ניתוח רב ממדי של שיתוף מידע סייבר ארגוני

אבירם זרחיה

התפתחות איום הסייבר מחייבת ארגונים לשנות דפוסי חשיבה ומערכי הגנה בהיבטים רבים. אחד מהם נוגע למדיניות הארגון באשר לשיתוף מידע סייבר עם גורמים חיצוניים ומעבָר מתפיסה של ארגון ממודר לתפיסה של ארגון משתף. השיתוף יוצר בעיה מורכבת ומרובת פנים בתחומי הטכנולוגיה, המשפט, התרבות הארגונית ואף הפוליטיקה. הקמת מערך שיתוף משרתת גורמים רבים, ובהם גופי הרגולציה, הממשל, רשויות החוק והביון, יצרני הפתרונות והשירותים ואף הארגונים עצמם, אך גם מעוררת התנגדות מצד גורמים פנים ארגוניים וארגוני ההגנה על הפרטיות.
מטרת המאמר היא להציג את נושא שיתוף המידע בסייבר על היבטיו ואתגריו השונים, לחשוף את הקורא לעולם המושגים המקיף אותו ולהציג תובנות ותחזיות באשר להתפתחות המגמה בעתיד.

מילות מפתח: סייבר, שיתוף מידע, פרטיות, רגולציה, אבטחת מידע, אמון.

מבוא

אחד האתגרים המשמעותיים של ארגונים בעידן הנוכחי הוא ההתמודדות עם איום הסייבר. השימוש המוגבר בטכנולוגיה במגוון ארגונים – ממשלתיים, ציבוריים ופרטיים – הופך אותם למטרה להתקפות המכוונות לאסוף מידע, לפגוע במידע או להשבית שירותים. התקפות על ארגונים מסחריים עלולות לפגוע במוניטין הארגון, לסכן את נכסיו הרוחניים והפיזיים ולגרום לעלויות כספיות כבדות. התקפות על גופים ותשתיות ממשלתיים וציבוריים עלולות, בנוסף, לפגוע בשגרת החיים של מדינה ואף בבריאות תושביה וביטחונם.

אבירם זרחיה הוא מומחה טכנולוגי להגנה בסייבר בחברת ג'וניפר נטוורקס, מרצה בתחום הסייבר ומתמחה בתוכנית לביטחון סייבר במכון למחקרי ביטחון לאומי.

במהלך העשור האחרון זלג עולם הפשיעה המסורתי למרחב הסייבר. השכלול בכלי הפריצה ודרכי התקיפה הוביל להיווצרות כלכלת פשיעה חדשה, מפותחת ומשוכללת, בסייבר. תהליך דומה עבר על מרחב הלוחמה בין מדינות, ורבים רואים בסייבר את ממד הלחימה החמישי של שדה הקרב המודרני, בנוסף ליבשה, אוויר, ים וחלל.

ההתמודדות עם איום הסייבר מחייבת השקעה בתשתיות אנושיות וטכנולוגיות בהתאם למדיניות ניהול הסיכונים הארגונית או הלאומית. איכות של מערך אבטחת מידע ארגוני מושפעת מגורמים שונים, שאחד המרכזיים בהם הוא יכולת איסוף וניתוח מידע הן על תעבורת משתמשים לגיטימית והן על התקפות, בין אם הצליחו ובין אם נכשלו. באמצעות יכולת זו ניתן לאתר מראש פרצות במערך האבטחה ולחסום אותן, וכן לזהות התקפות ולהגיב עליהן באופן יעיל ומהיר, ובכך לחסוך מהארגון התמודדות עם תוצאותיהן, או לפחות להקטין את השפעתן.

שיתוף מידע סייבר ארגוני הוא תקשורת של מידע הנוגע לאבטחת הארגון אל ישות חיצונית, במטרה להשיג תועלות הן לארגון המשתף והן לארגון המקבל. שיתוף כזה יוצר בעיה מורכבת ומרובת פנים ומהווה שינוי פרדיגמה בעולם טכנולוגיות המידע (IT). מודל השיתוף יכול להתקיים בתוך אותו מגזר שוק, בין חברות ממגזרים שונים, ואף בין ארגונים ובין גופי ממשל ובין ממשלות שונות. בשנתיים האחרונות נראה כי מתחזקת מגמת השיתוף וכי גופי רגולציה ואכיפת חוק, מקומיים ובין־לאומיים, מקדמים מגמה זו באמצעות הנחייה, עידוד או חקיקה. במקביל מתפתחת תעשייה של פתרונות אבטחה, המבוססת על שיתוף מידע בין גופים.

מטרת המאמר היא להציג את אתגר השיתוף על היבטיו השונים ולחשוף את הקורא לעולם המושגים המקיף את הנושא. המאמר מתבסס על מגוון מקורות אקדמיים, מחקריים, ממשלתיים, טכנולוגיים ועיתונאיים. הוא מציג תחילה את המצב הנוכחי והבעייתיות הנובעת ממנו, ממשיך בניתוח היבטים מעשיים של שיתוף ואופני מימושם, כולל נגיעה ברקע התאורטי של נושא האמון בין גופים, מפרט את התועלות והאתגרים לארגון, מתאר את מרחב ההזדמנויות העסקי, סוקר היבטי חוק, רגולציה ופרטיות, ומציע לסיכום מספר תובנות. רוב הדוגמאות במאמר לקוחות מארצות הברית, שבה מיזמי השיתוף, מאמצי התקינה, פעולות הממשל וסוכנויות הביון ותהליכי החקיקה חשופים ונמצאים במרכז הדיון הציבורי. תהליכים דומים עוברים על מדינות אחרות ובהן ישראל, גם אם אלה אינם חשופים במלואם לעיני הציבור.

ממידור לשיתוף

איום הסייבר מתקיים כממד פשיעה ולחימה משוכלל ומורכב, שהתפתח בשנים האחרונות בשני אפיקים מקבילים: **מרחב האיום** ו**חומרת האיום**. בהיבט **מרחב האיום**, ארגונים נדרשים להגן כיום לא רק על מערכות המחשוב והמידע הפנים ארגוניות, אלא גם על אמצעי הקצה המגוונים שברשות המשתמשים, כגון טלפונים חכמים ומחשבים ניידים, וכן על מערכות תשתית, כגון חשמל ומיזוג אוויר. כל זאת, באופן רציף, בדרך שתאפשר לספק שירותים מכל מקום ובכל זמן, כפי שמצופה מארגון בעידן הנוכחי.

בהיבט **חומרת האיום**, ההתקפות הופכות לקשות יותר לאיתור וכוללות גם אופני תקיפה שאינם מתועדים או ידועים ליצרניות פתרונות האבטחה. כאלה הם, למשל, "מתקפות יום אפס" (Zero Day Attacks)[1] והאקרים המשתפים ביניהם מידע באופן שוטף ובזמן אמת ויוצרים מצב בו כל נקודת תורפה שמתגלה במערכות, או נוזקה (Malware), ניתנות לשכפול ולמימוש כמתקפה בצדו האחר של העולם באופן כמעט מיידי. מחקר של מכון RAND שנערך לאחרונה בנושא זה,[2] מספק ניתוח של האופן בו "השווקים השחורים" של עולם הסייבר בנויים ומתפקדים כמערכת משולבת (Eco-System) בעלת תשתית ומבנה ברורים.

התפתחויות אלו יצרו קושי לארגונים להילחם לבדם את מלחמת הסייבר, וכתוצאה מכך הֵחל תהליך של שינוי בתפיסת ההגנה שלהם. ברוב הארגונים, למעט אלה הכפופים לרגולציה ומערכות צבאיות־ממשלתיות, תפיסת ניהול אבטחת המידע התאפיינה בנתק מוחלט מארגונים אחרים, הן בהיבט הטכנולוגי של מערכות המידע ואבטחת המידע והן בהיבט של שיתוף מידע על אירועי סייבר ואבטחה. המידע על התקפה או ניסיון התקפה, וכן תוצאות הניתוח שלו, נשמרו בתוך הארגון, סווגו והופצו לתפוצת נמענים פנים ארגונית מוגבלת בלבד. גילוי המידע לצד שלישי נתפס כסיכון לארגון, העלול להוביל לפגיעה במוניטין, לחשיפה משפטית ועוד.

לאחרונה אנו עדים לשינוי התפיסה, כאשר ארגונים ורשויות רבים שוקלים לנטוש את אסטרטגיית הארגון הממודר[3] לטובת מודל של שיתוף מידע עם גופים אחרים (Information Sharing). שיתוף מידע סייבר בין גופים, בדומה לזה המתקיים בין האקרים בצד ההתקפי, יצור מצב בו, למשל, מעטפת הגנה שנוצרה בארגון מסוים כדי להתמודד עם איום שהתגלה, תופץ כחיסון לארגונים אחרים, או לפחות כמידע שיעלה את רף הערנות והמודעות שלהם לאיום הספציפי.

העלויות הגבוהות המושתות על הארגון כדי שיוכל לעמוד ברף הנדרש להספקת מעטפת הגנה יעילה במשאבי זמן, אנשים וטכנולוגיה, יוצרות אינטרס ארגוני לשיתוף מידע והעברת חלק מהעלויות הללו לצד שלישי. מחקר שנערך בארצות הברית בנושא זה,[4] מנתח את הקשר בין שיתוף מידע סייבר ובין עלויות

האבטחה הארגוניות. ממצאי המחקר מראים כי חברות ששיתפו מידע נדרשו להשקעה כספית קטנה יותר במערך האבטחה, כדי להגיע לרמת הגנה זהה לזו של חברות שלא שיתפו מידע. מכאן שניתן להגיע לחיסכון כספי ישיר לארגון, בין היתר כתוצאה מהשיתוף. המדובר, לדוגמה, באיסוף ובהזנת מודיעין פרואקטיבי על חולשות והתקפות צפויות, בחיסון מפני התקפה שהתרחשה בארגון אחר, בשימוש באנשי מקצוע שיעזרו בניתוח אירועי אבטחה, ועוד.

סיבה נוספת לשינוי התפיסה הארגונית ביחס לשיתוף מידע הן התועלות העסקיות הישירות והעקיפות הנובעות מעמידה בסטנדרטים ורגולציות. במגזרים חיוניים מסוימים, כמו פיננסים, בריאות, אנרגיה ותקשורת, נדרשים ארגונים, כולל פרטיים, לאפשר למדינה פיקוח טוב יותר על התנהלותם, וזאת במספר היבטים. ברוב הרגולציות נכללת, בין היתר, דרישה לשיתוף מידע בין הארגון ובין רשות מפקחת כלשהי בכל הנוגע לאירועי סייבר או ניסיונות תקיפה. בצד החובות, ישנן גם תועלות ישירות ועקיפות לארגון מהרגולציה: ארגון פיננסי הפועל תחת רגולציית באזל III[5] – תקינה המתייחסת לגופים פיננסיים ומחייבת, בין היתר, שקיפות של סיכונים תפעוליים ובהם גם אירועי אבטחה מול הרגולטור – מחויב בהקצאת הון בהתאם לרמת הסיכונים שלו[6], ויכול לשפר רווחיות על ידי הקטנתם. דוגמה לתועלת עקיפה ניתן למצוא בארגון המספק שירותים, שמתאפשר לו להתמודד במכרז ממשלתי המחייב עמידה בתקינת ISO-27032,[7] הכולל אף הוא מתווה לשיתוף מידע.

עקרונות טכנולוגיים בשיתוף מידע

שיתוף מידע בין ארגונים באופן מאובטח הוא אתגר טכנולוגי ותפעולי בהיבטים רבים, החל מרמת הגדרת המטרות והמדיניות וכלה ברמת המימוש והשימוש. מתודות לפתרון האתגר צריכות לכלול איזון בין המרכיבים הבאים: היכולת לתמוך במספר גדול של ארגונים ולהוסיף אותם בקלות למיזם השיתוף (Scalability); היכולת לעשות שימוש במידע לאחר בדיקת מִתאם (קורלציה) וניתוחו קרוב לזמן אמת במטרה להפיק תועלת מרבית ממנו (Usability); מערך בקרות המבטיחות את קיום שלושת העקרונות הבאים: סודיות, שלמות וזמינות (Confidentiality, Integrity, Availability – CIA).[8] השלבים בבניית מערך לשיתוף מידע כוללים, בין היתר, הגדרת המטרות והמשתתפים, זכויות וחובות הארגונים החברים במיזם, ארכיטקטורה טכנולוגית, מודל אמון ובקרות ותהליכי עבודה.

שיתוף המידע בין ישויות שונות מחייב יצירת מערכת אמון ביניהן, כדי שניתן יהיה להבטיח כי המידע נכון ושלם וכי ניתן להפיק ממנו תועלת. זהו הבסיס האקדמי והתיאורטי לכל המודלים השימושיים והדוגמאות הנדונים במאמר. מרחב הדיון והפתרונות בנושא האמון משתרע בין רמת הרכיבים בתוך מוצר כמו

מחשב, דרך שילוב מוצרים שונים בתוך אותה מערכת, ועד לאמון בין מערכות שונות בארגונים שונים, כמו למשל מסחר באינטרנט. גופי תקינה, כגון Trusted Computing Group (TCG),[9] עוסקים במגוון היבטים של הנושא, אך שיתוף מידע סייבר הוא אתגר שהמודלים הקיימים לא סיפקו לו מענה שלם, ומכאן גם הצורך בחשיבה ותקינה נפרדות לנושא זה.

ניתן לזהות שלוש ארכיטקטורות עקרוניות לבניית תשתית שיתוף המידע,[10] שיש לבחור באחת מהן בשלב ייזום השיתוף. הארכיטקטורה הראשונה היא תפיסה של מרכז וקצוות (Hub and Spoke), המבוססת על אתר מרכזי המקבל את המידע מארגוני הקצה ומפיץ אותו לאחר היתוכו כשהוא מותאם לצרכנים השונים.[11] המרכז משמש כמסלקה המגֵנה על הפרטיות ועל הקניין הרוחני של כל ארגון, והיכולת לנתח בו כמות גדולה של מידע בצורה יעילה, מתאפשרת בין היתר בזכות ההתפתחות הטכנולוגית המואצת בתחום ה־Big Data. זו מאפשרת עיבוד וניתוח כמויות מידע גדולות ומהווה אבן יסוד בבניית יכולת להיתוך מידע ממקורות שונים. חסרונות המודל הם בעיקרם תוצר של התפיסה הריכוזית שלו: אתגרי גודל, תלות באתר המרכזי למבצעיות המערך, שיהוי בעיבוד המידע והפצתו ועוד.

הארכיטקטורה השנייה היא של פרסום לכל (Post to All), בה מתבצעת הפצה ישירה בין הארגונים. ארכיטקטורה זו מחייבת בהכרח תשתית ניתוח בארגונים, מכיוון שההפצה היא של מידע גולמי ולא של מידע לאחר היתוך. הארכיטקטורה השלישית משלבת בין שתי הקודמות, תוך ניצול היתרונות היחסיים בכל אחת מהן, אך במחיר מימוש מסובך ויקר יחסית.

מימוש השיתוף צריך להתבצע מבחינה טכנולוגית תוך שמירה על נכסי הארגון ופרטיותו, וזאת בשתי רמות: הראשונה היא שליטה על תוכן המידע המועבר (Information Control), המתבצעת בארגון עצמו כחלק מהגדרות האובייקטים אותם משתפים, וצריכה להיות מתוקננת בתסדיר (פורמט) מוסכם. חלק מהגדרות אלו נועדו להלבין את מקורות המידע כפי שקורה בעולם המודיעין, כך שלא ייחשפו פרטים שאינם הכרחיים אל מחוץ לארגון. הרמה השנייה היא הגבלת גישה למידע, הכוללת שליטה על מערך ההפצה שלו, לאן הוא מועבר ומי רואה אותו, וצריכה להתבסס על פרוטוקול שיתוף מתוקנן.

בחירה עקרונית נוספת שיש לבצע היא בין מודל שיתוף אוטומטי למודל שיתוף ידני. משמעות השיתוף הידני היא שגורם מורשה בארגון, בעל נגישות למערכת השיתופית, יזין ויקבל מידע אליה וממנה וישלוט בגישה למידע. למודל הידני חיסרון בולט – הגורם האנושי, המהווה חסם וצוואר בקבוק, בעיקר כאשר הארגון נמצא תחת מתקפה. חסרונות נוספים הם הקושי לשמור על עדכניות המידע לאורך זמן וחשיפתו לטעויות אנוש.

שיתוף אוטומטי מחייב להחליט תחילה על תסדיר אחיד ומנורמל של מידע, על מערכת חיישנים בארגון שתאסוף ותחלק אותו, על מערכת קבלת התרעות מקומית, ועל מימוש בקרות קפדני שנועד למנוע זליגת מידע שלא היה צריך להישלח. דרך זו מאפשרת להתגבר על המגבלות הקיימות בשיתוף הידני. יחד עם זאת, היא מחייבת התמודדות עם תרחישי התקפה אליהם חשוף מערך השיתוף האוטומטי, כמו הרעלת בסיס הנתונים השיתופי במידע כוזב (Database Poisoning).[12]

קיימות מספר פעילויות תקינה בסוגיה זו, אשר המתקדמת שבהן, שגם אומצה על ידי משרד ההגנה של ארצות הברית, כוללת תסדיר שיתוף מידע סייבר בשם Structured Threat Information eXpression (STIX™).[13] תסדיר זה מגדיר מבנה רשומה, ובה מידע הנוגע למשתמש ו/או תעבורה הנשלחת באופן יזום מהארגון אל ישות חיצונית או מישות חיצונית אל הארגון, כשהיא מכילה מגוון פרטים מובנים על אירוע אבטחה. תקינה נוספת הרלוונטית למיכון השיתוף קרויה Trusted Automated eXchange of Indicator Information (TAXII™),[14] והיא כוללת מבנה מסרים ופרוטוקולי רשת התומכים בהעברת מסרים מסוג STIX בין הישויות השונות. ישנם מספר פרוטוקולים משיקים נוספים, תחת ארכיטקטורת מעטפת הקרויה Cyber Observable Expression (CyBOX),[15] הנתמכים על ידי משרד ההגנה האמריקאי כחלק מהמאמץ למיכון השיתוף.

נראה כי מרבית המודלים התיאורטיים המוצעים באקדמיה,[16] או המודלים השימושיים המוצעים על ידי מכוני מחקר שונים,[17] מבוססים על מימוש אוטומטי, אֵמון וארכיטקטורת שיתוף של מרכז וקצוות. מאמצי התקינה שהוזכרו לעיל תואמים את רוח המודלים האקדמיים והשימושיים, כך שנראה כי יש קונצנזוס מבחינה טכנולוגית סביב הדרך הנכונה לבניית מערך כזה. ואכן, גופים משמעותיים כמו משרד ההגנה האמריקאי פועלים לקידום המיזמים על פי מתווה זה.[18] יחד עם זאת, הדרך למימוש שיתופי מידע אפקטיביים עדיין ארוכה, עקב ריבוי האתגרים הטכנולוגיים, העסקיים, התפעוליים, המשפטיים, ויש שיאמרו אף המוסריים, העומדים בפני מיזם השיתוף.

תועלות וסיכונים בשיתוף מידע

כדאיות השיתוף משתנה בהתאם למפת האינטרסים של הגופים המעורבים השונים. במקרה של ארגונים עסקיים, השיתוף מאפשר הגדלת רמת האבטחה וקיצור זמן התגובה להתקפה או לחיסון מפני התקפה עתידית אפשרית. זאת, באמצעות קבלת התראה מראש מהישות המרכזית ועזרה בזיהוי, ניתוח והתמודדות עם מתקפות. ניסוי שערך צוות חוקרים מדרום קוריאה מצא סימוכין להערכה זו.[19] השיתוף גם מאפשר את הקטנת הוצאות האבטחה של הארגון, וזאת

כתוצאה ממיקור חוץ, חלקי לפחות, של הניתוח והתגובה לצד שלישי. כמו כן, הארגון עשוי ליהנות מהקלות של הרגולטור כתוצאה מהגדלת השקיפות ועמידה בחובת הדיווח ובתנאים נוספים.

במקרה של מגזר יצרני הפתרונות והשירותים, מדובר בפלח שוק חדש, מוטה טכנולוגיה ובעל פוטנציאל גידול, היכול לבדל את עצמו באמצעות יצירת יתרונות תחרותיים בני קיימא. אחד השירותים העיקריים שמגזר זה יכול להציע הוא זיהוי דפוסי תקיפה אפשריים והפצת חיסונים והתראות לארגונים, וזאת על בסיס היתוך מידע של התקפות ומתקיפים שנאסף מהארגונים עצמם.

במרחב המדינתי, כדאי לגופי הרגולציה, הממשל והביון לעודד את מגמת השיתוף, מכיוון שבכך הם מגדילים את השקיפות של הארגונים, מקבלים תמונת מצב רחבה על זמינות השירותים ואמינות המידע, מבצעים אנליזות על פני רשתות וארגונים שונים לזיהוי דפוסי תקיפה שהתממשו או עלולים להתממש, ומאפשרים יכולת תגובה מהירה, תוך הפצת מידע לארגונים אחרים במטרה לחסן אותם. ניתן להניח כי לגוף הגנה מדינתי שזהו תחום עיסוקו יש יכולת גבוהה יותר מאשר לגופים פרטיים, לבנות כשירות טכנולוגית גבוהה של אנשיו ולשמור עליה, וכן את הרצון לשתף ארגונים אחרים במשאבים האנושיים והטכנולוגיים שברשותו. השיתוף הוא אינטרס לאומי מובהק, המאפשר לממשל להילחם את מלחמת הסייבר הלאומית ולהכות בפשיעה הקיברנטית באופן יעיל יותר, וכן ליצור שליטה בזמינותן של תשתיות לאומיות, ציבוריות ופרטיות קריטיות. דוגמה למימוש רגולציה בעלת תפיסה דומה, אך בתחום אחר, ניתן למצוא בהנחיות המשרד להגנת הסביבה בישראל בעניין פליטת מזהמים מתעשייה, המחייבות מפעלים בניטור ובדיווח רציפים ומקוונים של נתוני איכות האוויר בארובות ובמקורות מזהמים אחרים.[20]

על אף היתרונות שפורטו לעיל, ישנם מספר סיכונים הקשורים ישירות לשיתוף מידע סייבר בין ארגונים. ניתוח הסיכונים הללו צריך להתבצע במסגרת אסטרטגיית ניהול הסיכונים הארגונית, ולכלול את הסבירות של כל סיכון, את ההשפעה שלו, את הבקרות הנדרשות לשליטה בו ואת הדרכים לצמצם אותו. לדוגמה, הדרך להפחתת הסיכון לחשיפה משפטית לתביעות בגין גילוי מידע פרטי או עסקי, היא באמצעות חוקים ותקנות המעניקים הגנה משפטית של הממשל או הרגולטור. דוגמה נוספת היא הסיכון לאובדן נכסי מידע ארגוניים כתוצאה משיתוף לא מבוקר. הדרך להקטין סיכון זה היא באמצעות שימוש בתבנית שיתוף מובנית ומתוקננת שאינה כוללת מידע רגיש, וכן בבלמים נוספים, כמו הנחייה, רגולציה או חקיקה, שיחייבו את הארגון להסיר מידע פרטי או עסקי מהמידע שנועד לשיתוף לפני שליחתו.

הזדמנויות עסקיות

התפתחות איום הסייבר ושינוי תפיסת השיתוף של ארגונים מהווים הזדמנות עסקית ליצרני פתרונות טכנולוגיים, לגופי אינטגרציה ולספקי שירותים, שיכולים למנף את בסיס המוצרים, הידע והשירותים שלהם כדי ליצור ערכים מוספים סביב אתגר השיתוף.

אחת הדוגמאות להזדמנות כזאת נוגעת לאתגרים שמעמידות טכנולוגיות התקפה חדשניות, כמו התקפה מתוחכמת ועקבית (Advanced Persistent Threat – APT),[21] או ניצול פרצות אבטחה שאינן ידועות או שלא סופק להן עדיין פתרון. שתי הטכנולוגיות ההתקפיות הללו מורידות מיעילותם של מנגנוני ההגנה המסורתיים,[22] אך ניתן לפצות על כך, במידה מסוימת, באמצעות שירות אבטחה שיתופי בין־ארגוני. שיתוף כזה מאפשר זיהוי אנומליה בענן והשוואה של אירועים ארגוניים לא רק אל מול בסיס ההתנהגות באותו ארגון, אלא גם אל מול ארגונים דומים אחרים, ובכך הוא מחדד את מנגנון הזיהוי ומקטין את הסיכון שתעבורה תקינה תזוהה בטעות כחריגה. בנוסף לכך, לאחר זיהוי התקפה או תוקף בארגון מסוים, ניתן להפיץ את מרכיבי הזיהוי או את החיסון ליתר הארגונים, ובכך למנוע התקפה דומה אצלם.

מספר יצרני מערכות אבטחה מספקים פתרון לשיתוף מידע סייבר המבוסס על תשתית איסוף מידע מבוזרת, וזאת באמצעות מערך מבחנים (Probes) המשמשים לעיתים גם כ"מלכודות דבש" למתקיפים. אלה מותקנים בארגונים ואצל לקוחות קצה או בצמתים מרכזיים באינטרנט השייכים ליצרן. תשתית זו אוספת מידע בזמן אמת על התקפות ותוקפים, בחתכים של מיקום גיאוגרפי וסוג ההתקפה, ומפיצה אותו כשירות לארגונים החברים בשיתוף. המערכת מהווה בסיס נתונים מבוסס שיתוף בענן על תוקפים ו/או התקפות, ולעיתים אף כוללת רכיב של סינון וחסימה המתבסס על המידע המתעדכן באופן דינמי.

במקרה של ספקיות שירותי תקשורת ואחסון על גבי תשתית ענן, השיתוף מהווה הזדמנות להקטין את שיעור העזיבה של לקוחותיהן, וזאת באמצעות מתן עוד רובד אבטחה כערך מוסף.[23] הפתרון באמצעות ענן המשותף לכל הארגונים המתארחים מאפשר לספק השירותים, לאחר שזיהה התקפה בארגון אחד ועצר אותה, לטייב את מדיניות האבטחה עבור יתר הארגונים במטרה למנוע את הישנותה.

הזדמנות עסקית נוספת הקשורה ישירות למיזמי שיתוף היא בניית פתרון לאיסוף, ניתוח והפצה של מידע סייבר ברמה לאומית או מגזרית. למספר חברות אינטגרציה בעולם יש פתרון כולל ליצירת תמונת מצב, ניתוח אירועים, הפצת חיסונים, סימולטור אימונים ורכיבים נוספים, כמקובל במערכות צבאיות וציבוריות גדולות. כמו כן, יש יצרניות של פתרונות בצורת האזנה וניתוח מעמיק של התעבורה

(Deep Packet Inspection), המאפשרים לספקיות שירותי התקשורת לשתף מידע באופן סלקטיבי עם רשויות החוק, כדי שאלו יוכלו להאזין לרשתות הטלפוניה והאינטרנט ולדלות מתוכן איומים. חלק מהחברות הללו אף מספקות את רכיב הפתרון שאחראי לניתוח המידע, המבוסס על לוגיקה חכמה וכולל אנליזה לכמות עצומה של מידע הנאסף ממקומות שונים, חקר אנומליות וקורלציות בין אירועים.

ניתן להניח כי גל החדשנות הטכנולוגית בעולם של פתרונות ההגנה יימשך, מתוך צורך להתאים את מערכי ההגנה לאיומי הסייבר הקיימים והמתהווים. בנוסף ניתן להניח כי רעיון השיתוף, התופס מקום גדל והולך במדיניות ההגנה של ארגוני מפתח, ימשיך להוות הזדמנות עסקית לגורמים המסחריים הפועלים בתחום זה.

היבטי רגולציה ופרטיות

ישנם תחומים בהם הרגולטור ו/או החוק מחייבים כבר היום שיתוף מידע הנוגע לסיכוני סייבר ולאירועי סייבר, ונראה כי מגמה זאת הולכת ומתעצמת. זאת, נוכח הצורך של ממשלות להקים מערך הגנה לאומי ללחימה בפשיעה הקיברנטית, וכן ליצור שקיפות של אירועי סייבר בחברות ציבוריות או במגזרי שוק אסטרטגיים, כגון תקשורת, פיננסים ובריאות. כמו כן, רגולציות שונות, כגון בזל III ו־ISO-27032, מעודדות את שיתוף המידע בין הארגונים לרשויות, הן באמצעות הנחייה והן באמצעות הצעת תועלות והקלות כלכליות לארגונים המשתפים פעולה בנושא זה. מאמר המנתח את שקלול התמורות בין השקעות באבטחת מידע בגופים פיננסיים ובין שיתוף מידע סייבר,[24] מגיע למסקנה כי כדאיות השיתוף בין ארגונים גוברת ככל שיש תלות הדדית ביניהם, וכי ככל שהשיתוף בין גופים אלה גדל, כך קטנה ההשקעה שהם צריכים להשקיע באבטחת מידע. בשווקים מגזריים רבים (פיננסים וטלקומוניקציה למשל), הקישור בין הארגונים חיוני לתפקודם השוטף, ופגיעה בארגון אחד עלולה לפגוע בקלות גם בתפקודו של ארגון אחר. דוגמה לכך ניתן לראות בביצוע העברה פיננסית בין בנקים או בשיחת טלפון העוברת בין רשתות השייכות למפעילים שונים.

ארגונים דומים חולקים גם אתגרים משותפים, ולעיתים כאלה הייחודיים להם. לדוגמה, לארגוני הבריאות אתגר ייחודי של התמודדות עם התקפות סייבר על ציוד רפואי. שיתוף בין ארגונים אלה באיסוף מודיעין או בנוהלי הקשחה של ציוד כזה, יחסוך השקעות שכל אחד מהארגונים היה צריך לבצע בנפרד.

מספר מדינות חשפו את כוונתן להקים מערכי סייבר לאיסוף מידע, הכולל שילוב של גופים ממשלתיים וגופים פרטיים/ציבוריים בעלי חשיבות לאומית.[25] מהות המהלך היא יצירה של תמונת מצב סייבר כוללת, יכולת למתן מענה בכוח אדם איכותי במקרה של מתקפה, וכמובן הפצה מיידית של חיסון או מידע על מתקפה לכל הארגונים הכפופים. כאמור, הבסיס הטכנולוגי ליצירת מערך כזה

עשוי לחייב חקיקה ומצריך שיתוף מידע סייבר בין הארגונים, הקמת מרכז המשמש להיתוך המידע ויישום מנגנוני שמירה על נכסים ארגוניים ועל פרטיות.

ממשלת בריטניה הקימה מיזם שיתוף בשם Cyber Security Information Sharing Partnership (CISP), כחלק מתוכנית לאומית להתמודדות עם אתגרי הסייבר.[26] המיזם כולל כבר כיום יותר מ־250 ארגוני מפתח, וכן את רשויות החוק, ומטרתו היא להגדיל את היכולת להתמודד עם טרור ופשיעה קיברנטיים. בארצות הברית פועלים מתחילת שנות האלפיים מיזמים לשיתוף מגזרי בתחומים שונים, כגון בריאות, פיננסים ועוד, הנקראים Information Sharing and Analysis Centers (ISAC). רוב המיזמים הללו פועלים בבעלות ובמימון הארגונים החברים בהם, אך לאחרונה הם זוכים לגב טכנולוגי ואף מימוני של משרד ההגנה של ארצות הברית, המכיר באינטרס של הממשל להיות מעורב בנושא. דוגמאות למעורבות כזו הן מתן גישה למרכז התגובה הממשלתי להתקפות סייבר (US-CERT)[27] והקמת מיזם אב שמטרתו לאחד את המידע הבין־מגזרי בארצות הברית למארג אחיד.[28]

גם בישראל הוקם זה מכבר גוף ביטחוני בשם הרשות הממלכתית לאבטחת מידע, המופקד על הנחיה מקצועית של הגופים האזרחיים שתחת אחריותו בתחום אבטחת תשתיות מחשב חיוניות מפני איומי טרור וחבלה, אבטחת מידע מסווג והתגוננות מפני איומי ריגול וחשיפת מידע. כמו כן, פועל בישראל מטה הסייבר הלאומי, שבין יתר תפקידיו פועל לגבש יוזמות להקמת מרכזי שיתוף מגזריים בתחומים שונים, כמו אנרגיה, פיננסים ובריאות, ולהקמת מרכז לאומי לתגובה לאירועי סייבר.

ברור כי לחימה בפשיעה או בטרור קיברנטיים, שמטבעם חוצים גבולות גיאוגרפיים ופוליטיים, ניתנת לביצוע רק באמצעות שיתופי פעולה טכנולוגיים ומשפטיים בין מדינות. מיזם אחד כזה הוא תוכנית לשיתוף פעולה מחקרי בתחום הסייבר שניזומה על ידי נאט"ו והאיחוד האירופי.[29] מיזם נוסף הוא תשתית שיתוף המוקמת בנאט"ו, ומתאפיינת באוטומציה של המידע על בסיס STIX, מתוך מטרה לאפשר שיתוף בין ארגונים שונים במדינות החברות בברית.[30] בהיבט המשפטי, נוסחה ונחתמה אמנת בודפשט שנועדה לתאם בין מערכות החקיקה של המדינות החברות באיחוד האירופי, לשפר את שיטות החקירה המשולבת ולהגביר את שיתוף הפעולה בהתמודדות עם פשעי מחשב.

מאמר הסוקר שיתוף פעולה בין־לאומי בהגנה על תשתיות קריטיות מפני התקפות סייבר[31] מאשש את הסברה כי סיכויי ההצלחה של מיזם שיתוף המידע גוברים גם במישור הבין־לאומי, אם הישויות החברות הן בעלות אינטרסים ותפיסות תרבותיות ופוליטיות דומות. שיתוף מידע בין גופים שונים מהווה מטבעו אתגר בהיבט השמירה על סודיות, מכיוון שהוא מחייב הגדרה של גבולות השיתוף ובקרות שיוכלו להבחין בין מידע פרטי או פנים ארגוני ובין מידע שניתן לשתף בו.

במהלך השנים זוכות ממשלות לשיתוף פעולה שקט, הנאכף לעיתים בחקיקה, מצד ספקי שירותים, תשתיות ואפליקציה, וזאת הן לצורכי ביטחון לאומי והן לצורכי לחימה בפשיעה. התופעה הולכת ונחשפת בתקופה האחרונה, במיוחד לאחר שה"גארדיאן" הבריטי פרסם, על בסיס הדלפה של אדוארד סנודן, כי ה־NSA האמריקאי מאזין לתעבורה של חברות אמריקאיות מובילות, במסגרת תוכנית בשם PRISM.[32] בנוסף חשף העיתון כי גוף המודיעין הבריטי המקביל ל־NSA מנטר את תעבורת האינטרנט על גבי תשתיות הסיבים האופטיים בממלכה,[33] וכי סוכנות הביון הפנימית בבריטניה, MI5, מתכוונת לפרוס אמצעים טכנולוגיים המאפשרים ביצוע סינון למילות מפתח ולמידע נקודתי בכל תעבורת המידע במדינה.[34]

חשיפת המידע על תוכניות ההאזנה של ארצות הברית העלתה לכותרות שם את נושא ההגנה על הפרטיות וגבולות הכוח של הממשל בהתנהלותו מול האזרח, וכן את האפשרות להטלת סנקציות משפטיות על הגורמים המשתפים מידע. עד כה דחה בית המשפט העליון בארצות הברית תביעות נגד ענקיות הטלקום המקומיות ואשרר את חוקיות העברת המידע האינטרנטי ושיחות טלפון לרשויות הביון והחוק.[35] עם זאת, האפשרות לתביעה נגד ארגון המשתף מידע מהווה חסם לשיתוף, ואותו מעוניין הממשל להסיר.

החל מסוף שנת 2011 מקודמת בארצות הברית חקיקה העוסקת בשיתוף מידע בתחום הסייבר,[36] שמטרתה לאפשר לחברות פרטיות וציבוריות לשתף מידע בזמן אמת עם הממשל ועם ארגוני ביון ואכיפת החוק, אם יבחרו בכך וכחלק ממלחמת הסייבר, וזאת מבלי להסתכן בתביעות משפטיות על הפרת סודיות או פרטיות. הצעת החוק עברה בבית הנבחרים, הועברה לסנאט ומשם להתאמות בוועדה לענייני מודיעין,[37] והיא נמצאת עדיין בתהליך החקיקה. המתנגדים לחוק טוענים כי הוא מפר את התיקון הרביעי לחוקה,[38] הקובע תנאי סף לחיפוש ולקבלת מידע פרטי על אזרח, כמו למשל צו שופט וסיבה מוצדקת לחיפוש. לדבריהם, החקיקה תאפשר לרשויות הביון לקבל מידע פרטי או עסקי מספקיות תשתית ותוכן ללא הבלמים המופיעים בתיקון לחוקה. גם ברשתות החברתיות ובמרחבי האינטרנט בארצות הברית קיימות התארגנויות העוסקות בבעייתיות של החוק המוצע[39] ומנסות לגייס את הציבור להתנגד לו ולמנוע את אישורו הסופי.

המתח בין התומכים בחקיקה לשיתוף מידע סייבר ובין המתנגדים לה אינו ייחודי רק לתחום זה, אלא נוגע לכל נושא הפרטיות בממשק שבין המדינה לאזרחיה ולמידת המעורבות של "האח הגדול" בחייהם. דוגמאות לעימות דומה הן מיזם המאגר הביומטרי של ממשלת ישראל הנתקל בביקורת רבה, ומיזם העיר החכמה של בריטניה, הכולל רישות העיר במצלמות ותוכנות לזיהוי פנים.

תובנות לסיכום

המגמות בהתפתחות איום הסייבר העכשווי כוללות שימוש במתודולוגיית תקיפה מכוונת מטרה ולא רק אקראית, דילוג על פני גבולות גיאוגרפיים ומשפטיים, ניצול פרצות אבטחה שאינן ידועות ושימוש בפיסות קוד מודולרי עוין במרחב הקיברנטי. הצד התוקף מתַחזק קהילה משגשגת, בעלת מבנה, סדר פנימי ומערכת פיננסית תומכת, המאפשרים שיתוף קל ומהיר של מידע התקפי. נראה כי מימוש מודלים של קהילה גם בצד ההגנתי, ומעבר מפרדיגמת הארגון המבודד למיזם של שיתוף מידע, יובילו לתוצאות טובות יותר גם בתחום המגננה מפני התקפות סייבר. בראייה רחבה יותר, אחד המשאבים המשמעותיים ביותר המתהווים במאה ה־21 הוא חוכמת ההמונים והקהילה (The wisdom of crowds). ניתן לראות דוגמאות לכוחה של חשיבה משותפת בתחומים רבים, ותחום הסייבר אינו יוצא דופן בהיבט זה.

המעבר למודלים של שיתוף נתמך על ידי אחדות אינטרסים של מרבית כוחות השוק המעורבים, ובהם גופי הרגולציה, הממשל, רשויות החוק והביון, יצרני הפתרונות והשירותים, ואף הארגונים עצמם. כדאיות השיתוף עם גורמי חוץ היא, בין היתר, תוצר של חוסר היכולת של הארגון הבודד להילחם את מלחמת הסייבר לבדו. היא תורמת לא רק לחיזוק משמעותי של מערך האבטחה והשרידות שלו, אלא גם להצלחתו העסקית, עקב חיסכון בהשקעות, תעדוף על ידי הרגולטור ועוד.

ארכיטקטורות הפתרון והתקנים המתפתחים יאפשרו ליצור בעתיד מעטפת טכנולוגית לקישור בין ארגונים, תוך שמירה על נכסי הארגון. הם גם יתמכו בקישור בין מימושים נפרדים של שיתוף, שיוכלו להתחבר אחד לשני לכדי מארג היררכי של מידע, כמו למשל שיתוף בתוך שוק מגזרי שיתממשק לשיתוף ברמה הלאומית.

חלק מהצלחת כל תהליך של תקינה תלוי בכוחות השוק התומכים בו. במקרה זה נראה כי גורמי הממשל בארצות הברית, ובראשם משרד ההגנה, מקדמים את התהליך בנחישות. עם זאת, לא נראים עדיין מימושי שיתוף מידע אפקטיביים בקנה מידה גדול, וזאת עקב ריבוי אתגרים שאינם בהכרח טכנולוגיים, ולעיתים גם גישה שמרנית של מקבלי ההחלטות בארגונים.

עם הבשלת התחום, אנו צפויים לראות תחילה שיתופים בין גופים דומים באותו המגזר, ובהמשך – מימוש שיתופי מידע בקנה מידה גדול יותר. אחדות אינטרסים, תרבות ארגונית דומה ויחסי תלות בין ארגונים מגדילים את סיכויי ההצלחה של המיזם ומפחיתים מהסיכונים שבו.

שניים מהחסמים הבולטים לשיתוף הם החשש של ארגונים מפני קישור מערכות שעלול לחשוף מידע פנים ארגוני רגיש לגופים מתחרים, והחשש מפני קבלת מידע סייבר לא תקין עקב הרעלת בסיס הנתונים המשותף, דבר העלול לגרום לפגיעה בשירות. ניתן להקטין את הסיכון בשני החסמים באופן משמעותי

באמצעים טכנולוגיים ובתקינת תהליכים ופרוטוקולים שימומשו בישות השיתוף המרכזית.

האתגר הגדול יותר ניצב בפני ארגונים שהמהות העסקית שלהם נוגעת לנושא הסייבר, כמו יצרני פתרונות אבטחה, מוצרי ושירותי תוכנה או גופי הפרויקטים והאינטגרציה הגדולים בתחום זה. השאלה היא האם ניתן לגבש מודל עבודה כדאי בין יצרנים אלה, כך שישתפו ביניהם מידע סייבר, וזאת למרות שנושא האבטחה והסייבר הוא חלק מהתחום בו הם מתחרים. מודל כזה יצטרך לכלול בהכרח שילוב יסודות הן של תחרות והן של שיתוף פעולה (Coopetition), באופן שיספק יתרונות לכל אחד משותפי המיזם לאורך זמן.

הוויכוח בין התומכים ובין המתנגדים לשיתוף מידע ולפעילות החקיקה המאפשרת אותו עדיין נמשך. לאור זאת, ולאור כל היבטי הנושא שנדונו במאמר, השאלה שצריכה להישאל היא האם ישנה פרדיגמה אחרת בעולם טכנולוגיות המידע שתאפשר את ההתמודדות עם אתגרי הסייבר הנוכחיים והעתידיים ללא צורך בשיתוף, או שאין ברירה אלא לשלב כוחות במאבק ולאמץ בהקדם תקינה אחידה לתשתית שיתופית. בכל מקרה, תשתית כזו תצטרך לשמור ככל שניתן על האיזון בין זכויות הפרט ובין יכולת המדינה להגן על תשתיותיה, נכסיה ואזרחיה.

הערות

1 Zero Day Attack הוא ניצול של פרצת אבטחה ברכיב המותקף, שאינה ידועה ליצרן הרכיב או לכל גוף אחר מלבד הגורם המתקיף עצמו, או שידועה ליצרן ועדיין לא הופץ עבורה טלאי תוכנה (Patch).

2 אחד המחקרים שנערכו בשנה האחרונה בנושא זה על ידי מכון RAND מספק ניתוח של האופן בו "השווקים השחורים" של עולם הסייבר בנויים ומתפקדים, סוקר מגמות היסטוריות ומספק תחזיות לעתיד. חוקרי המכון ערכו ראיונות עומק עם מומחים המעורבים באופן רשמי או אחר בשווקים אלה, בהם אנשי אקדמיה, חוקרי אבטחה, עיתונאים, ספקי אבטחה וגורמי אכיפת החוק. הדו"ח מגיע למסקנה כי "השווקים השחורים" בסייבר מהווים ענף כלכלי של מיליארדי דולרים, עם תשתית איתנה ומבנה חברתי וארגוני ברור. ראו:
L. Ablon, M.C. Libicki, A.A. Golay, *Markets for Cybercrime Tools and Stolen Data*, RAND Corporation, 2014, http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf.

3 הגישה הדוגלת במידור מידע סייבר מתוארת במקורות רבים כחלק מהיערכות הארגון מול אירוע אבטחתי. דוגמה לכך הוא מודל ההיערכות המוצע של SANS, מתוך קורס העוסק בנושא. ראו: SANS, SEC504: Hacker Techniques, Exploits & Incident Handling, 2014.

4 L.A. Gordon, M.P. Loeb and W. Lucyshyn, "Sharing Information on Computer Systems Security: An Economic Analysis", *Journal of Accounting & Public Policy*, Vol. 22, No. 6, November-December 2003, pp. 461-485.

5 באזל III היא רגולציה בתחום הפיננסים, הכוללת עקרון שקיפות מול הרגולטור המחייב ארגונים פיננסיים לשתף סיכונים תפעוליים ואירועי סייבר. לפרטים נוספים ראו:
Basel III: A Global Regulatory Framework for more Resilient Banks and Banking Systems, http://www.bis.org/publ/bcbs189.pdf.

6 הוראת ניהול בנקאי תקין 206 של בנק ישראל מ־9 ביולי 2012, דנה בין היתר בקשר שבין רמת הסיכון התפעולי להלימות ההון של הבנק. ראו: http://www.bankisrael.gov.il/he/BankingSupervision/LettersAndCircularsSupervisorOfBanks/HozSup/h2341.pdf

7 תקינה הכוללת הנחיות הגנה בסייבר, וביניהן דרישה לשיתוף מידע בין ארגונים. ראו:
Information Technology – Security Techniques – ISO/IEC 27032:2012 Guidelines for Cybersecurity, July 16, 2012, http://www.iso.org/iso/catalogue_detail?csnumber=44375.

8 שלושת יסודות ה־CIA מהווים את עקרונות הבסיס הקלאסיים של אבטחת המידע: סודיות (Confidentiality) – שמירה על תוכן המידע מפני קריאה של גורם לא מורשה; אמינות ושלמות (Integrity) – שמירה על המידע כך שלא ישונה על ידי גורם לא מורשה; וזמינות (Availability) – שמירה על זמינות המידע והמערכות.

9 אתר ארגון TCG ראו: http://www.trustedcomputinggroup.org/

10 *Cyber Information-sharing Models: An Overview*, MITRE, October 2012, http://www.mitre.org/sites/default/files/pdf/cyber_info_sharing.pdf.

11 לפי ויקיפדיה, היתוך מידע הוא תהליך שמטרתו לקשר בין נתונים (Data), מידע (Information) וידע, (Knowledge) לחברם ולהצליבם ולמצוא קורלציה ביניהם, וזאת לצורך שיפור היכולת להעריך נתוני מיקום וזיהוי של ישויות עליהן מבצעים איסוף, וכן לצורך יצירת תמונת מצב והערכת איומים ורמת החשיבות שלהם. בנוסף, מתבצעת הערכה של איכות התוצרים ונוצרות דרישות ממקורות המידע, כחלק בלתי נפרד מתהליך היתוך המידע ובמטרה לשפר את תוצריו.

12 הרעלת בסיס הנתונים במידע כוזב עלולה להוביל ארגון הנחשף אליה לחסימת הפעילות שלו, פנימית או מול גופים אחרים (Denial Of Service). יתרונו של מערך שיתוף אוטומטי הוא גם חסרונו הגדול, והוא חשוף יותר ממערך שיתוף ידני להרעלה כזו, מכיוון שאינו כולל בקרה אנושית בזמן אמת.

13 S. Barnum, *Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™)*, February 2014, http://stix.mitre.org/about/documents/STIX_Whitepaper_v1.1.pdf.

14 M. Davidson, C. Schmidt, *TAXII Overview*, version 1.1, January 2014, http://taxii.mitre.org/specifications/version1.1/TAXII_Overview.pdf.

15 *CybOX – Cyber Observable eXpression – A Structured Language for Cyber Observables*, 2014, http://cybox.mitre.org/.

16 דוגמה לארכיטקטורת שיתוף עקרונית המתייחסת לנושא האמון במסגרת מחקר אקדמי היא ארכיטקטורה בשם PEI שהוצעה על ידי Krishnan ואחרים, וכוללת שלוש שכבות הכרחיות: שכבת המדיניות (Policy), המפרטת את מטרות השיתוף והגדרות האובייקטים, שכבת האכיפה (Enforcement), הכוללת את ארכיטקטורת הפתרון העקרונית, ולבסוף שכבת המימוש (Implementation), הכוללת ירידה לרמה הטכנולוגית של פרטי השיתוף. ראו:
R. Krishnan, R. Sandhu, K. Ranganathan, *PEI Models towards Scalable, Usable and High-Assurance Information Sharing*, **ACM**, New York, NY, USA, 2007, pp. 145-150.

17 מכון המחקר MITRE, הפועל במימון פדרלי, מפרט את אבני הדרך וההחלטות שצריכות להתקבל כחלק מתהליך בניית השיתוף. בין היתר נדרשות החלטות לגבי ארכיטקטורת השיתוף, מודל האמון בין הגופים, מיכון השיתוף, תפעול וחברות במיזם. ראו:
B. Bakis, *Cyber Partnership Blueprint: An Outline*, MITRE, October 2013, http://www.mitre.org/sites/default/files/publications/Bakis_Partnership_Blueprint_Outline_0.pdf;
מכון המחקר האמריקאי Bipartisan Policy Center פרסם מודל, בו גוף מרכזי משמש כמסלקה (Clearance Center) למידע המשותף לגופי התשתיות הקריטיות בארצות הברית. ראו:
Cyber Security Task Force: Public-Private Information Sharing, Bipartisan Policy Center (BPC), July 2012, http://bipartisanpolicy.org/sites/default/files/Public-Private%20Information%20Sharing.pdf.

18 המגזין Federal Blue Print מתאר את התקנים הטכנולוגיים למימוש שיתוף, אותם מקדם משרד ההגנה האמריקאי. ראו:
A. Merchant-Dest, *How the Department of Defense and the Department of Homeland Security are Taking Steps toward Information Sharing*, Federal Blue Print March 2014, http://federalblueprint.com/latest-news/department-defense-department-homeland-security-taking-steps-toward-information-sharing/.

19 צוות החוקרים מדרום קוריאה מוכיח, באמצעות ניסוי שערך, כי שיתוף המידע בין גופים שונים (Zones) מקצר את זמן התגובה להתקפה ומגדיל את רמת האבטחה. ראו:
B. Chang, D. Kim, H. Kim, J. Na, T. Chung, *Active Security Management Based on Secure Zone Cooperation*, Future Generation Computer System, 2004, 20(2), p. 283.

20 המשרד לאיכות הסביבה, **נהלים והנחיות לעניין פליטת מזהמים מתעשייה**, http://www.sviva.gov.il/subjectsEnv/SvivaAir/Industry/Pages/Regulations.aspx.

21 APT הוא מערך כלי התקפה בעולם הסייבר המכוון כלפי יעד ספציפי ומופעל על ידי האקרים מקצועיים, ולפיכך ניתן לפיתוח ולתפעול באופן שיקשה מאד על זיהויו בכלי הגנה סטנדרטיים.

22 שתי הטכנולוגיות ההתקפיות הללו מורידות מיעילות מנגנוני הגנה מסורתיים, שעיקרם זיהוי תבניות התקפה ברורות. הן מחייבות התייחסות מבוססת ניסיון כדי לזהות את האיום, ומעבר מפיתוח מוצרי אבטחה מבוססי חתימה (Signature Based) למוצרים מבוססי אנומליה בהתנהגות (Behavior Based Anomaly). שניים מהאתגרים העיקריים במוצרים מבוססי אנומליה הם הצורך ליצור בסיס התנהגותי ארגוני שמתעד את ההתנהגות הנורמלית של הארגון ומערכות המחשוב שלו במטרה לזהות חריגה מהתנהגות זו, והסכנה של הפרעה לתנועה לגיטימית עקב טעות בזיהוי.

23 נקרא גם שירות אבטחה מנוהל על ידי ספק השירותים (Managed Security Service Provider – MSSP).

24 K. Hausken, "Information Sharing among Firms and Cyber Attacks", *Journal of Accounting and Public Policy*, Vol. 26, No, 6, 2007, pp. 639-688.

25 דוגמה לאסטרטגיה של מדינה בהקמת מערך סייבר לאומי ניתן למצוא במסמך של ממשלת פינלנד הכולל, בין השאר, חזון ועקרונות לבניית מערך סייבר לאומי חוצה ארגונים ושורה של המלצות קונקרטיות לצעדים בכיוון זה. ראו:
Finland Cyber Security Strategy, Secretariat of the Security Committee, 2013, http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf.

26 תוכנית לאומית של ממשלת בריטניה להתמודדות עם איומי הסייבר:

The National Cyber Security Strategy, Our Forward Plans – December 2013, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/265386/The_National_Cyber_Security_Strategy_Our_Forward_Plans_December_2013.pdf

27 אתר מרכז התגובה האמריקאי להתקפות סייבר:
US-CERT – United States Computer Emergency Readiness Team, http://www.us-cert.gov

28 אתר מיזם השיתוף הבין־מגזרי בארצות הברית:
National Council of ISACs, http://www.isaccouncil.org/memberisacs.html

29 *The Multinational Cyber Defense Capability Development (MNCD2) Program*, http://mncd2.ncia.nato.int/Pages/default.aspx

30 *The Cyber Security Data Exchange and Collaboration Infrastructure (CDXI)*; L. Dandurand, *Cyber Security Information Exchange*, http://www.rsaconference.com/writable/presentations/file_upload/sect-t08-cyber-security-information-exchange.pdf

31 L. Tabanski, "International Cooperation in Critical Infrastructure Protection against Cyber Threats", *Atlantic Voices*, Vol. 2, No. 9, September 2012, http://sectech.tau.ac.il/node/114

32 המדובר בפעילות מעקב אלקטרונית של ה־NSA, שהושקה בשנת 2007, לאיסוף מידע לצורכי מודיעין, בין היתר מספקיות תשתית, תוכנה ותוכן, כמו Google, Yahoo, Microsoft, Apple, Skype, AOL. הפעילות נחשפה בהדלפה של אדוארד סנודן ל"גארדיאן" בשנת 2013.

33 E. MacAskill, J. Borger, N. Hopkins, N. Davies, J. Ball, "How does GCHQ's Internet Surveillance Work?", *The Guardian*, June 21, 2013, http://www.theguardian.com/uk/2013/jun/21/how-does-gchq-internet-surveillance-work

34 טכנולוגיית הניטור המאפשרת סינון מילות מפתח מתעבורת האינטרנט נקראת Deep Packet Inspection.

35 בית המשפט העליון בארצות הברית דחה תביעה נגד ענקיות הטלקום AT&T, Verizon ו־Sprint, ואשרר את החוקיות של העברת מידע מדוא"ל ומשיחות ל־NSA;
B. Kendall, "High Court lets Telecom Firms Wiretap Immunity Stand", *Wall Street Journal*, October 9, 2012, http://online.wsj.com/news/articles/SB10000872396390444024204578046312896501562

36 *Cyber Intelligence Sharing and Protection Act of 2013*, The Permanent Select Committee on Intelligence, 2013, http://intelligence.house.gov/bill/cyber-intelligence-sharing-and-protection-act-2013

37 *Cybersecurity Information Sharing Act of 2014*. עדכון שוטף על מצב החקיקה ניתן למצוא בספריית הקונגרס: http://thomas.loc.gov/home/thomas.php

38 Fourth Amendment: "The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized".

39 שניים מהגופים הפעילים בנושא זה הם הארגון להגנה על זכויות בעידן הדיגיטלי Electronic Frontier Foundation (EFF) וארגון בשם Fight for the Future – שניהם מריצים מערכה בשם CISPA Is Back להחתמת אזרחים על עצומה נגד החקיקה. ראו: http://www.cispaisback.org/; https://www.eff.org/cyberspying