Cyber Risk Perception among the Israeli Public

By: Yohay Avukay

Supervised by: Dr Daphne Raban

ABSTRACT

Cyberspace and computer systems allows modern society to function properly. Alongside the many opportunities that these systems allow, there are also risks – attackers of various types operating in different ways, with different intensity and different purposes. These attackers can cause damage in both cyberspace and physical space. With the rapid progress of digitalization in our life, it is important that the public will be aware of the cyber risks and know how to defend itself. To this end, this research focuses on understanding cyber risk perception among the public in Israel.

The study examines the perception of risk in two methods. One method is the application of the psychometric paradigm as a risk perception model. This model enables to estimate the intensity of the risks as perceived by the public. The second method is analyzing talkback interactivity in articles about cyber incidents, based on the theory that there is a differences in the level of interactivity between articles about controversial issues and moderate news.

The research questions focus on three areas. The first area is testing the intensity of cyber risks as perceived by the public. The second area is looking for differences between experts and non-experts in the perception of risk. The third area is testing if the level of talkback interactivity will be different in news articles about various types of cyber risks.

The findings indicate that according to the characteristics of risk perception, non-experts perceive the intensity of cyber risks differently from experts and see the risk of economic harm to a civilian (such as stealing money from a bank account, extortion of money by using ransomware taking over the PC, unauthorized credit card activities, etc.) as most intense. In addition, the talkback interactivity analysis showed that in this risk led to the highest level of overall talkbacks and interactive talkbacks.

This research contributes to the several relevant theories. First, I found that the psychometric model, with some adjustments, can be applied to the perception of cyber risks. Second, I found that it is possible to identify differences in cyber risk perception between experts and non-experts. Thirdly, as probably first performed in this field of research, we found that the talkback interactivity analysis can be applied to support the finding of the risk perception, especially in the characteristic of familiarity with risk.