Envisioning cyber situation awareness through participatory video prototyping

Annika Andreasson*
KTH Royal Institute of Technology
Stockholm, Sweden
anniandr@kth.se

Sinna Lindquist
FOI Swedish Defence Research Agency
Kista, Sweden
sinna.lindquist@foi.se

ABSTRACT

Our digital societies are vulnerable to cyber crises. Without cyber-resilient organizations, vital societal functions may suffer incidents or loss of service. The diverse roles involved in cybersecurity decision-making require cyber situation awareness to uphold robust cybersecurity. Existing systems and processes supporting cyber situation awareness are not tailored to organizational needs, either at the role or the group level. This study explores the need for socio-technical system support, presenting common operational pictures supporting cyber situation awareness for staff handling cyberthreats. The participatory design method video prototyping was used to elicit needs from staff in a large, complex, public sector organization providing essential services. All participants have roles in cybersecurity crisis and incident management. Results from the video prototyping workshop suggest that cybersecurity staff need (i) a single support system for incident management, and (ii) a shared data repository underpinning (iii) role-specific common operational pictures. The envisioned system support provides traceability and accountability.

Keywords

Cyber situation awareness, common operational picture, cyber crises, participatory design, video prototyping

INTRODUCTION

Accelerating digital transformation is making governments, organizations, and citizens reliant on digital technologies to provide essential services, manage business processes, and perform routine everyday tasks (Abidi et al., 2025). With this development, our digital societies are becoming increasingly vulnerable to various cyberthreats, which can stem from intentional, unintentional, or natural causes. Threat actors are keeping abreast of security measures taken to keep digital infrastructure and assets secure (World Economic Forum, 2024). Going forward, without cyber-resilient organizations vital societal functions and digital infrastructure may suffer incidents and loss of service (Hausken, 2020).

Staff involved in cybersecurity work require cyber situation awareness (CSA) to uphold strong cybersecurity in order for their organizations to be cyber-resilient, especially in times of crises. Existing systems and processes supporting CSA might not be sufficient for cyber-resilience (Bellini et al., 2025). In addition, systems supporting customized visualizations of common operational pictures (COP) for CSA are needed (Conti et al., 2013; Jiang et al., 2022; McKenna et al., 2015). In the context of permeating digitalization and rising cyberthreats, the aim of this study is to explore the system support needs for common operational pictures (COP) supporting CSA for staff involved in incident management. To that end, the following research question was formulated: *What are the needs for system support for common operational pictures to aid cyber situation awareness for staff involved in cybersecurity work in a large, complex organization?*

To answer the research question, this study focuses on the needs of staff involved in cybersecurity incident management in one large, complex organization with staff in different localities. The organization operates in the public sector, with several thousand members of staff employed in the core organization and its subsidiaries.

*corresponding author

Somewhat simplified, the organization is complex in the sense that it does not have a straightforward, hierarchical organizational structure, but rather consists of core administration and several satellite organizations fully or partially owned. The organization provides various essential services and infrastructure. The different parts of the organization share some systems but do not have shared systems supporting cyber crisis management for staff in all parts of the organization.

BACKGROUND

This section presents background to situation awareness, cyber situation awareness, and common operational pictures. It also provides a short introduction to cyber crises, and gives some background to participatory design.

Situation awareness, cyber situation awareness, and common operational picture

Cyber-resilience, according to Björck et al., is "the ability to continuously deliver the intended outcome despite adverse cyber events" (Björck et al., 2015, p. 312). For organizations to be cyber-resilient, the members of staff involved with cybersecurity work in the organizations need to have cyber situation awareness (CSA), a prerequisite for successfully exercising cybersecurity command and control (Brynielsson, 2006). There are several models and definitions of situation awareness (SA) presented in the research literature (Salmon et al., 2008). Mica Endsley's three-level SA model is one of the most widely used, and it defines situation awareness as "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future" (Endsley, 1995, p. 36). The model introduced by Endsley (1995) is an individualistic cognitive model comprising three levels, where Level 1 SA is perception, Level 2 SA is comprehension, and Level 3 SA is projection.

Franke and Brynielsson performed a systematic literature review on CSA where they take CSA to be a subset of SA that regards the cyber domain (Franke & Brynielsson, 2014). Research into CSA has mainly focused on technical solutions and not so much on the human side (Ahmad et al., 2021; Barford et al., 2010; Franke et al., 2022). Research concerned with the human side of CSA has often focused on operators in Security Operations Centers (SOC) defending networks (Ofte & Katsikas, 2023). Operators in the SOC are not the only members of staff in need of CSA in an organization, though. Different actors that become involved in handling cyber incidents have different CSA needs (Franke et al., 2022; Gutzwiller et al., 2020).

Often discussed in connection with SA (and sometimes in confusion with it) is the COP. A COP is an artifact of some kind with the aim to provide actors with a "picture" of what's going on, whereas SA is a mental state where an actor has awareness of what's going on (Franke et al., 2022). It is not difficult to see how they are related as, somewhat simplified, the purpose of a COP is, basically, to facilitate SA. The COP has its origins in the military domain, and is also an integral part of crisis management (Comfort, 2007; Copeland, 2008). According to Wolbers and Boersma (2013), the initial view of a COP as an "information warehouse", where information is managed and stored, is giving way to a view of a "trading zone", where actors negotiate the information to make sense of it. COPs are not only helpful tools during crisis management but they could also be used for organizational learning after the crisis (Pilemalm et al., 2021).

In the crisis management literature, different aspects of the relationship between SA and COP have been studied. For example, Danielsson et al. (2014) investigate the relationship between COP and SA, and their findings show how information from different sources influences and changes the COP over time, and that the COP is used as information input to form role-specific situation awareness. In Steen-Tveit and Radianti (2019), it is noted that if the actors involved in crisis management use other information-sharing channels, such as one-on-one phone calls or text communication, than those that are used to build the COP there is a risk that the actors do not share the information conveyed there with other actors who might need it to form their SA.

In the cyber domain, COPs have been studied in different areas, e.g., the military (Conti et al., 2013; Kim et al., 2023), or for sector-specific needs, such as the financial sector (Varga et al., 2021). A single COP is not sufficient to provide the required CSA for everyone in a specific organization though. McKenna et al. (2015) uses personas to suggest that diverse roles have different needs for cybersecurity visualizations. However, as pointed out by Jiang et al. (2022) there are few studies on cyber COPs for staff at all levels in an organization and this is an area for future research. This study addresses this research gap by investigating COP needs in support of CSA for (i) staff in various roles (ii) within the context of a large, complex organization.

Cyber crises

Events in the cyber domain have the potential to develop into cyber crises. Cyber crises can be seen as a type of transboundary crisis when they cut across multiple domains, progress at uneven rates, are challenging to foresee, involve numerous actors with unclear responsibilities, and lack predefined solutions (Kuipers & Boin, 2015). One example of a cyber event turning into a cyber crisis is the NotPetya attack. The NotPetya wiper malware, designed to destroy data, was first observed in Ukraine and then spread globally in 2017 (Stoddart, 2022). One of the global organizations impacted by the malware was the shipping company Maersk, where the malware caused disruptions in supply chains worldwide for Maersk customers, and Maersk themselves suffered a financial loss of about 250 to 300 million USD (Greenberg, 2018). The NotPetya attack has the characteristics of a transboundary crisis as outlined by Kuipers and Boin (2015).

While NotPetya was designed to destroy (Stoddart, 2022), there are other ways cyberthreats can cause harm. Vulnerabilities are a very common such threat to cybersecurity and cyber-resilience. Managing vulnerabilities is part of the everyday activities in most organizations. However, some vulnerabilities are more severe in nature and are rated as "critical", i.e., rated a 10 on the 1-10 vulnerability scale (FIRST, 2024). In the Swedish context, the Swedish Civil Contingencies Agency hosts the national Computer Security Incident Response Team, CERT-SE, which issues automatic notifications to direct attention to technical vulnerabilities and ways of mitigating them.[1] In 2021, one such critical vulnerability was found in the ubiquitous logging tool Log4j, which served as a basis for the scenario developed for the workshop conducted in this study. The vulnerability was ubiquitous and seen as such a severe threat that US, UK, New Zealand, Canadian, and Australian cybersecurity agencies issued a joint cybersecurity advisory statement with guidance on mitigating the vulnerability.[2] While there are reports of exploits of the vulnerability, it did not develop into a cyber crisis. However, at the time of working on mitigating the vulnerability, such an outcome could not be foreseen and the vulnerability was treated as having that potential.

Participatory design for socio-technical system development

The ideas of socio-technical systems originate from the 1950s, when, in the British post-war coal industry, it became evident that to uphold and develop effectiveness, the entire organization needed to be considered and understood. To insert new technology was simply not enough (Trist, 1981). Socio-technical systems are complex systems consisting of humans and technology and their relation, including organization, processes, goals, culture, stakeholders, and regulation (Davis et al., 2014). The complex relations between those entities make it difficult to foresee the effects of new system support systems (Hasan & Kazlauskas, 2009; Snowden, 2002). From a socio-technical design perspective, the goal is to achieve well-functioning organizations where efficiency and effectiveness are mirrored in a good work situation for the workers. To achieve this goal requires taking technical as well as social aspects into consideration during development. To reflect the complexity of the socio-technical system, there are approaches that allow development to be carried out in smaller steps, such as in an iterative development process (Rogers et al., 2023) and incremental development process (Dove et al., 2023). This way, lessons learned regarding what leads to a goal are utilized in future development steps. In such processes, different methods, such as user-centered design methods for investigating aspects such as user needs of the socio-technical system, can be used.

There are many ways to investigate the relationship between humans and computerized systems. In the human-computer interaction community, the user-centered design approach has shown a beneficial path to understanding users' needs since the 1980s (e.g., Norman and Draper (1986); Gould et al. (1991); Mao et al. (2005); Still and Crane (2017)) including participatory design methodology that, according to Bødker et al., "starts with the current practices of people in groups and organizations and uses future alternatives for joint reflection and action" (Bødker et al., 2022, p. 3). One such activity, or method, is video prototyping[3] (Mackay et al., 2000). User-based video prototyping as a method can be suitable in a systems development process as well as for the design of artifacts since it specifies the users, users' activities and handling of interfaces or artifacts, and the process of handling them (Brynielsson et al., 2013).

Video prototyping, which consists of a series of different activities, is a "quick and dirty" way of providing users with a voice to describe their needs for performing certain tasks. It is especially applicable in situations where it is difficult to get access to the users for several or longer periods of time, or to study their work in their real setting, or to understand their work under certain conditions, such as during an emerging cyber incident. The method is based on real situations, real users' experience, knowledge, and needs, i.e., specific needs, and suggests future solutions

[1] https://cert.se/rad-och-stod/ants/.

[2] https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-356a.

[3] Here we refer to video prototyping as an activity done by the users to show the designers, not the other way around, where video prototyping is done by designers to show users.

to those needs, i.e., general solutions and design ideas (Westerlund, 2009). In chronological order, the video prototyping methodology includes a brainstorming session on a specific topic, where participants share problems and needs with one another in words, written on post-it notes or verbally, and create storyboards to show their ideas as a way of step-by-step detailing the unfolding of a scenario. After the scenario planning, the participants assign actors and make the props that need to be part of the video prototyping, film the scenario, and finally, the participants show their video prototypes to one another, give feedback, and discuss the suggested design ideas.

There are several benefits to the method. The designers and researchers get the users' own descriptions of their needs and not filtered through the lens of a designer. This includes the process of a task as well as the interface, in narrated, drawn, and filmed format, that the users themselves have reviewed, all of which are valuable input to the analysis. For the users, video prototyping activities are a sort of informative and fun work-related get-togethers, often where unknown problems and issues within the work organization or between roles are brought into light.

METHOD

Using participatory design methods, this study explores the needs for system support presenting common operational pictures supporting cyber situation awareness for staff handling an emerging cyberthreat.

Participants

The seven participants in this study were all staff connected to a large, complex organization and they all require adequate CSA in their role. All but one participant had previous experience from various types of collaboration during the organization's handling of the critical Log4j vulnerability dubbed Log4Shell, which, at the time of discovery, the UK National Cyber Security Centre said had the potential to be "the most severe computer vulnerability in years" (National Cyber Security Centre, 2021). The six participants with experience of Log4Shell participated in a parallel case study on the handling of Log4Shell in their organization and were asked in connection with that study if they wanted to participate in another study relating to system support for cyber situation awareness. The seventh participant was recruited through their position in the organizational CERT. Participant group, role, and time in the role are outlined in Table 1.

Table 1. Participant groups and roles

Group	Participant	Role	Time in role
1	*P1*	CISO	11 yrs
1	*P2*	CERT technical lead (Consultant)	5 yrs
1	*P3*	Information security coordinator (Subsidiary)	7 yrs
2	*P4*	IT director	12 yrs
2	*P5*	CERT manager	5 yrs
2	*P6*	Process lead incident management	4 yrs
2	*P7*	CERT analyst	$<$ 1 yrs

Workshop

The recruited participants were invited by email to a workshop at the organization of one of the authors to minimize interruptions from the workshop attendants' respective workplaces and to provide a new setting. The workshop was scheduled for three hours and started with obtaining informed consent from the participants before a short presentation on user-centered design and video prototyping. The participants had been pre-divided into two groups with the aim of getting diverse roles and experiences in each group. The groups were presented with a scenario, outlined in Appendix A, which had similarities to the Log4j vulnerability from which they had previous experience so as not to spend too much time trying to understand the implications of the vulnerability. The first task of the workshop was for each group to create storyboards where they make their support system needs and COP needs concrete. They were instructed not to limit themselves in terms of what technology can do today or with compliance restrictions. The groups were provided with separate rooms to work in with workshop materials and a researcher serving as facilitator. After the storyboard session, the groups came together to present their ideas to each other and give feedback on each other's ideas. The second task was to produce a video prototype based on the storyboard and feedback showing their needs for support system and COP. When the filming was done, the groups gathered again to show their video prototyping ideas to each other and discuss them.

Empirical material

The video prototyping workshop generated a diverse empirical material. In addition to the films created by the participating groups, the participants in Group 1 created individual storyboards, whereas there was no storyboard, individual or group, created in Group 2, but rather a narrative. Photos from both groups, as well as researcher notes from the presentations and discussions during the day were collected. The empirical material is detailed in Table 2. Due to the sensitive nature of the material, the video prototypes themselves cannot be shared.

Table 2. Empirical material

Item	Description
Video1	Group 1 film 2 min 3 sec
Video2	Group 2 film 3 min 19 sec
Story1	Storyboard *P1* Group 1
Story2	Storyboard *P2* Group 1
Story3	Storyboard *P3* Group 1
Photo1	Photo from Group 1 work showing parts of process
Photo2	Photo from Group 2 work showing interfaces
ResNot	Researcher notes from presentations and discussion

Analysis

The empirical material listed in Table 2 was processed iteratively by the authors, focusing on the following issues: (i) what role-specific needs for COP information elements are expressed, and (ii) what needs for shared COP information elements are expressed, and (iii) what aspects of incident handling processes can be identified. To identify instances of these issues, the author(s) created the equivalent of a "service blueprint", i.e., a diagram that shows the relationships between people, process, and technology (Gibbons, 2017). Service blueprinting is a commonly used method within the user experience (UX) and service design community, to visualize who needs to do what, when, and with what, in a "swim-lane format" in order to design a service. In addition, it can also be used to generate and transfer insights between competencies by using the service blueprinting method during the analysis and design of complex matters, as for example in Magyari and Secomandi (2023).

The service blueprint diagram, as seen in Figure 1, shows the roles present in the empirical material, and the progression of events and certain needs expressed in connection with those events as manifested in the empirical material. The sticky-note shapes identify the source of the data, film, storyboard, or other to aid the researchers in back-tracking the empirical material. When identified events and needs were mapped up sequentially, additional needs were identified and marked with small sticky notes in different colors. This was done manually due to the sensitive nature of the topics discussed in the empirical material.

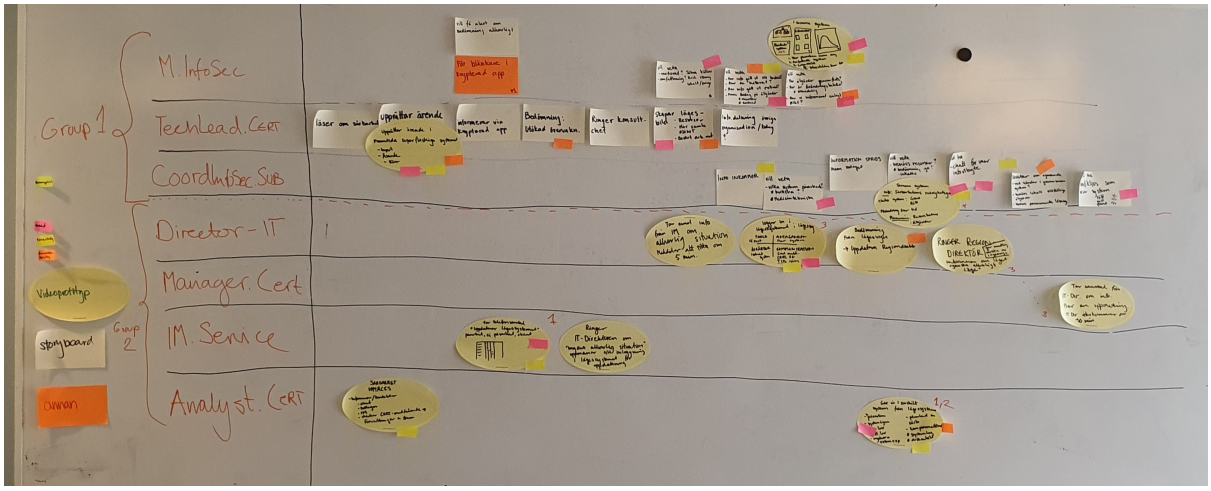

Figure 1. Ongoing analysis of the empirical material. Large sticky notes denote sources: oval for video prototype, yellow for storyboards, orange for other. Small sticky notes denote other aspects: pink for need, yellow for traceability, orange for accountability.

RESULTS

This section presents the results from the workshop in the form of summaries of the empirical material pertaining to each group.

Group 1

Video1 is a silent movie that starts by showing how *P2* creates a ticket for the vulnerability, as shown in Figure 2. *Story2* from *P2* additionally relates that they read up as much as they can on the vulnerability and also inform others (e.g., *P1*) through an encrypted app. With additional information they make the decision that there is need for additional monitoring of the incident and they start asking questions: What resources are available in the organization? Where to gather trustworthy open source intelligence (OSINT)? What working methodology should the CERT adapt?

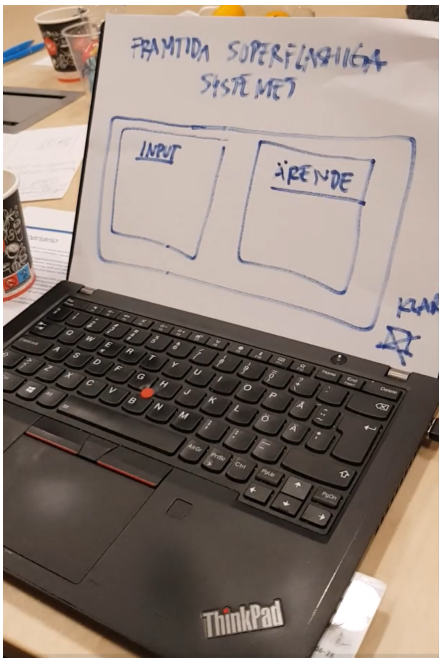

Figure 2. Screenshot from Video1 and view P2

Video1 continues to show *P3* on their premises working in the system seeing the vulnerability score critical 10, which is the highest score available, systems listed in red or green indicating status, as well as a plan for resources and emergency actions for their subsidiary, which can be seen in Figure 3. *Story3* from *P3* additionally relates that they have a need to know what systems are affected by the vulnerability. How many of the critical systems for the subsidiary are affected? How many of the systems with special legal compliance needs are affected? With additional information the assert that there is a need to call in additional resources and they would like a chat in the system to share specific information about the vulnerability. *P3* then needs to take additional decisions. What is happening in shared systems? What should be done locally in the subsidiary? Temporary actions to take? Permanent solutions? They have also drawn a traffic light showing the status of systems in percentages of red, yellow, and green, where they can follow the change as the situation unfolds.

Video1 ends with *P1*'s high-level view of the current status, Figure 4, with an overview of the organization, showing what divisions are affected, what percentage of systems are patched, a foursquare COP showing the status of Technology, Actions, Information, and Decisions, and a timeline showing the evolution of the situation. *Story1* provides additional needs of *P1*. They express the need to be alerted when an event is deemed serious with information, if it is verified information, the severity of the incident. Is there a risk for business impact? Organization-wide or local? They want to know if information has been shared with relevant stakeholders, and if they have confirmed receiving the information. They also want to know if the information has gone out externally, if there are suggestions for remedial actions, and what the remedial actions entail in the form of resource requirements. Have the remedial actions been confirmed performed? *P1* also wants to be able to see change over time to be able to judge if the rate of change is sufficient.

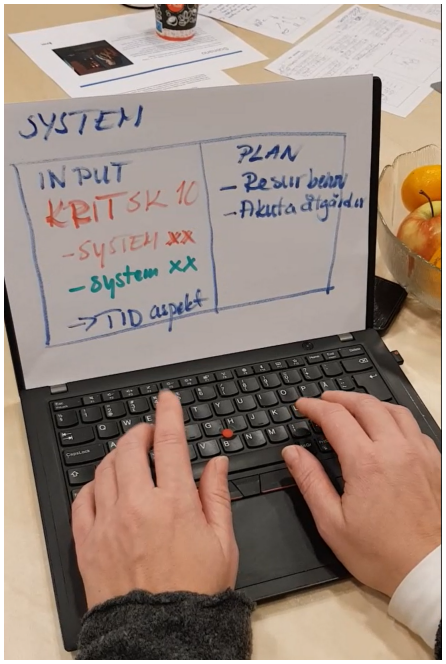

Figure 3. Screenshot detail from Video1 and view P3

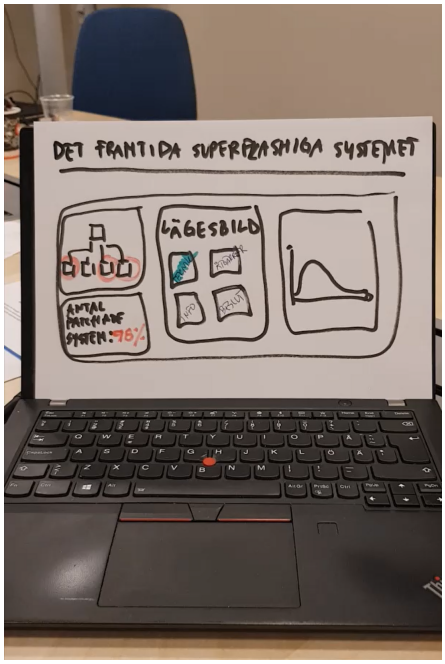

Figure 4. Screenshot detail from Video1 and view P1

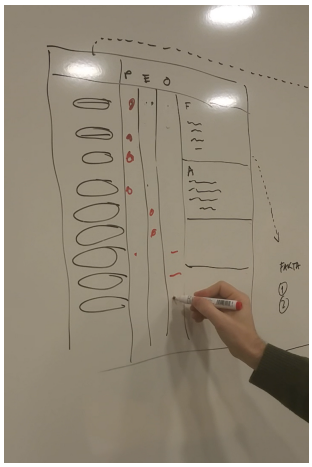

Figure 5. Screenshot detail from Video2 and view P7

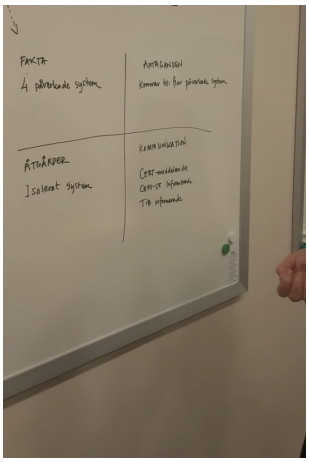

Figure 6. Screenshot detail from Video2 and view P4

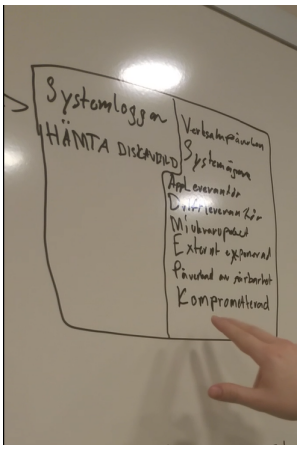

Figure 7. Screenshot detail from Video2 and view P7

Group 2

Video2 starts with *P7* stating they have found out about the critical vulnerability and they alert their manger (*P5*), colleagues, Incident Manager (IM) (*P6*), and send a CERT-message to all organizational units. *P6* receives the call from *P7* and proceeds to update the common operational system with what systems are affected, as depicted in Figure 5. That the CERT has an established process and calls IM is mentioned during the storyboard discussion and captured in *ResNot*.

Video2 continues with *P6* calling *P4* to inform them about the seriousness of the situation, and urging them to access the common operational system, which *P4* does. They look at a foursquare COP showing *Facts*, *Assumptions*, *Measures*, *Communication*, outlined in Figure 6. Based on what they see there, they decide that the Executive Officer needs to be informed. *P4* calls the Executive Officer (played by *P5*) to give a verbal account of what they see in their COP, and the Executive Officer asks to be updated in 30 min.

The ending of *Video2* shows *P7* viewing a single system from the long list of systems seen in Figure 5. *P7* says they are accessing a specific system in the common operational system to find information about the system's operational impact, who is system owner, application supplier, operational supplier, software package, if it is externally exposed and if it is compromised, the CERT marks it as such and gets a disk image, depicted in Figure 7.

IDENTIFIED NEEDS

The analysis of the results suggests that cybersecurity staff need (i) a single support system for incident management and (ii) a shared data repository underpinning (iii) role-specific COPs.

A single support system for incident management: It is evident from the workshop that both groups share a common understanding of their current process. The material from both groups integrates well to show all participants' roles in managing the incident. Having a single system offers seamless support for incident management. There is no need to change system support if changing work methodology, which *P2* considers, due to an incident being escalated outside the regular incident handling process. *Video2* clearly shows how the participants access the system support view with their desired COP as awareness of the vulnerability spreads through-out the organization. A single system supports the traceability of information shared during the incident as well as accountability for decisions taken.

The need for a single system is seen in both groups' empirical material. In Group 1 it was called "the future super-flashy system" and in Group 2 "the common operational system". This single system can handle everything and support all needs for incident management that the groups express. The system's support focus is on the management of an incident, from initial creation of the "ticket" as shown by Group 1 in Figure 2, to the resolution of the incident. The system needs to support all roles across organizational boundaries so that data and information can be shared without causing cognitive overload. Additionally, it should be apparent for each specific role where to enter what information into the system, and where to access the current COP.

A shared data repository: When having a single support system for the incident management process, across roles and organizations and with real-time updated information, all data needs to be available in a shared data repository. The COPs presented should be based on the same data and information, irrespective of who needs to look at the COP, and always populated by the most recent data. As shown by Group 2, *P6* enters information about the status for each system, which then is shown, e.g., as four affected systems in the foursquare view of *P4* in Figure 6. This supports traceability of how information was accessed and shared in the process and the decision maker can feel confident in making decisions based on the the latest information supporting accountability, as expressed by the desire to know if stakeholders have received information by *P1* in Group 1.

System support presenting role-specific COPs: Participants in both groups need role-tailored COPs to support their role-specific CSA needs, as shown in Figures 1-7. For the system to present such tailored COPs, the system is dependent on members of staff populating the system with the required information elements. To form the envisioned CSA staff needs COPs presenting information at the level of granularity required for their role, with the possibility for certain roles to drill down when desired. For example, each system *P7* marks as affected by the vulnerability gets aggregated for the COPs of *P1* and *P4*, as well as for the traffic-light of *P3*, and *P4* can drill down from the aggregated systems they see presented in their COP down to the specific systems presented in the COP of *P7*.

DISCUSSION

Although the desire to have one tool to do everything is not new, it could be interpreted as an expression of frustration that the previous experience with Log4Shell has highlighted that processes and systems do not function together seamlessly and that this becomes poignant during the managing of an incident as the cognitive load increases. One interpretation of the expressed wish for a single system is the need for one coherent process regarding the sharing of data and information, where data and information sharing can be both active and passive. Active, as exemplified by *P6* marking systems as affected by the vulnerability, and passive, as exemplified by *P1* keeping an eye out for the rate of change over time. By having a shared data repository feeding the system, no data should be missed or left out from the COP due to a missing link in the information-sharing process, hindering the CSA of staff. It is not uncommon that information gets stuck in silos in organizations where more than one organizational entity is involved in cybersecurity (Andreasson et al., 2024; Shahjee & Ware, 2022) or that actors communicate outside the established channels for COP building (Steen-Tveit & Radianti, 2019).

COPs traditionally have been viewed as one singular artifact that provides all the information necessary for decision-makers during crises or military operations, from which they can form their role-specific SA from the COPs contents (Danielsson et al., 2014). However, as seen in Artman and Persson (2000) collaboration around a COP could entice individual actors to present their role-specific perspectives of certain parts of the COP to encourage discussions regarding the ongoing mission. In this study, the workshop participants describe their role-specific information needs, showing that one COP does not fit all. Instead of forming their role-specific SA from one singular COP, as in Danielsson et al. (2014), they envision a customized COP for their role-specific needs created from a shared data repository. What is "common" in this context is the shared data repository, which is presented in customizable views for different roles. The information is shared and presented according to need. These views can still be used for negotiations or discussions, as in Wolbers and Boersma (2013).

In contrast to McKenna et al. (2015), who developed personas from interviews with users and designed visualizations based on that, or to Kim et al. (2023, who designed visualizations of a cyber COP based on document analysis of documents based on "Joint Publication 3-12, Cyberspace Operations" (Joint Chiefs of Staff, 2018), in the study presented here, the users themselves were invited to contribute from their experience through the participatory design method. As Jiang et al. (2022) pointed out, there is a lack of studies on systems that can provide tailored COPs, and more work should be devoted to this area. This study lays some ground for future work by addressing the need for COP support to improve CSA for several roles at different levels.

While not explicitly addressed in the empirical data, aspects of traceability and accountability are implicitly present in the expressed needs. This is most clearly shown in *Story1* created by *P1*, where they state that they need to confirm whether internal and external stakeholders have been informed and whether remedial actions have been taken. It is also seen in *Story3*, where *P3* wants a chat function to communicate with others involved in the incident management. Traceability and accountability are important not only during the managing of the incident, but also for any post-incident lessons learned activities, where the organization can learn from experience and make necessary changes to existing processes (Thompson, 2018).

Another aspect of the workshop itself is that, for the participants, the use of the video prototyping methodology provided additional value. Meeting in one place outside of their organization and in this particular constellation had never happened before. The work with the storyboards and films gave them a chance to share their previous experiences of the handling of the Log4j vulnerability. This vulnerability was treated as a cyberthreat of enormous proportions, where Computer Security Incident Response Teams sent out national emergency messages to draw attention to possible severe consequences of the exploitation of the vulnerability. It had not been clear how intensive the handling of the emerging cyberthreat had been for some roles, while at the same time, the information shared to higher levels in the organization was perceived as being at the right level of granularity and provided in a timely and competent way. The opportunity to share experiences was appreciated and enlightening and could be seen as a lessons-learned activity for improved incident response (Ahmad et al., 2021) that had previously not been conducted with these participants.

It is worth noting that none of the participants brought up having access to information about threat actors and their behavior in the system support. This is in line with the findings in Varga et al. (2018), where they investigated what the information requirements are for CSA at the national level and the participants in the study did not request information about threat actors. Also noteworthy is that there was no mention of the system supporting information sharing across organizations, e.g., sharing information with organizations in the same sector for the creation of a national-level sector COP. It is plausible to imagine that there are government agencies that want to have CSA when critical vulnerabilities or severe cyber incidents might have severe adverse effects at the national level, as suggested in the Swedish Government Official Report on the implementation of the European Union NIS2 Directive (SOU 2024:18, 2024).

Limitations

The identified needs are based on participants being asked not to restrict themselves to what is possible using today's technology or adhering to current compliance restrictions, but rather to imagine what might be possible in the future. While this opens up the possibility to think outside established practices and gives room to "impossible" ideas, those solutions might not be feasible.

While the videos generated fit well together, they are quite different in nature. They express diverse needs, which could be explained by the composition of roles included in the two groups. Also, in one of the groups, Group 2, the participants did not create group or individual storyboards but instead described their ideas verbally and drew on a whiteboard. That meant that the method was not strictly followed, and the empirical material for that group was not as rich, but the content that the storyboard was intended for was collected. However, the entire material generated is sufficient for analysis.

There are seven participants in this study, which could be regarded as a low number. However, the participants here are all part of one large socio-technical system, representing different cybersecurity roles involved in incident management that, at the time of the workshop, did not have the desired system support. The number of participants was seen as adequate for generating the empirical material. Other roles in the organization could have taken part, such as system architects or data protection officers, but the focus was on roles with direct involvement in crisis management.

There is also the issue regarding method efficiency and whether video prototyping is the best way to elicit needs from participants. In this case, as it is conducted in parallel with another study, the opportunity of having the participants gather for three hours was a time-efficient first step to elicit an overall insight into the participants' needs. For developing a system for the participant's expressed needs, another route could be data collection in the form of goal-directed task analysis (Endsley & Jones, 2011) as a part of a situation awareness-oriented design process (Endsley & Jones, 2024).

CONCLUSION

The aim of the study was to explore the system support needs for common operational pictures supporting cyber situation awareness for staff handling an emerging cyberthreat by answering the research question: *What are the needs for system support for common operational pictures to aid cyber situation awareness for staff involved in cybersecurity work in a large, complex organization?* From the empirical material generated by the video prototyping workshop, the results suggest that cybersecurity staff need (i) a single support system for incident management supporting the entire process, and (ii) a shared data repository, underpinning (iii) role-specific COPs when envisioning how to improve their CSA. This study could be conducted as the authors had a unique opportunity to gather participants with roles within cybersecurity in a large, complex, organization in one place for the duration of three hours. The participants had not previously gathered in this constellation to discuss their practices. Conducting workshops or reviews around past incident experiences could provide an opportunity for organizational learning (Ahmad et al., 2020; Pilemalm et al., 2021).

Analyzing the video prototypes through the service blueprint method was useful in terms of visualizing the process and seeing that the workshop participants, who represented different levels of responsibility and decision-making in the organization, were quite in agreement regarding the overall process. A next step would be to do a service blueprint with the staff involved in cybersecurity in the organization to validate this paper's findings, deepen the understanding of their respective needs during different stages when managing a cyberthreat, and test it on other similar incidents and crises. An interesting aspect of such an activity would be to investigate which parts of their process should go into a support system, and which should be done as they do it today, such as briefing one another via mobile phone. Another aspect would be to try to understand why it is important for certain tasks to keep the existing approach. The results from this study would also be interesting to evaluate with other cybersecurity staff in public sector organizations, both civilian and military, as well as cybersecurity staff from private sector organizations.

As mentioned previously, there is a lack of studies on systems that can provide specifically tailored COPs. The contribution of this study is showing that role-specific needs should be taken into account when designing for CSA support for multiple roles. The results from the study presented here can be seen as a starting point for further such research. A deeper investigation is needed to develop a system addressing the participants' expressed needs.

ACKNOWLEDGEMENTS

This research was supported by the Swedish Armed Forces and the Swedish Defence Research Agency. We are grateful for the contributions of our workshop participants and extend our thanks to them. Special thanks are also due to Joel Brynielsson for his assistance during the workshop.

APPENDIX A: SCENARIO

It is Friday evening and one of the CERT staff reads about a possible remote code execution vulnerability in the Depeche logging package Blog4j on reddit.

The Blog4j library is an open-source logging library provided by the Depeche Software Foundation. The library is often used in programs and services to collect logs for development, operations, and security. Several large suppliers use the open-source library in their services.

The next day, a tweet from a trusted source speculates that the vulnerability could be classified as a 10.0 on the CVSS scale. There is also a message from a FIRST actor about the vulnerability. In connection with this, there is a call to the IT director from a supplier's Swedish representative saying that their service uses the vulnerable component, but they have no further information.

A couple of hours later, suppliers like CISCO, Oracle, and Siemens publish their first communications about how their products are affected by the vulnerability.

REFERENCES

Abidi, O., Richet, J.-l., & Vitari, C. (2025). Digital transformation and resilience: Dimensions and interactions. *Journal of Global Information Management*, *33*(1), 1–64. https://doi.org/10.4018/JGIM.367873

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. https://doi.org/10.1002/asi.24311

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. https://doi.org/10.1016/j.cose.2020.102122

Andreasson, A., Artman, H., Brynielsson, J., & Franke, U. (2024). Cybersecurity work at Swedish administrative authorities: Taking action or waiting for approval. *Cognition, Technology & Work*, *26*(4). https://doi.org/10.1007/s10111-024-00779-1

Artman, H., & Persson, M. (2000). Old practices - New technology: Observations of how established practices meet new technology. *Proceedings of the 5th International Conference on the Design of Cooperative Systems (COOP'2000)*.

Barford, P., Dacier, M., Dietterich, T. G., Fredrikson, M., Giffin, J., Jajodia, S., Jha, S., Li, J., Liu, P., Ning, P., Ou, X., Song, D., Strater, L., Swarup, V., Tadda, G., Wang, C., & Yen, J. (2010). Cyber SA: Situational awareness for cyber defense. In S. Jajodia, P. Liu, V. Swarup, & C. Wang (Eds.), *Cyber Situational Awareness: Issues and Research* (pp. 3–13). Springer US. https://doi.org/10.1007/978-1-4419-0140-8_1

Bellini, E., D'Aniello, G., Flammini, F., & Gaeta, R. (2025). Situation awareness for cyber resilience: A review. *International Journal of Critical Infrastructure Protection*, *49*, 100755. https://doi.org/10.1016/j.ijcip.2025.100755

Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). Cyber resilience — Fundamentals for a definition. In A. Rocha, A. M. Correia, S. Costanzo, & L. P. Reis (Eds.), *New Contributions in Information Systems and Technologies* (pp. 311–316). Springer International Publishing. https://doi.org/10.1007/978-3-319-16486-1_31

Bødker, S., Dindler, C., Iversen, O. S., & Smith, R. C. (2022). *Participatory Design*. Springer International Publishing. https://doi.org/10.1007/978-3-031-02235-7

Brynielsson, J. (2006). *A gaming perspective on command and control* [Doctoral dissertation, Royal Institute of Technology].

Brynielsson, J., Johansson, F., & Lindquist, S. (2013). Using video prototyping as a means to involve crisis communication personnel in the design process: Innovating crisis management by creating a social media awareness tool. In S. Yamamoto (Ed.), *Human Interface and the Management of Information. Information and Interaction for Learning, Culture, Collaboration and Business,* (pp. 559–568). Springer. https://doi.org/10.1007/978-3-642-39226-9_61

Comfort, L. K. (2007). Crisis management in hindsight: Cognition, communication, coordination, and control. *Public Administration Review*, *67*(1), 189–197. https://doi.org/10.1111/j.1540-6210.2007.00827.x

Conti, G., Nelson, J., & Raymond, D. (2013). Towards a cyber common operating picture. *2013 5th International Conference on Cyber Conflict (CYCON 2013)*, 1–17.

Copeland, J. (2008). *Emergency response: Unity of effort through a common operational picture* (tech. rep.). Army War College Carlisle Barracks, PA.

Danielsson, E., Alvinius, A., & Larsson, G. (2014). From common operating picture to situational awareness. *International Journal of Emergency Management*, *10*(1), 28. https://doi.org/10.1504/IJEM.2014.061659

Davis, M. C., Challenger, R., Jayewardene, D. N. W., & Clegg, C. W. (2014). Advancing socio-technical systems thinking: A call for bravery. *Applied Ergonomics*, *45*(2, Part A), 171–180. https://doi.org/10.1016/j.apergo.2013.02.009

Dove, R., Lunney, K., Orosz, M., & Yokell, M. (2023). Agile systems engineering – Eight core aspects. *INCOSE International Symposium*, *33*(1), 823–837. https://doi.org/10.1002/iis2.13055

Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors*, *37*(1), 32–64. https://doi.org/10.1518/001872095779049543

Endsley, M. R., & Jones, D. G. (2011). *Designing for situation awareness: An approach to user-centered design* (2nd ed.). Taylor & Francis Group.

Endsley, M. R., & Jones, D. G. (2024). Situation awareness oriented design: Review and future directions. *International Journal of Human–Computer Interaction*, *0*(0), 1–18. https://doi.org/10.1080/10447318.2024.2318884

FIRST. (2024). Common Vulnerability Scoring System SIG.

Franke, U., Andreasson, A., Artman, H., Brynielsson, J., Varga, S., & Vilhelm, N. (2022). Cyber situational awareness issues and challenges. In A. A. Moustafa (Ed.), *Cybersecurity and Cognitive Science* (pp. 235–265). Academic Press. https://doi.org/10.1016/B978-0-323-90570-1.00015-2

Franke, U., & Brynielsson, J. (2014). Cyber situational awareness: A systematic review of the literature. *Computers & Security*, *46*, 18–31. https://doi.org/10.1016/j.cose.2014.06.008

Gibbons, S. (2017, August). Service Blueprints: Definition.

Gould, J. D., Boies, S. J., & Lewis, C. (1991). Making usable, useful, productivity-enhancing computer applications. *Commun. ACM*, *34*(1), 74–85. https://doi.org/10.1145/99977.99993

Greenberg, A. (2018). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *Wired*.

Gutzwiller, R. S., Dykstra, J., & Payne, B. (2020). Gaps and opportunities in situational awareness for cybersecurity. *Digital Threats: Research and Practice*, *1*(3), 1–6. https://doi.org/10.1145/3384471

Hasan, H., & Kazlauskas, A. (2009). Making sense of IS with the Cynefin framework. *In Proceedings of PACIS 2009*.

Hausken, K. (2020). Cyber resilience in firms, organizations and societies. *Internet of Things*, *11*, 100204. https://doi.org/10.1016/j.iot.2020.100204

Jiang, L., Jayatilaka, A., Nasim, M., Grobler, M., Zahedi, M., & Babar, M. A. (2022). Systematic literature review on cyber situational awareness visualizations. *IEEE Access*, *10*, 57525–57554. https://doi.org/10.1109/ACCESS.2022.3178195

Joint Chiefs of Staff. (2018). Joint Publication 3-12, Cyberspace Operations.

Kim, K., Youn, J., Yoon, S., Kang, J., Kim, K., & Shin, D. (2023). Study on cyber common operational picture framework for cyber situational awareness. *Applied Sciences*, *13*(4), 2331. https://doi.org/10.3390/app13042331

Kuipers, S., & Boin, A. (2015). Exploring the EU's role as transboundary crisis manager: The facilitation of sense-making during the ash crisis. In R. Bossong & H. Hegemann (Eds.), *European Civil Security*

Governance: Diversity and Cooperation in Crisis and Disaster Management (pp. 191–210). Palgrave Macmillan UK. https://doi.org/10.1057/9781137481115_9

Mackay, W. E., Ratzer, A. V., & Janecek, P. (2000). Video artifacts for design: Bridging the gap between abstraction and detail. *Proceedings of the 3rd conference on Designing interactive systems: processes, practices, methods, and techniques*, 72–82. https://doi.org/10.1145/347642.347666

Magyari, R., & Secomandi, F. (2023). Service blueprinting for better collaboration in human-centric AI: The design of a digital scribe for orthopedic consultations. *International Journal of Design*, *17*(3), 63.

Mao, J.-Y., Vredenburg, K., Smith, P. W., & Carey, T. (2005). The state of user-centered design practice. *Commun. ACM*, *48*(3), 105–109. https://doi.org/10.1145/1047671.1047677

McKenna, S., Staheli, D., & Meyer, M. (2015). Unlocking user-centered design methods for building cyber security visualizations. *Proceedings of the 2015 IEEE Symposium on Visualization for Cyber Security (VizSec 2015)*, 1–8. https://doi.org/10.1109/VIZSEC.2015.7312771

National Cyber Security Centre. (2021, December). Log4j vulnerability - what everyone needs to know.

Norman, D. A., & Draper, S. W. (1986). *User centered system design; new perspectives on human-computer interaction*. L. Erlbaum Associates Inc.

Ofte, H. J., & Katsikas, S. (2023). Understanding situation awareness in SOCs, a systematic literature review. *Computers & Security*, *126*, 103069. https://doi.org/10.1016/j.cose.2022.103069

Pilemalm, S., Radianti, J., Munkvold, B. E., Majchrzak, T. A., & Steen-Tveit, K. (2021). Turning common operational picture data into double-loop learning from crises–Can vision meet reality? *Proceedings of the 18th International ISCRAM Conference–Blacksburg, VA, USA May 2021*, 417–430.

Rogers, Y., Sharp, H., & Preece, J. (2023). *Interaction design: Beyond human-computer interaction* (Sixth edition). John Wiley; Sons.

Salmon, P. M., Stanton, N. A., Walker, G. H., Baber, C., Jenkins, D. P., McMaster, R., & Young, M. S. (2008). What really is going on? Review of situation awareness models for individuals and teams. *Theoretical Issues in Ergonomics Science*, *9*(4), 297–323. https://doi.org/10.1080/14639220701561775

Shahjee, D., & Ware, N. (2022). Integrated network and security operation center: A systematic analysis. *IEEE Access*, *10*, 27881–27898. https://doi.org/10.1109/ACCESS.2022.3157738

Snowden, D. (2002). Complex acts of knowing: Paradox and descriptive self-awareness. *Journal of Knowledge Management*, *6*(2), 100–111. https://doi.org/10.1108/13673270210424639

SOU 2024:18. (2024). *SOU 2024:18 Nya regler om cybersäkerhet*. Regeringskansliet.

Steen-Tveit, K., & Radianti, J. (2019). Analysis of common operational picture and situational awareness during multiple emergency response scenarios. *Proceedings of the 16th International ISCRAM Conference*.

Still, B., & Crane, K. (2017). *Fundamentals of user-centered design: A practical approach*. CRC press.

Stoddart, K. (2022). *Cyberwarfare: Threats to Critical Infrastructure*. Springer International Publishing.

Thompson, E. C. (2018). Eradication, recovery, and post-incident review. In E. C. Thompson (Ed.), *Cybersecurity Incident Response: How to Contain, Eradicate, and Recover from Incidents* (pp. 117–123). Apress. https://doi.org/10.1007/978-1-4842-3870-7_9

Trist, E. L. (1981). *The evolution of socio-technical systems* (Vol. 2). Ontario Quality of Working Life Centre Toronto.

Varga, S., Brynielsson, J., & Franke, U. (2018). Information requirements for national level cyber situational awareness. *2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, 774–781. https://doi.org/10.1109/ASONAM.2018.8508410

Varga, S., Brynielsson, J., & Franke, U. (2021). Cyber-threat perception and risk management in the Swedish financial sector. *Computers & Security*, *105*, 102239. https://doi.org/10.1016/j.cose.2021.102239

Westerlund, B. (2009). *Design Space Exploration: Co-operative creation of proposals for desired interactions with future artefacts*. Kungliga Tekniska högskolan.

Wolbers, J., & Boersma, K. (2013). The common operational picture as collective sensemaking. *Journal of Contingencies and Crisis Management*, *21*(4), 186–199. https://doi.org/https://doi.org/10.1111/1468-5973.12027

World Economic Forum. (2024). *Global Cybersecurity Outlook 2024* (tech. rep.). World Economic Forum.