Enhancing the Efficacy of Identifying Visual Patterns and Novel Anomalies in Real Time of Cyber Defenders with 3D Immersive VR

Reut Tamary-Hochman

School of Education

Ph.D. Thesis

Submitted to the Senate of Bar-Ilan University

Ramat-Gan, Israel January 2020

Abstract

The mission of a cyber security officer (CSO) during a cyber-attack is to identify anomalies in visual signals and clearly ascertain whether they are hostile. These signals occur in an environment overflowing with data that is constantly shifting shape and density in which the rate of change keeps accelerating and novel anomalies are occurring. In this environment, previous experience is disadvantageous and oftentimes harms the ability of the CSO to identify new and unkown patterns of anomalies.

Over the years, many studies focused on the cognitive process required to identify a visual change. These studies found that the ability to identify visual change is related to the location of the change on the retina. However, these studies did not discuss the identification of a new unfamiliar stimulus. Lately, studies have found that visual perception of an object in a person's field of vision is performed by creating an analogy between the object and a similar object stored in the person's memory. The meaning of this finding is the essence of the unique challenge that characterizes a human cyber monitor in a fast shifting and constantly accelerating forms of unknown anomalies. However, the literature review indicates, to the best of our knowledge, that no cognitive mechanism that would improve CSOs' skills has been developed.

By designing a cognitive training procedure for an empty Immersive Virtual Reality (IVR) environment, this study offers a unique contribution to existing cognitive theories of detecting novel anomalies that do not fit any previous pattern. Furthermore, the training procedure serves as a platform for improving the ability of any student to identify changes in environments loaded with data that change at a rate typical of the learning atmospheres in the 21st century.

This study tested, in a moderated model, the effect of IVR while identifying hidden forms in Embedded Figure Tasks (EFTs) on the ability to detect a new and unknown anomaly. Through a quasi-experiment with repeated measurements, we compared five research groups, four of whom practiced cognitive intervention while detecting cyber anomalies. The improvement of the results was tested by a pretest and posttest procedure. 120 participants were sampled in a cluster sampling. The participants were 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 Embedded Figure Tasks (EFTs) in an IVR empty 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 high-loaded environment (VRHVL), the higher their speed in detecting novel anomalies.