תפיסת סיכוני סייבר בקרב הציבור בישראל

מאת: יוחאי אבוקאי

בהנחיית: פרופסור דפנה רבן

<u>תקציר</u>

מרחב הסייבר מאפשר לחברה המודרנית לתפקד בכך שהוא התווך בו פועלות מערכות המחשב. לצד ההזדמנויות הרבות שמאפשרות מערכות אלו, קיימים גם איומים - יריבים מסוגים שונים הפועלים בשיטות שונות, בעוצמה שונה ולמטרות שונות. יריבים אלו יכולים לממש תקיפות סייבר ולגרום לנזקים הן במרחב הסייבר והן במרחב הפיזי. עם ההתקדמות המהירה של הדיגיטציה וכניסתה לכל תחומי העבודה וחיי היום-יום חשוב שהציבור הרחב יהיה מודע לנושא ויגן על עצמו במידת האפשר. לשם כך, מחקר זה מתמקד בהבנת התפיסות הקיימות בישראל לגבי עוצמת הסיכון מתקיפת סייבר.

המחקר בודק את תפיסת הסיכון בשתי גישות תיאורטיות. הגישה האחת הינה ביישום מאפייני תפיסת הסיכונים של הפרדיגמה הפסיכומטרית. מודל זה מאפשר לבצע דירוג של עוצמת הסיכונים כפי שהם נתפסים בעיני אזרח מן השורה לפי מאפיינים סובייקטיביים שונים. הגישה השניה הינה ניתוח תגובתיות של גולשים לכתבות באתרי חדשות אודות אירועי סייבר תחת התיאוריה כי מרחב טעון מעודד משתמשים, יותר מהמרחב המתון, להתייחס לתכנים ענייניים בכתבה ובטוקבקים ולקיים שיח רלבנטי. הנחה זו עומדת בבסיס מחקר זה אשר יבדוק את השוני בטוקבקים למול סוגים שונים של סיכוני סייבר אשר חלקם טעונים ומשמעותיים יותר מאשר אחרים.

שאלות המחקר מתמקדות בשלושה תחומים. התחום הראשון הינו בדיקת עוצמת סיכוני הסייבר הנתפסת בעיני הציבור, השני הינו בדיקת ההבדלים בין מומחים ולא-מומחים בתפיסת הסיכון והשלישי הינו בדיקת רמת התגובתיות לכתבות אודות אירועי סייבר כמדד לתפיסת נושא הכתבה כטעון או מתון.

ממצאי המחקר מצביעים על כך שעל פי מאפייני תפיסת הסיכון הציבור מעריך באופן שונה ממומחים את עוצמת סיכוני הסייבר ורואה באירועים של פגיעה כלכלית באזרח (כגון גנבת כסף מחשבון בנק, סחיטת כסף באמצעות כופרה המשתלטת על המחשב, פעולות לא מורשית בכרטיס אשראי וכדומה) את הסיכון העוצמתי ביותר. בנוסף לכך, גם בניתוח התגובתיות נמצא ששכיחות הטוקבקים הכללית והאינטראקטיבית נמצאה ברמה גבוהה בכתבות אודות אירועים מסוג של פגיעה כלכלית באזרח. כמו כן, נמצא שחלק ממאפייני תפיסת הסיכון אינם מתאימים לבדוק סיכונים בתחום הסייבר ולפיכך יש לבצע כיוונון וניסוח מחדש עבור מחקר נוסף בתחום זה.

תרומת המחקר להעשרת התיאוריות הרלוונטיות הינה בכמה תחומים. האחת, שניתן ליישם את מודל הפרדיגמה הפסיכומטרית, עם מספר התאמות, לתחום הסייבר. שנית, ניתן לחקור את תפיסת סיכוני הסייבר לפי סוג הנזק הפוטנציאלי וכן לחקור את ההבדל בין מומחים לסייבר ולא-מומחים. שלישית, כפי שכנראה בוצע לראשונה במחקר זה, ניתן להשתמש בניתוח התגובתיות כדי לחזק את מדידת מאפייני הסיכון בדגש על רמת ההכרות של הציבור עם הסיכון.

ולבסוף, מחקר זה הינו כנראה הראשון בישראל בו נערכה מדידה של תפיסת סיכוני הסייבר ומכאן תרומתו בסלילת הדרך למחקרים נוספים אשר יסייעו לתהליך הערכת וניהול סיכוני הסייבר בארגונים וברמה הלאומית.