אסטרטגיה לשילוב המגזר הפרטי בהגנת הסייבר הלאומי בישראל

שמואל אבן

בפברואר 2015 אישרה ממשלת ישראל את הקמת "הרשות הלאומית להגנה בסייבר", שתהווה זרוע ביצועית של המדינה להגנת המרחב האזרחי מפני איומי סייבר. אחד האתגרים של המדינה הוא לשלב בפעילות זו את המגזר הפרטי, הן כצרכן עיקרי של ההגנה והן כמשתתף במערך ההגנה. מאמר זה מציע למדינה אסטרטגיה בנושא. ככלל, מוצע שהמדינה תפעל להגן על מרחב הסייבר המדינתי עד לנקודת הכניסה הארגונית, וזאת באמצעות מעורבות עמוקה בארגונים המחוללים את הסייבר (חברות תקשוב, ספקי אינטרנט). כך יפחת הסיכון שהתקפות סייבר יגיעו לארגונים ולבתי האזרחים. כמו כן, מומלץ שהמדינה תרחיב את מעורבותה בהגנה נקודתית על ארגונים חיוניים במגזר הפרטי, תוך קביעת סדר עדיפויות לאומי, ואף תעמיק את הפיקוח, ההכוונה והתמריצים לעוסקים בהגנת הסייבר במגזר זה.

מילות מפתח: סייבר, ביטחון לאומי, ישראל, אסטרטגיה, מגזר פרטי

רקע

ישראל רואה בחומרה את האיומים בסייבר. ראש הממשלה בנימין נתניהו אמר בעניין זה בפברואר 2015: "האיום שנשקף בתחום הסייבר יכול לשתק מדינות. זה איום אסטרטגי שיכול להיות משתק ופוגע לא פחות מאיומים אחרים, ובתחומים מסוימים אף יותר, ואנחנו חייבים להיות ערוכים אליו ברמה הלאומית וברמה הבין־לאומית".[1] הדברים נאמרו במסגרת החלטת הממשלה להקים רשות לאומית להגנה בסייבר, "שתישא באחריות הלאומית הכוללת להגנת הסייבר, ותוקם במתווה תלת־שנתי הדרגתי".[2]

ד"ר שמואל אבן הוא חוקר בכיר במכון למחקרי ביטחון לאומי.

החלטה זו, כמו גם התפתחותו המהירה של מרחב הסייבר בעשרים השנים האחרונות, בכל תחומי העשייה האנושית, מעוררות את השאלה מהי אחריותה של המדינה בתחום ההגנה בסייבר וכיצד עליה לממש אותה. הנחת המוצא של הדיון היא שהדרך העיקרית לפרש את הנעשה בעולם הסייבר ולבחון את אחריות הממשלה לגביו היא באנלוגיה לנעשה עד כה במרחב "הפיסיקלי" התלת־ממדי ובשדה האלקטרומגנטי שעליו נשען הסייבר. זאת, תוך ביצוע התאמות לייחודיותו של מרחב הסייבר, כפי שאנו מבינים אותו.[3] ככלל, המדינה אמורה לשאת באחריות להגנה על אינטרסים לאומיים, על צורכי האוכלוסייה והמשק ועל שגרת החיים במדינה, וזאת גם בסייבר.

הבעיה היא שאחריות זו של הממשלה מתממשת כיום בהיקף מצומצם בלבד במגזר הפרטי, שהוא חלק הארי של האוכלוסייה והמשק.[4] המגזר הפרטי נושא בעצמו ברוב נטל ההגנה של מרחב הסייבר במדינה, וזאת לעומת המצב במרחבי פעולה אחרים ביבשה, באוויר ובים, שבהם כוחות הביטחון דומיננטיים בהגנת המדינה. באנלוגיה למרחב "הפיסיקלי", דומה המצב בסייבר למצב שבו כל פרט מגן על עצמו באמצעות מנעולים וסורגים, אבל המדינה אינה ערוכה להגיש לו עזרה ולהגן על הדרכים המובילות אליו מפני תקיפה.

מאמר זה מציע אסטרטגיה לשילוב המגזר הפרטי בהגנת הסייבר הלאומי בישראל. הוא כולל שלושה חלקים: בראשון מוצגים נתוני היסוד ותמונת המצב; בשני מובאת המלצה לאסטרטגיה לשילוב המגזר הפרטי בהגנת הסייבר הלאומי בישראל; בשלישי מובאת המלצה לקביעת סדר עדיפויות למעורבות הממשלה במגזר הפרטי במסגרת האסטרטגיה.

חלק א': נתוני יסוד ותמונת המצב

הסיכונים בסייבר על המדינה והמגזר הפרטי

הסיכון הגדול בתחום הסייבר שרואה המדינה הוא של חדירות ותקיפות ממניעים ביטחוניים־מדיניים על מערכות ביטחון, ממשל, תשתיות אזרחיות, המגזר העסקי ועוד. המדובר בחדירות ובתקיפות המבוצעות על ידי מדינות יריבות, ארגוני טרור וארגונים לאומניים למטרות ריגול, שיבוש או הרס. דוגמה: מתקפת סייבר רבת־עוצמה נגד חברת הנפט הלאומית הסעודית "עראמקו", באמצעות הווירוס "שאמון" (אוגוסט 2012). התקיפה, המיוחסת על פי הערכות לאיראן,[5] עשויה להמחיש שגם לאויבי ישראל יש נשק סייבר משמעותי.

הסיכון הנפוץ בתחום הסייבר במגזר הפרטי הוא של חדירות ותקיפות על יעדים כלכליים למטרות ריגול עסקי, פגיעה במתחרים, מעילות והונאות וכדומה. אלו נעשות על ידי גורמים עבריינים, מתחרים, עובדים עוינים וגנבי ידע. גניבת ידע עשויה להתבצע גם בידי סוכנויות של ממשלות זרות או שליחים מטעמן. הסיכון

הגדול של הריגול העסקי בסייבר ברמה הלאומית הוא ריקון המדינה מהקניין הרוחני שבתחומה. ישראל חשופה לסיכון זה בהיותה עתירת ידע וקניין רוחני, במיוחד במגזר ההי־טק, שעליו מתבססת צמיחת המשק.[6]

סיכון שכיח, הן במגזר הממשלתי והן במגזר הפרטי, הן תקלות במערכות תקשוב (למשל, תקלה בעת החלפת תוכנה) או בתשתיות המשמשות אותן מערכות (הפסקות חשמל, תקלות תקשורת). סיכון נוסף, לשני המגזרים, הוא פגיעה בסייבר בעקבות אסונות טבע, שריפות והצפות.

המושג הגנת סייבר

המושג "הגנה" משקף פעולות מסיביות ואקטיביות, לעומת "אבטחה" שהיא פעולה קלה ופסיבית יותר. בין החלטה להקמת "הרשות הלאומית לאבטחת מידע" בדצמבר 2002 ובין ההחלטה להקמת "הרשות הלאומית להגנה בסייבר" בפברואר 2015, עברה מדינת ישראל משימוש במושג אבטחת מידע לשימוש במושג הגנה בסייבר. הדבר מצביע על השינוי התפיסתי שחל אצלה ביחס לתחום זה. בארגונים במגזר הפרטי עדיין מקובל המושג "אבטחה", למשל אבטחת מערכות מידע.

הגנה על מרחב הסייבר המדינתי[7] או אבטחת הסייבר בארגונים (להלן: "הגנת סייבר") הן מכלול הפעולות, שנועדו להגן על המדינה או על ארגונים מפני דלף מידע מסווג דרך מערכות תקשוב, שימוש לא מורשה במערכות תקשוב, פגיעה בפעילות ובאמצעי תקשוב, ופגיעה במערכות משובצות מחשב (תחנות כוח, מגדלי פיקוח וכדומה) דרך הסייבר. כלומר, הגנת סייבר היא גם הגנה על הסייבר ותכולתו וגם הגנה בסייבר מפני תקיפות שעוברות דרך מרחב זה.

הגנת סייבר כוללת הגנה לוגית ופיסית על כל סוגי הרשתות ומערכות התקשוב על תכולתן – הכלים, הטכנולוגיות, הנתונים, רכיבי האחסון, הקשר ביניהם וזהות המשתמשים. בנוסף, שמירה על יכולת לתפקד במצב של אירוע סייבר (תקיפה, תקלה, אסון) ויכולת להחזיר במהירות האפשרית את כל אלה לתפקוד מלא לאחר אירוע. הגנת סייבר נדרשת גם מפני התקפות סייבר מרחוק (אינטרנט) או מהטווח הבינוני (התחברות לרשתות אלחוטיות בארגון), או מפני תקיפה ממגע קרוב (התחברות פיסית לרשת ארגונית, שימוש במשתף פעולה בארגון, גניבת ציוד מחשוב).

אבטחת המידע והסייבר בארגונים משלבת בין שני תחומים: הגנה לוגית (באמצעות תוכנה) על מערכות התקשוב ותחולתן, והגנה פיסית על המידע, החומרה, סביבת העבודה, פלטי מחשב מודפסים, הרשאות למערכות מידע, מורשים לכניסה למרחב העבודה, ארונות תקשורת והמבנה. באלה נכללות בדיקת מהימנות העובדים, הדרכה ובקרה על נגישות למערכות התקשוב. פירוש הדבר

הוא הגנה על מרחב הסייבר מבפנים ומבחוץ. לצד זאת נמשכת כמובן אבטחת המידע הפיסית המסורתית, שאינה בסייבר.

להבחנות שפורטו לעיל יש חשיבות גם לגבי חלוקת העבודה בתחום ההגנה בסייבר בין המדינה ובין ארגונים במגזר הפרטי, כפי שיוצג בהמשך.

בעיית הייחוס: מי עשה זאת?

טיפול בבעיה כלשהי מחייב לדעת בדרך כלל את מקורה. בשל אופיו של מרחב הסייבר, עשוי לעתים להתעורר קושי לזהות את הגורם שניתן לייחס לו את האירוע או אפילו את הקטגוריה: האם מדובר בתוקף פלילי, באויב מדינתי, באירוע שמקורו בתקלה? לעניין זה חשיבות גם בהקשר של מידת מעורבותה של המדינה בטיפול באירוע, ואף בפיצוי הנפגעים, כפי שניתן להשליך מהמרחב "הפיסיקלי" (למשל, פיצוי נפגעי טרור ונזקי מלחמה). במקרים לא מעטים ניתן להעריך את הגורם לאירוע באמצעות חקירת המכלול: נסיבות האירוע, חתימת התקיפה, שיטת הפעולה והתנהלותה, כלי התקיפה, המטרות וכדומה. גם אם הערכה כזו אינה מוצקה כדי לעמוד במבחן משפטי, היא יכולה להספיק לצורך קביעת מדיניות.

זכות הפרטיות בסייבר

זכות הפרטיות בסייבר היא סוגיה משפטית ואתית הנוגעת ליחסי ממשלה־פרט וליחסים בין הפרטים עצמם, וזוכה לעניין ציבורי.[8] לצורך הדיון יצוין כי מוסדות המדינה מנועים על פי חוק מלפעול באופן חופשי במערכות תקשוב של אזרחים וארגונים למיניהם, במיוחד במצב של שגרה. זו אחת הסיבות לכך שקשה לעשות שימוש ביכולות סייבר צבאיות ללחימה במרחב הסייבר האזרחי המקומי (להבדיל, למשל, מאשר במרחב האווירי). הגופים הממשלתיים המורשים לכך נדרשים לעשות זאת בצמצום ובהתאם להוראות החוק והדין. עם זאת, טכנולוגיות מתפתחות, כמו יכולות לזיהוי אנומליה בסייבר, מקלות על היכולת לזהות אירועי סייבר חריגים, גם בלא להיכנס לפרטי מידע אישי.

מאפייני המגזר הפרטי בסייבר

המגזר הפרטי הוא הקבוצה הגדולה במדינה, ונכללים בו תאגידים ובעלי עסקים פרטיים, תאגידים ציבוריים שאינם בשליטת הממשלה ואזרחים המשתמשים בסייבר לצרכיהם השונים. המגזר הפרטי הוא המקור להכנסות המדינה ממסים וממט"ח, וכן ספק עיקרי של מוצרים, שירותים, תעסוקה, פעילות חברתית ועוד. בלא ניהול נכון של הזדמנויות וסיכונים בסייבר, חברות רבות יתקשו להשיג את יעדיהן. חלקן יאבדו את היכולת להתחרות וייעלמו מהשוק. מכאן החשיבות להפחתת החשיפה של המגזר הפרטי לסיכונים של אירועי סייבר (תקיפות, ריגול, תקלות, אסונות).

במגזר הפרטי בולטים ארגונים שפעילותם נשענת כמעט במלואה על סייבר – בהם ארגונים המחוללים את הסייבר (חברות מחשוב, תקשורת, אינטרנט מידע ועוד), ארגוני המגזר הפיננסי (בנקים, חברות ביטוח, בתי השקעות, חברות כרטיסי אשראי ועוד), תעשיות עתירות ידע ועוד. הסייבר הפך ארגונים אלה לברי־גישה לתוקפים ביטחוניים ופליליים. דוגמה למתקפות סייבר על מערכת פיננסית היא פריצת סייבר רחבת היקף שבוצעה בדרום קוריאה בינואר 2014, שבמסגרתה נגנבו פרטי כרטיסי האשראי של כארבעים אחוזים מתושבי המדינה. בעקבות זאת התפטרו כשלושים בכירים בחברות פיננסיות שונות.[9] דוגמה נוספת היא מתקפה המיוחסת לאיראן, שבוצעה בשלהי שנת 2012 על עשרות אתרי בנקים אמריקאיים, שלא גרמה נזק ממושך.[10] בשלב זה אמנם לא ידוע על קריסת בנק כתוצאה מתקיפת סייבר (להוציא הונאות פיננסיות של אנשים מבפנים, תוך שימוש בסייבר הארגוני), אולם נראה שארגונים כאלה ובכלל אינם נוטים לחשוף את הנזקים שגרמו להם תקיפות בסייבר מחשש לפגיעה במוניטין.

בתוך כך גבר איום הסייבר גם על הארגונים האסטרטגיים, שלהם תשתיות ומתקני ייצור פיסיים, אותם ניתן לתקוף גם באמצעי לחימה קינטיים. המדובר בתחנות כוח, במפעלי מלט, מזון, תרופות וכימיה, בארגוני תחבורה, אנרגיה ועוד. לדוגמה, בעקבות מתקפת הסייבר באמצעות הווירוס "שאמון", נאלצה חברת הנפט הסעודית "עראמקו" להחליף את מערכות המחשוב (30 אלף תחנות עבודה ואלפיים שרתים).[11]

הארגונים במגזר הפרטי מגינים על עצמם באופן יחידני (לא מערכתי). האסטרטגיה שלהם להגנת מרחב הסייבר הארגוני כוללת: עיצוב הסייבר הארגוני להגנה – למשל, הקמת רשת פנים־ארגונית מאובטחת; פעולות למניעת חדירה עוינת מבחוץ (דרך האינטרנט) ומבפנים (דרך עמדות עבודה, נקודות חיבור, עובדים שכשלו). בנסיבות של חדירה – מתבצעות פעולות להגבלת הנזק, באמצעות איתור החודר ונטרולו, הגבלת תנועת החודר באמצעות כלים במערך ההגנה. בהמשך – ניהול אירוע הסייבר, הפעלת תוכנית להמשכיות עסקית במידת הצורך, שיקום וחזרה לתפקוד מלא, הפקת לקחים מהאירוע וחיזוק ההגנה.

המגזר הפרטי נושא במספר תפקידים במערך ההגנה המדינתי: תפקידו הראשון הוא כצרכן של הגנה בסייבר. בתפקידו השני הוא משתתף פסיבי במערך ההגנה – מגן על עצמו, מנטר תעבורה בתחומו (בכפוף להוראות רגולטוריות ולמגבלות בתחום הפרטיות), מדווח לרשויות על תקיפות אצלו. בתפקידו השלישי משתתף המגזר הפרטי באופן אקטיבי בהגנה – באמצעות מגזר התעשיות והשירותים בתחום אבטחת מידע וסייבר.

הגורמים המאיצים והמעכבים את התפתחות הגנת הסייבר במגזר הפרטי

המגמה הכללית במגזר הפרטי היא של עלייה במודעות לאבטחת הסייבר, אולם יש לזכור כי מגזר זה אינו עשוי מקשה אחת וגם יכולות התוקפים משתכללות. את התקדמות ההגנה בסייבר בארגון מכתיבים גורמים מעכבים וגורמים מאיצים. חשוב שהממשלה תכיר אותם, אם ברצונה להחליש את השפעת הגורמים המעכבים ולהגביר את השפעת הגורמים המאיצים.

גורמים מאיצים

בין הגורמים המאיצים את ההגנה בסייבר במגזר הפרטי ניתן למנות את הבאים:

א. הצורך להגן על הפעילות העסקית והרווחיות של חברה מפני סיכוני הסייבר הגוברים (האינטרס העיקרי).
ב. חשיפה ישירה לאירועי סייבר, עיסוק תקשורתי בנושא ומאמצי שיווק של חברות אבטחת הסייבר.
ג. רגולציה – הנחיות רגולטוריות לאבטחת מידע וסייבר הקיימות למשל במגזר הפיננסי ו"בגופים מונחים".
ד. הקמת פונקציות לאבטחת מידע וסייבר בארגונים. זו מחוללת פעילות שיטתית ומגבירה את המודעות.
ה. חפיפה ניכרת בין המענה לתקיפה בסייבר לבין המענה לסיכונים מסורתיים, כמו מניעת תקלות מחשוב, מניעת מעילות והונאות, אבטחת מידע. חפיפה כזו מאפשרת לתת מענה לכמה סיכונים באותה עלות.
ו. התפתחות תחום ניהול הסיכונים בארגונים, התורמת גם לניהול סיכוני אבטחת מידע וסייבר.

גורמים מעכבים

בין הגורמים המעכבים הגנה בסייבר במגזר הפרטי:

א. הגנה בסייבר כרוכה בעלויות כספיות גבוהות, המפחיתות מהרווח של הארגון או מתחרות על סעיפים אחרים בתקציב הארגוני.
ב. מערכות הגנה נתפסות לעתים כנטל על הפעילות התפעולית והעסקית. למשל, הן מגבילות את הגישה הישירה לאינטרנט ומכבידות בסיסמאות מורכבות. הן עלולות להאט מערכות תפעוליות ולהקשות גם על קבלת דוא"ל לגיטימי.
ג. המניעה היא פסיבית, וגם אם היא מוצלחת, ההישג של מנהל אבטחת מידע לא זוכה בהכרח להכרה (למרות שבארגונים קיימות תוכנות המדווחות על תקיפות שהתגלו וסוכלו).

ד. סיכון הפגיעה בסייבר הוא עוד אחד מהסיכונים שיש לנהלם בארגון, כמו סיכון לאובדן נתח שוק, סיכונים פיננסיים, סיכונים לאי־עמידה ברגולציה, סיכונים תפעוליים וכדומה.
ה. רגולציה מכבידה. במקרים מסוימים עלול ארגון לפעול שלא מתוך אמון ברגולציה אלא רק כדי לצאת ידי חובה, וזאת לפעמים גם על חשבון צעדי הגנה חשובים יותר.
ו. חשש לפגיעה במוניטין כתוצאה מדיווח על אירועי סייבר.

ארגונים ממשלתיים העוסקים בהגנת הסייבר האזרחי

קיימים ארגונים ממשלתיים לא מעטים העוסקים בתחום הגנת הסייבר האזרחי, הכולל בתוכו את המגזר הפרטי, שהוקמו או נכנסו לתחום עם התפתחות הסייבר. כיום, גופים אלה אינם בהכרח מתואמים ביניהם, מבחינת חלוקות האחריות והפעילות, בין היתר משום שהם כפופים למשרדי ממשלה שונים. הקמת הרשות להגנה בסייבר עשויה להיות הזדמנות להסדרת הפעילות בתחום זה במגזר האזרחי. להלן יוצגו הגופים הממשלתיים העיקרים ותחומי פעילותם בהקשר זה.

כוחות הביטחון

תפיסת הביטחון של ישראל נשענת בעיקרה על צה"ל, שלצדו פועלים כוחות ביטחון נוספים. צה"ל, כמו צבאות אחרים במדינות דמוקרטיות, מוגבל ביכולתו לפעול במגזר האזרחי במדינה בתחום הסייבר. עם זאת, ובאנלוגיה למוכר מהמרחב "הפיסיקלי", ניתן להניח שצה"ל, וכן "המוסד", נושאים בתפקידי הגנה על מרחב הסייבר המדינתי מפני אויבים מחוץ למדינה, וזאת בדרכים הבאות:

א. הרתעה של אויבים ויריבים מפני תקיפה בסייבר באמצעות קיומה של יכולת תגובה אמינה.[12]
ב. מתן התרעה מודיעינית למערך ההגנה המקומי מפני תקיפות סייבר מבחוץ.
ג. פעולות לסיכול תקיפה מחוץ למדינה.
ד. התקפות־נגד על מקורות התקיפה או בעקבות התקיפה.

לארגוני ביטחון שפועלים בתוך המדינה, כמו השב"כ, תפקיד מרכזי במערך ההגנה מפני מתקפות סייבר, כולל סיכול ופעולות אקטיביות. לפי החטיבה להגנת הסייבר בשב"כ: "המאבק להגנה על גופי התשתיות הקריטיות של ישראל מפני מתקפות הסייבר מלווה במלחמת מוחות [...] החומות בהחלט לא מספיקות, נדרשות גם תחבולות, כמו שימוש בסוכנים כפולים ועוד המצאות יצירתיות ברשת".[13]

הרשות הממלכתית לאבטחת מידע

הרשות הממלכתית לאבטחת מידע (רא"ם), שעל הקמתה החליטה הממשלה בדצמבר 2002, פועלת במסגרת השב"כ. היא "מופקדת על הנחיה מקצועית של

הגופים המונחים שבאחריותה בתחום אבטחת תשתיות מחשב חיוניות מפני איומי טרור וחבלה בתחום אבטחת מידע מסווג ומפני איומי ריגול וחשיפה".[14] רא"ם מנחה מספר עשרות של גופים אזרחיים במגזר הממשלתי והפרטי, שפגיעה בהם יכולה להסב נזק חמור למדינה. מדובר, בין השאר, ברכבת ישראל, בחברת "מקורות", בחברות הסלולר, בחברת החשמל, בחברת "בזק", בחברת "אל־על", בחברת "צים" ועוד. שלוש האחרונות היו חברות ממשלתיות שהופרטו.

המטה הקיברנטי הלאומי

המטה הקיברנטי הלאומי הוקם בינואר 2012 במשרד ראש הממשלה. ייעודו העיקרי הוא להוות "גוף מטה לראש הממשלה, לממשלה ולוועדותיה, אשר ממליץ על מדיניות לאומית ומקדם את יישומה בתחום הקיברנטי, בכפוף לכל דין והחלטות ממשלה". למעשה מדובר באחריות כוללת של המטה על מכלול הסייבר, ובמסגרת זו גם על ההגנה בסייבר. במסגרת זו, המטה אחראי לבצע הערכות מצב בתחום הגנת הסייבר האזרחי, לגבש מדיניות, להוות גורם מסדיר בתחומי הביטחון הקיברנטי ולגבש ולפרסם אזהרות, מידע והנחיות לציבור בנושא זה.[15]

הרשות הלאומית להגנה בסייבר

כאמור, ב־15 בפברואר 2015 אישרה הממשלה את הקמת הרשות הלאומית להגנה בסייבר. לפי הודעת הממשלה, "הרשות תנהל את פעולות ההגנה כדי לתת מענה מקיף נגד תקיפות סייבר, לרבות טיפול באיומים ובאירועים בזמן אמת. הרשות גם תפעיל מרכז לסיוע בהתמודדות עם איומי סייבר – ה־CERT הלאומי (Cyber Event Readiness Team) – במטרה לחזק את חוסנם של כלל הארגונים והמגזרים במשק [...] הרשות והמטה יהוו מערך סייבר לאומי אחוד במשרד ראש הממשלה, בראשות ראש המטה ד"ר אביתר מתניה".[16]

הממשלה אישרה באותו מעמד מספר צעדי מדיניות שימומשו על ידי הרשות הלאומית להגנה בסייבר בעתיד, בהם: מהלך להסדרת שוק שירותי הגנת הסייבר, הכולל בעלי מקצוע, מוצרים ושירותים רלוונטיים; הסדרה של היערכות הארגונים במשק בתחום הגנת הסייבר מתוך כוונה להתבסס ככל האפשר על העצמת הרגולטורים הקיימים; תוכנית להפעלת מנגנוני סיוע ותמרוץ לארגונים במשק שיפעלו להעלאת רמת מוכנותם לאיומי סייבר.

היחידה להגנת הסייבר בממשלה

ב־15 בפברואר 2015 הוחלט גם על הקמת היחידה להגנת הסייבר בממשלה, שתהווה גוף הנחיה מקצועית עבור כלל הממשלה. היחידה הוקמה במערך התקשוב הממשלתי במשרד ראש הממשלה. בהחלטת הממשלה נקבע כי היחידה תקים מרכז שליטה ובקרה ממשלתי מול איומי סייבר.[17]

בנק ישראל ומשרד האוצר

בנק ישראל ומשרד האוצר מנחים רגולטורית את המגזר הפיננסי גם בתחום הסייבר. הבנקים מונחים על ידי המפקח על הבנקים. חברות הביטוח ושאר הגופים הפיננסיים מונחים רגולטורית על ידי משרד האוצר.[18]

בשנת 2012 הוקמה בבנק ישראל יחידה האחראית על נושא הסיכונים התפעוליים בבנקים, ובראשם סיכוני הטכנולוגיה ואבטחת המידע.[19] בתחילת 2014 אישר בנק ישראל הקמת מרכז משותף להגנת הסייבר בבנקים, שירוכז תחת חברת שב"א הנמצאת בשליטת הבנקים. במקביל העביר בנק ישראל טיוטת חוזר לבנקים בנושא "ניהול הסיכון הקיברנטי", על פיה נדרשו הבנקים להתייחס במפורט להתמודדות עם איומי הסייבר, ובכלל זה לקבוע אסטרטגיה, להקים בבנק מערך הגנה על הסייבר, לצמצם הרשאות למערכות מידע, לפתוח חדר מצב בעת התקפת סייבר, לדווח לבנק ישראל על אירועי תקיפה בסייבר ועוד.[20]

הרשות למשפט, טכנולוגיה ומידע

הרשות למשפט, טכנולוגיה ומידע (רמו"ט) הוקמה על ידי משרד המשפטים בספטמבר 2006. היעדים של רמו"ט הם לחזק את ההגנה על מידע אישי, להסדיר ולפקח על השימוש בחתימות אלקטרוניות ולהגביר את האכיפה בנוגע לעבירות פגיעה בפרטיות. רמו"ט גם משמש כמרכז ידע לחקיקה ואף לגבי פרויקטים בעלי היבטים טכנולוגיים, כגון "ממשל זמין".[21]

משטרת ישראל

בנובמבר 2012 הכריז מפכ"ל המשטרה על הקמת יחידה חדשה ללוחמת סייבר. ההכרזה באה בעקבות התגברות הניסיונות של גורמים עוינים לבצע מתקפות מקוונות על תשתיות המחשבים בישראל והתפשטות פשיעת הסייבר.[22]

האינטרסים המשותפים לממשלה ולמגזר הפרטי בתחום הגנת הסייבר

לממשלה ולמגזר הפרטי יש, ככלל, אינטרס משותף לצמצם את הסיכונים במרחב הסייבר, שבו פועלים כולם, ולהתמודד בהצלחה עם אירועי סייבר למיניהם. עם זאת, כל אחד מהצדדים שם דגשים שונים במאמציו להגנה בסייבר.

לממשלה אחריות כוללת על הביטחון במדינה. ניתן להניח שהיא נותנת עדיפות להתמודדות עם התקפות סייבר מצד מדינות יריבות וארגוני טרור, בהשוואה למשל למצב של תקלת סייבר בחברה מסוימת הגורמת לנזק בהיקף דומה. בנוסף, בהיותה אחראית על האינטרס הציבורי, מעורבותה של הממשלה תהיה גדולה יותר ככל שציבור רב יותר יושפע מאירוע הסייבר.

המגזר הפרטי מוטרד, בראש ובראשונה, מפעולות פליליות של ריגול עסקי, פשיעה מבחוץ, מעילות והונאות של עובדים וספקים ותקלות בסייבר, הפוגעות

בתפקוד החברות וברווחים שלהן. הסיכון של מעילה גדולה או תקלה חמורה בחברה הוא גדול יותר מהסיכון של תקיפה על ידי אויבים של המדינה, שהינה בעיה קולקטיבית של כלל המגזר העסקי, שהאחריות לטיפול בה נתונה בידי הממשלה. לחברות פרטיות שעומדות בהוראות החוק יש אחריות מוגבלת (בע"מ), אם בכלל, לנזקים שעלולים להיגרם למדינה כתוצאה מאירועי סייבר, במיוחד כאשר מדובר בהתקפת אויב.

אף על פי כן, קיים מגוון של סיכונים בתחום הסייבר המשותפים לשניהם, וכן פתרונות הגנה רבים שאינם קשורים לסוג התוקף או לזהותו, כך שממילא מתחייב שיתוף פעולה הדוק בין שני הצדדים.

לכל אחד מהצדדים יש יתרונות יחסיים, החשובים לשיתוף הפעולה ביניהם. לדוגמה: לממשלה יש יתרון במודיעין, בקשרים ענפים עם ארגונים מקומיים ומדינות זרות,[23] בראייה כוללת וביכולת ארגונית ורגולטורית לרכז את כל השחקנים לצורך הקמת מערך הגנה אופטימלי והפעלתו. לעומת זאת, לארגונים במגזר הפרטי יש כמות גדולה של משאבי מחשב (בהם גם ניתן להציב חיישנים ומערכות הגנה, במגבלות החוק), יכולת לספק לממשלה מידע ואינדיקציות על מתקפות, מעבדות מתקדמות שבהן יכולה הממשלה לזהות את כלי התקיפה, יכולות טכנולוגיות הדרושות לייצור אמצעי הגנה, גישה עמוקה למערכות התקשורת במדינה ו"צבא" של אנשי סייבר אזרחיים שניתן לרתום למטרות המשותפות.

אחד הקשיים בדרך לשיתוף פעולה מלא בין הממשלה ובין המגזר הפרטי הוא, שלארגונים פרטיים אין עניין לחשוף את מרחב הסייבר בפני גורמי ממשלה ("האח הגדול"), בין היתר בשל הצורך לשמור על פרטיות הלקוחות, הספקים והעובדים; וכן בשל חשש לפגיעה במוניטין כתוצאה מדיווח על אירועי סייבר. זאת, במיוחד כאשר המדינה ממילא לא מציעה להם סיוע משמעותי בתמורה.

ככלל, ניתן להניח כי המגזר הפרטי מצפה מהמדינה לשיפור רמת הביטחון במרחב הסייבר המדינתי, בלא שזו תטיל עליו עלויות נוספות.

חלק ב': הצעה לאסטרטגיה לשילוב המגזר הפרטי בהגנת הסייבר הלאומי

שינוי דרמטי בהגנת הסייבר עשוי לחול בעתיד באמצעות שינוי מבני עמוק ברשת האינטרנט והסדרת התנועה בה על ידי ממשלות, כדי להגן על החברה האנושית. בינתיים, על המדינה למצוא פתרונות להגנה על הסייבר, הישימים במרחב האינטרנט הפתוח.

מטרת האסטרטגיה המוצעת היא לשלב את המגזר הפרטי בהגנת הסייבר הלאומי, הן כצרכן של הגנה בסייבר והן כמשתתף במערך ההגנה על הסייבר וזאת

לשם יצירת מרחב סייבר מדינתי מוגן ככל האפשר, תוך ניצול יעיל של משאבים לאומיים.

עקרונות האסטרטגיה

הגנה היקפית ומרחבית בסייבר

השאיפה היא שהמדינה תדאג ליצירת מרחב סייבר מדינתי מוגן ככל האפשר, עד ל"נקודת הכניסה הארגונית" (כפי שהיא דואגת, למשל, לאבטחת אספקת חשמל יציבה, מים זכים, דרכי תחבורה תקינות ועוד). גישה זו תחייב את המדינה לתת עדיפות לנקודות הכניסה ולצמתים של תשתיות הסייבר הישראלי, ובכלל זה להנחות ולפקח מקרוב על חברות תקשורת וספקי הגישה לאינטרנט. זאת, כדי לצמצם את הסבירות לתקיפה מרחוק של מערכות סייבר בארגונים ובבתי אזרחים. השאיפה היא שמחוללי הסייבר במדינה לא יגנו רק על עצמם, אלא גם יסכלו מתקפות העוברות דרכם. בנוסף, המדינה תגביר את הפיקוח גם על חברות מחשוב, שירותי אבטחת מידע וכדומה, כדי לשפר את ביטחון הסייבר במדינה בכללותו (לרבות במרחב הסייבר הארגוני).

מעורבות המדינה בהגנה נקודתית בסייבר על ארגונים במגזר הפרטי

המדינה תרחיב את מאמציה לשיפור ההגנה על הסייבר הארגוני בארגונים במגזר הפרטי שהשפעתם על הביטחון הלאומי (בתחום האזרחי והביטחוני) רבה, וזאת בהתאם לסדר העדיפויות שתקבע. מעורבות המדינה בהנחיה ובסיוע לארגונים לשם הגנה נגד איומים ביטחוניים ואיומים אזרחיים חריגים (פשע מאורגן, רעידת אדמה) תהיה נדבך נוסף על מערך ההגנה הרגיל שלהם, המשמש אותם כיום להתמודדות עם האיומים האזרחיים שמצויים אצלם בסדר עדיפות גבוה (אירועים פליליים, תקלות, שריפות ועוד).

מאמץ כללי לחיזוק ההגנה במגזר הפרטי

המדינה תפעל לחזק את הגורמים המאיצים ולהחליש את הגורמים המעכבים את התפתחות הגנת הסייבר במגזר הפרטי. המדינה תנהיג רגולציה במשורה ובהתייעצות מוקדמת עם מגזר זה. במקביל היא תעמיד לרשותו שירותים ייחודיים ומידע המבוססים על יתרון לגודל, ראייה כוללת, מומחיות נרכשת ונגישות למידע מודיעיני ולטכנולוגיות רגישות (במגבלות ביטחון מידע). המדינה תמליץ למגזר הפרטי על מערכות ושיטות הגנה, תספק לו התרעות, תייעץ לו ואף תתערב בעת משבר, והכל בהתאם לסדר העדיפויות שתקבע. להשלמת התמונה, המדינה תמשיך לבצע פעולות הגנה פסיביות ואקטיביות להגנת הסייבר המדינתי, גם בלא מגע עם המגזר הפרטי.

כיווני פעולה

כיווני הפעולה של האסטרטגיה המוצעת למדינה יהיו כלהלן:

א. **מיפוי מרחב הסייבר המדינתי וביצוע סקר סיכונים מקיף של המגזר הפרטי בסייבר**. במסגרת זו יש לחקור את ענפי המשק השונים ואת הקשר ביניהם, לנתח את גורמי הסיכון ולזהות נתיבים קריטיים ונקודות קריטיות האופייניים לכל מגזר בנפרד וכאלה המשותפים לכולם. הסקר יכלול שימוש בבדיקות חדירות. כך ניתן יהיה לתת עדיפות גבוהה בהגנה גם לחברות קטנות הנמצאות בצמתים קריטיים להגנת המדינה.

ב. **קביעת סדר עדיפויות של המדינה למעורבותה בהגנת המגזר הפרטי בסייבר**. סדר העדיפויות ייקבע לפי קריטריונים שתגבש המדינה בשיתוף פעולה עם המגזר הפרטי. הוא יתבטא בדרגות מעורבותה של המדינה בארגונים במגזר הפרטי בתרחישים שונים (פירוט בהמשך).

ג. **הכנת תוכנית עבודה להפחתת סיכוני הסייבר**. תוכנית זו תחתור למקסם את התועלת הלאומית מסך ההוצאה הלאומית המתוכננת להגנת הסייבר (כולל במגזר הפרטי) ואת התקציבים שמייעדת המדינה לצורך זה.

ד. **הסדרת השיטה ותחומי האחריות, הסמכות והתיאום של מוסדות הממשלה והארגונים במדינה העוסקים בתחום הגנת הסייבר**. לאור רשימת הגופים הממשלתיים הנוגעים להגנת הסייבר האזרחי ומשימותיהם, מוצע לקבוע או לרענן את הגדרת תחומי האחריות של גופים אלה, את מהות הקשרים ביניהם ואת הקשר שלהם למגזר הפרטי, וזאת מתוך ראייה מערכתית. למשל, יש לקבוע את חלוקת העבודה והסינרגיה בין השב"כ ובין המטה הקיברנטי הלאומי והרשות להגנה בסייבר, את תפקידו של משרד התקשורת שבתחומו פועלים מחוללי הסייבר ואת המנגנון לבירור מחלוקות בין הגופים.

ה. **הסדרת השיטה ותחומי האחריות, הסמכות והתיאום בין ארגוני ביטחון החוץ העוסקים בלוחמת סייבר**. כך, למשל, יש לקבוע מי אחראי על שרשרת ההתרעה בסייבר, הכוללת איסוף, מחקר ומתן ההתרעה, מי אחראי ליצור הרתעה בסייבר וכדומה.

ו. **עוצמת הרגולציה**. על הרגולציה להיות פשוטה, קלה לאכיפה ובעלת ערך ברור מבחינת עלות־תועלת. רגולציה עודפת במגזר הפרטי עלולה לגרום לכך שהעלויות הנוספות יפגעו ברווח ובשרידות של חברות. על עוצמת הרגולציה להיות מושפעת מרמות הנזק שייגרם למדינה ולמשק כתוצאה מתקיפת ארגון מסוים, וזאת בהתאם לסדר העדיפויות שייקבע. מוטב לקבוע את תחום ההגנה על הסייבר כחריג בתחום ההגבלים העסקיים, כך שחברות עסקיות מאותו מגזר יוכלו לחלוק מידע ביניהן ולשתף פעולה בתחום הגנת הסייבר, בהתאם להוראות שיקבעו.

ז. **אחריות גופי המגזר הפרטי כלפי הממשלה**. יש לקבוע את אחריותם של גופים אלה, למשל על ידי דיווח לרשויות, לספקים, ללקוחות ולצרכנים על חדירה לסייבר הארגוני, וזאת בנסיבות הרלוונטיות להם.

ח. **מתן תמריצים לחברות ולארגונים להתגונן בסייבר**. מדובר למשל במעורבות המדינה בייעוץ בנוגע למדיניות, שיטות ומוצרי הגנה בסייבר; סבסוד בדיקות חדירות של מערכות סייבר בארגונים, וכדומה.

ט. **פיקוח על שירותי ההגנה בסייבר במגזר הפרטי**. למשל, יש לבדוק ולהסמיך חברות המייעצות ומספקות שירותים ואמצעים להגנה בסייבר.[24] מוצע לבחון את תחום ביטוח הסייבר ולהסדירו במידת הצורך.

י. **צמצום מגבלות בירוקרטיות**. יש לצמצם את המגבלות הבירוקרטיות המעכבות את פעולות ההגנה בסייבר. לדוגמה: הקמת צוות הכוננות הלאומי למצבי חירום בסייבר (CERT) היא צורך בסיסי שהיה מוכר מזה שנים, אך רק בשנת 2015 הגיע תהליך ההקמה לשלב המכרזים.

יא. **מיצוב מעמדו של CERT**. יש לפעול כדי שצוות הכוננות הלאומי למצבי חירום בסייבר יהיה המקשר בין המדינה ובין המגזר הפרטי לשם העברת מידע דו־סטרי בתחום הסייבר. עליו ספק למגזר הפרטי ערך מוסף גבוה ולהיות זמין גם בתנאי משבר, כדי שייתפס כגורם מועיל.

יב. **שיפור היכולת של המדינה וארגונים פרטיים לפעול במגזר הפרטי להגנת הסייבר**. יש לעשות זאת בכפוף לערכים דמוקרטיים ובאמצעות עדכוני חקיקה, הכוונה של המגזר הפרטי (למשל, החתמת עובדים מראש בנוגע לכוונת החברה לנטר את תחנות העבודה שלהם), והגברת השימוש בטכנולוגיות לזיהוי אנומליה, ללא חשיפת תכנים פרטיים.

יג. **שיתוף פעולה עם גורמים בחו"ל**. מוצע ללמוד מניסיונן של מדינות זרות בנוגע להגנת המגזר הפרטי בסייבר ולפעול לשיתופי פעולה עם מדינות וארגונים זרים בתחום זה.

חלק ג': שיטה לקביעת סדר העדיפויות למעורבות ממשלתית במגזר הפרטי

הצורך לקבוע סדר עדיפויות בסיסי למעורבות הממשלה בהגנת הסייבר הוא בעל חשיבות, במיוחד בשל מגבלת המשאבים של המדינה. סדר העדיפויות הקונקרטי יושפע גם מהערכות מצב שיתבססו על סקרי סיכונים שוטפים, מידע מודיעיני וגורמים נוספים.

העיקרון הכללי הוא שלמדינה יש אינטרס מיוחד במעורבות בהגנת הסייבר במגזר הפרטי בשני מצבים: כאשר קיים סיכון לאירוע בעל השפעה מערכתית שלילית על המדינה (המשק, האוכלוסייה וכדומה); וכאשר יש סיכון של התקפה

מצד אויב. סיכון המגלם את שני המצבים יקבל תשומת לב עליונה, והדרך היעילה ביותר לטיפול בו תקבל עדיפות ראשונה. השאר הם מצבי ביניים, כפי שיפורט בהמשך.

שלושת הקריטריונים העיקריים לסדר העדיפויות של מעורבות הממשלה בהגנת המגזר הפרטי הם: הערכת תוחלת הנזק;[25] הגורם לסיכון (תקיפה מצד אויב, מצד גורם פלילי, תקלה, אסון); ועלות הפחתת הסיכון, במונחי זמן וכסף, ביחס לתוחלת הנזק (עלות־תועלת).

להלן נבחן את סדר העדיפויות הבסיסי להגנה בסייבר לפי כל אחד מהקריטריונים. הירידה לפרטים (על איזה סוג ארגון יש להגן בעדיפות א' וכדומה) נועדה להמחשת השיטה בלבד.

קריטריון ראשון: תוחלת הנזק

לממשלה עניין במעורבות בארגונים פרטיים, הן בהנחיה רגולטורית מוקדמת והן בהתמודדות עם משבר סייבר. לפי קריטריון זה עדיפות במעורבותה תינתן לאותם גופים שלפגיעה בהם תהיה תוחלת נזק גדולה על המדינה, יהיה הגורם לאירוע הסייבר אשר יהיה (אפילו תקלה).

המערכות והארגונים שיזכו לעדיפות במעורבות המדינה עשויים להיות, בעדיפות א', ארגונים גדולים ו/או בעלי השפעה מערכתית גבוהה מאוד מהסוגים הבאים:[26]

א. **מחוללי הסייבר – תשתיות תקשוב וארגוני תקשוב גדולים**. ארגונים אלה יוצרים את מרחב הסייבר המדינתי ואת הקשר בין המדינה לעולם. המדינה תיתן עדיפות גבוהה להגנתם ולמניעת מעבר התקפות דרכם. הריכוזיות הגבוהה בתחום התקשורת חושפת את ישראל לסיכוני סייבר גבוהים, אולם יש עמה גם יתרון בתחום ההגנה.

ב. **המערכת הפיננסית**. המדובר בבנקים, בחברות ביטוח, בקרנות פנסיה ובבתי השקעות. מלבד חשיבותם הרבה למשק ולחברה, יש להקנות עדיפות להגנתם מהסיבות הבאות: פעילותם העיקרית מתרחשת ברובד הדיגיטלי; הם מועמדים טבעיים לתקיפה בסייבר, מאחר שקשה מאוד לפגוע בהם באמצעים קינטיים; קשה ביותר לשקם אותם מפגיעה טוטלית בבסיסי הנתונים ובמערכת הגיבוי.

ג. **תשתית האנרגיה**. חברת החשמל, המהווה מקור אנרגיה ישיר לכלל המשק, אמנם נמצאת בבעלות המדינה, אולם קיימות גם תחנות כוח פרטיות. חברת החשמל עצמה ניזונה מגז טבעי המסופק על ידי חברות הגז במגזר הפרטי. לקטגוריה זו יש לשייך גם את ענף הדלק והזיקוק.

ד. **תשתית התחבורה האווירית, היבשתית והימית**. פגיעה בתפקודן של מערכות בקרה ושליטה בתשתיות אלו, באמצעות הסייבר, עלולה לחולל אירועים

רבי־נפגעים. חברות "אל־על" ו"צים" נחשבות למובילות לאומיות, אף שאינן ממשלתיות.

ה. **תשתית המים**. בנוסף לחברת "מקורות" הממשלתית, ישנם ספקי מים פרטיים. בקטגוריה זו יש לכלול גם את חברת תה"ל, המבצעת עבודות הנדסיות בתחום המים.

ו. **תעשיות המזון, החקלאות והתרופות**. לקבוצה זו במגזר הפרטי תפקיד מרכזי בביטחון אספקת המזון והתרופות בשגרה ובחירום.

ז. **חומרים מסוכנים**. המדובר בארגונים המספקים או משתמשים בחומרים מסוכנים במשק. לדוגמה, אמוניה המשמשת את התעשייה לצורכי קירור.

ח. **הקניין הרוחני של ישראל**. קריטריון זה חל על תעשיות ההי־טק, מכוני מחקר באוניברסיטאות ובבתי חולים וכדומה.

ט. **החברות המובילות בישראל –** בתחומי התוצר הלאומי, הון אנושי וייצוא.

י. **ספקים קריטיים**. המדובר בארגונים המשמשים ספקים למערכות קריטיות של הממשלה (מאגרי מידע רגישים של מערכת הביטחון, של משרדי הפנים והמשפטים, של המשטרה וכדומה) ושל ארגונים פרטיים הרשומים בעדיפות א'. מדובר גם בספקים זרים.

יא. **מגזר או מפעל מסוים** שקיים מידע שהוא מועמד לתקיפה קונקרטית או שהוא מותקף בפועל בעוצמה חריגה.

בעדיפות ב' נמצאים ארגונים גדולים ו/או בעלי השפעה מערכתית גבוהה מהסוגים הבאים:

א. ארגונים מהענפים שנמנו לעיל (פיננסים, תקשורת, תשתיות, תחבורה, תעשייה), שהשפעתם על המדינה והמשק מוגבלת משל אלה שצוינו בעדיפות א'.

ב. שירותים ציבוריים לא ממשלתיים (מערכות מצילות חיים יש לכלול בעדיפות א').

ג. ספקים פרטיים (שאינם בעדיפות א') של מערכת הביטחון, של ארגונים ממשלתיים ושל ארגונים פרטיים הרשומים בעדיפות א'.[27]

ד. החברות המובילות בישראל בתחומי התוצר הלאומי, הייצוא והתעסוקה (שאינן בעדיפות א').

ה. מאגרי מידע ציבוריים חשובים (אוניברסיטאות, מכוני מחקר ועוד) ומאגרים בחברות טכנולוגיה מתקדמת (שאינם בעדיפות א').

ו. מערכות ומאגרים של חומרים מסוכנים (שאינם בעדיפות א').

בעדיפות ג' נמצאים ארגונים בינוניים מכל הסוגים, שהשפעתם על המדינה והמשק מוגבלת משל אלה הנמצאים בעדיפות ב'. המדובר, למשל, במאגרי מידע ובשירותים ציבוריים לא ממשלתיים.

בעדיפות ד' נמצאים עסקים קטנים ואזרחים מן השורה. מדובר בקבוצה הגדולה ביותר של משתמשי סייבר. עם זאת, פגיעה בביטחון האישי בהיקף חריג עלולה להפוך לבעיה ברמה הלאומית, ועל כן תינתן עדיפות גבוהה יותר לתופעות שליליות בסייבר המשפיעות על קהלים גדולים.

קריטריון שני: הגורם לפגיעה בסייבר

סדר העדיפויות למעורבות המדינה, לפי קריטריון זה, יהיה כמפורט להלן: בעדיפות א' יימצאו גורמים עוינים הפועלים ממניעים ביטחוניים.[28] התקפה של אויב בסייבר תקבל עדיפות עליונה מצד המדינה, בשל אחריותה הגבוהה למצב כזה (להבדיל, למשל, מתקלה); וכן משום שהתקפת אויב על גורם מסוים עשויה להעיד על מתקפה רחבה יותר, ומאחר שלרוב הארגונים במגזר הפרטי אין יכולת להתמודד עם תקיפה של גורם ביטחוני זר ומתוחכם. כמו כן יהיו בסדר עדיפות זה התקפות של ארגוני פשע המתמחים בסייבר ("פשע מאורגן בסייבר"), וכן רעידת אדמה חזקה, בשל האפקט המערכתי הרחב שעלול להיות לתופעה זו.

בעדיפות ב' ימצאו גורמים פליליים – גורמי פשיעה, מתחרים העוברים על החוק, ותוקפים הפועלים ממניעים אחרים. עדיפות ג' תינתן לאסונות טבע (אם כי רעידת אדמה חזקה תהיה, כאמור, בעדיפות א') ואסונות אחרים (למשל, שריפות). עדיפות ד' תינתן לתקלות מקומיות בסייבר.

תרשים 1: השפעת המניע הביטחוני על סדר העדיפות למעורבות המדינה בהגנת הסייבר

במקרים לא מעטים עשויה להתעורר בעיית ייחוס (מי הגורם לאירוע). אז ראוי לנקוט עמדה מחמירה, בהתחשב בעלות־תועלת.

קריטריון שלישי: עלות־תועלת

ההנחה היא שראוי להשקיע את "השקל הנוסף" בהגנה על מקום בו תושג הפחתה מרבית של תוחלת הנזק. לדוגמה: בהינתן שני מפעלי תעשייה שתוחלת הנזק למדינה מפגיעה בהם היא זהה, העדיפות תינתן למפעל שבו ההפחתה של הסיכון זולה ומהירה יותר. דוגמה נוספת: הצבה של הגנות סייבר בחברת תקשורת עשויה להיות מועילה במיוחד אם היא תוזיל את סך עלות ההגנה בארגונים הקשורים לחברה. לפעמים מוטב להפחית סיכונים מסוימים שאינם בראש הרשימה לפי קריטריונים קודמים, אם ניתן להפחיתם במהירות ובעלות נמוכה בטרם יגדלו.

יישום סדר העדיפויות

המודל שהוצג לעיל מצביע על כך שכדי לקבוע סדר עדיפויות למעורבות המדינה בהגנת ארגון מסוים או קבוצות ארגונים, יש לקבוע סדר עדיפויות משוקלל המתבסס על שלושת הקריטריונים. משמעות סדר העדיפויות של המדינה לגבי ארגונים ומצבים הזכאים להגנה בעדיפויות א' ו־ב' (משוקלל)[29] היא שהמדינה תגלה מעורבות עמוקה וישירה בהגנת הסייבר בהם. מעורבותה זאת, ככל שתתאפשר, תכלול למשל: איסוף ומתן מודיעין, התקנת אמצעים לזיהוי מתקפות, קשר הדוק עם גורמי המחשוב בארגון, קביעת מדיניות ונהלים מחמירים, חובת דיווח מידית של כל הצדדים על אירועים חשודים בסייבר, פיקוח, סיוע בהתאוששות וכדומה. עדיפות א' תתבטא במעורבות הגבוהה ביותר של המדינה במניעה, בהגנה ובשיקום בהקשר למתקפת אויב. עם זאת, כאמור, מעורבות המדינה תהיה נדבך נוסף על מערך ההגנה הרגיל של הארגונים, המשמש אותם כיום להתמודדות עם האיומים האזרחיים שמצויים אצלם בסדר עדיפות גבוה (אירועים פליליים, תקלות, שריפות ועוד), ולא תחליף אותו.

לגבי ארגונים ומצבים בעדיפות ג' (משוקלל), המדינה תחייב קביעת מדיניות ונהלים סבירים בכל ארגון, תוך כדי פיקוח מזדמן על ביצועם. ארגונים אלה יהיו בקשר עם חדר המצב, שממנו הם יקבלו מידע התרעתי ברמת סיווג נמוכה. גם הם יחויבו בדיווח על אירועים חשודים בסייבר.

לגבי ארגונים בעדיפות ד' (משוקלל), המדינה תסייע בהסברה, בתקינה, בפיקוח על ספקי שירותי תקשורת ואבטחת מידע לציבור, וכו'. ארגונים אלה ייהנו, כמו כולם, משיפור רמת הביטחון במרחב הסייבר המדינתי בכללותו.

סיכום

הגנת הסייבר הלאומי במדינת ישראל רחוקה עדיין מגיבוש ומיסוד. ההמלצה המובאת במאמר זה, לגבש אסטרטגיה להגנת המגזר הפרטי בסייבר, מבוססת על עיקרון כללי, לפיו המדינה תפקח על מרחב הסייבר המדינתי עד לנקודת הכניסה הארגונית. הביצוע יהיה באמצעות מעורבות עמוקה בארגונים המחוללים את הסייבר במדינה (חברות מחשבים ותקשורת, ספקי אינטרנט וכדומה), כך שהסיכוי שהתקפות סייבר יחלפו דרכם אל ארגונים ובתי האזרחים יהיה קטן בהרבה. בצד זאת, תרחיב המדינה את הפיקוח ורגולציה על "גופים מונחים" ואחרים, שההגנה עליהם הכרחית להגנת הציבור והאינטרסים של המדינה. זאת, מעבר לנעשה כיום, הן מבחינת סוגי המגזרים שבהם המדינה פעילה, הן מבחינת מספר הארגונים המונחים והן מבחינת מגוון הפתרונות שהמדינה יכולה לתת. בנוסף, תסייע המדינה לארגונים אחרים ולציבור, באמצעות מידע והפניה לטכנולוגיות חדשות ולמיומנויות עדכניות. היא תעשה כול זאת על פי שיקולים של האינטרס הציבורי ובכפוף למגבלות ביטחוניות ולשמירה על הפרטיות.

הערות

1 "דברי ראש הממשלה בנימין נתניהו בפתח ישיבת הממשלה", **לשכת העיתונות הממשלתית**, 15 בפברואר 2015, http://gpo.gov.il/NewsRoom/GPOnews/Pages/OpenStart150215.aspx

2 "הממשלה אישרה הקמת רשות סייבר לאומית", **אתר משרד ראש הממשלה**, 15 בפברואר 2015, http://www.pmo.gov.il/MediaCenter/Spokesman/Pages/spokecyber150215.aspx

3 שמואל אבן ודוד סימן־טוב, **לוחמה במרחב הקיברנטי: מושגים, מגמות ומשמעויות לישראל**, מזכר 109, תל אביב: המכון למחקרי ביטחון לאומי, יוני 2011, עמ' 15.

4 המגזר הפרטי כולל את כל הישויות במדינה שאינן בשליטת הממשלה: אזרחי ישראל כפרטים, החברות הלא ממשלתיות – הפרטיות והבורסאיות ("ציבוריות"), תאגידים שלא למטרות רווח וכדומה. במגזר הממשלתי מצויים משרדי הממשלה ומוסדותיה, הרשויות המקומיות, חברות ממשלתיות (חברת החשמל, התעשייה האווירית ועוד) ותאגידים אחרים.

5 עמוס הראל, "הערכות: איראן מאחורי מתקפת הסייבר על חברות נפט במפרץ הפרסי", **הארץ**, 11 בספטמבר 2012, http://www.haaretz.co.il/news/world/1.1821619

6 שחר ארגמן וגבי סיבוני, "חשיפת המשק הישראלי לריגול סייבר עסקי", **צבא ואסטרטגיה**, כרך 6, גיליון 1, מארס 2014.

7 מרחב הסייבר המדינתי הינו אזור במרחב הסייבר הגלובלי, שבו יש למדינה יכולת השפעה ריבונית על האופן בו מוקמות, מנוהלות ומתופעלות תשתיות התקשורת, המחשוב והאינטרנט, תוך שימת דגש על הגישה לתשתיות אלו ולחופש העברת המידע בהן.

8 "Cybersecurity Privacy Practical Implications", *epic.org*, May 31, 2015, https://epic.org/privacy/cybersecurity

9 עירית אבישר, "בכירה בבנק ישראל: 'אנו שוקלים להקים מרכז סייבר בנקאי'", **גלובס**, 24 בינואר 2014, http://www.globes.co.il/news/article.aspx?did=1000911843

10 "מתקפת סייבר של איראן על בנקים אמריקניים", **Ynet**, 9 בינואר 2013, http://www.ynet.co.il/articles/0,7340,L-4330464,00.html

11 רויטרס, "פאנטה: מתקפת הסייבר בסעודיה – הכי הרסנית", **Ynet**, 12 באוקטובר 2012, http://www.ynet.co.il/articles/0,7340,L-4291322,00.html

12 רן דגוני, "ידלין: בלוחמת סייבר, מדינה צריכה לתקוף, לא רק להתגונן", **גלובס**, 29 באפריל 2015, http://www.globes.co.il/news/article.aspx?did=1001031543

13 ירון רפפורט, "השב"כ בעידן הקיברנטי: מבט מבפנים", *IsraelDefense*, 11 באפריל 2014,

14 **אתר שירות הביטחון הכללי**, http://www.shabak.gov.il/Pages/homepage.aspx

15 "המטה הקיברנטי הלאומי", **אתר משרד ראש הממשלה**, http://www.pmo.gov.il/branchesandunits/cyber/pages/default.aspx

16 "הממשלה אישרה הקמת רשות סייבר לאומית".

17 שם.

18 "הוראה לניהול סיכוני אבטחת המידע של הגופים המוסדיים", **משרד האוצר־אגף שוק ההון, ביטוח וחיסכון**, 16 באוקטובר 2006.

19 אבישר, "בכירה בבנק ישראל: 'אנו שוקלים להקים מרכז סייבר בנקאי'".

20 עירית אבישר, "בנק ישראל לבנקים: מנו מנהל להגנה ממתקפות סייבר", **גלובס**, 21 ביולי 2014, http://www.tbk.co.il/article/3120778

21 **אתר רמו"ט**, http://index.justice.gov.il/Units/ilita/Odot/Pages/Odot.aspx

22 "המשטרה מקימה יחידה חדשה ללוחמת סייבר", **ערוץ 2**, 12 בנובמבר 2012, http:// www.mako.co.il/news-israel/local/Article-a65e89befe3fa31004.htm

23 אביתר מתניה וטל גולדשטיין, "המטרה: שיתוף פעולה גלובלי מול איומי הסייבר", *IsraelDefense*, יוני 2013.

24 במצב בו השוק בנושא זה פרוץ והצרכן אינו יודע לזהות את איכות השירות, הצרכן וגורמים הקשורים עמו עלולים להיחשף לסיכוני סייבר, כולל לנזק בעת בדיקת חדירות.

25 תוחלת הנזק היא מכפלת אומדן הנזק למדינה (בהינתן פגיעה) כפול הערכת הסבירות (הסובייקטיבית) לפגיעה (ברמת ההגנה הנוכחית). הערכת הסבירות מתבססת גם על המודיעין שהתקבל בנושא. על כן, הערכת תוחלת הנזק היא דינמית.

26 כמה מהארגונים הללו כבר כלולים ברשימת ארגוני התשתיות הקריטיות המונחים על ידי רא"ם. עם זאת, ארגונים רבים וענפי משק חשובים מסוימים אינם כלולים ברשימה זו.

27 ניתן אמנם לתקוף ארגון בסייבר דרך ספקיו ואף דרך לקוחותיו (אם הם קשורים לרשת הארגונית), אולם ביכולתו להתגונן גם מפניהם. לכן, ארגון יכול להיות בעדיפות א' וספקיו בעדיפות ב'.

28 ניתן להניח שלמדינות יש יכולות תקיפה גבוהות ונשנות בסייבר לעומת תוקפים לא מאורגנים, אף שבתחום זה יתכנו בהחלט יוצאים מן הכלל.

29 ארגון מסוים יכול להיות בעדיפות א' בתרחיש ביטחוני ובעדיפות ב' בתרחיש אחר.