Enhancing the Efficacy of Identifying Visual Patterns and Novel Anomalies of Cyber-Defenders With 3D Immersive VR

David Passig, Bar-Ilan University, Israel
Reut Hochman, Bar-Ilan University, Israel

The IAFOR International Conference on Education in Hawaii 2022
Official Conference Proceedings

Abstract
The mission of a Cyber Security Officer (CSO) during a cyberattack is to identify anomalies in visual signals and to ascertain whether they are hostile. These signals occur in an environment overflowing with data, which is constantly shifting shape and density, and in which the rate of change keeps accelerating and novel anomalies arise. In this environment, previous experience is disadvantageous and oftentimes harms the ability of a CSO to identify novel patterns of anomalies. This study tested, in a moderated mediation model, the effect of Immersive Virtual Reality (IVR), while identifying hidden forms in Embedded Figure Tasks (EFTs), on the ability to detect a novel and unknown anomaly. Through a quasi-experiment with repeated measurements, we compared five research groups, four of which practiced cognitive intervention while detecting cyber anomalies. The improvement was tested through a pre-test and post-test procedure. A cluster sampling involved 120 students recruited from the Academy of Computer and Cyber Training at the Telecommunication Branch of the Israel Defense Forces. We found that participants who practiced the EFTs in an IVR information-diluted environment (VRLVL) detected novel anomalies faster than the control group. We also found that the higher the thought elasticity of the participants in an IVR highly-loaded environment (VRHVL), the higher their speed in detecting novel anomalies.

Keywords: 3D Immersive VR, Cyber, Cyber Security Officer, Cyberattack, Cyber Training, Anomalies, Visual Patterns, Embedded Figure Tasks

Introduction

The information age is characterized by digitized environments overflowing with data that are constantly shifting shape and density, and in which the rate of change keeps accelerating. However, our ability to process all the information obtained from our senses is limited and affected by various factors, the most dominant of which is attention (Posner & Petersen, 1990). Previous studies have found solutions to increase attention and the amount of information processed in a state of data overload and have also suggested ways to improve the ability to detect visual changes in an information-laden environment. These studies have found that it is possible to increase the amount of information a person can process in four ways: (a) by reducing the irrelevant information that comes to him/her (Bavelier, et al., 2012); (b) by directing attention exclusively to relevant stimuli (Coren, Ward & Enns, 1991); (c) by grouping an unlimited number of items into a single unit of meaning known as an "information chunk"; (d) and by creating an analogy to prior knowledge that is stored in memory (Bar, 2007).

However, these studies did not address the identification of a new and unfamiliar visual stimulus, where experience cannot be applied to the nature of the new stimulus or where that experience impairs a person's ability to identify new patterns—be they algebraic, textual, numerical or geometrical signatures (Passig, 2007; Bilalić & Mcleod, 2014; Storm & Patel, 2014). These situations characterize the mission of a human defender against cyberattacks, whose job it is to monitor the system while being required to identify new attacks for which nothing from his/her past knowledge is relevant. In the language of cyberdefense, these are called "zero-day vulnerabilities." In these instances, the human cyber-defender is required to detect a change in visual signals or patterns, to generalize it, and to produce the insight that a cyberattack is indeed underway. In this respect, the ability to classify change, as normal or abnormal, shifts rapidly.

The term "anomaly" is used to describe any deviation from a particular norm or law in a variety of fields. This is an irregularity that is difficult to explain in existing rules and theories. Such an attack is associated with a new type of attack on online databases, for which the defense methods used so far do not provide the required response. Today's common defense systems protect against known attacks based on known signatures (hallmarks). This method of defense provides a satisfying ping that alerts in the case of certain and known attacks, but it is useless in the face of the increasingly unrecognized attacks, which lack a familiar signature. Solving this problem requires different solutions (Garcia-Teodoro, et al., 2009). One possible solution is to monitor the anomaly of network activity, both by computerized systems and by human monitors (Riveiro et al., 2008).

Over the years, studies have addressed the cognitive process required to identify visual change (Simons & Levin, 1997). These studies have found that the ability to detect change is related to the place of the change when it appears on the retina, but the studies did not address where and how one might identify a new and unfamiliar stimulus. It was later discovered that visual perception of an object found around a person's eyes is affected by generating an analogy with a similar object found in one's memory (Bar, 2007). This finding implies that, in any case, we need to have a similar representation of the object in our memory. To the best of our knowledge, this sums up a defender's unique challenge in identifying real-time cyberattacks. The visual representation of a future attack is not similar to its past representation or to the alert algorithms that are stored in automated monitoring systems.

From a review of the literature on the detection of anomalies in the cyber realm, we have not yet found a cognitive model for training cyber-defenders in anomaly detection.

We have found additional cognitive differences in the research literature that seem to affect the way a person learns, perceives, and processes visual information, which is relevant to our inquiry. For example, it seems there is a marked difference between people whose way of learning depends on the external environment (FD: Field Dependent) in the process of visual identification and processing compared to those who do not depend on external cues (FI: Field Independent) (Dillon & Gabbard, 1998). This cognitive style distinguishes people based on their ability to absorb and process visual information and based on their ability to solve complex problems. People who are not dependent on their external environment to learn are quicker at identifying a particular geometric shape hidden within a variety of shapes, compared to those who are dependent on their external environment who may not recognize it at all. Angeli & Valanides (2004), also found that people who depend on their external environment have difficulty finding relevant information within information-laden environments. The possible explanation that has been suggested is that their minds are probably distracted by the environment and as a result, they struggle to isolate the target object from its surrounding.

Field Independent (FI) people have also been found to be able to isolate relevant information from complex environments, process it accurately, analyze ideas for the components that construct them, and frame them into new configurations—all the more than Field Dependent (FD) people, who are more traditional in their way of thinking. However, the implications of the cognitive style of FD or FI in the context of identifying visual information and processing it in a computerized environment are not unequivocal and the conclusions drawn by various researchers in this regard are contradictory (Angeli & Valanides, 2004).

In this regard, Lavie, Beck, and Konstantinou (2014) found that during tasks with a low perceptual load, the awareness of new stimuli increases, while during tasks with a high perceptual load, it decreases. The researchers also found that in the task of natural contrast, when the level of perceptual load is low, such as at the stage where one differentiates between “mountain” and “tree,” the number of neutral stimuli for perception increases. Conversely, in an unnatural contrast, that requires perceptual effort, the number of neutral stimuli that reach perception decreases. On the other hand, in a state of high cognitive load in working memory, a person tends to relate to neutral stimuli that may distract him/her from the target stimulus (Lavie, Hirst, de Fockert & Viding, 2004) and the number of new stimuli that rise to perception increases, and vice versa (Storm & Patel, 2014).

In the literature review, we found also that high levels of mental flexibility and diversity in information representation, including 3D, contribute to the process of identifying anomalies in an information-laden environment (Riveiro et al., 2008). We also found that the ability to detect a variable visual stimulus is affected by the subject's level of tolerance for uncertainty and his/her degree of dependence on the external environment (FD/FI) (Witkin, 1981).

The literature review also indicates that representation through 3D Immersive Virtual Reality (IVR) enhances mental flexibility (Passig & Eden, 2000b). Researchers (Jacob, Averbuch, Sacher, et al., 2013), also found that practicing 3D IVR improves cognitive skills, with an emphasis on planning ability and mental flexibility. These skills are defined as high-order cognitive abilities that are required to perform new or complex daily tasks.

Thus, we engaged to develop a cognitive model for identifying an object/signal/signature that is not based on experience. The cognitive model we tested is based on tolerance for uncertainty, mental flexibility, and independence in the external environment in identifying and processing the anomalous stimulus, to find a solution to the challenge of detecting an anomaly in a rapidly changing environment.

Procedure

This study was conducted in a quasi-experimental mode. We examined the effect of the practice of identifying hidden geometrical signatures in different modes of representation (2D or 3D IVR) and different types of information loads (information-laden environment or information-diluted environment), on the level of accuracy and speed in anomaly detection, with the following variables: tolerance for uncertainty, cognitive closure, and mental flexibility. The improvement in anomaly detection was examined in pre-and post-tests. The participants were sampled in a cluster-sampling method from differentiators in the final stage of the IDF Cyberdefense course and trainees in the first two weeks of another similar cyberdefense course.
Accordingly, we examined in the study five research conditions with five different groups of trainees as detailed herein.

Study groups:

- VRLVL (N=22): This group practiced the task of identifying hidden shapes in an information-diluted environment in 3D immersive virtual reality.
- VRHVL (N=19): This group practiced the task of identifying hidden shapes in an information-laden environment in 3D immersive virtual reality.
- 2DLVL (N=25): This group practiced the task of identifying hidden shapes in an environment that dilutes information in a 2D mode of representation.
- 2DHVL (N=21): This group practiced the task of identifying hidden shapes in an information-laden environment in a 2D mode of representation.
- Ctrl (N=33): This group didn't practice identifying hidden shapes, they developed a scenario of identifying anomalies in a pretest and a posttest.

Table 1 shows the breakdown of the research groups per mode of representation and information load.

Research groups	Information Representation	Information load
VRLVL	3DVR	Low
VRHVL	3DVR	High
2DLVL	2D	Low
2DHVL	2D	High
Ctrl	-	-

Table 1: Research Conditions per Modes of Representation and Information Loads

Note. 3D virtual reality in an information-diluted environment (VRLVL); 3D virtual reality in an information-laden environment (VRHVL); 2D in an information-diluted environment (

2DLVL); 2D in an information-laden environment (2DHVL); Control Group (Ctrl); 3D Virtual Reality (3DVR); 2D (2D).

Participants

This study included 120 participants, 34 of whom were women (27.9%) and 86 of whom were men (72.1%). Their age ranged from 18 to 24 years (M=18.5, SD=0.61), The range of their schooling years was from 12 to 15 years (M=12.4, SD=0.57).

Table 2 presents the distribution of participants per background variable divided by the five study groups. A $\chi 2$ test was performed for categorical background variables and further analysis (One Way ANOVA) for continuous background variables.

Variable name	VRLVL (n=22)		VRHVL (n=19)		2DHVL (n=21)		2DLVL (n=25)		Ctrl (n=33)		Statistical comparison
Gender, N (%)											
Women	6	(27.3)	8	(42.1)	6	(28.6)	6	(24.0)	8	(24.2)	$\chi 2$ (4) =2.18, p = .703
Men	16	(72.7)	11	(57.9)	15	(71.4)	19	(76.0)	25	(75.8)	
Age, M (SD)	18.14	(0.46)	18.16	(0.60)	18.4	(0.67)	17.96	(0.53)	18.12	(0.69)	F (4,115)=1.38, p=.244 η_p^2=.046
Education, M (SD)	12.05	(0.21)	12.05	(0.23)	12.32	(0.90)	12.12	(0.60)	12.15	(0.61)	F (4,115)=.831, p=.508 η_p^2=.028

Table 2: Distribution of Participants per Background Variables Divided by Study Groups

Note. 3D virtual reality in an information-diluted environment (VRLVL); 3D virtual reality in an information-laden Environment (VRHVL); 2D in an information-laden environment (2DHVL); 2D in an information-diluted environment (2DLVL); Control Group (Ctrl); all p's> .05

Looking at test values, $\chi 2$ presented in Table 2 indicates there was no significant dependence between the background variables and the demographics. Also, in the variance analysis, no significant differences were found in continuous background variables per study groups. Hence, there was no need for statistical monitoring of the background variables to examine the research hypotheses.

The study took about a year to complete. After receiving the appropriate approvals from the military authorities, we administered the test battery to the participants during the computer courses' selection process at the computer school and during the first week of the cyberdefense course.

In the first phase, the participants completed personal background questionnaires and cognitive questionnaires (tolerance for uncertainty, cognitive closure, and mental flexibility). Data was also collected regarding the achievement tests that they received during the screening process by the military authorities.

In the second stage, the participants performed a computer anomaly detection task. The first ten times they had to find the letter B, and the 11th time they had to find the letter D. Figure 1 shows a scenario used in the anomaly detection task to identify the letter B.

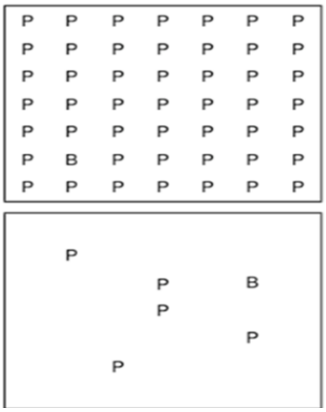

Figure 1: Scenario Used for Signal Detection Anomaly Task

In the third phase of the study, the four intervention groups practiced a hidden form task in the different representation modes. The intervention took about 20 minutes, and the participants were required to identify 20 hidden forms when their time and accuracy were automatically measured. The characteristics of the practice varied according to the study group. In the VRHVL group and the VRLVL group, the participants practiced the task of the hidden geometrical shapes in the computer while wearing the Oculus Rift virtual reality headset in an information-laden environment and an information-diluted climate. In contrast, the 2DHVL and 2DLVL groups practiced the test of the computer's hidden geometrical shapes without wearing a virtual reality headset in an information-laden environment and information-diluted climate.

In the fourth and final stage, the participants performed an anomaly detection task similar to the second stage of the procedure.

Data were obtained from the military authorities regarding the results of the five factors in BTS personality for cyber course trainees only. The ability to detect an anomaly (in real-time) in a cyber defense course was measured. This task remained confidential due to field security reasons, and the final grades were passed on to us using trainee assigned numbers.

Tests

Questionnaire for Thought Flexibility

In our study, we used a "circular" sub-test, based on a questionnaire for checking thought flexibility developed by Torrance (1966). We checked whether exercises that involved rotating 3D objects, which requires an ability to look at objects from different angles, would influence the participants' thought flexibility. The test included both verbal and non-verbal tasks. In the non-verbal tasks, the flexibility sub-test (in its non-verbal form—the clause of repetitive stimuli) is presented to each subject on a piece of paper featuring thirty-six identical circles.

Fig. 2 presents a screenshot of a (non-verbal) flexibility sub-test—the clause of repetitive stimuli.

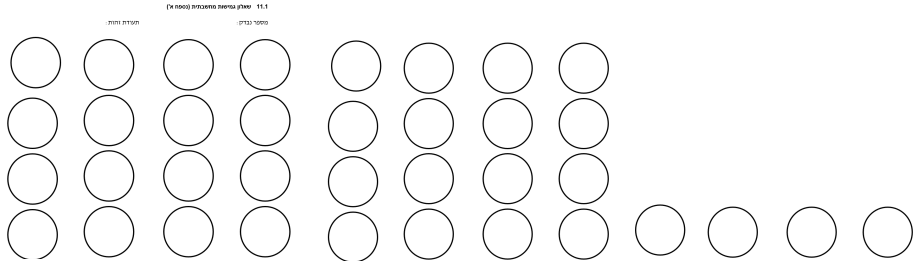

Figure 2: A (Non-Verbal) Flexibility Sub-Test

Tolerance for Uncertainty Questionnaire

In our study, we used a questionnaire for investigating the cognitive aspect known as "tolerance for uncertainty," (McDonald, 1970). The questionnaire includes 15 statements. Test participants are asked to give their opinion about the extent to which each statement is true or false. For example: "I have little interest in a problem that I don't think has a solution" (statement 1); the statements are ranked on a scale from 1 ("completely disagree") to 5 ("agree very strongly").

Cognitive Closures Questionnaire

Another questionnaire that we used in our study was intended to examine the cognitive aspect known as "closure." The questionnaire includes 16 statements. The subject must give his opinion about the extent to which these statements are true or false. For example: "I feel uncomfortable in unpredictable situations" (statement 1); "a regular life with fixed hours suits my temperament" (statement 2).

Embedded Figure Test

We examined a perceptual test for processing shapes. This test was computerized and involved 20 multiple-choice questions. The test lasted 12 minutes. The range of (raw) scores was 0-20. Participants had to identify a single shape out of five simple shapes, embedded inside a more complicated shape. The quicker each subject managed to locate the simple shape, the more his cognitive style tended to a lack of dependence on the complexity of the field. This test included questions of increasing difficulty. The exercise is based on four formulae that parallel the test of the hidden shapes drawn for this study, per different research conditions. Each group ran the exercise for around 20 minutes. The exercise was conducted using VR headsets. A small percentage of participants felt slightly dizzy for a brief period during the test. Their performance in the test was evaluated based on the total time required for each subject to identify the 20 scenarios. The longer it took, the weaker their performance. This test served our study as a research intervention to improve the detection of anomalies.

Figure 3 presents an example of a multiple-choice question in the hidden shapes test, featuring a graphical shape of a low level of difficulty.

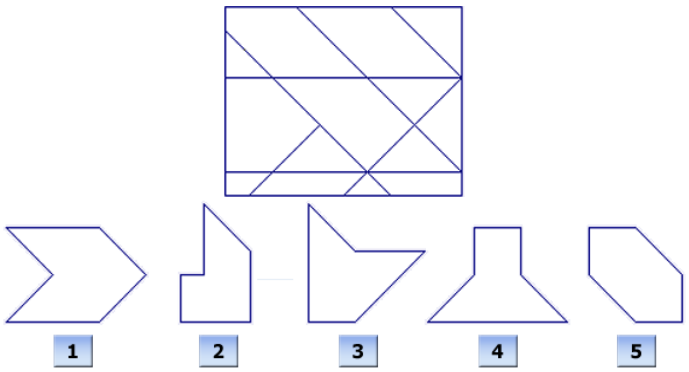

Figure: 3 A Multiple-Choice Question in the Hidden Shapes Test

A B

Figure 4: Sample of Screenshots of Practicing Hidden Shapes by Learning Environment: A. An Information-Laden Environment B. Information-Diluted Environment

Figure 5 shows an image of an Oculus Rift Virtual Reality (VR) headset we used in this study.

Figure 5: An Oculus Rift Virtual Reality (VR) Headset

Results

The findings indicate that at both measurement times, most participants detected anomalies; no clear difference in anomaly detection was found based on how the information was presented. As for the speed of the detection, in the post-intervention stage, regression analysis shows that consistently with the hypothesis, among participants in the 3D simulated reality group and the 2D simulated reality group, the time it took to complete the task was significantly shorter compared to the control group. Nevertheless, both of these research groups reached similar results, contrary to the hypothesis. As such, we noted that the addition to the explanation for the difference of these conditions obtained a marginal level of

significance. Finally, we noted that no significant moderation effect was found for the tolerance for uncertainty, cognitive closure, and thought flexibility variables concerning the contribution of the presentation to the predicted speed of anomaly detection. Nevertheless, it was found that the greater the level of thought flexibility, the longer the time it took to complete the task (marginal significance).

Predictors	Model A		Model B		Model C	
	$R^2\Delta$	β	$R^2\Delta$	β	$R^2\Delta$	β
Step I	.03		.03		.03	
Gender		.12		.12		.12
Age		-.10		-.10		-.11
Education		.05		.05		.01
Cognitive exams		-.12		-.12		-.11
Step I I	.06#		.06#		.06#	
Gender		.11		.11		.11
Age		-.11		-.11		-.12
Education		.04		.04		.01
Total score in cognitive exams		-.12		-.12		-.12
VR		-.28*		-.28*		-.29*
2D		-.27*		-.27*		-.28*
Step III	.00		.00		.03	
Gender		.12		.11		.13
Age		-.10		-.12		-.14
Education		.03		.04		.00
Total score in cognitive exams		-.14		.-12		-.12
VR		-.29*		-.28*		-.27*
2D		-.28*		-.28*		-.26*
Tolerance for uncertainty		-.06				
Cognitive closure				.03		
Flexible thinking						.16#
Step IV	.02		.00		.05	
Gender		.13		.11		.11
Age		-.10		-.12		-.14
Education		.03		.04		.02
Total score in cognitive exams		-.14		-.12		-.16
VR		-.30*		-.28*		-.28*
2D		-.27*		-.27*		-.26*
Tolerance for uncertainty		-.20				
Cognitive closure				.08		
Flexible thinking						.09
VR x Tolerance for uncertainty		.07		---		
2D x Tolerance for uncertainty		.20		---		
VR x Cognitive closure				-.08		
2D x Cognitive closure				.20		
VR x Flexible thinking						.21

2D x Flexible thinking			-.09
R^2	.11	.09	.16

Table 4: The Effect of Representation of Information on Speed of Identifying Anomaly —Hierarchical Regression

Note. Gender: 0=women; 1=men. Methods of information presentation: 3D virtual reality (VR); two-dimensional image (2D); Model A: Moderation effect of the tolerance for uncertainty metric (N=95); Model B: Moderation effect for cognitive closure metric (N=95); Model C: Moderation effect of flexible thinking metric (N=97). $p < .05$ * $p \leq .06$#.

As for the second research hypothesis, the pattern of results partially confirms it. The findings show that at both measurement times, most participants identified an anomaly, and no significant difference in anomaly detection was found based on the information load. As for the speed of the anomaly detection, in the post-intervention stage, regression analysis shows that consistently with the hypothesis, among participants in information-laden environments and information-diluted environments, the time it took to complete the task was significantly shorter compared to the control group. Nevertheless, these two research conditions made similar predictive contributions, contrary to the hypothesis. As such, note that the addition to the explanation of the differences between these conditions achieved significance. Finally, we note that no significant moderation effect was found in the case of the tolerance for uncertainty, cognitive closure, and thought flexibility variables concerning the contribution of information loads to predicting the speed of anomaly detection. Nevertheless, we found that the higher the level of thought flexibility, it took significantly longer to complete the task.

Predictors	Model A		Model B		Model C	
	$R^2\Delta$	β	$R^2\Delta$	β	$R^2\Delta$	β
Step I	.03		.03		.03	
Gender		.12		.12		.12
Age		-.10		-.10		-.11
Education		.05		.05		.01
Cognitive exams		-.12		-.12		-.11
Step I I		.06*		.06*		.07*
Gender		.12		.12		.12
Age		-12		-.12		-.13
Education		.03		.03		.00
Total score in cognitive exams		-.12		-.12		-.11
Empty		-.32*		-.32*		-.32*
Load		-.23*		-.23*		-.23*
Step III		.00		.00		.03#
Gender		.12		.12		.14
Age		-.11		-.13		-.15
Education		.03		.03		-.01
Total score in cognitive exams		-.13		-.11		-.11
Empty		-.32*		-.32*		-.31*
Load		-.23*		-.22*		-.21
Tolerance for uncertainty		-.05				
Cognitive closure				.05		
Flexible thinking						.17*

Step IV	.00		.02		.00	
Gender		.12		.12		.12
Age		-.10		-.14		-.14
Education		.03		.03		-.00
Total score in cognitive exams		-.12		-.08		-.11
Empty		-.33*		-.32*		-.32*
Load		-.24*		-.21#		-.22#
Tolerance for uncertainty		-.20				
Cognitive closure				.10		
Flexible thinking						.09
Empty x Tolerance for uncertainty		.13				
Load x Tolerance for uncertainty		.12				
Empty x Cognitive closure				-.13		
Load x Cognitive closure				.06		
Empty x Flexible thinking						.12
Load x Flexible thinking						.00
R^2		.11		.11		.12

Table 5: The Effect of the Environment on the Speed of Identifying Anomaly –Hierarchical Regression

Note. Gender: 0=women; 1=men. Information load: information-diluted environment (empty); information-laden environment (load); Model A: Moderation effect of the tolerance for uncertainty metric (N=95); Model B: Moderation effect for cognitive closure metric (N=95); Model C: Moderation effect of flexible thinking metric (N=97). $p < .05$ * $p \leq .06$#.

Finally, the pattern of results points to partial corroboration of the third research hypothesis. Regarding the detection of anomalies, no confirmation was obtained for the hypothesis, because the results point to most participants detecting anomalies at both measurement times, and no significant difference was found in anomaly detection based on the manner of the presentation of the information and the information load. As for the speed of anomaly detection, in the post-intervention stage, regression analysis shows that consistently with the hypothesis, among the participants in the 3D reality in the information-diluted environment, it took significantly less time to complete the task compared to the control group. Nevertheless, the contribution to the prediction of the 3D simulated reality in the information-diluted environment was not significantly different from the predictive contribution of other research conditions. Finally, we note that no significant moderation effect was found for the tolerance for uncertainty, cognitive closure, and thought flexibility variables concerning the contribution of the manner of the presentation of the information and the information load to predicting the speed of anomaly detection. Accordingly, the hierarchical regression analysis predicted significant effects that were not obtained using the PROCESS software.

Predictors	Model A		Model B		Model C	
	$R^2\Delta$	β	$R^2\Delta$	β	$R^2\Delta$	β
Step I	.03		.03		.03	
Gender		.12		.12		.12

Age		-.10		-.10		-.11	
Education		.05		.04		.01	
Cognitive exams		-.12		-.12		-.11	
Step II	.01		.06		.07		
Gender		.12		.12		.12	
Age		-.12		-.12		-.13	
Education		.03		.03		.00	
Total score in cognitive exams		-.12		-.12		-.11	
VRHVL		-.17		-.17		-.17	
VRLVL		-.28*		-.28*		-.28*	
2DLVL		-.24*		-.24*		-.25*	
2DHVL		-.20		-.20		-.20	
Step III	.00		.00		.03		
Gender		.12		.12		.14	
Age		-.13		-.10		-.14	
Education		.03		.03		-.00	
Total score in cognitive exams		-.11		-.13		-.11	
VRHVL		-.16		-.17		-.14	
VRLVL		-.29*		-.28*		-.28*	
2DLVL		-.24*		-.25*		-.28*	
2DHVL		-.20		-.20		-.20	
Tolerance for uncertainty		.05					
Cognitive closure				-.05			
Flexible thinking						.17	
Step IV	-.00		.04		.06		
Gender		.11		.09		.12	
Age		-.16		-.11		-.15	
Education		.03		.03		.01	
Total score in cognitive exams		-.07		-.10		-.16	
VRHVL		-.10		-.17		-.13	
VRLVL		-.27*		-.28*		*31.	
2DLVL		-.25*		-.21		-.24*	
2DHVL		-.20		-.21		-.19	
Tolerance for uncertainty		.11					
Cognitive closure				-.19			
Flexible thinking						.09	
VRHLV x Tolerance for uncertainty		.10					
VRLVL x Tolerance for uncertainty		-.02					
2DLVL x Tolerance for uncertainty		.01					
2DHVL x Tolerance for uncertainty		-.17					
VRHLV x Cognitive closure				.14			
VRLVL x Cognitive				.02			

closure					
2DLVL x Cognitive closure			.00		
2DHVL x Cognitive closure			.22		
VRHLV x Flexible thinking					.11
VRLVL x Flexible thinking					-.08
2DLVL x Flexible thinking					.22
2DHVL x Flexible thinking					-.06
R^2	.13	.14		.18	

Table 6: The Effect of the Representation of Information and the Environment on the Speed of Identifying Anomalies -- Hierarchical Regression

Note. Gender: 0=women; 1=men. Virtual reality in an information-laden environment (VRHVL); virtual reality in an information-diluted environment (VRLVL); 2D in an information-diluted environment (2DLVL); 2D in an information-laden environment (2DHVL). Model A: Moderation effect of the tolerance for uncertainty metric (N=95); Model B: Moderation effect for cognitive closure metric (N=95); Model C: Moderation effect of flexible thinking metric (N=97). $p < .05$

Discussion

In the first research hypothesis, we assumed that participants who performed the hidden shapes task in the 3D simulated reality group and the participants who performed this task in the 2D group would improve the precision and speed of their anomaly detection more than the participants in the control group, which did not perform these exercises. Additionally, participants who practiced the hidden shapes task in the 3D simulated reality group would improve the precision and speed of their anomaly detection more than participants who performed this exercise in the 2D group.

This hypothesis was partially corroborated, and it was found that participants who practiced the hidden shapes task in the 3D and 2D simulated realities demonstrated a greater improvement in the precision and speed of their anomaly detection than the participants in the control group.

Various explanations for this result can be found in the research literature. Rizzo and Schultheis (2001) argued that the environment of a 3D simulated reality makes participants forget that they are in a test, and thus reduces their sense of pressure and anxiety and improves their performance in comparison to the control group. They also found that in an immersive 3D environment, there is a comparative advantage in the performance of cognitive evaluation and diagnosis processes compared to traditional environments. The advantage is a product of elements of an environment free of environmental risks, and of elements of the ability to control examinable stimuli. According to them, experience in the simulated reality makes participants “forget” that they are in a test and makes it possible to check them less artificially than traditional test conditions. As such, the exercise in the 3D simulated reality creates a sense of “selective experience” based on the individual’s tendency to focus on specific, significant, and interesting information.

As for the selective experience, the experience of being present in a simulated reality exists when there is the ability to focus on a set of significant, interconnected, fluent, and coherent stimuli that neutralize the irrelevant stimuli in one’s physical surroundings, which blend into

the other characteristics of the simulated reality to create a comprehensive whole. The findings from our first hypothesis correspond with the findings of these and other studies, which have pointed to the fact that the simulated reality helps with several diverse cognitive functions (Passig and Eden, 2000; Brooks and Rizzo, 2005), such as visual perception of space (Tong, Marlin, Barrie, and Frost, 1995), and the raising of Cyber Situational Awareness (Kbil et al., 2018).

Brooks and Rizzo (2005) also note that in simulated reality, it is possible to broaden a person's perspective of a concept/task by using another visual perspective that was not possible in reality. These perspectives are called "frames of reference" (FOR). Participants may maintain these abilities after the hidden images exercise, carrying them through to the visual anomaly detection task, enabling them to identify anomalies more quickly than test groups, with the goal changing from B to D.

On the other hand, we found no confirmation for the 3D and 2D simulated realities contributing to boosting the rapid detection of anomalies, contrary to the first research hypothesis. One possible explanation for this might derive from the dispute in the research literature about the implications of FD or FI cognitive styles in the context of identifying visual information and processing it in computerized environments (Angeli and Valanides, 2004), and the fact that in our study, the cognitive exercise was one-off and non-continuous, and as a result, it is possible that the transference effect to the true situation was deficient. Another possible explanation for this might derive from prior gaming experience. Participants with prior gaming experience adjusted quickly to the Oculus Touch motion controllers, suggesting that the relevant dexterity and muscle memory for gaming console controller usage helps users adjusting from those controllers to handling input devices for VR experiences. Multiple participants acknowledged that such 3D visualizations of network topology could assist in their understanding of the networks they use daily (Kullman, Ryan & Trossbach, 2019).

We found supporting evidence for this finding in the literature, which indicated that passing from the anomaly detection test to the true situation among cyber-defenders improves the more challenging and longer the exercise is (Dutt et al., 2012).

Consistent with the second research hypothesis, the results also seem to indicate that among participants in the information-laden environment and the information-diluted environment, the time it took to detect anomalies was significantly shorter in comparison to the test group. This can be explained with reference to the term "hidden steering process." This process refers to the performance of the hidden shapes test with variable loads of information by the test group, not the control group. The research literature reports that the absence of steering for work processes creates another cognitive load, which finds expression in an extension of the participants' response time and a decline in their degree of accuracy, especially in questions with low levels of cognitive load (Waxman, 2016). Indeed, in our study, the visual anomaly detection was during activities with low cognitive loads, and therefore it is possible that the lack of steering in the control group alone created another cognitive load, beyond the existing visual load.

According to the research literature, cognitive load affects people's ability to perform tasks as a result of the connection between them and their working memory. Cognitive load is created by several factors, such as the visual load (Huanga et al., 2014); the type of question—local or global (Kima et al. 2014); and participants' prior knowledge about the processing of visual

information (Gaissmaeier et al., 2011). These create a scale of seven levels of cognitive load. In the research literature, we find that an increase in cognitive load, demanding a greater volume of working memory, will lead to a longer response time. It is possible that in our study, participants who were required to perform the anomaly detection task without prior exercises that might have distracted them from the core exercise experienced greater cognitive load than the test group, and therefore the response time for anomaly detection was longer compared to other research groups that experienced cognitive interventions with variable levels of information. Additionally, the results of our research point to a comparative advantage to the exercise in information-diluted environments compared to the test group, consistent with the findings of Riveiro (2001), who recommends reducing the cognitive visual load to the minimum necessary to perform a visual detection task.

In contrast to these findings, we found that the two research conditions—the information-laden and information-diluted environments—made similar predictive contributions, contrary to the second research hypothesis. This result may derive from the motivational aspect of the anomaly detection task. In the research literature, we find that in tasks with high levels of motivation, the noise effect ("information load" in our study), which is independent of the target stimulus, does not influence the degree of attention to the stimulus (Kjellberg, 2004). The participants in our study were students in the IDF's computing and cyber courses and therefore may have had high motivation to succeed in the course and their roles. It is also possible that they were highly motivated to succeed in this task. Veneruso et al., (2020), also showed that CyberVR is equally effective but more engaging as a learning method.

As for the third research hypothesis, in analyzing variance, we did not find a significant difference in all the metrics of cognitive style according to the research conditions before the intervention, in contrast to the study of Dutt et al. (2013), who found that the greater a human cyber defender's tolerance for uncertainty, the more his/her ability to detect anomalies improves. The lack of significance may be a product of the homogeneity of the participants in our study. As such, the predictive contribution of the 3D simulated reality in the information-diluted environment was not significantly different from that of the other research conditions. This finding is consistent with the dispute in the research literature around the question: do background noises positively or negatively affect hidden shape tests? The cognitive exercise in the study of Andrew et al. (2013) found that the contribution of background noises to the performance of the hidden shapes test depends on the specific task and therefore it is not possible to determine unequivocally that background noises impede or contribute to the hidden shapes task.

Additionally, we have shown that in cyber defense, teamwork is better than the protection provided by an individual defender, and therefore it is advisable to check how the cognitive exercise influences anomaly detection in cyberspace by cyber-defender teams (Reed et al., 2013).

Conclusion

This study aimed at testing a novel way to overcome the most difficult issue in cyber defenders training. Cyber-attacks have become a critical threat to the digital human civilization. Attackers are constantly developing new tactics to penetrate the backbone of crucial human digital services with novel anomalies that are becoming harder and harder to detect before they cause damage. This study has demonstrated that defense tactics need to

evolve as well to better serve human civilization against a threat that brings havoc to social order.

References

Amir Orbach, Gabi Siboni (2013). Failure of Classic Cyber Defense Methods - What's Next? *Army and Strategy, 5*, (1), 37-48.

Angeli, C., & Valanides, N. (2004). Examining the effects of text-only and text-and-visual instructional materials on the achievement of field-dependent and field-independent learners during problem-solving with modeling software. *Educational Technology Research and Development, 52(4)*, 23–3. https://doi.org/10.1007/BF02504715

Arabacioglu, B. C. (2010). Using fuzzy inference system for architectural space analysis. *Applied Soft Computing, 10,* 926–937. https://doi.org/10.1016/j.asoc.2009.10.011

Awh, E., Barton, B., & Vogel, E. K. (2007). Visual working memory represents a fixed number of items regardless of complexity. *Psychological Science*, *18*(7), 622-628. https://doi.org/10.1111/j.1467-9280.2007.01949.x

Bavelier, D., Achtman, R. L., Mani, M., & Föcker, J. (2012). Neural bases of selective attention in action video game players. *Vision Research*, *61*, 132-143. https://doi.org/10.1016/j.visres.2011.08.007

Bar, M. (2007). The proactive brain: using analogies and associations to generate predictions. *Trends in Cognitive Sciences*, *11*(7), 280-289. https://doi.org/10.1016/j.tics.2007.05.005

Bengtsson, J., Waye, K. P., & Kjellberg, A. (2004). Evaluations of effects due to low-frequency noise in a low demanding work situation. *Journal of Sound and Vibration*, *278*(1-2), 83-99. https://doi.org/10.1016/j.jsv.2003.09.061

Bilalić, M., & McLeod, P. (2014). Why good thoughts block better ones. *Scientific American*, *310*(3), 74-79. https:// doi.org/10.1038/scientificamerican 0314

Boersma, F. J., Muir, W., Wilton, K., & Barham, R. (1969). Eye movements during embedded figure tasks. *Perceptual and Motor Skills*, *28*(1), 271-274. https://doi.org/10.2466/pms.1969.28.1.271

Bowen, B. M., Devarajan, R., & Stolfo, S. (2011, November). Measuring the human factor of cyber security. In *2011 IEEE International Conference on Technologies for Homeland Security (HST)* (pp. 230-235). IEEE. https://doi.org/10.1109/THS.2011.6107876

Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys (CSUR)*, *41*(3), 1-58. https://doi.org/10.1145/1541880.1541882

Chinien, C. A., & Boutin, F. (1993). Cognitive Style FD/I: An important learner characteristic for educational technologists. *Journal of Educational Technology Systems*, *21*(4), 303-311. https://doi.org/10.2190/WVUW-Q5MU-YE9M-DFF4

Darrow, M. S. (1995). Increasing research and development of VR in education and special education. *VR in the School*, *1*(3), 5-8.

Dillon, A., & Gabbard, R. (1998). Hypermedia as an educational technology: A review of the quantitative research literature on learner comprehension, control, and style. *Review of Educational Research*, *68*(3), 322-349. https://doi.org/10.3102/00346543068003322

Dutt, V., Ahn, Y. S., & Gonzalez, C. (2013). Cyber situation awareness: modeling detection of cyber attacks with instance-based learning theory. *Human Factors*, *55*(3), 605-618. https://doi.org/10.1177/0018720812464045

Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers & Security*, *28*(1-2), 18-28. https://doi.org/10.1016/j.cose.2008.08.003

Goldstein, A. G., & Chance, J. E. (1965). Effects of practice on sex-related differences in performance on embedded figures. *Psychonomic Science*, *3*(1-12), 361-362. https://doi.org/10.3758/BF03343180

Gopher, D., Well, M., & Bareket, T. (1994). Transfer of skill from a computer game trainer to flight. *Human Factors*, *36*(3), 387-405. https://doi.org/10.1177/001872089403600301

Guilford, J. P. (1970). Creativity: Retrospect and prospect. *The Journal of Creative Behavior*, *4*(3), 149-168. https://doi.org/10.1002/j.2162-6057.1970.tb00856.x

Hall, C. C., Ariss, L., & Todorov, A. (2007). The illusion of knowledge: When more information reduces accuracy and increases confidence. *Organizational Behavior and Human Decision Processes*, *103*(2), 277-290. https://doi.org/10.1016/j.obhdp.2007.01.003

Jolliffe, T., & Baron□Cohen, S. (1997). Are people with autism and Asperger syndrome faster than normal on the Embedded Figures Test?. *Journal of Child Psychology and Psychiatry*, *38*(5), 527-534. https://doi.org/10.1111/j.1469-7610.1997.tb01539

Kabil, A., Duval, T., Cuppens, N., Le Comte, G., Halgand, Y., & Ponchel, C. (2018, March). Why should we use 3d collaborative virtual environments for cyber security? In 2018 IEEE fourth VR international workshop on collaborative virtual environments (3dcve) (pp. 1-2). IEEE. https://doi.org/10.1109/3DCVE.2018.8637109

Kemmerer, R. A., & Vigna, G. (2002). Intrusion detection: a brief history and overview. *Computer*, *35*(4), supl27-supl30. https://doi.org/10.1109/MC.2002.1012428

Kullman, K., Ryan, M., & Trossbach, L. (2019). VR/MR supporting the future of defensive cyber operations. *IFAC-PapersOnLine, 52*(19), 181-186. https://doi.org/10.1016/j.ifacol.2019.12.093

Lavie, N. (1995), Perceptual load as a necessary condition for selective attention. *Journal of Experimental Psychology: Human Perception and Performance*, *21*(3), 451. https://doi.org/10.1037/0096-1523.21.3.451

Lavie, N., Beck, D. M., & Konstantinou, N. (2014). Blinded by the load: attention, awareness and the role of perceptual load. *Philosophical Transactions of the Royal Society B: Biological Sciences*, *369*(1641), 20130205. https://doi.org/10.1098/rstb.2013.0205

Lavie, N., Hirst, A., De Fockert, J. W., & Viding, E. (2004). Load theory of selective attention and cognitive control. *Journal of Experimental Psychology: General*, *133*(3), 339. https://doi.org/10.1037/0096-3445.133.3.339

Lavie, N., & Robertson, I. H. (2001). The role of perceptual load in neglect: Rejection of ipsilesional distractors is facilitated with higher central load. *Journal of Cognitive Neuroscience*, *13*(7), 867-876. https://doi.org/10.1162/089892901753165791

Ludwig, I., & Lachnit, H. (2004). Effects of practice and transfer in the detection of embedded figures. *Psychological Research*, *68*(4), 277-288. https://doi.org/10.1007/s00426-003-0141-x

McConkie, G. W., & Currie, C. B. (1996). Visual stability across saccades while viewing complex pictures. *Journal of Experimental Psychology: Human Perception and Performance*, *22*(3), 563. https://doi.org/10.1037/0096-1523.22.3.563

Pantelidis, V. S. (1995). Reasons to Use Virtual Reality in Education. *VR in the Schools 1*(1), 1995. *URL: http://www.soe.ecu.edu/vr/reas.html (Revisited 2000)*.

Passig, D. (2007). Melioration as a higher thinking skill to enhance future intelligence. *Teachers College Record*, *109*(1), 24-50.

Passig, D., & Eden, S. (2000). Enhancing the induction skill of deaf and hard-of-hearing children with virtual reality technology. *Journal of Deaf Studies and Deaf Education*, *5*(3), 277-285. https://doi.org/10.1093/deafed/5.3.277

Passig, D., & Eden, S. (2000). Improving flexible thinking in deaf and hard of hearing children with virtual reality technology. *American Annals of the Deaf*, *145*(3), 286-291. https://doi.org/10.1353/aad.2012.0102

Passig, D., & Eden, S. (2001). Virtual reality as a tool for improving spatial rotation among deaf and hard-of-hearing children. *Cyberpsychology & Behavior*, *4*(6), 681-686. https://doi.org/10.1089/109493101753376623

Reed, T., Nauer, K., & Silva, A. (2013, July). Instrumenting competition-based exercises to evaluate cyber defender situation awareness. In *International Conference on Augmented Cognition* (pp. 80-89).

Riveiro, M., Falkman, G., & Ziemke, T. (2008, June). Improving maritime anomaly detection and situation awareness through interactive visualization. In *2008 11th International Conference on Information Fusion* (pp. 1-8). IEEE. https://doi.org/10.1002/widm.1266

Raiyn, J. (2014). A survey of cyber attack detection strategies. *International Journal of Security and Its Applications*, *8*(1), 247-256.https://doi.org/10.14257/ijsia.2014.8.1.23

Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-39454-6_9

Singer, P. W., & Friedman, A. (2014). *Cybersecurity: What everyone needs to know*. OUP USA.

Simons, D. J., & Rensink, R. A. (2005). Change blindness: Past, present, and future. *Trends in Cognitive Sciences, 9*(1), 16–20 .https://doi.org/ 10.1016/j.tics.2004.11.006

Smith, A. P., & Broadbent, D. E. (1980). Effects of noise on performance on embedded figures tasks. *Journal of Applied Psychology, 65*(2), 246. https://doi.org/10.1037/0021-9010.65.2.246

Sternberg, R. J., & Powell, J. S. (1983). Comprehending verbal comprehension. *American Psychologist, 38*(8), 878. https://doi.org/10.1037/0003-066X.38.8.878

Storm, B. C., & Patel, T. N. (2014). Forgetting as a consequence and enabler of creative thinking. *Experimental Psychology: Learning, Memory, and Cognition, 40*(6), 1594–1609. https://doi.org/10.1037/xlm0000006

Triesch, J., Ballard, D., Hayhoe, M., & Sullivan, B. (2003). What you see is what you need. *Vision, 3*(1), 9 .https://doi.org/10.1167/3.1.9

Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. *Science, 185*(4157), 1124–1131. https://doi.org/10.1126/science.185.4157.1124

Veneruso, S. V., Ferro, L. S., Marrella, A., Mecella, M., & Catarci, T. (2020). CyberVR: An Interactive Learning Experience in Virtual Reality for Cybersecurity Related Issues. In Proceedings of the International Conference on Advanced Visual Interfaces (pp. 1-8). https://doi.org/10.1145/3399715.3399860

Witkin, A. P. (1981). Recovering surface shape and orientation from texture. *Artificial Intelligence, 17*(1), 17-45. https://doi.org/10.1016/0004-3702(81)90019-9

Contact email: david.passig@biu.ac.il

Ethical compliance statements: This study has been approved by the IDF and the School of Ed at Bar Ilan U. ethics committee for research involving humans.