Cyber Vigilance: Effects of Signal Probability and Event Rate

Ben D. Sawyer[1], Victor S. Finomore[2], Gregory J. Funke[2], Vincent F. Mancuso[3], Matthew E. Funke[4],
Gerald Matthews[1], & Joel S.Warm[2,5]

[1] University of Central Florida, Orlando, FL,
[2]Air Force Research Laboratory, Wright Patterson Air Force Base, OH,
[3]Oak Ridge Institute for Science and Education, Wright-Patterson Air Force Base, OH,
[4]Naval medical Research Unit-Dayton, Wright-Patterson Air Force Base, OH,
[5]University of Dayton Research Institute, Dayton, OH.

ABSTRACT

Cyber security operators in the military and civilian sector face a lengthy repetitive work assignment with few critical signal occurrences under conditions in which they have little control over what transpires. In this sense, their task is similar to vigilance tasks that have received considerable attention from human factors specialists in regard to other operational assignments such as air traffic control, industrial process control, and medical monitoring. Accordingly, this study was designed to determine if cyber security tasks can be linked to more traditional vigilance tasks in regard to several factors known to influence vigilance performance and perceived mental workload including time on task, the probability of critical signal occurrence, and event rate (the number of stimulus events that must be monitored in order to detect critical signals). Consistent with the results obtained in traditional vigilance experiments, signal detection on a 40-minute simulated cyber security task declined significantly over time, was directly related to signal probability, and inversely related to event rate. In addition, as in traditional vigilance tasks, perceived mental workload in the cyber task, as reflected by the NASA Task Load Index, was high. The results of this study have potential meaning for designers of cyber security systems in regard to psychophysical factors that might influence task performance and the need to keep the workload of such systems from exceeding the information processing bounds of security operators.

INTRODUCTION

As described by the Chief Scientist of the Air Force, Dr. Mark Maybury, cyberspace is a domain from which, and through which, Air Force (AF) operations are performed and is essential for all such operations (Maybury, 2012). Given its importance, it is critical to maintain cyberspace security to prevent intrusion by enemy forces. Although software initially identifies potential attacks, human operators must render the final decision. Toward that end, cyber defenders are assigned to monitor network traffic for signs of intrusion, such as specific key words and /or internet protocol (IP) addresses, and forward evidence to intelligence services for further analysis (D'Amico, Whitley, Tesone, O'Brien, & Roth, 2005; Lin, 2010). The present scale of military network activity means vast amounts of information must be carefully examined.

In pursuit of that careful analysis and the larger mission, cyber defenders face highly repetitive work assignments featuring large quantities of data that must be processed, few critical occurrences, and little control over what transpires. Their task bears the signature of what is known as a *vigilance task* in which operators must focus their attention and detect infrequently occurring critical signals over prolonged periods of time (Hancock, 2013; Warm, Parasuraman, & Matthews, 2008). Vigilance tasks are a crucial element of many work environments wherein humans must monitor automated systems for adverse events including aviation, airport and border security, industrial process control, long distance driving, and the examination of anesthesia gauges during surgery. A number of studies have shown that accidents ranging from minor to major have resulted from vigilance failures by human observers (Warm, Finomore, Vidulich, & Funke, in press). Consequently, one might assume that cyber security operations would take advantage of what is known about vigilance to enhance mission system security. However, this does not appear to be the case.

To date, the only study to examine vigilance performance in the cyberspace context was carried out by McIntire and her associates (McIntire, McKinley, McIntire, Goodyear, & Nelson, 2013). They showed that the vigilance decrement, the temporal decline in performance efficiency that typifies vigilance performance (cf., Davies & Parasuraman, 1982; Warm et al., in press), also occurs in a simulated cyber task and that the decrement is accompanied by changes in oculomotor activity, such as blink frequency, duration, and pupil diameter, which could be used to detect when cyber operators are in need of rest or replacement.

In addition to time on task, vigilance performance is determined by a number of psychophysical factors which confront observers with perceptual challenges. Knowledge of those challenges might enable designers to develop cyber displays that can be interrogated more effectively by observers. Accordingly, one goal for the present study was to extend the linkage between vigilance and cyber tasks by determining if two of the most critical of those psychophysical factors, signal probability and event rate, also effect performance on a simulated cyber task. Signal probability refers to the likelihood that any stimulus event is a critical signal, while event rate refers to the number of stimulus events

Copyright 2014 Human Factors and Ergonomics Society. DOI 10.1177/1541931214581369

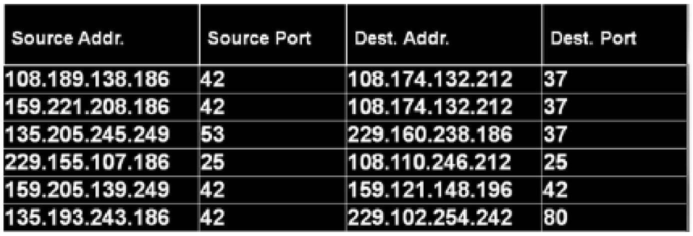
that must be monitored in order to detect critical signals. Performance efficiency in vigilance tasks varies directly with the probability of critical signals and inversely with event rate (Warm et al., in press; Warm & Jerison, 1984).

In addition to confronting observers with perceptual challenges, vigilance tasks also carry with them high levels of perceived mental workload as reflected by the NASA-Task Load Index (NASA-TLX; Hart & Staveland, 1988) which is considered to be one of the most effective measures of perceived mental workload currently available (Wickens, Hollands, Banbury, & Parasuraman, 2013). It provides a measure of overall or global workload on a scale of 0 to 100 and identifies the relative contribution of six sources of workload: Mental Demand, Physical Demand, Temporal Demand, Performance, Effort, and Frustration. As summarized by Finomore, Shaw, Warm, Matthews, and Boles (2013), Warm et al. (2008), and Wickens et al. (2013), a number of studies have shown that the global workload scores on vigilance tasks fall at the upper end of the NASA-TLX scale and that Mental Demand and Frustration are the primary components of the workload associated with vigilance tasks. A second goal for this study was to determine if a simulated cyber task also induces high workload in observers and if Mental Demand and Frustration are the primary components of workload in that task. Such knowledge may help supervisors and designers to better understand observers' reactions to cyber monitoring assignments.

METHOD

The study was conducted at the Air Force Research Laboratory, Wright-Patterson Air Force Base (WPAFB). Twenty-four volunteers (14 men and 10 women) were recruited from base personnel and the local population and paid $45 for their participation. The study was approved by the WPAFB Institutional Review Board.

Participants assumed the role of a cyber-defender monitoring strings of IP addresses and communication port numbers on a computer monitor. The task, which was similar to that employed by McIntire et al. (2013), was developed to simulate tasks representative of cyber defense operations. As shown in Figure 1, the display was composed of two columns of six IP addresses, each containing 12 digits, and two columns of six communication port numbers, each containing two digits. The task of the cyber-defender was to look for cases in which the IP address and communication port number at the top position of any column completely matched an IP address/communication port number that was already present in any one of the other position in that column (the critical signal for detection). At regular intervals throughout the task, the display would refresh and two new IP address/communication port numbers would appear in the top position of the columns. The previous entries would then move down to the next row immediately below it and the bottom series would disappear from the display.



Source Addr.	Source Port	Dest. Addr.	Dest. Port
108.189.138.186	42	108.174.132.212	37
159.221.208.186	42	108.174.132.212	37
135.205.245.249	53	229.160.238.186	37
229.155.107.186	25	108.110.246.212	25
159.205.139.249	42	159.121.148.196	42
135.193.243.186	42	229.102.254.242	80

Figure 1. In this example of stimuli displayed during the cyber task a critical signal is present in the right column, as there is a match between the IP address and communication port of the top position and the second position.

Two levels of signal probability (low and high) were combined with two levels of event rate (slow and fast) to produce four experimental conditions. Six participants were assigned at random to each condition. All participants served in a 40-min vigil divided into four continuous 10-min periods of watch in which the strings of IP addresses and port numbers were always visible on the computer screen. In the slow event rate-high signal probability condition, the display was updated 8 times/min (one event every 7.50 sec.) with a 20% chance of the appearance of a critical signal. In the slow event rate-low signal probability condition, updates also occurred 8 times/min, but with a 5% chance of critical signal appearance. In the fast event rate-high signal probability condition, the display was updated 16 times/min (one every 3.75 sec) with a 20% chance of the presence of a critical signal. In the fast event rate-low signal probability condition, updates also occurred 16 times/min, but with a 5% chance of critical signal appearance. Critical signal appearances were scheduled so that only one of the two IP address/communication port columns would have a signal at any given time. Accordingly, participants responded to critical signals by pressing the spacebar on a computer keyboard. Responses occurring within 3 sec of the appearance of a critical signal were considered as correct detections. All other responses were scored as false alarms. All participants were aware of this scoring procedure.

Preceding the main portion of the experiment, participants were given a 15 min training period on the cyber task during which they received auditory feedback in the form of a male voice indicating correct detections and false alarms. Feedback was not provided during the main task itself. Immediately following the conclusion of the main task, participants completed a computerized version of the NASA-TLX.

RESULTS

Performance Efficiency. Mean percentages of correct detections and their associated standard errors for all combinations of event rate, signal probability, and time on task are presented in Table 1.

Table 1. *Mean percent correct detection scores for all combinations of signal probability and event rate during each period of watch. Standard errors are in parentheses.*

		Period of Watch (10 minutes)				
Signal Probability	Event Rate	1	2	3	4	Mean
Low	Slow	**87.50**	**95.83**	**95.83**	**75.00**	**88.54**
		(5.59)	(4.17)	(4.17)	(15.81)	(7.43)
	Fast	**60.42**	**60.42**	**58.33**	**43.75**	**55.73**
		(7.51)	(7.51)	(6.97)	(7.74)	(7.43)
High	Slow	**95.83**	**91.67**	**88.54**	**80.21**	**89.06**
		(1.32)	(3.84)	(2.98)	(6.13)	(3.57)
	Fast	**77.08**	**77.60**	**76.56**	**77.60**	**77.21**
		(5.33)	(6.01)	(7.38)	(4.80)	(5.88)
Mean		**80.21**	**81.38**	**79.82**	**69.14**	
		(4.94)	(5.38)	(5.38)	(8.62)	

Perusal of the table will reveal that mean detection scores were lower in the context of the fast (M = 66.47%) as compared to the slow (M = 88.80%) event rate condition, and greater in the case of the high (M = 83.14%) as compared to the low (M = 72.14%) signal probability condition. In addition there was a notable decline in signal detections during the final period of watch. These impressions were confirmed by a 2 (event rate) × 2 (signal probability) × 4 (periods of watch) mixed analysis of variance (ANOVA) of the arcsines of the percent scores, which revealed significant main effects for event rate, $F(1, 20) = 17.53$, $p < .001$, $\eta_p^{\,2} = .47$, signal probability, $F(1, 20) = 4.26$, $p = .05$, $\eta_p^{\,2} = .18$, and periods of watch $F(2.05, 40.93) = 5.44$, $p = .008$, $\eta_p^{\,2} = .21$. The remaining sources of variance in the analysis were not significant ($p > .05$ in each case). However, the Event Rate × Signal Probability interaction closely approached significance, F (1, 20) = 3.86, $p = .06$, $\eta_p^{\,2} = .16$. In this and in the analysis of the workload scores to follow, the Box correction was applied when appropriate to compensate for violations of the sphericity assumption (Field, 2009).

The Event Rate × Signal Probability interaction is presented in Figure 2. It is evident in the figure that the scores for the two signal probability conditions were similarly high in the context of a slow event rate. By contrast, in the fast event rate condition, performance efficiency in the high probability condition was considerably better than in the low probability condition.

False alarms were rare in this study. The overall false alarm percentage across all experimental conditions was < 1%. Consequently, false alarms were not analyzed further.

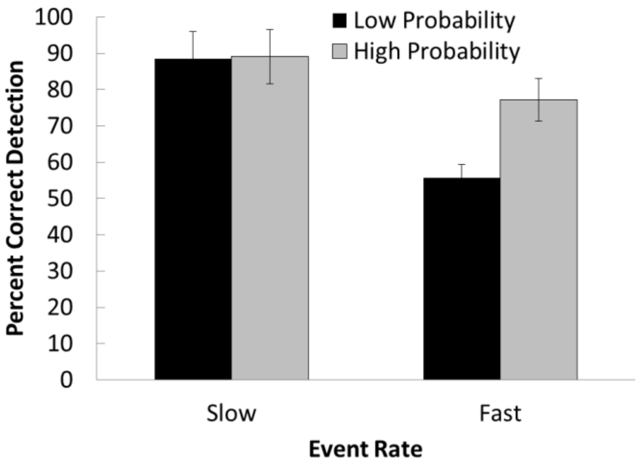


Figure 2. Mean percent detection scores for all combinations of signal probability and event rate. Error bars are standard errors.

Subjective Workload. Observers in all task conditions rated their workload on the six subscales of the NASA-TLX. Following a procedure recommended by Nygren (1991), workload scores were based solely on the ratings themselves and not on associated contrasts for each subscale. Mean workload values for all combinations of event rate, signal probability, and NASA-TLX subscales are presented in Table 2.

Table 2. *Mean NASA-TLX subscale scores for all combinations of signal probability and event rate. Standard errors are in parentheses.*

		Subscale						
Signal Probability	Event Rate	MD	PD	TD	P	E	F	Composite
Low	Slow	**72.50**	**15.00**	**75.00**	**33.33**	**72.50**	**39.17**	**51.25**
		(11.38)	(4.65)	(6.45)	(13.08)	(6.55)	(14.34)	(9.41)
	Fast	**67.50**	**33.33**	**77.50**	**42.50**	**80.00**	**50.83**	**58.61**
		(10.63)	(9.55)	(8.14)	(9.73)	(9.31)	(11.36)	(9.78)
High	Slow	**85.83**	**4.17**	**55.00**	**23.33**	**62.50**	**33.33**	**44.03**
		(3.75)	(0.83)	(13.66)	(5.87)	(12.23)	(10.46)	(7.80)
	Fast	**86.67**	**17.50**	**82.50**	**45.00**	**80.00**	**51.67**	**60.56**
		(5.11)	(8.73)	(7.39)	(12.32)	(7.64)	(8.82)	(8.33)
Mean		**78.13**	**17.50**	**72.50**	**36.04**	**73.75**	**43.75**	**53.61**
		(7.72)	(5.94)	(8.91)	(10.25)	(8.93)	(11.25)	(8.83)

Table 2. Mean NASA Task Load Index (TLX) scores are listed for the subscales of Mental Demand (MD), Physical Demand (PD), Temporal Demand (TD), Performance (P), Effort (E), and Frustration (F).

As can be seen in table 2, the overall composite workload rating for all task conditions (M = 53.61) fell above the midpoint of the scale (50), indicating that participants found the cyber monitoring assignment to be demanding. A 2 (event rate) × 2 (signal probability) × 6 (subscales) mixed ANOVA of the workload data revealed a significant main effect for event rate, F (1, 20) = 5.32, $p = .03$, $\eta_p^{\,2} = .21$, signifying that observers in the fast event rate condition (M = 59.58) found their vigilance assignments to be more challenging than those in the slow event rate condition (M = 47.64). A significant main effect was also found for subscales, F (2.88, 57.66) = 33.02, $p < .001$, $\eta_p^{\,2} = .62$. Bonferroni corrected t-tests with alpha set at .05 indicated that participants perceived Mental Demand, Temporal Demand, and Effort as the greatest contributors to overall workload. The means for these scales, which fell at the upper level of the workload index, differed significantly from those of all of the other scales ($p < .05$ in all cases) but not from each other. The main effect for signal probability and all of the interactions in the analysis lacked significance (*p* > .05 in all cases).

DISCUSSION

Consistent with results first reported by McIntire et al. (2013), performance efficiency on the cyber task was susceptible to the vigilance decrement. In this case, the decrement consisted of a notable drop in signal detection during the last period of watch after participants maintained a stable level of performance across three earlier watchkeeping periods. The temporal step-function in regard to the cyber task differs from the decrement seen in traditional vigilance tasks wherein a negatively accelerated progressive decline in performance efficiency over time is typical (Davies & Parasuraman, 1982).

A major model used to account for the deterioration of performance efficiency over time characteristic of vigilance tasks is anchored in resource theory, in which a limited-capacity information processing system allocates resources or reservoirs of energy to deal with situations that confront it. Since vigilance tasks require observers to make continuous signal/noise discriminations without rest, such tasks deplete available cognitive resources over time, resulting in the vigilance decrement (Davies & Parasuraman, 1982; Proctor & Vu, 2010; Warm et al., 2008). The step-function observed in the present study may be based on a combination of motivation and resource loss. More specifically, since the participants were engaged in what they were told was a critical Air Force assignment, cyber defense, and were paid a substantial sum for serving in the study, they may have been moved to sustain a high level of performance. However, over time they were unable to do so, potentially because of diminished information processing resources.

It is critical to note it was no forgone conclusion that the information-rich cyber task would result in a vigilance decrement. Some highly complex tasks exhibit reduced or nonexistent vigilance decrements, especially when they are operationally diverse (Adams & Humes, 1963, Lanzetta, Dember, Warm, & Berch, 1987). In other cases however, complexity can amplify the decrement (as in Jerison, 1963; for a review see Craig, 1991; Warm et al., in press). Given the pattern observed, cyber tasks appear to fall in the latter category.

It is evident that operators cannot sustain performance in cyber tasks over prolonged intervals of time. Consequently, this must be considered in work scheduling and, as McIntire and her associates point out (McIntire et al., 2013), in the development of non-invasive methods to enable supervisors to monitor an observer’s need of rest or replacement. The oculomotor changes described by McIntire et al. (2013) offer one approach by which supervisors might “monitor the monitor.” Another possibility that supervisors of cyber security operators might consider is the use of transcranial Doppler sonography, a noninvasive neuroimaging method involving sensors worn in a headband, to assess cerebral bloodflow velocity (CBFV). Several studies have shown that the vigilance decrement is accompanied by a decline in CBFV and that the changes in CBFV can forecast declines in operator efficiency (Matthews, Warm, Reinerman-Jones, Langheim, Washburn, & Tripp, 2010; Reinerman-Jones, Matthews, Langheim, &Warm, 2011; Warm, Matthews, & Parasuraman, 2009).

Consistent with the findings in a large number of vigilance studies (Warm et al., in press; Warm & Jerison, 1984), participants in the cyber task benefited from a high level of signal probability. In a cogent analysis of human factors principles in the control of vigilance, Craig (1984) pointed out that one way to enhance the quality of sustained attention in operational settings is to reduce signal uncertainty. Increments in signal probability clearly reduce signal uncertainty. Consequently, when signal probability is low, as is often the case in cyber security operations, controllers might give some thought to introducing artificial signals in order to increase the level of signal probability, and thereby the likelihood of critical signal detection. A strategy of this sort would require careful thought, however, for as Craig (1984) has pointed out, artificial signals also increase the frequency of false alarms, which could have a negative impact on cyber security operations.

Vigilance experiments often employ dynamic displays wherein the critical signals for detection are embedded in a matrix of recurring neutral background events. Although the background events maybe neutral in the sense that they require no overt response from the observer, they are far from neutral in their influence on signal detection. Signal detections vary inversely with event rate, and event rate serves as a moderator variable for other psychophysical factors. For example, the degrading effects of low signal amplitude are magnified in the context of a fast as compared to a slow event rate (Warm, et al., in press; Warm & Jerison, 1984). Outcomes such as these were also evident in the cyber task employed in this study. Signal detection was poorer in the context of a fast as compared to a slow event rate and the differential effects of variations in signal probability were only observed in the fast event rate condition.

Clearly, event rate is a key factor in cyber performance and should be considered in the design of cyber security systems. As in the case of the vigilance decrement, the effects of event rate can also be accounted for on the basis of the resource model. Fast event rates require the observer to make more frequent signal/noise discriminations than slow event rates, and therefore, deplete information-processing assets to a greater degree (Davies & Parasuraman, 1982). From an operational viewpoint, it might seem reasonable to expect that the more an operator is required to view the cyber display, the more likely the operator is to detect adverse events. The event rate effect indicates this is not necessarily the case, and designers of cyber displays should be heedful of establishing the event rate that maximizes performance in the systems that they develop.

Along this line, it should be noted that in traditional vigilance tasks, event rates less than 24/min are categorized as slow, while those greater than 24 events/min are considered as fast (Davies & Parasuraman, 1982; Warm et al., in press). In the current study, 8 events/min constituted the slow event rate while the fast event rate was only 16 events/min, a value well below the 24 events/min criterion for the definition of a fast event rate. This fast event rate value was chosen because pilot work revealed that observers could not perform the task effectively at event rates of 24/min or more. Evidently, cyber task performance is extremely sensitive to variations in event rate.

At first glance, vigilance tasks may seem to be relatively simple and under-stimulating assignments since all observers are required to do is view a display and take action when a critical event occurs. To the contrary, however, research has shown that the cost of mental operations in vigilance is high, as reflected in scores on the NASA-TLX and the finding that Mental Demand and Frustration are the primary components of workload in vigilance (Finomore et al., 2103; Warm et al., 2008; Wickens et al., 2013). The present results indicate that cyber operations also induce high levels of mental demand as seen through the lens of the NASA-TLX – overall workload ratings were above the midpoint of the NASA-TLX and the scores for the Mental Demand, Temporal Demand, and Effort components of workload fell at the upper level of the workload index. It is of interest to note that, while the portrait of critical workload components in the present cyber task included Mental Demand, it also included Temporal Demand and Effort, which are not often incorporated in the ensemble of key workload elements identified in more traditional vigilance tasks. These differences in workload components may be related to the need for rapid responding and display scanning inherent in the cyber task employed herein, and to the participants' awareness of the importance of the task they were performing for Air Force operations.

As described by Wickens et al. (2013), mental workload characterizes the demands that tasks make on the limited information processing capacity of observers. Excessive levels of demand lead to declines in performance efficiency and to heightened levels of task related stress. Consequently, the high level of workload reported in the current experiment should be a concern to designers of cyber security tasks. From the resource view, care should be taken not to develop cyber displays in which mental demand exceeds resource supply, and to generate remedies for cyber tasks that pose threats to that supply. Given the high workload of cyber tasks, managers should be mindful of the fact that cyber tasks can be stressful and of the implications of stress for performance efficiency and operator health (Hancock & Warm, 1989; Nickerson, 1992).

In sum, the present study was designed to determine if cyber tasks can be linked to more traditional vigilance tasks. The answer to that question is a resounding "yes." Accordingly, cyber system designers need to be aware of the information-processing demands imposed by vigilance tasks and the steps that can be taken to minimize the negative effects of these demands on operator performance in cyber environments.

REFERENCES

Adams, J. A., and Humes, J. M. (1963). Monitoring of complex visual displays. IV. Training for vigilance. *Human Factors, 5*, 147-153.

Craig, (1984). Human engineering: The control of vigilance. In J.S. Warm (Ed.), *Sustained attention in human performance* (pp. 247-291). Chichester, UK: Wiley.

D'Amico, A., Whitley, K., Tesone, D., O'Brien, B., & Roth, E. (2005). Achieving cyber defense situational awareness: A cognitive task analysis of information assurance analysts. *Proceedings of the Human Factors and Ergonomics Society, 49, 229-233.*

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

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, 55*, 1044-1063.

Hancock, P.A. (2013). In search of vigilance: The problem of iatrogenically created psychological phenomena. *American Psychologist, 68,* 97-109.

Hancock, P.A., & Warm, J.S. (1989). A dynamic model of stress and sustained attention .*Human Factors, 31*, 519-537.

Hart, S.G., & Staveland, L.E. (1988). Development of NASA TLX (task load index): Results of empirical and theoretical research. In P.A. Hancock & N. Meshkati (Eds.), *Human mental workload* (pp. 139-183). Oxford, UK: North-Holland.

Lanzetta, T. M., Dember, W. N., Warm, J. S., & Berch, D. B. (1987). Effects of task type and stimulus homogeneity on the event rate function in sustained attention. *Human Factors, 29*, 625-633.

Lin, H.S. (2010). Offensive cyber operations and the use of force. *Journal of National Security Law & Policy, 4,* 63-86.

Matthews, G., Warm, J.S., Reinerman-Jones, L.E., Langheim, L.,Washburn, D.A., & Tripp, L.D. (2010). Task engagement, cerebral blood flow velocity, and diagnostic monitoring for sustained attention. *Journal of Experimental Psychology: Applied, 16,* 187-203.

Maybury, M.T. (2012). *Cyber Vision 2025: United States Air Force Cyberspace Science and Technology Vision 2012-2025* (Technical Report No. AF/ST TR 12-01). Retrieved from http://www.defenseinnovationmarketplace.mil/resources/cyber/cybervision2025.pdf

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.

Nickerson, R.S. (1992). *Looking ahead: Human factors challenges in a changing world.* Mahwah, NJ: Erlbaum.

Nygren, T.E. (1991). Psychometric properties of subjective workload measurement techniques: Implications for their use in the assessment of perceived mental workload. *Human Factors, 33*, 17-33.

Reinerman-Jones, L.E., Matthews, G., Langheim, L.K., & Warm, J.S. (2011). Selection for vigilance assignments: A review and proposed new direction. *Theoretical Issues in Ergonomic Science, 12, 273-296.*

Proctor, R.W., & Vu, K-PL. (2010). Cumulative knowledge and progress in human factors. *Annual Review of Psychology, 61*, 623-651.

Warm, J.S., Finomore, V.S., Vidulich, & Funke, M.E. (in press). Vigilance: A perceptual challenge. In R.R. Hoffman, P.A. Hancock, R. Parasuraman, J.L. Szalma, & M. Scerbo (Eds.), *The handbook of applied perception research.* New York: Cambridge University Press.

Warm, J.S., & Jerison, H.J. (1984). The psychophysics of vigilance. In J.S. Warm (Ed.), *Sustained attention in human performance* (pp.15-60). Chichester, UK: Wiley.

Warm, J.S., Matthews, G., & Parasuraman, R. (2009). Cerebral hemodynamics and vigilance performance. *Military Psychology, 21*, S75-S100.

Warm, J.S., Parasuraman, R., & Matthews, G. (2008). Vigilance requires hard mental work and is stressful. *Human Factors, 50,* 433-441.

Wickens, C.D., Hollands, J.G., Banbury, S., & Parasuraman, R. (2013). *Engineering psychology and human performance* (4th ed.). Boston: Pearson.