Training to Instill a Cyber-Aware Mindset

Kelly Neville[1(✉)], Larry Flint[2], Lauren Massey[1], Alex Nickels[1],
Jose Medina[1], and Amy Bolton[3]

[1] Soar Technology, Inc., Ann Arbor, MI 32817, USA
Kelly.neville@soartech.com
[2] Ingenia Services, LLC, Wake Forest, NC 27587, USA
[3] Office of Naval Research, Arlington, VA 33303, USA

Abstract. The rapidly increasing sophistication of cyber threats occurring in parallel with our growing reliance on networked systems for everything from shopping to managing critical infrastructure is not a coincidence. Ransomware events, compromise of personal financial information, and hacking into critical infrastructure systems make the headlines on a seemingly daily basis. Still, the average system user continues to operate in a mode that signals belief those events will happen to someone else. This paper presents work conducted to determine training objectives and strategies for altering that "other guy" mentality and instilling a *cyber-aware mindset*. System users with a cyber-aware mindset should be less likely to fall for attacker ploys and more likely to actively contribute to their organization's cyber defense. We identify two major categories of training objectives: cyber awareness and mindset objectives. *Cyber awareness training objectives* encompass three main areas of knowledge and capability: system baseline performance, anomaly detection and response, and systems thinking. *Mindset training objectives* encompass cognitive adaptations associated with acquiring a new mindset. These are adaptations to knowledge structures, cognitive heuristics, and metacognition. These training objectives are being used to guide the design of a scenario-based video game for training a cyber-aware mindset. This work highlights the importance of relevant conceptual knowledge to cyber awareness and research needs associated with mindset change, including mindset-change measurement, which we have begun to address for the purpose of evaluating the video game's efficacy.

Keywords: Cyber awareness · Mindset training · Cognitive bias training

1 Introduction

Over the last three decades, individuals and organizations alike have increasingly moved their daily life into the digital realm. In cyberspace, we connect socially, interact professionally, and find ever-available sources of entertainment. We use it for shopping, banking, filing taxes, applying for government services, managing healthcare, sharing accomplishments, storing documents, traveling, finding recipes, displaying our family photo albums, educating ourselves, and much more. We are now, as individuals, families, organizations, and societies, heavily invested in the digital realm, and our most valuable information has become extensively interwoven into its fabric.

D. D. Schmorrow and C. M. Fidopiastis (Eds.): HCII 2019, LNAI 11580, pp. 299–311, 2019.
https://doi.org/10.1007/978-3-030-22419-6_21

The transition to cyberspace by consumers, corporations, and government agencies has provided new, interesting, and profitable opportunities for nefarious actors. Ranging from mischievous hooligans to criminal organizations to nation states the population of malicious cyber citizens has grown in step with the law-abiding population. According to the 2018 Verizon Data Breach Investigations Report, the year 2017 saw over 53,000 data breach incidents and 2,216 confirmed data breaches in industry. Among these were sophisticated multi-pronged attacks such as a set of coordinated bank heists that reaped over $40 million (Trustwave 2018). Cyber attackers have demonstrated an ability to outsmart, on a large scale, heavily defended systems. Their creativity and resourcefulness coupled with continued growth in proficiency, poses serious threats to all organizations, services, governments, and economies.

1.1 Every System Is at Risk

Many organizations, including many U.S. military organizations, keep their most sensitive data and capabilities on isolated systems and networks. The so-called air gap may slow down cyber attackers but it does not deter them. For example, Russian hackers have gained entry to hundreds of air-gapped U.S. utilities (Greenberg 2017; Smith 2018) via conventional spearfishing and watering hole attacks on utility vendors (Greenberg 2017) and reportedly continue to do so. The hackers stole vendor credentials and used them to directly access utilities' networks and collect information about network configurations, software, hardware, administrative accounts, and more. One report indicates that the hackers could have "thrown switches" and "disrupted power flows" (Greenberg 2017). The same malware found on U.S. utility networks has been used to wreak havoc in the Ukraine, shutting down the electrical grid, blocking operators from using their own systems to intervene, and shutting down battery backups to the operations facilities (Greenberg 2017; Smith 2018).

Military organizations are especially at risk for being targeted by cyber attack. While security of consumer financial transactions is critical, the military relies on networks, including commercial infrastructure, for our nation's defense. Their networks represent a treasure trove of data that could be used to an adversary's significant advantage. They likewise support a trove of invaluable capability that a cyber attack could cripple or co-opt.

Improving our military's ability to operate and defend itself in cyberspace is an operational imperative; defending our networks and the systems relying on those networks is fundamental to maintaining supremacy in the cyber domain. To that end, the U.S. Department of Defense has taken strides to improve the numbers and effectiveness of skilled professional cyber defenders and to provide for effective training of cyber operators. However, they are a finite resource faced with attackers who patiently probe the perimeter and all avenues of approach to identify cyber vulnerabilities.

1.2 Everyone Is a Sensor

The maturing sophistication of attack methods, increased complexity of our networks, and sheer persistence work to the advantage of the attacker. The nature of networks and our reliance on them (required access by all hands) increases the attack surface as every individual with network access is a potential threat vector. Accordingly, attackers regularly incorporate human threat vectors into their tactics. Cyber intrusions that led to the bank heists mentioned above were enabled by social engineering via both phone calls and phishing emails (Trustwave 2018). The Ukrainian power outage attacks began with a phishing email impersonating a message from the Ukrainian parliament (Greenberg 2017).

Although the potential to gain system access through operator inattention, error, gullibility, or negligence cannot be eliminated, it can be diminished with training. Furthermore, we propose that with training, system operators' role can be elevated from that of threat vector and vulnerability to one of threat deflector and strength. We propose that with training, human operators can be leveraged as sensors, providing warnings and indications of an attack that may be undetected by cyber operators.

Because cyber attacks are inherently difficult to deter and detect, effective defensive strategies require a holistic and layered approach. System operators or users should be at least one of those layers. Although system operators may lack the expertise to distinguish routine technical anomalies from intentional malicious activity, they nevertheless can play an important role in cyber security. For example, operators can alert cyber professionals about unusual or indicative symptoms. Cyber-aware operators may also provide professional cyber teams with valuable supporting data, know what additional cues to look for, and gauge whether or not they can continue to use their systems. If not, cyber-aware operators will know how to adapt. As noted by Canham (2019), a cyber attack on an accounting and payroll system is more likely to be detected by the accountant using the system than by software that monitors network activity for anomalous activity.

1.3 Supporting Meaningful Participation

To become an effective layer in their organization's cyber defense, personnel require education, training, and a fundamental appreciation for their critical role in defending the network. A given operator will only infrequently encounter intentional malicious activity on his or her systems. Consequently, remaining vigilant to the possibility of an attack is challenging. Further, researchers have found that control operations personnel remain biased toward treating system anomalies as hardware, electrical, cooling, or product flow problems, versus as problems with software and networks (e.g., Line et al. 2014). As a result, when a cyber intrusion affects system performance, operators may be biased toward assuming a physical, non-cyber source as the cause.

We propose that enabling personnel to support their organization's cyber defense depends on two primary training program elements: Foundational knowledge about cyber threats to operations and high fidelity practice. Knowledge structures, i.e., schemata, mental models, and frames, guide what we perceive and how we understand and responds to situations (Klein et al. 2006; Neisser 1976). Adding cyber threat information to operators' knowledge structures should therefore change how they think about their work. More specifically, it should guide the tuning of attention and metacognition to support vigilance and awareness of cyber attack as a possible source of symptoms. We refer to this tuned vigilance and awareness as a *cyber-aware mindset.*

High-fidelity practice allows attention and metacognition to become tuned to the new cyber-defense responsibility in ways guided by the foundational knowledge and performance feedback (i.e., to evolve into a cyber-aware mindset).

2 Method

2.1 Literature Review

Cyber-aware training objectives were identified by reviewing research literature covering the following topics:

- Training to support incident detection and response in process control operations;
- Cyber operations competency taxonomies; and
- Analyses of the cognitive work of cyber professionals.

As we reviewed, we culled training recommendations for cyber awareness. Similar and overlapping objectives were reconciled to produce a single set.

We also reviewed literature related to mindset change. The literature encompassed:

- Characteristics and culture of high reliability organizations;
- Expertise acquisition in complex cognitive work; and
- Minimizing cognitive bias.

2.2 Iterative Problem Space Assessment and Design

In ongoing assessment and design work, the research team holds weekly meetings to discuss training system development plans and the evolving software prototype in light of training objectives, problem space constraints, and problem space affordances. This process is shaped by literature review findings, team members' experience bases, interviews with intended end users about the performance of their systems, and discussions with other stakeholders.

3 Results

3.1 Cyber Awareness Training Objectives

Cyber awareness training objectives we identified are listed in Table 1 and fall into three major categories:

- System Baseline: Baseline knowledge and disciplined monitoring;
- Anomaly Identification and Reporting: Perceptual learning and supporting knowledge; and
- Systems Thinking: Comprehension of relationships within and affecting your organization's computing systems, mission, and cyber protection system.

Two resources, Paul and Whitley (2013) and Line et al. (2014), were especially influential.

Table 1. Cyber awareness training objectives

System Baseline: Baseline Knowledge and Disciplined Monitoring
Regularly check and maintain the accuracy of your system's configuration.
Maintain awareness of the status of your system's health.
Maintain awareness of the health and status of systems with which your system interacts.
Know what normal system activity (system performance and displayed information) looks like.
Know established indicators of non-normal system functioning.
Use available system utilities to check or monitor system performance and processes for unexpected activity.
Maintain awareness of trends and changes in your system's performance and information displays. Use them to derive expectations for normal system function.
Anomaly Identification and Reporting: Perceptual learning and supporting knowledge
Be able to detect deviations from typical information and system activity patterns, including deviations from typical patterns of deviations. Be able to recognize the absence of information.
Know and be able to recognize the signs of cyber events and other anomalies that have occurred in the past.
Account for information reliability when assessing or reporting anomalous activity.
Know how to report an anomaly in terms that contribute to its evaluation by a cyber analyst.
Systems Thinking: Comprehension of relationships within and affecting your organization's: - **Computing systems and networks,** - **Mission, and** - **Cyber protection system**
Understand how cyber attacks can impact an organization's systems, defenses, and effectiveness.
Be familiar with different attack scenarios, ways the attack can progress over time, and possible outcomes. Understand that attacks tend to unfold over time.
Know that data flows among systems and other system interdependencies. Understand how cyber attack effects cascade over time and across attack phases.
Know how to identify and use alternative resources to compensate for unavailable or compromised systems.

- Paul and Whitley's (2013) investigation of the cyber awareness practices of cyber security analysts responsible for network intrusion detection. They conducted interviews with six analysts and twenty-five hours of observation and then derived a list of forty-four questions analysts ask themselves to establish and maintain awareness of new and ongoing network events.
- Line et al.'s (2014) assessment of cyber awareness in six large Norwegian energy distribution system operators (DSOs). They conducted semi-structured interviews with representatives of six DSOs to assess cyber attack preparedness and identify knowledge gaps. Interview results were compared with the results of the authors' preparatory work investigating the elements of effective cyber situation awareness.

We also consulted taxonomies of cyber security competencies proposed by the National Institute of Standards and Technology (NIST), Carnegie Mellon University Software Engineering Institute, and Intelligence and National Security Alliance (INSA) (Cyber Intelligence Task Force 2015). These competencies contributed only minimally to the list in Table 1 as they are intended for cyber security professionals, not system users. Similarly, much of the research literature on training requirements for cyber security focuses on cyber professionals and, although it had influence, it did not weigh heavily in the determination of training objectives.

3.2 Mindset Training Objectives

The identified mindset training objectives are rooted primarily in the literature on expertise in complex cognitive work. They target the development of:

- Knowledge structures,
- Cognitive heuristics, and
- Skeptical metacognition.

Below, we discuss each area of cognitive development and how it relates to system operators' acquisition of a cyber-aware mindset. Specific training objectives are presented following the discussion.

Knowledge Structures. The term *knowledge structure* encompasses the constructs *template*, *schema*, *frame*, and *mental model.* Researchers have established that experts in complex work domains have elaborate, interconnected knowledge structures that contain both verbal and nonverbal details about the work, work conditions, variability in work conditions, what can happen next, why, and more (e.g., Borko and Livingston 1989; Boulton 2016). These rich, sophisticated knowledge structures enable flexibility, anticipation, and the ability to mentally evaluate options (e.g., Klein 1993; Klein et al. 2006), They affect the way a person interprets incoming information, choices they make, and even what they see and do not see (Klein et al. 2007; Neisser 1976).

In their influential article on the effects of a person's *stress mindset*, Crum et al. (2013) define mindset as "…a mental frame or lens that selectively organizes and encodes information, thereby orienting an individual toward a unique way of understanding an experience and guiding one toward corresponding actions and responses" (p. 717). We assess this mindset definition as consistent with the definition of a knowledge structure, which also "organizes and encodes information," orients, and guides. We hypothesize that a cyber-aware mindset requires knowledge structures that are enriched with knowledge about the cyber landscape.

People experience difficulty in handling information that conflicts with their existing mental model of a situation (e.g., Chi 2005; Feltovich et al. 1988; Lewandowsky et al. 2012). Feltovich and his colleagues demonstrated that people use a range of strategies to discount and rationalize their disregard of conflicting, albeit accurate, information. Endsley (2018) calls attention to the implication that the underlying mental model needs to be changed in order to change behavior. She suggests that to reduce people's vulnerability to misinformation that is consistent with an inaccurate mental model, alternative narratives may need to be introduced "to create a foundation for new information" and "help explain old information in a new light" (p. 1091).

Endsley (2018) suggests that resistance to mental model change might be overcome by using visualization and interactive simulations strategies. Because people have difficulty processing information when it is not addressed by their current knowledge structures, others have suggested the use of interactive simulations that allow learners to learn from mistakes and experience the consequences of an inaccurate mental model (Feltovich et al. 1988; Klein and Baxter 2009). Lewandowsky et al. (2012) point to studies showing "that the continued influence of misinformation can be eliminated through the provision of an alternative account that explains *why*…" (p. 117).

Cognitive Heuristics. *Cognitive heuristics* are mental shortcuts humans use to assess situations and make decisions more efficiently. An example is recalling the last time or last fifty times you encountered a situation similar to the one you are in and making the same decisions. We assume the current situation is approximately the same as it was last time or times and do not invest resources to evaluate the details.

This typically works well and it usually allows us to invest time and effort in other cognitive work. However, if the situation turns into something different from what it was assumed to be, decision and performance mistakes occur. Mistakes committed due to reliance on an incorrect mental model are seen as evidence of a cognitive bias. Reliance on the wrong past situation, for example, is called Framing Bias. Framing Bias relates directly to cyber-aware mindset training. Research on Framing Bias suggests that when people lack experience with cyber-threats, they are unlikely to assess situations through cyber-aware glasses (Cornelissen and Werner 2014). Alternatively, it may be effective to train personnel about cognitive bias and how to avoid it. This training could help operators recognize the tendency to rely on past, pre-cyber-threat experiences that may no longer be relevant or useful. Further, training may reveal new ways to use cognitive heuristics advantageously and may help operators change or update their heuristics.

There is evidence to support the idea that training can be used to reduce cognitive-bias effects. Symborski et al. (2017) demonstrated that video game play that includes feedback and instruction about biases can be effective at reducing the effects of a variety of cognitive bias. Biases addressed by the video game training include the Fundamental Attribution Error (a judgment is made based on a behavior without considering the context and possibly history surrounding the behavior), Bias Blind Spot (we see other's thinking as biased but not our own), confirmation bias (a tendency to only attend to information that confirms our own views), Anchoring Bias (a tendency to anchor on the first option or possibility considered), Representativeness Heuristic (we base our assessment of probability on similarity to past situations without considering data such as actual occurrence rates), and Projection Bias (the tendency to think others share our priorities, attitudes, and beliefs). The research team found positive effects (measured using game performance) immediately after training and three months later.

Morewedge et al. (2015) compared the debiasing effects of sixty minutes spent performing the videogames used by Symborski et al. with thirty minutes spent watching an educational video that explained, demonstrated, and provided mitigations for each bias. Both training formats produced statistically significant reductions in biased thinking and improvements in knowledge about biases. For each of the six biases, the videogame led to improvements that were at least statistically equivalent to those produced by video watching; in most cases, however, improvements were greater for the videogame condition.

These two studies represent a relatively sparse research literature on how to decrease cognitive bias through training. Endsley (2018) remarks on this in her discussion of the role of cognitive bias in creating vulnerability to social engineering tactics used by cyber attackers, saying “far more research is needed” (p. 1091).

Skeptical Metacognition. Metacognition refers to higher order thinking (thinking about thinking) and active control over one’s cognitive processes (e.g., Flavell 1979). Metacognition adapts cognitive work to the demands of a given work activity, environment, and goal set. Among other roles, it can guide our use of cognitive heuristics thereby reducing the likelihood of using a heuristic inappropriately (i.e., of cognitive bias; e.g., Mumford et al. 2007).

By means of training and experience, metacognition can be adapted to perform its oversight duties in a critical and skeptical way. This translates into metacognition that is always alert, questioning, and assessing one’s own cognitive activities and performance. Skeptical metacognition can help operators recognize if they are discounting the risk of cyber attack on their system and when they may be walking into a social engineering trap.

Brand-Gruwel et al. (2005) recommend supporting metacogntive proficiency by using a cognitive apprenticeship training approach that helps to bring internal cognitive processes out into the open. Klein and Borders (2016) developed a technique called ShadowBox$^{\mathrm{TM}}$ that accomplishes this goal of surfacing cognitive processes but without the time requirements that comes with a one-on-one apprenticeship. ShadowBox$^{\mathrm{TM}}$ is a scenario-based technique designed to train people to think like experts in a target domain without requiring the real-time involvement of domain experts. Trainees are asked to rank and justify their rankings for sets of options given to them at decision points ot realistic scenarios. They subsequently compare their rankings and rationale to those of experts. The method has been used successfully to train military personnel to make decisions using a new mindset; specifically, using a good stranger mindset instead of the traditional security mindset (Klein et al., 2018). In a review of their ShadowBox$^{\mathrm{TM}}$ evaluation work, Klein et al. (2018) credit the technique’s ability to produce ‘aha’ moments; i.e., realizations that cause the trainee to reconsider their mindset and mental model. This is yet another aspect of cognitive work that requires more research. The authors note, “Clearly, there is a lot to learn about…how to help people make mindset shifts, how to measure mindset shifts, and how to differentiate mindsets from other cognitive processes” (p. 683). Likewise, very little research exists on the training of metacognition more generally.

Table 2 lists mindset training objectives that address the role played by knowledge structures, cognitive heuristics, and metacognition in achieving a cyber-aware mindset.

Table 2. Training objectives based on cognitive elements of mindset and mindset change

Mindset Training Objectives
Adapt or replace pre-cyber-warfare knowledge structures so that they contain cyber-defense knowledge (e.g., knowledge listed in Table 1).
Develop skeptical metacognition that supports vigilance and helps to protect against cognitive bias.
Understand how cognitive bias can impact cyber attack detection and recognition.
Know strategies and procedures for reducing the influence of cognitive bias on anomaly detection and response.

3.3 Problem Space Assessment

The problem space assessment highlighted the following constraints:

- Many organizations do not yet know or are still in the process of determining how system users should react if they become suspicious of an attack on their system or if an attack detection alert is triggered by their system.
- Many military organizations do not, in general, allow system users to take independent action outside of pre-defined procedures, limiting users’ ability to investigate anomalies and glitches in their systems.
- Department of Defense (DoD) are required to annually complete a web-based cyber security awareness module. This training is focused on administrative functions and is designed to help system users learn to avoid phishing and other social engineering tactics. Similar training is available to personnel in the private sector. Training generally does not, however, prepare users to support cyber attack detection and response activities in their organizations. Nor does the annual DoD training address potential cyber events on weapons or command and control systems.
- Many organizations do not support high-fidelity training and practice for cyber attack detection and response (e.g., Line et al. 2014). Reasons vary across sectors but in at least some cases, concerns about permanent impacts on operational system function and unrecoverable disruption of expensive training exercises are cited (e.g., Wells 2019).

There are additionally decisions to be made about the level and accuracy of detail in light of the risk of producing a source of information that could benefit cyber adversaries.

3.4 Training Strategy

Iterative design activities, informed by literature review, target user interviews, and stakeholder discussions has led us through a series of design concepts. Throughout this evolution, each concept has reflected the conceptualization of learning as a process of adaptation, co-evolution, and emergence (Neville et al. 2019; Schraagen et al. 2008). They also reflect tradeoffs to address problem space constraints. We have arrived at a scenario-based video game concept in which players assume an adversary position and observe effects of their attack choices on simulated system users. Resources and a guide will help them understand at a high level possible attack goals, resources, tactics, challenges, timelines, and more. Using the support sources, trainees will plan attacks and play them out for points and to see what happens. Feedback will be a critical element and will follow the model of the ShadowBox^{TM} technique, which uses a comparison with experts' ranked choices and rationale as feedback.

Table 3 maps the current training strategy against awareness and mindset training objectives in Tables 1 and 2, respectively. Prototype training will be set in an office environment, with which most people are familiar with intent to adapt future versions to train users of operational systems. We hypothesize that awareness developed in an office computing environment will generalize easily to other work domains.

Table 3. Cyber-mindset training objectives mapped to training strategy elements

Training objectives	Training strategy elements
Cyber awareness training objectives - System baseline - Anomaly identification and reporting - Systems thinking	Support sources will provide visualizations and information about: - A target crew's level of vigilance, difficult-to-detect changes from baselines - Ways to confuse operators, delay responding, and disrupt reporting chains - Relationships among system elements, flows of data and communications, redundancies and other defenses
Mindset training objectives	- ShadowBox^{TM} feedback on cognitive aspects of work, including mindset - Scenarios that support the acquisition of integrated, contextualized knowledge structures - Guidance and practice at taking advantage of an operator's cognitive biases

4 Discussion

The cyber realm is complex on a number of counts; it is vast and largely invisible, a sea of highly interactive and dynamic elements, with pathways and associations that are changing continuously. Cyber-threat activity adds to this realm additional dynamics that significantly escalate the already-extremely-high baseline level complexity. Although cyber-threat activity impacts individuals, organizations, and societies in dramatic and crippling ways, its invisibility and complexity make it difficult to even begin to comprehend, much less defend against.

Yet, some amount of comprehension is necessary. The bad guys cannot be the only ones with cyber-attack knowledge. Our warfighters need at least a base-level incorporated into their knowledge structures. The training tool we are developing will allow us to vary the amount and detail of content to empirically evaluate the amount of cyber knowledge and comprehension required produce a mindset shift and engage operators as a layer of cyber defense.

To date, cyber training for system users predominantly teaches basic procedural information for avoiding being tricked into serving as a cyber-attack conduit. This type of training needs to be extended to empower system users to be active, educated participants in their organization's cyber protection. Training is needed that makes visible and graspable to non-cyber professionals the largely invisible and unknown realm of cyber threats and defense.

Recently, the Navy introduced simulation-based combat systems trainers that allow Sailors to practice their roles in integrated air and missile defense (IAMD) and anti-submarine warfare (ASW) on an isolated network of non-operational, training-designated shipboard systems. Using these high fidelity training systems, sailors are able to practice responding to and working around systems compromised by any number of causes, including cyber attack. These practice opportunities are effective at teaching what to do, i.e., procedural knowledge, but Sailors would benefit from training system features, accompanying instruction, or complementary training that teaches 'why' and 'how', i.e., conceptual knowledge. Conceptual knowledge enables the adaptive use of procedural knowledge across variations in complex work dynamics. Conceptual knowledge about cyber threats could help Sailors to correctly perceive, process, think about, and respond appropriately to information in our new cyber-vulnerable world.

We propose complementary training that could be taken prior to or in parallel with simulation-based practice and that will give operators a cyber-defense enriched knowledge base and adapt their metacognition and use of cognitive heuristics to the modern cyber-threat-pervasive environment. To spur these cognitive adaptations, we propose a holistic training strategy that uses scenarios, supplementary training resources, feedback about cognitive underpinnings of performance, and an adversarial perspective.

Future work will be focused on continued development of the training system and the development of training efficacy assessment plans. A key part of the training efficacy assessment work will be identifying meaningful measures of mindset adoption and impact. Typically, measures are aligned with training objectives. However, our primary interest is in direct measures of mindset change, versus of changes related to specific training objectives. In ShadowBox$^{\mathrm{TM}}$ studies, mindset change has been assessed by evaluating changes in trainees' choices and rationale relative to experts' choices and rationale. We plan to step outside the training system to assess transfer to a real office computing environment and generalizability to other types of work environment. In addition, following the development of mindset-change measures, we can conduct empirical work to assess the role of each training objective identified in this paper.

Future work is also needed to more thoroughly investigate a number of research needs highlighted by this effort. Research is needed, as examples, to better understand how to use training to reduce cognitive bias, how to train or otherwise foster metacognitive proficiency, how to help people make mindset shifts, and how to assess learner progress in these complex aspects of cognitive work.

Acknowledgements. We would like to acknowledge the significant contributions of Dr. Julie Marble and Alice Jackson of Johns Hopkins University Applied Physics Laboratory to the work described in this paper. This research was sponsored by the Office of Naval Research (ONR). The views expressed in this paper are those of the authors and do not represent the official views of the organizations with which they are affiliated.

References

Borko, H., Livingston, C.: Cognition and improvisation: differences in mathematics instruction by expert and novice teachers. Am. Educ. Res. J. **26**(4), 473–498 (1989)

Boulton, L.: Adaptive flexibility: examining the role of expertise in the decision making of authorized firearms officers during armed confrontation. J. Cogn. Eng. Decis. Making **10**(3), 291–308 (2016)

Brand-Gruwel, S., Wopereis, I., Vermetten, Y.: Information problem solving by experts and novices: analysis of a complex cognitive skill. Comput. Hum. Behav. **21**(3), 487–508 (2005)

Canham, M.: Human element in cyber. Presented at the Cyber TRAINsitions Workshop, 10–11 January, University of Central Florida Institution for Simulation and Training (2019)

Chi, M.T.H.: Commonsense conceptions of emergent processes: why some misconceptions are robust. J. Learn. Sci. **14**, 161–199 (2005)

Cornelissen, J.P., Werner, M.D.: Putting framing in perspective: a review of framing and frame analysis across the management and organizational literature. Acad. Manag. Ann. **8**(1), 181–235 (2014)

Crum, A.J., Salovey, P., Achor, S.: Rethinking stress: the role of mindsets in determining the stress response. J. Pers. Soc. Psychol. **104**(4), 716–733 (2013)

Cyber Intelligence Task Force: Cyber intelligence: Preparing today's talent for tomorrow's threats. Intelligence and National Security Alliance (INSA), September 2015

Endsley, M.: Combating information attacks in the age of the internet: new challenges for cognitive engineering. Hum. Factors **60**, 1081–1094 (2018)

Feltovich, P.J., Spiro, P.J., Coulson, R.L.: The nature of conceptual understanding in biomedicine: the deep structure of complex ideas and the development of misconceptions (Technical report no. 440). University of Illinois at Urbana-Champaign: Center for the Study of Reading (1988)

Flavell, J.H.: Metacognition and cognitive monitoring: a new area of cognitive–developmental inquiry. Am. Psychol. **34**(10), 906–911 (1979)

Greenberg, A.: How an entire nation became Russia's test lab for cyberwar. Wire Magazine, 20 June 2017. https://www.wired.com/. Accessed Feb 2019

Klein, G.A.: A recognition-primed decision (RPD) model of rapid decision making. In: Klein, G. A., Orasanu, J., Calderwood, R., Zsambok, C.E. (eds.) Decision Making in Action: Models and Methods, pp. 138–147. Ablex, Norwood (1993)

Klein, G., Baxter, H.C.: Cognitive transformation theory: contrasting cognitive and behavioral learning. In: Cohn, J.V., Schmorrow, D., Nicholson, D. (eds.) The PSI Handbook of Virtual Environments for Training and Education: Developments for the Military and Beyond. Learning, Requirements, and Metrics, vol. 1, pp. 50–64. Praeger Security International, Westport (2009)

Klein, G., Borders, J.: The ShadowBox approach to cognitive skills training: an empirical evaluation. J. Cogn. Eng. Decis. Making **10**(3), 268–280 (2016)

Klein, G., Borders, J., Newsome, E., Militello, L., Klein, H.A.: Cognitive skills training: lessons learned. Cogn. Technol. Work **20**(4), 681–687 (2018)

Klein, G., Moon, B., Hoffman, R.R.: Making sense of sensemaking 2: a macrocognitive model. IEEE Intell. Syst. **21**(5), 88–92 (2006)

Klein, G., Phillips, J.K., Rall, E., Peluso, D.A.: A data/frame theory of sensemaking. In: Hoffman, R.R. (ed.) Expertise Out of Context, pp. 113–158. Erlbaum, Mahwah (2007)

Lewandowsky, S., Ecker, U.K., Seifert, C.M., Schwarz, N., Cook, J.: Misinformation and its correction: continued influence and successful debiasing. Psychol. Sci. Public Interest **13**(3), 106–131 (2012)

Line, M.B., Zand, A., Stringhini, G., Kemmerer, R.: Targeted attacks against industrial control systems: is the power industry prepared? In: Proceedings of the 2nd Workshop on Smart Energy Grid Security, pp. 13–22. ACM, November 2014

Michener, J.: Beating the air-gap: how attackers can gain access to supposedly isolated systems. Energy Central, 24 August 2018. www.energycentral.com. Accessed Feb 2019

Morewedge, C.K., Yoon, H., Scopelliti, I., Symborski, C.W., Korris, J.H., Kassam, K.S.: Debiasing decisions: improved decision making with a single training intervention. Policy Insights Behav. Brain Sci. **2**(1), 129–140 (2015)

Mumford, M.D., Friedrich, T.L., Caughron, J.J., Byrne, C.L.: Leader cognition in real-world settings: how do leaders think about crises? Leadersh. Q. **18**(6), 515–543 (2007)

Neville, K.J., et al.: A complex cognitive skills acquisition framework. In: International Conference on Naturalistic Decision Making (2019, paper under review)

Neisser, U.: Cognition and Reality: Principles and Implications of Cognitive Psychology. W. H. Freeman, San Francisco (1976)

Paul, C.L., Whitley, K.: A taxonomy of cyber awareness questions for the user-centered design of cyber situation awareness. In: Marinos, L., Askoxylakis, I. (eds.) HAS 2013. LNCS, vol. 8030, pp. 145–154. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-39345-7_16

Schraagen, J.M., Klein, G., Hoffman, R.R.: The macrocognition framework of naturalistic decision making. In: Schraagen, J.M., Millitello, L., Ormerod, T., Lipshitz, R. (eds.) Naturalistic Decision Making and Macrocognition, pp. 3–25. Ashgate, Aldershot (2008)

Smith, R.: Russian hackers reach U.S. utility control rooms, homeland security officials say. Wall Street J. (2018). www.wsj.com. Accessed Feb 2019

Symborski, C., Barton, M., Quinn, M.M., Korris, J.H., Kassam, K.S., Morewedge, C.K.: The design and development of serious games using iterative evaluation. Games Culture **12**(3), 252–268 (2017)

Trustwave: 2018 Trustwave global security report. Trustwave, Chicago (2018)

Verizon: 2018 Data Breach Investigations Report, 11th edn. Verizon (2018)

Wells, D.F.: Cyber training. Paper presented at the Cyber TRAINsitions Workshop, 10–11 February, University of Central Florida, Institution for Simulation and Training (2019)