met de enquête: doet uw organisatie mee aan ISIDOOR 2023?

- ○ Ja (1)
- ○ Nee (2)

Ga naar: Einde enquête Als Check participation = 2

Pagina-einde

Einde blok: Check

Start van blok: Section 1. Team demographics

Intro1 U heeft een team geobserveerd dat meedoet aan ISIDOOR IV 2023. De volgende vragen gaan over de organisatie en vervolgens dieper in op het soort team en het doel dat het team had.

Let op: per team dat is geobserveerd een aparte enquête invullen!

Org Name Wat is de naam van de organisatie?

_____

Org Sector In welke sector is de organisatie actief? Als de organisatie in meerdere sectoren actief is, kies dan de sector waarin de organisatie voornamelijk actief is.

- ○ Algemene kolom (1)
- ○ Chemie (2)
- ○ Cyberstelsel (3)
- ○ Drinkwater (4)
- ○ Energie (5)
- ○ Financiën (6)
- ○ Gemeenten (7)
- ○ Haven (8)
- ○ Luchtvaart (9)
- ○ MKB (10)
- ○ Nucleair (11)
- ○ Attributie & opsporing (12)
- ○ Rijksoverheid (13)
- ○ Telecom (14)
- ○ Toeleveranciers (15)
- ○ Transport (16)
- ○ Waterbeheer (17)
- ○ Zorg (18)
- ○ Anders, namelijk (19) _____

Type of team Welk type team heeft u geobserveerd?

- ○ Een operationeel/technisch team (bijvoorbeeld Incident response team / operationeel crisis team / Commando Plaats Incident (COPI) (1)
- ○ Een tactisch team (bijvoorbeeld tactisch crisisteam, Regionaal Operationeel team (ROT)) (2)
- ○ Een strategisch team (bijvoorbeeld strategisch crisis team, beleids team, gemeentelijk beleidsteam (GBT), regionaal beleidsteam (RBT) (3)
- ○ Politiek/ministerieel team (bijvoorbeeld DCC / IAO / ICCb / MCCb) (4)
- ○ Anders, namelijk (5)
  _____

Goal of team Wat is het formele doel van het team dat u heeft geobserveerd?

- ○ Incident response - technisch/operationele activiteiten die nodig zijn voor analyse, de-escalatie en technisch oplossen van het incident. (1)
- ○ Incident handling - activiteiten die nodig zijn om terug te gaan naar de normale operatie, systemen en beveiliging te herstellen, inclusief logistiek, communicatie, planning, coördinatie, processen en procedures. (2)
- ○ Crisis response – activiteiten die nodig zijn om de acute fase van een crisis te beheersen en de impact te minimaliseren, inclusief stakeholder management en crisiscommunicatie. (3)
- ○ Ik weet het niet (4)
- ○ Anders, namelijk (5)
  _____

Pagina-einde

Einde blok: Section 1. Team demographics

Start van blok: Section 2. Observations of team sensemaking behavioral markers

Intro2 In dit onderzoek kijken we naar hoe teams omgaan met de duiding van een nationale cyber crisis zoals tijdens ISIDOOR IV 2023 wordt geoefend. Dit duidingsproces heeft tot doel om eerdere gebeurtenissen te verklaren en te anticiperen op toekomstige gebeurtenissen. Duiding gaat dan ook om het proces van data binnen een **frame** te kunnen plaatsen en een frame te maken rondom de beschikbare data.

Een **frame** is eigenlijk een organiserend middel, zoals bijvoorbeeld een verhaal, het script van een film of een stadskaart. Iets waarmee mensen elkaar duidelijk kunnen maken wat er aan de hand is.

Hieronder geef ik een lijst van gedragingen die je mogelijk hebt kunnen waarnemen bij het team tijdens de ISIDOOR-oefening.

Let op: de vragen gaan over hetzelfde team dat je geselecteerd hebt in de vorige sectie!

Klein Kruis alsjeblieft de gedragingen aan die je hebt waargenomen bij het team van jouw organisatie dat je hebt geobserveerd tijdens de ISIDOOR-oefening. Tijdens de

ISIDOOR oefening heb ik gezien dat het team dat ik observeerde de volgende gedragingen liet zien:

- ☐ Het team heeft criteria of regels geformuleerd om het frame te identificeren (1)
- ☐ Een teamlid kondigde aan wat het frame is (2)
- ☐ Het team werkt samen om het frame te identificeren (3)
- ☐ Het team kiest een teamlid om de rol van de advocaat van de duivel op zich te nemen en twijfels te uiten over de geschiktheid van het kader (4)
- ☐ Het team stelt regels of criteria op om hen te waarschuwen dat het kader mogelijk niet geschikt is (5)
- ☐ Teamleden uiten en bespreken wat er mis zou kunnen gaan met het huidige frame (6)
- ☐ Het team vergelijkt frames en besluit uiteindelijk om voor één te stemmen (7)
- ☐ Het team komt tot consensus over welk frame het meest geschikt is (8)
- ☐ De voorzitter van het team kondigt aan welk frame het meest geschikt is. (9)
- ☐ Het team vergelijkt frames en eindigt met het stemmen voor één (10)
- ☐ Een teamlid stelt een frame voor en het wordt overgenomen, aangepast of afgewezen terwijl het team frames vergelijkt (11)
- ☐ Het team speculeert over gegevens (data) en suggereert causale overtuigingen (overtuigingen die iemand heeft over de oorzakelijke verbanden

tussen gebeurtenissen); de voorzitter van het team of een teamlid combineert deze standpunten tot een frame (12)

☐ Het team werkt samen om concurrerende frames samen te stellen (13)

☐ Het team bespreekt en wijst afwijkingen in de gegevens af als voorbijgaande signalen of anderszins onbeduidend (14)

☐ De gegevensverwerkers van het team (bijvoorbeeld informatiefunctionarissen) sturen de activiteiten van de gegevensverzamelaars (andere teams of personen buiten het team) aan om nieuwe gegevens te zoeken om het frame te verifiëren (15)

☐ De gegevensverwerkers en gegevensverzamelaars van het team werken samen om nieuwe relaties te ontdekken die het frame behouden of uitbreiden (16)

Opinion Klein Zijn er nog zaken die je bij dit onderwerp zijn opgevallen aan het team?

_____

_____

_____

_____

_____

Pagina-einde

Einde blok: Section 2. Observations of team sensemaking behavioral markers

Start van blok: Section 3. Observations of situational sensemaking

Intro3 Deze sectie gaat over het delen van informatie, het begrijpen van de crisis en het begrijpen van de plek van het eigen team in het (in- en externe) netwerk tijdens de ISIDOOR-oefening. Kruis alsjeblieft de gedragingen aan die je hebt waargenomen bij het team van jouw organisatie dat je hebt geobserveerd tijdens de ISIDOOR-oefening.

Kalkman SitSens Kruis alsjeblieft alle antwoorden aan die van toepassing zijn. Tijdens de ISIDOOR-oefening heb ik waargenomen dat mijn team de volgende gedragingen vertoonde:

- ☐ De teamleden delen informatie over de cybercrisis met elkaar (1)
- ☐ De teamleden presenteren hun informatie zo feitelijk en objectief mogelijk (2)
- ☐ Het team kan een gedeeld gemeenschappelijk beeld van de cybercrisis creëren (3)
- ☐ Het team begrijpt de aard van de cybercrisis (4)
- ☐ Het team begrijpt de oorzaak van de cybercrisis (5)
- ☐ Het team begrijpt de potentiële toekomstige risico's van de cybercrisis (6)
- ☐ Het team begrijpt de gevolgen van de cybercrisis voor hun eigen organisatie (7)
- ☐ Het team weet welke andere teams betrokken zijn binnen hun eigen organisatie (8)
- ☐ Het team weet welke andere organisaties betrokken zijn buiten hun eigen organisatie (9)
- ☐ Het team gebruikt informatie van andere organisaties om hun eigen beeld van de cybercrisis aan te scherpen of aan te vullen (10)

Opinion SitSens Zijn er nog zaken die je bij dit onderwerp zijn opgevallen aan het team?

_____

_____

_____

_____

_____

Pagina-einde

Einde blok: Section 3. Observations of situational sensemaking

Start van blok: Section 4. Observations of identity-oriented sensemaking

Intro4 In deze sectie zullen we de rol van het team en de teamidentiteit tijdens de simulatie van de cybercrisis onderzoeken. Markeer alsjeblieft de gedragingen die je hebt waargenomen bij het team van jouw organisatie tijdens de ISIDOOR-oefening.

Kalkman Indiv Role Welke rol nemen de individuele teamleden voornamelijk aan?

- ○ Organizational liaison: vertegenwoordigt een organisatieonderdeel (1)
- ○ Team member: is primair lid van het team (2)
- ○ Professional/expert: is een expert op een bepaald onderwerp (3)

Kalkman Team role Kruis alsjeblieft zoveel mogelijk vakjes aan die van toepassing zijn. Tijdens de ISIDOOR-oefening heb ik waargenomen dat het team dat ik observeerde de

volgende gedragingen vertoonde.

- [ ] Het team weet wat hun eigen rol is in deze cybercrisis. (1)
- [ ] Het team heeft een gezamenlijke identiteit. De teamleden identificeren zich met het team als geheel en hebben een gevoel van een gemeenschappelijk doel en voelen zich verbonden met elkaar. (2)
- [ ] Het team heeft de focus op hun eigen niveau van opereren (operationeel, tactisch, strategisch (3)
- [ ] Het team komt tot een gezamenlijke conclusie waarvoor ze aan tafel zitten (4)

Team role opinion Denk nog eens terug aan de rol van het team dat je hebt waargenomen tijdens de simulatie van de cybercrisis. Hoe was deze rol zichtbaar?

_____

_____

_____

_____

_____

Team id opinion Denk nog eens terug aan de identiteit van het team dat je hebt waargenomen tijdens de simulatie van de cybercrisis. Hoe was deze identiteit zichtbaar?

_____

_____

_____

_____

_____

Pagina-einde

Intro5

In deze sectie zullen we kijken naar de gevolgen van de acties die crisisteams uitzetten. Deze beïnvloeden ook het vervolg van de crisis zelf. Het team zal hierover ook in gesprek gaan, door te kijken naar de vraag: hoe maakt het uit wat wij doen? Daarnaast werken teams mogelijk ook aan de hand van bestaande plannen en procedures.

Markeer alsjeblieft de gedragingen die je hebt waargenomen bij het team van jouw organisatie tijdens de ISIDOOR-oefening.

Kalkman ActSens Kruis alsjeblieft zoveel mogelijk vakjes aan die van toepassing zijn. Tijdens de ISIDOOR-oefening heb ik waargenomen dat het team dat ik observeerde de

volgende gedragingen liet zien:

- [ ] Het team verwijst naar of maakt gebruik van bestaande plannen, procedures, etc. (1)
- [ ] Het team is het eens over welke bestaande plannen/procedures etc. van toepassing zijn (2)
- [ ] Het team debatteert over tegenstrijdige plannen/procedures (3)
- [ ] Het team verwijst terug naar eerdere acties in een nieuwe vergadering (4)
- [ ] Het team past de resultaten van de vorige acties toe op een nieuw betekenis gevend proces (5)
- [ ] Het team houdt rekening met wat andere teams (binnen de eigen organisatie) hebben gedaan (6)
- [ ] Het team houdt rekening met wat andere organisaties hebben gedaan (7)

ACT teams Denk nog eens terug aan het rekening houden met wat *andere teams* hebben gedaan. Met welke andere teams binnen de eigen organisatie hield het team rekening en hoe was dit zichtbaar?

_____

_____

_____

_____

_____

ACT orgs Denk nog eens terug aan het rekening houden met wat *andere organisaties* hebben gedaan. Met welke andere organisaties hield het team rekening en hoe was dit zichtbaar?

_____

_____

_____

_____

_____

Pagina-einde

Einde blok: Section 5. Observations of action-oriented sensemaking

Start van blok: Section 6. Your organisation

Intro6 In deze sectie vragen we je een aantal demografische gegevens van je organisatie in te vullen en om aan te geven hoe je organisatie omgaat met Incident Response en Crisis Response.

X→

Org Size Wat is de grootte van de organisatie? Aantal werknemers:

- 1-9 (1)
- 10-49 (2)
- 50-99 (3)
- 100-249 (4)
- 250-499 (5)
- 500-999 (6)
- 1000-4999 (7)
- 5000 of meer (8)
- Weet ik niet (9)

Org ISAC Is de organisatie onderdeel van een Information Sharing and Analysis Centre (ISAC)?

- ○ Ja (1)
- ○ Nee (2)
- ○ Weet ik niet (3)

Org SecCERT Is de organisatie onderdeel van een sectorale Computer Emergency Response Team (CERT) of Computer Security Incindent Response Team (CSIRT)?

- ○ Ja (1)
- ○ Nee (2)
- ○ Weet ik niet (3)

Pagina-einde

In-house IR Heeft uw organisatie een eigen (in-house) Incident Response team?

- ○ Ja (1)
- ○ Nee, het is extern ingehuurd (2)
- ○ Anders, namelijk (3) _____

IR model Maakt uw organisatie gebruik van een gestandaardiseerd Incident Response model voor het inrichten van Incident Response binnen de organisatie?

- ○ Ja, van de NIST Incident Response Lifecyle (1)
- ○ Ja, van de SANS Incident Response Cycle (2)
- ○ Ja, van het F3EAD model voor Intelligence driven Incident Response (3)
- ○ Nee (4)
- ○ Ik weet het niet (5)
- ○ Anders, namelijk (6) _____

CR organization Heeft uw organisatie een crisisorganisatie ingericht die losstaat van de reguliere organisatie?

- ○ Ja (1)
- ○ Nee (2)
- ○ Ik weet het niet (3)

All-hazard Maakt uw organisatie gebruik van een all-hazard aanpak van crisissituaties?

- ○ Ja (1)
- ○ Nee (2)
- ○ Ik weet het niet (3)
- ○ Anders, namelijk (4) _____

Crisis WOW Welke werkwijze gebruikt de organisatie in crisissituaties?

- ○ Netcentrische werkwijze waarin informatie continu met alle betrokkenen gedeeld wordt (1)
- ○ Hiërarchische werkwijze waarin informatie via vooraf vastgestelde kanalen de organisatie in gaat en ook weer terugkomt (2)
- ○ Ad hoc en opportunistisch, zonder onderliggende vastgestelde afspraken over het uitwisselen van informatie (3)
- ○ Anders, namelijk (4) _____

Info doctrine Hoe kijkt de organisatie aan tegen crisis informatie management?

- ○ Alle informatie over de crisis wordt vergaard, geanalyseerd, gerapporteerd en georganiseerd, op een gestructureerde en uniforme manier. Op basis hiervan worden besluiten genomen. (1)
- ○ Alle informatie over de crisis moet worden besproken in de crisisteams, waarbij betekenis, waarde en gevolgen van deze informatie worden beoordeeld. Pas daarna worden besluiten genomen. (2)
- ○ Anders, namelijk (3) _____

CMS Werkt uw organisatie bij crisis situaties met een crisis management systeem als technische ondersteuning voor het crisis management?

- ○ Ja, wij gebruiken het Landelijk Crisis Management Systeem (1)
- ○ Ja, wij gebruiken een ander crisismanagement systeem, namelijk […] (2)
- ○ Nee, wij gebruiken alleen interne systemen (3)
- ○ Anders, namelijk (4) _____

Pagina-einde

Intro7 Welke aanbevelingen zou je nog mee willen geven als het gaat om het verbeteren van de duiding van cyber crisis situaties? Deze vragen zijn optioneel.

Teamsense+ Op welke wijze zou volgens u de duiding van een cyber crisis verbeterd kunnen worden *op team niveau*?

_____

_____

_____

_____

_____

Orgsense+ Op welke wijze zou volgens u de duiding van een cyber crisis verbeterd kunnen worden *op organisatie niveau*?

_____

_____

_____

_____

_____

MultipleOrgsense+ Op welke wijze zou volgens u de duiding van een cyber crisis verbeterd kunnen worden *tussen organisaties*?

_____

_____

_____

_____

_____

Other Opinions Zijn er nog andere zaken die u wilt meegeven in het kader van dit onderzoek?

_____

_____

_____

_____

_____

Einde blok: Section 7. Own observations

Start van blok: Thanks

E-mail

Hartelijk dank voor het invullen van de vragenlijst! Mocht je belangstelling hebben om de resultaten persoonlijk te ontvangen na afloop van het onderzoek, laat dan hieronder je e-mail adres achter.

Dit is optioneel en je e-mail adres wordt enkel gebruikt om je te informeren in het kader van dit onderzoek.

_____

Einde blok: Thanks

Appendix – Full interview protocol

Interview preparations

Introductie

Super fijn dat je wilt meewerken aan mijn onderzoek! Voordat ik wil beginnen met het interview wil ik je toestemming vragen om het op te nemen en een automatische transcriptie te starten.

[consent = starten opname en transcriptie, taal op NL zetten!]

Voorstellen

Mijn naam is Maaike Aansorgh, ik werk als crisismanager Energie bij netbeheerder Alliander en doe daarnaast de Executive Master Cyber Security aan de Universiteit Leiden. Op dit moment ben ik een afstudeeronderzoek aan het doen naar hoe crisisteams chocola maken van een cyber crisis.

En wie ben jij. Waar werk je en wat doe je?

Heb je nog vragen vooraf?

Het onderzoek

Ik zal mijn onderzoek even kort introduceren. In mijn afstudeeronderzoek kijk ik naar hoe teams omgaan met de betekenisgeving of duiding van een nationale cyber crisis zoals bijvoorbeeld tijdens ISIDOOR IV 2023 wordt geoefend. Dit duidingsproces heeft tot doel om eerdere gebeurtenissen te verklaren en te anticiperen op toekomstige gebeurtenissen.

Duiding gaat dan ook om het proces van beschikbare data binnen een **frame** te kunnen plaatsen en een **frame** te maken rondom de beschikbare data.

Een **frame** is eigenlijk een organiserend middel, zoals bijvoorbeeld een verhaal, het script van een film of een stadskaart. Iets waarmee mensen elkaar duidelijk kunnen maken wat er aan de hand is.

Framing is daarmee een onderdeel van beeldvorming over de crisis. In dit onderzoek heb ik gekeken naar gedrag van incident response en crisis response teams, en hoe zij omgaan met framing.

Framing bestaat uit een aantal componenten die in gedrag kunnen terugkomen.

1. Het identificeren van een frame
2. Het ter discussie stellen van een frame
3. Opnieuw framen door frames te vergelijken
4. Opnieuw framen door een nieuw frame te maken
5. Het uitbreiden van een frame

Daarnaast heb ik onderzoek gedaan naar soorten ‘sensemaking’ vragen die in crisis teams gesteld kunnen worden. Dat bestaat uit de volgende componenten:

1. Situational sensemaking, waarbij information sharing, crisis understanding en network understanding onderwerpen zijn
2. Identity-oriented sensemaking, waarbij gekeken wordt naar welke rol de teamleden aannemen en de rol en identiteit van het team zelf
3. Action-oriented sensemaking, waarbij gekeken wordt naar het gebruik van voorbereide plannen (scripted actions) en of een team rekening houdt met de veranderende crisis realiteit (actions and enactment)

Doel van dit interview

Jij bent vertegenwoordiger van een organisatie die andere organisaties helpt om incident response en crisis response bij oa cyber crises in te richten en daarop te trainen en oefenen. Het doel van ons gesprek is om vanuit jouw perspectief te kijken naar drie thema's:

1. Hoe geven de organisaties waar je mee werkt betekenis/duiding aan een cyber crisis?
2. Welke uitdagingen zie je op het gebied van betekenis/duiding geven aan een cyber crisis?
3. Hoe zou betekenis/duiding geven aan een cyber crisis kunnen worden verbeterd?

Interview questions based on the 3 main themes

Sensemaking binnen crisisteams die te maken krijgen met een cybercrisis

1. Hoe maken organisaties waar je mee werkt chocola van een cyber crisis? Welk gedrag laten zijn zien met betrekking tot framing? Welke soort duidingsvragen stellen zij?
   How do you see IR and CR teams you work with make sense of a cyber crisis? What behavior do they show in terms of framing? What types of sensemaking questions do they ask?

2. Zijn er verschillen tussen operational/technical, tactical, strategic or political teams?
   Are there differences between operational/technical, tactical, strategic or political teams?

3. Hoe kunnen deze verschillen worden verklaard volgens jou?
   How can these differences be explained according to you?

Uitdagingen

4. Wat zijn de voornaamste uitdagingen die je ziet waar het gaat om sensemaking van cyber crises? Waar komt dat door?
   What challenges do you see? Why? What causes this?

Verbeteren van sensemaking

5. Op welke wijze zou volgens jou de duiding van een cyber crisis verbeterd kunnen worden *op team niveau*?
   How can sensemaking of a cyber crisis become better on intra-team level?

6. Op welke wijze zou volgens jou de duiding van een cyber crisis verbeterd kunnen worden *op organisatie niveau tussen teams*?
   How can sensemaking of a cyber crisis become better on inter-team level within one organization?

7. Op welke wijze zou volgens jou de duiding van een cyber crisis verbeterd kunnen worden *tussen organisaties*?
   How can sensemaking of a cyber crisis become better on inter-organizational level?

Final question: Welke zaken vallen jou op rondom dit onderwerp die je nog niet hebt genoemd maar wel relevant zijn?