Computers & Security 126 (2023) 103069

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Understanding situation awareness in SOCs, a systematic literature review ☆

Håvard Jakobsen Ofte*, Sokratis Katsikas

Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Gjøvik 2802, Norway

ARTICLE INFO

Article history:
Received 17 October 2022
Revised 12 December 2022
Accepted 15 December 2022
Available online 16 December 2022

Keywords:
Situation awareness
Security operations center
Cyber security
Human performance System performance

ABSTRACT

Situation awareness is shown through human factors research to be a valuable construct to understand and improve how humans perform while operating complex systems in critical environments. Within cyber security one such environment is the Security Operations Center (SOC). With the increasing threat of hybrid warfare, knowledge about situation awareness within SOC environments, where human error or low performance may be detrimental, must be developed. This paper reports on the results of a Systematic Descriptive Literature Review of the current research on situation awareness within SOCs. The goal of the paper is to analyze how situation awareness is understood in the current research. To achieve this goal three aspects of understanding were addressed: Theoretical foundations; levels of conceptualization; and measurement of situation awareness. Theoretical foundations in the literature were assessed by how situation awareness was defined and the presence of references to theoretical models of SA. The results show a clear trend of basing the research on Endsley's three level situation awareness model; this model has been developed into a domain specific formulation called "Cyber Situation Awareness". Some parts of the literature, particularly in research aimed at developing tools for improving situation awareness, lack a theoretical foundation; some refer to alternative theoretical foundations of situation awareness like Stanton et al.'s Distributed Situation Awareness. Further, a balance between conceptualizations on the individual, group and system level has been identified. Within research aimed at developing tools for improving situation awareness there are some examples of specialized and precise measurements of situation awareness, but in general the research seems too reliant on indirect measures of situation awareness. The paper concludes with the proposition of connecting the systems-based theoretical perspective of distributed situation awareness into the research, utilizing a systems level conceptualization of situation awareness. This might prove to be a useful bridge between the human cognitive perspective of situation awareness and the development of the complex technical environment of critical importance that SOCs represent.

1. Introduction

Cyber security attracts increasing attention in both public debate and national strategies. IT systems and networks are rapidly becoming an infrastructure which other systems, services and institutions are dependent upon. With increasing geo-political unrest and the use of cyber-attacks as part of hybrid warfare, the security of this infrastructure has become a prioritized area of development and research. There is no universally agreed upon definition of cyber security, but the use of the term is increasingly preferred over partly overlapping terms like information security, computer security, and IT security (Schatz et al., 2017). It has been argued that cyber security is a broader construct than information security because it also includes the human aspect of security (von Solms and van Niekerk, 2013). "Cyber" is here referring to IT systems, the networks these systems operate through, and the physical infrastructure these systems operate on. Cyber security refers to activities aimed at securing these systems, networks, and infrastructure from intended or unintended harm or malfunction, and the consequential state of security these activities are aimed at achieving. Cyber systems are rapidly becoming ingrained into all parts of

Abbreviations: HFR, Human Factors Research; SA, Situation Awareness; ISA, Individual Situation Awareness; DSA, Distributed Situation Awareness; SSA, Shared Situation Awareness; CSA, Cyber Situation Awareness.

☆ This work was supported by the Research Council of Norway under Project nr 333900 *"Situation awareness in virtual security operations centers"* and Project nr 310105 *"Norwegian Centre for Cyber Security in Critical Sectors (NORCICS)"*.

* Corresponding author.
E-mail addresses: havard.ofte@ntnu.no (H.J. Ofte), sokratis.katsikas@ntnu.no (S. Katsikas).

https://doi.org/10.1016/j.cose.2022.103069

infrastructure and services. The consequence is a simultaneous increase of reliance on cyber systems and higher exposure to cyber-attacks. Some examples like the Stuxnet attack (Chen and Abu-Nimeh, 2011), the SolarWinds breach (Willett, 2021), the attack on Norsk Hydro (Oueslati et al., 2019), and several other more recent incidents affecting systems operating in critical sectors around the world highlight this growing vulnerability and the potential devastating consequences of cyber-attacks.

The entities responsible for cyber security in critical sectors e.g., network providers, power-suppliers, public services, manufacturing facilities, and large organizations often centralize this responsibility. The responsibility is often placed upon a group of expert human operators within a *Security Operation Center (SOC)*. There are different terms used for centers responsible for cyber security that emphasize different aspects of operations e.g., *Cyber Security Operation Centers (CSOCs), Network Operations Centers (NOCs)* and *Security Intelligence Centers (SICs)* (Vielberth et al., 2020; Zimmerman, 2014). For consistency, such centers are hereby referred to only as "SOCs". A SOC is responsible for cyber security within a specified set of cyber systems through activities like monitoring, analyzing, and reacting to potentially harmful events (Vielberth et al., 2020).

The criticality of cyber security combined with the centralization of this responsibility to a small group of experts actualizes the human factors within SOCs. A large body of literature within Human Factors Research (HFR) addresses how to reduce human error and optimize performance among human operators of complex systems within critical domains like SOCs.

This paper reports on the results of a Systematic Descriptive Literature Review of the current research on situation awareness within SOCs with an eye towards analyzing how situation awareness is understood. To achieve this goal three aspects of understanding were addressed: What are the theoretical foundations of situation awareness; what are the levels of conceptualization of situation awareness; and how is situation awareness measured. In addition to systematizing the current knowledge in the field, the analysis of these core aspects of understanding situation awareness within existing research makes this literature review a unique contribution. By reviewing the content of the research in the light of their inherent core understanding of the phenomenon of situation awareness provides insight into how to understand situation awareness within the context of SOCs.

The remaining of the paper is structured as follows: Section 2 presents the relevant background. Section 3 describes in detail the method used to perform the literature review. Section 4 presents the results of our analysis that are discussed, along with their implications on future research, in Section 5. In Section 6 we turn our attention to the limitations of our study and, finally, Section 7 summarizes our conclusions.

2. Background

A widely researched construct within HFR is *Situation Awareness (SA)* (Lee et al., 2017). SA has several definitions in the research literature, but most generally it refers to the process of gathering information about a situation and converting this information into an awareness that can differentiate between the suitability of potential actions.

2.1. Theory and definitions of SA

Several partly opposing definitions and theoretical models of SA have been proposed (Salmon et al., 2008). The most recognized definition within HFR is Endsley's cognitive three-level model of the *Individual SA* process (Endsley, 1995). This model, graphically depicted in Fig. 1, is hereby referred to as *Individual SA (ISA)*, defined by Endsley 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). ISA has been shown to be of critical importance for timely and effective human response. Research has largely been focused towards contexts where human performance is critical e.g., flight control, nuclear power plant control, military operations and first responders (Lee et al., 2017). A wide range of methods for assessing and measuring SA have been developed as part of this research (Endsley and Garland, 2000).

Several different definitions of SA that expand or challenge the ISA model have been proposed. One of the issues that has led to the expansion of definitions is how to understand and assess the SA of a group of people. Endsley's model that centers on the individual has been the basis for later models of SA that focus on groups. Endsley herself has been an active contributor to this development.

More recently a somewhat opposing model to ISA, explaining SA on a systems level, has been proposed. This model of *Distributed SA (DSA)* is defined as "*activated knowledge for a specific task within a system*" (Stanton et al., 2006). DSA views the process and results of SA as something not only residing in individual humans, but as something distributed across both human and non-human agents. The DSA model argues that ISA has a too individualistic and linear approach to understand the SA process. The research following the DSA definition has made some progress in developing operationalizations and measurements of SA (Salmon et al., 2017). DSA's critique of ISA has been countered by researchers within the cognitive HFR tradition, most notably by Endsley herself, pointing out that DSA does not contradict ISA, but only emphasizes a different level of analysis (the system as a whole) (Endsley, 2015). One clear contradiction between the two strains of SA research is the view on whether SA can reside in non-human agents. DSA proposes that the different aspects of SA might well reside in different types of agents throughout a system i.e., perception might be assigned to an Intrusion Detection System (IDS), the comprehension to an Artificial Intelligence (AI) subsystem, and the projection into the future by a human operator. Endsley, on the other hand, refutes the notion of computers having "situation models" analogous to humans and having overall responsibility of complex systems: "*When a human no longer has that responsibility, then human SA will be moot and the automatons can take over. But I do not think this will be happening any time in the near future in most complex and safety-critical systems*." (Endsley, 2015). This shows some contention within the ISA paradigm against attributing SA processes to information systems or AI or that the results of such processes might reside in non-human systems as awareness.

2.2. Conceptualizations of SA

The conceptualizations of SA vary between different theories of SA and contexts. Herein we categorize three different levels of analysis used within SA research, namely the *Individual* Level, the *Group* Level, and the *System* Level. The Individual Level and the Group Level are both mainly based on the theoretical model of ISA. The System level of analysis in the literature is often based on the theoretical model of DSA.

At the Individual Level, SA is conceptualized as the mental state of an individual human operator resulting from the process described by the ISA model (Endsley, 1995). At the Group Level, SA has several conceptualizations. *Team SA* (TSA) is conceptualized as the sum of all the individuals' SA within a team. TSA is achieved through connecting the different individuals' SA to each other through the inputs and outputs of the ISA model i.e., one person's "Performance of action" may become another person's "State of

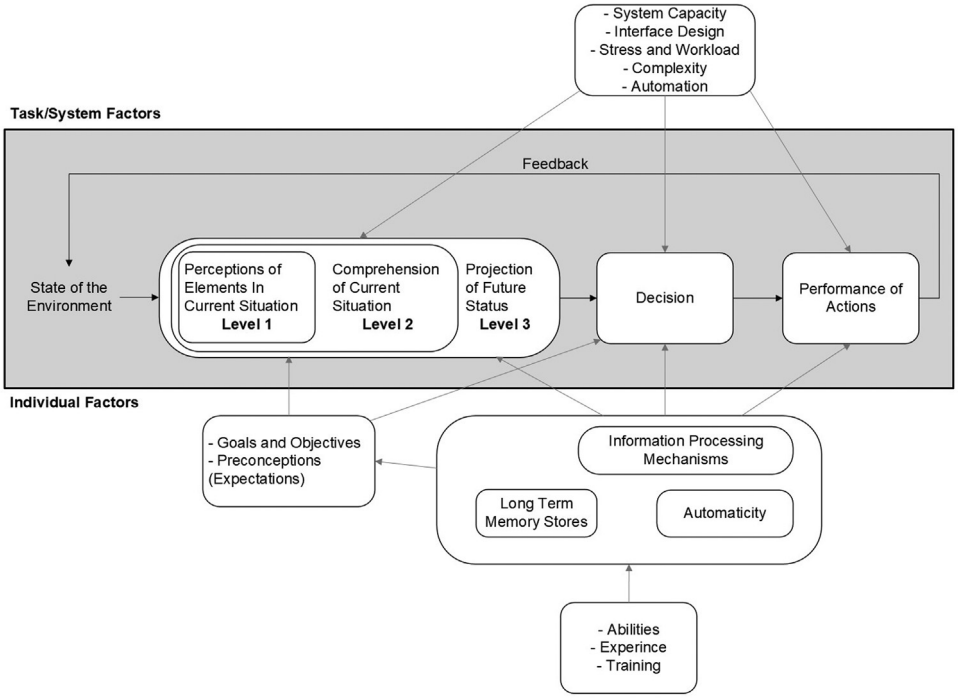

Fig. 1. Endsley's ISA-model (Endsley, 1995)

The Environment" on which SA in turn is based. This linking of individuals' SA forms "the chain" of TSA (Kaber and Endsley, 1998). *Shared SA (SSA)* is also a conceptualization on the Group Level of analysis. It refers to the extent to which individuals within a team have overlapping awareness of a situation i.e., percept, comprehend and project the situation in the same way when they are given the same information and overlapping SA requirements (Kaber and Endsley, 1998). At the System Level, SA is conceptualized as an emergent property of a dynamic and collaborative process between the human and non-human agents (Salmon et al., 2017). The DSA literature has largely focused on descriptive research with the aim to explain different aspects of the complex dynamics of these collaborative processes (Salmon et al., 2017).

Within the research literature on SA there are examples of other theories with somewhat different conceptualizations. Some of these are commented upon when relevant throughout the sequel.

2.3. Measurements of SA

A wide range of techniques for measuring SA have been developed (Salmon et al., 2009). Examples are: Freeze probe techniques like SAGAT (Endsley, 1988b); Real time probe techniques like SPAM (Durso et al., 1998); Self-rating techniques like SART (Taylor, 2017); and Observer rating techniques like SABARS (Matthews and Beal, 2002). In addition, the measurement of performance as an outcome of changing SA parameters is widely used, as well as proxy-measures for SA i.e., measuring indices of SA processes like eye-tracking (Salmon et al., 2009). As a starting point for establishing domain specific measurements, the method of *Task Analysis* is often used (Salmon et al., 2009). Variants such as *Cognitive Task Analysis* and *Work Domain Analysis* are also used, but they all have in common that qualitative methods like interviews and observation are used to map the aspects of a working environment that forms the basis for the SA process (Salmon et al., 2009). All the mentioned measuring techniques have been used to measure SA both at the individual and the group level. Both the ISA and DSA operationalizations of SA use these measurements although they were developed within the ISA paradigm (Salmon et al., 2009). Within the research on DSA, it has proven difficult to find stable and generalizable operationalizations of SA at the Systems Level, and measurements are mostly used as part of descriptive research (Salmon et al., 2017).

2.4. SA in cyber security

Within the field of cyber security, the subject of SA has attracted growing attention from academic research. Within this context, SA is both referred to technically, as the process of compiling, compressing and fusing data, but also linked to the cognitive theoretical foundation of ISA. The connection between the technical and cognitive view on SA was presented in an edited volume where the specific term of *Cyber SA* (CSA) was presented (Jajodia et al., 2009). Therein CSA was presented as a subset of SA where the SA requirements for the human operators are aimed at cyber security. The technical SA is linked to the cognitive process as a central part of the environment and tools the operators interact with to gain CSA (Jajodia et al., 2009).

A later systematic literature review on CSA following this understanding has also been published (Franke and Brynielsson, 2014). The review showed that the majority of the literature was mainly focused on developing tools or solutions that could benefit CSA without evaluating or measuring the effect on SA specifically. This gap was confirmed by a more recent review (Gutzwiller et al., 2020), concluding with the following call for research to: "*(1) understand what cyber SA is from the human operators' perspectives, then (2) measure it so that (3) the community can learn whether SA makes a difference in meaningful ways to cybersecurity, and whether methods, technology, or other solutions would improve SA and thus, improve those outcomes.*"

This literature review aims to assess the current state of research on SA within the specific context of SOCs. Although the reviews on CSA are relevant, the identified gaps invite a more specific investigation of SA from the operator's perspective. The hu-

man operators within cyber security are arguably most specifically identified within the context of SOCs. A SOC consists of a defined and organized group of specialists tasked with the security of a defined set of networks and systems. The operators' work environment and demands are complex and dynamic, and their decision making is often time constrained and with potential critical consequences. The context of SOCs is thus similar to environments where SA is shown through experimental research to be of critical importance, like Power Plant Control Rooms, Flight Control, Military Mission Control (Lee et al., 2017).

By defining this context, the review is aimed at the first research gap pointed out in (Gutzwiller et al., 2020). In order to understand what CSA is from the human operator's perspective, this article reviews existing research on SA in SOCs. This review departs from existing reviews on CSA which identify the human operator based on cyber security related tasks, to focus on overall SA for human operators specifically responsible for cyber security in a defined context.

This further allows for a review of the theoretical foundations of SA within the relevant literature. CSA seems to have a strong connection to ISA, alongside a more technical perspective on SA. But CSA does not show a theoretical connection to DSA as a system level conceptualization of SA. This begs the question whether the level of analysis on SA research in SOCs and the theoretical foundations in the field are aligned. This literature review therefore addresses research questions that explore how the current research literature understands SA in a SOC setting.

3. Method

The literature review was conducted systematically following prescribed methods for descriptive reviews (Fink, 2019). The review was chosen to be descriptive because the preliminary search revealed that the body of research present which has comparable measurements of SA is not large. This assessment of the current research is confirmed by other reviews (Franke and Brynielsson, 2014; Gutzwiller et al., 2020).

The method of conducting descriptive reviews describes the review process through 5 phases: **Research question, Databases, Search strings, Screening and filtering**, and **Review of included papers** (Fink, 2019). The methodological considerations and decisions are presented below chronologically following these phases. The PRISMA guidelines is an evidence-based set of items recognized as required when reporting systematic reviews and meta-analyses (Page et al., 2021). The PRISMA guidelines were consulted and followed when applicable. The systematic literature review was conducted in April 2022.

3.1. Research questions

Through a preliminary literature search different aspects of how SA is understood within cyber security were considered. The context of SOCs was chosen to assist in clarifying how SA is understood by limiting the review to a context of human operators in a setting comparable to more developed and mature SA research (Gutzwiller et al., 2020). Existing literature reviews on CSA showed signs of one-sided theoretical foundation used within the research literature. The existing reviews did not address the different levels of analysis in conceptualizing SA. Although existing reviews address how SA is measured in the research, this review includes this aspect in order to analyze connections between theory, conceptualizations and measurements within the literature. Accordingly, the following research questions were defined to address these issues:

1 What theoretical foundations of SA are used within the context of SOCs?
2 What levels of conceptualization for SA are used?
3 What techniques for measuring SA are used?

Table 1
Terms included in search string.

SA			SOC
	Situation Awareness	AND	Security Operations Center
OR	Situational Awareness	OR	Security Operation Center
		OR	Security Operations center
		OR	Security Operation center
		OR	Network Operations Center
		OR	Network Operation Center
		OR	Network Operations center
		OR	Network Operation center
		OR	(Cybersecurity OR Cyber Security) AND Team

3.2. Databases

A preliminary search was done within 8 online databases of scientific research. These were selected based on the recommendations within a guide of doing literature reviews within computer science (Silva and Neiva, 2016), and some databases referenced in existing relevant literature review on CSA (Franke and Brynielsson, 2014). After assessing overlap in the search results, five scientific databases were selected for the systematic literature search, namely Scopus, IEEE Xplore, EBSCO Academic Search Complete, Web of Science Core Collection, and Science Direct. The databases were accessed through their respective websites; no third-party search providers were used.

3.3. Search string

The following two terms were chosen to be part of the search string: "situation(al) awareness" and "SOCs". The first term was given two possible variations within the search string i.e., "situation awareness" OR "situational awareness". These two terms are interchangeable within the relevant literature (Endsley, 1994), and the preliminary search results showed that the string needed to include both of these parallel terms. The second term was given a wide set of variations in the search string. This was because a wide variety of different terms is used for operations centers responsible for cyber security throughout the relevant literature e.g., "security operations center" OR "network operation center". The search string also included "cyber security" AND "team" combined, as a term functioning as a variant of SOC. The terms included in the search string are presented in Table 1.

Table 1 shows how the search string was constructed. When a record had present at least one term variant (presented as separate rows) from the SA column and at least one term variant from the SOC column, it was returned as a hit. In some of the databases the additional requirement of also including either the term *Human Factor* OR *Human Performance* was included in the search string. This was done to exclude papers referring only to technical aspects of SA in SOCs from databases that returned higher numbers of hits.

The phrasing of the Boolean search string varied somewhat between databases, also depending on the databases' search operators and rules for phrasing the search string. In some databases it was also necessary to exclude non-academic papers, through filters. Some of the databases had restrictions to the allowed number of Boolean operators. The variants of SOC-terms resulting in the maximal hits were chosen through testing. Table 2 presents a detailed overview of search strings and filters used for each respective database.

The search strings were tested and adjusted several times before they were applied. Literature that was taken note of as relevant in the preliminary search was used as a marker that the

Table 2
Boolean search strings used.

Database	Scopus	IEEE Xplore	EBSCO Academic Search Complete	Web of Science Core Collection (Clarivate)	Science Direct
Search string	(TITLE-ABS-KEY (“situation awareness” OR “situational awareness”) AND “human factor”) AND (ALL (“security operations center” OR “security operation center” OR “security operations center” OR “security operation center” OR “network operations center” OR “network operation center” OR “network operations center” OR “network operation center” OR ((“cybersecurity” OR “cyber security”) AND “team”)))	((“All Metadata”: “situation awareness” OR “situational awareness”) AND (“human performance” OR “human factor”)) AND (“Full Text & Metadata”: “security operations center” OR “security operation center” OR “security operations center” OR “security operation center“ OR “network operations center” OR “network operation center” OR “network operations center” OR “network operation center” OR ((“cybersecurity” OR “cyber security”) AND “team”))	TX (“situation awareness” OR “situational awareness”) AND TX ((“cybersecurity” OR “cyber security”) AND “team”) OR (“security operations center” OR “security operation center” OR “security operations center” OR “security operation center” OR “network operations center” OR “network operation center” OR “network operations center” OR “network operation center”)	ALL= (“situation awareness” OR “situational awareness”) AND ALL= ((“human factor” AND “cyber security”) OR (“human factor” AND “cybersecurity”) OR “security operations center” OR “security operation center” OR “security operations center” OR “security operation center” OR “network operations center” OR “network operation center” OR “network operations center” OR “network operation center”)	Title abstract or keywords: (“situation awareness” OR “situational awareness”) Find Articles with these terms: (“security operations center” OR “security operation center” OR “security operations center” OR “security operation center” OR “network operations center” OR “network operation center” OR ((“cybersecurity” OR “cyber security”) AND “team”)
Filters	None	None	Excluded source types: Magazines, Trade Publications and Newspapers	None	Excluded Article type: Book chapters

search string included relevant literature. The number of search results was used as a marker for the specificity of the search string.

The preliminary search results indicated a large body of research regarding development of tools for data fusion and computer visualization that referred to increased Situational Awareness as a goal without measuring this or referring to any specific understanding or definition of Situation Awareness. The search string was applied adaptively in the respective databases to reduce the number of such results. This was done by specifying that the first search term (SA) had to be present within the title, keywords or abstract of the result and that the second term (SOC) could be present anywhere within the record. This decreased the number of results outside the scope of the review considerably.

3.4. Screening and filtering

After the search had been conducted, the resulting records were gathered and scanned for duplicates. The duplicates were removed and then the records were screened. The screening consisted of assessing if the records violated the exclusion criteria. The screening included only one exclusion criterion, namely that the record must represent an original academic study. This was assessed through screening metadata like title author, type of publication and, in some cases, the abstract. Exclusion criteria relating to type of study, year of publication or funding were considered but not used. The decision to not administer such exclusion criteria was based on the findings from the preliminary literature review that indicated a limited number of studies that addressed SA in SOCs. In order to give a useful overview of the current literature, all types of academic studies were included e.g., theoretical proposals, reviews, qualitative studies, quantitative studies. Both conference papers and journal articles were included. This was done to include as many relevant studies as possible, but also to allow for the most recent development of the research field to be included in this review.

The following inclusion criteria were used in the filtering process:

1 The study had to address SA specifically. The study had to either refer to a specific definition or theoretical background for SA or give an own explanation of how SA was understood.
2 The study had to be conducted in a SOC setting or address a SOC setting in the paper. A SOC setting was defined as a specified group of human operators responsible for the cyber security of a specified system and/or network.

The filtering process was conducted by attaining the full text manuscript of the records identified. First the abstracts were assessed against the inclusion and exclusion criteria. If all the inclusion criteria were met in the information given in the abstract and no exclusion criteria were met, the study was included in the review. If the abstract was not enough to discern whether or not the inclusion and exclusion criteria were met, the complete manuscript was assessed. All the studies that met both the exclusion and inclusion criteria were fully reviewed. The number of records included and excluded in each part of the process is shown in Fig. 2 and presented in Section 4.1. End Note™20 was used for managing the records, for identifying duplicates and for retrieving full text manuscripts.

3.5. Review of included articles

A review process and synthesis of the results was conducted and documented. First, the number and types of studies were identified. Then the topic or themes of the studies were identified and categorized. This gave a broad overview of the reviewed literature. Then, the studies were reviewed according to the research questions. All the included studies were read in full and categorized in relation to the three research questions. The categorization of the studies was coded by identifying different aspects within each study and subsequently summarizing all identified aspects of each study. The following is a description of the categories and codes used:

- **Theoretical foundation of SA** was assessed through identifying what definitions of SA and theoretical references were used. This assessment included two separate codes for each study,

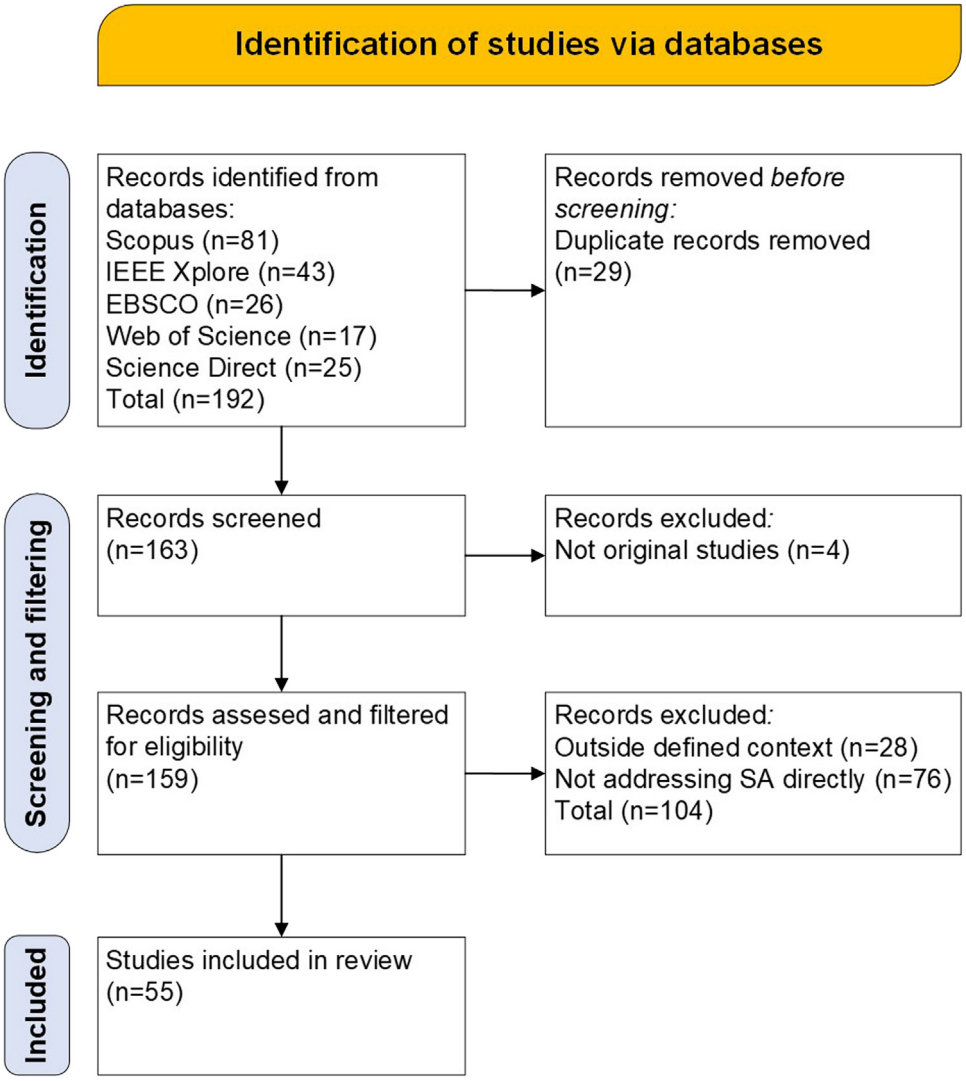

Fig. 2. Flowchart identification, screening, and filtering

namely the definition used; and additional theoretical references. Thus, the theoretical foundation used within studies was assessed both on the dominant theoretical foundation (definition) and the presence of other theoretical foundations within the study.

- **Conceptualization of SA** was assessed through considering what level of analysis the study referred to regarding SA i.e., if it considered SA on the individual, group, or systems level. If the study included several levels of analysis, it was coded as having multiple conceptualizations. This was identified through reviewing the full study manuscript and inferring on what level SA was expressed as residing. In addition, the term used for SA in the paper was recorded.
- **Measurement of SA** was assessed by identifying what indicators of SA the study presented. The following categories of measurement techniques were used:
- Performance (Measures of objective task performance by an individual, group or system as an indicator of SA quality)
- Direct observation (Measuring SA with probing measurements, like SAGAT (Endsley, 1988b))
- Observer rating (Measuring SA by an observants' rating of the operators SA, like SABARS (Matthews and Beal, 2002).)
- Self-rating (Measuring SA through participant self-rating of SA, like SART (Taylor, 2017).)
- Task analysis (Assessing SA through descriptive methods of identifying processes and tasks relevant for the context specific SA processes, like Cognitive Task Analysis (Salmon et al., 2009))
- Proxy (Inferring SA through measurements of factors known to affect SA or be affected by SA, like Workload or eye movements (Salmon et al., 2009))

The studies that referred to several measurements of SA were coded as "multiple". If the study referred only to SA as affecting performance without referring to any other method of measuring SA, it was identified as understanding performance as a measure of SA. The resulting codes were then reviewed in relation to each other i.e., if there were patterns in the conceptualizations and theoretical foundations of SA in the papers. NVivo© 1.5.1 was used to review and code the references included in the review.

4. Results

The results are presented in three parts. Firstly, the results from the search in databases and the screening and filtering process are presented. Then the papers included in the final review are presented and categorized according to type of studies and main themes. Finally, the results of the analysis aimed at categorizing how SA is understood are presented.

4.1. Search results, screening, and filtering

The search string used in the chosen databases yielded a total of 192 results. The search results were checked for duplicates, screened, and then filtered following the inclusion and exclusion criteria described in Section 3.4. Fig. 2 presents the number of records included and excluded in the different stages of the screening and filtering process, following the PRISMA guidelines (Moher et al., 2011):

Fig. 2 shows that 29 duplicate records were removed, leading to 163 records going through the screening process. 4 records were removed in the screening due to violating the exclusion criteria of not being original studies. In the filtering process a total of 104 studies were excluded from the review because they did not meet the inclusion criteria of addressing SA specifically and/or being outside of the context of SOCs. The process resulted in 55 studies included in the final review.

4.2. Main themes and study types

The final review showed that 23 of the studies were focused on the development of tools that somehow were aimed at increasing the quality of SA in SOC settings. The tools described ranged from data filtering and fusion (Cinque et al., 2020; Huang et al., 2016; Matey et al., 2022; Salvi et al., 2022; Settanni et al., 2017a; Sunny et al., 2014; Zhong et al., 2018), to information sharing (Leszczyna et al., 2019; Park et al., 2017; Settanni et al., 2017b; Wallis and Leszczyna, 2022), to visualization (Giacobe, 2013; Husák et al., 2022; Mullins et al., 2020), to tools for assessing or automating human performance (Dutt et al., 2013; Dutt and Gonzalez, 2012; Kokkonen and Puuska, 2018; Sarkar et al., 2022; Shah et al., 2018; Shurrab and Awan, 2015; Zhong et al., 2015; Zhu et al., 2021). There was also a review of the existing tools for increasing SA within power grid systems (Le Blanc et al., 2017).

There were in total 14 review papers; some of them also presented theoretical or implementation proposals for further development of SA within SOC environments (Ahmad et al., 2019; Andrade and Yoo, 2019; Brynielsson et al., 2016; Cain and Schuster, 2014, 2016; Debatty and Mees, 2019; Franke and Brynielsson, 2014; Gomez et al., 2019; Gutzwiller et al., 2020; Hall et al., 2015; McNeese and Hall, 2017; Nazir and Han, 2022; Pahi et al., 2017). The reviews ranged in content from specifically addressing the current state of the art of SA within cybersecurity (Franke and Brynielsson, 2014; Gutzwiller et al., 2020), to broader reviews concluding with the proposition of a model of cognitive processes within cyber security (Andrade and Yoo, 2019). Some of the reviews focused on different measurements of SA within cyber security, giving suggestions to further development (Brynielsson et al., 2016; Cain and Schuster, 2016).

There were six qualitative and observational studies included in the review (Ahrend et al., 2016; Eldardiry and Caldwell, 2015; Gutzwiller et al., 2016; Kanstrén and Evesti, 2016; Kokkonen and Puuska, 2018; Paterson, 2014; Smith et al., 2021). Two of these studies were task analysis studies identifying and mapping what tasks human operators face within SOCs and how these tasks are organized (Gutzwiller et al., 2016; Paterson, 2014). The other four were mixed studies including interviews, observation, and text-based analysis. Three of the studies reviewed were case studies examining different organizational and management issues related to incidents and exercises in SOC environments (Ahmad et al., 2021; Bhatt et al., 2014; Granåsen and Andersson, 2016). There were two survey studies included in the review (Chandra et al., 2022; Varga et al., 2018). There were in total six effect and experimental studies included in the review (Champion et al., 2012; Cooke et al., 2019; Happa et al., 2021; Jaeger and Eckhardt, 2021; Kostelic, 2020; Thangavelu et al., 2021).

Overall, the review showed a clear trend that the current research of SA within SOCs is mostly focused on the development of tools and methods that can alleviate SA-requirements for the human operators through reducing cognitive complexity.

4.3. Understanding of SA

As part of the review the studies were analyzed with regards to three different aspects of understanding SA, namely theoretical foundation of SA; conceptualization of SA; and measurement of SA. Table 3 presents an overview and the complete categorization of all the reviewed papers, what type of study each one is, and the coding of the papers on the three aspects of understanding SA. It presents what type of studies are present, their theoretical foundation, conceptualization, and measurement of SA. The table is grouped from top to bottom by study type. Then within each study type the different levels of analysis in conceptualizing SA is grouped together.

4.4. Theoretical foundations of SA

How SA is defined within each research paper was analyzed and coded as part of the review process. 16 of the 55 papers used Endsley's individual three-stage definition of ISA. Most of these papers cited or paraphrased the definition given in Endsley's 1995 article (Endsley, 1995), while some referred to later repetitions of the same definition. When considering the study type, the ISA definition is the one most used in review or theoretical proposals. 8 out of 14 such papers use ISA as its only definition and 3 additional reviews include ISA as one of multiple SA definitions. Half of the qualitative studies (3 out of 6) use the ISA definition.

Many of the articles (18) used or referred to the definition given in the 2009 book *Cyber Situational Awareness – Issues and Research* edited by Jajodia et al. (Jajodia et al., 2009). Within this book, a chapter by Tadda & Salerno gives a slightly modified definition of SA: "*Situation awareness is the perception of the elements of the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future to enable decision superiority*" (Tadda and Salerno, 2010). This definition of CSA can be said to be a slightly modified ISA definition. The book and the chapter discuss some additional definitions of SA apart from Endsley's; however, they do not refer to Stanton's systemic definition of DSA in any way.

There are 7 papers that refer to Franke et al.'s review of research on CSA (Franke and Brynielsson, 2014) when introducing SA as a construct. Franke et al.'s review itself refers to Jajodia/Tadda's CSA as its definition. These 7 papers may be said to define SA somewhat vaguely, by only referring indirectly to a definition.

In combination ISA and CSA provide the definition of SA to 41 out of 55 papers. Considering that CSA is mostly based on ISA the dominating theoretical position of Endsley's three-stage model is apparent. When considering study types, it becomes apparent that the research on tool development is mainly influenced by CSA, but this type of study has the weakest theoretical foundation of SA with 6 out of 23 studies not giving any definition of SA. This is remarkable, considering that the filtering already excluded almost half of identified studies (76 out of 156) because they did not address SA directly. The reviews or proposals are mainly citing ISA as definition, the qualitative studies equally site ISA and CSA while all of the case studies and survey studies point to CSA as definition. Interestingly, it is among the few experi-

Table 3
Categorization of reviewed papers.

Description of papers			Theoretical foundation of SA		Conceptualization of SA		
Author	Year	Type of Study	Definition	Theory Referenced	Level of analysis	Term for SA	Measurement of SA
Dutt et al.	2013	Tool Development	Jajodia (CSA)	Tadda	Individual SA	CSA	Performance
Matey et al.	2022	Tool development	Jajodia (CSA)	Endsley	Individual SA	CSA	Performance/Proxy
Zhong et al.	2015	Tool development	No	No	Individual SA	CSA	Task Analysis
Giacobe et al.	2013	Tool development	Tyworth	Endsley	Individual SA	Cyber-SA	Multiple
Kokkonen & Puuska	2018	Tool development	Endsley (ISA)	Endsley	Group SA	SA	Self rating/Observer rating
Giacobe	2013	Tool development	Endsley (ISA)	Endsley	Group SA	CSA	Multiple
Huang et al.	2016	Tool development	Franke (CSA)	No	Group SA	CSA	Performance
Leszczyna et al.	2019	Tool development	Jajodia (CSA)	Endsley	Group SA	SA	Performance
Shurrab & Awan	2015	Tool development	Jajodia (CSA)	Endsley	Group SA	CSA	Performance
Wallis & Leszczyna	2022	Tool development	Jajodia (CSA)	No	Group SA	CSA	Performance
Mullins et al.	2020	Tool development	Jajodia (CSA)	Endsley	Group SA	CSA	Task Analysis/Performance/Proxy
Le Blanc et al.	2017	Tool development	No	No	Group SA	CSA	Task Analysis
Park et al.	2017	Tool development	Endsley (ISA)	Endsley	Systems SA	CSA	Performance/Proxy
Cinque et al.	2020	Tool development	Franke (CSA)	No	Systems SA	SA	Performance
Salvi et al.	2022	Tool development	Franke (CSA)	No	Systems SA	CSA	Performance/Proxy
Settanni et al.	2017	Tool development	Franke (CSA)	No	Systems SA	National Cyber SA	Performance/Proxy
Skopik	2019	Tool development	Franke (CSA)	No	Systems SA	CSA	Task Analysis
Dutt & Gonzalez	2012	Tool development	Jajodia (CSA)	Tadda	Systems SA	CSA	Performance/Proxy
Husák et al.	2022	Tool development	Jajodia (CSA)	Tadda	Systems SA	CSA	Performance/Proxy
Sunny et al.	2014	Tool development	Jajodia (CSA)	Barford	Systems SA	CSA	Performance/Proxy
Zhong et al.	2018	Tool development	Jajodia (CSA)	Endsley	Systems SA	CSA	Performance/self rating
Sarkar et al.	2022	Tool development	No	No	Systems SA	SA	Performance
Settanni et al.	2017	Tool development	No	No	Systems SA	CSA	Performance
Zhu et al.	2021	Tool development	No	Bass	Systems SA	SA	Performance
Shah et al.	2018	Tool development	No	No	Systems SA	SA	Proxy
Gutzwiller et al.	2020	Review	Endsley (ISA)	Endsley	Individual SA	CSA	Multiple
Brynielsson et al.	2016	Review/proposal	Endsley (ISA)	Endsley	Individual SA	CSA	Multiple
McNeese & Hall	2017	Review	Endsley (ISA)	Endsley	Group SA	CSA	Proxy/Self rating/Performance
Pahi et al.	2017	Review	Endsley (ISA)	Endsley	Group SA	CSA	Task Analysis
Debatty & Mees	2019	Review/proposal	Endsley (ISA)	Endsley	Group SA	Cyber Defense SA	Performance/Proxy
Champion et al.	2012	Review/proposal	Endsley (ISA)	Endsley	Group SA	CSA	Task analysis/Self rating/Performance
Andrade & Yoo	2019	Review	Endsley (ISA)	No	Systems SA	Cyber security SA	Performance
Ahmad et al.	2019	Review/proposal	Endsley (ISA)	Endsley/Smith	Systems SA	SA	Performance/Proxy
Cain & Schuster	2016	Review/proposal	Endsley (ISA)/Stanton (DSA)	Endsley/Stanton	Systems SA	Complementary SA	Task Analysis
Hall et al.	2015	Review/proposal	Jajodia (CSA)	Tadda	Systems SA	CSA	Performance/Proxy
Cain &Schuster	2014	Review	Endsley (ISA)/Jajodia (CSA)/Stanton (DSA)	Endsley/Tadda/Stanton	Systems SA	SA	Performance/Proxy
Nazir & Han	2022	Review	Endsley (ISA)/Jajodia (CSA)	Endsley/Tadda/Bass	Systems SA	CSA	Proxy
Gomez et al.	2019	Review/proposal	No	No	Systems SA	SA	Performance
Franke & Brynielsson	2014	Review	Jajodia (CSA)	Endsley	Multiple	CSA	Multiple
Ahmad et al.	2021	Case study	Franke (CSA)	No	Group SA	CSA	Task Analysis
Granåsen & Anderson	2016	Case study	Jajodia (CSA)	Endsley/Barford	Group SA	CSA	Performance/Self rating
Bhatt et al.	2014	Case study	Jajodia (CSA)	Endsley/Tadda	Systems SA	CSA	Performance
Kanstrén & Evesti	2016	Qualitative study	Endsley (ISA)	Endsley	Individual SA	Cyber security SA	Task Analysis
Gutzwiller et al.	2016	Qualitative study	Jajodia (CSA)	Endsley	Individual SA	Cyber Cognitive SA	Task Anlysis
Eldardiry & Caldwell	2015	Qualitative study	Endsley (ISA)	Endsley	Group SA	Network Security SA	Task analysis
Paterson	2014	Qualitative study	Jajodia (CSA)	Tadda	Group SA	SA	Task Analysis
Smith et al.	2021	Qualitative study	No	No	Group SA	SA	Task analysis/Self rating/Performance
Ahrend et al.	2016	Qualitative study	Endsley (ISA)	Endsley	Systems SA	CSA	Task analysis
Chandra et al.	2022	Survey study	Franke (CSA)	Endsley	Group SA	CSA	Performance/Proxy
Varga et al.	2018	Survey study	Jajodia (CSA)	Endsley	Group SA	CSA	Task Analysis
Thangavelu et al.	2021	Effect study	Endsley (ISA)	Endsley	Individual SA	CSA	Performance/Proxy
Happa et al.	2021	Experimental study	Jajodia (CSA)	Jajodia	Individual SA	SA	Performance
Jaeger & Eckhardt	2021	Experimental study	Own	Endsley/Stanton/ Salmon/Adams	Individual SA	Situational information security awareness	Proxy/Self rating/Performance
Kostelic	2020	Experimental study	Smith & Hancock	Endsley/Salmon/ Stanton	Individual SA	SA	Performance/Proxy
Rajivan & Cooke	2017	Experimental study	Endsley (ISA)	Endsley	Group SA	SA	Task Analysis/Performance/Proxy

mental studies that we find the most diversity among definitions of SA.

Three of the review papers refer to multiple definitions of SA (Cain and Schuster, 2014, 2016; Nazir and Han, 2022). The fact that these reviews point to multiple definitions of SA shows that there is some ongoing theoretical debate surrounding the issue of how to understand SA within the context of SOCs. Although most research adheres to the ISA model or its decedent CSA, the fact that reviews point out that there are alternative perspectives available keeps the research field aware of this issue.

There are 3 articles that include the definition of DSA specifically, but none of the articles claims to prefer this definition (Cain and Schuster, 2014, 2016; Kostelic, 2020). 2 additional papers refer indirectly to the DSA definition. One of these papers presents an alternative definition of CSA given by Tyworth et al. (Tyworth et al., 2012). Tyworth's definition refers to both Endsley's definition of ISA and Stanton et al.'s definition of DSA. On the other hand, it does not refer to Jajodia/Tadda's definition of CSA. The other paper that indirectly use the DSA definition proposes an own, specialized definition of *Situational information security awareness*: "*we define situational information security awareness as a user's knowledge of particular security threats transported by security-related information cues captured in a situational process in the immediate system environment*" (Jaeger and Eckhardt, 2021). This definition connects the result of the situational awareness process to the mental state of a user, but it includes the system into the process of gaining situational awareness. Thus, we can see the influence of the system level perspective which the DSA model offers.

One article refers to the definition given by Smith and Hancock in 1995: "*We define situation awareness (SA) as adaptive, externally directed consciousness*" (Smith and Hancock, 1995). This definition can be described as cognitively oriented, but it is more general than Endsley's ISA model.

8 of the reviewed papers did not give any clear definitions or references to a definition of SA. They only briefly address how SA as a construct is understood and can be said to lack a clear definition of SA. Of these, 3 papers use the term CSA, and it might be assumed that they follow Jajodia/Taddas definition.

If we look beyond the definitions used there are a total of 32 out of 55 articles that refer to Endsley's theoretical work in some way (Endsley, 1988a, 1995; Endsley and Garland, 2000). This points out that the prominent place that Endsley and the ISA model holds within the field of SA also is the case within research on the SOC setting. In total there are 18 articles that refer to the 2009 book edited by Jajodia et al. (Jajodia et al., 2009). This book contains both the definition CSA presented earlier, but also a specification of what kinds of systems, tasks and settings within cyber security are relevant to SA processes. 10 of the articles that use the CSA definition also reference Endsley as part of their theoretical foundation. There are only 3 articles that refer directly to Stanton et al.'s theoretical foundation of DSA (Stanton et al., 2006). There is one additional article that indirectly refers to DSA through referring to Tyworth's definition of CSA (Tyworth et al., 2012). It is somewhat interesting that there are so few papers that lean towards a more system level theoretical foundation, given the dominance of research aimed at developing systems providing some sort of SA advancing feature. There are 2 papers that refer to Smith & Hancock's theoretical work on SA (Smith and Hancock, 1995). In addition, there is one article referring to Adams et al.'s theoretical work on SA (Adams et al., 1995), which focuses on the perpetual cycling of the mental schemas that are the product of SA, and the process of changing these as a consequence of using them to interpret information. Two articles refer to Bass et al.'s work on improving Cyber SA (Bass, 1999, 2000). This foundation is somewhat different from others because it is not based within HFR. This theoretical foundation comes from data fusion instead. One of the articles refers to Bass as its only theoretical foundation for SA (Zhu et al., 2021), but the other refers to Bass' theory alongside those of Endsley and Jajodia (Nazir and Han, 2022).

A total of 15 articles do not reference directly to any theoretical foundation for their understanding of SA. 5 of these articles refer to the literature review by Franke et al. (Franke and Brynielsson, 2014) that again refers to Jajodia (Jajodia et al., 2009). But they do not directly refer to any other theoretical foundations. There are 8 articles that lack both a definition of SA and a theoretical foundation for their understanding. As a peculiar case there is one article that gives a definition for SA completely parallel to Endsley's ISA or Tadda & Salerno's CSA definition without referring to either of them directly (Andrade and Yoo, 2019).

4.5. Conceptualizations of SA

The second research question of this review is what levels of analysis SA is conceptualized on in the literature. The levels of analysis were divided into three main categories: (1) Individual SA i.e., conceptualizing SA as the mental product of an individual human operator's SA processes; (2) Group SA i.e., conceptualizing SA as the total awareness product of all the individual SAs combined and communicated between them; and (3) Systems SA i.e., the total awareness product of a whole sociotechnical system SA process.

Of the 55 articles there were 12 that used an individual operationalization of SA. This kind of operationalization is in line with the initial individually focused ISA model of Endsley (Endsley, 1995). It is an interresting observation that the individual conceptualization is used among many different types of studies. But it is most prominent in the few identified experimental studies. This might point towards the earlier mentioned point that SA at an individual level is the most developed level of analysis when it comes to validated measurements of SA.

Many of the articles (20) operationalized SA on a group level. This is in line with later developments of the ISA model, like CSA (Jajodia et al., 2009) or Team SA (Salmon et al., 2008). The Group level conceptualization is present within all the study types. Within the papers the Group level conceptualization is often emphasized within research dealing with how to communicate SA-relevant information between humans, from systems to groups, or between groups at different levels of an organization or between organizations.

Even more of the articles (22) operationalize SA at a system level. This is aligned with the development of DSA (Stanton et al., 2006). The fact that so much of the literature conceptualizes SA on a systems level is a notable observation. The systems level conceptualization is particularly prominent among papers using the CSA definition of SA. CSA does not in itself provide a systems theory of SA, but it highlights the importance of using systems to support the human SA processes.

One review article refers to multiple operationalizations of SA (Franke and Brynielsson, 2014). This gives a good overview of the different research topics connected to SA within cyber security.

In addition to analyzing the levels of analysis of SA, the actual terms used for referring to SA were registered. Although the terms do not provide ample opportunity to deep consideration, they provide a good overview for other researchers trying to orient themselves within a mixture of SA definitions, theories, and labels.

Within the reviewed literature there were several different terms used when referring to SA. *Situation Awareness* or *Situational Awareness* was used as the only term in 14 of the 55 papers. The term CSA was the most used term within the reviewed literature; 33 of 55 papers used this term. 2 papers referred to *Cyber Security SA*. Then there were several terms used only by one article each: Cyber Defense SA, Cyber Cognitive SA, National Cyber SA, Network

Security SA, Situational information security awareness, and Complementary SA. These terms were proposed as part of the aim of the respective article.

4.6. Measurements of SA

The third research question was what measurements of SA are used or referred to within research on SA in the setting of SOCs. In order to answer this, all the reviewed articles were categorized on what measurement techniques were used or referred to in the articles.

In total there are 5 out of 55 articles that used or referred to multiple measurements SA. These included most or all of the seven measurements categories shown in Table 3.

There were 13 articles that only referred to *Performance* as their measure of SA. This indicates a vague connection to the operationalizations, and measurements of SA described in the defining literature. Performance is an indirect measurement of SA and does not ensure a good assessment by itself (Endsley and Garland, 2000). 27 articles included Performance as one of several measurements of SA; these include the 5 articles that used many or all the measurements.

There were 2 papers that only used *Proxy measurements* for SA. This is also a poor assessment of SA on its own, because of its indirect nature (Endsley and Garland, 2000). There were an additional 23 studies that used or referred to proxy measurements as one of several measurements.

There were 12 articles that only referred to using *Task Analysis* as a measurement of SA. Task Analysis might be a good first step for establishing a precise measurement of SA, and several of the studies claimed doing just that. There were totally 9 additional studies that used or referred to Task Analysis as one of several measurements.

A total of 12 studies used or referred to *self-reporting* as one of several measurements of SA. Self-reporting is a practical tool but should not be used alone because of the clear danger for respondent bias (Endsley and Garland, 2000). There were only 6 studies that used *probing techniques* or *observer rating*, and all used them alongside other measurements.

To summarize the results, Fig. 3 visualizes how all the reviewed papers understand SA. The papers are grouped according to type, with subgroups representing different levels of conceptualizing SA. The theoretical foundations are represented as arrows connected to different theories and definitions of SA. The connections between theories and definitions also show how these are connected. Fig. 3 shows how ISA and CSA dominate the understanding of SA within the papers, but it also shows how the DSA model is present within some of the research. Fig. 3 provides a good overview of the overall understanding of SA in research within SOC environments.

5. Discussion

The results of this review show some clear patterns regarding the current research on SA in SOCs. Firstly, there are few studies that actually measure SA. Apart from the 5 articles proposing operationalizations or methods of assessing or measuring SA there are only 3 survey studies, 6 qualitative studies and 5 effect or experimental studies. This suggests that the empirical basis for drawing conclusions on the nature and impact of SA within SOC environments is very limited. This aligns with the conclusions of earlier reviews (Franke and Brynielsson, 2014; Gutzwiller et al., 2020).

Secondly, it is clear that the definitions used and the theoretical background for SA within SOCs are quite uniform. With some notable exceptions, the definitions used are heavily ISA-dominated, referring either to the definition of Endsley (ISA) or that of Tadda & Salerno (CSA) presented as part of Jajodia's book on Cyber Situational Awareness (Jajodia et al., 2009). The notable exceptions point to DSA (Stanton et al., 2006), Smith & Hancock (Smith and Hancock, 1995), Adams et al. (Adams et al., 1995) or Bass (Bass, 1999). The case that the theoretical foundations is somewhat lacking within the current research literature can also be made. With a total of 16 out of 55 articles lacking either a clear definition of SA or clear theoretical foundation, some of the research might be using SA more as a buzzword rather than a well-defined construct. Especially within the research done on tools developed for increased quality of SA there are a few examples of emphasizing the importance of SA without giving any actual clarification on how they understand SA: *"Correlating large amounts of data, collected from a multitude of relevant sources, is fundamental for Security Operation Centers (SOCs) to establish cyber situational awareness, and allow to promptly adopt suitable countermeasures in case of attacks"* (Skopik, 2019). When such formulations are not followed up by more specific explanation of how SA is understood or what kind of mechanisms would improve SA, it appears mostly as signaling homage to a popular idea.

The results from the review point towards a development of the theoretical foundation through the specialization of the term CSA, but the theoretical foundation is not as conscious in much of the research. Although there is a sound theoretical foundation within the defining literature of CSA, it seems like the research on development of tools refers to CSA as a generalized term for the human cognitive process within SOC environments. SA as defined by Endsley (Endsley, 1995) is influenced by a wide range of factors like workload, communication, and the quality of information visualization. Consequently, tools that improve these factors may improve SA. Still, it might be a bold claim that any visualization or data fusion tool that represents some data in SOCs more effectively will ultimately increase the quality of SA for the human operators. This would indicate what we already know as a fact, namely that the existing tools are impeding the potential quality of SA. Based on the reviewed literature, there is no clear evidence that this is the case. On the other hand, there seem to be clear indications throughout the literature that there is a general lack of knowledge about how the performance of human operators in SOCs is affected by SA.

The few studies that have investigated this issue point towards such a connection (Champion et al., 2012; Happa et al., 2021; Jaeger and Eckhardt, 2021; Kostelic, 2020; Thangavelu et al., 2021). One study even has investigated how different factors affect SA in SOC-related teams (Rajivan and Cooke, 2017). Although these are notable contributions, there is still a large evidence gap before statements can be made about what tools are needed to gain better SA, and ultimately better performance, from individuals and teams of human operators within SOCs.

There is a fairly equal distribution of research on the different levels of conceptualizing SA within the literature. Some of the research done on developing tools that operationalize SA on a system or group level do not present a clear definition or theoretical foundation to their understanding of SA; this should be investigated further. When considering theoretical fit between the conceptualization and definitions used for SA there seems to be a mismatch. CSA is the most common definition within the Tools development literature. To a large extent, Jajodia et al.'s edited volume specifies the ISA model within the cyber security context and calls it CSA. The book presents how different parts of the cyber domain can be understood by the human operator in effective ways to gain good SA, and how systems might aid the operators in this process. In this way it is pointing towards a more system level understanding of SA. Still, it stays within the ISA paradigm and keeps the systems,

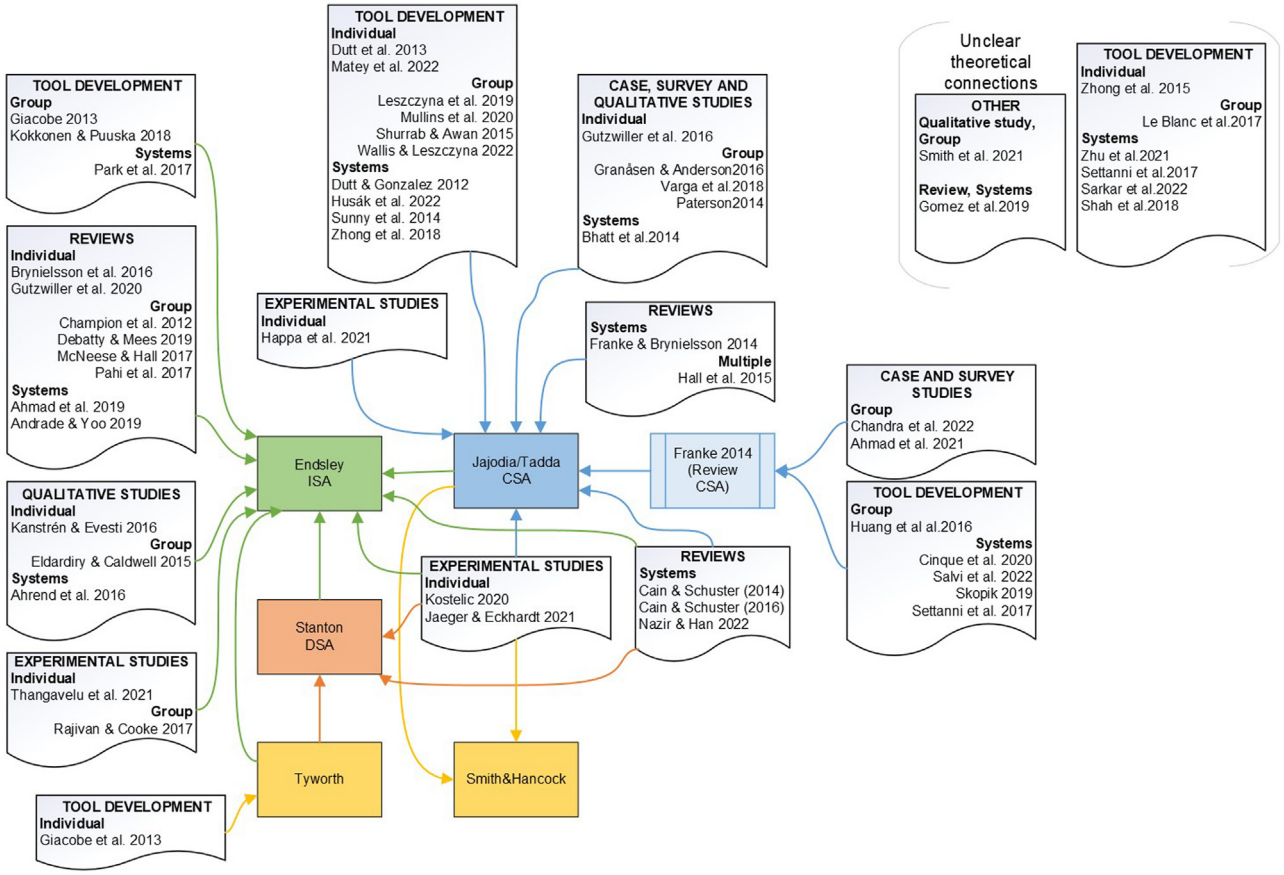

Fig. 3. Visualization of how the papers understand SA

so to speak, out of the SA. According to the CSA model, the awareness resides in the human operator and the systems are only tools assisting the human in this process. Somehow, it still seems that CSA is on the cusp of adopting a system view of SA when the volume's introduction states: "*The goal of this book is to explore ways to elevate the Cyber Situational Awareness capability of an enterprise to the next level by measures such as developing holistic Cyber Situational Awareness approaches and evolving existing system designs into new systems that can achieve self-awareness.*" The fact that DSA or other system level theories are not mentioned in the defining work on CSA (Jajodia et al., 2009) seems to be at the root of the theoretical and conceptual mismatch identified in this literature review. Many of the tools proposed in the literature aim to overtake parts of the SA process, as opposed to only assist human operators. Although this is a clearly expressed goal in the CSA literature, the theoretical foundation is mainly based on Endsley's work which clearly rejects such an understanding of SA. In order to bridge this gap, one could argue for an updating of the CSA definition in a way that includes the systems perspective in the definition. Another solution might be to establish new definitions of SA in SOC environments. This last approach seems less promising, given that quite a few of the papers identified in this review that are aimed at proposing SA definitions, show no clear signs of adoption from other research.

The heavy use of Performance as an indirect measurement of SA is also an interesting feature in the reviewed literature. Out of the 40 articles using or referring to this measurement there are 6 operationalizing SA on individual level, 12 at group level and 22 at system level. This indicates that the measurement of performance within systems is the most common operationalization of SA when conceptualized on the system level. This seems logical, given that the other well-known measurements focus on the mental states of the human operators. This again points to how the ISA paradigm is dominating SA research within this field. Although DSA operationalizations and measurements are not well developed, it might have informed the current research by providing ideas about how one could operationalize SA residing in systems. Overall performance of the system as the only measure leaves SA as a black box phenomenon, lowering SA's potential explanatory power.

6. Limitations

The limitations in this literature review are related to three issues, namely Search results; Screening and filtering; and Analysis.

The search results are limited by both the chosen databases and the search strings. Although the preliminary search included more databases, this did not yield any additional unique results. Still, this does not guarantee that no such results would have been found given searches within other databases. The search string also may have restricted the search by not including relevant alternative terms. After reviewing the results, it seems evident that there are a wide variety of different terms used both for SA and for SOCs. Some relevant results may have been missed by excluding variations of these terms. However, the fact that 163 results were filtered down to 55 points towards a broad enough search strategy.

The filtering of the literature also poses possible limitations. The choice to exclude results from settings other than SOCs might have

excluded relevant research. There were some papers that could inform the review on the measurement of SA (Ask et al., 2021a; Sharma et al., 2019), some papers regarding relevant factors like communication within SOCs (Ask et al., 2021b) or security awareness (Gkioulos et al., 2017). The fact that even after filtering 163 results down to 55 there still were some of the reviewed articles that lacked clear theoretical foundation for SA indicates that the filtering was not too strict.

7. Conclusion

The conducted literature review presents an outline of the current scientific research of SA within SOCs. Endsley's ISA model (Endsley, 1995) is dominant within the research, although it has been slightly modified and re-termed into CSA by a growing number of research papers (Jajodia et al., 2009). There are some notable exceptions which also refer to the proposed DSA model (Stanton et al., 2006), but the dominant definition of CSA does not include this model in its theoretical foundation. There is a balance between the three levels of conceptualization with 13 on individual level, 20 on group level and 22 on system level. The number of studies conceptualizing SA on system level leaves a gap regarding the lack of reference to system level definitions or theoretical foundations within the literature. The DSA model represents one possible candidate for such an approach to SA (Stanton et al., 2006). Yet, DSA or other potential system-level definitions are not widely present in the reviewed literature. This should be investigated in further research.

The majority of the research done on SA in SOCs is aimed at developing tools that in one way or another try to automate tasks to ease SA processes for the human operator. This suggests a potential theoretical alignment with the systems approach that DSA presents.

The implication of this suggestion might also contribute to the further development of SA within cyber security in general and within SOC environments specifically. Perhaps Gutzwiller's first proposition (Gutzwiller et al., 2020) of understanding what CSA is from the human operators' perspective should be expanded with the system perspective of DSA. This would imply the following suggestion: CSA literature should understand what CSA is from both the human operators' perspective and from a system perspective.

This development might be questioned in further research. The fact that the majority of research done on SA within SOCs is developing tools that in one way or another try to automate tasks to ease SA processes for the human operator, suggests a potential alignment with the systems approach DSA presents. Although the focus on tool development might be criticized for only using SA as a buzzword, DSA might introduce a theoretical bridge for research focusing on development of system tools.

Declaration of Competing Interest

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.

CRediT authorship contribution statement

Håvard Jakobsen Ofte: Conceptualization, Methodology, Investigation, Data curation, Writing – original draft, Visualization. **Sokratis Katsikas:** Conceptualization, Methodology, Validation, Writing – review & editing, Supervision.

Data availability

Data will be made available on request.

References

Adams, M.J., Tenney, Y.J., Pew, R.W., 1995. Situation awareness and the cognitive management of complex systems. Hum. Factors 37 (1), 85–104.

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. Comput. Secur. 101.

Ahmad, A., Webb, J., Desouza, K.C., Boorman, J., 2019. Strategically-motivated advanced persistent threat: definition, process, tactics and a disinformation model of counterattack. Comput. Secur. 86, 402–418.

Ahrend, J.M., Jirotka, M., Jones, K., 2016. On the collaborative practices of cyber threat intelligence analysts to develop and utilize tacit Threat and Defence Knowledge. 2016 International Conference on Cyber Situational Awareness, Data Analytics and Assessment. CyberSA 2016.

Andrade, R.O., Yoo, S.G., 2019. Cognitive security: a comprehensive study of cognitive science in cybersecurity. J. Inf. Secur. Appl. 48, 102352.

Ask T.F., Knox B.J., Lugo R., Hoffmann L., Sütterlin S. A gamification approach to improving interpersonal situational awareness in cyber defense. 2021a.

Ask, T.F., Lugo, R.G., Knox, B.J., Sütterlin, S., 2021b. Human-Human Communication in. In: Cyber Threat Situations: A Systematic Review. International Conference on Human-Computer Interaction. Springer, pp. 21–43 b.

Bass, T., 1999. Multisensor data fusion for next generation distributed intrusion detection systems. In: Proceedings of the IRIS National Symposium on Sensor and Data Fusion: Citeseer, pp. 24–27.

Bass, T., 2000. Intrusion detection systems and multisensor data fusion. Commun. ACM 43 (4), 99–105.

Bhatt, P., Yano, E.T., Amorim, J., Gustavsson, P., 2014. A cyber security situational awareness framework to track and project multistage cyber attacks. In: Proceedings of the 9th International Conference on Cyber Warfare and Security (ICCWS-2014), pp. 356–360.

Brynielsson, J., Franke, U., Varga, S., 2016. Cyber Situational Awareness Testing. Advanced Sciences and Technologies for Security Applications, pp. 209–233.

Cain, A.A., Schuster, D., 2014. Measurement of situation awareness among diverse agents in cyber security. In: 2014 IEEE International Inter-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support. CogSIMA, pp. 124–129 2014.

Cain, A.A., Schuster, D., 2016. Applying measurement to complementary situation awareness. In: 2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support. CogSIMA, pp. 121–125 2016.

Champion, M.A., Rajivan, P., Cooke, N.J., Jariwala, S., 2012. Team-based cyber defense analysis. In: 2012 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support. CogSIMA, pp. 218–221 2012.

Chandra, N.A., Ratna, A.A.P., Ramli, K., 2022. Development and simulation of cyberdisaster situation awareness models. Sustainability (Switzerland) 14 (3).

Chen, T.M., Abu-Nimeh, S., 2011. Lessons from stuxnet. Computer (Long Beach Calif) 44 (4), 91–93.

Cinque, M., Della Corte, R., Pecchia, A., 2020. Contextual filtering and prioritization of computer application logs for security situational awareness. Fut. Gener. Comput. Syst. 111, 668–680.

Cooke, I.A., Scott, A., Sliwinska, K., Wong, N., Shah, S.V., Liu, J., et al., 2019. Toward robust models of cyber situation awareness. Adv. Intell. Syst. Comput. 127–137.

Debatty, T., Mees, W., 2019. Building a cyber range for training CyberDefense situation awareness. 2019 International Conference on Military Communications and Information Systems. ICMCIS 2019.

Durso, F.T., Hackworth, C.A., Truitt, T.R., Crutchfield, J., Nikolic, D., Manning, C.A., 1998. Situation awareness as a predictor of performance for en route air traffic controllers. Air Traffic Control Q. 6 (1), 1–20.

Dutt, V., Ahn, Y.S., Gonzalez, C., 2013. Cyber situation awareness: modeling detection of cyber attacks with instance-based learning theory. Hum. Factors 55 (3), 605–618.

Dutt, V., Gonzalez, C., 2012. Cyber situation awareness through instance-based learning: modeling the security analyst in a cyber-attack scenario. Situational Awareness in Computer Network Defense: Principles, Methods and Applications 125–140.

Eldardiry, O.M., Caldwell, B.S., 2015. Improving information and task coordination in cyber security operation centers. In: IIE Annual Conference and Expo, pp. 1224–1233 2015.

Endsley, M.R., 1988a. Design and evaluation for situation awareness enhancement. In: Proceedings of the Human Factors Society annual meeting, Los Angeles, CA. Sage Publications Sage CA, pp. 97–101 a.

Endsley, M.R., 1988b. Situation awareness global assessment technique (SAGAT). In: Proceedings of the IEEE 1988 national aerospace and electronics conference: IEEE, pp. 789–795 b.

Endsley, M.R., 1994. Addendum–Situation awareness: some reflections and comments. Situational awareness in complex systems 315–317.

Endsley, M.R., 1995. Toward a theory of situation awareness in dynamic systems. Hum. Factors 37 (1), 32–64.

Endsley, M.R., 2015. Situation awareness misconceptions and misunderstandings. J. Cogn. Eng. Decis. Mak. 9 (1), 4–32.

Endsley, M.R., Garland, D.J., 2000. Situation Awareness Analysis and Measurement. CRC Press.

Fink, A., 2019. Conducting Research Literature reviews: From the Internet to Paper. Sage publications.

Franke, U., Brynielsson, J., 2014. Cyber situational awareness – a systematic review of the literature. Comput. Secur. 46, 18–31.
Giacobe, N.A., 2013. A picture is worth a thousand alerts. In: Proceedings of the Human Factors and Ergonomics Society, pp. 172–176.
Gkioulos, V., Wangen, G., Katsikas, S.K., Kavallieratos, G., Kotzanikolaou, P., 2017. Security awareness of the digital natives. Information 8 (2), 42.
Gomez, S.R., Mancuso, V., Staheli, D., 2019. Considerations for human-machine teaming in cybersecurity. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), pp. 153–168.
Granåsen, M., Andersson, D., 2016. Measuring team effectiveness in cyber-defense exercises: a cross-disciplinary case study. Cogn. Technol. Work 18 (1), 121–143.
Gutzwiller, R., Dykstra, J., Payne, B., 2020. Gaps and opportunities in situational awareness for cybersecurity. Digit. Threats 1 (3).
Gutzwiller, R.S., Hunt, S.M., Lange, D.S., 2016. A task analysis toward characterizing cyber-cognitive situation awareness (CCSA) in cyber defense analysts. In: 2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support, CogSIMA, pp. 14–20 2016.
Hall, M.J., David Hansen, D., Jones, K, 2015. Cross-domain situational awareness and collaborative working for cyber security. 2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment 2015.
Happa, J., Agrafiotis, I., Helmhout, M., Bashford-Rogers, T., Goldsmith, M., Creese, S., 2021. Assessing a decision support tool for SOC analysts. Digit. Threats 2 (3).
Huang, Z., Shen, C.C., Doshi, S., Thomas, N., Duong, H., 2016. Fuzzy sets based team decision-making for Cyber Situation Awareness. In: Proceedings - IEEE Military Communications Conference MILCOM, pp. 1077–1082.
Husák, M., Sadlek, L., Špaček, S., Laštovička, M., Javorník, M., Komárková, J., 2022. CRUSOE: a toolset for cyber situational awareness and decision support in incident handling. Comput. Secur. 115, 102609.
Jaeger, L., Eckhardt, A., 2021. Eyes wide open: the role of situational information security awareness for security-related behaviour. Open Inf. Syst. J. 31 (3), 429–472.
Jajodia, S., Liu, P., Swarup, V., Wang, C., 2009. Cyber Situational Awareness. Springer.
Kaber, D.B., Endsley, M.R., 1998. Team situation awareness for process control safety and performance. Process Saf. Prog. 17 (1), 43–48.
Kanstrén, T., Evesti, A., 2016. A study on the state of practice in security situational awareness. In: 2016 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), pp. 69–76.
Kokkonen, T., Puuska, S., 2018. Blue team communication and reporting for enhancing situational awareness from white team perspective in cyber security exercises. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), pp. 277–288.
Kostelic, K., 2020. Guessing the game: an individual's awareness and assessment of a game's existence. Games 11 (2), 17 (20734336).
Le Blanc, K., Ashok, A., Franklin, L., Scholtz, J., Andersen, E., Cassiadoro, M, 2017. Characterizing cyber tools for monitoring power grid systems: what information is available and who needs it? In: 2017 IEEE International Conference on Systems, Man, and Cybernetics. SMC, pp. 3451–3456 2017.
Lee, J., Wickens, C., Liu, Y., Boyle, L., 2017. Designing For People. ShangHai, p. 173.
Leszczyna, R., Wallis, T., Wróbel, M.R., 2019. Developing novel solutions to realise the European energy – information sharing & analysis centre. Decis. Support Syst. 122, 113067.
Matey, A.H., Danquah, P., Koi-Akrofi, G.Y., 2022. Predicting cyber-attack using cyber situational awareness: the case of independent power producers (IPPs). Int. J. Adv. Comput. Sci. Appl. 13 (1), 700–709.
Matthews, M.D., Beal, S.A., 2002. Assessing Situation Awareness in Field Training Exercises. Military Academy West Point NY Office of Military Psychology and Leadership.
McNeese, M.D., Hall, D.L., 2017. The cognitive sciences of cyber-security: a framework for advancing socio-cyber systems. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), pp. 173–202.
Moher, D., Altman, D.G., Liberati, A., Tetzlaff, J., 2011. PRISMA statement. Epidemiology 22 (1), 128.
Mullins, R., Nargi, B., Fouse, A., 2020. Understanding and enabling tactical situational awareness in a security operations center. In: Advances in Intelligent Systems and Computing, pp. 75–82.
Nazir, H.M.J., Han, W., 2022. Proliferation of cyber situational awareness: today's truly pervasive drive of cybersecurity. In: Security and Communication Networks, p. 2022.
Oueslati, N.E., Mrabet, H., Jemai, A., Alhomoud, A., 2019. Comparative study of the common cyber-physical attacks in industry 4.0. In: 2019 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC). IEEE, pp. 1–7.
Page, M.J., McKenzie, J.E., Bossuyt, P.M., Boutron, I., Hoffmann, T.C., Mulrow, C.D., et al., 2021. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. Syst. Rev. 10 (1), 1–11.
Pahi, T., Leitner, M., Skopik, F., 2017. Analysis and assessment of situational awareness models for national cyber security centers. In: ICISSP 2017 - Proceedings of the 3rd International Conference on Information Systems Security and Privacy, pp. 334–345.
Park, H.K., Kim, M.S., Park, M., Lee, K., 2017. Cyber situational awareness enhancement with regular expressions and an evaluation methodology. In: MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM), pp. 406–411.
Paterson, D.M., 2014. Work Domain Analysis for network management revisited: infrastructure, teams and situation awareness. In: 2014 IEEE International Inter-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support. CogSIMA, pp. 103–109 2014.
Rajivan, P., Cooke, N., 2017. Impact of team collaboration on cybersecurity situational awareness. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), pp. 203–226.
Salmon, P.M., Stanton, N.A., Walker, G.H., Baber, C., Jenkins, D.P., McMaster, R., et al., 2008. What really is going on? Review of situation awareness models for individuals and teams. Theor. Issues Ergon. Sci. 9 (4), 297–323.
Salmon, P.M., Stanton, N.A., Walker, G.H., Jenkins, D., Ladva, D., Rafferty, L., et al., 2009. Measuring Situation Awareness in complex systems: comparison of measures study. Int. J. Ind. Ergon. 39 (3), 490–500.
Salmon, P.M., Stanton, N.A., Walker, G.H., Jenkins, D.P., 2017. Distributed Situation awareness: Theory, Measurement and Application to Teamwork. CRC Press.
Salvi, A., Spagnoletti, P., Noori, N.S., 2022. Cyber-resilience of critical cyber infrastructures: integrating digital twins in the electric power ecosystem. Comput. Secur. 112, 102507.
Sarkar, S., Teo, Y.M., Chang, E.-C., 2022. A cybersecurity assessment framework for virtual operational technology in power system automation. Simul. Modell. Pract. Theory 117, 102453.
Schatz, D., Bashroush, R., Wall, J., 2017. Towards a more representative definition of cyber security. J. Digit. Forensics, Secur. Law 12 (2), 8.
Settanni, G., Shovgenya, Y., Skopik, F., Graf, R., Wurzenberger, M., Fiedler, R., 2017a. Acquiring cyber threat intelligence through security information correlation. In: 2017 3rd IEEE International Conference on Cybernetics, CYBCONF 2017 - Proceedings a.
Settanni, G., Skopik, F., Shovgenya, Y., Fiedler, R., Carolan, M., Conroy, D., et al., 2017b. A collaborative cyber incident management system for European interconnected critical infrastructures. J. Inf. Secur. Appl. 34, 166–182 b.
Shah, A., Ganesan, R., Jajodia, S., Cam, H., 2018. A methodology to measure and monitor level of operational effectiveness of a CSOC. Int. J. Inf. Secur. 17 (2), 121–134.
Sharma, A., Nazir, S., Ernstsen, J., 2019. Situation awareness information requirements for maritime navigation: a goal directed task analysis. Stem Cells Int. 120, 745–752.
Shurrab, O., Awan, I., 2015. Performance evaluation for process refinement stage of SWA system. In: Proceedings - 2015 International Conference on Future Internet of Things and Cloud, FiCloud 2015 and 2015 International Conference on Open and Big Data. OBD, pp. 240–247 2015.
Silva, R., Neiva, F., 2016. Systematic literature review. Computer Science - A Practical Guide.
Skopik, F., 2019. The limitations of national cyber security sensor networks debunked: why the human factor matters. In: Proceedings Of The 14th International Conference On Cyber Warfare And Security (ICCWS 2019), pp. 405–412.
Smith, K., Hancock, P.A., 1995. Situation awareness is adaptive, externally directed consciousness. Hum. Factors 37 (1), 137–148.
Smith, R., Janicke, H., He, Y., Ferra, F., Albakri, A., 2021. The agile incident response for industrial control systems (AIR4ICS) framework. Comput. Secur. 109, 102398.
Stanton, N.A., Stewart, R., Harris, D., Houghton, R.J., Baber, C., McMaster, R., et al., 2006. Distributed situation awareness in dynamic systems: theoretical development and application of an ergonomics methodology. Ergonomics 49 (12–13), 1288–1311.
Sunny, S., Pavithran, V., Achuthan, K., 2014. Synthesizing perception based on analysis of cyber attack environments. In: 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 2027–2030.
Tadda, G.P., Salerno, J.S., 2010. Overview of Cyber Situation Awareness. Cyber situational awareness: Springer, pp. 15–35.
Taylor, R.M., 2017. Situational awareness rating technique (SART): the development of a tool for aircrew systems design. Situational awareness: Routledge 111–128.
Thangavelu, M., Krishnaswamy, V., Sharma, M., 2021. Impact of comprehensive information security awareness and cognitive characteristics on security incident management – an empirical study. Comput. Secur. 109.
Tyworth, M., Giacobe, N.A., Mancuso, V., Dancy, C., 2012. The distributed nature of cyber situation awareness. In: 2012 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support. IEEE, pp. 174–178.
Varga, S., Brynielsson, J., Franke, U., 2018. Information requirements for national level cyber situational awareness. In: Proceedings of the 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining. ASONAM, pp. 774–781 2018.
Vielberth, M., Böhm, F., Fichtinger, I., Pernul, G., 2020. Security operations center: a systematic study and open challenges. IEEE Access 8, 227756–227779.
von Solms, R., van Niekerk, J., 2013. From information security to cyber security. Comput. Secur. 38, 97–102.
Wallis, T., Leszczyna, R., 2022. EE-ISAC—practical cybersecurity solution for the energy sector. Energies 15 (6), 2170 19961073.
Willett, M., 2021. Lessons of the SolarWinds hack. Survival (Lond) 63 (2), 7–26.
Zhong, C., Lin, T., Liu, P., Yen, J., Chen, K, 2018. A cyber security data triage operation retrieval system. Comput. Secur. 76, 12–31.
Zhong, C., Yen, J., Liu, P., Erbacher, R., Etoty, R., Garneau, C., 2015. ARSCA: a computer tool for tracing the cognitive processes of cyber-attack analysis. In: 2015 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision. CogSIMA, pp. 165–171 2015.
Zhu, L., Wang, W., Luo, R., Cai, Z., Peng, S., Zhang, Z., 2021. Situational awareness of E-learning system based on cyber-attack and vulnerability. In: Lecture Notes

in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), pp. 154–159.
Zimmerman, C., 2014. Cybersecurity Operations Center. The MITRE Corporation.

Håvard J. Ofte is an Industrial Ph.D.-student of Information Security and Communication Technology at the Norwegian University of Science and Technology (NTNU). He is also a Research Manager at NC-Spectrum AS which provide information and network security within Norwegian critical infrastructure. He has experience from R&D within Norwegian health sector and business consultancy. Education: M.ph. in Work and Organizational Psychology, University of Oslo, Norway; B.A. in Work and Organizational Psychology, University of Oslo, Norway.

Sokratis K. Katsikas is the Director of the Norwegian Center for Cybersecurity in Critical Sectors and Professor with the Dept. of Information Security and Communication Technology of the Norwegian University of Science and Technology (NTNU). His research activity has resulted in more than 300 published books; book chapters; journal papers; and papers in conference proceedings. He has led or participated in more than 60 funded national and international R&D projects. Education: Ph.d. in Computer Engineering & Informatics, University of Patras, Greece; MSc in Electrical & Computer Engineering, University of Massachusetts, USA; Dipl. Eng. in Electrical Engineering, University of Patras, Greece.