Available online at www.sciencedirect.com

ScienceDirect

Procedia Manufacturing 3 (2015) 5214 – 5221

Procedia MANUFACTURING

6th International Conference on Applied Human Factors and Ergonomics (AHFE 2015) and the Affiliated Conferences, AHFE 2015

Augmenting cyber defender performance and workload through sonified displays

Vincent F. Mancuso[a,]*, Eric T. Greenlee[b], Gregory Funke[c], Allen Dukes[c], Lauren Menke[d], Rebecca Brown[d], Brent Miller[c]

[a] *ORISE/AFRL 711th HPW/RHCP, Wright-Patterson AFB, OH*
[b] *University of Alabama, Tuscaloosa, AL*
[c] *711th Human Performance Wing, RHCP, Wright-Patterson AFB, OH*
[d] *Ball Aerospace & Technologies Corporation, Fairborn, OH*

Abstract

Military cyber operations occur in a cognitively intense and stressful environment, and consequently, operator burnout is relatively high when compared to other operational environments. There is a distinct need for new and innovative ways to augment operator capabilities, increase performance, manage workload, and decrease stress in cyber. In this study, we assessed how a sonified display could address these requirements. Sonification has been demonstrated to be a useful method for presenting temporal data in multiple domains. Participants in the experiment were tasked with detecting evidence of a cyber attack in a simulated task environment modeled after "Wireshark," a popular packet analyzer program. As they completed the task, participants either did or did not have access to a redundant sonified display that provided an auditory representation of the textual data presented in Wireshark. We expected that the sonified display would improve operator performance and reduce workload and stress. However, our results did not support those expectations – access to the sonification did not affect performance, workload, or stress. Our findings highlight the need for continued research into effective methods for augmenting cyber operator capabilities.

Keywords: Cyber; Sonification; Workload; Stress

* Corresponding author. Tel.: +1-937-938-3612
E-mail address: vincent.mancuso.1.ctr@us.af.mil

doi:10.1016/j.promfg.2015.07.589

1. Introduction

Over the last decade, cyber defense has become a high priority for both private industry and government. As our dependence on cyber/-physical systems continues to increase, the need for effective and resilient defense has become more apparent. Much of the research on cyber defense has taken a technological and computational perspective, focusing on issues such as algorithm development and optimization. While we must continue to address these critical issues, we cannot continue to ignore the human-in-the-loop. Modern military cyber operations exist within a complex socio-technical system, in which cyber defenders must balance data, teamwork, and organizational constraints [1-3]. Even with the most advanced technologies, the effectiveness of this entire system hinges on synergistic interactions between humans and technology. In response to this issue, Human Factors researchers have recently begun to identify critical gaps in cyber operator performance.

Within cyber defense, operators progress through three primary stages: threat detection, situation assessment, and threat assessment [1]. These stages align with the JDL Data Fusion Model [4]. In the first level, threat detection, cyber defenders inspect available data for suspicious activities. In the second level, situation assessment, cyber defenders acquire data from other sources (e.g., from different sensors, reports from analysts, organizational policies, etc.) to achieve an understanding of the current situation. Finally, in level three, threat assessment, cyber defenders triangulate information across the first two levels to decide whether there is a valid threat present. To date, most human-centered cyber research has been in support of the above process through the development of novel network visualizations (e.g. [5-7]). While there has been limited empirical support for the utility of those displays, there is also worry that adding another complex visualization to operators' toolboxes may add to the information overload problem they already face [8-9].

1.1. Cyber sonification

An alternate augmentation strategy that may be effective in augmenting operator performance while maintaining manageable workload is information sonficiation. Sonification is a way of transforming data and its relationships into an acoustic signal for the purposes of communication and/or interpretation [10]. Sonification can be employed to present information in a way that is distinct from visual displays in that sound is a temporal medium that contains spatial characteristics, while visual displays are primarily spatial with temporal features [11]. Additionally, when dealing with complex datasets, visual displays can be very intensive and crowded, and auditory displays can be used as a compliment or replacement to reduce visual workload in such situations [12].

Due to the deluge of data and the inherent temporality of cyber security, sonification may be especially suitable to aid operator performance. Previous sonification attempts in cyber have been limited and focused on computational mapping of cyber data to auditory attributes to facilitate network situation awareness. For example, in an early sonified interface for network data, “Peep,” Gilfix and Couch [13] proposed transforming events on monitored networks into nature-inspired acoustic signals. This simplistic system was created to allow operators to identify anomalies such as high traffic load or email spam. Applying a similar approach, Ballora, Giacobe, and Hall [14], proposed a framework to examine packet flows between sender and receiver IP address and port number to create an auditory rendering of the interaction. The goal of this sonification was to make the listener aware of common patterns in network traffic so that they could pick out unexpected patterns in the data stream. In both of these examples, the sonification was intended to be ambient, allowing operators to monitor network traffic patterns peripherally. Other systems, such as *Stetho* [15], *InteNtion* [16], SonNet [17], and the *Self Organized Criticality Sonification System (SOCS)* [18], advocate similar approaches.

1.2. Purpose

While previous research on cyber sonification has addressed important issues such as computationally transforming network data into auditory signals, most have not been subjected to evaluations of their efficacy, leading to questions about their generalizability and applicability in operating environments. Additionally, the current focus on situation awareness as the only outcome of interest does not account for other key contributors to human performance in cyber operations such as workload and stress [19]. To address these gaps, the purpose of this experiment was to assess the utility of a simple sonification scheme for cyber data on key outcomes such as performance, workload, and stress. Specifically, we assessed how the sonification of simulated packet analysis logs may help cyber analysts identify malicious traffic across a simulated network.

2. Method

2.1. Participants

Thirty individuals (16 men, 14 women) with ages ranging from 18 to 32 years (M = 23.5 years) served as participants in this study in exchange for $30. The study was conducted at the Air Force Research Laboratory at Wright-Patterson Air Force Base, and all participants were recruited from the local population and base personnel. All participants reported normal hearing and normal or corrected-to-normal vision.

2.2. Experimental design

A 2 (task condition) × 5 (trial) mixed design was employed. Each study consisted of 5 experimental trials in a simulated cyber search tasks. Period order weas counter balanced across participants. In each period, performance was calculated based on the total number of accurate threat detections, false alarms and misses.

Fifteen participants were assigned at random to a *visual-only* condition in which all task-critical information was conveyed visually; the remaining 15 participants were assigned to the *sonification* condition in which task-critical information was represented both visually and auditorily.

2.3. Materials and apparatus

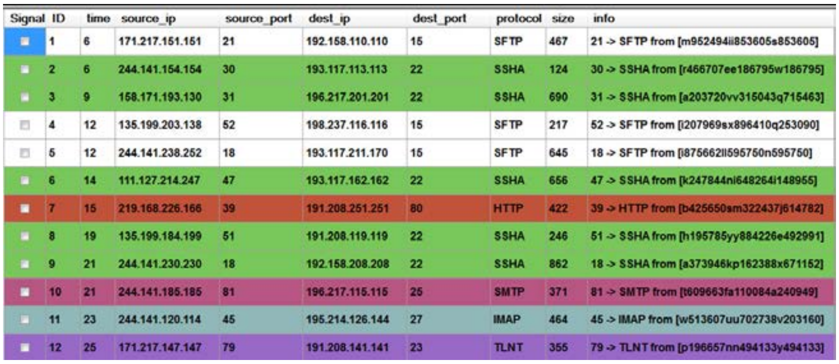
Participants completed the experimental task, the TLX, and DSSQ (each described below) on a computer terminal. The computer was equipped with a standard 16:9 monitor and Sennheiser HD-280 Pro headphones. Participants were seated and centered in front of the display at an unconstrained viewing distance of approximately 45 cm.

NASA-Task Load Index Questionnaire. Upon conclusion of each experimental trial, participants completed the NASA-Task Load Index (TLX; [21]). This survey has been validated as a standard measure of perceived mental workload in human performance research and provides an overall index of perceived task workload on a scale of 0 to 100 by combining the contributions of six sources of mental workload: mental demand, temporal demand, physical demand, performance, effort, and frustration.

Dundee Stress State Questionnaire. Both pre- and post-task, participants completed the Dundee Stress State Questionnaire (DSSQ, [20]), a validated measure of stress states. Items on the DSSQ have been factor analyzed into three second-order factors: subjective engagement, distress, and worry. Engagement refers to qualities of energy, motivation and concentration. Distress is defined by feelings of tension, positive hedonic tone and confidence and control. Worry relates to self-focused attention, low self-esteem and cognitive interference generated by the task and by personal concerns. Scores on the DSSQ are estimated using weights derived from a previous study providing normative data [20]. Factor scores are distributed with a mean of 0 and standard deviation of 1, so that the values calculated for a sample represent deviations from normative values in standard deviation units.

2.4. Procedure

For participants assigned to the *visual-only* condition, the experimental session began with administration of the pre-task version of the DSSQ. Upon completion of this survey, participants were informed that they would be taking on the role of an Air Force cyber defender tasked with searching network traffic logs for evidence of malicious activity perpetrated by a fictional hacker whose attacks were identifiable by a specific “signature.” The network logs were presented within a computer interface that was designed to emulate the format and functionality



Signal	ID	time	source_ip	source_port	dest_ip	dest_port	protocol	size	info
□	1	6	171.217.151.151	21	192.158.110.110	15	SFTP	467	21 -> SFTP from [m952494ii853605s853605]
□	2	6	244.141.154.154	30	193.117.113.113	22	SSHA	124	30 -> SSHA from [r466707ee186795w186795]
□	3	9	158.171.193.130	31	196.217.201.201	22	SSHA	690	31 -> SSHA from [a203720vv315043q715463]
□	4	12	135.199.203.138	52	198.237.116.116	15	SFTP	217	52 -> SFTP from [i207969sx896410q253090]
□	5	12	244.141.238.252	18	193.117.211.170	15	SFTP	645	18 -> SFTP from [i875662ll595750n595750]
□	6	14	111.127.214.247	47	193.117.162.162	22	SSHA	656	47 -> SSHA from [k247844ni648264i148955]
□	7	15	219.168.226.166	39	191.208.251.251	80	HTTP	422	39 -> HTTP from [b425650sm322437j614782]
□	8	19	135.199.184.199	51	191.208.119.119	22	SSHA	246	51 -> SSHA from [h195785yy884226e492991]
□	9	21	244.141.230.230	18	192.158.208.208	22	SSHA	862	18 -> SSHA from [a373946kp162388x671152]
□	10	21	244.141.185.185	81	196.217.115.115	25	SMTP	371	81 -> SMTP from [t609663fa110084a240949]
□	11	23	244.141.120.114	45	195.214.126.144	27	IMAP	464	45 -> IMAP from [w513607uu702738v203160]
□	12	25	171.217.147.147	79	191.208.141.141	23	TLNT	355	79 -> TLNT from [p196657nn494133y494133]

Fig. 1: Examples from the display used to present simulated network traffic.

of commonly used network packet analysis software, such as Wireshark (see Figure 1). Within this display, each line represented one network transmission, and each column represented a parameter of that signal (e.g., source IP address, packet size, etc.).

Target packets in this experiment were indicated by the combination of several features in a single network packet. Specifically, target packets were characterized by “signatures” – network transmissions that originated from either of two Source IP addresses, were directed to either of two Destination IP addresses, used either of two Protocols, and packet size was 500 bytes or more. Participants were instructed that any transmission matching a signature on at least three of the four target parameters should be marked as a signal by clicking the “Signal” button in the IDS display with a computer mouse. In order to facilitate search for this signature, transmissions were color-coded based on Protocol – a default option in popular network packet analyzers, including those used by the Air Force.

Following task instructions and a practice session, lasting approximately 30 min, participants engaged in five 10-minute trials. In each trial, a unique network log was presented, consisting of 600 network transmissions. Of those transmissions, 120 in each log matched the cyber intrusion signature (signal probability = 20%). Participants were able to scroll freely through the entire network log, and search was self-paced. The number of correct detections and false alarms were recorded for each trial.

After each 10-minute trial, participants reported their workload on the NASA-TLX. Following the fifth trial, participants completed the NASA-TLX and the post-task DSSQ.

For participants in the *sonification* condition, the study began with an introduction to auditory displays and training regarding the sonification employed in this experiment. Sonification took the form of a pair of sequential musical notes separated by 100 ms, each note lasting 250 ms. The first note represented the Source IP address and was always played by a string instrument; each possible source IP was represented by a specific string instrument playing a specific note. The second note in each pair represented the Destination IP address, and each possible Destination IP was represented by a specific wind instrument and note. The loudness of the musical note pair represented the Packet Size. When the Packet Size was smaller than 500 bytes, both musical notes were played at 50 dBA; when Packet Size was 500 bytes or more, both notes were presented at 70 dBA. The sonification of any transmission was activated by participants clicking on that packet in the network log.

Prior to beginning the experiment in the *sonification* condition, participants completed a two-alternative forced choice procedure during which sonification cues were presented and participants were tasked with identifying the visually presented network information represented by the auditory cue. Participants were trained to a 95% accuracy criterion for all elements of the network sonification. Complete network logs were not presented and the nature of the search task was not revealed during this training session. A mandatory 10 minute break was given between this training and the start of the search task procedures.

2.5. Validation of the task platform

The simulated network packet analyzer used in the current study was developed from conversations with Air Force cyber subject matter experts (SMEs). Further, these SMEs stated that the types of cognitive demands present in the current experiment were comparable to those of their real-world tasks. Based on this review, we concluded that the cyber search task was a valid representation of real-world defensive cyber operations.

3. Results

3.1. Performance

Performance efficiency was considered in terms of number of correct detections. False alarms were exceedingly rare in this experiment; 20% of participants committed no false alarms, and the average rate of false alarms accounted for only 2.1 percent of participant responses. For this reason, false alarms were not analyzed, and will not be discussed further.

The number of correct detections were analyzed using a 2 (task condition) × 5 (periods of watch) mixed model Analysis of Variance (ANOVA). In this and all subsequent analyses Box's epsilon was employed to correct violations of the sphericity assumption. The results of the analysis indicated that correct detections increased across periods of watch, $F(2.99, 83.80) = 68.35$, $p < .001$, $\eta_p^2 = .71$. The main effect of task condition and the task condition by period interaction were not statistically significant, $p > .05$ in each case. Mean correct detections (and associated standard errors) for each task condition and trial are presented in Table 1.

Table 1: Mean correct detections for each task condition and trial. Standard errors are reported in parentheses.

	Trial (10 minutes)				
Task Condition	1	2	3	4	5
Visual-Only	29.47 (2.02)	38.33 (2.85)	44.40 (3.22)	47.87 (3.46)	52.40 (3.22)
Sonification	24.93 (2.02)	34.47 (2.85)	39.67 (3.22)	44.20 (3.46)	47.27 (3.22)
Average	27.20 (1.43)	36.40 (2.02)	42.04 (2.28)	46.05 (2.45)	49.84 (2.28)

3.2. Workload

NASA-TLX ratings were analyzed using a 2 (task condition) × 5 (trial) × 6 (TLX subscale) ANOVA. This analysis revealed a marginal effect for period of watch, $F(2.10, 58.88) = 3.06$, $p = .052$, $\eta_p^2 = .10$, an effect that is best described as a nonlinear decline in overall ratings of task demand from a total workload of 48.92 (SE = 2.24) in the first period to a total workload of 44.47 (SE = 2.47) in the final period (Figure 2).

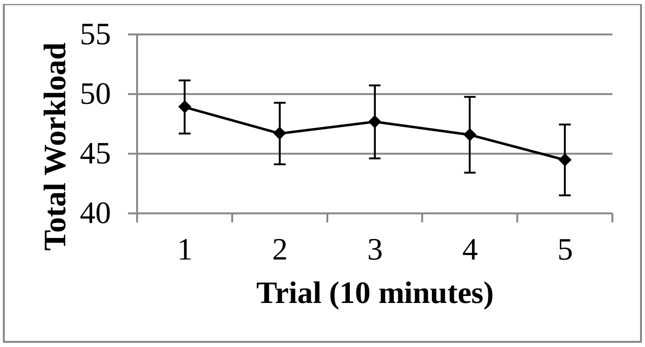


Fig. 2: NASA-TLX scores across trials (Error bars represent SE)

The analysis also revealed a main effect of subscale, $F(2.99, 83.82) = 35.60$, $p < .001$, $\eta_p^2 = .56$. As can be seen in Table 2, workload ratings were greatest for Mental Demand and Effort, while ratings of Temporal Demand and, to a lesser degree, Performance Demand and Frustration, were higher than ratings of Physical Demand. No other sources of variance in the analysis were statistically significant (all $p > .05$).

Table 2: NASA-TLX ratings by task condition and subscale. Standard errors are presented in parentheses.

	Subscale					
Task Condition	Mental Demand	Physical Demand	Temporal Demand	Performance Demand	Effort	Frustration
Visual-Only	73.07 (5.30)	21.80 (6.46)	64.60 (6.21)	42.87 (5.55)	72.27 (5.59)	35.60 (6.46)
Sonification	60.87 (6.45)	10.93 (3.02)	50.73 (5.40)	41.00 (5.67)	57.79 (6.03)	30.93 (6.08)
Average	66.97 (4.18)	16.37 (3.57)	57.67 (4.12)	41.93 (3.97)	65.00 (4.11)	33.27 (4.44)

3.3. Stress

To assess the effects of the sonification on task-induced stress, change scores, calculated as post-task score minus pre-task score, were computed for each of the three DSSQ subscales. Change scores were then analyzed for statistically significant differences using a 2 (task condition) × 3 (subscale) ANOVA. This analysis indicated no significant effect of task condition and no interaction between task condition and subscale. However, there was a significant main effect of DSSQ subscale, $F(1.95, 54.60) = 9.08$, $p < .001$, $\eta_p^2 = .25$. As indicated in Figure 2, distress increased during task performance, and worry and engagement decreased slightly. Follow-up one-sample *t*-tests of mean subscale change scores revealed that only the increase in distress was significant, $p = .001$.

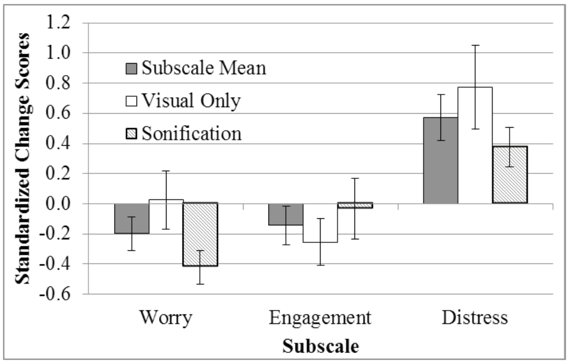


Fig. 3: Standardized DSSQ change scores for each subscale in each task condition. Error bars represent standard errors.

4. Discussion

4.1. Performance and workload in cyber operations

In their survey of cyber operators, Chappelle and colleagues [19] found clear evidence that cyber operations include stressful and cognitively demanding tasks. In their study, cyber operators reported that their primary stressors were a result of occupational stress, such as shift work, shift changes, and hours of work. Surprisingly, the operators did not acknowledge task-based factors as resulting in primary stress. While the present study represents a simulated “snap-shot” of cyber operations, our results indicate that task-based factors may be additional stressors to consider in such environments.

With regard to workload, participants in all conditions rated Mental Demand, Temporal Demand, and Effort above the midpoint on the scale, indicating substantial workload (e.g., [22]). Additionally, the change scores on the DSSQ showed that distress increases significantly as a result of participating in the task.

Interestingly, despite the demands and stress associated with the task, performance increased across trials. However, we would not expect this learning effect in "real-world" cyber operations. The total length of the experiment was quite limited when compared to actual cyber shift work. Chappelle and colleagues [19] reported that operators worked over 51 hours a week, with limited rest breaks. Given the monotonous nature of the task, over a longer period (8-10 hours), the task may begin to take on characteristics of a vigilance task, in which performance would begin to degrade over time (i.e., operators would experience the vigilance decrement; [23]). Indeed, prior research in cyber has demonstrated attributes of a vigilance task [24]; however that study represented cognitive work that would be done by an operator responsible for monitoring live network traffic, rather than reviewing network log, as was the case in this task. Additionally, over this period of time we would expect that the workload and stress effects found in this given study would be magnified, potentially adding more to the burnout effects discussed by Chappelle et al. [19].

4.2. Sonification

Unfortunately, there was no evidence that the employed sonification system improved operator performance or reduced workload or stress. While the current sonification system was not augmentative, these results should not be considered typical of sonification in general and should not dissuade researchers from future attempts to sonify cyber defense tasks.

Sonification has been beneficial in a variety of non-cyber domains, and the potential for cyber sonification has been indicated by previous attempts to sonify network data [12-18]. While there is no universal recipe for successful sonification, previous research indicates that sonification systems can be useful for data exploration tasks similar to the current task [25]. However, sonification may be more useful for unobtrusively conveying peripheral, secondary task information with a high degree of temporal detail [12]. For the sake of task simplicity, participants in the current study were not required to parse temporal detail from the network log. Consequently, the simulated attack "signature" employed corresponds to some of the simpler attack signatures that cyber defenders need to detect; that said, cyber SMEs also report that some attack signatures are more complicated and require an understanding of the temporal relationships between multiple transmissions. Perhaps a sonification system would be better suited for cyber defense if it were designed to aid detection of these temporally complex threats.

As an additional consideration, previous research has demonstrated that when a task requires cognitive integration of visual and auditory information streams, multimodal displays may not improve performance compared to unimodal visual displays [26]. In the present task, it is likely that participants were integrating the visual color codes and the sonification cues to determine whether each network transmission matched the attack "signature." It is possible that this integration may have prevented augmentative effects. This limitation should be considered during the design of future sonification systems in order to avoid requiring that operators integrate information from multiple modalities in order to complete a single cyber task.

5. Limitations and future work

When interpreting our results, two key limitations should be noted. First, the task we used represented a simplistic representation of a cyber task. While the task had been validated by SMEs as representing the cognitive factors present in cyber operations, its simplistic nature may have marginalized other workload effects and stressors that may be present in a real-world cyber task. Second, due to lack of availability, we could not recruit cyber operators as participants in this experiment, and therefore we relied on novice participants. The inexperience of the participants was demonstrated in a significant learning effect (rather than a decrement with time-on-task), and may have modified the workload and stress ratings we observed.

Even though we used a simplified task with novice participants, the findings in the present study still represent a meaningful contribution and have implications for future research. Similar to the results reported by Chappelle et al. [19], we found that cyber tasks may result in high levels of workload and distress. This finding further highlights the need for further research to develop approaches to augment cyber operator performance, and to help them manage workload and stress. While our attempt at augmenting operators in this experiment was not successful, sonification has previously been shown to help reduce workload and limit stress [12], suggesting it may still be a fruitful research area. Future research should address new techniques for sonifying cyber data, perhaps focusing on testing their utility for augmentation of a secondary, rather than primary, task.

References

[1] D'Amico, A., Whitley, K., Tesone, D., O'Brien, B., & Roth, E. (2005, September). Achieving cyber defense situational awareness: A cognitive task analysis of information assurance analysts. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting (Vol. 49, No. 3, pp. 229-233). SAGE Publications.

[2] Mahoney, S., Roth, E., Steinke, K., Pfautz, J., Wu, C., & Farry, M. (2010, September). A cognitive task analysis for cyber situational awareness. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting (Vol. 54, No. 4, pp. 279-283). SAGE Publications.

[3] Tyworth, M., Giacobe, N., Mancuso, V., McNeese, M., & Hall, D (2013). A Human-In-The-Loop Approach to Understanding Situation Awareness in Cyber Defense Analysis. EAI Endorsed Transactions on Security and Safety, 13(2), 1-10.

[4] Llinas, J. and Hall, D.L. (1998). An Introduction to Multi-Sensor Data Fusion. IEEE Report 0-7803-4455-3/98

[5] D'Amico, A., & Kocka, M. (2005, October). Information assurance visualizations for specific stages of situational awareness and intended uses: lessons learned. In Visualization for Computer Security, 2005.(VizSEC 05). IEEE Workshop on (pp. 107-112). IEEE.

[6] Fink, G. A., North, C. L., Endert, A., & Rose, S. (2009, October). Visualizing cyber security: Usable workspaces. In Visualization for Cyber Security, 2009. VizSec 2009. 6th International Workshop on (pp. 45-56). IEEE.

[7] Giacobe, N. A. (2013, September). A Picture is Worth a Thousand Alerts. In Proceedings of the 57th Annual Meeting of the Human Factors and Ergonomics Society, 30 September - 4 October (pp. 172-176). San Diego, CA, HFES.

[8] Boyce, M. W., Duma, K. M., Hettinger, L. J., Malone, T. B., Wilson, D. P., & Lockett-Reynolds, J. (2011, September). Human Performance in Cybersecurity A Research Agenda. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting (Vol. 55, No. 1, pp. 1115-1119). Las Vegas, NV. HFES.

[9] Mancuso, V. F., Christensen, J. C., Cowley, J., Finomore, V., Gonzalez, C., & Knott, B. (2014, September). Human Factors in Cyber Warfare II Emerging Perspectives. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting (Vol. 58, No. 1, pp. 415-418). Chicago, Il. HFES

[10] Kramer, G., Walker, B., Bonebright, T., Cook, P., Flowers, J., Miner, N.; Neuhoff, J., Bargar, R., Barrass, S., Berger, J., Evreinov, G., Fitch, W., Gröhn, M., Handel, S., Kaper, H., Levkowitz, H., Lodha, S., Shinn-Cunningham, B., Simoni, M., Tipei, S. (1999). The Sonification Report: Status of the Field and Research Agenda. Report prepared for the National Science Foundation by members of the International Community for Auditory Display. Santa Fe, NM: ICAD.

[11] Mountford, S. J., & Gaver, W. (1990). Talking and listening to computers. The art of human-computer interface design, 319-334.

[12] Vickers, P. (2011). Sonification for process monitoring. In Hermann, T., Hunt, A., Neuhoff, J. G., editors, The Sonification Handbook, chapter 18, pages 455–491. Logos Publishing House, Berlin, Germany

[13] Gilfix, M., & Couch, A. L. (2000). Peep (the network auralizer): Monitoring your network with sound. In 14th System Administration Conference (LISA 2000), (pp. 109-117). New Orleans, Louisiana, USA: The USENIX Association.

[14] Ballora, M., Giacobe, N. A., & Hall, D. L. (2011, May). Songs of cyberspace: an update on sonifications of network traffic to support situational awareness. In SPIE Defense, Security, and Sensing (pp. 80640P-80640P). International Society for Optics and Photonics.

[15] M. Kimoto and H. Ohno, "Design and Implementation of Stetho — Network Sonification System," in Proceedings of the 2002 International Computer Music Conference, Göteborg, 2002, pp. 273–279.

[16] R. Giot and Y. Courbe, "InteNtion–Interactive Network Sonification," in Proceedings of the 18th International Conference on Auditory Display (ICAD 2012), 2012, pp. 235–236.

[17] K. E. Wolf and R. Fiebrink, "SonNet: A Code Interface for Sonifying Computer Network Data," in NIME'13 — 13th International Conference on New Interfaces for Musical Expression, Daejeon + Seoul, Korea, 2013, pp. 503–506.

[18] P. Vickers, C. Laing, and T. Fairfax, "Sonification of a Network's Self-Organized Criticality," arXiv preprint arXiv:1407.4705, 2014.

[19] Chappelle, W., McDonald, K., Christensen, J., Prince, L., Goodman, T., Thompson, W., & Hayes, W. (2013). Sources of Occupational Stress and Prevalence of Burnout and Clinical Distress Among US Air Force Cyber Warfare Operators (No. AFRL-SA-WP-TR-2013-0006). SCHOOL OF AEROSPACE MEDICINE WRIGHT PATTERSON AFB OH.

[20] Matthews, G., Campbell, S.E., Falconer, S., Joyner, L.A., Huggins, J., Gilliland, K., Grier, R., & Warm, J.S. (2002). Fundamental dimensions of subjective state in performance settings: Task engagement, distress, and worry. Emotion, 2, 315–340.

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

[22] Finomore, V. S., Shaw, T. H., Warm, J. S., Matthews, G., & Boles, D. B. (2013). Viewing the workload of vigilance through the lenses of the NASA-TLX and the MRQ. Human Factors: The Journal of the Human Factors and Ergonomics Society, 55(6), 1044-1063.

[23] Davies, D.R., & Parasuraman, R. (1982). The psychology of vigilance. London: Academic Press.

[24] McIntire, L., McKinley, R. A., McIntire, J., Goodyear, C., & Nelson, J. (2013). Eye metrics: An alternative vigilance detector for military operators. Military Psychology, 25, 502-513.

[25] Walker, B. N. & Nees, M. A. (2011). Theory of sonification. In T. Hermann, A. Hunt, & J. G. Neuhoff (Eds.). The Sonification Handbook. (9-39). Logos Verlag, Berlin, Germany.

[26] Wickens, C. D. & Goettle, B. (1984). Multiple resources and display formatting: The implications of task integration. Proceedings of 28th Meeting of the Human Factors Society, 722-726.