חשיפת המשק הישראלי לריגול סייבר עסקי

שחר ארגמן וגבי סיבוני

מרחב הסייבר מתאים במיוחד לגניבת מידע עסקי ולריגול. הנגישות למידע לצד היכולת לשמור על אנונימיות, תוך טשטוש עקבות, מאפשר לגורמים שונים לעסוק בגניבת מידע בעל ערך, שנזקה עלול להיות רב. תופעה זו רלוונטית מאוד גם למדינת ישראל, החשופה במידה ניכרת לאיומי הסייבר בשל היותה עתירת טכנולוגיה מתקדמת כשחלקה של התעשייה מבוססת החדשנות והנשענת על קניין רוחני ייחודי, הוא רב מאוד. המאמר בוחן את היקף התופעה בעולם תוך נסיון לאמוד את היקף נזקיה הכספיים במדינות העולם ואף בישראל במסגרת הבהרת המורכבות של אומדנים אלה. מחברי המאמר מנסים להעלות את המודעות של הגורמים הרלוונטיים בישראל ובעולם להיקף התופעה תוך נסיון לתת המלצות באשר לכיווני ההתמודדות איתה.

מילות מפתח: סייבר, ריגול, ריגול עסקי, קניין רוחני, פשיעת סייבר, גניבת סייבר, טכנולוגיה

"There are two types of companies: companies that have been breached and companies that don't know they've been breached [...] the vast majority of companies have been breached"
Shawn Henry[1]

"The price tag for intellectual property theft from U.S. companies is at least $250 billion a year [...] it's the greatest transfer of wealth in history"
Gen. Keith B. Alexander[2]

שחר ארגמן הוא ראש אגף במטה הסייבר הלאומי.
אל"ם (מיל') ד"ר גבי סיבוני הוא ראש תוכנית צבא ואסטרטגיה וראש תוכנית לוחמת סייבר במכון למחקרי ביטחון לאומי.

רקע

המרחב הקיברנטי הוא תולדה של ההתפתחות הטכנולוגית המואצת בעשורים האחרונים. תחילה חוברו להן יחדיו מערכות תקשורת ומערכות ממוחשבות שפעלו כרשתות מקומיות. לאחר מכן חוברו הרשתות אלו לאלו לכדי מרחב פעולה והוויה גלובלי. מאז הולך המרחב הקיברנטי ומתפתח במספר מישורים: בעושר אמצעי המחשוב המקושרים ביניהם, במספר הרשתות ובסוגיהן, בנפחי התעבורה של המידע, ברמת הקישוריות, במגוון היישומים ובמידת התלות הכלכלית והחברתית בו.

בד בבד עם היתרונות העצומים הגלומים במרחב הסייבר, טומן מרחב זה בחובו איומים חדשים וחמורים, ההופכים אותו לתווך חדש לפעילות עוינת. פעילות כזו עלולה להתבטא הן בפגיעה בידע ובתפקוד בתוך מרחב הסייבר והן בפגיעה במרחב הפיזי דרך מרחב הסייבר.[3] לצד התרחבות השימוש הכולל במרחב הסייבר, גם הפעילות העוינת המתקיימת בו נמצאת בעלייה מתמדת.[4] מגוון האיומים בסייבר הוא רחב ביותר.

הוא כולל מניעת שירות, השחתת אתרים, חשיפת פרטים לצורך הפחדה והשפעה, פשיעה מסוגים שונים, ריגול מסחרי וביטחוני ופגיעה בתשתיות לאומיות אסטרטגיות, במאגרי מידע, במערכות שליטה ובקרה ואף במערכות נשק.

מרחב הסייבר מהווה, מעצם טבעו, ממד מתאים במיוחד לפעילות ריגול בכלל ולריגול עסקי בפרט. ריגול בין חברות מסחריות אינו תופעה חדשה, אולם השימוש במרחב הסייבר מאפשר יצירת נגישות למידע רב באופן פשוט יותר, תוך שמירה על חשאיות ברמה טובה. הנזק כתוצאה מריגול עסקי קיבל בימינו ממדים חדשים ומאיימים כתוצאה מהתאמתו האופטימלית של מרחב הסייבר לפעילות מסוג זה. מרחב הסייבר הפך לתווך מרכזי לביצוע פעולות ריגול גם בשל העובדה שגופי מודיעין מדינתיים פועלים בו כדי להשיג מטרות מדינתיות – פוליטיות, ביטחוניות, טכנולוגיות וכלכליות. זאת, לצד פעילות של ארגוני פשיעה, העושים זאת למען בצע כסף. מהמידע הרב המתפרסם לאחרונה על העיסוק של מדינות בריגול במרחב הסייבר, ובפרט על מאבקי הסייבר בין ארצות הברית לסין, עולה כי הריגול העסקי הפך לכלי מרכזי בין מדינות בכלל ומעצמות בפרט, כחלק ממלחמה כלכלית ביניהן וממאמציהן להשגת דומיננטיות גלובלית.

מדינת ישראל חשופה במידה ניכרת לאיומי הסייבר עקב היותה עתירת טכנולוגיה מתקדמת. הידע הרב שנוצר בארגונים כלכליים, מדעיים ואחרים במדינת ישראל נשמר, משונע ומנוהל במרחב הסייבר, ועל כן הוא נגיש לגורמי תקיפה שונים. בנוסף, חלקה של התעשייה מבוססת החדשנות והקניין הרוחני הייחודי בתוך כלכלת ישראל הוא משמעותי מאד. תעשיית חברות ההזנק הישראלית היא מהמובילות בעולם, וגם נתון זה מגביר כמובן את המוטיבציה לריגול עסקי בישראל.

בשל העובדה שמערכי ריגול ייעודיים מתקדמים (APTs – Advanced Persistent Threats) כמעט ואינם מתגלים על ידי אמצעי ההגנה הסטנדרטיים שבהם נעשה שימוש לצרכי אבטחה בחברות מסחריות, ניתן להניח שחברות ישראליות, במיוחד כאלו המפַתחות ידע ייחודי, מהוות יעד לריגול מסחרי ולגניבת קניין רוחני, כמו במדינות מתקדמות אחרות.

מטרת מאמר זה היא לבחון את השימוש במרחב הסייבר לצורך ריגול עסקי וגניבה של קניין רוחני. בנוסף מבקש המאמר להציף את המורכבות של הערכת היקף התופעה והנזקים הכספיים שהיא גורמת, ולבסוף – לנתח את היקף הריגול המסחרי בישראל. זאת, כדי להגביר את המודעות אליו בשיח הציבורי, ובעקבותיה – את הפעילויות הנדרשות לצמצום התופעה ונזקיה.

הסייבר כתווך לריגול עסקי

ריגול עסקי קיים אמנם משחר ההיסטוריה, אולם עם מעבר העולם העסקי לפעילות ענפה בסייבר, התפתח מאד גם הריגול העסקי במרחב זה. מרחב הסייבר מתאים מעצם טבעו לפעילות ריגול, ובמיוחד לריגול עסקי. הוא מאפשר פעילות אנונימית באופן יחסי, לרבות העברה נוחה ובטוחה של כמויות מידע עצומות בלי תלות במרחק ובגבולות. במקביל, הוא מקשה מאד על קורבן הריגול – יהיה זה ארגון מסחרי או ממשלתי – להבחין בעצם פעילות הריגול. אפילו אם הנתקף הבחין בתקיפה וזיהה את הכלים ששימשו לביצועה (Spyware), יש לו קושי לשייך את הפעולה הזדונית שהתגלתה לגורם המבַצע ולבסס האשמה אמינה לגבי זהות הגורם התוקף.

הריגול המסחרי בסייבר מתאפשר בעלות נמוכה מאד בהשוואה לדרכי איסוף מודיעיני אחרות, ובסיכונים מבצעיים נמוכים. כך, לדוגמה, פעילות ריגול במרחב הסייבר מצמצמת מאד את הצורך בסוכנים ביעד. תודות למצב עניינים זה, יכולים היום גורמי ביון ברחבי העולם להעצים את יכולותיהם, הן באיסוף המתבצע כולו במרחב הסייבר[5] והן על ידי שילוב כלי ריגול "קלאסיים" עם היכולות החדשות במרחב זה. כך, פעילות הריגול הופכת לפשוטה יותר לַתוקף ומסוכנת יותר לנתקף. לדוגמה, פעילות ריגול בה מעורב סוכן העובד בארגון המותקף, הופכת לפשוטה יותר בעידן הסייבר: העברת המידע הגנוב קלה יותר, וקשה יותר לשייכה לגורם המבַצע. גם יחסן של רשויות החוק לפשיעה בסייבר מקל ומצמצם את הסיכון לעוסקים בריגול המסחרי. כך, פורץ שייתפס בפריצה פיזית לחברה מסחרית לצורך גניבת מידע, צפוי לשלם על כך מחיר גבוה הרבה יותר מעמיתו השולח את ידו להשגת אותו מידע דרך המקלדת.

ריגול עסקי יוגדר כהוצאה לא ברשות של מידע עסקי חסוי שאינו נחלת הכלל, שמטרתה השגת יתרון טכנולוגי ו/או רווחים כלכליים. מידע כזה כולל נתונים

בתחומי האסטרטגיה, התכנון, החדשנות הטכנולוגית, תהליכי פיתוח מוצרים, תהליכי ייצור ושיווק, תוכניות פרסום, מצב פיננסי, סוגיות משפטיות, אנשי מפתח, נתוני שכר, נתוני מכרזים ועוד. הגניבה יכולה להיעשות לא רק מארגונים מתחרים אלא גם מגופים דוגמת מכוני מחקר אקדמיים, שבהם יש מידע רב ערך.

השגת המידע כרוכה, במקרים רבים, בעבירה על החוק, להבדיל מאיסוף מידע עסקי ממקורות גלויים. פעילות זו היא ענף אחד במשפחה רחבה של "פשיעה כלכלית", הכוללת מעילות והונאות, גניבות, הרס ושיבוש פעילות עסקית ועוד. ריגול עסקי המבוצע בידי מדינה נעשה, בדרך כלל, במטרה לחזק את הכלכלה המקומית, כדי ליצור יתרון לכלכלת אותה מדינה או לסקטור מסויים בכלכלתה ביחס לכלכלות מתחרות בעולם.

העלייה בהיקף הריגול העסקי המבוצע במרחב הסייבר משקפת את השינויים הטכנולוגיים, הכלכליים והחברתיים שמתרחשים בשנים האחרונות באופן שבו מידע נוצר, משונע, נאגר ומנוהל בארגונים כלכליים ומדעיים ובגופים רגישים אחרים. כמעט כל הרשומות המסחריות והמדעיות, אפילו הרגישות ביותר, נשמרות באופן דיגיטלי ונגישות דרך רשתות מחשב ברחבי העולם. לאור זאת, ולאור העדיפות שנותנים כיום תוקפים מתוחכמים דוגמת גופי מודיעין מדינתיים או ארגוני פשע מתוחכמים, מתאפשר לגופים אלה לעשות שימוש במרחב הסייבר לביצוע גניבת מידע מסחרי ועסקי. גניבות אלו הן בשיעור גדול משמעותית מכל ריגול עסקי שהיה מוכר בעבר, הן במידת החשיבות והרגישות של המידע הגנוב לבעליו והן בכמותו.

הניסיון מראה שרק חברות מעטות מסוגלות לזהות תקיפות מתוחכמות המבוצעות על ידי ארגון ביון מדינתי או ארגון פשיעה מתקדם, ומעטות עוד יותר מסוגלות להתגונן בפניהן באופן יעיל.[6] ישנן דוגמאות רבות המצביעות על כך, שגם החברות הרגישות ביותר בתעשיות הביטחון בארצות הברית היו טרף קל יחסית לריגול מסחרי (או ביטחוני) דרך הרשת שבוצע על ידי ארגונים מדינתיים, כנראה מתוך מוטיבציה מסחרית.[7]

דוח של המשרד הלאומי למניעת ריגול בארצות הברית (ONCIX), שהוגש לקונגרס האמריקאי,[8] כולל התייחסות לאיום גניבת המידע המסחרי וליריבים המרכזיים המבצעים פעילות זו בארצות הברית. סין ורוסיה נזכרות בדוח כבעלות היכולות הגבוהות ביותר בתחום זה, ומאופיינות בו כמדינות "האגרסיביות ביותר באיסוף של מידע מסחרי וטכנולוגי אמריקאי".[9] בדוח נוסף של אותו גוף לקונגרס האמריקאי, מיולי 2012,[10] מצוטטים דברי גנרל ג'יימס קְלָפֶּר,[11] בעדותו בפני הקונגרס על הערכת האיומים הלאומית של קהילת המודיעין האמריקאית. קלפר העיד כי גופי מודיעין של מדינות יריבות מפתחים באופן עקבי מתודולוגיות וטכנולוגיות המאתגרות את יכולותיהם של גופי הממשל והסקטור הפרטי בארצות הברית להגן

על הסודות הלאומיים והמסחריים שלה.[12] ואכן, דוח הערכת האיומים האמריקאי לשנת 2013 מצביע על עלייה של איום הסייבר לראש רשימת האיומים על ארצות הברית,[13] לפני איומי הטרור והפצתו של נשק להשמדה המונית.

מורכבות הערכת הנזק של הריגול המסחרי

מטֶבע הדברים, יש קושי רב להעריך את מידת הנזק הנגרם כתוצאה מריגול מסחרי. הסיבות העיקריות לקושי זה נוגעות למגוון היבטים, בהם הקושי המתודולוגי לכמת את היקף הנזק הנגרם ליריב כתוצאה מאובדן הקניין הרוחני, ובשל העובדה שרק חלק מזערי מכלל פעילויות הריגול המתקדם מתגלה. ריצ'ארד ביטליך, מנהל האבטחה בחברת Mandiant, המתמחה בתחקור אירועי תקיפה בסייבר, העיד בפני ועדה ממשלתית בארצות הברית כי מתוך סך אירועי התקיפות המתוחכמות לצרכי ריגול שמקורן בסין, אותם תחקרה החברה, רק שישה אחוזים מהאירועים שהתגלו היו ידועים לחברות המותקפות. נתון זה מצביע על פער גדול מאד בין עוצמת התופעה לבין הבנת המחיר הכבד שהמשק משלם כתוצאה מריגול מסחרי.[14] בנוסף, פעילות הריגול המסחרי בסייבר, המבוצעת על ידי ארגונים מתקדמים, ממומשת בכלים ייעודיים לריגול, שכלי ההגנה הסטנדרטיים בהם עושים שימוש מרבית הארגונים אינם מסוגלים לזהות, לחסום או לנטרל. יש לזכור כי במרחב הסייבר קיים היום יתרון מובהק לתוקף.

ארגוני ביון רבים עושים שימוש בסייבר כזירה מרכזית לאיסוף ידיעות, ויכולות שפותחו לצורך כך בגופים ביטחוניים משיגות את המענה ההגנתי הנוכחי לאיומים אלו. זאת ועוד, התוקף הייעודי הממוקד נהנה גם מהיתרון שהוא יכול ללמוד על כלי האבטחה של המגן ואף להצטייד בהם,[15] וכך לבצע סימולציות המאפשרות לו למצוא את התנאים לא להתגלות על ידי כלי האבטחה בהם עושה הנתקף שימוש.[16] בנוסף לכך, פעילות הריגול המדינתית מבוצעת על ידי גופי מודיעין המאורגנים לצורך זה, בעוד שהיערכות להגנה מחייבת התארגנות מדינתית כוללת, המערבת גופים ביטחוניים וגופים מהמגזר הממשלתי שאינו ביטחוני וכן מהמגזר הפרטי – התארגנות שמטֶבעה היא מסורבלת ואיטית יותר.

ארגון ה־FBI העריך כי מול כל אירוע בו חברה אמריקאית זיהתה שרשתות המחשב שלה נפרצו, התרחשו כמאה אירועים דומים, בהם חברות שרשתות המחשב שלהן נפרצו לא הבחינו בכך.[17] דוח של חברת האבטחה האמריקאית Mandiant, שפורסם בפברואר 2013,[18] קובע כי תכליתו של מערך התקיפה הסיני היא ריגול מסחרי וכי הוא תקף באותה שנה 141 חברות מערביות, בעיקר בארצות הברית. זוהי דוגמה לפעילות ריגול מסחרי המבוצעת על ידי גוף מדינתי, שהתנהלה במשך שנים ולא עלתה כלל לתודעה הציבורית עד לפרסום הדוח.[19] אפשר להקיש מדוגמה זו על כך שחברות אחרות, הנתקפות על ידי מערכי תקיפה מתקדמים,

אינן מצליחות במרבית המקרים להבחין בתקיפה. גם במקרים המעטים שבהם הן מצליחות לזהות שהן הותקפו, הנושא אינו מגיע לידיעת הציבור, והמשמעויות הכלכליות והאבטחתיות לא נלמדות בהקשר המדינתי הכולל.

במקרים המעטים שחברות וארגונים מצליחים להבחין בקיומה של פעילות ריגול המתבצעת נגדם, ואף מאתרים תוכנת ריגול שהותקנה במחשבי הארגון, הם מתקשים להעריך את היקף וסוג המידע שכבר דלף מתוך רשתותיו. הכישלון בהגנה על נכסי החברה או הארגון גורם לכך שאחראֵי האבטחה בהם נוטים לעתים להעריך בחסר את הנזקים שגרמה פעילות הריגול.

הנטייה הטבעית כשמתגלה כלי תוכנה לא מוכר – תוכנה זדונית במחשבי החברה – היא להסיר אותו ולוודא שהמערכות ממשיכות לעבוד. רק במקרים מעטים מאד נערכת חקירה פורֶנזית מקיפה שמטרתה היא להבין את מהות התקיפה ולאתר את הכלים ששימשו למימושה, וזאת בשל עלותה הגבוהה הן בהיבט הכספי והן במשך הזמן הנדרש לביצוע החקירה הפורֶנזית שבמהלכה נפגע המענה התיקשובי בחברה. גם אם מתבצעת חקירה פורנזית מלאה ומקצועית, וזו מצליחה לחשוף את העובדות כהווייתן, וגם כאשר הנהלת החברה מקבלת תמונה מלאה ואמינה בנוגע לגניבת המידע המסחרי, ישנם מקרים רבים בהם הארגון מעדיף שלא לחשוף את הגניבה, או לכל הפחות לצמצם את הערכת הנזק, מתוך תקווה להקטין בכך את ממדי הפגיעה במוניטין שלו כתוצאה מפרסום האירוע. הפגיעה במוניטין עלולה, כמובן, לסכן את היחסים עם בעלי המניות, ציבור המשקיעים, הספקים, הלקוחות ובעלי עניין אחרים.

לבסוף, קיים קושי מובנה להעריך את ההיקף הכספי של הקניין הרוחני. ברור שערכו של הקניין הרוחני אינו משתקף בהכרח בערכה של ההשקעה שבוצעה כדי ליצור אותו. זו, כנראה, האמירה ההחלטית ביותר שניתנת להיאמר בעניין: לדוגמה, שווי התשואות העתידיות שיימנעו מהחברה כתוצאה מגניבת מידע עסקי דרך המרחב הקיברנטי הוא נתון סובייקטיבי המועד לספקולציות.

לאור סיבות אלו ונוספות, יש קושי רב לאמוד את הנזק המצטבר הנגרם לארגון כתוצאה מהריגול המסחרי בסייבר. קושי זה גובר כאשר מנסים לאמוד את הנזק הכלכלי הנגרם מתופעה זו למדינה. כתוצאה מכך, ההערכות המתפרסמות על מידת הנזק המדינתי הנגרם מגניבת מידע מסחרי ברשת נעות על פני מנעד רחב מאד.

שיטות הערכת הנזק המסחרי בעולם

מחקרים שונים, הדנים בתופעת הריגול המסחרי ועלותו, מנסים להציע מתודולוגיה לביצוע הערכת הנזק. פערי המידע המשמעותיים בנושא זה, הנובעים מהסיבות שהוזכרו לעיל, והקושי המובנה לתת להם מענה, מהווים אבן נגף להערכת היקף התופעה.

מקובל לחלק את עלות הפשיעה הקיברנטית לשלוש קבוצות עיקריות:[20] **עלות היערכות**, כמו מאמצי אבטחה, התאמה לתקני אבטחה נדרשים והוצאות ביטוח; **עלות נזק ישיר**, כמו פגיעה בתפקוד, תיקון הפגיעה, עלויות זמן עבודה, סגירת פרצות ושחזור מידע, הפסדים ישירים לעסק, פיצוי לקוחות, קנסות וסוגיות משפטיות; **אומדן נזק עקיף**, כמו אובדן אמון הלקוחות, אובדן עסקאות והכנסות עתידיות, פגיעה במותג וכדומה.

הגישות השונות להערכת הנזק מתבססות על סקרים וניתוח תיאורטי. במחקרים מבוססי סקרים מתבקשים מנהלים ומומחי IT בחברות מסחריות לאמוד את הנזק. מתוך אומדני קבוצת המדגם מתבצעת הרחבה אל הכלל. דא עקא שקיים פער עמוק בין הבנת התופעה אצל הנשאלים בקבוצת המדגם ובין היקף התופעה בפועל. פער זה מתעצם לאור העובדה שקבוצת המדגם צפויה להיות מוּטָה: אלה שחוו תקיפות כואבות אינם נוטים להתנדב ולספר על כך, ולפיכך אין זה צפוי שייקחו חלק במחקרים כאלה. לאור כל זאת, נדרשים מחקרים אלה לבצע תיקון מתאים של ממצאיהם. עניין זה כשלעצמו משפיע באופן דרמטי על הבנת היקף התופעה.

שיטת הניתוח התיאורטי מבוססת על מודל חישוב הנסמך על נתונים גלויים, השערות והערכות מומחים לאבטחת מידע, אנשי עסקים, כלכלה וגורמי אכיפה. גם מודל זה סובל מהפער בין איכות המידע הזמין ובין נתוני האמת וההתבססות על הערכות. דוגמה למחקר מסוג זה היא הערכת הנזק שנגרם כתוצאה מגניבה מסחרית בסייבר באנגליה, שנעשתה על ידי חברת Detica.[21]

הערכת סיכון ומדידתו חיוניים להבנת התופעה של גניבה במרחב הסייבר ולחלוקת משאבים אופטימלית להתגוננות מפניה. יש לכן עניין רב לארגונים ומדינות לאמוד את העלות הנגרמת להם כתוצאה מגניבת מידע. גנרל קית אלכסנדר, מפקד פיקוד הסייבר האמריקאי והעומד בראש הסוכנות לביטחון לאומי (NSA), טען בסימפוזיון על האיומים המתהווים בסייבר כי חברות אמריקאיות מאבדות כ־250 מיליארד דולר בשנה כתוצאה מגניבה של קניין רוחני.[22] הוא ציטט את הדוח של חברת "סימנטק", המעריך את "הנזק השנתי הישיר מפשיעת סייבר ב־114 מיליארד דולר, אולם הנזק המוערך הזה יכול לעלות ל־388 מיליארד דולר אם כוללים בו את הזמן וההזדמנויות העסקיות שאבדו".[23] דוח ועדה לבחינת גניבת קניין רוחני אמריקאי מעריך שהנזקים הנגרמים כתוצאה מגניבה כזאת עולים על 300 מיליארד דולר בשנה.[24]

מדינות נוספות על ארצות הברית מנסות גם הן להעריך את היקף התופעה: המשרד הפדרלי הגרמני להגנה על החוקה מעריך שלחברות גרמניות נגרם הפסד שנתי הנאמד בין 28 ל־71 מיליארד דולר וכי בין שלושים לשבעים אלף מקומות עבודה אובדים עקב ריגול כלכלי זר. דרום קוריאה דיווחה שהעלויות שנגרמו לה

כתוצאה מריגול כלכלי שבוצע על ידי גורמים זרים בשנת 2008 היו 82 מיליארד דולר, לעומת 26 מיליארד דולר ב־2004. לפי דיווח זה, שישים אחוזים מהקורבנות היו עסקים קטנים ובינוניים, ומקורן של מחצית מתקיפות הריגול המסחרי הוא בסין. משרד הכלכלה, המסחר והתעשייה של יפן ערך ב־2007 סקר בקרב 625 חברות יצרניות ומצא כי יותר מ־35 אחוזים מהחברות שנטלו בו חלק דיווחו על הפסד טכנולוגי כלשהו וכי יותר משישים אחוזים מהמקרים המדווחים היו קשורים לסין. גורמים בריטיים רשמיים העריכו כי ההתקפות על מערכות מחשב, כולל ריגול תעשייתי וגניבה של מידע מסחרי של חברות, עולות למגזר הפרטי הבריטי 34 מיליארד דולר לשנה. יותר מארבעים אחוזים מסכום זה נגרמים מגניבה של קניין רוחני, כמו מִפרטים, נוסחאות וסודות של חברות.[25]

טבלה 1: סיכום הערכות הנזקים כתוצאה מריגול כלכלי במדינות שונות בעולם

מדינה	הערכת הנזק השנתי כתוצאה מגניבת מידע מסחרי וקניין רוחני (במיליארדי דולר)	מידת הנזק כחלק מהתמ"ג (באחוזים)
ארצות הברית	300–250	2.0–1.67
דרום קוריאה	82	7.3
גרמניה	71–28	2.0–0.8
אנגליה	34	1.4

יש לציין כי המעריכים השונים לא נתנו הסבר לאופן שבו הם הגיעו להערכת עלות הנזק – ככל הנראה בשל הקשיים להעריך את הנזקים הישירים, ובמיוחד העקיפים, מפשיעת הסייבר. לקשיים אלה ניתן אולי להוסיף אינטרסים שונים של הגופים החוקרים, בעיקר של חברות אבטחת מידע מסוימות, החשודות בכך שיש להן עניין בניפוח ממדי התופעה.

מחקר שפורסם על ידי קבוצת המחקר של חברת McAfee,[26] ביולי 2013, מנסה להתמודד עם מורכבות ההערכה של עלות הפשיעה בסייבר. המחקר מציב סימני שאלה על אומדני העלות המתפרסמים במאמרים שונים ומנמיך את הערכות הנזק למשק האמריקאי המושמעות על ידי גופים רשמיים. המחקר לא קובע הערכות מוחלטות של עלויות הנזק, אך מראה למשל כי גבול הנזק העליון למשק האמריקאי נע על פי שיטת הערכה אחת בין 0.5 ל־2.0 אחוזים מהתמ"ג,[27] בעוד שעל פי שיטה אחרת הוא לא עולה על אחוז אחד מהתמ"ג.[28]

ריגול מסחרי בישראל

מדינת ישראל רגישה מאד לאיומי סייבר בכלל ולריגול מסחרי בפרט, עקב היותה מדינה עתירת טכנולוגיה מתקדמת. חלק ניכר מהייצוא של ישראל נשען על חברות שיש להן תלות רבה בקניין רוחני, וניתן לפיכך להניח שהיא מהווה יעד לגניבת קניין זה. בנוסף, חלקה של התעשייה המבוססת חדשנות וקניין רוחני ייחודי בכלכלת ישראל הוא משמעותי מאד: תעשיית חברות ההזנק הישראליות היא מהמובילות בעולם, וגם מצב זה מגביר את המוטיבציה לריגול עסקי בישראל. על אלה יש להוסיף את המודעות הנמוכה בקרב המגזר העסקי בישראל לסיכוני הריגול בסייבר, המביאה להעדפה של נוחות עבודה וניצול הזדמנויות עסקיות על פני אבטחה. ניתן אפוא להניח, שכמו במדינות מתקדמות אחרות, כך גם בישראל, חברות מסחריות, במיוחד אלו המפתחות ידע ייחודי, מהוות יעד לריגול מסחרי ולגניבת קניין רוחני. מבין 141 חברות מסחריות שהותקפו על ידי מערך התקיפה APT1, כמתואר על ידי חברת Mandiant, שלוש היו חברות ישראליות.[29]

מדינת ישראל הייתה בין המדינות המובילות בעולם בהפנמת איום הסייבר לתשתיותיה הקריטיות, אך לא בהפנמת איום הריגול העסקי. כבר ב־2003 הוקמה הרשות לאבטחת מידע – רא"ם[30] – שייעודה הוא אבטחת התשתיות הקריטיות של מדינת ישראל מפני תקיפות המבוצעות בתווך הקיברנטי ומאיימות לפגוע בתשתיות אלה, ומפני גניבת סודות מדינה. המגזר העסקי הפרטי והציבורי בישראל לא זכה למענה דומה, ואין כיום גוף בעל אחריות להגנת מגזר זה מפני ריגול מסחרי בסייבר. כתוצאה מכך, ישראל נמצאת כיום בפיגור בנוגע להגנת המגזר העסקי ביחס למדינות רבות בעולם, ובהן ארצות הברית. במדינות אלו התגבשה ההבנה שיש חשיבות להגנה מדינתית על הנכסים המסחריים הלאומיים וכי המדינה אחראית למתן נדבכי הגנה מדינתיים מפני האיומים בסייבר למשק בכלל ולמגזר הפרטי בפרט. הבנה זו הביאה להטלת אחריות לנושא על גוף או גופים מדינתיים, שמתפקידם להוביל את פעילות ההגנה המדינתית בסייבר במטרה לחזק את ההגנה הכוללת בתחום זה.[31]

קיים קושי רב להעריך את הנזק הנגרם למשק הישראלי מהריגול המסחרי. בישראל אין חובת דיווח על מציאת כלי איסוף במחשבי חברה, למעט הנחיות מינימליות בנוגע למידע הקשור למרשם האוכלוסין ולרגולציה במגזרים ייחודיים דוגמת הבנקים והגופים מפוקחי הרשות לאבטחת מידע והממונה על הביטחון במערכת הביטחון. גם אין בישראל חובה חוקית לפרסם אובדן מידע עסקי רגיש של חברה,[32] ואין בה גוף האחראי להגנת המגזר המסחרי בסייבר, שמתוקף תפקידו לרכז מידע מסוג זה ולעשות בו שימוש להפקת לקחים ולחיזוק מענה הגנתי כולל. לאור זאת, הסיכוי לאיתור ריגול מסחרי בסייבר בישראל הוא נמוך מאד. זו כנראה הסיבה לדיווחים המעטים הנוגעים לגניבת ידע מסחרי וקניין רוחני מחברות ישראליות.

למרות המגבלות והקושי בהערכת הנזק מתקיפות סייבר, ניתן להניח שארגונים עסקיים ואחרים בישראל חשופים לגניבות מסחריות בהיקפים שאינם נופלים מאלה של מדינות מתקדמות אחרות. זאת, הן בשל הדימוי של ישראל כמובילה בעולם בפיתוח ידע חדשני והן לאור הליקויים בהגנה שהוזכרו לעיל. אם מתבססים על ההנחות השמרניות, לפיהן נזקי הגניבה המסחרית בסייבר מגיעים לאחוז אחד מהתמ"ג הלאומי, הנזק השנתי מגניבות כאלו בישראל מגיע לכ־2.5 מיליארד דולר. עבודת מחקר ראשונית להערכת נזקי הריגול העסקי בישראל, שנעשתה עבור מטה הסייבר הלאומי על ידי חברת המחקר Meidata, אומדת את הנזק השנתי למשק הישראלי מריגול עסקי בין מיליארד לשלושה מיליארד דולר. אין ספק שנזק בסדר גודל כזה, שעולה בהתמדה משנה לשנה, מחייב היערכות לאומית ומצדיק השקעה משמעותית בהתגוננות אצל חברות וגופים נתקפים, המשלמים את המחיר העיקרי של תופעת הריגול העסקי.

תובנות מסכמות

מדינת ישראל, בה קיימת תודעה ביטחונית גבוהה, הייתה מן המדינות החלוצות בהבנת הסיכונים הביטחוניים המתפתחים במרחב הסייבר המתהווה עוד לפני שאותרה פגיעה כלשהי בתשתית קריטית בישראל. יחד עם זאת, הסיכון הטמון בגניבת סודות מסחריים וקניין רוחני של חברות כלכליות ישראליות לא מזוהה גם כיום כאיום משמעותי לחוסנה של המדינה. זאת, גם לאחר הצגת עדויות ברורות לכך שמדינות וארגוני פשע עושים שימוש רב במרחב הסייבר לביצוע ריגול עסקי, שיש לו השפעות כלכליות ניכרות על חברות מסחריות ועל מדינות, תוך שימוש בכלים מתקדמים ביותר.

האיום הכלכלי על חברות מסחריות כתוצאה מריגול עסקי מוגדר על ידי ראש קהילת המודיעין הלאומית האמריקאית כאיום המוחשי הראשון במעלה על ארצות הברית וממוקם לפני איום טרור והפצתו של נשק להשמדה המונית. עלות הנזק הנגרם כתוצאה מריגול עסקי בסייבר היא משמעותית, ונמצאת במגמת עליה, ומשלם אותה, בראש ובראשונה, המגזר העסקי. על פי מחקרים שונים, מרכיב העלות של הריגול המסחרי הוא הדומיננטי ביותר בתוך סך סוגי הפשיעה בסייבר.[33] מדינת ישראל, שכלכלתה מוכוונת ידע חדשני, חשופה גם היא לפשיעה קיברנטית, ובכלל זה לריגול עסקי.

קיים קושי רב לאמוד את הנזק מריגול מסחרי במרחב הסייבר. לכן, ניתן לראות מִנעד רחב של אומדנים בדוחות שונים. הקושי להעריך באופן אמפירי את הנזקים, ומרכזיותן של הערכות מומחים הבאות לתת מענה לפער באיכות הנתונים שנאספים, מהווים אבן נגף בכל השיטות לאומדן הנזקים הנגרמים מריגול מסחרי. זהו המקור לפערים הגדולים בהערכות של נזקים אלה. למרות

הקשיים, הם אינם מייתרים את הצורך בהערכות הנוגעות להבנת המשמעות של תופעת הריגול העסקי; הערכות כאלו הן הבסיס להבנתן של מדינות את התופעה ולהיערכותן אליה.

מוצע לפעול לפיתוח מתודולוגיה יציבה, שתוכל לספק כלים להערכה אמינה של הנזקים שבהם עסק מאמר זה. כך תגדל המודעות לשיפור ההגנה מול האיום ומול הנזקים שהוא גורם. כדי לקדם את הנושא, יש לשפר בראש ובראשונה את היכולת לאסוף מידע אמין על התופעה באמצעות מנגנונים לדיווח על אירועי סייבר. לצידם יש לפתח כלי הערכה משופרים שיתנו מענה לפערי המידע הקיימים בין הדיווחים וההערכות של הסקרים לגבי מספר האירועים והערכת הנזק שהם גורמים מצד אחד ובין התמונה בפועל מצד שני. זהו פער מובנה, בשל העובדה שבמרבית המקרים, המותקפים כלל אינם מודעים לכך שהותקפו וכי מידע עסקי שלהם נגנב, ולפיכך אינם מסוגלים, גם בדיעבד, לקשר בין נזק עסקי לבין גניבת מידע עסקי מהארגון, שכאמור, הם אינם יודעים דבר עליה. בנוסף לכך, שיפור המענה האזרחי הכולל במרחב הסייבר בישראל, תוך קביעת גורם אחראי בעל סמכות מתאימה, יוכל לאפשר פיתוח של תפיסת התמודדות מקיפה עם הגניבות המסחריות במרחב הסייבר, מתוך ראייה לאומית רחבה.

כאמור, מטרת מאמר זה היא להאיר את תופעת הריגול העסקי המתבצע בתווך הקיברנטי ואת הנזקים שנגרמים למשק הישראלי בעטיה. בהיעדר מחקרי עומק על התופעה, קשה להצביע על היקפה המדויק, אולם ניתן להעריך שהוא משמעותי לכלכלה הישראלית ומצוי במגמת עליה ניכרת. המענה לתופעה זו צריך להכיל מגוון פעילויות, וביניהן: מחקרים ממוקדים על היקפה ופילוחה בסקטורים שונים; שיפור האבטחה במגזר העסקי; פיתוח תעשיית ביטחון הסייבר; מהלכים מדינתיים שיוכלו לתת מענה לריגול העסקי המדינתי המתבצע במרחב הסייבר, לרבות שיתופי פעולה והסְדרות מול מדינות עמיתות הסובלות גם הן מהתופעה.

המענה לתופעת הריגול העסקי במרחב הסייבר הוא מורכב ועתיר משאבים. נדמה שהגדלת המודעות אליה, הן בקרב הגורמים העסקיים והן בקרב מקבלי ההחלטות בישראל, היא תנאי הכרחי לתחילת פעילות לצמצום נזקי הפשיעה הקיברנטית בכלל ונזקי הריגול המסחרי בפרט. זאת, כדי להביא את יכולת ההגנה הישראלית בסייבר למיצוי נכון אל מול כלל האיומים.

הערות

1 Nicole Perlroth, "Study May Offer Insight into Coca-Cola Breach", *The New York Times*, November 30, 2012, http://bits.blogs.nytimes.com/2012/11/30/study-may-offer-insight-into-coca-cola-breach/?_r=0 .

2 גנרל אלכסנדר הוא מפקד פיקוד הסייבר האמריקאי ועומד בראש הסוכנות לביטחון לאומי (NSA) בארצות הברית. ראו:

Carrie Lukas, "It's Time for the U.S. to Deal with Cyber-Espionage – Adversaries draining intellectual property from American companies must come to an end", *US News*, June 4, 2013, http://www.usnews.com/opinion/articles/2013/06/04/chinas-industrial-cyberespionage-harms-the-us-economy.

3 למשל, הפעלת מערכות שליטה ובקרה, השולטות על בַּקָרים ממוחשבים לתהליכים תעשייתיים, באופן שונה מהתהליך הסדור, כך שייגרמו נזק לתהליך התעשייתי או הרס של המערכות התעשייתיות עצמן.

4 Francois Paget, "2014 Threats Predictions: Cybercrime and Hacktivism Will Continue to Grow", McAfee Labs, January 8, 2014, http://blogs.mcafee.com/mcafee-labs/2014-threats-predictions-cybercrime-and-hacktivism-will-continue-to-grow.

5 הדוגמה הבולטת למעקב המבוצע כולו במרחב הסייבר העולמי היא מערכת המעקב העולמית PRISM של ה־NSA, שנחשפה מתוך הדלפותיו של אדוארד סנודן. המעקבים במרחב הסייבר שביצע ה־NSA נעשו לכאורה לצורך שמירה על ביטחונם של אזרחים אמריקאים. אולם, ישנם דיווחים שמעקבים כאלה בוצעו גם אחר תעשיות שעניינו את ארצות הברית, בעיקר בתחום היכולות הביטחוניות המתקדמות. ראו:
Glenn Greenwald and Ewen MacAskill, "NSA Prism Program Taps in to User Data of Apple, Google and Others", *The Guardian*, June 7, 2013. http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data;
Scott Shane, "No Morsel Too Minuscule for All-Consuming N.S.A.", *The New York Times*, November 2, 2013, http://www.nytimes.com/2013/11/03/world/no-morsel-too-minuscule-for-all-consuming-nsa.html?pagewanted=1&_r=0.

6 Mandiant Report, "APT1 Exposing One of China's Cyber Espionage Units", February 2013. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

7 ראו כדוגמה את תקיפת הסייבר המוצלחת ב־2011 על חברת "לוקהיד מרטין" לצורך גניבת תוכניות מטוס החמקן המתקדם F–35.

8 Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace, Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011, Annex B – West and East Accuse China and Russia of Economic Espionage*, October 2011, http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

9 **שם**, עמ' 4.

10 *Foreign and Economic Espionage Penalty Enhancement Act of 2012*, House of Representatives Report 112-610, 2012, http://www.fas.org/irp/congress/2012_rpt/ecoesp.pdf.

11 קלפר הוא ראש קהילת המודיעין הלאומית האמריקאית (DNI – Director of National Intelligence).

12 James R. Clapper, Director of National Intelligence, "Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence", January 31, 2012, p. 8, http://www.intelligence.senate.gov/120131/clapper.pdf.

13 James R. Clapper, Director of National Intelligence, "Statement for the Record on the Worldwide Threat Assessment of the Us Intelligence Community, Senate Select Committee on Intelligence", March 12, 2013, http://www.intelligence.senate.gov/130312/clapper.pdf.

14 Devlin Barrett, "U.S. Outgunned in Hacker War", *Wall Street Journal*, March 28, 2012, http://online.wsj.com/article/SB10001424052702304177104577307773326180032.html.

15 ברוב המקרים, כלי האבטחה הם כלים מסחריים סטנדרטיים.

16 ראו דוח מפורט בהקשר זה ב:
Mandiant Report, "APT1 Exposing One of China's Cyber Espionage Units".

17 IBTimes Staff Reporter, "America's Top Cyberwarrior Says Cyberattacks Cost $250 Billion A Year", July 13, 2012, http://www.ibtimes.com/americas-top-cyberwarrior-says-cyberattacks-cost-250-billion-year-722559.

18 Mandiant Report, "APT1 Exposing One of China's Cyber Espionage Units".

19 החברה מזכירה בדוח כי היא חקרה עשרות מערכי תקיפה מתקדמים, יותר מעשרים מתוכם מערכים בעלי מאפיינים דומים, שמקורם בסין. החברה בחרה, מסיבות משלה, לפרסם בדוח התייחסות למערך אחד בלבד.

20 R. Anderson, C. Barton, R. Böhme, R. Clayton, M. van Eeten, M. Levi, T. Moore and S. Savage, "Measuring the Cost of Cybercrime", in: *Workshop on the Economics of Information Security*, WEIS, 2012.
http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

21 Detica, *The Cost of Cyber Crime*, A Detica Report in partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office, UK, 2011, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60942/THE-COST-OF-CYBER-CRIME-SUMMARY-FINAL.pdf.

22 IBTimes Staff Reporter, "America's Top Cyberwarrior Says Cyberattacks Cost $250 Billion A Year".

23 Emil Protalinski, "NSA: Cybercrime is the Greatest Transfer of Wealth in History", *ZDnet*, July 10, 2012.
http://www.zdnet.com/nsa-cybercrime-is-the-greatest-transfer-of-wealth-in-history-7000000598/.

24 The IP Commission Report, *The Report of the Commission on the Theft of American Intellectual Property*,
http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.

25 Office of the Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace*.

26 McAfee, *The Economic Impact of Cybercrime and Cyber Espionage*, Center for Strategic and International Studies, July 2013,
http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf.

27 **שם**, עמ' 14.

28 **שם**, עמ' 15.

29 Mandiant Report, "APT1 Exposing One of China's Cyber Espionage Units".

30 הרשות הלאומית לאבטחת מידע – רא"ם – כפופה לשב"כ. היא הוקמה מכוח החלטת ממשלה מדצמבר 2002.

31 האחריות הכוללת לתחום ההגנה הלאומית על המשק האמריקאי מוטלת על המשרד להגנת המולדת, הפועל בשיתוף פעולה הדוק עם משרד ההגנה (המכיל גופי מודיעין, דוגמת "הסוכנות לביטחון לאומי" ו"הסוכנות הלאומית למניעת ריגול", שפעילים מאוד בתחום ההגנה מפני מתקפות בסייבר וריגול מסחרי), "לשכת החקירות הפדרלית" (FBI)

ומשרד המשפטים.

32 כשמדובר באירוע פריצה בסייבר לחברה ציבורית בישראל, שעלול להשפיע על פעילותה או על נכסיה, יתכן שתהיה חובה לדווח עליו לבורסה, משום שעלולה להיות לו השפעה על שיקול הדעת של משקיע סביר ביחס לקניה או מכירה של מניית החברה.

33 Detica, *The Cost of Cyber Crime*, p. 3.