תפיסת סיכוני סייבר בקרב הציבור בישראל

יוחאי אבוקאי ודפנה רבן[1]

תקציר

עם ההתקדמות המהירה של הדיגיטציה חשוב, שהציבור הרחב יהיה מודע לאיומי הסייבר, ויגן על עצמו במידת האפשר. מחקר זה מתמקד בהבנת התפיסות הקיימות בישראל לגבי עוצמת הסיכון מתקיפת סייבר בשתי גישות תיאורטיות. הגישה האחת הינה ביישום מאפייני תפיסת הסיכונים של הפרדיגמה הפסיכומטרית. הגישה השניה הינה ניתוח תגובתיות של גולשים לכתבות באתרי חדשות אודות אירועי סייבר.

שאלות המחקר מתמקדות בבדיקת: א. עוצמת סיכוני הסייבר הנתפסת בעיני הציבור, ב. הבדלים בין מומחים ולא-מומחים בתפיסת הסיכון, ג. טעינות הסיכון עפ"י רמת התגובתיות לכתבות אודות אירועי סייבר כמדד לתפיסת נושא הכתבה כטעון או מתון.

על פי מאפייני תפיסת הסיכון הציבור מעריך באופן שונה ממומחים את עוצמת סיכוני הסייבר ורואה באירועים של פגיעה כלכלית באזרח את הסיכון העוצמתי ביותר. בנוסף לכך, גם ניתוח התגובתיות מעיד ששכיחות הטוקבקים הכללית והאינטראקטיבית נמצאה ברמה גבוהה בכתבות אודות אירועים מסוג של פגיעה כלכלית באזרח. נמצא שחלק ממאפייני תפיסת הסיכון אינם מתאימים לבדיקת סיכונים בתחום הסייבר.

תרומת המחקר: א. ניתן ליישם את מודל הפרדיגמה הפסיכומטרית, עם מספר התאמות, לתחום הסייבר, ב. ניתן לחקור את תפיסת סיכוני הסייבר לפי סוג הנזק הפוטנציאלי וכן לחקור את ההבדל בין מומחים לסייבר ולא-מומחים, ג. 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.

מבוא

המושג "מרחב הסייבר" מתייחס לסביבה הווירטואלית בה פועלות מערכות המחשבים ו"תקיפת סייבר" הינה פעילותו של תוקף לפגוע או להרוס רשת או מערכת ממוחשבת. במקרים של תקיפת סייבר, יתכנו סוגי נזק שונים אשר חלקם מתממשים בעולם הפיזי וחלקם במרחב הסייבר כגון שיבוש שירותים חיוניים, גנבת מידע פרטי, מחיקת מאגרי מידע ומחשבים, פגיעה ברווחי חברה או בכיסו של האזרח. נזק בלתי מוחשי יכול להתבטא בפגיעה תודעתית שעשויה לפגוע במורל הציבור, באמון בממשל ובמוסדותיו או בתחושת בטחון אישית (Chertoff, 2008).

מחקר זה מתמקד בהערכת פגיעה תודעתית, המיוצגת על ידי התייחסות הציבור הישראלי לסיכוני הסייבר. שתי גישות תיאורטיות מצויות בבסיס המחקר. האחת הינה תפיסת הסיכונים של הפרדיגמה הפסיכומטרית (Lichtenstein, Fischoff & Slovic, 1982). מודל זה מאפשר לבצע דירוג של סיכונים, כפי שהם נתפסים בעיני אזרח מן השורה לפי מאפיינים סובייקטיבים שונים כגון רמת ההכרות עם הסיכון, מידת

[1] החוג לניהול מידע וידע והחוג למנהל עסקים, הפקולטה לניהול, אוניברסיטת חיפה draban@univ.haifa.ac.il

ההיחשפות אליו מרצון ויכולת להימנע ממנו. הגישה השניה מניחה כי מרחב טעון, בהשוואה למרחב מתון, מעודד משתמשים להתייחס לתכנים ענייניים המופיעים בכתבות עיתונות ובטוקבקים. הנחה זו איפשרה לבדוק את השוני בטוקבקים למול סוגים שונים של סיכוני סייבר, אשר חלקם טעונים ומשמעותיים יותר מאשר אחרים (פלמון, 2013).

תרומתו של המחקר הינה בהבנת תפיסת סיכוני הסייבר בקרב הציבור הישראלי, ובשיפור היכולת לאמוד את ההשפעה התודעתית על הציבור. הבנה זו יכולה לקדם את מאמץ ההסברה מול הציבור - גם בכך שיינתן יותר מידע מקצועי אודות הסיכונים, המטרידים אותו ביותר, וגם בכך שיינתנו כלים ושיטות אבטחה להתמודד עם סיכונים אלו. בנוסף, ניתן לבחון חידוד מסרים לציבור לגבי סיכונים, שמומחים מעריכים כעוצמתיים יותר, אך הציבור לא מבין את חומרתם. ולבסוף, ניתן יהיה לחשוב על אוטומציה של ניתוח טוקבקים באתרי חדשות לצורך אבחון מהיר של תגובות הציבור לאיומי סייבר ובהמשך גם לאיומים מסוגים שונים.

רקע תיאורטי

סוגי הסיכונים במרחב הסייבר

מרחב הסייבר מאפשר לחברה המודרנית לתפקד, בכך שהוא התווך בו פועלות מערכות מחשב המנהלות תשתיות חיוניות כגון ייצור חשמל והולכתו לבתים, שליטה בתנועת רכבות וכלי רכב, תקשורת בין בני אדם וקווי יצור במפעלים. בעידן המידע, נוספו תשתיות חדשות, שהן על טהרת המידע – מאגרי מידע הנוגעים לאזרחים, ביצוע רכש ומסחר, ניהול חשבונות הבנק ועוד (טבנסקי, 2011). לצד ההזדמנויות הרבות, שמאפשרות מערכות המחשב והתקשורת המקושרות במרחב זה, קיימים גם איומים.

במרחב הסייבר פועלים יריבים שונים, בשיטות שונות, בעוצמה משתנה ולמטרות שונות. לדוגמא, מדינה תחדור למערכות המחשב של אויביה במטרה לרגל אחריהם, לשבש את פעולת מערכותיהם, ליצור יכולת הרתעה וכן כלוחמה פסיכולוגית, במטרה להשפיע תודעתית על דעת קהל ומקבלי החלטות (אבן וסימן טוב, 2011). ארגון טרור ואף פצחן (האקר) בודד, ביכולותיו הפיזיות המוגבלות לתקוף מדינה, יוכל לנצל את מרחב הסייבר למלחמה א-סימטרית בכך, שהנזק אותו יוכל לממש אינו נמצא ביחס ישר לגודלו. (סיבוני, כהן ורוטברט, 2013). ארגוני פשע ואף פושעים בודדים ינצלו את האפשרות לרווח כספי בכל דרך אפשרית- אם על ידי מכירת מידע, מכירת כלי תקיפה, מתן נגישות למערכות ארגוניות או למחשבים נגועים, דרכם ניתן לממש התקפה על ידי צד שלישי (Filshtinskiy, 2013). ארגונים אידיאולוגיים, כדוגמת אנונימוס, פוגעים במערכות או מפרסמים מידע רגיש של גורמי ממשל וחברות מסחריות, אשר פועלות בניגוד לאמונתם (Deseriis, 2013). ולבסוף, אדם בודד, הפועל בצורה עצמאית – אם ממניעים כלכליים, אידיאולוגיים או פשוט מתוך נקמה במעסיקו (Brenner, 2013). הדוגמאות לעיל ממחישות את המגוון הגדול של אפשרויות תקיפת סייבר ואת הנזקים, הנגרמים במרחב הפיזי ובמרחב הקיברנטי. סוגי התקיפה והיקפי הנזקים מסוכמים בטבלה 1.

עם ההתקדמות המהירה של הדיגיטציה וכניסתה לכל תחומי העבודה וחיי היום-יום חשוב שהציבור הרחב יהיה מודע לנושא סיכוני הסייבר ויגן על עצמו במידת האפשר. לשם כך, מחקר זה מתמקד בהבנת התפיסות הקיימות בישראל לגבי עוצמת הסיכון מתקיפת סייבר, בהתבסס על הפרדיגמה הפסיכומטרית המוסברת בפרק הבא.

טבלה 1: סיכום סוגי הסיכונים בתחום הסייבר

סוג הסיכון	גורמים אפשריים למימוש הסיכון	פירוט פוטנציאל הנזק – על פי אירועי העבר
פגיעה בשירותים לאזרח	1. לוחמת סייבר - תקיפת אויב במלחמה 2. טרור קיברנטי – תקיפת ארגוני טרור	שיבוש או השבתה של שירותים לאזרחים – החל משירותים בסיסיים כגון חשמל ומים וכלה בשירותי מידע מקוונים.
פגיעה כלכלית באזרח	1. גורמי פשע או פושע בודד 2. אזרח אחר - ממניע שנאה, רצון לנקמה וכדומה	1. גנבת כסף באופן ישיר (לדוגמא מחשבון הבנק) 2. תשלום בגין סחיטה (לדוגמא תשלום לתוקף כדי שישחרר את ההצפנה שביצע במחשב)
פגיעה בפרטיות של האזרח	1. גורמי פשע או פושע בודד 2. טרור קיברנטי - תקיפת ארגוני טרור 3. אזרח אחר (ממניע שנאה, רצון לנקמה וכדומה)	1. פרסום מידע אישי שאינו ידוע ברבים אודות לקוחות החברה או אזרחי המדינה. 2. גנבת פרטי הזדהות של אזרח. 3. שימוש לא מורשה בנתוני האזרח.
פגיעה בביטחון המדינה	1. לוחמת סייבר - תקיפת אויב במלחמה 2. טרור קיברנטי - תקיפת ארגוני טרור 3. עובד פנימי	1. גנבת מידע מסווג ביטחוני 2. שיבוש / השבתת מערכות מחשב ביטחוניות
פגיעה ברווחי חברה ובתדמיתה	1. גורמי פשע 2. טרור קיברנטי - תקיפת ארגוני טרור 3. מדינת אויב (בשגרה ובמלחמה) 4. חברה מתחרה 5. עובד פנימי	1. גנבת מידע עסקי רגיש - פטנטים ותוכניות לצרכי תחרות עסקית או פרסומם לצרכי פגיעה תדמיתית. 2. גנבת כסף באמצעות שימוש במערכות המחשב של החברה. 3. ירידה בערך המניות של החברה.
השפעה תודעתית על דעת קהל	1. טרור קיברנטי - תקיפת ארגוני טרור 2. לוחמת סייבר - מדינת אויב 3. ארגונים אידיאולוגיים	1. השפעה במישרין על ידי פרסום מידע שקרי או פוגעני 2. השפעה בעקיפין על ידי מימוש נזקים.

תפיסת סיכון

תפיסת סיכון מתייחסת להערכה של אדם לגבי עוצמת סיכונים מסוגים שונים. בתחילת שנות ה- 80 גובש מודל בשם "הפרדיגמה הפסיכומטרית" במטרה להגיע לייצוג כמותי ומשמעותי של תפיסת הסיכון (Slovic, Lichtenstein, Fischoff & 1982). הפרדיגמה מייצגת שני ממדים: א. רמת המוכרות של הסיכון, הכולל מאפיינים של רמת הידע של הנבדק לגבי הסיכון, הערכה לגבי רמת הידע המדעי הקיים ומידת החשיפה לאיום שלא מרצון; ב. חומרת האיום, הכולל מאפיינים של יכולת השלמה עם הסיכון, חומרת הנזק ועד כמה הוא קטסטרופלי בהיבט של השפעה על הדורות הבאים.

גישה אחרת להערכת הסיכון מבוצעת ע"י הצגת מרכיבי סיכון ובקשה מנבדקים לציין את הדמיון בין זוג גורמי סיכון. טכניקת סילום רב ממדית משמשת לבניית ייצוג מרחב הדמיון. בצורה זו נמצא, לדוגמא, שהתאבדות נשפטה כדומה יותר לפעולות אלימות אחרות (מלחמה, טרור) למרות השוני בפרופיל מאפייני הסיכון (Green & Brown, 1980). עוד מודל הינו Addtree Algorithm (Sattath & Tversky, 1977) ולפיו יוצרים קשרים באורכים שונים בין הסיכונים וכך נוצרת היררכיה של צברי סיכונים. במחקר אשר עשה

שימוש במודל זה נמצאו הצברים הבאים: תאונות, פעולות אלימות, אסונות טכנולוגים ומחלות (1983, Johnson & Tversky). מודל אחר הינו Repertory Grid (Kelley, 1955) אשר יושם במחקר לתפיסת סיכון שבו הוצגו לנבדקים סדרות של 3 גורמי סיכון והנבדקים התבקשו לענות בכל פעם באיזו צורה שני גורמי סיכון דומים זה לזה ושונים מגורם שלישי (Green & Brown, 1980).

ממחקרים אלו עולות מספר תובנות. הראשונה היא, שניתן לכמת ולנבא את כיצד ניתפס הסיכון. השנייה היא, שסיכון מפורש באופן שונה ע"י קבוצות שונות ולבסוף, עולה תופעה אשר הוגדרה כ"אופטימיות נאיבית" כאמונה שאירועים טובים יתרחשו לנבדק ביתר תדירות מאשר אירועים שליליים בהשוואה לאנשים אחרים וזאת בלי קשר להסתברות האובייקטיבית (Lichtenstein et al, 1982).

עד היום, בוצע שימוש בפרדיגמה הפסיכומטרית במחקרים להערכת תפיסת סיכונים מתחומים שונים. במחקרים, אשר בוצעו באוסטרליה (Sargent & Brooks, 2010) ובשבדיה (Sjöberg, 2005), נעשה שימוש בפרדיגמה להשוואה בין סיכוני טרור, פשע וסיכונים אישיים (כגון תאונת דרכים), כאשר המחקר באוסטרליה שימש ככלי לממשל לבדיקת אפקטיביות קמפיין הסברה נגד טרור. במחקר בארה"ב נבדקה תפיסת סיכוני הסייבר בתחום של מסחר מקוון (Gabriel & Nyshadham, 2008), ובוצע מדרוג של סיכונים אישיים שונים כגון גנבת זהות, גנבת כסף וגנבת מידע אישי. במחקר נוסף נחקרה תפיסת סיכוני הטרור לפי פרמטרים שונים כגון מגדר, סבירות התממשות הסיכון באופן כללי וספציפית לנבדק, וההשפעה של כעס וחרדה על מדיניות הממשל לטיפול בטרור (Lerner, Gonzalez, Small & Fischhoff, 2003).

למיטב ידיעתנו, עד היום לא בוצע מחקר שיטתי של תפיסת סיכונים בקרב הציבור לגבי אירועי סייבר אשר התרחשו (Soyer, 2013). מחקר זה בא למלא את הפער, ולבדוק מול סוגים שונים של סיכוני סייבר את תפיסת הסיכון של הציבור בישראל, לפי מאפייני תפיסת הסיכון של הפרדיגמה הפסיכומטרית וכן, כפי שבאה לידי ביטוי באינטראקטיביות בטוקבקים לאירועי סייבר שפורסמו בעיתונות המקוונת.

הפרדיגמה הפסיכומטרית

סיכון הינו אירוע בעל הקשר לנזק אשר עלול לקרות ליחיד, לקבוצה או לאנושות כולה. מכיוון שסיכון אינו מוערך רק במאפיינים כמותיים, אלא גם בהקשרים חברתיים ופסיכולוגיים, סיכון מוערך בצורה שונה על-ידי אנשים שונים (Slovic, 1987). ניתן לבצע חלוקה בין מאפיינים רכים ומאפיינים קשים. מאפיינים קשים הינם עובדות ונתונים לגבי הנזק אשר התממש מהסיכון, כגון מספר הנפגעים ועלות כלכלית של תיקון הנזק. מאפיינים רכים מבוססים על הערכה סובייקטיבית כגון, חלוקה צודקת של הסיכון, השפעה על הדורות הבאים, יכולת שליטה בסיכון, והאם הסיכון נלקח מרצון או בלית ברירה (Covello et al, 1987).

בחירה מרצון – האם אדם בחר מרצונו לקחת את הסיכון כגון, נהיגה ברכב וסיכון של תאונת דרכים, לעומת זיהום אויר ובלית ברירה נשימתו. נמצא, שהעובדה שלאדם אין ברירה אלא לקחת את הסיכון, מעצימה את רמת הסיכון בעיניו גם אם זהו סיכון דומה מבחינת מספר הנפגעים. אדם מוכן יותר לקבל סיכון מרצונו מאשר זה שנכפה עליו – גם אם הוא פי 1000 יותר מסוכן בפועל (Eagly & Chaiken, 1993). לעיתים, סיכון נלקח מרצון מתוך ציפיה לרווח. כמו כן, אדם אשר לקח סיכון, סובר שיוכל לעצור את הסיכון בכל זמן. לפעמים, הסיכון שנלקח הינו האלטרנטיבה הטובה ביותר, בעיני אדם, בהשוואה לחלופות (Eagly & Chaikan, 1993).

שליטה בסיכון – סיכון אשר אדם יכול לשלוט בו נתפס כפחות עוצמתי מסיכונים שהם בשליטתם של אחרים או כלל לא בשליטה. לרוב, אדם יבחר שלא להיכנס למצבים שהם מחוץ לשליטתו בגלל תחושת חוסר הביטחון, חוסר אונים וחוסר היכולת להגן על עצמו. יש להבהיר, כי הכוונה היא לאמונה, שניתן לשלוט בסיכון, ולאו דווקא ליכולת לשלוט בו בפועל. נמצא שסטטיסטית, אנשים מעריכים עוצמת סיכון עבורם, אישית, כנמוכה יותר מאשר עוצמת אותו הסיכון לכלל האוכלוסייה (Sjöberg, 2000). תכונה זו נקראת

אופטימיות נאיבית: אדם נותן אמון רב ביכולותיו האישיות או ביכולות של גורם אחר עליו הוא סומך (כגון רשויות ממשלתיות, כוהן דת, טייס מוסמך) עד כדי הכחשה של הסיכון (Schmidt, 2004).

השפעה מושהית להתממשות הסיכון – הפרש הזמן בין התממשות הסיכון ובין הזמן בו נגרם הנזק בפועל. בגלל ההשהיה, קשה להעריך בפועל את הנזק מהסיכון ולקשרו לאירוע הראשוני בו הסיכון קרה. דוגמאות לכך הן סיכון של סרטן ריאות הנגרם מעישון, סיכון של השפעה שלילית על הסביבה משימוש בגידולים מהונדסים גנטית והחור באוזון הנגרם משימוש בגזי חממה (Schmidt, 2004).

גורם סיכון טבעי לעומת סיכון יציר האדם – הבדל משמעותי בתפיסת הסיכון נמצא בין סיכונים, אשר נגרמו מנסיבות טבעיות לעומת סיכונים אשר נגרמו על ידי האדם, כאשר האחרונים נתפסים כיותר נמוכים וזאת בגלל יכולת האדם לשלוט בסיכון אותו הוא עלול לגרום, אחריותו לנזק וכן בכך, שקיימת היכולת להימנע מהסיכון על ידי התנהגות זהירה או ידע טוב יותר. היבט נוסף הינו כוונות שליליות של הגורם אשר מממש את הסיכון. לדוגמא – אי טיפול בחומרים מסוכנים מסיבות של חיסכון בעלויות המפעל (Schmidt, 2004). גישה הפוכה לכך היא, שדווקא סיכונים טבעיים נתפסים כנמוכים יותר, מכיוון שניתן ליחסם לחוקי הטבע, רצון האל, גורלו של העולם ולא לכוונות זדון של בני האדם (WBGU, 1998).

התרגלות לסיכון ומידת הכרתו – לאורך זמן, אדם מתרגל לקיומו של הסיכון ותופס אותו כבעל עוצמה נמוכה יותר, למרות שאובייקטיבית עוצמת הסיכון לא השתנתה לעומת סיכונים חדשים ולא מוכרים (Slovic et al, 1986). גורם אשר משפיע על ההתרגלות לסיכון הוא מידת הוודאות לגבי החשיפה לסיכון. אם אדם יודע, שהוא חשוף לאורך זמן לסיכון, אז הוא מתרגל אליו ולאורך זמן מעריכו כנמוך יותר.

תפוצת הסיכון והרווח ממנו - אדם מוכן לקבל על עצמו סיכון, שנפוץ בצורה שיוויונית או סיכון שהרווח מלקיחתו מחולק בצורה הוגנת. סיכון פחות מקובל כאשר הסיכון שקבוצה אחת לוקחת וקבוצה אחרת נהנית מרווחיו (Davy, 1996). זהו שיקול חברתי, שאינו קשור לעוצמת הנזק בפועל מהסיכון, אך הוא משפיע על תפיסת הסיכון. דוגמא לחלוקה חברתית של סיכון הינה פיצוי כספי לאוכלוסייה אשר בשטחה מוקמים מתקני טיפול בחומרים מסוכנים.

תהודה תקשורתית – החברה המודרנית מושפעת מאוד מנושאים, המופיעים בערוצי התקשורת השונים – טלוויזיה, עיתונים, רדיו ואתרי חדשות באינטרנט. אם סיכון מדווח בתקשורת, אנשים רבים לפתע הופכים מודעים אליו ומודאגים ממנו. כמו כן, אם הסיכון מופיע בחדשות אז כנראה שהוא אמיתי – לפי ההיגיון שמה שמדווח בתקשורת הוא אמיתי (Schmidt, 2004) ומתוך אמון ביכולתה של התקשורת לבחור את הנושאים הראויים לדיווח. יתרה מזאת, הופעה בתקשורת של גורם מוסמך, אשר מספק מידע חיובי לגבי סיכונים יכול להשפיע על תפיסת הסיכון בצורה שלילית. לדוגמא – אם גורם ממשלתי בכיר מופיע בחדשות ואומר שהמים ראויים לשתייה והאוויר נקי – הוא עלול לגרום לתופעה הפוכה של דאגה וחשד (Covello et al, 1987). ניתן להניח שסיכון אשר מכוסה בתקשורת משפיע על תפיסת הסיכון ומהווה גורם מגביר לעוצמת הסיכון. יחד עם זאת חשוב לציין שהתקשורת מושפעת גם מהציבור, ומכסה נושאים בכלל וסיכונים בפרט אשר מעניינים אותו (WBGU, 1998).

תפיסת סיכון בקרב מומחים לעומת לא-מומחים

מומחים מוגדרים כאנשים מוכשרים ברמה גבוהה בתחום ידע או פעילות מוגדר וספציפי. תפיסת הסיכון שלהם מושפעת בעיקר ממאפיינים קשים והערכותיהם תואמות במידה רבה את הנתונים הסטטיסטיים. לעומת זאת, בקרב לא-מומחים תפיסת הסיכון תושפע גם ואף יותר ממאפיינים רכים (WBGU 1998) וכתוצאה מכך שיפוטיהם עשויים להיות שונים משיפוטי המומחים.

התפיסה הרכה המבוססת על התנסות אישית, הינה דרך מהירה ואינטואיטיבית להערכת סיכונים וקבלת החלטות. לעומתה, התפיסה הקשה מבוססת על תהליכים איטיים ומחושבים של מדידה, ניתוח ועיבוד מידע (Slovic et al. 2004). עם זאת, כאשר מומחה מתבקש לחרוג מעבר לנתונים הזמינים לו ולבצע

הערכה סובייקטיבית, נמצא שגם מומחה מתבסס על אותם מאפיינים כמו לא-מומחה וישנה הסכמה רבה לגבי מאפיינים כגון הידע על הסיכון והשליטה בו (Kahneman et al. 1982, Henrion & Fischhoff 1986). מהסיבה הזו, ישנה חשיבות להערכת המאפיינים הרכים בתפיסת הסיכון, לא פחות ואולי אף יותר מהנתונים היבשים.

בתחום הסייבר, ניתן להגדיר כמומחים בעלי תפקידים בתחום זה או בתחומים משיקים כגון ניהול ופיתוח מערכות מידע, רשתות תקשורת וכדומה. דוגמא לכך ניתן לראות במחקר שנערך בקרב ארגונים שונים ברחבי ארה"ב להשוואת תפיסת הסיכון בין עובדים מומחים ועובדים לא-מומחים (Posey et al. 2014). המחקר מצא הבדל בהערכת המומחים והלא-מומחים לגבי רמת העוצמה והסוגים של הסיכונים המאיימים על הארגון ושל היכולת להתגונן מפניהם. בעוד שהמומחים דירגו את רשלנות העובדים הפנימיים כאיום הגדול ביותר על הארגון (35% מקרב המומחים), קבוצת הלא-מומחים דירגו את ההאקרים כאיום הגדול ביותר (39% מקרב הלא-מומחים). ממצאים אלו מבוססים על הערכה מקצועית של המומחים אשר מבינים שעובד פנימי בעל גישה והרשאות למערכות הפנימיות של החברה מהווה איום פוטנציאלי גדול הרבה יותר מאשר האקר התוקף את החברה מבחוץ. לעומת זאת, עובד לא-מומחה יעריך את ההאקר, כנראה על פי תחושה, כאיום רב יותר (Posey et al. 2014).

תפיסת סיכונים בתחום הסייבר

בתחום הסייבר, כבתחומים אחרים, גדלה ההבנה שיש להעריך את הסיכונים לא רק בשיטות ממדעי המחשב והנדסת האלקטרוניקה הנמצאות בשימוש המומחים, אלא גם בגישות המבוססות על הבנת התפיסה, האמונה, המניעים וההתנהגות של קהל המשתמשים בטכנולוגיות המידע (Choobineh, 2007). מחקרים בתחום זה מציינים שמרבית בסיס הידע לגבי סיכוני הסייבר מבוסס על הערכה של מומחים אשר למעשה מנותקים מהידע של משתמשים "רגילים" הנחשפים לחולשות אבטחה במשימותיהם היומיומיות ותופסים את הסיכונים בתחום זה בצורה שונה (Albrechtsen et al. 2009). תפיסת הסיכון האישית משפיעה על מאמצי הארגון להגן על עצמו ובסופו של דבר על רמת האבטחה בפועל של המידע, רשתות התקשורת ומערכות המחשב (Albrechtsen, 2007). מסיבה זו, ארגונים נדרשים להבין את תפיסת הסיכון של המשתמשים הלא-מומחים על מנת להתאים לכך את המדיניות, שיטות ואמצעי אבטחת המידע ולשפר את האפקטיביות שלהם בארגון (Adams & Blandford, 2005).

העלייה באירועי גניבת זהות וניצול חולשות אנוש מעלות את החשש שהציבור אינו מספיק מודע לסיכוני הסייבר, לשיטות ולאמצעים אותן יוכל ליישם כדי להגן על עצמו (Jackson et al. 2005). משנת 2010 החלו להתבצע מחקרים המודדים את תפיסת סיכוני הסייבר. מחקר בסין (Huang et al. 2010) בדק את תפיסת הסיכון בקרב 602 נבדקים לא-מומחים שמשתמשים ביום-יום במחשבים וטלפונים סלולריים למשימותיהם היומיומיות. לנבדקים הוצגו 21 סוגים שונים של קוד זדוני ואיומים נוספים בתחום הסייבר. המחקר איחד לרשימה אחת של סיכונים את זהות התוקפים (האקרים, ארגוני טרור, מדינות וכדומה), כלי התקיפה (וירוסים, תולעים), בעיות התנהגויות (רשלנות, חוסר מקצועיות) וסוגים של תקיפות (מניעת שירות, האזנה לתעבורת מידע). נמצאו הבדלים מובהקים במאפייני רמת ההכרות עם הסיכונים, רמת העוצמה, חומרת הנזק, סבירות התממשות הסיכון והמודעות לסיכון. ששת הסיכונים אשר קיבלו את הציון המשוקלל הגבוה ביותר הינן נוזקות (תוכנה מזיקה) מסוג דלת אחורית, סוס טרויאני ווירוסים וכן תוקפים מסוג האקרים.

עד כה סקרנו את סוגי הסיכונים בתחום הסייבר, מודלים למדידת תפיסת הסיכון, הבדלים בתפיסה בין מומחים ולא-מומחים ומחקר תפיסת הסיכון בתחום הסייבר. הפרק הבא מתייחס לאינטראקטיביות של גולשים לידיעות המפורסמות בעיתונות המקוונת (אתרי אינטרנט) ולאפשרויות להיעזר במופעים מסוג זה לצורך הערכת תחושת הציבור ביחס לסיכונים.

אינטראקטיביות בטוקבקים בעיתונות מקוונת

מחקרה של פלמון (2013) מפריד בין נושאים טעונים ונושאים שאינם טעונים בכל הנוגע לטוקבקים בעיתונות מקוונת. המחקר הנוכחי הולך צעד אחד קדימה ע"י יישום מדרג לעוצמת סיכון סייבר המתואר בכתבה עיתונאית כסוג של מדרג טעינות.

מאפייני הטוקבקים לכתבות המפורסמות באינטרנט הינם שונים מתגובות למידע המפורסם בערוצי תקשורת אחרים כגון תגובות המפורסמות בעיתון או מאזינים העולים לשידור ברדיו (הכט 2003, אלקין-קורן 2003, Reich 2011). כמות הטוקבקים רבה יותר –עשרות ואף מאות לעומת תגובות בודדות בערוצים אחרים. בעיתונות המקוונת התגובות הן מידיות וספונטניות, התיווך הוא מינימלי בסינון התגובות אשר מפורסמות- לעומת תגובות הנשלחות לדוגמא לעיתון. קיימים מאפייני שפה ייחודיים לכתיבה באינטרנט לעומת ערוצים אחרים. ולבסוף, מנגנון התגובה באתר האינטרנט מאפשר צמידות בין זמן פרסום התגובות וזמן פרסום הכתבה וכן אינטראקטיביות בין התגובות עצמן.

אינטראקטיביות בטוקבקים באה לידי ביטוי בינם לבין הכתבה ובינם לבין עצמם כפי שמוסבר במחקרה של פלמון (2013) על בסיס הנחותיו של רפאלי (1988). לצורך מדידה, גובשו שלושה סוגי מסרים: א. מסר דקלרטיבי אשר אינו מתייחס לכתבה או למסרים אחרים ומהווה הצהרה של הכותב, ב. מסר ריאקטיבי אשר מתייחס לכתבה בפרט או לכותב הכתבה ודעותיו בכלל וג. מסר אינטראקטיבי אשר מתייחס לטוקבק קודם וכולל התייחסות לתכני הכתבה, הכתב או תכני טוקבקים קודמים. מסר יחשב לאינטראקטיבי אם הוא חלק מרצף של שלושה מסרים לפחות: כתבה – מסר ריאקטיבי – מסר אינטראקטיבי. לצורך כך, ניתוח התוכן בטוקבק יאפיין את סוג המסר ולא מיקומו הפיזי/כרונולוגי ברצף המסרים לכתבה. מדד נוסף הינו הצפיפות האינטראקטיבית המחושבת על ידי חלוקת מספר המסרים האינטראקטיביים בסך כל המסרים שהתקבלו לכתבה.

מחקרה של פלמון העלה שהמרחב הטעון הנלווה לכתבות בנושאים הקונפליקטואליים מעודד השתתפות ואינטראקטיביות ברמת שכיחות הטוקבקים (אך לא ברמת הצפיפות האינטראקטיבית) וזאת על בסיס התיאוריה שבמרחב הטעון קיים צורך גדול יותר של הגולשים לייצר אינטראקציה ואינטראקטיביות עם עמיתיהם. במחקר הנוכחי יושמה תיאוריה זו על מנת לבדוק איזה סוג של סיכון סייבר נחשב בעיני הגולשים כטעון יותר או פחות, עפ"י התגובתיות.

השערות המחקר

מטרת מחקר זה הינה לבדוק תפיסת עוצמות שונות של סיכוני סייבר בקרב האוכלוסייה בישראל כפי שהן באות לידי ביטוי בהתאם למאפייני תפיסת הסיכון של הפרדיגמה הפסיכומטרית ובהתייחסות הקהל לפרסומים בתקשורת. עבור כל מאפיין סיכון נבדקו ההבדלים בין סוגי הסיכונים שתוארו בטבלה מספר 1. בנוסף, נבדקו ההבדלים בין קבוצת המומחים והלא-מומחים. טבלה מספר 2 מציגה את ההשערות שנבדקו.

טבלה 2: רשימת ההשערות למאפייני תפיסת הסיכון

מאפיין הסיכון	השערה
רמת ההכרות	H1.1: ככל שהסיכון מוכר יותר, כך הוא ייתפס כפחות עוצמתי
	H1.2: רמת ההכרות של הסיכונים בקרב המומחים תהיה גבוה יותר מזו של הלא-מומחים
אופטימיות נאיבית	H2.1: ככל שהאופטימיות הנאיבית גבוהה יותר, כך הסיכון ייתפס כפחות עוצמתי
	H2.2: רמת האופטימיות הנאיבית בקרב המומחים תהיה נמוכה יותר מזו של הלא-מומחים
נסיבות טבעיות	H3.1: ככל שהסיכון עלול להתרחש מנסיבות טבעיות, כך הסיכון ייתפס כיותר עוצמתי

	H3.2: המומחים יעריכו ברמה נמוכה יותר את התממשות הסיכון בנסיבות טבעיות
היקף החשיפה לסיכון	H4: ככל שהחשיפה לסיכון רבה יותר, כך הסיכון ייתפס כפחות עוצמתי
חופש בחירה	H5: ככל שניתן לבחור בסיכון, כך הסיכון ייתפס כפחות עוצמתי
תועלת מהסיכון	H6: ככל שהתועלת מהסיכון רבה יותר, כך הסיכון ייתפס כפחות עוצמתי
מניעת הסיכון	H7.1: ככל שניתן למנוע את הסיכון, כך הסיכון ייתפס כפחות עוצמתי
	H7.2: המומחים יעריכו ברמה גבוהה יותר מהלא-מומחים את אפשרות מניעת הסיכון

שלוש ההשערות הבאות נוגעות למאפייני אינטראקטיביות העולים מסוגי סיכונים שונים.

H8: שכיחות הטוקבקים לכתבה תעלה עם העליה ברמת העוצמה הנתפסת של הסיכונים

H9: שכיחות הטוקבקים האינטראקטיביים לכתבה תעלה עם העליה ברמת העוצמה הנתפסת של הסיכונים

H10: צפיפות הטוקבקים האינטראקטיביים לכתבה תעלה עם העליה ברמת העוצמה הנתפסת של הסיכונים

משתני המחקר

משתנים בלתי תלויים:

סוג הסיכון המתואר **בשאלון או בכתבה** עפ"י טבלה מספר 1

רמת המומחיות (מומחה/לא-מומחה) בתחום הסייבר

משתנים תלויים:

1. ציון בסולם של 1-4 למאפייני תפיסת עוצמת הסיכון בהתאם לפרדיגמה הפסיכומטרית: רמת ההכרות עם הסיכון, אופטימיות נאיבית, מימוש הסיכון גם בנסיבות טבעיות, היקף החשיפה לסיכון, חופש בחירה בסיכון, תועלת מהסיכון ואפשרות למנוע את הסיכון.
2. שכיחות טוקבקים כללית בכתבה.
3. שכיחות טוקבקים אינטראקטיביים בכתבה.
4. צפיפות האינטראקטיביות – שכיחות הטוקבקים האינטראקטיביים מסך כל המסרים בכתבה.

שיטת המחקר

המחקר נערך בשלושה שלבים. בשלב הראשון קבוצה של מומחים קיבלה כתבות עיתונות ובהן תיאור ארועי סייבר. המומחים סיווגו את הארועים לסוגי סיכון לפי טבלה 1 ודרגו את עוצמת הסיכונים. בשלב השני הועבר שאלון עוצמת סיכוני סייבר בהתאם לפרדיגמה הפסיכומטרית לקבוצת מומחים (אחרים) וכן לקבוצת לא-מומחים. בשלב ג' בוצע ניתוח תוכן כמותי לטוקבקים של כתבות עיתונות.

שלב א'

מדגם: 20 מומחים בתחום הסייבר, בעלי ניסיון מקצועי בתחום אבטחת מידע של לפחות 10 שנים.

שיטת המחקר – שאלון ובו שש ידיעות עיתונות, כאשר בכל עמוד מוצגת תמונת מסך של כתבה מאתר חדשות מקוון לגבי אירוע סייבר. המומחה מתבקש לתייג את סוג הסיכון המדווח בכתבה ובנוסף, כל מומחה מדרג את סוגי הסיכונים השונים לפי רמת עוצמתם בסולם של 1-6.

שלב ב'

מדגם: 30 מומחים בתחום הסייבר (לא אותם נבדקים משלב א') ו- 30 איש (מדגם נוחות) שעיסוקם אינו בתחום הסייבר ואף לא בתחום מערכות המחשב/תקשורת. כל הנבדקים היו מבוגרים בגילאים 30-60 בעלי השכלה גבוהה.

שיטת המחקר – שאלון מקוון הציג את האירועים כאשר עבור כל אירוע ענו הנבדקים על שאלות המבוססות על מאפייני הפרדיגמה הפסיכומטרית, כפי שנבדק במחקר ישראלי (זכאי, 1994). הפניה למשתתפים בוצעה במהלך יום אחד כאשר מיד לאחר הפניה נשלח הקישור לשאלון במייל. השאלון נשאר פתוח למענה במשך 24 שעות. בחלון זמן זה בוצע מעקב אחר אתרי החדשות על מנת לוודא שאין פרסום חריג של אירוע סייבר או אירוע משמעותי אחר (טרור וכדומה) אשר עשוי להשפיע על מענה הנבדקים. כל הנבדקים היו בעלי חשבון Gmail וכך ניתן להגביל את הנבדקים למענה אחד.

שלב ג'

שיטת ניתוח התוכן מבוססת על מחקרה של פלמון (2013) לגבי האינטראקטיביות בטוקבקים וההבדלים בין נושאים טעונים ונושאים מתונים.

מקורות המידע –נאספו 192 כתבות בנושא אירועי סייבר מ- 3 אתרי חדשות מתוך ה- 10 המובילים בישראל לפי סקר TIM אשר בוצע ב- 2013 (84 מ- Ynet, 66 מ- Walla ו- 42 מ- Mako). הכתבות נאספו מהשנים 2013-2016 וכללו 6958 טוקבקים.

אפיון ובחירת הכתבות – הכתבות מתארות אירוע אשר התרחש בישראל או בעולם ורלוונטי לאחד מסוגי הסיכון בתנאי שהנושא העיקרי הינו אירוע סייבר ספציפי. כתבות הכוללות תכנים הקשורים לסייבר אך לא לאירוע ספציפי לא נכללו. לדוגמא: כתבה אודות מבצע צוק איתן בה מוזכר שהיה אירוע סייבר, לצד אירועי טילים, מנהרות וכדומה, סקירה כללית אודות תוקף מסוים כגון ארגון אנונימוס, כתבות המדווחות על מלחמה של תוקף בתוקף שלא משפיעה על האזרח כגון תקיפה של האקרים מוסלמים ע"י האקרים ישראלים וכיו"ב.

שיטת ניתוח הכתבות –בוצע ניתוח לטוקבקים בשיטה ידנית קרי ספירה של מספר הטוקבקים הכולל ומספר הטוקבקים האינטראקטיביים. סה"כ נמצאו 6958 טוקבקים בכתבות השונות. יש לציין שבחלק מהכתבות הופיעו גם טוקבקים המוזנים כעדכונים (post) מפייסבוק וגם הם נספרו. כמו כן, במקרים בודדים אותו טוקבק בדיוק חזר על עצמו שוב - אם בגלל הזנה כפולה בטעות ואם בכוונה. לצורך אחידות, נספרו גם התגובות הכפולות.

בדיקת מהימנות – בוצעה בדיקת מהימנות בין שופטים בכ- 10% מהכתבות (20 מתוך 192). בניתוח הממצאים נמצאה רמת מהימנות גבוהה של Cronbach's Alpha=0.99.

תוצאות

השלב הראשון – חוות דעת מומחים

המרכיב הראשון של השאלון שהועבר למומחים (n=20) בדק את תיוג ששת האירועים לששת סוגי הסיכונים. לפי סולם של 1-6 התקבלו התוצאות המסוכמות בטבלה מספר 3.

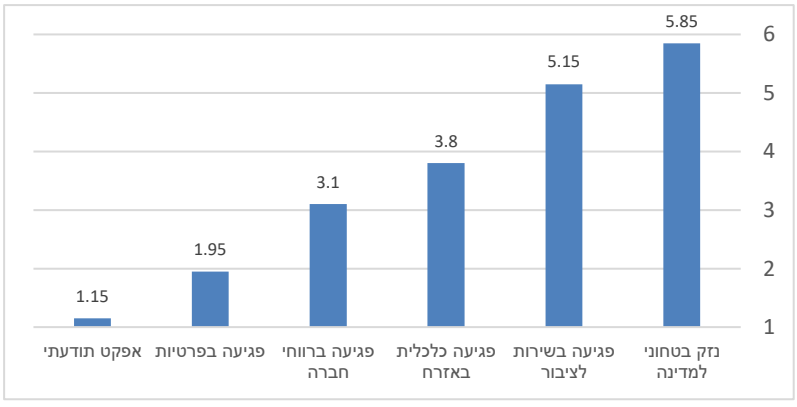
טבלה 3: הערכת רמות הסיכונים של האירועים בקרב מומחים בסולם של 1-6. 1=קשר חלש.

	אפקט תודעתי	נזק בטחוני למדינה	פגיעה כלכלית באזרח	פגיעה בפרטיות	פגיעה ברווחי חברה	פגיעה בשירות לציבור
האקרים שלחו SMS פוגעני	**5.5**	3.4	1.3	3.7	2.2	3.9
פריצה למערכת המחשב של סוללת פטריוט	4.5	**5.9**	2.3	1.1	3.2	3.3
האקרים גנבו כסף מלקוחות בנקים	4.2	1.9	**5.6**	3.6	3.4	3.3
חשיפת פרטי גולשים מאתר אשלי מדיסון	3.7	1.6	3.5	**5.6**	3.5	2.9
גנבת מידע מחברת SONY	4.7	1.6	2.3	3.2	**5.7**	3
פריצה והשבתת מערכות בבית חולים	3.9	2.8	2.5	3.2	3.4	**5.4**

האירועים המשויכים לכל סוג סיכון היוו את הבסיס לאיתור הכתבות בשלב השלישי של המחקר, כך שעבור סיכון של פגיעה תודעתית אותרו כתבות אודות מידע פוגעני אשר פורסם בערוצי תקשורת שונים (SMS, אתרי אינטרנט, רשתות חברתיות וכדומה), עבור נזק בטחוני למדינה אותרו כתבות אודות פריצה למערכות צבאיות וביטחוניות, עבור פגיעה כלכלית באזרח אותרו כתבות של גנבת כסף, עבור פגיעה ברווחי חברה אותרו כתבות של תקיפת מערכות מחשב של חברה, ועבור פגיעה בשירות לציבור אותרו כתבות של שיבוש או השבתת שירותים הניתנים לציבור הרחב.

איור מספר 1 מציג את דירוג עוצמת ששת סיכוני הסייבר בעיני המומחים. מאיור 1 ניתן לראות שהסיכון המוערך כפחות עוצמתי מכולם ע"י מומחים הינו אפקט תודעתי. דירוג זה מהווה מקור להשוואה למול עוצמת הסיכונים בהתאם למאפייני הפרדיגמה הפסיכומטרית שהתקבלה בשלב השני של המחקר.

איור 1: דירוג עוצמת ששת סיכוני הסייבר לפי הערכה ישירה בסולם 1-6



השלב השני – תפיסת הסיכון לפי מאפייני הפרדיגמה הפסיכומטרית

המדגם כלל 30 מומחים בתחום הסייבר ו- 30 לא-מומחים אשר אינם עובדים בתחום הסייבר בפרט ובתחום מערכות מידע/מחשוב בכלל. רמת העניין הממוצעת של המומחים בתחום הסייבר הינה גבוהה (ממוצע 3.76 בסולם 1-4, ס"ת 0.42) ושל הלא-מומחים הינה נמוכה (ממוצע 1.8, ס"ת 0.89). חלוקה מגדרית של המדגם הינה 60% גברים ו- 40% נשים. טווח הגילאים הינו 30 עד 60 כאשר 35% בטווח 30-39, 50% בטווח 40-49 ו- 15% בטווח 50-60.

סטטיסטיקה תיאורית

עבור כל סיכון נבדקו שבעה ממאפייני תפיסת הסיכון בסולם 1-4. סיכום התוצאות מוצג בטבלה מספר 4. הסיכון נתפס כבעל עוצמה נמוכה יותר ככל ש:

רמת ההכרות גבוהה יותר, ככל שניתן למנוע את הסיכון, ככל שהתועלת מלקיחת סיכון גבוהה יותר, ככל שנתפס שיש חופש בחירה רב יותר לקחת את הסיכון, ככל שגורמים רבים יותר חשופים לסיכון , ככל שהסיכון נתפס כנסיבות טבעיות וככל שמאמינים ש"לי זה לא יקרה".

טבלה 4: ממוצע הציון לסוגי הסיכונים השונים בחלוקה למומחים ולא מומחים

		רמת היכרות עם הסיכון	מניעת הסיכון	תועלת מלקיחת סיכון	חופש הבחירה בסיכון	חשיפה שווה לסיכון	נסיבות טבעיות	אופטימיות נאיבית
נזק בטחוני	לא מומחים	1.80	3.30	3.20	1.67	1.80	51.7	2.53
	מומחים	3.27	2.23	3.23	1.27	1.87	1.50	1.37
שיבוש שירותים	לא מומחים	2.03	1.97	3.73	1.43	2.43	2.00	2.33
	מומחים	3.47	2.13	3.57	1.30	2.30	2.80	1.73
פגיעה כלכלית באזרח	לא מומחים	2.27	2.60	2.80	401.	2.83	1.83	2.07
	מומחים	3.63	3.16	2.37	1.37	2.97	1.33	1.50
פגיעה ברווחי חברה	לא מומחים	2.37	3.03	3.57	1.30	2.97	1.83	2.17
	מומחים	3.73	3.10	3.63	1.27	2.93	1.43	1.47
פרטיות	לא מומחים	3.33	1.53	2.30	2.67	2.80	1.73	1.77
	מומחים	3.93	3.53	2.00	3.07	3.10	1.20	751.
אפקט תודעתי	לא מומחים	3.67	2.03	3.47	2.40	3.13	1.87	3.12
	מומחים	3.97	3.70	3.57	2.50	3.47	1.30	1.50

ניתן לראות שרמת ההכרות של המומחים עם הסיכונים היא גבוהה משל הלא-מומחים בכל הסיכונים. בשתי הקבוצות הסיכון המוכר ביותר הינו מסוג של אפקט תודעתי והפחות מוכר הינו מסוג של נזק בטחוני. טווח הנתונים מעיד על רמת המומחיות כאשר אצל המומחים טווח התשובות לרמת ההיכרות נע בין 3.27 ל-3.97 (הפרש 0.7 בסולם ההיכרות מעיד על היכרות גבוהה עם כל סוגי הסיכון). אצל הלא-מומחים טווח התוצאות נע בין 1.80 ל-3.67 (הפרש של 1.87 בסולם ההיכרות).

בקרב מומחים נתפס הסיכון של אפקט תודעתי כאפשרי ביותר למניעה והסיכון בעל הסיכוי הנמוך ביותר למניעה הינו שיבוש שירותים. לעומתם, הלא-מומחים העריכו שהסיכון האפשרי ביותר למניעה הינו נזק בטחוני והסיכון בעל הסיכוי הנמוך ביותר למניעה הינו פגיעה בפרטיות.

בקרב מומחים הסיכון בעל התועלת הגבוהה ביותר הינו פגיעה ברווחי חברה והתועלת הנמוכה ביותר הינו סיכון מסוג פגיעה בפרטיות. בקרב הלא-מומחים הסיכון בעל התועלת הגבוהה ביותר הינו שיבוש שירותים והסיכון בעל התועלת הנמוכה ביותר, בדומה למומחים, הינו פגיעה בפרטיות.

בסיכון מסוג פרטיות נמצא חופש הבחירה הרב ביותר בשתי הקבוצות. הסיכון עם חופש הבחירה הנמוך ביותר בקרב מומחים הינו נזק בטחוני ופגיעה ברווחי חברה ואילו לא-מומחים דרגו פגיעה ברווחי חברה כסיכון עם חופש בחירה נמוך.

בקרב שתי הקבוצות הסיכון, שנתפס כבעל החשיפה השווה ביותר, הינו אפקט תודעתי, ואילו הסיכון, שנתפס כבעל החשיפה הפחות שווה הינו נזק בטחוני. שתי הקבוצות תפסו שיבוש שירותים כסיכון גבוה למימוש בנסיבות טבעיות, ואת פגיעה פרטיות כסיכון בעל הציון הנמוך.

הציונים, בקרב מומחים, עבור כל הסיכונים, הינם נמוכים יותר מאשר הלא-מומחים במשתנה אופטימיות נאיבית. בקרב המומחים הסיכון בעל הציון הגבוה ביותר הינו פגיעה בפרטיות, והסיכון בעל הציון הנמוך ביותר הינו נזק בטחוני. בקרב לא-מומחים הסיכון שקיבל את הציון הגבוה ביותר הינו מסוג אפקט תודעתי, והסיכון שקיבל את הציון הנמוך ביותר הינו מסוג פגיעה בפרטיות.

בדיקת השערות

בכל המשתנים לא נמצאה התפלגות נורמלית. לפיכך, בוצעו מבחנים א-פרמטריים:

עבור כל ההשערות המתוארות בטבלה מספר 2 בוצע מבחן Kruskal-Wallis לבדיקת מובהקות להבדל בתפיסת סוגי הסיכונים. לצורך בדיקת הבדל בתפיסה בין קבוצת המומחים (n=30) והלא- מומחים (n=30) בוצע מבחן t למדגמים בלתי-תלויים, ולצורך ניתוח המשך לבדיקת מובהקות ההבדלים בין הסיכונים השונים, בוצע מבחן Wilcoxon.

סיכום בחינת השערות

בפרק זה נחקרו שבעה מאפיינים של תפיסת הסיכון בשתי קבוצות – מומחים ולא-מומחים. בכל מאפיין נבדקו ההבדלים בתפיסה למול שישה סוגים של סיכוני סייבר. בנוסף, נבדקו ההבדלים בין קבוצת המומחים והלא-מומחים במאפיינים בהם צפוי היה הבדל מובהק עקב יתרונם של המומחים לאור היכרותם עם תחום הסייבר. טבלה 5 מרכזת את מימצאי בחינת ההשערות.

טבלה 5: ריכוז ממצאי ההשערות לשלב השני

מאפיין הסיכון	השערה	ממצאים
רמת ההכרות	H1.1: ככל שהסיכון מוכר יותר, כך הוא ייתפס כפחות עוצמתי	ההשערה **אוששה** בקרב המומחים והלא-מומחים הסיכון העוצמתי ביותר - נזק בטחוני הסיכון הפחות העוצמתי - אפקט תודעתי
	H1.2: רמת ההכרות של הסיכונים בקרב המומחים תהיה גבוה יותר מזו של הלא-מומחים	ההשערה **אוששה**
אופטימיות נאיבית	H2.1: ככל שהאופטימיות הנאיבית גבוהה יותר, כך הסיכון ייתפס כפחות עוצמתי	ההשערה **לא אוששה** בקרב המומחים. ההשערה **אוששה** בקרב הלא-מומחים: הסיכון העוצמתי ביותר – פגיעה בפרטיות הסיכון הפחות העוצמתי –אפקט תודעתי
	H2.2: רמת האופטימיות הנאיבית בקרב המומחים תהיה נמוכה יותר מזו של הלא-מומחים	ההשערה **אוששה**
נסיבות טבעיות	H3.1: ככל שהסיכון עלול להתרחש מנסיבות טבעיות, כך הסיכון ייתפס כיותר עוצמתי	ההשערה **אוששה** בקרב המומחים: הסיכון העוצמתי ביותר – שיבוש שירותים הסיכון הפחות העוצמתי – פגיעה בפרטיות ההשערה **לא אוששה** בקרב הלא-מומחים.

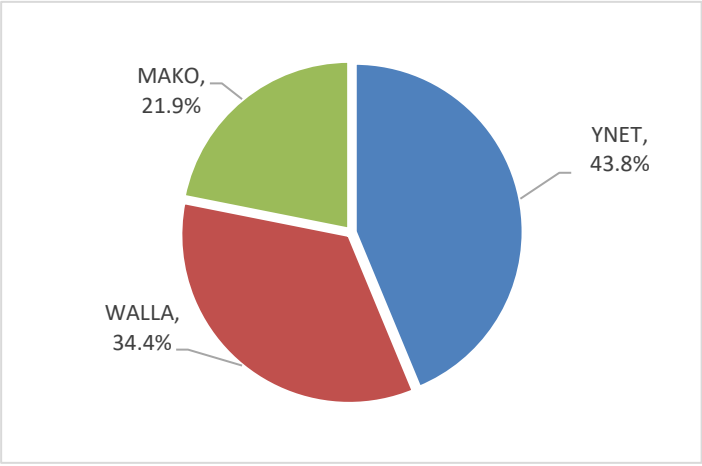
	H3.2: המומחים יעריכו ברמה נמוכה יותר את התממשות הסיכון בנסיבות טבעיות	ההשערה **אוששה** (למעט עבור הסיכון של שיבוש שירותים)
היקף החשיפה לסיכון	H4: ככל שהחשיפה לסיכון רבה יותר, כך הסיכון ייתפס כפחות עוצמתי	ההשערה **אוששה** בקרב המומחים והלא-מומחים הסיכון העוצמתי ביותר - נזק בטחוני הסיכון הפחות העוצמתי - אפקט תודעתי, פגיעה בפרטיות
חופש בחירה	H5: ככל שניתן לבחור בסיכון, כך הסיכון ייתפס כפחות עוצמתי	ההשערה **אוששה** בקרב המומחים והלא-מומחים הסיכון העוצמתי ביותר - נזק בטחוני, פגיעה ברווחי חברה הסיכון הפחות העוצמתי – פגיעה בפרטיות
תועלת מהסיכון	H6: ככל שהתועלת מהסיכון רבה יותר, כך הסיכון ייתפס כפחות עוצמתי	ההשערה **אוששה** בקרב המומחים והלא-מומחים הסיכון העוצמתי ביותר – פגיעה בפרטיות הסיכון הפחות העוצמתי – שיבוש שירותים, פגיעה ברווחי חברה
מניעת הסיכון	H7.1: ככל שניתן למנוע את הסיכון, כך הסיכון ייתפס כפחות עוצמתי	ההשערה **אוששה** בקרב המומחים והלא-מומחים הסיכון העוצמתי ביותר – שיבוש שירותים, פגיעה בפרטיות הסיכון הפחות העוצמתי – אפקט תודעתי, נזק בטחוני
	H7.2: המומחים יעריכו ברמה גבוהה יותר מהלא-מומחים את אפשרות מניעת הסיכון	ההשערה **אוששה** (למעט עבור הסיכון של נזק בטחוני)

ממצאי השלב השלישי – ניתוח אינטראקטיביות בכתבות

תיאור המדגם

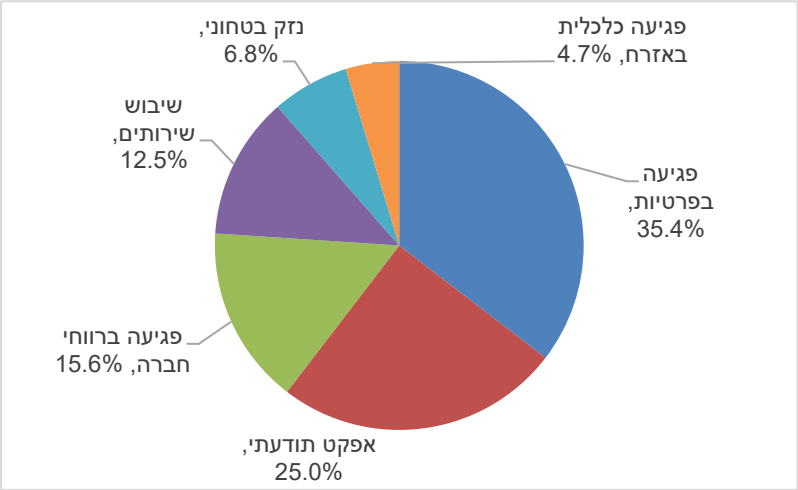
המדגם כלל את כל הכתבות (n=192) המתארות אירועי סייבר בשנים 2013-2016 מאתרי החדשות YNET, WALLA, ו- MAKO בהתאם לחלוקה המתוארת באיור מספר 2:

איור 2: שכיחות הכתבות אשר נבדקו בחלוקה לאתרי החדשות השונים



נמצא שוני במספר הכתבות אודות כל סוג סיכון - בהתאם לחלוקה המוצגת באיור 3.

איור 3: שכיחות הכתבות בחלוקה לסוגי הסיכונים השונים



מספר הכתבות הרב ביותר נמצא עבור אירועים, המתויגים כפגיעה בפרטיות (68), ומספר הכתבות הנמוך ביותר נמצא עבור אירועים, המתויגים כפגיעה כלכלית באזרח (9).

סטטיסטיקה תיאורית

טבלה 6 מסכמת את נתוני כלל הטוקבקים בחלוקה לסוגי הסיכונים.

טבלה 6: סטטיסטיקה תיאורית למספר הטוקבקים בכתבות לפי סוגי הסיכונים

	n	ממוצע	חציון	מינימום	מקסימום	סטיית תקן
פגיעה בפרטיות	68	32.38	12.5	0	339	59.68
אפקט תודעתי	48	27.3	14.5	0	183	35.38
פגיעה ברווחי חברה	30	22.03	8.5	1	91	28.2
שיבוש שירותים	24	28	21.5	0	93	28.75
נזק בטחוני	13	97.6	41	8	382	111.77
פגיעה כלכלית באזרח	9	93.66	27	3	470	159.53

ממוצע הטוקבקים הגבוה ביותר נמצא בכתבות מסוג נזק בטחוני. ממוצע הטוקבקים הנמוך ביותר היה בכתבות מסוג פגיעה ברווחי חברה. טבלה 7 מסכמת את נתוני הטוקבקים האינטראקטיביים בחלוקה לסוגי הסיכונים.

טבלה 7: סטטיסטיקה תיאורית למספר הטוקבקים האינטראקטיביים בכתבות לפי סוגי הסיכונים

	n	ממוצע	חציון	מינימום	מקסימום	סטיית תקן
פגיעה בפרטיות	68	9.6	3	0	87	17.33
אפקט תודעתי	48	6.16	2.5	0	63	9.11
פגיעה ברווחי חברה	30	6.4	1	0	38	10.1
שיבוש שירותים	24	8.66	4	0	53	12.71
נזק בטחוני	13	23.23	14	1	72	23.54
פגיעה כלכלית באזרח	9	33	7	0	184	61.22

ממוצע הטוקבקים האינטראקטיביים הגבוה ביותר נמצא בכתבות מסוג פגיעה כלכלית באזרח והנמוך ביותר נמצא בכתבות מסוג פגיעה ברווחי חברה. טבלה 8 מתארת את ניתוח צפיפות הטוקבקים האינטראקטיביים בחלוקה לסוגי הסיכונים.

טבלה 8: סטטיסטיקה תיאורית לצפיפות האינטראקציה בכתבות לפי סוגי הסיכונים

	n	ממוצע (%)	חציון (%)	מינימום	מקסימום (%)	סטיית תקן
פגיעה בפרטיות	68	22.39	21.11	0	70	20.16
אפקט תודעתי	48	19.26	14.29	0	100	19.9
פגיעה ברווחי חברה	30	17.29	8.89	0	62.35	19.17
שיבוש שירותים	24	23.29	17.71	0	100	24
נזק בטחוני	13	24.58	26.63	8.33	38.24	9.7
פגיעה כלכלית באזרח	9	26.95	30.99	0	42.86	13.9

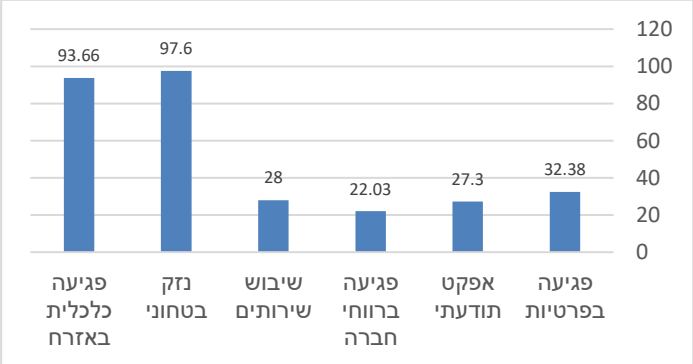
ממוצע הצפיפות הגבוה ביותר נמצא בכתבות מסוג פגיעה כלכלית באזרח והנמוך ביותר נמצא בכתבות מסוג פגיעה ברווחי חברה.

בדיקת השערות

H8: שכיחות הטוקבקים לכתבה תעלה עם העליה ברמת העוצמה הנתפסת של הסיכונים

ההשערה מניחה שיהיה הבדל בשכיחות הטוקבקים בין הכתבות אודות סוגי הסיכונים השונים, כאשר שכיחות טוקבקים הינו מאפיין, המצביע על נושא טעון/סוער יותר מנושאים אחרים. ממוצע שכיחות הטוקבקים בכתבה מתואר באיור מספר 4:

איור 4: ממוצע שכיחות הטוקבקים בכתבה בחלוקה לסוגי הסיכון השונים

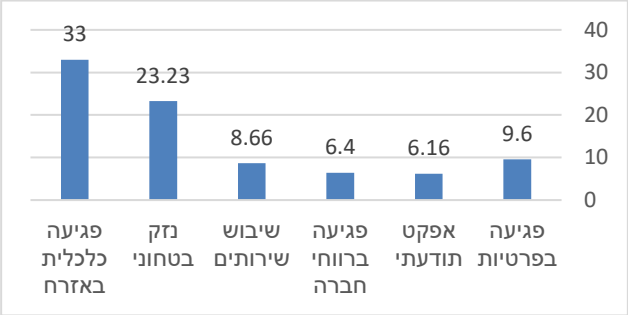


במבחן Kruskal-Wallis נמצא הבדל מובהק בין הכתבות בממוצע שכיחות טוקבקים בכתבה עם סוגי הסיכונים השונים ($p < .05$). בניתוח המשך בוצע מבחן Bonferroni (ההתפלגות של כל סיכון במשתנה זה נמצאה נורמלית) ונמצאו הבדלים מובהקים ($p < .05$) בין זוגות סיכונים. השערה H8 אוששה בכך שנמצא הבדל מובהק בין סוגי הסיכונים השונים ונמצא ממוצע שכיחות טוקבקים גבוה בכתבות אודות סיכון בעוצמה גבוהה מסוג נזק בטחוני ופגיעה כלכלית באזרח. כמו כן, נמצא ממוצע שכיחות טוקבקים נמוך בכתבות אודות סיכון בעוצמה נמוכה מסוג אפקט תודעתי ופגיעה בפרטיות.

H9: שכיחות הטוקבקים האינטראקטיביים לכתבה תעלה עם העליה ברמת העוצמה הנתפסת של הסיכונים

ההשערה מניחה שיהיה הבדל בשכיחות הטוקבקים האינטראקטיביים בין הכתבות אודות סוגי הסיכונים השונים, כאשר שכיחות טוקבקים האינטראקטיביים הינו מאפיין המצביע על נושא טעון/סוער יותר מנושאים אחרים. ממוצע הטוקבקים האינטראקטיביים מוצג באיור 5.

איור 5: ממוצע שכיחות טוקבקים אינטראקטיביים בכתבה בחלוקה לסוגי הסיכון השונים



במבחן Kruskal-Wallis נמצא הבדל מובהק בממוצע שכיחות טוקבקים אינטראקטיביים בכתבה בין הכתבות עם סוגי הסיכונים השונים ($p < .05$).

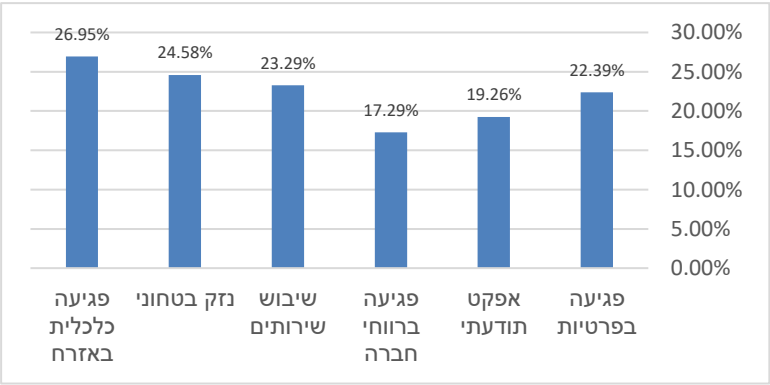
בניתוח המשך בוצע מבחן Bonferroni (ההתפלגות של כל סיכון במשתנה זה נמצאה נורמלית) ונמצאו הבדלים מובהקים ($p < .05$) בין זוגות סיכונים.

השערה H9 אוששה באופן חלקי מכיוון שנמצא הבדל מובהק רק בין סיכון פגיעה כלכלית באזרח, בו נמצא הממוצע הגבוה ביותר, ובין שאר הסיכונים.

H10: צפיפות הטוקבקים האינטראקטיביים לכתבה תעלה עם העליה ברמת העוצמה הנתפסת של הסיכונים

ההשערה מניחה שיהיה הבדל בצפיפות הטוקבקים האינטראקטיביים בין הכתבות אודות סוגי הסיכונים השונים, כאשר צפיפות טוקבקים האינטראקטיביים הינו מאפיין המצביע על נושא טעון/סוער יותר מנושאים אחרים. ממוצע צפיפות הטוקבקים האינטראקטיביים בכתבות מתחלק באופן הבא:

איור 6: ממוצע צפיפות טוקבקים אינטראקטיביים בכתבה בחלוקה לסוגי הסיכון השונים



במבחן Kruskal-Wallis נמצא שאין הבדל מובהק בין הכתבות עם סוגי הסיכונים השונים לגבי המשתנה של צפיפות טוקבקים אינטראקטיביים.

דיון

המחקר בדק כיצד נתפסים סיכוני סייבר בקרב הציבור בישראל. לצורך כך נאספו ממצאים בשני צירי מחקר: הציר הראשון הינו שאלון המבוסס על מאפייני תפיסת הסיכון לפי הפרדיגמה הפסיכומטרית (Slovic, 1987). השאלון שימש גם לבדיקת ההבדלים בתפיסת הסיכון בין מומחים ולא-מומחים. ציר המחקר השני הינו ניתוח כמותי של מדדי האינטראקטיביות בכתבות אודות אירועי סייבר אשר התרחשו בשנים 2013-2016. שני צירי מחקר אלו אינם מנותקים אחד מהשני. ההנחה בבסיס מחקר זה היא שהכתבות המפורסמות באתרי החדשות מעלות את מודעות הציבור לאירועי הסייבר ומשפיעות על מאפייני תפיסת הסיכון ברמת ההכרות עם סיכונים אלו, אפשרויות המניעה, סוגי תוקפים (האקרים, מדינות וכדומה) ותחושת האופטימיות הנאיבית באם הסיכון יקרה לי אישית.

בשלב הראשון של המחקר, כשלב מקדים, הועבר שאלון שמטרתו לקבל חוות דעת מומחים בתיוג אירוע ספציפי המופיע בכתבה לסוג סיכון כפי שאופיין ברקע התיאורטי. כמו כן, קבלת חוות דעת בשאלה ישירה לגבי עוצמת הסיכונים השונים ודירוגם בסולם של 1 -6. לצורך הדיון, יבוצע מדרג של שלוש רמות סיכון – גבוה, בינוני ונמוך, כמפורט בעמודה השמאלית של טבלה 9:

טבלה 9: תיוג אירועים לסיכונים ורמת עוצמתם

אירוע ספציפי	תיוג לסוג סיכון	עוצמת הסיכון	רמת סיכון קטגורית
פריצה למערכות שליטה בסוללת טילי פטריוט	נזק בטחוני	6	סיכון גבוה
השבתת מערכות בית חולים	פגיעה בשירות לציבור	5	
פריצה לחשבונות בנק	פגיעה כלכלית באזרח	4	סיכון בינוני
פריצה וגנבת מידע מחברת SONY	פגיעה ברווחי חברה	3	
חשיפת פרטי גולשים באתר אינטרנט	פגיעה בפרטיות	2	סיכון נמוך
שליחת SMS פוגעני	אפקט תודעתי	1	

תיוג האירועים לסיכונים וקביעת עוצמת הסיכון ע"י המומחים בוצע ככל הנראה לפי מאפיינים "קשים" (Slovic et al. 2004) המבוססים על ניסיונם והכשרתם המקצועית, ולא על בסיס תחושות בטן.

דיון במאפייני תפיסת הסיכון

כללי

ישום מודל הפרדיגמה הפסיכומטרית לתחום סיכוני הסייבר הינו יחסית חדש, ולכן ישנו אתגר בהסבת המאפיינים להיגדים רלוונטיים לתחום הסייבר וכן בחיזוי תגובות מומחים ולא-מומחים. מחקר זה מהווה המשך למחקרים קודמים אשר שימוש במודל זה בתחום סיכונים אחר כגון נפילת טילים על ישראל (זכאי, 1994) וכן מחקרים מועטים שעשו שימוש במודל בתחום הסייבר (Huang et al. 2010). האחרון, הגדיר את סיכוני הסייבר כ- 21 סוגים שונים של נוזקות (וירוסים, תולעים, סוסים טרויאנים וכדומה), שיטות תקיפה (האזנה לתעבורת תקשורת, הנדסה חברתית, דיוג וכדומה) ואחרים (תקלות אנוש, נזקי טבע וכדומה). המחקר הנוכחי בדק את הסיכון מזווית אחרת - של הנזק הסופי של התקיפה, ולא של האופן בו היא בוצעה. הסיבה העיקרית היא שכך ניתן להתמקד במגוון המצומצם של הנזקים הסופיים – 6 סוגים כפי שהוגדר במחקר זה, לעומת המגוון הרחב מאוד של שיטות ואמצעי התקיפה. בנוסף, התמקדות בנזק ולא בשיטת התקיפה מאפשר שפה משותפת וחיבור עם הכתבות בנושא אירועי סייבר אשר אינן מפרטות את שיטת התקיפה (ולעיתים אף לא את סוג התוקף) אלא את הנזק הסופי.

דיון בהשערות למאפייני הסיכון

עבור כל מאפיין של הפרדיגמה הפסיכומטרית נוסחה השערה לגבי ההשפעה של המאפיין על רמת עוצמת הסיכונים השונים. עבור 4 מאפיינים מתוך 7, נוסחו גם השערות הנוגעות להבדל צפוי בין קבוצת מומחים

ולא מומחים, כאשר ההנחה בבסיס מחקר זה היא שבמאפיינים בהם למומחים קיים ידע רב בהרבה מזה של לא-מומחים יהיה הבדל מובהק בממצאים. לעומת זאת, במאפיינים בהם למומחים אין ידע רב לא צפוי הבדל מובהק והם יעברו להערכה סובייקטיבית המבוססת על המאפיינים ה"רכים" על פיהם לא-מומחים פועלים (Kahneman et al. 1982, Henrion & Fischhoff 1986).

במאפיינים של רמת הכרות, היקף החשיפה לסיכון ואפשרות מניעת הסיכון נמצאו הבדלים מובהקים בין הסיכונים השונים הן בקבוצת המומחים והן בקבוצת הלא-מומחים. הסיכונים שהוערכו ברמת עוצמה גבוהה הינם נזק בטחוני ושיבוש שירותים והסיכונים שהוערכו ברמת עוצמה נמוכה הינם פגיעה בפרטיות ואפקט תודעתי. הבדלים אלו מאפשרים להסיק שמאפיינים אלו רלוונטיים לתחום סיכוני הסייבר.

במאפיין של תועלת מהסיכון נמצאו הבדלים מובהקים כך שהסיכונים שדורגו ברמת עוצמה גבוהה הינם פגיעה בפרטיות ופגיעה כלכלית באזרח. זהו דירוג הפוך לזה שהתקבל בחוות דעת המומחים בשלב הראשון של המחקר. הסיבה לכך יכולה להיות ההבנה שעבור גורמים עסקיים, בטחונים וממשלתיים התועלת להשתמש במערכות מחשוב היא גבוהה ותידרש למרות הסיכון. לעומת זאת, עבור אדם פרטי, התועלת להשתמש בשירותי מחשוב אינה גוברת על הנזק הפוטנציאלי של פגיעה בפרטיותו או גנבת כסף מכיסו. יתכן, ששימוש במאפיין זה הינו רלוונטי במיקוד לסיכונים בהם אכן יש בחירה לאדם הפרטי כגון שימוש ברשתות חברתיות, פורומים, קניה מקוונת, שירותי ממשל זמין, שירותי ענן ושאר השירותים בהם אדם יכול לבחור אם להשתמש תוך הבנה שבכך הוא נחשף לסיכון שפרטיו יגנבו.

במאפיין של אופטימיות נאיבית נמצאו הבדלים מובהקים רק בקרב קבוצת הלא-מומחים. יתכן שעבור מומחים מאפיין זה אינו רלוונטי מכיוון שהערכתם וניסיונם המקצועי גובר על האופטימיות שאינה מבוססת על עובדות. כמו כן, יתכן שהמאפיין של האופטימיות הנאיבית אינו מספיק מדויק לתחום סיכוני הסייבר ונדרש מאפיין הנוגע לרמת הקרבה של האזרח אל הנזק הסופי. כלומר, ככל שהנזק יותר יקרה לאדם באופן אישי כך הוא ייתפס כיותר עוצמתי. השערה מתוקנת זו יכולה להתאים לממצאים בהם עוצמת הנזקים המתרחשים לצבא, בית חולים וחברה עסקית מדורגים נתפסת כנמוכה יותר מעוצמת נזקים הנוגעים לפגיעה כלכלית באדם או חשיפת מידע פרטי שלו.

במאפיין של נסיבות טבעיות נמצאו הבדלים מובהקים רק בקרב קבוצת המומחים. יתכן שמאפיין זה דורש ידע מקדים והערכה מקצועית שאינה מספקת אצל לא-מומחים ולכן יתכן שמאפיין זה פחות רלוונטי עבור לא-מומחים לתחום סיכוני הסייבר. מעצם היותם מומחים, ניתן היה לשער שרמת היכרותם עם הסיכונים השונים תאפשר להם להעריך טוב יותר את הסיכוי שאלו יתממשו בנסיבות טבעיות. באירועים אשר הוצגו בשאלון התממש נזק המחייב התערבות של אדם – אם זה בגנבת מידע, העברת כספים או שינוי תכנים. רק באירוע של שיבוש שירותים נגרם נזק של השבתת מערכת מחשב – וזהו נזק שגם יכול להתממש בנסיבות טבעיות. הממצאים תומכים בכך – בכל הסיכונים מומחים העריכו ברמה נמוכה יותר מלא-מומחים את הסבירות שהסיכון יתממש בנסיבות טבעיות, למעט האירוע של שיבוש שירותים. בניתוח המשך נראה כי נמצאו הבדלים מובהקים רק בין שיבוש שירותים והסיכונים האחרים. ממצאים אלו מובילים למסקנה שמאפיין זה פחות רלוונטי להערכת הסיכונים בתחום הסייבר ובמידה ומיישמים אותו נדרש להציג אירועים אשר כולם עשויים להתממש מנסיבות טבעיות.

במאפיין של חופש בחירה בשתי הקבוצות סיכוני נזק בטחוני, שיבוש שירותים, פגיעה כלכלית באזרח ופגיעה ברווחי חברה דורגו בעוצמה גבוהה ללא הבדל מובהק ביניהם. הסיכונים פגיעה בפרטיות ואפקט תודעתי דורגו בעוצמה נמוכה ללא הבדל מובהק ביניהם. ממצאים אלו מביאים למסקנה שמאפיין זה נדרש להתאמה לצורך יישומו לתחום סיכוני הסייבר. גם מומחים וגם לא-מומחים מעריכים שישנה בחירה רבה יותר לשימוש פרטי במחשב ובאתרי אינטרנט לעומת חוסר בחירה של חברה עסקית, צבא או ממשל להשתמש במערכות מידע. יתכן, שבדומה למאפיין התועלת מהסיכון השימוש במאפיין זה הינו רלוונטי במיקוד לסיכונים בהם אכן יש בחירה לאדם הפרטי כגון שימוש ברשתות חברתיות, פורומים, קניה

מקוונת, שירותי ממשל זמין, שירותי ענן ושאר השירותים בהם אדם יכול לבחור אם להשתמש תוך הבנה שבכך הוא נחשף לסיכון שפרטיו יגנבו.

לסיכום, המאפיינים של רמת היכרות ותועלת מסיכון מתאימים לזיהוי סיכוני סייבר ואבחנה בין הציבור הרחב לבין מומחים. המאפיינים של נאיביות אופטימית וחופש בחירה אינם מסייעים לזיהוי סיכוני סייבר ואילו את המאפיין של חופש בחירה יש לחקור עוד ולהתאים לסביבת הסייבר.

דיון בהשערות לניתוח הכתבות

בשלב השלישי של המחקר נבדקה התגובתיות של הציבור לאירועים שונים בתחום הסייבר כפי שהתפרסמו בעיתונות המקוונת (Mako ,Walla ,Ynet) בשנים 2013 – 2016. שלב זה מבוסס על מחקרים קודמים אשר קבעו שאינטראקטיביות בכתבות אודות נושאים טעונים הינה גבוהה יותר מהאינטראקטיביות בכתבות אודות נושאים יומיומיים (פלמון, 2013). ההנחה בבסיס מחקר זה הינה שסיכוני סייבר בעלי עוצמה גבוהה מהווים, מבחינת הגולשים, נושאים טעונים יותר מסיכוני סייבר בעלי עוצמה נמוכה ולכן מדדי האינטראקטיביות לגביהם יהיו גבוהים יותר.

עבור ההשערה שממוצע שכיחות הטוקבקים לכתבה תהיה גבוהה יותר בכתבות אודות סיכונים ברמת עוצמה גבוהה נמצא שהגולשים תופסים בסיכוני הנזק הביטחוני והפגיעה הכלכלית באזרח כסיכונים בעלי עוצמה גבוהה לעומת שאר הסיכונים. הסיכון נזק בטחוני הינו סיכון שדורג כבעל עוצמה גבוהה גם על ידי המומחים בשלב הראשון וגם בשלב השני (בשישה מתוך שבעת מאפייני הסיכון). סיכון הפגיעה הכלכלית באזרח דורג על ידי המומחים בשלב הראשון כבעל עוצמה בינונית. בשלב השני, דירגו אותו קבוצת המומחים ב-6 מתוך 7 המאפיינים ברמת עוצמה בינונית. מסקנה שניתן להסיק משלושת שלבי המחקר הינה ששני סיכונים אלו נתפסים כבעלי עוצמה בינונית עד גבוהה – הן על ידי מומחים והן על ידי לא-מומחים וקהל הגולשים (לגביו לא ניתן להסיק את רמת המומחיות).

עבור ההשערה שממוצע שכיחות הטוקבקים האינטראקטיביים לכתבה תהיה גבוהה יותר בכתבות אודות סיכונים ברמת עוצמה גבוהה נמצא הבדל מובהק רק בין הסיכון של פגיעה כלכלית באזרח ובין שאר הסיכונים. ממצא זה מעיד על כך שמבחינת הגולשים זהו נושא טעון יותר לעומת נושאים אחרים. ניתן להסביר ממצאים אלו בכך שסיכון הפגיעה הכלכלית באזרח מגלם נזק כלכלי אישי לאדם פרטי ולא לחברה או ממשל ולכן הגולשים יגיבו יותר לכתבה בכלל, ויגיבו יותר אחד לשני בפרט בבקשה למידע כיצד האירוע משפיע עליהם באופן אישי, כיצד ניתן למנוע זאת, האם יש יותר מידע לגבי זהות הנפגעים מאותו אירוע וכן בתשובות לשאלות אלו ופרשנות לגבי חומרת האירוע והתוקפים. מספר הכתבות המצומצם (4.7% אודות סיכון זה מתוך כלל הכתבות) מעיד על כך שזהו סיכון עם חשיפה מצומצמת לציבור, באופן יחסי לסיכונים אחרים. ולכן כאשר כבר מתפרסמת כתבה אודות סיכון זה כנראה שישנה תגובתיות רבה יותר בבקשות למידע, שאלות, תשובות ותגובות נוספות. חיזוק לכך ניתן למצוא במאפיין רמת ההכרות בפרדיגמה הפסיכומטרית על פיו ככל שרמת ההכרות נמוכה יותר כך הסיכון ייתפס כעוצמתי יותר. לפיכך, סיכון שמתפרסם מעט ולכן מוכר פחות לציבור, ייתפס כטעון יותר ובהתאם תופיע בו תגובתיות רבה יותר.

עבור ההשערה שצפיפות הטוקבקים האינטראקטיביים לכתבה תהיה גבוהה יותר בכתבות אודות סיכונים ברמת עוצמה גבוהה נמצא שסיכון הפגיעה הכלכלית באזרח ממוקם ראשון מבין שאר הסיכונים במשתנה הנבדק אך לא נמצא הבדל מובהק בין סוגי הסיכונים השונים. הסבר לכך יכול להיות טמון בעובדה שאמנם מספר הטוקבקים האינטראקטיביים היה גבוה יותר בסיכון זה יחסית לסיכונים אחרים, אך גם כמות הטוקבקים הריאקטיביים והדקלרטיביים הייתה גדולה עד כדי כך שבחישוב הצפיפות, ההבדל בין הסיכונים היטשטש. מסקנה שניתן להסיק מכך היא שההבדלים בין נושאים טעונים במשתנה זה, לעומת נושאים אחרים, הינם פחות מובהקים או כלל לא ויש לבדוק משתנים נוספים.

תרומת המחקר להעשרת התיאוריה הרלוונטית

ככלל, מאפייני הפרדיגמה הפסיכומטרית טרם יושמו בצורה נרחבת למדידת תפיסת הסיכונים בתחום הסייבר. במחקר זה, כנראה לראשונה, נחקרו סיכונים אלו מהזווית של הנזק הפוטנציאלי והתקבלו מספר מסקנות אשר חלקן נוגעות ליישום שיטות המחקר בהן נעשה שימוש בתחומי מחקר אחרים (תפיסת מאפייני הסיכון וניתוח התגובתיות) וחלקן נוגעות לממצאים הספציפיים אשר התקבלו במחקר זה.

מסקנה ראשונה היא שניתן ליישם, באופן חלקי, את מודל הפרדיגמה הפסיכומטרית לתחום הסייבר. התיאוריה של מדידת סיכונים במאפיינים ה"רכים" של הפרדיגמה הפסיכומטרית הינה גישה המתאימה לציבור שחסר ידע בתחום סיכונים מסוים. שימוש במודל זה, תוך ביצוע ההתאמות שהוצעו, יאפשר להצביע על פערי הידע של הציבור בישראל לגבי הסיכונים אליהם הוא חשוף ולהכוון לאמצעי ושיטות האבטחה אשר עומדות לרשותו כדי להתגונן. הבנה זו יכולה לסייע במיקוד פעילותם של הגורמים המתאימים בישראל האמונים להגנה על מרחב הסייבר הישראלי.

מסקנה שניה היא שניתן לחקור את תפיסת סיכוני הסייבר לפי סוג הנזק. זהו יישום שונה של מחקר קודם שבדק את תפיסת הסיכונים לפי מודל הפרדיגמה הפסיכומטרית מהזווית של הגורם לנזק, קרי אמצעי ושיטת התקיפה (Huang et al. 2010). יישום המודל במחקר הנוכחי לפי סוג הנזק מאפשר להבין את תפיסת הסיכונים מזווית נוספת ובכך לקבל תמונה רחבה יותר של תחום זה.

מסקנה שלישית היא שחשוב לחקור את השוני בין מומחים ולא-מומחים גם בתחום הסייבר. במחקר זה נמצאו הבדלים מובהקים בתפיסת הסיכון בין מומחים ולא-מומחים. ממצאים אלו מחזקים את התאוריה לגבי ההבדלים בתפיסת סיכון בין מומחים ולא-מומחים (Posey et al. 2014) ומעשירים את המחקרים המועטים, יחסית, שבוצעו לגבי סיכונים בתחום הסייבר.

מסקנה רביעית היא שדירוג הסיכונים שונה בין מומחים ולא-מומחים. מומחים דירגו גם בשלב הראשון של המחקר וגם בשלב השני את הנזק הביטחוני ושיבוש שירותים כבעלי עוצמה גבוהה, את פגיעה ברווחי חברה ופגיעה כלכלית באזרח כבעלי עוצמה בינונית ואת פגיעה בפרטיות ואפקט תודעתי כבעלי עוצמה נמוכה. לא-מומחים דירגו את פגיעה כלכלית באזרח, פגיעה בפרטיות ושיבוש שירותים כבעלי עוצמה גבוהה, את נזק בטחוני ופגיעה ברווחי חברה כבעלי עוצמה בינונית ואפקט תודעתי כבעל עוצמה נמוכה.

מסקנה חמישית היא שניתן לעשות שימוש בחקר התגובתיות לכתבות לצורך הערכת עוצמת סיכון. התאוריה הקיימת עוסקת בחקר התגובתיות כלפי נושאים טעונים ונושאים מתונים (פלמון, 2013). במחקר זה בוצע, כנראה לראשונה, שימוש בתאוריה זו לבדיקת ההבדל ביו סוגי סיכונים שונים כאשר בסיס ההנחה היא שסיכונים שנתפסים בעוצמה גבוהה מהווים נושאים טעונים וסיכונים שנתפסים בעוצמה נמוכה מהווים נושאים מתונים. לוגיקה זו מרחיבה את השימוש בחקר התגובתיות לתחום מחקר תפיסת הסיכונים ומשלבת ביניהם.

מסקנה שישית היא שניתן לעשות חיבור בין ממצאי מחקר תגובתיות ובין מחקר תפיסת הסיכונים. במחקר זה, כנראה לראשונה, בוצע מחקר בשתי שיטות שונות לאותו תחום של סיכוני סייבר תחת בסיס ההנחה שהמאפיינים ה"רכים" של תפיסת הסיכון מושפעים מרמת הידע של הנבדק, וזו מושפעת במידה רבה מהחשיפה לאירועים המתפרסמים באתרי החדשות. זהו כיוון מחקרי חדש המחבר בין שתי דיסציפלינות שונות ויכול להרחיב את ההבנה לגבי עוצמת התגובתיות מחד ותפיסת הסיכונים מאידך.

מסקנה שמינית היא שהסיכון של פגיעה כלכלית באזרח נתפס כבעל העוצמה הגבוהה ביותר בקרב הציבור. במחקר זה נמצא שבסיכון זה נמצאה הרמה הגבוהה ביותר של תגובתיות גולשים, באופן מובהק, לעומת הסיכונים האחרים שדווחו בכתבות. המשמעות היא שהציבור רואה את האירועים שדווחו בתקשורת אודות סיכון זה כנושא טעון יותר לעומת אירועים אחרים. בכך ישנה התאמה לממצאי השלב השני בקרב קבוצת לא-מומחים אשר דירגה את סיכון הפגיעה הכלכלית באזרח כבעל העוצמה הגבוהה ביותר. הממצאים הדומים משני כלים שונים אלו (מאפייני הסיכון וניתוח תגובתיות) מאפשרים להבין טוב יותר מאיזה סיכון

בתחום הסייבר הציבור מוטרד ביותר. הבנה זו יכולה לקדם את מאמץ ההסברה מול הציבור - גם בכך שיינתן יותר מידע מקצועי אודות הסיכונים המטרידים אותו ביותר וגם בכך שיינתנו כלים ושיטות אבטחה להתמודד עם סיכונים אלו.

מגבלות המחקר והצעות למחקרים עתידיים

המגבלות העיקריות של המחקר נוגעות להיקף איסוף הנתונים. המדגם ששימש לשאלון היה מצומצם יחסית (60 נבדקים) ולא נבנה באופן שמייצג את כלל האוכלוסיה. טוקבקים נבדקו רק באתרי חדשות בעוד שאנשים נוהגים להגיב גם בפורומים, בלוגים ואתרים אחרים.באופן טבעי, מחקר עתידי יכול להתבסס על איסוף נתונים נרחב יותר שיאפשר זיהוי תפיסת סיכון בסקטורים שונים במשק.

מחקר עתידי יכול לפתח את תפיסת הסיכון והאופן בו נבדק מגיע לאירוע בשיטות נוספות כגון משחק סימולציה אשר מציג אירועים שונים בפני הנבדק ותגובתו נמדדת לפי מדדים פיזיולוגיים המייצגים מתח וחרדה. באופן זה ניתן להבין מזוויות נוספות את תפיסת הסיכונים.

במחקר זה כל מאפיין נבדק בשאלה אחת. ניתן להעמיק ולבדוק כל מאפיין במספר שאלות המנוסחות אחרת, בודקות ממספר זוויות את אותו מאפיין, ממחישות אותו בצורה שונה וכך עשויים לקבל ממצאים מדויקים ומפורטים יותר.

במחקר המשך ניתן לבדוק כיצד קבוצה נתונה תופסת את סיכוני סייבר לעומת סיכונים אחרים – סיכונים טכנולוגיים דומים (כגון השבתת מערכות בגלל תקלת מחשוב) או סיכונים שונים לגמרי (כגון אסונות טבע). מחקר כזה יוכל לשפוך אור נוסף לגבי מידת ההבנה והמודעות של הציבור בתחום הסייבר ובהמשך להוות בסיס לתוכנית הכשרה והכנה, כפי שמבוצע בתחום ההערכות לחירום מפני טילים של פיקוד העורף. בנוסף, מוצע לבדוק ע״י ניתוח תוכן איכותני האם ניתן לזהות תגובות ייחודיות לסיכוני סייבר כחלק מהתרעה לגבי סף הסובלנות של הציבור לארוע מסוג מסויים.

סיכום

מטרתו של מחקר זה הייתה לחקור את תפיסת סיכוני הסייבר בקרב הציבור בישראל. לצורך כך בוצע שימוש בשתי גישות תיאורטיות ושיטות מחקר. האחת בדקה את תפיסת סיכוני הסייבר על ידי שימוש במאפייני הפרדיגמה הפסיכומטרית. השנייה, ניתוח תגובתיות של גולשים לכתבות באתרי חדשות אודות אירועי סייבר. שתי גישות אלו יושמו לראשונה בישראל לתחום סיכוני הסייבר. יתרה מזאת, ככל הנראה נכון לכתיבת מחקר זה, טרם יושם מודל הפרדיגמה הפסיכומטרית לצורך בדיקת סיכוני סייבר מבחינת הנזק הפוטנציאלי שלהם. נמצא שחלק ממאפייני תפיסת הסיכון אינם מתאימים לבדוק סיכונים בתחום הסייבר ולפיכך יש לבצע כיוונון וניסוח מחדש בעת מחקר נוסף בתחום זה.

הציבור תופס באופן שונה ממומחים את סיכוני הסייבר – בעוד למומחים ראייה מערכתית רחבה שמייחסת עצמה גבוהה לסיכונים בטחוניים, הציבור הרחב קרוב אצל עצמו 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. מימצא זה עלה בשתי הגישות המחקריות שננקטו כאן. מאחר שתובנה זו עלתה מהגישה הפסיכומטרית ניתן להעריך כי העיתונות אינה מביאה להבלטה מיוחדת של התקיפות הכלכליות ובכך מזמינה יותר תגובות, אלא רחשי הלב של הציבור הם כאלה שמושכים את הקשב הציבורי לכיוון הכלכלי. הממצאים מצביעים על כך שלציבור בישראל חסרה הבנה מספקת לגבי סיכוני הסייבר השונים והיקף האיומים. ככל הנראה, המצב כיום הוא שהציבור ניזון בעיקר מדיווחים בתקשורת בכלל ומכתבות בעיתונות המקוונת בפרט כמקור מידע עיקרי על הסיכונים המאיימים עליו. המידע המפורסם בתקשורת אינו מהווה מקור מספק להסברה אודות האיומים השונים בתחום הסייבר. זהו תחום משתנה ודינמי לעומת תחומי סיכונים אחרים (כגון אסונות טבע, פיגועי טרור, נפילות

טילים וכדומה) ולכן יש צורך בהזרמת מידע עיתית ומהימנה מגופים ממשלתיים אשר יכלול הסבר על רמת העוצמה של הסיכונים השונים ובעיקר את דרכי ההתמודדות. בנוסף, יכולים גופים ממשלתיים לתדרך את התקשורת לגבי סיקור אירועי סייבר כדי לשקף את עצמתם באמצעות הדיווחים.

רשימת מקורות

אבן ש. וסימן-טוב ד. (2011), לחימה במרחב הקיברנטי: מושגים, מגמות ומשמעויות לישראל, *המכון למחקרי בטחון לאומי*, מזכר 109.

אלקין-קורן נ. (2003), המתווכים החדשים ב'כיכר השוק 'הווירטואלית, *ממשל ומשפט*, כרך ו', גיליון 2, עמ' 381-420.

הכט י. (2003), השיח המקוון כמתווך חברתי. *אתר יעקב הכט*. אוחזר מ: http://jacobhecht.com

זכאי ד. (1994). תפיסת סיכון, התנהגות צייתנית וחרדה מצבית של נוער ישראלי בעת מלחמת המפרץ. *מגמות*, כרך 4, עמ' 325-343.

סיבוני ג., כהן ד. רוטברג א. (2013), איום ארגוני הטרור במרחב הסייבר, מרחב הסייבר והבטחון הלאומי, *צבא ואסטרטגיה*, כרך 5, גיליון 3, עמ' 3-25.

פלמון י. (2013). אינטראקטיביות בטוקבקים בעיתונות המקוונת בישראל, *אוניברסיטת חיפה*.

Adams, A., and Blandford, A. "Bridging the gap between organizational and user perspectives of security in the clinical domain," *International Journal of Human-Computer Studies* (63:1-2) 2005, pp. 175-202.

Albrechtsen, E., and Hovden, J. "The information security digital divide between information security managers and users," *Computers & Security* (28:6) 2009, pp. 476-490.

Albrechtsen, E. "A qualitative study of users' view on information security," *Computers & Security* (26:4) 2007, pp. 276-289.

Brenner J. F. (2013), Eyes wide shut: The growing threat of cyber attacks on industrial control systems, *Bulletin of the Atomic Scientists,* v. 69, n. 5, p. 15-20.

Chertoff M. (2008), The U.S. National Infrastructure Protection Plan, *the U.S. Department of homeland security*.

Choobineh, J., Dhillon, G., Grimaila, M.R., and Rees, J. "Management of information security: Challenges and research directions," *Communications of the Association for Information Systems* (20:1) 2007, pp. 958-971.

Davy B. 1996. Fairness as compassion: towards a less unfair facility siting policy. *Risk: Health, Safety and Environment*. v. 7, n. 2, p. 99-108.

Deseriis M. (2013), Is Anonymous a New Form of Luddism? A Comparative Analysis of Industrial Machine Breaking, Computer Hacking, and Related Rhetorical Strategies. *Radical History Review*, v. 117, p. 33-48.

Eagly, A. H. & Chaiken S. (1993). The psychology of attitudes. *Harcourt Brace Jovanovich College Publishers*.

Filshtinskiy S. (2013), Privacy and Security: Cybercrime, Cyberweapons, Cyber Wars: Is There Too Much of It in the Air? Where reality stops and perception begins. *communications of the acm*, v. 56, n. 6, p. 28-30.

Gabriel I. J. & Nyshadham E. (2008). A Cognitive Map of People's Online Risk Perceptions and Attitudes: An Empirical Study. *InHawaii International Conference on System Sciences, Proceedings of the 41st Annual*.

Green C. H. & Brown R. A. (1980). Through a glass darkly: Perceiving perceived risks to health and safety. *Research paper, School of Architecture, Duncan of Jordanstone College of Art, University of Dundee, Scotland.*

Huang, D. L., Rau, P. L. P., & Salvendy, G. (2010). Perception of information security. *Behaviour & Information Technology*, *29*(3), 221-232.

Jackson, J., Allum, N. and Gaskell, G. (2005). Perceptions of Risk in Cyber Space, In: R. Mansell, & R.Collins, (Eds.), *Trust and Crime in Information Societies*. Edward Elgar, London.

Johnson E. J. & Tversky A. (1983). Affect, generalization, and the perception of risk. *Journal of Personality and Social Psychology*, v. 45, n. 1,p. 20-31.

Lerner J. S., Gonzalez R. M., Small D. A. & Fischhof, B. (2003). Effects of fear and anger on perceived risks of terrorism a national field experiment. *Psychological science*, v. 14, n. 2, p. 144-150.

Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). Bridging the divide: a qualitative

comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information & management*, *51*(5), 551-567.

Reich Z. (2011). User Comments: The transformation of participatory space. In J. B. Singer et al. (Eds.), *Participatory journalism: Guarding open gates at online newspapers*. p. 96-118. West Sussex, UK: Wiley-Blackwell,

Sargent R. & Brooks D. J. (2010). Terrorism in Australia: A psychometric study into the Western Australian public perception of terrorism. *Edith Cowan University*.

Sattath S. & Tversky A. (1977). Additive similarity trees. *Psychometrika*, v. 42, n. 3, p. 319-345.

Schmidt, M. (2004). Investigating risk perception: a short introduction. Chapter 3 in: Schmidt M. 2004. Loss of agro-biodiversity in Vavilov centers, with a special focus on the risks of genetically modified organisms (GMOs). *PhD Thesis*, Vienna, Austria

Sjöberg L. (2000). Factors in risk perception. *Risk analysis*, v. 20, n. 1, p. 1-11.

Sjöberg L. (2005). The perceived risk of terrorism. *Risk Management*, p. 43-61.

Slovic P. (1987). Perception of risk. *Science*, v. 236, n. 4799, p. 280-285.

Slovic P. Fischhoff B. & Lichtenstein S. (1986). The psychometric study of risk perception. *Risk evaluation and management.* Springer US, p. 3-24.

Slovic, P., Fischhoff, B. & Lichtenstein, S. (1982). Why study risk perception. *Risk analysis*, v. *2*, n. 2, p. 83-93.

Slovic, P., Finucane, M. L., Peters, E., & MacGregor, D. G. (2004). Risk as analysis and risk as feelings: Some thoughts about affect, reason, risk, and rationality. *Risk analysis*, *24*(2), 311-322.

Soyer H. (2013). Internet Science Risk, Risk Perception, and Cyberwar. *Network Architectures and Services*, p. 113-120.

WBGU 1998. World in Transition: Strategies for global environmental risks. *Annual report of the German Advisory council on global change* (WBGU).