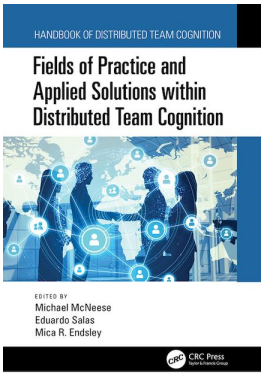

Fields of Practice and Applied Solutions within Distributed Team Cognition

Michael D. McNeese, Eduardo Salas, Mica R. Endsley

Team Dynamics of Cybersecurity

Publication details
https://test.routledgehandbooks.com/doi/10.1201/9780429459542-6
Vincent Mancuso, Sarah McGuire
Published online on: 29 Sep 2020

6 Team Dynamics of Cybersecurity *Challenges and Opportunities for Team Cognition*

Vincent Mancuso and Sarah McGuire

CONTENTS

INTRODUCTION

In December of 2015, consumers of several Ukrainian power companies, totaling around 230,000 people, were left without electricity for up to six hours, following a cyber-attack that switched off numerous substations throughout the country (Zetter, 2016). This outcome was part of a carefully crafted campaign, involving numerous acts of spearphishing, taking command and control of supervisory control and data acquisition (SCADA) systems, destruction of computing infrastructure and data, and a denial of service attack to create mass confusion and uncertainty. In a single coordinated campaign, adversaries not only impacted computing network systems, but also caused kinetic effects across a nation's power grid. In addition, this attack demonstrated the potential for cyber-attacks to impact human behavior, an element of cyber-attacks that has become an important reality to the American public through the topic of election interference.

While not the first instance of such an attack, this incident has become a seminal example of the breadth of impact and interdependencies of cyber on other national assets. What was once considered to be part of the information domain of warfare has since evolved to an interconnected system which includes control of computing systems, critical infrastructure, resources, and human actors. While the vectors of many modern cyber-attacks may be through computing systems and networks, the effects often materialize in other domains. With this realization, cybersecurity and operations have become a pivotal discussion within our national security organizations, from both an operational and research perspective.

In response to this, over the last decade, researchers and practitioners across the government, industrial base, and academia have become invested in establishing a secure and resilient cyberspace. With new threats emerging on a daily basis, significant investments into research and development for new cybersecurity capabilities are being made. Currently much of the research in cyber is grounded in the computer science, mathematics, and engineering fields, with a strong focus on developing algorithms, architectures, and visualizations to help improve detection of malicious activity on a network. The result of this work has led to numerous competencies and capabilities to aid in the defense of our cyber infrastructure and improve our national security posture. While this work continues to have utility, the human element of cyber is equally as critical an element of cybersecurity.

As there continue to be strides made in developing technological competencies to support cybersecurity, our understanding and support to the human-in-the-loop in such environments is still immature. From a human-centered viewpoint, cyber is a cognitively demanding profession. Cyber analysts and defenders rely primarily on their own cognitive resources to interpret observed network activity and translate it into tangible information surrounding the potential of an attack and options for remediation. The majority of this synthesis activity takes place internally in the human mind, placing a significant cognitive burden on them: "the cognitive skill

involved in detecting relationships is so critical that any procedures or aids that can expedite or enhance it would improve the analysis process" (D'Amico et al., 2005). In the event of an attack or threat, cyber defenders must identify the adversaries and their capabilities, identify the intended victims, and formulate a hypothesis of the intent of the attack (Caltagirone et al., 2013). During their everyday work, cyber defenders must maintain a mental model of "normal network behavior" despite a constantly shifting landscape: critical networked infrastructure may change without warning, tasking may be rerouted, and agile adversaries are constantly adapting their strategy to elude detection.

If these tasks were not difficult enough, the dynamic and intangible nature of the cyber environment, often referred to as cyberspace, creates a complex and challenging cognitive domain. Cyberspace consists of numerous unique and overlapping networks, nodes within those networks (i.e. any logical device with a network address or analogous identifier, including computing resources that produce, consume, or route data packets, constitutes a node), associated system data (i.e. routing tables, access control lists, etc.), and applications. Across each of these, cyberspace is defined in three layers: *physical*, *logical*, and *cyber-persona*.

- The *physical* layer of cyberspace comprises the physical equipment that transports data and the nodes or systems that process, store, or prepare data for transport. These entities are geographically located in the physical world and are subject to kinetic effects.
- The *logical* layer consists of information and computing assets and their relationships. Together the physical and logical layers can be described as the "terrain" of the cyber domain.
- The *cyber-persona* layer is the digital representation of the identity, authorization, and activities of individual entities (human or computer controlled) in cyberspace, including their behavior in the logical layer and applicable permissions and credentials. This layer is most easily understood as the entities that make use of the network.

Increasing the complexity, cyberspace is a dual role environment in which effects can be achieved, and is an environment for sharing information and synchronization of organizational resources. As organizations often rely on cyberspace resources for their everyday operations, its protection has significant importance to achieving organizational goals.

While these definitions provide structure, they still suffer from complexities that have defining features that separate themselves from each other, making them distinct entities. Unlike the traditional domains of effects, land, sea, and air, cyberspace exists on a digital plane rather than a physical one (Fairfax, Laing, & Vickers, 2015). Cyberspace is an intangible environment, in which the tactical space where operations occur can align with one or many of the traditional effect domains. Where other types of security have physical anchors in the environment, cyberspace exists as a combination of hosts, switches, routers, and entities which are not attached to any physical locations such as the logical, cyber-persona, and supervisory planes of cyberspace (Fanelli & Conti, 2012).

Without physical anchors, analysts are free to create their own mental schema of the environment, based on their own assumptions, biases, and tasking. Additionally, this can result in analysts developing and pivoting between multiple mental models of the network, depending on their current situation. While there is some benefit to having multiple mental models, there are also numerous drawbacks. With the lack of physical anchors, it can be difficult for analysts and commanders to understand the impact of their actions on the environment.

Teamwork in Cybersecurity

Many of the tasks that exist within cybersecurity, such as monitoring networks, host-based analyses, and incident response, are part of a larger sociotechnical system, dependent on numerous actors across multiple organizations (Cooke et al., 2013; Tyworth, Giacobe, Mancuso, & Dancy, 2012). Effective team collaboration in cybersecurity relies on accurate and shared situational awareness of command priorities, network health and status, and resource allocation and tasking. After completing analysis, cyber defenders must efficiently communicate their findings up the chain of command for a decision on an effective course of action. Research has shown that when engaging in tightly coupled collaborations, versus more loose collaborations, cyber defense analysis teams perform better and demonstrate lower biases in their decision making (Rajivan et al., 2013). In their cognitive task analysis of cyber analysts, D'Amico et al. (2005) extracted six unique roles, that are often distributed across numerous analysts, triage, escalation analysis, correlation analysis, threat analysis, incident response, and forensic analysis. In their model, these activities are distributed across three primary stages, detection, situation assessment, and threat assessment, which map to the tactical and strategic stages of warfare. As these activities are distributed across a sociotechnical process, information sharing is critical to ensure that at each phase, the responsible analyst has the most current and relevant situation awareness information. Tyworth et al. (2012) demonstrated this information sharing is not as simple as to be expected, with analysts with different specializations sharing information haphazardly, without providing necessary information, referred to as "throwing [reports] over the metaphorical wall" between organizations. Whenever these breakdowns in team collaboration occurred, organizational-level cyber performance deteriorated, with analysts losing track of critical data, operating in a degraded decision space, and creating incomplete and ineffective boundary objects, which hindered future collaborations. On the other hand, when teams are able to effectively and efficiently share information, even without explicit communication, they are able to outperform teams with less effective collaborative processes (e.g. Buchler, Rajivan, Marusich, Lightner, & Gonzalez, 2018).

Needless to say, teams play a critical role in cybersecurity (Champion, Rajivan, Cooke, & Jariwala, 2012), however the organizational, geographic, and technological boundaries are a deterrent to collaboration amongst analysts. In their study, Tyworth et al. (2012) found that as a result of poor team composition, lack of awareness across the organization, and boundaries between analysts, there was very little communication and information sharing across functional domains. As the information moves up the organizational hierarchy, managers who are being reported to may not necessarily

be cyber experts; thus, the analysts and defenders must extract and abstract information into a decision-quality product from raw data (Staheli et al., 2016).

Inter-organizational teams face additional challenges in accessing key information. Providing a framework that permits the free flow of information between organizations while maintaining organizational security and adhering to information security policy is a challenge to collaborative analysis (Hui et al., 2010). Often incidents require correlation of activity across multiple levels of ownership (or classification in the government), enclaves, and organizations to fully understand the impact or identify trends, creating further barriers to effective collaboration. These coordinative challenges are further compounded by the local needs of the cyber defenders in juxtaposition to the global needs of network operations.

Current research in cyber focuses on issues such as developing algorithms and intelligent systems to enable a secure cyberspace, generally brushing aside issues such as awareness and performance metrics, or even a common definition for "cyber." Research continues to ignore the human, even though originating definitions of cyber situation awareness identified their role as critical (Bass, 2000). Regardless of the efficacy of current and future systems, the human element remains an essential part of the system, thus a new discussion on human-centered cyber cognition is necessary.

Cybersecurity is a largely interdependent social system, in which analysts must share information within and across organizational boundaries, collaborate, and make decisions in order to ensure the security of the network (Staheli et al., 2016). Analysts within cybersecurity are often distributed on several axes. From a functional standpoint, cybersecurity is often distributed across multiple analysts with focus on different expertise domains such as intrusion detection, threat analysis, policy, and operational considerations (Tyworth et al., 2012). Similarly, in many organizations, cyber is often organized by functional areas, with departments focused on administration, intelligence, operations, planning, command and control, and logistics (with command and control and intelligence being mostly unique to military organizations). Within these structures, there are numerous interdependent tasks, in which analysts must collaborate and share critical information with others across organizational boundaries.

These structures diverge from teams considered within team cognition and associated literature, which often assumes tightly coupled collaborative processes and dependencies that require synchronized behaviors. Currently, there is relatively limited available research on human-centered cyber cognition, mostly due to a lack of understanding, availability, and access to the necessary resources to conduct cyber research. Whether it is due to classification, in government, or trade secrets, in industry, it can be difficult, if not impossible, for researchers to gain access to necessary data, environments, and experts to conduct the foundational background research to fully understand the cognitive and collaborative work at play. Additionally, as much of this research can lead to an identification of pain points and deficiencies within an organization, being able to share such information is equally if not more of a challenge.

Many have called for an increase in research in these areas (Boyce et al., 2011; Knott et al., 2013; Mancuso et al., 2014), and there are many areas that are likely

to bear fruit concerning situation awareness and performance (Gutzwiller, Fugate, Sawyer, & Hancock, 2015). However, currently human-centered cyber often focuses on the analytical and decision-making processes of a singular analyst, with less attention on collaboration, information sharing, and shared situation awareness in cyber defense. This lack of research in team cybersecurity has created a significant gap, as cyber defenders are required to find ad hoc methods to transition from individual to team decision making, creating numerous opportunities for future research and applications of the vast amount of prior work in team collaboration, cognition, and dynamics.

PURPOSE

With the continued and growing importance of cybersecurity, we must continue to push beyond a techno-centric perspective in both research and practice. While the individual human-in-the-loop is critically important in cybersecurity, we must approach them from a perspective that they are part of a larger sociotechnical system, with interdependencies and interactions between multiple humans, organizations, and technologies (Endsley & Connors, 2012; Fink, North, Endert, & Rose, 2009; Tyworth et al., 2012).

The goal of this paper is to focus on team dynamics in cybersecurity and reflect on the major issues in such environments, describe how team cognition research can be applied, and then discuss both research and practical implications. Specifically, we will focus on four main issues of team cognition in cyber: team situation awareness, role definitions and staffing, team hand-offs, and team performance measures. Within each of these topics, we will provide an overview of how the challenge manifests itself within cybersecurity, a discussion on how research in team cognition and dynamics may apply, and potential directions for both researchers and practitioners. Building on these areas, we will discuss emerging considerations such as human-machine teaming, which may have implications for how cyber operations are conducted in the near and distance futures.

TEAM COGNITION IN CYBER: CHALLENGES

Team Cyber Situation Awareness

Overview

While cyber is a relatively immature research area for both the human and computational sciences, cyber situation awareness (SA) has emerged as a persistent thread in terms of understanding analyst decision making, algorithm development, and the design of novel visualizations. Of all the human-centered issues, cyber SA has received by far the most attention, with numerous special journal issues, conferences, and grants being funded in this area.

This is not necessarily surprising—SA is frequently cited as a critical contributor to individual and team performance in complex and dynamic environments. Originally coined by former chief scientist of the United States Air Force Mica R. Endsley (1995) during her research on the cognitive process of pilots, the most

ubiquitous definition of SA describes it as "the perception of elements in the environment with a volume of time and space, the comprehension of their meaning, and projection of their status in the near future." As it has been demonstrated in numerous domains, experts believe that accurate, timely, and comprehensive cyber SA provides critical input for decision making when engaging an elusive, adaptive adversary in a constantly changing operational environment.

Unlike more kinetic domains, cyber SA is inherently complex, due to the invisible nature of the cyber environment, the emergent and adaptive threat environment, and data flow rates with a high noise to signal ratio, which transcend human cognitive ability (Endsley & Connors, 2014). From a collaborative perspective, team cyber SA can be considered to be the distribution of critical SA information across a team or organization based on hierarchical role (i.e. analyst, supervisor, commander) and specialization and functional areas (i.e. intrusion detection, network security, intelligence, etc.), and shared and communicated in combination between human cognitive and collaborative behavior and information systems and technological artifacts (Staheli et al., 2016; Tyworth et al., 2012).

In their interviews with analysts, Gutzwiller, Hunt, and Lange (2016) identify three critical elements of cyber SA: the network, the world, and the team. These have some overlap with three classes of awareness defined in Department of Defense Joint Publication 3–12 (2018): Cyberspace Operations: network/system awareness, mission awareness, and adversary awareness. *Network/system awareness* is comprised of key information about the critical cyber terrain in accomplishing the mission, including the status of servers and end points across the network. *Mission awareness*, in which the team is a component, pertains to information about the current tasking and objectives, and the progress and work of the team/organization towards that goal. Finally, *adversary awareness* involves an up-to-date understanding of the threat environment and interdependencies that exist on external networks, organizations, or adversaries. In order to make informed, effective decisions, cyberspace analysts across organizations must have an accurate understanding of what is occurring within their own network and in the world at large (including the activity of their adversaries), and an interpersonal awareness of the requisite situational awareness possessed by others in order to make informed accurate decisions. While building and maintaining accurate cyber situation awareness at the individual level is a cognitively demanding task (D'Amico, Tesone, & Whitley, 2005), these challenges are multiplied at the team and organizational level. Research has shown that situation awareness information and the decisions that are associated with it are often distributed across the organization structure (Staheli et al., 2016).

Analysts must identify their adversaries, locate and isolate victims, formulate a hypothesis of the intent of the attack, and project remediation opportunities, while coordinating and collaborating with others over geographic, functional, and organizational boundaries (Caltagirone, Pendergast, & Betz, 2013; Tyworth et al., 2012). In order to accomplish this, analysts must build a shared situational awareness model while dealing with information overload and balancing team structure and dynamics and communication and collaborative processes (Champion et al., 2012). This is further confounded with a lack of current accurate information on the network and adversaries. Many of the decisions an individual is responsible for in cyber require

a current and accurate map of the cyber assets that they currently support. These maps are often developed manually in a tedious and error-prone process, making their accuracy and currency a continuous question (Goodall, D'Amico, & Kopylec, 2009). Additionally, with adversaries constantly changing their tools, techniques, and practices (TTPs), analysts are often tasked with building SA in an incomplete and adversarial decision space.

If the act of obtaining individual situational awareness is not already challenging enough, the distribution of expertise and specializations across organizational boundaries adds to the complexity. Even if every single analyst in an operations center has accurate cyber SA, if the necessary information is not shared, fused, and enriched across the team, the overarching team and organizational SA will be incomplete, resulting in a negative impact on decision making and performance.

Unlike more tightly coupled collaborative domains, in cyber, rather than explicit communication, analysts implicitly collaborate through data (e.g., data dumps, intrusion sets, etc.) and incident reports (D'Amico & Whitley, 2008). To make effective decisions at the individual level, it is not only important that they possess the requisite knowledge and awareness of the situation themselves, but also have an interpersonal awareness and shared understanding of others. For example, during their observations and data collections at a collegiate cyber defense challenge, Buchler at al. (2018) found that experienced teams shared fewer face-to-face communications, relying more heavily on role specialization, implicit communication, and information sharing via collaborative software.

Even with numerous interdependencies across individuals, the majority of the analytical work occurs at the individual level. To better understand, lessons can be leveraged from the classical definition of cooperative collaboration offered by Dillenbourg, Baker, Blaye, and O'Malley (1995, p. 2) in which work is "accomplished by the division of labor among participants, as an activity where each person is responsible for a portion of the problem solving," as compared to collaborative work, where there is a "mutual engagement of participants in a coordinated effort to solve the problem together."

Team SA is typically approached through a lens of multiple people who recognize that they are within the same collaborative system performing a tightly coupled task with coordinated action. In this case, a team is a social entity made up of multiple individuals working together with high interdependency, shared values, and a common goal (Dyer, 1984). However, contrary to this, cyber work is often completed independently, but still maintains a common goal amongst workers, which in turn creates shared values and desires. This creates a large interdependent system, in which individuals act independently with varying levels of coordination and cooperation to achieve a common goal.

Applications of Team Cognition

While individual SA is an important factor in cyber, the "big picture" or complete organizational cyber SA is distributed across multiple people and organizations (Tyworth, Giacobe, Mancuso, McNeese, & Hall, 2013). When scaled to the team or organization level, SA can be described as "the sharing of a common perspective between two or more individuals regarding current environmental events, their

meanings, and their projected future" (Wellens, 1993). Similarly, Endsley (1989) defines team SA as "the degree to which every team member possesses the situation awareness required for his or her responsibilities" (Endsley, 1989). These models of SA suggest that it is a state of human cognition shared across multiple people that consists of a mental model of the current situation and an assessment of the impact of competing actions on the environment. The decision maker utilizes a separate decision-making loop which fuses their internal mental model with external information (from the environment and other individuals' mental models) to decide which action to perform.

Team research has long studied SA in many complex domains, such as air traffic control (e.g. Endsley & Rodgers, 1994; Kaber, Perry, Segall, McClernon, & Prinzel III, 2006; Rodgers, 2017), aviation (e.g. Jones & Endsley, 1996; Taylor, 2017; Wickens, 2002), and emergency response operations (e.g. Harrald & Jefferson, 2007; McNeese et al., 2005; McNeese, Mancuso, McNeese, Endsley, & Forster, 2014), to name a few. In recent years, research has identified team cyber SA as a critical element in improved performance and decision making in cyber (e.g. D'Amico et al., 2005; Gutzwiller et al., 2015, 2016; Tyworth et al., 2012).

At the team level SA can be further understood using mental model theories, where complimentary mental models, made up for taskwork and teamwork, have interactions leading to improved team performance (e.g. Klimoski & Mohammed, 1994; Mohammed & Dumville, 2001). Within the task mental model, team members must have an understanding of the technology and systems they are interacting with, the requisite knowledge to complete the task, an understanding of processes and strategies, and an awareness and understanding of the environment, its condition, and dynamics. The teamwork mental model, on the other hand, pertains to an understanding on how the technology is distributed across the team, on how the team interacts, and the division of roles, responsibilities, and knowledge. This also has overlap with transactive memory theories, in which performance is driven by a consensus of expertise, specialization across the group, and accuracy of knowledge (Austin, 2003). Transactive memory states that in order for a team to achieve a maximum performance, the team must be made up of individuals with deviations in their specialization, a consensus and awareness of who is an expert in what, and the knowledge at the individual level must be accurate.

Team cognition research shows that in order for teams to leverage their own situation awareness and knowledge, they must also possess awareness of team and its collaborative dynamics. To achieve this awareness, individuals must effectively communicate and share information, both of which have been shown to be a predictor of team performance (DeChurch & Mesmer-Magnus, 2010). These collaborative processes can not only improve SA at the team level, but also help reduce errors, manage task complexity, and reduce ambiguity and stress (Salas, Cooke, & Rosen, 2008). Without these underlying processes, individuals are unable to obtain the necessary information to update their own SA mental model, and cannot make a fully informed decision, having a negative impact on the overall team and organizational performance.

In the context of cyber, when the analysts are distributed across functional, geographic, and temporal boundaries, these collaborations and the development

of shared awareness often occurs within technologies such as shared wikis, message boards, and collaborative portals. Using these technologies, the humans rely on implicit and shared artifacts to enable their collaborations, known as "boundary objects." In their seminal paper, Star and Griesemer (1989) define boundary objects as "objects which are both plastic enough to adapt to local needs and constraints of the several parties employing them, yet robust enough to maintain a common identity across sites" (p. 393). As applied to cyber, boundary objects serve as the technological medium for fostering collaborations and helping individuals to ground their own actions within the context of the larger collaborative and interdependent system.

Based on previous research on team SA and related constructs, several directions for future work, both research-focused and applied, begin to emerge.

Research Implications

Currently, one of the biggest problems that exists within cyber SA is the processes around and the ability to share relevant cyber SA information across the numerous boundaries that exist across organizations. Cyber work is often distributed across individuals, teams, and organizations, and a complete SA mental model depends on an awareness of the knowledge, information, abilities, and priorities of others. If an analyst needs critical information to complete their task, and does not know where to obtain it, they will not be able to improve their SA, due to a lack of critical information and knowledge, and thus cannot make fully informed decisions.

The majority of the discussions on teamwork in fields such as organizational psychology, human factors, and social psychology assumes teams with tightly collaborative processes across minimal amounts of boundaries (e.g. collocated rather than geographical, without organizational boundaries, an implicit motivation to share information, etc.). However, the cyber environment offers numerous challenges and complexities, such as distributed workforces, organizational boundaries, and the desire to withhold information for the purpose of secrecy/classification levels, the "need-to-know," maintaining competitive advantages, and shielding outsiders from knowledge of their organization's deficiencies and vulnerabilities. In 2016 in the United States, the Federal Bureau of Investigation (FBI) Crime Complaint Center (IC3) listed a total of 350,000 reported cyber crimes and estimated this number represented only 15% of the total that occurred (FBI, 2016). This lack of information sharing within and across organizations has become a major decrement to our ability to maintain team cyber SA and perform cyber operations with relevant and timely information.

In such a distributed team environment, the question of how teams can and should share information for the purpose of situational awareness development is a critical question. With an existing deluge of data pouring in that cyber defenders are responsible for, providing too much external information (from other individuals) could result in information overload and have a negative impact on performance. On the other hand, too little information could result in poor decision making and continued persistent threats across the network.

When cyber SA is discussed there is a general understanding that the overarching categories revolve around awareness of the network, the adversary, and the current goals of the organization. While effective in communicating the cyber

SA at a general level, when applied to cybersecurity, these categories may be too broad. There is a clear research need for a better understanding of cyber SA across an organizational hierarchy. While there has been some work to better understand cyber SA (e.g. Tyworth et al., 2012, 2013), future work should focus on better understanding how cyber SA is distributed across the team and larger organization. During their interviews with cyber analysts and decision makers, Staheli et al. (2016) showed that across an organizational hierarchy, the types of decisions and information vary in term of scope and impact and better understanding the information needed to make those decisions has enormous impact. Such a focus could combine methods such as cognitive walkthroughs, contextual inquiry, and cognitive task analysis to social network and job analyses to extract what the critical cyber SA for each individual is and then chart the dependencies as they go across an organization.

As this understanding of cyber SA is formed, research can pivot to studying how assisted information sharing technologies can help cyber operators share and locate critical information to form cyber SA. In their development of the CARINA system, Staheli et al. (2016) applied a user-centered design approach to the development of a system that could help improve organizational information sharing. Building on this approach, researchers can leverage emerging AI technologies to help deliver up-to-the-minute information and break down organizational boundaries and hidden knowledge profiles that may emerge between cyber operators and organizations.

Table 6.1 provides a summarization of the exemplar challenges and associated research directions for team cyber SA in cybersecurity, as well as relevant citations from both cyber and team cognition literature.

TABLE 6.1
Summary of Challenges and Research Directions for Team Cyber SA

Challenge	Research Directions	Relevant Citations
Critical information sharing across geographic, functional, and organizational boundaries	• Cross-boundary mental model formation and alignment • Effective information sharing methodologies	Caltagirone et al. (2013) Caltagirone, Pedergast & Betz, 2013 Staheli et al. (2016) Tyworth et al. (2012)
Lack of explicit collaboration, rather relying on data sharing, collaborative systems, and incident reports to share information	• Develop new and understand existing boundary objects for cyber operations	D'Amico and Whitley (2008) Dillenbourg et al. (1995) Dyer (1984) Star and Griesemer (1989)
Lack of complete cyber SA within and across organizations	• Application of team cognitive models, such as transactive memory and team mental models, to cyber SA theory	Austin (2003) D'Amico et al. (2005) Gutzwiller et al. (2015) Klimoski and Mohammed (1994) Mohammed and Dumville (2001) Tyworth et al. (2012)

Practical Implications

Once the exact cyber SA needs of both the individual, team and organization, and their dependencies and interactions are better understood, we can begin to discuss improving the effectiveness of the teamwork. To understand and improve how collaboration occurs within the system, research must be able to identify and extract key boundary objects from the environment. Using this knowledge, researchers must focus on specific behavioral factors that impact information sharing and then prototype and develop information sharing applications and test them in both laboratory and field-based applications. Using a Living Laboratory approach (McNeese, Mancuso, McNeese, Endsley, & Forster, 2013), researchers can first build a baseline for the current state of information sharing within a team or organization and then leverage the knowledge on what their cyber SA needs are to develop reconfigurable prototypes and deploy them in synthetic task environments for iteration. Eventually they can develop operational prototypes to understand how they could impact and improve cyber SA at the individual, team, and organizational levels. This work can help lead to better tooling, both for individual and team-based cyber analysis.

Role Definitions and Staffing

Overview

Teams within cybersecurity can be composed of multiple individuals performing similar tasks, such as a team comprised of all host analysts. However, even within these seemingly homogenous teams, there can be a wide range of specializations with individuals having varying levels of expertise across the wide range of tools and software used within cybersecurity. Teams can also be comprised of multiple functional roles including forensic, threat, and intel analysts (D'Amico & Whitley, 2008; Zimmerman, 2014). Team composition, which is the balance of not only roles but individual characteristics including education, training, and experience, is an important factor in performance. In cybersecurity, however, there is a growing shortage of trained workers to fill positions. This shortage is causing ambiguity in roles and responsibilities as analysts have to complete tasks that should span multiple positions and it is causing increased workload and occupational stress. According to the 2017 Global Information Security Workforce Study, there will be a global shortage of 1.8 million cybersecurity workers by 2022 (ISC^2). A report by Herjavec Group (2017) predicts an even larger shortage, anticipating 3.5 million unfilled jobs by 2021. This gap between supply and demand has increased by 20% compared to a previous forecast made in 2015. The primary reason for the anticipated shortfall is a lack of individuals with the right training to fill positions. In a survey of cybersecurity and IT professionals (Oltsik, 2017), more than 50% stated that staff size in cybersecurity analytics and operations is currently inappropriate. Specific shortages are reported in the areas of proactive threat hunting, prioritizing and investigating alerts, and computer forensics. To fill the demand, it is estimated that one-third of those currently being hired in cybersecurity come from non-cyber, information technology, and engineering backgrounds.

Those without a cybersecurity background are learning on the job. While they are filling a need for more staff, they may not necessarily fit into a specific job role, which can lead to ambiguity in defining the roles and responsibilities of the current workforce. Staffing levels and role ambiguity are elements that could lead to occupational stress. Chappelle et al. (2013) conducted a survey of cyber operators, both active duty military and civilian contractors, and found that insufficient manning, inadequate tools, and keeping up with the rapidly changing threat environment and new technologies are contributing factors to workplace stress. In a survey of cybersecurity specialists at the National Security Agency, Paul and Dykstra (2017), found that both fatigue and frustration increased significantly across an operation. Increased stress can negatively affect both individual and team performance. An increase in staffing and the development of advanced human-machine teaming capabilities that can automate repetitive tasks are needed to tackle this growing challenge of staffing and workload (McCallam, Frazier, & Savold, 2017).

In 2010, the National Initiative for Cybersecurity Education was created to improve cybersecurity awareness education and workforce development (Newhouse, Keith, Scribner, & Witte, 2017; Paulsen et al., 2012). As part of this initiative the NICE Cybersecurity Workforce Framework was developed, which is comprised of three components to describe cybersecurity work roles. There are seven high-level groupings of cybersecurity functions. This includes the categories of Analyze, Collect and Operate, Investigate, Operate and Maintain, Oversee and Govern, Protect and Defend, and Securely Provision. Within the seven groups are a total of 33 specialty areas of cybersecurity work including areas such as Digital Forensics, Cyber Operations, and Vulnerability Management. Specific work roles are then broken down further into 52 categories that provide specific knowledge, skills, and abilities associated with each. Having this type of framework can aid in the development of training and education programs as well as individual job descriptions. However, the framework does not provide guidance on what the diversity of skillsets should be when developing a cybersecurity operations center, forensic analysis team, threat assessment team, etc. within an organization. Therefore, the diversity of individual skillsets that are required for completing certain tasks still requires further research.

Applications of Team Cognition

Given the shortage in cybersecurity workforce, it is essential that organizations are able to retain their staff. Role ambiguity is the lack of understanding in the tasks that need to be completed as part of one's job. Ambiguity about the expectations of a role tends to lead to job dissatisfaction (Kahn, Wolfe, Quinn, Snoek, & Rosenthal, 1964). Abramis (1994) conducted a meta-analysis of studies that examined role ambiguity and found a negative correlation of moderate effect between job satisfaction and role ambiguity. For job performance, analysis was performed separately for studies in which performance was assessed independently, such as supervisor ratings, and those in which performance was self-assessed. A negative correlation was found but it was weak and predominately for self-assessed performance only, suggesting that ambiguity may affect subjective evaluations of one's job but its effect on objective evaluations of performance needs further investigation (e.g. Driskell & Salas,

1991). Beauchamp, Bray, Eys, and Carron (2002) examined role ambiguity within the defensive and offensive responsibilities of athletes and found that ambiguity concerning the scope of responsibilities was the primary predictor of efficacy and performance. They also found that the relationship between ambiguity and performance was reduced when controlling for efficacy as a potential mediator. Similarly, in a survey of employees in a private sector company, Manas et al. (2018) found that role ambiguity negatively affected engagement at work. Decrease in engagement can lead to decreased individual performance, which can affect the team. Occupational stress due to ambiguity in roles and responsibilities can also affect team performance due to a restriction in attentional focus (Driskell, Salas, & Johnston, 1999). When under stress, an individual may experience information overload. This overload can result in an individual focusing only on their own task, neglecting group tasks and social cues that can then result in degraded team performance.

High team performance is dependent on the skillsets of each individual that makes up the team, which includes both functional and team skillsets. Belbin (1993) has defined nine different team roles including plant (creative, source of inspiration), resource investigator (discoverer), coordinator (maintains objectives, protocol), shaper (focused on achieving results), monitor/evaluator (analyzes ideas, decides after discussion), teamworker (holds team together), implementer (organizer), completer/finisher (ensures standards are maintained), and specialist. For these team skillsets there is inconclusive research on whether there is a relationship between the diversity of skillsets and performance. Van de Water, Ahaus, and Rozier (2008) found that there was no difference in performance between balanced and unbalanced teams according to Belbin's categories. However, they stated that the lack of finding could be due to unclear definitions on what a balanced team is. Similarly, Batenburg, van Walbeek, and der Mauer (2013) did not find that diversity of roles corresponded to higher performance. However, these studies were focused on teams' skills and not on the balance of functional knowledge within the teams.

Stewart (2006) conducted a meta-analysis of studies that examined the design or construct of teams and team performance. Heterogeneity was examined in the included studies for multiple characteristics including demographic, personality, and background characteristics including education and revealed little effect on team performance. Aggregated characteristics of a team though including expertise were found to have a positive correlation with performance.

Constructing a team by balancing the skillsets across team members is just one of four team composition models described by Mathieu, Tannebaum, Donsbach, and Alliger (2014). The other three models described include the traditional personnel–position fit model which assumes that teams will be more effective if individuals have the knowledge, skills, and abilities for their respective positions: the personnel model with teamwork considerations, which is based on the idea that team performance is improved through team-related competencies including coordination, communication, leadership, and decision making. This model suggests teams that possess more generic team-related skills will be higher performing than teams with less team skillsets. The fourth model is a contribution model, which assumes that characteristics of a specific individuals may contribute more or less to team performance than others due to their roles and responsibilities.

Which model though leads to highest team performance is inconclusive and more research is needed.

Role ambiguity and team composition can also impair a team's shared mental models. Job dissatisfaction can lead to increased turnover rates which will make it difficult for teams to form shared mental models. If groups have a shared understanding and knowledge of a situation they are more likely to work in a coordinated manner (Klimoski & Mohammed, 1994). Teams that have expertise and experience in common are more likely to process information and act in common ways. Edwards, Anthony Day, Arthur Jr., and Bell (2006) examined the similarity and accuracy of team mental models and how it relates to performance. If a mental model is accurate it is expected to also be similar across a team. However, it is possible that a team may have the same mental model but it is not correct. As expertise increases across the team, it is expected that both accuracy and similarity of the team's mental model will increase. Edwards et al. (2006) examined the performance of three teams with difference expertise levels and found that approximately one-quarter of the variance in team performance was accounted for by the team skillset/expertise composition.

Research Implications

Further research is needed on the skillsets and job roles of cybersecurity teams. Little research has been done on the individual skillsets on a team that will lead to improved performance. Henshel et al. (2016) examined training certifications, education of team members, and performance in cyber exercises and found that having college as the highest level of education and having obtained a cybersecurity training certificate was significantly related to proficiency metrics including the time from inject to the approval for taking action. However, it is not only cyber-specific skills that need to be studied. Ben-Asher and Gonzalez (2015) found in a laboratory study that there was no difference in the ability to detect network attacks between individuals who were considered experts in cybersecurity and novices who had little to no expertise in cybersecurity. Potential explanations for the lack of difference between experts and novices in identifying attacks is that knowledge needs to include both situational knowledge of the environment and domain knowledge. Experts may have a hard time identifying attacks when they are unfamiliar with the network layout and baseline activities within the network. However, it also suggests that further work is needed in cyber on understanding how individuals accumulate information during a decision-making process and what basic cognitive skills are related to successful threat detection.

To fill the current staffing demands, people are entering cybersecurity from other fields. It could be useful to use cognitive aptitude tests to evaluate these candidates for traits that might indicate that they would be successful in the field. Selecting individuals with the right skillsets will lead to improvement in overall performance in a cyber team. A cyber aptitude model has been proposed by Campbell, O'Rouke, and Bunting (2015) and accounts for both critical thinking and job-specific knowledge. For job-specific knowledge, they used the NICE framework discussed in the previous section. For the critical thinking component, they indicated measuring four components including proactive and reactive thinking ability and real-time and deliberate action ability. Further research on which cognitive abilities are most

TABLE 6.2
Summary of Challenges and Research Directions for Role Definitions and Staffing

Challenge	Research Directions	Relevant Citations
Lack of staffing is leading to ambiguity in defined roles and responsibilities within cybersecurity teams	• Understand skillsets and job roles of high-performing cybersecurity teams	Ben-Asher and Gonzalez (2015) Henshel et al. (2016) Oltsik (2017)
Many individuals entering cybersecurity have no prior experience in the field	• Identify cognitive attributes that are associated with high-performing cyber analysts	Campbell et al. (2015) Oltsik (2017)
Varying skillsets and experience levels make it challenging to distribute work	• Development of capabilities for improving distribution of workload across teams	Gersh and Bos (2014)

important for success in the field of cybersecurity, such as pattern recognition, vigilance, and spatial visualization, is needed. Tests for these abilities should be identified or developed and evaluation of performance of individuals determined to have high aptitude based on cognitive skills is needed.

Once a team is formed, it is important to adequately allocate workload across the team. Clearly defining roles and responsibilities can lead to improved work allocation. Further research is needed on the development of tools to improve the triaging of events across analysts so that if one analyst becomes overburdened the workload can be shifted in order to improve overall performance. Novices working in cybersecurity are biased to thinking that most alerts are real and need investigation, while more experienced analysts think about alert criteria, probability of an event, and thresholds for events to trigger when making a judgment (Gersh & Bos, 2014). Novices may spend significant amounts of time investigating alerts that are false alarms, increasing the workload of more senior analysts. Development of tools, particularly larger capabilities used for intrusion detection and prevention, that can help guide and provide assistance to novices as they are learning on the job can aid in the distribution of workload across operators with a range of experience levels.

Table 6.2 provides a summarization of the exemplar challenges and associated research directions for role definitions and staffing in cybersecurity, as well as relevant citations from both cyber and team cognition literature.

Practical Implications

The tactics, techniques, and procedures (TTPs) used by adversaries continues to rapidly change, and with that the diversity of skills required of cyber operators. Teams need to have a heterogeneous set of task and teamwork skills and need to work together in a collaborative way to quickly and efficiently identify and mitigate

threats. While frameworks are being developed defining the knowledge skills and abilities for specific job roles, further work on the development of guidance is needed for the skillsets that should make up specific teams within cybersecurity. It is estimated that for every 5,000 alerts, almost 12% are legitimate events that are never investigated or remediated due to lack of staffing (Cisco, 2017). To increase the size of the workforce in cybersecurity, both task-specific knowledge and relevant cognitive skills that are related to high performance should be considered.

Hand-Offs and Cross-Site Coordination

Overview

Hand-offs are the transition of information and responsibility from one individual to another. In cybersecurity, an alert could involve coordination and collaboration across analysts requiring multiple hand-offs within an investigation. These hand-offs may occur within a team or across the organization. Information on an incident may be submitted to an IT or security help desk by a user, with information on time, location, and sequence of events being transferred to an appropriate analyst for investigation. During an investigation there may also be hand-offs among analysts who are jointly working on different components or aspects of the same incident. Depending on the nature of the alert, multiple skillsets may be needed with for example network, host, or forensic analysts jointly working together. Key information needs to be shared in order to effectively complete the investigations, with frequent hand-offs occurring based on evidence found.

Hand-offs of information may also occur across shifts. In some organizations, security operations centers (SOCs) operate 24/7. During shift changes hand-offs of investigations occur from one analyst to another so that they continue to be handled efficiently without delay. It is important that during the hand-off information is accurately provided so that there is not duplication of work that has been already conducted. Daily update briefings may also occur within an organization, in which information on key investigations is shared across entire teams. Such briefings provide opportunities for all individuals including leadership to have shared situational awareness of key events and for coordination across the team. Larger organizations may be geographically dispersed with coordination and information sharing needing to occur across sites. Different sites may have their own workflows and procedures leading to challenges in coordination.

The hand-off of information is not only necessary within an organization for handling an incident—cyber intelligence needs to be shared across organizations. There are many tools and frameworks such as MITRE's Structured Threat Information Expression (STIX), Common Vulnerability Reporting Frame (CVRF), etc. (see also Asgarli & Burger, 2016) that have been and are being developed. These frameworks do not necessarily use the same conventions, which impairs the ability to share information and improve overall performance across multi-organization teams including government agencies, universities, and commercial companies.

Every hand-off of information is a potential source of error in an investigation. Miscommunication can lead to events being mishandled or an investigation being delayed. Hand-offs between shifts are common in other fields, particularly in

hospitals, where hand-offs of patient care occur daily. It has been found that 80% of severe medical errors are attributed to miscommunications during the hand-offs of patient care (Joint Commission, 2012). Effective communication across teams is therefore essential throughout the investigative process. There are many methods currently in use in cybersecurity to transfer information. Information may be transferred verbally during face-to-face or phone conversations. Information is often shared electronically using chat tools and email, or more formal ticket systems may be used in which key information fields are filled out at the start of the investigation, with updated information added throughout the investigation. To effectively convey information, it is important for team members to know the roles, tasks, and information requirements of the other analysts (Cannon-Bowers & Salas, 1998).

Applications of Team Cognition

Hand-offs of information have been studied often in relation to patient care in the medical field. Keebler et al. (2016) conducted a meta-analysis that examined the use of different hand-off protocols and found that the amount of information provided during a hand-off increased after a formal protocol was implemented, which resulted in improved patient outcomes and overall improved satisfaction with the hospital or organization. However, Jiang et al. (2017) found conflicting results, with an increase in reported discrepancies in patient care when an electronic hand-off tool was implemented. This result suggests that any hand-off procedure needs to be thoroughly tested and training provided to all staff. In addition, process-oriented changes are also needed to improve the overall hand-off procedure of information.

Hand-off protocols serve as prompts, providing the categories of information that should be included. Having a standard protocol can lead to reduced cognitive bias among individuals on what information should be shared. Cybersecurity analysts examine a high volume of alerts every day, many of which are false positives. Einhorn and Hogarth (1978) state that outcomes are coded based on frequencies. Therefore, based on past experiences, some analysts may be prone to not share information on certain alerts as they are confident based on the frequency of past events that it is a false alarm.

The complexity of information sharing is increased when teams are located across sites or when teams only communicate virtually. O'Leary and Cummings (2007) stated that outcomes of geographically dispersed teams are in general negative, with reduced communications and real-time problem solving and increased coordination complexity. However, there are some potential positive outcomes, such as the sharing of non-redundant information. Espinosa, Nan, and Carmel (2015) examined what aspects of geographic dispersion may affect team performance. Participants completed a map creation task and communication was completed through an electronic chat tool. They found that temporal distance did correlate to an increase in the time it took to complete a task and that distance was negatively associated with accuracy and quality. They found that distance had no effect on the conveyance of information, rather it was positively associated with communication frequency and negatively associated with turn-taking, while both frequency and turn-taking had a positive effect on the convergence of information. Therefore, the results suggest that it is not necessarily the distance but the pattern of communication that impacts team performance. This

is supported by Marlow, Lacerenza, Paoletti, Burke, and Salas (2018) who found that frequency and quality of communications among teams is positively related to performance, with a stronger relationship for communication quality.

Oshri, van Fenema, and Kotlarsky (2008) mentioned that communication technologies are not enough to prevent breakdowns in coordination/communication between sites. Rather, there needs to be trust and ties between teams to facilitate information sharing between sites. Distributed sites will often have their own processes. They investigated transactive memory for two projects which had globally distributed teams. As discussed previously, transactive memory is a combination of communication between individuals and the memory processes of individuals (Wegner Erber, & Raymond, 1991; Wegner, 1995) and is tightly linked with team performance, as individuals know who to refer to for specific information. Without co-location or periodic training, however, it may be hard to develop a transitive memory system. Oshri et al. (2008) found that for globally distributed teams, using standard templates helped with obtaining the appropriate information and then transferring it to the other teams. Hansen (1999) had similar findings, in that for the sharing of complex information strong ties are needed within subunits of an organization. For distributed or multi-team systems it is therefore important to have formal mechanisms defined for meetings, schedules, timelines, and other forms of communication for them to be effective (Shuffler & Carter, 2018).

Information sharing during hand-offs should not only contain factual information but an individual's sensemaking of the situation. Uitdewilligen and Waller (2018) examined information sharing in 12 multidisciplinary crisis teams. As part of their study they examined a model of information sharing that includes fact sharing, interpretation sharing, which is a combination of the individual's expertise and their interpretation of events, and projection sharing, which is the sharing of information regarding anticipated or potential future events. High-performing teams spent more time sharing information before making decisions and they also had more sharing of interpretations, i.e. individuals working together to make sense of the situation, than low-performing teams. Faraj and Xiao (2006) examined coordination within a trauma setting. Based on observations and interviews they defined two types of coordination. The first type of coordination is *expertise coordination*, which is related to managing the knowledge and expertise of individuals. This involves knowing who to coordinate with for crucial knowledge, essentially knowing the expertise of team members. In cyber, this could involve knowing who to coordinate with to conduct host-based analysis, to analyze network packets, etc. The other type of coordination is *dialogic coordination*, which is more contextually based and may be unpredictable. As an investigation unfolds, actions may be less predictable, and it may be necessary for skill-based boundaries to be discarded and everyone to coordinate together to solve the problem.

Research Implications

There are multiple methods that are currently used to hand-off investigations. Hand-offs can occur synchronously with information being communicated verbally in person or over the phone, or virtually using chatrooms. However, the majority are likely occurring asynchronously using tools such as ticketing systems or other collaborative

TABLE 6.3
Summary of Challenges and Research Directions for Hand-Offs and Cross-Site Coordination

Challenge	Research Directions	Relevant Citations
Hand-offs occur often across shifts and across analysts during an investigation	• Development and testing of incident hand-off procedures	Keebler et al. (2016) Jiang et al. (2017)
Teams can be globally distributed, each with their own procedures	• Development of tools to improve the sharing of information and communication for distributed cyber teams	Espinosa et al. (2015) Marlow et al. (2018) O'Leary (2007) Shuffler and Carter (2018)
Fact-only-based information shared across teams could lead to misunderstanding or lead to decisions being made based on prior experience	• Research is needed on the content of information that is shared within hand-offs and within information sharing tools; this includes both fact-based information and sensemaking information	Einhorn and Hogarth (1978) Farah and Xiao (2006)

tools. Studies should be conducted examining how different information sharing tools and their level of synchronicity affect communication patterns and ultimately performance in incident handling. Information or collaborative tools are not only useful for sharing information. They can also provide a workspace where individuals can provide information on their searches, analysis methods, and findings. The utility of a such a tool is based on the opportunistic problem-solving model (Hayes-Roth, Hayes-Roth, Rosenchein & Cammarata, 1979) and the architecture for a similar concept that supports collaborative planning has been developed (DeStefano, Lachevet, & Carozzoni, 2008). This has the benefit of allowing the individual to offload their working memory as they may be working on multiple investigations at the same time and it provides a space for multiple analysts to work together, aiding collaborative sensemaking.

Table 6.3 provides a summarization of the exemplar challenges and associated research directions for hand-offs and cross-site coordination in cybersecurity, as well as relevant citations from both cyber and team cognition literature.

Practical Implications

Having a hand-off protocol could reduce reporting bias. Every individual may not consider information to be of the same priority level which can result in high variability in the information that is provided during hand-offs. Having a set protocol can lead to improved shared mental models across staff, as everyone will have an understanding of what information is considered of high importance. However, there can also be negative consequences to standardizing hand-off protocols. Reporting information in a standard format may require more time, further increasing the workload of analysts who are already dealing with high volumes of daily alerts to investigate. In addition, if the hand-off procedure is too rigid, information that may be unique to a specific investigation may not be shared as it does not fit within the protocol. As new threats continue to emerge, it is essential that any procedure allows

for flexibility. There is a need for structure for formal coordination and clearly defining responsibilities, however it needs to be a flexible structure that can handle the rapid response needed for incident response in cybersecurity.

Team Measures

Overview

Performance in cyber, like many other topics, is currently considered to be a technological problem. When a new tool or capability for cybersecurity is deployed, individuals have an in-depth understanding of the performance of the technology, how much memory it uses, how much data it requires, its processing speed, etc., with limited insight into the impact on the human. At best, subjective and outcome-based measures are relied on, but more often than not human performance is simply ignored all together.

Measuring human-centered outcomes in cyber is a major challenge. Similar to safety science, cybersecurity metrics are often grounded in outcome: was the threat removed, was there information spillage, what was the data loss, etc. While these types of measures are important in understanding the overall security posture of an organization, they provide little to no real-time feedback to analysts or their supervisors to help them regulate their behaviors and change their processes or strategies. Currently, analysts have to rely on their own instincts to regulate their behaviors or wait for after-action reviews to provide them with feedback on their performance. However, a problem still arises in that if the adversary continues to go undetected, the analysts and organization may have no idea that they are performing poorly, and may continue down that path until it is too late.

Human-centered cyber metrics have major implications on the design, implementation and analysis of cyber exercises, which are becoming common ways to test and field new capabilities and provide training to cyber analysts (Patriciu & Furtuna, 2009; Sommestad & Hallberg, 2012). Whether exercises are fielded for the purpose of evaluation, competition, or training, the understanding of human processes, behaviors, attitudes, and performance is critical.

For evaluation there is a desire to understand the performance of a team with and without a certain tool. In this case, the measures of performance are critical in better informing the continued development or acquisition of future cyber capabilities for that team. In competitions, there is a desire to measure the skills of individuals and teams so that at the conclusion of an event, an assessor can make a judgment on the efficacy of a team and their ability to complete a task. For training, performance is important in showing an improvement to an individual or team and understanding their processes can shed light on their knowledge, skills, and abilities in conducting their tasks. At the conclusion of a cyber exercise, participants are provided with a "hot-wash" of their performance. Currently, much of this is based on performance outcomes: did they find the attacker, did they document the evidence, etc., and sometimes based on augmented subjective ratings by subject matter experts. However, without clear performance and process metrics, participants are unable to understand how their processes and actions may have impacted these outcomes and have no way in the future to regulate their behaviors to improve performance.

Additionally, from a technology development standpoint, outcome measures provide limited insight into how the capability impacted performance. It is possible that the team came to the correct conclusions while using the tool in an incorrect way, or by chance. By leveraging only outcome measures, a team may be assigned a good or bad score, without full insight into whether or not they achieved those outcomes in a positive manner. This could lead to a team forming a poor metacognitive awareness mental model and not regulating their behaviors in situations where they achieved a high score while using incorrect processes, or over-regulating if they used correct processes but achieved a low score (Dinsmore, Alexander, & Loughlin, 2008).

Applications of Team Cognition

Performance itself is typically an outcome-based measure, thus it is important to not only collect accurate performance metrics, but to identify its antecedents and collect appropriate metrics at each level. Typically, in the literature, when discussing different types of team-level metrics, they look at two other areas in addition to team performance, specifically team attitudes and behaviors (Cohen & Bailey, 1997). Based on varying mediation and moderating effects of the team's attitudes and behaviors, team performance represents the outcomes of team collaboration, that is, how well they performed in a given task. Team attitudes, or perceptions, typically capture a team's collective reaction to the teams functioning and performance. Team behaviors include any interpersonal aspects of their collaboration, including communications, planning, and coordination.

Team Performance

Team performance metrics aim at capturing indicators of a team's efficacy at completing a given task. Measuring team performance is very challenging and the difficulty increases with task complexity. In simple laboratory tasks, measures such as accuracy and reaction time may be sufficient indicators in how well an individual is performing, however it is unknown how they may scale to a more naturalistic environment in which the tasks are not as controlled. Regardless, there is no individual silver bullet, as measures need to be combined with other environmental variables to provide a more tangible performance score. For example, the Human Performance Scoring Model (HPSM; Wellens & Ergener, 1988), which interprets team interactions into measurable actions against simulated events based on their accuracy and reaction time, has been used in numerous team-based environments (e.g. Hellar & McNeese, 2010; Mancuso, Minotra, Giacobe, McNeese, & Tyworth, 2012). When moving to more complex tasks, team performance becomes more nuanced and requires a combination of outcome measures with online task-specific knowledge that has direct ties to team performance (i.e. Baker & Salas, 1997; Cannon-Bowers & Salas, 2001; DeChurch & Mesmer-Magnus, 2010; Mathieu, Maynard, Rapp, & Gilson, 2008). These types of measures require a subject matter expert to extract critical information or procedural knowledge from the task and quiz participants on it, with the assumption that if they possess it, they will be making positive progress in their task. For example, the Situation Awareness Global Assessment Technique (SAGAT; Endsley, 1988) queries a team (or individual) on

critical knowledge that represents each level of situation awareness that is critical in performing a task. Similarly, accuracy and similarity grids can be used to elicit indicators on the team's mental model during a task session (Cooke, Salas, Cannon-Bowers, & Stout, 2000).

While any individual measure may not provide a full picture, triangulation across measures can provide a more robust picture of team performance. By picking multiple methods, one does not only capture the team performance outcome (as would be the case with a mission performance metric), but additionally captures aspects of the team processes that lead to that outcome and the team's interpretation of their actions. When combined, one can form a complete understanding of the team's performance, how they accomplished their goal, and their mindset in doing so. Such information can be critical in not only evaluating, but also in training and improving team performance and processes.

Team Attitudes

Team attitudes may be the most commonly captured team measurement, possibly due to their ease of use, as they are most often delivered as a survey instrument. Many of the metrics used to assess team attitudes are grounded in research on individuals, however their importance is often magnified when moving to the team level (Cannon-Bowers & Salas, 2001).

One important team attitude that has been shown to impact performance is team emotional state or affect (e.g., Mathieu et al., 2008; Schwarz, 2000). The Positive and Negative Affectivity Scales (PANAS; Watson, Clark, & Tellegen, 1988), and its expanded version the PANAS-X (Watson & Clark, 1999), are the most popular metric for capturing affect. Perceived stress is another example of another team attitude that has been shown to be relevant in assessing team behavior and performance. A common assessment of stress is the Dundee Stress State Questionnaire (DSSQ; Matthews et al., 2002) and its shortened version the Short Stress State Questionnaire (SSSQ; Helton & Garland, 2006). Both the DSSQ and SSSQ are based on Mathews et al.'s (1999) three factors of stress—worry, distress, and engagement—which have been shown to have a correlation with performance. Another construct which shares commonalities with stress that is also relevant to team tasks is workload. To assess workload researchers often utilize the NASA Task Load Index (NASA-TLX; Hart & Staveland, 1988). More recently, Helton, Funke, and Knott (2014) proposed a modified NASA-TLX that includes an additional six items to account for the collaborative requirements of teamwork. Other tools for assessing workload in individual and team tasks include the Bedford Scale (Roscoe, 1987), the Cooper Harper Scale (Cooper & Harper, 1969), the Subjective Workload Assessment Technique (SWAT; Reid & Nygren, 1988) and the Subjective Workload Dominance Technique (SWORD; Vidulich, Ward, & Schueren, 1991), and the Workload Profile (WP; Tsang & Velazquez, 1996).

Team attitudes can also focus on perceptions of cognitive activity, which is shown to be separable from, but equally as important as actual cognition (e.g. Endsley, Selcon, Hardiman, & Croft, 1998; Rousseau, Tremblay, Banbury, Breton, & Guitouni, 2010). Numerous metrics of perceived situation awareness have been applied at the team level, such as the Situation Awareness Rating Technique (SART;

Taylor, 2017), the Crew Awareness Rating technique (CARS; McGuinness & Foy, 2000), the Mission Awareness Rating Technique (MARS; Matthews & Beal, 2002), the Situational Awareness Rating Scale (SARS; Waag & Houck, 1994), and the Situation Awareness Subjective Workload Dominance Technique (SA-SWORD, Vidulich & Hughes, 1991). Perceived situation awareness has been shown to have interacting and mediating effects with actual situation awareness and team performance, and thus has been identified as a critical measure to capture when considering situation awareness in team tasks (Hamilton, Mancuso, Mohammed, Tesler, & McNeese, 2017).

Finally, a team's perceptions of themselves, sometimes referred to as *team viability* (Mathieu et al., 2008), is an important construct in metacognitive regulation of team behaviors. Such attributes are often considered one of the most important antecedents of effective group work (Beal, Cohen, Burke, & McLendon, 2003). These metrics relate to opinions on how well the team perceives their ability to work together and complete their task. The Group Environment Questionnaire (GEQ; Carron, Widmeyer, & Brawley, 1985) has been the standard in measuring cohesion in groups. The survey accounts for four factors of cohesion, group integration, and attractions in regard to task and social work (Cota, Evans, Dion, Kilik, & Longman, 1995). Other metrics that may be captured to assess the team viability include collective efficacy (Riggs & Knight, 1994), perceived collaboration (Lyons, Funke, Nelson, & Knott, 2011), and trust (MacDonald, Kessel, & Fuller, 1972; Mayer & Davis, 1999) to name a few.

Team Behaviors

While the performance and survey metrics described in the previous section can give insight into team knowledge and performance and the team's perceptions of their interactions, they do not account for their actual behaviors. Methods including observer evaluations and communication analyses can capture important aspects of team behaviors. Such metrics are especially useful in complex situations, such as field exercises (e.g. Matthews & Beal, 2002) or real-world situations (Mazzocco et al., 2009), where surveys may not be administered and the experimenter may not have the control necessary to implement metrics for performance.

There are two ways of capturing team behavior from observable ratings: global rating scales and frequency of behaviors. Global rating scales, also known as behaviorally anchored rating scales (Kendall & Salas, 2004), rely on observers to identify key behaviors linked to performance and subjectively rate their effectiveness at that time. An example of this is the Anti-Air Warfare Team Performance Index (Johnston, Smith-Jentsch, & Cannon-Bowers, 1997), in which a subject matter expert identifies key behaviors that indicate superior, adequate, and poor performance. These require observers to simply rate the frequency of various critical actions, without having to make a subjective judgment on the quality.

In addition to their performance-based and survey form, several metrics can also be calculated based on observer ratings. For example, the Situation Awareness Behaviorally Anchored Rating Scale (SABARS; Matthews & Beal, 2002) is an observer rating technique that has been used to assess live infantry exercises. Other attributes of team interactions that have been measured through subject

matter expert evaluations include team transactive memory (Smith, 1999), learning (Edmondson, 1999), team coordination, and cohesion (Brannick et al., 1993). In addition to capturing metrics on team interactions, observations can also be used as a way to give insight into the performance of a team during a task (Brannick, Roach, & Salas, 1993).

In an effort to reduce some of the subjectivity, team communications can also be used to understand a team's cognitive and collaborative behaviors (Salas, Bowers, & Cannon-Bowers, 1995). Researchers have posited that enhanced metrics on team communication are the best indicators of team cognition (Cooke, Gorman, Myers & Duran, 2013). Commonly used metrics such as frequency counts or discourse durations can provide information about the amount of information that is being shared during a team task (Volpe, Cannon-Bowers, Salas, & Spector, 1996). These however do not account for the content of the communication, which would require external coders and may introduce subjectivity. Several researchers often rely on task-based coding schemes and include categories that are specific to the given task (e.g. Russell, Funke, Knott, & Strang, 2012). However, more general coding schemes can also be used, such as Entin and Entin (2001) and can help facilitate analyses such as anticipation ratios (overall, action, and information). These ratios can provide useful metrics for understanding team cognition by indicating whether teams spend more time anticipating the needs of their team or have to request their needs specifically.

Research Implications

Many of these measures have been validated in both laboratory and field contexts, however they have limited use and almost no validation within the context of cyber. In methods such as SAGAT, there must be a critical understanding of the environment such that an expert can extract key information requirements that map to Level 1, 2, and 3 SA (Endsley, 1988). The question of what is important for cyber SA is still open and important (Bardford et al., 2010). Several researchers have attempted to provide frameworks (e.g. D'Amica et al., 2005; D'Amico & Whitley, 2008; Champion et al., 2012; Gutzwiller et al., 2015, 2016), however many of these serve as one-off characterizations of a particular mission set. From a naturalistic viewpoint, a subject matter expert can articulate what they think is important in a task, but without a common understanding and framework for mapping, the results are not generalizable or comparable across studies, making the measure only useful within an individual assessment. Continued research should focus on developing frameworks that support previous work in team measurement so that findings across studies can be compared, allowing for a broader understanding of the role of team knowledge, attitudes, behaviors, and performance in cybersecurity tasks.

Another critical detail that must be discussed is the issue of ecological validity and applicability. While many of these measures have been tied to team performance in the lab and in several contexts, the unique nature of the cyber environment may have implications for how an instrument is used or its outcome. For example, an instrument like SAGAT is dependent on online knowledge of specific task critical information. In cyber, it is often the case that analysts rely on information repositories or other distributed cognitive artifacts. In this situation, it is not exactly critical to know and possess specific pieces of information, but rather, to know and understand

where it is located, resonating with previous work on transactive memory (Wegner et al., 1991) and distributed cognition (Hutchins, 2006). This type of knowledge, of where to find information, can have similar performance effects as actually possessing the information and can also be used as an indicator of complete situational awareness (Sparrow, Liu, & Wegner, 2011; Stanton et al., 2006). Future research should conduct studies to better understand how previously validated measurements and instruments translate within cyber environments. This will help us better understand the greater theoretical underpinnings of each measurement and help produce generalizable instruments that can be used in cyber team research.

Table 6.4 provides a summarization of the exemplar challenges and associated research directions for team measurement in cybersecurity, as well as relevant citations from both cyber and team cognition literature.

Practical Implications

Many of the measures and metrics discussed in this section were designed and are often used in laboratory or controlled exercise settings. While they may not be ready for field use, cyber practitioners should begin to leverage previous work discussed here and elsewhere in collecting human-centered data during their assessments. Tool developers should be using situation awareness instruments to ensure that their users are able to obtain or locate the critical information in their tool, and use their findings to make interface updates and changes. Similarly, exercise developers, whether

TABLE 6.4
Summary of Challenges and Research Directions for Team Measures in Cybersecurity

Challenge	Research Directions	Relevant Citations
Performance in cyber is considered mostly from the technological perspective	• Triangulation across multiple measures (including technological) to develop more holistic and robust team performance measures	Baker and Salas (1997) Cannon-Bowers and Salas (2001) DeChurch and Mesmer-Magnus (2010) Wellens and Ergener (1988)
Current measurement techniques are often provided after the fact and provide little insight into team processes, procedures, or other intangible elements of teamwork.	• Correlation and development of team affect, stress, and workload scales to tangible outcomes in cybersecurity • Development (or extension of existing) of cyber team viability and cohesion instruments	Beal et al. (2003) Helton et al. (2014) Helton and Garland (2006) Lyons et al. (2011) Mathieu et al. (2008) Riggs and Knight (1994) Schwarz (2000)
Lack of ecological validity and applicability to cyber environments for existing measures	• Validation of existing instruments in high-fidelity environments (i.e. cyber exercises) • Development and validation of subject matter expert derived instruments (i.e. SAGAT) for general cyber tasks	Matthews and Beal (2002) Mazzocco et al. (2009) Patriciu and Furtuna (2009) Sommestad and Hallberg (2012) Sparrow et al. (2011)

for competition or training, should use the deluge of knowledge across the team literature and human sciences to begin to implement more rich metrics into their events. Cyber events could be a great opportunity to team with human factors and psychology researchers to help better understand cyber analyst processes and behaviors, and in turn, they could help the exercise developers with the design of these activities. As the research in these measurements becomes more mature and less invasive, a discussion on how to best implement into operations for the purpose of monitoring and organizational efficacy can then begin.

FUTURE DIRECTIONS FOR TEAM COGNITION IN CYBER

In this chapter, we have aimed to provide an overview of the current challenges for teamwork and team cognition that exist within cyber operations and security. However, as cyber is a digital domain, it also exists on the forefront of technology adoption. With this continued evolution, the issues of AI-human interaction and human-machine teaming are a growing challenge, with which many of the issues discussed in this chapter will overlap. As technology and the cyber environment continue to evolve, the reliance and presence of advanced and intelligent technology will also continue to grow. While we will most likely never reach a point in time in which technology will fully replace the human, technology working alongside humans is becoming more of a reality. With a move towards human-machine teaming, new research questions emerge, which team cognition may be especially suited to address. Many of the behaviors discussed in this chapter on how humans interact with others, such as team compositions, hand-offs, information sharing, etc., will still exist, however, between a human and a machine. This raises new questions about the role of team cognition in these environments: Is a human working with a machine a team? Does their cognitive structure exist as an individual or a team? What are the dynamics that exist between the collaboration? Before we can address these, we must first take a step back and understand what human-machine teaming is and identify paths for future exploration.

While human-machine teaming may be the new "hot" term, coupled with artificial intelligence, researchers have been discussing similar topics for well over a decade under the names automation and autonomy. Research recognizes automation across a spectrum, which ranges from the human doing everything to the computer being completely autonomous (Miller & Parasuraman, 2003). Much previous work does not necessarily deal with the autonomations or autonomous systems possessing "intelligence," however many of the same issues that plague human-machine teaming, such as trust, are equally as pervasive.

While we are not at the point where we have a full array of intelligent agents working alongside humans in cyber, within this spectrum, cyber has long relied on autonomous systems. Among the many types of automation in cyber, there are systems that automatically prioritize alerts based on a set of rules, systems that analyze files for potential malware, and algorithms that detect anomalous activity based on packets, connections, log-on events, and other data streams. There is also ongoing work to automate the processes of analysts through playbook-type workflow tools (Applebaum, Johnson, Limiero, & Smith, 2018), however, in most cases systems are

providing information to the user and the user needs to review the results and decide on and implement an alternative action. The systems are providing recommendations but human and machine are not currently working as a team.

As these advance and mature, human-machine teaming can lead to improved performance if machines provide assistance in areas that are cognitively demanding for humans. One area is by improving the performance of novices by guiding them within a tool. Silva, Emmanuel, McClain, Matzen, and Forsythe (2015) had both novice and experts complete a forensic puzzle game, in which they had to answer questions regarding snapshots from different cyber tools. Results of the study were preliminary, however, using eye tracking they found that novices took longer to find the information of interest compared to experts. Further research is needed on features that can be added to tools to improve the performance of analysts with less experience. Automation and human-machine teaming could also help in areas that are difficult for all experience levels such as in identifying infrequent events. Sawyer and Hancock (2018) conducted an experiment in which participants interacted with an email testbed, in which they had to detect malicious emails. The rate at which malicious events occurred was of one of three levels: 1%, 5%, or 20% of the time. They found that response accuracy and response time was lowest for malicious events that occurred only 1% of the time compared to 5% and 20%. This is an exemplar where an AI teammate can be useful in augmenting human performance.

The cyber environment has unlimited potential for such capabilities and human-machine teaming. Cyber analysts need to integrate information from multiple data streams over wide time windows. Turner and Miller (2017) stated that studies are needed in which performance is examined when automation is used for intuitive processes, which are processes that do not involve working memory, and analytic processes, which are serial and affect working memory, in order to understand how different levels of automation affect an individual's ability to fuse information received. Without the appropriate assistance, it may be difficult for an analyst to piece together information from different analytic tools to identify malicious events. Having an agent that could pivot between tools and correlate information could aid the work of a human analyst. Based on the information gathered, there is also the potential for automating courses of action to further reduce the workload of human analysts. Russel and Norvig (2013) defined a taxonomy of agents that determine a course action, including simple reflex agents, which use only current information to make decisions, model-based agents, which infer actions based on model outcomes/predictions, goal-based agents, which determine an action in order to contribute to an overall goal, utility-based agents, which determine a course of action based on its desirability, and learning-based agents, which determine a course of action based on passed outcomes.

For a human-machine team to be most effective, the machine or agent needs to be trusted and found acceptable by its human counterpart. While a machine is able to respond and provide information instantaneously, this might not be beneficial as the timing of automated activities needs to be appropriate. If a machine presents information too quickly, a human analyst will be unable to interpret the results and decide on a response fast enough or will possibly reject the results as incomplete. If the machine though takes too long to complete its computations, the human analyst

might ignore the machine agent, interpreting and deciding on courses of action on their own (Goodman, Miller, Rusnock, & Bindewald, 2016). Another important factor for the acceptance and use of automated capabilities is trust. Schaefer, Chen, Szalma, and Hancock (2016) conducted a meta-analysis of 30 studies to examine trust in automation and moderating factors. Emotive factors such as attitudes, comfort, and satisfaction with automation were the human traits that had the strongest effect size on the development of trust. Automation capability and behavior were the most important machine traits that affected trust. Hillsheim et al. (2017) found that trust in automation is also dependent on workload, with a higher workload associated with lack of trust of an agent. An agent may be viewed as untrustworthy if an individual's workload increases as a result of the agent. Lyons and Stokes (2012) found that trust and reliance in information is also modified by risk. They examined reliance on machine versus human when conflicting information is received for different levels of risk. Within the task they had to decide which route to send a military convoy based on route parameters, a tool that provided information on historical threats, or a human aid that provided a report based on intelligence. They found that high risk resulted in less reliance on the human aid. Studies examining the use of automation when making judgments during high- and low-risk cyber operational environments needs to be evaluated.

Like the discussion on performance for regular teams, performance of human-machine teams will need to be evaluated to determine if and how different types of automation improves cyber incident response. Damacharla, Javaid, Gallimore, and Devabhaktuni (2018) defined three metrics for benchmarking performance for human-machine teams. One metric is productive time, which is the total time of both autonomous and manual operation. The second metric was cohesion, which is a measure of how well a group remains united when completing tasks. One method for measuring cohesion is communication patterns. The final metric is the number of interventions needed to correct errors made by the machine. These metrics have not been studied in-depth for human-machine teams and testing and validation of all three metrics as well as development of additional performance metrics is needed.

This section aimed to provide an initial overview of automation and human-machine teaming literature, not an exhaustive list. We have provided initial potential directions for applying team cognition and automation to cybersecurity, but there is unlimited potential for researchers to address. While the reality of a fully intelligent team member may still be years away, it is on the horizon, and there are critical questions that must be addressed. Human factors and team cognition researchers should work to develop experimental protocols and methodologies to begin to understand how including an intelligent agent or machine into a team impacts our fundamental understanding of team cognition.

CONCLUSION

Cybersecurity, while growing in momentum, still remains a relatively unexplored frontier for human factors and team cognition scientists. In this paper, our goal was to begin to provide context-linking team research with current issues in cybersecurity to help steer future research, and provide information to practitioners who may

want to leverage extant literature in their jobs. Based on an understanding of the cyber domain, we identified cyber SA, role definition and staffing hand-offs, and team measurement as exemplar topics which team cognition was especially suited to address. For each topic, we defined and outlined the problem space in relation to cybersecurity, discussed how team cognition may apply to it, and then discussed the implications for research and practice. Throughout this review we highlighted that improved processes and capabilities are needed in order to share information more effectively and improve SA within and across geographically distributed teams.

We also discussed a new frontier in team science which has numerous implications to cybersecurity: human-machine teaming. Processes within cybersecurity such as anomaly or malware detection are being automated, however there is little research to date on how a human and synthetic agent should work together within the cyber domain to reduce the workload of analysts and improve the detection of malicious activity. Moving forward, researchers and practitioners should continue to work together to help apply previous work in team cognition to the cyber environment, as well as continue to push the state of understanding in a new context to help improve our understanding of human interaction and begin to understand the implications of including intelligent machines into teams.

REFERENCES

Abramis, D. J. (1994). Work role ambiguity, job satisfaction, and job performance: Meta-analyses and review. *Psychological Reports*, *75*, 1411–1433.

Applebaum, A., Johnson, S., Limiero, M., & Smith, M. (2018, June). Playbook oriented cyber response. In *2018 National Cyber Summit (NCS)* (pp. 8–15). Huntsville, AL, USA: IEEE.

Asgarli, E., & Burger, E. (2016). Semantic ontologies for cyber threat sharing standards. In *IEEE symposium on technologies for homeland security*. Waltham, MA USA: IEEE.

Austin, J. R. (2003). Transactive memory in organizational groups: The effects of content, consensus, specialization, and accuracy on group performance. *Journal of Applied Psychology*, *88*(5), 866–878.

Baker, D. P., & Salas, E. (1997). Principles for measuring teamwork: A summary and look toward the future. In *Team performance assessment and measurement: Theory, methods, and applications* (pp. 331–355). Mahwah, N.J: Lawrence Erlbaum Associates.

Barford, P., Dacier, M., Dietterich, T. G., Fredrikson, M., Giffin, J., Jajodia, S., . . . Ou, X. (2010). Cyber SA: Situational awareness for cyber defense. In *Cyber situational awareness* (pp. 3–13). Boston, MA: Springer.

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

Batenburg, R., van Walbeek, W., & in der Mauer, W. (2013). Belbin role diversity and team performance is there a relationship? *Journal of Management Development*, *32*(8), 901–913.

Beal, D. J., Cohen, R. R., Burke, M. J., & McLendon, C. L. (2003). Cohesion and performance in groups: A meta-analytic clarification of construct relations. *Journal of Applied Psychology*, *88*(6), 989–1004.

Beauchamp, M. R., Bray, S. R., Eys, M. A., & Carron, A. V. (2002). Role ambiguity, role efficacy, and role performance: Multidimensional and mediational relationships within interdependent sport teams. *Group Dynamics: Theory, Research, and Practice*, *6*(3), 229–242.

Belbin, M. (1993). *Team roles at work*. Oxford: Butterworth-Heinemann.

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

Boyce, M. W., Duma, K. M., Hettinger, L. J., Malone, T. B., Wilson, D. P., & Lockett-Reynolds, J. (2011). *Human performance in cybersecurity a research agenda*. Paper presented at the Proceedings of the Human Factors and Ergonomics Society Annual Meeting, Las Vegas, NV.

Brannick, M. T., Roach, R. M., & Salas, E. (1993). Understanding team performance: A multimethod study. *Human Performance*, *6*(4), 287–308.

Buchler, N., Rajivan, P., Marusich, L. R., Lightner, L., & Gonzalez, C. (2018). Sociometrics and observational assessment of teaming and leadership in a cybersecurity defense competition. *Computers & Security*, *73*, 114–136.

Caltagirone, S., Pendergast, A., & Betz, C. (2013). *The diamond model of intrusion analysis (ADA586960)*. Retrieved from Defense Technology Innovation Center www.dtic.mil/docs/citations/ADA586960.

Campbell, S. G., O'Rouke, P., & Bunting, M. F. (2015). *Identifying dimensions of cyber aptitude: The design of cyber aptitude and talent assessment*. Paper presented at the Proceedings of the Human Factors and Ergonomics Society Annual Meeting.

Cannon-Bowers, J. A., & Salas, E. (1998). Team performance and training in complex environments: Recent findings from applied research. *Current Directions in Psychological Science*, *7*(3), 83–87.

Cannon-Bowers, J. A., & Salas, E. (2001). Reflections on shared cognition. *Journal of Organizational Behavior*, *22*, 195–202.

Carron, A. V., Widmeyer, W. N., & Brawley, L. R. (1985). The development of an instrument to assess cohesion in sport teams: The group environment questionnaire. *Journal of Sport Psychology*, *7*(3), 244–266.

Champion, M., Rajivan, P., Cooke, N. J., & Jariwala, S. (2012). *Team-based cyber defense analysis*. Paper presented at the IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), New Orleans, LA.

Chappelle, W., McDonald, K., Christensen, J., Prince, L., Goodman, T., Thompson, W., & Hayes, W. (2013). *Sources of occupational stress and prevalence of burnout and clinical distress among U.S. Air Force cyber warfare operators*. ARFL Report: ARFL-SA-WP-TR-2013-006.

Cisco. (2017). *Annual cybersecurity report*. Retrieved from www.cisco.com/go/acr2017.

Cohen, S. G., & Bailey, D. E. (1997). What makes teams work: Group effectiveness research from the shop floor to the executive suite. *Journal of Management*, *23*(3), 239–290.

Cooke, N. J., Champion, M., Rajivan, P., & Jariwala, S. (2013). Cyber situation awareness and teamwork. *ICST Trans. Security Safety*, *1*(2), e5.

Cooke, N. J., Gorman, J. C., Myers, C. W., & Duran, J. L. (2013). Interactive team cognition. *Cognitive Science*, *37*(2), 255–285.

Cooke, N. J., Salas, E., Cannon-Bowers, J. A., & Stout, R. J. (2000). Measuring team knowledge. *Human Factors*, *42*(1), 151–173.

Cooper, G. E., & Harper Jr, R. P. (1969). *The use of pilot rating in the evaluation of aircraft handling qualities* (No. AGARD-567). Neuilly-Sur-Seine, France: Advisory Group for Aerospace Research and Development.

Cota, A. A., Evans, C. R., Dion, K. L., Kilik, L., & Longman, R. S. (1995). The structure of group cohesion. *Personality and Social Psychology Bulletin*, *21*(6), 572–580.

Damacharla, P., Javaid, A., Gallimore, J., & Devabhaktuni, V. (2018). Common metrics to benchmark human-machine team (HMT): A review. *IEEE Access*, *6*, 38637–38655.

D'Amico, A., Tesone, D., Whitley, K., O'Brien, B., Smith, M., & Roth, E. (2005). *Understanding the cyber defender: A cognitive task analysis of information assurance analysts*. Report No. CSA-CTA-ll. Secure Decisions. Funded by ARDA and DOD.

D'Amico, A., & Whitley, K. (2008). The real work of computer network defense analysts. In *VizSEC 2007* (pp. 19–37). Berlin and Heidelberg: Springer.

DeChurch, L. A., & Mesmer-Magnus, J. R. (2010). Measuring shared team mental models: A meta-analysis. *Group Dynamics: Theory, Research, and Practice*, *14*(1), 1–14.

DeStefano, C., Lachevet, K., & Carozzoni, J. (2008). *Distributed planning in a mixed-initiative environment*. Rome, NY: Air Force Research Laboratory, Systems and Information Interoperability Branch.

Dillenbourg, P., Baker, M. J., Blaye, A., & O'Malley, C. (1996). The evolution of research on collaborative learning. In *Learning in humans and machine: Towards an interdisciplinary learning science* (pp. 189–211). Emerald Group Publishing Limited Bingley, UK.

Dinsmore, D. L., Alexander, P. A., & Loughlin, S. M. (2008). Focusing the conceptual lens on metacognition, self-regulation, and self-regulated learning. *Educational Psychology Review*, *20*(4), 391–409.

Driskell, J. E., & Salas, E. (1991). Group decision making under stress. *Journal of Applied Psychology*, *76*(3), 473–478.

Driskell, J. E., Salas, E., & Johnston, J. (1999). Does Stress Lead to a loss of team perspective? *Group Dynamics: Theory, Research, and Practice*, *3*(4), 291–302.

Dyer, J. L. (1984). Team research and team training: A state-of-the-art review. *Human Factors Review*, *26*, 285–323.

Edmondson, A. (1999). Psychological safety and learning behavior in work teams. *Administrative Science Quarterly*, *44*(2), 350–383.

Edwards, B. D., Anthony Day, E., Arthur Jr, W., & Bell, S. T. (2006). Relationships among team ability composition, team mental models and team performance. *Journal of Applied Psychology*, *91*(3), 727–736.

Einhorn, H. J., & Hogarth, R. M. (1978). Confidence in judgement: Persistence of the illusion of validity. *Psychological Review*, *85*(5), 395–416.

Endsley, M. R. (1988). Situation awareness global assessment technique (SAGAT). In *Aerospace and electronics conference, 1988. NAECON 1988. Proceedings of the IEEE 1988 National Conference* (pp. 789–795). Dayton, OH: IEEE.

Endsley, M. R. (1989). *Situation awareness in an advanced strategic mission (No. NOR DOC 89–32)*. Hawthorne, CA: Northrop Corporation.

Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *37*(1), 32–64.

Endsley, M. R., & Connors, E. S. (2014). Foundation and challenges. In *Cyber defense and situational awareness* (pp. 7–27). Cham: Springer.

Endsley, M. R., & Rodgers, M. D. (1994). Situation awareness information requirements analysis for en route air traffic control. In *Proceedings of the Human Factors and Ergonomics Society annual meeting* (Vol. 38, No. 1, pp. 71–75). Los Angeles, CA: SAGE Publications.

Endsley, M. R., Selcon, S. J., Hardiman, T. D., & Croft, D. G. (1998). A comparative analysis of SAGAT and SART for evaluations of situation awareness. In *Proceedings of the Human Factors and Ergonomics Society annual meeting* (Vol. 42, No. 1, pp. 82–86). Los Angeles, CA: SAGE Publications.

Entin, E. E., & Entin, E. B. (2001). Measures for evaluation of team processes and performance in experiments and exercises. In *Proceedings of the 6th international command and control research and technology symposium* (pp. 1–14). Annapolis, MD, USA: International C2 Institute.

Espinosa, J. A., Nan, N., & Carmel, E. (2015). Temporal distance, communication patterns, and task performance in teams. *Journal of Management Information Systems*, *32*(1), 151–191.

Fairfax, T., Laing, C., & Vickers, P. (2015). Network situational awareness: Sonification and visualization in the cyber battlespace. In *Handbook of research on digital crime, cyberspace security, and information assurance* (pp. 334–349). Hershey, PA: IGI Global.

Fanelli, R., & Conti, G. (2012, June). A methodology for cyber operations targeting and control of collateral damage in the context of lawful armed conflict. In *2012 4th international Conference on Cyber Conflict (CYCON 2012)* (pp. 1–13). Tallinn, Estonia: IEEE.

Faraj, S., & Xiao, Y. (2006). Coordination in fast-response organizations. *Management Science*, *52*(8), 1155–1169.

Federal Bureau of Investigation (FBI). (2016). *Internet crimes report 2016*. Retrieved from https://pdf.ic3.gov/2016_IC3Report.pdf

Fink, G., North, C. L., Endert, A., & Rose, S. (2009). *Visualizing cybersecurity: Usable workspaces*. Paper presented at the 6th International Workshop on Visualization for Cyber Security. Atlantic City, NJ.

Gersh, J. R., & Bos, N. (2014). *Cognitive and organizational challenges of big data in cyber defense*. Paper presented at the 1st workshop on Human-Centered Big Data Research. Raleigh, NC.

Goodall, J. R., D'Amico, A., & Kopylec, J. K. (2009, October). Camus: Automatically mapping cyber assets to missions and users. In *MILCOM 2009–2009 IEEE military communications conference* (pp. 1–7). Atlantic City, NJ: IEEE.

Goodman, T., Miller, M. E., Rusnock, C. F., & Bindewald, J. (2016). Timing within human agent interaction and its effects on team performance and human behavior. In *Proceedings of the IEEE international multi-disciplinary conference on Cognitive Methods in Situation Awareness and Decision Support, CogSIMA 2016* (pp. 35–41). San Diego, CA: IEEE.

Gutzwiller, R. S., Fugate, S., Sawyer, B. D., & Hancock, P. A. (2015). The human factors of cyber network defense. In *Proceedings of the Human Factors and Ergonomics Society annual meeting* (Vol. 59, No. 1, pp. 322–326). Los Angeles, CA: SAGE Publications.

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 *Proceedings of the IEEE international multi-disciplinary conference on Cognitive Methods in Situation Awareness and Decision Support, CogSIMA 2016* (pp. 14–20). San Diego, CA: IEEE.

Hamilton, K., Mancuso, V., Mohammed, S., Tesler, R., & McNeese, M. (2017). Skilled and unaware: The interactive effects of team cognition, team metacognition, and task confidence on team performance. *Journal of Cognitive Engineering and Decision Making*, *11*(4), 382–395.

Hansen, M. T. (1999). The Search-Transfer Problem: The Role of Weak Ties in Sharing Knowledge across Organization Subunits. *Administrative Science Quarterly*, *44*(1), 82–111. https://doi.org/10.2307/2667032

Harrald, J., & Jefferson, T. (2007). Shared situational awareness in emergency management mitigation and response. In *System sciences, 2007. HICSS 2007* (pp. 23–23). Waikoloa, HI: IEEE.

Hart, S. G., & Staveland, L. E. (1988). Development of NASA-TLX (Task Load Index): Results of empirical and theoretical research. *Advances in Psychology*, *52*, 139–183.

Hayes-Roth, B., Hayes-Roth, F., Rosenchein, S. J., & Cammarata, S. (1979). *Modeling planning as an incremental, opportunistic process* (No. RAND/N-1178-ONR). Santa Monica, CA: RAND Corp.

Hellar, D. B., & McNeese, M. (2010, September). NeoCITIES: A simulated command and control task environment for experimental research. In *Proceedings of the Human*

Factors and Ergonomics Society annual meeting (Vol. 54, No. 13, pp. 1027–1031). Los Angeles, CA: SAGE Publications.

Helton, W. S., Funke, G. J., & Knott, B. A. (2014). Measuring workload in collaborative contexts: Trait versus state perspectives. *Human Factors*, *56*(2), 322–332.

Helton, W. S., & Garland, G. (2006). Short stress state questionnaire: Relationships with reading comprehension and land navigation. In *Proceedings of the Human Factors and Ergonomics Society annual meeting* (Vol. 50, No. 17, pp. 1731–1735). Los Angeles, CA: SAGE Publications.

Henschel, D., Deckard, G. M., Lufkin, B., Buchler, N., Hoffman, B., Rajivan, P., & Collman, S. (2016). Predicting proficiency in cyber exercises. In *Proceedings of MILCOM 2016–2016 IEEE military communications conference*. Baltimore, MD: IEEE.

Herjavec Group. (2017). *Cybersecurity jobs report.* A Special Report from the Editors at Cybersecurity Ventures. Retrieved from https://cybersecurityventures.com/jobs/.

Hui, P., Bruce, J., Fink, G., Gregory, M., Best, D., McGrath, L., & Endert, A. (2010). *Towards efficient collaboration in cybersecurity.* Paper presented at the 2010 International Symposium on Collaborative Technologies and Systems (CTS), Chicago, IL.

Hutchins, E. (2006). The distributed cognition perspective on human interaction. *Roots of human sociality: Culture, cognition and interaction*, 1, 375.

ISC². (2017). *Global information security workforce study: Benchmarking workforce capacity and response to cyber risk*. Retrieved from https://iamcybersafe.org/gisws/.

Jiang, S. Y., Murphy, A., Heitkemper, E. M., Hum, S., Kaufman, D. R., & Mamykina, L. (2017). Impact of an electronic handoff documentation tool on team shared mental models in pediatric critical care. *Journal of Biomedical Informatics*, *69*, 24–32.

Johnston, J. H., Smith-Jentsch, K. A., & Cannon-Bowers, J. A. (1997). Performance measurement tools for enhancing team decision making. In M. T. Brannick, E. Salas, & C. Prince (Eds.), *Team performance assessment and measurement: Theory, research, and applications* (pp. 311–330). Hillsdale, NJ: Erlbaum.

Joint Commission. (2012). *Joint commission center for transforming healthcare releases targeted solutions tool for hand-off communications.* Retrieved from www.jointcommission.org/assets/1/6/TST_HOC_Persp_08_12.pdf

Joint Publications. (2018). *Joint Publications 3–12 cyberspace operations.* Retrieved from www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/3-0-Operations-Series/.

Jones, D. G., & Endsley, M. R. (1996). Sources of situation awareness errors in aviation. *Aviation, Space, and Environmental Medicine*, *67*(6), 507–512.

Kaber, D. B., Perry, C. M., Segall, N., McClernon, C. K., & Prinzel III, L. J. (2006). Situation awareness implications of adaptive automation for information processing in an air traffic control-related task. *International Journal of Industrial Ergonomics*, *36*(5), 447–462.

Kahn, R. L., Wolfe, D. M., Quinn, R. P., Snoek, J. D., & Rosenthal, R. A. (1964). *Conflict and ambiguity: Studies in organizational roles and individual stress*. Oxford, UK: John Wiley.

Keebler, J. R., Lazzara, E. H., Patzer, B. S., Palmer, E. M., Plummer, J. P., Smith, D. C., . . . Riss, R. (2016). Meta-analyses of the effects of standardized handoff protocols on patient, provider and organizational outcomes. *Human Factors*, *58*(8), 1187–1205.

Kendall, D. L., & Salas, E. (2004). Measuring team performance: Review of current methods and consideration of future needs. *The Science and Simulation of Human Performance*, *5*, 307–326.

Klimoski, R., & Mohammed, S. (1994). Team mental model: Construct or metaphor? *Journal of Management*, *20*(2), 403–437.

Knott, B. A., Mancuso, V. F., Bennett, K., Finomore, V., McNeese, M., McKneely, J. A., & Beecher, M. (2013). Human factors in cyber warfare: Alternative perspectives.

In *Proceedings of the Human Factors and Ergonomics Society annual meeting* (Vol. 57, No. 1, pp. 399–403). Los Angeles, CA: SAGE Publications.

Lyons, J. B., Funke, G. J., Nelson, A., & Knott, B. A. (2011). Exploring the impact of cross-training on team process. In N. A. Stanton (Ed.), *Trust in military teams* (pp. 49–70). Aldershot, UK: Ashgate.

Lyons, J. B., & Stokes, C. K. (2012). Human-human reliance in the context of automation. *Human Factors*, *54*(1), 112–121.

MacDonald Jr, A. P., Kessel, V. S., & Fuller, J. B. (1972). Self-disclosure and two kinds of trust. *Psychological Reports*, *30*(1), 143–148.

Mañas, M. A., Díaz-Fúnez, P., Pecino, V., López-Liria, R., Padilla, D., & Aguilar-Parra, J. M. (2018). Consequences of team job demands: Role ambiguity climate, affective engagement, and extra-role performance. *Frontiers in Psychology*, *8*, 2292.

Mancuso, V. F., Christensen, J. C., Cowley, J., Finomore, V., Gonzalez, C., & Knott, B. (2014). Human factors in cyber warfare II: Emerging perspectives. In *Proceedings of the Human Factors and Ergonomics Society annual meeting* (Vol. 58, No. 1, pp. 415–418). Los Angeles, CA: SAGE Publications.

Mancuso, V. F., Minotra, D., Giacobe, N., McNeese, M., & Tyworth, M. (2012). idsNETS: An experimental platform to study situation awareness for intrusion detection analysts. In *2012 IEEE international multi-disciplinary conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)* (pp. 73–79). Chicago, IL: IEEE.

Marlow, S. L., Lacerenza, C. N., Paoletti, J., Burke, C. S., & Salas, E. (2018). Does team communication represent a one-size-fits-all approach?: A meta-analysis of team communication and performance. *Organizational Behavior and Human Decision Processes*, *144*, 145–170.

Mathieu, J. E., Maynard, M. T., Rapp, T., & Gilson, L. (2008). Team effectiveness 1997–2007: A review of recent advancements and a glimpse into the future. *Journal of Management*, *34*(3), 410–476.

Mathieu, J. E., Tannebaum, S. I., Donsbach, J. S., & Alliger, G. M. (2014). A review and integration of team composition models: Moving toward a dynamic and temporal Framework. *Journal of Management*, *40*(1), 130–160.

Matthews, G., Campbell, S. E., Desmond, P. A., Huggins, J., Falconer, S., & Joyner, A. (1999). Assessment of task-induced state change: Stress, fatigue and workload components. *Automation technology and human performance: Current research and trends*, 199–203.

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.

Mayer, R. C., & Davis, J. H. (1999). The effect of the performance appraisal system on trust for management: A field quasi-experiment. *Journal of applied psychology*, *84*(1), 123.

Mazzocco, K., Petitti, D. B., Fong, K. T., Bonacum, D., Brookey, J., Graham, S., . . . Thomas, E. J. (2009). Surgical team behaviors and patient outcomes. *The American Journal of Surgery*, *197*(5), 678–685.

McCallam, D. H., Frazier, P. D., & Savold, R. (2017, July). Ubiquitous connectivity and threats: Architecting the next generation cybersecurity operations. In *2017 IEEE 7th annual international conference on CYBER technology in automation, control, and intelligent systems (CYBER)* (pp. 1506–1509). Kaiulani, HI: IEEE.

McGuinness, B., & Foy, L. (2000). A subjective measure of SA: The Crew Awareness Rating Scale. In D. B. Kaber and M. R. Endsley (Eds.), *Human performance, situation awareness and automation: User centered design for the new millennium*. Atlanta, GA: SA Technologies.

McNeese, M. D., Connors, E. S., Jones, R. E., Terrell, I. S., Jefferson Jr, T., Brewer, I., & Bains, P. (2005). Encountering computer-supported cooperative work via the living lab:

Application to emergency crisis management. In *Proceedings of the 11th international conference of human-computer interaction*.

McNeese, M. D., Mancuso, V. F., McNeese, N. J., Endsley, T., & Forster, P. (2013). *Using the living laboratory framework as a basis for understanding next-generation analyst work*. Paper presented at the SPIE Defense, Security, and Sensing, Baltimore, MD.

McNeese, M. D., Mancuso, V. F., McNeese, N. J., Endsley, T., & Forster, P. (2014). An integrative simulation to study team cognition in emergency crisis management. In *Proceedings of the Human Factors and Ergonomics Society annual meeting* (Vol. 58, No. 1, pp. 285–289). Los Angeles, CA: Sage Publications.

Miller, C. A., & Parasuraman, R. (2003). Beyond levels of automation: An architecture for more flexible human-automation collaboration. In *Proceedings of the Human Factors and Ergonomics Society 47th annual meeting*. Denver, CO.

Mohammed, S., & Dumville, B. C. (2001). Team mental models in a team knowledge framework: Expanding theory and measurement across disciplinary boundaries. *Journal of Organizational Behavior*, *22*(2), 89–106.

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). *National Initiative for Cybersecurity Education (NICE) cybersecurity workforce framework*. NIST Special Publication 800–181. Retrieved from https://doi.org/10.6028/NIST.SP.800-181.

O'Leary, M. B., & Cummings, J. N. (2007). The spatial, temporal, and configurational characteristics of geographic dispersion in teams. *MIS quarterly*, 433–452.

Oltsik, J. (2017). Cybersecurity skills shortage hurts security analytics, operations. *CSO*. Retrieved from https://search.proquest.com/docview/1922897602?accountid=12492.

Oshri, I., van Fenema, P., & Kotlarsky, J. (2008). Knowledge transfer in globally distributed teams: The role of transactive memory. *Information Systems Journal*, *18*, 593–616.

Patriciu, V. V., & Furtuna, A. C. (2009). Guide for designing cybersecurity exercises. In *Proceedings of the 8th WSEAS international conference on E-activities and information security and privacy* (pp. 172–177). Stevens Point, WI: World Scientific and Engineering Academy and Society (WSEAS).

Paul, C. L., & Dykstra, J. (2017). Understanding operator fatigue, frustration, and cognitive workload in tactical cybersecurity operations. *Journal of Information Warfare*, *16*(2), 1–11.

Paulsen, C., McDuffie, E., Newhouse, W., & Toth, P. (2012). NICE: Creating a cybersecurity workforce and aware public. *IEEE Security and Privacy*, *10*(3), 76–79.

Rajivan, P., Champion, M., Cooke, N. J., Jariwala, S., Dube, G., & Buchanan, V. (2013, July). Effects of teamwork versus group work on signal detection in cyber defense teams. In *International conference on augmented cognition* (pp. 172–180). Berlin and Heidelberg: Springer.

Reid, G. B., & Nygren, T. E. (1988). The subjective workload assessment technique: A scaling procedure for measuring mental workload. In P. A. Hancock & N. Meshkati (Eds.), *Human mental workload* (pp. 185–218). Amsterdam: Elsevier.

Riggs, M. L., & Knight, P. A. (1994). The impact of perceived group success-failure on motivational beliefs and attitudes: A causal model. *Journal of Applied Psychology*, *79*, 755–766.

Rodgers, M. (2017). *Human factors impacts in air traffic management*. Abingdon: Routledge.

Roscoe, A. H. (1987). *The practical assessment of pilot workload*. AGARD-AG-282. Neuilly-Sur-Seine, France: Advisory Group for Aerospace Research and Development.

Rousseau, R., Tremblay, S., Banbury, S., Breton, R., & Guitouni, A. (2010). The role of metacognition in the relationship between objective and subjective measures of situation awareness. *Theoretical Issues in Ergonomics Science*, *11*(1–2), 119–130.

Russel, S., & Norvig, P. (2013). Intelligent agents. In *Artificial intelligence: A modern approach* (pp. 47–57). Upper Saddle River, NJ: Pearson Education Limited.

Russell, S. M., Funke, G. J., Knott, B. A., & Strang, A. J. (2012). *Recurrence quantification analysis used to assess team communication in simulated air battle management*. Paper presented at the Proceedings of the Human Factors and Ergonomics Society Annual Meeting.

Salas, E., Bowers, C. A., & Cannon-Bowers, J. A. (1995). Military team research: 10 years of progress. *Military Psychology*, *7*(2), 55–75.

Salas, E., Cooke, N. J., & Rosen, M. A. (2008). On teams, teamwork, and team performance: Discoveries and developments. *Human Factors*, *50*(3), 540–547.

Sawyer, B. D., & Hancock, P. A. (2018). Hacking the human: The prevalence paradox in cybersecurity. *Human Factors*, *60*(5), 597–609.

Schaefer, K. E., Chen, J. Y., Szalma, J. L., & Hancock, P. A. (2016). A Meta-analysis of factors influencing the development of trust in automation: Implications for understanding autonomy in future systems. *Human Factors*, *58*(3), 377–400.

Schwarz, N. (2000). Emotion, cognition, and decision making. *Cognition & Emotion*, *14*(4), 433–440.

Shuffler, M. L., & Carter, D. R. (2018). Teamwork situated in multiteam systems: Key lessons learned and future opportunities. *American Psychologist*, *73*(4), 390.

Silva, A., Emmanuel, G., McClain, J. T., Matzen, L., & Forsythe, C. (2015). *Measuring expert and novice performance within computer security incident response teams*. Lecture Notes in Computer Science Volume 9183, 2015, pp. 144–152, 9th International Conference on Augmented Cognition, AC 2015 held as part of 17th International Conference on Human Computer Interaction, HCI International 2015, Los Angeles, United States, 2 August 2015 through 7 August 2015.

Smith, D. R. (1999). *The effect of transactive memory and collective efficacy on aircrew performance*. Dayton, OH: Wright State University.

Sommestad, T., & Hallberg, J. (2012). Cyber security exercises and competitions as a platform for cybersecurity experiments. In *Nordic conference on secure IT systems* (pp. 47–60). Berlin and Heidelberg: Springer.

Sparrow, B., Liu, J., & Wegner, D. M. (2011). Google effects on memory: Cognitive consequences of having information at our fingertips. *Science*, *333*(6043), 776–778.

Staheli, D., Mancuso, V., Harnasch, R., Fulcher, C., Chmielinski, M., Kearns, A., . . . Vuksani, E. (2016). Collaborative data analysis and discovery for cybersecurity. In *WSIW@ SOUPS*. Denver, CO: USENIX Association.

Stanton, N. A., Stewart, R., Harris, D., Houghton, R. J., Baber, C., McMaster, R., . . . Linsell, M. (2006). Distributed situation awareness in dynamic systems: Theoretical development and application of an ergonomics methodology. *Ergonomics*, *49*(12–13), 1288–1311.

Star, S. L., & Griesemer, J. R. (1989). Institutional ecology, translations' and boundary objects: Amateurs and professionals in Berkeley's Museum of Vertebrate Zoology, 1907–39. *Social Studies of Science*, *19*(3), 387–420.

Stewart, G. L. (2006). A meta-analytic review of relationships between team design features and team performance. *Journal of Management*, *32*(1), 29–55.

Taylor, R. M. (2017). Situational Awareness Rating Technique (SART): The development of a tool for aircrew systems design. In *Situational awareness* (pp. 111–128). New York: Routledge.

Tsang, P. S., & Velazquez, V. L. (1996). Diagnosticity and multidimensional subjective workload ratings. *Ergonomics*, *39*(3), 358–381.

Turner, K. L., & Miller, M. E. (2017). *The effect of automation and workspace design. Humans' ability to recognize patterns while fusing information*. Paper presented at IEEE Conferences on Cognitive and Computational Aspects of Situation Management (CogSIME), Savannah, GA.

Tyworth, M., Giacobe, N. A., Mancuso, V. F., & Dancy, C. D. (2012). *The distributed nature of cyber situation awareness*. Paper presented at the 2012 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support, New Orleans, LA.

Tyworth, M., Giacobe, N. A., Mancuso, V. F., McNeese, M. D., & Hall, D. L. (2013). A human-in-the-loop approach to understanding situation awareness in cyber defense analysis. *EAI Endorsed Transactions on Security and Safety*, *1*(2), 1–10.

Uitdewilligen, S., & Waller, M. (2018). Information sharing and decision-making in multidisciplinary crisis management teams. *Journal of Organizational Behavior*, *39*(6), 731–748.

Van de Water, H., Ahaus, K., & Rozier, R. (2008). Team roles, team balance and performance. *Journal of Management Development*, *27*(5), 499–512.

Vidulich, M. A., & Hughes, E. R. (1991). Testing a subjective metric of situation awareness. In *Proceedings of the Human Factors and Ergonomics Society annual meeting* (Vol. 35, No. 18, pp. 1307–1311). Los Angeles, CA: SAGE Publications.

Volpe, C. E., Cannon-Bowers, J. A., Salas, E., & Spector, P. E. (1996). The impact of cross-training on team functioning: An empirical investigation. *Human Factors*, *38*(1), 87–100.

Waag, W. L., & Houck, M. R. (1994). Tools for assessing situational awareness in an operational fighter environment. *Aviation, Space, and Environmental Medicine*, *65*(5 Suppl), A13–A19.

Watson, D., & Clark, L. A. (1999). *The PANAS-X: Manual for the positive and negative affect schedule-expanded form*. Iowa City, IA: The University of Iowa.

Watson, D., Clark, L. A., & Tellegen, A. (1988). Development and validation of brief measures of positive and negative affect: The PANAS scales. *Journal of Personality and Social Psychology*, *54*(6), 1063–1070.

Wegner, D. M. (1995). A computer network model of human transactive memory. *Social Cognition*, *13*(3), 319–339.

Wegner, D. M., Erber, R., & Raymond, P. (1991). Transactive memory in close relationships. *Journal of Personality and Social Psychology*, *61*(6), 923–929.

Wellens, A. R. (1993). Group situation awareness and distributed decision making: From military to civilian applications. In N. J. J. Castellan (Ed.), *Individual and group decision making: Current issues* (pp. 267–287). Hillsdale, NJ: Lawrence Erlbaum Associates.

Wellens, A. R., & Ergener, D. (1988). The CITIES game: A computer-based situation assessment task for studying distributed decision making. *Simulation & Games*, *19*(3), 304–327.

Wickens, C. D. (2002). Situation awareness and workload in aviation. *Current Directions in Psychological Science*, *11*(4), 128–133.

Zetter, K. (2016, March 3). *Inside the cunning, unprecedented hack of Ukraine's power grid*. Retrieved September 20, 2019, from www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

Zimmerman, C. (2014). *Ten strategies of a world-class cybersecurity operations center.* MITRE Corporate Communications and Public Affairs.