Human-Human Communication in Cyber Threat Situations: A Systematic Review

Torvald F. Ask[1,2][0000-0002-1907-0004], Ricardo G. Lugo[1][0000-0003-2012-5700], Benjamin J. Knox[1][0000-0002-4540-9534], and Stefan Sütterlin[2,3,4][0000-0002-4337-1296]

[1] Norwegian University of Science and Technology, Gjøvik, Norway
[2] Østfold University College, Halden, Norway
[3] Tallinn University of Technology, Tallinn, Estonia
[4] Albstadt-Sigmaringen University, Sigmaringen, Germany
torvaldfask@gmail.com

Abstract. In cyber threat situations, decision-making within organizations and between the affected organization and external entities are high-stake situations. They require human communication entailing technical complexity, time pressure, interdisciplinary, and often insufficient information basis. Communication in cyber threat situations within socio-technical systems can thus be challenging and has a variety of implications for decision-making. The cyber-physical system is a rapidly changing socio-technical system that is understudied in terms of how cyber events are communicated and acted upon to secure and maintain cyber resilience. The present study is the first to review human-to-human communication in cyber threat situations. Our aims are to (1) outline how human-human communication performance in cybersecurity settings have been studied; (2) to uncover areas where there is potential for developing common standards for information exchange in collaborative settings, and; (3) to provide guidance for future research efforts. The review was carried out according to the PRISMA guidelines and articles were searched for on Google Scholar, ScienceDirect, Taylor & Francis, and IEEE. Primary research articles and reviews focusing on human-human communication in cyber threat situations published in peer reviewed journals or as conference papers were included. A total of 17 studies were included in the final review. Most of the studies were correlational and exploratory in nature. Very few studies characterize communication in useful goal-related terms.

Keywords: Cyber Threat Communication, Human Factor, Systematic Review.

1 Introduction

A Cyber Threat Situation (CTS) is the potential occurrence of a cyber-attack aiming to damage, disrupt, or steal a cyber asset. A cyber asset can be understood as a completely or partly digitized protected organizational resource (Whitman & Mattord, 2012). With the increased digitization of society and global network coverage, the cyber threat landscape is evolving and so is the need for research on the prevention and effective

handling of cybersecurity threats. Organizations often assign their cybersecurity operations to Security Operation Centers (SOCs). SOCs are teams and organizational units that cover multiple security activities such as preventing, detecting, assessing, and responding to cyber threats and incidents (Muniz et al., 2015). Within the SOC organizational structure, technical tasks such as asset monitoring, detection, analysis, forensics, network security, intelligence, and communicating suggestions for cyber threat- and cyber incident response are assigned to technical staff while subsequent decision-making tasks such as how to act on threat and incident reports are assigned to other individuals (decision-makers; Muniz et al., 2015). Consequently, there is a potential knowledge gap between technical personnel and decision-makers.

Cyber professionals, known as cyber operators in military sectors and cyber analysts in civil sectors (interchangeably referred to as COs), make up the technical personnel in SOCs and face a unique set of challenges spanning the cyber, physical, and social domain (Jøsok et al., 2016). This cyber-physical working environment of human-machine and human-human interaction creates a complex Socio-Technical System (STS) that is subject to high rates of innovation, increasing network interconnectedness, and rapid flow of information (Zanenga, 2014). Decision-making in STSs has its own set of challenges. In cyberspace, the impact of decisions and actions on own and third party infrastructure is influenced by connectivity between different decision-making agents (Tikk-Ringas et al., 2014). In a cybersecurity setting, there is a persisting element of uncertainty regarding the presence, persistence, and consequences of adversarial behavior. This suggests that decision-makers need to prioritize multiple assets based on known and unknown risk and cognitively transition between cyber and physical contexts when estimating the impact of their decisions (Jøsok et al., 2016).

Due to the multiple impact-dimensions of cyber defense decisions, communication between human agents is at the core of good cyber defense decision-making (Knox et al., 2018). Strategic-level decision-making and tactical-level technical developments need simultaneous integration but are usually distributed over different roles, both vertically and horizontally within an organization. Since CO activity and decision-making is distributed among different roles within the SOC (Muniz et al., 2015), there are multiple dyadic relationships that simultaneously influence the information requirements of cyber threat communication. The information communicated from a CO during a CTS must be modular enough to be interpreted by all dyads. This can be challenging when stakeholders belong to non-technical sectors or lack technical skills. In a recent review, Agyepong et al. (2020) identified communication as one of the challenges facing SOCs. How cyber events are communicated and acted upon in the physical domain to secure and maintain cyber resilience is currently not well understood. In this paper, we systematically review the literature on human-human communication in CTSs.

1.1 An Accurate Recognized Cyber Picture is Critical for Effective Cyber Defense Decisions

Successful decision-making based on human interaction requires a shared situational awareness of the CTS. This includes a mutual understanding of what caused the

situation, the current state of assets, potential adversaries, how the situation is evolving, and which actions to take to mitigate detrimental outcomes. An organization's Cyber Situational Awareness (CSA) influences whether an organization maintains control in its cyberspace (Franke & Brynielsson, 2014). Seven requirements that need to be met to have full CSA for cyber defense have been suggested (Barford et al., 2009): (1) awareness of the current situation; (2) awareness of the impact of the attack; (3) awareness of how situations evolve; (4) awareness of adversarial behavior; (5) awareness of why and how the current situation is caused; (6) awareness of the quality and trustworthiness of the CSA information, and; (7) assessment of plausible outcomes. Having an accurate Recognized Cyber Picture (RCP; or Cyber Common Operational Picture) is crucial to achieve CSA. While CSA can be understood as being aware of the underlying state of a specific cyber environment at any given moment (Franke & Brynielsson, 2014), RCPs consist of actively selected and actionable information specifically pertaining to cyber threats (Cyber Threat Intelligence; CTI) and aim to update stakeholders CSA and support their decision-making. To achieve this goal, RCPs should contain the information suggested by Barford et al. (2009).

In the process of cyber threat communication, the CO must first investigate the threat to create the initial RCP, then it is shared (shared RCP; sRCP) across platforms, in differing modalities, and often across organizations, hierarchical layers, professional backgrounds, and societal sectors. When the CO shares the RCP, the CO must translate information that is often inherently complex and at times vague. The receiving partner may lack the expertise of the CO and have a mindset that is oriented towards action in the physical world (Knox et al., 2018). Thus, the cyber-to-physical relay of RCPs is subject to many challenges which may render the sRCP inaccurate, losing critical information. Consequently, the sociocognitive demands of the tasks performed by COs are complex, demanding high cognitive load, and require both technical (e.g. digital forensic analysis) and non-technical skills (e.g communication; Jøsok et al., 2017). More research is needed on CO communication efficacy.

1.2 Cognitive Aspects of Cybersecurity Performance and Implications for Cyber Threat Communication

Through enhanced information flow, cyber increases human operative abilities (Buchler et al., 2016) while simultaneously creating an environment at odds with human cognition (Zachary et al., 2013). Due to high levels of social barriers, situational shift, and uncertainty, COs must understand and skillfully apply a variety of cognitive processes to adapt to complex and changing task demands (Jøsok et al., 2016, 2017; Knox et al., 2019a). Although these challenges are acknowledged by the adoption of science-based educational approaches to meet the cognitive demands of cyber (e.g. Knox et al., 2019a), common best practices to meet these demands currently do not exist.

Research conducted in collaboration with our lab put forward the Hybrid Space (HS; Figure 1, a) framework (Jøsok et al., 2016) to conceptualize the cognitive landscape COs must navigate. The HS framework focuses on the interconnectedness between cyber- and physical space, and the tension between tactical and strategic goals in decision-making. If a CO is more oriented towards cyber, communicative challenges

may arise when the COs communicates with someone located in the strategic-physical quadrant who in turn must relay the information to an individual with orientation in another quadrant (Figure 1, b; Jøsok et al., 2017). Further socio-cognitive complexity is added when a group of individuals in different hierarchical layers and different tasks all communicate with each other, requiring constant re-adjustment of communication style and message content (Figure 1, c; Jøsok et al., 2017). From the perspective of the CO, knowing where you are in the HS requires metacognitive awareness, indicated by relationships between metacognitive awareness and self-reported cognitive movements within the HS (Knox et al., 2017). When other individuals enter a CO's HS, the CO needs to be aware of their presence in the space and adopt perspective taking to understand their CSA, their grasp of the RCP, and to communicate efficiently one's own RCP understanding. This helps facilitate that involved partners can develop and calibrate shared CSA so that decisions incorporate both tactical and strategic approaches in both the physical and cyber domain (Knox et al., 2018).

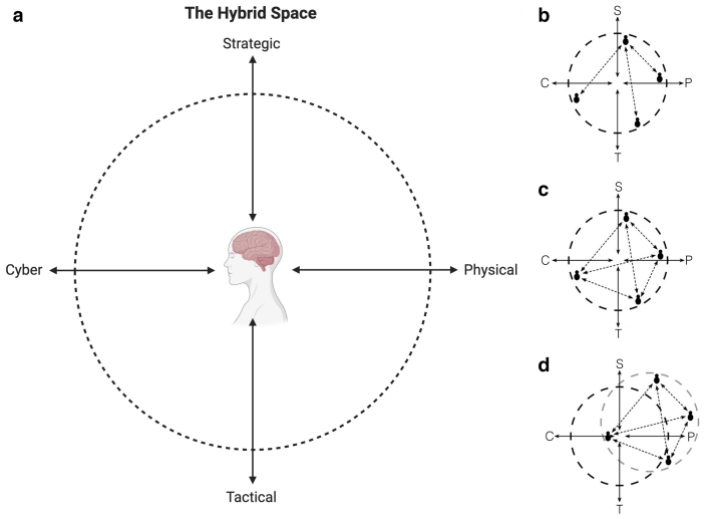

Fig. 1. a The Hybrid Space Framework (Jøsok et al., 2016, 2017) conceptualizing the cognitive landscape cyber operators must navigate. **b** Hierarchical structure, complicated relations. **c** Hierarchical structure, complex relations. **d** Sliding space. C = Cyber. S = Strategic. P = Physical. T = Tactical.

Good cyber defense relies on effective team coordination (Forsythe et al., 2013) and COs working in teams must actively engage in dynamic problem solving to acquire knowledge from each other and the environment (Jøsok et al., 2017). In line with the shifting task demands of the HS, the HS might move along its axis as the focus of the team changes (Figure 1, d; Jøsok et al., 2017) thus changing communicational needs.

1.3 Current approaches to solving communication problems in the Hybrid Space: The Orienting, Bridging, Locating (OLB) Model

The process of communication from threat detection to the CO submitting the RCP to a decision-maker is subject to many iterative sub-processes and factors that affects the sRCP and decision-making. Building on the HS framework, our lab proposed the Orienting, Locating, Bridging (OLB) model (Figure 2; Knox et al., 2018) as a tool to improve communication flow. Although metacognitive awareness is associated with movements in the HS (Knox et al., 2017) and the OLB model provides guidelines for how to apply the HS framework to improve communication (Knox et al., 2018), more research on HS movements and subsequent communication efficiency is needed.

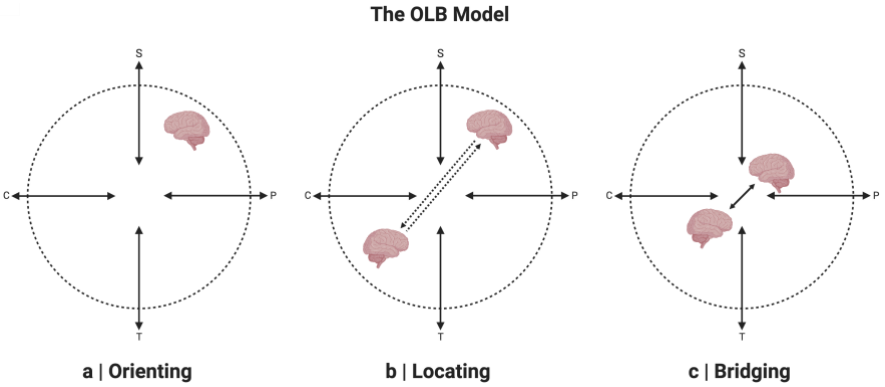

Fig. 2. Orienting, Bridging, Locating (OLB) model. The OLB model (Knox et al., 2018) is a three-stage pedagogical tool to ground communication between cyber operators and their communication partners. C = cyber. S = strategic. P = physical. T = tactical.

1.4 Aim

Given the lack of knowledge regarding human cyber threat communication, in this paper, we review the literature on communication in CTSs. Our aims are to (1) outline how human-human communication performance in cybersecurity settings have been studied, (2) to uncover areas where there is potential for developing common standards for information exchange in collaborative settings, and (3) to provide guidance for future research efforts. While laws and regulations can both be promoters and impediments to information sharing practices (see Pala & Zhuang, 2019), reviewing laws are currently outside the scope of this article.

2 Methods

The systematic review was carried out according to the PRISMA guidelines (Moher et al., 2009). We wanted to review qualitative and quantitative original research articles and reviews that studied human-human communication of cyber threat information.

2.1 Review procedure

1. Identify literature on human-human communication in CTSs through database searches.
2. Categorize the publications according to type and methodological approaches.
3. Provide a summary of the selected articles in order of methodological approaches and which aspect of communication that was studied.
4. Synthesis and discussion of findings followed by suggestions for future research.

2.2 Literature collection methodology

There was no limit to publication year. Only articles written in English were considered. Databases and search terms are listed in Table 1. Any peer reviewed conference papers and journal articles that either: (1) described characteristics of human communication of cyber threat information; (2) suggested ways to improve the relay of cyber threat information between humans; (3) assessed how aspects of human communication related to cybersecurity performance, or; (4) assessed neuroscientific, cognitive, and psychological constructs related to communication were considered for inclusion. Communication could either be the primary focus of the studies or part of a broader focus.

Table 1. Overview of databases, search terms, filters, hits, and date of last search

Database	Search terms	Filters	Hits	Date of last search
Google Scholar	"communication", "cyber threat", “human-interaction experiment”, "recognized cyber picture", "cyber common operational picture", "cyber threat communication"	None	590	Feb. 11. 2021
ScienceDirect	“communication”, “cyber threat”, “human-interaction experiment”, "recognized cyber picture", "cyber common operational picture", "cyber threat communication"	Reviews and research articles	1251	Feb. 11. 2021
IEEE	“communication”, “cyber threat”, “human-interaction experiment”, “recognized cyber picture”, “cyber common operational picture”, "cyber threat communication"	None	388	Feb. 11. 2021
Taylor & Francis	“communication”, “cyber threat”, “human-interaction experiment”, “recognized cyber picture”, “cyber common operational picture”, "cyber threat communication"	None	11	Feb. 13. 2021

2.3 Descriptive information and statistics

Characteristics of each study such as literature type and methodology, results and outcomes including statistics, and studied population were summarized and presented in tables.

3 Results

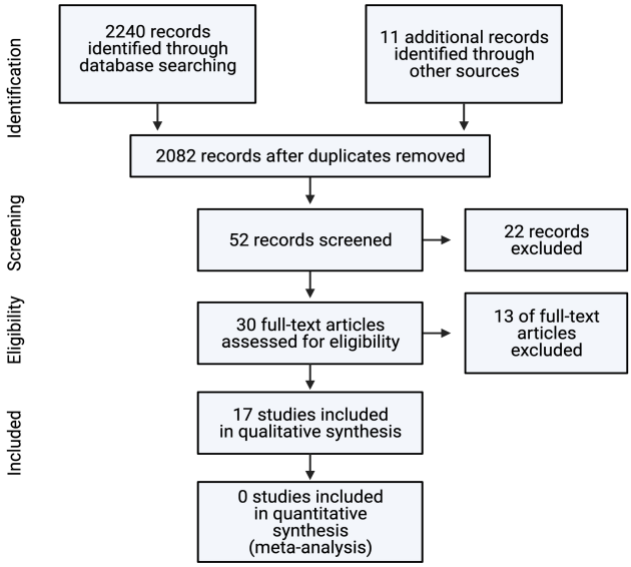

Fig. 3. Flow diagram depicting different phases of the systematic review.

The phases of the review are depicted in the flow diagram in Figure 3. Of studies assessed for eligibility, 13 were excluded due to: (1) proposing technical tools for improved CSA without assessing effects on human communication; (2) only focusing on organization-media communication after a security breach; (3) focusing on increasing the frequency of threat reporting without suggesting ways to organize cyber threat information or making human-to-human communication more effective; (4) not studying human-to-human relay of cyber threat information or associated human factors; (5) applying mathematical modeling of communication and collaboration without human subjects. A total of 17 studies were included in the final review. 12 of the selected articles studied some aspect of cognition and its role in cybersecurity performance. 6 of the studies were conducted on team-based cyber defense exercises (CDXs), Table Top Exercises (TTXs) or Cyber Defense Games (CDGs). There was not enough data to conduct a meta-analysis. None of the studies were published prior to 2012, average publication year was 2016. Overview of the identified publications according to type and methodology is provided in Table 2.

Table 2. Overview of the selected publication according to type and methodology

	Methodology			
Type	Qualitative	Quantitative	Mixed	Total
Conference paper	3	2	3	8
Journal Article	6	3		9

Knowledge Type				
Empirical	5	5	3	13
Theoretical	4			4
Total	9	5	3	17

3.1 Quantitative and mixed studies on cyber threat communication

Five studies examined communication in cyber teams during CDXs, TTXs, or CDGs (Buchler et al., 2018; Champion et al., 2012; Finomore et al., 2013; Henshel et al., 2016; Lugo et al., 2017). One study assessed the role of expectations on security information sharing (Mermoud et al., 2018). One study assessed the role of beliefs on knowledge absorption of cyber threat information (Percia David et al., 2020). One study assessed the knowledge requirements of strategic level decision makers (Garcia-Granados & Bahsi, 2020). Table 3 summarizes the selected quantitative/mixed articles.

Table 3. Overview of quantitative and mixed studies included in the review

First author, year	Design	Effect sizes	Results	Outcome	Population (N; sex)	Comments
Buchler, 2018	Correlational; naturalistic: Survey, structured observation	ComCol on: Maintain services: R2 = 0.42 (−0.13, 1.00); Scenario injects: R2 = 0.54 (−0.03, 1.13); Red team: R2 = 0.27 (−0.23, 0.79)	Maintain services: β1 = 0.65 (−0.21, 1.54)*; Scenario injects: β1 = 0.74 (−0.04, 1.53)**; Red team: β0 = −0.00 (−0.94, 0.90)*	ComCol joint positive predictor of maintain services, scenario injects, and joint negative predictor of scores against red team	Students in cyber defense competition (N=64; sex not reported)	
Garcia-Granados, 2020	Correlational; Literature review, expert panel survey	Not applicable	43 topics identified. SLDM must know all of them. ART had highest average ranking.	Overview of which topics SLDM must have knowledge about and ranked order of priority.	CISOs (N=10; sex not reported)	
Champion, 2012	Correlational: Unstructured interview, observation, TTX	Not reported	(F(1,15) = 4.584*); 60.17% correctly classified	Number of security alerts reduce team effectiveness and CTSA	Proprietary sample (N=24; sex not reported)	Cognitive load = NASA-TLX.
Finomore, 2013	Experiment; naturalistic, within-subjects design	Not reported	Correct: F(2, 11.06) = 9.00*; None (M = 87.5%), Medium (M = 87.5%), High (M = 37.5%). Time: F(2, 9.88) = 14.10*; Medium (M = 16 min, 30 sec), None (M = 16 min, 54 sec), High (M = 27 min, 48 sec) inject.	Untruthful statements diminish team performance	Paid participants (N=24, m = 9)	

Henshel, 2016	Correlational; naturalistic	Not reported	Average arguing 2.05 of 7; Average task redistribution 5.66 of 7.	Arguing negatively correlated with TTP and Correct categorization of NIST event.	US army's Computer Network Defense Teams (N=446; M = 96%)	
Lugo, 2017	Correlational; naturalistic	X-axis: (R2=.245**); Y-axis: (R2= .124*)	Communication demands associated with cyber-physical actions (X) and tactical-strategic decision-making (Y)	Hybrid space performance movements operationalized (4 variables) as DV	Cyber defense cadets (N=31; sex not reported)	IV: TWLS; DV: Hybrid space
Mermoud, 2018	Correlational survey	Spearman's p Frequency: .184 - .244**. Intensity: .169-.275**.	Value of info, social reciprocity, institutional design, and trust associated with SIS.	2 DV: Frequency & Intensity of information sharing	MELANI-net cybersecurity managers (N=262; sex not reported)	6 hypotheses tested
Percia David, 2020	Correlational; questionnaire	Spearman's p: Resource = 0.2860; Usefulness = 0.2779; Reward = 0.0258; Reciprocity = 0.3543.	Resource belief***, usefulness belief***, and reciprocity belief*** positively associated with knowledge absorption	Knowledge about which beliefs are associated with knowledge absorption of cyber threat information	MELANI-net cybersecurity managers (N=262; sex not reported)	Follow-up of Mermoud, 2018.

Notes. P<.05 = *, P<.01 = **, P<.001 = ***. ART = Advanced persistent threat. CDX = Cyber defense exercise. CISO = Chief information security officer. ComCol = Communication and Collaboration. CTSA = Cyber team situational awareness. DV = dependent variable. IV = independent variable. NIST = National Institute of Standards and Technology. SIS = Security information sharing. SLDM = Strategic level decision-maker. TTP = Time between start of inject to returned approval by team controller. TTX = Tabletop exercise. TWLS = Team workload scale.

The role of communication in cyber team performance. To understand how to develop human cyber skill-sets in cyber operational environments, communication and collaboration (ComCol) among team members along with years of experience, and number of roles inhabited by team members were examined as predictors of maintain-service tasks, scenario-injects, performance against the red (attacker) team, and incident response (Buchler et al., 2018). ComCol scores strongly and positively predicted performance on maintain-service tasks and scenario-injects. ComCol scores also predicted performance against the red team, although negatively. ComCol scores did not strongly predict incident response scores (Buchler et al., 2018). Simultaneous analysis of all predictors showed that the ComCol factor was not a unique predictor of performance (Buchler et al., 2018).

As a follow-up to no-findings (Jøsok et al., 2019; Knox et al., 2017, 2019b) on individual traits associated with cyber tactical and strategic decision-making performance, Lugo et al. (2017) investigated the effects of team workload demands on performance in a CDX simulation for testing officer cadets' teamwork perceptions. Outcome measures were based on the HS framework (Jøsok et al., 2016). Previous studies (Jøsok et al., 2019; Knox et al., 2017, 2019b) showed that both cognitive and metacognitive factors could explain cyber-physical interactions, but could not explain any tactical-strategic decision-making during the CDX. ComCol performance demands showed increased involvement on tactical and strategic decision-making outcomes as well as facilitating cyber-physical transitions (Lugo et al., 2017). Only dissatisfaction with team performance was identified as a negative team factor. The results suggested

that situational and team factors need to be taken into consideration alongside individual factors to explain performance (Lugo et al., 2017).

Several factors influence cyber team CSA (CTSA) among COs. Based on the observation that intra-team communication problems were fundamental challenges to CTSA among COs participating in CDXs (Champion et al., 2012), a TTX pilot study was conducted. Team performance dropped by 0.42% per security alert added, affecting perceived attack path, collaborative team report detailing the order and specifics of security breaches, and CTSA. Mental demands were somewhat high and CTSA was moderate to low and declined with increased information (Champion et al., 2012). The authors suggested that information overload drives abnormalities in both team structure and team communication, and that team cyber defense processes must be restructured to facilitate sharing of workload and information. Lack of communication was suggested to be one of the most important contributors to the findings (Champion et al., 2012). The authors did not correlate mental fatigue scores with communication metrics.

In line with findings regarding the challenges associated with communication problems in cyber teams (Champion et al., 2012), detrimental effects of arguments on team performance were reported in initial findings from a study on predictors of cyber team proficiency in CDXs (Henshel et al., 2016). The effect of communication on the following Blue Team proficiency metrics were assessed: (1) Time-to-Detect: Time between start of inject and first validated detection report; (2) Time-to-apProval (TTP): Time between start of inject to returned approval by team controller; (3) Time-to-End (TTE): Time between start of inject to blue team filing close out report, and; (4) Category Correct (CatCorrect): Percent of National Institute of Standards and Technology (NIST) category of inject correctly identified by the blue team. Frequent arguing was found to be significantly and negatively correlated with TTP as well as CatCorrect. Task redistribution when necessary was significantly and positively correlated with TTE and CatCorrect (Henshel et al., 2016). The authors did not report correlation coefficients or p-values but note that most of the data will be reported elsewhere (Henshel et al., 2016).

While other studies (Champion et al., 2012; Henshel et al., 2016) mainly looked at communication with respect to cyber-attacks aimed at assets, one study (Finomore et al., 2013) sought to study the influence of human-directed cyber-attacks on team communication and performance. Distributed team members in a CDG were exposed to misleading information and effects on team processes and decision-making were measured. They all received unique factoids and had to compare them to the factoids received by other team members through communication over a shared radio channel (Finomore et al. 2013). Within-subjects design was employed and divided in conditions None, Medium, and High. For the Medium condition, the inject was suggestive and contradicted supportive information. In the High condition the injects contradicted expert factoids and were phrased as facts. There were no injects in the None condition. Injects in the High condition had the most detrimental effect on team performance both on number of correct answers as well as time spent on completion. How the injects affected communication specifically was not assessed (Finomore et al. 2013).

Knowledge requirements of SLDMs. To tackle communication problems between strategic-level decision makers (SLDMs) and their CO teams, a study (Garcia-Granados & Bahsi, 2020) tried to identify topics of knowledge requirements that could serve as basis for training or CDXs for SLDMs without IT or security background. A

literature search identified 43 topics of knowledge that were sorted based on incident rate to assess their emphasis in the literature. 10 chief security information officers from different industries rated the topics on the level of knowledge needed. A higher rank meant that the topics were attributed a higher knowledge priority (Garcia-Granados & Bahsi, 2020). Although having a low incident rate in the literature, "Advanced Persistent Threat" had the highest average ranking. The lowest ranked topic was "Access control models". No topic was rated as 'no knowledge' meaning that the participants meant SLDMs needed some knowledge about all the topics that were identified (Garcia-Granados & Bahsi, 2016). Topics associated with third party security attained a lower average rank.

The role of expectations on sharing of cyber threat information. The role of incentives for Security Information Sharing (SIS) between human agents working in institutions were assessed to see if expectations of usefulness, reciprocity, institutional barriers, reputation, and trust would affect SIS (Mermoud et al., 2018). A questionnaire was administered to participants of the closed user group of the Swiss Reporting and Analysis Center for Information Assurance (MELANI) which is a government organization that provides a platform to facilitate SIS between Critical Infrastructures (Mermoud et al., 2018). Six hypotheses were tested regarding the effect of expectations on frequency and intensity of SIS, and the moderating role of trust. They found that the value of information a human agent expects to receive from SIS significantly increases the intensity of SIS, but not frequency. Expectancy of social reciprocity significantly increased both intensity and frequency of SIS, as did expectations that SIS would be facilitated by their institution. Both transactional reciprocity and trust between human agents significantly increased frequency of SIS but not intensity. Reputation was not a significant predictor of SIS. They found partial support for their hypothesis regarding the moderating role of trust. It negatively and significantly moderated the relationship between value and the intensity, but not the frequency of SIS. Trust negatively and significantly moderated the relationship between transactional reciprocity and SIS (Mermoud et al., 2018). Education was negatively associated with the frequency of SIS. Gender, age, length of membership in MELANI, and industry affiliation were not significant predictors of SIS.

The role of beliefs on knowledge absorption of cyber threat information. Building on the previous findings of Mermoud et al. (2018) regarding the role of incentives on SIS, Percia David et al. (2020) assessed the relationship between various resource beliefs and tacit cybersecurity knowledge absorption in a study of cybersecurity managers participating in MELANI (the same closed user-group as in Mermoud et al., 2018). Knowledge absorption was not tested directly, but measured through participants rating the amount of exclusive information they received through SIS. They found that the belief that valuable knowledge could be acquired (resource belief), expectations of augmenting efficiency of cyber-security production (usefulness belief), and willingness to reciprocate when receiving valuable information (reciprocity belief) were all positively associated with cybersecurity knowledge absorption. The belief that participation in knowledge-transfer processes would result in reward (reward belief) was not associated with knowledge absorption. Neither were any control variables except prior participations in ISAC events (Percia David et al., 2020).

3.2 Qualitative studies on cyber threat communication

Three studies examined the collaborative and information sharing practices of COs and made suggestions for how to improve the information sharing practice (Ahrend et al., 2016; Skopik et al., 2018; Staheli et al., 2016). One study examined the information requirements different stakeholders had to find a RCP useful (Varga et al., 2018). Two studies researched the role of team mental models (TMMs) in team communication (Hámornik & Krasznay, 2017; Steinke et al., 2016). One study assessed the role various aspects of communication had on performance during CDXs (Jariwala et al., 2012). One study examined how communication impacts the level of trust given to individuals and how it affects cybersecurity risk assessment (Henshel et al., 2015). One study surveyed the literature on Technical Threat Intelligence (TTI) to define what it entails (Tounsi & Rais, 2018). Table 4 summarizes the selected qualitative articles.

Table 4. Overview of qualitative studies included in the review

First author, year	Design	Results	Outcome	Population (N, sex)	Comments
Ahrend, 2016	Exploratory: Semi-structured interview, user diary, thematic analysis.	6 themes, 5 subthemes.	Knowledge about how COs collaborate to organize threat and defense information and tailor it to the needs of the client.	Threat intelligence service providers (N=5; m=4).	Supports Staheli, 2016
Hámornik, 2017	Exploratory: Semi-structured interviews.	TMM is developed and updated by both internal and external communication.	Good TMMs may reduce need for communication during high-risk incident responses and under high time pressure.	Industry experts operating SOCs or performing SOC related activities (N=13; sex not reported).	Similar communication methods as reported by Ahrend, 2016
Henshel, 2015	Exploratory: Review and synthesis	Trust framework with four subcategories of communication: 'accuracy', 'thoroughness or completeness', 'timeliness', and 'honesty'.	Trust framework for risk assessment related to human factors in the cyber domain	Not applicable	
Jariwala, 2012	Exploratory: Observation, questionnaires, focus group	Distributed leadership, open task communication, active feedback, asking for help, offering aid crucial in cyber team performance.	Communication aspects relevant for cyber team performance.	Computer security students (N=20; m=18)	
Skopik, 2016	Exploratory: Review/survey	Suggestions to increase and optimize information sharing among COs and stakeholders.	Structural overview of the dimensions of cyber threat information sharing.	Not applicable	
Staheli, 2016	Exploratory; semi-structured interviews	COs collaborate and communicate more with each other than decision-makers. COs are dis-incentivized to share CTI.	A user-centered collaborative system for COs called Cyber Analyst Real-Time Integrated Notebook Application.	Cybersecurity personnel spanning several job junctions and 8 sectors (N=37; sex not reported)	Supports Ahrend et al., 2016

Steinke, 2015	Exploratory: Review	Methods for improving communication and developing TMMs for CERTs.	Suggestions for enhancement of CERT communication	EMS teams, MR teams, NPPO teams.	
Tounsi, 2018	Exploratory: Review	Trust is an important factor for successful sharing of threat intelligence.	Identification of factors when sharing threat intelligence.	Not applicable	Supports Henshel, 2015 and Steinke, 2015
Varga, 2018	Exploratory: Open-ended survey	Enriched, non-speculative information about an event and how to mitigate it in the short- and long-term. No one requested information on adversarial behavior.	RCP Information elements that are useful for stakeholder's CSA.	National government agencies, regional county administrative boards, county council, local municipal actors, commercial companies that mainly operate nation-wide infrastructure (N=28; Sex not reported)	

***Notes*.** CERT = Cyber emergency response team**.** CO = Cyber operator. CSA = Cyber situational awareness. EMS = Emergency medical systems. MR = Military response. NPPO = Nuclear power plant operating. RCP = Recognized cyber picture. SOC = Security operation center. TMM = Team mental model.

Interviews on the SIS practices of COs. Analyst level COs engage in several informal collaborative and coordination practices when gathering CTI (Ahrend et al., 2016; Staheli et al., 2016). The information needed about a threat differ between clients, thus, RCPs need to be enriched with client-specific information (Ahrend et al., 2016; Staheli et al., 2016). COs communicate through email and phone calls with clients to identify their CTI needs, which is done through onboarding procedures and ongoing communication centered around CTI reports (Ahrend et al., 2016). Gathering information on similar threats that occurred in the past is called gathering Threat and Defense Knowledge (TDK). If a CO was not the one investigating the original cyber threat, COs communicate with the CO who did to gather TDK (Ahrend et al., 2016). This is done by requesting artifacts and information either by face-to-face communication or over email. COs learn about who have encountered similar threats through team meetings, conferences, blogs, and eavesdropping on conversations in and around the office (Ahrend et al., 2016). If COs cannot find information about threats they often assume it does not exist. Existing databases for SIS is circumvented due to not meeting the needs of the COs (Ahrend et al., 2016). COs are often de-incentivized to share data or interim analyses as their reputation as experts is built upon being the one to uncover cyber threats (Staheli et al., 2016) and not sharing information is common (Skopik et al., 2018).

The collaborative ecosystem may involve many organizations with CSA being distributed across COs but the collaborative practices are less common higher up in the SOC hierarchy (Staheli et al., 2016). A typical decision-making hierarchy can be structured with analyst level COs at the bottom, then further up you have supervisors, managers, and then directors at the top (Staheli et al., 2016). While analyst level COs make decisions about what information to include in the RCP, strategic level COs make decisions about whether to send or revise RCPs. Interaction is often uni-dimensional with information being ‘pushed up’ and decisions being ‘pushed down’ the hierarchy (Staheli et al., 2016). A centralized system that incentivizes documenting, SIS and that allows for organizing files to avoid ‘cluttering’ is needed to facilitate communication

of CTI between COs (Ahrend et al., 2016; Staheli et al., 2016). Staheli et al. (2016) proposed a user-centered collaborative system for COs but it needs testing.

Review on the SIS practices of COs. In their extensive survey, Skopik et al. (2016) identify five primary dimensions of information sharing; (1) Efficient cooperation and coordination; (2) Legal and regulatory landscape; (3) Standardization efforts; (4) Regional and International implementations, and; (5) Technology integration into organizations (Skopik et al., 2016). The authors discuss two taxonomies for information and note that TS-CERT taxonomy (Kácha, 2014) is more convenient due to the main categories being universal while sub-categories being part of the description rather than a classification schema. The authors also identify 4 scenarios where cybersecurity information is shared; (1) SIS about recent or ongoing incidents; (2) SIS about service dependencies; (3) SIS about the technical service status, and; (4) when requesting assistance of organizations (Skopik et al., 2016). Shortcomings regarding SIS practices concern Cyber Emergency Response Teams (CERTs) not sharing incident data with other CERTs (ENISA, 2011). Recommendations were made to enrich incident information with additional metadata to provide insights into observed events (ENISA, 2011) and to develop verification methods and criteria for assessing the quality of the data sources. There was demand for establishment of SIS communities with defined scopes (ISO, 2012). A CTI exchange (ITU-T, 2012) model was proposed.

Interview on stakeholder's RCP information requirements. Most of the reviewed studies approach RCPs from the perspective of SOCs. To address the limited research on stakeholder's RCP needs, one study examined the information elements an RCP must contain to be perceived as relevant for the stakeholder's CSA (Varga et al., 2018). Respondents said RCPs needed non-speculative factual descriptions of the events leading up to an incident and that information came from multiple trustworthy sources; otherwise the quality of the information had to be explicitly stated (Varga et al., 2018). The RCP needed information on the internal state of one's own organization, correct time stamps of events, affected location, size of event, up-to-date picture of organizational stance, all taken and planned actions, explicit view of one's own information requirements, communication plan with approved messages, whom to coordinate responses with, and list of available resources. Difficulties regarding information sharing such as adaptation of information to the situation and receivers were mentioned. The information needed in a RCP depended on the situation but included operational information (Varga et al., 2018). Most wanted information on the consequences an incident had to one's own organization and how it would evolve; few wanted to know the impact on other organizations. Differences were seen between regional and service-specific actors, where regional actors need RCPs to facilitate crisis management collaboration while service-specific actors use RCPs to maintain continuity in a service (e.g. electricity) provided to customers and to inform governments agencies with information for a broader perspective. No one asked for information about adversarial behavior (Varga et al., 2018).

Interview on the role of TMMs in SOC team communication. Due to the known role of TMMs on team performance, Hámornik & Krasznay (2017) explored the role of team communication on TMMs in SOC teams. Communication facilitating team-level cognitive processes needs to be explicit and is more effective prior to security events. When security events occur, cognitive load is high, capacity for effective

communication is low, and coordination is implicit (Hámornik & Krasznay, 2017). 13 industry experts who are operating a SOC or performing tasks related to SOCs were interviewed using a semi-structured approach. They reported that local team members communicate within the team verbally or by using email, chat, or ticketing systems. Remote teams communicate via computer-mediated channels, phone calls, and occasional but rare face-to-face meetings (Hámornik & Krasznay, 2017). The TMMs are developed and updated by both internal and external communication. If the mental models are well functioning, explicit communication and coordination activities may not be required during high-risk incident responses and under high time pressure. The authors propose that team cognitions such as constructing and updating TMMs via communication is key in SOC team performance and suggest that research should be focused on measuring the effect of communication on TMMs (Hámornik & Krasznay, 2017).

Review on the role of TMMs in team communication. CERTs are composed of two or more individuals who prepare for and respond to cybersecurity incidents. By examining other emergency response team's methods of adaptation to incidents, Steinke et al. (2015) identified 5 areas that could be improved to increase CERTs effectiveness. One area concerned enhancement of communication. Information richness and reduction in complexity of interaction was important for effective communication; more one-way communication and less two-way exchanges of information. All necessary information should be communicated at once. The authors (Steinke et al., 2015) propose that CERTs can develop TMMs and transactive memory through cross-training, guided team self-correction training, role identification behaviors, pre-mission communication briefings, individual and team after-action reviews and debriefings pointing to where communication broke down, where interactions and coordination did not occur where they should have, and by making electronic knowledge maps displaying team member roles and expertise (Steinke et al., 2015). The authors note that the dynamic and evolving nature of cyber can make it hard to adopt strategies from other incident response teams and must therefore be experimentally tested on CERTs.

Observation and focus group on the role of communication on team performance during CDXs. Among all the studies on cyber team communication, only one detailed the goal of communication within teams (Jariwala et al., 2012). Two cybersecurity teams, Team A and Team B were observed to assess the influence of team communication and coordination on performance. Team A outperformed Team B. Team A had distributed leadership among three members which facilitated sharing of completed tasks and information. Team B had one leader who at times was uncertain about what the team was working on. Team A openly discussed each other's tasks and provided feedback. When Team A members needed help with a task, the team adjusted and assisted the team member until the they could resume independence. Team A members asked for and offered aid more than they planned and assigned roles. When a task could not be completed, leaders would instruct members pick up another task where completion was feasible. Team B had members that never spoke during the length of the CDX, partly attributed to cultural and language barriers (Jariwala et al., 2012).

Review on the impacts of communication on the level of trust given to COs and how it affects cybersecurity risk assessment. In their review of trust as a human

factor in cybersecurity risk assessment, Henshel et al. (2015) describes how their 'trust framework' relates to communication in cyber defense situations. According to their framework, trust is increased by a CO who can effectively communicate with superiors and other COs, log incident reports with minimal false negatives and false positives, communicate information in a timely manner, and employ competency when applying cyber defense tools (Henshel et al., 2015). Communication is efficient when there is common ground and it is built on shared mental models. Based on the concept of defender trust, they divide communication in four subcategories; 'accuracy', 'thoroughness or completeness', 'timeliness', and 'honesty' (Henshel et al., 2015). Effective communication for cyber defenders requires timeliness as any amount of wasted time will increase the window for attackers to do damage or go undetected. Honesty is integral to trust whilst dishonest communication harms both team effectiveness and the accuracy of defensive efforts in the cyber domain (Henshel et al., 2015).

Review on subdivisions of technical threat intelligence. In response to the diversity of CTI research and subsequent lack of consensus of what CTI is, Tounsi and Rais (2018) reviewed the literature on TTI, a subset of CTI, and its multiple sources, the gathering methods, information lifespan, and intended receivers. The authors found that fast sharing of CTI alone was not sufficient to avoid targeted attacks (Tounsi & Rais, 2018). In support of the framework suggested by Henshel et al. (2015), trust was identified to be an important factor for successful SIS; trusted environments and anonymous sharing were listed as possible solutions when organizations engage in SIS (Tounsi & Rais, 2018). The interconnectedness of organizational SIS is increased through the recent use of portals and blogs to exchange semi-automatic threat information. When the quantity of threat information is large, security teams must contextualize the threat data they collect with the specific vulnerabilities and weaknesses they have internally (Tounsi & Rais, 2018). As in the reports of Ahrend et al. (2016) and Staheli et al. (2016), a need for common standards for information sharing were expressed (Tounsi & Rais, 2018).

4 Discussion

The aim of this paper was to: (1) outline how human-human communication performance in cybersecurity settings have been studied; (2) uncover areas where there is potential for developing common standards for information exchange, and; (3) provide guidance for future research efforts. We found that very little research has been done on human-human communication in CTSs and most of the current studies are correlational and exploratory in nature. One study assessed what kind of information that was deemed useful for stakeholders' RCP (Varga et al., 2018). None of the stakeholders interviewed listed adversarial behavior as useful. This could indicate that stakeholders are more oriented towards action in the physical world than in cyber. This can be useful knowledge for COs and suggest use cases for the HS framework (Jøsok et al., 2016, 2017) and the OLB model (Knox et al., 2018) which address these potential problems at both a theoretical-conceptual and practical level, respectfully. The HS framework might be a useful tool for stakeholders to become aware of their own cognitive 'blind spots', while the OLB model can be used by COs to enrich CTI with

information on adversarial behavior and make salient how this behavior contributes to the evolution of the CTS.

Steinke et al. (2015) suggested that enriched, one-way communication of cyber threat information where all necessary information is communicated once would enhance CERTs cybersecurity performance. The relevance of these findings is addressed in the HS framework (Figure 1, a-d; Jøsok et al., 2016, 2017) which illustrates how communication between individuals located across the HS space gets increasingly complex when information is relayed across the space and individuals. When cyber threats occur, timely responses are often key, especially during cyber threat incidents with high time pressure. For one-way communication to be effective, updated and effective TMMs are necessary (Hámornik & Krasznay, 2017; Steinke et al., 2015). Cyber TMMs that are updated through communication and coordination prior to the occurrence of cyber incidents may allow for less communication during high-risk incidents with high time pressure (Hámornik & Krasznay, 2017; Steinke et al., 2015). Cyber teams perform better in CDXs when they spend more of their time communicating help needs and aid-offerings than planning and role-assigning (Jariwala et al., 2012). Based on these findings, longitudinal studies on cyber TMMs and how they relate to the evolution of communication practices could provide novel insights into how and when cyber threat communication can be optimized for performance.

Support for the notion that too much communication during cyber threat incidents can be detrimental to performance is seen in naturalistic studies showing that ComCol negatively predicts scores against attacker teams (Buchler et al., 2018). This, however, might depend on the quality and type of communication, the aspect of performance that is in question (Buchler et al., 2018; Champion et al., 2012; Henshel et al., 2016; Jariwala et al., 2012), and level of expertise (Lugo et al., 2017; Buchler et al., 2018). For example, communication positively predicts handling of both maintenance tasks and scenario injects (Buchler et al., 2018) and productive communication regarding task progress-updates and stating the need of help can enhance incident handling (Jariwala et al., 2012). Under-communication can also be detrimental to team performance by leading to team members working on the same tasks without knowing (Champion et al., 2012). Distributed team leadership might mitigate these issues if individuals holding leadership positions also spend time communicating with team members to know which tasks they are working on (Jariwala et al., 2012). Indeed, the dynamic and evolving nature of cyber and the broad demands of expertise might favor distributed leadership (Jøsok et al., 2017). ComCol performance demands influence tactical and strategic decision-making outcomes and cyber-physical transitions in the HS (Lugo et al., 2017). As opposed to the Buchler et al. (2018) study on CO experts, these cadets were novices. ComCol demands might be necessary in training and development, but may become less relevant with experience.

To update their own and clients CSA, COs enrich RCPs with useful TDK by communicating with both team members and COs from other organizations as well as their clients when investigating a cyber incident (Ahrend et al., 2016; Staheli et al., 2016). This practice is most common for analyst level COs but less and less common higher up in the decision-making hierarchy (Staheli et al., 2016). Albeit making decision-making more effective, these structural inefficiencies can be detrimental to CSA and shared mental models in the organization, cause communication and coordination problems, and potentially reduce creativity among COs (Staheli et al.,

2016). This can be illustrated with the HS framework (Jøsok et al., 2016) when COs and SLDMs are in different quadrants of the HS without knowing where the other organizational members are. Studies assessing or manipulating the RCP-related resource-beliefs of COs and SLDMs (Mermoud et al., 2018; Percia David et al., 2020) may be useful in determining the effect of shared mental models on the resulting RCP.

The reviewed literature has several limitations. Most of the studies were the first to assess the relationships they studied and have thus not been replicated, although they seem to converge on some common principles. Half of quantitative studies (Buchler et al., 2018; Lugo et al., 2017; Mermoud et al., 2018; Percia David et al., 2020) report effect sizes and one study did not report effect sizes nor p-values (Henshel et al., 2016). Sensitivity issues might be the reason why few studies report participant characteristics such as which sector respondents belong to. The Varga et al. (2018) study was conducted exclusively on Swedish participants with a large disproportion of respondents belonging to national agencies and critical infrastructure operators, meaning that the robustness of the findings may vary according to which sector provided the answers. This issue is discussed by the authors (Varga et al., 2018). In general, cybersecurity personnel are hard to access and naturalistic studies are tricky to conduct because contextual variables are hard to manipulate partly due to restricted collaboration with CDX organizers. This is apparent in the reviewed literature and is a barrier that needs to be overcome. Few studies (Jariwala et al., 2012; Steinke et al., 2015) elaborate on the quality and characteristics of communication. A focused effort is needed to develop quantitative measures of communication that can be readily applied in CDXs in addition to measures of TMM development. Moreover, only two studies assessed individual and team measures (Champion et al., 2012; Lugo et al., 2017) although only one study assessed the relationship between these measures (Lugo et al., 2017). Thus, there is also a need for studies simultaneously assessing individual and team factors related to communication and performance.

4.1 Future directions and conclusion

Communication in CTSs has not received much attention and the nature and quality of studies vary. Studies assessing both team factors and individual factors simultaneously are almost non-existent. We found only one study where variables were manipulated to see their effects on communication and more basic and experimental studies are needed. CDX organizers could benefit from collaborating with cognitive scientists to experimentally manipulate aspects of the CDX such that new insights can be achieved. It would be useful to manipulate and quantify TMM development prior to and during a CDX or TTX to measure the effect on communication. Standards for characterizing and assessing cyber team communication need to be developed and implemented in studies.

5 Funding

This study was conducted as part of the Advancing Cyber Defense by Improved Communication of Recognized Cyber Threat Situations (ACDICOM; project number 302941) project. ACDICOM is funded by the Norwegian Research Council.

References

Agyepong, E., Cherdantseva, Y., Reinecke, P., & Burnap, P. (2020). Challenges and performance metrics for security operations center analysts: a systematic review. *Journal of Cyber Security Technology*, *4*(3), 1-28. DOI: 10.1080/23742917.2019.1698178

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)*. Doi:10.1109/cybersa.2016.7503279

Barford, P., Dacier, M., Dietterich, T. G., Fredrikson, M., Giffin, J., Jajodia, S., … Yen, J. (2009). Cyber SA: Situational awareness for cyber defense. *Cyber Situational Awareness*, 3–13. Doi:10.1007/978-1-4419-0140-8_1

Buchler, N., Fitzhugh, S.M., Marusich, L.R., Ungvarsky, D.M., Lebiere, C., & Gonzalez, C. (2016). Mission command in the age of network-enabled operations: social network analysis of information sharing and situation awareness. *Frontiers in Psychology*, *7*, 937.

Champion, M. A., Rajivan, P., Cooke, N. J., & Jariwala, S. (2012). Team-based cyber defense analysis. *2012 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support*. Doi:10.1109/cogsima.2012.6188386

ENISA. (2011). Proactive detection of network security incidents. https://www.enisa.europa.eu/activities/cert/support/ proactive-detection/survey-analysis. Last accessed 03.20.21.

Finomore, V., Sitz, A., Blair, E., Rahill, K., Champion, M., Funke, G., … & Knott, B. (2013) Effects of cyber disruption in a distributed team decision making task. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *57*(1), 394-398.

Forsythe, C., Silva A., Stevens-Adams, S., & Bradshaw, J. (2013). Human dimension in cyber operations research and development priorities. In: Schmorrow D.D., Fidopiastis C.M. (eds) *Foundations of Augmented Cognition. AC 2013*. *Lecture Notes in Computer Science*, *8027*. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-39454-6_44

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

Garcia-Granados, F. & Bahsi, H. (2020). Cybersecurity knowledge requirements for strategic level decision makers. *International Conference on Cyber Warfare and Security 2020*. DOI: 10.34190/ICCWS.20.102

Hámornik, B. P., & Krasznay, C. (2017). A team-level perspective of human factors in cyber security: Security Operations Centers. *Advances in Human Factors in Cybersecurity*, 224–236. Doi:10.1007/978-3-319-60585-2_21

Henshel, D., Cains, M. G., Hoffman, B., & Kelley, T. (2015). Trust as a human factor in holistic cyber security risk assessment. *Procedia Manufacturing*, *3*, 1117–1124.

Henshel, D. S., Deckard, G. M., Lufkin, B., Buchler, N., Hoffman, B., Rajivan, P., & Collman, S. (2016). Predicting proficiency in cyber defense team exercises. *MILCOM 2016 - 2016 IEEE Military Communications Conference*. doi:10.1109/milcom.2016.7795423

ISO. (2012). Iso/iec27010: Information technology – security techniques –information security management for inter-sector and interorganizational communications.

ITU-T. (2012). Recommendation ITU-T x.1500 cybersecurity information exchange techniques.

Jariwala, S., Champion, M., Rajivan, P., & Cooke, N. J. (2012). Influence of team communication and coordination on the performance of teams at the iCTF Competition. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *56*(1), 458–462.

Jøsok, Ø., Knox, B. J., Helkala, K., Lugo, R. G., Sütterlin, S., & Ward, P. (2016). Exploring the Hybrid Space. *Foundations of Augmented Cognition: Neuroergonomics and Operational Neuroscience*, 178–188. doi:10.1007/978-3-319-39952-2_18

Jøsok, Ø., Knox, B. J., Helkala, K., Wilson, K., Sütterlin, S., Lugo, R. G., & Ødegaard, T. (2017). Macrocognition applied to the Hybrid Space: Team environment, functions and processes in cyber operations. *Lecture Notes in Computer Science*, 486–500.

Jøsok, Ø., Lugo, R., Knox, B. J., Sütterlin, S., & Helkala, K. (2019). Self-regulation and cognitive agility in cyber operations. *Frontiers in psychology*, *10*, 875.

Kácha, P. (2014). Idea: security event taxonomy mapping. *In: 18th International Conference on Circuits, Systems, Communications and Computers, 2014*.

Knox, B. J., Jøsok, Ø., Helkala, K., Khooshabeh, P., Ødegaard, T., Lugo, R. G., & Sütterlin, S. (2018). Socio-technical communication: The hybrid space and the OLB model for science-based cyber education. *Military Psychology*, *30*(4), 350-359.

Knox, B. J., Lugo, R. G., Jøsok, Ø., Helkala, K., & Sütterlin, S. (2017). Towards a Cognitive Agility Index: The Role of Metacognition in Human Computer Interaction. *In International Conference on Human-Computer Interaction*, 330–338.

Knox, B. J., Lugo, R. G., & Sütterlin, S. (2019a). Cognisance as a human factor in military cyber defence education. *IFAC-PapersOnLine*, *52*(19), 163–168.

Knox, B. J., Lugo, R. G., Helkala, K., & Sütterlin, S. (2019b). Slow education and cognitive agility: Improving military cyber cadet cognitive performance for better governance of cyberpower. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, *9*(1), 48-66.

Lugo, R., Kwei-Nahr, P., Jøsok, Ø., Knox., B., Helkala, K., & Sütterlin, S. (2017). Team Workload Demands Influence on Cyber Detection Performance. 1*3th International Conference on Naturalistic Decision Making 2017, 223-225.*

Mermoud, A., Keupp, M. M., Huguenin, K., Palmié, M., & Percia David, D. (2018). Incentives for human agents to share security information: A model and an empirical test. *2018 Workshop on the Economics of Information Security (WEIS). - Innsbruck.*

Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2009). Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. *Journal of Clinical Epidemiology*, *62*(10), 1006–1012. doi:10.1016/j.jclinepi.2009.06.005

Muniz, J., McIntyre, G., & AlFardan, N. (2015). *Security Operations Center: Building, Operating, and Maintaining Your SOC*. Cisco Press, Indianapolis.

Pala, A., & Zhuang, J. (2019). Information sharing in cybersecurity: A review. *Decision Analysis*. doi:10.1287/deca.2018.0387

Percia David, D., Keupp, M. M., & Mermoud, A. (2020). Knowledge absorption for cyber-security. *Computers in Human Behavior*, *106*, 106255. doi:10.1016/j.chb.2020.106255

Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security*, *60*, 154–176. doi:10.1016/j.cose.2016.04.003

Staheli, D., Mancusco, V., Harnasch, R., Fulcher, C., Chiemelinski, M., Kearns, A., … & Vuksani, E. (2016). Collaborative data analysis and discovery for cyber security. *SOUPS 2016: Twelfth Symposium On Usable Privacy and Security*.

Steinke, J., Bolunmez, B., Fletcher, L., Wang, V., Tomassetti, A. J., Repchick, K. M., … Tetrick, L. E. (2015). Improving cybersecurity incident response team effectiveness using teams-based research. *IEEE Security & Privacy*, *13*(4), 20–29. Doi:10.1109/msp.2015.71

Tikk-Ringas, E., Kerttunen, M., & Spirito, C. (2014). Cyber security as a field of military education and study. *Joint Forces Quarterly*, *75*(4), 57–60

Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security*, *72*, 212–233.

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)*.
Whitman, M. E., & Mattord, H. J. (2012). *Principles of information security* (4th ed.). Boston, MA: Course Technology
Zachary, W., Rosoff, A., Miller, L. C., Read, S. J. (2013). Context as a cognitive process: an integrative framework for supporting decision making. *The 8th International Conference on Semantic Technologies for Intelligence, Defense, and Security (STIDS 2013).*
Zanenga, P. (2014). Knowledge eyes: Nature and emergence in society, culture, and economy. *2014 International Conference on Engineering, Technology and Innovation (ICE)*.