דרכי ההגנה על תשתיות חיוניות במרחב הסייבר בישראל

אלדד הבר* וטל ז׳רסקי**

העידן הדיגיטלי הביא עימו סיכונים רבים ומגוונים. כך, למשל, מתקפת סייבר עלולה לפגוע ולשבש את תפקודה התקין של מדינה באמצעות פגיעה בתשתיות אשר חיוניות לתפקודה. פגיעות או שיבושים בתשתיות חיוניות אלה עלולים לגרום נזקים כלכליים, חברתיים וסביבתיים נכבדים, ואף פגיעות אפשריות בנפש. אם בעבר היו האיומים שנשקפו לתשתיות חיוניות פיזיים בעיקרם, כיום, בעידן הטכנולוגי, נוסף מימד חדש שכרוך בסיכונים רבים נוספים, ועל מפעילי תשתיות אלה להתמודד עימם.

ההכרה הפורמלית באיומים הללו באה לידי ביטוי במדינת־ישראל בשנת 2002, עם הקמתה של הרשות הממלכתית לאבטחת מידע. רשות זו מופקדת על מדיניות האבטחה וההגנה של אותם גופים שהחוק מגדיר כתשתיות חיוניות. במילים אחרות, ישראל בחרה להטיל את האחריות להגנה על תשתיות חיוניות בישראל על גוף ייעודי של שירות הביטחון הכללי, המעביר הנחיות מחייבות למפעילות התשתית. לעומת זאת, מעצבי מדיניות רבים בעולם נקטו גישות מתערבות פחות להגנה על התשתיות החיוניות במדינותיהם מפני מתקפות סייבר, כגון הסדרה וולונטרית המבוססת בעיקרה על שיתוף מידע ו/או שיתוף־פעולה בין מפעילי התשתיות החיוניות לבין הממשל. איזה מן המודלים הללו הינו המודל המיטבי להגנה על תשתיות חיוניות? האם המודל הישראלי מתערב יותר מדי בפררוגטיבה הניהולית של חברות פרטיות או שמא התערבות זו הכרחית כאשר עסקינן בתשתיות חיוניות? האם יש לבחון הסדרים חדשים בעידן הדיגיטלי להגנה

---

* מרצה בכיר, המרכז למשפט וטכנולוגיה ופורום סייבר, הפקולטה למשפטים, אוניברסיטת חיפה; עמית מחקר, מרכז ברקמן לחקר האינטרנט והחברה, אוניברסיטת הרווארד.

** פרופסור חבר, המרכז למשפט וטכנולוגיה ופורום סייבר, הפקולטה למשפטים, אוניברסיטת חיפה.

אנו מודים למיכאל בירנהק, לדב האוסן־כוריאל, לליאור טבנסקי, לגלעד ידין, לשרון ידין, לעידו סביליה, לגבי סיבוני ולחיים רביה על הערותיהם. כמו־כן אנו מודים למשתתפי הכנס ״טרור מקוון״ שנערך ב־18.12.2014 בפקולטה למשפטים, אוניברסיטת חיפה, על הערותיהם המועילות, ולירדן שייר ולאייל שרף על עזרתם במחקר. המאמר נכתב בתמיכת מענק מחקר של קרן תשתיות של משרד המדע והטכנולוגיה.

על תשתיות חיוניות מפני מתקפות סייבר? אלה חלק מהשאלות העומדות בבסיסו של מחקר זה.

מאמר זה מבקש לבחון מודלים של הגנה על תשתיות חיוניות מפני מתקפות סייבר, תוך התמקדות במודל הישראלי. הוא פותח בהגדרות וטקסונומיות של הגנה על תשתיות חיוניות. לאחר־מכן המאמר סוקר את המודל הישראלי להגנה על תשתיות חיוניות מפני מתקפות סייבר, תוך השוואה בינו לבין מודלים שננקטו במדינות אחרות. מכאן המאמר פונה לדיון ביקורתי במודלים של אסדרה, ומבחין בין מודל אסדרתי מצומצם – אשר מסתפק בדרישות להעברת מידע, במתן תמריצים, ובגרסתו הקיצונית ביותר בהטלת חובות ואחריות בדיעבד – לבין מודלים אגרסיביים יותר, אשר מכתיבים מראש את דרך ההתמודדות עם איום זה. בחינה זו מובילה למסקנה כי המודל שננקט בישראל מעניק כוח רב מדי בידי המדינה בכל הנוגע בעיצובה של מדיניות הגנת הסייבר של מגזרים רבים ומגוונים, מה־גם שהוא אינו בהכרח נכון ויעיל. עקב כך המאמר מציע לצמצם את המודל הישראלי – אשר מנחה את מפעילי התשתיות מראש כיצד ראוי לפעול – למקרים מיוחדים, וכן בוחן כמה מנגנונים אחרים להבטחת רמה נאותה של הגנת סייבר.

מאמר זה חשוב בעת הזו לנוכח איום הסייבר ההולך ומתהווה, ולנוכח העובדה שמדינת־ישראל בוחנת כיום מחדש את ההסדר הקיים, ואף הקימה במסגרת זאת רשות לאומית להגנה אופרטיבית בסייבר וכן מטה סייבר, אשר עשויים להוות תפנית משמעותית בגישתה של המדינה להגנה על תשתיות חיוניות מפני מתקפות סייבר. לאחרונה ממש אף שונה החוק המרכזי העוסק בעניין זה בשינוי זמני אשר עשוי ליהפך לקבוע. לפיכך המאמר מבקש להציע ארגז כלים והמלצות למעצבי המדיניות בישראל בבואם לדון במודלים חדשים להגנה על תשתיות חיוניות בישראל.

מבוא. א. הגנה על תשתיות חיוניות: 1. חשיבות ההגנה על תשתיות: הגדרות וטקסונומיות; 2. הצורך בהגנה על תשתיות חיוניות מפני מתקפות סייבר. **ב. המודל הישראלי: עבר, הווה ועתיד. ג. מודלים מקבילים להגנה על תשתיות חיוניות:** 1. המודל האמריקאי; 2. המודל האירופי. **ד. מודלים להגנה על תשתיות מפני איומי סייבר: אסדרת שוק, הסדרה מוגבלת, תמריצים והסדרה לאחר מעשה:** 1. מודל השוק וכשליו; 2. התערבות מינימליסטית – חובות גילוי והזרמת מידע; 3. בעיית ההחצנות – הסדרה לאחר מעשה ומתן תמריצים. **ה. מודלים להגנה על תשתיות מפני איומי סייבר: הסדרה ״אגרסיבית״ אקס־אנטה:** 1. רא״מ כמשל: חזרה ליסודות המודל הישראלי, ייחודו ויתרונותיו; 2. חסרונותיה של הסדרה ממשלתית מראש. **ו. המודל המוצע. ז. סיכום.**

מבוא

תשתיות חיוניות – כשמן כן הן. לפיכך ההגנה על תשתיות אלה הינה הכרחית. פגיעות או שיבושים בתשתיות אלה – אשר רבות מהן מצויות עתה בבעלות פרטית[1] – עלולים לגרום נזקים כלכליים, חברתיים וסביבתיים נכבדים, ואף להסב פגיעות בנפש. מערכות אלה אף משמשות דרך קבע את המערך הצבאי של המדינה, ועל־כן פגיעה בהן מתורגמת במהרה לפגיעה אסטרטגית בבטחונה.[2] בעבר הגנה על תשתיות חיוניות התבצעה בעיקר באמצעות אבטחה פיזית. כאשר המדינה ביקשה להגן על סכרים, למשל, היא הציבה בצידם מגדלי שמירה, והוסיפה לעיתים גדרות ויחידות משמר. אך פני המציאות השתנו כתולדה של ההתקדמות הטכנולוגית. כיום מרבית התשתיות החיוניות מנוהלות ומופעלות באמצעות מערכות בקרה דיגיטליות השולטות במכלול פעולותיה של המערכת ומכונות ״מערכות Supervisory Control and Data Acquisition״ (או בקיצור ״מערכות SCADA״),[3] אשר בחלקן נגישות מרחוק. הטכנולוגיה מביאה עימה יתרונות רבים, אשר באים לידי ביטוי בהתנהלות יעילה יותר ובביצועים משופרים, אולם השינויים הטכנולוגיים מביאים עימם גם סיכונים. על־כן הגנה על תשתיות חיוניות מצריכה כיום דרכי אבטחה נוספות וייחודיות, אשר מטפלות גם במימד של התקפות הסייבר המכוונות נגד מערכות דיגיטליות.

החשש מפני מתקפות סייבר[4] הצטרף לפיכך בשנים האחרונות למכלול הסיכונים שמדינה ריבונית צריכה להתמודד עימם בבואה להגן על תושביה ותשתיותיה החיוניות: חשמל, מים, בנקים, גז, בתי־חולים ותקשורת. אופי התקיפה עשוי להיות מגוון ובלתי־צפוי. מתקפות סייבר עלולות לעכב ולהשבית את פעילותה של המערכת הדיגיטלית, להרוס אותה, לכוון אותה לפגיעה בתשתיות פיזיות, כמו־גם למחוק ולשנות מידע המצוי באותה מערכת דיגיטלית ובאלה המחוברות אליה. התרחישים השונים להתממשותם של סיכונים אלה עוברים ממוחם הקודח של תסריטאי הוליווד אל שולחנם העמוס של ראשי מערכות הביטחון וההגנה. מתרבות העדויות שהתקפות כאלה לא רק אפשריות, אלא כבר התרחשו.[5]

---

1 גבי סיבוני ״הגנת נכסים ותשתיות קריטיות מפני תקיפה קיברנטית – הממד הסטטוטורי״ **צבא ואסטרטגיה** 3(1) 81 (2011).

2 Paul Rosenzweig, Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World 158 (2013).

3 יצרניות מובילות של מערכות SCADA הן החברות Siemens ו־Honeywell. ראו http://w3.siemens.com/mcms/human-machine-interface/en/visualization-software/scada/pages/default.aspx וכן https://www.honeywellprocess.com/en-US/explore/products/control-monitoring-and-safety-systems/scada-systems/Pages/default.aspx.

4 המונח ״סייבר״ הינו כינוי נפוץ למרחב הקיברנטי (cyberspace), אשר מיוחס פעמים רבות בעיקרו למרשתת. קצרה היריעה במאמר זה מלהציע טקסונומיה מפורטת למונח כללי זה. לשם הבהרה, במאמר זה המונח ״מתקפת סייבר״ מתייחס לשימוש באמצעי דיגיטלי נגד מערכת דיגיטלית במטרה לשבש את פעילותה או להסב נזק לה או למידע שאגור בה.

5 יש דוגמאות לא־מעטות להתקפות מוצלחות וכן לנסיונות התקפה שסוכלו. אחת מהן היא התקיפה שנערכה בינואר 2012 על אתר הבורסה בתל־אביב על־ידי ההאקר ה״סעודי״. ראו Rosenzweig, לעיל ה״ש 2, בעמ׳ 184. כמו־כן, באימונים שערך צבא ארצות־הברית התאפשר חיבור למערכת SCADA מרוחקת ובוצעו פעולות שהובילו לשרפת גנרטור דיזל. ראו שם, בעמ׳ 177. דוגמה

קשה לטעון כי איום הסייבר תופס את מדינת־ישראל בלתי־מוכנה. עוד בשנת 2002 הקימה מדינת־ישראל את הרשות הממלכתית לאבטחת מידע (להלן: רא״מ), המהווה חלק משירות הביטחון הכללי. רשות זו אחראית, בין היתר, למדיניות האבטחה וההגנה על מידע ומחשב בגופים אשר מוגדרים כמפעילי מערכות ממוחשבות חיוניות.[6] לתפקידיה של רא״מ יש כמה גוונים: ראשית, היא מופקדת על **הנחיה** מקצועית של אותם גופים בנוגע לאבטחתן של תשתיות מחשב חיוניות; שנית, היא **מפקחת** על יישום הנחיותיה; ושלישית, היא מוסמכת לנקוט **סנקציות** נגד מפֵרים אשר מחויבים להישמע להנחיותיה.[7]

ההחלטה על הקמת רא״מ, כולל הגדרת סמכויותיה הנרחבות ודרכי פעולתה, מבטאת ומשקפת את תפיסתם של מעצבי המדיניות בישראל. המודל שאומץ מעניק כֹּוח רב בידי יחידה סודית של שירות הביטחון הכללי לעצב את המדיניות של הגנת הסייבר של מגזרים רבים ומגוונים. ייתכן בהחלט שמודל זה, החודר אף לפררוגטיבה הניהולית של חברות פרטיות, ואולי גם חושף מידע אישי של אזרחים לפני רשויות עלומות, הוא ייחודי בעולם. על־כן ראוי לבחון אם הוא נכון ויעיל.[8] בדיקה זו תאפשר גם דיון על־אודות העולם החדש והחשוב של הגנת הסייבר – תחום אשר צובר רלוונטיות הן לגבי גופים ציבוריים, הן לגבי גופים פרטיים והן לגבי הפרט החי בעולם הדיגיטלי – באמצעות כלים מקובלים בניתוח המשפטי של מנגנוני הסדרה ואסדרה.[9] החיבור בין עולם ההסדרה והאסדרה לבין עולם הסייבר חשוב והכרחי, שכן הוא מאפשר לקרב מומחים משני עולמות אלה, אשר לעיתים אינם מודעים לדיונים המקבילים המתקיימים בסוגיה זו. החיבור האמור הינו תרומתו המרכזית של המחקר דנן.

ההתמודדות עם השאלה בדבר דרך הסדרתה של הגנת הסייבר על תשתיות חיוניות הינה הכרחית וחשובה, במיוחד בעת הזו. לנוכח איום הסייבר ההולך ומתהווה, מדינות רבות בוחנות מהי הדרך הנכונה להתמודד עימו. מדינת־ישראל בוחנת אף היא מחדש את ההסדר הקיים,

---

177. דוגמה מרכזית של מתקפת סייבר על תשתית חיונית התרחשה באוקראינה בסוף שנת 2015, כאשר תוכנה זדונית פגעה בשלוש ספקיות חשמל במדינה. בעקבות מתקפת הסייבר נותרו מאות אלפי אנשים ללא חשמל במשך ימים אחדים. ראו ״לראשונה תועדה התקפת סייבר שגרמה להפסקת חשמל נרחבת״ **הארץ** 5.1.2016 www.haaretz.co.il/news/world/europe/.premium-1.2815157. לטענות מהתקשורת בדבר תקיפות מסוג זה ראו, למשל, ״ארגון סורי ערך מתקפת סייבר נגד מערכת המים של חיפה״ **כלכליסט** 25.5.2013 www.calcalist.co.il/internet/articles/0,7340,L-3603293,00.html; אחיה ראב״ד ו־AP ״מנהרות הכרמל נסגרו עקב מתקפת האקרים״ **ynet** 27.10.2013 www.ynet.co.il/articles/0,7340,L-4446249,00.html.

6 ראו דיון בפרק ב להלן, במיוחד ליד ה״ש 52 ואילך.

7 ראו דיון להלן בה״ש 59–70 ובטקסט שלידן.

8 סוגיה זו לא נדונה כמעט בספרות האקדמית הישראלית ככלל והמשפטית בפרט. לכתיבה קיימת ראו, למשל, מיכאל בירנהק ״משפט המכונה: אבטחת מידע וחוק המחשבים״ **שערי משפט** ד 315 (2005); ליאור טבנסקי ״לחימה במרחב הקיברנטי: מושגי יסוד״ **צבא ואסטרטגיה** 3(1) 65 (2011); סיבוני, לעיל ה״ש 1, בעמ׳ 82; Lior Tabansky & Isaac Ben Israel, Cybersecurity in Israel (Springer 2015).

9 במאמר זה נשתמש לחלופין במונחים ״אסדרה״ ו״הסדרה״, אך אין בשימוש במונחים אלה כדי לרמז על דיונים מעמיקים יותר בספרות האקדמית הנוגעת במהותה של האסדרה באופן כללי ובזהות המְאַסדר. לדיון מעמיק יותר בטקסונומיה של אסדרה ראו שרון ידין **רגולציה: המשפט המנהלי בעידן החוזים הרגולטוריים** (2016).

ובתוך כך מייסדת רשות לאומית להגנה אופרטיבית בסייבר (להלן: רשות הסייבר) וכן מטה סייבר. הקמת מוסדות אלה עשויה להוות תפנית משמעותית בגישת המדינה להגנה על תשתיות חיוניות מפני מתקפות סייבר.[10] זאת, לנוכח החלטות ממשלה שעל־פיהן הרשות החדשה תקבל על עצמה חלק מהאחריות הכוללת להגנת המרחב האזרחי של ישראל מפני איומי סייבר,[11] וכן אומצה הוראת־שעה אשר מעבירה לזמן מוגבל (ולאחר קבלת צו מתאים מראש הממשלה) חלק מסמכויותיה של רא״מ בעניין זה לרשות הסייבר.[12] מוקדם עדיין לקבוע מסמרות בדבר מבנה הסמכויות של רשות הסייבר ככל שהדבר נוגע בהגנה על תשתיות חיוניות. אולם השינויים המבניים האמורים מעידים כי מודל ההגנה על תשתיות חיוניות בישראל והפילוסופיה שמאחוריו השתנו או עשויים להשתנות. לנוכח חשיבותה של סוגיה זו, שינוי מעין זה מצריך דיון אנליטי מעמיק ודחוף אשר יכרוך יחדיו מתודולוגיות אנליטיות שונות ויציגן יחדיו לטובת ניתוח עתידי. כמו־כן, המתודולוגיות המוצעות על־ידינו לבחינת מודל ההגנה על תשתיות חיוניות בישראל נדלות מתוך שימוש בפריזמה תיאורטית והשוואתית.

בחלק א נספק כמה הגדרות ומוטיווציות להמשך המחקר, תוך הסברת ייחודיותו של איום הסייבר. בחלק ב נסקור את המודל הישראלי להגנת סייבר על תשתיות חיוניות. בחלק ג ננתח מודלים אמריקאיים ואירופיים להגנה על תשתיות חיוניות מפני מתקפות סייבר. הכרת מודלים אלה – לרבות השיקולים שהנחו מדינות אחרות והכלים והתהליכים ששימשו אותן – חשובה כדי לאפשר דיון משווה בדרכי ההסדרה של תשתיות חיוניות. לאחר־מכן נעבור לדיון ביקורתי במודלים שונים של אסדרה והסדרה. בחלק ד נתחיל במודל אסדרתי מצומצם, אשר מסתפק בדרישות להעברת מידע, במתן תמריצים, ובגרסתו הקיצונית ביותר – בהטלת חובות ואחריות בדיעבד. בחלק ה נציג מודלים אגרסיביים יותר, אשר פונים לדרך של התמודדות מראש עם איום זה. בחלק זה יתמקד הניתוח, במידה רבה, בדיון ביקורתי במודל המוחל בישראל, על מאפייניו השונים. בחלק ו ננסה ליישב בין הביקורות השונות שהוצגו, ונציין דגשים אחדים למודל ראוי אשר יסתמך על הניתוח והדיון שקיימנו. המודל יציע לצמצם את המודל המקובל בישראל – אשר מנחה את מפעילי התשתיות מראש כיצד ראוי לפעול – למקרים מיוחדים. במקומות שבהם תצומצם התערבות המדינה, יציע המודל לאמץ כמה מנגנונים אחרים כדי להתמודד עם הצורך בהסדרת רמה נאותה של הגנת סייבר. בחלק האחרון נסכם בכמה מילות אזהרה בנוגע לדרך התנהלותו של הדיון בסוגיה דנן, ונצביע על כיווני מחקר עתידיים.

מאמר זה, כדרכם של מאמרים המבקשים לפתוח צוהר לנושא חדשני, מצריך התבוננות על סוגיות חשובות העולות בהקשר של הגנת הסייבר, דוגמת זכויות האדם (ובעיקר הזכות לפרטיות) שעלולות להיפגע ממאמצי המדינה לתת הגנת סייבר ראויה. כמו־כן נסקור בקצרה בלבד את דרכי הפעולה של המדינה במאבקה נגד התקפות סייבר, את הייחוד שבדרכי פעולה

---

10 ברק רביד ״השב״כ ומטה הסייבר נאבקים מי יילחם בהתקפות מחשבים, נתניהו נמנע מהחלטה״ **הארץ** 14.9.2014 www.haaretz.co.il/news/politics/.premium-1.2432606.

11 מוטי בסוק ״נתניהו: תוקם רשות לאומית להגנה אופרטיבית בסייבר״ **TheMarker** 21.9.2014 www.themarker.com/news/1.2439795.

12 חוק להסדרת הביטחון בגופים ציבוריים (הוראת שעה), התשע״ו–2016, ס״ח 1219 (16.8.2016); צו להסדרת הביטחון בגופים ציבוריים (הוראת שעה) (קצין מוסמך לעניין גוף המנוי בתוספת החמישית לחוק), התשע״ז–2016, ק״ת 442 (29.12.2016).

אלה ואת האתגרים שהן מציבות (בין היתר בהקשר של משפט בין־לאומי). נוסף על כך נידרש בכלליות לסוגיית ההגדרה הראויה של המושג "תשתיות חיוניות" ומה ראוי להיכלל בתוכה. סוגיות אלה ואחרות ראויות בהחלט לדיון מעמיק בכתיבה עתידית.

א. הגנה על תשתיות חיוניות

1. חשיבות ההגנה על תשתיות: הגדרות וטקסונומיות

תשתיות לאומיות פעילות ומאובטחות חשובות לתפקודן של מדינות ולהגנה על האינטרסים החיוניים להן. כשלב ראשון בדיון באתגר של אבטחתן, אנו נדרשים לכמה הגדרות וטקסונומיות. היות שמרבית הדיון המתקיים בנושא זה בישראל נובע מחוק העוסק במַטריה זו – חוק להסדרת הבטחון בגופים ציבוריים, התשנ״ח–1998 (להלן: חוק הביטחון) – נשתמש בטקסונומיה המוצגת בחוק זה.

חוק הביטחון פועל על בסיס שלוש קטגוריות – אבטחה פיזית, אבטחת מידע ואבטחת תשתית חיונית ממוחשבת – ומגדיר אילו גופים, ציבוריים ופרטיים כאחד, כלולים בכל אחת מהקטגוריות, בהתאם לאופי האיום הנשקף להם (אין מניעה שאותו גוף ייכלל ביותר מקטגוריה אחת). כאמור, מאמר זה מתמקד בהגנה על תשתיות חיוניות מפני סיכוני סייבר, ובכך ניתן לבדלו מדיון במישור מקביל העוסק באבטחה פיזית בלבד. על־פי החוק, ולשם הגנה על אותן תשתיות לאומיות, המדינה עשויה לחייב גופים שונים, הן ציבוריים הן פרטיים (כגון אוניברסיטאות),[13] להקים ולנהל מערך אבטחה לשמירה על אותן תשתיות ו/או להכפיף אותן למנגנון אבטחה חיצוני. ברוב המקרים הגוף החיצוני האמור הוא משטרת ישראל; שירות הביטחון הכללי מופקד על הגנת מוסדות ומתקנים רגישים יותר.[14]

הסוגיות הנוגעות בסייבר ובמחשוב מתחלקות, על־פי חוק הביטחון, לכמה סוגי תרחישים. תרחיש אחד – אשר לא נעסוק בו – נוגע באבטחת מידע מסווג מפני העתקתו וגנֵבתו. זוהי סוגיה הנוגעת באבטחת מידע או cybersecurity. גופים שונים אוגרים מידע מסווג, בין על־אודות פעילותם שלהם ובין על־אודות אזרחים. בתגובה, המדינה מחייבת חלק מאותם גופים לעמוד בסטנדרטים של אבטחת מידע לשם שמירה על מידע זה.[15] דברים אלה מוסדרים אף הם בחוק הביטחון, אשר כולל רשימה של גופים הכפופים להסדרה זו.[16] התרחיש שבו נתמקד ברשימה זו הוא פעולות הנדרשות לאבטחת המערכות הממוחשבות החיוניות עצמן, ולא רק לאבטחת המידע המצוי בהן. אלה פעולות הדרושות לשמירה על מערכות ממוחשבות, על המידע האגור בהן ועל יכולתן להפעיל מערכות פיזיות הנשלטות על־ידיהן מפני תקיפה

---

13 ס׳ 1 לחוק הביטחון (הגדרת "קצין מוסמך"); וכן התוספת השלישית לחוק הביטחון.

14 התוספת הראשונה לחוק הביטחון.

15 ס׳ 1 לחוק הביטחון, הגדרת "פעולות לאבטחת מידע".

16 התוספות הראשונה והשנייה לחוק הביטחון. למדינה יש תפקיד עקיף נוסף בהקשר זה, בכך שיש בידה סמכות לקבוע תקנות הנוגעות ברמת האבטחה הנדרשת במאגרים המכילים מידע אישי על־פי ס׳ 34 לחוק הגנת הפרטיות, התשמ״א–1981.

ממוחשבת.[17] כל זאת כדי לאפשר המשכיות תפקודית של מערכות חשובות אלה בכל עת. מובן שההפרדה בין שלוש הקטגוריות שצוינו – אבטחה פיזית, אבטחת מידע ואבטחת תשתית חיונית ממוחשבת – הינה בעייתית ואינה חדה. כך, התקפה על מערכת ממוחשבת חיונית עשויה להיות פיזית, ועשויה אף להיות משולבת עם תקיפות אחרות. כמו־כן, פגיעה במידע עשויה להוות גם פגיעה בתשתית, ולהפך. לפיכך במאמר זה נעשה שימוש בקטגוריה אחרונה זו, קרי אבטחת תשתית חיונית ממוחשבת, תוך נכונות לגלוש ממנה גם לתחומים שעשויים להיחשב חלק משתי הקטגוריות האחרות.

לאחר ההבחנה (המעושה במידה רבה) בין הקטגוריות השונות, יש צורך בקביעת גבולות לסמכויות המדינה בהקשר זה. אבן־הבוחן להכללת גוף בקטגוריה שבה נעסוק (אבטחת מערכות ממוחשבות חיוניות) היא הגדרתו כאחראי לתשתית חיונית וכמפעיל שלה. לפיכך נפנה להגדרה של ״תשתית חיונית״. באופן כללי, ההגדרה של תשתית חיונית משתנה עם הזמן, ומתוחמת באופן שונה במדינות שונות.[18] במקור הוגדרו תשתיות חיוניות (אשר לעיתים מכונות ״תשתיות קריטיות״ – critical infrastructure – מושג אשר נשתמש גם בו במהלך סקירתנו) כתשתיות ששיבושן עלול לגרום נזקים צבאיים וכלכליים משמעותיים.[19] עם הזמן הורחבה ההגדרה בשיח העולמי בעניין זה, וכיום היא כוללת גם תשתיות שפגיעה בהן עלולה לפגום בניהול התקין של המדינה ו/או אזרחיה.[20] ההגדרה האמורה אינה אחידה בין מדינות, אך לרוב היא מתייחסת למספר נרחב של מגזרים, ביניהם תעשיות כימיקלים, תשתיות חשמל, טלקומוניקציה, גז ודלק, בנקים וכלכלה, תחבורה, שירותי בריאות, הספקת מים, שירותי חירום, שירותי ממשל, חקלאות ומזון. לעיתים הורחבה ההגדרה אף ליעדים אסטרטגיים, כגון אתרים לאומיים שתקיפתם עלולה לפגוע קשות במורל האזרחים במדינה.[21] יצוין כי במודל הישראלי ההגדרה והסיווג נעשים אד־הוק; גופים אשר נקבע כי הם ראויים להיחשב תשתיות חיוניות המצדיקות הגנת סייבר מסווגים ככאלה על־ידי הכללתם ברשימה ייעודית.[22] ראוי עוד לציין כי אין בהכרח צורך להתייחס ל״תשתיות קריטיות״ כאל מושג דיכוטומי. חלק מהמודלים האסדרתיים בעולם מגדירים כמה ״שכבות״ של תשתיות קריטיות, ובהתאם להן כמה מערכות

---

17 ס׳ 1 לחוק הביטחון, הגדרת ״פעולות לאבטחת מערכות ממוחשבות חיוניות״.

18 ליאור טבנסקי ״הגנה על תשתיות קריטיות מפני איום קיברנטי״ **צבא ואסטרטגיה** 3(2) 63, 64 (2011) (להלן: טבנסקי ״הגנה על תשתיות״).

19 John Moteff, Claudia Copeland & John Fischer, Critical Infrastructures: What Makes an Infrastructure Critical? 2 (Congressional Research Service, 2003), *available at* http://www.fas.org/irp/crs/RL31556.pdf.

20 לצורך השוואה, בארצות־הברית ההגדרה של תשתיות חיוניות היא זו: "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters". ראו 42 U.S.C. § 5195c(e) (2012).

21 כך, לדוגמה, בגרמניה. ראו Federal Ministry of the Interior, National Strategy for Critical Infrastructure Protection (CIP Strategy) (2009), *available at* http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/EN/CIP-Strategy.pdf?__blob=publicationFile (להלן: CIP Strategy).

22 ס׳ 1 לחוק הביטחון.

אסדרתיות שונות, אשר כל אחת מהן מצריכה מידה שונה של התערבות וקשיחות. מודל זה של ״שכבות״ מאפשר התאמה מאוזנת ומדויקת יותר בין הסיכונים, הכלים האסדרתיים הנדרשים והפגיעות שהשימוש בכלי אסדרה אלה עלול לגרום.[23]

2. הצורך בהגנה על תשתיות חיוניות מפני מתקפות סייבר

הצורך בהגנה על תשתיות חיוניות אינו ייחודי לסייבר. האפשרות של פגיעה בתשתיות חיוניות הייתה קיימת עוד לפני עידן המחשוב.[24] פגיעה כאמור עשויה להיגרם בין במכוון ובין לא במכוון. האפשרות האחרונה מתייחסת לפגיעות הנגרמות עקב טעות אנוש, תקלת מערכת וכמובן אסון־טבע.[25] אך מעבר לכך יש פעולות מכוּונות שמטרתן לפגוע בתשתיות חיוניות, ואת קיומן יש להביא בחשבון.[26]

הסיבות לפגיעה מכוּונת מגוונות. הפגיעה עשויה להיות חלק ממאבק מזוין בין מדינות מסוכסכות, כמו־גם פעולה של גורמים פליליים, של עובדים (בהווה או לשעבר) מתוסכלים, של פעילים חברתיים או של ארגון טרור. פעולת טרור עשויה להיות אטרקטיבית ומבוקשת במיוחד, שכן תקיפה כאמור תאפשר לארגון להגשים חלק מיעדיו בסיכויי הצלחה גבוהים, תוך סיכון ועלות נמוכים, וזאת מכמה סיבות.[27] ראשית, טווח הפגיעה בתשתיות חיוניות (או היקף המטרות האפשריות) עשוי להיות רחב יחסית. כלומר, אין בהכרח צורך בפגיעה ישירה במרכז השולט בתשתיות עצמן. לדוגמה, לשם פגיעה במערכת החשמל, אין צורך לפגוע ישירות במוקד חברת החשמל, אלא ניתן לפגוע במרכזים מקומיים או בקווי חשמל.[28] שנית, הנזק שייגרם מתקיפת תשתיות חיוניות יהיה רב עקב התלות ההדדית ביניהן, שכן תשתיות חיוניות

23 Ryan Ellis, *Regulating Cybersecurity: Institutional Learning or a Lesson in Futility?*, 12(6) IEEE Security & Privacy 48, 52 (2014). יצוין כי מודל אסדרתי זה יאומץ ככל הנראה בישראל, לנוכח המלצה בכיוון זה בהחלטה 2443 של הממשלה ה־33 ״קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר״ (15.2.2015) (להלן: החלטת ממשלה 2443). בס׳ 3(ז) לנספח א להחלטה האמורה נאמר לעניין אסדרה עתידית כי ״האסדרה תגדיר רמות שונות של הגנה והסמכה״. העובדה שבהוראת־השעה קיימות שתי רשימות נפרדות של גופים המיועדים להסדרה שונה – התוספת הרביעית והתוספת החמישית – ייתכן שמעידה על מעבר לאופן פעולה מעין זה.

24 ראו Ted G. Lewis, Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation 1 (2006).

25 John D. Moteff, Critical Infrastructures: Background, Policy, and Implementation 1 (Congressional Research Service, 2014), *available at* http://www.fas.org/sgp/crs/homesec/RL30153.pdf.

26 United States Government Accountability Office, Cybersecurity: National Strategy, Roles, and Responsibilities Need to be Better Defined and More Effectively Implemented (2013), *available at* http://www.gao.gov/assets/660/652170.pdf.

27 למאפיינים אלה ראו Joe D. Whitley et al., *Homeland Security, Law, and Policy Through the Lens of Critical Infrastructure and Key Asset Protection*, 47 Jurimetrics J. 259, 268–273 (2007).

28 במקרה של משק החשמל, בעיקר אם הוא מבוסס על תשתית חכמה, יש נקודות גישה רבות מאוד. ראו, למשל, Steven M. Bellovin et al., *Can It Really Work? Problems with Extending EINSTEIN 3 to Critical Infrastructure*, 3 Harv. Nat'l Sec. J. 1, 27 (2007).

רבות תלויות האחת ברעותה.[29] כך, למשל, פגיעה במערכת החשמל תשפיע על ייצור אנרגייה, שירותי טלקומוניקציה, שירותי חירום ועוד.[30] שלישית, הפגיעה בתשתיות חיוניות יוצרת "נראוּת" (או "impact"). נראוּת זו מתמרצת את ארגוני הטרור לבצע פגיעות מעין אלה שבאמצעותן יוכלו להציג את יכולתם, להוסיף לארגון יוקרה ואף להשפיע פסיכולוגית על הציבור. לבסוף, מפעילים רבים של תשתיות חיוניות עשויים לא לעמוד בסטנדרטים גבוהים של אבטחה עקב כשלי שוק שונים.[31] על־כן הפגיעה בתשתיות אלה עשויה להיות קלה באופן יחסי.

אנו נמצאים עתה בעידן של דיגיטציה. כדי להכיר את אופי האיומים בשעה זו, ראוי לציין שלושה פרמטרים הנדונים בספרות ובניירות מדיניות לצורך הערכת הסיכון וגיבוש הצורך בהתערבותם של מְאַסדרים בעניין ההגנה על תשתיות חיוניות:[32] ראשית, יש לבדוק את **ההשלכות** הצפויות של התקפה על התשתית החיונית הנדונה; שנית, יש לבדוק את **פגיעותה** של המערכת דנן, כלומר, להעריך את הסיכוי להצלחת התקפה כאמור או להתרחשות אירוע הרסני אחר; שלישית, יש לבחון את **היקף האיום** לביצוע תקיפה כאמור – גורם זה נגזר מהכוונות ומהיכולות של תוקפים פוטנציאליים, ומבוסס כמובן על הערכות מודיעין שונות בהקשרים ובזמנים שונים. עיון בשלושת הפרמטרים האמורים מבהיר היטב מדוע עולם הסייבר מחייב בדיקה מיוחדת של הסיכונים לפגיעה בתשתיות חיוניות ושל ההגנה הנחוצה עליהן. עולם הסייבר נושא עימו כמה מאפיינים מבדלים אשר ראויים להתייחסות, ולפיכך אי־אפשר להעתיק את המדיניות והאסטרטגיה הננקטות בהקשר של הגנה פיזית על תשתיות אל ממדי הסייבר של אתגר זה.[33] נדגים בקצרה את השינוי שעידן הסייבר מביא עימו בכל הנוגע בפרמטרים אלה. בתחילת דברינו הסברנו כיצד ההשלכות של תקיפת סייבר עלולות להיות הרות־אסון. עתה ניתן את דעתנו לשינוי שעולם הסייבר יוצר בפגיעותן של תשתיות חיוניות ובהיקף האיום עליהן (תוך התייחסות נקודתית לסוגיית ההשלכות).

דיגיטציה, סייבר ופגיעוּת – לפני העידן הדיגיטלי חששו מפעילי תשתיות חיוניות בעיקר מפני מתקפות פיזיות על תשתיותיהם, כמו־גם מנזקים שייגרמו כתוצאה משיתוף־פעולה בין גורם פנימי לבין גורם עוין, ונערכו נגד סיכונים אלה. הדיגיטציה הקטינה חלק מהסיכונים האמורים, עקב השימוש במנגנוני אבטחה משופרים, אולם העובדה שמרבית התשתיות החיוניות בחברה המודרנית עושות שימוש – ואפילו תלויות באופן זה או אחר – במערכות

---

29 ראו Rosenzweig, לעיל ה"ש 2, בעמ' 3 (בצטטו את Nassim Taleb, המסביר כי החיבוריות במערכות גורמת לכך שאירועים נכנסים לסחרור במהירות רבה). ראו גם Therese Kerfoot, Cybersecurity: Towards a Strategy for Securing Critical Infrastructure from Cyberattacks 9 (Silicon Flatirons Center, 2012), *available at* http://siliconflatirons.org/documents/publications/report/CybersecurityPaper.pdf.

30 לדוגמה, השבתת מערכת חשמל שהתרחשה בארצות־הברית בשנת 2003 גרמה נזק לתחבורה, לשירותי חירום, לשירותי מידע וטלקומוניקציה ואף לתעשיות המזון. ראו Whitley et al., לעיל ה"ש 27, בעמ' 269. לדיון נוסף בעניין ראו Kerfoot, לעיל ה"ש 29.

31 ראו דיון להלן בתת־פרק ד1.

32 ראו, לדוגמה, את הניתוח של המחלקה לבטחון המולדת בארצות־הברית (ה־DHS) במסמך המאוזכר להלן בה"ש 117.

33 טבנסקי "הגנה על תשתיות", לעיל ה"ש 18, בעמ' 72.

מחשוב ותקשורת יוצרת מימד נוסף של פגיעות,[34] במיוחד כאשר יש בהן מרכיב של גישה מרחוק ואפילו שליטה מרחוק.[35] נוסף על כך יש רגליים לסברה כי תשתיות דיגיטליות הינן פגיעות באופן אינהרנטי, שכן הן אינן ניתנות להגנה מוחלטת. אומנם שוק אבטחת המידע מתפתח כל העת ומייצר מערכות הגנה מתקדמות, אולם הגנות אלה מתיישנות במהרה כאשר מולן מתייצבים כלי תקיפה חדישים יותר. לבסוף, תשתיות חיוניות פגיעות יותר למתקפות סייבר, שכן מתקפות מעין אלה עלולות להיות מתמשכות ואדפטיביות, מה שמעלה את הסיכוי לפגיעה במערכת.[36]

היקף איום הסייבר: משאבים וסמיכות גיאוגרפית – מאחר שקיים רצון משמעותי לבצע פעולות עוינות, הקטנת העלויות הכרוכות בהן תביא לידי הגדלת הסיכון להתרחשותן. על פניו, תקיפות סייבר מוצלחות דורשות משאבים נכבדים, ועל־כן אין הכרח שייווצר כאן סיכון מוגבר. לדוגמה, על־פי פרסומים בעיתונות והערכות מומחים, לצורך ההתקפה המתוחכמת שבוצעה על מערכות הבקרה (SCADA) של חברת סימנס שהופעלו בכורים גרעיניים באיראן נדרשו מאמץ מודיעיני עצום וכן השקעה גדולה בכתיבת הקוד שבבסיס תולעת המחשב Stuxnet.[37] אולם תקיפה מהסוג שהתרחש לכאורה באיראן היא רק סוג אחד של מתווה פעולה. תקיפות סייבר יעילות ומזיקות יכולות להיות ״טפשות״ הרבה יותר. מתקפות סייבר יכולות לנצל פרצות אבטחה פשוטות יחסית, ללא השקעה כלכלית משמעותית מצד התוקף. אכן, מתרבות עדויות בדבר היכולת לבצע מתקפות מזיקות באמצעות תוכנות הזמינות ברשת.[38] עקב כך, ובהתאמה, מספר האתרים החשופים להתקפה קיברנטית גדול יותר ממספר האתרים החשופים להתקפות פיזיות. הרשת אף מאפשרת מתווה לפעולות תקיפה מתוחכמות יותר (אך עדיין זמינות כמעט לכל דכפין) באמצעות ה־darknet – מערך אנונימי להעברת מידע וכספים שבאמצעותו ניתן לרכוש כלי תקיפה חדישים, ״להזמין״ תקיפות מורכבות יותר ולתאם את הפעלתן, וכל זאת מבעד למבטן החודר של הרשויות.[39]

היקף האיום מתעצם ומתרחב גם עקב הסרת המגבלות הפיזיות הטבעיות המתקיימות במצב של תקיפה פיזית בלבד. תקיפות פיזיות מצריכות לרוב סמיכות גיאוגרפית אל המטרה – דרישה

34 Gareth Evans, *Protecting Critical Infrastructure in the Digital Age*, ARMY-TECHNOLOGY.COM (Feb. 14, 2012), http://www.army-technology.com/features/feature protecting-critical-infrastructure-in-the-digital-age ("In the digital age, however, things have become more complex, as conflict has gone online – and the potential implications for CIP [critical infrastructure protection] are enormous").

35 Derek E. Bambauer, *Ghost in the Network*, 162 U. PA. L. REV. 1011, 1022, 1051 (2014) (להלן: Bambauer, *Ghost*); RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR 99 (2014).

36 במתקפת סייבר יש סבירות גבוהה יותר לנסיונות חוזרים ונשנים לפריצת המערכת וללמידת הפגיעות שלה. ראו Derek E. Bambauer, *Conundrum*, 96 MINN. L. REV. 584, 618 (2011).

37 RONALD J. DEIBERT, BLACK CODE: INSIDE THE BATTLE FOR CYBERSPACE 176–180 (2013).

38 שם, בעמ׳ 168. בהקשר הישראלי ראו תיאור של דרך תקיפתו של ״ההאקר הסעודי״: Lior Tabansky, *Cybercrime: A National Security Issue?*, 4 MIL. & STRATEG. AFF. 117, 130 (2012).

39 שם, בעמ׳ 127. לסקירה מקיפה יותר של דינמיקה זו וגבולותיה ראו גבי סיבוני, דניאל כהן ואביב רוטברט ״איום ארגוני הטרור במרחב הסייבר״ **צבא ואסטרטגיה** 5(3) 3, 8–9, 19 (2013), המציינים גם כי טרם ידוע על התממשותו של תרחיש זה.

שמגבילה מלכתחילה את קבוצת התוקפים הפוטנציאליים לאלה שיש להם אפשרות גישה פיזית למקום (ואף מאפשרת את הקטנת הסיכון באמצעות הרחקה פיזית של גורמים עוינים). אולם מתקפת סייבר יכולה לעיתים להתבצע ממרחק רב,[40] תוך ניצול אפשרויות של גישה מרחוק. כל שהתוקף זקוק לו הוא ידע טכנולוגי (ולעיתים גם מודיעיני),[41] גישה למחשב ורשת תקשורת. בכך יש כדי להגדיל במידה משמעותית את מספר התוקפים הפוטנציאליים, ולפיכך הסיכון של קיום מתקפה מעין זו מתעצם. היקף הסיכון מתרחב גם משום שתקיפה ממקום רחוק המצוי מחוץ למעגל השליטה של המדינה המותקפת מקילה על התוקף, מאחר שאין הוא נדרש להכין תוכנית מילוט. הדבר מפשט את מתווה הפעולה של התוקף, מקטין את סיכוניו ולכן גם מגדיל את המוטיווציה לביצוע הפעולה.

זיהוי ושיוך: פגיעות מוגברת והיקף מוגבר – מתקפות סייבר כוללות במקרים רבים מאפיינים היוצרים קושי ואפילו כשל בזיהוי קיומה של תקיפה, כמו־גם בשיוכה לתוקף מסוים.[42] מאפיינים אלה מגדילים אף הם את הסיכון הגלום בתקיפות סייבר נגד תשתיות חיוניות, וזאת מכמה סיבות: ראשית, מתקפת הסייבר תתגלה לרוב רק לאחר ביצוע התקיפה, שאז ההרס כבר עלול להיות משמעותי.[43] כמו־כן, חדירה למערכת מחשוב אינה מתגלה בהכרח בעת החדירה עצמה, כך שהתוקף יכול להפעיל את המתקפה בכל עת שיחפוץ. מעבר לכך, לעיתים לא ברור כלל אם מדובר בהתקפה או שמא הייתה זו תקלה גרידא.[44] למאפיינים אלה יש השלכה כפולה: ראשית, השעיית ההפעלה ועמימותה עלולות להגביר את הנזק שייגרם ממנה, שכן התקיפה תתוזמן כך שהיא תיצור פגיעה מְרבית; שנית, מאפיינים אלה עלולים להגביר את היקף התקיפות, מכיוון שהן יאפשרו לתוקף להתרחק אל מחוץ לטווח השליטה של הנתקף לפני זיהוי התקיפה.

נוסף על כך, התקפות סייבר עלולות להערים קשיים באשר לזיהוי מקור הפגיעה ולייחוסה לפוגע.[45] הדיגיטציה מאפשרת טשטוש של עקבות התוקף או שתילת סימני זיהוי שגויים

---

40 Rosenzweig, לעיל ה״ש 2, בעמ׳ 4.

41 סיבוני, כהן ורוטברט, לעיל ה״ש 39.

42 Zhen Zhang, *Cybersecurity Policy for the Electricity Sector: The First Step to Protecting Our Critical Infrastructure from Cyber Threats*, 19 B.U. J. Sci. & Tech. L. 319, 330 (2013) (“Cyber events are difficult to predict, plan for, and identify”); Patrick W. Franzese, *Sovereignty in Cyberspace: Can It Exist?*, 64 A.F. L. Rev. 1, 31 (2009). ראו גם Clarke & Knake, לעיל ה״ש 35, בעמ׳ 123.

43 קושי בזיהוי ההרס שמתקפת סייבר יכולה לגרום התגלה, לדוגמה, בעקבות השימוש בתולעת המחשב הידועה Stuxnet, אשר פגעה בשנת 2010 בתוכנית הגרעין של איראן באמצעות הרס הצנטריפוגות ששימשו תוכנית זו. ראו Michael B. Kelley, *The Stuxnet Attack on Iran’s Nuclear Plant Was ‘Far More Dangerous’ Than Previously Thought*, Business Insider (Nov. 20, 2013), http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11?IR=T.

44 לדוגמה, אנשי חברת תעופה סברו כי מדובר בתקלה, אך בהמשך הגיעו למסקנה שמדובר במתקפת סייבר. רפאל קאהאן ״דיווח: האקרים סינים הם שהפילו את מערכות יונייטד איירליינס״ **כלכליסט** 30.7.2015 www.calcalist.co.il/internet/articles/0,7340,L-3665784,00.html.

45 Computer Sci. & Telecomms. Bd., Nat’l Acad. of Scis., Cybersecurity Today and Tomorrow: Pay Now or Pay Later 4–5, 27 (2002), *available at* http://citadel-information.com/wp-content/uploads/2012/08/cybersecurity-today-and-tomorrow-pay-now-

ומטעים. במקרים רבים התקיפה מבוצעת באמצעות מחשבו של משתמש תמים, ואז זהות התוקף האמיתי עשויה לא להתגלות לעולם.[46] מאפיין זה מגביר גם הוא את המוטיווציה לתקיפות (שכן הוא מקטין את הסיכון לתגובה מצד הנפגע) ולפיכך מרחיב את היקפן הפוטנציאלי.

לסיכום נציין כי עידן הסייבר מביא עימו תועלות ושיפורים רבים בכל הנוגע בניהולן של התשתיות החיוניות, בדמות הוזלת עלויות, הקטנת טעויות והקלה בניהול – גם מרחוק. אולם בד בבד עידן זה מצריך שינוי מהותי בתפיסת ההגנה על תשתיות חיוניות. מתקפת סייבר נדמית על פניה כמצריכה ידע, משאבים ומומחיות, אך בפועל היא עשויה להיות פשוטה, מהירה, אנונימית, נגישה וזולה יותר ממתקפות פיזיות ״רגילות״. עקב כך הבינו מעצבי מדיניות במדינות רבות כי יש לבחון מחדש את האיום על תשתיות חיוניות הנובע ממתקפות סייבר, ולהציע מדיניות ייחודית בנושא. במדינות אלה נקודת הפתיחה לדיון בבחירת האמצעים הראויים להגנת סייבר על תשתיות חיוניות היא בחינת עקרונות ההגנה מפני מתקפות סייבר.[47] אף שקיים שוני בין מדינות שונות בהגדרת עקרונות אלה, הן מתבססות בעיקרן על העקרונות של מוכנות ומניעה, איתור ותגובה, הפוגה והתאוששות, וכן שיתוף־פעולה בין־לאומי.[48] עם זאת, יישום עקרונות אלה יכול להתבטא בדרכים רבות ומגוונות. נעבור כעת לסקירה ולבחינה של דרכי יישום אלה, תוך הכרה בכך שבאימוץ פתרונות מסוגים שונים כרוכות עלויות כלכליות וכן פגיעות אפשריות בשוק, בחדשנות ואף בזכויות אדם של גורמים מעורבים וגורמים בלתי־מעורבים.

ב. המודל הישראלי: עבר, הווה ועתיד

המודל הישראלי להתמודדות עם ההגנה על תשתיות חיוניות מפני סיכוני סייבר הינו מודל ריכוזי, סודי במידה רבה, של גורם המפקח בצורה מקיפה על פעולותיהם של מפעילי התשתיות האמורים, תוך מתן הנחיות ישירות לפעולה מראש. מוקד הדיון בהסדרת האבטחה של גופים חיוניים בישראל מתרכז בחוק הביטחון. חוק הביטחון מגדיר מהו ״גוף ציבורי״ הכפוף להסדרתו – הגדרה הכוללת גם גופים פרטיים שאופי פעולתם ציבורי – וקובע מהן הפעולות

---

or-pay-later-national-research-council-2002.pdf. לניתוח בעיית הייחוס לפוגע קונקרטי ראו Scott J. Shackelford & Richard B. Andres, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, 42 Geo. J. Int’l L. 971, 979 (2011); David D. Clark & Susan Landau, *Untangling Attribution*, 2 Harv. Nat’l Sec. J. 323, 329 (2011).

46 Clarke & Knake, לעיל ה״ש 35, בעמ׳ 14 ו־23.

47 ראו התייחסות לעקרונות מעין אלה בהוראת ניהול בנקאי תקין 361 ״ניהול הגנת הסייבר״ 10 (16.3.2015); החלטה 2444 של הממשלה ה־33 ״קידום ההיערכות הלאומית להגנת הסייבר״ ס׳ 5 (15.2.2015).

48 ראו, למשל, בארצות־הברית: U.S. Dep’t of Homeland Sec., National Infrastructure Protection Plan 4 (2013) (להלן: NIPP 2013); ובאיחוד האירופי: *Policy on Critical Information Infrastructure Protection (CIIP)*, European Commission – Digital Single Market (Feb. 7, 2013), https://ec.europa.eu/digital-single-market/news/policy-critical-information-infrastructure-protection-ciip.

הדרושות לשם אבטחתם של גופים ציבוריים מפני איומים שונים. הולדת החוק לא רמזה בהכרח על התפקיד המרכזי שהוא עתיד למלא. בראשית דרכו, בשנת 1998, לא עסק חוק הביטחון בהגנה על תשתיות חיוניות ממוחשבות, אלא מנה רשימה של גופים המחויבים בפעולות אבטחה פיזיות לשמירה על בטחון האנשים המעורבים והמצויים בהם, בטחון הציבור או בטחון המדינה. נוסף על כך עסק החוק בפעילות לאבטחת מידע שחשיפתו עלולה לפגוע בבטחון המדינה.[49] רשימת הגופים המפוקחים מנתה באותה עת גופים פרטיים מעטים בלבד.[50]

ההכרה באיום הממשי שמתקפות סייבר מציבות לתשתיות חיוניות במדינת־ישראל באה לידי ביטוי בהחלטת ממשלה ב/84 של ועדת השרים לענייני ביטחון לאומי (להלן: הקבינט) מיום 11.12.2002,[51] ובשינויים בחוק הביטחון משנת 2005 אשר הגשימו את יעדיה של החלטת ממשלה זו. זאת, באמצעות הוספת קטגוריית אבטחה נוספת לחוק – "אבטחת מערכות ממוחשבות חיוניות" – והחובה למנות "אחראי" לאבטחתן של מערכות אלה.

נוסף על כך נדרשו שינויים בתשתית המשפטית הקיימת כדי להתאימה להתמודדות עם איומי הסייבר. הקבינט קבע אילו גופים יהיו כפופים להסדרה מיוחדת בהקשר זה.[52] בסופו של יום צומצמה הרשימה האמורה לרשימה הקיימת כיום בתוספת הרביעית לחוק הביטחון, המתעדכנת מדי פעם בפעם.[53] שינוי התוספת הרביעית (ואף החמישית, הנוגעת בהוראת־השעה אשר תידון בהמשך) לחוק הביטחון יכול להיעשות על־ידי השר לבטחון הפנים – בהתייעצות עם השר הממונה (השר הממונה על גוף ציבורי או שר הממונה על ביצוע חוק המסדיר את פעולותיו של גוף ציבורי), באישורה של ועדת הפנים ואיכות הסביבה של הכנסת ובאישורו של ראש הממשלה – כאשר מדובר בטעמים של בטחון המדינה, שלום הציבור ובטחונו.[54] לנוכח הסדר זה אין באפשרותנו להבין מהן אמות־המידה להוספת גופים לרשימה האמורה (או להסרת גופים ממנה), שכן אלה לא התפרסמו. עקב כך קשה להצביע על מדיניותה המוצהרת של ישראל בעניין זה, מעבר להבנה הכללית שמדובר בגופים "חשובים" שנבחרו במפורש. הרשימה כוללת כמה גופים ממשלתיים (שבהם לא נתמקד ברשימה זו) וכן גופים פרטיים. בתחום האנרגייה מדובר בחברות בתי־זיקוק ובבעלי החזקות נפט ("אשקלון", "תמר", "דלית", "נועה" ו"לויתן"); בתחום הכלכלי – הבורסה לניירות־ערך; בתחום הכימיקלים – חברת חיפה כימיקלים וחברת דשנים וחומרים כימיים; בתחום התקשורת – בזק, חברת מדיטרניאן

---

49 ס' 1 לחוק הביטחון.

50 פרט 8 לתוספת השנייה לחוק הביטחון, כנוסחו המקורי בשנת 1998, אשר כלל את החברות בזק, פלאפון, סלקום, פרטנר, ברק וכמה חברות טלקומוניקציה.

51 החלטה ב/84 של ועדת השרים לענייני ביטחון לאומי "אחריות להגנה על מערכות ממוחשבות במדינת ישראל" (11.12.2002) (להלן: החלטה ב/84). ראו גם רועי גולדשמידט "המרחב הקיברנטי וההגנה על תשתיות חיוניות" 1 (הכנסת – מרכז המחקר והמידע, 12.5.2013).

52 נספח א להחלטה ב/84, לעיל ה"ש 51.

53 התוספות הרביעית והחמישית לחוק הביטחון.

54 ס' 18(א) לחוק הביטחון.

נאוטילוס (ישראל) (מפעילת הכבל התת־ימי) וכמה חברות תקשורת נוספות (המרכיבות בעת הזו את התוספת הרביעית).[55]

החלטת הממשלה ותיקוני החוק שבאו בעקבותיה התמודדו גם עם דרך מימושה של מדיניות ההגנה על תשתיות חיוניות מפני מתקפות סייבר. לצורך כך קבעה ההחלטה כי האחריות להגנה על מערכות ממוחשבות תוטל על חמישה גופים: (1) הגופים עצמם המפעילים את המערכות הממוחשבות;[56] (2) ועדת היגוי העליונה להגנה על מערכות ממוחשבות;[57] (3) יחידה ממלכתית להגנה על מערכות ממוחשבות; (4) משרדי ממשלה; (5) גופים "מיוחדים" (כגון צה"ל, אשר אינם חלק מעניינוּ כאן).[58] ועדת ההיגוי העליונה מופקדת על בחינת הגופים ה"חיוניים" אשר זקוקים להגנה. אולם הפיקוח על ההגנה בפועל נעשה באמצעות היחידה המיוחדת האמורה: הרשות הממלכתית לאבטחת מידע (רא"מ), שהיא יחידה ייעודית של שירות הביטחון הכללי.[59] לאחרונה נוספה לרשימה זו גם "הרשות הלאומית להגנת הסייבר".

כאמור, כדי להגשים את יעדי ההחלטה, תוקן חוק הביטחון לצורך התאמת המנגנונים המשפטיים המצויים בו. החוק קובע כי לגבי הגופים האמורים בתוספת הרביעית יהיה נציג השב"כ "הקצין המוסמך", אשר סמכויותיו הרחבות מוגדרות לכל אורך החוק.[60] הקצין המוסמך מאשר את מינוי האחראי לאבטחתן של מערכות ממוחשבות חיוניות באותו גוף.[61] מעבר לכך, בסמכותו של הקצין המוסמך לתת "הנחיות מקצועיות",[62] לרבות כאלה הנוגעות ב"בקרה ודיווח". על הגוף הציבורי לפעול בהתאם להנחיות אלה על־פי חוק,[63] ונראה כי ניתן לנקוט סנקציות נגד מֵפרים.[64] במקרה של חוסר שביעות־רצון מההנחיות שנקבעו על־ידי הקצין המוסמך, החוק קובע מנגנונים לערעור ולבקשה לעיון חוזר בהן. נוסף על כך, הקצין המוסמך (לענייננו, כאמור, נציג השב"כ) רשאי להיכנס בכל עת לגופים המנויים בתוספת הרביעית, על־מנת לבדוק אם מולאו בהם ההוראות לפי חוק הביטחון וההנחיות שניתנו על־פיו.[65] כאשר הגוף המנוי בתוספת הרביעית פועל על בסיס רישיון, חובות אלה מצוינות בתנאיו.[66]

---

55 חברות התקשורת הנוספות המופיעות כיום בתוספת הרביעית לחוק הביטחון הן פלאפון תקשורת, סלקום ישראל, פרטנר תקשורת, 012 סמייל טלקום, 013 נטוויז'ן, בזק בינלאומי, הוט טלקום ומירס תקשורת.

56 תפקידיהם של הגופים המונְחים מוגדרים בס׳ 5(ב) להחלטה ב/84, לעיל ה"ש 51.

57 בראש ועדת ההיגוי עומד ראש המועצה לביטחון לאומי, וחברים בה נציגים בכירים של כל משרדי הממשלה מכל המגזרים, נציגי מערכת הביטחון ונציג היועץ המשפטי לממשלה. ראו פרוטוקול ישיבה מס׳ 142 של ועדת הפנים והגנת הסביבה, הכנסת ה־19, 24—25 (1.5.2007) (להלן: פרוטוקול מס׳ 142).

58 ס׳ 2 להחלטה ב/84, לעיל ה"ש 51.

59 שם, ס׳ 3—4.

60 ס׳ 1 לחוק הביטחון.

61 שם, ס׳ 2א.

62 שם, ס׳ 10(א).

63 שם, ס׳ 10(ב).

64 טבנסקי "הגנה על תשתיות", לעיל ה"ש 18.

65 ס׳ 15 לחוק הביטחון.

66 ראו, לדוגמה, ס׳ 66 לרשיון כללי לסלקום ישראל בע"מ למתן שירותי רדיו טלפון נייד בשיטה התאית (רט"ן) [נוסח משולב] נכון ליום ח׳ בטבת התשע"ה (30 בדצמבר 2014). הסעיף האמור

לנוכח החשיבות הרבה של תפקיד הקצין המוסמך, אם חוק הביטחון (בנוסחו המתוקן) מהווה את נקודת הפתיחה להכרת מדיניות הסייבר בישראל, רא״מ מהווה את אבן הראשה בה.[67] תפקידיה של רא״מ מגוונים. כאמור, היא נדרשת לעמוד בקשר עם הגופים המונְחים, וגם מופקדת על התיאום ביניהם.[68] נוסף על האמור, החלטת הממשלה הטילה על רא״מ חובות נוספות הנוגעות בגיבוש תורה ובאיסוף מודיעין בענייני סייבר.[69] יצוין כי לרא״מ יש אף סמכויות הנגזרות מחוקים אחרים – למשל, לעניין ההגנה על המאגר הביומטרי – אשר לא יידונו ברשימה זו.[70]

אולם ממשלת ישראל החלה בתהליכים שונים לשינוי מדיניות ההגנה על מרחב הסייבר בישראל. באוגוסט 2011 החליטה הממשלה להקים מטה קיברנטי לאומי במשרד ראש הממשלה, שמטרתו להסדיר את האחריות לטיפול בתחום הקיברנטי, לקדם את יכולת ההגנה על המרחב הקיברנטי בישראל וכן לקדם מחקר ופיתוח בתחום הקיברנטי וחישוב־העל.[71] בנושא של הגנה על תשתיות חיוניות קבעה ההחלטה כי הממשלה תפעל ״לשפר את ההגנה על תשתיות לאומיות שהן חיוניות לקיומם של חיים תקינים במדינת ישראל, ולחסנן, ככל הניתן, מפני התקפה קיברנטית״.[72] יעדים אלה באו לידי ביטוי במסמכי ההקמה של המטה, אשר התחיל לפעול בשנת 2012.[73]

בהמשך, בהחלטת ממשלה 2444 (15.2.2015), נקבע כי הרשות הלאומית להגנת הסייבר (גוף־על שיכלול גם את המטה הקיברנטי) תגבש מתווה להעברת ״שטח הפעולה בתחום פעולות לאבטחת מערכות ממוחשבות חיוניות״ מהשב״כ אל הרשות האמורה.[74] נוסף על כך נקבע כי תוקם ועדת היגוי אשר תאשר את הצעות השב״כ בנוגע לשינויים ברשימת הגופים

קובע גם חובה למלא אחר הוראות הביטחון המופיעות בנספח (יג). נספח זה אינו מפורסם בפומבי.

67 לפחות לעת עתה – ראו את הדיון לעיל ליד ה״ש 12 וכן להלן ליד ה״ש 77–78.

68 ראו את דבריו של צבי חרפק, מנהל אגף מערכות מידע ותקשוב בחברת החשמל, במסגרת הדיון בנושא ״׳מלחמה ברשת׳ – מלחמה על דעת הקהל והגנה על תשתיות לאומיות״ – פרוטוקול ישיבה מס׳ 18 של ועדת המדע והטכנולוגיה, הכנסת ה־17, 11 (26.7.2006) www.knesset.gov.il/protocols/data/rtf/mada/2006-07-26.rtf.

69 ס׳ 4(ה) להחלטה ב/84, לעיל ה״ש 51.

70 ראו חוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, התש״ע–2009; מבקר המדינה **דוח ביקורת: תיעוד לאומי ביומטרי – תקופת מבחן** (2015). יצוין כי הרשות לניהול המאגר הביומטרי הועברה בהוראת־השעה לתוספת החמישית, כך שנראה שחלק מסמכויות הניהול הנוגעות בה יועברו לרשות הסייבר.

71 החלטה 3611 של הממשלה ה־32 ״קידום היכולת הלאומית במרחב הקיברנטי״ (7.8.2011).

72 שם.

73 ״מטה הסייבר הלאומי״ **משרד ראש הממשלה** www.pmo.gov.il/BRANCHESANDUNITS/CYBER/Pages/default.aspx.

74 ס׳ 9 להחלטה 2444 של הממשלה ה־33 ״קידום ההיערכות הלאומית להגנת הסייבר״ (15.2.2015) (להלן: החלטה 2444). בס׳ 10 נקבע במפורש כי החלטה זו גוברת על החלטה ב/84 אשר נדונה לעיל.

המפוקחים על־ידי המנגנון הקבוע בחוק הביטחון לעניין מערכות ממוחשבות של תשתיות קריטיות.[75]

סמכותה של רשות הסייבר לפעול בהקשר זה החלה לצאת מן הכוח אל הפועל. באוגוסט 2016 התקבלה הוראת־שעה (אשר תוקפה יישמר עד ל־31.12.2018) המעבירה חלק מסמכויותיה של רא״מ אל רשות הסייבר. זאת, בכפוף ובהתאם לצו של ראש הממשלה שיתייחס לכל אחד מהגורמים שיועברו לגורם חדש זה (בעת כתיבת שורות אלה כבר אושרה בצו העברת מירב הגופים, והשלמת ההעברה צפויה בקרוב). על־פי הוראת־שעה זו, כל הגופים שהיו מנויים בתוספת הרביעית, למעט גופי התקשורת, הועברו לתוספת חדשה – החמישית – וסמכויותיו של הקצין המוסמך בנוגע לגופים המנויים בתוספת החמישית יועברו לרשות הסייבר.[76] לפיכך מעמדה של רא״מ לאחר הקמת המטה הקיברנטי (אשר בינתיים שונה שמו ל״מטה הסייבר הלאומי״),[77] כמו־גם היחס בין סמכויותיהם של הגופים הללו, אינם ברורים נכון למועד כתיבתן של שורות אלה.

הקמת הרשות החדשה עשויה אף להוסיף מימד לפעילות המדינה בתחום הגנת הסייבר על תשתיות חיוניות. סעיף 2(א) להחלטת ממשלה 2444 מסביר כי אחד מתפקידי הרשות האמורה הוא לטפל באירועי סייבר בזמן־אמת. סעיף 2(ב) מוסיף כי הרשות אף תפעיל מרכז לסיוע עם התמודדות סייבר, המכונה ״ה־CERT הלאומי״ (CERT – Computer Emergency Response Team). כחלק מכך תפקידה של הרשות הוא לרכז ולשתף מידע רלוונטי, ולהוות ״נקודת ממשק מרכזית בין גופי הביטחון לבין הגורמים במשק״. תפקידים אלה מצריכים פעילות מהירה וממשק מיידי בין המדינה לבין אותם גופים פרטיים שייקבע כי הגנתם נדרשת. נראה כי זהו מימד חדש וחשוב במודל ההגנה המתרקם.[78]

ג. מודלים מקבילים להגנה על תשתיות חיוניות

מדינות רבות מכירות כיום בצורך בהגנה על תשתיות חיוניות מפני מתקפות סייבר.[79] באופן כללי נראה כי הנטייה הכללית במדינות אלה היא להסדרה וולונטרית של מנגנוני ההגנה על התשתיות החיוניות.[80] בחלק זה נסקור בקצרה שני מודלים עיקריים – זה הנוהג בארצות־הברית וזה הנוהג באירופה.

75 שם, נספח א, פרק 2.

76 ראו לעיל ה״ש 12.

77 ס׳ 11(ד) להחלטה 2444, לעיל ה״ש 74.

78 Tabansky & Ben Israel, לעיל ה״ש 8, בעמ׳ 55–56. ראו גם את הדיון להלן בה״ש 188 ובטקסט שלידה.

79 לסקירה על ההגנה על תשתיות חיוניות מפני מתקפות סייבר ב־34 מדינות ראו Scott J. Shackelford et al., *Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 Tex. Int'l L.J. 303 (2015).

80 שם, ליד ה״ש 260.

1. המודל האמריקאי

(א) המודל הכללי – התערבות מוגבלת

הגישה האמריקאית להגנה על תשתיות חיוניות מתבססת בעיקרה על התערבות ממשלתית מוגבלת והסתמכות על הסכמים וולונטריים עם בעלים ומפעילים של תשתיות חיוניות.[81] עם זאת, ניתן לראות מעורבות רציפה ומקיפה של הממשל, אשר מעידה על עניין רב בתחום והבנת חשיבותו. על־כן קשה לטעון כי ההחלטה לצמצם את המעורבות הישירה והאגרסיבית של גופי המדינה בתחום זה נובעת מהזנחה, אף שניתן בהחלט לתלות אותה בתפיסה אידיאולוגית המאפשרת לגופים פרטיים כר פעולה נרחב.

חשיבות ההגנה על תשתיות חיוניות דיגיטליות קיבלה לראשונה הכרה בארצות־הברית באמצע שנות התשעים של המאה העשרים. במטרה לבחון את חשיבות ההגנה על תשתיות חיוניות מפני מתקפות טרור, יצר הנשיא קלינטון את ״קבוצת־העבודה על תשתיות חיוניות״ (Critical Infrastructure Working Group – CIWG). קבוצה זו בחנה את פגיעותה של ארצות־הברית למתקפות טרור, ופרסמה דוח בנושא במרץ 1996. הדוח הוביל להקמת ״הוועדה הנשיאותית להגנה על תשתיות חיוניות״ (President's Commission on Critical Infrastructure Protection – PCCIP), שנתנה את דעתה להיבטי הפגיעות הנוגעים במחשוב.[82] ה־PCCIP הובילה לשתי החלטות נשיאותיות במאי 1998 (Presidential Decision Directives (PDD) 62 & 63).[83] מתוקף שתי ההחלטות הללו נוצרו סוכנויות חדשות, ביניהן ה־National Infrastructure Protection Center (NIPC) שה־FBI יצר תחתיו.[84] החלטה PDD-63 זיהתה את המגזרים השונים

---

81 Dan Assaf, *Models of Critical Information Infrastructure Protection*, 1 Int'l J. Crit. Infrastructure Protection 6, 7–8 (2008). להמחשת אופייה הוולונטרי של ההסדרה בארצות־הברית ראו, למשל, תוכנית של ה־DHS שהחלה לפעול בפברואר 2014, אשר קוראת לגופים פרטיים להשתתף בשמירה על תשתיות חיוניות: *Critical Infrastructure Cyber Community C^3 Voluntary Program*, Homeland Security (June 17, 2015), https://www.dhs.gov/ccubedvp.

82 Exec. Order No. 13,010, 61 Fed. Reg. 37,347 (Jul. 15, 1996). תפקידו של ה־PCCIP היה לדווח לנשיא על האיומים הנשקפים לתשתיות החיוניות בארצות־הברית, להמליץ על מדיניות לאומית להגנה על תשתיות חיוניות, להעריך את ההשלכות המשפטיות של הגנה על תשתיות חיוניות, ולהציע שינויים אסדרתיים לצורך יישום ההמלצות. על הרקע ליצירת ועדה היסטורית זו ראו Clarke & Knake, לעיל ה״ש 35, בעמ׳ 106–107. על החלטות הוועדה ראו בכלליות Kathi A. Brown, Critical Path: A Brief History of Critical Infrastructure Protection in the United States (2006).

83 Presidential Decision Directive 63 (May 22, 1998) (להלן: החלטה PDD-63); Press Release, White House, Fact Sheet: Combating Terrorism Presidential Decision Directive 62 (May 22, 1998), *available at* http://www.fas.org/irp/offdocs/pdd-62.htm.

84 ראו Whitley et al., לעיל ה״ש 27, בעמ׳ 262. נוסף על ה־NIPC הוקמו סוכנויות פדרליות ייעודיות דוגמת ה־National Infrastructure Advisory Council (NIAC) וה־Critical Infrastructure Assurance Office (CIAO). ראו Eric A. Greenwald, *History Repeats Itself: The 60-Day Cyberspace Policy Review in Context*, 4 J. Nat'l Sec. L. & Pol'y 41, 46–49 (2010); החלטה PDD-63, לעיל ה״ש 83.

שנדרשת הגנה עליהם, וקבעה ארבעה תחומי הגנה מגזריים.[85] בינואר 2000 הובילו מסקנות ה־PCCIP להקמת תוכנית לאומית להגנה על תשתיות מידע (National Plan for Information Systems Protection).[86] יצוין כי לתוכניות אלה קדמו מערכות קודמות אשר נבנו בתקופת המלחמה הקרה ויצרו רשימות של משאבי־מפתח (לרבות גופים פרטיים) שעליהם הגנו משרד הביטחון וה־FBI.[87]

מתקפות הטרור שהתרחשו ב־11 בספטמבר 2001 הובילו לבדיקה של מכלול ההגנה על ארצות־הברית ומוסדותיה, והגבירו את ההבנה כי יש לספק הגנה נאותה יותר לתשתיות חיוניות מפני מתקפות בכלל ומפני מתקפות סייבר בפרט. בהמשך לשני צווים נשיאותיים שהוציא הנשיא בוש,[88] חוקק ה־USA PATRIOT Act בשנת 2001. החוק הקים את ה־National Infrastructure Simulation and Analysis Center (NISAC) – מרכז אשר נכלל מאוחר יותר במחלקה לבטחון המולדת (Department of Homeland Security – DHS). גוף זה ריכז לתוכו סמכויות רבות שהיו בידי סוכנויות ממשלתיות שונות, ובתוך כך גם את הסמכויות הנוגעות בהגנה על תשתיות קריטיות. המטרה בהקמת ה־NISAC הייתה להחליף גופים קודמים שעסקו בתשתיות חיוניות (דוגמת NIPC) וכן לספק ניתוח אסטרטגי של ההשלכות האפשריות של הפרעות בתשתיות חיוניות ברחבי המדינה. בשנת 2002 חוקק הקונגרס את ה־Homeland Security Act, אשר בין היתר מחייב את ה־DHS לפתח תוכנית לאומית להגנה על תשתיות (National Infrastructure Protection Plan – NIPP).[89] עד כה פורסמו שלושה דוחות NIPP – בשנת 2006, בשנת 2009 ולאחרונה בשנת 2013. הדוח האחרון מקטלג את התשתיות החיוניות לשישה־עשר מגזרים, ומחלק את האחריות להגנתן בין סוכנויות ייעודיות (sector-specific agencies – SSAs).[90] מטרת ה־NIPP היא ליצור מודלים והערכות סיכון, לפתח תוכניות הגנה

85 החלטה PDD-63, שם, יצרה גם את תפקיד המתאֵם הלאומי לאבטחה, להגנת תשתיות ולמאבק בטרור. ראו Moteff, לעיל ה״ש 25, בעמ׳ 4.

86 Myriam Dunn Cavelty, Cyber-Security and Threat Politics 91–92 (2008).

87 Brown, לעיל ה״ש 82, בעמ׳ 36–50.

88 צו 13,228 הקים את המשרד לבטחון המולדת (Office of Homeland Security), אשר קדם להקמת המחלקה לבטחון המולדת מכוח חקיקה, ואת המועצה לבטחון המולדת (Homeland Security Council). צו 13,231 הקים את המועצה הנשיאותית לשמירה על תשתיות חיוניות (President's Critical Infrastructure Protection Board) ואת המועצה המייעצת הלאומית לתשתיות (National Infrastructure Advisory Council). ראו Moteff, לעיל ה״ש 25, בעמ׳ 8–9.

89 Homeland Security Act 2002, Pub. L. No. 107-296, § 214, 116 Stat. 2135. החוק הקנה סמכות לנשיא ולמזכיר הביטחון הלאומי לפתח תוכניות להגנה על תשתיות חיוניות. ראו Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks*, 88 Tex. L. Rev. 1533, 1556 (2010). ראוי לציין כי החוק גם מקנה הגנות מסוימות למפעילי תשתיות חיוניות אשר משתפים מידע רלוונטי באופן וולונטרי עם רשות פדרלית.

90 NIPP 2013, לעיל ה״ש 48, בעמ׳ 11.

ואסטרטגיות של עמידות, ולספק לכל מגזר קווי מדיניות.[91] השתתפותם של גורמים פרטיים הינה וולונטרית (למעט חריגים שנדון בהם בהמשך).[92]

בשנת 2003 פרסם הממשל האמריקאי מסמך בשם ״האסטרטגיה הלאומית לאבטחת מרחב הסייבר״.[93] במסמך חשוב זה התייחס הממשל לחשיבות ההגנה על תשתיות חיוניות בארצות־הברית, אך בד בבד קבע כי הממשל הפדרלי לא יאבטח את מערכות המחשב של גופים פרטיים, אף אם הם נכנסים בגדר תשתיות חיוניות.[94] בעקבות פרסום המסמך הוציא הבית הלבן צו נשיאותי שמנחה את יישום ההמלצות הקבועות בו.[95] בשנת 2006 הוקם ה־Critical Infrastructure Partnership Advisory Council (CIPAC), שמטרתו לשמש גוף מתווך בין הגופים השלטוניים המופקדים על שמירת תשתיות חיוניות לבין הגופים הפרטיים המהווים תשתית חיונית.[96] עם הזמן יצר ה־DHS משרדים שונים העוסקים בניתוח ההגנה על תשתיות חיוניות.[97]

עם כניסתו לבית הלבן הורה הנשיא אובמה על בחינה מחדש של אסטרטגיות ההגנה על מרחב הסייבר.[98] בחינה זו הובילה לפרסום שני דוחות: Cyberspace Policy Review בשנת 2009, ו־International Strategy for Cyberspace בשנת 2011.[99] בין היתר הדגישו

---

91 39 Weekly Comp. Pres. Doc. 1816 (Dec. 17, 2003), בעמ׳ 18; Talbot Jensen, לעיל ה״ש 89, בעמ׳ 1557.

92 U.S. Dep't of Def., Defense Industrial Base: Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan (2007), *available at* http://www.dhs.gov/xlibrary/assets/nipp-ssp-defense-industrial-base.pdf. ראו גם Talbot Jensen, לעיל ה״ש 89, בעמ׳ 1577.

93 White House, The National Strategy to Secure Cyberspace (2003), *available at* https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

94 שם, בעמ׳ 11 ("[T]he federal government could not – and, indeed, should not – secure the computer networks of privately owned banks, energy companies, transportation firms, and other parts of the private sector").

95 Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*, Homeland Security (Dec. 17, 2003), *available at* https://www.dhs.gov/homeland-security-presidential-directive-7.

96 *Critical Infrastructure Partnership Advisory Council*, Homeland Security (Jul. 29, 2015), http://www.dhs.gov/critical-infrastructure-partnership-advisory-council.

97 Homeland Infrastructure Threat and Risk Analysis Center (HITRAC); National Infrastructure Simulation and Analysis Center (NISAC); Office of Cyber and Infrastructure Analysis (OCIA). ראו, למשל, *Office of Cyber and Infrastructure Analysis (OCIA)*, Homeland Security (Jul. 28, 2015), https://www.dhs.gov/office-cyber-infrastructure-analysis.

98 ראו Shackelford et al., לעיל ה״ש 79, בעמ׳ 324–325.

99 Cyberspace Policy Review: Assuring a Trusted and resilient Information and Communications Infrastructure (White House, 2009), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf; International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World 20–21 (White House, 2011), *available at* https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

הדוחות את חשיבות ההגנה על תשתיות חיוניות, והובילו להקמת גוף צבאי שמטרתו לרכז את פעילות הסייבר הצבאית בארצות־הברית ((U.S. Cyber Command ("CYBERCOM").[100] אולם הנשיא אובמה הדגיש עדיין כי הממשל לא יקבע סטנדרטים מחייבים של אבטחה לחברות הפרטיות.[101] בפברואר 2013 פרסם אובמה צו נשיאותי (Presidential Policy Directive 21 (PPD-21)) שקרא לעדכון נוסף של התוכנית הלאומית להגנה על תשתיות (NIPP). באותו חודש הוציא הנשיא גם הוראה (Executive Order (EO) 13636 – Improving Critical Infrastructure Cybersecurity) שהנחתה את הממשל הפדרלי ליצור תיאומים עם בעלים ומפעילים שונים של תשתיות חיוניות על־מנת לשפר את ההגנה על המידע ואת אבטחת הסייבר, לפתח במשותף גישות מבוססות־סיכון לאבטחת סייבר וליישמן.[102]

בהתאם ובהמשך להוראות אלה פרסם ה־NIST (גוף התקינה המרכזי של ארצות־הברית), בפברואר 2014, מסגרת לשיפור ההגנה הקיברנטית על תשתיות חיוניות,[103] אשר נוצרה באמצעות שיתוף־פעולה ציבורי–פרטי. מסגרת זו מכילה סטנדרטים, הנחיות ופרקטיקות לעידוד הגנה על תשתיות חיוניות, אך לא חובות משפטיות. ה־NIST פרסם גם מפת דרכים לשיפור ההגנה על תשתיות חיוניות בארצות־הברית בשנים הקרובות.[104] בסוף 2014 הרחיב הקונגרס את מתחם האחריות של ה־NIST, כאשר דרש ממנה ליצור סטנדרטים ופרקטיקות של אבטחת סייבר לתשתיות קריטיות וכן לתמוך בפיתוחם של סטנדרטים ופרקטיקות כאלה.[105]

בדצמבר 2014 חוקקה ארצות־הברית את ה־ National Cybersecurity Protection Act (NCPA),[106] אשר הקים את ה־ National Cybersecurity and Communications Integration Center (NCCIC). תפקידו של מרכז זה הוא לבסס פלטפורמה בעבור הממשל והמגזר הפרטי לצורך שיתוף מידע על איומים ותקריות ולצורך מתן עזרה טכנית. בין היתר, ה־NCCIC מפעיל את ה־CERT של מערכות השליטה בתעשייה (ICS-CERT), שמטרתו היא להפחית סיכונים בכלל המגזרים באמצעות שיתופי־פעולה (גם בזמן־אמת) עם רשויות האכיפה והמודיעין

100 U.S. Cyber Command, United States Strategic Command (Jan. 12, 2015), http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-comm and-uscybercom/.

101 Clarke & Knake, לעיל ה״ש 35, בעמ׳ 118.

102 גישות מבוססות־סיכון לאבטחת סייבר מתבססות על תהליך שבוחן, בין היתר, את פגיעותן של מערכות, את סבירותן של מתקפות סייבר ואת הנזק הפוטנציאלי של מתקפות אלה. באמצעות תהליך כזה ניתן, למשל, להבחין בין תשתיות חיוניות שונות מבחינת רמת פגיעותן, ולהעניק להן הגנה בהתאם. ראו The White House, Executive Order 13636 – Improving Critical Infrastructure Cybersecurity (2013), *available at* http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

103 National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity (Feb. 12, 2014), *available at* https://www.nist.gov/document-3766.

104 NIST Roadmap for Improving Critical Infrastructure Cybersecurity (Feb. 12, 2014), *available at* http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf.

105 ראו Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274.

106 National Cybersecurity Protection Act of 2014, Pub. L. No. 113-282, § 2519, 128 Stat. 3066.

ותיאום שיתופי־פעולה ושיתוף מידע בין מפעילים לבין הסוכנויות השונות.[107] מרכז זה אמור לכלול נציגים מסוכנויות פדרליות, נציגי ממשל פדרלי ומדינתי ומפעילים מהמגזר הפרטי, כולל מפעילי תשתיות חיוניות, בהתאם לשיקול־הדעת של המזכיר לענייני הגנת מולדת.[108] בפברואר 2015 ניתן צו נשיאותי נוסף,[109] שנועד לעודד את הקמתם של ארגונים לניתוח ולעיבוד של מידע שיספקו מסגרת להגנה על תשתיות קריטיות.[110]

בדצמבר 2015 חוקקה ארצות־הברית את ה־Consolidated Appropriations Act, אשר מכיל בתוכו את ה־Cybersecurity Act of 2015.[111] חוק זה מתיר לחברות פרטיות לנטר את הרשתות שלהן, להפעיל אמצעי הגנה ולשתף עם חברות אחרות ועם הממשל האמריקאי אמצעי הגנה או מידע שיש בו ״סממנים של איום סייבר״ (cyber threat indicators).[112] עם מגבלות מסוימות, החוק מקים מסגרת לשיתוף־פעולה וולונטרי של חברות פרטיות עם ה־DHS (גם בהקשרים שמעבר לתשתיות חיוניות). בתמורה לשיתוף־הפעולה יקבלו החברות הללו חסינות משפטית ופטור מחובת יידוע לפי חוק חופש המידע בגין פעולות הנוגעות בשיתוף־פעולה זה.[113] חוק זה אינו מהווה נקודת מפנה דרמטית בגישה האמריקאית להגנה על תשתיות חיוניות מפני מתקפות סייבר. יצוין כי לפני הקונגרס היו מונחות כמה הצעות חוק הנוגעות בהיבטים שונים של הגנת סייבר, אשר ייתכן שיידונו בגרסאות שונות בעתיד.[114]

(ב) מקרים חריגים — התערבות מקיפה יותר

למרות האמור לעיל, אין זה מדויק לומר כי מדיניות הסייבר של ארצות־הברית בכללותה מבוססת על הסדרים וולונטריים. יש מגזרים שונים הכפופים לאסדרה ברמות שונות, הכוללת החלת סטנדרטים של אבטחה עליהם, גם בהקשר של סייבר. כך, למשל, בתעשיית הכימיקלים ובמגזר האנרגייה קיימים מודלים החורגים מההסדרה הוולונטרית.[115] באשר **לחברות הכימיקלים**, החוק (משנת 2007)[116] מחייב אותן לעמוד בסטנדרטים פדרליים של הגנה על התשתיות, אשר נקבעו על־ידי ה־DHS ומתייחסים גם לסייבר. מדובר במסמך כללי המונה

107 ראו The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), https://ics-cert.us-cert.gov.

108 *Congress Passes Four Cybersecurity Bills*, The National Law Review (Dec. 13, 2014), http://www.natlawreview.com/article/congress-passes-four-cybersecurity-bills.

109 Exec. Order No. 13691, 80 Fed. Reg. 9347 (Feb. 20, 2015).

110 שם, ס׳ 2.

111 Consolidated Appropriations Act of 2016, Pub. L. No. 114-113, 29 Stat. 2242 (2016).

112 שם, ס׳ 104.

113 שם.

114 ראו, למשל, H.R. 1560 114th Cong., 1st Sess., § 203 (2015–2016); Cybersecurity Information Sharing Act of 2015, 114th Cong. 1st Sess., § 754 (2015); H.R. 3523 112th Cong., 2d Sess. (2012).

115 כך גם מפעילי תשתיות בנמלי ארצות־הברית. הללו מפוקחים על־ידי משמר החופים וכפופים ל־Maritime Transportation Security Act of 2002, Pub. L. No. 107-295, 116 Stat. 2064, אשר מחיל אף הוא סטנדרטים נוקשים. ראו Moteff, לעיל ה״ש 25, בעמ׳ 30–31.

116 Homeland Security Appropriations Act of 2007, Pub. L. No. 109-295, § 550, 120 Stat. 135.

שמונה־עשר עקרונות רחבים שיש לפעול לפיהם (risk-based performance standards – RBPS). לשם הבהרת דרכי יישומם של העקרונות, פורסם מסמך ייעוץ (guidance) מקיף, אשר אינו מחייב, אלא רק מהווה דוגמה לצעדים שניתן לנקוט על־מנת לעמוד בעקרונות ה־RBPS.[117] נוסף על העמידה בעקרונות, וכדי לאפשר את אכיפתם, ה־DHS אף מחייב גופים אלה לענות על שאלון מקיף אשר מצריך סקירה של אמצעי ההגנה השונים הננקטים ומאפשר ל־DHS להעריך נכונה את הסיכונים הנשקפים לגופים השונים ואת הצעדים שיש לנקוט.[118] חוק זה עודכן לאחרונה לפני שנים מספר,[119] ובנוסחו הקיים הוא אף כולל ״שיניים אסדרתיות״ המאפשרות מתן קנסות[120] ואף צו סגירה למפעל לכימיקלים אשר יימצא כי אינו עומד בכללים הנדרשים.[121] ניתן להניח כי ההסדרה המיוחדת לענף זה נובעת מההשלכות הקטסטרופליות האפשריות של כשל בפעילותו.

התערבות אסדרתית נוספת נוגעת כאמור **בתעשיית האנרגייה**, אשר ידועה בפגיעותה להתקפות ולכשלים מסוגים שונים.[122] תחילה נסקור את מגזר התחנות הגרעיניות, אשר זכה בהסדרה ייחודית, המתבצעת על־ידי ה־Nuclear Regulatory Commission. תחנות אלה מחויבות לעמוד בכללים הנוגעים בעמידוּת מפני תקיפות, בין היתר מפני תקיפות סייבר, כמו־גם להגיש לאישור הנציבות תוכנית באשר לדרכים שבכוונתן לנקוט על־מנת לעמוד ביעד זה. כדי לסייע לגופים לעמוד ביעד העמידוּת האמור, פרסמה הנציבות האמורה מסמך מייעץ – ה־Regulatory Guide 5.71.[123] יצוין כי מסמך זה הינו וולונטרי, שכן ניתן לעמוד בדרישות העמידוּת גם בדרכים אחרות.[124]

רוב הרשויות האחרות העוסקות במשק החשמל (יותר מאלף וחמש מאות גופים פרטיים)[125] מוסדרות על־ידי ה־Federal Energy Regulatory Commission (FERC). נציבות FERC קובעת סטנדרטים שמגזר האנרגייה חייב לעמוד בהם, לרבות סטנדרטים הנוגעים בסייבר.[126] הליך קביעת הסטנדרטים בהקשר זה הינו ייחודי: הם נקבעים על־ידי התעשייה

117 ראו Risk-Based Performance Standards Guidance: Chemical Facility Anti-Terrorism Standards (Department of Homeland Security, 2009), *available at* https://www.dhs.gov/xlibrary/assets/chemsec_cfats_riskbased_performance_standards.pdf.

118 ראו CSAT Security Vulnerability Assessment Application – Instructions (Jan. 3, 2011), http://www.dhs.gov/sites/default/files/publications/csat_sva-instructions_508.pdf.

119 CFATS Act of 2014, Pub. L. No. 113-254, 128 Stat. 2898 (להלן: CFATS Act).

120 מדובר בקנסות משמעותיים של עד מיליון דולר להפרה. ראו Susan J. Court, *Federal Cyber-Security Law and Policy: The Role of the Federal Energy Regulatory Commission*, 41 N. Ky. L. Rev. 437, 437 (2014).

121 CFATS Act § 624.

122 Bellovin et al., לעיל ה״ש 28, בעמ׳ 27.

123 U.S. Nuclear Regulatory Commission, Regulatory Guide 5.71 (Jan. 2010), https://scp.nrc.gov/slo/regguide571.pdf.

124 Nuclear Reactors, Materials, and Waste Sector-Specific Plan 29–30 (DHS, 2010), *available at* http://www.dhs.gov/xlibrary/assets/nipp-ssp-nuclear-2010.pdf.

125 Court, לעיל ה״ש 120, בעמ׳ 437.

126 ראו, למשל, *Energy Sector-Specific Plan – An Annex to the National Infrastructure Protection Plan* 94–96 (2010), https://www.dhs.gov/xlibrary/assets/nipp-ssp-energy-2010.pdf.

(באמצעות גוף המכונה NERC, המאגד בתוכו גופים פרטיים), ולאחר־מכן מאושרים על־ידי ה־FERC (שהיא כאמור זרוע של הממשל הפדרלי).[127] הליך האישור כולל משא־ומתן בין המדינה לבין נציגי התעשייה.[128] תהליך זה חוזר על עצמו לצורך עדכונים, ועד עתה הוא בוצע ארבע פעמים.[129] גם אכיפת הכללים נעשית בצורה משולבת: הגוף המייצג את התעשייה – ה־NERC – ממליץ על הטלת הסנקציות; וה־FERC בודקת, וברוב המקרים אוכפת כמבוקש.[130]

איטיותו של הליך זה ואולי אף נטייתו להחלת סטנדרטים רופפים יחסית עוררו ביקורת. כך, באחד המקרים אושרה גרסה של סטנדרטים (הרביעית) אך עד שהגיע המועד ליישומה, היא כבר התיישנה והוחלט להחליפה באחרת, עדכנית יותר.[131] נוסף על כך אין זה ברור אם ל־FERC יש עתודות כוח־אדם מספקות לצורך עריכת הבדיקות הנדרשות.[132] אכן, דוח של מחלקת האנרגייה האמריקאית העלה ספקות בדבר יעילותו של הליך אסדרה זה ככל שהדבר נוגע ביכולות העבודה, היישום והעמידה בזמנים.[133] דוח אחר (של ה־GAO) ביקר אף הוא את מנגנון ההסדרה הזה,[134] וציין כי שיתוף־הפעולה בין הגופים הציבוריים והפרטיים מוביל להסדרה לא־ראויה – כללית, שטחית ולעיתים מקילה מדי – עקב האינטרסים הספציפיים של התעשייה (בעיקר לעניין היקף החיבור שלה למרשתת). נוסף על כל אלה, אף אנשי ה־FERC עצמם התלוננו לאחרונה על המודל האמור, אם כי מהיבט אחר; הם הלינו כי ההליך האמור מתאפיין בשקיפות רבה מדי, אשר מאפשרת העברת מידע מיותר לתוקפים, וכן בקשיחות מוגזמת, המגבילה את יכולתם להגמיש את הכללים ולתת מענה מהיר לשחקנים מסוימים. מנימוקים אלה הם ביקשו שסמכויותיהם יורחבו.[135]

כנגד זה, לפחות כותב אחד[136] סבור כי ההסדר האמור, למרות מגרעותיו, עשוי להוות פתרון מיטבי, וכי ניתן בהחלט ללמוד ממנו על הדרך הנכונה להסדיר הגנה על תשתיות מפני איומי סייבר. התכונה החיובית המרכזית של מודל זה היא הדרך שבה הוא כופה על חברות מתחרות לעבוד יחדיו. מודל זה אומנם איטי, אך הוא מתייחס לדרישות שהתעשייה לבדה לא

Mandatory Reliability Standards for Critical Infrastructure Protection, Order No. 706, 122 FERC ¶ 61,040, order on reh'g, Order No. 706-A, 123 FERC ¶ 61,174 (2008), order on clarification, Order No. 706-B, 126 FERC ¶ 61,229 (2009), order on clarification, Order No. 706-C, 127 FERC ¶ 61,273 (2009). כן ראו Assaf, לעיל ה״ש 81, בעמ׳ 7–8.

127 Ellis, לעיל ה״ש 23, בעמ׳ 49.

128 Court, לעיל ה״ש 120, בעמ׳ 449.

129 שם, בעמ׳ 441.

130 שם, בעמ׳ 450.

131 שם, בעמ׳ 443–444.

132 Clarke & Knake, לעיל ה״ש 35, בעמ׳ 168. המחברים אף קוראים להעביר סמכויות ביקורת אלה לגוף בקרת סייבר מרכזי (שם, בעמ׳ 266).

133 Court, לעיל ה״ש 120, בעמ׳ 454.

134 United States Government Accountability Office, Electricity Grid Modernization (2011), *available at* http://www.gao.gov/assets/320/314410.pdf. ראו גם Robert K. Palmer, *Critical Infrastructure: Legislative Factors for Preventing a "Cyber-Pearl Harbor"*, 18 Va. J.L. & Tech. 289, 340–341 (2014).

135 Court, לעיל ה״ש 120, בעמ׳ 454.

136 Ellis, לעיל ה״ש 23, בעמ׳ 52–54.

הייתה מעלה. נוסף על כך הוא מאפשר יתרונות שמודל אסדרה מלא (top-down) לא היה מביא לידי ביטוי, כגון שיתוף רב יותר של ידע שנצבר אצל הגופים הפרטיים־המסחריים.

(ג) המודל האמריקאי – סיכום ופנים לעתיד

המודל האמריקאי נסמך בעיקרו על השתתפות וולונטרית של מפעילי תשתיות חיוניות. הממשל, מצידו, מספק לבעלי התשתיות החיוניות מידע על איומים ותקריות, ויוצר מסגרת לשיתוף־פעולה ולשיפור ההגנה הלאומית. יש אף תשתית משפטית לאסדרה עקיפה של ההתחייבויות הוולונטריות של גופים לעמידה בסטנדרטים ראויים באמצעות גופי אסדרה כלליים, דוגמת הרשות לסחר הוגן (FTC) והרשות לניירות־ערך (SEC).[137] אולם ההסדרה אינה עשויה מקשה אחת.

נוסף על כך יש לציין כי הממשל האמריקאי מפעיל מערכת הגנה מתקדמת, בין היתר להגנה על תשתיות, בעלת השם היומרני ״איינשטיין 3״.[138] המערכת בודקת (באמצעות התחברות לספקי תקשורת מובחרים) את מכלול התקשורת המיועדת לכמה אתרים פדרליים עוד לפני שהמידע מגיע אליהם, תוך השוואת דפוסי המידע לדפוסים מוכרים של התקפות סייבר.[139] בכך המערכת פועלת למניעת התקפות באופן פעיל ובעוד מועד. לאחרונה ניכרת מגמה של הצטרפות וולונטרית של גופים פרטיים למטריית ההגנה של מערכת זו. יש הטוענים כי הצטרפות זו אינה וולונטרית ממש, שכן הדבר מהווה תנאי להספקת שירותים וציוד לרשויות מדינתיות שונות. נוסף על כך נשמעו קולות בדבר הרחבת המערכת לתעשיות נוספות. כנגד זה נשמעות אמירות של מומחים כי מערכת זו עתידה להיכשל, וכי היא אף כוללת סיכונים לחירויות הפרט.[140]

לפיכך המודל האמריקאי רחוק מלהיות מודל מתערב כמודל הישראלי.[141] ארצות־הברית אומנם פעילה מאוד ביצירת ועדות ומועצות שונות אשר אחראיות להערכת סיכונים, לתיאום מידע ולהגברת שיתופי־הפעולה, אך המודל שאותו אימצה נסמך ברובו על השתתפות וולונטרית עם התערבות אסדרתית נקודתית ומצומצמת בשני מגזרים בלבד.

---

137 Shackelford et al., לעיל ה״ש 79, בעמ׳ 322; Kerfoot, לעיל ה״ש 29, בעמ׳ 25.

138 Rosenzweig, לעיל ה״ש 2, בעמ׳ 96–100.

139 ראו U.S. Department of Homeland Security, Privacy Impact Assessment for EINSTEIN 3 – Accelerated (E^3A) (Apr. 19, 2013), http://www.dhs.gov/sites/default/files/publications/PIA%20NPPD%20E3A%2020130419%20FINAL%20signed.pdf.

140 Bellovin et al., לעיל ה״ש 28, בעמ׳ 27. לביקורת עדכנית על תפעול מערך זה על־ידי ה־DHS ראו Eduard Kovacs, *DHS's Einstein Security System Has Limited Capabilities: Audit*, Security Week (Feb. 1st, 2016), http://www.securityweek.com/dhss-einstein-security-system-has-limited-capabilities-audit.

141 יצוין גם שבשוק התקשורת הממשל מעודד רמת הגנה מסוימת אך אינו מחייב אותה. ראו *Cyber Security and Network Reliability*, FCC (Aug. 20, 2015), https://www.fcc.gov/encyclopedia/cyber-security-and-network-reliability: "The solution to this problem is not a top-down government response".

עוד יצוין כי נראה שהמודל **הקנדי** דומה בתפיסתו מאוד לזה האמריקאי, בהטילו את האחריות על הגופים הפרטיים אך תוך מימון של פעילות בתחום[142] ופיתוח יוזמות של שיתוף־פעולה בין גופים פרטיים לציבוריים.[143] עם זאת, גם שם נשקלת האפשרות להרחיב את ההסדרה לצעדים מחייבים יותר.[144]

2. המודל האירופי

נביא עתה סקירה של המגמות המרכזיות בהתמודדות האירופית עם אתגר ההסדרה והאסדרה של הגנת הסייבר על תשתיות חיוניות. נראה כי ההכרה הראשונית בצורך להגן על תשתיות חיוניות החלה לקרום עור וגידים ביוני 2004, בעקבות סדרת פיגועי הטרור שאירעו ברכבות נוסעים במדריד. מועצת האיחוד האירופי ביקשה מנציבות האיחוד להכין אסטרטגיה להגנה על התשתיות החיוניות של מדינות האיחוד. בעקבות זאת פרסמה הנציבות הצעה (communication) ל־Critical Infrastructure Protection in the Fight Against Terrorism.[145] הנציבות המשיכה בקו זה בשנת 2005, ופרסמה מסמך דיון (Green Paper) בנוגע להגנה על תשתיות חיוניות, אך טרם בחרה בחקיקה.[146] בעניין זה אף הוקם בשנת 2004 גוף אירופי ייעודי – European Network and Information Security Agency (ENISA)[147] – אשר מספק ייעוץ למדינות החברות בדבר דרכי אבטחה כמו־גם בנוגע להפעלת מנגנוני CERT.[148]

בשנת 2006 הציגה הנציבות הצעה לדירקטיבה הנוגעת ישירות בהגנה על תשתיות חיוניות כלל־אירופיות, ובד בבד אימצה את תוכנית ה־EPCIP (European Programme for Critical

---

142 *Federal Government to Fund Protection of vital Cyber Systems*, WORTZMANS (Apr. 22, 2015), http://www.wortzmans.com/blog/federal-government-to-fund-protection-of-vital-cyber-systems; *Budget Plan – Chapter 4.3: Protecting Canadians* (Apr. 21, 2015), http://www.budget.gc.ca/2015/docs/plan/ch4-3-eng.html.

143 ראו Scott J. Shackelford & Zachery Bohm, *Securing North American Critical Infrastructure: A Comparative Case Study in Cybersecurity Regulation*, 40 CAN.-U.S. L.J. 61, 66–69 (2016).

144 *2015 Budget Outlines 'Cyber Security' Legislation*, THESTAR.COM (Apr. 21, 2015), http://www.thestar.com/news/canada/2015/04/21/2015-budget-outlines-cyber-security-legislation.html.

145 Commission (EC), Critical Infrastructure Protection in the Fight Against Terrorism (Communication) COM (2004) 702 final, 20 October 2005. ראו גם: Åsa Fritzon et al., *Protecting Europe's Critical Infrastructures: Problems and Prospects*, 15 J. CONTINGENCIES & CRISIS MGMT. 30, 32 (2007).

146 Commission (EC), European Programme for Critical Infrastructure Protection (Green Paper) COM (2005) 576 final, 17 November 2005.

147 הוקם על־פי Council Regulation (EC) 460/2004 of 10 March 2004 Establishing the European Network and Information Security Agency [2004] OJ L77.

148 ראו https://www.enisa.europa.eu/topics/national-csirt-network. לדיווח ולדיון בדבר הרחבת תפקידה של ENISA בהקשר זה ראו Dan Raywood, *ENISA Receives Strengthening Vote to Appoint Executive Board and Create CERT*, SC MAGAZINE UK (Apr. 18, 2013), https://www.scmagazineuk.com/enisa-receives-strengthening-vote-to-appoint-executive-board-and-create-cert/article/545122/.

Infrastructure Protection) להגנה על תשתיות חיוניות של האיחוד כולו.[149] הדירקטיבה אומצה בשנת 2008,[150] וחייבה את המדינות החברות באיחוד ליישם את תוכנית ה־EPCIP ולקובעה כחקיקה. הצעדים האמורים מהווים אומנם התקדמות משמעותית בהגנה על תשתיות חיוניות באיחוד האירופי, אך תחולת הדירקטיבה מוגבלת. ראשית, היא מתייחסת להגנה על מגזרי האנרגייה והתחבורה בלבד. שנית, מכוח העובדה שהדירקטיבה חלה רק על תשתיות המוגדרות ״אירופיות״, היא מתייחסת רק לתשתיות המשרתות שתי מדינות באיחוד לפחות. זאת ועוד, במסמכים מאוחרים יותר נמתחה ביקורת על כך שהדירקטיבה לא הטילה על גופים פרטיים חובה ברורה לדווח על תקיפות, ולא יצרה מנגנון להעברת מידע בין המדינות החברות.

בהמשך לדירקטיבה, ב־30 במרץ 2009, אימצה הנציבות האירופית מדיניות לשמירה על תשתיות מידע חיוניות.[151] במרץ 2011 המשיכה הנציבות בפעילות האסדרה, וקראה להמשך המאמצים לבניית גישה קוהרנטית ושיתופית בין מדינות האיחוד בנושא הגנת הסייבר.[152] בהמשך להמלצותיה של הנציבות, פרסם הפרלמנט האירופי, ביוני 2012, החלטה בנושא מערכות המידע החיוניות.[153] ההחלטה מציעה, בין היתר, לחזק את שיתוף־הפעולה הציבורי־פרטי ברמת האיחוד האירופי.

שינוי משמעותי לעניין זה מצוי בפתח. בשנת 2016 קיבל האיחוד דירקטיבה חדשה[154] המחייבת את החברות באיחוד להקים, בתוך שנתיים, רשות לאומית שתעסוק בהגנה על הרשת ועל מידע (סעיף 8), ביצירת צוות מחשוב לתגובה במצבי חירום (CERT, או בלשון הדירקטיבה — CSIRT) (סעיף 9) ובאימוץ אסטרטגיה לאומית ותוכניות עבודה לשמירה על מידע (סעיף 7). עוד נקבע בדירקטיבה כי הרשויות השונות באיחוד יקיימו שיתופי־פעולה ביניהן וכן עם גופים חיצוניים (סעיפים 11—13).

נוסף על כך, ולענייננו, המדינות נדרשות לנקוט פעולות כדי להבטיח רמת הגנה נאותה על מערכות המידע של מפעילי תשתיות חיוניות (לפי ההגדרה הייחודית של דירקטיבה זו). כדי להגשים זאת, על מפעילי תשתיות אלה להעריך את הסיכונים שהם ניצבים בפניהם, ולאמץ

---

149 Commission (EC), European Programme for Critical Infrastructure Protection (Communication) COM (2006) 786 final, 7 June 2007.

150 Council Directive (EC) 2008/114 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection [2008] OJ L345/75.

151 Commission (EC), Protecting Europe from Large Scale Cyber-Attacks and Disruptions: Enhancing Preparedness, Security and Resilience (Communication) COM (2009) 149 final, 30 March 2009.

152 Commission (EC), Achievements and Next Steps: Towards Global Cyber-Security (Communication) COM (2011) 163 final, 31 March 2011.

153 European Parliament resolution on critical information infrastructure protection – achievements and next steps: towards global cyber-security (2012), *available at* http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2012-0237&language=EN&ring=A7-2012-0167.

154 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (להלן: דירקטיבת ה־NIS).

אמצעים מידתיים להבטחת שמירה על המערכות ועל המידע (בכפוף לסנקציות אם לא יעשו כן). על־פי סעיף 15 לדירקטיבה, המדינה צריכה לדרוש ממפעילים אלה מידע לגבי מדיניות האבטחה שלהם, תוצאות בדיקות אבטחה שערכו וחומרים נוספים אשר יאפשרו לה להעריך את רמת האבטחה באותן תשתיות. הדירקטיבה מורה גם שאם המדינה מזהה כשלים ובעיות, עליה לפרסם הנחיות מחייבות לתיקון כשלים אלה על־ידי המפעילים. מפעילי התשתיות החיוניות יהיו גם אחראים לדווח לרשויות המתאימות על תקריות שיש להן השפעה משמעותית על שירותים בסיסיים שהם מספקים (סעיף 14). הדירקטיבה יצרה משטר מקל יותר בעבור גופים המוגדרים ״ספקי שירות דיגיטלי״, הכוללים מנועי חיפוש, שירותי מחשוב ענן ושווקים וירטואליים (סעיפים 16–18).

בכל הנוגע בשירותי התקשורת החיל האיחוד זה כבר צעדים אגרסיביים הרבה יותר. בתיקון משנת 2009 לדירקטיבה האירופית הנוגעת בתקשורת (אשר יישומה ברמה המדינתית נדרש עד 2011) נקבע כי המדינות החברות נדרשות להתאים את חקיקתן כדי לאפשר פיקוח מקיף על חברות התקשורת בעניין אבטחת המידע.[155] הפיקוח כולל בדיקות שהחברות נקטו אמצעי הגנה ראויים וכן מילאו את חובתן לדווח על פגיעות אבטחה לרשות המוסמכת. הדירקטיבה אף מדגישה כי חשוב שלרשויות המדינתיות יוענקו סמכויות אשר יאפשרו איסוף מידע ועריכת ביקורות בדבר רמת האבטחה.

מעבר להסדרה במסגרת האיחוד האירופי, מדינות שונות באיחוד התייחסו לסוגיית ההגנה על תשתיות קריטיות מפני מתקפות סייבר באופן פרטני. השונות בין המדינות בהיבט זה רחבה, אך ברבות מהן יש לכל־הפחות בקרה שנעשית על־ידי הגוף המדינתי בלוויית המלצות.[156] צ׳כיה, כדוגמה מעברה האחד של הקשת, חוקקה בשנת 2014 חוק בנושא של הגנת סייבר, אשר מציג לפרטי־פרטים את הדרישות מן התשתיות הקריטיות בכל הקשור לדיווח ולביקורת,[157] וכן את סמכויותיו של הגוף המדינתי שהוקם על־מנת להתערב בפעולותיהן.[158] מן העבר האחר, בבריטניה (ככל שזאת שייכת לאיחוד האירופי) מוצעת הסדרה וולונטרית באמצעות רשות ממשלתית ייחודית – ה־NCSC.[159] מדינות אחרות נוקטות עמדת־ביניים. לדוגמה, בגרמניה הוקם ה־KRITIS, אשר מטרתו המוצהרת היא עידוד שיתוף־פעולה, תיאום והעברת

---

155 Council Directive 2009/140/EC of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services [2009] OJ L 337/37, arts. 13a–13b.

156 ראו פירוט בדוח Methodologies for the identification of Critical Information Infrastructure Assets and Services 9–12 (ENISA, 2014). ראו גם Scott J. Shackelford & Amanda N. Craig, *Beyond the New "Digital Divide": Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity*, 50 Stan. J. Int'l L. 119, 175–176 fig. 4 (2014) (טבלה המראה כי כמה מבין מדינות אירופה מפעילות מודלים מנדטוריים בחלק מהמקרים).

157 Act on Cyber Security, No. 181 § 4(3) (Czech).

158 שם, ס׳ 13.

159 ראו *About Us*, National Cyber Security Centre, https://www.ncsc.gov.uk/about-us.

מידע בין המגזר הפרטי למגזר הציבורי. אולם ממשלת גרמניה הבהירה כי אם לא תושג בדרכים אלה רמת הגנה מתאימה, תשקול גרמניה שינוי של החוקים ומעבר לכללים אגרסיביים יותר.[160] אכן, גרמניה בחרה לאחרונה במודל מתערב יותר, ומעתה היא מחייבת מפעילי תשתיות חיוניות להטמיע מערכות אבטחת סייבר העומדות בסטנדרט המקובל בתעשייה, וכן לדווח על תקלות במערכות. אי־עמידה בתנאי החוק עלולה לגרור קנסות של עד 100,000 אירו.[161]

לסיכום, נכון לעת הזו האיחוד האירופי נוקט אף הוא גישה מתערבת פחות מהגישה הישראלית. אומנם, הוא יוצר מסגרות לשיתוף מחויב של ידע בין המדינות החברות; הוא פועל ליצירת מסגרות מחייבות של העברת מידע בזמן־אמת, ייעוץ, הכְוונה ואף ביקורת ובקרה; ואנו רואים גישה קפדנית יותר המוחלת על חברות התקשורת. אולם גישה זו אינה חודרת עדיין לנבכי החברות הפרטיות כמו המודל הישראלי. עם זאת, ייתכן שבעתיד יעבור האיחוד האירופי למדיניות אגרסיבית יותר, שכן אפשרויות בכיוון זה כבר מונחות כיום על שולחן הדיונים.

ד. מודלים להגנה על תשתיות מפני איומי סייבר: אסדרת שוק, הסדרה מוגבלת, תמריצים והסדרה לאחר מעשה

1. מודל השוק וכשליו

בטרם נפנה לבחון מודלים שונים של הסדרה ואסדרה בסוגיה שלפנינו, יש לשאול תחילה אם ניתן להסתפק באסדרה מינימלית (או אולי אפילו להסתדר ללא אסדרה של נושא זה כלל) מתוך הנחה שכוחות השוק יוכלו להוביל לבדם לתוצאה סופית מקובלת וראויה. במילים אחרות, יש לבחון אם חברות פרטיות המפעילות את התשתיות החיוניות יתומרצו לאמץ סף התנהלות סביר בהקשר של הגנת סייבר רק מכוח התחרות וכוחות שוקיים וחברתיים אחרים הפועלים עליהן, וזאת מתוך מטרה להשיא את רווחיהן או להימנע ממשבר תקשורתי במצב של כשל מערכות שייגרם ממתקפת סייבר. המחשבה היא שהחברה אולי תפעל ביוזמתה שלה להגן על המותג,

---

160 CIP Strategy, לעיל ה״ש 21, בעמ׳ 14–17. ראו גם Federal Ministry of Interior, Cyber Security Strategy for Germany 5 (2011), *available at* https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile. לפעולה ראשונית בכיוון זה, בדמות יישום קנסות, ראו Jimmy Nicholls, *German Critical Infrastructure faces €100,000 in fines*, Computer Business Review (Jul. 16, 2015), http://www.cbronline.com/news/cybersecurity/physical/german-critical-infrastructure-faces-100000-in-fines-4623867.

161 ראו מסמך של ממשלת גרמניה בעניין: http://dip21.bundestag.de/dip21/btd/18/040/1804096.pdf. ראו גם *Germany Passes Strict Cyber-Security Law to Protect 'Critical Infrastructure'*, RT (Jul. 11, 2015), http://www.rt.com/news/273058-german-cyber-security-law/. כמו־כן נראה כי הסטנדרט המוחל על מפעילי תקשורת בגרמניה גבוה אף יותר, ואמור להעניק את ההגנה הטובה ביותר האפשרית. ראו הסברים בסקירה זו: Jones Day, *Germany Rushes to Adopt a New IT Security Act*, Lexology (Jul. 21, 2015), http://www.lexology.com/library/detail.aspx?g=d1ae36f6-f4ae-45d4-8470-32e0afce588d.

על לקוחותיה (מחשש שהם יעברו לחברה אחרת או יקטינו את צריכתם) כמו־גם על מתקני החברה עצמם מפני תוצאותיה המזיקות של תקיפה אפשרית כזו.[162]

יש לציין כי לצמצום האסדרה בתחום זה יש יתרונות רבים.[163] כך, הישענות על כוחות השוק מאפשרת חיסכון של ההוצאות הכרוכות באסדרה מדינתית ובפתרון בעיות של תיאום והעברת מידע בין רשויות מדינה שונות, כמו־גם פטור מהעלויות החברתיות והכלכליות של חיכוך אסדרתי בין מְאַסדרים לבין גופים מוסדרים. צמצום האסדרה עשוי גם לצמצם את הטעויות השיטתיות הכרוכות באסדרה אגרסיבית, ואף להקטין את החשש לפגיעה בזכויות־יסוד (כגון זכויות קניין של חברות וזכויות אדם של הציבור אשר יושפע מכך) כתוצאה מהתערבות־יתר מצד המדינה.

אך ההנחה המקובלת היא כי חברות פרטיות **אינן** משקיעות משאבים מספקים בהגנת הסייבר.[164] נבדוק בקצרה את הסיבות לכך. ראשית, לעיתים מפעילי התשתיות מהווים מונופול או מתנהלים בשוק אוליגופוליסטי. נוסף על כך, במקרים רבים מושתות עלויות גבוהות על צרכנים הבוחרים לעבור בין חברות שונות[165] או שקיימים חסמי מעבר אחרים. במצבים מעין אלה ניתן להתייחס לשחקנים בשוק זה כאל בעלי כוח שוק. כאשר עסקינן בחברות המספקות תשתיות חיוניות, מדובר בהספקת מוצר שביקושו קשיח במידה רבה, ועל־כן הפגיעה הכלכלית שתיגרם לפירמה מתקיפת סייבר שתתרחש אולי עקב הגנה בלתי־מספקת אינה צפויה להיות משמעותית. בשל העדר התחרות, הפגיעה בלקוחות לא תיתרגם לנטישתם, ואולי אף לא להקטנת פעילותם. לפיכך היקף ההכנסות מהלקוחות אינו צפוי להיפגע. נוסף על כך, המונופול אף לא יוטרד במיוחד מהנזקים לתשתית שייגרמו מהתקפות הסייבר, שכן הוא יוכל להיפרע בגינם מהלקוחות באמצעות ייקור התעריפים או אף לקבל פיצוי מהמדינה עקב נזקי ״מלחמה״ (ככל שמתקפת הסייבר תוגדר ככזו). ייתכן שבעל התשתית הקריטית יוכל להיפרע מלקוחותיו גם במצב של תעריפים מפוקחים, שכן אלה מבוססים במקרים רבים על עלויות התפעול, אשר יתייקרו עקב התקיפה והתגובה עליה. נוסף על כך, ייתכן שהגוף המעניק שירותים חיוניים סבור

---

162 לטענות ברוח זו מפי נציגי התעשייה ראו Kerfoot, לעיל ה״ש 29, בעמ׳ 6; Rosenzweig, לעיל ה״ש 2, בעמ׳ 100–101.

163 נראה שזו אכן הפילוסופיה המנחה את המְאַסדרים בארצות־הברית, לפחות לפי עדותם שלהם בעניין. ראו Clarke & Knake, לעיל ה״ש 35, בעמ׳ 121 (שם הם מסבירים כי תופעל הסדרה רק אחרי שצעדים וולונטריים ייכשלו).

164 ראו, למשל, מחקרים שנערכו בשנים 2009 ו־2011 על־ידי חברת McAfee, אשר חשפו כי חברות רבות משקיעות משאבים מעטים בלבד בהגנת סייבר, בעיקר, לטענתן, עקב עלויות גבוהות. על־אף האינטרס הכלכלי הברור של עורכת המחקר, המחקרים מצביעים על מגמה מסוימת. ראו McAfee & Ctr. for Strategic & Int'l Studies, In the Dark: Crucial Industries Confront Cyberattacks 1 (2011), *available at* http://www.mcafee.com/in/resources/reports/rp-critical-infrastructure-protection.pdf; McAfee, In the Crossfire: Critical Infrastructure in the Age of Cyber War 14 (2009), https://www.dsci.in/sites/default/files/NA_CIP_RPT_REG_2840.pdf; Nathan Alexander Sales, *Regulating Cyber-Security*, 107 Nw. U. L. Rev. 1503, 1507, 1511 (2013). ראו גם Kerfoot, לעיל ה״ש 29, בעמ׳ 4. נראה שזו גם הנחת־היסוד של חוקרים ישראלים בתחום זה. ראו Tabansky & Ben Israel, לעיל ה״ש 8, בעמ׳ 37.

165 McAfee, לעיל ה״ש 164, בעמ׳ 6.

כי גם אם יספוג פגיעות ונזקים כבדים אשר ישתקו אותו, תיחלץ המדינה לעזרתו ותסייע לו מבחינה כלכלית ותפעולית (דוגמת אותם גופים פיננסיים אשר סברו, במידה מסוימת של צדק, כי הם גדולים מכדי ליפול), ועל־כן הוא לא ישקיע מספיק בהגנתו.[166] אומנם, כל מונופול יודע כי אין הוא חסין לחלוטין מפני השלכותיהן של התקפות סייבר, וכי התנהלות שערורייתית מצידו תוביל ללחץ ציבורי ולפעילות של מחוקקים ומְאַסדרים אשר סופה להסב לו הפסדים.[167] על־כן גם מונופול מתומרץ לשמר רמת הגנה מסוימת.[168] אך בסופו של יום נראה כי התמריץ של חברות מעין אלה להשקיע בהגנת סייבר אינו מספק.[169]

אולם לא כל מפעילי התשתיות החיוניות פועלים בשוק מונופוליסטי או אוליגופוליסטי. קיימים מצבים שבהם יש תחרות בין ספקים שונים של תשתית קריטית. זה המצב בשוק הסלולר בישראל, אשר כולל חמישה שחקנים מרכזיים, מהם שלושה בעלי תשתית בפרישׂה ארצית מלאה.[170] אך נראה כי יש מקום לבחון הסדרה של הגנת הסייבר גם במצבים (הנדירים יחסית, יש לומר) שבהם יש תחרות בין מפעילי התשתית הקריטית או קיימים תמריצי שוק אחרים להבטחת רמת אבטחה סבירה. זאת, משלוש סיבות אשר יובילו את החברות האמורות להשקעה בלתי־מספקת בהגנת תשתית הסייבר שלהן: קיומן של **החצנות משמעותיות**, **מחסור במידע ומחסור בידע**. חלק מהסיבות האמורות הינן ייחודיות להקשר של הסייבר, ועל־כן ראוי לתת להן את הדעת. הדיון בטענות אלה יפה גם למצבים של מונופול, שכן סיבות אלה רק מעמיקות את החשש שבהקשרים מעין אלה הסדרה עצמית על־ידי המונופול בנושא זה עתידה לנחול כישלון חרוץ. את יתרת חלק זה נקדיש אם כן לדיון בשלוש הסיבות האמורות.

במקרים רבים הפגיעה שנגרמת כתוצאה מהתקפת סייבר בהעדר הגנה ראויה יוצרת **החצנות שליליות**. במצב האמור ייווצרו נזקים שהחברה תגרום אך לא תפנים מכוח מנגנוני שוק שונים, גם במצב של תחרות; הנזק שייגרם לצרכנים ולאחרים מתקיפת סייבר מוצלחת יעלה במידה ניכרת על הנזק שנטישת צרכנים, הקטנת פעילות או עריכת תיקונים בדיעבד עלולים להסב לפירמה הנדונה. אכן, הפגיעה בתשתיות גורמת נזקים מרוחקים רבים במגזרים אחרים אשר מושפעים מהשבתת הפעילות. לדוגמה, הפסקת פעילות במערכת חשמל או תקשורת משליכה על תחומי חיים רבים אחרים. יתר על כן, לעיתים מחדלי אבטחת סייבר של חברה מסוימת

166 Andrew Ross Sorkin, Too Big to Fail: The Inside Story of How Wall Street and Washington Fought to Save the Financial System – and Themselves (2010).

167 לדיון בדבר הכוחות החברתיים והפוליטיים שהמונופול כפוף להם ראו Albert O. Hirschman, Exit, Voice, and Loyalty: Responses to Decline in Firms, Organizations, and States (1970).

168 יצוין כי עקב אדישותו של המונופול לעלויות ייתכן שבמצבים מסוימים הוא לא ייֵרתע כלל מהשקעת־יתר בהגנת הסייבר, שכן הוא יוכל להיפרע בגין עלויות אלה מלקוחותיו. אולם נשאיר את הדיון בנקודה מורכבת זו לפעם אחרת.

169 Sales, לעיל ה״ש 164, בעמ׳ 1517: ("strategically significant firms in uncompetitive markets are less likely to adequately invest in cyber-security than ordinary firms in competitive markets").

170 משרד התקשורת "מדיניות שיתוף ברשת גישה רחבת פס של בעל רישיון כללי למתן שירותי רט״ן" (15.5.2014) www.moc.gov.il/sip_storage/FILES/1/3551.pdf.

(למשל, חברת תקשורת) לא יגרמו כל נזק לתשתית שלה עצמה, אך יגרמו נזק משמעותי לתשתית אחרת, אשר לא יופנם כלל על־ידי החברה האחראית למחדלים.[171]

כאשר ספקית התשתית הקריטית מפנימה רק חלק מהנזקים הנגרמים ממחדליה, היא מתומרצת בחסר למנוע אותם. הדבר מסביר היטב מדוע חברות התשתיות נחשבות כמקנות הגנה בלתי־מספקת; לנוכח תוחלת ההפסד הנמוכה יחסית הצפויה להן, אין להן תמריץ מספק להשקיע את המשאבים הדרושים על־מנת להבטיח הגנת סייבר ראויה על תשתיתן. לפיכך, כדי לרפא כשל שוק זה, יש לנקוט אמצעים שיביאו לידי הפנמה מתאימה של נזקי פגיעת הסייבר.

סיבה נוספת שעלולה לגרום לליקויים בהגנת הסייבר היא **מחסור במידע**. לטענה זו יש שני צדדים – חוסר מידע **של צרכנים** (שגם לו יש שני פנים לכל־הפחות) וחוסר מידע **של הפירמות** – ויש בה מאפיינים כלליים כמו־גם כאלה שייחודיים לדיון נקודתי זה. טענת חוסר המידע של **הצרכנים** ברורה וצפויה. באופן תיאורטי, צרכנים צפויים לאותת לפירמה (או למְאַסדר) את דבר אי־שביעות־רצונם ממדיניות הגנת הסייבר של הפירמה, ובכך לתמרץ את הפירמה לנקוט צעדים משמעותיים וראויים. אולם הצרכנים אינם ערוכים לעשות כן, היות שאין בידיהם מידע מתאים. הכשל בנקודה זו נוגע בשני הֶקשרים וחסכי מידע נפרדים – מידע בדבר רמת ההגנה הננקטת ומידע בדבר אופי הפגיעות הנגרמות. לפירמות יש כמובן תמריץ מובהק לא למסור לצרכנים מידע מלא בדבר הפריטים האמורים, שכן מידע בדבר תקיפות שהתרחשו בעבר או בדבר חולשות בהווה עלול להוביל לפגיעה במותג ובעובדים, כמו־גם לאחריות אפשרית בנזיקין או מכוח דינים אחרים.[172] נוסף על כך, נראה שאין די בהעברת מידע כאמור, שכן צרכנים רבים אינם מסוגלים להבין אותו. לפיכך, כדי לאפשר לכוחות השוק לתמרץ הבטחת הגנה ראויה בהקשר זה, יש לספק לציבור כלים להבנת המידע.

טענת חוסר המידע של **הפירמה** בדבר תקיפות סייבר מורכבת יותר. מקובל לסבור כי הפירמות מצויות בעמדת יתרון על כל גורם אחר בגישתן לידע הנוגע בתחום פעילותן ובנכסיהן (במיוחד אל מול צרכנים, אך גם אל מול מְאַסדרים).[173] על־כן, לכאורה, דווקא הפירמות מצויות במצב המיטבי בכל הקשור להיערכות לסיכוני סייבר. אך להתקפות סייבר יש כמה מאפיינים מיוחדים – צורתן משתנה ללא הרף, ויש צורך במידע מודיעיני על־מנת לחזותן. כמו־כן, התקפה שהתרחשה בהקשר אחד עשויה להיות מועתקת גם להקשר אחר. לפיכך המידע הרלוונטי ביותר בנוגע לאופייה ולעיתויה של התקפת סייבר קרובה עשוי להיות מבוזר בין פירמות או להימצא אצל גופים אחרים העוסקים בעניין. פירמה הפועלת לבדה תיכשל במתן הגנה מספקת, שכן אין בידה מידע ברמה המיטבית.[174] כמו־כן יש חשיבות לתזמון קבלת המידע, לעיתים בזמן־אמת. מאפיינים אלה מצדיקים הקמה של מנגנוני CERT.[175]

171 Kerfoot, לעיל ה״ש 29, בעמ׳ 7; Rosenzweig, לעיל ה״ש 2, בעמ׳ 162–163.

172 שם, בעמ׳ 161.

173 George Loewenstein, Cass R. Sunstein & Russell Golman, *Disclosure: Psychology Changes Everything*, 6 Ann. Rev. Econ. 391 (2014).

174 לסקירת טענה זו, וכן לטענה נגדית, שלפיה חוסר זה במידע אינו משמעותי, וגם אם הוא קיים, הוא אינו ניתן לריפוי בקלות על־ידי העברת מידע, ראו Derek E. Bambauer, *Sharing Shortcomings*, 47 Loy. U. Chi. L.J. 465, 468–472 (2015) (להלן: Bambauer, *Sharing*).

175 לעניין זה ראו סקירה להלן בה״ש 188 ובטקסט שלידה.

אולם ראוי להמשיך ולהקשות מדוע לא יצליחו פירמות לאתר את הכשל האמור לבדן ולפעול באופן וולונטרי כדי לרפאו. הרי הן יוכלו, לדוגמה, להעביר מידע רלוונטי בנושאים האמורים ביניהן (גם בזמן־אמת, תוך הסתמכות על מנגנון CERT מסחרי), ובכך להתמודד עם סיכוני הסייבר. התשובה לתהייה זו היא שהעברת המידע בין הפירמות צפויה להימנע או לפחות להתעכב משתי סיבות: אינטרסים כלכליים וכללים משפטיים. פירמה עשויה למנוע העברת מידע הנחוץ לאחרות לשם הגנתן מכיוון שהיא תרצה להימנע מלסייע למתחרות (גם אם מבחינה כלכלית יעיל שהיא תעביר את המידע, שכן תמורתו היא תקבל התראות עתידיות, הפירמה עשויה לטעות ולא לנקוט פעולה זו) או משום שהדבר עלול לחשוף יתרונות או סודות מסחריים שלה.[176] במצבים אחרים פירמה עשויה להסס למסור את המידע בשל הגבלות בנוגע להעברת מידע בין פירמות מתחרות מכוח חוקי ההגבלים העסקיים.[177] כמו־כן, כאשר המידע נוגע בנתוני תקשורת או קשור לצריכה, חברות עשויות לחשוש מהיחשפות לתביעות בגין הפגיעה בפרטיותם של הלקוחות שעלולה להיגרם אם המידע יועבר.[178] לנוכח האמור ייתכן שיש צורך בהתערבות אסדרתית, ולו כדי לעודד או לאפשר את העברת המידע האמור בין הגופים הרלוונטיים ללא החששות המסחריים או המשפטיים האמורים.

נוסף על כך ניתן לטעון כי הפירמות לא יצליחו להתוות מדיניות סייבר מתאימה עקב **מחסור בידע**. כאן, להבדיל מהטיעון הקודם, אין מדובר בכשל נקודתי של מחסור במידע, אלא בחוסר במומחיות הנדרשת כדי לאסוף מידע הנוגע בתקיפות, להעריך את הסיכון לתקיפה בצורה נכונה או לנקוט את ההגנות הנדרשות. ניתן לסבור כי בהקשר זה היתרון מצוי בידי המדינה או שהידע מבוזר בין גופים רבים ושונים אשר רק המדינה מסוגלת לרכזם לאכסניה אחת.

לצורך המחשת נקודה זו, מציין החוקר פול רוזנצווייג כי כאשר גוגל הייתה נתונה בהתקפת סייבר, היא פנתה ל־NSA לצורך קבלת עזרה.[179] מדוגמה זו, שבה חברה פרטית מובילה בתחומה פנתה לגוף מדינתי (בעל מאפיינים בטחוניים מובהקים) לשם קבלת סיוע, למד רוזנצווייג כי תחום הגנת הסייבר עשוי ליצור אתגרים ייחודיים בהיבט של הידע אפילו לחברת טכנולוגיה מתקדמת ביותר כמו גוגל. ניתן להניח כי הדבר נכון שבעתיים לגבי חברות שאינן נמצאות בחוד החנית הטכנולוגית, כגון חברות לתשתיות. חברות אלה לוקות בחוסר ידע בדבר דרך המגננה הראויה מפני התקפות סייבר ובדבר אופי התקיפה העתידית. הן אף אינן יודעות על התקפות אחרות שמתרחשות ואשר קיומן עשוי להוות אינדיקציה לסיכון מוגבר שהתקפה דומה

176 לעיתים אף פירמות ומנהליהן פועלים באופן לא־רציונלי או עם רציונליות חסומה. ראו Avishalom Tor, *Understanding Behavioral Antitrust*, 92 TEX. L. REV. 573, 632–634 (2014). לכשלים בהתנהלותן של חברות בהקשר של סייבר ראו KERFOOT, לעיל ה״ש 29, בעמ׳ 11.

177 שם, בעמ׳ 35.

178 ROSENZWEIG, לעיל ה״ש 2, בעמ׳ 168, מטיל ספק בדבר קיומה של בעיה אמיתית בהקשר זה. ראו גם Bambauer, *Sharing*, לעיל ה״ש 174, בעמ׳ 470—472. בהקשר הישראלי אפשר לסבור כי העברת המידע עשויה להיות הפרה של ס׳ 8(ב) או ס׳ 2(8) או 2(9) לחוק הגנת הפרטיות, אם המידע האמור נמסר על־ידי הלקוח למטרה מסוימת וללא כוונה שהוא יועבר הלאה.

179 ROSENZWEIG, לעיל ה״ש 2, בעמ׳ 158.

תתרחש גם אצלן. לפיכך נדרש פתרון אסדרתי שיסייע להן – פתרון שתכליתו היא העברת ידע שהצטבר בידי המדינה.

עד כאן שטחנו כמה טיעונים בדבר כשלי שוק ובעיות אחרות שעלולות למנוע את בעלי התשתיות עצמם מלהבטיח רמת הגנה נאותה. נציין עוד כי הטיעונים האחרונים, המתייחסים למחסור בידע ובמידע, נוגעים במאפיינים שייחודיים לתחום הסייבר. כדי להתמודד עם אתגרים אלה ניתן לנקוט כמה סוגי פעולות. המשך פרק זה יוקדש לפתרונות מינימליסטיים, שמבקשים להסתמך על כוחות השוק ותמריצי הפירמות במקביל לריפוי הכשלים שצוינו באופן נקודתי.

2. התערבות מינימליסטית – חובות גילוי והזרמת מידע

(א) תיקון כשלי מידע – חובות גילוי לצרכנים ולציבור

כאמור, אחד הכשלים המונעים הסדרה מיטבית של הגנת סייבר על־ידי הפירמות עצמן וכוחות השוק הוא מחסור במידע רלוונטי בידי הלקוחות בנוגע לשני ממדים: מידת ההגנה הננקטת על־ידי הפירמות; ואופי הפגיעות עצמן, אם וכאשר הן מתרחשות. נתחיל במידע הנוגע בפגיעות הסייבר לאחר מעשה. סוגיה זו כבר נדונה למעשה במשפט, אם כי בהקשר שונה מעט – אבטחת מנגנונים של מידע אישי וחשיפת מידע הנוגע בפרטים.[180] בהקשרים אלה נקבעו כללים המחייבים מסירת מידע בנוגע לכשלים באבטחת המידע האישי לאלה שהדבר עלול להשפיע עליהם.[181] ייתכן שיש מקום להחיל כללים דומים גם בהקשרים שבהם המידע אינו אישי, ואף אין פגיעה במאגר מידע כלל, אלא התקיימה פריצה שפגעה בתשתיות הנוגעות בצרכנים. במילים אחרות, יש אולי מקום לחייב את התשתיות החיוניות להודיע ללקוחות על כל פגיעה בתשתית הסייבר שלהן שיש לה השלכות שליליות עליהם.

ראוי לציין כי על המודל של גילוי כשלי אבטחה הנוגעים במידע פרטי נמתחו ביקורות הרלוונטיות גם לענייננו.[182] התראות אלה עלולות להיות תכופות, ופעמים רבות שגויות, ועל־כן הצרכנים ומקבלי ההחלטות יחדלו לתת בהן אמון או אפילו להעניק להן תשומת־לב ראויה.[183] כמו־כן, צרכנים ימעיטו בחומרת הבעיה (בין היתר בהשפעת הטיית האופטימיות)[184] או שהחברות יעריכו את תגובת הצרכנים בחסר ועל־כן יזלזלו בה ולא ייערכו

---

180 ראו Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 Mich. L. Rev. 913, 932–935 (2007). כן ראו הסדר דומה באסדרה האירופית החדשה: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), arts. 33–34.

181 הראשונה שאימצה כללים אלה הייתה מדינת קליפורניה: Cal. Civ. Code §§ 1798.28, 1798.82, 1798.84 (West Supp. 2006).

182 לדיון דומה בתועלות המעטות של חובות גילוי ראו Kerfoot, לעיל ה״ש 29, בעמ׳ 18–19.

183 Schwartz & Janger, לעיל ה״ש 180, בעמ׳ 916; Fred H. Cate, *Another Notice Isn't Answer*, USA Today (Feb. 27, 2005), http://usatoday30.usatoday.com/news/opinion/2005-02-27-consumer-protection-oppose_x.htm.

184 Shmuel I. Becher & Tal Z. Zarsky, *E-Contract Doctrine 2.0: Standard Form Contracting in the Age of Online User Participation,* 14 Mich. Telecomm. & Tech. L. Rev. 303, 313

כראוי למניעתן של פגיעות הסייבר. מסיבות אלה ניתן להעריך כי את פער המידע בין הצרכנים לחברות התשתיות לא יהיה אפשר לצמצם באמצעות מנגנון גילוי זה לבדו.

מודל גילוי אחר עשוי לחייב את ספקי התשתיות הקריטיות לדווח לציבור על מנגנוני האבטחה שברשותם או על תוצאות בדיקות הכשירות שנערכו אצלם. כאשר הציבור ילמד על קיומה של רמת אבטחה נמוכה, יהיו לדבר השלכות כלכליות שליליות על הפירמה, אשר תבקש לפיכך למנוע את היווצרותן מראש. יצוין כי מודל זה טומן בחובו בעיות רבות אף יותר מאשר קודמו. ראשית, שוב יש חשש שהציבור לא ייַחס משקל ראוי לרמת האבטחה הירודה שהתגלתה,[185] מה־גם שמדובר בסיכון שלא התממש ועל־כן הטיית האופטימיות של הצרכנים עלולה שוב לפגוע בשיקול־דעתם.[186] שנית, קיימים שיקולי מדיניות כבדי־משקל נגד חשיפת כשלי אבטחה, שכן דיווחים כאמור שקולים לסימון מטרה על גבן של תשתיות קריטיות מועדות, והדבר עלול להוביל לניצול הכשלים על־ידי תוקפים.[187] לנוכח הסיכוי הקלוש שמגילויים אלה תצמח תועלת שתהא גבוהה מהנזק האפשרי, קשה להצדיקם.

(ב) תיקון חסכים במידע ובידע ומתן חסינות

נעבור עתה לדון בכשלים הנוגעים בפירמות עצמן וביכולתן לאסוף מידע וידע בנוגע להתקפות סייבר. כדי להתמודד עם אתגר זה, הציעו מְאַסדרים מנגנונים אשר ישפרו את זרימת המידע והידע. כאמור, ככל שהדבר נוגע **במידע**, אחד המודלים הבולטים הוא זה של ה־CERT. מודל זה נסמך בעיקרו על שיתוף במידע ושיתוף־פעולה בין ארגונים במדינה, והוא מיועד לטפל באירועי סייבר ובנקודות תורפה, לפעול באופן פרואקטיבי למניעת איומי סייבר, לפתח ידע בנוגע להתגוננות ולהפיצו לקהל־היעד, לספק הסברה בנוגע לאיומי סייבר ולהעלות את המודעות אליהם, ולפתח ולטפח קשרים עם גופים מקבילים בעולם.[188] לעיתים המנגנון מופעל על־ידי המדינה, אשר מרכזת את הדיווחים ומוסיפה גם את המידע המצוי בידיה, ולעיתים הדבר נעשה באמצעות גורם פרטי.

כאמור, עלולה להיות בעיה של תמרוץ־חסר להשתתפות פעילה בתרומת מידע למיזם (וייתכן אף חשש ל"רוכבים חופשיים" בחלק מהמקרים).[189] לפיכך נשקלים אמצעים משלימים, כגון מתן פטור מאחריות וחסינות – במקרה של העברת המידע הנוגע בתקיפות סייבר למדינה (אשר תעביר אותו בהמשך לגופים אחרים) – מפני תביעה בגין פגיעה בפרטיותם

(2008); Neil D. Weinstein, *Optimistic Biases About Personal Risks*, 246 SCIENCE 1232, 1233 (1989).

185 לטיעון דומה, שלפיו צרכנים רבים אינם בקיאים ברמות האבטחה השונות ולכן לא יֵדעו בהכרח להבדיל בין הרמות השונות שחברות שונות מציעות, ראו Bambauer, *Ghost*, לעיל ה"ש 35, בעמ' 1031.

186 ראו לעיל ליד ה"ש 184 להסבר בדבר מושג זה.

187 ROSENZWEIG, לעיל ה"ש 2, בעמ' 172.

188 ראו, למשל, באתר של "המרכז הלאומי להתמודדות עם איומי סייבר" (CERT-IL): https://cert.gov.il/About2/mission/Pages/mission.aspx. ראו גם התייחסות לעיל בה"ש 78, 107 ו־148 ובטקסט שלידן.

189 ראו דיון לעיל בה"ש 173–178 ובטקסט שלידן.

של צרכנים או בגין עוולות אחרות.[190] פתרון קיצוני יותר עשוי להיות חיוב בעלי התשתיות לדווח על מידע המגיע אליהם בזמן־אמת, כדי שיהיה אפשר להעבירו הלאה.

כזכור, קיים גורם נוסף שעלול למנוע הגנה אפקטיבית בסייבר, והוא המחסור **בידע** המאפיין מפעילי תשתיות קריטיות רבים. גם כשל זה עשוי להירפא באמצעות יצירת מנגנונים שיאפשרו ויעודדו העברת ידע בין גופים פרטיים שונים. דרך אחת היא דרישה מגוף תקינה אחד לרכז ידע באמצעות עריכת תקן רלוונטי.[191] דרך חלופית עשויה להיות יצירת מסגרות לעידוד שיתופי־פעולה בין חברות תשתיות לבין חברות העוסקות באבטחת סייבר, כמו־גם בין חברות התשתיות עצמן.[192] יצוין כי לאחרונה מסתמנת רוויה גם בתחום הסטנדרטים להגנה, וייתכן שיש מקום להתערבות של גורם מדינתי אשר יעודד שיתוף־פעולה ככל שיהיה בכך צורך ויאותת איזה מבין הסטנדרטים שפורסמו בעניין יש להעדיף.[193] אלה במידה רבה הפעולות שחלק מאותן החלטות מדיניות של הממשל הפדרלי בארצות־הברית שנדונו לעיל מקדמות.[194]

3. בעיית ההחצנות – הסדרה לאחר מעשה ומתן תמריצים

גם אם ייפתרו בעיות המחסור בידע ובמידע, עלולה להיוותר בעינה בעיית ההחצנות, אשר מובילה לתמרוץ־חֶסֶר להטמעת הגנת הסייבר. אף אם באמתחתה של פירמה מצוי הידע הנדרש, היא עלולה להירתע מההוצאות הניכרות שהגנת הסייבר מצריכה, אשר עשויות לעלות על התועלת הטמונה בהגנה זו מבחינת הפירמה. על־כן יש צורך במנגנונים שונים להפנמת החצנות אלה או במתן תמריצים אחרים כדי לצמצמן. המנגנונים האמורים להלן מוכרים, אך החלתם בהקשרים של סייבר מחייבת התאמות ומעוררת שאלות ייחודיות שיידונו כאן.

(א) החצנה, הפנמה והטלת אחריות לאחר מעשה

הדרך האינטואיטיבית ביותר להפנמת ההחצנות האמורות היא הטלת אחריות ותשלומים על הפירמות בגין יצירת סיכוני סייבר והתממשותם.[195] זאת, באמצעות הטלת אחריות נזיקית לאחר מעשה (ואולי אף יצירת מנגנון להגשת תובענות ייצוגיות בגין נזקים שנגרמו לנפגעים). דרכי פעולה נוספות הן קביעת קנסות מנהליים או הגדרת אחריות פלילית לחברות ולעומדים בראשן במקרה של אי־עמידה בסיפי התנהלות תקינה.

---

190 Rosenzweig, לעיל ה״ש 2, בעמ׳ 169; H.R. 1560 114th Cong., 1st Sess., § 106 (2015–2016). ייתכן שראוי, לשם צמצום האפשרות של פגיעה בפרטיות במקרה כזה, למנוע מהמדינה כליל את האפשרות לגשת למידע. ראו Kerfoot, לעיל ה״ש 29, בעמ׳ 34; Bambauer, *Sharing*, לעיל ה״ש 174, בעמ׳ 468–472. ראו גם את הצעדים שננקטו באירופה בדירקטיבת ה־NIS, לעיל ה״ש 154, ס׳ 20, המורים למדינות לפעול לעידוד דיווח של גופים על אירועים, כמו־גם ליצור תשתית לדיווח כאמור.

191 ראו לעיל ה״ש 103 והטקסט שלידה.

192 ראו לעיל את הדיון במודל האמריקאי בה״ש 96, 102 ו־107–114 ובטקסט שלידן.

193 Kerfoot, לעיל ה״ש 29, בעמ׳ 6.

194 בהתייחס לשימוש ב־NIPP ולהסתמכות על החלטה מס׳ 7 לעניין זה של ה־Homeland Security Presidential Directive. ראו שם, בעמ׳ 33.

195 שם, בעמ׳ 14; Rosenzweig, לעיל ה״ש 2, בעמ׳ 173.

ברמה האנליטית, ככלי להשגת התוצאה הנדרשת של הגנת סייבר ראויה, מודל אסדרתי זה נתקל בשני אתגרים מרכזיים: ראשית, הסדרת התנהגות מראש (קרי, אימוץ מנגנוני הגנה ראויים) באמצעות אחריות בדיעבד; שנית, קביעת סטנדרט התנהלות ראוי על־ידי גוף מדינתי (מחוקק, מְאַסדר או בית־משפט) והשוואתו לאחר מעשה להתנהלותן של הפירמות בפועל.

הסדרה באמצעות הטלת אחריות לאחר מעשה מבוססת על הרתעת הפירמה מביצוע פעולות שיובילו לתוצאות שליליות (״מודל הרתעה קלסי״).[196] אך שימוש בהרתעה גרידא בהקשר זה עלול להיות בעייתי.[197] מצד אחד, הסנקציה החריפה לאחר מעשה אינה מובילה בהכרח לשינוי התנהגות אצל הגורם האחראי. חשש זה מוכר גם בתחומים אחרים שבהם המדינה קובעת יעדי בטיחות,[198] במיוחד כאשר הן האחריות והן הנזק אינם ודאיים וקשים מאוד להערכה מראש ולהוכחה בדיעבד, וכך גם זיהוי האמצעים המתאימים למניעת הנזק. נוסף על כך, ובמיוחד בכל הנוגע בהטלת אחריות פלילית, קביעת כללים נוקשים מדי עלולה לגרום ליציאת שחקנים ראויים מהשוק,[199] ובכך להוביל לתוצאות לא־רצויות אחרות, כגון פגיעה בתחרות או באיכות השירות.

אתגר נוסף ביישום מודל אסדרתי זה בהקשר של סייבר כרוך בקביעת סטנדרט האחריות וביישומו.[200] כזכור, במודל זה, אם חברה לא תעמוד בסיפי התנהלות מוגדרים של הגנה על תשתיות חיוניות, היא תיחשף לתביעות, ומפעיליה עשויים לעמוד לדין אם הסיכונים יתממשו. גופים מדינתיים ייתקלו בקשיים רבים בטרם יוכלו למלא משימה זו בצורה טובה. המועמד ה״טבעי״ לקביעת סף אחריות לאחר מעשה כאמור (כבכל תביעת נזיקין) הוא בית־המשפט. אולם קשה לראות כיצד הוא יוכל להתמודד עם אתגר מורכב זה. לפניו עומדות שתי אפשרויות פעולה מרכזיות: הסתמכות על סטנדרט עמום אשר בית־המשפט ייצוק בו תוכן מפעם לפעם; או שימוש בכלל אשר ייקבע על־ידי צד שלישי – גוף תקינה ממשלתי או אחר – שעליו יסתמך בית־המשפט (ובכך יהפוך אותו לחובה לגבי הגופים הפועלים בתחום).[201]

שתי האפשרויות שצוינו אינן מיטביות. מחד גיסא, שימוש בסטנדרטים עמומים יכניס אי־ודאות לשוק הנדון – כלומר, הפירמות יתקשו להבין את הנדרש מהן על־פי פסיקת בית־המשפט – ודבר זה יגרור עלויות. מאידך גיסא, שימוש בכללים עלול לגרום לקיבעון ולפגיעה בחדשנות הנדרשת בהגנה על הסייבר. לנוכח זאת יש להטיל ספק ביכולתו של בית־המשפט לבצע הסדרה למפרע בצורה יעילה ונכונה. הסתמכות על קביעות של גורם חיצוני (לרבות גורם מדינתי) עשויה אומנם להתגבר על חלק מהבעיות הללו, אך אפשרות מעין זו דומה מאוד

---

196 על גישת ההרתעה וניתוח כלכלי של פשע ראו Gary S. Becker, *Crime and Punishment: An Economic Approach*, 76 J. Pol. Econ. 169, 199 (1968).

197 כך, למשל, מודל ההרתעה הפלילי בוקר פעמים רבות בעבר על כך שהוא אינו מוביל להפחתת הפשיעה. ראו, למשל, Dan M. Kahan, *The Theory of Value Dilemma: A Critique of the Economic Analysis of Criminal Law*, 1 Ohio St. J. Crim. L. 643, 644 (2004).

198 לטיעון זה בהקשר של הגנת הסייבר ראו Deirdre K. Mulligan & Fred B. Schneider, *Doctrine for Cybersecurity*, 140 J. Am. Acad. Arts & Sci. 70, 70–71 (2011), *available at* http://www.cs.cornell.edu/fbs/publications/publicCYbersecDaed.pdf.

199 Kerfoot, לעיל ה״ש 29, בעמ׳ 14.

200 Rosenzweig, לעיל ה״ש 2, בעמ׳ 173.

201 Shackelford et al., לעיל ה״ש 79, בעמ׳ 315.

למהלכים של הסדרה ישירה מראש על־ידי המדינה, שיידונו להלן, ועל־כן לא נבחן אותה בהקשר הנוכחי.

מעבר לכך, ייחוס של רשלנות, גרימת נזק או אחריות לבעל תשתית לאחר מעשה יהיה משימה קשה ביותר.[202] קיים קושי ראייתי משמעותי להוכיח כי גורם מסוים הוא רשלן, מזיק או אחראי בכל הנוגע בהתקפות סייבר, ופעמים רבות ייתכן שכמה גורמים תשתיתיים הובילו בהתרשלותם לנזק.[203] במצב אחרון זה בית־המשפט עשוי להידרש לסוגיית האחריות היחסית של גופים שונים, וגם בה הוא יתקשה להכריע. נוסף על כך יידרש בית־המשפט (או המחוקק, אם העניין יגולגל לפתחו) להכריע בסוגיות מורכבות הנוגעות בהיקף הנזק העקיף ו/או הכלכלי שבגינו יהיה אפשר לתבוע, ובמקביל להחליט למי תהיה זכות עמידה לתובעו.[204] מתן מענה לשאלות אלה אינו כרוך כמובן רק בהכרעה לגבי עובדות (שהיא משימה קשה ביותר בפני עצמה), אלא מחייב הכרעת מדיניות אשר תתווה את היקף האחריות הראוי, כמו־גם התייחסות לאיתורו של מונע הנזק הזול אשר יעיל להטיל עליו את האחריות (גם כאן אסדרה ממוקדת עשויה לסייע, אך מודל מעין זה יידון כאמור להלן). נוסף על כך, הסדרה באמצעות אחריות לאחר מעשה נוטה להסתמך על הסדרה מבוססת־תוצאה, בניגוד להסדרה הבוחנת תהליך (שכן הליך פגום שלא הוביל לתוצאה בעייתית לא ימצא את דרכו לבית־המשפט). אולם יש הסוברים כי דווקא הסדרה המתרכזת בבדיקת הליכים מתאימה יותר להקשר של אבטחת מידע וסייבר.[205]

לסיכום נקודה זו, ראוי לציין כי מנגנוני הפנמה המבוססים על אחריות לאחר מעשה – נזיקית, מנהלית או פלילית – מעוררים קשיים. אומנם, ייתכן שיש מקום לאימוץ המודל מסיבות אחרות, כגון הגשמת יעדים של צדק מתקן (נושא אשר מצריך בדיקה והתייחסות נפרדות),[206] אולם אין בו לבדו להוביל להגנה הנדרשת.

פתרון אפשרי לאתגר האמור, אשר נותן מענה חלקי, הוא התפתחות שוקי ביטוח לאחריות האמורה.[207] כאשר יהיה אפשר לבטח את האחריות לנזקי התקפות הסייבר, יהיו אלה חברות הביטוח שיתמודדו עם האתגרים הנדונים. חברות הביטוח יקבעו וינטרו את כללי ההתנהגות של הגופים הרלוונטיים השונים, ואף יעדכנו אותם בהתאם להתקדמות הטכנולוגיה ולהתממשות הסיכונים. שוק ביטוח זה הינו עדיין בחיתוליו, וכרוכים בו קשיים ייחודיים, ועל־כן היבט זה מצוי מעבר ליריעתו של מאמר זה.

---

202 Kerfoot, לעיל ה״ש 29, בעמ׳ 16.

203 בעניין זה הוצע לעשות שימוש בכלי המשפטי של אחריות יחד ולחוד, אך אף הצעה זו כרוכה בקשיים. ראו שם, בעמ׳ 39.

204 Shackelford et al., לעיל ה״ש 79, בעמ׳ 345; Rosenzweig, לעיל ה״ש 2, בעמ׳ 172; David W. Opderbeck, *Cybersecurity, Data Breaches, and the Economic Loss Doctrine in the Payment Card Industry*, 75 Md. L. Rev. 935 (2016).

205 ראו Ira S. Rubinstein & Woodrow Hartzog, *Anonymization and Risk*, 91 Wash. L. Rev. 703, 732 (2016).

206 אריאל פורת **נזיקין** כרך א 55 (2013); ישראל גלעד **דיני נזיקין – גבולות האחריות** 59–60 (2012).

207 Kerfoot, לעיל ה״ש 29, בעמ׳ 19–20; Rosenzweig, לעיל ה״ש 2, בעמ׳ 173; Opderbeck, לעיל ה״ש 204, בעמ׳ 973–974.

(ב) בעיית ההחצנות ומתן תמריצים

ניתן לסבור כי את נטיית כוחות השוק לתמרץ בחסר את בעלי התשתיות בכל הקשור להבטחת הגנת סייבר אפשר לרפא באמצעות מודל וולונטרי אשר יעניק תמריץ חיובי לחברות להתאים את עצמן לאתגרי הסייבר.[208] בדרך זו תוכל המדינה להניע את הפירמות לאמץ מנגנוני הגנה אשר נראים בעיניה מתאימים. התמרוץ עצמו יכול להיעשות בכמה דרכים: באמצעות תשלום ממש (כפרס או ככיסוי הוצאות) כנגד עמידה בתנאים מוגדרים בנוגע להגנת סייבר;[209] באמצעות מתן זכות גישה למכרזים ממשלתיים (או מתן עדיפות במכרזים אלה) רק לעומדים בסיפי התנהלות קבועים;[210] או על־ידי מתן הטבות באמצעות מערכת המס על־פי אמות־מידה הקשורות לתחום.[211] ברמה הפשוטה ביותר, ניתן להציע שהמדינה תיתן שירותי הגנת סייבר בחינם לאותם מפעילי תשתיות פרטיים אשר יחפצו בכך, כאשר התמריץ הוא קבלת שירות חשוב והגנתי זה ללא תמורה.

אולם גם בתמריצים חיוביים אין כדי למנוע לחלוטין את הבעיות שצוינו בהקשר של החלת מנגנונים אחרים להפנמת עלויות. גם כאן ייתכן שהחברות לא ייענו לאתגר הוולונטרי, ויבחרו לא להגיב על התמריץ ולא לשנות את התנהלותן לאחר שקילת העלויות הכרוכות בכך. נוסף על כך, יישום מדיניות כאמור עלול להיתקל בקשיים פוליטיים. הציבור, אשר גם כך אינו שבע־רצון במקרים רבים מהתנהלותן של חברות התשתיות, לא ישמח שכספי המיסים ינותבו לכיסי החברות האמורות בגין שירותים שהוא היה מצפה שהן יספקו בעצמן.

לסיכום, מנגנון אסדרתי הנשען על כוחות שוק, חובות גילוי, העברות ידע, מתן תמריצים או הסדרה בדיעבד אינו מספק.[212] לפיכך יש לשקול מנגנוני הסדרה אחרים שיפעלו אקס־אנטה ויניעו את הפירמה באופן מפורש לנקוט צעדי מנע נגד התקפות סייבר.

ה. מודלים להגנה על תשתיות מפני איומי סייבר: הסדרה ״אגרסיבית״ אקס־אנטה

1. רא״מ כמשל: חזרה ליסודות המודל הישראלי, ייחודו ויתרונותיו

״וקרני ראם קרניו, בהם עמים ינגח יַחְדָּו אפסי ארץ״

דברים לג 17

208 Kerfoot, לעיל ה״ש 29, בעמ׳ 21. ייתכן שגם בישראל יבחר המְאַסדר לפתח פתרון זה, שכן הוא מוצע (אם כי בצורה כללית למדי בשלב זה) בהחלטת ממשלה 2443, לעיל ה״ש 23, ס׳ 1(ו).

209 Bambauer, *Ghost*, לעיל ה״ש 35, בעמ׳ 1070–1072.

210 ראו, למשל, את הצעתו של Bambauer להנהיג את ״שיטת המקל והגזר״ – שם, בעמ׳ 1062–1078. ראו גם Kerfoot לעיל ה״ש 29, בעמ׳ 5.

211 Rosenzweig, לעיל ה״ש 2, בעמ׳ 173.

212 לעמדה דומה שהובעה בארצות־הברית ראו Mark Clayton, *Why Obama's Executive Order on Cybersecurity Doesn't Satisfy Most Experts*, The Christian Science Monitor (Feb. 13, 2013), http://www.csmonitor.com/USA/Politics/2013/0213/Why-Obama-s-executive-order-on-cybersecurity-doesn-t-satisfy-most-experts.

מענה אפשרי למכלול הבעיות והכשלים המאפיינים את הפתרונות שנדונו לעיל לאתגר של אבטחת התשתיות הוא מתווה אסדרתי אשר מגדיר לכל בעלי התשתיות את מנגנוני ההגנה מפני מתקפות סייבר שעליהם לאמץ, מפקח על היישום ואוכף את הביצוע על הסרבנים. יתרה מזו, כדי להתגבר על חלק מהבעיות בהפעלת מנגנון זה, אפשר לרכז את הסמכות לעניין ההסדרה האמורה בידי גוף מדינתי ואסדרתי **אחד**. נוסף על כך, כדי לשלב את מכלול הידע שנרכש על־ידי המדינה עם המנגנון המדינתי האמור – אשר מקורו, בין היתר, בזרועות הביטחון – יש להפעילו בצורה סודית. אולם מנגנון מעין זה אינו חף מבעיות. נוסף על כך, ניתן ליישמו בווריאציות שונות. הן הבעיות והן הווריאציות האמורות ייסקרו להלן. במהלך דיון זה נבחן בצורה ביקורתית את המודל האסדרתי הישראלי, הפועל על־פי המתווה האמור.

אולם בטרם נעבור לבחינת המודל הישראלי, ראוי להזכיר כי מודל זה אינו הדרך היחידה ליצור אסדרה והסדרה אקס־אנטה בתחום. העוגן המשפטי להפעלה מקדמית של סמכות המדינה עשוי ללבוש צורות שונות. לדוגמה, ניתן להפעיל אסדרה מעין זו באמצעות מודל של רשיונות:[213] תחילה המדינה קובעת כי הפעלת תשתית חיונית תתבצע רק על־פי רישיון (או זיכיון); לאחר־מכן המדינה קובעת ברשיונות אלה את החובה לעמוד בדרישות מסוימות; ובהמשך המדינה פועלת לפקח על יישום הדרישות האמורות, לאוכפן ולעדכנן. היות שמודל זה אינו יוצר שינויים מהותיים ברמת הניתוח שייפרש כאן, לא נדון בו.

המודל הישראלי לאסדרה מראש נותן מענה מעניין לקשיים שפורטו בחלק ד. ראשית, וחשוב מכל, המודל מתגבר על בעיית תמרוץ־החֶסֶר של הפירמה לעמוד בסטנדרט התנהלות ראוי. זאת, באמצעות הגדרת הסטנדרט ואכיפתו מראש על־ידי גורם חיצוני. שנית, המודל מתגבר לכאורה על הבעיות של חסכי המידע והידע שהפירמות מתמודדות עימן. הפתרון המוצע בהקשר זה פשוט והחלטי: ריכוז משימות האבטחה בידי גורם ממשלתי מבטיח שמכלול המידע הנוגע בהתקפות יעבור בין הגופים השונים בתיווך הגוף הממשלתי. על כך ניתן להוסיף גם מידע מודיעיני המצוי בידי המדינה. במתווה זה גם ניתן להתגבר על העדר התמרוץ להעברת המידע בין הגופים, שכן הדבר ייעשה בכפייה. אף בעיית הידע מקבלת פתרון, שכן המומחיות מתרכזת אצל גוף מרכזי/מדינתי אחד, אשר מרכֵּז משאבים ביצירתו, מייעץ לכלל בעלי התשתית, ומאפשר את העברת התובנות הנלמדות בהקשר אחד להקשרים אחרים.

גם היסוד השני המונהג בישראל – הסודיות בהפעלת מנגנון השליטה – נושא עימו יתרונות. חשיפת מידע בדבר דרכי הפעלתן של מערכות ההגנה (או כשליהן) עלולה לשמש תוקפים פוטנציאליים ולהגביר את סיכויי הצלחתם. במקרים כאלה מחיר השקיפות גבוה למדי, ואילו הסודיות מקדמת את ההגנה.[214]

היסוד השלישי שמאפיין את המודל הישראלי הוא ריכוזיות רבה. ריכוז מירב סמכויות ההנחיה בידי גוף אחד נותן מענה לאי־היעילות הנוצרת בשעה שסמכויות אלה מפוזרות בין

---

213 להצעה להשתמש בחוק רישוי עסקים לשם הסדרת ההגנה על תשתיות חיוניות בישראל ראו סיבוני, לעיל ה״ש 1, בעמ׳ 86–87.

214 Yochai Benkler, *A Public Accountability Defense for National Security Leakers and Whistleblowers*, 8 HARV. L. & POL'Y REV. 281, 294 (2014).

כמה מְאַסדרים. במצב של פיזור סמכויות מתפתחים מאבקי כוח ויוקרה סביב סמכויות ודרכי פעולה, ומאבקים אלה עלולים להוביל להחלטות שאינן מבוססות על אינטרסים מקצועיים טהורים. ייתכן שהמתח בין הרשויות נובע מדגשים אסדרתיים שונים (ומוצדקים) של כל רשות,[215] אולם מתח זה מוביל לתוצאה בעייתית. הריכוזיות הקיימת בישראל בהקשר זה מונעת בעיות אלה במידה מסוימת. כמו־כן היא מאפשרת העברה טובה יותר של מידע וידע בין גופים שונים.

כאן המקום לציין כי הריכוזיות בטיפול בתשתיות חיוניות בישראל אינה מוחלטת. מלבד רא״מ קיימים גופים נוספים המסדירים את האבטחה הקיברנטית של תשתיות חיוניות – לפחות בהגדרתן הרחבה. הדבר ניכר בעיקר בתחום הפיננסי. בנק ישראל, אשר מונחה על־ידי רא״מ, מסדיר את פעילות הבנקים בישראל באמצעות המפקח על הבנקים, וזאת גם בתחום הסייבר. בעניין זה פורסמה הוראה 357 בדבר ניהול תקין של טכנולוגיית המידע,[216] המהווה מסגרת מנחה להסדרי אבטחת מידע. על הוראה זו נוספה הוראה 361,[217] המחייבת מינוי גורם בכיר שיופקד על הגנת הסייבר בגוף הפיננסי, יישום כמה עקרונות בולטים של הגנה זו (זיהוי, ניתוח, הכלה, הכרעה והשבה), שיתוף מידע בין גופים וכן הרחבת הניטור והמודיעין. נוסף על כך הקים בנק ישראל, בשנת 2012, פורום להגנת סייבר, הכולל נציגים של בנקים וחברות כרטיסי אשראי. קיים גם שיתוף־פעולה מסוים בין הבנקים לבדם, המוגבל להעברת מידע על־אודות אירועים והתראות של מתקפות סייבר. בנק ישראל שוקל להרחיב את שיתוף־הפעולה בין הבנקים באמצעות מרכז סייבר בנקאי, אשר יכלול ויסדיר שיתוף מידע, מחקרים ומודיעין בנושא סייבר.[218] חברות הביטוח והגופים המוסדיים, לעומת זאת, כפופים להוראת הממונה על שוק ההון, ביטוח וחיסכון, אשר קבע קווי־יסוד לניהול סיכוני המידע ופרסם הוראות בעניין.[219]

יש גופי ממשלה נוספים המפקחים על תשתיות חיוניות, בין היתר בהיבט של הגנת סייבר. כך, משרד התקשורת מתווה מדיניות כללית לגבי תשתיות תקשורת, ואף הקים מחלקה העוסקת בהגנת הסייבר.[220] כמו־כן, לשר התקשורת יש סמכות[221] להכריז על מצב של ״שעת חירום״, ולתת לבעל רישיון הוראות שונות המיועדות להבטיח את פעולתן של תשתיות התקשורת. גוף

215 Kerfoot, לעיל ה״ש 29, בעמ׳ 25–26 ו־29.

216 ראו הוראת ניהול בנקאי תקין 357 ״ניהול טכנולוגיית המידע״ (עדכון אחרון ב־29.4.2012) www.boi.org.il/he/BankingSupervision/SupervisorsDirectives/DocLib/357.pdf.

217 הוראת ניהול בנקאי תקין 361 ״ניהול הגנת הסייבר״ (16.3.2015) www.boi.org.il/he/BankingSupervision/SupervisorsDirectives/DocLib/361.pdf.

218 עירית אבישר ״בכירה בבנק ישראל: ׳אנו שוקלים להקים מרכז סייבר בנקאי׳״ **גלובס** 24.1.2014 www.globes.co.il/news/article.aspx?did=1000911843.

219 ראו הממונה על שוק ההון, ביטוח וחיסכון ״הוראה לניהול סיכוני אבטחת המידע של הגופים המוסדיים״, mof.gov.il/hon/documents/%D7%94%D7%A1%D7%93%D7%A8%D7%94-%D7%95%D7%97%D7%A7%D7%99%D7%A7%D7%94/mosdiym/memos/2006-9-06.pdf.

220 במסגרת ״אגף חירום וביטחון״ קיים אגף ״ביטחון וסייבר״. ראו ״כתובות וטלפונים״ **מדינת ישראל – משרד התקשורת** (עדכון אחרון ב־9.11.2016) www.moc.gov.il/76-he/MOC.aspx.

221 ראו ס׳ 13א לחוק התקשורת (בזק ושידורים), התשמ״ב–1982 (להלן: חוק התקשורת).

נוסף המפקח על תשתיות חיוניות הוא הרשות למשפט, טכנולוגיה ומידע (רמו״ט).[222] רשות זו מתפקדת כרשות האחראית לפרטיות במידע, ועוסקת בהסדרת מאגרי המידע שבידי מפעילי התשתיות הקריטיות. יצוין עוד כי גם בתחום הציבורי־הבטחוני יש פיצול סמכויות בסוגיה זו.[223]

אין זה ברור מהי הסיבה ל״כיסי״ סמכות אלה ולפיצולים שהם יוצרים לעניין הגופים הפיננסיים.[224] נטען כי אלה הוחרגו מסמכות רא״מ כדי למנוע את כפיפותם של הגופים לשירות הביטחון, דבר שהיה עלול להרתיע השקעות של זרים בישראל.[225] ייתכן גם שפעילותה המצומצמת יותר של רא״מ בתחום הפיננסי הינה תולדה של תפיסה אסטרטגית שגופים אלה אינם ראויים להיקרא ״תשתיות קריטיות״. לחלופין, ייתכן שהפיצול הוא דווקא תולדה של פשרות בין מוקדי כוח כלכליים ופוליטיים. כך או כך, ההסדרה בתחום הפיננסי מהווה דוגמה לכך שגם בישראל תיתכן אסדרה באמצעות גוף ציבורי שאינו בעל מאפיינים בטחוניים, אשר תתנהל בשקיפות רבה יותר ותוך הסתמכות מקיפה יותר על כוחות השוק.

עוד ראוי לציין כי על־פי הוראת השעה שנדונה לעיל, מודל הפיקוח הישראלי עומד לעבור פיצול נוסף, שלפיו גופי התקשורת (הכלולים בתוספת הרביעית) יוסדרו על־ידי רא״מ ואילו סמכות הפיקוח על גופים אחרים (המפורטים בתוספת החמישית) תעבור בהדרגה לרשות הסייבר.[226] גם מתווה זה מוסיף מורכבות ופיצול נוסף, וקצרה היריעה ברשימה זו מלדון בסיבות שהובילו למהלך זה (אשר ללא ספק מצדיק דיון עתידי, ככל שהוא אכן ייהפך לקבוע).

עד כאן סקרנו את היתרונות של שיטות הסדרה ואסדרה המקנות סמכות למדינה לקבוע אקס־אנטה את מתווה הגנת הסייבר, כמו־גם מאפיינים נוספים של השיטה הננקטת בישראל, אשר מבוססת על סודיות וריכוזיות. אך בצד יתרונות אלה עלולות להתעורר גם בעיות. במסגרת דיוננו להלן בבעיות אלה נפריד בין שלושת המאפיינים של המודל הישראלי, לפחות ככל שהדבר נוגע בתקופה שבה שלטה רא״מ במהלך ללא עוררין (סמכות ואכיפה, סודיות וריכוזיות).

---

222 הרשות למשפט, טכנולוגיה ומידע (רמו״ט) היא יחידה במשרד המשפטים שתפקידה לחזק את ההגנה על מידע אישי, להסדיר את השימוש בחתימות אלקטרוניות ולפקח עליו, ולהגביר את האכיפה של עֲברות פגיעה בפרטיות. רמו״ט משמשת גם מרכז ידע בממשלה לחקיקה ולפרויקטים בעלי היבטים טכנולוגיים, כגון ממשל זמין. ראו www.justice.gov.il/Units/ilita/Odot/Pages/Odot.aspx.

223 טבנסקי ״הגנה על תשתיות״, לעיל ה״ש 18, בעמ׳ 72. הממונה על הביטחון במערכת הביטחון (מלמ״ב) אחראי לאבטחת המידע במשרד הביטחון ובמפעלים הבטחוניים; המוסד אחראי לאבטחת המידע שלו עצמו; וצה״ל, באמצעות מחלקת הגנת הסייבר, מנהל את אבטחת המידע והאבטחה שלו. גולדשמידט, לעיל ה״ש 51, בעמ׳ 6.

224 ראו Tabansky & Ben Israel, לעיל ה״ש 8, בעמ׳ 39, פס׳ 5.4.1.

225 ראו בעניין זה את דבריה של אסתר לבנון (יושבת-ראש הבורסה, שהייתה קודם לכן בכירה בשירות הביטחון). דבריה מעניינים היות שהם פותחים צוהר נדיר למערך השיקולים בדבר כלילתם (או אי־כלילתם) של גופים בין אלה המוסדרים על־ידי חוק הביטחון. ראו פרוטוקול מס׳ 142, לעיל ה״ש 57, בעמ׳ 24–25.

226 ראו לעיל ה״ש 12 והדיון בטקסט שלידה.

2. חסרונותיה של הסדרה ממשלתית מראש

(א) הסדרה מראש והאפקטיביות של צמצום פערי הידע

כאמור, מסתמנת מגמה בכמה מדינות שעל־פיה המדינה תקבע ותאכוף את הדרך הנכונה להבטיח הגנת סייבר. אולם נראה שכמעט כל החוקרים בתחום סבורים כי אסטרטגיה זו שגויה (ואחד הכותבים אף כינה אותה ״היבריס״).[227] ככל שהדבר נוגע בדרכי הגנה בסייבר, קשה להאמין שרמת המומחיות בקרב המדינה תהיה הגבוהה ביותר.[228] להפך, סביר להניח כי לפחות ברוב המקרים תשתרך המדינה בהקשר זה מאחור.[229] אומנם, המדינה יכולה לפנות לגופים חיצוניים ולהיעזר בדעתם, אולם כך יכולים לעשות גם הגופים המוסדרים. ושוב, אין סיבה להניח כי למדינה תהיה היכולת לערוך אינטגרציה בין חוות־דעת שונות ולזהות את כלי ההגנה הטוב ביותר. לפיכך בנקודה זו יש לאזן בין ההנחה שהמדינה (להבדיל מהחברות) תשאף לבחור סטנדרט הגנה ואבטחה ראוי ומתאים, ללא עירוב שיקולי חיסכון ורווח לא־ראויים, לבין החשש שהמדינה לא תקבל את ההחלטה המושכלת ביותר בשל מחסור בידע.

על אמירה כללית זו ניתן להוסיף חמישה דגשים הנוגעים באופן מיוחד בסוגיית הסייבר, אשר עשויים להחמיר את החשש דנן מהחלטות המדינה. **ראשית**, יש חוקרים הסוברים כי הפגיעה הנובעת ממודל ההסדרה בידי המדינה הינה רחבה עוד יותר, ופוגעת גם במחקר העתידי ובחדשנות. כאשר המדינה היא שמכתיבה את דרך ההתנהלות, ולא השחקנים בשוק, הדבר משפיע על התקדמות החדשנות והמחקר בתחום בכללותו, שכן השוק והחוקרים מתאימים את עצמם להמלצותיהן של הרשויות.[230] ההשפעות של תופעה זו בעייתיות ביותר, שכן הן עלולות להוביל למיקוד החדשנות בכיוונים לא־מתאימים (שאינם משקפים את הצרכים האמיתיים), ומתחם האיומים העתידיים האמיתי ייוותר ללא מענה.

ראוי לסייג מעט ביקורת זו. תחום הסייבר מתאפיין בהתפתחות מהירה מאוד, אשר מבוססת במידה רבה על חברות הזנק (בישראל לבדה יש מאות כאלה).[231] אין זה מתחייב שדפוס חדשנות מעין זה יושפע מבחירות או אפילו מהכְּוונה של המדינה במגזר צר יחסית של תשתיות חיוניות. ספק אם התקציבים והמקורות אשר יופנו לפרויקט מסוים בהקשר זה ישפיעו בצורה ניכרת על החלטותיהם של יזמים אשר רואים לנגד עיניהם שווקים רחבים יותר. עם זאת, ביקורת זו עשויה להתעצם במצבים שבהם המדינה מגדירה בין משימותיה את המטרה להשפיע

---

227 Kerfoot, לעיל ה״ש 29, בעמ׳ 32.

228 שם, בעמ׳ 38. ראו גם Michael J. O'Neil & James X. Dempsey, *Critical Infrastructure Protection: Threats to Privacy and Other Civil Liberties and Concerns with Government Mandates on Industry*, 12 DePaul Bus. L.J. 97, 111 (2000).

229 Rosenzweig, לעיל ה״ש 2, בעמ׳ 163.

230 Kerfoot, לעיל ה״ש 29, בעמ׳ 8.

231 ראו Tabansky & Ben Israel, לעיל ה״ש 8, בעמ׳ 28, פס׳ 3.8.2 (שם נמסר כי נכון לשנת 2014 פועלות בישראל כ־200 חברות סייבר, אשר כמחציתן נוסדו בין 2010 ל־2014).

על המחקר והחדשנות בתחום הסייבר בדרכים שונות. אכן, זה המצב בישראל, שבה החדשנות מוזכרת בהחלטות הממשלה הנוגעות במטה הסייבר.[232]

שנית, גם אם נאמר שבנקודת זמן ראשונית המדינה יכולה להעניק לגופים הנחיה סבירה, חסרונה הגדול הוא באיטיות תגובתה ובאי־יכולתה לשנות את אופי ההנחיות, אשר מבוססות על מדיניות מסוימת, לצורך התמודדות עם שינויים שחלים במציאות, בפרופיל האיומים ובטכנולוגיה.[233] נראה כי קשה למצוא מתחרים לתחום הסייבר ככל שהדבר נוגע במהירות השינויים החלים בתחום. גופים ממשלתיים, לעומת זאת, נוטים מטיבם להגיב לאט. במקרים רבים אין בכך פסול – התגובה האיטית מביאה עימה צעדים שקולים ומחושבים, כיאה לגוף המתבקש להגשים את רצון הציבור בכללותו. אך נראה כי בתחום דנן האיטיות עלולה להיות לרועץ. לא בכדי פורטה לעיל דרך הפעולה של ה־FERC, אשר באחד המקרים קבעה כאמור סטנדרטים שהתיישנו עד שהגיע המועד ליישומם ועל־כן הוחלט להחליפם.[234] כאמור, הביקורת שהתעוררה על מודל פעולה זה התמקדה בחוסר היכולת להגיב על סיכונים בזמן, דבר אשר גרר פגיעה אפשרית בביטחון של תשתיות החשמל.

נסייג ונאמר כי הביקורות הכלליות הנוגעות באיטיות התגובה של המדינה (כמו זו שהוצגה לעניין ה־FERC)[235] אינן רלוונטיות בהכרח למודל (הישראלי) הספציפי שנדון כאן. ההליך האמור שם חִייב שיג ושיח בין גופים פרטיים וציבוריים, דבר ש״תרם״ לאיטיות התגובה, אך אין הוא מחויב בהכרח בישראל. עם זאת, לתובנה שלפיה רשויות המדינה, **מעצם טיבן**, פועלות לרוב באיטיות רבה יותר, בעיקר בכל הנוגע בעדכון נהלים ובהחלפתם, יש נפקות גם בהקשר הישראלי. כך, האיטיות שבה התעדכנה הרשימה שהופיעה בתוספת הרביעית לחוק הביטחון (המגדירה את הגופים הכפופים לרא״מ ועתה מופיעה ברובה בתוספת החמישית), גם כאשר מתרחשים שינויים בשוק, מעוררת את החשש שהטיעון הכללי שהובא כאן בנוגע לאיטיות התגובה יפה גם לענייננו.[236]

שלישית, עולה חשש שפיקוח ואכיפה על־ידי המדינה יובילו את הגופים המוסדרים לנקוט את מדיניות ה״צ׳ק ליסט״ (או box-checking).[237] כאשר האחריות מונחת על כתפי המדינה, יוכל התאגיד להיתלות בהסדרה שהוא כפוף לה, ולא לשקוד על רמת אבטחה נאותה. הוא יבחר לעמוד ברמת האבטחה הנדרשת ממנו – לא פחות אך גם לא יותר. טיעון זה נכון אומנם לכל מנגנון הסדרה קפדני, אך בהקשר דנן החששות רבים יותר משום שהמציאות משתנה במהירות. לפיכך יש הסוברים כי ראוי לשמר ואף להעצים את מעורבותם של הגופים המוסדרים בהליך.

232 החלטת ממשלה 2443, נספח א – ״עיקרי תפיסת האסדרה הלאומית בהגנת הסייבר״, ס׳ 3(ו) ו־3(ח); נספח ב – ״יחידה להסדרת שוק שירותי הגנת הסייבר״.

233 Gus P. Coldebella & Brian M. White, *Foundational Questions Regarding the Federal Role in Cybersecurity*, 4 J. NAT'L SECURITY L. & POL'Y 233, 241 (2010).

234 ראו ביקורת על ה־FERC לעיל ליד ה״ש 131–135.

235 Ellis, לעיל ה״ש 23, בעמ׳ 52.

236 לניתוח אופי השינויים של הרשימה שבתוספת הרביעית לחוק ראו את הדיון להלן ליד ה״ש 245–247.

237 Palmer, לעיל ה״ש 134, בעמ׳ 364. יצוין כי ביקורת זו יפה גם למצבים שבהם הבקרה תיעשה על־ידי צדדים שלישיים שיערכו בדיקות התאמה (או compliance) על בסיס רשימה קבועה.

יצוין כי המודל האסדרתי בישראל אינו מכפיף לחלוטין את חברות התשתיות לרא״*מ* ולרשות הסייבר, ואינו מנתק אותן ממעגל קבלת ההחלטות, אלא ממנה את רא״*מ* (או רשות הסייבר) כגוף מנחה (שאת הנחיותיו חובה לקבל). בשל הסודיות של דרך הפעלת המודל בישראל אי־אפשר לדעת באיזו מידה מערכת היחסים בין הגוף המנחה לגופים המונְחים מובילה להתממשותו של סיכון זה, ועל־כן אי־אפשר להעריך את החשש האמור כאן בצורה טובה.

רביעית, החשש שהמדינה אינה השחקן המתאים לריכוז ולהעברה של ידע הנוגע בהגנת סייבר מתחדד לנוכח השינויים המתרחשים במתווה הטכנולוגי בקרב חברות התשתיות. בעבר השתמשו חברות מעין אלה במערכות מחשוב ייחודיות אשר נכתבו במיוחד בעבורן (proprietary). אולם בניסיון לחסוך בהוצאות, כמו־גם לעודד יכולת התממשקות עם מערכות אחרות, מסגרות רבות עוברות להשתמש בתוכנות־מדף – COTS.[238] מעבר זה כרוך ביתרונות ובחסרונות ככל שהדבר נוגע באבטחה. מכל מקום, ככל שמדובר באבטחת מערכות המבוססות על תוכנות־מדף, מתחדד הספק לגבי הקביעה כי דווקא למדינה יש יתרון בהבנתן ובהגנתן. במקרה זה השוק המסחרי העולמי מתמודד כולו עם אתגרים קרובים, וסביר להניח כי שם מצויה המומחיות בתחום.

חמישית, ואולי חשוב מכל, למנגנון מדינתי זה יש משמעות רק אם נלוות אליו סמכויות אכיפה מתאימות, אך לא ברור כלל שזהו המצב. על פניו, המדינה יכולה לנקוט סנקציות מגוונות נגד חברות התשתיות, לרבות השעיית פעילותן, אם הן אינן פועלות בהתאם לדרישות המוגדרות.[239] אולם בפועל במקרים רבים הדבר אינו פשוט. כפי שמקרה־המבחן של הסדרת משק החשמל בארצות־הברית מלמד,[240] אכיפה מצריכה משאבי כוח־אדם, ואלה אינם זמינים בהכרח. כמו־כן, במקרים רבים הגופים המוסדרים הינם חזקים ובעלי השפעה, ולא בקלות יוכל המְאַסדר להעניש (בוודאי לא בחומרה, שהרי הם שולטים בתשתית חיונית!). מובן שגם כאן הסודיות האופפת את הפעלת המודל בישראל מקשה התייחסות לתקפותה של טענה זו בארץ. יצוין כי גם ללא אכיפה יוכל המודל האמור לשפר את מתווה הגנת הסייבר, מעצם העובדה שהוא מעביר מידע וידע בזמן־אמת לפירמה, אך נדגיש כי את היעדים הללו ניתן להגשים גם תוך שימוש במודל שונה ומקל יותר.

(ב) הסדרת המדינה, עיוותי ידע ושיקולים זרים

הטלת המשימה של קביעת סטנדרטים לאבטחה על גופים מדינתיים, אשר מחייבים מצידם את הגופים הפרטיים לסור למרותם, מעלה חשש שבחירת הדרג המקצועי בסטנדרט תנבע מלחצים ומשיקולים זרים. חשש זה מחמיר בתחום שבו עסקינן, בהיותו תחום חדשני ומורכב, לוט בסודיות, מחד גיסא, ובעל השלכות כלכליות גדולות, מאידך גיסא. ראוי לציין כי במקרה שלפנינו התייעצות של הדרג המקצועי עם גורמים חיצוניים רצויה, מבורכת, וכנראה אף הכרחית. אך הקו בין התייעצות רצויה לבין השפעה פסולה הוא דק, והפיקוח על חצייתו קשה ומורכב. במקרה דנן ניתן לחזות שתי מערכות לחצים שיפעלו לעוות את שיקול־דעתה של

238 commercial off-the-shelf. לדיון בסוגיה זו ראו Clarke & Knake, לעיל ה״ש 35, בעמ׳ 140.
239 ראו דיון לעיל ליד ה״ש 118–121.
240 ראו דיון לעיל בחלק ג1(ב), ליד ה״ש 125 ואילך.

הרשות, אשר מגיעות משני מוקדי לחץ: האחד, של גופי טכנולוגיה; והאחר, של מתחרים בגופים המפוקחים. במקרה הראשון תשתקף הבעיה ברמת הגנה לא־מיטבית; ואילו במקרה השני יתבטא הנזק לא בפגיעות במימד הסייבר דווקא, אלא בפגיעות אחרות בתחרות ובצרכנים.

החשש הראשון פשוט יותר להבנה. לחברות ולבעלי אינטרס יש תמריץ מובהק להפעיל לחצים על המְאַסדר לבחור בדרך ובסטנדרט מסוימים אשר יניבו הכנסות ודאיות לכיסם.[241] בספרות הנוגעת בכלכלה הפוליטית תופעה זו מכונה rent seeking.[242] הדבר עלול להוביל לבחירה בטכנולוגיות ובחברות אשר אינן מעניקות הגנה מיטבית. בהקשר זה לבחירה במערכות הגנה מסוימות יש השלכות מרחיקות־לכת. כאן ניתן לטעון כי על פניו מדובר בשוק קטן ובמספר מצומצם של חברות שצורכות את השירות, ולכן סביר להניח כי התמריץ להפעלת לחצים מעין אלה קטן, והשפעת הדינמיקה האמורה תהיה מצומצמת. אולם שוק הגנת הסייבר, בישראל במיוחד, רווי מאות (אם לא אלפי) חברות המציעות שירותים מסוגים שונים. איתות מהמדינה על בחירה בדרך מסוימת יהווה סמן משמעותי לאיכות, אשר ישפיע על ספק שירות ההגנה הן בשוק הישראלי והן בשווקים בין־לאומיים. על־כן יש לחברות אלה אינטרס מובהק להשפיע, באופן משמעותי, על המְאַסדר שימליץ על אימוצן. השלכותיה של הדינמיקה שתוארה כאן עלולות להיות חמורות, ובראשן האפשרות שתאומץ הגנה טכנולוגית לא־ראויה. אך ההשלכה עשויה להיות גם דרמטית פחות, בדמות דרישה של אמצעי הגנה מיותרים. רכישתם של אמצעים אלה והשימוש בהם ייצרו עלויות ללא צורך שעלולות להכביד על חברות התשתיות, אשר יגלגלו אותן אחר כבוד לצרכנים. אי־השקיפות שקיימת בהקשר זה אינה מאפשרת לנו להבין באיזו מידה התשלומים שאנו משלמים בעבור התשתיות הקריטיות כוללים רכיב של תשלום בעבור הגנת סייבר, אשר עשוי להיות מיותר בחלקו ותולדה של דינמיקה לא־ראויה זו.

החשש השני מורכב מעט יותר. הוא מתייחס למצבים שבהם הגופים שמנסים להשפיע אינם חברות טכנולוגיה, אלא מתחרים של גופים הכפופים להסדרה. בשוק תחרותי ינסה כל גוף להשיג יתרון על יריבו. דרך אחת עשויה להתבטא בניסיון של גוף להביא לידי כך שעל יריבו יושתו חובות אסדרתיות מכבידות. ניתן לכנות התנהלות מעין זו ״שיסוי אסדרתי״ — פעולות של בעלי אינטרס (לעיתים בכסות של דאגה לגיטימית להגנת המדינה או הצרכנים) המיועדות להשפיע על מְאַסדר שיקבע הסדרים הפוגעים בגופים המתחרים בהם.

חששות אלה מבוססים על מקרים שאירעו בעבר. בארצות־הברית התרחשו כמה אירועים שעוררו חשד ל״שיסוי אסדרתי״. לדוגמה, ה־FCC נדרש על־ידי אזרחים מודאגים (או שמא היו אלה בעלי אינטרס?) לוודא כי אמצעי תקשורת מתקדמים בתחילת דרכם, דוגמת הטלפוניה הסלולרית והמקוונת, יספקו יכולות מתקדמות של התקשרות בשעת חירום. זאת, בדומה לדרישות המוטלות על ספקי התקשורת הקיימים (טלפוניה נייחת). בעניין זה הזהירה סוזן

241 KERFOOT, לעיל ה״ש 29, בעמ׳ 7; ROSENZWEIG, לעיל ה״ש 2, בעמ׳ 162–163.

242 KERFOOT, לעיל ה״ש 29, בעמ׳ 7; DENNIS C. MUELLER, PUBLIC CHOICE III 342 (2003).

קרופורד כי ייתכן שמי שעמדו מאחורי הדרישות הללו היו חברות התקשורת הוותיקות, אשר ביקשו בכך לעכב את מתחרותיהן ולהשית עליהן עלויות כבר בתחילת דרכן.[243]

בהקשר של התוויית מדיניות סייבר ייתכן שיַקשה הקורא ויטען כי חששות אחרונים אלה אינם רלוונטיים, שהרי בעלי התשתיות הכפופים להסדרה הינם בהגדרתם מונופולים, ועל־כן אין הם ניצבים אל מול החשש הנדון, שמקורו במתח תחרותי. יתר על כן, אף אם קיים מתחרה, גם עליו תושת מערכת חובות דומה, ועל־כן אין לו אינטרס להשפיע על אופי ההסדרה ועומקה. אך אופיים הדינמי של מבני השווקים הופך חשש זה לרלוונטי. שוקי התשתיות עוברים שינויים שבמסגרתם נכנסים למשחק שחקנים חדשים – אשר לא נחשבו עד עתה מבחינה אסדרתית כמשתייכים לשוק המוסדר בקפידה – ומתחרים בבעל התשתית הקיימת.

בדיקה ראשונית בדבר קיומה והתפתחותה של תופעת "השיסוי האסדרתי" יכולה להתייחס לשאלה כיצד נקבע אם גוף ייפול תחת סמכותה של רא"מ בהקשר של הסדרת תחום הסייבר.[244] על־פי החוק שקדם לתיקוני 2016 ולהוראת־השעה, קביעה מעין זו נעשתה על־ידי ועדת ההיגוי בהתאם להמלצת רא"מ, ואושרה על־ידי גורמים בממשלה ובכנסת. קביעה כאמור יצרה עלויות נוספות לגוף (או ללקוחותיו) שהוחלט כי יהיה כפוף לסמכות האסדרה של רא"מ, ועל־כן נוצר תמריץ לפירמות לנסות לפעול להחלת המנגנון האמור על מתחרותיהן ולהחרגת עצמן ממנו.

עיון במתווה האסדרה של תשתיות קריטיות, כפי שנציג בקצרה מייד, מראה כי החששות מתופעת "השיסוי האסדרתי" במקומם הם. בדיקת הגופים השונים שהוגדרו כתשתית חיונית בישראל, לעומת אלה שהוחלט לא להגדירם ככאלה, מצביעה על מרווח שיקול־הדעת שיש בידי רשויות המדינה. מרווח זה עשוי לשמש אמצעי בידי פירמות לפעול לכך שדווקא מתחריהן יוכפפו לאסדרה. בכך תנוצל המערכת האסדרתית הקיימת לרעה, תוך פגיעה בתחרות וביעילות האסדרה ככלל. העובדה שיש שורה ארוכה של החלטות (או הימנעויות מהחלטות) שקשה להסבירן מעוררת את החשש שניצול לרעה כאמור עשוי בהחלט להתרחש. אין סיבה מיוחדת לסבור שחשש זה יוקהה עם כניסתה של רשות הסייבר לפעולה בהקשר זה. השינוי היחיד שהתרחש בכל־זאת היה העברת מירב הגופים הנדונים כאן מהתוספת הרביעית לתוספת החמישית, כאמור.

להלן כמה דוגמאות שמקנות מידה של ממשות לטענה זו: מגזר הדלק כולל רשימה ארוכה של חברות תשתית, אך שמה של שותפות דלק פי גלילות נעדר ממנה, אף־על־פי שהיא אחת משלוש התשתיות הללו בישראל;[245] במגזר המים ניתן למצוא רק את חברת מקורות, אך לא את תאגידי המים המקומיים; במגזר התחבורה נמצא את רשות שדות התעופה ורכבת ישראל,

243 Susan P. Crawford, *The Ambulance, the Squad Car, & the Internet*, 21 Berkeley Tech. L.J. 873, 876, 883 (2006).

244 לחידוד הקושי בהקשר זה אפשר לתת את הדעת להגדרה השונה והרחבה יותר שניתנה ל"נושא תשתית חיונית" ול"תחום תשתית חיונית" בחוק לקידום התחרות ולצמצום הריכוזיות, התשע"ד–2013 (ס' 2 והתוספת לחוק).

245 על משק הדלק בישראל ראו עוד "משק הדלק בישראל" **אתר משרד התשתיות הלאומיות, האנרגיה והמים** (20.8.2015) energy.gov.il/Subjects/Fuel/Pages/GxmsMniFuelEconomy InIsrael.aspx.

אך לא את הרכבת הקלה הפועלת בירושלים או את מנהרות הכרמל, אשר על־פי הדיווחים כבר בוצעה שם מתקפת סייבר;[246] מגזר הבריאות מעורר תמיהה מיוחדת, היות שהוא כולל את מגן דוד אדום אך לא את בתי־החולים וקופות־החולים;[247] לבסוף, מגזר התקשורת (אשר ייוותר כאמור בסמכות רא״מ) מעורר אף הוא עניין מיוחד, שכן נכללים ברשימה גופים רבים, אך מפעילי הסלולר הווירטואלי ואף חברת גולן טלקום אינם מופיעים בה (להבדיל מחברת הוט, אשר נכללת בה), אם כי ניתן אולי להסביר זאת בכך שלמפעילי הסלולר הווירטואלי אין תשתית תקשורת משלהן. כאמור, אין באמור לעיל כדי לרמוז כי ההחלטה בדבר הכללתם או אי־הכללתם של גופים נבעה מלחץ פסול או הינה שגויה על פניה. אולם ניתן להסיק מן האמור, בזהירות מסוימת, כי קיים חשש להתממשות תוצאה בעייתית כתולדה של לחצים פסולים.

תהליך קבלת ההחלטה אם גוף ייכלל בתוספת הרביעית לחוק הביטחון (וכיום — גם בחמישית) וכתוצאה מכך יוכפף להסדרת רא״מ (או רשות הסייבר) שונה מתהליך קבלתן של כל ההחלטות האחרות בנוגע להסדרת הגנת הסייבר שבהן התרכז מאמר זה. ההתמקדות בהחלטה זו בדיוננו כאן נבעה כמובן מהעובדה שהקביעה אם גוף יוסדר אם לאו הינה הבחירה היחידה הפתוחה לעיון הציבור. תהליך ההחלטה האמור עובר דרך הרשויות המחוקקת והמבצעת ומקבל לבסוף פומבי, להבדיל מההחלטות האחרות, אשר נשמרות בחשאי וכפופות להחלטות מקצועיות בלבד. אולם אין בהבחנה זו משום רמיזה כי ״השיסוי האסדרתי״ אינו מתקיים בהקשרים אחרים הנוגעים בהגנת הסייבר על תשתיות חיוניות. ניתן אומנם להניח כי גיבוש התוספות הרביעית והחמישית עובר במסגרות שבהן קבוצות־לחץ מיומנות פעילות, כגון משרדי ממשלה והכנסת, ועל־כן הליך זה מועד יותר לפורענות. אך ניתן בהחלט לחשוש שגם הליך סודי ומקצועי (כגון התוויית הנחיות בנוגע להגנת סייבר), אשר אך מעטים שותפים לו אך השלכותיו גדולות, יהיה מועד לנסיונות השפעה במידה לא־פחותה. לכן ניתן בהחלט להקיש ממסכת הבחירה של גופים לתוספות הרביעית והחמישית אל שאר פעולותיהן של רא״מ ורשות הסייבר בהקשר של דיוננו.

(ג) סודיות

חיסרון נוסף במודל הישראלי טמון בסודיות ובהעדר השקיפות של פעולותיו. לדוגמה, איננו יודעים מהן אמות־המידה לבחירת הגופים שיהיו כפופים להנחיה; מהו הסטנדרט המוחל; אם הגוף המנחה מתייעץ עם מומחים חיצוניים (ומהי מומחיותם); אילו עלויות מושתות על החברות ו/או על הציבור; ועד כמה הגופים המנחים נחשפים לפרטים אישיים של לקוחות התשתיות. הסודיות משפיעה על הדיון בשני ממדים: מחד גיסא, היא מרכיב במדיניות ההגנה על תשתיות חיוניות ועל־כן חלק מהדיון דנן; מאידך גיסא, היא יוצרת נעלמים רבים אשר

---

246 יוסי הטוני ״דיווח: מתקפת סייבר גרמה לשיתוק מנהרות הכרמל לשעות רבות״ **אנשים ומחשבים** 28.10.2013 www.pc.co.il/it-news/134965.

247 נראה כי הסמכות בעניין זה היא של מנכ״ל משרד הבריאות, וזאת מכוח סמכותו הכללית. ראו חוזר מנכ״ל משרד הבריאות 3/15 ״הגנה על מידע במערכות ממוחשבות במערכת הבריאות״ (15.2.2015) www.health.gov.il/hozer/mk03_2015.pdf. נסייג ונאמר כי חלק מבתי־החולים הם ממשלתיים, אך יש גם לא מעט שאינם בבעלות הממשלה.

מקהים – ולעיתים מעקרים – חלקים מסוימים בביקורת על המנגנון, שכן היא מחייבת מעבר לדיון מופשט או כזה המבוסס על הנחות אשר ייתכן שהן שגויות. יצוין כי הסודיות אינה מרכיב הכרחי בהפעלת המודל הנדון כאן. בארצות־הברית, לדוגמה, ניתן לקרוא באתרים פתוחים על תקני האבטחה המומלצים כמו־גם את ההנחיות המוכתבות (במקרים המעטים שהרשויות אכן מכתיבות אותן). ניתן אף לעיין בשאלונים המועברים לבעלי התשתיות שבאמצעותם הרשות בוחנת את מידת הסיכון הגלום בפעילותן. אך בשל נוכחותה המשמעותית במודל הישראלי והשפעותיה הניכרות, נקדיש לה כאן כמה פסקאות.

הסודיות מהווה לכאורה מנגנון שאמור להבטיח רמת אפקטיביות גבוהה של הגנת הסייבר, וזאת בהתאם לתובנה המקובלת כי חשיפת מידע לציבור – וכתוצאה מכך הנגשתו לאויב – עלולה לפגוע ביעדי ביטחון; "loose lips sink ships" הינה המימרה הידועה מתקופת מלחמת־העולם השנייה אשר מבטאת תובנה זו בבהירות. אף־על־פי־כן, השקיפות הינה דווקא אמצעי שעשוי להבטיח הגנה טובה יותר. במקרים רבים שקיפות עשויה לאפשר בקרה ואף ביקורת על פעולותיהם של המְאַסדר ושל חברות התשתיות. ביקורת מעין זו מסייעת לגופים האמורים – ואף מתמרצת אותם – להשתפר ולהגביר את עמידותם מפני התקפות.[248]

טענה אחרונה זו מתחזקת מכוח ההבחנה בין הגנת הסייבר שבה עסקינן לבין הֶקשרים בטחוניים אחרים, דוגמת זה הנוגע במיקומן של אותן אוניות או צוללות שהיו מושא המימרה הנודעת שלעיל ממלחמת־העולם השנייה. יש מקום לסבור כי שקיפות של ההנחיות הנוגעות בהפעלתם של מנגנוני אבטחה אינה מסכנת את רמת האבטחה כמו חשיפת מיקומיהם של כלי מלחמה בשעת קרב.[249] במידה רבה, אופי מערך ההגנה גלוי ממילא לתוקפים פוטנציאליים רבים. על־כן שקיפות בּרִירנית עשויה לא להגדיל את הסיכון לתקיפה מוצלחת, ואף להביא עימה את היתרונות העולים מקבלת ביקורת רחבה ובונה.

זאת ועוד, הסודיות עלולה להביא לידי פגיעה באמון הציבור בכל הנוגע בביצוע פעולות ההגנה האמורות. בארצות־הברית, לדוגמה, יש הטוענים כי ה־NSA אינו זוכה בדריסת־רגל מספקת בתחום הגנת הסייבר בשל החשש הציבורי מארגון (סודי) זה.[250] החשש הציבורי מחלחל אל כמה מאושיות השלטון ומהשחקנים הרלוונטיים: אל הפוליטיקאים, אשר עשויים לחשוש מפגיעה תדמיתית אם יעניקו גיבוי להרחבת סמכותה של סוכנות הביון; אל העיתונות, אשר עשויה להעניק סיקור שלילי לפעולות הגנה אלה; ואף אל החברות הפרטיות המספקות את התשתיות או את אמצעי ההגנה, אשר עשויות לבחור (ככל שבאפשרותן לעשות זאת) לא לשתף פעולה בהקשר זה עם המדינה (הפועלת תחת מעטה סודיות) משיקולי תדמית.

---

248 ראו, למשל, Benkler, לעיל ה״ש 214, בעמ׳ 284 ("Secrecy insulates self-reinforcing internal organizational dynamics from external correction").

249 ראו שם, בעמ׳ 294–295; Karen Scarfone, Wayne Jansen & Miles Tracy, Guide to General Server Security 2–4 (Nat'l Inst. for Standards & Tech., Special Publication 800-123, 2008), *available at* http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-123.pdf; Jerome H. Saltzer & Michael D. Schroeder, *The Protection of Information in Computer Systems*, 63 Proc. IEEE 1278 (1975), *available at* http://www.cs.virginia.edu/~evans/cs551/saltzer.

250 Rosenzweig, לעיל ה״ש 2, בעמ׳ 197.

סוגיית הסודיות קשורה גם לסוגיית החוקתיות והמידתיות שבמודל האסדרה וההסדרה הישראלי, אשר תידון להלן בחלק־משנה (ה). לאזרחים יש זכות בסיסית (אשר ניתנת כמובן לצמצום ולאיזון) לשקיפות בפעולות המדינה.[251] ללא עין מפקחת, הסודיות מגדילה את החשש שמקבלי החלטות יחרגו מייפוי־הכוח שניתן להם לפעול. לעומת זאת, השקיפות מפחיתה חשש זה, ועשויה לסייע בבקרה שזכויות־יסוד אחרות – ובעיקר הזכות לפרטיות – אינן נפגעות באופן לא־מידתי. זאת, בעיקר באמצעות הבטחת שיח ציבורי ומשפטי בעניין, אשר יקדם הפעלת מנגנוני ביקורת והגנה.

אין בטיעונים האמורים כאן כדי להוביל למסקנה כי על הגוף שיסדיר את הגנת הסייבר לפרסם את כלל ההנחיות שהוא נותן לגופים השונים או את דרכי עבודתו. אולם ניתן למצוא דרכי־ביניים, כגון פרסום עקרונות כלליים של דרכי העבודה, אשר יאפשרו הגשמה חלקית של יעדי השקיפות. דרך־ביניים נוספת היא העברת המידע למומחים מייעצים. ייתכן שהדבר נעשה גם כיום, אך ראוי – ולוּ כדי לרכוש את אמון הציבור – לתת לדבר ההתייעצויות הללו פומבי. יצוין כי כבר כיום רא״מ כפופה לביקורת מטעם מבקר המדינה.[252] עם זאת, נראה כי גם דוחות המבקר בעניין זה אינם מפורסמים, ועל־כן חלק מיעדי השקיפות שצוינו כאן אינם מוגשמים.

(ד) ריכוזיות (יתר?)

נעבור לדון עתה במה שנראה כאחד היתרונות הגדולים של המודל הישראלי – אופיו הריכוזי. לטענתנו, ריכוזיות זו עלולה לעיתים לעמוד לו לרועץ. טענה זו נשענת על עיקרון מקובל בהקשר של הגנת סייבר – עקרון ההטרוגניות (diversity), דהיינו, הדרישה שמנגנונים שונים יוגנו בשיטות שונות.[253] ההטרוגניות חשובה שכן מגדילה את הסיכוי שאם אחד ממנגנוני ההגנה ייפרץ או יוכח כשגוי וחלש תתקיים עדיין הגנה מכוח מנגנונים אחרים. יתרה מזו, במצב של הטרוגניות לא יוכלו התוקפים להעתיק נסיון תקיפה מוצלח למערכות אחרות. באופן זה יצומצם וימוקד הנזק שייגרם מהניסיון האמור. על פניו, כאשר מדובר בְּמַאֲסדר ריכוזי, הטרוגניות זו עלולה להיפגע.

באשר לתקפותו של טיעון זה לגבי המצב בישראל אפשר להקשות ולטעון כי תהיה זו טעות להניח שאם גוף יחיד מסדיר את הגנת הסייבר של גופים רבים, משמעות הדבר היא בהכרח שהוא מסדיר את כל הגופים באופן זהה או דומה. על פניו, דווקא דרך פעולה ריכוזית תוכל להבטיח הטרוגניות בצורה הטובה ביותר, שכן גוף ריכוזי יוכל לוודא כי עקרון ההטרוגניות מיושם באופן מלא וכי המערכות שבהן נעשה שימוש מבוזרות ושונות זו מזו, ובכך להגביר את עמידותה של המערכת בכללותה. אולם אפשר שמְאַסדר ריכוזי יובל על־ידי הנהלה אחת, אשר תתבסס על פילוסופיה יחידה והבנה מסוימת של סיכונים נדונים. מאפיין זה עלול להוביל – לעיתים אף מבלי דעת – לאחידות מסוימת במנגנוני ההגנה של מכלול התשתיות במדינה, ובכך

251 Tal Z. Zarsky, *Transparent Predictions*, 2013 U. Ill. L. Rev. 1503, 1530; Mark Fenster, *The Opacity of Transparency*, 91 Iowa L. Rev. 885, 895–896 (2006).

252 ס׳ 22א לחוק מבקר המדינה, התשי״ח–1958.

253 Bambauer, *Ghost*, לעיל ה״ש 35, בעמ׳ 1058–1061; Rosenzweig, לעיל ה״ש 2, בעמ׳ 180; Benkler, לעיל ה״ש 214, בעמ׳ 295.

לפגיעות אינהרנטית כתוצאה מהפעלת המודל. לנוכח האמור, החלופה של הסדרה באמצעות בעלי התשתית עצמם (תוך שהמְאַסדר משמש גוף מייעץ בלבד) עשויה להקנות יתרון, מכיוון שהדבר יעודד הטרוגניות קונספטואלית.[254] פתרון אחר עשוי להיות אסדרה באמצעות מְאַסדרים מגזריים. אולם פתרון אחרון זה צפוי להוליד מאבקים על כוח ושליטה בתחומי אסדרה, שיגרמו קשיים רבים. בהקשר זה נציין שוב את השינוי שלפיו סמכות האסדרה תפוצל ככל הנראה בין רא״מ לרשות הסייבר – התפתחות שקשה לאמוד את השפעתה בנקודת זמן מוקדמת זו.

(ה) חוקתיות ומידתיות

גם אם נסכים כי פעילותה של המדינה להבטחת רמת הגנה נאותה על תשתיות קריטיות מפני פגיעות סייבר הינה חשובה, עליה לעמוד – ככל פעילות אחרת של המדינה – במבחני המידתיות. זאת, במיוחד לנוכח העובדה שחלק מהיבטיה של פעילות זו עלולים לפגוע בזכויות הפרט. נבחן עתה כמה פגיעות אפשריות כתוצאה מהמודל האמור, ונציג כלים לבדיקה אם מדובר בפגיעות מידתיות, כמו־גם ממצאים ראשוניים בדבר תוצאותיה של בדיקה מעין זו. יצוין כי נושא זה מצדיק מאמר בפני עצמו, ואנו נסתפק כאן בהצגת נקודות מרכזיות לשם הכרת הדיון והנעתו.

ראשית, ניתן לטעון כי פעולותיה של רא״מ (ובהמשך – של רשות הסייבר) פוגעות **בזכות הקניין** ו**בחופש העיסוק** של הפירמות המוסדרות – שתי זכויות אשר מוגנות בחוקי־יסוד. באשר לפגיעה בקניין,[255] מכיוון שחלק מהגופים המושפעים מההחלטות של רא״מ ורשות הסייבר הינם פרטיים, השתה של חובות, הגבלות ועלויות עליהם על־ידי הגוף הממשלתי מהווה פגיעה בקניינם. באשר לפגיעה בחופש העיסוק, הצורך של הגופים המוסדרים להישמע להוראות המדינה מתנגש בזכותם ״לעסוק בכל עיסוק, מקצוע או משלח יד״.[256] הניתוח החוקתי בעניין שני טיעונים אלה דומה, ובשני המקרים השאלה העיקרית נוגעת במידתיותם של הצעדים הננקטים: האם הצעדים האמורים אכן משרתים את הגשמת היעד של הבטחת עמידותה של התשתית מפני התקפות? והאם אי־אפשר להגשים יעד זה באמצעי פוגעני פחות?[257] אם אכן יש בצעדים האמורים כדי להגן במידה משמעותית על התשתיות האמורות, אזי סביר להניח שהטענות החוקתיות ייסוגו.

---

254 Coldebella & White, לעיל ה״ש 233, בעמ׳ 241 (“A centrally planned, one-size-fits-all regulatory scheme would almost certainly eliminate useful, industry-developed security measures and replace them with an ill-fitting, nondynamic slate of requirements”).

255 ס׳ 3 לחוק־יסוד: כבוד האדם וחירותו.

256 ס׳ 3 לחוק־יסוד: חופש העיסוק.

257 ס׳ 8 לחוק־יסוד: כבוד האדם וחירותו; בג״ץ 3477/95 **בן־עטייה נ׳ שר החינוך, התרבות והספורט**, פ״ד מט(5) 1, 12–13 (1995). מנקודת־מבט חוקתית עשויות לעלות שאלות חשובות נוספות לגבי המודל הישראלי, כגון אם ההגבלות הקיימות הן ״בחוק״ או ״לפי חוק... מכוח הסמכה מפורשת בו״ (ס׳ 8 לחוק־יסוד: כבוד האדם וחירותו). לעניין משמעותו של המונח ״הסמכה מפורשת״ ראו בג״ץ 6824/07 **מנאע נ׳ רשות המסים**, פ״ד סד(2) 479, 498–499 (2010).

עוד נציין כי ייתכן שתתקבל הטענה כי אין כלל פגיעה בזכות לקניין ובחופש העיסוק, שכן החברות האמורות – כבעלות רישיון מהמדינה להפעיל את התשתיות – קיבלו ממנה זכות מותנית, וההתנאה כוללת את הסכמתם של מקבלי הרישיון מראש לתנאי הרישיון (אשר עשויים להשתנות מזמן לזמן), הכוללים גם התייחסות לפיקוח המדינה בנושאי אבטחת הסייבר, מה־גם שמדובר בגופים אשר מוגדרים לעיתים ״דו־מהותיים״ ועל־כן כפופים לאסדרה ולחובות מן המשפט הציבורי.[258] ניתן אף לסבור כי בהטלת החובות האמורות לא תהיה פגיעה בזכות הקניינית, תוך הסתמכות על תפיסה קניינית ״ריאליסטית״ שלפיה זכות הקניין של הגופים האמורים כוללת אחריות ואף חובה להגן על מערכותיהם בדרך האמורה.[259]

אולם בתשובה שלעיל – גם אם נקבל אותה, ואין אנו מכריעים בכך – אין די. שאלת החוקתיות והמידתיות נוגעת גם בזכויות־יסוד אחרות הנפגעות באותה אסדרה. כך, למשל, יש להתייחס לאתגרים שהמודל הישראלי מציב לזכות לפרטיות. זכות זו נכללת אף היא בחוק־יסוד: כבוד האדם וחירותו,[260] מעבר לחוק הייעודי שהוקדש לה, הוא חוק הגנת הפרטיות. כאן הפגיעה החוקתית היא לא בבעלי התשתיות, אלא במשתמשיהן, ועל־כן אי־אפשר להיעזר בטיעון הנגדי שצוין לעיל בדבר הרישיון המותנה. במקרה שלפנינו יש פוטנציאל משמעותי לפגיעה בזכות הפרטיות. נזכיר כי חלק ניכר מחברות התשתיות באות במגע ישיר עם צרכנים, וכתוצאה מכך אוספות מידע רב הנוגע בחייהם האישיים. הדוגמה הקיצונית ביותר היא חברות התקשורת. לחברות אלה יש גישה ישירה לנתוני תקשורת המאפשרים שרטוט מדויק של חיי האדם על בסיס המקורות שמהם הוא שואב מידע. מעבר לכך, לנציגי המדינה האוכפים את אבטחת הסייבר (אשר יהיו נציגי רא״מ גם לפי המתווה החדש) יש גישה לחברות התקשורת המאפשרת ממשק עם התקשורת עצמה שהפרט מנהל באמצעות התשתית. כך או כך, פוטנציאל הפגיעה בפרטיות הוא משמעותי ביותר.[261]

שאלת הפגיעה בפרטיות עשויה להיות מהותית בבחינת המודל הישראלי, אך בירורה מחייב מידע נוסף על אופי פעולתה של המדינה, אשר אינו מצוי בידינו בהיותו חסוי. אחת הבעיות המרכזיות שעלולות להתעורר במודל הישראלי, אשר כולל פיקוח ישיר של גוף ממשלתי על מתקני התשתיות הקריטיות, היא מידת התערבותה של המדינה בגוף המונחה. ככל שנציגי המדינה מצויים דרך קבע ובאופן פיזי אצל הגופים המונְחים ו/או נהנים מגישה למערכות הממוחשבות של אותם גופים (בין היתר לצורך עריכת ביקורות), הם עשויים להיחשף אגב

---

258 לעניין הרישיון המותנה והשפעתו על הפגיעה בזכות הקניינית ראו בג״ץ 4806/94 **ד.ש.א. איכות הסביבה בע״מ נ׳ שר האוצר**, פ״ד נב(2) 193, פס׳ 5 לפסק־דינו של השופט זמיר (1998). לעניין ההגדרה של גוף דו־מהותי ודרך ההתייחסות המשפטית אליו ראו ע״א 3414/93 **און נ׳ מפעלי בורסת היהלומים (1965) בע״מ**, פ״ד מט(3) 196 (1995).

259 ראו חנוך דגן **קניין על פרשת דרכים** 185 (2005). לאימוץ עמדה זו בפסיקה ראו ע״א 8622/07 **רוטמן נ׳ מע״צ – החברה הלאומית לדרכים בישראל בע״מ**, פס׳ 78–87 לפסק־דינו של השופט פוגלמן (פורסם בנבו, 14.5.2012).

260 ראו ס׳ 7 לחוק־יסוד: כבוד האדם וחירותו.

261 שאלת הפגיעה בפרטיות שנוצרת בהקשרים אלה נדונה לא מעט בספרות. לסקירה ראו Bambauer, *Sharing*, לעיל ה״ש 174, בעמ׳ 469–472, 477–479.

עבודתם למידע רגיש המצוי בידי החברה הפרטית.[262] הקִרבה של אנשי הגוף המדינתי המפקח למידע אישי, ועימה הפוטנציאל לפגיעה בפרטיות, הינה גורם שיש לתת לו את הדעת ולאזנו עם מסכת היתרונות שהמודל הישראלי אמור לאפשר. מובן שהמפתח לאיזון האמור (לאחר זיהוי מדויק של אופי הפגיעה בזכות הפרטיות בהקשר זה) טמון במושג המידתיות: נדרשת בדיקה בדבר האפשרות להפעיל חלופות פוגעניות פחות (כגון העברת מידע בין הגופים באופן ישיר), בהינתן המודל הספציפי שבו נעשה שימוש לצורך מתן הגנת סייבר נאותה בתחום התשתיות.

נקודה אחרונה שנציין בעניין שיח הזכויות והמידתיות אינה נוגעת בזכות־יסוד דווקא, אלא בחשש מפני פעולה שלטונית לא־ראויה. המנגנונים המשפטיים והטכנולוגיים שנדונו כאן – ובעיקר העובדה שהם אפופים סודיות – פותחים פתח להסדרת־יתר (overreach).[263] הם מעוררים חשש לגידול זוחל (המכונה creep) של סמכויות המדינה, שעלול להוביל לחתירה תחת שלטון החוק. ראוי להזכיר כי בישראל עומדות לגוף המוסדר, על־פי חוק הביטחון, כמה אפשרויות לערער על החלטות הנוגעות בדרך שבה הוא נדרש להגן על תשתיותיו מפני מתקפות סייבר.[264] נוסף על כך, העניין כפוף לביקורתו של מבקר המדינה.[265] עם זאת, קיים עדיין החשש שבכלים אלה אין כדי לעצור את זליגת כוחה של המדינה אל מעבר להרשאה הנתונה לה בחוק. מובן שגם בסוגיה זו מידתיות היא המפתח לניתוח: האם ריכוז הסמכויות ועוצמתן אכן נחוצים להתמודדות עם האיום או שמא ניתן לעשות כן באמצעי שסכנותיו פחותות?

ו. המודל המוצע

נגבש עתה את הביקורות שהובאו לעיל לכלל המלצות בדבר הצעדים שראוי לנקוט לשם הסדרת הגנת הסייבר בתשתיות חיוניות, תוך שאנו מביאים בחשבון את שלושת הפרמטרים הבאים לצורך הערכת הסיכון וגיבוש הצורך בהתערבות: השלכותיה של ההתקפה, פגיעותן של המערכות והיקף האיום.[266] לנוכח הסודיות האופפת רבות מהפעולות הנדונות כאן, מתן המלצות מדויקות הינו משימה בלתי־אפשרית, שכן דרוש עדיין מחקר נוסף כדי להבין אילו מהבעיות שצוינו לעיל אקוטיות יותר. אולם נראה כי בכמה מקומות הטענות, החששות

262 סמכות מעין זו כבר קיימת לכוחות הביטחון ככל שהדבר נוגע בבעלי רישיון למתן שירותי תקשורת, וזאת על־פי ס׳ 13(ב)(2) לחוק התקשורת. אולם ראוי לבדוק הכרה בכל סמכות נוספת לביצוע פעולות מעין אלה.

263 ראו Rosenzweig, לעיל ה״ש 2, בעמ׳ 7.

264 ס׳ 10א ו־11 לחוק הביטחון.

265 ס׳ 22 לחוק הביטחון.

266 ראוי בהקשר זה לציין מודל שהוצע על־ידי ד״ר גבי סיבוני. סיבוני הציע להקים ארגון לאומי להגנת סייבר בהיבטים האזרחיים, אשר יתווה מדיניות בנוגע להגנת סייבר על המגזר האזרחי ויפעל למימושה. לפי הצעה זו, הארגון יספק הנחיה מקצועית בתחום ההגנה האזרחית במרחב הסייבר; יהווה את גוף מטה הסייבר הלאומי; יהיה גוף התגובה הלאומי במרחב האזרחי שמחוץ למדינת־ישראל; ויופקד על חקירת תקיפות סייבר במגזר האזרחי. גבי סיבוני ״המענה הלאומי להגנה האזרחית בסייבר: המלצות למקבלי החלטות״ **המכון למחקרי בטחון לאומי** (2013) heb.inss.org.il/index.aspx?id=4354&articleid=5904.

והביקורות שהובאו במאמר מאפשרים בכל־זאת מתן המלצות. מכל מקום, התרומה המרכזית בחלק זה טמונה בהצגת המתחים בין התועלות והחסרונות שצוינו לעיל, והדרך שבה הם מתקשרים למסקנות קונקרטיות. נדגיש כי מקוצר היריעה הדברים מובאים באופן ראשוני בלבד, וכי בשנים הקרובות יהיה צורך לעיין בדברים שוב לנוכח השינויים החקיקתיים והאסדרתיים שמקורם בכניסתה של רשות הסייבר לפעולה בהקשר זה.

נפתח בכמה תובנות שנראה כי אין עליהן מחלוקת: קיים סיכון לתקיפות סייבר מתמשכות על תשתיות חיוניות, והן עלולות להסב נזק משמעותי. נראה כי החברות הפרטיות אשר מפעילות תשתיות אלה לא ייתנו מענה מספק לסיכון זה לבדן ומרצונן החופשי. כמו־כן, אף שבעניין זה אין קונסנזוס, נראה כי הסדרה לאחר מעשה באמצעות קנסות או אחריות שתיבחן על־ידי בית־המשפט אינה רצויה ואינה יעילה. עד כאן נדמה כי הכיוון של הסדרה מראש שנקט המְאַסדר הישראלי הינו בעיקרו הנכון, ואינדיקציה לכך היא התכנסותן של כמה מדינות נוספות לכיוון זה.

ניתן להמשיך ולומר, בזהירות הראויה, כי היות שבמקרים רבים ההסדרה האמורה משפיעה על זכויות־יסוד, הצורך בעמידה במבחני המידתיות מעורר קושי משמעותי באימוץ תשתית אסדרתית כוללנית אשר חובקת את כל בעלי התשתיות, כפי שנעשה בישראל. מכיוון שהֶקשרים שונים יוצרים חששות שונים, מצד אחד, וכן מתווה אחר של השלכות, פגיעות והיקף איום, מצד אחר, יש צורך במערך אסדרתי מודולרי אשר ישתנה מהקשר להקשר. כבר ראינו כי בישראל, ובוודאי בעולם, נעשים צעדים בכיוון זה. יצוין כי מתווה התשתיות החיוניות הישראלי כבר אינו פשוט או מצומצם, וכולל מאות גופים (שחלקם מוסדרים בחוק הביטחון וחלקם אינם מוסדרים בו). על־כן מתווה מדורג יותר – שייצור כמה סוגים של תשתיות ויתאים לכל אחד מהם מערך של זכויות, חובות ודרישות – הוא צורך השעה. במידה מסוימת ההבחנה במסגרת הוראת־השעה בין הגופים בתוספת הרביעית לבין אלה שבחמישית הינה צעד בכיוון מבורך זה.

בהקשר זה ראוי להעלות גם את סוגיית הסודיות. לגישתנו, גם זו צריכה להיות מודולרית; בהקשרים מסוימים חשוב לזרות אור על פעולות המדינה או לכל־הפחות לאפשר פיקוח וביקורת עליהן, במיוחד לנוכח הפגיעה האפשרית בזכויות וכן לנוכח העובדה שסודיות אינה מובילה תמיד לרמת הגנה מיטבית. גם כאן העברת חלק מהפעילות אל מחוץ לתחום סמכותה של רא״מ, ולפיכך אל מחוץ לתחום סמכותו של שירות הביטחון הכללי, עשויה להיות צעד חשוב בכיוון זה.

מעבר לכך, המענה שניתן בישראל לשלושת האתגרים המרכזיים – **העברת מידע**, **העברת ידע** ובעיית **ההשקעה בחסר** – חייב להשתנות. יתרונו של המתווה הישראלי נעוץ באלגנטיות ובפשטות שבו. אולם לנוכח הביקורות והקשיים השונים שנדונו נראה כי אין מנוס ממעבר למודל מורכב יותר. לעניין **העברת המידע** נראה, לנוכח כשלים שונים, כי על המדינה להמשיך לנקוט צעדים שיובילו להעברתו בין הגופים – הן בשגרה והן בזמן־אמת. לפיכך מומלץ שהמדינה תיצור מסגרות להעברת המידע, ואף תעניק חסינות מפני תביעות בגין העברת מידע זה כדי למתן את חששותיהן של החברות הפרטיות. עם זאת, החששות מפני פגיעה בפרטיות – במיוחד כאשר מידע אישי עשוי להגיע לידי המדינה – מצדיקים את חסימת גישתה של המדינה אל המידע האמור. משמע, יש לבחון יישום של מודל מידתי המאפשר את העברת המידע בין

הגופים הפרטיים (ושוב, תוך הקפדה על פרטיותם של מושאי המידע ככל האפשר) בעידוד המדינה, אך לא בהכרח בתיווכה.

הנושא של **העברת ידע**, במטרה לצמצם פערים הנוצרים לכאורה בין מפעילי התשתיות, מאתגר אף הוא. המנגנון הקיים בישראל אפקטיבי, אך כרוך בבעיות. לפיכך בנושא זה ראוי ללמוד דווקא ממדינות אחרות, אשר יוצרות שולחנות עגולים ומערכות שבהן הגופים הפרטיים עובדים יחדיו על־מנת להעביר את המידע בינם לבין עצמם. גם המדינה שותפה להליך זה, אך לא מעבר לכך. משמע, למדינה אין הסמכות להכתיב את הסטנדרט, אך היא יכולה בהחלט לתת משוב על הנעשה ולתרום מהמומחיות ומהניסיון שהצטברו אצלה. בדרך זו יוכל גם המידע המצטבר בקרב הפירמות לזרום לכיוון פירמות אחרות.[267]

לבסוף, בבואנו להתמודד עם החשש שהחברות **ישקיעו בחסר** בהגנת הסייבר, עלינו לזכור את החשיבות בשימור מעורבותן של החברות עצמן. לא נרצה שתושרש בקרבן תרבות ה״צ׳ק ליסט״, ונרצה לשמר את התגובה המהירה האופיינית למגזר הפרטי. לפיכך רצוי להימנע מלנסות להתגבר על כשל זה באמצעות מנגנון שינחה את מפעילי התשתיות באופן ישיר באשר להגנות שיש לנקוט. תחת זאת, ולנוכח בעיות אחרות שציינו, ראוי להמיר במקרים רבים את ההנחיה הנוקשה מראש בעריכת ביקורות אשר יוודאו כי המפעילים עומדים בסטנדרט תפעולי מספק. ביקורות אלה צריכות להיות בעלות שני פנים: בדומה למהלך שאומץ לאחרונה בדירקטיבה האירופית, על המדינה לדרוש מהגופים מידע על הצעדים שהם נוקטים, וכן לערוך ביקורות שמדמות תקיפות מסוגים שונים ובודקות מוכנות.[268] דוח מבקר המדינה שעסק במוכנותה של תהיל״ה[269] למתקפות שונות מהווה נקודת מוצא מעניינת לדיון זה.[270] הדוח חושף אומנם כשלים בניהול הפרויקט, אך מאידך גיסא מפנה זרקור נדיר אל פעולות רא״מ ואל יכולותיה הגבוהות בעריכת ביקורות אפקטיביות ביותר בנושא הגנת הסייבר. נראה כי יש לשמר יכולת זו ולקוות שזו תתקיים גם אצל רשות הסייבר. במצב של איתור כשלים כאמור תוכל המדינה לדרוש את תיקונם ואף לאיים על התשתיות האמורות בביטול רשיונן. חשיפת הכשלים גם תביא לידי פגיעה ציבורית ותדמיתית שממנה יבקשו החברות להימנע. יצוין כי במקרים מסוימים, כאשר יש חשש לפגיעה בפרטיות משום שעריכת הביקורת מחייבת מתן גישה למידע אישי, ראוי שעריכת הביקורות תועבר לגוף שלישי/אזרחי, אשר ידווח למדינה על מחדלים וכשלים שיימצאו.[271] זאת, בשל החשש המוגבר שנוצר כאשר מידע אישי מצוי בידי המדינה.

---

267 להצגת בעיות המתעוררות במודל מעין זה ראו Rachel Nyswander Thomas, *Securing Cyberspace Through Public-Private Partnership: A Comparative Analysis of Partnership Models* 26–30 (2012), *available at* http://csis.org/files/publication/130819_tech_summary.pdf. להצעה למודל משופר ראו שם, בעמ׳ 53.

268 ראו ה״ש 154 והטקסט שלידה.

269 תהיל״ה הוקמה כיחידה במשרד האוצר שפעלה להקמת תשתיות כלל־ממשלתיות שמסייעות למשרדי הממשלה להעניק שירותים לציבור, ועם הזמן נהפכה למערך ממשל זמין תחת התקשוב הממשלתי. על־אודות מערך ממשל זמין ראו e.gov.il/AboutUs/Pages/AboutUs.aspx.

270 מבקר המדינה **דוח שנתי 64ג – לשנת 2013 ולחשבונות שנת הכספים 2012** 1590 (2014).

271 לשינוי דומה שנערך בארצות־הברית, אשר העביר את היכולת לשמור כמויות רבות של נתוני תקשורת מהמדינה לידי חברות הטלפוניה, ראו Jennifer Steinhauer & Jonathan Weisman, *U.S. Surveillance in Place Since 9/11 Is Sharply Limited*, N.Y. Times, Jun. 2, 2015.

אולם ייתכנו בכל־זאת מקרים שבהם המדינה תחשוש כי הצעדים שהגופים הפרטיים נוקטים אינם מספקים, וכי מתקיימת השקעה בחסר. במקרים אלה על המדינה לאכוף את דעתה על הגוף הפרטי. אולם יש לוודא כי מצב דברים זה יהיה היוצא־מן־הכלל, ויישמר רק למקרים שבהם פגיעה עלולה לשאת השלכה קטסטרופלית ממש למתקנים (דוגמת מפעלים כימיים וגרעיניים, אשר אפילו בארצות־הברית מוסדרים בהסדרת־חובה). יתר על כן, גם במקרים אלה נדרשים מנגנוני פיקוח מדינתיים וחיצוניים על־מנת לוודא שמירה על זכויות האזרח כמו־גם העדר שיקולים זרים. לפיכך הפיקוח הראוי עשוי להצריך השתתפות של גוף מקצועי נוסף שיהיו חברים בו גם נציגי התעשייה או גורמים בלתי־תלויים. זאת, להבדיל מהמצב הנוהג כיום, שבו ערר על החלטת המדינה מוגש לגוף אשר כל חבריו הם עובדי מדינה או מזוהים עם הממסד.[272]

התייחסותנו האחרונה היא לתשתיות חיוניות המעניקות שירותי תקשורת, ובעיקר תקשורת נייחת וספקיות גישה למרשתת. בהקשר זה נראה כי אתגר ההגנה הינו כפול: ראשית, יש להגן על תשתית חיונית זו; שנית, התשתית האמורה משמשת לעיתים בסיס לתקיפה של תשתיות אחרות. דוגמה למערכת המיועדת לספק הגנה כפולה כזו היא מערכת ״איינשטיין 3״ בארצות־הברית שהוזכרה לעיל, אשר מנטרת את אמצעי התקשורת תוך חיפוש מתווים של תקיפות המיועדות לגופים ולתשתיות אחרים.[273] לנוכח הסכנה הכפולה מתחזקת ההצדקה לאפשר לרשויות המדינה לנטר גופים אלה בצורה מקיפה יותר. אולם דווקא בהקשר של גופים אלה עולים החששות הגדולים ביותר לפגיעה בפרטיותם של משתמשים, אשר פרטיהם יועברו למדינה כחלק מניטור זה. לפיכך ייתכן שתשתיות אלה מצריכות אסדרה ייחודית, כפי שגובשה באירופה,[274] הכוללת הסדרים מיוחדים (אשר יעוגנו בחוק) בדבר סמכותה של המדינה לגשת לתשתיות אלה ולמידע המצוי בהן אשר עשויים גם להיחשב מידתיים יותר במבחן החוקתי. בעניין זה הכוונה להותיר את אסדרתם של גופי תקשורת אלה דווקא בידי רא״מ מדאיגה, שכן מערכת אסדרתית זו משתייכת לזרוע מודיעין סודית אשר אינה מורגלת בנוהלי שקיפות (במידה רבה של צדק), אף שאלה נדרשים בהקשרים מסוימים, כגון במקרה דנן.

ז. סיכום

> ״מתגברים הניסיונות לבצע מתקפות סייבר על תשתיות המחשבים במדינת ישראל. מדי יום נעשים ניסיונות רבים לחדור למערכות המחשב של ישראל״ — כך הודה היום בפעם הראשונה ראש הממשלה, בנימין נתניהו. לדבריו, מטה

272 ס׳ 11(א) לחוק הביטחון.
273 ראו דיון לעיל ליד ה״ש 138–140.
274 ראו דיון לעיל בה״ש 155 ובטקסט שלידה.

הסייבר הלאומי ״פועל לבלום את הניסיונות הללו על ידי פיתוח מה שהייתי מכנה כיפת ברזל דיגיטלית לישראל להגנה מפני טרור מחשבים״.[275]

לעיתים העוצמה האמיתית של ביטוי רטורי גלומה לא ברעיון המפורש שהוא מביע, אלא במטפורות שהוא נזקק להן. מטפורות אלה גורמות לכך שהקורא או המאזין יקבלו על עצמם את עולם הדימויים של הדובר, על מכלול הנחותיו הנסתרות. בכך הטיעון הרטורי מנצח בקרב עוד לפני שהחל.[276] בהצטיידנו בתובנה זו, נתייחס עתה בזהירות לדברי ראש הממשלה כי מדינת־ישראל זקוקה ל״כיפת ברזל דיגיטלית״. על פניו, קריאה זו מביעה דאגה אמיתית של המדינה לאזרחיה, ומצביעה על כוונתה לנסות להגן עליהם מפני איומים חיצוניים המתרגשים עליהם – בליסטיים/קינטיים וקיברנטיים כאחד – באמצעות מערכת שתופעל על־ידי המדינה תחת מעטה בטחוני. החיבור המטפורי בין ״כיפת הברזל״ לסייבר מחזק את הקו בהסדרה הקיימת בישראל שלפיו למדינה יש – וצריך להיות – תפקיד פעיל בהגנה על תשתיות.

אך ראוי לדייק בדברים. האם אפשר לומר כך בפשטות שיכולת העמידה של גוף פרטי אל מול איום סייבר אפסית כמו יכולת העמידה של גופים פרטיים – יהיו מתוחכמים ככל שיהיו – בפני מתקפת גראדים? במקרה האחרון נראה כי תפקידה של המדינה ברור. אזרחים אינם ערוכים ואינם יכולים להקים מערכות ליירוט טילים ופגזים. פשיטא שהגנה כאמור הינה ״משאב ציבורי״ אשר מתפקידה של המדינה הריבונית להעניק. לעומת זאת, הטיעון כי על המדינה לתת מענה להגנה על תשתיות חיוניות בבעלות פרטית מפני מתקפות סייבר אינו פשוט או אינטואיטיבי באותה מידה.[277] יכולתן של החברות הפרטיות להגן על עצמן מפני מתקפות סייבר טובה לאין ערוך מיכולתן ליירט גראדים במעופם. לפיכך, בטרם ניישם את הקריאה להחלת ״כיפת ברזל דיגיטלית״, ראוי שנשקול לעומק את המודלים השונים להגנה על תשתיות מפני מתקפות סייבר, תוך דיון במגוון הגורמים שנסקרו ברשימה זו.

ראוי לציין כי קיימים רכיבים נוספים אשר רלוונטיים להסדרה כאמור אך לא נסקרו כאן. אחד מהם הוא ההיבט הבין־לאומי. היות שהמרשתת הינה מדיום חוצה גבולות, אך טבעי הוא שמתקפות סייבר אינן שמורות למדינה מסוימת. המידע והידע שנדונו לאורך עבודה זו יכולים אף הם לזרום בין מדינות, אם הללו יחפצו בכך ויראו בכך יעד משותף. אכן, יש צורך בהגברה ובשיפור של שיתופי־הפעולה של ישראל עם מדינות נוספות בעולם.[278] שיתוף־פעולה זה צריך להתבסס על שיתוף מידע בדבר מוכנות למתקפות סייבר ומניעתן, איתורן ותגובה עליהן, והפוגה והתאוששות מהן. מובן ששיתוף המידע בין הגופים חייב להיות מוגבל במידה מסוימת, באופן שיאזן בין הצורך לשמור על סודיות בנוגע לרמת ההגנה על תשתיות חיוניות ויעדים אסטרטגיים אחרים בישראל, מחד גיסא, לבין הצורך בשיתוף מידע לשם שיפור מכלול המערכות, מאידך גיסא. אולם סוגיה זו ראויה לדיון מעמיק ברשימה נפרדת.

---

275 מוטי בסוק ״נתניהו מודה: ישראל נתונה למתקפת סייבר; ׳נפתח כיפת ברזל דיגיטלית׳״ **TheMarker** 14.10.2012 www.themarker.com/news/1.1841996.

276 George Lakoff & Mark Johnson, Metaphors We Live By (2008).

277 לדיון מקביל ומעניין בקושי הטמון בשימוש במטפורה של מערכות הגנה אווירית בהקשר של סייבר ראו Rosenzweig, לעיל ה״ש 2, בעמ׳ 175; Sales, לעיל ה״ש 164, בעמ׳ 1518.

278 אכן, זה אחד היעדים המוגדרים בהחלטת ממשלה 2444, לעיל ה״ש 74 (ס׳ 8).

במאמר זה פרשנו את מאפייניה הייחודיים של ההגנה על תשתיות חיוניות מפני מתקפות סייבר, תוך שילובם עם הטיעונים המקובלים נגד אסדרה מדינתית מתערבת – הן מראש והן למפרע. סקירתנו הראתה כי יש טיעונים לא־מעטים נגד אסדרה מתערבת מראש, וכי זו אף אינה המגמה המקובלת במדינות מובילות. לנוכח זאת יש מקום לערוך שינויים במנגנון המופעל בעניין זה בישראל, ולעקוב אחר השינויים המתקיימים במערכת כבר עתה. אך מעבר לכך, יש מקום למחקר נוסף בתחומים אלה, וכמובן לפיתוח השיח הציבורי בסוגיה הנוגעת בכולנו – צרכנים, משתמשי טכנולוגיה ואזרחים במדינה ליברלית.