Developing decision support for cybersecurity threat and incident managers

Rick van der Kleij , Jan Maarten Schraagen , Beatrice Cadet , Heather Young

PII: S0167-4048(21)00359-X
DOI: https://doi.org/10.1016/j.cose.2021.102535
Reference: COSE 102535

To appear in: *Computers & Security*

Received date: 13 April 2021
Revised date: 28 September 2021
Accepted date: 2 November 2021

Please cite this article as: Rick van der Kleij , Jan Maarten Schraagen , Beatrice Cadet , Heather Young , Developing decision support for cybersecurity threat and incident managers, *Computers & Security* (2021), doi: https://doi.org/10.1016/j.cose.2021.102535

Developing decision support for cybersecurity threat and incident managers

Rick van der Kleij [a, c, *], Jan Maarten Schraagen [b], Beatrice Cadet [a] & Heather Young [a]

[a] Department of Human Behaviour and Training, TNO, The Netherlands

[b] Department of Human Machine Teaming, TNO, The Netherlands

[c] Research group Cybersecurity in the SME Sector, The Hague University of Applied Sciences, The Netherlands

[*] Correspondence: Rick.vanderkleij@tno.nl

Abstract: Cybersecurity threat and incident managers in large organizations, especially in the financial sector, are confronted more and more with an increase in volume and complexity of threats and incidents. At the same time, these managers have to deal with many internal processes and criteria, in addition to requirements from external parties, such as regulators that pose an additional challenge to handling threats and incidents. Little research has been carried out to understand to what extent decision support can aid these professionals in managing threats and incidents. The purpose of this research was to develop decision support for cybersecurity threat and incident managers in the financial sector. To this end, we carried out a cognitive task analysis and the first two phases of a cognitive work analysis, based on two rounds of in-depth interviews with ten professionals from three financial institutions. Our results show that decision support should address the problem of balancing the bigger picture with details. That is, being able to simultaneously keep the broader operational context in mind as well as adequately investigating, containing and remediating a cyberattack. In close consultation with the three financial institutions involved, we developed a critical-thinking memory aid that follows typical incident response process steps, but adds

big picture elements and critical thinking steps. This should make cybersecurity threat and incident managers more aware of the broader operational implications of threats and incidents while keeping a critical mindset. Although a summative evaluation was beyond the scope of the present research, we conducted iterative formative evaluations of the memory aid that show its potential.

Keywords: Cybersecurity; Cognitive task analysis; Cognitive work analysis; Decision support; Incident response; Information security risk management

1. Introduction

External and internal developments pose a challenge for teams tasked with managing cybersecurity threats and incidents. Not only is the number of threats and incidents growing, but also the complexity and sophistication of attacks has increased over the years resulting in successful intrusions with more severe forms of security breaches (Allianz, 2020; Naseer, Naseer, Ahmad, Maynard, & Siddiqui, 2021; Shinde & Kulkarni, 2021; Schlette, Böhm, Caselli, & Pernul, 2020; Verizon, 2020). At the same time, the threat and incident management function for individual organizations is under-developed with a strong focus on the technological dimension with little consideration of practical capability (O'Neill, Ahmad, & Maynard, 2021). Incident management processes are becoming more difficult due to the growing number of indicators that need to be considered when dealing with threats and incidents. These include new threat actors, intensified threat actor activity, increased availability of threat intelligence, and improved visibility on networks and workstations as new data sources are being connected to cyber defense centers or CDCs. The CDC, a new name coined for a security operations center, brings together security response experts from across the company to ensure rapid response and resolution to security threats.

As automation of response processes often lags behind in the highly dynamic and constantly changing cybersecurity environment, CDCs need to manually assess and follow up on the rising number of threats and incidents. Time delays in the detection and response to threats and incidents are a source of significant expense to organizations (Naseer et al., 2021). The work is also becoming increasingly difficult due to many internal processes and criteria that need to be considered, such as threat intelligence (knowledge that allows security teams to prevent or mitigate incidents), prioritization (how urgent is the threat or incident), resolution (who should be involved in the incident response team) and external communication (who needs to know about this threat or incident). As a result, organizations

look to adopt tools and methods that could help them speed up the process of threat and incident response and improve the quality of the work (Naseer et al., 2021).

In addition to internal processes, there are also requirements from external parties that need to be considered in cybersecurity threat and incident management. This is the case particularly in large, high-value organizations, such as institutions in the financial sector, which is the focus of this paper. Regulatory scrutiny has increased significantly over the last years as regulators and supervisors are considering cyber to be the most critical threat to financial institutions (see also, Dupont, 2019). Consequently, regulators and supervisors require organizations in the financial sector to report major incidents such as data breaches, DDoS attacks and malware campaigns, and run programs to test and improve their resilience against sophisticated cyberattacks (e.g., the TIBER-EU framework: ECB, 2018).

This study is aimed at supporting cybersecurity threat and incident managers (CTIMs) within CDCs - professionals who are responsible for resolving threats and incidents at different levels of escalation - by exploring if decision support can help them make quick and accurate assessments and initiate actions. We take a deliberately broad view of "decision support" by not restricting it to intelligent systems, but extending it to memory aids, such as previously developed for troubleshooting (Schaafstal, Schraagen, & Van Berlo, 2000) or visualizations, such as previously developed for crisis management (Schraagen & Van de Ven, 2008). Decision support could help speed up threat and incident management by providing relevant cues and triggers and reduce decision making flaws and mistakes. This could result in a reduced impact of threats and incidents on business (e.g., threat is assessed in a timely manner and is managed by the right team of people) and better regulatory compliance (e.g., incident is reported to regulator on time). Much research has already been conducted on the use and effectiveness of decision support systems in various domains (e.g., Arnott & Pervan, 2008). However, as the cyber domain is relatively new, to our knowledge

little research has been carried out to understand the extent to which these systems can aid decision making by CTIMs.

Previous studies have shown that cybersecurity professionals need to exhibit a strong cyber-situational awareness, including juggling information such as regarding the health of the network, historical and current network activity, and performing a continual assessment of risk (Ahmad, Maynard, Desouza, Kotsias, Whitty, & Baskerville, 2021; Mahoney et al., 2010; Shin, Son, Khalil, & Heo, 2015). Cybersecurity incident response teams work with a set of software tools to sort through network traffic logs and visualize the flow of information in order to detect and attribute potential intrusions. Skilled operators are able to determine whether any network activity is anomalous in a high-noise environment, and judge whether to pass this information up to a superior to investigate further (D'Amico & Whitley, 2008; Genge, Kiss, & Haller, 2015). The complexity of this task is evidenced by its distributed nature: multiple operators use different tools to detect clues signaling potential intrusions. These clues may be perceived at different locations on the network, by different operators, at different times, and may be classified differently by each operator based on their own experiences and judgment.

Until now, the cognitive mechanisms by which cybersecurity professionals accurately respond to threats and incidents have not been fully studied. Although some cognitive task and work analyses have been carried out with cybersecurity experts (e.g., Asgharpour, Liu, & Camp, 2007; Champion, Jariwala, Ward, & Cooke, 2014; Chen, Shore, Zaccaro, Dalal, Tetrick, & Gorab, 2014; Mahoney et al., 2010; Naseer et al., 2021), these studies have mostly focused on decomposing the job of cybersecurity experts into key task stages or to determine the role of formal and informal education in job performance. The current study uses a well-established method of cognitive task analysis (Applied Cognitive Task Analysis; Militello & Hutton, 1998) to probe more deeply into the cognitive processes used by cybersecurity

professionals. Whereas cognitive task analysis (CTA) tries to account for the variability in behavior caused by differences in knowledge and cognitive strategies, they do not provide a basis for dealing with unanticipated events (Vicente, 1995). Cognitive work analysis (CWA) was developed to deal with these types of events (Vicente, 1999). Given that cybersecurity professionals are frequently confronted with unanticipated events, we also included elements of cognitive work analysis. For this purpose, we conducted two rounds of in-depth interviews with 10 experienced CTIMs from the CDCs of three financial institutions.

This paper is structured as follows. The first part describes in detail the work of CTIMs in large organizations with a mature information security incident response management practice, it gives a short overview of the state of the art of decision support in the cyber domain, and describes the method used for collecting data. In the second part, in order to get a good understanding of the cognitive processes, structural problems and dilemmas CTIMs face when resolving threats and incidents, we describe the results of CTA and CWA approaches we used to conduct an in-depth analysis of the cognitive elements of CTIMs' work to arrive at the functional requirements of decision support. In the third part we describe the outcomes of workshops with CDC professionals, in which the results of the CTA and CWA were validated and ideas for support were discussed; and we describe a decision support prototype that was developed in close consultation with designers and the financial institutions involved. The fourth part concludes the paper and outlines future work.

2. Incident response

Most large organization invest in an information security management (ISM) function to protect their digital assets (Ahmad, Desouza, Maynard, Naseer, & Baskerville, 2020). The ISM function ensures protective measures (see Ahmad, et al., 2020 for a more elaborate overview of this function). Alongside this function, many organizations also employ an

incident response (IR) management function, which can be seen as a practice area of ISM, to promptly respond to and resolve incidents (Ahmad, et al., 2020). This IR function to threats and incidents in organizations is manifested in diverse configurations. In the financial sector, particularly banks, IR will usually consist of a permanent operational-level team addressing a broad range of cyber security threats and incidents (Ahmad, et al., 2020). In the financial institutions that participated in our study, these teams were placed inside CDCs while IR management is called threat and incident management.

The CDC operates as three tiers with clear responsibilities and workflow processes. Level 1 and 2 operators are typically responsible for the first (and usually second) analysis of events and alerts that are triggered by security incident and event monitoring or security event monitoring solutions. These solutions provide real time analysis of security alerts generated by applications and network hardware. Those applications are generally rule based, which means that alerts are triggered by event conditions that for instance involve user authentication, intrusions or malware detection. The tasks of these operators are to make a first assessment, triage the problem, build context into a ticketing system and direct response for low-criticality incidents. Operators should also determine if an alert could be a real incident given that the vast majority of alerts are false positives. Consequently, an important part of the operator's job is to identify alerts that require follow up.

The follow up is usually done by a more experienced Level 3 operator with broader purview over global IT operations and analytics tools, which can detect bigger picture patterns. After the assessment by this third-line operator (or lower-level operator), the alert is handed over to the incident response team within the CDC (sometimes called the cyber emergency response team). Within the incident response team, the CTIM is responsible for investigating the alerts sent by CDC operators and determines whether the alert is a confirmed incident that requires incident response. In addition to the alerts handed over by

operators, the CTIM in the CDCs we investigated also analyses threats that are reported via other sources, such as vendors and other external stakeholders.

3. Decision support in incident response

An important task of a CDC team in IR is to make sense of the immense amount of network monitoring data, including during large-scale cyber-attack campaigns involving advanced persistent threats. Human capacity limitations in the context of cognitive processing of data make this a challenging task. Managers often need to make quick decisions and take mitigating measures based on their awareness of the situation at that moment, which is often limited and sometimes biased (Albanese & Jajodia, 2014). Support that could help alleviate some of these challenges and assist in defensive cyber operations is highly desirable.

Decision support systems (DSSes) is the area of the information-systems discipline that focuses on supporting and improving decision making. Essentially, DSSes is about developing and deploying systems to support decision processes (Arnott & Pervan, 2008). CTIM already have access to a wide range of systems to support decision processes, including security standards, training resources, vulnerability databases, best practices, catalogues of security controls, security checklists, benchmarks, threat information feeds and reports, and recommendations (Albanese & Jajodia, 2014; see also Healey, Hao, & Hutchinson, 2017). In most cases, these systems are in the form of a personal DSS, which is usually a small-scale system developed to support an individual or small number of managers in a decision task (Arnott & Pervan, 2008).

Examples of personal DSSes typical for the cybersecurity work field are playbooks and critical incident plans (CIPs). Although they serve multiple functions from procedural compliance to communication plans, most personal DSSes serve as cognitive aids to ensure that defensive cyber responders do not forget important steps in handling either routine or

emergent events. A playbook is a linear style checklist of required steps and actions required to successfully respond to specific incident types and threats. Incident response playbooks provide a simple step-by-step, top-down approach to orchestration. They help establish formalized IR processes and procedures within investigations and can ensure that required steps are systematically followed, which can help to meet and comply with regulatory frameworks such as GDPR (DFLabs, 2019). The aim of a CIP is usually to create a critical incident response policy and procedure for responders allowing them to have the capacity to respond appropriately in the event of a critical incident; to return to normal as quickly as possible after the incident; and to limit the effects of the incident on operations and any parties affected by the incident. Because these types of personal DSSes free up mental resources, they would ideally allow defensive cyber responders to mentally offload the many repetitive tasks that must be completed in a largely predictable sequence and to focus more on the complex decision making that is often required during emergent events.

In conclusion, the CDC team, especially the CTIMs, are faced with an increasingly demanding environment and as a result face many cognitive challenges. Although some forms of decision support have been developed, these tend to be linear and procedural, have the potential to consume too many mental resources, and are frequently not geared to unexpected and difficult cyberattacks, all of which undermines compliance and effectiveness. Moreover, these forms of decision support have mostly not been informed by the results of an analysis of the cognitive demands and requirements faced by defensive cyber responders. We therefore carried out both a CWA and a CTA in order to arrive at requirements for and prototype of a DSS that fits the demands of cybersecurity professionals. Given our focus on work demands and cognition, and within the constraints imposed by the COVID-19 pandemic, we conducted (remote) interviews rather than workplace observations (which were

prohibited during the pandemic) or case studies (which would not have yielded the required level of detail of knowledge and cognitive processes).

4. Method

4.1. Participants

A qualitative research approach was undertaken to explore the structural problems and dilemmas CTIMs face when resolving threats and incidents. From April 10, 2020 until September 2, 2020, a total of ten CDC-professionals from three large financial institutions in the Netherlands participated in the study. Each institution provided three (Organization 1 and 2) or four (Organization 3) contacts. The professionals were positioned at different levels of the CDC, called tiers. Regarding their background, three interviewees had studied and worked in the field of IT security before their current position, three had experience in computer science (e.g., programming), three had qualifications and past positions in digital forensics and one came from the field of intelligence. The participants' level of experience in threat intelligence or IR also varied: four out of ten were in their position or a similar one for less than a year. The most experienced participant held his position for five years. That the participants' tenures had been short shows the novelty of the field and the absence of specific academic and professional paths to access those positions; three participants had learned their profession on the job.

4.2. Procedure

The interviews were conducted in two rounds: all ten participants were interviewed in Round 1, and six of them (two from each organization) were interviewed in Round 2. Round 1 consisted of a Cognitive Task Analysis (CTA) to identify the main difficulties for CTIMs. Round 2 aimed at exploring the most relevant difficulty using a CWA and understanding functional requirements for a potential decision support system. In order to obtain an

indication of the level of expertise of the various professionals interviewed, the three activities that make up the CTA (see following section) were preceded by demographic questions on their education and experience, including the number of years in their current position. Most of the interviews were carried out through online meetings due to COVID-19-related social distancing measures. Each interview took approximately two hours. Interviews were recorded, transcribed verbatim and analyzed by the authors.

4.3. Cognitive task analysis

The overall research question that we addressed during the CTA was: What are the structural problems and dilemmas CTIMs face when resolving threats and incidents? For the CTA, we followed the applied cognitive task analysis (ACTA) approach described by Militello and Hutton (1998), one of the most frequently cited methods in CTA. CTA is a generic label that covers numerous methods and techniques for uncovering knowledge and cognitive strategies (for an overview, see Schraagen, Chipman, & Shalin, 2000; Crandall, Klein, & Hoffman, 2006). We chose ACTA, as it is a very specific, well-documented, and easy-to-use method. ACTA consists of three activities: task diagram, knowledge audit, and simulation interview. All three activities were carried out.

In the task diagram activity, the interviewee was asked to break down their work into between three and six subtasks. Next, the interviewee was asked to select the most cognitively demanding subtask for further analysis in the second activity, the knowledge audit. If necessary, the interviewer would explain “cognitively demanding” in terms of judgments, assessments and problem solving skills. The knowledge audit provides details and examples of cognitive elements of expertise; it contrasts what experts know and novices do not. Within the knowledge audit, the interviewers pursued the most cognitively demanding task in more detail by asking eight probe questions, and for each example provided, asked

which cues and strategies the professional relied on and in what way the example could be difficult for a less experienced person. The eight probe questions were:

1. Is there a time when you walked into the middle of a situation and knew exactly how things got there and where they were headed?
2. Can you give me an example of what is important about the big picture for this task? What are the major elements you have to know and keep track of?
3. Have you had experiences in which part of a situation just "popped out" at you; in which you noticed things going on that others didn't catch? What is an example?
4. When you do this task, are there smart ways of working or of accomplishing more with less that you have found especially useful?
5. Can you think of an example when you improvised in this task or noticed an opportunity to do something better?
6. Can you think of a time when you realized that you would need to change the way you were working order to get the job done?
7. Can you describe an instance when you spotted a deviation from the norm or knew something was amiss?
8. Have there been times when the equipment pointed in one direction, but your own judgment told you to do something else? Or when you had to rely on experience to avoid being led astray by the equipment?

In the simulation interview the interviewee was asked to describe a particular threat or incident they had experienced. First, they were asked to list the major events that occurred during this threat or incident. Second, for each major event, they were asked to indicate the actions they would take, their assessment of the situation, the critical cues that led to this situation assessment and these actions, and the potential errors an inexperienced person would be likely to make in this situation.

The results of the CTA interviews were transcribed and captured in tables. A thematic analysis (Braun & Clarke, 2012; Joffe, 2012) was conducted to arrive at categories of common cognitive difficulties. To this end, text was coded based on recurring words (e.g., "confidence," "time," "critical thinking"), and a definition was established for each category based on these key words. Subsequently, each interviewee's statements were grouped into the various categories, which were subsequently grouped into a smaller number of themes.

Next, a list of cognitive difficulties was established, based on the themes and discussions among the researchers. This list was populated with elements from the Knowledge Audit, as this activity focused on the value of expertise, potential errors and strategies used to deal with the cognitive difficulties. The list with cognitive difficulties was presented to the stakeholders who were asked to prioritize them. Based on this prioritization, the most pressing difficulty as identified by the interviewees was chosen for further analysis using a CWA.

4.4. Cognitive work analysis

Having focused on the individual cognitive difficulties experienced by the cybersecurity professionals, the next step was to broaden our scope to the work domain in general, in order to find leverage points for decision support within the organization, as well as to describe more formally the cybersecurity threat and incident decision-making process. To this end, we carried out a work domain analysis using the abstraction hierarchy, as well as a CTA using the decision ladder as representations (Vicente, 1999). We did not carry out the strategies analysis, social organization and cooperation analysis, and worker competencies analysis, partially because of time constraints, but mostly because the aims and scope of this research were focused on decision support rather than the allocation, distribution and coordination of work or the competencies required by workers to fulfill the system's work demands. In contrast to CTA, for which numerous methods and techniques are available, CWA is mostly bound by the highly influential approach first described by Vicente (1999). Given its

prominence in the literature and its widely accepted use (see Bisantz & Burns, 2009; Burns, 2020), we decided to use this approach as well. CWA has been applied mostly in domains such as process control and military command and control (Jenkins, Stanton, Salmon, & Walker, 2009). These domains have shown that it is possible to derive practical design recommendations from the abstraction hierarchy and the decision ladder, in terms of "which" information needs to be displayed and "where and when" information should be presented. The current study builds upon and differs from previous studies in that it combines both CTA and CWA and aims to develop decision support for cybersecurity professionals at a more abstract level than adding yet another computer system and developing a new interface design for such a system.

The abstraction hierarchy is usually the first phase in a cognitive work analysis and gives a representation of the functional structure of a given domain, in our case, cybersecurity. The functional structure is composed of purposes, values, priorities, purpose-related functions, object-related processes and physical objects. This representation is independent of the user and the environment and provides the constraints every actor in the domain has to satisfy (for more details, see Naikar, 2013). There are several formats that analysts commonly adopt for presenting work domain models. The one we have chosen here is what Naikar (2013) refers to as the "tabular abstraction hierarchy." This format shows the level of abstraction of the constraints, though not their level of decomposition or means-ends relationships. A control task analysis takes the shape of a decision ladder template, mapping three stages identified as situation assessment, options analysis and planning. While this analysis focuses on what needs to be done, it is not concerned with how or by whom this activity can be carried out. This is important, as it leaves open the precise way in which decision support may take shape. We drafted a first version of the abstraction hierarchy and decision ladder and successively refined these representations through the round two interviews with six cybersecurity

professionals from the financial institutions, chosen from the pool of interviewees of the first round.

4.5. Workshops

The result of the CTA – the list of cognitive difficulties – was presented in a workshop to the second-round interviewees, to receive feedback on the findings and either to choose relevant elements to investigate further or as the basis of the solution concept. Additionally, a second workshop was carried out to critically review the decision-support solutions ideated and to understand integration requirements of the proposed solutions with current ways of working. For the ideation sessions that preceded this workshop, we invited colleagues with expertise in product design or cybersecurity from our organization to the table, on the topic of what support could look like. Besides the researchers, six members from the financial institutions participated in this second workshop: each organization committed two experienced CDC members. After presenting the results of the interviews and the proposed solutions for decision support, workshop participants were divided in two teams, following the dialectical inquiry approach proposed by Mason and Mitroff (1981). Research has demonstrated that this approach is more effective than a simpler expert-based approach involving no conflict (Schwenk & Valacich, 1994). Each team had to pitch and defend two of the four solutions, while preparing arguments against the other two. After considering the different options, participants were asked to vote for their favorites by distributing 100 points among the different solutions, giving the most points to their preferred solution and few or no points to their least preferred solution. The results were used to decide which proposed solution to move forward with.

5. Results

5.1. Cognitive task analysis

The goal of the first round of interviews was acquire a good overview of the cognitive work processes of CIMs and CTMs and to identify relevant difficulties in their work. Every transcript was analyzed, and specific elements were extracted to create a coding frame (Joffe, 2012) to guide the thematic analysis. For the sake of brevity and illustration, Table 1 shows only a small part of the coding frame. The first column shows the particular code with its definition, the second column shows in which interview this code occurred, and the third column provides one or two examples in the form of a quote from an interviewee.

Table 1. Coding frame.

Code	Interview	Example (quote)
Time management *The interviewee mentions the duration required by himself or the organization to complete a specific task.*	B1, C3, B2, B3, B4, A2, A3, C1	"He did not have to stand in the front line with the team. He could have a look at investigations without the regular time pressure, take a step back from on-going operations."
Duality details/big picture, facts & procedures/open-mind, critical mindset *The interview mentions both the need to be close to details, facts and processes and the need to look up, step back from the raw data, get knowledge elsewhere and connect the dots.*	B1, C3, B2, B3, B4, A1, A2, A3, C1, C2	"Always rely on tools + knowledge and experience." "did additional checks: critical thinking and curiosity."
Reactivating knowledge at the right time *The interviewee mentions the need to not only acquire knowledge but also to be able to practically use it when a specific threat/alert/incident occurs.*	B1, B2, B3, A3	"Having the right experience at the right moment."
Follow processes	B1, C3, B4, A1, A2, A3, C1,	"So should use one way which includes

The interviewee mentions his/her work follows written processes.	C2	everything we know and knowledge of what is outside."

Following the six-phase approach to thematic analysis discussed by Braun and Clarke (2012), we next shifted from codes to themes. Four thematic areas were identified: (1) building up relevant experience and knowledge, (2) stakeholder communications, (3) analysis and (4) external stressors. These themes will be discussed in more detail below.

5.1.1. Building up relevant experience and knowledge. The first thematic area relates to the general knowledge and skills in the field of IT, in the overall threat landscape and of organizational and business matters. Relevant expertise and knowledge seem to be mostly acquired throughout the career path, over the years, but not through education. Indeed, interviewees mentioned the benefits of having general knowledge and experience, especially in the broader context of the organization. The goal is to be able to apply external and broad knowledge to internal and specific processes of threat management and IR. According to the interviewees, part of this general knowledge includes knowledge about the specific tools. To get such a large span of knowledge and skills, experts mentioned the necessity for people in their position to be driven by curiosity and to develop a network inside and outside of the company. Ultimately, the presence or absence of external knowledge can be a factor contributing to the level of capabilities.

5.1.2. Communication. The second thematic area is communication. This refers to communication activities with external parties such as threat intelligence networks, outsourced service providers and third parties; with internal stakeholders ranging from technical people to business and strategic actors within the organization; and team members to get or deliver information, be it a request for specific actions, information or actionable intelligence. For this exchange of information, building trusted connections was seen as

essential by some experts, especially within the threat intelligence network across organizations. However, these communications can be made difficult for multiple reasons. To begin with, professionals may sometimes have to deal with a large number of parties, of diverse backgrounds and using different professional languages, which by nature complicates the exchange of information especially in stressful situations. Finally, participants mentioned the difficulty answering unclear requests for information when stakeholders cannot identify and specify the information needed.

5.1.3. Analysis. The third thematic area is analysis. This phase in IR introduces several paradoxical problems, which were mentioned by the experts. First, the importance on one hand of adhering to a strict application of processes and reliance on the facts, and on the other hand of keeping the big picture, or broader context, in mind, thinking out of the box, and, to some extent, being critical of the information and its verification while showing confidence in choices made. Second, the need to anticipate future limitations, needs and series of events, while discouraging the making of assumptions. Finally, analysts need to be able to compare, but at the same time make correlations between different alerts and events, which occur in the same timeframe or at different times.

5.1.4. External stressors. Several stressors were identified, which represent environmental conditions and external stimuli that might influence the quality of the work of CTIMs. The first type of stressors identified are induced by either time pressure, by other people (consciously or not), or by the organization. They are related to the impact an event has on the operations of the financial institution: availability of the service for either customers or internal parties, or potential financial losses, for instance. The second stressor is caused by the inherent limitations and occasional failures of the tools used, which require the analyst or responder to keep a critical mindset at all times. Finally, the large amount of information *and* the systems *and* people to consider when resolving incidents is one of the

challenges mentioned most in this research. It creates a heavy cognitive load and makes most processes in place difficult to adhere to.

5.2. Thematic analysis: Cognitive difficulties

A total of ten distinctive cognitive difficulties emerged from the thematic analysis: (1) to acquire and apply broad and extensive knowledge to specific threats and incidents related to organizational processes, (2) to centralize information, (3) to know how much information is needed, (4) to communicate with stakeholders and/or external parties, (5) to take both details and the bigger picture into account, (6) to stick to procedures while keeping a critical mindset, (7) to deal with large numbers of people involved and/or machines infected, (8) to deal with residual risk, (9) to compare situations when there is little experience in the field, and (10) to approach new threats and incidents. Table 2 shows three thematic areas (the fourth area, external stressors, is already included in the cognitive difficulties), the ten cognitive difficulties, findings from the interviews and a quote to illustrate the difficulty.

Table 2. Thematic areas and cognitive difficulties.

Thematic area	Cognitive difficulty	Findings	Example (quote)
Building up relevant experience and knowledge	To acquire then apply broad and extensive knowledge to specific threats and incidents related to one organization	Threat and incident management requires knowledge and skills on a lot of different topics within IT, IT security, Threat Intelligence and of the organization	"Sometimes, as CDC we miss certain knowledge, for instance our knowledge about the cloud environment."
	To centralize information	Respondents need to deal with an overload of information, while at times, relevant pieces might be missing. Additionally, tools	"So we should use one way which includes everything we know and knowledge of what is outside."

		cannot always centralize all the information efficiently because of their architecture or because of the imperfection of human inputs.	
	To know how much information is needed	Respondents find it difficult because it requires a certain level of confidence in the knowledge and risk assessment.	"Analysts have to deal with a lot of information, which is sometimes incomplete. It is even more complex for juniors to handle it."
	To approach new threats and incidents.	Participants mention the habit of relying on documentation and existing procedures, however novel cases have by nature no support documentation, which can be destabilizing. Additionally, time pressure increases the difficulty to deal with a novel and potentially complex case.	"Sometimes, tech and existing processes are not enough, when something new happens for example. Being able to puzzle up elements."
Communications	Communications with stakeholders or external parties	The difficulty lies in the variety of backgrounds, professional cultures and languages. Furthermore, stakeholders usually have difficulties in clearly assessing their needs which translates in the message they communicate to	"Not everything or everyone is always available for questions."

		analysts. Finally, the team may not always be well settled and known within the organization.	
Analysis	To take both details and the bigger picture into account	This is difficult for respondents as it requires switching view mode (from the technical logs to thinking in a more abstract way about the organization and the threat landscape) and avoiding well-known biases such as tunnel vision.	"By being connected to the community he knows that this could happen more often, that clients will get more targeted. Some people tend to solely focus [by choice/mindset] on technical cues shown by the system." "A junior does a lot of investigation first instead of just having some high overview of what is really going on."
	To stick to procedures while keeping a critical mindset	Respondents find this difficult as their work is by nature heavily controlled by processes, which tend to automate the way analysts proceed. It therefore takes additional effort to take a step back and take a critical stand on what is happening. It feels like a double constraint.	"I always rely on tools and on knowledge and experience. I also do additional checks, because critical thinking and curiosity are important."
	To deal with high numbers of people involved or machines infected	With a high number of points of interactions, memory can get overloaded and the communication difficulties are enhanced.	"Because it spread so fast, it was really difficult to follow the rabbit and trace to where it originated from. Many servers started also alerting. It was really difficult to trace this. It was a nightmare."

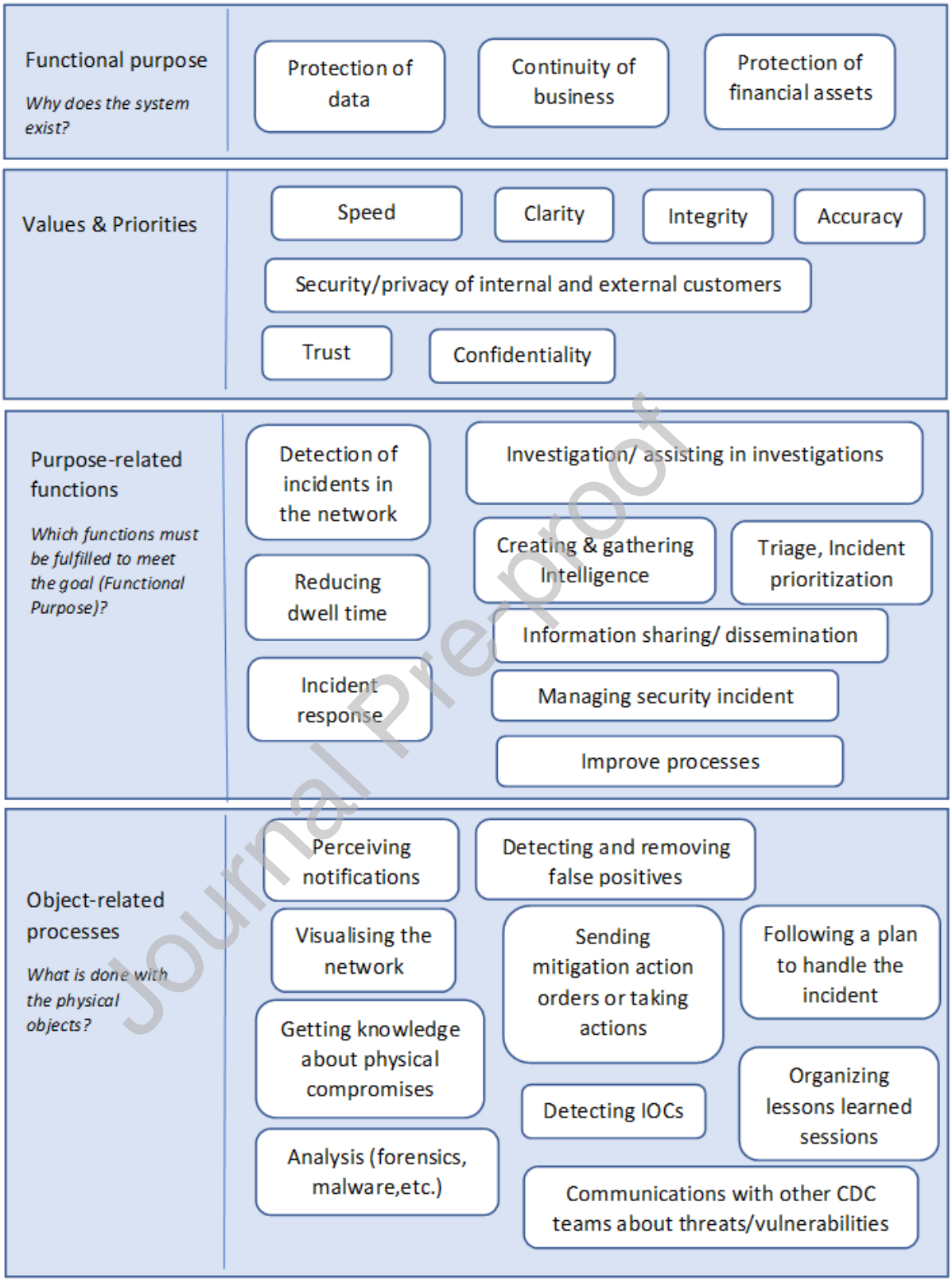
	To deal with residual risk	It requires confidence to submit results with even a very low uncertainty. Respondents feel the responsibility implied in their duties.	"There is always a residual risk. You may not have covered everything. A new machine may include a vulnerability that we don't know about. There is always threat and risk."
	To compare situations when there little experience in the field	Analysts and incident responders may lack experiences and therefore content with which to compare situations.	"He compared to what he knew was available at other organizations."

The list of cognitive difficulties was presented to a group of experienced CDC members and the CDC manager in a workshop setting (one CDC member and manager from each financial institution). After a discussion about the results, participants were asked to prioritize the difficulties listed (see Table 2). The problem of balancing the bigger picture with details, that is, being able to simultaneously keep the broader operational context in mind, developing the operational picture from fragments of information, as well as adequately investigating, containing and remediating a cyberattack ("the task at hand"), was unanimously chosen as the most pressing cognitive difficulty in cyber defensive operations. While all difficulties identified were said to be relevant, participants recognized that their team members struggled to change view modes: from a detailed and technical perspective to an overview of the events and their insertion into the organization. They believed this difficulty could be an obstacle to optimizing the defense of the organization against cyberthreats and incidents by allowing more mistakes in judgement, missing critical elements in the analysis, and missing opportunities for optimization of the event handling.

5.3. Cognitive work analysis

The goal of the CWA was to identify the functional requirements of a support system to aid CTIMs in the triage process of threats and incidents by taking both the big picture and details into account. To these ends, an abstraction hierarchy and a decision ladder were developed.

The abstraction hierarchy is presented in Figure 1. The abstraction hierarchy makes clear that although the functional purpose of the CDC team can be summed up in three goals (i.e. protection of data, continuity of business, and protection of financial assets), the number of purpose-related functions, object-related processes and cyber/physical objects is very large. In addition, the values and priorities against which the purpose-related functions are assessed in meeting the overall functional purpose are quite numerous and sometimes conflicting (e.g., speed versus accuracy; clarity versus confidentiality). The purpose-related functions portray the functions that a cybersecurity team must be capable of supporting (e.g., detection of incidents in the network) so that it achieves its functional purposes when confronted with a particular trigger or alert. The purpose-related functions may be subdivided into on the one hand those functions dealing with the primary process (often referred to in domain-specific terms as: observe, triage, investigate, contain, remediate, check, and post-incident evaluation), and on the other hand those dealing with broader issues of information sharing/dissemination and creating and gathering intelligence. The former may be considered the “details” that team members can focus on to the exclusion of the latter “bigger picture” functions that are more geared to finding related events, checking if an event is related to an incident that is already open, involving and communicating with the asset owner/management and technical contacts, and informing other relevant parties within or outside the organization of the threat or incident and mitigating measures.



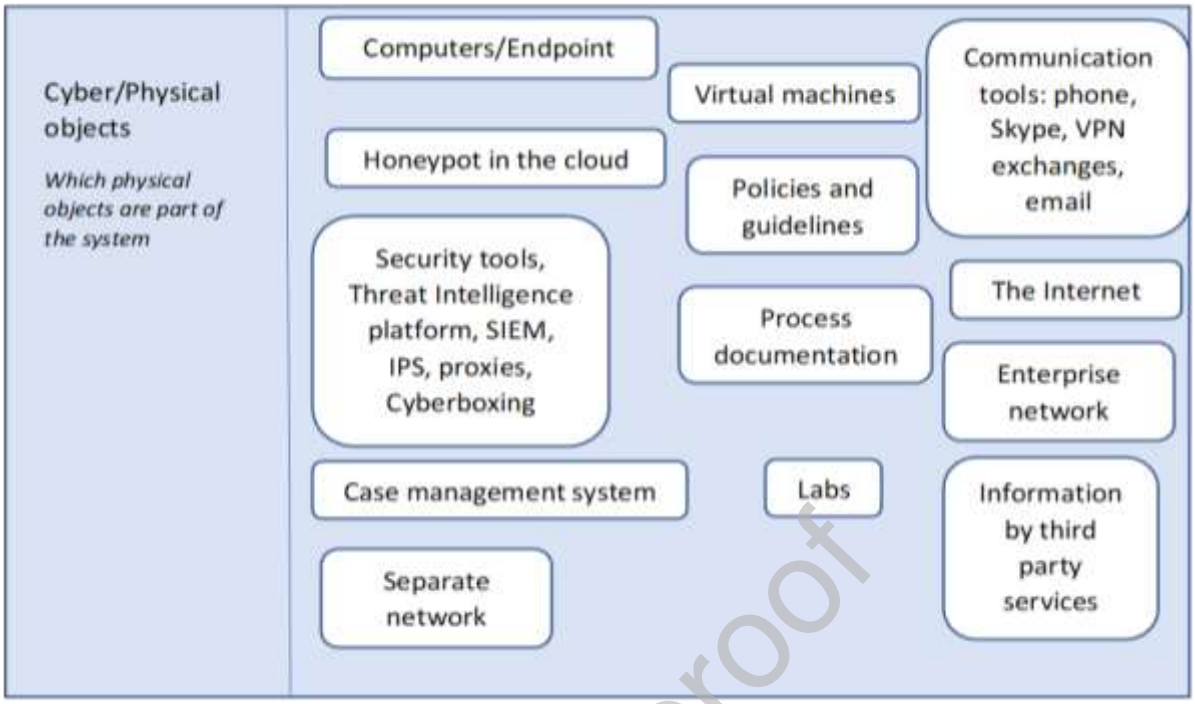


Figure 1: Abstraction hierarchy.

The difficulty of balancing the bigger picture activities with detailed activities is further explored in the control task analysis using a decision ladder (see Figure 2). Each of the purpose-related functions was discussed with each of the six participants in terms of the processes and knowledge states depicted in the decision ladder.

The control task analysis showed interviewees to rely on tools and process documentation, frequently skipping the upper parts of the decision ladder and taking shortcuts (not displayed in Figure 2; shortcuts involve going directly from the lower left of the ladder to the lower right). For example, an CTIM will use a specific playbook based on the name of the event, describing all necessary steps (in Figure 2, they would move directly from comprehension to plan comprehension). While those indications will allow them to technically solve the issue at stake, they will not provide the CTIM with cues to think critically and set the event into a larger perspective for the organization or the threat landscape (i.e., they skip future state awareness and desired state awareness). Therefore, most

of them will not feel the need to analyze different options (and hence will also skip options awareness and understanding of consequences). Furthermore, as expected, a large number of alerts, the re-occurrence of similar alerts and incidents, and time constraints encourage the analyst to take shortcuts in the decision-making process by, again, not contemplating different options before proceeding to the planning of actions (moving directly from comprehension to plan comprehension). Instead, they may solely solve an isolated incident, from a technical perspective, which may lead to overlooking potential direct threats or mistakes (i.e., moving from awareness on the left side of the ladder directly to awareness on the right side).

Although using shortcuts is based on experience and is enforced by the limited time available for carrying out IR (on the average around 30 mins.), the process sometimes goes awry because threats change every day and hence processes can often be outdated. There are also many different systems to look at and interviewees frequently mentioned that they forgot to check a particular system, forgot to inform other people, or they simply forgot what they had already done. What compounds matters is that getting an answer from another person or from a system may take considerable time – something they do not have. Interviewees also mentioned that playbooks are frequently too long to read and do not fit every situation. In short, the rule-based support that has been developed in the form of playbooks is inadequate in supporting CTIMs.

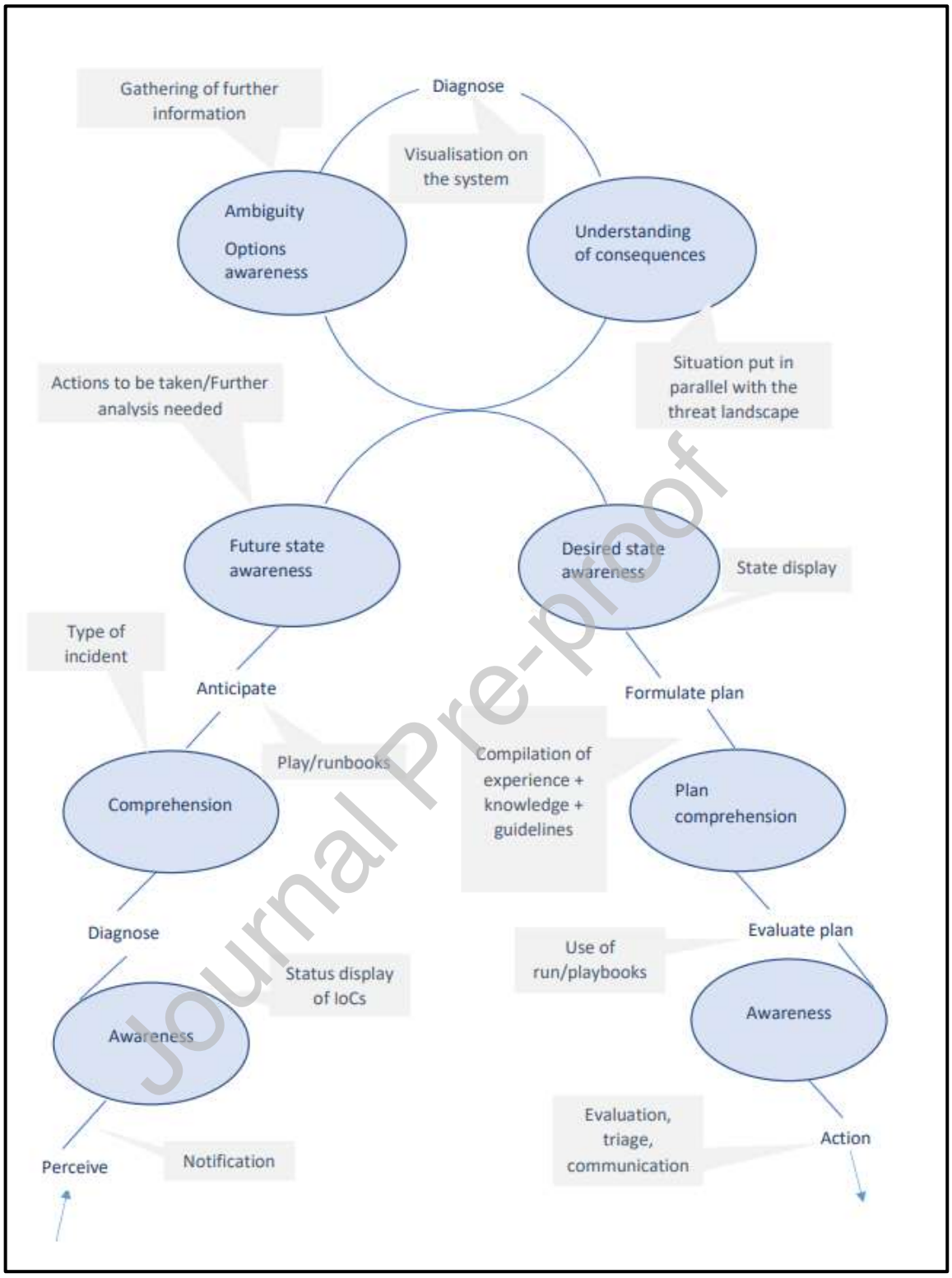


Figure 2: Control task analysis for CTIMs.

In conclusion, in the second round of interviews using the abstraction hierarchy and decision ladder, we successfully placed and corroborated the cognitive difficulty of attending to both the bigger picture and details in a larger context of time pressure and the involvement of multiple parties. Interviewees expressed a need for a different form of decision support than the proceduralized, rule-based support already provided via playbooks. As one respondent stated: "It would be nice to have a decision table or workflow that fits every situation with just a few words."

5.4. Functional requirements

In the workshop with the experienced CDC members and their managers, the following functional requirements were identified. First, support should not be in the form of yet another tool. This is not so much driven by the abundance of tools already present, but rather by the human-factors issue that additional tooling that does not replace existing tools might lead to higher workload and, hence, less time available for the cyber defensive operations. Given that CTIMs are already time-pressured, any tool added to the existing tool suite would result in more diversification of the limited time available, given that analysts need to be reminded of the new tool, need to be able to learn it and use it, and it needs to provide additional value. Second, support should help reactivate existing knowledge structures. CTIMs constantly learn, thus adding to their existing and extensive knowledge base. The difficulty is to activate the right elements at the right moment. Third, more than just injecting knowledge, we need to enhance the use of critical thinking skills in the process. Fourth, time pressure is one of the biggest issues. A solution needs to be quickly implementable without adding to the workload.

5.5. Evaluation of ideated solution directions

Based on the problem of considering the bigger picture and details in the decision-making process and the functional requirements to do so, we held several ideation sessions, inviting

colleagues with an expertise in product design or cybersecurity from our organization to the table, on the topic of what support could look like. These sessions resulted in four support concepts – a critical thinking tool, microlearnings, improvements to existing IR management procedures, and a new CDC team member role – which were subsequently presented to experienced CDC members and their managers in the workshop that was mentioned before.

IR management typically takes place under conditions of uncertainty, complexity, ambiguity, and volatility. Under these conditions CTIMs could benefit from a framework or tool that specifies how they should think fast, correctly, and evaluate evidence during each stage of IR (Hettema, 2021). The concept of a *critical thinking tool* would require someone to evaluate each piece of evidence in a tool as either supporting or not supporting a particular initial hypothesis concerning the stages of incident resolution. This way, the tool would provide the analysts with an overview of the evidence both for and against an hypothesis. Research has shown that critical thinking support tools can help lessen confirmation biases (Cook & Smallman, 2008; Schraagen & Van de Ven, 2008).

In the context of the present research, *microlearnings* can be operationalized as small reminders that pop up during low-workload periods and that are thought to be effective for learning, as they are presented in-context and when the analyst needs them (e.g., Mohammed, Wakil, & Nawroly, 2018). They do require context-sensitivity and personalization, which are currently active fields of research. Alternatively, scenario-based training using critical scenarios has also been demonstrated to provide training value (La Fleur, Hoffman, Gibson, & Buchler, 2021; O'Neill et al., 2021). For instance, O'Neill and colleagues (2021) developed and demonstrated the potential usefulness of a scenario-based training approach to assist organizations in overcoming socio-technical barriers to IR. What is important here is that scenarios are developed with particular learning objectives in mind, that critical events are injected in the scenario (e.g., by a third party), and that objective performance

measurements are collected for each event. It is also important to provide proper feedback afterwards so learning will ensue.

Considering the *redesign of the IR management process*, previous work that we carried out for the Royal Netherlands Navy on improving training in faultfinding in technical equipment on board naval vessels found that incident management procedures as provided by the technical suppliers were frequently developed from an engineer's point of view and were, therefore, not always very usable in practice (Schaafstal, Schraagen, & Van Berlo, 2000). Also, an inherent limitation of these procedures is that they do not cover every imaginable instance. Usually, they are based on lessons learned from past incidents. In the financial sector there is a parallel with the rule-based or problem-oriented support already provided by playbooks: these do not cover all possible incidents. Further, they are often developed to comply with rules rather than from a user's perspective. The experiences in the airline industry have shown, for instance, that checklists need to be developed with a large focus on what pilots already know and are able to use under time pressure (Gawande, 2010). Ensuring optimal usability therefore requires that end users are involved in the development of new procedures.

It was a common observation in our interviews that when confronted with an incident, the time pressure perceived by CTIMs acts as blinders, and may prevent them from maintaining an overview of the bigger picture. This contributes to the problem we found in our interviews of being "drowned by details." Hence, in the process of acquiring cyber-situation awareness, stakeholders need to perceive raw alerts as well as build the operational picture and understand its significance in the context of the cybersecurity objectives (Ahmad, et al., 2021). One promising solution at the level of how the work is being organized is to define a *new team member role* for someone who is not directly involved in the actual process but is able to keep an overview of what everyone is doing, what information needs to

be obtained elsewhere, and how the process is going timewise. For this we need to define the competencies such a person should have, as well as their exact role vis-à-vis the other analysts involved.

The workshop participants took part in a 100-points distribution exercise resulting in the following scores for the different solutions. The critical thinking tools received 55 points, the microlearning 115, the redesign of the IR management process 440 and the new role 90. It was thereby decided that the most appealing direction for support for the problem of considering the bigger picture and details in the decision-making process would be to improve the current IR management process. Although this option was favored over the others, several participants mentioned that, ideally, the concept of critical-thinking support should be integrated in incident managing procedures, since they are related anyway. Integrating critical thinking methods in incident management procedures, such as the CIP or playbooks, for instance in the form of a checklist, would adhere to requirements while at the same time optimizing the IR processes. As mentioned, the CIP describes the policies and procedures for incident managers to respond appropriately in the event of a critical incident, to return to normal as quickly as possible after the incident and to limit the effects of the incident on operations.

6. Critical thinking memory aid

During ideation sessions with the project team, using several ideation techniques such as brainstorming and challenging assumptions, we decided to include critical thinking elements into the redesign of the IR management process, considering the bigger picture and details in this decision-making process. We chose to do this in the form of a memory aid for CTIMs. This memory aid, that consists of critical thinking elements and IR process steps, is depicted in Figure 3. The hexagon tiles show the details of the process, while on the outer borders of

the hexagons the broader operational context that needs to be considered is displayed. CTIMs are not forced to go through this memory aid in a particular order, although the processes are listed in clockwise order. In practice, processes can blur or be repeated, and often pivot from analysis to detection, or even from containment to detection, as further levels of hostile penetration are discovered (Hettema, 2021). The following seven process steps are included in the memory aid: observe, triage, investigate, contain, remediate, check, and post-incident evaluate. Once an incident has been observed, cybersecurity teams evaluate the incident and determine the severity of the threat and the urgency for further investigations. The next step is to contain the incident to prevent it causing further damage to the organization. Remediation processes involve the treatment of a security breach. Finally, the effectiveness of the measures taken is checked and time is taken to reflect on the incident handling activities to incorporate lessons learned in the playbooks. When considered together, these process steps provide a high-level overview of IR management processes as observed by us in the financial sector. These activities align with existing functional frameworks for incident management and linear process models consisting of sequential stages, such as the US National Institute of Standards and Technology (NIST) computer security incident handling guide for improving critical infrastructure cybersecurity (Grance, Kent, & Kim, 2014; see also, Ahmad et al., 2021; Shinde & Kulkarni, 2021).

The purpose of the critical thinking memory aid is to provide support to CTIMs to balance “the bigger picture” (broader operational context of the incident; hence, impact on corporate operations) with “the task at hand” (the immediate imperatives), while keeping a critical mindset, and preventing them from jumping to conclusions. This supports the effective and appropriate ability to respond to critical incidents: to return to normal as quickly as possible after the threat or incident and to mitigate or contain the effects of on operations.

Figure 3. Critical thinking memory aid for threat and incident management.

The aid is expected to be useful particularly in larger incidents in which synchronization of activities becomes more important. It may be used to document progress in dealing with the incident across the various incident resolution phases, which is useful for communicating the status to various stakeholders in terms of what has been done and what still needs to be done. The aid may be implemented in both physical and digital format. As a physical tool, it may be printed out in large format and used in shared workspaces for communication purposes and to support shared understanding of the incident between the CDC team members. As a digital tool, it can also serve as a clickable interface to more detailed playbooks and instruction sets. By allowing CTIMs to oversee the process, while at the same time providing more detailed information on how to handle the incident, the memory aid is, in our opinion, a promising way to address the problem of balancing the bigger picture with details. Given our focus on obtaining requirements for the decision aid, the details of the implementation (e.g., use of hexagons, color, circular layout), as well as a study on its effectiveness during actual use, remain topics for future research.

7. Discussion

The purpose of this research was to develop decision support for CTIMs in the financial sector. To this end, we carried out a CTA (Militello & Hutton, 1998) and a CWA (Vicente, 1999). Our results showed that the most pressing problem faced by CTIMs is balancing the bigger picture and details, that is, being able to simultaneously keep the broader operational context in mind while adequately investigating, containing and remediating a cyberattack, while maintaining a critical mindset. Keeping the bigger picture in mind is important because of the broader implications of cyberattacks for other (parts of) organizations, as well as links with related events. Due to time pressure, high cognitive load and the sheer number of systems and stakeholders involved, there is a tendency amongst CTIMs to either forget about the bigger picture or to weigh activities in favor of detailed rule-based procedures that may work with simple and common incidents but approach their limitations with more complex and uncommon incidents. In close consultation with the three financial institutions involved, we developed a form of decision support that met the following functional requirements: (1) the decision support should help reactivate knowledge structures that are already present, (2) more than just injecting knowledge, we need to enhance the use of critical thinking skills in the process, and (3) any tool needs to be quickly implementable without adding to the workload. Based on these requirements, a critical thinking memory aid was identified as a viable support direction, but only when integrated in existing knowledge structures. The memory aid we developed, therefore, follows cybersecurity IR processes but adds bigger picture elements and critical thinking steps to make managers more aware of the broader implications of threats and incidents.

Our work is of significance for the development of support for CTIMs for several reasons. Because gaining access to larger organizations is extremely difficult due to the

sensitivity of the operations in question, there are only few case studies of cybersecurity IR (see also, Ahmad et al., 2021). Notwithstanding the challenge of gaining access, we managed to do so, not for one, but for three large organizations, allowing for a multiple-case study. As compared to single in-depth case studies, this allows for better generalizability of our results and stronger theory building due to greater reliability of evidence (Ahmad et al., 2021). Further, we managed to study cybersecurity IR in large, high value financial institutions that have a highly mature cybersecurity posture. These organizations could be seen as cybersecurity role models for others. Our results are useful for the development of cyber resilience capabilities in at least two types of organizations: those looking to develop their cybersecurity practice to address the rise of cybersecurity attacks, as well as more mature organizations in cybersecurity posture that want to learn how to improve their existing cybersecurity operating procedures.

A limitation of this study is that we did not carry out a summative evaluation, in which the focus is on the outcome or overall quality of the tool (Nielsen, 1993). It is therefore not possible to say whether and how it will be used, nor whether it will be more successful than current aids such as NIST's framework for improving critical infrastructure cybersecurity. Nevertheless, although we do not underestimate the challenges of implementing decision aids in current work practices, there are several reasons to be cautiously optimistic. First, our findings are based on a fairly large sample size that we could interview twice for an extended period of time (1.5-2 hours for the applied cognitive task analysis; 1.5 hours for the work domain analysis and control task analysis). Militello and Hutton (1998) recommend including six to eight highly experienced practitioners; we have included ten employees in total from three different financial institutions. Given that after six interviews common themes emerged, we are confident that we uncovered the major themes after all ten interviews. In addition, the

iterations of the tabular abstraction hierarchy converged on a common representation after six interviews.

Second, after each phase in our research, we presented the intermediate results to a panel of six representatives, two from each of the three financial institutions, who had not been interviewed, to check whether we were complete and correct in our understanding, and to validate the directions we intended to take next. During the actual development of the critical thinking memory aid, we again solicited feedback from the financial institutions in order to ensure that the product we would develop would fit into their current work processes. These activities all fall under the general heading of "formative evaluations," an important activity in any usability research which focuses on feeding back information to the design team to guide subsequent developments of tooling (Nielsen, 1993).

Third, we received many documents from the participating financial institutions describing their current work processes, procedures, regulatory frameworks and support tools. These were very helpful for us to make sure our decision aid would add something to formal controls, such as playbooks, while not straying too far away from current practice. In conclusion, then, although a summative evaluation was beyond the scope of this research, we did carry out numerous formative evaluations that strongly indicate we were on the right track. An interesting avenue to pursue in future research is, therefore, to evaluate the memory aid we developed in terms of effectiveness, efficiency, and usability in field studies or during cybersecurity exercises.

CTIMs often work in teams. These teams can be formalized or ad hoc in nature, in that members are called together when the need arises. Although the ability of these teams to respond to incidents is hampered by a broad range of socio-technical issues (O'Neill et al., 2021), recent research has demonstrated that teams are better able to solve complex tasks than individual operators, potentially due to the distribution of expertise among operators

(Rajivan & Cooke, 2018). Integrating this research with the prior literature on cybersecurity work roles and responsibilities (see, for example, Shinde & Kulkarni, 2021) may provide insight into more optimal team configurations and methods for optimizing efficacy. Using the abstraction hierarchy as a starting point, a social organization and cooperation analysis would be able to specify the allocation, distribution and coordination of work (Vicente, 1999). For instance, one of the decision support options we generated and discussed in the final workshop was the inclusion of a new team member role to keep an overview of what other team members are doing, what information needs to be obtained elsewhere, and how the process is going timewise. This role serves the purpose-related functions of information sharing and dissemination, managing the security incident and improving processes (see Figure 1). Whether the new team member role is a feasible option remains to be seen, particularly while experienced analysts, especially those with good social skills, are already scarce and coordination requirements with the other team members need to be met (Van der Kleij, Kleinhuis, & Young, 2017).

In conclusion, this research is a first step in developing decision support for CTIMs in financial institutions. Based on two-rounds of interviews with ten professionals from three financial institutions, and using a structured approach to uncover the cognitive requirements for decision support, we developed a critical-thinking memory aid that follows existing IR management processes, but adds bigger picture elements and critical thinking steps to make CTIMs more aware of the broader operational implications of threats and incidents while keeping a critical mindset.

Acknowledgments

This work was performed within a shared research programme on cyber security, in which Dutch financial institutions and TNO, partially supported by the Ministry of Economic

Affairs and Climate, cooperate with the aim to innovate on cyber security. The sequence of the first and second author was determined by the toss of a coin: both contributed equally to this paper. The authors gratefully acknowledge the participating financial institutions for supporting this study and the CTIMs who agreed to participate in the interviews. The authors also wish to thank Dr. Jelle Groenendaal for his assistance with this research effort.

Credit author statement

Rick van der Kleij: Conceptualization, Funding acquisition, Resources, Project administration, Supervision, Visualization, Writing - Review & Editing, Writing - Original Draft, Investigation, Validation, **Jan Maarten Schraagen:** Conceptualization, Visualization, Supervision, Writing - Review & Editing, Writing - Original Draft, Investigation, Formal analysis, Methodology **Beatrice Cadet:** Investigation, Writing - Review & Editing, Writing - Original Draft, Visualization, Formal analysis **Heather Young:** Writing - Review & Editing, Investigation

Declaration of interests

☒ The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

☐The authors declare the following financial interests/personal relationships which may be considered as potential competing interests:

References

Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology*, *71*(8), 939-953.

Ahmad, A., Maynard, S. B., Desouza, K. C., Kotsias, J., Whitty, M. T., & Baskerville, R. L. (2021). How can organizations develop situation awareness for incident response: A case study of management practice. *Computers & Security*, *101*, 102122.

Albanese, M., Cam, H., & Jajodia, S. (2014). Automated cyber situation awareness tools and models for improving analyst performance. In R.E. Pino, A. Kott, & M. Shevenell (Eds.), *Cybersecurity systems for human cognition augmentation* (pp. 47-60). Cham: Springer.

Allianz (2020). Allianz Risk Barometer. Retrieved at 15-10-2020 from https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/allianz-risk-barometer-2020-cyber-incidents.html

Arnott, D., & Pervan, G. (2008). Eight key issues for the decision support systems discipline. *Decision Support Systems*, *44*(3), 657-672.

Asgharpour, F., Liu, D., & Camp, L.J. (2007). Mental models of computer security risks. In S. Dietrich, & R. Dhamija (Eds.), *International Conference on Financial Cryptography and Data Security*. Berlin: Springer.

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior*, *48*(1), 51-61.

Bisantz, A.M., & Burns, C.M. (Eds.) (2009). *Applications of Cognitive Work Analysis*. Boca Raton, FL: CRC Press.

Braun, V. & Clarke, V. (2012). Thematic analysis. In H. Cooper (Ed.), *APA Handbook of Research Methods in Psychology: Vol. 2 Research Designs* (pp. 57-71). Washington, D.C.: American Psychological Association.

Burns, C.M. (2020). Cognitive work analysis: Models of expertise. In P. Ward, J.M. Schraagen, J. Gore, & E. Roth (Eds.), *The Oxford Handbook of Expertise*. Oxford: Oxford University Press.

Champion, M., Jariwala, S., Ward, P., & Cooke N.J. (2014). Using cognitive task analysis to investigate the contribution of informational education to developing cyber security expertise. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 58*(1), 310-314.

Cook, M.B., & Smallman, H.S. (2008). Human factors of the confirmation bias in intelligence analysis: Decision support from graphical evidence landscapes. *Human Factors, 50*(5), 745-754.

Chen, T.R ,Shore D.B ,Zaccaro S.J ,Dalal R.S ,Tetrick L.E ,Gorab A.K. (2014). An organizational psychology perspective to examining computer security incident response teams. IEEE Secur. Priv. 2014;12(5):61–7 .

Crandall, B., Klein, G., & Hoffman, R.R. (2006). *Working minds: A practitioner's guide to cognitive task analysis*. Cambridge, MA: The MIT Press.

D'Amico, A. & Whitley, K. (2008). The real work of computer network defense analysts. In G. Conti, J.R. Goodall, & K.L. Ma (Eds), *Proceedings of the Workshop on Visualization for Computer Security* (pp. 19-37). Berlin: Springer.

D'Amico, A., Whitley, K., Tesone, D., O'Brien, B., & Roth, E. (2005). Achieving cyber defense situational awareness: A cognitive task analysis of information assurance analysts. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 49*(3), 229-233.

DFLabs (2019). The Difference Between Playbooks and Runbooks in Incident Response. Retrieved at 15-10-2020 at https://www.dflabs.com/resources/blog/the-difference-between-playbooks-and-runbooks-in-incident-response/

Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. *Journal of Cybersecurity*, *5*(1), tyz013.

ECB (2018). TIBER-EU FRAMEWORK – How to implement the European framework for Threat Intelligence-based Ethical Red Teaming (europa.eu). Retrieved from the internet on September 16th, 2021 from https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf

Franke, U., & Brynielsson, J. (2014). Cyber situational awareness: A systematic review of the literature. *Computers & Security*, *46*(1), 18-31.

Gawande, A. (2010). *The checklist manifesto: How to get things right.* New York: Metropolitan Books.

Genge, B., Kiss, I., & Haller, P. (2015). A system dynamics approach for assessing the impact of cyber attacks on critical infrastructure. *International Journal of Critical Infrastructure Protection*, *10*, 3-17.

Grance, T., Kent, K., & Kim, B. (2004). *Computer Security Incident Handling Guide:*. US Department of Commerce, Technology Administration, National Institute of Standards and Technology.

Healey, C. G., Hao, L., & Hutchinson, S. E. (2017). Lessons Learned: Visualizing Cyber Situation Awareness in a Network Security Domain. In P. Liu, S. Jajodia, & C. Wang (Eds.), *Theory and Models for Cyber Situation Awareness* (pp. 47-65). Cham: Springer.

Hettema, H. (2021). Rationality constraints in cyber defense: Incident handling, attribution and cyber threat intelligence. *Computers & Security*, *109*, 102396.

Jenkins, D.P., Stanton, N.A., Salmon, P.M., & Walker, G.H. (2009). *Cognitive work analysis: Coping with complexity*. Farnham, England: Ashgate Publishing Limited.

Joffe, H. (2012). Thematic analysis. In D. Harper and A. Thompson (Eds), *Qualitative Research Methods in Mental Health and Psychotherapy: A Guide for Students and Practitioners* (pp. 209-223). Chichester: Wiley-Blackwell.

La Fleur, C., Hoffman, B., Gibson, C. B., & Buchler, N. (2021). Team performance in a series of regional and national US cybersecurity defense competitions: Generalizable effects of training and functional role specialization. *Computers & Security*, *104*, 102229.

Liu, P., Jajodia, S., & Wang, C. (Eds.) (2017). *Theory and models for cyber situation awareness*. Cham: Springer.

Mahoney, S., Roth, E., Steinke, K., Pfautz, J., Wu, C., & Farry, M. (2010). A cognitive task analysis for cyber situational awareness. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 54*(4), 279-283.

Mason, R.O., & Mitroff, I.I. (1981). *Challenging strategic planning assumptions*. New York: Wiley.

Militello, L.G., & Hutton, R.J. (1998). Applied cognitive task analysis (ACTA): A practitioner's toolkit for understanding cognitive task demands. *Ergonomics*, *41*(11), 1618-1641.

Mohammed, G. S., Wakil, K., Nawroly, S. S. (2018). The effectiveness of microlearning to improve students' learning ability. *International Journal of Educational Research Review, 3*(3), 32-38.

Naikar, N. (2013). *Work domain analysis: Concepts, guidelines, and cases.* Boca Raton, FL: CRC Press.

Naseer, A., Naseer, H., Ahmad, A., Maynard, S. B., & Siddiqui, A. M. (2021). Real-time analytics, incident response process agility and enterprise cybersecurity performance: A

contingent resource-based analysis. *International Journal of Information Management, 59,* 102334.

Nielsen, J. (1993). *Usability engineering*. San Diego: Academic Press.

Rajivan, P., & Cooke, N. (2018). Information pooling bias in collaborative security incident analysis. *Human Factors, 60*(5), 626-639.

O'Neill, A., Ahmad, A., & Maynard, S. (2021). Cybersecurity Incident Response in Organisations: A Meta-level Framework for Scenario-based Training. *arXiv preprint arXiv:2108.04996*.

Schaafstal, A., Schraagen, J.M., & Berlo, M. van (2000). Cognitive task analysis and innovation of training: The case of structured troubleshooting. *Human Factors, 42,* 75-86.

Schlette, D., Böhm, F., Caselli, M., & Pernul, G. (2020). Measuring and visualizing cyber threat intelligence quality. *International Journal of Information Security*, 1-18.

Schraagen, J.M.C., Chipman, S.F., & Shalin, V.L. (Eds.) (2000). *Cognitive task analysis*. Mahwah, NJ: Lawrence Erlbaum Associates.

Schraagen, J.M.C., & Ven, J.G.M. van de (2008). Improving decision making in crisis response through critical thinking support. *Journal of Cognitive Engineering and Decision Making, 2*(4), 311-327.

Schwenk, C., & Valacich, J.S. (1994). Effects of devil's advocacy and dialectical inquiry on individuals versus groups. *Organizational Behavior and Human Decision Processes, 59*(2), 210-222.

Shin, J., Son, H., Khalil, R., & Heo, G. (2015). Development of a cyber security risk model using Bayesian networks. *Reliability Engineering and System Safety, 134*(1), 208-217.

Shinde, N., & Kulkarni, P. (2021). Cyber incident response and planning: a flexible approach. *Computer Fraud & Security, 2021*(1), 14-19.

Van der Kleij, R. Kleinhuis, G., & Young, H. (2017). Computer Security Incident Response Team Effectiveness: A Needs Assessment. *Frontiers in Psychology*. doi: 10.3389/fpsyg.2017.02179.

Verizon (2020). 2020 data breach investigations report. Retrieved 06/9/2021 from: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

Vicente, K. (1995). Task analysis, cognitive task analysis, cognitive work analysis: What's the difference? *Proceedings of the Human Factors and Ergonomics Society 39th Annual Meeting, 39*(9), 534-537.

Vicente, K. (1999*). Cognitive Work Analysis: Toward safe, productive, and healthy computer-based work*. Mahwah, NJ: Lawrence Erlbaum Associates.

Biographical Sketch

Dr. Rick van der Kleij is an Industrial/Organizational psychologist with an interest in cyber security. He works as a senior researcher at the Netherlands Organisation for Applied Scientific Research. Rick is also associate lector at the Center of Expertise Cybersecurity at The Hague University of applied sciences. His current work focuses on the human element in cybersecurity and the performance of teams that are professionally involved in cybersecurity, such as computer security incident response teams and the employees of cybersecurity operations centers. Rick is convinced that behavioral aspects are key to improving cyber security within organizations and society as a whole.

Jan Maarten Schraagen is Principal Scientist at TNO. His research interests include resilience engineering, team communication processes, and human-machine teaming. He is main editor of *Cognitive Task Analysis* (2000) and *Naturalistic Decision Making and Macrocognition* (2008) and co-editor of the *Oxford Handbook of Expertise* (2020). He is editor in chief of the *Journal of Cognitive Engineering and Decision Making* and member of the editorial board of *Cognition, Technology and Work*. Dr. Schraagen holds a PhD in Cognitive Psychology from the University of Amsterdam, The Netherlands.

With a background in intelligence and psychology, Beatrice has specialized in cybersecurity by taking an integrative approach, working on bridging the gap between the human and technical aspects. Her previous endeavors include being an international safety consultant for Zeeko, a Dublin-based start-up working on online safety and a cyber threat analyst for RedSocks Security/Bitdefender NL. Now a scientist integrator at TNO, Beatrice has had the chance to work on a diverse range of topics regarding online safety, security and

intelligence. She is also involved as a speaker and member for Chorus, a community of experts on social engineering and disinformation.

Dr. Heather Young is a social psychologist and has worked at the Netherlands Organisation for Applied Scientific Research TNO for over 20 years in various areas including trust and cyber secure behavior. Her current focus is on the processing and effects of disinformation.