הגנת מרחב הסייבר הלאומי

יגאל אונא

האתגרים הניצבים בפני מדינת ישראל בתחום הסייבר מושפעים, בדומה למתרחש בתחומים נוספים ואף ביתר שאת מהם, מתהליכים חברתיים, תרבותיים וטכנולוגיים בין־לאומיים רחבים. ניתן להצביע על שני אתגרים־מגמות המשפיעים על מרחב הסייבר וגם מושפעים ממנו. המגמה הראשונה, שהיא המגמה העולמית המובילה, היא אתגר הדאטה. המשאב המשמעותי ביותר של 15 השנים האחרונות, וככל הנראה גם של העשורים הבאים, הוא המידע. הסוגיות המרכזיות הקשורות לאתגר זה הן איך להעביר, לשנע, לאחסן, לנהל ולמצות את התועלת מהדאטה. לפני 15 שנה החברות הגדולות בעולם היו אלו שערכן נחשב לגבוה ביותר – חברות האנרגיה, הגז והנפט. כיום אלו הן חברות המידע. המרוץ לעוצמה במידע ולשליטה בו צפוי להימשך ואף לגבור.

המגמה השנייה היא האתגר הטכנולוגי – "האינטרנט של כל הדברים" (Internet of Everything) שהוא, מעֵבר ל"אינטרנט של הדברים" (Internet of Things), גם חיבור לרקמות אנושיות חיות לטובת ניטור וריפוי מחלות ועוד. ישראל מתמודדת עם אתגר זה טוב יחסית בהשוואה לנעשה בזירה הבין־לאומית, ועם זאת, יש עדיין מקום להשקעה גדולה יותר שלה בתחום, כפי שמגובש במסגרת מיזם המערכות הנבונות הטכנולוגי החדש, על פי הנחיה של ראש הממשלה, לאיתור הטכנולוגיות המרכזיות בהן ישראל תתמקד בעתיד הקרוב – הבינה המלאכותית, מיחשוב קוונטי וטכנולוגיות אחרות בתחום הדאטה. זאת, כדי להיערך טוב יותר לעתיד בהיבטי העוצמה הלאומית הכלכלית, החברתית והאחרת.

ההגדרות של המושגים "סייבר", "לוחמת סייבר" ו"מרחב הסייבר" משתנות ומתעדכנות ללא הרף. "מערך הסייבר הלאומי" במשרד ראש הממשלה פועל על בסיס הגדרה מרחיבה שתוכל להישאר רלוונטית תמיד, ולוודא שישראל תהיה

יגאל אונא הוא ראש "מערך הסייבר הלאומי". המאמר מתבסס על דבריו שנאמרו בכנס של המכון למחקרי ביטחון לאומי, בשיתוף עם המרכז האקדמי שערי מדע ומשפט בהוד השרון, שנערך ב־24 באוקטובר 2018 לרגל השקת המזכר "רגולציה במרחב הסייבר" שנכתב על ידי ד"ר אל"ם (מיל') גבי סיבוני ועידו סיון־סביליה.

מוגנת באופן הרחב ביותר מפני כלל האיומים על טכנולוגיות התקשורת והמידע (ICT), כמו גם מפני מִתארי איום נוספים.

בהקשר זה, ראוי שנשים לב לרצף של תקיפות מדינתיות שהתרחשו בשנים האחרונות. אחת הדוגמאות המפורסמות לתקיפה מדינתית היא התקיפה המתמשכת על אוקראינה. מדובר ברצף של תקיפות מסוגים שונים, המתקיים מאז שנת 2014. אף אחת מתקיפות אלו לא הביאה לקריסת המדינה האוקראינית, אך הן משבשות לחלוטין את הכלכלה ופוגעות באמון הציבור בשלטון וביכולתו למשול.

בחינת התפתחותם של מרחב הסייבר ותקיפות הסייבר מלמדת שבתחילה נועדו התקיפות למטרת ריגול והשגת מידע. תקיפות מסוג זה ממשיכות להתרחש מאז, ואף בהיקף ובעוצמה רבים יותר. במשך הזמן התברר כי כאשר חודרים למערכת מחשב, ניתן לא רק להוציא ממנו את המידע, לשבש אותו, לשבש באמצעותו תהליכים קריטיים ואף לגרום לפגיעה פיזית ולמוות, אלא גם לגרום לפגיעה תודעתית ולהשפעה שלילית – שוב, באמצעות סייבר, קרי, על ידי חדירה או פריצה למערכת מידע ללא רשות והשגת נגישות אליה.

דוגמה עדכנית לפגיעה תודעתית ניתן למצוא בניסיונות הפגיעה במערכת הבחירות בארצות הברית בשנת 2016, שכתבי האישום שהגישה התביעה האמריקאית טוענים כי הותקפה בסייבר. מקרה זה מצביע במפורש על ההשפעה התודעתית שיש לתקיפה ועל הצלחתה לטלטל מערכת בחירות שלמה. דוגמאות נוספות לפגיעה תודעתית הן החדירה לחשבונות הדוא"ל הפרטיים של סנאטורית אמריקאית ושל פקיד בכיר בממשל האמריקאי, הפעם לא למטרות ריגול או גרימת נזק, אלא כדי לצבור חומר שניתן יהיה להדליף אותו בעיתוי הנכון ובערוץ הנכון, כדי לגרום לכאוס ולפגוע באמון הציבור האמריקאי במערכת הפוליטית והדמוקרטית בארצות הברית.

דוגמה מפורסמת לתקיפת תודעה בתחום הכלכלי התרחשה שבועיים לאחר הפיגוע במרתון בוסטון בשנת 2013. בחשבון ה"טוויטר" של סוכנות הידיעות "אסושיאייטד פרס" (Associated Press) פורסם ציוץ שבו נאמר: "פיצוץ בבית הלבן, הנשיא אובאמה נפצע". האירוע השפיע מיד על הבורסה האמריקאית. התוקף במקרה זה לא היה מספיק מתוחכם, שכן לקח לסוכנות הידיעות רק שבע דקות להבין כי מישהו חדר למערכות המחשב שלה. היה זה ניסיון פשוט של ניחוש סיסמה, שנקרא בעגה המקצועית תקיפת "כוח בוטה" (Brute Force). במקרה זה הסתפק התוקף בהפצת הידיעה בלבד, ולכן הנזק היה קטן יחסית. המדהים בפרשה היה גילוי זהותם של העומדים מאחורי הפריצה: ארבעה האקרים סורים שהיו שייכים ל"צבא הסורי האלקטרוני". התקיפה שהם ערכו הייתה ביטוי למתיחות ששררה בין הממשל האמריקאי בראשות הנשיא אובמה ובין סוריה סביב השימוש בנשק הכימי שלה.

התובנה העיקרית מאירוע זה היא שארבעה אנשים (במקרה זה סורים), נעדרי יכולות של מעצמה, הפגינו פוטנציאל לגרימת נזק כלכלי למעצמה העולמית מספר אחת. לא מדובר בחדירה למחשבי הבורסה או למערכת הבנקאית של ארצות הברית, אלא ביצירת השפעה תודעתית. לכן, כאשר עוסקים באיפיון ההגנות על תשתיות קריטיות ובטיב התשתיות הקריטיות שעליהן יש להגן, צריך לכלול בהן גם את אמון הציבור ולהתייחס אליו כאל תשתית קריטית. במסגרת זו יש לבחון כל העת מה עלול היריב, באשר הוא, לעשות באמצעות תקיפות בסייבר וחדירה למערכות מחשב ולרשתות מחשב, כדי לערער בדרך זו את אמון הציבור.

האסימטריה בין יריבים מסוג זה ובין מדינות פועלת לעיתים נגד המדינה, שהיא הרבה יותר דיגיטלית, תלויה הרבה יותר במערכות מתקדמות והיא הבעלים של התשתיות הקריטיות מבוססות המחשב. לארגוני טרור חסרי מדינה, כמו דאעש וחמאס, שהם בעלי יכולות סייבר, יש יתרון אסימטרי, שכן אין להם תשתיות קריטיות, מערכות פיננסיות ואף לא ציבור שיש לרכוש את אמונו ביכולתם למשול בו. ערעור אמון הציבור יכול להיעשות באמצעות פגיעה במערכת הפיננסית, במערכת הפוליטית או במערכת הדמוקרטית. לא צריך שמשהו באמת יקרוס במערכות הללו; מספיקה התחושה שמשהו רע הולך לקרות בהן. בעיה זו הופכת למורכבת עוד יותר בעידן הסייבר, שבו משטח התקיפה הולך ומתרחב. תרחישים אלה מדירים שינה מ"מערך הסייבר הלאומי".

מתארי איום נוספים שיש לתת עליהם את הדעת נוגעים להתפשטותם של כלי תקיפה מעצמתיים. הדוגמה המובהקת ביותר לכך אירעה במאי 2017, כאשר כלי סייבר שמיוחס לארצות הברית (Eternal Blue) זלג החוצה ממעבדות ה־NSA והגיע לידיה של צפון קוריאה, שהשתמשה בו ב"מתקפת כופר" (Ransomware) ברחבי העולם. ארצות הברית, שכאמור, ייצור כלי התקיפה מיוחס לה, הותקפה בעצמה, וכמוה גם בריטניה. דוח בריטי רשמי על התקיפה הצביע על 139 ניתוחים דחופים במערכת הבריאות הבריטית שנדחו ועל נזק בשווי של 2.5 מיליארד ליש"ט. להבדיל מנשק גרעיני, שזליגה שלו לידי גורמי טרור התרחשה עד כה רק בסרטים הוליוודיים, זליגה של אמצעי תקיפה מעצמתי בתחום הסייבר התרחשה במקרה זה במציאות.

כשמדובר במרחב הסייבר, כל השחקנים מחזיקים ביכולות, ולו בשל טבעם של כלי הסייבר: מדובר בקוד, שכאשר משגרים אותו, הוא בדרך כלל לא מושמד, ולפיכך קל להשתמש בו שוב כ"ראש חץ קיברנטי", הרבה יותר מאשר ב"ראש נפץ קינטי" שלא התפוצץ. זאת, כאמור, אם הנשק לא הושג קודם על ידי דליפתו ממעבדות הייצור שלו, כפי שקרה במקרה האמריקאי. מכאן, שישראל חשופה לשימוש בכלים מעצמתיים כנגדה.

מתארי איום נוספים, שקצרה היריעה מלפרט, הם האיום על שרשרת האספקה ועל ההגנה עליה, וכן פשיעת סייבר, שהאבחנה בינה ובין איומי הסייבר בממד הביטחון הלאומי הולכת ומיטשטשת, ככל שכנופיות פשע עובדות בשביל גופים ממשלתיים וביטחוניים זרים. כל המגמות והמתארים הללו מחייבים מודעות ופעולה בכל האמצעים כדי להתגונן מפניהם.

ישראל הייתה בין המדינות הראשונות שהשכילו לזהות מגמות ואיומים אלה. כבר בשנת 2002 הוגדרה ההגנה על תשתיות מחשב ומידע כקריטית וחיונית והוטלה על השב"כ. לאחר עשור הבינה המדינה כי נדרש לעשות מעבר לכך, וב־2012 הוקם, ביוזמת ראש הממשלה נתניהו, מטה לאומי שנועד לעסוק באסטרטגיה ובכל היבטי הסייבר הלאומיים. שנתיים לאחר מכן עלה הצורך ברשות אופרטיבית נפרדת שתטפל באירועי סייבר במרחב האזרחי, וב־2016 הוקמה "הרשות הלאומית להגנת הסייבר". מהר מאוד הבינה המדינה שלא טוב ששתי יחידות סמך אלו יפעלו בנפרד ואף בתחרות, והן אוחדו בינואר 2018 למערך אחוד, "מערך הסייבר הלאומי", שמשימתו הראשונה, המרכזית והעיקרית הינה הגנה על מרחב הסייבר הישראלי.

משימתו השנייה של "מערך הסייבר הלאומי", הכרוכה בעבותות עם הראשונה, היא קידום המובילות הישראלית בזירת הסייבר העולמית. מדינת ישראל יצרה מערך (Ecosystem) ייחודי בסייבר, המשלב ממשל, אקדמיה ותעשייה, מתוך תפיסה שללא השקעה בהון האנושי ובתעשייה, לא תתאפשר הגנה איכותית ועליונות לאורך זמן. ישראל ו"מערך הסייבר הלאומי" שלה הקימו, יחד עם האוניברסיטאות השונות, שישה מרכזי מחקר אקדמיים, וכן גיבשו מודל לקידום תעשיית הסייבר הישראלית ולהשקעה בתעשייה זו, התורמת למדינה, לחברה ולכלכלה, ובדרך זו גם לחוסן הלאומי בכלל ולהגנת הסייבר בפרט.

על מקומה של התעשייה הישראלית בתחום הסייבר ניתן ללמוד מהסקר השנתי של 500 החברות המובילות במרחב זה – ה"סייבר סיקיוריטי ונצ'רס" (Cyber Security Ventures). בסקר מופיעות 354 חברות אמריקאיות, אך שנייה לארצות הברית היא ישראל, עם 42 חברות. במקום השלישי מדורגת בריטניה עם מחצית מממספר החברות של ישראל, ואחריהן משתרך שובל ארוך של חברות ממדינות שונות. על פי הסקר, ישנן עוד כארבעים חברות ישראליות היושבות בארץ ורשומות בארצות הברית משיקולי מס ומסחר בורסאי, כך שהמספרים האמיתיים הם כ־310 חברות אמריקאיות מול כשמונים חברות ישראליות, כלומר פי ארבעה, כאשר היחס בין הכלכלות ובין האוכלוסיות בשתי מדינות אלו גבוה יותר בסדרי גודל.

ישראל השכילה לגבש אסטרטגיית הגנה בסייבר הכוללת שלוש שכבות: עמידות, חוסן והגנה לאומית. שכבת העמידות מקבילה להיגיינה, מעין שטיפת ידיים לפני האוכל כדי לשמור על הבריאות. השקעה בשכבה זו היא זולה יותר בסדר גודל מכל השקעה בשכבות הבאות. הרגולציה מכוונת בעיקר לשכבה זאת;

שכבת החוסן מתבססת על ההנחה שיהיו התקפות, ובכדי להחלים מהן כמה שיותר מהר ועם כמה שפחות נזק, יש להיערך בהתאם. השכבה השלישית, בה "מערך הסייבר הלאומי" לא עוסק כלל, היא הטיפול בתוקפים ובסיכולם. צה"ל וגופי הביטחון האחרים הם אלה שעוסקים בכך, אם כי "מערך הסייבר הלאומי" שותף למאמץ כגורם שמסייע, מכווין ומספק מידע.

אסטרטגיה זו עומדת בבסיס מבנהו של "מערך הסייבר הלאומי". המערך מפעיל מרכז חירום לאומי לטיפול באירועי סייבר, שפועל 24 שעות ביממה בכל ימות השנה. זהו מתקן ה־CERT הלאומי, היושב בפארק הסייבר בבאר שבע. כל אזרח וכל גוף שחושד שהוא מותקף בסייבר, יכול לפנות למרכז ולקבל מענה, סיוע ראשוני והכוונה.

לישראל יכולות סייבר עצמאיות רבות ברמה מעצמתית. עם זאת, גם במצבה הנוכחי יש לה צורך חיוני בשיתוף פעולה בין־לאומי. מערך הסייבר מקיים, לפיכך, שיתופי פעולה עם יותר משבעים מרכזי חירום במדינות שונות ברחבי העולם לטיפול באירועי סייבר. הוא גם חבר ולוקח חלק בפורומים בין־לאומיים בתחום הסייבר ושותף לתוכניות סיוע של גופים שונים, כמו הבנק העולמי, הבנק לפיתוח אמריקה הלטינית ואחרים. שיתוף הפעולה בסייבר נועד, בראש ובראשונה, לצרכים אופרטיביים והגנתיים. מי שתוקף את ישראל, למשל אירן, לא עושה זאת באופן ישיר, אלא עובר דרך מדינות אחרות, רובן ידידותיות לישראל. ככל שישראל תקיים יותר קשרים ותיצור שפה משותפת עם אותן מדינות, כך מלאכת ההגנה וההתרעה תהיה קלה, יעילה וטובה יותר.

דוגמה טובה לשילוב כוחות בין־לאומי, ש"מערך הסייבר הלאומי" מוביל ומשקיע בו מאמצים רבים, היא הגנת הסייבר בתעופה האזרחית, שנועדה להתמודד עם תופעות הקשורות במודרניזציה של התעופה, דבר שהוא מבורך כשלעצמו. מטוסי נוסעים, כמו "דרימליינר" ו"איר־באס 380", הם עתירי טכנולוגיה. תוכניות טיסה במטוסים החדישים ביותר, כמו גם בישנים יותר, מגיעות כיום על גבי מחשבי טאבלט ולא בכתב, כפי שהיה בעבר. זוהי רק דוגמה אחת לכיווני תקיפה אפשריים בסייבר. כדי להיערך לכך, המערך הביא להקמת מאגד (קונסורציום) של חברות ישראליות, בהובלת התעשייה האווירית, עם חברות כמו "צ'ק פוינט" ו"אל־על", לפיתוח ולהספקת מענים בתחום זה.

התמקדות "מערך הסייבר הלאומי" בהגנת הסייבר בתעופה האזרחית מביאה לידי ביטוי את השילוב בין שתי המשימות הראשיות שלו: הגנת מרחב הסייבר הישראלי – במקרה זה התעופה האזרחית, ובכללה שדות התעופה שמוגדרים כתשתיות קריטיות – וקידום המובילות העולמית של ישראל בסייבר. השילוב של תעופה, ביטחון וסייבר מתקשר במישרין לעוצמתה וליתרונה היחסי של ישראל.

מבלי להתעלם מהשיח הציבורי המתקיים בימים אלה על הגנת התהליך הדמוקרטי, "מערך הסייבר הלאומי" מתמקד באוריינטציה טכנולוגית סייברית ומקיים בחינה מערכתית כוללת, הרבה לפני יום הבחירות. המערך מקיים שיתוף פעולה עם ועדת הבחירות המרכזית לגבי תהליך ספירת הקולות, שהוא קצהו של תהליך שלם. כמו כן, המערך מספק לכלל המשק, לגופי התקשורת, למכוני הסקרים ולגופים נוספים שדרכם ניתן להשפיע על דעת הקהל המלצות להגנה על עצמם בסייבר, כדי לוודא שהתהליך הדמוקרטי בישראל יהיה נקי מהשפעות זרות ומהפרעות לא רצויות בתרחישי סייבר שונים.

בדמוקרטיה קיימת הפרדת רשויות. בסייבר נהוג לדבר על הפרדת רשתות. "מערך הסייבר הלאומי" מנחה תשתיות קריטיות שבאחריות הממשלה, אך אינו מנחה את הרשויות האחרות, כמו הרשות המחוקקת או הרשות השופטת. לא נכון לעשות זאת במשטר דמוקרטי, ומערך הסייבר מקפיד על כך ביותר. כך נמנעת הממשלה (באמצעות מערך הסייבר) מלהנחות את ועדת הבחירות המרכזית, את הכנסת או את מבקר המדינה בתחום הסייבר, ובמקום זאת פועלת על פי המודל של "הנחייה מרצון", כלומר, שיתוף פעולה וולונטרי בחילופי ידע, הפועל בצורה טובה. גופים אלה עצמאים להחליט מה הם עושים בתחום הסייבר וההגנה עליו ואיך הם עושים זאת, ו"מערך הסייבר הלאומי" מספק להם את הידע, המודיעין והתמיכה הכוללת כדי שיעמדו במשימה, כל אחד בתחומו ועל פי הגדרת האחריות שלו.

"מערך הסייבר הלאומי" עמל בימים אלה על גיבוש ארכיטקטורת הגנה לאומית בראייה רב־שנתית, טכנולוגית מתקדמת, שבסופה יהיה ניתן לשתף כמה שיותר מידע עם גורמים במרחב הסייבר הישראלי ולהגיע לגילוי, זיהוי וסילוק מוקדמים של תקיפות סייבר. חוק הסייבר, אותו מקדם "מערך הסייבר הלאומי", מהווה כלי קריטי להצלחת ההגנה על הסייבר במדינת ישראל. לצורך זה מקדם מערך הסייבר גם את קואליציית הסייבר הבין־לאומית מול הדרגים הבכירים של מדינות רבות הידידותיות לישראל.

העיקרון המנחה את "מערך הסייבר הלאומי" הוא שיתופיות, יצירת שותפויות והרחבת מעגל שותפי ההגנה, שכן אף גורם אחד – לא סוכנות, לא משרד ממשלתי וגם לא מדינה – לא יכולים להתמודד לבדם עם האתגרים העצומים שנסקרו כאן בתמציתיות רבה. יחדיו נעמוד איתן; בנפרד – ניפול.