Cyber Friendly Fire: Research Challenges for Security Informatics

Frank L. Greitzer
PsyberAnalytix LLC
Richland, Washington 99352
Email: Frank@PsyberAnalytix.com

Thomas E. Carroll
Pacific Northwest National Laboratory
P.O. Box 999, MS-IN K3-12
Richland, Washington 99352
Email: Thomas.Carroll@pnnl.gov

Adam D. Roberts
Pacific Northwest National Laboratory
P.O. Box 999, MS-IN J4-45
Richland, Washington 99352
Email: Adam.Roberts@pnnl.gov

***Abstract*—This paper addresses cognitive implications and research needs surrounding the problem of cyber friendly fire (FF). We define cyber FF as *intentional offensive or defensive cyber/electronic actions intended to protect cyber systems against enemy forces or to attack enemy cyber systems, which unintentionally harms the mission effectiveness of friendly or neutral forces*. Just as with combat friendly fire, maintaining situation awareness (SA) is paramount to avoiding cyber FF incidents. Cyber SA concerns knowledge of a system's topology (connectedness and relationships of the nodes in a system), and *critical knowledge elements* such as the characteristics and vulnerabilities of the components that comprise the system and its nodes, the nature of the activities or work performed, and the available defensive and offensive countermeasures that may be applied to thwart network attacks. Mitigation strategies to combat cyber FF—including both training concepts and suggestions for decision aids and visualization approaches—are discussed.**

I. Introduction

While friendly fire (FF) is a familiar term, cyber FF is a new concept for the information security community, who is just beginning to grasp the concept. To date there have been two published definitions of cyber FF. The first, from Greitzer *et al.* [1], is:

> *Cyber Fratricide, or cyber friendly fire, refers to intentional, offensive, or defensive cyber/electronic actions intended to protect cyber systems against enemy forces or to attack enemy cyber systems, which result in inhibiting, damaging, or destroying friendly or neutral infrastructure or operations.*

Andrews and Jabbour [2] provide the second:

> *The employment of friendly cyber defenses and weapons with the intent of either defending the blue cyber systems from attack from red or gray forces, or attacking the enemy to destroy or damage their people, equipment, or facilities, which results in unforeseen and unintentional damage to friendly cyber systems.*

These definitions have many similarities: cyber FF is a consequence of offensive or defensive actions, the actions were performed with purpose, and the damage occurs to friendly or neutral cyber assets. Both definitions imply or overtly identify consequences of the action as unintentional. Furthermore, incidents that are born from accidents, negligence, carelessness, or malicious insiders are not friendly fire. From there, the definitions diverge. Greitzer et al. consider harm to both cyber systems and mission effectiveness, while Andrews and Jabbour focus only on systems. A recent Air Force chief scientist's report on technology horizons mentions the need for "a fundamental shift in emphases from 'cyber protection' to 'maintaining mission effectiveness' in the presence of cyber threats" [3]. Thus, mission effectiveness, and not only systems, is an appropriate focus for friendly fire incidents. In addition, we argue that cyber FF consequences may be felt well beyond cyber space. Consider cyber physical systems that closely integrate physical, computational, and communication components to sense and effect changes in the real world. These systems are heavily employed in critical infrastructure to control and monitor processes. Adversely impacting the operation of these systems may result in large-scale power failures, toxic waste releases, or explosions that can have catastrophic consequences on the environment and life.

With this discussion in mind, we offer the following revised definition of cyber FF:

> *Cyber friendly fire is intentional offensive or defensive cyber/electronic actions intended to protect cyber systems against enemy forces or to attack enemy cyber systems, which unintentionally harms the mission effectiveness of friendly or neutral forces.*

The following two examples illustrate cyber FF incidents that derive from defensive actions that unintentionally harm the organization's missions:

Illustrative Example 1. Company XYZ moved their corporate website and email to a hosting company to save money. A hacker who obtained an administrator's account on the hosting company's servers begins to disrupt services by attempting to hack into Company XYZ's hosted web server. An administrator at Company XYZ notices this hacking activity and quickly takes actions to protect company resources by blocking traffic from the hosting company. Company XYZ is no longer able to obtain access to their corporate website or their email, both of which reside at the hosting company.

Illustrative Example 2. A current vulnerability to widely-deployed web serving software is being actively exploited.

978-1-4673-6213-9/13/$31.00 ©2013 IEEE

The vendor for the software has issued a security patch. Company XYZ, who relies on the software as a critical component of their e-business platform, rapidly deploys the fix on their infrastructure. The patch introduces a problem into the software, causing transactions to fail and frustrating potential customers who are attempting to purchase the company's products.

The next examples illustrate defensive actions that unintentionally harm friendly assets, but do not constitute FF:

Illustrative Example 3. Company XYZ stores client personally identifiable information in a central database. The database is compromised by an adversary, who then actively engages in exfiltrating the stored data. Company XYZ administrators detect the extrusion of data and take action to stem the flow of data by severing the Internet connection until they can remediate and recover from the attack. The administrators fully comprehend that no client is able to access the company's services while disconnected, but the induced harm is far less than harm of continued data exfiltration.

Illustrative Example 4. A network administrator is writing a new firewall rule to block specific malicious network traffic. Before the rule can be completed, the administrator's Bengal cat leaps onto her keyboard, depressing several keys, which mangles and activates the rule. The rule disrupts traffic to the company's web server cluster, inhibiting clients from processing products.

II. Cognitive Approaches to Cyber Friendly Fire Research

The concept of cyber FF is similar in many respects to combat friendly fire [1], and from a cognitive perspective, the fundamental issue is with maintaining situation awareness (SA). The scientific literature on SA is substantial and no attempt is made here to report exhaustively on this topic. In short, the most accepted definition of SA is given by Endsley [4]: SA is the perception of the elements in the environment within a volume of time and space (Level 1 SA), the comprehension of their meaning (Level 2 SA), and the projection of their status into the future (Level 3 SA).

SA depends on an accurate mental model [5]. Mental models have been described as well-defined, highly organized, and dynamic knowledge structures that are developed over time from experience (e.g., [6]). By representing organized "chunks" of information in the environment, mental models serve to reduce the information load that would otherwise overwhelm the ability of decision makers to attend, process, and integrate the large amount of information that is inherent in complex operational environments. Cues in the environment activate these mental models, which in turn guide the decision-making process. Appropriate and effective mental models enable experienced decision makers to correctly assess and interpret the current situation (Level 1 and Level 2 SA) as well as to select an appropriate action based on patterns (mental models) stored in their long-term memory [7].

A. Cyber Situation Awareness

Considering that a lack of SA is often a contributing factor to human errors in decision making, it is clear that a study of cyber FF should focus on factors that affect the cyber security officer's/system administrator's SA. What constitutes cyber SA?

Tadda and Salerno [8] mapped constructs of SA to more cyber-relevant network environments. A SA process model was constructed that has general applicability as well as specific relevance to cyber SA. The paper also suggested a set of metrics that may be useful in assessing the effectiveness of tools for supporting SA. Consistent with Tadda and Salerno's characterization of SA, our notion of cyber SA focuses on knowledge of a system's topology (connectedness and relationships of the nodes in a system), the characteristics and vulnerabilities of the components that comprise the system (and populate the nodes), the nature of the activities or work performed, and the available defensive (and offensive) countermeasures that may be applied to thwart network attacks. SA must also include an understanding of *why* each node exists, *what* it is doing, and the harm associated with disrupting that function as a response to attack. The trade-offs between accepting the ongoing risks of attack must be properly balanced against the damage done to the overall organization's mission, and the process of balancing those elements should motivate and guide the defender to select responses that minimize the total amount of harm.

More specifically, we may speculate on implications for cyber defense and cyber SA based on the notion of "digital SA."[1] Given the complexity of cyber structures (particularly at the national scale of critical infrastructures such as the Internet or the electric power grid), it is necessary to take a "system of systems" perspective. In this view, there is never 100 percent certainty or complete knowledge, and it must be assumed that systems will be attacked (*i.e.*, it is not possible to prevent all attacks with certainty). Thus, an appropriate cyber security strategy is *resiliency*, *i.e.*, the ability to anticipate, avoid, withstand, minimize, and recover from the effects of attacks (or for that matter, from the effects of natural disasters). To anticipate and avoid the effects of attacks or other adverse circumstances, a high level of SA is required. In particular, there is a critical need for operators to *anticipate* and *apply protocols* to avoid *cascade effects* in the network, thereby avoiding unintended consequences of defensive or offensive actions. The following types of knowledge (*critical knowledge units*) are required to invoke this anticipatory process:

- Knowledge of each enterprise, enterprise's network structure, and network component
- Knowledge of each computer system of interest in each enterprise/component
- Knowledge of each I/O port on each computer and how it is being used
- Record of traffic flow and volume on every I/O port

[1] The following discussion is based in part on an essay on situation awareness in Wikipedia: http://en.wikipedia.org/wiki/Situation_awareness

- Knowledge of the results of computing expected during the normal operation of each of the components in the network based on the current traffic flow and volume
- Knowledge of operating limits for each component, enabling the decision maker to project "faults" that may lead to shutdowns and cascade failures
- Knowledge of alternative corrective actions for such faults.

An additional consideration regarding the role of SA and cognitive models in cyber FF is the importance of Team SA: the degree to which each team member possesses the SA required for his or her responsibilities [4] and in particular, the extent to which team members possess the same SA on *shared* SA requirements [9], [10]. Conflicts between goals and/or failures to coordinate goals among different members of the team are major underlying/root causes of many cyber FF incidents.

Given these considerations, a recommended approach to study SA and cyber FF is to adopt a cognitive systems perspective, and particularly a naturalistic decision making approach, to capture the mental models that constitute the above types of knowledge. Implications for training and/or tool development include:

- A strategy to train operators within this naturalistic decision-making paradigm to raise awareness and understanding of the above critical knowledge units.
- A tool development strategy to design and implement decision aids and/or visualizations that support the acquisition of, or use of, the above critical knowledge units.

B. *Four Trends That Make Digital SA Harder*

Four current trends greatly increase the difficulty of performing digital SA.

(1) First, missions are defined in terms of abstract resources and not actual systems and devices. For example, a mission in support of business-to-business portal is defined in terms of number of concurrent users and user experience attributes, such as page response time. The requirements are translated into resource and location requirements (e.g., "ten web servers in the East Coast data center will be tasked for this mission"). The mission planner may never be aware of what actual resources are allocated, the underlying network topology, or where the resources are even geographically located.

(2) The second trend that makes digital SA hard is that organizations are outsourcing the responsibility of infrastructure to third party providers who build and maintain an independent infrastructure that concurrently supports one or more autonomous organizations. The provider may not be external—it may be a separate department within the organization that supports all the organization's missions (e.g., Defense Information Systems Agency (DISA) supports the IT infrastructure for the DoD). Infrastructure As A Service (IAAS) exemplifies this practice. The provider may, at its discretion and in compliance with Service Level Agreements (SLAs), perform maintenance that may temporarily disrupt service; depending on the sensitivities of missions, this may reduce effectiveness. Combined with Trend 1, communication between the parties is difficult because organizations speak/plan in terms of missions while the provider speaks/plans in terms of resources.

(3) Dynamic management of resources, as seen in cloud, grid, and utility computing environments, make for flexible resource allocations that are revised with changing demands and requirements. Even if the users are certain about the identity of the resources at a time t, the cloud management may choose to migrate at time $t+1$ the processes to systems made up of different components that exist on a different continent. And of course, the underlying network topology is modified too.

(4) Finally, organizations are augmenting their networks with increasingly large number of sensors, which, as one may expect, is overloading human analysts with oceanic volumes of data. The theory behind this trend is that by capturing all information available at the device and network level that detection of any and all attacks would be possible. Unfortunately, there has not been a corresponding improvement in data fusion, analysis, and detection methods, and the vast amounts of data have swamped analysts.

III. Mitigation Approaches

In this section, we describe approaches and tools to mitigate cyber FF.

A. *Training*

To address training requirements and approaches to reduce cyber FF, it is useful to examine factors that impact cognition and human performance, particularly with regard to SA. Research has demonstrated a number of factors that impact performance; in the present context, effects of stress, overlearning, and issues relating to cognitive bias are particularly relevant. Greitzer and Andrews [11] review cognitive foundations and implications for training to mitigate combat friendly fire. Here we describe aspects of this research that are pertinent to training requirements for cyber FF.

1) Effects of Stress on Performance: Stress has strong effects on every aspect of cognition from attention to memory to judgment and decision making. Under stress, attention appears to channel or tunnel, reducing focus on peripheral information and centralizing focus on main tasks [12]. Originally observed by Kohn [13], this finding has been replicated often, first by seminal work from Easterbrook [14] demonstrating a restriction in the range of cues attended to under stress conditions (tunneling) and many other studies (see [15]). Research by Janis and Mann [16] suggests that peripheral stimuli are likely to be the first to be screened out or ignored, and that under stress, individuals may make decisions based on incomplete information. Similarly, Friedman and Mann [17] note that individuals under stress may fail to consider the full range of alternatives available, ignore long-term consequences, and make decisions based on oversimplifying assumptions—often referred to as heuristics. Research on the effects of stress on vigilance and sustained attention, particularly regarding effects of fatigue and sleep deprivation, shows that vigilance tends to be enhanced by moderate levels of arousal (stress), but sustained attention appears to decrease with fatigue and loss of sleep [18].

2) Overlearning: Several investigations have shown that tasks that are well-learned tend to be more resistant to the effects of stress than those that are less-well-learned. Extended practice leads to commitment of the knowledge to long term memory and easier retrieval, as well as automaticity and the proceduralization of tasks. These over-learned behaviors tend to require less attentional control and fewer mental resources [19], [20], which facilitates enhanced performance and yields greater resistance to the negative effects of stress—*i.e.*, overlearned behaviors are less likely to be forgotten and more easily recalled under stress. Van Overschelde and Healy [21] found that linking new facts learned under stress with preexisting knowledge sets helps to diminish the negative effect of stress. On the other hand, there is also a tendency for people under stress to "fall-back" to early-learned behavior [22]–[24]—even less efficient or more error prone behavior than more recently-learned strategies—possibly because the previously learned strategies or knowledge are more well-learned and more available than recently acquired knowledge.

3) Effects of Stress on Learning: Research suggests that high stress during instruction tends to degrade an individual's ability to learn. The research literature consistently demonstrates that elements of working memory are impaired, although the mechanisms behind these effects are poorly understood [15]. Stress appears to differentially affect working memory phases [25], [26]. One instructional strategy to address stress effects is to use a phased approach with an initial learning phase under minimum stress, followed by gradual increasing exposure to stress more consistent with real-world conditions [11]. Similarly, stress inoculation training attempts to immunize an individual from reacting negatively to stress exposure. The method provides increasingly realistic pre-exposure to stress through training simulation; through successive approximations, the learner builds a sense of positive expectancy and outcome and a greater sense of mastery and confidence. This approach also helps to habituate the individual to anxiety-producing stimuli.

4) Team Performance: Finally, it is important to consider group processes in this context. Research on team decision making indicates that effective teams are able to adapt and shift strategies under stress; therefore, team training procedures should teach teams to adapt to high stress conditions by improving their coordination strategies. Driskell, Salas, and Johnston [27] observed the common phenomenon of Easterbrook's attentional narrowing is also applicable to group processes. They demonstrated that stress can reduce group focus necessary to maintain proper coordination and SA—*i.e.*, team members were more likely to shift to individualistic focus than maintaining a team focus.

5) Implications: Based on the foregoing discussion, we can summarize the challenges and needs for more effective training in general terms as well as more specifically focused on cyber defense and mitigation of cyber FF: training should incorporate stress situations and stress management techniques, development of realistic scenarios that systematically vary stress (e.g., as produced by varying cognitive workload through tempo of operations and density of attacks), and addressing challenges in preparing cyber warriors to overcome cognitive biases. The following factors should be included in designing training approaches:

- Training should provide extended practice, promoting more persistent memory and easier retrieval, and to encourage automaticity and the proceduralization of tasks to make them more resistant to the effects of stress.
- Training scenarios should include complex/dynamic threats that reflect the uncertainties of the real world—scenarios that force trainees to operate without perfect information and that incorporate surprises that challenge preconceptions or assumptions.
- Training scenarios should be designed to encourage the habit of testing one's assumptions to produce more adaptive, resilient cyber defense performance in the face of uncertainty.
- Training should enhance awareness of the effects of stress on cognitive performance—such as tunneling and flawed decision making strategies that ignore information—and coping strategies to moderate these effects. The training should be designed to make as explicit as possible what might happen to skill and knowledge under stress.
- Train awareness of cognitive biases and practices for managing these biases
- Emphasize habits of testing assumptions and moving beyond traditional reactive behaviors to train techniques for more adaptive, resilient performance in the face of uncertainty.
- Team training should focus on strategies for maintaining group cohesion and coordination, mitigating the tendency for team members to revert to an individual perspective and lose shared SA.
- Training should exercise the execution of cognitive tasks by both individuals and groups.

B. Tools

A key objective in the study of factors influencing cyber FF and mitigation strategies is to identify features of decision support tools with potential to reduce the occurrence of cyber FF. Our review of relevant research, as summarized in the foregoing discussion, strongly suggests that tools and visualizations to improve cyber SA are key ingredients of desired solutions. Important functions should include decision aids to support memory limitations, to counteract the negative effects of stress on performance (e.g., perceptual narrowing), and to avoid the negative consequences of cognitive biases on decisions.

1) Supporting Memory Limitations that Reduce Situation Awareness: As stated earlier, support for the cyber analyst should strive to encourage proactive decision making processes that anticipate and apply protocols to avoid cascade effects in the network, and concurrently avoid unintended consequences of defensive or offensive actions. We identified a set of critical knowledge units required for enhanced SA and anticipatory decision making, including knowledge of components of the network, details of each computer system, I/O ports, traffic flow/volumes, and ability to project impacts of possible courses of action. Decision aids and/or visualization support is needed to alleviate memory lapses and limitations by providing readily accessible information on network topology and component assets/vulnerabilities —typically referred to as external representations or external memory by researchers advocating the study of "distributed cognition" in the broader context of the social and physical environment that must be interwoven with the decision maker's internal representations (also referred to as "situated cognition" [28], [29]). Thus, a decision aid that displays critical knowledge units for components that are being considered for application of remedial actions may help to avoid cyber FF effects that impair system effectiveness. This concept is similar to what Tadda and Salerno [8] refer to as "Knowledge of Us" (data relevant to the importance of assets or capabilities of the enterprise)—hence, a process that identifies to the decision maker whether there is a potential or current impact to capabilities or assets used to perform a mission. Similarly, a tool may be envisioned that helps the decision maker understand and prioritize risks that may be computed for various possible alternative actions.

2) Mitigating Cognitive Biases: Gestalt psychology tells us that we tend to see what we expect to see. Expectancy effects can lead to such selective perception as well as biased decisions or responses to situations in the form of other cognitive biases like confirmation bias (the tendency to search for or interpret information in a way that confirms one's preconceptions) or irrational escalation (the tendency to make irrational decisions based upon rational decisions in the past). The impact of cognitive biases on decision performance—particularly response selection—is to foster decisions by individuals and teams that are based on prejudices or expectations that they have gained from information learned before they are in the response situation. Decision aids and visualizations are needed that help to reduce confirmation bias, irrational escalation, and other forms of impaired decision making. One possible form of decision support designed to counteract these biases is the use of the analysis of competing hypotheses (e.g., [30]). Other concepts that may serve as sources of ideas and strategies for the design of decision aids may be derived from problem solving techniques discussed by Jones in The Thinker's Toolkit [31].

C. Implications

Based on the foregoing discussion, we summarize the challenges and needs for more effective training and decision support to improve cyber defense and mitigate cyber FF:

- Training recommendations
  - Incorporate stress situations and stress management techniques
  - Develop realistic scenarios that systematically vary stress (e.g., as produced by varying cognitive workload through tempo of operations and density of attacks)
  - Address challenges in preparing cyber warriors to overcome cognitive biases
  - Conduct experiments to assess effectiveness of different training approaches
- Information analysis and decision support recommendations
  - Conduct experiments to help identify effective features of decision support and information visualization tools. Will conventional training approaches to improve analytic process (e.g., analysis of alternative hypotheses, other decision making tools and strategies) be effective in the cyber domain? Our intuition suggests that the answer is "no" because of the massive data, extreme time constraints requiring near real-time responses, and the largely data-driven nature of the problem. New types of data preprocessing (triage) and visualization solutions will likely be needed to improve SA.
  - Perform cognitive engineering research to develop prospective information analysis and visual analytics solutions to enhance SA and decrease cyber FF.

IV. Conclusions and Future Direction

Research in cyber FF should be founded upon scientific principles and empirical studies in human factors and cognitive engineering, such as seminal human factors work on SA by Endsley [4] and later by Tadda and Salerno [8], who mapped constructs of SA to more cyber-relevant network environments. The present paper has sought to define research questions and to lay a foundation for empirical investigations of factors contributing to the cyber FF phenomenon and impacts on performance of proposed mitigations that can be in the form of training/awareness or decision aids.

Along these lines, we conducted a preliminary study at PNNL to help address these research questions; detailed description of the testbed and experimental methods are provided in [32]. In brief, we created a virtual e-commerce business in a cyber security testbed and performed a pilot study to demonstrate feasibility of an experimental methodology to assess effectiveness of decision aids and visualizations for cyber security analysis. Because the experiment was limited to a very small number of participants, interpretation of results was speculative, but the design and implementation of the testbed itself serve to advance the research goals described here. Related research is ongoing: An advanced concept that is currently being pursued by PNNL cyber security research programs is the notion of Asymmetric Resilient Cybersecurity (ARC)[2], which is characterized by goals of standing up resilient and robust cyber infrastructure and network architectures that present a "moving target" to potential attackers in an attempt to overcome and hopefully reverse the current asymmetric state of affairs that favors the adversary. The goals and challenges of this program align with issues (and in ways can be seen as amplifying the cyber FF challenge—consider maintaining enterprise-wide SA when the network, systems, and components continuously an dynamically "move") that we

[2] Information about PNNL's Asymmetric Resilient Cybersecurity (ARC) Lab Direct Research & Development Initiative can be found at: http://cybersecurity.pnnl.gov/arc.stm

have articulated in our research on cyber FF. This research also directly meets essential needs of DOE cyber security and counterintelligence (DOE CIO, DOE-IN) as well as cyber security programs within the DoD and the intelligence community.

The fundamental research goal is to develop a scientific understanding of the behavioral implications of cyber FF. Research is needed to extend our current understanding of cyber SA and to develop metrics and measures for cyber FF. The principal scientific research questions include: What are root causes of cyber FF? What are possible mitigating solutions, both human factors and technical/automated? We have examined relevant research and cognitive theory, and we have taken some initial steps toward investigating these research questions in empirical laboratory studies using realistic test scenarios in a cyber SA/FF testbed facility [32]. Continued empirical research is required to investigate the phenomenon and relevant contributing factors as well as mitigation strategies. A major objective should be to investigate approaches to and assessment of effectiveness of cyber FF mitigation strategies, such as training and decision aids/tools. Such research promises to advance the general field of cyber SA and inform other ongoing cyber security research. In addition, it is hoped that this research will facilitate the design and prototyping of automated or semi-automated systems (or decision aids) to increase cyber SA and eliminate or decrease cyber FF; this provides a foundation for development of commercial products that enhance system effectiveness and resiliency.

Acknowledgment

The authors wish to express appreciation to Dr. Dee Andrews, who provided 2009–2011 funding from the AFRL Human Effectiveness Directorate to support this research. Portions of the research were also funded by PNNL's Asymmetric Resilient Cybersecurity (ARC) Laboratory Research & Development Initiative. The views expressed in this report are the opinions of the Authors, and do not represent official positions of the Pacific Northwest National Laboratory, the Department of Energy, or the Air Force Research Laboratory.

References

[1] F. L. Greitzer, S. L. Clements, T. E. Carroll, and J. D. Fluckiger, "Towards a research agenda for cyber friendly fire," Pacific Northwest National Laboratory, Tech. Rep. PNNL-18995, 2009.

[2] D. H. Andrews and K. T. Jabbour, "Mitigating cyber friendly fire: A sub-category of cyber mishaps," *High Frontier*, vol. 7, no. 3, pp. 5–8, 2011.

[3] United States Air Force Chief Scientist (AF/ST), "Report on technology horizons: A vision for Air Force Science & Technology during 2010–2013," 2010.

[4] M. R. Endsley, "Towards a theory of situation awareness in dynamic systems," *Human Factors*, vol. 37, no. 1, pp. 32–64, 1995.

[5] N. Sarter and D. Woods, "Situation awareness: A critical ill-defined phenomenon," *International J. Aviation Psychology*, vol. 1, no. 1, pp. 45–57, 1991.

[6] S. W. J. Kozlowski, "Training and developing adaptive teams: Theory, principles, and research," in *Making Decisions Under Stress: Implications for Individual and Team Training*, J. A. Cannon-Bowers and E. Salas, Eds. Washington, D.C.: America Psychological Association, 1988.

[7] D. Serfaty, J. MacMillan, E. E. Entin, and E. B. Entin, "The decision-making expertise of battle commanders," in *Naturalistic Decision-Making*, C. E. Zsambok and G. Klein, Eds. New York: Lawrence Erlbaum, 1997.

[8] G. P. Tadda and J. S. Salerno, "Overview of cyber situation awareness," in *Cyber Situational Awareness: Issues and Research*, S. Jajodia, P. Liu, V. Swarup, and C. Wang, Eds. New York: Springer, 2010, pp. 15–35.

[9] M. R. Endsley and W. M. Jones, "Situation awareness, information dominance, & information warfare," US Air Force Armstrong Laboratory, Tech. Rep. AL/CF-TR-1997-0156, Feb. 1997.

[10] ——, "A model of inter- and intrateam situation awareness: Implications for design, training, and measurement," in *New Trends in Cooperative Activities: Understanding System Dynamics in Complex Environments*, M. McNeese, E. Salas, and M. Endsley, Eds. Santa Monica, CA: Human Factors and Ergonomics Society, 2001.

[11] F. L. Greitzer and D. H. Andrews, "Training strategies to mitigate expectancy-induced response bias in combat identification: A research agenda," in *Human Factors Issues in Combat Identification*, D. H. Andrews, R. P. Herz, and M. B. Wolf, Eds., 2010.

[12] J. Kavanagh, "Stress and performance: A review of the literature and its applicability to the military," RAND, Tech. Rep. TR-192, 2005.

[13] H. Kohn, "Effects of variations of intensity of experimentally induced stress situations upon certain aspects of perception and performance," *J. Genetic Psychology*, vol. 85, pp. 289–304, 1954.

[14] J. A. Easterbrook, "The effect of emotion on cue utilization and the organization of behavior," *Psychological Review*, vol. 66, pp. 183–201, 1959.

[15] M. A. Staal, "Stress, cognition, and human performance: A literature review and conceptual framework," National Aeronautics and Space Administration, Tech. Rep. NASA/TM-2004-212824, Aug. 2004.

[16] I. L. Janis and L. Mann, *Decision Making*. New York: The Free Press, 1977.

[17] I. A. Friedman and L. Mann, "Coping patterns in adolescent decision-making: An Israeli-Australian comparison," *J. Adolescence*, vol. 16, pp. 187–199, 1993.

[18] D. R. Davies and G. S. Tune, *Human Vigilance Performance*. London: Staples Press, 1970.

[19] J. Leavitt, "Cognitive demands of skating and stick handling in ice hockey," *Canadian J. Applied Sport Sciences*, vol. 4, pp. 46–55, 1979.

[20] M. D. Smith and C. J. Chamberlin, "Effect of adding cognitively demanding tasks on soccer skill performance," *Perceptual and Motor Skill*, vol. 75, pp. 955–961, 1992.

[21] J. P. Van Overschelde and A. F. Healy, "Learning of nondomain facts in high- and low-knowledge domains," *J. Experimental Psychology: Learning, Memory, and Cognition*, vol. 27, pp. 1160–1171, 2001.

[22] M. Allnutt, "Human factors: Basic principles," in *Pilot Error*, R. Hurst and L. R. Hurst, Eds. New York: Aronson, 1982, pp. 1–22.

[23] R. P. Barthol and N. D. Ku, "Regression under stress to first learned behavior," *J. Abnormal & Social Psychology*, vol. 59, no. 1, pp. 134–136, 1959.

[24] R. B. Zajonc, "Social facilitation," *Science*, vol. 149, pp. 269–274, 1965.

[25] S. Kuhlmann and O. T. Wolf, "Arousal and cortisol interact in modulating memory consolidation in healthy yound men," *Behavioral Neuroscience*, vol. 120, no. 1, pp. 217–223, 2006.

[26] S. Kuhlmann, M. Piel, and O. T. Wolf, "Impaired memory retrieval after psychosocial stress in healthy young men," *J. Neuroscience*, vol. 25, no. 11, pp. 2977–2982, 2005.

[27] J. E. Driskell, E. Salas, and J. Jonston, "Does stress lead to a loss of team perspective?" *Group Dynamics: Theory, Research, and Practice*, vol. 3, pp. 291–302, 1999.

[28] D. A. Norman, *The Psychology of Everyday Things*. Basic Books, 1988.

[29] J. Hollan, E. Hutchins, and D. Kirsh, "Distributed cognition: Toward a new foundation for human-computer interaction research," *ACM Transactions on Computer-Human Interaction*, vol. 7, no. 2, pp. 174–196, 2000.

[30] R. J. Heuer, Jr., "Analysis of competing hypotheses," in *Psychology of Intelligence Analysis*. Center for the Study of Intelligence, Central Intelligence Agency, 1999.

[31] M. D. Jones, *The Thinker's Toolkit: Fourteen Powerful Techniques for Problem Solving*. New York: Three Rivers Press, 1998.

[32] F. L. Greitzer, T. E. Carroll, and A. D. Roberts, "Cyber friendly fire," Pacific Northwest National Laboratory, Tech. Rep. PNNL-20821, Sep. 2011.