אתגרי שיתוף מידע בסביבה פנים־מגזרית

גבי סיבוני והדס קליין

שיתוף מידע בסייבר כולל שיתוף של שיטות תקיפה, כלים ואמצעים לתקיפה, מטרות תקיפה, חולשות[1] שאותרו ודרכי התמודדות עם איומים. שיתוף מידע מהווה את אחד מעקרונות ההגנה האסטרטגיים, ומטרתו היא להגביר את החוסן הכולל[2] במרחב הקיברנטי. כיום פועלים בעולם ובישראל מיזמים שונים ומגוונים לשיתוף מידע, שרמת האפקטיביות של מרביתם אינה מיטבית.

מאמר זה עוסק במספר אתגרים מעולם הכלכלה ומדעי המדינה הניצבים בפני מיזמים פנים־מגזריים לשיתוף מידע, ובוחן את מידת ההשפעה שלהם. לאורך המאמר מוצגות דוגמאות של התמודדות עם אתגרים דומים בעולמות תוכן אחרים. לבסוף, מובאות המלצות להפחתת מידת השפעתם של האתגרים על תכנון ויישום תוכניות לשיתוף מידע בסביבה פנים־מגזרית.

מילות מפתח: ביטחון סייבר, שיתוף פעולה, שיתוף מידע, פרטיות, רגולציה, אבטחת מידע, אמון, תחרות, "בעיית הטרמפיסט".

מבוא

אחד העקרונות המתפתחים לחיזוק ההגנה בסייבר הינו שיתוף במידע קונקרטי ואמין על חולשות קיימות, אופני התקפה, זיהוי גורמים מתקיפים, זיהוי המניע ועוד. שיתוף זה נעשה באופן שנועד לאפשר למקבל המידע ליישם הגנות במהירות, ובכך למנוע את התפשטות האיום. מודל השיתוף צריך להתקיים בין ארגונים הפועלים באותו מגזר שוק וחשופים לאיומים דומים, בין אם מהמגזר שלהם (מכנה משותף,

ד"ר גבי סיבוני, ראש התוכנית לביטחון סייבר במכון למחקרי ביטחון לאומי.
הדס קליין, מנהלת תכנית ביטחון סייבר במכון למחקרי ביטחון לאומי.

כגון שיוך מדיני, יריבים זהים וכדומה), ובין אם ממגזרים אחרים, וכן בין המגזר הפרטי למגזר הממשלתי ובין רשויות מדינתיות ממדינות שונות. ככל ששיתוף מידע יהיה רחב יותר, ניתן יהיה לייצר הגנות טובות יותר ולהתמודד עם תקיפות באופן יעיל יותר.[3]

שיתוף המידע תורם להגברת החוסן נגד מתקפת הסייבר לכל אורך מחזור חייה – החל מהשלבים המוקדמים בהם התוקף אוסף מודיעין בכדי לאתר את מטרתו, וכלה בשלבים מתקדמים בהם המתקפה מתרחשת הלכה למעשה. שיתוף מידע אפקטיבי ורחב יוכל לתרום לשיפור ההגנה בפני מתקפות סייבר,[4] בין השאר על ידי:

- שיפור מנגנוני התרעה (Early warnings) באופן שרמת העדכניות, הדיוק והרלוונטיות שלהם תגדל.
- תמיכה במאמצי המניעה (Prevention) והפעולות הנדרשות למניעת התממשותם של איומי סייבר.
- שיפור מאמצי הגילוי (Detection) כדי להביא לזיהוי מוקדם של התקפה ולאפשר ניתוח מדויק של היקף הפגיעה.
- ולבסוף, שיפור תהליכי התגובה וההתאוששות ממתקפה (Reaction & Recovery).

מתקפת סייבר מפורסמת, הממחישה את הצורך האקוטי בשיתוף מידע, היא המתקפה שכונתה "שוד הכספומטים הגדול".[5] במסגרת מתקפה זו, כנופיית פצחנים שדדה 45 מיליון דולר בשני מבצעים נקודתיים. חברי הכנופיה הצליחו להעלות את תקרת האשראי של חשבונות בנק ברחבי העולם ולבצע עשרות אלפי משיכות מזומנים בטרם נתפסו. השוד התבצע בשני גלים: האחד, ב־21 בדצמבר 2012, שבו השיגו הפצחנים מידע מחמישה חשבונות בנק והעלו בהם את תקרת האשראי. באותו היום משכו צוותי השטח מזומנים מ־4,500 כספומטים בסך כולל של חמישה מיליון דולרים. בגל השני, ב־19 בפברואר 2013, היו הפורצים נועזים עוד יותר. הפעם הם השיגו מידע על 12 חשבונות בנק והחלו בסדרה של 36,000 משיכות מכספומטים בניו יורק וב־24 מדינות נוספות בארצות הברית ובעולם, בסך כולל של ארבעים מיליון דולר.

העובדה המעניינת במקרה זה, החשובה להפקת לקחים, היא חוסר שיתוף הפעולה שהיה קיים בין הגורמים שחקרו את הפרשה ובין הגורמים הממונים על מניעת מתקפות ועל אבטחת נכסי המידע בבנקים. שיטת ההתקפה והמאפיינים של כלי התקיפה היו זמינים לגורמי אכיפת החוק כמעט מרגע ביצוע השוד הראשון. מסקנות ניתוח התקיפה הועברו לגופים המותקפים, אולם בשל מחסור בתהליכי שיתוף אפקטיביים, לא נוצרה תמונת מצב כוללת ולא הועבר המידע הרלוונטי למוסדות פיננסיים אחרים, באופן שיאפשר להם להיערך למתקפות דומות.

לצד היתרונות הברורים של שיתוף מידע, ראוי להזכיר גם את החסרונות שלו, ובהם האפשרות שמנגנונים לשיתוף מידע עלולים לסייע לתוקפים ואף להכשיר תוקפים חדשים, וזאת בנוסף לסיכונים אחרים הקיימים בתהליך.[6] אף על פי כן, קיימת ההסכמה אצל מומחי תוכן, כי יתרונות השיתוף עולים על חסרונותיו וסיכוניו וכי מימוש מנגנוני שיתוף מידע באופן מושכל יגביר את החוסן הקיברנטי הכולל.

מטרתו של מאמר זה היא להתמקד באתגרים העומדים בפני מיזמי שיתוף מידע הפועלים במרחב הפנים־מגזרי, תוך הצגת מורכבותם, לנתח דוגמאות מוצלחות של שיתופי פעולה פנים־מגזריים מעולמות תוכן אחרים, ולבסוף להביא המלצות להגברת האפקטיביות של מיזמים לשיתוף מידע במרחב זה.

מרחב השיתוף

במצב מיטבי, חברות אשר חוות פריצה למאגרי המידע שלהן – בין אם המדובר בפריצה על רקע פלילי ובין אם מדובר על פריצה ממניעים של ריגול או על פריצה על ידי גורם האקטיביסטי – יבצעו מספר מהלכים כחלק מתהליך ההתאוששות והחזרה לשגרה: בראש ובראשונה הן יפנו לגופי אכיפת החוק לצורך חקירת האירוע ומיצוי הדין. בנוסף, הן ישתפו את לקוחותיהן לצורך פעולות ניטור משותפות ובחינת השפעת האירוע. כל זאת, במטרה להפחית את הסיכוי להתרחשותו של אירוע מתגלגל ומתוקף חובת הדיווח לרשויות, לצרכנים, לספקים וכדומה. הדבר חיוני במיוחד בעת אירוע של גניבת מאגרים המכילים פרטי משתמש. במקרים בהם החברה המותקפת היא חברה ציבורית, ידווחו פרטי המקרה גם לרשות ניירות ערך ולכלל הציבור, כדי לתת אפשרות למשקיעים לקבל החלטות הנוגעות להשקעתם בחברה. לבסוף, החברה הנפגעת תשתף במידע חברות הפועלות באותו המגזר,[7] ואשר על פי ההערכות עשויות להיות חשופות לאותו איום. שיתוף זה ראוי שיתבצע באמצעות מרכז שיתוף מידע מגזרי, אשר יקבל את הנתונים, יבצע הערכת מצב ויפיץ את פרטי המקרה הרלוונטיים ליתר חברי המגזר, ובמקביל יפיץ מידע רלוונטי לגופי שיתוף בין־מגזריים, דוגמת חדרי מצב לאומיים.[8]

כדי ששיתוף הפעולה יהיה אפקטיבי ורחב, הוא חייב להיות ממוקד ומעוגן ולהתקיים בשני מרחבים: המרחב ה**בין־מגזרי**, קרי שיתוף מידע בין גופים המשתייכים למגזרים שונים, והמרחב ה**פנים־מגזרי**, כלומר שיתוף מידע בין גופים המשתייכים לאותו מגזר.

מידי שנה, ב־7 באפריל, תוקפים ארגונים המזדהים בשם "אנונימוס" גופים המזוהים כישראליים (מתקפת #OpIsrael). היערכות למתקפה זו מחייבת שיתוף מידע **בין מגזרים** שונים (תקשורת, בריאות, תחבורה, פיננסים, אנרגיה ועוד). במסגרת שיתוף זה מעבירים גופים מדינתיים, דוגמת חדר המצב הלאומי, שירות

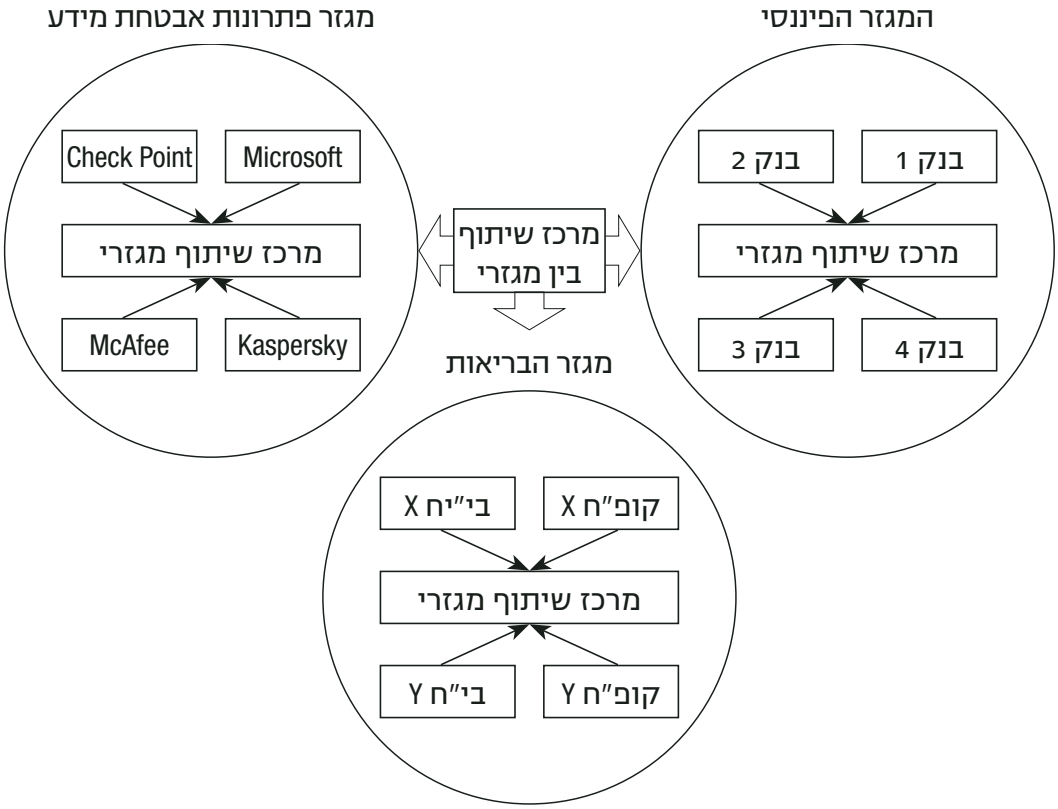
הביטחון הכללי, מטה הסייבר הלאומי ועוד, מידע לכלל המגזרים הרלוונטיים במשק הישראלי. בחלק מהמקרים מועבר המידע למרכזים קיברנטיים מגזריים (מק"ם), כמו המרכז המִגזרי לתחום האנרגיה והמרכז המִגזרי לתחום הבנקאי, המוקמים בימים אלה בישראל.[9]

חשיבות רבה קיימת גם לשיתוף מידע **פנים־מגזרי**. חקירות רבות של אירועי סייבר מלמדות כי שיטות פעולה, ניצול פרצות וחולשות ואף מתקפות דיוג (Phishing) מתאפיינים בכך שהם מתפשטים ברחבי המגזר. כמו כן, חקירת אופן הפעולה של קבוצות פשיעה במרחב הסייבר מלמדות כי אלו פעילות מאוד באיסוף מידע מקדים באופן מגזרי.[10] זאת ועוד, תעשיית פיתוח נוזקות מתאפיינת בהתמקצעות, המבוססת לעיתים על מערכות מגזריות. כזו היא, למשל, קבוצת הפצחנים Lizard Squad,[11] המתמקדת בפיתוח נוזקות ובמתקפות על אתרי משחקים.

שיתוף פנים־מגזרי צריך להתבסס על מודל שבו קבוצה של יצרני וצרכני מידע משתפים מידע האחד עם השני, אולם במקום לשלוח אותו ישירות ביניהם, המידע נשלח למינהלה מרכזית המַרכזת את המידע ומנהלת את הפצתו לכל יתר הצרכנים. מידע זה משותף על בסיס רלוונטיות מגזרית – לדוגמה, מידע על כלי התוקף חולשה קיימת במערכת הנפוצה במגזר. למעשה, מדובר במרכז שיתוף המהווה ישות לסליקת מידע בארגונים שונים, המשמשים הן כספקים והן כלקוחות של המידע.

דוגמה הממחישה את הצורך ב**שיתוף מידע דו־מרחבי** (שיתוף פנים־מגזרי ובין־מגזרי המתבצע במקביל) היא שיתוף מידע של יצרני טכנולוגיות הגנה בסייבר עם עמיתים למגזר, לצורך ניהול מאגר איומים וחולשות עדכני, רלוונטי ומדויק ככל האפשר במטרה לשרת את כלל משתמשי המרחב הקיברנטי, ולצד זאת שיתוף מידע עם גורמי אכיפה ורשויות מדינתיות במטרה לסייע במאבק בפשיעה בסייבר.[12]

להלן תיאור סכמטי של מרחב השיתוף במידע.



איור 1: מרחב השיתוף במידע

אתגרי שיתוף מידע בתוך אותו מגזר

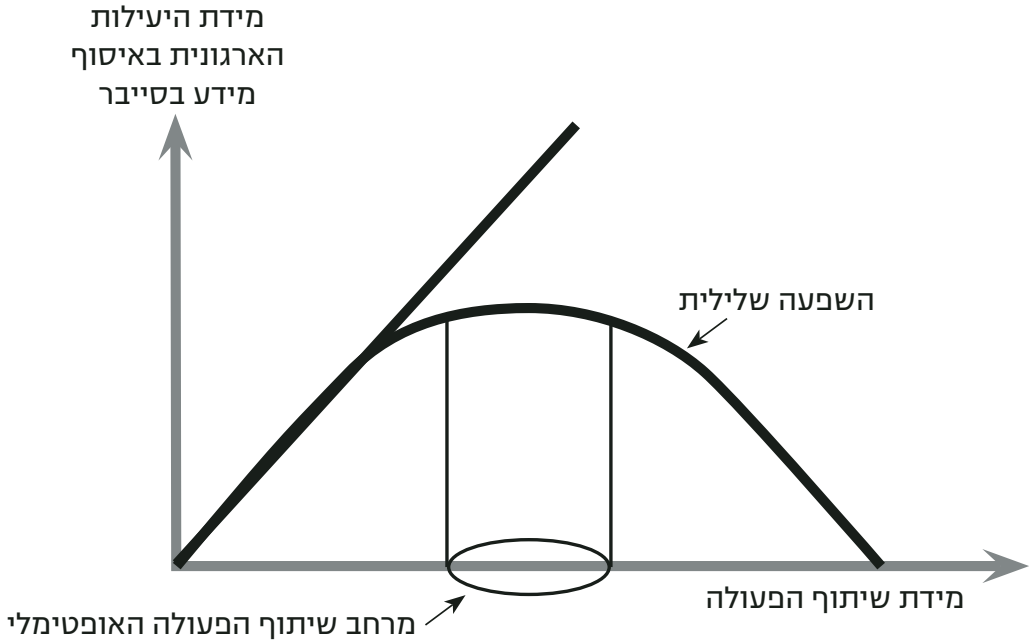
למרות ששיתוף המידע הפך למונח שגור בקרב העוסקים במרחב ביטחון הסייבר, ולמרות שהמטרה העומדת מאחוריו ברורה, שיתוף המידע בפועל מתבצע באופן חלקי בלבד. מספר הגופים הלוקחים חלק פעיל בשיתוף מידע אינו גבוה, ונפח המידע המשותף, כמו גם רמת הרלוונטיות שלו, אינם עולים בקנה אחד עם הצרכים.

מחקר שבחן את התמריצים והחסמים לשיתוף מידע מול איומי סייבר העלה כי לצד התמריצים קיימים חסמים – היבטים כלכליים הנובעים מחיסכון בעלויות, וכן היבטים הנובעים מאיכות המידע המשותף, ערכו והשימוש בו.[13] הנושאים העיקריים בצד החסמים היו החשש מקבלת מידע באיכות ירודה, חשיפת אירועי אבטחת מידע העלולה לפגוע במוניטין, וניהול כושל של מיזמים לשיתוף מידע. עוד התברר כי חברות וארגונים נוטים לא לשתף מידע בשל החשש שהוא עלול להועיל למתחריהם,[14] או בשל החשש שהדבר עלול לפגוע בדימוי החברה בעיני הציבור כמי שאינה מסוגלת להגן על נכסיה, ובכך לגרום לירידה במכירותיה ובשוויה.[15] חסם נוסף מוגדר על ידי כלכלנים כ"בעיית הטרמפיסט"[16] (Free rider problem) – מצב שבו מתקיים חוסר הדדיות, קרי מצב בו מתחרים משתמשים במידע שקיבלו לתועלתם, אולם מנגד אינם תורמים מידע משלהם.

מרבית המחקרים מתארים חסמים אשר המשותף להם היא הסביבה המגזרית בה הם פועלים. אלמלא פעלו הארגונים באותה סביבה מגזרית, סביר להניח כי חסמים אלה לא היו באים לידי ביטוי. למעשה, ניתן להסיק כי אחד הגורמים המשמעותיים המעכבים פיתוח מיזמים מוצלחים של שיתוף מידע הוא גורם התחרות. ארגונים הפועלים בסביבה תחרותית מתקשים לכונן מיזמי שיתוף מידע, למרות הידיעה הברורה ששיתוף כזה מועיל לכלל השותפים.

תחרות ושיתוף פעולה – הרקע התאורטי

לכאורה, תחרות ושיתוף פעולה הינם שני יסודות מנוגדים. על כן, מתעוררת השאלה האם הם יכולים להתקיים בצוותא? בתנאים של תחרות ללא שיתוף פעולה, גובר האינטרס האישי על האינטרס הקבוצתי. לעומת זאת, כאשר משתפי הפעולה מסתמכים באופן מוחלט על השותפים, מתקיים מצב של חוסר יעילות. לפיכך, יש צורך למצוא את נקודת האיזון, בה מתקיימת רמה מסוימת של שיתוף פעולה בין ארגונים הפועלים באותו המגזר, באופן שיועיל לכלל הארגונים. בהמשך חשוב להשקיע תשומות ומאמצים ליצירת בסיס איתן לשיתוף פעולה, כך שהתחרות ושיתוף הפעולה ישלימו האחד את השני ויתקיימו זה לצד זה. ניתן לתאר את נקודת האיזון הזו באופן המתואר באיור 2.



איור 2: מרחב שיתוף הפעולה

שיתוף פעולה בין גופים מתחרים יעמוד במבחן המציאות וישפר את מערכי ההגנה רק אם יכלול שילוב של תחרות ושיתוף פעולה, באופן שיספק יתרונות לכל אחד מהשותפים לאורך זמן. Brandenburger ו־Nalebuff טבעו לראשונה את המושג Co-Opetition בספר שפרסמו ב־1996.[17] Co-Opetition הוגדר בספר כאסטרטגיה עסקית המורכבת משיתוף פעולה (Cooperation) ותחרות (Competition), שמטרתה היא שיתוף פעולה בין מתחרים כדי להשיג יתרונות שאי אפשר להשיגם בדרך אחרת.

לפי אסטרטגיית ה־Co-opetition, כדי להרבות בהזדמנויות עסקיות ולהגדיל רווחים, עדיף להפסיק להשקיע מאמצים אינסופיים בניסיונות להיות טובים יותר מהמתחרים, ובמקביל לנסות ולהגדיל את סך ההזדמנויות המשותפות איתם, על ידי שיתוף פעולה שתועלתו היא בעלת ערך גבוה יותר בהקשר של ביטחון סייבר. דוגמה ל־Co-opetition ניתן למצוא בשיתוף הפעולה המאתגר בין חברת "סמסונג" הקוריאנית ובין חברת "סוני" היפנית, במסגרתו הביאו שתי חברות הענק לשיפור משמעותי בתהליכי החדשנות שלהן, שעודד גם את היצרנים הקטנים להשתתף בתהליך ולקדם אינטרסים מגזריים משותפים.[18] לעומת זאת, יש ארגונים העוסקים בפיתוח, המאמינים לעיתים שאין מקום לשיתוף פעולה המבוסס על החלפת מידע. מחשבה זו מקורה על פי רוב בחשש של ארגונים אלה שהארגון המתחרה יגנוב את רעיונותיהם, או ששיתוף הפעולה יגרום למתחרה לייצר מוצרים טובים יותר.

מציאת נקודת האיזון מחייבת לנתח את גורמי ההצלחה של מגזרים אחרים אשר מימשו תהליכים מובנים של שיתוף פעולה, וזאת למרות התחרותיות ועל אף השמירה ההדוקה על הקניין הרוחני שלהם. דוגמה למיזם מגזרי מוצלח של שיתוף פעולה ניתן למצוא בתחום הבנקאות: בראשית ימיהם של הכספומטים בישראל, היה הלקוח יכול למשוך מזומנים רק ברשת הבנקאית שאליה השתייך ורק במכשירים שבסניפי הרשת. לקוח של בנק הפועלים, למשל, לא היה יכול למשוך מזומנים במכשיר של בנק לאומי. כעבור שנים אחדות הוקמה חברת "שירותי בנקאות אוטומטיים" (שב"א), אשר הציבה במקומות ציבוריים מכשירים ששירתו את לקוחות כל הבנקים. בשלב מאוחר יותר הסכימו הבנקים לשפר את השירות ללקוחותיהם ולאפשר לכל לקוח להשתמש בכל מכשירי הכספומט בישראל.

בעבר נבחנה האפשרות שחברת שב"א תקים גם את מרכז הסייבר המגזרי הפיננסי בישראל, ואף הוגשה לצורך זה בקשה לממונה על ההגבלים העסקיים, שנדרש לדון בנושא מתוקף רגולציית ההגבלים העסקיים בישראל. בסופו של דבר, הוחלט לאחרונה להקים את מרכז הסייבר הפיננסי כחלק מחמ"ל הסייבר הלאומי (CERT). אחד האתגרים שאיתם יידרש המרכז החדש להתמודד יהיה נטרול "בעיית הטרמפיסט", כלומר איתור נקודת האיזון בין הבנקים, באופן שיבטיח המשך איסוף מידע ושיתופו באופן אופטימלי.

דוגמה נוספת לשיתוף פעולה מגזרי ניתן למצוא בתעשיית התרופות והפארמה. תעשייה זו רואה את שיתוף הפעולה כהכרחי, ומשתפת מידע באמצעות גוף שלישי המתווך בין בקשות המידע ובין המחקר. ניתן למצוא דוגמאות רבות של פיתוח תרופות המבוסס על מחקרים שנערכו בסביבת Open source. לדוגמה, מיזם משנת 2010,[19] שבמסגרתו התאגדו חברות תרופות ענק, יזמים ומכוני מחקר במטרה לקדם שיטות מחקר לצורך פיתוח תרופות לשתי מחלות נפש נפוצות. מיזם זה היה תולדה של ההבנה, כי למרות ההתקדמות העצומה בידע בתחום הביולוגיה המולקולרית, ועל אף המאמצים האדירים של כל הגורמים העוסקים בפיתוח תרופות, קצב הפיתוח של תרופות חדשות ירד, ככל הנראה בשל התחרות הגואה בין חברות תרופות יריבות מצד אחד, וההיקף המצומצם של החלפת מידע בין האקדמיה לתעשייה מצד שני.

בעולם של טכנולוגיות מידע ניתן ללמוד משיתוף פעולה בין חברות טכנולוגיה מתחרות שהתאגדו יחדיו כדי לקבוע תקנים למוצרים ולטכנולוגיות חדשות. כך, למשל, קביעת הַתקנים השונים של הֶתקנים נתיקים לשמירת נתונים, כמו וידאו, DVD וכדומה, מהווה זירה קבועה של שיתופי פעולה מצד אחד ותחרות מצד שני בין החברות "סוני", "פיליפס", "קודאק" וחברות רבות נוספות.

שיתוף מידע סייבר בסביבה תחרותית

ניתן להבחין בין שני מניעים עיקריים לתחרות בין ארגונים בהקשרים של ביטחון סייבר והשחקנים הפועלים בתחום שיתוף המידע: תחרות כלכלית ותחרות על האשראי (קרדיט).

תחרות כלכלית

תחרות כלכלית היא תחרות הנובעת מקושי בשיתוף פעולה בשל שאיפה לעליונות מסחרית והגדלת נתח שוק. סוג זה של תחרות קיים בעיקר בקרב ארגונים מוּנְחֵי רווח. בהקשרים של ביטחון סייבר ניתן להבחין בסוג כזה של תחרות אצל חברות העוסקות בפיתוח מוצרים ושירותים בעולם הגנת הסייבר – יצרני אנטי וירוס, יצרני "חומות מגן", ספקי שירותי אבטחת מידע מנוהלים (MSSP)[20] וכדומה.

המטרה של שיתוף מידע בין חברות המספקות שירותי ביטחון סייבר היא יצירת תשתית שיתוף אופטימלית, באופן שיאפשר מצב בו כל איום שיתגלה במוצרי חברה אחת יגרום לעדכון הפתרונות של כלל החברות, וכך יביא לשיפור ההגנה הכוללת של צרכני ביטחון הסייבר. כדי ליצור את שיתוף המידע המתואר, על חברות אלו להבין שעל אף גורם התחרות, שיתוף פעולה ביניהן הוא כדאי. האתגר גדול במיוחד בקבוצת היצרנים שאצלם המהות העסקית נוגעת לנושא ביטחון סייבר.

מנקודת מבט מסחרית, חברות העוסקות בפיתוח מוצרי הגנה מבינות כי מסדי הנתונים עליהם נשענים המוצרים השונים (דוגמת החתימות הדיגיטליות של נוזקות) הם חומר הגלם העומד בליבת המערכות. מנוע אבטחה, מתוחכם ככל שיהיה, לא יספק מענה הולם ועדכני אם יישען על נתונים חלקיים או לא רלוונטיים. לכן, אמינותם ועדכניותם של הנתונים הן מהגורמים החשובים ביותר באיכות המערכות וגורם מרכזי בהצלחתן המסחרית. בתנאי תחרות, קיים קושי רב בהעברת מידע רוחבי בין יצרני הטכנולוגיה השונים, במיוחד בין חברות שמידע זה מהווה את מוקד התחרות ביניהן.

גם בין חברות המספקות שירותי אבטחת מידע מנוהלים קיים שיתוף פעולה מוגבל. שיתוף זה מתבצע באופן עיתי בלבד ונעדר מנגנונים ותהליכים מובנים התומכים בצורכי העדכניות של הנתונים.

כיום אנו עדים למספר יוזמות לשיתוף מידע בקרב מגזר טכנולוגיות ביטחון הסייבר. יוזמות אלו פועלות במקביל, והחברות המקדמות אותן קוראות לשותפים למגזר לקחת בהן חלק. כך נוצר מצב בו חברות שונות במגזר טכנולוגיות ביטחון הסייבר מנסות לקדם פתרונות לבעיה, אך עושות זאת בדרך שמחריפה את אחד החסמים המובהקים לפתרון, ולמעשה פוגעות בעיקרון הבסיסי עבורו הוקמו – שיתוף פעולה לצורכי יצירת ערך מוסף. דוגמה לכך ניתן לראות בהכרזה, באוקטובר 2014, של החברות Fortinet, Palo Alto Symantec ו־Intel Security, העוסקות בטכנולוגיות ביטחון סייבר, על מיזם Cyber Threat Alliance, כשבמקביל, חברת "מיקרוסופט" פועלת לקידום מיזם דומה הנקרא VIA.

כדי ששיתוף המידע יהיה אפקטיבי, באופן שבו החברות יפיצו ויקבלו את המידע כשהוא עדיין "חם ורלוונטי", יש צורך לבסס פתרונות שיתוף מידע ממוכנים. בתחום זה מתקיימות מספר פעילויות תקינה הנתמכות על ידי משרד ההגנה של ארצות הברית, תחת ארכיטקטורת מעטפת הקרויה CyBOX.

תחרות על האשראי (קרדיט)

תחרות זו נובעת מקושי בשיתוף מידע בשל השאיפה להוקרה מקצועית ולפיתוח מוניטין, התפיסה כי ידע הוא כוח, ותרבות בין־ארגונית המתאפיינת לעיתים במאבקי כוח. סוג זה של תחרות ניתן למצוא גם במגזר המדינתי, בקרב גופים הפועלים לקידום ושיפור רמת ביטחון הסייבר הלאומית ובקרב גופים שאינם פועלים למטרות רווח, דוגמת מכוני מחקר ואקדמיה.[21] המצדדים בתיאום בין־ארגוני ובתוכניות משולבות טוענים כי הבעיות עִמן מתמודדת מדינה הן מורכבות, ולכן לטיפול בהן נדרשת גישה משולבת. הם מכירים בעובדה כי תיאום יכול ליצור יתרון לגודל וכי מהלך של מספר ארגונים הוא עוצמתי ויעיל יותר, ולעומת זאת,

פיצול מרובה וחפיפה בין תוכניות מחייבים תיאום רב, המסרבל את תהליך השיתוף ופוגע באפקטיביות שלו.

אחד המודלים,[22] שבחן דרכים להתמודדות עם חסמים במסגרת שיתופי פעולה בין גופים מדינתיים, זיהה מספר נקודות המחייבות התייחסות, כדי שאפשר יהיה להתגבר על חסמים אלה:

- **ריבונות**: ארגון נוהג להתייחס לעצמו כבעל ריבונות בעולם התוכן והסמכות שלו, ועל כן ארגון מדינתי ישתף פעולה רק אם הדבר תורם באופן ישיר למטרותיו וליעדיו. גם מקרים בהם שיתוף הפעולה מגובה במדיניות מחייבת מצריכים מידה מסוימת של השתתפות מרצון. אנשים רואים לנגד עיניהם, בראש ובראשונה, את התרומה הישירה לארגון שלהם, ורק לאחר מכן את התרומה של המאמץ לטובת הכלל.
- **מורכבות שיתוף הפעולה**: הגדרת תהליכי השיתוף מורכבת וכוללת מידה מסוימת של חוסר ודאות באשר לדרך הפעולה הנכונה. חשוב להתייחס להיבט זה בשלב התוויית התהליך, באמצעות הוספת בקרות ובדיקות היתכנות.
- **ממד הגודל**: שיתופי פעולה בין ארגונים גדולים וחזקים מבחינה תקציבית ובין ארגונים חלשים וקטנים יותר עלולים להיתפס על ידי הארגונים הקטנים כמאיימים ומחייבים. חוסר איזון זה מוביל להתנגדויות בתהליכי התיאום.
- **תרבות ארגונית ושיטות עבודה**: לכל ארגון תרבות ארגונית ייחודית, הכוללת שיטות תכנון, בקרה ולוחות זמנים. קיימת נטייה בקרב השותפים להתייחס לשיטות העבודה שלהם כטובות וכמתאימות ביותר.
- **פערי תקשורת ושפה משותפת**: בכל ארגון קיימים דפוסי תקשורת וטרמינולוגיה ייחודיים. חשוב להגדיר שפה משותפת ומובנת בקרב כלל השותפים.
- **סוגיית האסימטריה בין השותפים**: בהנחה שהשותפים אינם שווים בכוחם ובגודלם, יש לשאול מה היקף ואיכות המידע המסופק, לעומת היקף ואיכות המידע המתקבל.
- **חוסר יציבות וחוסר ודאות**: עולם הסייבר מתאפיין בסיכונים רבים המתפתחים חדשות לבקרים. על כן, שיתוף באמצעים טכנולוגיים של נתחים מסוימים בקניין הרוחני של חברה, מהווה סיכון של חשיפת המידע לגורמים לא רצויים.
- **תמריצים לשיתוף**: שיתוף פעולה באמצעות גוף הממונה על התיאום לא יפתור את כלל הבעיות והחסמים שבדרך. חשוב להגדיר תמריצים שיעודדו את כלל השותפים לתרום למאמץ המשותף.

דוגמה לשיתוף מידע פורה ניתן לראות בפעילות פורום המכונה Intellipedia, שהוקם כחלק מלקחי מתקפת הטרור על ארצות הברית בספטמבר 2001. במסגרת לקחים אלה, הבינו מקבלי ההחלטות בזרועות הביטחון האמריקאיים כי התפיסה, לפיה כל גוף מפתח ומנהל לעצמו את הידע, אינה תורמת לביטחון הלאומי. לקח זה נבע

מכך שהמידע המודיעיני שהיה קיים ערב הפיגועים לא זרם בין סוכנויות הביטחון השונות של המדינה, ובכך נמנעה היכולת לסכל את הפיגועים. כתוצאה מכך, מערך הביטחון האמריקאי הקים פורום משותף שתכליתו לסייע לארגונים השונים לשתף מידע. גם כאן אנו עדים לתחרות על משאבים, על מקורות מידע ועל יוקרה, אולם הצלחת הפורום מתבססת על ההבנה הקיימת בקרב הארגונים השונים כי רק שיתוף במידע ייצור רווח לציבור בצורת הגברתו של הביטחון הלאומי.

בארצות הברית פועלים מתחילת שנות האלפיים מיזמים למרכזי שיתוף מידע במגזרים שונים, כגון מגזר הבריאות, הפיננסים ועוד. מיזמים אלה מכונים Information Sharing and Analysis Centers (ISAC). כל המרכזים פועלים תחת עקרונות דומים, ולצידם קיים מרכז לאומי (National Council of ISACs – NCI), אשר מטרתו היא לקדם את שיתוף המידע הפנים־מגזרי באמצעות הגדרת עקרונות ותהליכי עבודה, וכן לקדם את הקשרים בין המרכזים השונים. רוב המיזמים הללו נמצאים בבעלות הארגונים החברים בהם, והם נתמכים מבחינה טכנולוגית וכלכלית על ידי המשרד להגנת המולדת של ארצות הברית.

מטֶבע הדברים, חברות הפועלות באותו מגזר מתחרות אחת בשנייה, אך מכיוון שהמהות העסקית שלהן אינה בתחום הסייבר, הן משתפות פעולה בתחום זה. לדוגמה, המרכז של המגזר הפיננסי לשיתוף מידע וניתוחו (Financial Sector Information Sharing and Analysis Center – FS-ISAC) מתמקד בשיתוף מידע במגזר הפיננסי בארצות הברית. מרכז זה פועל תחת העקרונות האופרטיביים הבאים: הארגון שייך לחברים בו, מנוהל על ידם ומתַחזק מאגרים הכוללים מידע על אירועי סייבר, אירועי אבטחה פיזיים, איומים, נקודות תורפה ופתרונות. המידע נאסף מהחברים בארגון, וכן מגורמים חיצוניים, כמו גופי ביטחון ממשלתיים ומרכַּזי שיתוף מידע אחרים. קיימות מספר דרגות של חברות במרכז, ובהתאם להן נקבע התשלום: ככל שרמת החברות גבוהה יותר, הארגון מקבל יותר שירותים וחשוף ליותר מידע. בהיבט התפעולי, ניתן להעביר למרכז לשיתוף מידע של המגזר הפיננסי מידע הן באופן אנונימי והן באופן גלוי. המידע נבדק על ידי צוות הפועל במשך כל שעות היממה, שבעה ימים בשבוע. הצוות מנתח ומסווג את הנתונים ומפיץ את המידע לחברים בהתאם לעקרונות.

מחקר שנערך בעקבות מספר אירועי סייבר חמורים במגזר הפיננסי ובקרב ארגונים החברים ב־FS-ISAC בחן מודלים חלופיים לקידום ושיפור השיתוף במידע, הן מבחינה כמותית והן מבחינה איכותית.[23] המחקר כָּלל שימוש בכלים מעולם תורת המשחקים, באמצעותם בחנו את המודלים הקיימים לתשלום דמי חברות במרכזי שיתוף המידע ואת השפעתם על רמת השיתוף. תוצאות המחקר הראו שרוב המודלים הקיימים במרכזי שיתוף מידע יוצרים חוסר איזון בין הציפיות הגבוהות של החברים לקבל מידע ובין הנכונות הנמוכה שלהם לשתף מידע. הדבר

מוביל לחוסר איזון משמעותי ואינו עולה בקנה אחד עם הצהרת הכוונות שכל חבר נדרש לה בעת ההצטרפות.

עוד בחן המחקר מודל תיאורטי חדשני, אשר בבסיסו עומד הרעיון שהתשלום בגין חברות במרכז שיתוף המידע ישמש כביטוח המסַפק כיסוי לנזקי התקפת סייבר. זאת, בשונה מהמודלים המקובלים, המבוססים על תשלום דמי חברות על פי דרגות השימוש. מפַתחי המודל החדש הראו שכאשר תשלום בגין חברות במיזם שיתוף מידע מבוסס על מדרגות הנקבעות על פי היקף השימוש, אין לארגונים החברים כל תמריץ לשתף את עמיתיהם במידע על תקריות סייבר שהתרחשו אצלם. לעומת זאת, כאשר המודל הוא תשלום פרמיה המבוססת על גודל ההפסד הצפוי לכל הארגונים יחד כתוצאה מתקרית ביטחון סייבר, שתמורתו מקבלים ביטוח הממומן ממאגר כלל הפרמיות, יש לחברים אינטרס לשתף מידע, שכן הארגון יהיה בטוח יותר ככל שיתר הארגונים יהיו בטוחים יותר.

המלצות

לאור הניתוח דלעיל, ובהנחה שלשיתוף מידע פנים־מגזרי חשיבות עליונה בשיפור ההגנה הקבוצתית, ניתן לאפיין מספר המלצות שיסייעו להצלחת הקמתם של מיזמים לשיתוף מידע סייבר בסביבה פנים־מגזרית:

- **מיפוי שותפים**: בשלב הייזום, פיתוח הרעיון וההבנה של התוצאה המצופה, יש לבצע תהליך מיפוי של שותפים פוטנציאליים וחשיבה על הרכבם הרצוי. בשלב זה נערכים מגעי גישוש ראשוניים, וכל צד בוחן האם הוא מוכן עקרונית להצטרף לשותפות. רצוי להגדיר בצורה מדויקת ככל הניתן את התוצאות אליהן מכוונים מיזם השיתוף והכלים העומדים לרשותו, לרבות כלים טכנולוגיים, רגולטוריים, כלכליים, הסברתיים וכדומה.
- **יחס עלות־תועלת**: ארגונים לא יירתמו לשתף מידע בכל מחיר. שיתוף מידע מוצלח תלוי בכך שהתועלת לכל אחד מהצדדים תהיה גבוהה יותר מהזמן והעלויות הכרוכות בשותפות. במקרים מסוימים נדרש יהיה לבחון אפשרות של עידוד התמיכה בשיתוף המידע באמצעות תמריצים. ראוי שגופים המשתפים מידע יכירו ויבינו את היתרון הכמותי והערך הכלכלי הטמון בשיתוף מוצלח. דרך זו נמצאה כיעילה ביצירת תמריץ לתהליכי שיתוף. כך גם בהקשר להסדרת התקציב של מיזם שיתוף המידע. יש לבצע את הסדרתו בשלבים הראשונים של המיזם, באופן שיהיה ברור לכלל השותפים מי נושא בעלויות התוכנית.
- **סוגי שותפים**: מומלץ להגדיר מיהם השותפים למהלך. יש להבחין בין שלושה סוגי שותפים – בעלי העניין, בעלי המידע ובעלי הסמכות – ולהעריך את חשיבותם ותרומתם להגברת האפקטיביות של המיזם. לכל שותף זווית ייחודית. לצורך הגברת האמון בין השותפים, יש צורך להַבְנות את התקשורת ביניהם

וליצור שפה משותפת. כאן חשובה יצירת "חוויה משותפת" ובניית שגרת פעילות, שיוסכם עליהן כבר בשלבי תכנון המיזם.

- **מחויבות וסמכות**: יש ליצור שלד של מחויבות מינימלית, אליו יהיו מחויבים כל השותפים בכל שלב, החל משלבי הייזום והתכנון וכלה ביישום ובהערכה העיתית של אפקטיביות התוכנית. רצוי לבחון מספר סוגיות מרכזיות הנוגעות לסמכות לקבלת ההחלטות, להובלת התהליך כולו וללוח הזמנים, וכן את מי נכון לשלב, מתי ובאיזה אופן. הצלחת השותפות מותנית בכך שכל צד לה יודע מראש מה מצופה ממנו לתרום לתהליך ומה יקבל בתמורה. יש לקבוע את גזרת הפעולה ותחומי האחריות של כל אחד מהשותפים ולהדגיש את התלות ההדדית ביניהם. מומלץ להגדיר כבר בשלב התכנון הראשוני את הגורם המוביל, שיהיה בעל הסמכות והאחריות על התהליך ותוצריו. ניתן לאפיין שני סוגי הובלה: מקצועית, המתבצעת על ידי האחראי המקצועי הרלוונטי ביותר, ותהליכית, המתבצעת על ידי גורם בעל מומחיות מתודולוגית בניהול תהליכים שיתופיים, הנתפס כנטול אינטרסים אישיים. יש להעמיד בראש הפרויקט דמות ספציפית המחויבת למטרות המשותפות.
- **אגו ויוקרה**: התמודדות עם היבטים של אגו ויוקרה מחייבת התייחסות מקדימה. במקום להניח שאין אגו וכולם פועלים משיקולים מקצועיים, טוב יהיה להניח שהמצב הפוך, וכך להדגיש את ייחודיות השחקנים ולראות באגו את הערך המקצועי שמביא כל גוף לתוכנית השיתוף. ראוי להכיר בגבולות האחריות של כל ארגון ולתת מקום לניסיון ולידע הנצבר שלו.
- **מנגנון קבלת החלטות**: פתרון מחלוקות טמון בבניית מנגנון לקבלת החלטות והכרעות, כחלק ממבנה השותפות. כבר בשלב התכנון יש להגדיר את המנגנון הנדרש לקבלת החלטות במצבי קונפליקט. חשוב להכיר בכך שתנאי הסף לטיפול במחלוקות הוא לזקק אותן ולהגיע להסכמה בין השותפים על מהות המחלוקת. לפני הכרעה יש למצות את השיח וההידברות ולאפשר מידה מרבית של שקיפות.
- **בקרה**: מנגנוני בקרה והערכה הינם משמעותיים ביותר להצלחה. הבקרה צריכה להיות מבוצעת באמצעות מנגנונים סדורים המעוגנים בפעילות המשותפת ונשענים על השגת יעדים ומדדים תפוקתיים. על אלה להיקבע באופן שילַווה מקצועית את היישום ויסייע בקבלת החלטות נכונות מבוססות נתונים, רצוי על ידי גוף מעריך חיצוני ואובייקטיבי. בהתאם להערכה המסכמת, ניתן לקבל החלטה באשר למידת יישום התוכנית ולצורך להכניס בה חידושים ושינויים. חשוב לשים דגש גם על בחינה עיתית של שינויים חיצוניים העשויים להשפיע על מידת האפקטיביות של המיזם, כגון שינויים רגולטוריים וטכנולוגיים.
- **שיתוף מדינתי**: יש לעודד גופים ציבוריים ברמה המדינתית לשתף מידע ביניהם. המדובר בגופים כגון CERTs לאומיים ומוסדות ממשלתיים אחרים. חשוב שגופים

אלה ייקחו חלק פעיל בקידום הנושא ובפיתוח פלטפורמות שיתנו מענה לחסמים השונים. יש לגבש תוכניות הכשרה לצורך יצירה, פיתוח ושמירה על מיומנות ומומחיות הנדרשות לתפעולם של מרכַּזי שיתוף המידע. יחד עם זאת, חשוב למצוא את האיזון בין המעורבות של המדינה בניהול ומימוש תהליכי שיתוף לבין הצורך של מגזרים מסוימים להגן על המידע המשותף בשל סוגו ורגישותו. קיימים מגזרים אשר המידע שבחזקתם רגיש לפרטיות באופן מובהק (לדוגמה, מגזר הביטוח). במקרים כאלה על המדינה לאפשר עצמאות בשיתוף, הכוללת התערבות מינימלית.

ברמה האופרטיבית של תכנון מיזם לשיתוף מידע, יש לוודא שהמידע רלוונטי לגופים המשתתפים במיזם וכי הוא באיכות מתאימה ובתזמון הנכון. לצורך זה יש לקיים פורומים, שמטרתם היא להגדיר את תהליכי השיתוף לפרטיהם. לדוגמה, שיתוף במידע על כתובת האינטרנט (IP) של תוקף מסוים הוא דבר הכרחי. יחד עם זאת, קיימים מאפייני תקיפה ייחודיים אחרים שחשוב להימנע משיתוף מידע לגביהם, וזאת כדי למנוע ניצול לרעה של המידע המשותף.

סיכום

יש חשיבות רבה לשיתוף מידע בתחום הסייבר, שכן המידע הנחוץ להתמודדות עם האיומים על תחום זה מפוזר כיום בין מדינות וארגונים בכל רחבי העולם. שיתוף מידע כזה יכול לכלול עדכון הדדי לגבי תקיפות (שיטות, אמצעים, מטרות), חולשות שאותרו ודרכי התמודדות עם איומים ספציפיים וכלליים. שיתוף מידע מיטבי מאפשר הצגת תמונת מצב של איומי סייבר באופן עדכני ורלוונטי, ברמות המגזר, המדינה והזירה העולמית. עוד מאפשר שיתוף המידע לתמוך בתהליכי קבלת החלטות הנוגעות להשקעת משאבים ראויים ורלוונטיים מול האיומים המתפתחים. לבסוף, שיתוף מידע מוצלח מסייע גם בתהליכי מחקר ופיתוח של פתרונות שנועדו להתמודד עם איומי הסייבר.

כיום קיימים מיזמי שיתוף מידע רבים, המנוהלים כיוזמות מדינתיות, מגזריות או פרטיות. אחד המנגנונים המשמעותיים והמובילים ביותר הוא המידע שחברות אבטחה והגנה חולקות עם לקוחותיהן – מידע שמקורו לרוב בלקוחות החברה המותקפים. ההנחה היא שמנגנון זה פועל בצורה מיטבית. מנגנון שיתוף מידע נוסף, המזוהה כבעל אפקטיביות גדולה אם כי לא מיטבית, ניתן למצוא במרכַּזי השיתוף המגזריים. כן קיימים מנגנוני שיתוף מידע בארגונים רבים, המוקמים באופן אינטואיטיבי, לא פורמלי ובצורה חלקית. חשוב להקים מיזם גלובלי שיפעל על פי העקרונות התפעוליים של מיזם חברות האבטחה. כלל המידע שייאסף במסגרת המיזם הגלובלי יותך וינותח, כפי שנעשה במסגרת המיזם של חברות האבטחה, ואז יופץ המידע המעובד בחזרה לכל הלקוחות של כל השותפים.

על אף האתגרים הרבים הניצבים בפני מימוש מיזמים לשיתוף מידע, כפי שהדבר הוצג במאמר זה, הקמתם של מרכזי שיתוף מידע הינה קריטית לשיפור הביטחון הקיבוצי במרחב הסייבר. לפיכך, ראוי שהמנגנונים המוצעים כאן ישולבו כחלק מ"ארגז הכלים" שישמש לייזומם, תכנונם והפעלתם של מרכזים כאלה.

הערות

1 חולשות הינן נקודות תורפה (לעיתים מזוהות וידועות), אשר על פי רוב נובעות מתכנון לקוי ומאפשרות לתוקף לנצלן לחדירה למערכת או לשיבוש אופן פעולתה.

2 מושג רחב המתייחס לעמידותו ולעוצמתו של המרחב הקיברנטי מול איומים וסיכונים העשויים לשבש את פעילותו או את אופן השימוש בו.

3 הדיון המתקיים בקרב מומחים בנושא שיתוף מידע בסייבר מעלה לא אחת טענות כי תהליך זה טומן בחובו גם סיכונים, ובעיקרם העובדה שעצם שיתוף המידע עלול להיחשף לציבור הרחב, ובכך לסייע לתוקפים ואף להכשיר תוקפים חדשים. זאת, בנוסף לסיכונים אחרים הקיימים בתהליך. סקירה רחבה בנושא זה ראו: *Incentives and Challenges for Information Sharing in the Context of Network and Information Security*, ENISA, 2010.

4 Gabi Siboni, "An Integrated Security Approach: The Key to Cyber Defense," *Georgetown Journal of International Affairs*, May 7, 2015.

5 Marc Santora, "In Hours Thieves Took $45 Million in A.T.M. Scheme," *The New York Times*, May 9, 2013, http://www.nytimes.com/2013/05/10/nyregion/eight-charged-in-45-million-global-cyber-bank-thefts.html?_r=1.

6 סקירה מלאה של היתרונות והסיכונים ניתן למצוא, כאמור, ב־*Incentives and Challenges for Information Sharing in the Context of Network and Information Security.*

7 מגזר (סקטור) הינו קבוצה של גופים בעלי מאפיינים דומים במשק, אשר פועלים בסביבה עסקית דומה ויש להם מטרות דומות; למשל, "המגזר העסקי" או "הסקטור העסקי".

8 חדרי מצב לאומיים קיימים במדינות רבות בעולם. מטרתם היא לעסוק בבניית תמונת מצב לאומית בסייבר ובתיאום שיתוף המידע בין מגזרים, וכן בין גופים מדינתיים לגופים אזרחיים.

9 עמי רוחקס דומבה, "תכירו, מרכז קיברנטי מגזרי לתחום האנרגיה בישראל", *Israel Defense*, 25 בנובמבר 2015.

10 L. Ablon, M. Libicki, A. Golay, *Markets for Cybercrime Tools and Stolen Data*, National Security Research Division, Rand Corporation, 2014.

11 Jimmy Blake and Amelia Butterly, "Who are Lizard Squad and what's Next for the Hackers?," *BBC*, January 27 2015, http://www.bbc.co.uk/newsbeat/article/30306319/who-are-lizard-squad-and-whats-next-for-the-hackers.

12 סקירה רחבה המתארת את הגופים והיוזמות הפועלים לקידום שיתוף מידע בסייבר ראו: אבירם זרחיה, "ניתוח רב ממדי של שיתוף מידע סייבר ארגוני", **צבא ואסטרטגיה**, כרך 6, גיליון 3, דצמבר 2014.

13 *Incentives and Challenges for Information Sharing in the Context of Network and Information Security.*

14 Andrew Nolan, *Cybersecurity and Information Sharing Legal Challenges and Solutions*, Congressional Research Service, March 16, 2015.

15 M.C. Arcuri, M. Brogi, G. Gandolfi, *The Effect of Information Security Breaches on Stock Returns*, Università di Roma "La Sapienza," 2014.

16 Russell Hardin, "The Free Rider Problem," *The Stanford Encyclopedia of Philosophy*, Spring 2013.

17 Adam M. Brandenburger and Barry J. Nalebuff, *Co-Opetition*, Doubleday, 1996.

18 Devi R. Gnyawali, Byung-Jin Park, "Co-opetition between Giants: Collaboration with Competitors for Technological Innovation," *Research Policy*, Volume 40, Issue 5, June 2011.

19 פרופ' יונתן רבינוביץ מאוניברסיטת בר־אילן ממובילי פרויקט בינלאומי שעשוי להביא לפריצת דרך בפיתוח תרופות למחלות נפש נפוצות, אוניברסיטת בר־אילן, משרד הדוברות, 7 בדצמבר 2010.

20 שירותי ניטור רציף של מערכות אבטחת המידע וביצוע ניתוח והתאמות בין נתונים לצורך זיהוי מוקדם ופרואקטיבי של איומים. ניתוח זה מתבצע באמצעות היתוך כלל הנתונים המגיעים מכלל לקוחות החברה והפצת המידע הרלוונטי בחזרה לחברות.

21 במקרים מסוימים, גם מגזר זה מתאפיין בתחרות כלכלית.

22 Susanna P. Campbell, Michael Hartnett, *A Framework for Improved Coordination: Lessons Learned from the International Development, Peacekeeping Peacebuilding, Humanitarian and Conflict Resolution Communities*, October 31, 2005, https://www.regjeringen.no/globalassets/upload/ud/vedlegg/missions/framework.pdf.

23 Charles Zhechao Liu, Humayun Zafar and Yoris Au, "Rethinking FS-ISAC: An IT Security Information Sharing Network Model for the Financial Services Sector," *Communications of the Association for Information Systems*, Vol. 34, 2014.