EAI Endorsed Transactions
on Security and Safety

Research Article

Cyber situation awareness and teamwork

Nancy J. Cooke[1,*], Michael Champion[1], Prashanth Rajivan[1] and Shree Jariwala[1]

[1]Arizona State University, Santa Catalina Hall 7271 E. Sonoran Arroyo Mall Mesa, AZ 85212

Abstract

Cyber analysis is a complex task that requires the coordination of a large sociotechnical system of human analysts working together with technology. Adequate situation awareness of such a complex system requires more than aggregate situation awareness of individuals. Teamwork in the form of communication and information coordination is at the heart of team-level situation awareness. In this position paper, we report observations from previously conducted cognitive task analyses that suggest that teamwork is lacking in many cyber analysis organizations. Communication is ineffective, team roles are inconsistent across organizations, reward structures and selection may thwart collaboration, and the environment is conducive to individual work. Suggestions for improving teamwork in the cyber domain are offered.

Keywords: complex systems, cyber defence, cyber situation awareness, situation awareness, teamwork.

Received on 30 March 2012; accepted on 30 March 2013, published on 03 May 2013

doi: 10.4108/trans.sesa.01-06.2013.e4

1. Introduction

From sensor data exploitation to the management of mundane and persistent email, workers are increasingly finding a significant portion of their work days devoted to total data immersion, often to the point of cognitive overload. Nowhere is this more obvious or more problematic than the world of the cyber analyst. One of the primary tasks of cyber analysts is intrusion detection which involves monitoring, filtering, and fusing large amounts of data emanating from disparate sources such as network activity logs, and alerts from intrusion detection systems (IDS) in order to find patterns that may correspond to potential cyber attacks (D'Amico & Whitley, 2008 ; Boyce et al., 2011). Analysts are often required to stare at screens of alerts, processing them each within minutes (D'Amico, Whitley, Teson, O'Brien, & Roth, 2005). Alerts generated from current IDSs are mostly false alarms and thus the onus is on the analysts to distinguish the alerts that correspond to an attack from false alarms (D'Amico, et al., 2005). Thus a combination of factors that include overwhelming amounts of data, numerous false alarms, and time stress leads to cognitive overload in cyber defense analysts (Champion, Rajivan, Jariwala, & Cooke 2012).

2. Cyber Situation Awareness

Situation awareness (SA) plays an important role in the analysts' effective processing of alerts. As is true in the cockpit, nuclear power plant, and on the battlefield, good SA is essential for making correct decisions and taking appropriate actions (Fracker, 1991). Lack of SA is often cited as the key reason for human errors (Endsley, 2000). Situation awareness is defined as "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future" (Endsley, 1995, p. 36). Endsley's definition and model of SA has been adopted by researchers in the cyber domain and is similar to the JDL (Joint Directors of Laboratories) data fusion model, a four-level model that describes how data

* Corresponding author. Email:Nancy.Cooke@asu.edu

from multiple sources can be integrated to get a unified view (Hall & Llinas, 1997).

Information overload, which is excessive in the cyber domain, has been identified as one of the key factors impacting SA (Taylor, 1990 ; Endsley 2000). Endsley (1995) suggests that situation awareness is a product of the situation assessment process performed by operators while working with large quantities of information. Technologies such as data filters (example: Wireshark and Snort), fusion algorithms (Stotz & Sudit, 2007) and visualizations (Shiravi, Shiravi, & Ghorbani, 2011) are being developed to assist in cyber analysis and to provide analysts a better picture of the complex cyber world. However, it is important to recognize that the "awareness" in situation awareness resides neither with the analyst alone, nor with the technology alone, but with the joint human-technology system (McNeese, Cooke, & Champion, 2011).

2.1 Team Cyber Situation Awareness

Indeed, the cyber analysis task is accomplished by a system much broader than a single human and single machine. There are many analysts working at different levels in many different organizations with extensive technology to address cyber threats. In this paper we address the issue of teamwork in cyber analysis. A team is a special type of group in which members of the team have specialized backgrounds and work together in an interdependent fashion (Salas, Dickinson, Converse, & Tannebaum, 1992). Teams are becoming ubiquitous in our modern technological society (Fiore, Salas, Cuevas, & Bowers, 2003) because a single individual cannot possess the requisite skills and background knowledge to take on modern tasks like cyber analysis independently. Some tasks like air traffic management or open heart surgery are nearly impossible to execute without a team.

Team SA is an important factor to be considered in designing human-machine systems and interfaces in which multiple individuals interact to comprehend the situation (Shu & Furuta, 2005). Endsley defines team SA as "the degree to which every team member possesses the SA required for his or her responsibilities" (Endsley, 1995). According to this perspective, the team's performance depends on the level of situation awareness in each of the team member and one member's poor SA can affect the team's performance. However, this model of team SA does not go far enough (Gorman, Cooke, & Winner, 2006). It may be relevant to homogenous groups, but not to heterogeneous teams and this collective perspective may not suffice as teams increase in size (Cooke et al., 2009). If a team is truly an interdependent group then each team member will have different, though perhaps overlapping, perspectives on the situation. In a complex and dynamic world it is likely that two or more perspectives on the team will need to be fused in order to have SA that extends beyond an analyst's screen of alerts. The fusion takes place through some form of team interaction – often communication. For example, one analyst may be aware of a denial of service attack on a network server and once this information is joined with another analyst's awareness of two other similar attacks on a different network a bigger picture emerges. Without the interaction, the team as a whole cannot perceive, comprehend, and project.

In short, team SA is much more than the sum of individual SA (Salas, Prince, Baker, & Shrestha, 1995). This follows from the perspective of Interactive Team Cognition (Cooke, Gorman, Myers, & Duran, in press) that espouses that cognitive processing at the team level occurs through team interactions situated in a rich context. This view of team cognition can be contrasted with others that focus on the aggregate of individual knowledge (e.g., Langan-Fox, Code, & Langfield-Smith, 2000). Thus by placing the focus on team interaction, team situation awareness can be described as the coordinated and efficient perception of change in the environment by team members that serves as the basis for effective action (Gorman, Cooke, & Winner, 2006). According to this view of team SA, members of a team become aware of different aspects of the situation and knit the pieces of the puzzle together through communication or other interactions to achieve team situation awareness and to take appropriate actions. Salas et al., (1995) and Cooke, Salas, Kiekel, and Bell (2004) suggest that it is through team interactions that team members transform individual knowledge to collective knowledge and in the process achieve team situation awareness. We take this ecological perspective of team SA in this paper (Cooke, Gorman, & Rowe, 2009).

Our position is that because the cyber analysis task requires situation awareness over a vast network that it is ideally suited for teamwork among individuals with varying background knowledge and skills armed with technology that can collaboratively facilitate situation awareness. However, we also suggest that the cyber world has not readily adopted a collaborative model of cyber analysis and that individual analysts work alone, even if in a group, thus missing out on the advantages of teamwork that include team situation awareness. In the remainder of this paper we make some observations relevant to this lack of teamwork in the cyber world and follow up with some suggestions for cyber teaming

3. Some Observations on Cyber Teamwork

The authors of this paper previously reported findings from a cognitive task analysis of cyber analysts from various government and private organizations and cyber exercises (for more information see Champion, Rajivan, Jariwala, & Cooke 2012). For these sessions, we interviewed 10 cyber experts in an unstructured interview during a workshop, observed the United State Air Force Academy (USAFA) Cadets in a Cyber Defense Exercise (CDX) sponsored by the National Security Agency (NSA), and observed and interviewed the International

Capture The Flag (iCTF) competition hosted by the University of California, Santa Barbara. The objective of the CDX exercise was to test the Academy's cadets in a cyber defense task. The objective of the iCTF competition was to place 86 international cyber teams against one another in order to compromise system securities, exfiltrate information, maintain a covert money market (money laundering) system, and complete objectives geared towards a cyber task. After the interviews from cyber defense analysts and the data collection from the CDX and iCTF competitions, we combined our notes and organized them by task, task structure, communication, and tactics of defense (e.g. watch a current attack and let it begin to understand the target, stop an attack at the beginning, and so on).

In addition to our work, there are a number of other published analyses of the cyber task that corroborate what we have found (D'Amico, et al., 2005; Stanard, Thordson, McCloskey, & Vincent, 2001). Both research teams used cognitive task analysis methodology to create interview questions and organize results for cyber analysts. Though these reports and our own analyses are broader in their coverage of the cyber task domain, we focus here on several observations pertinent to teamwork among cyber analysts. In the sections below we highlight some teamwork issues that we and others have observed in the cyber domain.

3.1 Communication among cyber analysts is ineffective

Communication has been described as cognitive processing at the team level (Cooke, et al., in press; Cooke et al., 2009; Cooke, Gorman, & Winner, 2007). In other words communication is the team-level processing of information to develop situation awareness. Therefore ineffective communication can lead to poor team cognition including poor team SA and possibly, a deleterious outcome.

We observed effective and ineffective communication structures for the two teams observed at the iCTF competition. In our observations of cyber exercises we found that although attempts were made to streamline and guide communication there were inevitable breakdowns. In several of the competitions we observed that teams often wasted time by duplicating efforts because of a lack of communication. This would occur when participants would try to solve a problem on their own without communicating to their teammates about what they had completed or if they were stuck.

Communication may be further hindered by the organizations that employ cyber analysts. Organizational stovepipes and security barriers may actively prevent communication between individuals. Much information is classified or compartmentalized such that knowledge sharing is not allowed; not only between the global communities of analysts, but also within the organization. For example, sharing information between different federal departments is a rather complicated process (United States Government Accountability Office, 2011). Analysts interviewed often-cited classifications and complicated systems as a point of stress and hindrance. In an interview with one government analyst, it was pointed out that there were instances in which recently monitored system alerts would become classified information if found to be suspicious enough. Sometimes the classification level would be higher than that of the analysts' who classified the original alert. This was noted to lead to issues with identifying other similar alerts because the frame of reference had been removed. Therefore communication can be prohibited not just by the organization, but also by analysts and officials who err on the side of caution and believe that it is safer not to share information when the situation is ambiguous. Without the ability to communicate, team SA is not possible.

3.2 Team roles for cyber analysts are inconsistent within and across organizations

D'Amico, et al., (2005) concluded through a cognitive task analysis (CTA) for the US Air Force that there are six roles of the cyber analysis task: Triage, Escalation Analysis, Correlation Analysis, Threat Analysis, Incident Response, and Forensic Analysis. Similarly, Killcrece, Kossakowski, Ruefle, and Zajicek (2003) outlined a number of positions commonly reported to exist in Computer Security Incident Response Teams (CSIRTs) that correspond with the findings of D'Amico and her colleagues. Roles in teamwork help to orient and structure the team and capitalize on team member specializations. However, Killcrece, et al. (2003) also stated that there is no standard set of roles, leaving this decision to each CSIRT. Although guidelines pertaining to roles exist, actual implementation and adherence is much lower. A study conducted by the U.S. Government Accountability Office (GAO) concluded that there were many conflicts regarding role positions, responsibilities and implementations across organizations (United States Government Accountability Office, 2011).

We have observed that the role structure of the cyber analysis task can also differ within an organization. Indeed, the GAO report indicated that though roles are laid out, there is often confusion among analysts as to the responsibilities associated with these roles. With an improper or inadequate organizational role structure, degraded task performanceis possible (Dubé, Tremblay, Banbury, & Rousseau, 2010). For example, we observed that in some cases roles were duplicated within teams during the iCTF and CDX competitions. This causes teams to ineffectively utilize their resources and potentially undermines the ability of the team to efficiently monitor a network.

Finally, there is some evidence that suggests that the functional assignment of non-overlapping roles as is typical in cyber analysis organizations (e.g. Champion et al, 2012; United States Government Accountability Office, 2011; D'Amico et al, 2005; Killcrece et al, 2003) may not be as effective as cross-functional teams in which functions are shared. That is, teams full of specialists are not always as effective as teams for which roles overlap significantly. Performance differences were noted between functional, team members who have tasks and responsibilities assigned solely to them, and cross-functional, team members who share all responsibilities. Specifically, cross-functional teams out-performed functional teams (Mancuso, 2012). In general, there is a science of teamwork and team composition that has not been adequately tapped for this domain.

3.3 Organizations can thwart collaboration

There are a number of ways that organizations contribute to poor team SA. The organizations which hire analysts propagate poor communication through reward structures that encourage them to act alone. Stanard, Thordson, McCloskey, and Vincent (2001) found that operators within an organization often chose to conduct their investigations individually. Moreover, we observed that analysts would rather be able to claim a significant "find" for themselves and for their own personal advancement, rather than sharing the success with the team as a group effort. This tendency was often supported by the employer who offered incentives for significant finds. Thus, as a consequence of the reward structure, knowledge is safeguarded rather than shared. This reward structure, combined with a sense of esteem from solving a problem alone, fosters individual work. Individual work may foster individual SA, but not the team SA required to understand the larger complex cyber system.

In addition to reward structures, personnel selection practices may also favor individual work over teamwork. The 2006 IT Work Force Capability Assessment (ITWCA) report illustrates that ineffective teamwork may be systemic of the personnel rather than the task. When personnel were surveyed regarding important job attributes required for their positions, interpersonal skills were not ranked high or relevant. Regardless of the reasons why, the lack of value placed on interpersonal skills is incorporated into how the analysts view the role. This shared view may be perpetuating itself as analysts define the roles not only for themselves and impact how supervisors and newer analysts see the role.

3.4 The environment facilitates individual work

The physical environment can promote individual rather than collaborative work. Simply the layout of a work room suggests the nature of collaboration. Central areas where people can convene at breaks and open workspaces in which people can see one another suggest to workers that collaboration is valued. On the contrary, we have observed that cyber analysts stare at computer monitors for hours at a time and are spread apart from others often in rooms that all face large common screens.

Software available to analysts also affords specific work styles. Both analysts and students in the competitions reported that communication of more complex ideas became cumbersome using the available technology to communicate. In the case of analysts, the organizational constraints would often limit the resources available for communication such as using public methods of transporting information (either through instant messaging or cloud based storage services). Further, the software currently used by analysts is focused on aiding the work of an individual analyst, rather than the team.. Overall, the analyst environment encourages individual work at the expense of teamwork.

4. Fostering collaboration among cyber analysts

Cyber situation awareness takes place within a large and complex sociotechnical system. Many human and machine components need to work together in a coordinated fashion. We propose that making some changes to facilitate analyst teamwork would enhance team cyber situation awareness and ultimately cyber security.

4.1 Improving communication among cyber analysts

Communication is essential to establishing team SA. With missing or ineffective communication due to poor teamwork skills or organizational prohibitions, team SA is compromised. Team training on teamwork skills such as communication has been shown to be effective for improving team performance (Salas, Cooke, & Rosen, 2008). Simulation based training in which team members experience system breakdowns or "perturbations" has also been found to make for more flexible and adaptive teams (Gorman, Cooke, & Amazeen, 2010). Dealing with the multi-layered security and classification issues is a more complex issue. This is something that needs to be addressed through policy changes. The goal at a minmum should be to avoid disrupting communications within a team of analysts.

4.2 Clarifying team roles and leveraging team science

A team of interdependent individuals is not able to function without role clarity. Who knows what? Who takes what action? Who needs to know this? There is a

significant body of science on team structure and team roles (Salas, Cooke & Rosen, 2008) that can be leveraged in support of team SA for the cyber analysts. Additional research is needed that extends this team science to the cyber domain. Once support for a structure has been identified then team members roles need to be clarified in training, supported in the work environment, and applied consistently.

4.3 providing organizational support for cyber teamwork

If organizations support the goal of team SA which is required to have a less myopic sense of threats in cyber space, then reward structures should be established accordingly. An entire team can be rewarded for finds, rather than a single individual. However, care needs to be taken to avoid disrupting interteam collaboration by promoting competition. This careful balance of rewading teamwork and avoiding team competition is another topic for further study in this domain.

In addition, organizations should appreciate the importance of teamwork skills and should promote these through selection or training of the workforce**.** Organizations play an important role in team SA and with some relatively minor adjustments can be catalysts of teamwork rather than impediments to it.

4.4 Designing the environment to facilitate teamwork

Parallel to organizational adjustments, there are some relatively minor adjustments in the physical work environment that can encourage teamwork and team SA. These include increased open spaces, shared break areas, arrangement of workspaces, and layout of common displays. The physical environment plays an important role in team development and even minor changes such as changing workspace locations have been found to improve teamwork (Fouse, Cooke, Gorman, Murray, Uribe, & Bradbury, 2011). The design of tools and technologies to aid the cyber analyst can also thwart or promote teamwork. The area of CSCW (computer supported collaborative work; Grudin & Poltrock, 2012) should be leveraged in the development of these aids.

5. Conclusion

A large organization of individuals working with technology to improve individual cyber SA and to ultimately identify cyber threats is not a system, but rather a loose collection of independent components. Brittleness, redundancy of function, confusion, and a missing "big picture" result from this type of organization. Global SA of the larger cyber system is traded off for local successes at identifying small isolated threats which may even mask the larger threat. Implementing best teamwork practices and leveraging team science can unite these components and provide the integration necessary for team SA and an effective sociotechnical system.

References

[1] Boyce, M. W., Duma, K. M., Hettinger, L. J., Malone, T. B., Wilson, D. P., & Lockett-Reynolds, J. (2011). Human performance in cybersecurity. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 55*(1) 1115-1119.

[2] Champion, M., Rajivan, P., Cooke, N. J., & Jariwala, S. (2012). Team-Based Cyber Defense Analysis. 2012 IEEE *International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support*. (New Orleans).

[3] Cooke, N. J., Salas, E., Kiekel, P. A., & Bell, B. (2004). Advances in measuring team cognition. *Team Cognition: Understanding the Factors that Drive Process and Performance*, 83–106.

[4] Cooke, N. J., Gorman, J. C., Myers, C. W., & Duran, J.L. (in press). Interactive Team Cognition, *Cognitive Science.*

[5] Cooke, N. J., Gorman, J. C., & Rowe, L. J. (2009). An Ecological Perspective on Team Cognition. In E. Salas, J. Goodwin, & C. S. Burke [eds.], *Team Effectiveness in Complex Organizations: Cross-disciplinary Perspectives and Approaches*, pp. 157-182. SIOP Organizational Frontiers Series, Taylor & Francis.

[6] Cooke, N. J., Gorman, J. C., & Winner, J. L. (2007). Team cognition. In F. Durso, R. Nickerson, S. Dumais, S. Lewandowsky, and T. Perfect, *Handbook of Applied Cognition, 2nd Edition*, pp. 239-268, Wiley.

[7] D'Amico, A., Whitley, K., Teson, D., O'Brien, B., & Roth, E. (2005). Acheiving cyber defense situational awarness: A cognitive task analysis of information assurance analysts. *Proceedings of the Human Factors and Ergonomics Society 49th Annual Meeting* (pp. 229-233). Sage.

[8] D'Amico, A., & Whitley, K. (2008). The real work of computer network defense analysts *VizSEC 2007*, 19-37.

[9] Dubé, G., Tremblay, S., Banbury, S., & Rousseau, V. (2010). Team Performance and Adaptability in Crisis Management: A comparison of cross-functional and functional teams. *Proceedings of the Human Factors and Ergonomics Society* (pp. 1610-1614). Sage.

[10] Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors, 37*, 32–64.

[11] Endsley, M. R. (2000). Theoretical underpinnings of situation awareness: A critical review. *Situation Awareness Analysis and Measurement*, 3-32.

[12] Fiore, S. M., Salas, E., Cuevas, H. M., & Bowers, C. A. (2003). Distributed coordination space: Toward a theory of distributed team process and performance. *Theoretical Issues in Ergonomics Science, 4*(3-4), 340-364.

[13] Fouse, S., Cooke, N. J., Gorman, J. C., Murray, I., Uribe, M., & Bradbury, A. (2011). Effects of Role and Location switching on team performance in a collaborative planning environment. *Proceedings of the 55th Annual Conference of the Human Factors and Ergonomics Society, 55*, (Santa Monica, CA: Human Factors and Ergonomics Society) 1442-1446.

[14] FRACKER, M. L. (1991). *Measures of Situation Awareness: Review and Future Directions,*
[15] GORMAN, J. C., COOKE, N. J., & AMAZEEN, P. G. (2010). Training adaptive teams. *Human Factors, 52,* 295-307.
[16] GORMAN, J.C., COOKE, N. J., & WINNER, J.L. (2006). Measuring team situation awareness in decentralized command and control systems. *Ergonomics, 49,* 1312-1325.
[17] GRUDIN, J. & POLTROCK, S. (2012). CSCW: Computer Supported Cooperative Work. . In M. SOEGAARD & R.F. DAM [eds.], *Encyclopedia of human-computer interaction.* Interaction-Design.org Foundation
[18] HALL, D. L., & LLINAS, J. (1997). An introduction to multisensor data fusion. *Proceedings of the IEEE, 85*(1), 6-23.
[19] KILLCRECE, G., KOSSAKOWSKI, K., RUEFLE, R., & ZAJICEK, M. (2003). *Organizational Models for Computer Security Incident Response Teams (CSIRTs)* (CMU/SEI-2003-HB-001, ADA421684). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.
[20] LANGAN-FOX, J., CODE, S., & LANGFIELD-SMITH, K. (2000). Team mental models: Techniques, Methods, and Analytic Approaches. *Human Factors, 42,* 242-271.
[21] MANCUSO, V. (2012). An Interdisciplinary Evaluation of Transactive Memory in Distributed Cyber Teams. Unpublished doctoral dissertation, College of Information Sciences and Technology, The Pennsylvania State University, State College, Pa
[22] MCNEESE, M., COOKE, N.J., CHAMPION, M.A. (2011) Situating Cyber Situation Awareness. *Proceedings of the 10th International Conference on Naturalistic Decision Making.*
[23] SALAS, E., COOKE, N. J., ROSEN, M.A. (2008). On Teams, Teamwork and Team Performance: Discoveries and Developments. *Human Factors: Golden Anniversary Special Issue, 50,* 540-547.
[24] SALAS, E., PRINCE, C., BAKER, D. P., & SHRESTHA, L. (1995). Situation awareness in team performance: Implications for measurement and training. *Human Factors: The Journal of the Human Factors and Ergonomics Society, 37*(1), 123-136.
[25] SALAS, E. DICKINSON, T. L., CONVERSE, S. A., & TANNENBAUM, S. I. (1992). Toward an understanding of team performance and training. In R. W. SWEZEY & E. SALAS [eds.], *Teams: Their training and performance* (pp. 3-29). Norwood, NJ: Ablex.
[26] STANARD, T., THORDSON, M., MCCLOSKEY, M., & VINCENT, P. (2001). *Cognitive Task Analysis and Work-Centered Support System Recommendations for a Deployed Network Operations Support Center.* Air Force Research Laboratory.
[27] SHIRAVI, H., SHIRAVI, A., & GHORBANI, A. (2011). A survey of visualization systems for network security. *Visualization and Computer Graphics, IEEE Transactions on,* (99), 1-1.
[28] SHU, Y., & FURUTA, K. (2005). An inference method of team situation awareness based on mutual awareness. *Cognition, Technology & Work, 7*(4), 272-287.
[29] STOTZ, A., & SUDIT, M. (2007). Information fusion engine for real-time decision-making (INFERD): A perceptual system for cyber attack tracking. *Information Fusion, 2007 10th International Conference on,* 1-8.
[30] TAYLOR, R. (1990). Situational awareness rating technique(SART): The development of a tool for aircrew systems design. *AGARD, Situational Awareness in Aerospace Operations 17 p(SEE N 90-28972 23-53),*
[31] United States Federal Chief Information Officer's Council. (2006). *Federal IT Workforce Survey 2006 Data Analysis Report: Information for Human Capital Planning.* Washington.
[32] United States Government Accountability Office. (2011). *Cybersecurity human capital: Initiatives need better planning and coordination.* Washington D.C.