מערך הסייבר הלאומי – משרד ראש הממשלה

דו״ח הערכת השפעות אסדרה (RIA)

חוק הגנת הסייבר הלאומית, התשפ״ו – 2026

כתב וערך: רון גילרן
ראש תחום (מדיניות רגולציה)
אגף אסטרטגיה והתעצמות

ינואר 2026

תוכן העניינים

תוכן העניינים 2

תקציר מנהלים 3

פרק ראשון: רקע על הסוגייה והתהליך 6

א. רקע כללי והאינטרס המוגן 6

ב. המצב האסדרתי הקיים 6

ג. היקף ועומק התהליך 10

פרק שני – ניתוח הבעיה 11

א. מונחי יסוד בעולם הסייבר 11

ב. התופעה הבלתי רצויה 13

ג. הנזקים כתוצאה מהתופעה הבלתי רצויה 16

ד. הבעיה וגורמי השורש שלה 20

ה. סיכום 25

פרק שלישי – למידה מהעולם 27

א. עיקרי הממצאים 28

ב. הגדרת רגולציה מהעולם שתשמש כתשתית לגיבוש הרגולציה המקומית 36

ג. סיכום 39

פרק רביעי – גיבוש חלופות, ניתוח והשוואה 41

א. סיכום ביניים: הגדרת הבעיה והגדרת מטרות ההתערבות 41

ב. חלופות שנשקלו 42

ג. השוואה בין חלופות 49

ד. סיכום ובחירה בחלופה המועדפת 51

פרק חמישי – זיהוי וניתוח השפעות של החלופה הנבחרת 53

א. זיהוי השפעות (כללי) 53

ב. ניתוח השפעות כלכליות 54

פרק שישי – עיצוב החלופה הנבחרת 60

א. מודל האסדרה – ריכוזי מול מבוזר 60

ב. עיקרי האסדרה המוצעת 61

פרק שביעי - הגדרת יעדים וקריטריונים 70

נספח א': תיאור תהליך העבודה 73

נספח ב': תקיפות סייבר בולטות מן השנים האחרונות 83

תקציר מנהלים

בעשור האחרון הפך מרחב הסייבר לזירת עימות מרכזית, המציבה איום הולך וגובר על מדינות וארגונים בעולם, ועל ישראל בפרט. איום זה הופך מוחשי במיוחד נוכח התלות הכמעט מוחלטת של המשק המודרני במערכות דיגיטליות – תלות הכוללת גם את התשתיות והארגונים החיוניים שלנו, בתחומים כמו אנרגיה, בריאות, מים, תקשורת, שירותי הממשלה ועוד. מכיוון **שפוטנציאל הפגיעה במקרים אלו חורג מהנזק לארגון הבודד**, ועלול לפגוע בציבור ובמשק כולו, נדרש מענה מדינתי-לאומי לצורך הגנה על הרציפות התפקודית, היציבות הכלכלית והביטחון הלאומי של ישראל. **צורך זה הפך דחוף עוד יותר נוכח התגברות תקיפות הסייבר מאז ה-7 באוקטובר, וביתר שאת מאז מבצע 'עם כלביא'.**

מערך הסייבר הלאומי אמון על הגנת הסייבר של מדינת ישראל. ככזה, הוא שוקד זה מכבר על עבודת מטה מקיפה שתעריך את דרכי ההתמודדות הרצויות עם האיום, ותמליץ על דרך הפעולה העדיפה מנקודת מבט לאומית. בשים לב להיקף האיום וחומרתו, המגמות שנצפו במדינות מערביות בעלות שווקים מפותחים, והשונות ברמות הסיכון הנשקפות לארגונים שונים, ממליץ מערך הסייבר לקדם **חקיקה לאומית** להגנת מרחב הסייבר, שתהווה השדרה המרכזית של אסדרת התחום בישראל[1].

מסמך זה מציג סיכום של עבודת המטה שנעשתה לצורך ניסוח החוק. הוא כולל ניתוח של הבעיה המרכזית ושל גורמי השורש שלה ; מציע סקירה בינ"ל מפורטת על הנעשה בעולם ; סוקר את החלופות השונות שנבחנו ; ומציג את עיקרי החלופה המומלצת – חקיקה של חוק סייבר לאומי המחיל, בין היתר, אסדרה על ארגונים שיסווגו "חיוניים"[2].

עבודת המטה נמשכה למעלה משנתיים, וכללה תהליך היוועצות וסדרת דיונים מעמיקים עם משרדי הממשלה (בדגש על משרדי המשפטים והאוצר), המשרדים הרגולטוריים/היחידות המגזריות וגופי ביטחון, לצד שיחות עם מומחים מהאקדמיה, מהמגזר השלישי ומארגונים במשק. תהליך גיבוש החוק היה אינטנסיבי והצריך אלפי שעות עבודה במצטבר. פירוט אודות תהליך העבודה ניתן למצוא **בנספח א'.**

נוכח מורכבות הנושא, מספר השחקנים המעורבים, היותה של האסדרה המוצעת חדשה בישראל (גם אם מעוגנת ומבוססת היטב בהשוואה בינלאומית) – הוחלט לבצע תהליך RIA מעמיק. במסגרת זו הושם דגש מיוחד הן על השוואה מעמיקה ומפורטת לבנצ'מארק הבינ"ל, והן על ניתוח כלכלי מדוקדק, המבסס היטב את התועלות של התערבות ממשלתית אל מול העלויות של המשך המצב הקיים.

---

[1] במובן זה, החוק המוצע משלים את החוק להסדרת הביטחון בגופים ציבוריים (תשנ"ח-1998), העוסק, בין היתר, בהגנת הסייבר של תשתיות מדינה קריטיות (תמ"ק).

[2] יודגש כבר עתה כי "ארגון חיוני" כהגדרתו באסדרה המוצעת אין משמעו "מפעל חיוני" כהגדרתו בחוק שירות עבודה בשעת חירום.

כפי שישתקף בנתוני הדו״ח **(פרק שני), ישראל היא אחת האומות המותקפות ביותר בסייבר בעולם,** והיא חווה את איומי הסייבר הגלובליים בעצימות גבוהה במיוחד. לפי דו״ח ההגנה הדיגיטלית של מייקרוסופט לשנת 2025, **ישראל היא המדינה השלישית בעולם במספר התקיפות** במחצית הראשונה של השנה, בראש ובראשונה כלפי מגזר ה-IT[3].

תקיפות אלה מסבות לכלכלה נזק עצום הנאמד במיליארדי ₪ מדי שנה, ועשויות לפגוע באופן משמעותי ברציפות התפקודית של המשק, הן בשגרה והן בחירום. על אף הנזקים הפוטנציאליים והממשיים לאינטרס הציבורי כתוצאה מתקיפות אלה – ארגונים רבים אינם נוקטים באמצעים מספקים להגן על עצמם בסייבר, ובכך מגבירים משמעותית את ההסתברות למתקפות סייבר מוצלחות ובעלות השלכות קשות. בעיה זו נעוצה בארבעה גורמי שורש שונים: **היעדר מודעות; א-סימטריה של המידע; החצנות שליליות; והיעדר דיווח ושיתוף מידע.** כל אלה מועצמים ע״י פערים במודל האסדרה הנוכחי, ובראשם חוסר אחידות בסמכויות ובמשאבים של יחידות הסייבר המגזריות במשרדי הממשלה. בנוסף, בולטת בהיעדרה מסגרת חוקית בהירה המגדירה את חלוקת האחריות, הסמכויות וממשקי העבודה בין יחידות אלה לבין מערך הסייבר.

לדידנו, כשלי שוק אלה מצדיקים התערבות ממשלתית כלשהי בתחום. ממצאי ההשוואה הבינ״ל המעמיקה שביצענו מראים בבירור כי התערבות זו לבשה צורה של **אסדרה חוקית** ברוב מכריע של המדינות המערביות, וספציפית בכל אחת מ-5 המדינות שנבדקו במסגרת הלמידה הבינ״ל. את עיקרי הממצאים של ההשוואה הבינ״ל ניתן למצוא **בפרק השלישי** לדו״ח; הסקירה המלאה מצורפת לדו״ח בקובץ נפרד.

כדי לטפל בשורשי הבעיה נשקלו חלופות שונות **(פרק רביעי)**, בהן אסדרה עצמית, תביעות אזרחיות, תמריצים כלכליים ורגולציה על מוצרים. מהניתוח עולה כי מנגנונים אלה אינם מספקים מענה מיטבי לסיכון בארגונים חיוניים, בשונה מהמגזר העסקי הכללי. כיום, הגורם האנושי וממשקיו מהווים פרצה מרכזית המאפשרת תקיפות סייבר. לכן, הסתמכות בלעדית על פתרונות טכנולוגיים או על כוחות השוק מותירה ארגונים חשופים לאיומים שמקורם בהיעדר תהליכים סדורים או בטעויות אנוש. מסיבה זו, חלופת האסדרה נמצאה כאפקטיבית ביותר: היא מפחיתה סיכונים בארגונים חיוניים, מטפלת בכשלי שוק וסוגרת את הפערים הרגולטוריים, תוך הלימה למגמות הבינלאומיות.

הפרק החמישי מציע ניתוח מפורט של המשמעויות הכלכליות של החלופה הנבחרת. אל מול עלות שנתית של כ-12 מיליארד ₪ מנזקי תקיפות סייבר, העלות הכלכלית לארגון בודד צפויה לנוע בין 0 ל-1.9 מלש״ח, והיא תלויה הן בגודלו של הארגון והן ברמת הבשלות הנוכחית של הגנת הסייבר שלו. **ככל שארגונים מוגנים היטב בסייבר כבר במצב הנוכחי, העלות השולית עבורם כתוצאה מן האסדרה צפויה להיות נמוכה יותר.**

[3] https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf; עמ׳ 10, 46-43.

בהתאם לממצאים המפורטים בדו״ח אנו מעריכים כי פעולות ההגנה שינקטו מכוח האסדרה יביאו לחיסכון משמעותי בעלויות הנובעות מתקיפות סייבר. בנוסף, לחלופת האסדרה תועלות רבות אחרות שאינן ניתנות לחלוטין לכימות, כמו הגנה על חיי אדם, שמירה על רציפות תפקודית של המשק, שמירה על פרטיות, הגברת אמון הציבור בשירותים הדיגיטליים, וישור קו של ישראל עם המקובל בעולם. הגם שמספר הארגונים החיוניים עליהם יחול החוק עדיין לא ידוע במדויק, אנו סבורים כי מדובר ברגולציה בעלת השפעה משקית.

הפרק השישי עוסק בכמה היבטים מעשיים יותר של החלופה הנבחרת. ראשית, הוא עוסק במודל האסדרה. המודל שאנו מציעים לאמץ הוא **מודל מבוזר**, לצד הגדרה ברורה יותר של סמכויות ותפקידי מערך הסייבר כגורם הלאומי המוביל והמתכלל את ניהול הגנת הסייבר הלאומי. היחידות המגזריות יהיו אמונות על שיפור רמת הגנת הסייבר המגזרית בהתאם למדיניות ואסטרטגיית הגנת הסייבר הלאומית; קידום אסדרה מגזרית מעבר לחובות הלאומיות; מיפוי הארגונים במגזר ואיסוף נתונים; ביצוע פיקוח ואכיפה בפועל, ועוד. תפקידי מערך הסייבר יכללו קידום מדיניות ואסטרטגיה לאומית; ריכוז תמונת המצב הלאומית של הגנת הסייבר; חיזוק החוסן הלאומי בהגנת סייבר וקידום התמודדות עם תקפות סייבר; הנחייה מקצועית של היחידות המגזריות, ועוד.

הרגולציה צפויה לחול על אותם ארגונים שיענו לתנאי ההגדרה ״ארגונים חיוניים״ במגזרים הכלולים בחוק. המגזרים נקבעו בהתאם לבנצ׳מארק הבינ״ל, עם התאמות מינימליות לשוק הישראלי: משרדי הממשלה; תקשורת; אנרגיה; בריאות; כימיקלים, רעלים וחומרים מסוכנים; מים וביוב; תחבורה; רשויות מקומיות; משק כללי (מזון); שירותים דיגיטליים ושירותי אחסון; וחקלאות. הארגונים החיוניים בכל מגזר נקבעו לפי **תבחינים מגזריים יעודיים** שגובשו בהיוועצות עם היחידות המגזריות. זאת, בניגוד לאפשרות של תבחין גורף חוצה-מגזרים (למשל, ״ארגונים בינוניים ומעלה״ כפי שמחייבת האסדרה האירופאית) שלטעמנו לא בשלה העת ליישמו בישראל.

על הארגונים החיוניים שבחוק יחולו שתי חובות עיקריות: ראשית, **חובה לנהל את סיכוני הסייבר** שלהם, זאת ע״י ביצוע דרישות רמת ההגנה שבחוק; ושנית, **לדווח על אירועי סייבר משמעותיים** כפי הגדרתם בחוק. לרגולטורים המגזריים, לצד שאר סמכויותיהם, תהיה סמכות לתת הוראות לגופים שבאחריותם בעת תקיפת סייבר חמורה, ובמקרים מסוימים (בעלי היבטים לאומיים כמוגדר בחוק) – סמכות זו תהיה של מערך הסייבר הלאומי.

לסיכום: חלופת האסדרה תתרום משמעותית ליצירת סטנדרט אחיד של ניהול סיכונים וחובת דיווח, תיישר קו עם הנורמות הבינלאומיות ודרישות ההגנה הנגזרות ממנה, ותבטיח כי הגנת הסייבר בארגונים חיוניים תנוהל כאינטרס לאומי מחייב ולא כשיקול עסקי וולונטרי. דו״ח הפורום הכלכלי העולמי (WEF 2024) מספק תימוכין אמפיריים חזקים ליעילות חלופת האסדרה: 60% מהמנהלים הבכירים מסכימים כיום כי רגולציה בתחומי הגנת הסייבר מפחיתה בפועל את הסיכון באקו-סיסטם של הארגון שלהם – עלייה של 21% בהשוואה לשנת 2022[4]. הדו״ח מדגיש כי ״רגולציה אפקטיבית מרימה את כל הסירות״ (Effective regulation lifts all boats), קרי – היא מייצרת רשת ביטחון בסיסית לא רק בארגונים המפוקחים, אלא מעלה את רמת ההגנה בכלל המשק.

[4] https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf, עמ׳ 31.

פרק ראשון: רקע על הסוגייה והתהליך

א. רקע כללי והאינטרס המוגן

בעשור האחרון הפך מרחב הסייבר לזירת עימות מרכזית, המציבה איום הולך וגובר על מדינות וארגונים ברחבי העולם, ועל מדינת ישראל בפרט. איום זה הופך מוחשי במיוחד נוכח התלות הכמעט מוחלטת של החברה והמשק המודרני במערכות דיגיטליות. עבור מדינת ישראל, המצויה תחת איומים ביטחוניים משמעותיים, פגיעות בנכסי הסייבר של ארגונים חיוניים הופכת לאיום ישיר על היכולת לספק שירותים כאלה לאזרחים (בריאות, מים, אנרגיה, תחבורה וכו') – בשגרה ובחירום כאחד.

האינטרס הציבורי המוגן במסגרת זו חורג אפוא מדליפת מידע גרידא של ארגון כזה או אחר; הוא נוגע לליבת החוסן הלאומי ולביטחונו האישי של האזרח: פגיעת סייבר במתקן תשתית או במוסד רפואי מרכזי אינה רק כשל טכני, אלא אירוע העלול לפגוע ברציפות התפקודית של המשק, כמו גם באמון הציבור במדינה ובמוסדותיה.

היות ובמקרים אלה **פוטנציאל הפגיעה חורג מהנזק שעשוי להיגרם לארגון הבודד הנתקף, ועלול להביא לפגיעה רחבה יותר בציבור או במשק** – נדרש מענה מדינתי-לאומי (רגולטורי, אחר או משולב), על מנת להגן על הרציפות התפקודית של ישראל, יציבותה הכלכלית, ובכללו של דבר – על ביטחונה הלאומי.

ב. המצב האסדרתי הקיים

בישראל, הגוף המרכזי האמון על קידום הגנת מרחב הסייבר במשק (ובכלל זה תשתיות קריטיות וארגונים חיוניים) הוא **מערך הסייבר הלאומי** (גם: **"מס"ל"**). המערך, שהוקם מכוח החלטת הממשלה 3270[5], איחד בתוכו למעשה שני גופים ותיקים יותר – מטה הסייבר והרשות הלאומית להגנת הסייבר, וככזה הוא ממלא שורת תפקידים.

בראש ובראשונה, המערך מנחה בתחום הגנת הסייבר את **תשתיות המדינה הקריטיות** שהוגדרו בחוק (מכאן ואילך: **"תמ"ק"** או **"גופי תמ"ק"**) – קבוצה מצומצמת של כמה עשרות גופים הנחשבים לנכסים הקריטיים ביותר של המדינה. הוא עושה זאת באמצעות מתן הנחיות על מערכות ממוחשבות חיוניות בכל הנוגע לפעולות אבטחה, לרבות הנחיות בעניין בקרה ודיווח. סמכות זו של המערך מעוגנת בחוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998[6].

[5] לסקירה של החלטות הממשלה הרלוונטיות, ראו: https://www.gov.il/he/Departments/news/govdecisions

[6] https://www.nevo.co.il/law_html/law01/111m1_001.htm

במקביל, המערך אמון על קידום וחיזוק החוסן **של המשק** בסייבר, ובכלל זה על העלאת הכשירות של **מגזרים** וגופים. תפקיד זה עוגן בהחלטת הממשלה 2443[7] שהתקבלה בשנת 2015. ההחלטה קבעה כי *"אסדרת היערכות **הארגונים** במשק בתחום הגנת הסייבר תיעשה [...] באמצעות העצמה של הרגולטורים הקיימים..."*. במודל זה, נדרשו משרדי הממשלה השונים להקים יחידות מגזריות ייעודיות להגנת סייבר, שתפקידן להסדיר ולאסדר את הגנת הסייבר בארגונים החיוניים שתחת אחריותם. ההחלטה קבעה כי יחידות אלה תפעלנה "בהנחיה מקצועית של הרשות הלאומית להגנת הסייבר" – שלימים הפכה למס"ל.

מערך הסייבר מינה **מנחה סקטוריאלי** לכל יחידה המגזרית שהוקמה (ככל שהוקמה), שתפקידו להוות גשר מקצועי וניהולי בין המערך והמגזר. בין היתר, המנחה מזהה מגמות, פערים ועיסוקים במגזר. באמצעות קשר ישיר אל מול מנהל היחידה המגזרית, הוא מצביע על עוגנים שיש להתייחס אליהם בתכנית העבודה, ומשמש גורם מקשר בין היחידה לגורמים רלוונטיים במערך. המנחה המגזרי גם אוסף נתונים כמותיים מהנעשה במגזר, ואלה מאפשרים להעריך את רמת ההגנה בסייבר בכל מגזר בנפרד וכן ברמה הלאומית. חלק מהיחידות המגזריות מפעילות, לבד או בשיתוף מס"ל, SOCמגזרי[8].

יצויין כי בחלוף עשור מהחלטת הממשלה 2443, רק חלק ממשרדי הממשלה הקימו יחידות מגזריות יציבות ומתפקדות, בעוד בחלק אחר של המשרדים הוקמו יחידות לפרק זמן קצר או שלא הוקמו כלל. על פי רוב, היה הדבר תלוי בקשב של המשרד הממשלתי הספציפי לסיכוני סייבר ולהפנמת הסיכון; ליכולתו של המשרד להקדיש לנושא משאבי תקציב וכח אדם; וגם למידה שבה כבר היו למשרד מנגנוני חקיקה ורגולציה שהיה ניתן להחיל על תחום הגנת הסייבר.

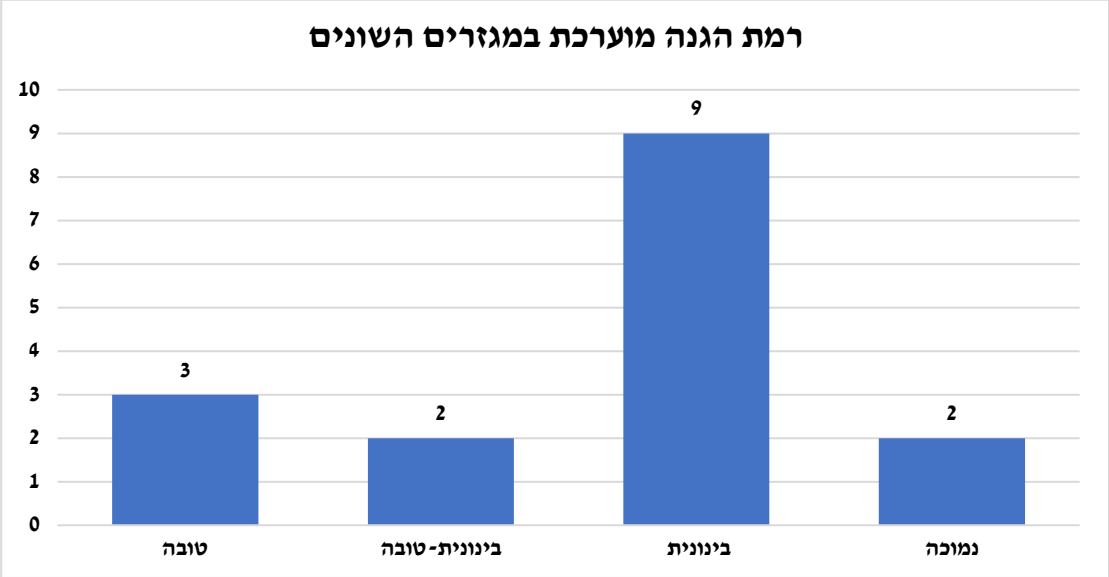
דפוס הפעולה שתואר כאן מבטא למעשה **מודל מבוזר מאוד**, שבו כל רגולטור ממשלתי אמון על קידום הגנת הסייבר בגופים שתחת אחריותו, באמצעות הכלים הרגולטורים והסמכויות שהוקנו לו מראש (ככל שהוקנו כאלה), באמצעות ליווי מקצועי של מס"ל. ואולם, **מאחר ולכל רגולטור סט <u>שונה</u> של סמכויות שהוקנו לו בחקיקה היעודית שלו (כאמור – במידה והוקנו כאלה מלכתחילה) – קיימת שונות רבה בין היחידות המגזריות ביכולתן להעניק מענה מיטבי להגנת הסייבר במגזרים שלהן, ובראיה כלל-משקית, זו נותרת במידה רבה מוגבלת.**

סקר שביצעה מחלקת מדידה ומצפן במערך הסייבר, בשילוב עם הערכות מומחים, מעלה כי מתוך 16 מגזרי משק, 5 נמצאים ברמת הגנה בינונית-טובה או טובה, תשעה ברמת הגנה בינונית, ושניים ברמת הגנה נמוכה[9].

[7] החלטה 2443: https://www.gov.il/BlobFolder/news/govdecisions/he/2443.pdf; החלטה 2444: https://www.gov.il/BlobFolder/news/govdecisions/he/2444.pdf

[8] SOC – Security Operations Center, מרכז אבטחת מידע.

[9] המדידה מתייחסת בעיקר לגופים החיוניים ולגופי תמ"ק בכל מגזר.



בפרק הבא, בו נציג ניתוח של הבעיה בשוק הגנת הסייבר, נתייחס גם לחולשות היחסיות של המודל הנוכחי.

<u>הגנה על שרשרת האספקה והוראת שעה להתמודדות עם אירועי סייבר במגזר השירותים הדיגיטליים</u>

בתחום הגנת הסייבר נודעת חשיבות מיוחדת לגופים המהווים "שרשרת אספקה." ככלל, שרשרת אספקה היא שם כולל למכלול הגופים והפעולות הנעשות *בדרך* לאספקת שירות או מוצר מהארגון ללקוח. **כשמדובר בהגנת סייבר**, שרשרת האספקה כוללת גם את כל הגורמים הדיגיטליים המעורבים באספקת השירות או המוצר ללקוח, ובכלל זה מפתחי או ספקי תוכנה, שירותי אחסון, תפעול מרחוק, ספקי רשתות, שירותי ענן, וכן חברות המעניקות שירותי ניהול מחשוביים ושירותי תמיכה טכנית[10].

תקיפות סייבר באמצעות שרשרת אספקה הן מתקפות שבהן התוקפים מנצלים חולשות או נקודות כשל באחד השלבים או הגורמים שמעורבים בתהליכי פיתוח, ייצור, הפצה או תחזוקה של מוצר או שירות – בין אם מדובר ברכיבי חומרה, תוכנה, ספקי שירותי ענן או קבלני משנה – כדי לחדור אל הארגון. וקטור החדירה הזה הפך נפוץ יותר בשנים האחרונות, בין היתר בשל הסתמכות הולכת וגוברת של ארגונים על פתרונות חיצוניים וספקים גלובליים. דוחות של ENISA (European Union Agency for Cybersecurity) מצביעים אף הם על המגמה, ומגדירים את שרשרת האספקה כיעד מועדף של גורמי איום בשל הפוטנציאל לפגיעה רחבה בבת־אחת במגוון רחב של ארגונים, המקושרים כולם לאותו ספק שירותים[11].

[10] https://csrc.nist.gov/pubs/sp/800/161/r1/final.
[11] https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf, בעיקר בעמ' 124-129

בשנת 2018 השיק מערך הסייבר כלי יעודי לנושא הגנת הסייבר בשרשראות אספקה ("שאלון שרשרת אספקה של מס"ל"), והיא מפורסמת באתר המערך כהמלצה למשק[12]. המערך פרסם לגופי התמ"ק הנחיה מקצועית המבוססת על מתודולוגיה זו. בסוף 2019 פרסמה יחידת הסייבר בממשלה (יה"ב) – האחראית להכוונה והנחיה מקצועית של כלל משרדי הממשלה ויחידות הסמך בתחום הגנת הסייבר – הנחיה ייעודית בנושא שרשרת אספקה, ולפיה בהתקשרויותיהם עם נותני שירותים עליהם להקפיד כי נותני השירותים עומדים במתודה[13].

מאז פריצתה של מלחמת חרבות ברזל זיהה מערך הסייבר התגברות ניכרת בניסיונות למתקפות סייבר נגד ספקי שירותי אחסון ושירותים דיגיטליים, המהווים גופי שרשרת אספקה לארגונים רבים במשק, ובכלל זה לארגונים חיוניים. לצורך הגנה על הציבור ושמירה על הרציפות התפקודית במשק בזמן המלחמה, חוקק **כהוראת שעה** החוק להתמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה-חרבות ברזל), התשפ"ד-23[14]. בין היתר, הוראת השעה מאפשרת למערך הסייבר (וכן לשירות הביטחון הכללי ולמלמ"ב, לפי הנסיבות המנויות בחוק) לתת לספקי שירותים דיגיטליים ושירותי אחסון **הוראות** כיצד להתמודד עם תקיפת סייבר חמורה, כהגדרתה בחוק. הוראת השעה קובעת לאותם ספקים גם חובת דיווח על תקיפת סייבר משמעותית, ומטילה עליהם חובה לעדכן בכך ארגונים מקושרים על תקיפה חמורה בנסיבות הקבועות בה.



[12] https://www.gov.il/he/pages/supply_chain_guide.
[13] הנחיית יה"ב 5.19.
[14] לנוסח העדכני, ראו כאן:
https://main.knesset.gov.il/activity/legislation/laws/pages/lawprimary.aspx?t=lawlaws&st=lawlaws&lawitemid=2212973

ג. היקף ועומק התהליך

מערך הסייבר הלאומי שוקד על הרחבת המענה האסדרתי להגנה בסייבר לפחות מאז אמצע העשור הקודם. שני ניסיונות כאלה - תזכיר חוק הגנת הסייבר ומערך הסייבר הלאומי[15] משנת 2018, וחוק סמכויות לשם חיזוק הגנת הסייבר (הוראת שעה)[16] מ-2021, לא הבשילו לכדי חקיקה, בין היתר בשל הסתייגויות שעלו מצד בעלי עניין שונים – הן בממשלה והן מחוצה לה. כאמור, חקיקה לאומית מסוימת קיבלה ביטוי זמני בהוראת השעה להתמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון, אך היא עוסקת בעיקר במתן מענה וסיוע לגופים נתקפים **לאחר קרות אירוע סייבר**, ולא בהעלאת חוסן לשם מניעתו מראש.

מסמך זה יתאר את עבודת המטה ואת תזכיר החוק שנוסח כתוצאה ממנה. שני אלה משקפים במידה רבה את הלקחים והניסיון שנצברו במשך השנים, לרבות במסגרת הניסיונות הקודמים לקדם את אסדרת התחום. אלה באים לידי ביטוי בעיקר **במעבר ממודל ריכוזי מובהק** ששם דגש על סמכויות ההתערבות של מערך הסייבר, **למודל מבוזר** ומאוזן יותר, המתמקד בעיקרו העלאת רמת ההגנה של הארגונים החיוניים במשק בעזרת הרגולטורים המגזריים שלהם. לאור מורכבות הנושא, חומרת האיום, מספר השחקנים המעורבים, היותה של האסדרה המוצעת חדשה (גם אם מעוגנת ומבוססת היטב בהשוואה בינלאומית), והצורך לאזן בין האינטרס הציבורי לאינטרסים ושיקולים אחרים – הוחלט לבצע תהליך RIA נרחב.

נוכח ההתקדמות שחלה באסדרת הגנת הסייבר בארגונים חיוניים במדינות ה-OECD בפרק הזמן הזה, **דגש מיוחד הושם הפעם על סקירה בינ"ל משווה מעמיקה במיוחד.** עיקרי הסקירה המשווה יובאו בפרק השלישי של המסמך, ואת הסקירה המלאה ניתן למצוא בקובץ המלאה הצמוד לדו"ח זה. פרק נוסף בתהליך **שהוקדשו לו משאבים רבים הוא פרק הניתוח הכלכלי.** מערך הסייבר שם לו כיעד להביא בחשבון היבטים כלכליים ומשקיים רחבים שעה שהוא מסדיר את הגנת מרחב הסייבר האזרחי, וביצע ניתוחי עלות-תועלת מקיפים ביותר.

תיאור מפורט של תהליך העבודה ניתן למצוא בנספח א'.

[15] https://www.gov.il/he/departments/news/cyberlawpublic
[16] https://www.law.co.il/media/computer-law/cyber_defense_bill_draft_version2_2021.pdf

פרק שני – ניתוח הבעיה

א. מונחי יסוד בעולם הסייבר

"מרחב הסייבר" הוא כינוי כולל לאוסף מערכות ותשתיות טכנולוגיית מידע – המרכזית שבהן היא רשת האינטרנט - המשמשות להעברת מידע ונתונים, מקיימות אינטראקציה וקישוריות זו עם זו ועם מערכות אחרות, ואינן מוגבלות על ידי אילוצים פיזיים או גבולות גיאוגרפיים. במחצית המאה האחרונה הפך המרחב הזה למקור של פריחה כלכלית ורווחה חברתית חסרות תקדים, אך באותו זמן, גם למוקד מרכזי של חיי המדינה, הכלכלה והחברה. בהתאמה, הוא נעשה **כר פורה למטרות התקפיות, שיכולות להגיע עד כדי פגיעה בביטחון הלאומי, ביציבות הכלכלית, ברציפות התפקודית המשקית, ואף בסדר הציבורי כולו**[17].

תקיפת סייבר היא תקיפה במרחב הסייבר שמסכנת נכסי סייבר או מערכות ותשתיות הנתמכות על ידם. היא מתבטאת בפגיעה חלקית או מלאה בזמינות, אמינות וסודיות הנכסים במרחב ובמידע השמור, העובר דרכם או מעובד על ידם.

את התקיפות נהוג לחלק לפי מניעיהן, לארבע קטגוריות מרכזיות[18]:

- **CNA** (COMPUTER NETWORK ATTACK): תקיפה שמטרתה לפגוע בתפקוד התקין של הארגון, זאת ע"י גרימת נזק למחשב/רשת. ישנן חומרות שונות לאירועי CNA – מהשבתת תהליכים ספציפיים לזמן מוגבל ועד מחיקת מידע לצמיתות או פגיעה פיזית הדורשת שיקום ארוך.
- **CNE** (COMPUTER NETWORK EXPLOITING): תקיפה שמטרתה לאסוף מידע, הן לצורך איסוף מידע (ריגול, השגת יתרון תחרותי – בין מדינות או בין ארגונים עסקיים וכד'), והן כתשתית לפעולות CNA עתידיות.
- **CNI** (COMPUTER NETWORK INFLUENCE): תקיפה לצרכי השפעה ושינוי תודעה, בין היתר באמצעות פרסומי תעמולה, או ע"י שינוי ההתנהלות וההתנהגות של הארגון דרך החדרת מידע כוזב והורדת רמת האמון במערכת. המאפיינים הייחודיים של מרחב הסייבר – היכולת להגיע לקהל עצום בשניות בודדות ובעלות אפסית – הופכים אותו לשיטה כדאית במיוחד בפני מי שמבקשים לנצלו למטרות השפעה על התודעה.
- **CNF** – (COMPUTER NETWORK FRAUD) (הונאה כספית): תכלית זו מתמקדת בהשגת רווח כספי באמצעות הונאה, סחיטה או גניבה ישירה. דוגמאות כוללות מתקפות כופרה, גניבת פרטי תשלום או ניצול משאבי ענן למטרות פליליות. איום זה מביא לסיכון כספי ישיר, לפגיעה במוניטין העסקי ואף לחשיפה משפטית.

---

[17] הרשקוביץ, שוורץ אלטשולר וסביליה, "מהו סייבר – חלק א'", המכון הישראלי לדמוקרטיה, מחקר מדיניות. אוקטובר 2021. עמ' 18-14 (מכאן ואילך: "**מהו סייבר – חלק א**"). https://www.idi.org.il/books/36467. הגדרה נוספת של מרחב הסייבר ניתן למצוא בהחלטת הממשלה 3611 (07.08.2011): "המתחם הפיזי והלא פיזי, שנוצר או מורכב מחלק או מכל הגורמים הבאים: מערכות ממוחשבות, רשתות מחשבים ותקשורת, תוכנות, מידע ממוחשב, תוכן שמועבר באופן ממוחשב, נתוני תעבורה ובקרה והמשתמשים של כל אלה."

[18] ראו עמ' 18 בסיבוני ג' ואסף ע', קווים מנחים לאסטרטגיה לאומית במרחב הסייבר, מזכר 149, המכון למחקרי ביטחון לאומי, 2015; מהו סייבר – חלק א', עמ' 65-64.

התקיפה מתאפשרת, בין השאר, באמצעות ניצול **חולשה** (vulnerability) – שם כולל לנקודת תורפה בנכס דיגיטלי או בתוכנה אשר ניתן לנצלה כדי לחולל תקיפת סייבר[19]. לדוגמא, אם מערכת הפעלה אינה מעודכנת בעדכוני האבטחה העדכניים ביותר, תוקף פלוני יכול לזהות את הבעיה, לנצל אותה, ולחדור ביתר קלות אל המערכת. חולשה בנכס דיגיטלי יכולה לבוא לידי ביטוי גם בהחדרה פיזית של התקן לא מורשה, או בהתנהגותו של משתמש לא זהיר בנכס, שנפל קרבן לניסיון הטעיה. בכל אחד מהמקרים האלה נוצרת אפשרות לתוקף להתחבר למערכת ולפעול בה כבתוך שלו[20].

משעה שהתוקף ניצל את החולשה, הוא יכול, בין השאר, לחבל (Compromise) בנכס על ידי שימוש ב**נוזקה** (malware) – תוכנה זדונית המשמשת אותו לשיבוש המערכת, השחתתה, גניבת המידע שבה, כמו גם להמשך הפצת הנוזקה למחשבים נוספים[21] להשגת תכליות נוספות. נוזקה כזו יכול שהתוקף יצור אותה מאפס, ירכוש אותה מוכנה, או יבצע בה תיקונים.

במרחב הסייבר קיימות מגוון תקיפות, להלן חלק מהן:

- הנדסה חברתית | Social Engineering - מניפולציה פסיכולוגית הגורמת לעובדים למסור מידע או לבצע פעולה שמסכנת את הארגון.
- פישינג | Phishing (דיוג) – צורה ספציפית של הנדסה חברתית: התחזות במייל או בהודעה כדי לגרום לעובד למסור סיסמאות או ללחוץ על קישור זדוני.
- תוכנת כופר | Ransomware - נוזקה שמצפינה ("נועלת") את כל קבצי הארגון ודורשת תשלום כופר תמורת שחרורם.
- תקיפת מניעת שירות | DDoS - הצפת השרתים או האתר באינספור פניות "זבל" כדי להשבית אותם ו"להפיל" את השירות.
- מילוי פרטי הזדהות | Credential Stuffing - ניסיון אוטומטי לפרוץ לחשבונות באמצעות סיסמאות שדלפו בעבר מאתרים אחרים.
- הזרקת SQL | SQL Injection - החדרת קוד זדוני לטופס באתר (כמו תיבת חיפוש) במטרה לגנוב את כל מאגר הנתונים.
- תקיפת "האדם שבתווך" | Man-in-the-Middle (MitM) - האזנת סתר לתקשורת האינטרנט (נפוץ ב-Wi-Fi ציבורי) כדי ליירט ולגנוב מידע.
- פירצת יום-אפס | Zero-Day Exploit - ניצול פרצת אבטחה בתוכנה שעדיין אינה מוכרת ליצרן, ולכן אין לה עדיין תיקון.
- מניפולציה על מודלי AI - Prompt Injection / Model Extraction - הזנת קלטים זדוניים למערכות בינה מלאכותית בארגון, במטרה לעקוף את נהלי האבטחה שלהן או לחשוף מידע חסוי עליו המודל אומן.

[19] שם.
[20] מהו סייבר, חלק א' – עמ' 32-31.
[21] שם, עמ' 33.

ב. התופעה הבלתי רצויה

דוחות בינלאומיים עדכניים מצביעים על הסלמה עקבית במרחב הסייבר, המתאפיינת לא רק בעלייה כמותית במספר התקיפות, אלא גם בשינוי איכותי בשיטות הפעולה וביעדים[22].

- הפורום הכלכלי העולמי (WEF), בדו"ח הסיכונים הגלובלי שלו לשנת 2025, מדרג את הסיכון של "לוחמת וריגול סייבר" כאחד מחמשת הסיכונים הגלובליים החמורים ביותר הצפויים בשנתיים הקרובות, מה שמדגיש את מרכזיותו של האיום על ברמה הגלובלית[23]. בטווח הארוך זהו הסיכון ה-9 בחשיבותו, מתוך 33 סיכונים גלובליים.
- מחקר של Check Point Research מראה כי בשנת 2024 ארגון הותקף בממוצע 1,673 פעמים - עליה של 44% ביחס לשנה הקודמת. היקף התקיפות הגבוה ביותר נרשם בסקטורים חינוך, ממשל, בריאות ותקשורת; העליה הדרמטית ביותר בהיקף התקיפות היתה במגזר החומרה והתוכנה (עד 179% יותר בהשוואה ל-2023)[24].
- ב-IBM דיווחו כי 70% מתקיפות הסייבר שכוונו כנגד גופים ממשלתיים ושירותים ציבוריים ב-2024 עירבו גם תשתיות חיוניות, כשב-31% מהמקרים וקטור החדירה לארגונים הללו היה שימוש בחשבונות מהימנים של משתמשים[25].
- סוכנות האיחוד האירופי לאבטחת סייבר (ENISA) מזהה בדו"ח תמונת האיומים לשנת 2024 כי שני האיומים הראשיים שדווחו בשנה החולפת היו התקפות מניעת שירות מבוזרות (DDoS/RDOS) וכופרה (Ransomware). יחד הם היוו יותר ממחצית מסך האירועים שנצפו באופן גלובלי[26].
- בעשור האחרון נרשם גם גידול דרמטי בשימוש בשיטות של הנדסה חברתית – ספציפית התחזות באמצעות מיילים עסקיים - Business Email Compromise (BEC)[27], שאחד המרכיבים העיקריים בתוכה הוא סיפור כיסוי (Pretexting)[28] (ראו תרשים להלן).
- אינדקס החדשנות Dell Technologies מעלה כי ב-2023, ארגונים ברחבי העולם איבדו בממוצע מידע בהיקף של 2.17 טרה-בייט, שעלותו 2.61 מיליון דולר. 55% מהארגונים בעולם, לפי הסקר, חוו באותה שנה מתקפת סייבר או אירוע סייבר אחר, בעלות ממוצעת של 1.92 מיליון דולר לאירוע[29]. כאמור, בהמשך הפרק מובאת התייחסות להערכת העלויות הכלכליות כתוצאה מתקיפות סייבר.

---

[22] NISA, *ENISA Threat Landscape 2024*, October 2024. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

[23] https://www.weforum.org/publications/global-risks-report-2025, עמ' 12.

[24] https://www.checkpoint.com/security-report/?flz-category=items&flz-item=report--cyber-security-report-2025 ; עמ' 34.

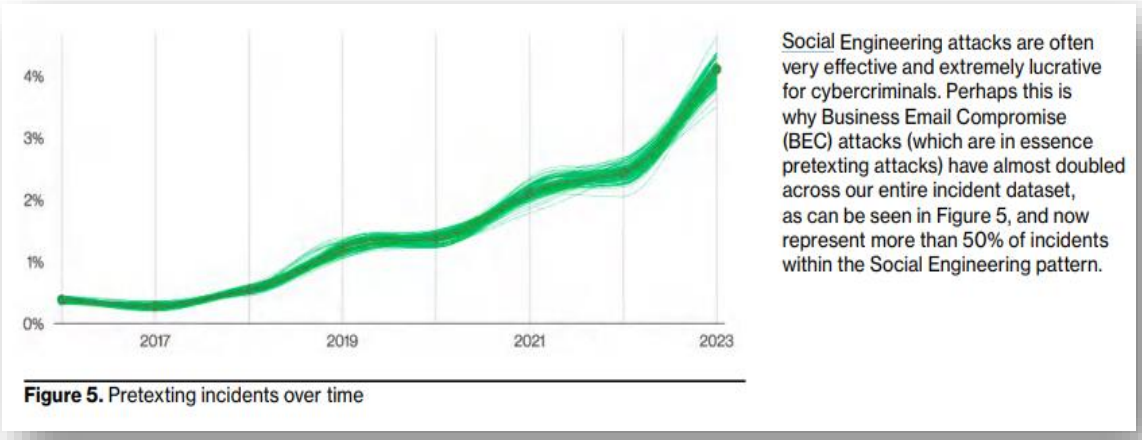
[25] https://www.ibm.com/downloads/documents/us-en/1227cc9e83cb97ae ; עמ' 45.

[26] NISA, *ENISA Threat Landscape 2024*, October 2024. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 בעמ' 9 לדוגמה.

[27] https://www.microsoft.com/en-us/security/business/security-101/what-is-business-email-compromise-bec

[28] Data Breach Investigations Report 2023, Pp. 8-9. לגישה לדוח המלא יש לספק פרטי משתמש: https://www.verizon.com/business/resources/reports/dbir/2023/results-and-analysis-intro/.

[29] https://www.delltechnologies.com/asset/en-nz/products/data-protection/briefs-summaries/global-data-protection-index-infographic-global.pdf



עליה בהיקף השימוש ב Pretexting כשיטה ספציפית של הנדסה חברתית (מתוך דו"ח DBIR לשנת 2023, עמ' 8 שם)

ישראל חווה את איומי הסייבר הגלובליים בעצימות גבוהה במיוחד. דו"חות בינ"ל – כמו גם נתוני מערך הסייבר – מצביעים על עלייה ניכרת בהיקף ובחומרת האיומים על המשק הישראלי.

- לפי דו"ח ההגנה הדיגיטלית של מייקרוסופט ל-2025, **ישראל היא המדינה השלישית בעולם במס' התקיפות** במחצית הראשונה של השנה, בראש ובראשונה כלפי מגזר ה-IT[30]. מגזרים חיוניים אחרים שנמצאים במוקד התקיפות הם מגזרי האנרגיה, הרשויות מקומיות, הממשלה, הבריאות, ועוד. הדו"ח מדגיש את האיום הנשקף מצד איראן: כשני שליש (64%) מכלל פעילות הסייבר של קבוצות תקיפה מדינתיות איראניות מופנית נגד ישראל.
- הדו"ח השנתי של Radware שם את ישראל במקום השני כמדינה הנתקפת ביותר בתקיפות DDos בשנת 2024, עליה של שני מקומות בדירוג ביחס ל-2023[31], ומדגיש אף הוא את הקשר שבין מתחים גאו-פוליטיים לפעילות עוינת במרחב הסייבר.
- חוקרי Check Point הישראלית מצאו כי בשנת 2024 המספר הממוצע של תקיפות סייבר על ארגון ישראלי עמד על 2,054. נתון זה גבוה ב-23% מהממוצע העולמי באותה תקופה, ומשקף עליה של 58% בהשוואה ל-2023. המחקר, שהוצג בכנס CPX Vienna 2025 הדגיש את הגידול המשמעותי במינוף של כלי AI לביצוע מתקפות סייבר מתוחכמות, כמו גם הפצת דיסאינפורמציה[32].

[30] https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf ; עמ' 10, 43,46.

[31] https://www.radware.com/getattachment/59aeeea8-21b3-4606-9f76-f4bfda903f64/Radware_Full_Year_Threat_Report_2025_RWI-426.pdf.aspx, בעמ' 25

[32] https://www.pc.co.il/news/%D7%90%D7%91%D7%98%D7%97%D7%AA-%D7%9E%D7%99%D7%93%D7%A2-%D7%95%D7%A1%D7%99%D7%99%D7%91%D7%A8/424214 ; מידע אושר עצמאית.

גם נתוני מערך הסייבר תומכים את העליה בהיקף האיום הקיברנטי: בשנת 2022 טיפל מערך הסייבר הלאומי בלמעלה מ-9,000 **דיווחים** על אירועי סייבר; בשנת 2023 המספר זינק ב-43% לכ-13,000 **דיווחים**; ובשנת 2024 נמשכה ההחמרה עם עלייה נוספת של 24% ליותר מ-17,000 **דיווחים**[33]. לפי נתוני המערך, מלחמת חרבות ברזל הביאה עמה עליה לא רק במספר התקיפות הכולל, אלא גם במספר האירועים המשמעותיים – פי 2.5 אירועים עם פוטנציאל נזק ממשי נכון לסוף 2023.

התקיפות התעצמו באופן הדרגתי ועברו מהתמקדות במתקפות לגניבת מידע, למתקפות המכוונות לגרימת שיבוש ונזק של ממש לארגונים ולציבור. הן כוונו בין היתר לארגונים חיוניים וליצירת אפקט רחב, באמצעות כיוון לחברות במגזר השירותים הדיגיטליים, הנחשבות שרשרת אספקה לארגונים רבים. ככל שהמלחמה התקדמה, זוהו יותר קבוצות תקיפה הפועלות מטעם איראן וחיזבאללה. התמתנות הלחימה הקינטית במגוון זירות לא הביאה לירידה מקבילה בהיקף ניסיונות התקיפה במרחב הקיברנטי.

[33] לדו"ח 2024: https://www.gov.il/BlobFolder/news/booklet_yearly_summary_2024/he/booklet_yearly_summary_2024.pdf; לדו"ח 2023: https://www.gov.il/BlobFolder/news/booklet_yearly_summary_2023/he/booklet_yearly_summary_2023_e.pdf; לדו"ח 2022: https://www.gov.il/BlobFolder/news/booklet_yearly_summary_2022/he/%D7%93%D7%95%D7%97%20%D7%A9%D7%A0%D7%AA%D7%99%20%D7%A1%D7%95%D7%A4%D7%99%202022.pdf. נשים לב כי מספר הדיווחים השנתי עדיין נמוך משמעותית ממספר התקיפות כפי שעולה מדו"חות חיצוניים (למשל דו"ח Check Point שהובא לעיל). פער זה הוא עדות נוספת על תת-הדיווח של אירועי סייבר – נושא שעוד נעסוק בו בהמשך.

ג. הנזקים כתוצאה מהתופעה הבלתי רצויה

<u>פגיעה, שיבוש והשבתה של תשתיות וארגונים חיוניים</u>

מנקודת מבט מדינתית, תקיפות CNA כנגד **ארגונים חיוניים** הן בעלות פוטנציאל נזק משמעותי. ארגונים חיוניים (Essential Entities)[34] הוא המינוח המקובל לנכסים החשובים ביותר לתפקודה התקין של המדינה, שבלעדיהם עלולים להיפגע בטחונה הלאומי, יציבותה הכלכלית, ושלום הציבור במובנו הרחב: מערכות הבריאות, החשמל, התקשורת, התחבורה, המים והביוב, המערכת הפיננסית, שירותי החירום, משרדי הממשלה ועוד. ארגונים המשתייכים למגזרים אלה – כמו כל ארגון מודרני - מופעלים באמצעות מערכות בקרה ושליטה דיגיטליות המחוברות לרשת, ומשכך מהוות יעד נחשק לתוקפים – לרבות מדינתיים[35].

בחודש אוקטובר 2021, למשל, אירעה מתקפת כופרה על מערכות המחשוב של בית החולים הלל יפה בחדרה, שהביאה לשיבושים בטיפולים לא דחופים. כעבור כמה שעות הודיע בית החולים כי הוא מבקש שלא להפנות אליו חולים במקרים שאינם דחופים. לאחר מספר חודשים דיווח משרד הבריאות כי עלות שיקום בית החולים הגיעה ל-36 מיליון שקלים[36].

דוגמא אחרת: בשיאה של מגפת הקורונה בשנת 2020 סבלו מערכות המים הישראליות ממתקפות סייבר מרובות. אלה נועדו לסכן את מערכות הבקרה של תחנות שאיבה, מתקני מים, מפעלי שפכים ומשאבות לצרכי חקלאות. מטרת התקיפה היתה לשנות את מינוני הכלור וכימיקלים אחרים במי השתיה, ולשבש את האספקה בתקופה קריטית. אילו הייתה המתקפה מצליחה, היו עלולים להיווצר עומסים מוגברים עוד יותר על בתי החולים, חקלאים היו נאלצים להשמיד את היבולים שלהם בכמויות גדולות, ואלפים היו עלולים להישאר בלא אספקה סדירה של מים. גם באפריל 2023 הושבתו מערכות השקיה בגליל העליון בשל מתקפת סייבר. יומיים לפני התקיפה ניתנה אזהרה ממערך הסייבר; חקלאים שניתקו את השליטה מרחוק נמנעו מפגיעה, בעוד מי שנמנעו מכך – נפגעו.

בנספח ב' ניתן למצוא דוגמאות נוספות לתקיפות סייבר מן השנים האחרונות כנגד תשתיות וארגונים חיוניים, שהביאו לנזקים ממשיים ברמה הלאומית במגוון מדינות.

---

[34] במקרים מסוימים, למשל באוסטרליה, נעשה שימוש **גם** במינוח תשתיות קריטיות – Critical Infrastructure כדי לתאר ארגונים.

[35] מהו סייבר – חלק א', עמ' 73-72.

[36] https://main.knesset.gov.il/news/pressreleases/pages/press08112021a.aspx.

לצד השיבוש התפקודי, תקיפות סייבר גובות מחיר כבד בזירה נוספת, סמויה יותר אך הרסנית לא פחות: פגיעה בפרטיות האזרחים ושחיקת אמון הציבור במוסדות המדינה ובארגונים השומרים על המידע שלו. בעידן הנוכחי, תוקפים עושים שימוש במידע גנוב לא רק למטרות סחיטה, אלא ככלי נשק במערכה על התודעה במטרה לזרוע בהלה, מבוכה ואי-אמון חברתי.

כך למשל, באוגוסט 2023, הותקף המרכז הרפואי "מעייני הישועה" בבני ברק[37]. מעבר להשבתת המערכות המינהליות (שגררו הוראה שלא להפנות חולים חדשים עד להודעה חדשה), התוקפים איימו לפרסם מידע רפואי אינטימי ורגיש ביותר של מטופלים, והרשויות בישראל אישרו כי ישנה אינדיקציה ממשית לדלף מידע אישי רגיש.

דוגמה נוספת: בחודש מרץ 2020 החלה מתקפת סייבר על הממשל הפדרלי של ארצות הברית, שהצליחה לפרוץ לגופי ממשל רבים. מתקפת הסייבר בוצעה על ידי קבוצת הפריצה "Cozy Bear". התוקפים ניצלו פרצות אבטחה במוצרים, בשירותים ובתשתית הפצת התוכנה של כמה **חברות נותנות שירותים**, בין היתר לגופי הממשל האמריקאי, וכך השיגו דריסת רגל לפרק זמן של חודשים עד שנים במערכות גופי ממשל רגישים, כמו משרד האוצר האמריקאי. בחברת התוכנה **SolarWinds** הצליחו התוקפים להחדיר קוד זדוני אל מערכת האוטומציה של בניית תוכנה. קוד זה הופץ ללקוחות החברה וכך הצליחו התוקפים לפרוץ לארגונים ממשלתיים רבים ולהחדיר רשתות בוטים זדוניים לתוכם.

הפריצה למחשבי הממשל נחשבת לחמורה ביותר אי פעם בארצות הברית, וזאת בשל רגישות הנתונים, הפרופיל הגבוה של היעדים, ומשך הזמן הארוך שבמהלכו הייתה לפורצים גישה למידע. לא ברור כמה מידע נגנב, אך על פי הערכות של גורמים רבים מדובר היה בסכנה ממשית לביטחון הלאומי, שכן חלק ניכר מהמחשבים שנפרצו היו שייכים לסוכנויות ביטחון ולפנטגון. עד היום לא ברור היקף הנזק שנגרם. כמו בתקיפות משמעותיות אחרות, גם במקרה זה התברר כי **סיסמא חלשה במיוחד** היתה במוקד הפריצה[38].

[37] https://www.gov.il/he/pages/08082023-01

[38] https://crsreports.congress.gov/product/pdf/IN/IN11559 ; https://www.govinfo.gov/content/pkg/CHRG-117hhrg43755/html/CHRG-117hhrg43755.htm.

נזקים כלכליים

על אף הקושי להעריך במדויק את הנזקים הכלכליים מתקיפות סייבר, ההערכה הרווחת היא שהנזק מהן עשוי לפגוע קשות בכלכלתן של מדינות ובכלכלה הגלובלית. כבר ב-2018 קבע דוח של הפורום הכלכלי העולמי כי **אירוע סייבר הוא אחד מחמשת הסיכונים הגדולים ביותר בעולם בעשור הקרוב**[39].

הקשיים לאמוד את הנזקים הכלכליים מתקיפות סייבר נעוצים בשתי סיבות עיקריות: ראשית – בנטייה של חברות וארגונים להסתיר את פגיעות הסייבר שלהם ולא לדווח עליהן[40]; ושנית – בשל הקושי להבחין בין נזקים שנגרמו ישירות כתוצאה מתקיפת הסייבר ונזקים שנגרמו מסיבות אחרות. מתקפות סייבר לרוב אינן מתגלות באופן מיידי; לעיתים הן נראות כמו תקלות רגילות, ולעיתים השפעתן מתבטאת בדרכים עקיפות. הגורמים לכך כוללים טשטוש מכוון של העקבות על ידי התוקפים, מורכבות ותלות-הדדית בין מספר רב של מערכות, וקושי לקשר אירוע מסוים ישירות לתקיפה.

את העלויות הנובעות מתקיפות סייבר ניתן לחלק לשתי קטגוריות, ובהערכות שיוצגו להלן שתיהן מובאות בחשבון:

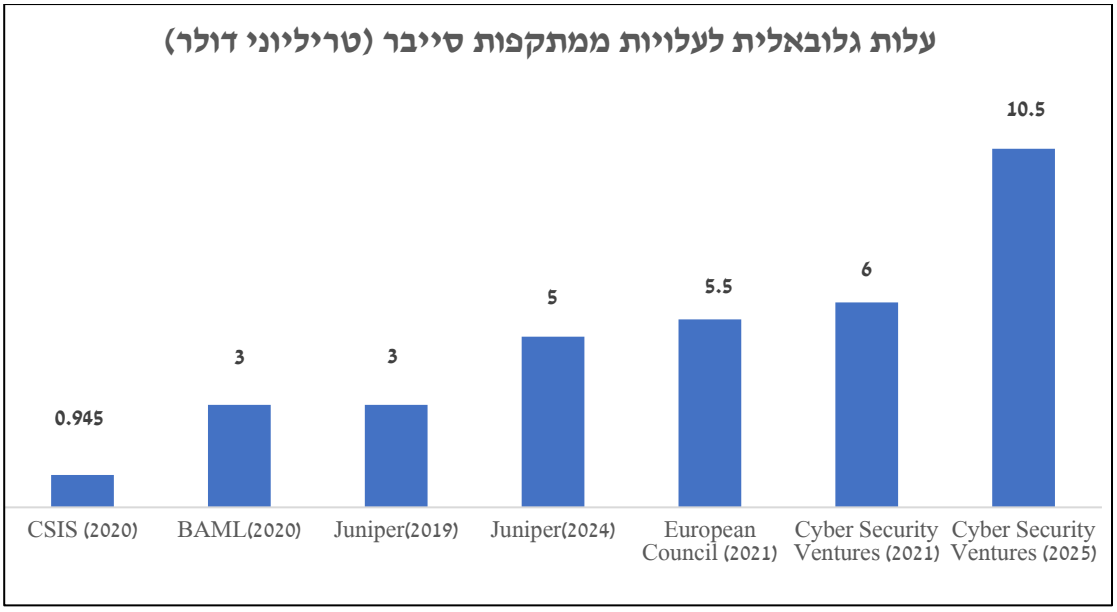
עלויות ישירות – כוללות בין השאר תשלומים לצוות תגובה ראשוני, החלפת תשתיות חומרה ותוכנה, התמגנות מחודשת, שירותי יעוץ, הודעה ללקוחות, ייעוץ משפטי, הפסד כספי כתוצאה ממאמצי שחזור נתונים, תביעות ושיפוי בגין נזקים שנגרמו לצד שלישי, קנסות ועלויות ישירות כתוצאה מההפרעה לרציפות התפקודית וההמשכיות העסקית של הארגון. **עלויות עקיפות** – כוללות בין השאר אובדן הכנסות עתידיות, אבדן הזדמנויות עסקיות, פגיעה במוניטין ושיקומו, ועלות חשיפת מידע סודי של העסק[41].

בשנים האחרונות בוצעו כמה מחקרים והערכות בנוגע לעלויות העולמיות הנגרמות כתוצאה ממתקפות סייבר. ההערכות בוצעו על ידי ממשלות, מכוני מחקר, חברות אבטחת מידע, וגופים כלכליים נוספים. צוות של הכלכלן הראשי במערך הסייבר הלאומי ביצע השוואה של ההערכות השונות הללו, ותוצאותיהן מוצגות בגרף שלהלן:

[39] The Global Risks Report 2018, World Economic Forum: https://www.weforum.org/reports/the-global-risks-report-2018

[40] התופעה של תת-דיווח על אירועי סייבר קיבלה תוקף בשורת מחקרים ונתונים שפורסמו ע"י מקורות שונים בעולם, כולל מקורות רשמיים. דו"חות של הסנאט האמריקאי, משרד המשפטים וה-FBI, העריכו כי בין 75% ל-90% מתקיפות הסייבר אינן מדווחות: Use of Cryptocurrency in Ransomware Attacks, Available Data, and National Security Concerns - USA Senate Committee on Homeland Security and Governmental Affairs, 2022; https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf;

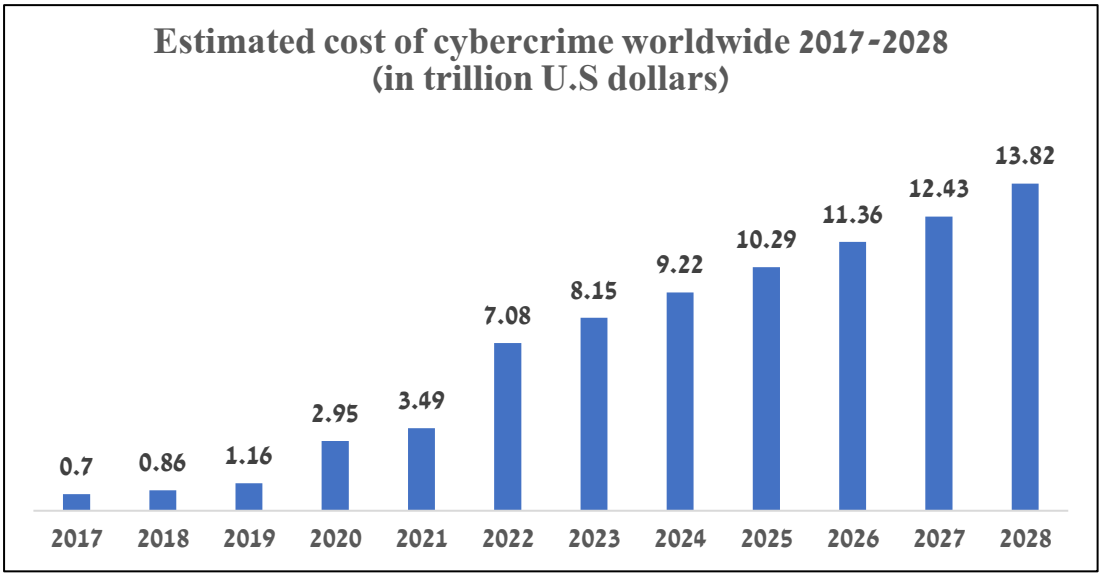
[41] הכלכלן הראשי, מערך הסייבר: "הערכת העלות הכלכלית של מתקפות סייבר בישראל," מאי 2024. https://www.gov.il/he/pages/economic_cost_of_cyber_attacks_8_5_2024



עלות גלובלית כתוצאה מתקיפות סייבר לפי מחקרים שונים (מקור: דו"ח הכלכלן הראשי של מערך הסייבר, 2024).

כפי שניתן לראות, הערכת העלות השנתית הגלובאלית בגין תקיפות סייבר נעה **בין כ-1 טריליון ל-6 טריליון דולר** עבור השנים 2020-2021, כאשר בשנת 2025 הצפי היה לעלות של 10.5 טריליון דולר.

בנוסף לכך, חברת Statista העוסקת בחקר נתונים והצגתם, מעריכה כי בשנים 2023-2028[42], העלות העולמית כתוצאה ממתקפות סייבר תגדל כל שנה בכ-10%, ותסתכם ב-13.82 טריליון דולר בשנת 2028.



שיטת החישוב האגרגטיבית הננקטת במחקרים שצוטטו לעיל מתאפיינת בכמה חסרונות, וביניהם שונות גבוהה בין הממצאים, הצורך להיעזר בהנחות מסוימות, וכן אינטרסים כלכליים של מממני

[42] https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide

המחקר. מאידך, גם אם נאמץ את הערכת הנזק הנמוכה ביותר (כפי שעשה מערך הסייבר בניתוח הכלכלי המלא שלו, וראו לעניין זה הדוח המלא)[43] – **נותר מעט מאוד מקום לספק באשר להיקף האדיר של נזקים כלכליים כתוצאה מתקיפות סייבר.**

כדי להתמודד עם החסרונות המבניים בשיטה האגרגטיבית, האקסטרפולציה של הערכת הנזקים בישראל בלבד בוצעה על בסיס הערכת הנזק השמרנית ביותר (0.945 טריליון דולר, לפי מחקר CSIS), ובנוסף, בוצע תחשיב מקביל בשיטת Bottom-Up. בשיטה זו הנזק הכלכלי המצטבר חושב לא על סמך מחקרי מאקרו והתאמתם לנתוני המשק הישראלי, אלא כתוצאה של מכפלת העלות הממוצעת לתקיפה (ישרה + עקיפה) בכמות התקיפות המוערכת בישראל. שני סוגי הניתוחים העלו כי **הנזק הכלכלי המצטבר כתוצאה מתקיפות סייבר בישראל מוערך בכ-12 מיליארד ₪ בשנה.** לפירוט מלא אודות שיטת החישוב, המתודולוגיה, הנחות המוצא, מקדמי הביטחון וכיו"ב – ראו כאמור את הדו"ח המלא (הפניות בהערות השוליים).

ד. הבעיה וגורמי השורש שלה

עד כה תיארנו את התופעה הבלתי רצויה – ריבוי תקיפות הסייבר; הראינו כי היא שיטתית; ועמדנו על האופן שבו היא שכיחה במיוחד בישראל. אך מהי למעשה **הבעיה** הגורמת להישנותן של תקיפות סייבר? למה הן ממשיכות לקרות, וביתר שאת לאורך זמן?

כדי להשיב על כך, יש לבחון את אבני היסוד של הגנת הסייבר. תפיסת ההגנה המקובלת בעולם נשענת על המודל המשולש של "אנשים, תהליכים וטכנולוגיה" (People, Process, Technology - PPT). על פי מודל זה, הטכנולוגיה היא רק רגל אחת, שאינה יכולה לעמוד לבדה ללא שתי הרגליים האחרות:

- אנשים (People): המשאב האנושי בארגון (עובדים ומנהלים), רמת המודעות שלהם לסיכונים והכשרתם לזהות ולמנוע איומים, או להתמודד עמם נכונה בזמן אמת.
- תהליכים (Processes): שיטות העבודה, הנהלים והמדיניות (Governance) שנועדו להסדיר את אבטחת המידע. החל ממדיניות-על של הדירקטוריון, ועד לפרוטוקולים יומיומיים כמו ניהול הרשאות, חובת אימות דו-שלבי (MFA) ונוהל תגובה לאירוע.
- טכנולוגיה (Technology): חוסנם של מערכות ונכסים דיגיטליים, בהם אנשים משתמשים על מנת למכן ולייעל תהליכים, ובתוכם אף כלי ההגנה הטכניים (חומרה ותוכנה), החל מאנטי-וירוס בסיסי ועד מערכות ניטור והגנה מתקדמות מבוססות AI.

שורה של מחקרים וסקרים מלמדים כי ארגונים ועסקים לוקים בחסר בעיקר לגבי שני המרכיבים הראשונים של המשולש: 'אנשים' ו'תהליכים'. כך, על אף שתקיפות סייבר הן תופעה שיטתית ומוכרת היטב, ולמרות שהנזקים כתוצאה מהן ברורים ומגובים אמפירית – הנתונים מראים כי חלק ניכר של הארגונים אינם נוקטים באמצעים הדרושים כדי לצמצם את הסיכון.

[43] ראו לעיל הערת שוליים 38 וגם כאן:
https://www.gov.il/BlobFolder/news/economic_cost_of_cyber_attacks_8_5_2024/he/the_economic_damage_estimate_report_of_cyber_attacks_in_israel.pdf

כך למשל, מדד המוכנות של Cisco (מרץ 2024)[44] מצא כי רק אחוזים בודדים מהארגונים בעולם מוגדרים כבעלי רמת מוכנות 'בשלה' (Mature) (ובכלל זה בקרב ארגונים עם 1000 עובדים ויותר) - בעוד הרוב המוחלט לוקה בחסר ביישום ההגנות. נתון זה מתכתב עם ממצאי Microsoft (2024)[45], המראים כי הרוב המכריע של התקיפות המוצלחות מתאפשרות דווקא בשל היעדר יישום של 'היגיינת סייבר בסיסית (כגון MFA וניהול הרשאות).

תמונת מצב זו משתקפת גם בישראל. על אף היותה מובילה טכנולוגית, ניכר כי ארגונים רבים במשק אינם נוקטים באמצעי ההגנה הנדרשים. להלן כמה דוגמאות:

- דוחות של מבקר המדינה (2022, 2024) קבעו כי ברשויות מקומיות רבות אין רמת מוכנות מספקת להתמודדות, מניעה או צמצום של אירועי סייבר, וזאת חרף העלייה החדה ברמת האיום בעת מלחמת 'חרבות ברזל'[46].
- בביקורת של הרשות לניירות ערך מראשית 2023 נמצא כי חלק ניכר מהחברות הציבוריות שנבדקו אינן נוקטות אמצעים מספקים, ואינן ערוכות להתמודדות עם תקיפות סייבר[47]: בין היתר, עלה מהדו"ח כי הדירקטוריונים של כ-70% מחברות המדגם לא קיבלו דיווחים עיתיים הנוגעים לסטטוס הגנת הסייבר ואבטחת המידע בחברה; **כ-83% ממערכי אבטחת המידע בחברות שנדגמו אינם מיישמים אף לא אחד מהתקנים המקובלים בתחום אבטחת המידע או הסייבר;** וכ-40% מהחברות לא ביצעו הערכת סיכוני סייבר בשלוש השנים האחרונות.
- מחקר שביצעה הרשות לעסקים קטנים ובינוניים העלה כי ברבע מהארגונים שנדגמו לא נעשה שימוש באף אמצעי התגוננות מפני מתקפות סייבר. רק 40% מהארגונים במחקר עשו שימוש בשלושה כלי התגוננות או יותר[48].
- ולבסוף, דו"ח של חברת Fortinet מנובמבר 2024 העלה כי 67% מהמנהלים הבכירים בארגונים חוששים מכך שלעובדיהם אין מודעות מספקת לסיכוני אבטחה ברשת, עליה של 11% ביחס ל-2023. בישראל שיעור המנהלים המודאגים גבוה יותר ועומד על 80%[49].

צבר הנתונים שהוצגו כאן מלמד כי חלק ניכר מהארגונים נוטים שלא ליישם רמת הגנה מספקת בסייבר. נטייה זו היא שמאפשרת לתוקפים לתקוף ביתר קלות, והיא זו שאחראית במידה רבה על הנזקים (הפיזיים, הכלכליים והאחרים) כתוצאה מתקיפות מוצלחות. אך **מדוע ארגונים לא נוקטים פעולות כדי להגן על עצמם בסייבר?**

---

[44] https://newsroom.cisco.com/c/dam/r/newsroom/en/us/interactive/cybersecurity-readiness-index/documents/Cisco_Cybersecurity_Readiness_Index_FINAL.pdf, עמ' 4, 25-24

[45] https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf בעמ' 23-42.

[46] [46] https://library.mevaker.gov.il/sites/DigitalLibrary/Documents/2022/Shilton/2022-Shilton-401-M.Meda-Taktzir.pdf, ראו למשל בעמ' 1248;
https://library.mevaker.gov.il/sites/DigitalLibrary/Documents/2024/Shilton/2024-Shilton-301-Gviya-Taktzir.pdf בעמ' 125-120.

[47] https://www.new.isa.gov.il/images/Fittings/isa/asset_library_pic/al_lobby/al_lobby-6280ee7d64354/review24123.pdf

[48] https://www.sba.org.il/hb/PolicyAndInformation/Researches/Documents/Cyber2024.pdf; עמ' 6.

[49] https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/08_Report/ftnt-service-report-security-awareness-training-2024.pdf; https://www.pc.co.il/news/419848/.

<u>החצנות שליליות</u>

בפרספקטיבה כלכלית, להגנת סייבר יש מאפיינים רבים של **החצנה שלילית**[50]. החצנה שלילית היא עלות או תועלת שנגרמת מעסקה כלכלית ומוטלת על אנשים או פירמות שלא מעורבים ישירות בעסקה. דוגמה מוכרת לכך היא הבעיה הציבורית של זיהום אויר: המפעלים מזהמים את האוויר כחלק מתהליך הייצור, אך הנזק באיכות האוויר פוגע לא במפעל - אלא באזרחים הנושמים אותו.

גם בעולם הסייבר, ההשפעות של תקיפה או תקלה עלולות להיות משמעותיות יותר עבור גורמים חיצוניים – הלקוחות מקבלי השירות - מאשר עבור הארגון עצמו. ארגונים מתמחרים את ההשקעה בהגנה על בסיס הנזק הצפוי **להם** (אובדן הכנסות, עלות שחזור), אך לעיתים קרובות הנזק לציבור, ללקוחות או לארגונים אחרים המחוברים אליהם בשרשרת האספקה – גדול עשרות מונים. דוגמה מובהקת לכך היא למשל שימוש במוצרי IoT (כגון מצלמות אבטחה ביתיות): היצרן חוסך בעלויות אבטחה והצרכן נהנה ממוצר זול, אך מכשירים אלו נפרצים בקלות והופכים לחלק מ"רשתות בוטים (Botnets) המבצעות מתקפות ענק על תשתיות מדינה. במקרה זה, שני הצדדים לעסקה (היצרן והקונה) לא סופגים את הנזק, אלא הציבור הרחב.

תיאורטית, ארגון עלול שלא להפנים באופן מלא את הסיכון לציבור שיש בפגיעת סייבר בו (א) משום שהדבר כרוך במשאבים; (ב) מכיוון שקיימת בעיה של מחסור בידע, במידע, וממילא המידע הוא א-סימטרי (ראו פירוט בנושאים אלה בהמשך); (ג) מאחר וארגונים נוטים באופן טבעי שלא להפנים סיכונים שהם חיצוניים להם; ו-(ד) משום שבעולם הסייבר ישנה חשיבות מובהקת לעמידות <u>רוחבית</u> של ארגונים בעלי מאפייני סייבר דומים.

מצב זה יוצר תמריץ כלכלי מעוות המכונה "**תלות הדדית באבטחה**" (**Interdependent Security**). בדומה לחיסונים בעולם הרפואי, רמת הביטחון של הארגון הבודד תלויה לא רק בו, אלא גם בחוסנם של הספקים והשותפים שלו. כאשר ארגון מניח ש"האחרים ישקיעו בהגנה" ובכך יגנו גם עליו, נוצרת "**בעיית הטרמפיסט**" (**Free-Riding**): כל שחקן מחכה שהאחרים יישאו בעלויות ההגנה על המערכת האקולוגית המשותפת, ובפועל – רמת ההגנה המצרפית של המשק צונחת אל מתחת לרף הרצוי. סקרים אחרונים מלמדים כי שיקול זה משחק תפקיד בקבלת ההחלטות של ארגונים על השקעות בסייבר, כשאחת הסיבות הבולטות להשקעה שכזו הוא ציות לרגולציה מחייבת[51].

אסטרטגיית הסייבר הלאומית של ארה"ב (2023) זיהתה כשל זה כגורם המרכזי לחוסר הביטחון במרחב הדיגיטלי, וקבעה כי כוחות השוק לבדם לא יפתרו את הבעיה כל עוד הגופים המייצרים את הסיכון אינם נושאים באחריות לתוצאותיו[52].

---

[50] ראה למשל: OECD 2008 'Economics of malware: Security decisions, incentives and externalities', http://www.oecd.org/internet/interneteconomy/40722462.pdf

[51] ראו בדו"ח ה-RIA של NIS2, בעמ' 23, וה"ש 80.

[52] ראו למשל בעמודים 8-9 וכן בפרק 3 לאסטרטגיה: https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

א-סימטריה של המידע

אינפורמציה א-סימטרית (Asymmetric information) היא כינוי לכשל שוק הנובע מכך שלא לכל המשתתפים בפעילות הכלכלית יש אותו מידע רלוונטי בנוגע לעסקה.

בעולם הסייבר, כשל שוק זה לובש צורה יחודית: הוא עוסק בא-סימטריה המובנית שבין איומי הסייבר למאמצי ההגנה: בעוד שאיומי הסייבר צומחים בקצב מעריכי, בין היתר הודות לאוטומציה, בינה מלאכותית וקישוריות גוברת, הרי שההשקעה באבטחה והטמעת הגנות בארגונים מתקדמות בקצב ליניארי ואיטי יחסית. בהתאם, עלויות התקיפה יורדות – בעוד עלויות ההגנה עולות.

פער זה אינו סטטי; הוא יוצר "חוב סייבר" (Cyber Debt) מצטבר, המעמיק ככל שהזמן עובר. פער זה עלול להותיר את המשק הישראלי חשוף בנקודות תורפה היסטוריות. הפורום הכלכלי העולמי (WEF) עמד על כך בדו"ח הסיכונים שלו, בציינו כי פחות מ-1 מכל 10 משיבים סבור שבשנתיים הקרובות בינה מלאכותית יוצרת תעניק יתרון למגינים על פני התוקפים, לעומת 9% בלבד שסברו כי היא תסייע למגינים יותר[53] .

הא-סימטריה של המידע באה לידי ביטוי בעולם הסייבר בשתי דרכים נוספות: הארגון הבודד לרוב אינו חשוף לתמונת המודיעין המלאה, וחסר את היכולת להעריך נכונה את המוטיבציות, התחכום והמשאבים העומדים לרשות התוקפים (אשר חלקם פועלים בחסות מדינתית או כארגוני פשיעה עתירי משאבים). פער ידע זה מוביל באופן שיטתי להערכת-חסר של רמת האיום, וכפועל יוצא – להימנעות מנקיטת צעדי ההגנה הנדרשים[54].

לבסוף, במישור היחסים שבין ספק ולקוח - למרבית הלקוחות בשוק – ובכללם ארגונים – אין יכולת להעריך ברמה טובה דיה את רמת האבטחה של המוצרים ו/או השירותים שהם רוכשים. נוצר אפוא שוק שבו הצרכנים לא יודעים להעריך את ההבדל בין המוצרים השונים, והם במידה רבה אדישים ביחס לנושא אבטחת המידע של המוצר או השירות שהם מקבלים. בהיעדר שקיפות, השוק אינו מתגמל ספקים המקפידים על הגנה, ונוצר תמריץ שלילי להשקעה באבטחת מידע[55].

הגורם האנושי, היעדר מודעות והיעדר מומחיות

כפי שהוצג לעיל, ארגונים רבים טרם הפנימו את עוצמת הסיכון הקיברנטי. כתוצאה מכך, הגנת סייבר נתפסת לא אחת כ"הוצאה" שיש לצמצם ולא כהשקעה אסטרטגית המבטיחה את רציפות הארגון. חולשה תפיסתית זו מתורגמת ישירות לפרצות בשטח: בניגוד לדעה הרווחת המייחסת פריצות לתחכום טכנולוגי עילאי, הסטטיסטיקה מראה כי החוליה החלשה היא דווקא האדם.

[53] https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf בעמ' 6.
[54] NIS Impact Assessment, UK Gov, April 2018;
[55] מהו סייבר, חלק א', עמ' 30-29. ראו גם בדו"ח הערכת השפעות רגולציה של האיחוד האירופאי לגבי מוצרים דיגיטליים - https://www.astrid-online.it/static/upload/impa/impact_assessment_cyber_resilience_act.pdf בעמ' 10-4. ראו גם בדו"ח הפורום הכלכלי הבינ"ל (ה"ש 53 לעיל), בעמ' 28.

כך למשל, על פי דו"ח חקירות הפרצות של Verizon לשנת 2024 (DBIR), "האלמנט האנושי" (Human Element) היה הגורם המרכזי ב-68% מכלל פרצות אבטחת המידע בעולם[56]. נתון זה כולל טעויות אנוש, רשלנות, נפילה במתקפות דיוג (Phishing) ושימוש בסיסמאות חלשות או גנובות. המשמעות היא שרוב גדול של האירועים יכול היה להימנע לו הגורם האנושי היה מיומן ועירני יותר. הבעיה מחריפה בשל "אי-הנראות" של הסיכון. בניגוד לעולם הפיזי, סיכוני סייבר אינם מוחשיים. העובדה שלא ניתן "לראות" את הסיכון תורמת לתופעות של דחיינות ושאננות, הבאה לידי ביטוי בעיקר באופן הטיפול בעדכוני אבטחה (Patching). כשנחשפת חולשה בתוכנה, היצרן לרוב מפרסם עדכון הגנה. אך בעוד שהתוקפים פועלים במהירות מסחררת ומתחילים לסרוק ולחפש קורבנות בתוך 5 ימים (זמן חציוני), רוב הארגונים משתהים זמן רב בתיקון – 55 ימים ויותר במחצית מהמקרים[57].

ניתוח של מערך הסייבר הלאומי מ-2023 מצביע על כך שחלק ניכר מהתקיפות החמורות בישראל התבססו על חולשות ישנות (**בנות שנה ויותר**!) שפורסמו מזמן אך לא תוקנו בארגון הנפגע[58], מה שמעיד על כשל ניהולי ותהליכי עמוק.

<u>בעיית הדיווח ושיתוף המידע</u>

הגורם הרביעי לכשל השוק הוא בעיית "תת-הדיווח" והיעדר שיתוף המידע. בעולם הסייבר מתקיימת "דילמת אסיר" קלאסית: בעוד ששיתוף מידע על תקיפות חיוני להגנת הכלל, עבור הארגון הבודד, הדיווח נתפס כפעולה המסבה נזק ישיר – פגיעה במוניטין, ירידת ערך המניה, וחשיפה לקנסות רגולטוריים אפשריים או לתביעות ייצוגיות[59] . כתוצאה מכך, ארגונים רבים בוחרים להסתיר אירועי סייבר או לדווח עליהם באיחור ניכר. מצב זה יוצר נזק כפול: בטווח המיידי, הוא מונע מהמדינה לסייע בבלימת האירוע; בטווח הארוך, הוא מונע למידה רוחבית.

<u>פערים במודל האסדרה הנוכחי</u>

לצד גורמי שורש אלה, יש לתת את הדעת גם על החולשות של המצב האסדרתי הקיים. כפי שתואר בראשית הפרק, בשנת 2015 קיבלה ממשלת ישראל את החלטות הממשל 2443 ו-2444. החלטות אלה קבעו כי משרדי הממשלה השונים יקדמו את הגנת הסייבר של ארגונים חיוניים בתחומם, וזאת בהנחיה מקצועית של מערך הסייבר הלאומי. בעשור שחלף מאז החלטות הממשלה הוקמו יחידות מגזריות להגנת סייבר בחלק ממשרדי הממשלה, אך שהמצב שהתקבע סובל מכמה חולשות יסודיות:

[56] https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf, עמ' 12-13; https://csrc.nist.gov/CSRC/media/Events/FISSEA-30th-Annual-Conference/documents/FISSEA2017_Witkowski_Benczik_Jarrin_Walker_Materials_Final.pdf

[57] https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf, עמ' 21.

[58] https://www.gov.il/he/departments/news/booklet_yearly_summary_2022, סיכום שנת 2022 של מערך הסייבר הלאומי (להלן: "סיכום שנה 2022 של מערך הסייבר") עמ' 17-20.

[59] עמ' 19; Zibak, A., & Simpson, A. (2019). Cyber threat information sharing: Perceived benefits and barriers. ARES '19; Gal-Or, E., & Ghose, A. (2005). The Economic Incentives for Sharing Security Information. Information Systems Research, 16(2), 186–208. https://pages.stern.nyu.edu/~aghose/ISR.pdf.

- פערים ביכולת ופיקוח ובסמכויות אכיפה של הרגולטורים: לחלק מהרגולטורים המגזריים אין רגולציית סייבר יעודית, והם מוגבלים ביכולתם לאכוף רמת הגנה מספקת על הארגונים שהם מאסדרים;
- פערים משמעותיים ברמת ההגנה של הארגונים החיוניים: ההשקעה השונה בכ"א ובתקציבים מוביל לפערים משמעותיים ברמת ההגנה בין מגזרים שונים במשק. כך למשל, בחלק מהמגזרים מופעל SOC מגזרי, ובחלק לא.
- חוסר באסדרה לאומית רחבה: היעדר מסגרת חוקית המגדירה בבירור את חלוקת האחריות, הסמכויות וממשקי העבודה בין מערך הסייבר, הרגולטורים המגזריים והארגונים. עמימות זו יוצרת חוסר סנכרון בניהול ההגנה, ופוגעת ביכולת לייצר תמונת מצב לאומית אפקטיבית בשגרה ובחירום.

מאפיינים אלה אינם כשלי שוק בפני עצמם, אך הם גורמים מעכבים בפני המאמצים המדינתיים לטפל באותם כשלי שוק.

ה. סיכום

בפרק זה הצגנו ניתוח מעמיק של הבעיה הציבורית. התחלנו בהצגת מונחי יסוד מעולם הסייבר; הצגנו תופעה בלתי רצויה שיטתית ומוכחת אמפירית (תקיפות סייבר); עמדנו על הנזקים כתוצאה ממנה (כלכליים, תפעוליים וציבוריים); מיפינו את הבעיה הגורמת לה (הגנה בלתי מספקת מצד ארגונים ופרטים), וחשוב מכל – את גורמי השורש שלה (החצנות שליליות, א-סימטריה של המידע, מודעות לא מספקת והיעדר דיווח). בנוסף ראינו כי קיימים פערים במודל האסדרה הנוכחי, שבאופן טבעי מקשים על היכולת להתמודד עם כשלי השוק. התרשים הבא מציג את הדברים בצורה ויזואלית.

ניתוח בעיית הסייבר: מהשורש ועד הנזק



פרק שלישי – למידה מהעולם

"בפיתוח רגולציה, קובעי מדיניות ורגולטורים צריכים לאסוף ראיות ומומחיות גם מחוץ למדינה שלהם. נדיר שמתעוררת סוגיה חדשה ששום מדינה או ארגון בין-לאומי לא התמודדו איתה בעבר [...] גם כאשר אין אמנה המחייבת אימוץ כללים מהעולם, יש לקחת אותם בחשבון ולהסתמך עליהם; וכאשר נסיבות ספציפיות מחייבות לחרוג מהם, יש להצדיק זאת על סמך ראיות..."[60]

התופעה של סיכונים במרחב הסייבר והנזקים הכבדים הנגרמים מהם לא נעלמה מעיניהם של קובעי ומעצבי מדיניות ברחבי העולם, ובפרט במדינות ה-OECD. מאז אמצע העשור הקודם קידמו מדינות כמו ארה"ב, אוסטרליה, בריטניה ומדינות האיחוד האירופאי שורת חוקים להגנת הסייבר בארגונים חיוניים. בסוף 2024 נכנסה לתוקפה הדירקטיבה האירופאית *השנייה* להגנת מערכות מידע ורשתות (דירקטיבת NIS2) – המגלמת את הלקחים שנלמדו מהדירקטיבה הראשונה, שחוקקה ב-2016 ונכנסה לתוקפה שנתיים לאחר מכן.

כפי שראינו, בישראל קיימת לעומת זאת אסדרה חלקית בלבד של תחום הגנת הסייבר, במודל מבוזר מאוד שבו כל מגזר מסדיר עצמאית את תחום הגנת הסייבר, כפוף להנחיה מקצועית של מערך הסייבר. במצב זה קיימת שונות רבה הן בתוכן האסדרה שארגונים חיוניים נדרשים לה, והן ברצון וביכולת של חלק מהמאסדרים לבצע פיקוח ואכיפה יעילים. כך, היכולת לשפר את רמת ההגנה המצרפית במשק ולסייע לארגונים בטיפול בתקיפות סייבר נפגעת באופן ניכר.

מערך הסייבר בחר לבדוק כיצד התמודדו 5 מדינות עם התופעה הבלתי רצויה: בריטניה, גרמניה, אוסטרליה, הולנד וארה"ב. חמש המדינות הן בהגדרה "מדינות מערביות בעלות שווקים מפותחים," בהתאם לנדרש בחוק עקרונות האסדרה, תשפ"ב-2021.

כדאי לשים לב שהמודל של "אין-רגולציה" או פתרונות וולונטריים גרידא לא נבחר (ולמיטב ידיעתנו אף לא נשקל) באף אחת מן המדינות שנסקרו. בדו"ח הערכת השפעות הרגולציה של דירקטיבת NIS ציינה מועצת האיחוד כי האסדרה שהייתה קיימת לפני כניסת הדירקטיבה לתוקף הייתה עמוסת פערים, ויצרה מסגרות רגולטוריות לא-אחידות, מבחינת המגזרים המכוסים ומבחינת תוכן הרגולציה כאחד. עוד צוין באותו מסמך כי הגישה הוולונטרית להגנת סייבר הניבה עד לאותה נקודה רמה לא שוויונית של מוכנות (לאירועי סייבר) ושיתוף פעולה מוגבל (מצד הארגונים). מסקנתם הייתה כי **נוכח המטרה של העלאת רמת המוכנות לתקיפות סייבר, החלופה המובילה היא החלופה הרגולטורית**[61].

כך, בכל 5 המדינות שנבדקו קיימת **חקיקה לאומית** המסדירה את חובותיהם של מפעילי שירותים חיוניים לנקוט צעדים מסויימים להגנת הסייבר. חובות אלה הן בעיקרן חובה לנהל את סיכוני

[60] OECD Best Practice for Regulatory Policy – International Regulatory Co-operation (2021).
[61] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013SC0031. ראו בעיקר בעמ' 3 ואילך. לגרסה המלאה של דוח ה-RIA: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013SC0032.

הסייבר בארגון (בכל המדינות פרט לרמה הפדרלית בארה"ב), ולדווח על אירועי סייבר משמעותיים. **החובות חלות רק ביחס לקבוצת הסקטורים (מגזרים) שהוגדרו כחיוניים או קריטיים, כשבכל סקטור נקבעו בדרך-כלל תבחינים או תנאי סף, שרק גופים העומדים בהם יהיו מחוייבים לעמוד בדרישות הרגולציה – זאת, מתוך תפיסה של ניהול סיכונים, ובמטרה לצמצם את הנטל הרגולטורי.**

א. עיקרי הממצאים

<u>בריטניה</u>

הרגולציה העוסקת בהגנת הסייבר של תשתיות קריטיות בבריטניה מעוגנת ב-Network and Information Systems Regulations מ-2018[62]. החוק (הידוע גם כ-NIS UK) היווה היישום הלאומי של NIS, והוא נותר בתוקפו (ואף עודכן) גם לאחר פרישתה של בריטניה מן האיחוד.

NIS UK מסדיר את תחום ההגנה בסייבר בחמישה סקטורים בלבד: **אנרגיה, מים, בריאות, תחבורה, ותשתיות דיגיטליות**[63]. הסדרה של הגנת הסייבר בשאר המגזרים עוגנה בדברי חקיקה שנכנסו לתוקפם טרם כניסתה של NIS לתוקף[64]. לגבי כל אחד מחמשת הסקטורים נקבעו תתי-סקטורים, ובהתאמה **רשויות מוסמכות (Competent Authorities)** – קרי, משרדי ממשלה או יחידות מסוימות שלהן – שהן האחראיות ליישום, אכיפה ופיקוח של החוק[65]. הרשויות המוסמכות הן האחראיות הבלעדיות על יישום החקיקה, האכיפה והפיקוח עליה – ומכאן שככלל, מודל הרגולציה הבריטי כולל אמנם חקיקה לאומית, אך הוא **ביזורי באופן מובהק.**

פרט למפעילים של שירותים חיוניים (=ארגונים חיוניים) בחמשת הסקטורים, החוק חל גם על ספקים של שירותים דיגיטליים רלוונטיים (RDSP – Relevant Digital Service Providers). בהתאם ל-NIS, אלה הן ישויות המספקות שירותים של מנועי חיפוש מקוונים, שווקים מקוונים או שירותי מחשוב ענן, תחת קריטריונים מסוימים[66].

החובות הנובעות מהרגולציה חלות **אך ורק על ארגונים העומדים בתנאי סף מסויימים (Thresholds),** שנקבעו בתוספת השנייה לחוק, ואשר פעילותם נשענת על מערכות רשת ומערכות מידע[67]. ככלל, מנגנון תנאי הסף שנקטה החקיקה הבריטית נשען כמעט לחלוטין על **תבחינים כמותיים** (כמות לקוחות / משתמשים / ייצור). יוצא דופן הוא סקטור הבריאות, שם לא נקבע תנאי סף כמותי, אם כי מבוסס-הגדרה.

החוק קובע כי על מפעיל שירותים חיוניים לעדכן את הרשות המוסמכת היעודית לגבי כל אירוע סייבר שיש לו השפעה משמעותית על המשכיות השירות החיוני שאותו מפעיל מספק, וזאת תוך **ללא**

[62] https://www.legislation.gov.uk/uksi/2018/506
[63] מוגדרים בסעיף 8(1) לחוק ובתוספת הראשונה לחוק.
[64] תשובה לשאילתה מאת נציגי DCMS בבריטניה.
[65] סעיף 3 לחוק והתוספת הראשונה.
[66] סעיף 1(3)(e) לחוק; ראו הרחבה על הקריטריונים בהשוואה הבינ"ל המלאה המוגשת בצמוד לדו"ח זה.
[67] סעיף 8(1) לחוק.

שיהוי ובכל מקרה תוך 72 שעות מרגע שנוגע למפעיל השירות החיוני על האירוע[68]. בתיקונים המוצעים לחוק בזמן כתיבת מסמך זה, פרק הזמן לדיווח צפוי לרדת ל-24 שעות.

בנוסף, החוק קובע כי מפעיל של שירות חיוני **חייב לנקוט בצעדים טכניים וארגוניים הולמים ומידתיים כדי לנהל את הסיכונים הנשקפים לבטיחות מערכות הרשת והמידע שלו,** עליהן נשען השירות אותו הוא מעניק. על המפעיל לנקוט בצעדים דומים גם כדי למנוע ולצמצם את ההשפעה של אירועי סייבר, מתוך מטרה להבטיח את רציפות השירות[69].

משרד הדיגיטל, התרבות והספורט הבריטי (Department for Digital, Culture, Media and Sport – DCMS), שהיה האחראי בזמן החקיקה על הנחיית שאר משרדי הממשלה לעניין ישום החוק, פרסם מדריך[70] לרשויות מוסמכות כיצד עליהן להעריך את הציות של הגופים שתחת אחריותן להוראות החוק. בין היתר, התייחס המסמך לדרכים שבאמצעותן יש להעריך את העמידה בחובות ניהול הסיכון, וקבע כי מומלץ בחום (אם כי לא חובה) להעריכה כנגד 14 העקרונות המפורטים בין היתר במסמך "מסגרת הערכת הסייבר" – Cyber Assessment Framework (CAF), אותו חיבר ה-NCSC[71].

יודגש, כי ה-CAF מציב **עקרונות ויעדים בלבד, ואינו כולל כל הנחיה ספציפית באשר לשאלה כיצד יש להשיג את אותן תוצאות**. באחריות מפעילי השירות החיוניים לקבוע את הצעדים ההולמים לניהול הסיכון בהקשר הספציפי שלהם, תוך התייעצות וקבלת הכוונה מהרשויות המוסמכות[72]. בהקשר זה, ה-CAF מפנה לשורה ארוכה מאוד של תקנים, סכימות, מסמכי הדרכה וכיו"ב, שהוא מחשיב אותם רלוונטיים ליישום 14 העקרונות. בין היתר ניתן למנות תקנים ומדריכים כמו ISO/IEC 27001 & 27002, NCSC Risk Management Guidance, ISO 55001 - Asset Management, NCSC Supply Chain Security, IEC 62443, NCSC 10 Steps: Incident Management, NIST ועוד[73]. לרשויות המוסמכות גם שמורה הסמכות לפרסם **מדריכים יעודיים** לסקטור שתחת אחריותן[74].

חובת ניהול הסיכון לגבי ספקים של שירותים דיגיטליים מפורטת מעט יותר ביחס לשאר המפעילים החיוניים. שירותים דיגיטליים (הכוללים כאמור שלוש קטגוריות – שווקים מקוונים, מנועי חיפוש מקוונים ושירותי מחשוב ענן) נדרשים באותה חובה כללית לניהול הסיכון כשאר ספקי השירותים החיוניים, אלא שיישום החובה כולל את ההיבטים שצוינו בסעיף 2 בדירקטיבת האיחוד האירופי

---

[68] סעיף 11(3)(b) לחוק.
[69] סעיף 10 (1) עד (3) לחוק.
[70] לעניינו, ראו פרק 3.1, Security Measures, במדריך: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/700500/NIS_-_Guidance_for_Competent_Authorities.pdf
[71] https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance
[72] מדריך ה-DCMS, בעמ' 13.
[73] לכל אחד מ-14 העקרונות הפניה לתקנים ו/או מדריכים הרלוונטיים אליו: https://www.ncsc.gov.uk/collection/caf/table-view-principles-and-related-guidance
[74] יצויין כי בתשובה לשאילתה ששוגרה לשותפים בבריטניה, פורשה הסמכות כחובה; עם זאת, מלשון החוק עולה בבירור כי לא מדובר בחובה. החובה הנקובה (בסעיף 3(3)(b) לחוק, היא לפרסם מדריך, מבלי שהיא כוללת התייחסות פרטנית לשאלת ניהול הסיכון.

2018/151: בטיחות מערכות ושירותים; טיפול באירועים (Incident Handling); ניהול ההמשכיות התפעולית; פיקוח, בקרה ובחינה; וציות לתקנים בינ"ל[75].

כדי לבצע פיקוח ואכיפה, החוק העניק לרשויות המוסמכות את הסמכות לדרוש מן הגופים המפוקחים מידע; לבצע ביקורות ופעולות פיקוח; לתת התראות; להטיל קנסות; ובתנאים מסוימים אף להתחיל בהליכים אזרחיים. לפירוט והפניות בנושא זה אנא ראו הסקירה הבינ"ל המלאה המצורפת לדו"ח זה בקובץ נפרד.

<u>גרמניה</u>

החוק העיקרי שאסדר את הגנת הסייבר בגרמניה מאז אמצע העשור הקודם הוא חוק המשרד הפדרלי לאבטחת מידע (BSIG)[76]. החוק מגדיר את תפקידיו וסמכויותיו של המשרד הפדרלי עצמו (BSI) בתחומי אבטחת מידע ומערכות מידע, וכן קובע חובות מסוימות על מפעילים של תשתיות קריטיות[77] לצורך הגנה על מערכות המידע שלהם[78]. בדומה לבריטניה, גם בגרמניה ישנה אבחנה בין מפעילי תשתיות חיוניות (מקביל ל-OES בבריטניה) לבין מפעילי שירותים דיגיטליים (DSPs). ב-5 בדצמבר 2025 נכנס לתוקפו החוק החדש, המיישם את דירקטיבת 2NIS – עליה נרחיב בהמשך. בשלב זה נסקור את החוק הגרמני המקורי.

התשתיות החיוניות שעליהן חל BSIG הן מתקנים, מערכות או חלקים שלהן, העומדים, במצטבר, בשלושה תנאים: הם בעלי חשיבות גדולה לתפקוד של הקהילה, היות שכשל או פגיעה בהם יוביל לפגיעה משמעותית באספקת שירותים או יהווה איום על ביטחון הציבור; הם משתייכים לאחד הסקטורים הבאים: **אנרגיה, טכנולוגיית מידע וטלקומוניקציה, תחבורה ותנועה, בריאות, מים, מזון, פיננסים וביטוח, וניהול פסולת עירונית**[79]; והם עומדים באחד או יותר מהתבחינים הספציפיים שנקבעו לגוף חיוני (Thresholds – בדומה לבריטניה), פר סקטור, שפורטו בתקנות יעודיות (תקנות KritisV[80]).

יש לשים לב כי החקיקה הגרמנית <u>לא קבעה</u> "רשויות מוסמכות" לכל אחד מהסקטורים (כפי שנעשה למשל בבריטניה, או כפי שנראה בהמשך – בהולנד) – דבר המלמד על **האופי הריכוזי יותר של מודל האסדרה** הגרמני. עם זאת, לא אחת נדרש ה-BSI לתיאום עם הרשות המוסמכת הרלוונטית טרם ביצוע צעדים מסוימים שהוא מוסמך לבצע לפי חוק. מכל מקום, מנגנון התבחינים או תנאי הסף

[75] סעיף 12(2)(c) לחוק; לפירוט מקיף אודות מה כולל כל אחד מהסעיפים יש לפנות לסעיפים 2,3 ו-4(1) להנחיות האיחוד האירופי 2018/151.

[76] https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html

[77] התרגום המילולי הוא "קריטי" (Critical), אך לצורך הבהירות נבהיר כי הכוונה היא למפעילי תשתיות חיוניות, במובנן המוכר לנו בישראל, כ"גופי A" (ולא תשתיות מדינה קריטיות – תמ"ק). לצורך הבהירות, מכאן ואילך נשתמש אפוא בביטוי "שירותים חיוניים" ולא "קריטיים".

[78] חלק הארי של החוק עוסק בהרחבת סמכויותיו של ה-BSI, לרבות המלצה על אמצעי אבטחה או שימוש במוצרי אבטחה ספציפיים, וכן בחינה של מוצרי ומערכות IT. בנוסף החוק מצין כי ה-BSI יכין ויפרסם רשימת סטנדרטיים מינימליים לאבטחת IT, למען מפעילי התשתיות הקריטיות, אותן יכול משרד הפנים הפדרלי לאמץ בצורה של תקנות מנהלתיות.

[79] סעיף 2, הגדרה (10) לחוק ה-BSIG.

[80] https://www.gesetze-im-internet.de/bsi-kritisv/BSI-KritisV.pdf

לצורך הגדרתו של 'מפעיל שירות חיוני' דומה מאוד לזה שננקט בבריטניה, והוא נשען במידה רבה מאוד על **תבחינים כמותיים**[81].

החובות החלות על ארגונים חיוניים לפי החוק הגרמני דומות לאלה שנקבעו בבריטניה: החובה לדווח על אירועי סייבר משמעותיים, והחובה לנהל את סיכוני הסייבר. כך, ארגונים שבתחולת החוק לפי התבחינים שנקבעו היו חייבים לדווח **מידית** למשרד הפדרלי [BSI] על שיבושים בזמינות, במהימנות, באותנטיות או בסודיות של מערכות, רכיבי או תהליכי טכנולוגיית המידע שלהם, **שהובילו או יכולים להוביל** לכשל או לפגיעה משמעותית ביכולת להשתמש בשירותים אותה הם מפעילים. בנוסף, הם נדרשים לנקוט בצעדים הארגוניים והטכניים ההולמים על מנת למנוע שיבושים לזמינותם של אותם שירותים, וכדי להגן על המהימנות, האותנטיות והסודיות של מערכות טכנולוגיית המידע שלהם. בנקיטת צעדים כאמור יש לעקוב אחר ההתפתחויות החדשניות האחרונות (State of the Art)[82]. מפעילים של תשתיות קריטיות ושותפיהם בתעשייה **רשאים להציע ל-BSI סטנדרטים ייעודיים לתעשייה** ספציפית לטובת יישום החובה הכללית לניהול הסיכון, והוא יקבע אם מדובר באמצעים מתאימים – **תוך התייעצות עם הרשות המוסמכת הרלוונטית**, וכן עם המשרד הפדרלי להגנה אזרחית וסיוע באסונות[83].

על מפעילי התשתית הקריטית **להוכיח ציות לחובת ניהול הסיכון מדי שנתיים**, והדבר יכול שיעשה באמצעות בקרות, מבחנים או התעדה/הסמכה (Certification), שיועברו לעיון ה-BSI, בתוספת תיעוד של כשלי ה-IT שהתגלו. ה-BSI רשאי לדרוש תיקון כשלים כאמור, והוא גם רשאי להשתמש בצד שלישי כדי לוודא עמידה בחובת ניהול הסיכון.

בדומה לנעשה בבריטניה, חובת ניהול הסיכון ב-BSIG לובשת צורה מעט יותר קונקרטית כשהיא מוחלת על מפעילים של שירותים דיגיטליים. כאן קובע החוק הוראה כללית דומה לזו שהובאה לעיל ("נקיטת אמצעים ארגוניים וטכניים הולמים..."), אף מוסיף כי בנקיטת צעדים כאמור יש להביא בחשבון את ההיבטים הבאים: בטיחות מערכות ומתקנים; זיהוי, ניתוח והכלה של אירועי אבטחה; ניהול ההמשכיות התפעולית; פיקוח, ניטור ובחינה; וציות לתקנים בינ"ל[84].

בהלימה עם המודל הריכוזי, ה-BSI אחראי למלא תפקידים בהתאם לסעיפים 8A עד 8C ו-8F, העוסקים בחובת ניהול סיכון וחובת דיווח של מפעילי תשתיות קריטיות, DSP וחברות בעלות חשיבות מיוחדת לאינטרס הציבורי[85]. כפועל יוצא מכך, שמורות לו הסמכויות לאסוף ולהעריך מידע; לבצע סריקת פורטים בתנאים מסוימים; לדרוש מידע; לתת הוראות; לספק סיוע בעת אירוע סייבר; לשתף מידע ולהטיל קנסות. לפירוט והפניות ראו הסקירה המלאה המצורפת בצמוד לדו"ח זה.

---

[81] https://www.gesetze-im-internet.de/bsi-kritisv/BSI-KritisV.pdf; המידע מתוך "מבנה הרגולציה בתחום הסייבר – סקירה השוואתית", מאת חברת MEIDATA (ר' שם בעמ' 17-21).

[82] סעיף 8a(1) לחוק.

[83] סעיף 8a(2) לחוק.

[84] סעיף 8c(3) לחוק. לפירוט מקיף אודות מה כולל כל אחד מהסעיפים יש לפנות לסעיפים 2,3 ו-4(1) להנחיות האיחוד האירופי 2018/151.

[85] סעיף 3 (17) לחוק.

<u>אוסטרליה</u>

החקיקה המסדירה את תחום ההגנה בסייבר באוסטרליה, ובכלל זה את חובותיהן של ישויות האחראיות על "נכסים קריטיים", מעוגנת בחוק לאבטחת תשתיות קריטיות[86].

גם כאן, בדומה לבריטניה ולגרמניה, קבעה החקיקה את הסקטורים הקריטיים שרק לגביהם תחול הרגולציה. הסקטורים הם 11 במספר - **תקשורת, אחסון או עיבוד נתונים (Data); שירותים ושווקים פיננסיים; מים וביוב; אנרגיה; רפואה ובריאות; השכלה גבוהה ומחקר; מזון ומכולת; תחבורה; טכנולוגית חלל; ותעשיית הביטחון**[87].

לגבי כל סקטור נקבעה רשימה של "נכסים קריטיים" אפשריים – והם יחשבו כאלה, ביחס לסקטור שלהם, רק אם עמדו (כמו בבריטניה ובגרמניה) בתנאי סף או תבחינים שנקבעו בחוק. ואולם, בניגוד לבריטניה ולגרמניה, **התבחינים שנקבעו בחוק האוסטרלי <u>אינם</u> כמותיים בעיקרם**, אלא בחלקם הלא מבוטל "איכותניים," ובחלק מהמקרים אף שמיים-ספציפיים.

חובת הדיווח על אירועי סייבר משמעותיים כפי תיאורם לעיל חלה אך ורק על תשתיות קריטיות <u>שצוינו במפורש בתקנות</u>, או שהשר הכריז עליהן בהצהרה מכח סעיף 51 לחוק כי חלה עליהן חובת הדיווח[88]. דו"ח על אירוע סייבר שהייתה או יש לו <u>השפעה משמעותית</u> יוגש **בהקדם האפשרי, ובכל מקרה בתוך 12 שעות** מרגע שנוגע לישות המדווחת עליו.

ישות האחראית לנכס קריטי **שצוין בתקנות**[89] ו/או הוכרז ע"י השרה לביטחון פנים חייבת ליצור עבורו תכנית ניהול סיכונים. מטרת התכנית לזהות סיכונים שיש חשש ממשי שהתממשותם תוביל להשפעה רלוונטית על הנכס ; לצמצם את הסיכונים, ככל שניתן ובמידה שניתן ; ולצמצם את השפעות הסיכונים במידה והתממשו. **הישות חייבת להגיש דו"ח שנתי בנוגע לתכנית ניהול הסיכונים** שלה 90 יום לאחר תום השנה הפיננסית[90].

תקנות שהותקנו בשנת 2023 קובעות, בין היתר, כי התכנית תכלול **תהליך או מערכת** אשר, ככל שניתן לצפות מבחינה מעשית, יפחיתו או ימנעו סיכוני סייבר, וכן יצמצמו את ההשפעה הרלוונטית של סיכונים כאלה על הנכס. על תהליך או תכנית כאמור **לעלות בקנה אחד עם אחד מהתקנים או מסמכי המסגרת שננקבו בתקנה**, ובנוסף בתנאים הספציפיים שנקבעו בה. כך למשל, התכנית יכולה לעלות

---

[86] החוק חוקק לראשונה ב-2018, ועבר תיקונים ב-2022. לנוסח העדכני והמשולב: https://www.legislation.gov.au/Details/C2022C00160. "נכסים קריטיים" (critical infrastructure assets) הם, לעניינו, מקבילים ל"מפעילי שירותים חיוניים," או מה שמוכר בישראל כ"גופי A". להרחבה בנוגע למערכות בעלות חשיבות לאומית, שהן קטגוריה צרה יותר של נכסים בעלי רמת חשיבות וקריטיות גבוהה יותר (Systems of National Significance – SoNS) – ראו בהמשך.

[87] סעיף 8D לחוק.

[88] סעיף 30BB לחוק. סעיף 51 הוא הסעיף המאפשר לשר להכריז על נכס תשתית קריטית גם אם לא הוגדר כך מכח התבחינים שבחוק. לדוג': באוסטרליה, נכס קריטי בסקטור הבריאות הוא בית חולים בעל יחידת טיפול נמרץ. סעיף 51 מעניק לשר את האפשרות, בתנאים מסוימים, להכריז גם על ביה"ח שאין לו יחידת טיפול נמרץ כאמור כי הוא נכס קריטי של סקטור הבריאות. רק אם הכרזה כאמור תכלול במפורש דרישה לביצוע חובת דיווח על אירוע סייבר, אותו נכס יהיה מחויב בה.

[89] סעיף 30ABA כולל הוראות בדבר אופן התקנת התקנות, לרבות התייעצות עם הציבור והבאה בחשבון של עמדותיו ככל שהוגשו כאלה, וזאת במסגרת זמן שלא תפחת מ-28 ימים. כך, בדומה לחובת הדיווח - עצם הגדרתו של נכס כנכס קריטי אינה מקימה עבורו את חובת ניהול הסיכון באופן אוטומטי, ויש להכלילו קודם לכן בתקנות.

[90] סעיף 30AA, 30AB (1) לחוק, 30AG.

בקנה אחד עם התקן האוסטרלי Australian Standard AS/ISO/IEC 27001:2015; לחילופין, היא יכולה להישען על מודל ה- Essential Eight Maturity של מנהלת האותות האוסטרלית, ובתנאי שהנכס יגיע לרמת בגרות 1 כמפורט באותו מסמך. הטבלה מציינת אפשרויות נוספות [91].

יצוין כי החקיקה האוסטרלית כוללת התייחסות לקטגוריה נפרדת של נכסים – **מערכות בעלות חשיבות לאומית (Systems of National Significance – SoNS)** – שלגביהן חלות חובות מוגברות בתחום ניהול הסיכונים. מערכות מסוג זה עשויות להידרש להכנת תכנית תגובה להתמודדות עם אירועים; ביצוע תרגילים בתחום בטיחות סייבר; ביצוע הערכת פגיעויות (Vulnerability Assessment); והגשת דו"חות תקופתיים או מבוססי אירוע לפי דרישת המזכיר – הכל כמפורט בחלק 2C של החוק ובהתאם לתקנות שיקבעו ע"י השר.

סמכויות הפיקוח והאכיפה נתונות בעיקרן למשרד לביטחון פנים, והן כוללות הטלת קנסות, מתן צווי מניעה, מתן הוראות, פתיחה בחקירה, סמכות לדרוש מידע, וסמכות לדרוש התקנת תוכנה (כמוצא אחרון במקרים חריגים, ורק לגבי SoNS). בניגוד למדינות האחרות שנסקרו, החוק האוסטרלי מגדיר מקרי קצה שבהם השר לביטחון פנים רשאי להגיש לרשות המוסמכת הרלוונטית **בקשה להתערבות**. בקשה שכזו עשויה לכלול **אחד או יותר מסוגי הדברים הבאים**: גישה למערכות, ביצוע שינויים במערכת או במחשב עצמו, ביצוע ניתוח של המערכות, התקנת תוכנות על מחשב, גישה מרחוק, שחזור, העתקה, שינוי או מחיקת תאריך במחשב, וכן ניתוק מחשב או מכשיר ממוחשב[92]. לפירוט – ראו בסקירה המלאה המצורפת בצמוד לדו"ח זה.

<u>הולנד</u>

בשנת 2018 נכנס לתוקפו החוק לביטחון מערכות תקשורת ומידע (the Security of Network and Information Systems Act, או בשמו המקוצר בהולנדית – WBNI). החוק קובע את חובותיו של משרד המשפטים והביטחון בנושא ביטחון הסייבר ומערכות המידע של תשתיות קריטיות ומשרדי ממשלה בהולנד, ובכלל זה מחיל חובות מסוימות גם על התשתיות הקריטיות עצמן. בדומה ל- NIS UK, WBNI הוא היישום הלאומי של דירקטיבת NIS בהולנד. נכון למועד כתיבת שורות אלה, החוק החדש, שיישם את דירקטיבת 2NIS, טרם נכנס לתוקף.

בדומה לחקיקה הבריטית והגרמנית, גם WBNI מחיל חובות הגנה בסייבר על שלוש קטגוריות של גופים: מפעילים של <u>שירותים חיוניים</u> – המשתייכים לאחד משבעת הסקטורים הבאים (המנויים בתוספת השניה ל-NIS): **אנרגיה, תחבורה, בנקאות, תשתיות לשווקים פיננסיים, בריאות, אספקה והפצה של מי שתיה, ותשתיות דיגיטליות**[93]; <u>מפעילי שירותים חיוניים "אחרים"</u>[94] כפי שתקבע הממשלה בתקנות; וקטגוריות <u>ספקי השירותים הדיגיטליים</u>, שכמו בבריטניה ובגרמניה (בהתאמה ל-NIS) כוללת שווקים מקוונים, מנועי חיפוש מקוונים, ושירותי מחשוב ענן – <u>להוציא</u> עסקים קטנים

---

[91] ראו סעיף 8 בתקנות Security of Critical Infrastructure (Critical Infrastructure risk management program) Rules (LIN 23/006) 2023. https://www.legislation.gov.au/Details/F2023L00112

[92] סעיף 35AC לחוק.

[93] בהתאם לסעיף 4(1) וסעיף 5.1.a לחוק WBNI, ובהתאמה מלאה לתוספת השנייה ל-1NIS; ראו גם: https://digital-strategy.ec.europa.eu/en/policies/nis-directive-netherlands.

[94] סעיף 5.1.b לחוק

וזעירים כפי הגדרתם בהנחיות האיחוד האירופאי (קרי, עסקים בעלי פחות מ-50 עובדים ומאזן/מחזור שנתי של 10 מיליון אירו ופחות)[95].

עבור כל אחד מהסקטורים קובע החוק, בדומה לבריטניה, רשות מוסמכת, כשחלק מהרשויות אחראיות על יותר מסקטור אחד[96]. הכללתן בחוק מבטאת את **המודל הביזורי למדי** של רגולציית הסייבר במדינה.

בעקבות העברת החוק, הותקנו גם **תקנות**[97], הקובעות, לצד נושאים אחרים המטופלים בהן, תבחינים ל"מפעילים של שירותים חיוניים" ו"מפעילי שירותים חיוניים אחרים". חלק נכבד של התבחינים הם תבחינים איכותניים (אם כי לא רק), המפנים לדירקטיבות אירופאיות או לפרטי חקיקה לאומיים בהם ניתנה לשר הרלוונטי הסמכות לקבוע גופים מסויימים למטרות שונות.

ככלל, רכיבי החקיקה דומים מאוד לנהוג בבריטניה ובגרמניה; לפירוט נוסף ניתן לפנות לסקירה המלאה המצורפת בצמוד לדו"ח זה.

<u>ארצות הברית</u>

במרץ 2022 חתם הנשיא ביידן על החוק לדיווח על אירועי סייבר בתשתיות קריטיות (CIRCIA). החוק מעניק לסוכנות לאבטחת סייבר ותשתיות (CISA) כ-3 וחצי שנים לקבוע חקיקה שתחייב דיווח על אירועי סייבר בתשתיות קריטיות. בהתאם למסגרת הזמנים שנקבעה, טיוטת חקיקה כאמור יצאה להתייעצות ציבורית כשנתיים לאחר מכן. הטיוטה המוצעת קובעת כי ישויות וארגונים הנכללים בחוק (ראו להלן) מחויבות לדווח על אירועי סייבר 'מכוסים' בתוך 72 שעות, ועל תשלומי כופרה בתוך כ-24 שעות. הם גם חייבים לספק דוחות משלימים ברגע שהתקבל מידע מהותי חדש בנוגע לאירוע שדיווחו עליו. החוק היה צפוי להיכנס לתוקף עד ספטמבר 2025, אך למיטב ידיעתנו פרסומו הסופי נדחה למחצית 2026.

הצעת החוק חלה על כל גוף המוגדר "גוף מכוסה". גוף מכוסה הוא ישות הנמצאת **באחד ממגזרי התשתית הקריטית** המפורטים בהנחיית המדיניות הנשיאותית 21 (PPD-21) העומד באחד או יותר משני סוגי הקריטריונים העיקריים הבאים:

(1). קריטריון גודל אוניברסלי (רוחבי) – חל על ישויות בכל מגזרי התשתיות הקריטיות. גוף נחשב לגוף מכוסה אם הוא **חורג מתקן הגודל של העסקים הקטנים** (small business size standard) שנקבע על ידי מינהל העסקים הקטנים (SBA), המבוסס על קוד סיווג התעשייה הצפון אמריקאי (NAICS) בין אם לפי מספר עובדים ובין אם לפי הכנסה שנתית;

(2). קריטריונים מבוססי סקטור (קריטריונים **משתנים**) - קריטריונים ספציפיים שנועדו 'ללכוד' גופים קריטיים במגזרים מסוימים, וזאת ללא קשר לגודלם של אותם גופים. למשל, בסקטור

[95] הגדרה Digital Service Provider בסעיף 1 לחוק WBNI

[96] סעיף 4 לחוק.

[97] https://wetten.overheid.nl/BWBR0041520/2021-05-01 - נוסח משולב של התקנות הכולל את התיקון האחרון משנת 2021.

טכנולוגיית המידע (IT), גוף הוא ישות מכוסה, ללא קשר לגודלו, אם הוא מספק חומרה/תוכנה/שירותי IT לממשלה הפדרלית; אם הוא עוסק בפיתוח או תחזוקת "תוכנה קריטית"; אם הוא יצרן מקורי, ספק או אינטגרטור של רכיבי OT (טכנולוגיה תפעולית); או אם הוא עוסק בפונקציות הקשורות ל-DNS.[98]

בניגוד לחובת הדיווח, ארה"ב לא אימצה עדיין חקיקה **פדרלית** לאומית סדורה המחילה חובת ניהול סיכונים על גופים חיוניים בכלל הסקטורים במשק האמריקאי. שורה של החלטות נשיאותיות – ובראשן החלטה נשיאותית 13636, דירקטיבה נשיאותית 21, החלטה נשיאותית 13800 ובמידה מסוימת גם החלטה נשיאותית 14028 מחייבות את הסוכנויות הפדרליות המפקחות על חברות ממגזרי תשתיות קריטיות להטיל רגולציית ציווי ושליטה רכה ביזורית באמצעות פיתוח כללים לניהול סיכונים ולהגנת סייבר. בהתאם התוו מחלקות החקלאות, ההגנה, האנרגיה, ביטחון המולדת, התחבורה והאוצר המלצות ודרישות להגנת סייבר, כל אחת כלפי מגזר התשתית הקריטית שעליו היא מפקחת, כמו גם תכניות לשיתוף פעולה עם שחקנים מהמגזר הפרטי וממשלות ברמת ה-states.[99] כך, במדינות מסוימות קיימים חוקים יעודיים הדורשים נקיטת אמצעים סבירים, ספציפית לצורך הגנה על מידע פרטי, בין היתר בניו-יורק, קליפורניה, וירג'יניה, קולורדו ומסצ'וסטס[100]. בניו-יורק קיימת גם רגולציה המחייבת ארגונים מכוסים לבצע בדיקות חדירות אחת לשנה, בסקטור השירותים הפיננסיים.[101]

הנחיות רגולטוריות חזקות יותר בדבר ניהול הסיכון, גם הן בד"כ באמצעים של רגולציה רכה יחסית[102], קיימת ברגולציה ייעודית לסקטורים ספציפיים – בין היתר בסקטור הממשל (הסוכנויות הפדרליות); סקטור התחבורה; הסקטור הפיננסי; סקטור הבריאות; ובסקטור טכנולוגיות המידע – אם כי רק בהתקשרויות עם הממשל הפדרלי. כמו כן קיימת חקיקה ברמת המדינות, התובעת נקיטת אמצעי בטיחות סבירים להגנה על פרטיות המידע.

CISA מפרסמת באתר הבית שלה[103] רשימה מקיפה ביותר של מקורות מידע בדבר ניהול הסיכון, הכוללים מתודות ושאלונים להערכה עצמית, הפניה ל-NIST, כלים חינמיים ברשת ועוד. עוד פרסמה הסוכנות מסמכים פרטניים אודות ניהול הסיכון פר-סקטור, לכל אחד מ-16 הסקטורים החיוניים שנקבעו בדירקטיבת המדיניות הנשיאותית 21.

---

[98] https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements

[99] רחל ארידור הרשקוביץ ותהילה שוורץ אלטשולר. "מהו סייבר? חלק ב': אתגרי האסדרה של הגנת הסייבר". המכון הישראלי לדמוקרטיה, מחקר מדיניות 173. ינואר 2023. עמ' 34.

[100] https://iapp.org/media/pdf/resource_center/global_legal_group_iclg_cybersecurity_2022.pdf, עמ' 202.

[101] שם, עמ' 203.

[102] הכוונה לרגולציה הדורשת, למשל, "נקיטת אמצעים סבירים לניהול הסיכון" – תוך מתן בחירה למפוקח כיצד ליישמם

[103] https://www.cisa.gov/cyber-resource-hub

ב. הגדרת רגולציה מהעולם שתשמש כתשתית לגיבוש הרגולציה המקומית

מן הסקירה הבין-לאומית עולה תמונה ברורה למדי: כל המדינות אימצו פתרון רגולטורי להתמודדות עם הסיכון של תקיפת סייבר בארגונים חיוניים; וכל הפתרונות הללו כללו שני נדבכים משמעותיים: חובת דיווח על אירועי סייבר משמעותיים, וחובות בסיסיות לניהול סיכוני הסייבר. חלק מן המדינות (בריטניה, הולנד) אימצו מודל מבוזר שבו הרגולטור המגזרי הוא האמון על יישום, פיקוח ובקרה על האסדרה; בחלק אחר (גרמניה ואוסטרליה) אימצו מודל ריכוזי יותר, שבו יש משרד אחד האמון על האסדרה – אם כי גם שם יש לרגולטורים המגזריים תפקידים וסמכויות. בארה"ב ניתן לזהות סוג של מודל מעורב (דיווח – פדרלי; ניהול סיכון – טרם, למעט בנוגע לגופים של הממשלה).

שני הנדבכים הללו – חובת דיווח על אירועי סייבר משמעותיים וחובת ניהול הסיכון – הם למעשה לב ליבה של דירקטיבת NIS (וביתר שאת של NIS2) – שהשפעתן עוברת כחוט השני כמעט בכל המדינות שנבדקו. כך, גרמניה והולנד יישמו את NIS הלכה למעשה, הודות למעמדן כחברות באיחוד האירופאי. לצד שאר מדינות האיחוד, הן נמצאות בזמן כתיבת שורות אלה בשלבים האחרונים של עדכון החקיקה הלאומית שלהן בהתאם ל-NIS2. בריטניה, כפי שהוצג לעיל, יישמה אף היא את NIS, אך לא שינתה את החקיקה הלאומית שלה גם אחרי יציאתה מהאיחוד. למעשה, עבודת המטה הבריטית על עדכון החקיקה ממשיכה להסתמך במידה רבה על NIS2[104]. אפילו בארה"ב החלה עבודה לבחינת הדמיון והשוני בין חובות הדיווח הקיימות בארה"ב לאלה הנדרשות ב-NIS2[105], ומבדיקה שקיימנו עולה כי גם נורבגיה - שאינה חברה באיחוד האירופי - פועלת כדי להתאים את החקיקה הלאומית שלה ל-NIS2[106]. מכל הבחינות האלה נראה כי ככל שתאומץ חלופה רגולטורית להתמודדות עם הסיכון, הרי ש-**NIS, וליתר דיוק NIS2, היא נקודת היחוס הטבעית לקביעתה של אסדרה על התחום בישראל.** להלן סיכום תמציתי של עיקריהן:

<u>המגזרים שבתחולה</u>

אחת המסקנות העיקריות מיישמה של NIS הייתה הצורך **להרחיב משמעותית את המגזרים שבתחולה**, עקב הגידול המהיר והדרמטי בתלותם של מגזרים רבים נוספים ברשתות ובמערכות מידע[107]. כך, NIS חלה רק על ארגונים חיוניים בסקטורים אנרגיה, תחבורה, בנקאות, תשתיות של השווקים הפיננסיים, בריאות, מים ותשתיות דיגיטליות. בנוסף NIS חלה על ספקי שירותים דיגיטליים, הכוללים שווקים מקוונים, מנועי חיפוש מקוונים, שירותי מחשוב ענן. NIS 2 הרחיב את מס' המגזרים המכוסים באופן ניכר, וכולל ארגונים בכל המגזרים המנויים ב-NIS, <u>ובנוסף</u> את מגזרי הביוב, ניהול שירותי ICT, מנהל ציבורי, חלל, שירותי דואר ושליחויות, ניהול פסולת, כימיקלים, מזון, ייצור, ספקים דיגיטליים (כולל שווקים מקוונים, מנועי חיפוש מקוונים, פלטפורמות של רשתות חברתיות) ואת סקטור המחקר.

---

[104] בין היתר, בהרחבת מס' הגופים שבתחולה בסקטור השירותים הדיגיטליים; ובחיזוק סמכויות הפיקוח והאכיפה שבידי הרגולטורים – שני נושאים שבאים לידי ביטוי ב-NIS2.

[105] https://www.dhs.gov/news/2024/03/20/dhs-and-dg-connect-announce-initiative-comparing-cyber-incident-reporting-better; https://www.dhs.gov/publication/comparative-assessment-dhs-harmonization-cyber-incident-reporting-federal-government

[106] שיחה של מחלקת קש"ח במערך הסייבר הלאומי עם נציגים מאוניברסיטת NUTU בנורבגיה.

[107] דו"ח RIA של NIS2, עמ' 13.

תבחיני הסף לארגון חיוני

דירקטיבת NIS אפשרה לכל מדינה לקבוע את התבחינים לארגון חיוני בכל מגזר באופן עצמאי[108]. הדבר יצר שונות גדולה מאוד בין מדינה למדינה בנוגע להגדרת הארגונים החיוניים. NIS2 ביקש לפתור את הבעיה ע"י האחדה וסטנדרטיזציה, ולצורך זה קבע תבחינים אחידים וגורפים: **"ארגון חיוני" (essential entity)** הוא כל ארגון גדול במגזרים שהוזכרו לעיל, המעסיק יותר מ-250 עובדים והמחזור השנתי שלהם גבוה מ-50 מיליון אירו); בנוסף – נותני שירותי TDL, DNS ללא קשר לגודלם; ספקים של שירותי תקשורת אלקטרונית ציבורית שהם עסק בינוני ומעלה; ישויות של המנהל הציבורי ברמה הארצית; וכל ישות אחרת שהמדינה המיישמת קבעה כי היא עונה להגדרה ישות חיונית[109]. **"ארגון חשוב" (important entity)** הוא כל ארגון במגזרים שהוזכרו לעיל שאינו ממלא אחר התנאים ל"ארגון חיוני", ובלבד שהוא ארגון בינוני (מעסיק יותר מ-50 עובדים אך פחות מ-250, והמחזור השנתי שלו גבוה מ-10 מיליון אירו אך נמוך מ-50 מיליון אירו), ושהמדינה קבעה כי יש להכלילו בתחולת החוק בשל חשיבות השירות שהוא מספק[110]. למדינות החברות באיחוד עדיין שמורה הזכות לקבוע ארגונים חיוניים וחשובים בהתאם לתבחינים כלליים שנקבעו בדירקטיבה[111].

דרישות מינימליות לניהול הסיכון

אחת המסקנות מיישום NIS הייתה כי מדינות שנות יישמו באופן שונה למדי את הדרישה כי ארגונים חיוניים ינקטו אמצעים מינימליים לניהול סיכוני הסייבר שלהם. כך, NIS דרשה כי מפעילי שירותים חיוניים "ינקטו **אמצעים טכניים וארגוניים הולמים ומידתיים** כדי לנהל את הסיכונים הנשקפים לאבטחת הרשת ומערכות המידע שבהן הם משתמשים בפעולותיהם. בהתחשב בחדשנות, אמצעים אלה יבטיחו רמת אבטחה המתאימה לסיכון הנשקף[112]." עוד דרשה הדירקטיבה כי "מפעילי שירותים חיוניים ינקטו אמצעים מתאימים כדי למנוע ולמזער את ההשפעה של אירועים המשפיעים על אבטחת הרשת ומערכות המידע המשמשות לאספקת שירותים חיוניים, במטרה להבטיח את המשכיותם[113]."

NIS 2 הולכת כברת דרך ארוכה יותר, ומפרטת **מה אמצעים כאלה אמורים לכלול לכל הפחות**. על ישויות חיוניות לנקוט בצעדים טכניים, תפעוליים וארגוניים הולמים כדי לנהל את הסיכון הנשקף למערכות מידע ורשתות בהן נעשה שימוש, וכדי למנוע או לצמצם את ההשלכות של אירועים כאלה. הצעדים צריכים לקחת בחשבון את החידושים האחרונים ביותר בתחום (State of the Art), סטנדרטים בינ"ל וכן את עלויות הביצוע[114].

הצעדים הנדרשים בפסקה הקודמת יתבססו על גישת "כל הסיכונים" (all-hazards approach), במטרה להגן על מערכות מידע ורשתות והסביבה הפיסית שלהן, **ויכללו לכל הפחות את ההיבטים**

[108] סעיף 5, NIS1.
[109] סעיף 3.1 סעיפים קטנים (a) עד (g), NIS 2.
[110] סעיף 3.2, NIS 2.
[111] סעיף 3.1(e), NIS2, וההפניה לסעיף 2.2(b)-(e).
[112] סעיף 14.1, NIS.
[113] סעיף 14.2, NIS.
[114] סעיף 21.1, NIS 2.

הבאים: מדיניות לניתוח סיכונים וביטחון מערכות מידע; התמודדות עם אירועים; המשכיות עסקית; שרשראות אספקה; אבטחה של רשתות ומערכות מידע, לרבות התמודדות עם חולשות ודיווח עליהן; מדיניות ונהלים להערכת היעילות של ניהול הסיכון; פרקטיקות בסיסיות של היגיינת-סייבר; מדיניות ונהלים בנוגע לשימוש בקריפטוגרפיה או היכן שרלוונטי, הצפנה; ביטחון משאבי אנוש, בקרת גישה וניהול נכסים; שימוש בפתרונות הזדהות לתקשורת בטוחה בתוך הארגון, היכן שרלוונטי[115].

<u>חובת דיווח על אירועי סייבר משמעותיים</u>

NIS דרש ממפעילי שירותים חיוניים לדווח ללא שיהוי לרשויות המוסמכות או ל-CSIRT הלאומי על אירועים שיש להם השפעה משמעותית על המשכיות השירותים החיוניים שהם מספקים. הודעות יכללו מידע המאפשר לרשות המוסמכת או ל-CSIRT לקבוע מהי ההשפעה חוצת-הגבולות של האירוע. עצם הדיווח לא יהפוך את המדווח למי שנושא באחריות מוגברת[116].

NIS2 קובע כי מפעילי שירותים חיוניים ידווחו לרשויות המוסמכות או ל-CSIRT על אירועים שיש להם השפעה משמעותית על המשכיות השירותים החיוניים שהם מספקים. היכן שנדרש, מפעילי שירותים ידווחו גם למקבלי השירות על אירועים משמעותיים כאמור[117].

אירוע משמעותי מוגדר כאירוע שגרם או מסוגל לגרום לשיבוש תפעולי חמור לשירותים המסופקים ע״י הישות החיונית, או לגרום לה נזק כלכלי; וכן אם הוא פגע או יש לו היכולת לפגוע בישויות אחרות ע״י גרימת נזק חומרי או שאינו חומרי[118].

דיווח ראשוני על האירוע יעשה ללא שיהוי ובכל מקרה תוך 24 שעות; דיווח משלים על התקרית – תוך 72 שעות; ודו״ח מסכם ומלא על התקרית בתוך כחודש[119]. עשויים להידרש דוחות משלימים ככל שיש מידע חדש שלא דווח קודם לכן.

<u>סמכויות פיקוח ואכיפה</u>

הבקרה שביצעה הנציבות האירופית על היישום של דירקטיבת NIS העלתה כי צעדי הפיקוח והבקרה שהדירקטיבה העניקה למדינות השונות היו לא מספקים. ראשית, ביצוע ביקורת ואכיפה בדיעבד בלבד (*ex-post*) הוכחו כלא אפקטיביים, בעיקר בנוגע לספקים של שירותים דיגיטליים. שנית, בדומה להיבטים אחרים של הדירקטיבה, שררה שונות ניכרת בין סמכויות הפיקוח והאכיפה במדינות שונות.

[115] סעיף 21.2 סעיפים (a) עד (j), NIS 2.
[116] סעיף 14.3, NIS.
[117] סעיפים 23.2-23.1, NIS 2.
[118] סעיף 23.3, NIS 2.
[119] סעיף 23.4, NIS 2.

כך, NIS קבע כי לרשויות המוסמכות יהיו הסמכויות והאמצעים הדרושים להעריך עמידה של מפעילי שירותים חיוניים בהתחייבויותיהם לפי סעיף 14 (חובת ניהול הסיכון וחובת הדיווח); לרשויות המוסמכות יהיו הסמכויות והאמצעים לדרוש ממפעילים של שירותים חיוניים לספק (א) את המידע הדרוש להערכת אבטחת הרשת ומערכות המידע שלהם, לרבות תיעוד של מדיניות האבטחה; (ב) ראיות ליישום יעיל של מדיניות אבטחה, כגון תוצאות ביקורת אבטחה שבוצעה על ידי רשות מוסמכת או מבקר מוסמך, ובמקרה האחרון, לספק אותן לרשות המוסמכת[120].

NIS 2 מרחיב משמעותית את סל הכלים לפיקוח ואכיפה. לרשויות המוסמכות יהיו לכל הפחות סמכויות הפיקוח הבאות (*ex-ante*) במה שנוגע **לישויות חיוניות**: ביצוע ביקורות בחצרי הארגון או מרחוק, לרבות ביקורות רנדומליות המבוצעות ע"י אנשי מקצוע; ביצוע בדיקות אבטחה שוטפות; ביקורות ad-hoc לרבות על בסיס אירוע משמעותי; סריקות אבטחה מבוססות שיטה שקופה ופומבית של ניהול סיכונים; בקשה לדרוש מידע הנחוץ להערכת הצעדים שנקטה הישות ביחס לחובותיה לנהל את סיכוני הסייבר שלה; בקשה לגישה למידע, מסמכים ומידע הנחוצים לצורך ביצוע הפיקוח; בקשה לקבל ראיות לביצוע מדיניות הסייבר של הארגון[121].

סמכויות אכיפה יכללו לכל הפחות מתן אזהרות בדבר הפרה; אימוץ הוראות מחייבות, לרבות במה שנוגע לצעדים הכרחיים למניעה או טיפול באירוע סייבר; מתן הוראות לחדול מהפרה או לבצע במלואן את חובות הדיווח וניהול הסיכון; להורות לישות ליידע צדדים שלישיים על אירוע סייבר; להורות על ביצוע המלצות של גופי ביקורת, ועוד. אם כלל הצעדים האלה **לא הועילו, רשות מוסמכות יכולה להשעות זמנית רישיון של ישות עד לתיקון הליקויים, וכן להשעות אדם מתפקיד ניהולי בישות[122].**

ג. סיכום

בכל מדינות ההשוואה אימצו חקיקה מחייבת להגנת סייבר בארגונים חיוניים, הנשענת על שני נדבכים מרכזיים – חובת דיווח על אירועי סייבר וחובת ניהול סיכונים. בעוד שמודל הפיקוח משתנה בין מדינות (ריכוזי מול ביזורי), ניכרת מגמה עולמית של התכנסות לסטנדרטים של דירקטיבת NIS2 האירופית, המהווה כיום את נקודת הייחוס המרכזית בתחום. סטנדרט זה מרחיב משמעותית את רשימת הסקטורים המפוקחים, מחמיר את דרישות הדיווח (דיווח תלת שלבי בנוסף לדו"ח סיכום), ומפרט דרישות ניהול סיכון מפורטות יותר, לרבות עיסוק בשרשרת האספקה, הצפנה והיגיינת סייבר. להלן הצגה ויזואלית מסכמת[123].

[120] סעיפים 15.1-15.2, NIS.
[121] סעיף 32.2, NIS 2.
[122] סעיפים 32.4-32.5, NIS 2.
[123] הוכנה באמצעות Notebook LM.

הגנת סייבר על ארגונים חיוניים: מבט השוואתי

מדינות שונות בעולם אימצו מודלים רגולטוריים שונים להתמודדות עם איומי סייבר על ארגונים חיוניים. המודלים נשענים בעיקר על שני נדבכים מרכזיים: חובת דיווח על אירועים וחובת ניהול סיכונים. דירקטיבת NIS של האיחוד האירופי מהווה כיום את נקודת הייחוס המרכזית להתפתחות הרגולציה בתחום.

השוואה בין מדינות: אסדרת הגנת הסייבר על ארגונים חיוניים

	ארה"ב	הולנד	אוסטרליה	גרמניה	בריטניה
מודל רגולטורי	**מבוזר/מעורב:** אין חוק מדרלי אחיד; סוכנויות שונות מפקחות על סקטורים שונים.	**מבוזר:** בדומה לבריטניה, עם רשויות ייעודיות לכל סקטור.	**מעורב:** משרד הפנים הוא הגוף המרכזי, אך קיימת חלוקת סמכויות.	**ריכוזי:** המשרד הפדרלי לאבטחת מידע (BSI) הוא הגוף המרכזי.	**מבוזר:** רשויות ייעודיות לכל סקטור (Competent Authorities).
חובת דיווח על אירוע משמעותי	תוך 72 שעות (על אירוע) ותוך 24 שעות (על תשלום כופר).	בדומה לבריטניה וגרמניה, על בסיס דירקטיבת NIS.	תוך 12 שעות.	דיווח מיידי ל-BSI.	תוך 72 שעות.
חובת ניהול סיכון	אין חובה פדרלית אחידה; קיימת רגולציה סקטוריאלית "רכה" וחנחיות של CISA.	בדומה לבריטניה וגרמניה, על בסיס דירקטיבת NIS.	חובה להגיש תבנית ניהול סיכונים שנתית בהתאם לתקנים מוכרים (כמו ISO 27001).	נקיטת צעדים ארגוניים וטכניים בהתאם לסטנדרט העדכני (חזרנו State of the Art).	מבוססת על 14 עקרונות (CAF) וסטנדרטים ביג"ל.
פיקוח ואכיפה	סמכויות הפיקוח מבוזרות בין סוכנויות פדרליות שונות בהתאם לסקטור.	בדומה לבריטניה, על בסיס דירקטיבת NIS.	סמכויות רחבות למשרד הפנים, כולל מתן הוראות, הטלת קנסות, ובנוקרי קצה - התערבות ישירה במערכות.	סמכויות איסוף מידע, מתן הוראות והטלת קנסות ע"י ה-BSI.	סמכויות דרישת מידע, ביקורת, מתן התראות והטלת קנסות ע"י הרשויות המוסמכות.

נקודת הייחוס: עיקרי דירקטיבת NIS2 של האיחוד האירופי

הרחבה משמעותית של סקטורים

הדירקטיבה חלה על יותר סקטורים, כולל ניהול פסולת, דואר, ייצור מזון וכימיקלים.

האחדת ספי הכניסה

קביעת תבחינים אחידים ונורפים להגדרת "ארגון חיוני" ו"ארגון חשוב" לפי גודל ומחזור.

פירוט דרישות לניהול סיכונים

הגדרת רשימת מינימום של 10 אמצעים נדרשים, כולל אבטחת שרשרת אספקה והיינינת סייבר.

החמרת חובות הדיווח והאכיפה

קביעת לוחות זמנים מדויקים לדיווח (24 שעות ראשוני, 72 שעות משלים) וסמכויות פיקוח ואכיפה מורחבות.

NotebookLM

פרק רביעי – גיבוש חלופות, ניתוח והשוואה

א. סיכום ביניים: הגדרת הבעיה והגדרת מטרות ההתערבות

ארגונים בישראל, וביניהם ארגונים חיוניים, חשופים לאיום הולך וגדל של תקיפות סייבר. תקיפות אלה מסבות לכלכלה נזק עצום הנאמד במיליארדי ₪ מדי שנה, ועשויות לפגוע באופן משמעותי ברציפות התפקודית של המשק, הן בשגרה והן בחירום. על אף הנזקים הפוטנציאליים והממשיים לאינטרס הציבורי כתוצאה מתקיפות סייבר – ארגונים רבים אינם נוקטים באמצעים המינימליים להגן על עצמם בסייבר, ובכך מגבירים משמעותית את ההסתברות למתקפות סייבר מוצלחות ובעלות השלכות קשות. בעיה זו נעוצה בארבעה גורמים שונים: היעדר מודעות; א-סימטריה של המידע; החצנות שליליות, והיעדר דיווח ושיתוף מידע. כל אלה מועצמים ע"י הפערים במודל האסדרה הנוכחי.

כשלי שוק אלה, ובפרט החצנות שליליות והיעדר דיווח, מצדיקים התערבות ממשלתית **כלשהי** בתחום. כפי שראינו בפרק הקודם, התערבות זו לבשה צורה של **אסדרה חוקית** בכל אחת מ-5 המדינות שנבדקו במסגרת הלמידה הבינ"ל (ולמעשה ברוב מכריע של מדינות מערביות בשלות שווקים מפותחים).

מכל מקום, תכלית ההתערבות הממשלתית – הן אם בצורת אסדרה חוקית או בדרך אחרת - הינה טיפול באותם כשלי שוק, באופן שיאפשר העלאת רמת ההגנה של הארגונים החיוניים במשק, תוך ניסיון לצמצם במידת האפשר את הנטל הרגולטורי הכרוך בכך. העלאת החוסן ברמת הארגון הבודד צפויה להעלות בהתאמה גם את החוסן המשקי המצרפי, בעתות שגרה וחירום כאחד.

להלן המטרות הכלליות הנגזרות מן התכלית:

1. כינון מודל אסדרה לאומי, הכולל בין השאר חלוקת תפקידים, סמכויות ואחריות, לרבות בין מערך הסייבר והרגולטורים המגזריים;
2. יצירת רמה מינימלית משותפת ומחייבת של הגנת סייבר בארגונים החיוניים למשק הישראלי, בהתאם לעקרון של ניהול סיכונים;
3. יצירת מנגנון של דיווח ושיתוף מידע באופן שיסייע לשפר את רמת ההגנה המצרפית במשק;
4. עליה ניכרת בהיקף ובשיעור הארגונים החיוניים בישראל הנוקטים באמצעים הדרושים לצמצום סיכוני הסייבר שלהם, בהתאם לרמה המינימלית המשותפת המחייבת;
5. צמצום בהיקף האירועים המשמעותיים בעלי פוטנציאל נזק בסייבר בארגונים חיוניים בישראל;
6. שיפור ביכולת ההתמודדות עם תקיפות סייבר בזמן אמת, כמו גם יכולות ההתאוששות והחזרה לשגרה
7. צמצום השלכותיהן של תקיפות סייבר חמורות על ארגונים חיוניים בעלי משמעות לרציפות התפקודית של המשק, בשגרה ובחירום.

ב. חלופות שנשקלו

<u>אי התערבות - המשך המצב הקיים</u>

במסגרת חלופה זו כל רגולטור ממשלתי אמון על הגנת הסייבר בארגונים שתחת אחריותו, באמצעות הכלים הרגולטורים והסמכויות הפרטיקולריות שהוקנו לו עפ"י חוק, ככל שהוקנו כאלה, במסגרת ישום החלטות הממשלה הרלוונטיות 2443 ו-2444.

- *כלי המדיניות העיקרי של החלופה* הוא רגולציה של כללים מחייבים, על פי רוב במדרג נורמטיבי נמוך (חוזרי מנכ"ל, סעיפי רישיון, אישורי קב"ט וכיו"ב).
- ההוראות המגזריות, היכן שהן קיימות, לא כוללות בכל המקרים **גם** חובת דיווח על אירועי סייבר **וגם** הוראות הנוגעות לניהול סיכוני סייבר; קיימת שונות בהוראות בין מגזר למגזר.
- *על מי חלות ההוראות:* בחלק מהיחידות המגזריות, ההוראות והכללים חלים על כל הגופים המאוסדרים על ידן, כשהיחידה המגזרית מתעדפת את הפיקוח והבקרה בהתאם למדיניות אכיפה. בחלק אחר של היחידות, ההוראות דיפרנציאליות בהתאם למאפייני הארגון, לפי שיקול דעתו של הרגולטור ו/או תבחינים שקבע, ככל שקבע.
- *מנגנון הפיקוח והאכיפה:* בקרב חלק מהרגולטורים קיימות סמכויות לדרוש ידיעות ומסמכים, להיכנס למקום או לתפוס חפצים. כמו כן **לחלק** מהרגולטורים סמכות להטיל עיצומים מנהליים או קנסות, להורות על תיקון ליקויים, לבטל, להגביל או להתלות רישיון, ועוד. הסמכויות שונות בין מאסדר למאסדר.
- *מודל השינוי:* בהיעדר פעולה מונעת או מצמצמת כלשהי, גורמי השורש של הבעיה צפויים להיוותר על כנם, והיקף הנזקים כפי שתוארו בפרק ניתוח הבעיה צפוי לגדול; זאת, על בסיס ההנחה שהתוקפים נעשים מתוחכמים ומהירים יותר, שעה שמאמצי ההגנה אינם מדביקים את הפער באותו הקצב.
- ספציפית, אי-התערבות משמעה גם היעדר טיפול בפערים שהתגלו בעשור האחרון **במודל האסדרה**, ובכלל זה היעדר מסגרת חוקית המגדירה בבירור את חלוקת האחריות, הסמכויות וממשקי העבודה בין מערך הסייבר, הרגולטורים המגזריים והארגונים. כפי שכבר הוזכר, מצב זה יוצר חוסר סנכרון, ופוגע ביכולת לייצר תמונת מצב לאומית אפקטיבית בשגרה ובחירום.
- *השוואה בינ"ל:* חלופה זו אינה כוללת חקיקה לאומית רוחבית לצורך "יישור קו" וקביעת סטנדרט אחיד לארגונים חיוניים ולגופים המאסדרים – בניגוד גמור למה שראינו במדינות ההשוואה.
- *ישימות החלופה:* גבוהה – המשך המצב הקיים.

במסגרת חלופת אי-ההתערבות, המדינה נמנעת מנקיטת צעדים חדשים. המשמעות המעשית של בחירה בחלופה זו אינה קיפאון - **אלא החרפה ברמת הסיכון והנזק הכלכלי**, שכן קצב התחכום וההיקף של איומי הסייבר עולים בהרבה על קצב השיפור הוולונטרי בהגנה של הארגונים. חלופה זו צפויה לשמר אפוא את המצב בו מגזרים רבים נותרים עם רמת הגנה לא מספקת, וללא תמריץ לשינוי סדרי העדיפויות והקצאת המשאבים הנדרשת. כתוצאה מכך, החשיפה לנזקים עתידיים גדלה.

מבחינה כלכלית, חלופה זו אינה גוררת אמנם עלויות אסדרה או ציות חדשות, אך היא טומנת בחובה **עלות אלטרנטיבית כבדה** של נזקים ישירים מתקיפות, לצד פגיעה עקיפה בסביבה העסקית. בהקשר זה, היעדר יישור קו עם מגמות האסדרה העולמיות עלול להרתיע משקיעים זרים המחפשים יציבות וביטחון בתשתיות, ולפגוע במוניטין ובאטרקטיביות של המשק הישראלי.

<u>רגולציה עצמית (וולונטרית)</u>

בחלופה זו מוצע כי הארגונים החיוניים יקבעו כל אחד לעצמו אמות מידה לניהול סיכוני סייבר, בין היתר בהתאם לסכמות, מדריכים ו/או תקנים לאומיים או בינ״ל לא מחייבים. הארגונים ידווחו על כך לרגולטור, והוא יפרסם את המידע לציבור. הציבור יוכל לשקול את רמת ההגנה בסייבר של הארגון טרם קבלת שירותים מהארגון החיוני. הבחירה שבידי הצרכן אמורה להוות תמריץ חיובי לארגון החיוני לקבוע סטנדרטים ראויים להגנת סייבר, ולעמוד בהם.

חלופה זו פחות מתאימה כפתרון להעלאת רמת הגנת הסייבר **בארגונים חיוניים**. מודל של רגולציה עצמית מתאים יותר לשוק חופשי שבו לצרכן יש מרחב גדול במיוחד לבחירה וברירה בין חלופות. בשוק הישראלי הקטן והריכוזי, בוודאי במה שנוגע לשירותים חיוניים כמו בתי חולים, משרדי ממשלה, שירותי תחבורה, יצרני אנרגיה וכדומה – נראה שהציפייה כי הצרכן יבחר בנותן השירות בעל הגנת הסייבר הטובה ביותר אינה מציאותית. בהתאם, לא נמצא כי חלופה זו ננקטה באף אחת ממדינות ההשוואה.

עוד כדאי להביא בחשבון כי *גם היום* חלק גדול מהארגונים החיוניים חופשיים לנהל את סיכוני הסייבר שלהם כראות עיניהם ולטובת האינטרסים העצמיים שלהם ולפרסם את המידע לציבור; ואולם, כפי שראינו בפרק ניתוח הבעיה – רבים מהם עדיין בוחרים שלא לעשות זאת. בין אם כתוצאה מחוסר מודעות, מחסור במידע, הנוחות שבהחצנת הנזק למקבלי השירות או רצון להימנע מדיווח – לא נמצא עד כה שארגונים חיוניים – ודאי לא כולם - התכנסו *וולונטרית* סביב סטנדרט מספק של הגנת סייבר, על אף היתרונות שצעד כזה כולל עבור רמת ההגנה שלהם. לכן חלופה זו לא צפויה לפתור בצורה מניחה את הדעת את הסוגיות שזוהו כגורמי שורש לבעיה. כמובן שגם אין בה כדי לתקן את הפערים במודל האסדרה הנוכחי.

<u>זכויות תביעה אזרחיות</u>

בחלופה זו נשקל לתת אפשרות למי שנפגעו כתוצאה מאירוע סייבר בארגון חיוני לתבוע את הארגון בגין הנזק שנגרם להם, ולקבל ממנו פיצוי בהתאם. להלכה, האיום האפשרי של מתן פיצוי כספי לנפגעים אמור לתמרץ את הארגונים להעלות את רמת הגנת הסייבר שלהם באופן וולונטרי, כדי לצמצם את האפשרות לאירועי סייבר חמורים, ובהתאם, למנוע תשלום פיצוי לנפגעים מהם.

הבעיה בחלופה זו היא שלא נראה שביכולתה להשפיע באופן ממשי על הסיכון: האפשרות לתבוע אזרחית ארגון בשל אי-הקפדה מספקת או אפילו רשלנות בהגנת סייבר קיימת כבר היום, וראו למשל

בהקשר זה מס׳ תביעות יצוגיות שהוגשו בשנת 2021 כנגד חברת שירביט[124]. אף על פי כן, כעניין של עובדה, דרך פעולה זו אינה מנוצלת לעתים תכופות על ידי הציבור, אולי משום שהיא כרוכה בהתדיינות ארוכה וסבוכה בבתי המשפט. מנקודת מבט משפטית, הוכחת הנזק עשויה להיות מורכבת, והפיצוי עשוי להיות לא מרתיע דיו (כפי שקרה אמנם במקרה שירביט, שם נפסקו כ-5 מלש״ח בסה״כ, כשסכום הפיצוי לכל נפגע עמד על כמה מאות ₪ לכל היותר). מבחינה זו, נראה אפוא כי התמריץ המשפטי לא הוכיח עצמו.

חיסרון יסודי נוסף של החלופה הוא שהיא מניעה לפעולה בדיעבד, לאחר תקיפת סייבר, ומעניקה תמריץ נמוך יחסית לפעולה מונעת מקדימה, לפני התקיפה.

החלופה לא פותרת באופן ישיר את בעיית המודעות והא-סימטריה של המידע. היא עשויה, תיאורטית, לתת מענה לבעיית ההחצנות השליליות, אך מבחינה מעשית ראינו כי עד כה כשלה בכך. בדומה לחלופה של רגולציה עצמית, נראה כי מודל של זכויות תביעה אזרחיות מתאים פחות לפתרון הבעיה בארגונים חיוניים, שמטבעם מצוידים במחלקות משפטיות ענפות, כשלמקבל השירות יש מעט יכולת להתמודד עמן בהתדיינויות משפטיות. גם מבחינה זו, נראה כי החלופה לא צפויה לפתור באופן משמעותי את הבעיה.

<u>פעולות הסברה, חינוך ומודעות</u>

מוצע להוציא לפועל תכנית הסברה, חינוך ומודעות אשר תטפל בבעיית חוסר-המודעות של הארגונים החיוניים והנהלותיהם לסיכוני סייבר. במסגרת זו יבוצעו פרסום באמצעי תקשורת ההמונים (טלויזיה, רדיו), קמפיינים ממומנים ברשתות החברתיות, וכן הגברה של מאמצי ההסברה מטעם היחידות המגזריות מול הארגונים החיוניים בענפי המשק אותם הן מאסדרות (היכן שקיימות יחידות כאלה). מדובר בחלופה לא רגולטורית, שאינה כוללת הוראות מחייבות.

יתרונה של החלופה בכך שהיא נותנת מענה לאחד מגורמי השורש של הבעיה – חוסר מודעות: משעה שנוצרה המודעות, אחד מגורמי השורש של הבעיה בא לכאורה על פתרונו – כך שארגונים חיוניים עשויים להסדיר טוב יותר, ובכוחות עצמם, את הגנת הסייבר שלהם.

ואולם, מנקודת מבט של ניהול סיכונים, החלופה המוצעת עדיין מותירה את הבחירה אם לנקוט באמצעים להגנת סייבר בידי הארגונים עצמם. זוהי אפשרות מתקבלת על הדעת ביחס לארגונים קטנים ובינוניים, שההשפעה של כל אחד מהם *בנפרד* על המשק הישראלי אינה משמעותית ברמה הלאומית; אך היא פחות מתאימה כשאנו עוסקים בארגונים החיוניים לתפקודו התקין והרציף של המשק, הנתונים לאיומים מצד קבוצות תקיפה מדינתיות או סמי-מדינתיות. מבחינה זו, יש בהחלט מקום להגברת מאמצי ההסברה, החינוך והמודעות (בעיקר ביחס לארגונים בינוניים, קטנים ואפילו זעירים) – אך **לבדה** היא אינה יכולה לשמש פתרון אפקטיבי להעלאת רמת ההגנה **ביחס לאותם גופים המהווים את הסיכון הגדול ביותר**.

[124] https://www.calcalist.co.il/local_news/article/rketdjrd3.

<u>תמריצים כלכליים</u>

חלופה זו מציעה לקדם את הגנת הסייבר של ארגונים חיוניים באמצעות שני סוגי תמריצים כלכליים: **ישירות** - באמצעות פיצוי מדינתי לארגון שנתקף בסייבר, בתנאי שעמד בסטנדרטים מינימליים של הגנה; **ובעקיפין** – דרך מנגנון של חובת ביטוח סייבר.

כפי שראינו לעיל בכמה חלופות, גם המודל של פיצוי ישיר עשוי להתאים לארגונים קטנים ובינוניים יותר מאשר לארגונים חיוניים. מנקודת מבט של ניהול סיכונים, המדינה אינה יכולה לקחת את הסיכון שמא קבוצה מסוימת של ארגונים חיוניים תחליט "לחיות עם הסיכון" ולוותר על התמריץ המוצע לה. בהנחה שלעולם תהיה קבוצה (גם אם קטנה) של ארגונים שיבחרו שלא לנצל את התמריץ, הרי זהו סיכון שיתכן וניתן לקחת ביחס לכמה אלפי עסקים קטנים ובינוניים – אך **לא ראוי לקחת ביחס לארגונים החיוניים ביותר לתפקוד התקין של המשק והחברה הישראלית.**

הדבר נכון כמובן גם ביחס למודל הביטוח, אלא שלגביו יש לקחת בחשבון נתונים נוספים: כידוע, רכישת ביטוח סייבר מחייבת תהליך חיתום לאישור הפוליסה. כך, הצעת המחיר של חברת הביטוח (=הפרמיה שישלם הארגון) תביא לידי ביטוי את הערכת המבטח לרמת הסיכון של הארגון, סביבתו העסקית, מורכבותו הטכנולוגית, וכן את אמצעי ההגנה שנקט כדי לצמצם את הסיכון. מאחר וחברת הביטוח תישא ב"עלות הטעות" סביר שהיא תדרוש מרווחי הגנה נוספים ברמת ההגנה הנדרשת מהגוף. על פי רוב דרישות אלה דומות בצורה משמעותית לדרישות המופיעות בתקנים בינ"ל דוגמת ISO ו-NIST.

בחלק לא מבוטל מן המקרים המשמעות הכלכלית של רכישת ביטוח סייבר לארגון כוללת **גם** את מחירי הפרמיה **וגם** את העלויות של העלאת רמת ההגנה הנדרשת בתהליך החיתום. מבדיקה שביצע מערך הסייבר, פרמיות ביטוח סייבר לרוב נעות בין אלפי דולרים בודדים עבור עסקים קטנים ויכולים להגיע למאות אלפי דולרים בשנה ואף למיליוני דולרים לחברות ציבוריות. היחס בין הפרמיה השנתית המשולמת על ידי הארגון לתקרת הכיסוי משתנה בהתאם לגורמים רבים, אך נע בממוצע בין 0.1% ל-1.5% מתקרת הכיסוי (לדוגמה, אם היחס עומד על0.8% - הארגון ישלם פרמיה שנתית של 400,000 אלף דולר, בגין כיסוי של עד 50 מיליון דולר)[125].

מהבדיקה שביצע אגף הכלכלן הראשי במערך הסייבר עלה גם כי הן באירופה והן בישראל, חברות גדולות נוטות לבטח עצמן בביטוח סייבר יותר מאשר חברות קטנות ובינוניות[126]. נתון זה מטיל בספק את היעילות של הטלת ביטוח חובה, היות ויש אינדיקציות ראשוניות לכך שהשוק עשוי להתקדם בכיוון זה בכוחות עצמו. מכל מקום, תחום ביטוח הסייבר נחשב לתחום דינמי ומתפתח, בו המודלים האקטואריים עדיין אינם מגובשים במלואם לאור מחסור בבסיסי נתונים רחבים ומהימנים שהצטברו לאורך מספר רב של שנים.

[125] על סמך שיחות שקיים צוות הכלכלן הראשי במערך הסייבר עם גורמים בשוק הביטוח.

[126] סקר שימושים בטכנולוגיות מידע ותקשורת (ICT) והגנת סייבר בעסקים (2020) של הלמ"ס; 33% מהחברות הגדולות (מעל 250 עובדים) היו מבוטחות בביטוח סייבר, לעומת 9% בלבד מהחברות הקטנות (מתחת ל-50 עובדים). לפי נתוני Eurostat (2022) שיעור החברות הגדולות המבוטחות באירופה הוא 45%, בעוד בארגונים בינוניים השיעור עומד על 35% ובקטנים על 22%.

שיקולים נוספים שבגינם יש מקום להיזהר מהלטיל **חובת** ביטוח סייבר הם כדלקמן:

- שונות בין הארגונים – לאור שונות בין הארגונים החיוניים בהיבטי מאפייני העסק (כגון: כמות עובדים, מורכבות טכנולוגית, מצב פיננסי, ענף עיסוק), לא ניתן לתת המלצה גורפת לרכש/חיוב ברכש לעסק.
- עלויות עודפות – כאמור, הטלת חובת ביטוח מייצרת בהכרח מצב שבו הארגון מוציא כספים הן על העלאת רמת ההגנה שלו והן על תשלום הפרמיה לחברת הביטוח - סכום שיכול להגיע גם למאות אלפי דולרים בשנה. ואולם, ניתן להעלות את רמת ההגנה גם מבלי לשלם את הפרמיה.
- קבוצה ריקה – יתכן שבחלק מהארגונים קיימת רמת הגנה מספקת. בקרב קבוצה זו הטלת החובה לרכוש ביטוח סייבר לא תביא לשיפור רמת ההגנה, אלא תהווה התערבות שלא לצורך בניהול הסיכונים הפיננסי שלהם.
- השוואה בינלאומית – בבדיקה שקיימנו לא נמצאה מדינה המחייבת או ממליצה באופן ישיר לרכוש ביטוח סייבר. לחילופין, בארה"ב, בריטניה ואוסטרליה קיימת **המלצה לבחון** רכישת ביטוח כאמור.

<u>העלאת רמת האבטחה של מוצרים דיגיטליים (חקיקה/וולונטרית)</u>

כזכור, הגנת סייבר נשענת על שלוש רגליים: אנשים, תהליכים וטכנולוגיה (מוצרים). כפי שראינו לעיל, שלושה מארבעת גורמי השורש שהצבענו עליהם כמקור לבעיה נוגעים בעיקר לאנשים ותהליכים: היעדר מודעות, החצנות שליליות והיעדר דיווח ושיתוף מידע.

שונה בהקשר זה הוא גורם השורש של א-סימטריה במידע, לפחות במובן של א-סימטריה במידע בין תוקפים לנתקפים ובין יצרני התוכנות והחומרות לבין הארגונים העושים בהם שימוש. עולה השאלה – האם טיפול בגורם השורש <u>הטכנולוגי</u> הזה בצורה מבנית כלשהי, עשוי להפחית את התלות של הארגון באנשים ובתהליכים, ובכך לצמצם את הסיכון לתקיפות סייבר משמעותיות.

בדיקה שביצע מערך הסייבר העלתה כי בכמה מדינות בעולם ביקשו לטפל ברמת המוגנות של מוצרים דיגיטליים, אם כי בדרכים שונות: חלק מהמדינות אימצו **(לצד** חוק הסייבר הלאומי שלהן, לא במקומו) חקיקה המחייבת מוצרים דיגיטליים לעמוד בחובות אבטחה מסוימות. הדוגמה הבולטת ביותר לכך היא ה- Cyber Resilience Act (CRA)[127] של האיחוד האירופי, שנכנס לתוקפו בחודש דצמבר 2024 ויחול באופן מחייב על היצרניות החל מדצמבר 2027. החוק מטיל חובה על יצרני חומרה ותוכנה לעמוד בדרישות אבטחה בתכנון, עיצוב, פיתוח, ייצור, אספקה ותחזוקה של מוצרים דיגיטליים, תוך התייחסות ממוקדת לטיפול בחולשות (זיהוי, תיעוד, עדכוני אבטחה ויידוע המשתמשים).

[127] https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

מדינות אחרות, כמו גרמניה, סינגפור ופינלנד, החילו תכניות תיוג (labeling) מחייבות – הדורשות מיצרנים ומשווקים לסמן על גבי המוצרים הדיגיטליים את רמת האבטחה שלהם. כאן הציפיה היא שהמידע שינתן לצרכן יעודד אותו לרכוש את אותם מוצרים המסומנים כבטוחים יותר לשימוש דיגיטלי. באוסטרליה, הודו, ויאטנם, יפן ומצרים קיימות המלצות לא מחייבות של התעשיה (Code of Practice) לבצע סימון כאמור.

הבעיה היא שאין ביכולתה של הממשלה להטיל את החובות האמורות – בין אם בחקיקה או דרך תכנית תיוג – אך ורק על יצרנים ומשווקים המפיצים למשק מוצרים דיגיטליים שיהיו בשימוש ארגונים חיוניים. היצרן, היבואן והמשווק לא יודעים למפרע אם מי שישתמש במוצר הוא אדם פרטי, עסק קטן או ארגון חיוני. אם יאומץ פתרון כמוצע בחלופה האמורה – הרי שמאליו הוא חייב **לחול על כלל היצרנים, היבואנים והמשווקים של מוצרים דיגיטליים.**

להחלה *רחבה ואוניברסלית* של פתרון כזה יש כמה חסרונות בהקשר של העלאת רמת הגנת הסייבר בארגונים חיוניים:

- חלק ניכר מסיכוני הסייבר נובעים מתקיפות הנדסה חברתית (בפרט דיוג), היעדר היגיינת סייבר בסיסית (למשל סיסמאות חלשות או היעדר הזדהות כפולה) ועוד. טיפול ברמת האבטחה של מוצרי סייבר לא יודע לתת מענה לסיכונים האלה – שהשלכותיהם בארגונים חיוניים עלולה להיות חמורה במיוחד. במילים אחרות, החלופה מטפלת אמנם בהיבט ה"מוצרים" (Products/Technology), אך אינה מטפלת בהיבטי האנשים (People) והתהליכים (Processes). כזכור, רוב גורמי השורש לבעיה שהצבענו עליהם בפרק הניתוח משתייכים לשני היבטים אלה.
- בדומה לחלופות אחרות שהזכרנו לעיל, המודל של <u>תכנית תיוג</u> (בין אם מחייבת או וולונטרית) נראה כפתרון פחות מתאים להעלאת רמת ההגנה בארגונים חיוניים. ההגיון של חלופת התיוג (labeling) הוא במתן מידע לצרכן, באופן שיסגור את פערי המידע שלו מול היצרן, ויאפשר לו לקבל החלטה מושכלת (במקרה זה – לרכוש מוצר דיגיטלי מאובטח ומוגן יותר). ואולם, לצרכן עדיין יש את החופש לבחור במוצר מאובטח פחות, או לא מאובטח כלל. זה סיכון שהממשלה יכולה לנהל כשמדובר בעסקים קטנים ובינוניים, או באנשים פרטים; אך לא בנוגע לארגונים החיוניים ביותר של המדינה.
- עוד כדאי להזכיר כי לפי דו"ח ה-RIA שליווה את חקיקת ה-PSTI בבריטניה, היעילות של תכניות תיוג מוגבלת באופן יחסי: הממשלה שם צופה שינוי של 19% בלבד לטובת רכישת מוצרים מאובטחים, בפרק זמן של 10 שנים[128]
- מבחינה זו, חלופה טובה ומידתית יותר עשויה להיות הטלת חובה **על הארגונים החיוניים עצמם** – צד ה"ביקוש" – לעשות שימוש אך ורק במוצרים בעלי סטנדרט אבטחה מספק, בהתאם למדיניות ניהול הסיכונים של עצמם ו/או בהתאם להנחיות הרגולטור. כפי שראינו בפרק הסקירה הבינ"ל, זהו אחד המרכיבים בדרישות רמת ההגנה שממשלות שונות השיתו על ארגונים חיוניים במסגרת חקיקת הסייבר שלהן.

[128] Pp.4 ,https://assets.publishing.service.gov.uk/media/627a7730d3bf7f5c05c3eee0/Impact_Assessment.pdf

<u>רישיון</u>

חלופה זו מציעה *להתנות מראש בתנאי הרישיון* של ארגונים חיוניים במשק עמידה בחובות הגנת סייבר בסיסיות, בהתאם לתקינה ישראלית או בינ״ל מקובלת. תחת זאת, ארגון לא יוכל לשמש שחקן במשק אם **מלכתחילה** לא הבטיח עמידה בתנאים מסויימים שיקבע הרגולטור (בין אם הרגולטור המגזרי או מערך הסייבר הלאומי כמנחה מקצועי). יכול שהדרישות יהיו שונות בין מגזר אחד למשנהו, בשל השוני האינהרנטי בין המגזרים השונים, תחומי העיסוק שלהם, וסיכוני הסייבר שהם חשופים להם. משמעות הדבר היא בהכרח עלייה ברמת ההגנה של הארגונים, היות והם מחויבים לה כתנאי מקדים לפעילותם במשק.

כעניין של עובדה, חלק ניכר מהארגונים החיוניים שבהם אנו עוסקים הם עסקים טעוני רישיון ממילא: בתי חולים, חברות תחב״צ גדולות, יצרני אנרגיה משמעותיים, חברות תקשורת גדולות וכיו״ב. בחלק מהמגזרים כבר היום קיימות דרישות הגנת סייבר כחלק מתנאי הרישיון. אף על פי כן, רגולטורים מגזריים שיש להם כבר היום הסמכות להתלות רישיונות בגין, למשל, אי-דיווח על אירוע סייבר – מעולם לא עשו בה שימוש, ככל הנראה בשל היותה צעד לא-מידתי נוכח מהות ההפרות שבוצעו עד היום.

מדובר אם כן בחלופה שהיא גם רדיקלית למדי, אך גם לא מאוד מעשית, שכן הממשלה אינה יכולה לאפשר מצב שבו ארגונים חיוניים יחדלו מלפעול עד שיעמדו בתנאי הרישיון. לכל הפחות, נדרשים כלים נוספים לאכיפת דרישות הגנת סייבר, פרט לסמכות להתלות רישיון.

<u>אסדרה לאומית</u>

חלופה זו מציעה להסדיר את הגנת הסייבר בארגונים חיוניים במשק באמצעות **חקיקה לאומית** אשר תגדיר חובות מינימליות לרמת הגנה וניהול סיכונים, וכן חובת דיווח על תקיפות סייבר חמורות. החקיקה תעניק סמכויות פיקוח ואכיפה ייעודיות, לרבות סמכות להטלת עיצומים מנהליים מרתיעים על ארגונים שלא יעמדו בחובות החוק.

- **כלי המדיניות העיקרי של החלופה:** רגולציה של כללים מחייבים, במדרג נורמטיבי גבוה של **חקיקה ראשית**.
- **עיקר תוכנן של ההוראות:** החובה לדווח על תקיפת סייבר חמורה והחובה לעמוד ברמת הגנה נדרשת – שמשמעותה המעשית ביצוע סדרת פעולות אשר מפחיתות משמעותית את הסיכון הנובע מתקיפות סייבר, בהתאם לעקרונות של ניהול סיכונים.
- **על מי יחולו ההוראות:** מתוך תפיסה של ניהול סיכונים, מוצע להחיל את החובות אך ורק על **ארגונים חיוניים** במשק, וזאת על מנת לצמצם את הנטל הרגולטורי ולהחילו על אותם ארגונים שמהם נשקף הסיכון הגבוה ביותר לציבור. הארגונים יקבעו בהתאם לתבחינים אוניברסליים ושקופים בכל ענף משק.

- **מנגנון הפיקוח והאכיפה:** פיקוח ואכיפה קלאסיים, באמצעות דרישת ידיעות ומסמכים וכניסה למקום, לצורך פיקוח ובקרה על יישום ההוראות. אי-עמידה בהוראות החוק עלולה לגרור הטלת עיצומים כספיים ואף להוות עבירה פלילית במקרים של הפרת הוראות שיפורטו בחוק.
- **מודל השינוי:** פיקוח ואכיפה קלאסיים מעודדים ומחייבים ציות. החשש מעיצומים כספיים גבוהים ומענישה צפוי להניע את הארגונים להקפדה על הוראות החוק ולפתור את הבעיה של החצנות שליליות - שכן המודל אינו מסתמך על רצונם הטוב של הארגונים אלא מחייב אותם לפעול.
- **השוואה בינ"ל:** כפי שראינו, חלופה זו של אסדרה חוקית היא החלופה המובילה במדינות ההשוואה (ולמעשה ברוב מכריע של המדינות המערביות), בדגש על האיחוד האירופאי. NIS2-מרחיבה את היקף הגופים המאוסדרים (יותר מכפי הצפוי בהצעה הישראלית – ראו לעניין זה בפרק ו'), ומחמירה את דרישות הדיווח וניהול הסיכונים הנדרשות מארגונים חיוניים.
- **ישימות החלופה:** החלופה מצריכה קידום חקיקה ראשית. מגמות האסדרה בעולם, כמו גם הצורך הגובר בטיפול בסיכוני סייבר ברמה הלאומית, מהווים תנאים תומכים לקידום מהלך כזה.

ג. השוואה בין חלופות

על מנת לבסס את הבחירה בחלופה המיטבית, ובהמשך לתיאור החלופות השונות, להלן ניתוח משווה המסכם את היתרונות והחסרונות של כל אחת מהן. הניתוח הוא ניתוח רב-משתני והוא יביא בחשבון את השיקולים הבאים:

- אפקטיביות בהפחתת הסיכון – קרי, עד כמה החלופה מסוגלת לצמצם בפועל את הסיכון לפגיעה ברציפות התפקודית של המשק; בהקשר זה יובאו בחשבון גם מטרות ההתערבות כפי שנוסחו בראשית הפרק;
- טיפול בכשלי שוק - היכולת של החלופה לפתור את בעיות השורש המבניות, ובראשן ההחצנות השליליות ופערי המידע (א-סימטריה);
- עיתוי ההשפעה - האם החלופה פועלת כצעד מניעתי (Ex-Ante) או כתגובה בדיעבד(Ex-Post); האם היא תורמת לבניית חוסן (Resilience);
- שיקולי עלות-תועלת - הערכת היעילות הכלכלית והנטל המושת על הארגונים – בשלב זה נציג שיקול זה ברמת המאקרו; ניתוח כלכלי מעמיק יבוצע לחלופה הנבחרת, בפרק הבא;
- התאמה למגמות בינ"ל - מידת ההלימה לסטנדרטים המקובלים במדינות המערב, בדגש על הרגולציה האירופית והאמריקאית.

בשלב זה נשמיט מן הניתוח את חלופת הרישיון ואת חלופת ההסברה. מהטעמים שהבאנו לעיל ברור כי מדובר בחלופות פחות רלוונטיות לבעיה שבה אנו עוסקים (כל אחת מסיבות שונות).

קריטריון השוואה	**אי-התערבות (המצב הקיים)**	**רגולציה עצמית (וולונטרית)**	**זכויות תביעה אזרחיות**	**תמריצים כלכליים / ביטוח**	**רגולציה על מוצרים (Product Security)**	**אסדרה חוקית מחייבת (החלופה הנבחרת)**
מנגנון הפעולה	המשך סמכויות קיימות (אם ישנן) ללא מסגרת לאומית אחידה.	הארגון קובע לעצמו סטנדרט ומדווח לציבור; הצרכן "בוחר" בבטוח ביותר.	הניזוק תובע את הארגון לאחר נזק; החשש מתביעה אמור לתמרץ הגנה.	פיצוי מדינתי לנתקף או חובת ביטוח; חברת הביטוח מכתיבה סטנדרטים.	חיוב יצרנים לעמוד בסטנדרטים (כגון Cyber Resilience Act).	**חקיקה ראשית** הקובעת חובות ניהול סיכון, דיווח וסמכויות אכיפה (עיצומים).
אפקטיביות בהפחתת סיכון (בארגונים חיוניים)	**נמוכה.** המצב הנוכחי הוכיח שאינו מספק; פערי הגנה משמעותיים נותרים בעינם בחלק לא מבוטל של הארגונים והמגזרים.	**לא מספקת.** לא מוביל בהכרח לשיפור ההגנה בארגונים חיוניים, בעיקר היכן שהמודעות נמוכה ויש תמריץ חזק להחצנות שליליות	**נמוכה.** הפיצוי הנפסק (דוגמת "שירביט") נמוך ולא מייצר הרתעה מספקת.	**בינונית.** תלוי בבשלות שוק הביטוח; ההחלטה עדיין אצל המבוטח אם לבטח (ולנקוט אמצעים כדי להבטיח פרמיה סבירה)	**חלקית.** מטפל בטכנולוגיה אך לא ב"גורם האנושי" (פישינג, סיסמאות) המהווה רוב הסיכון.	**גבוהה.** מחייבת סטנדרט אחיד, סוגרת פערים ומצמצמת החצנות שליליות.
טיפול בכשלי שוק (החצנות, מידע, מודעות)	לא מטפל. כשלי השוק נותרים בעינם.	לא מטפל בהחצנות שליליות; חשש שארגונים יעדיפו לחסוך עלויות ולהטיל סיכון על הציבור.	מטפל חלקית ובדיעבד; לא פותר את בעיית המידע (א-סימטריה) מול הארגון החזק.	עלול ליצור "סיכון מוסרי" (Moral Hazard) – הסתמכות על הביטוח במקום על מניעה.	מטפל בא-סימטריה טכנולוגית, אך לא בכשל הניהולי/תהל יכי בארגון.	כופה הפנמת עלויות (טיפול בהחצנות), סוגר פערי מידע (חובת דיווח).
עיתוי ההשפעה	-	תלוי רצון טוב.	**בדיעבד** (Ex-Post). רק לאחר שנגרם נזק מתבצעת הפעולה.	מניעתי, אך תלוי בחידוש פוליסות ובתנאי שוק משתנים.	מניעתי (Design), אך ההשפעה איטית.	**מניעתי ושוטף.** דרישה מתמדת לעמידה בסטנדרט וניהול סיכונים.
עלות ונטל רגולטורי	נמוך לטווח קצר, אך הולך וגדל בטווח הארוך (בשל גידול בהיקף ותחכום התקיפות)	נמוך לארגון, גבוה לציבור (שנושא בסיכון).	עלויות משפטיות גבוהות (התדיינות בבתי משפט), יעילות נמוכה.	**גבוה** - "קנס כפולי": תשלום גם לפרמיה וגם להגנה.	גבוה ליצרנים וליבואנים (מתגלגל לצרכן).	בינוני-גבוה לארגון (השקעה בהגנה), אך **החזר השקעה חיובי** למשק במניעת נזק (ראו פירוט בהמשך).

התאמה למגמות בינ"ל (Benchmarking)	מנוגד למגמה (העולם מחמיר רגולציה).	לא קיים במדינות ההשוואה עבור ארגונים חיוניים.	ככל הנראה קיים כמשלים, אך לא כפתרון מרכזי באף מדינה.	מומלץ ככלי משלים (ארה"ב, אנגליה), אך לא מנדטורי ובכל מקרה לא כתחליף לרגולציה.	מגמה עולה (EU CRA), אך תמיד **לצד** חוק סייבר לאומי, לא במקומו.	**הסטנדרט המוביל.** תואם לדירקטיבת ה-NIS2 האירופית ולחקיקה בארה"ב ואוסטרליה.

ד. סיכום ובחירה בחלופה המועדפת

ניתוח החלופות השונות מעלה תמונה ברורה: מנגנוני השוק החופשי וההסדרה העצמית אינם מספקים בהכרח מענה הולם לסיכונים המערכתיים הניצבים בפני המשק הישראלי. קצב ההגנה הוולונטרי של הארגונים (גם אם לא כולם) עדיין איטי יחסית להיקף התקיפות ורמות התחכום שלהן (כפי שהצגנו בפרק בשני). כשהגורם האנושי מעורב בשיעור כה גבוה של תקיפות סייבר (גם בהקשר זה הוצגו נתונים בפרק השני) – נראה שהסתמכות על פתרונות טכנולוגיים **בלבד** (כגון רגולציה על מוצרים) או על כוחות שוק, מותירה לפחות חלק מהארגונים (ובכלל זה הארגונים החיוניים) חשופים לכשלים בתהליכים ובמודעות עובדים.

בחינת החלופות הלא-רגולטוריות העלתה כי הן סובלות מחסרונות מהותיים: הסתמכות על תביעות אזרחיות נראית דה-פקטו כלא-מרתיעה (כפי שנלמד למשל ממקרה "שירביט"), שכן היא פועלת בדיעבד ואינה מייצרת תמריץ מניעתי מספק. תמריצים כלכליים וביטוח נראים פתרונות חלקיים בלבד, המטילים נטל כספי כפול על הארגון ואינם מבטיחים כיסוי לארגונים בסיכון גבוה. רגולציה עצמית מתאימה אולי לעסקים קטנים (ובחלק מהארגונים הגדולים מאוד), אך המדינה אינה יכולה להמר על רצון טוב כאשר מדובר בתשתיות חיוניות שקריסתן תפגע ברציפות התפקודית של המשק.

לעומת זאת, החלופה של אסדרה חוקית מחייבת מסתמנת כפתרון האפקטיבי והבשל ביותר, ולראיה היא קיימת במדינות מערביות בעלות שווקים מפותחים כבר מאמצע העשור הקודם. גם דו"ח הפורום הכלכלי העולמי (WEF 2024) מספק לכך תימוכין אמפיריים חזקים: 60% מהמנהלים הבכירים מסכימים כיום כי רגולציה בתחומי הסייבר והפרטיות מפחיתה בפועל את הסיכון באקו-סיסטם של הארגון שלהם – עלייה של 21% בהשוואה לשנת 2022. הדו"ח מדגיש כי "רגולציה אפקטיבית מרימה את כל הסירות" (Effective regulation lifts all boats), קרי – היא מייצרת רשת ביטחון בסיסית המקדמת את רמת ההגנה בסייבר בכל המשק[129].

לחילופין, ENISA, הגוף הטכני להגנת סייבר של האיחוד האירופאי, ביצע סקר בקרב 947 חברות אירופאיות ב-27 מדינות האיחוד כשלוש שנים לאחר כניסתה של NIS לתוקף. כ-50% מן המגיבים ציינו כי **לאסדרה הייתה השפעה משמעותית או משמעותית מאוד של רמות אבטחת המידע שלהם.** 50% מהמשיבים גם ציינו כי יישום הדירקטיבה האירופאית חיזק את יכולות הניטור שלהם (ב-2022 נתון זה צמח ל-62%), וכרבע, 26%, אמרו כי הדירקטיבה שיפרה את היכולת שלהם להתאושש

[129] https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf, עמ' 31.

מתקיפת סייבר[130]. יתכן כי לממצאים אלה היה קשר להרחבת הדירקטיבה כפי שבאה לידי ביטוי ב-2NIS: חוות הדעת של מועצת האיחוד קבעה כי "**ללא הרחבה של החובות הרגולטוריות, מספר תקיפות הסייבר באיחוד האירופאי צפוי לגדול,** ולהשית עלויות גדולות יותר – הן על הארגונים הנתקפים עצמם, אך גם על הכלכלות האירופאיות ואזרחיהן בכללותן[131]."

נוכח הכישלון של מנגנוני השוק ליצור רמת הגנה מספקת בכוחות עצמם, והצורך הדחוף בטיפול בהחצנות שליליות, **החלופה הטובה ביותר היא אסדרה חוקית מחייבת**. חלופה זו תייצר סטנדרט אחיד של ניהול סיכונים וחובת דיווח, תיישר קו עם הנורמות הבינלאומיות (כדוגמת דירקטיבת ה-NIS2 האירופית), ותבטיח כי הגנת הסייבר בארגונים חיוניים תנוהל כאינטרס לאומי מחייב ולא כשיקול עסקי וולונטרי. החלופה היא חלופה **בעלת השפעה משקית** כהגדרתה בחוק עקרונות האסדרה (ראו פירוט בנושא זה בפרק הבא).

[130] NIS IMVERSTMENT, pp. 6, 66-67 . https://www.enisa.europa.eu/publications/nis-investments-2021 ; NIS INVESTMENT, pp. 39. https://www.enisa.europa.eu/publications/nis-investments-2022.

[131] RIA של 2NIS, עמ' 13-16 ; 23-33.

פרק חמישי – זיהוי וניתוח השפעות של החלופה הנבחרת

א. זיהוי השפעות (כללי)

המושפעים **הישירים** העיקריים מחלופת האסדרה המחייבת הם קבוצה של ארגונים חיוניים המשתייכים למגזרים חיוניים, כפי שיוגדרו בחקיקה (פירוט בנושא זה ראו בפרק הבא – "עיצוב החלופה הנבחרת"). אלה צפויים לשאת בעלויות הנובעות מדרישות החוק – ניהול סיכוני הסייבר ודיווח על אירועים חמורים.

אימוץ החלופה ישפיע משמעותית גם על **הרגולטורים המגזריים**: הם יקבלו לידיהם כלי אכיפה ופיקוח משמעותיים לצורך העלאת רמת ההגנה בסקטורים שהם מאסדרים, וסמכותם לאסדר את הנושא תהיה מעוגנת בחקיקה ראשית. בעיקר יושפעו מהחקיקה אותם רגולטורים שאין להם במצב הנוכחי יחידת סייבר מגזרית יעודית – שכן החוק מחייב הקמת יחידה כאמור.

לארגונים צפוי להיווצר תמריץ חיובי להקפיד על דרישות החוק כדי להימנע מעיצומים כספיים גבוהים ועניינה פלילית, שכעת **כלל** היחידות המגזריות יוכלו להפעיל.

חלוקת הסמכות והאחריות צפויה גם היא להשתנות במידה מסוימת. בין תפקידיו של המערך יכללו קידום מדיניות ואסטרטגיה לאומית; ריכוז תמונת המצב הלאומית של הגנת הסייבר; חיזוק החוסן הלאומי בהגנת סייבר וקידום התמודדות עם תקיפות סייבר; הנחייה מקצועית של היחידות המגזריות, ועוד. היחידות המגזריות יהיו אמונות על שיפור רמת הגנת הסייבר המגזרית בהתאם למדיניות ואסטרטגיית הגנת הסייבר הלאומית; קידום אסדרה מגזרית מעבר לחובות הלאומיות; מיפוי הארגונים במגזר ואיסוף נתונים; ביצוע פיקוח ואכיפה בפועל, ועוד. היחידות יציגו למערך הסייבר את תכנית העבודה השנתית שלהן להעלאת רמת החוסן במגזר, ויגישו דו"ח תמונת מצב אחת לשנה.

נקיטת פעולות הגנה צפויה לשפר את רמת ההגנה של הארגונים שבתחולת החוק. מניתוח של מחקר אמפירי שנעשה בישראל[132] אודות ההשפעה של השקעה בפעולות הגנה, עולה כי חברות גדולות בעלות הכנסה גבוהה, שנשענות על מסחר אלקטרוני ושירותי ענן, יכולות **להוריד את הסיכוי למתקפת סייבר בכ-50%** - אם הן מיישמות לפחות שש פעולות אבטחה בסיסיות יחסיות כגון סיסמאות חזקות, עדכוני תוכנה ואימות רב שלבי.

מחקר נוסף, שביצעו במשותף אוניברסיטת קיימברידג' וחברת Bit Sight חשף את המשמעות הגדולה של בקרות ההגנה בתחום הסייבר על ירידת הסיכויים להיתקל בתקיפות סייבר. המחקר התבצע באמצעות סימולציה של שלושה סוגי תקיפות (כופר, תקלה בשירותי ענן, ודליפת מידע) על-פי ארבע

[132] על בסיס מחקר של פרופ' ניל גנדל ונועה ברניר מאוניברסיטת תל אביב יחד עם חוקרים מובילים מהעולם. ראו גם בדו"ח השנתי של מערך הסייבר לסיכום שנת 2023, בעמ' 32.
https://www.gov.il/BlobFolder/news/booklet_yearly_summary_2023/he/booklet_yearly_summary_2023_e.pdf.

קטגוריות של הגנת סייבר. **התוצאות הראו כי יישום של בקרת הגנת סייבר בודדת יכול לצמצם את הסתברות למתקפת סייבר ב-7% עד 35%,** תלוי בסוג הבקרה. הפעלת שילוב בקרות מארבע הקטגוריות בו-זמנית עשויה להביא לירידה משמעותית עוד יותר בהסתברות למתקפה[133].

לפי סקר שערכה חברת IBM, ההוצאה הממוצעת הנלווית למתקפת סייבר עם רמה נמוכה של מנגנוני הגנה מסתכמת ב-5.36 מיליון דולר. לעומת זאת, ארגונים עם רמת אבטחה גבוהה צפויים להוצאה ממוצעת נמוכה יותר משמעותית, של 3.78 מיליון דולר. רמות האבטחה מורכבות בהתאם למתודולוגיית הסקר מ-27 מנגנוני הגנה כגון הכשרת עובדים, קיומה של תוכנית תגובה, היעזרות בצוות תגובה, ביטוח סייבר, כלי הגנה, שימוש בכלי AI ועוד. מנגנונים אלו נבחנו במסגרת הסקר על מנת לגבש תמונת מצב של רמת ההגנה בארגונים וההקשר לגובה הנזק[134].

ב. ניתוח השפעות כלכליות

לחלופת האסדרה צפויות להיות עלויות, אשר ניתן לחלקן לארבע קטגוריות:

- ההוצאה של ארגון על ניהול סיכוני הסייבר כנדרש בחוק;
- הוצאות לארגון הנובעות מהיכרות עם החקיקה;
- הוצאות לארגון הנובעות מעלויות ציות ודיווח;
- עלויות **לממשלה** הנובעות מצרכי היחידות המגזריות.

[133] Daffron, J., Copic, J., La Malfa, G., Jung, J., Sridhar, K., Ilardo, M., Coburn, A., Evan, T.; Cyber Security Cost Effectiveness for Business Risk Reduction; 2022; Cambridge Risk Framework series; Centre for Risk Studies; University of Cambridge. Pp. 5.

[134] Cost of a Data Breach Report 2023. Pp.29. ניתן להוריד את הדו"ח המלא בקישור: https://www.ibm.com/reports/data-breach.

הוצאות לארגון על ניהול סיכוני הסייבר

כימות ההוצאות הצפויות על ניהול סיכוני הסייבר מביאה בחשבון כמה הנחות והערכות:

עלות מלאה ליישום דרישות ההגנה – עלות זאת כוללת את עלות התוכנה והחומרה לארגון החיוני ואת תוספת משאבי כוח האדם לארגון (ארגוני/מיקור חוץ) על מנת לעמוד בדרישות ההגנה:

- עלויות תוכנה וחומרה - הערכת עלויות אלה התבססה על עבודה כלכלית שבוצעה על ידי CIS[135], אשר בחנה את העלות של יישום בקרות הגנת סייבר לפי גודל הארגון. יודגש כי ארגון חיוני יכול לממש הגנה ראויה במגוון דרכים, מה שיוצר שונות גדולה למדי בהערכת העלויות. לאור העובדה כי הדרישות בחוק אינן בהלימה מלאה לדרישות של CIS, אמדנו את תוספת העלות ב-30% ביחס לעלות שנקבעה על ידי CIS, זאת בהתבסס על ניתוח הבקרות השונות בעזרת מומחים מהתחום.
- עלויות כוח אדם – אנו מניחים כי דרישות רמת ההגנה הראויה שבחוק יחייבו משאבי כוח אדם לצורך יישומן בארגון. לצורך הכימות הכלכלי הערכנו כי חברה בינונית תידרש ל-3 עובדים וחברה גדולה תידרש ל-5 עובדים אשר יעסקו בהגנה בסייבר, כשמשאבי כוח האדם יכולים להיות עובדים אורגניים בחברה או במיקור חוץ. הערכות אלו בוססו באמצעות מומחים בתחום, והשוואה לעבודות כלכליות דומות שבוצעו בנושא. בהתאם לסקרי שכר, הערכנו כי עלות המעסיק הממוצעת לעובד היא כ- 35,000 ₪ לעובד.

רמת ההגנה הנוכחית הארגון – ארגונים שונים מקיימים במצב הנוכחי רמות שונות של בקרות הגנה בסייבר, ולכן העלות הנוספת שתושת עליהם מכוח החוק אינה אחידה. כך, ארגון שרמת ההגנה שלו גבוהה יידרש להקצאת משאבים נמוכה (אם בכלל), וארגון שרמת ההגנה שלו נמוכה יידרש ליותר משאבים על מנת לשפר את רמת ההגנה:

- רמה גבוהה (1) – הארגון מקיים רוב מכריע של דרישות ההגנה בסייבר בהתאם לחוק; ארגונים כאלה ידרשו להגדיל הוצאותיהם ב 0%-10% מסך העלות המלאה ליישום דרישות ההגנה.
- רמה בינונית (2) - הארגון מקיים מדיניות הגנה בסייבר אך נדרש להשלים בה מספר דרישות על מנת לעמוד בדרישות הגנת הסייבר ראויה בהתאם לחוק. ארגונים כאלה ידרשו להגדיל את הוצאותיהם ב- 20%-30% מסך העלות המלאה ליישום דרישות ההגנה.
- רמה נמוכה (3) – ארגון שידרש להשלים מספר משמעותי של דרישות על מנת לעמוד בהגנה סייבר ראויה בהתאם לחוק. ארגונים כאמור, יידרשו להגדיל את הוצאותיהם ב-50%-60% מסך העלות המלאה ליישום דרישות ההגנה כדי לעמוד בדרישות החוק.

גודל הארגון - לאור הקשר בין גודל הארגון לעלות יישום דרישות ההגנה בסייבר, בצענו הבחנה בין ארגונים בינוניים (עד 100 עובדים) לארגונים גדולים (מעל 100 עובדים). ההגדרה הינה בהלימה להגדרות הסוכנות לעסקים קטנים ובינוניים במשרד הכלכלה ככל שהדבר נוגע למספר העובדים.

[135] The Cost Of Cyber Defense- CIS Controls Implementation Group 1, CIS, 8/23

בהתאם להנחות העבודה שהוצגו לעיל, התקבלה מטריצת עלות שנתית המפרטת את העלות של עמידה בדרישות ההגנה לפי גודל הארגון ורמת ההגנה הנוכחית שלו. נזכיר: מדובר בעלות תוספתית למצב הקיים, ולא בכלל העלויות המקושרות להגנת סייבר, שננקטות ללא קשר למצב החדש המוצע בחלופת האסדרה:

רמת הגנה	חברה בינונית	חברה גדולה
עלות מלאה	1.4 מלש״ח	3.1 מלש״ח
1 – גבוהה	0-0.1 מלש״ח	0-0.3 מלש״ח
2 - בינונית	0.3-0.4 מלש״ח	0.6-0.9 מלש״ח
3 - נמוכה	0.7-0.8 מלש״ח	1.5-1.9 מלש״ח

במטרה להתמודד עם המורכבות בחישוב עלויות הגנת הסייבר, ועל מנת לספק רמת סמך נוספת לאומדן שבצענו, ערכנו השוואה של הממצאים שקיבלנו אל מול הממצאים שהוצגו במסגרת ה-RIA לחוק הגנת הסייבר הבריטי [136],[137]. מהניתוח עלה כי בבריטניה התוספת לחברה בינונית תהיה שוות ערך ל-0.4 מלש״ח, ולחברה גדולה – 0.7 מלש״ח[138]. סכומים אלו נמוכים מהתוצאות שהתקבלו מהערכת העלויות שביצענו. ממצא זה מחזק את הסברה כי האומדן שבצענו אינו מהווה הערכת חסר לעלויות הגנת הסייבר לארגונים השוני (בהתאם, יתכן כי מדובר בהערכת-יתר).

כימות העלות המצרפית להוצאות הגנה בסייבר לארגונים החיוניים יתאפשר באמצעות מכפלת כמות הארגונים בעלות פר ארגון (בהתאם למיקומו במטריצה שלעיל). עם השלמת מיפוי הארגונים החיוניים, גודלם ורמת ההגנה בהם, יהיה ניתן לבצע הערכה זו.

[136] Impact Assessment - The Network and Information Systems Regulation 2018, April 2018 - Department for Digital, Culture, Media and Sport, UK.

[137] Post Implementation Review of the Network and Information Systems Regulations 2018, May 2020- Department for Digital, Culture, Media and Sport, UK

[138] יודגש כי החישוב לוקח בחשבון את רמת ההגנה בבריטניה ולכן מהווה מדד ייחוס בלבד לנושא.

עלויות היכרות (חד פעמיות) עם החוק

הארגונים החיוניים יידרשו ללמוד את משמעויות החוק והדרישות הרגולטוריות הנובעות ממנו. תהליך זה כרוך בהעסקת מומחים משפטיים ובייעוץ מקצועי לגבי אופן יישום החוק. לצורך הערכת העלות של מרכיבים אלה השתמשנו בהנחות שנלקחו במסגרת ה-RIA הבריטית[139] , ונתונים נוספים שהתפרסמו בבריטניה לאחר יישום החקיקה[140]. לפי הנחות אלה היכרות ראשונית עם החוק תצריך:

- 12 שעות יועץ משפטי בארגון – הבנת החקיקה והדרישות מהארגון.
- 6 שעות מנהלי אבטחת מידע בארגון – הבנת החקיקה והדרישות מהארגון.
- לצורך החישוב נלקח בחשבון שכר שעתי של עו"ד בארגון - 350 ₪ לשעה [141], ושכר של מנהל אבטחת מידע בארגון – 415 ₪ לשעה [142].

	כמות שעות	עלות לשעה (₪)	סה"כ (₪)
יועץ משפטי	12	350	4,200
מנהל טכנולוגיות מידע	6	415	2,490
סה"כ עלות לארגון חיוני			6,690

בהתאם לכך, עלות ההיכרות עם החקיקה מסתכמת לכ- 7 אש"ח לארגון בממוצע (עלות חד פעמית)

עלויות ציות ודיווח

ארגונים חיוניים שהחול יחול עליהם צפויים לקבל מעת לעת הנחיות לביצוע מהרגולטור המגזרי שלהם, ובמקרי קיצון גם ממערך הסייבר הלאומי. בנוסף, הם נדרשים לדווח על תקיפות סייבר חמורות, כפי הגדרתן בחוק.

הערכת העלות בהקשר זה מבוססת גם היא על ההנחות שעמדו בבסיס ה-RIA הבריטית, שתוקפה מחדש לאחר יישום החקיקה בבריטניה. עלויות אלו כוללות עלויות של ייעוץ משפטי ועיסוק של מנהלי אבטחת הסייבר בארגון.

[139] - Impact Assessment - The Network and Information Systems Regulation 2018, April 2018 - Department for Digital, Culture, Media and Sport, UK.

[140] Post Implementation Review of the Network and Information Systems Regulations 2018, May 2020- Department for Digital, Culture, Media and Sport, UK

[141] בהתאם לשכר ממוצע של כ-45,000 אש"ח (ממוצע הטווח של שכר עו"ד בכיר בחברה לפי דוח השכר הגדול CODEX – 2023), 180 שעות בחודש ועלויות מעביד של 35% נוספים.

[142] בהתאם לשכר ממוצע של 55,000 ₪ (שכר של CISO מנוסה/בכיר- סקרי שכר), 180 שעות בחודש ועלויות מעביד של 35% נוספים.

	עלויות ציות- כמות שעות	עלויות דיווח על מקרים – כמות שעות	עלות לשעה (₪)	סה״כ (₪)
יועץ משפטי	10	2	350	4,200
מנהל טכנולוגיות מידע	14	2	415	6,640
סה״כ עלות שנתית לארגון חיוני				**10,840**

בהתאם להערכה המפורטת לעיל, עלויות ציות ודיווח (במידה ויהיו אירועים) מוערכת בכ- 11 אש״ח בממוצע בשנה לארגון חיוני.

<u>עלויות לממשלה</u>

עד כה הוצגו עלויות של חלופת האסדרה שיושתו על הארגונים החיוניים, אך חלופת האסדרה כוללת גם עלויות **לממשלה**. אלה נובעות בעקרן מהקצאת כוח אדם ותקציבים, שידרשו הן לחיזוק היחידות המגזריות הקיימות, והן להקמתן של יחידות חדשות היכן שהן לא קיימות.

כזכור, ליחידה המגזרית כמה תפקידים: עליהן להנחות באופן שוטף את הארגונים החיוניים שבמגזר אותו הם מאסדרים, לקבל דיווחים ולסייע להם במידת הצורך בתפעול של אירועי סייבר, וכן לבצע פעולות אכיפה, פיקוח ובקרה בהתאם לחוק.

לצורך הערכת העלות הנדרשת, גובשה מתודולוגיה לחלוקת היחידות המגזריות לגדלים – גדולה מאוד, גדולה, בינונית וקטנה – וזאת על סמך כמות הארגונים החיוניים בכל מגזר, מורכבותם, ומערכות ייחודיות המשתייכות למגזר, ככל שיש כאלה.

בהתאם למוצע בהצעת החוק, אנו מניחים כי לכל יחידה מגזרית יהיה לכל הפחות ראש יחידה + צוות הנחיה, בקרה ופיקוח. היחידות רשאיות (אך אינן חייבות) להקים SOC מגזרי. ככל שיוקם ויאויש SOC כזה, הוא יחייב כוח אדם נוסף.

יצוין כי ראש היחידה המגזרית ומנהל SOC, ככל שיהיה כזה, צפויים להיות עובדי מדינה. ניתן להניח ששאר בעלי התפקידים, ובכלל זה צוות ההנחיה, הבקרה והפיקוח, יהיו עובדים במיקור חוץ.

לפי הניתוח שביצע אגף הגנה סקטוריאלית במערך הסייבר, מפתחות כוח האדם הנדרשים ליחידה מגזרית הנם כדלקמן:

	כמות היחידות	ראש יחידה	צוות הנחיה, בקרה ופיקוח
יחידה גדולה מאוד	**1**	**1**	**13**
יחידה גדולה	**6**	**1**	**7**
יחידה בינונית	**1**	**1**	**5**
יחידה קטנה	**3**	**1**	**2**

נתוני האיוש **הנוכחיים** במשרדי הממשלה, שמהם תיגזר התוספת הנדרשת (בהתאם למפתחות שלעיל), אינם מפורסמים כאן מטעמי בטחון מידע. השלמת כוח האדם ליחידה המגזרית עשויה להתבצע באמצעות מיצוי משאבי כוח האדם הקיימים במשרדים או ממקורות אחרים. חשוב להדגיש כי קיים שוני בין היחידות: בעוד שיחידות מגזריות מסוימות נמצאות באיוש גבוה ועשויות לא להידרש לתוספת כלל, אחרות נדרשות להקמה מחדש.

<u>תועלות בחלופת האסדרה</u>

כפי שהצגנו בפרק ב', הנזק הכולל מתקיפות סייבר מוערך ב-12 מיליארד ₪ מדי שנה בהתאם להערכה שבוצעה על ידי מערך הסייבר הלאומי[143]. בהינתן פעולה מתקנת בדמות החקיקה המוצעת, ובהסתמך על המידע שהוצג לעיל, אנו מעריכים כי פעולות ההגנה שינקטו מכוח החוק יביאו לחיסכון משמעותי בעלויות אלה. הערכה זו מביאה בחשבון כי שוק הסייבר הוא שוק עם תלות הדדית וקישוריות גבוהה, כך שהעלאת רמות החוסן בקרב חלק מהארגונים עשויה להקרין גם על ארגונים שאינם בתחולת החוק.

חשוב לציין כי לצד התחשיב הכלכלי שפורט בפרק זה, יש לחלופת האסדרה תועלות רבות נוספות שקשה לכמתן: שמירה על חיי אדם, ביטחון אישי, הגנה על הרציפות התפקודית במשק (חסכון באבדן שעות עבודה, למשל) וכן שמירה על הפרטיות ועל אמון הציבור. כפי שצוין מוקדם יותר בדו"ח זה, ניתן להעריך כי אסדרת סייבר מתקדמת ומאוזנת תתרום לשיפור האטרקטיביות הכלכלית של ישראל למשקיעי זרים, בעיקר כשאסדרה דומה כבר נהוגה במדינות מערביות בעלות שווקים מפותחים.

[143] מערך הסייבר הלאומי, הערכת העלות הכלכלית של תקיפות סייבר, הערכת הנזק הכלכלי של תקיפות סייבר בישראל (Gov.il).

פרק שישי – עיצוב החלופה הנבחרת

א. מודל האסדרה – ריכוזי מול מבוזר

החלופה הנבחרת היא אסדרה חוקית מחייבת. כפי שראינו בפרק השלישי, זוהי חלופה שאומצה בכל אחת ממדינות ההשוואה (וגם במדינות מערביות רבות אחרות), אם כי בכל מדינה היא לבשה צורה מעט שונה. בריטניה, למשל, אימצה מודל מבוזר מובהק, שבו לרגולטורים המגזריים יש עצמאות מקסימלית ביישום החקיקה הלאומית; בגרמניה, לחילופין, ה-BSI הוא גוף מרכזי חזק שמרבית הסמכויות בחוק (ובכלל זה סמכויות פיקוח ואכיפה) מצויות בידיו. שאלת המודל – ריכוזי, מבוזר, או אחר – מתעוררת כמובן גם בישראל.

שתי החלופות המבניות (הריכוזית והמבוזרת) מציעות תוכן מהותי זהה – דהיינו, הטלת חובת דיווח וחובת ניהול סיכוני סייבר על ארגונים חיוניים. לדידנו, ההכרעה ביניהן צריכה להיעשות, בין היתר, על בסיס שיקולים של איזון בין צרכים מגזריים ואינטרסים לאומיים, ישימות ומהירות הישום, חלוקה בהירה של סמכויות ואחריות, ניצול מקסימלי של נקודות החוזק של כל שחקן, והסתייעות במודלים בינ״ל דומים, ככל שהדבר אפשרי. על סמך אלה, אנו ממליצים על מודל אסדרה מבוזר – לצד הגדרה ברורה יותר של סמכויות ותפקידי מערך הסייבר כגורם הלאומי המתכלל את ניהול הגנת הסייבר במדינת ישראל.

המודל האסדרתי הקיים בישראל, המבוסס על החלטות הממשלה 2443 ו-2444, הוא במהותו מודל מבוזר מאוד. מצד אחד – הוא מאפשר לרגולטורים המגזריים עצמאות רבה בקידום הגנת הסייבר בענפיהם; מצד שני – כפי שראינו - התשומות, המשאבים, היכולות והכלים שכל רגולטור משקיע בתחום שונים מאוד, ולצד גורמים נוספים הם מביאים לפערים ניכרים במצב ההגנה במגזרים שונים במשק. למערך הסייבר יש, להלכה, תפקיד של ״מנחה מקצועי,״ של המגזרים, אך חלוקת התפקידים והסמכויות בינו לבין המאסדרים המשרדיים לוקה לעתים בעמימות מסוימת.

מן הפערים הקיימים במודל האסדרה הנוכחי צומחות, להלכה, שתי אפשרויות: מעבר למודל ריכוזי מובהק, שבו כלל הסמכויות נתונות בידי מערך הסייבר; או ביצוע תיקונים נדרשים במודל המבוזר כך שיתנו מענה לפערים הקיימים. בבחירה שבין שתי חלופות אלה, אנו סבורים כי יש יתרון מובהק לאפשרות השנייה:

- ראשית, מעבר למודל ריכוזי דורש שינוי מבני וארגוני מקיף ואיטי (בכוח אדם, משאבים וסמכויות), העלול לקחת זמן רב, ובעיקר - לפגוע ברגולטורים שכבר הקימו יחידות מגזריות מתפקדות ומבוססות היטב.
- שנית, לרגולטורים המגזריים יש יתרון בולט בהיכרות אינטימית של ענפי המשק שהם מאסדרים. שימור סמכויות הניהול השוטף בידיהם, כמו גם הפיקוח והאכיפה, מאפשר להתאים את דרישות ניהול הסיכון לאופי הייחודי של כל מגזר.

- על מנת לנצל את היתרון היחסי בכלל הסקטורים באופן דומה, יש להעצים ולחזק את היחידות המגזריות הזקוקות לכך – ולא לעבור למודל אסדרתי ריכוזי שונה לחלוטין. לשם כך יוצר את החובה להקמת יחידה מגזרית בכל המגזרים החיוניים, ויוצר "השוואת תנאים" בין היחידות השונות במה שנוגע לתפקידים, סמכויות וכלי פיקוח ואכיפה.
- לצד העצמאות של היחידות המגזריות במודל המבוזר המוצע, נדרש גורם מדינתי מוביל שיש לו הכלים והסמכויות לראות תמונה לאומית כוללת, ולהכווין את המשק בהתאם. לשם כך מפורטים בהצעת החוק התפקידים והסמכויות הן של היחידות המגזרית – והן של מערך הסייבר.

ב. עיקרי האסדרה המוצעת

נעמוד כעת בקצרה על משמעויות החלופה הנבחרת (אסדרה לאומית מחייבת במודל מבוזר) מבחינה מעשית. פרק הסקירה הבינ"ל כלל התייחסות מפורטת לשני האדנים המרכזיים של החלופה – חובת דיווח וחובת ניהול הסיכון – ולכן בפרק זה נציג את הנושאים בתמצות יחסי.

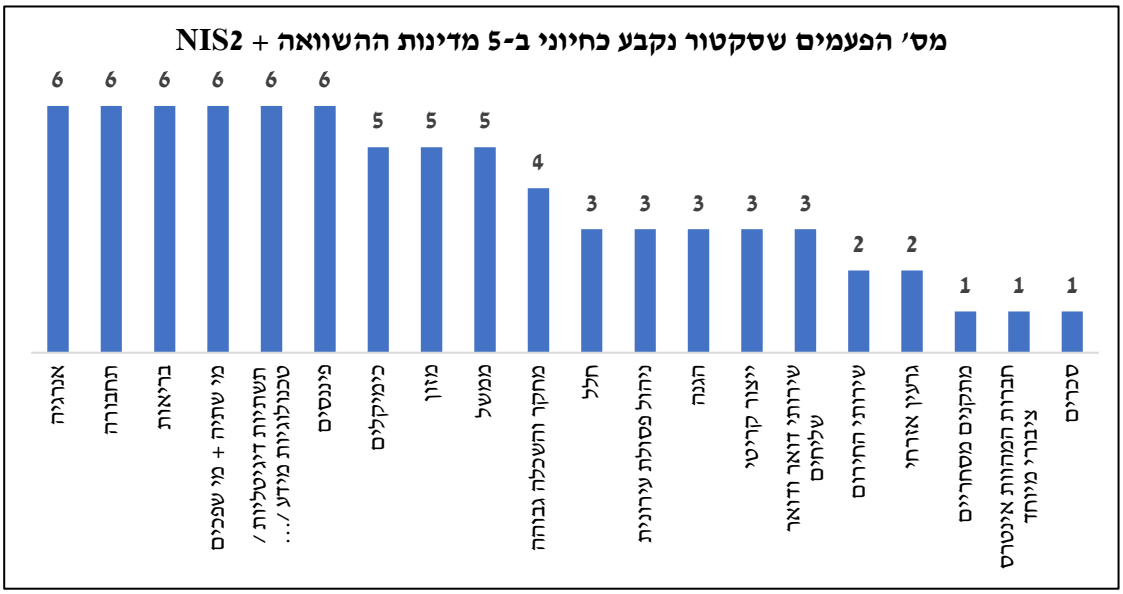
<u>על מי ועל מה הרגולציה חלה?</u>

הרגולציה צפויה לחול על אותם ארגונים שיפלו בגדר ההגדרה "ארגונים חיוניים" במגזרים הכלולים בחוק. המגזרים נקבעו בהתאם לבנצ'מארק הבינ"ל, עם התאמות מינימליות לשוק הישראלי: משרדי הממשלה; תקשורת; אנרגיה; בריאות; כימיקלים, רעלים וחומרים מסוכנים; מים וביוב; תחבורה; רשויות מקומיות; משק כללי (מזון); שירותים דיגיטליים ושירותי אחסון; חקלאות.

כל המגזרים החיוניים שיכללו באסדרה המוצעת נחשבים למגזרים חיוניים בלפחות 4 מ-5 מדינות ההשוואה+NIS2 [144]. ככלל, מספר המגזרים החיוניים באסדרה המוצעת נמוך ממספר המגזרים החיוניים במדינות ההשוואה (למעט אוסטרליה), וביחוד בהשוואה ל-NIS2, שם המספר עומד על 18[145].

[144] מהסקירה הבינ"ל עלה כי מגזר החקלאות כלול על פי רוב בתוך מגזר המזון; רשויות מקומיות – בתוך ממשל [NIS2 מתירה לכל מדינה להחליט על אילו רמות של הממשל המרכזי/מקומי היא מחילה את האסדרה]. תקשורת – לעתים בנפרד ולעתים כחלק מתשתיות דיגיטליות.

[145] בפועל הפער גדול עוד יותר, בשל הבדלים מסוימים במיון המגזרים בין ישראל לאיחוד האירופאי. למשל, באירופה "ממשל" הוא מגזר אחד, ובאסדרה המוצעת אנו מתייחסים אליו, כאמור, כשני מגזרים שונים – "ממשל" ו"רשויות מקומיות."



התבחינים לקביעת ארגון חיוני בכל מגזר מפורטים בתוספת לחוק. אנו סבורים כי בשלב זה יש עדיפות למודל של תבחינים מגזריים ממוקדים, על פני תבחין אוניברסלי גורף חוצה-מגזרים ("כל ארגון בינוני ומעלה"), כפי שקובעת דירקטיבת NIS2. לעת הזו נראה כי השיטה האירופאית רחבה מדי, תכלול כמות גדולה מאוד של עסקים בישראל – מה גם שבאירופה מדובר בגל **השני** של חקיקת סייבר לאומית, בעוד בישראל מדובר בפעם **הראשונה** שהתחום מוסדר ברמה הלאומית.

בנוסף, מוצע לאפשר מנגנון החרגה (opt-in או opt-out) של ארגון לתוך רשימת הארגונים החיוניים או מחוצה לה, וזאת באמצעות ועדה מייעצת בראשות נציג הרגולטור המגזרי, בהשתתפות נציג מס"ל, משרד האוצר, משרד הביטחון והיעוץ המשפטי לממשלה.

<u>חובת דיווח</u>

בדומה לבנצ'מארק הבינ"ל, ארגון חיוני נדרש לדווח על תקיפת סייבר משמעותית כפי הגדרתה בחוק (ראו להלן). הדיווח יעשה פעם אחת כך שיגיע הן לידיעת הרגולטור המגזרי (לצרכי ידיעה, טיפול וסיוע ככל הנדרש), והן למערך הסייבר (בעיקר לצורך החזקת התמונה הלאומית הרב-מגזרית). גורם מסמיך לפי החוק רשאי לקבוע כי הדיווח יוגש לרגולטור המגזרי, ויועבר על ידו למערך הסייבר הלאומי עם קבלתו.

תקיפת הסייבר צריכה להיות מדווחת אם יש חשש ממשי שהיא אינה מוגבלת לארגון הנתקף, עלולה להביא לפגיעה או גישה בלתי מורשית לנכס מידע משמעותי, או אם היא עלולה לפגוע באופן משמעותי בזמינות, ברציפות או במהימנות השירות של הארגון. כדי להעריך זאת רשאי הארגון להביא בחשבון בין השאר שיקולים כמו מספר המשתמשים המושפעים מן התקיפה, סוג הפגיעה והיקפה, ומשך הזמן שהיא נמשכת.

הדרישה לדיווח מיידי הכרחית לאור אופי האיום. נוכח הסיכונים בישראל, ומאחר והחוק הישראלי עוסק בתקיפות (זדון) ולא בתקלות סתם, חלון הזמן לתגובה אפקטיבית, סגירת מעגל ומניעת התפשטות הוא קצר ביותר. דיווח שאינו נעשה בסמוך לגילוי שומט את הקרקע תחת היכולת המבצעית לסייע לארגון ולהזהיר את המשק.

נזכיר: בבריטניה היה נהוג לבצע את הדיווח תוך 72 שעות – אך התיקון לחוק הגנת הסייבר שם צפוי להוריד את פרק הזמן ל-24 שעות[146]; בארה"ב – תוך 72 שעות, ועבור מתקפות כופרה תוך 24 שעות; באוסטרליה – 12 שעות לתקיפת סייבר חמורה (ברת דיווח) ו-72 שעות לתקיפות אחרות (לא רלוונטי); בגרמניה – באופן מיידי; בהולנד – באופן מיידי. אחרי ש-NIS2 יכנס לתוקפו אירופה, שתי המדינות הללו ידרשו דיווח "באופן מיידי ובכל מקרה תוך 24 שעות"; דיווח משלים באופן מיידי ועד 72 שעות; ועוד דיווח אוחר מסכם לאחר כחודש. מכל מקום, העמדה המקצועית של מערך הסייבר היא שאין הרבה טעם בדיווח על תקיפת סייבר חמורה 72 שעות לאחר התרחשותה.

<u>רמת הגנת סייבר</u>

הדרישה העיקרית מארגונים חיוניים בחוק, גם היא בדומה לבנצ'מארק הבינ"ל, היא לקיים רמת הגנה ולנהל את סיכוני הסייבר שלו. ככלל, כדי לעמוד בדרישה לקיום רמת הגנה נדרשת כאמור, על הארגון החיוני לעמוד **בדרישות** המפורטות בתוספת, המחולקות ל-9 "משפחות" של בקרות – בדומה לנקוב בדירקטיבת NIS2[147]. כפי שיפורט בהמשך, כלל הדרישות מקובלות בתקינה הבינ"ל הרווחת בתחום. עוד יודגש כי ככל שמאסדר מגזרי ידרוש זאת, הארגונים ידרשו לעמוד באסדרה המגזרית שיקבע אותו מאסדר.

מערך הסייבר התלבט ארוכות באשר לאופן שבו תיושם החובה לרמת הגנה ראויה. הלמידה מן העולם לא הצביעה על חלופה מובהקת בהקשר זה. כך, בבריטניה, גרמניה והולנד החקיקה קבעה (טרם כניסת NIS2 לתוקף) חובה כללית על ארגון חיוני "לנקוט בצעדים טכניים וארגוניים הולמים ומידתיים כדי לנהל את הסיכונים הנשקפים לבטיחות מערכות הרשת והמידע שלו" – אך כל אחת מהן פרטה את העיקרון באופן שונה לכדי יישום.

- בבריטניה למשל נקבע כי הרגולטורים המגזריים ינחו את הארגונים החיוניים כיצד ליישם את העיקרון, ויבחנו אותם בהתאם למסגרת הלאומית CAF שהגה ה-NCSC.
- בגרמניה נקבע כי איגודים מקצועיים בכל סקטור רשאים להציע ל-BSI תקנים מגזריים לניהול הסיכון, ועליו לאשרם. בגרסה החדשה של החוק הגרמני, החל מ-2025, תיכלל רשימת חובות ברמת הכותרת בהתאם ל-NIS2, ללא הפניה לתקנות, אך עם הפניה בדברי ההסבר לתקנים בינ"ל.

[146] https://publications.parliament.uk/pa/bills/cbill/59-01/0329/240329.pdf; ראו בסעיף 15 להצעת החוק: "Reporting of Incidents by Regulated Persons".
[147] בדירקטיבה ישנן 10 משפחות; אנו מציעים לאחד 2 משפחות כך שבהצעה הישראלית ישנן 9.

- בהולנד לעומת זאת נכתבו תקנות ייעודיות[148] הכוללות פירוט של הדרישות לניהול הסיכון.
- גם באוסטרליה נקבעו תקנות לצורך פירוט הדרישות לניהול הסיכון, ולצורך יישומן על הארגון החיוני לעמוד באחד מבין חמישה תקנים וסכמות בינ״ל שצוינו בתקנות[149].

כאמור, עם כניסת דירקטיבת NIS2 לתוקף, חלה חובה חוקית שאמצעי ההגנה יכללו לכל הפחות את 10 הנושאים שקבעה הדירקטיבה (ראו פירוט להלן).

העקרונות שהנחו את מרכז מתודולוגיה במערך הסייבר בקביעת מנגנון היישום לרמת הגנת סייבר היו כדלקמן:

- ✓ הצורך בהוראות מקיפות (הנוגעות הן להגברת החוסן – Resiliency - של הארגון מבעוד מועד; יכולותיו להתמודד עם אירועי סייבר; ושמירה על רציפות תפקודית);
- ✓ התאמה ל-NIS2 ולתקינה בינ״ל;
- ✓ דרישות המהוות את ה׳מינימום האולימפי׳;
- ✓ דרישות שקופות וקלות להתמצאות ולהבנה;
- ✓ דרישות שהן ברות השגה;

בשלב הראשון הוחלט, בדומה למודלים בינלאומיים (כגון בריטניה וגרמניה), שלא לחייב אימוץ תקינה קשיחה **במלואה**, אלא להתבסס על רשימת דרישות המהווה רמת ההגנה הנדרשת. גישה זו נבחרה לאור הקשיים השונים הכרוכים באימוץ והטמעה **מלאים** של תקנים בינ״ל. אלה כוללים, בין היתר, את הצורך להתאים את התקן לסוג וגודל הארגון, תרגום התקן המלא לעברית, מעקב אחר עדכונים ושינויים של גוף התקינה, התאמת התקן לדרישות רגולציה מקומית, רתימת הארגון לאימוץ אפקטיבי של התקן, ועוד. לכן מדינות רבות בחרו ליצור סכימות לאומיות ומתומצתות המבהירות לארגון מה מצופה ממנו, לכל הפחות, כדי לשמור על רמת הגנת סייבר נאותה (ראו דוגמאות בקובץ הצמוד לדו״ח זה המציג את ההשוואה הבינ״ל המלאה).

בשלב השני נקבע כי הרשימה תכלול דרישות ביצוע (Requirements) ולא עקרונות כלליים (Principles) או בקרות (Controls). ההחלטה התקבלה כדי למנוע עמימות, להקל על הממונה בארגון לדרוש משאבים, ולמנוע מצב של תת-הגנה (ובמקרים נדירים גם כפילויות) הנובע מחוסר בהירות. דרישות אלו מפורטות אך אינן מכתיבות את ה״איך״ הטכני המדויק. למשל:

[148] https://wetten.overheid.nl/BWBR0041520/2021-05-01 - נוסח משולב של התקנות הכולל את התיקון האחרון משנת 2021.

[149] https://www.legislation.gov.au/F2023L00112/latest/text, ראו בס׳ 8.

עקרונות	דרישות
הגנת סייבר ברשת האספקה	• מיפוי של התהליכים, מערכות ונכסי המידע אשר משפיעים באופן ישיר על תפקודו של הארגון החיוני ; • הפעלת מערך טכנולוגי של גיבויים אשר ישמש כתשתית להמשכיות עסקית והתאוששות מאסון ; • קיום תוכנית ארגונית סדורה ומאושרת להמשכיות עסקית והתאוששות מאסון בהיבטי הגנת מידע וסייבר.
ניתוח סיכונים ואבטחת מערכות מידע	• מינוי צוות יישום אבטחת מידע והגנת סייבר ; • זיהוי מושאי אבטחת המידע והגנת הסייבר ; • הערכת הסיכון וחישוב רמת הסיכון במושאי ההגנה.

הדרישות עצמן מחולקות כאמור ל-9 נושאים, בהלימה לנושאים a-j שבדירקטיבת NIS2 (כאמור, 2 קטגוריות אוחדו לאחת). כמו כן, לטובת גמישות ותאימות מיטבית למגזרים ספציפיים, נקבע כי הרגולטור המגזרי רשאי לקבוע הוראות **נוספות** לעניין רמת הגנת הסייבר לארגונים החיוניים במגזר אותו הוא מאסדר, בהתייעצות עם מערך הסייבר. הוראות אלה יכולות להוסיף על רמת ההגנה הנדרשת בחוק הסייבר הלאומי, אך לא לגרוע מהן.



עקרונות הליבה להגנה בחוק הסייבר הישראלי (קטגוריות ליבה)

דרישות ההגנה בחוק הסייבר מאורגנות סביב תשעה עקרונות ליבה פונקציונליים, המשקפים את מחזור החיים של תכנית הגנת סייבר ארגונית מודרנית. הם נועדו לספק לגופים החיוניים מפת דרכים ברורה ופרקטית ליישום ההגנה הנדרשת.

להלן תשעת העקרונות המרכזיים והדרישות העיקריות בכל אחת מהם:

1. **ניתוח סיכונים והגנה על נכסי סייבר**: קטגוריה זו מהווה את הבסיס לכל תכנית ההגנה. היא דורשת זיהוי ומיפוי מתמשך של נכסי סייבר, נתונים ותהליכים חיוניים; ביצוע סקרים ובדיקות אבטחה יזומות לזיהוי סיכונים; ניהול והערכת סיכוני סייבר מתמשכת; קיום תכנית עבודה מאושרת לטיפול בסיכונים; ואיוש צוות ייעודי ליישום התכנית. כמו כן, היא כוללת דרישות טכניות מפורטות להגנת הרשת, פילוחה, ניהול תצורה מאובטח, הגנה מפני תוכנות זדוניות וניהול אמצעים ניידים ומדיה נשלפת.

2. **היערכות והתמודדות עם אירועי סייבר**: קטגוריה זו מתמקדת במוכנות הארגון לתגובה יעילה בעת אירוע. היא מחייבת קיום תכנית ארגונית לטיפול באירועים, מינוי והכשרת צוותי ניהול משבר ותגובה לאירועים (IR), ביצוע תרגילים, וקיום תכנית ניטור טכנולוגי הכוללת איסוף וניתוח יומני רישום (לוגים). בנוסף, נדרש מנגנון דיווח על אירועים חשודים, קריטריונים לסיווג אירועים, ותהליכי תקשורת ותחקור לאחר אירוע.

3. **רציפות תפקודית והמשכיות השירות**: מטרת קטגוריה זו היא להבטיח את יכולת הארגון להמשיך ולספק שירותים חיוניים גם במהלך ולאחר אירוע סייבר חמור. הדרישות כוללות ביצוע ניתוח השפעה עסקית (BIA), כמו גם קיום תכניות מאושרות להמשכיות עסקית (BCP) והתאוששות מאסון (DRP). דגש מיוחד מושם על תכניות גיבוי מקיפות, הבטחת זמינות משאבים באמצעות יתירות, וביצוע תרגולים סדירים.

4. **הגנת סייבר בשרשרת האספקה**: קטגוריה זו מכירה בכך ששרשרת האספקה היא אחד מוקדי הסיכון המרכזיים. היא דורשת קיום מדיניות ארגונית לניהול סיכוני סייבר בשרשרת האספקה, מיפוי מתמשך של ספקים, ביצוע הערכות סיכונים לספקים (לרבות באמצעות שאלונים וסקרי חוסן), וקיום תכנית להפחתת סיכונים אלו. **דרישה קריטית נוספת היא הכללת סעיפי הגנת סייבר מחייבים בחוזים עם ספקים.**

5. **פיתוח ותחזוקת מערכות, טיפול בפגיעויות וחשיפתן, ותהליכי רכש**: קטגוריה זו עוסקת באבטחה לאורך כל מחזור חיי המערכת. היא מחייבת קיום נוהל פיתוח מאובטח (בין אם פנימי או במיקור חוץ), נהלים לניהול שינויים, ניהול תיקוני אבטחה (טלאים), וניהול פגיעויות טכניות, לרבות חשיפה מתואמת.

6. **מדיניות ונהלים להערכת אפקטיביות מאמץ ההגנה**: קטגוריה זו מתמקדת בממשל ובפיקוח. היא דורשת מהארגון לאמץ מסגרת ניהול סיכונים מוכרת (כגון NIST 53-800 או ISO 27001), לקיים מדיניות הגנת סייבר ארגונית מקיפה, למנות ממונה הגנת סייבר (CISO) הכפוף ישירות למנכ"ל, ולהפעיל ועדת היגוי עליונה. כמו כן, נדרש מעקב עיתי אחר התקדמות תכנית העבודה והכנת דוחות תקופתיים להנהלה.

7. **היגיינת סייבר בסיסית והדרכות**: קטגוריה זו שמה דגש על הגורם האנושי. היא מחייבת פיתוח ומימוש תכנית מודעות והדרכות לכלל העובדים, ההנהלה והספקים, וכן תכנית הכשרות ואימונים ייעודית לעובדים בעלי תפקידים טכניים בתחום הסייבר.

8. **הצפנה והסתרת נכסי סייבר**: קטגוריה זו עוסקת בהגנה על המידע עצמו. היא דורשת תהליך מתמשך לסיווג נכסי הסייבר והנתונים, וקביעה ויישום של מדיניות ונהלים לשימוש באמצעים קריפטוגרפים להצפנת נתונים, הן במנוחה והן בתנועה, בהתאם לרמת הסיווג והסיכון.

9. **בקרת גישה, ניהול נכסים וטיפול בגורם האנושי**: קטגוריה זו מאגדת באופן ייחודי מספר תחומים קריטיים. היא דורשת מדיניות לניהול משתמשים והרשאות גישה על בסיס עקרונות "הצורך לדעת" ו"הרשאה מינימלית", נהלים מחמירים לניהול גישה פריווילגית, הגנה על מערכות ניהול, ותהליך ניהול זהויות ואימות (IAM). דרישה מרכזית היא יישום מלא של אימות רב-גורמי (MFA). בנוסף, הקטגוריה כוללת דרישות לבדיקות רקע ואמינות לעובדים ונהלי קליטה, עזיבה ושינוי תפקיד.

חשוב להדגיש כי מבנה הדרישות בחוק הסייבר הישראלי תוכנן במיוחד כדי להשיג מטרות מעשיות החורגות מעצם הציות הרגולטורי. הקטגוריות והדרישות הספציפיות שבהן נועדו לבנות חוסן ארגוני אמיתי. הן מספקות לארגונים חיוניים כלים ומסגרות עבודה המאפשרות התמודדות טובה ויעילה גם עם אירועי סייבר חמורים, ובסופו של דבר, דואגות לכך שרציפות השירות החיוני לציבור תישמר גם תחת מתקפה. גישה זו, המשלבת תאימות עם בניית יכולות, היא שמציבה את החוק ככלי אסטרטגי להגנה לאומית.

בשלב השלישי נקבע כי אופן היישום של **הדרישות** יעשה על ידי עמידה בבקרות **הרלוונטיות** המצויות ברשימת התקנים הבינ"ל הבאים: ISO2700 1/2, NIST800-53 ברמות Moderate או-High שלו; וכן ב- NIST Cybersecurity Framework גרסה 2.0. לצורך זה, יפרסם מערך הסייבר באתר האינטרנט שלו גילויי דעת, אשר יסבירו בין היתר את הרציונאל מאחורי כל דרישה, את ההקשר הרחב שלה ביחס לדרישות אחרות, והצעה של מגוון לדרכים ליישום. בנוסף, ארגון רשאי לפנות ליחידה המגזרית בה הוא מאוסדר כדי לבחון האם האמצעים בהם נקט עונים על הדרישות שבחוק. במקרה זה, היחידה מחויבת לתת לו חוות דעת מקדמית. הרגולטור המגזרי אף רשאי לפטור ארגון חיוני מדרישות רמת ההגנה, בכפוף לתנאים המנויים בחוק, אם זה הוכיח (באמצעות הערכה של צד שלישי) עמידה מלאה בתקנים ביחס לשירותי הליבה שלו.

<u>התערבות נוכח תקיפות סייבר חמורות ומתן הוראות אחרות</u>

האסדרה המוצעת מקנה את הסמכות למתן הוראות לארגון חיוני בעת תקיפת סייבר חמורה (או חשש ממשי לתקיפה) ליחידה המגזרית הרלוונטית כפי הגדרתה בחוק.

אם היחידה המגזרית קבעה שתקיפה היא תקיפה חמורה וכי נדרשת מעורבות היחידה, עובד מוסמך שלה יודיע על כך לארגון, יפרט את התשתית העובדתית לקביעה, ויעניק לארגון הזדמנות לפעול בעצמו לטיפול בתקיפה. רק במידה שהארגון החיוני לא פעל באופן הולם, רשאי העובד המוסמך המגזרי לתת לו הוראות כתובות או בעל פה, ואלה ינתנו בתיאום עם מערך הסייבר הלאומי. במתן הוראות אלו, העובד המוסמך המגזרי מחויב לשקול, בין היתר, את השפעתן על הזכות לפרטיות, פעילות הארגון ועלות היישום.

הוראות כאמור יוכלו להינתן ע"י עובד מוסמך של מערך הסייבר, אם מתקיימים תנאים המלמדים על איום בסדר גודל לאומי משמעותי, כגון כזה הכולל חשש לתקיפה שתתפשט במהירות לארגונים רבים, תתפשט ליותר ממגזר משק אחד, או תפגע בביטחון המדינה או הציבור. במקרה כזה, הסמכויות כלפי הארגון החיוני יופעלו בהוראת עובד מוסמך של המערך, וזאת לאחר יידוע הרשות המוסמכת וככל הניתן באמצעותה.

מחוץ לעולמות ההתערבות בתקיפה החמורה, מערך הסייבר רשאי לתת הוראה דחופה לארגון חיוני לנקוט אמצעים למניעת **סיכון סייבר משמעותי** העלול לאפשר תקיפה חמורה, וזאת באישור ראש הממשלה. הוראה זו מוגבלת לתקופה של עד 30 יום וניתנת להארכה פעם אחת, והיא ניתנת על אף שאין עדיין תקיפה. המדובר, למשל, בהוראה לסגירה דחופה של פגיעות חמורה, בטרם תנוצל ע"י תוקף.

מנגנוני פיקוח, אכיפה וענישה

החוק מחזק את המודל המבוזר באמצעות הענקת סמכויות פיקוח ואכיפה משמעותיות לרגולטורים המגזריים. עובד מוסמך מגזרי רשאי לדרוש מארגון ידיעות ומסמכים לשם פיקוח על ביצוע הוראות החוק. כמו כן, הוא רשאי לבצע בקרה לשם פיקוח על יישום דרישות ההגנה.

בנוגע לאכיפה וענישה, החוק קובע שני מנגנונים עיקריים:

- **עיצומים כספיים:** ממונה ברשות המוסמכת של היחידה המגזרית רשאי להטיל עיצום כספי על ארגון חיוני שמפר הוראות המפורטות בתוספת החמישית, כאשר סכומי העיצום יכולים להגיע עד 640,000 ש"ח להפרה. החוק מאפשר הטלת תוספת לעיצום בשל הפרה נמשכת והפרה חוזרת, ומאפשר מתן התראה מנהלית כתחליף מקדמי לעיצום.
- **עונשין (פלילי):** אי נקיטה באמצעים שהורה עליהם ראש מערך הסייבר הלאומי או אי-מילוי הוראה להתמודדות עם תקיפה חמורה עלול להוביל ל**מאסר של שנתיים** או לקנס לפי חוק העונשין.

מנגנוני בקרה (איסוף המידע)

החוק מחייב הקמת מנגנוני בקרה ואיסוף מידע הן ברמה הלאומית והן ברמה המגזרית. ברמה המגזרית, כל יחידה מגזרית מחויבת לרכז את נתוני רמת ההגנה בסייבר בארגונים החיוניים במגזר המשק ולשתף אותם עם מערך הסייבר הלאומי באופן שוטף, ולכל הפחות אחת לרבעון. היחידה המגזרית מכינה גם עדכון מסכם שנתי הכולל נתונים על רמת ההגנה, פיקוח ואכיפה, ופעולות להטלת עיצומים, ומגישה אותם למערך הסייבר. בנוסף, כדי להבטיח פיקוח ממשלתי ופרלמנטרי על אופן יישום החוק, מוצע כי מערך הסייבר ידווח ליועץ המשפטי לממשלה ולועדת החוץ והביטחון של הכנסת, אחת לשנה, על נושאים בעלי משמעות כמפורט בהצעת החוק.

פרק שביעי - הגדרת יעדים וקריטריונים

האתגר במדידת יעילות אסדרה בסייבר מתכתב במידה מסוימת עם עקרונות כלכלת הביטחון של פרופ׳ אשר טישלר: הקושי לזקוף את ה׳שקט׳ הביטחוני אך ורק לזכות פעולות המגן. טישלר טוען שבעולמות הביטחון, התוצאה לעולם תלויה לא רק בפעולות המדינה (נניח השקעה במודיעין או במאמצי הגנה), אלא גם **במשתנה חיצוני** שאינו בשליטתנו- התנהגות היריב[150]. כך, ירידה בכמות תקיפות הסייבר החמורות בתקופה מסוימת לא בהכרח מעידה על אפקטיביות האסדרה, אלא עשויה לנבוע, למשל, מכך שקבוצות התקיפה בחרו מסיבותיהן להוריד פרופיל או למקד מאמצים בזירה אחרת.

במציאות שבה איננו שולטים במוטיבציית התוקף (וכן לא ברמת התחכום והיכולות שלו), המדידה האפקטיבית ביותר צריכה להתמקד במשתנים **שכן** נמצאים בשליטתנו, ובראשם רמת הבשלות (Maturity)והחוסן של הגופים המפוקחים. במובן זה, נזכיר כי אחת ממטרות האסדרה היא לפתור את כשלי השוק - ביניהם החצנות שליליות, היעדר מודעות וא-סימטריה מול התוקפים - ולחייב את הארגונים לבצע פעולות **שיקטינו את מרחב הסיכון** (גם אם לעולם לא יבטלו אותו לחלוטין).

לפיכך, מדידת השיפור ברמת המוכנות של מגזר - למשל, מעבר מרמת בשלות ״בינונית״ ל״טובה״ - היא האינדיקציה המעשית ביותר ליעילות. היא אמנם לא מבטיחה חסינות מוחלטת, אך היא מוודאת שתשתית ההגנה התחזקה, כך שכאשר התוקף יבחר לפעול, סיכויי ההצלחה שלו יפחתו והיכולת להכיל את האירוע תשתפר.

על בסיס זה אנו מציעים לבחון את האפקטיביות של האסדרה לפי שיעור המגזרים החיוניים שהערכת בשלות ההגנה שלהם, לפי המתודה שקבע מערך הסייבר[151], היא לכל הפחות ״בינונית-טובה״. זהו מדד אובייקטיבי המשקף בצורה ישירה את מידת הציות לחוק ואת סגירת הפערים בהגנה. ככל ששיעור הארגונים המצייתים עולה, כך הנחת העבודה היא שמשטח התקיפה המגזרי מצטמצם.

---

[150] https://www.ssoar.info/ssoar/bitstream/handle/document/11585/ssoar-2000-blume_et_al-security_needs_and_the_performance.pdf?sequence=1&isAllowed=y&lnkname=ssoar-2000-blume_et_al-security_needs_and_the_performance.pdf וכן כאן: Ross Anderson, Rainer Böhme, Richard Clayton, and Tyler Moore, ״**Security Economics and the Internal Market**,״ European Network and Information Security Agency (ENISA), January 29, 2008.

[151] מתודולוגיית הערכת בשלות ההגנה מבוססת על סקר המבוצע על ידי מס״ל, באמצעות שאלון אחיד המיושם בעיקר בגופי התמ״ק ובגופים חיוניים במגזרי המשק. לצורך השלמת ההערכה, משולבים אומדני מומחים המבוססים על אינדיקציות לחוסן בפועל, לרבות אירועי סייבר, מבדקי חוסן וחולשות פתוחות.

יעד	מדד	רף הצלחה	סוג הנתונים ומקורם	תדירות איסוף הנתונים	מועד לבחינה (מתום תקופת המעבר)
עליה ברמת החוסן הכוללת	שיעור המגזרים החיוניים שהערכת בשלות ההגנה שלהם מדורגת לכל הפחות "בינונית-טובה", וזאת בהתאם למתודה סדורה שיקבע מערך הסייבר.	75% מהמגזרים החיוניים בעלי הערכת בשלות "בינונית-טובה" לכל הפחות.	דוחות סיכום שנתיים של הרגולטורים המגזריים שיועברו למערך הסייבר וסקר המשולב עם הערכת המנחים המגזריים במערך, בהתאם למתודולוגיה שתקבע.	אחת לשנה (סקר חדש יותנע באופן יזום אחת לכשנתייםלכל היותר)	3 שנים

כדי להימנע מתמונת מצב סטטית העלולה להסתיר קיפאון או נסיגה בקרב חלק מהמגזרים (שנקודת המוצא שלהם הייתה גבוהה יחסית מלכתחילה), מוצע לשלב מדד דינמי לבחינת השיפור השוטף: שיעור המגזרים החיוניים שהציגו שיפור מובהק בציון הבשלות שלהם (קרי - מעבר בין רמות בשלות או הישארות ברמת הבשלות הגבוהה ביותר).

יעד	מדד	רף הצלחה	סוג הנתונים ומקורם	תדירות איסוף הנתונים	מועד לבחינה (מתום תקופת המעבר)
עליה ברמת החוסן פר מגזר	שיעור המגזרים החיוניים שהערכת בשלות ההגנה שלהם השתפרה באופן מובהק (מעבר לרמת בשלות גבוהה יותר או הישארות ברמת בשלות טובה).	100% מהמגזרים החיוניים שיפרו את רמת הבשלות שלהם (או נותרו ברמה הגבוהה ביותר האפשרית)	דוחות הסיכום השנתיים של הרגולטורים המגזריים המועברים למערך הסייבר, בשילוב הערכת המנחים המגזריים במערך על סמך מתודולוגיה שתקבע.	אחת לשנה	3 שנים

מטרה נוספת של האסדרה היא כזכור יצירת מנגנון של דיווח ושיתוף מידע באופן שיסייע לשפר את רמת ההגנה המצרפית במשק. במובן זה, חובת הדיווח שמחילה האסדרה המוצעת על ארגונים חיוניים צפויה להביא לגידול ניכר בהיקף הדיווחים. ואולם, עלייה גולמית במספר הדיווחים לבדה עלולה להטעות, שכן היא עשויה לשקף גידול חיצוני בתקיפות (עליו אין לנו השפעה) או שיפור טכני בניטור, ולאו דווקא ציות לחוק. אנו מציעים אפוא לקיים מעקב אחר היקף הדיווחים, תוך הבאה בחשבון (א) של שיפור ביכולות הניטור; (ב) תוך התייחסות לרמת האיום והסיכון בכל סקטור. מוצע לאפשר למערך הסייבר שהות של בניית המדד באופן מיטבי שיביא לידי ביטוי מורכבות זו, תוך שת"פ עם היחידות המגזריות, בזמן ההערכות שעד כניסת החוק לתוקף.

על אף שאנו צופים ששיפור ברמות החוסן יביא גם לשיפור ביכולות ההתמודדות וההתאוששות, אנו מציעים שלא למדוד בשלב זה זמני התאוששות. מדד שכזה עשוי להיתקל בקשיים תפעוליים משמעותיים, למשל- מתי בדיוק מסתיים האירוע? כשהשרתים חוזרים לאוויר, או רק כשהפעילות העסקית משתקמת במלואה? הגבול הזה מטושטש ונתון לפרשנות, והניסיון להגדירו **לצרכי תכלית רגולטורית רחבה** מורכב מאוד - בייחוד כשאנו עוסקים בארגונים ממגוון רב של ענפי משק ומגזרים.

נספח א': תיאור תהליך העבודה

מערך הסייבר הלאומי שוקד על קידום אסדרה לאומית רחבה להגנה בסייבר לפחות מאז אמצע העשור הקודם. שני ניסיונות כאלה, הראשון – תזכיר חוק הגנת הסייבר ומערך הסייבר הלאומי[152], משנת 2018 ; והשני – חוק סמכויות לשם חיזוק הגנת הסייבר (הוראת שעה)[153] מ-2021, לא הבשילו לכדי חקיקה, בין היתר בשל הסתייגויות משמעותיות שעלו מצד בעלי עניין שונים – הן בממשלה והן מחוצה לה.

בהמשך לכך, קיבלה הממשלה ביום 1 באוגוסט 2021 את החלטה מס' 219, שעניינה "בחינת רגולציה חכמה בסייבר וכללים וסמכויות למתן הנחיות בעת תקיפת סייבר מתמשכת, תוך שילוב שיקולים כלכליים." ההחלטה הורתה להקים צוות בין-משרדי בראשות מנכ"ל משרד ראש הממשלה, שיבחן, בין היתר, את הצורך ביצירת אסדרה נפרדת עבור גופים שאינם מנויים בתוספות הרביעית והחמישית לחוק להסדרת הביטחון בגופים ציבוריים. אסדרה כאמור, ככל שיוחלט עליה, תעסוק בכללים וסמכויות למתן הנחיות הן לגבי **היערכות** למתקפת סייבר והן לגבי מתן **הנחיות** בזמן תקיפת סייבר שעודנה בעיצומה לאותם גופים.

במהלך שנת 2022 קיים הצוות הבין-משרדי ארבע פגישות.

- הפגישה הראשונה כללה הצגה של תמונת המודיעין והאיומים ; התשתית הנורמטיבית בתחום הגנת הסייבר ; תמונת המצב בישראל בחלוקה למגזרים ; הצגת הבעיה (היעדר הפנמה של סיכוני הסייבר) ותמיכתה בנתונים.
- הפגישה השנייה כללה הצגה של "שכבות ההגנה במשק הישראלי" (ארגונים / חוסן מערכתי / הגנה לאומית) וכן סקירה בינ"ל השוואתית ראשונה שכללה את אירופה (NIS ו-NIS2), בריטניה, גרמניה, ארה"ב ואוסטרליה.
- המפגשים השלישי והרביעי כללו סקירה של תחום הגנת הסייבר בכמה משרדי ממשלה שהיו להם באותו שלב יחידות מגזריות: משרד הבריאות, הגנת הסביבה, התחבורה, האנרגיה והתקשורת. לגבי כל משרד הוצגו הסמכויות הקיימות (ככל שקיימות), על מי הן חלות, הגדרת הגופים החיוניים, מודל ההפעלה, ועוד.

השלב הבא כלל **העמקה ניכרת ומשמעותית בעולמות ההשוואה הבינ"ל**, בין היתר כפי שהורתה החלטת הממשלה 219. בשלב ראשון בוצעה הסקירה ע"י חברת Meidata. הסקירה סיפקה מידע בסיסי, בד"כ ברמת מאקרו, על אסדרת הגנת הסייבר ב-5 מדינות עליהן החליט הצוות הבין-משרדי (בריטניה, גרמניה, ארה"ב, אוסטרליה והולנד). בשל שאלות רבות שהתעוררו מן הסקירה הראשונית, והמורכבות הרבה של הנושא, המשיך אגף מדיניות במערך הסייבר **לסקירה מעמיקה ופרטנית של החקיקה** בכל אחת מ-5 המדינות (מצורפת לדו"ח זה בקובץ נפרד).

[152] https://www.gov.il/he/departments/news/cyberlawpublic
[153] https://www.law.co.il/media/computer-law/cyber_defense_bill_draft_version2_2021.pdf

בנוסף, בוצעה ע״י המערך סקירה מעמיקה של הדירקטיבות האירופאיות – NIS1 ו-NIS2, נוכח ההשפעה הרבה שלהן על כל מדינות האיחוד האירופאי ואף מעבר לו. כפי **שהוצג בפרק ג׳** לעיל, בכל מדינות ההשוואה אומץ מודל רגולטורי להעלאת החוסן ולהתמודדות עם אירועי סייבר בארגונים חיוניים. עיקר העבודה על הסקירה הבינ״ל הסתיימה ביוני 2023, והיא עודכנה מפעם לפעם בהתאם להתפתחויות בפועל במדינות ההשוואה.

ביולי 2023 קיים מערך הסייבר סדנא בת יומיים בהשתתפות נציגים מאסטוניה, ליטא, צ׳כיה ואיטליה, להעמקה בדירקטיבות NIS ו-NIS2, תחת פלטפורמת TAIEX. בסדנא השתתפו גם נציגים מכמה משרדי ממשלה, וביניהם משרד האוצר, משרד המשפטים, בנק ישראל, ועוד.

מטרת הסדנא היתה לשמוע באופן ישיר על דרכי היישום של האסדרה בפועל (ובכלל זה האתגרים שנבעו ממנה) – להבדיל מקריאת חומרים כתובים בלבד. אלה הן מקצת התובנות שעלו מן הסדנא:

- NIS היא דירקטיבה מחייבת, המהווה המינימום ההכרחי עבור כל אחת ממדינות אירופה החברות באיחוד. במובן זה ישראל נהנית מיתרון מסוים, היות והיא משוחררת מהחובה להסכים עם מדינות אחרות שעה שהיא יוצרת את הרגולציה המדינתית שלה. מאידך, יש כמובן יתרון ביצירת מסגרת אסדרתית הדומה בעיקרה לנהוג במדינות אירופה.
- על אף המחויבות לדירקטיבת NIS, עדיין יש שונות מסוימת בחקיקה הפרטיקולרית של מדינות שונות באירופה. לתרבות המקומית יש חשיבות בקביעת רגולציה: במדינות בעלות רמות הציות נמוכות באופן יחסי, הרגולציה שם תובענית יותר (מבוססת-תהליך). במדינות עם רמות ציות וולונטרי גבוהות, הרגולציה רכה ומאפשרת יותר (מבוססת-תוצאה).
- NIS היא חלק ממארג רחב יותר של אמצעים רגולטוריים שנועדו להתמודד עם סיכונים הקיימים במרחב הדיגיטלי, בין היתר החקיקה לאסדרת מוצרים דיגיטליים (Cyber Resilience Act) ועוד.

בד בבד עם העמקת ההשוואה הבינ״ל, עסקו הגורמים הרלוונטיים במערך, ובפרט באגף מדיניות, אגף מודיעין והכוונה, אגף הגנה סקטוריאלית והלשכה המשפטית, בגיבוש **תמונת המצב** לגבי רמת ההגנה במגזרים החיוניים בישראל והאסדרה המגזרית הקיימת. בין היתר הובאו בחשבון הממצאים של סקרי בשלות שערך אגף המדידה במערך הסייבר במגזרים השונים; מצב היחידה המגזרית; היקף האירועים במגזר והמגמה שנצפתה (עליה/ירידה); תמונת המודיעין; אירועי דגל במגזרים מסוימים; האם המגזר מאוסדר בד״כ לפי הבנצ׳מארק הבינ״ל, והסמכויות הקיימות בכל מגזר לטיפול בתחום הגנת הסייבר. הממצאים חידדו את הפערים הקיימים ברמת ההגנה בסייבר (ראו **בפרק א׳** לעיל) – רק 3 מ-16 מגזרים קיבלו הערכה גבוהה לגבי רמת ההגנה בסייבר. תמונת מצב זו מוצגת מעת לעת לממשלה.

לצד זאת, מאמץ מיוחד הושקע **בסיוע ליחידות המגזריות בגיבוש תבחינים לארגונים חיוניים**, כל אחת בענף המשק הרלוונטי לה. הגם שהסקירה הבינ״ל שביצע אגף מדיניות במס״ל כללה נושא זה, עלה הצורך לבצע התאמות של הממצאים למציאות הישראלית, וכן להבין מה ההשלכות של התבחינים השונים מבחינה מעשית. לצורך זה, נעזר המערך בחברת הייעוץ מקינזי, שביצעה עבודת

העמקה בנושא זה לגבי המגזרים הבאים: תחבורה, פיננסים, אנרגיה, שירותים דיגיטליים, תקשורת, מזון וחקלאות, מים וביוב, בריאות, כימיקלים, ממשל, אקדמיה וחלל.

עבור כל אחד מהמגזרים, נסקרה הדרך שבה נקבעו תבחינים לארגונים חיוניים ב-5 מדינות ההשוואה; לאחר מכן הוצגו שתי חלופות לתבחין ישראלי המבוסס על אותו רציונלי, ומשמעויותיו: מי הארגונים שיוגדרו כחיוניים, ומי הארגונים שלא יוגדרו חיוניים. העבודה הסתיימה בחודש אוגוסט 2023.

בשבועות שלאחר מכן, החל מערך הסייבר בסדרת **פגישות עם היחידות המגזריות השונות** לטובת הצגת עקרונות החקיקה המתגבשת, ובכלל זה סוגיית הארגונים החיוניים. הובהר לנציגי היחידות כי ככל שקיימים במגזר תבחינים מבוססים לגופים חיוניים, ניתן להותירם על כנם ואין הכרח לבצע התאמות לממצאי הסקירה הבינ"ל. אלה מובאים כשירות של המערך – על מנת להוות מעין השראה או רעיון לקביעת תבחינים, היכן שלא נקבעו כאלה, או שיש רצון לחשוב עליהם מחדש.

אירועי ה-7.10 קטעו את רצף הפגישות עם הרגולטורים המגזריים, והן התחדשו בראשית שנת 2024. הרגולטורים שנטלו חלק בדיונים כללו את רשות המים; משרד האנרגיה; משרד התקשורת; משרד החקלאות; המשרד להגנת הסביבה; המפקח על הבנקים; רשות שוק ההון וביטוח; משרד הבריאות; משרד הכלכלה; משרד הפנים, משרד התחבורה ומערך הדיגיטל, הרשות לניירות ערך ומשרד הדתות.

להלן שלבים מרכזיים נוספים בתהליך שביצועם החל ב-2023:

- **הערכת עלויות כלכליות** - צוות של הכלכלן הראשי במערך הסייבר ביצע אמדן ראשוני של העלויות הנובעות מן החקיקה (עלויות למדינה + עלויות למפוקחים). ממצאי הסקירה הוצגו **בפרק ה'** בדו"ח זה. במסגרת התהליך, ביצע הכלכלן הראשי פנייה יזומה למספר ארגונים חיוניים שהחוק צפוי לחול עליהם, באמצעות היחידות המגזריות המפקחות עליהם. מן המשובים עלה כי התחשיבים שביצע המערך סבירים ואף שמרניים. הערכת העלויות כאמור, לרבות משמעויות לממשלה, הוצגה לנציגי אגף התקציבים והחשב הכללי במשרד האוצר, המועצה הלאומית לכלכלה, משרד ראש הממשלה והמועצה לביטחון לאומי (מל"ל).
- במחצית 2023 הוצגו עקרונות החקיקה המתגבשת לקבוצה של ארגונים ממגזר הטכנולוגיה, על מנת לקבל את התייחסותן הראשונית. ככלל, החברות שהשתתפו בפגישה (בהשתתפות שרת המודיעין דאז) התמקדו בסוגיית חובת דיווח על תקיפות סייבר חמורות.
- במהלך השנים 2023-2024 בוצע בהזדמנויות שונות (למשל במסגרת שבוע הסייבר בישראל, בביקורי עבודה בחו"ל או בישראל) שיח ישיר עם אנשי מדיניות רגולציה בבריטניה, גרמניה, צ'כיה ואסטוניה בניסיון ללמוד מיישום האסדרה באותן מדינות.
- **דיונים מול נציגי משרד האוצר** (בעיקר מאגף התקציבים) - בעקבות הממצאים החד-משמעיים שעלו מההשוואה הבינ"ל ובדיוני הצוות הבין-משרדי המוזכר לעיל, החל מערך הסייבר בגיבוש מסמך "מתווה עקרונות" לחקיקה. המתווה הוצג לנציגי אגף התקציבים במשרד האוצר, והתקיימו עליו כמה דיונים בין החודשים דצמבר 2022 עד יוני 2023. בדיונים אלה הדגישו נציגי אגף התקציבים, לצד נושאים אחרים, את הצורך ברגולציה מידתית, דיפרנציאלית, מבוססת ניהול-סיכונים, העולה בקנה אחד עם הבנצ'מארק הבינ"ל.

- בהמשך לכך גיבשה הלשכה המשפטית במערך הסייבר את **הטיוטה הראשונה** של הצעת החוק הנוכחית, אשר הועברה לאוצר. בהמשך להפצת הטיוטה החלה סדרה של דיונים בהשתתפות נציגי מס״ל והאוצר, וכן חלופה מתמשכת של נוסחים, הערות, מענים וכיו״ב. בשלהי 2023 אף התקיימו כמה פגישות בהשתתפות ראש מערך הסייבר דאז, בניסיון להביא להבשלת התזכיר עד סוף אותה שנה.

אירועי ה-7.10 הסיטו כאמור את עבודת המטה על החוק הראשי ממסלולה. מאז פריצתה של המלחמה זוהתה, בין השאר, עליה ניכרת בניסיונות למתקפות סייבר נגד ספקי שירותי אחסון ושירותים דיגיטליים, המהווים גופי שרשרת אספקה לארגונים רבים במשק, ובכלל זה לארגונים חיוניים. לצורך הגנה על הציבור ושמירה על הרציפות התפקודית במשק בזמן המלחמה, חוקק כהוראת שעה החוק להתמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה-חרבות ברזל), התשפ״ד-2023[154]. הוראת השעה הוארכה מעת לעת, ולאחרונה עד ליום 31.1.26. ההארכה האחרונה כללה גם תיקונים, ובכללם ניתוק הקשר בין הוראת השעה לחרבות ברזל.

בין היתר, הוראת השעה מאפשרת למערך הסייבר (וכן לשירות הביטחון הכללי ולמלמ״ב, לפי הנסיבות המנויות בחוק) לתת לספקי שירותים דיגיטליים ושירותי אחסון **הוראות** כיצד להתמודד עם תקיפת סייבר חמורה, כהגדרתה בחוק. הוראת השעה גם קובעת לאותם ספקים חובת דיווח על תקיפת סייבר משמעותית, ומטילה עליהם חובה לעדכן בכך ארגונים מקושרים על תקיפה חמורה בנסיבות הקבועות בה.

הגם שמדובר בחקיקה נפרדת, הערות שהתקבלו במסגרת העבודה על הוראת שעה הוטמעו גם לנוסח החוק המוצע (ככל שהיו רלוונטיות). כמו כן, הוטמעו בנוסח המוצע לקחים מתקופת יישום הוראת השעה.

שני שלבים נוספים בתהליך בוצעו בשנת 2024:

- **התייעצות רוחבית על האסטרטגיה הלאומית הסייבר** - בעקבות אירועי ה-07.10 הורה ראש מערך הסייבר דאז לבצע בחינה מחדש של ״האסטרטגיה הלאומית בסייבר״ למדינת ישראל. טיוטת האסטרטגיה כללה בין היתר את הצורך לחזק את ההגנה על הארגונים החיוניים, לרבות באמצעות אסדרה חוקית. המלצה זו ואחרות הוצגו לשורה ארוכה של שותפים ובעלי עניין במהלך שנת 2024, ובכלל זה גופי ביטחון, גופים ממשלתיים, גורמים בתעשיית הסייבר וכן אנשי אקדמיה ומומחים. אלה העירו, בין השאר, כי:
  - מאמץ החקיקה צריך להביא בחשבון את הקושי בשיתופי פעולה בין גורמים ממשלתיים שונים;
  - יש צורך לייצר מסגרת רגולטורית גמישה ודינמית שתוכל ״לרוץ בקצב הטכנולוגיה״;
  - יש חשיבות בשילוב סטנדרטיזציה ותקינה בינ״ל;

[154] לנוסח העדכני, ראו כאן: https://main.knesset.gov.il/activity/legislation/laws/pages/lawprimary.aspx?t=lawlaws&st=lawlaws&lawitemid=2212973

- הנסיבות והמאפיינים של ישראל שונים מהעולם כך שהאפקטיביות של מסמכי השוואה בינ״ל עשויה להיות מוגבלת בהקשרים מסוימים ;
- את הצורך לשלב רגולציית ציווי ושליטה (command and control) עם כלי מדיניות אחרים, כגון הענקת ידע, מתן תמריצים, רכישת ביטוח, תקינה למוצרי תוכנה וחומרה, ועוד.
- עוד עלה באותה מסגרת הצורך ליצור מסגרת אכיפה מול נתקפים חוזרים, שאינם פועלים לסגירת פערי אבטחה בסייבר ; והצורך לשמור על חוק מאוזן, שאינו פוגע בכלכלה או בזכויות הפרט.

- **הצגת דרישות ניהול הסיכון לפורום ראשי היחידות המגזריות** - במהלך שנת 2024 הציג ראש מרכז תורה במערך הסייבר, את רשימת הדרישות הצפויות להיכלל בחוק הסייבר לפורום של מנהלי היחידות המגזריות במשרדי הממשלה[155]. נכחו בה כל ראשי היחידות המגזריות, כמו גם ראשי המרכזים באגף הנחיה סקטוריאלית במערך הסייבר.
  - במהלך השיחה הוסבר הרציונל של גיבוש הדרישות, ובראשן התאימות לעשרת העקרונות המופיעים בדירקטיבת NIS2 (ראו **בפרק ו׳** לעיל). עוד הוסבר, כי הדרישות שגובשו נותנות מענה ל-3 מאמצים בהגנת סייבר: להיערכות (חוסן), להתמודדות עם אירועים, ולרציפות תפקודית. הודגם כיצד כל אחד מהעקרונות נותן מענה לאחד (או יותר) משלושת המאמצים.
  - עבור כל עקרון לרמת ההגנה הנדרשת המוצעת, פורטו הדרישות שגובשו, בהתאם למדריך ENISA (דאז עדיין במעמד טיוטה) ליישום העקרונות. התנהל שיח ער וחיובי סביב הדרישות ל״הגנה ראויה״ ; נשאלו שאלות והועברו חידודים מקצועיים.
  - ניכר היה שמנהלי היחידות זיהו את האפקטיביות של דרישות הבסיס לרמת הגנה, ועלה מצידם כי הן אינן מבטאות מאמץ היוצא מגדר הרגיל מצד הארגונים. עוד הוסבר, כי על מנת לעמוד בדרישות החוק ובניסיון להקטין נטל רגולטורי, יצטרכו הארגונים לעמוד בדרישות באמצעות ישום החלקים הרלוונטיים בתקינה בין לאומית.

עבודת המטה המוצגת במסמך זה נמשכה למעלה משנתיים, וכללה תהליך היוועצות נרחב וסדרת דיונים מעמיקים עם משרדי הממשלה (בדגש על משרדי המשפטים והאוצר), המשרדים הרגולטוריים/היחידות המגזריות וגופי ביטחון, לצד שיח עם מומחים מהאקדמיה, מהמגזר השלישי ומארגונים במשק. את המלאכה הובילו גורמי המקצוע במערך הסייבר: הלשכה המשפטית, אגף מדיניות, האגף להגנה סקטוריאלית, לשכת ראש המערך וה-CERT הלאומי. תהליך גיבוש החוק היה אינטנסיבי והצריך אלפי שעות עבודה במצטבר.

להלן ריכוז הסוגיות המרכזיות, השאלות והתובנות שעלו במסגרת הדיונים, והתייחסות המערך אליהן.

[155] רשימת הדרישות כפי שהיתה ידועה נכון לאותו זמן ; לא חלו שינויים משמעותיים ביחס לנוסח המופיע בתזכיר החוק.

1. **טענה: האסדרה המוצעת אינה שוקלת במידה מספקת שיקולים כלכליים ומשקיים, ועלולה להוביל להכבדת הנטל הכלכלי ולהתייקרות מחירים.**

מענה:

א. ניתוח עלויות פרטני: דוח זה מציג ניתוח מפורט של העלויות הצפויות. מהניתוח עולה כי העלויות הבירוקרטיות (דיווח, ציות ולמידת החוק) הן זניחות. העלות העיקרית נובעת, מטבע הדברים, מפעולות הגנת הסייבר עצמן (ניהול סיכונים) בדגש על ארגונים חיוניים אשר כיום רמת ההגנה בסייבר שלהם אינה מספקת. כפי שהוצג בפרק ה', העלות לארגון בודד מוערכת בטווח שבין 0 ל-1.9 מלש"ח בשנה, כתלות בגודלו ובמצב ההגנה הנוכחי שלו. משמעות הדבר היא שעבור ארגונים שמצב ההגנה בסייבר שלהם תקין כבר היום – העלות השולית הנובעת מהחוק צפויה להיות נמוכה.

ב. המחיר הכלכלי של היעדר הגנה: יש לבחון את העלות מול התועלת במבט משקי רחב. הסיכון הכלכלי המשמעותי אינו נובע מעלות הציות לחוק, אלא מהנזקים האדירים הנגרמים כתוצאה מהגנת סייבר חסרה. כפי שהוצג, המצב הנוכחי מסב למשק נזק המוערך כבר כיום בכ-12 מיליארד ש"ח בשנה. נזקים אלו הם שמייצרים כבר עתה "מס סייבר" סמוי ועלויות עודפות למשק הישראלי, והחוק נועד לצמצם אותם.

ג. צמצום הנטל הרגולטורי: מערך הסייבר נקט בשתי גישות מרכזיות כדי להבטיח את צמצום הנטל הרגולטורי: ראשית - רף דרישות של המינימום ההכרחי: רשימת הדרישות שגובשה על ידי מרכז התורה והמתודולוגיה במערך מהווה סטנדרט בסיסי והכרחי המבוסס על תקינה בין לאומית, גישה שזכתה לתיקוף גם מצד ראשי היחידות המגזריות; שנית, במיקוד הגופים שבתחולה: בשונה מהרגולציה האירופית (NIS 2) המכילה חובות על כל "עסק בינוני" (עשרות אלפי ארגונים), המודל הישראלי מבוסס בשלב זה על תבחינים מגזריים הממקדים את החוק במספר מצומצם יחסית של גופים חיוניים. מיקוד זה מבטיח שהנטל בשלב זה יחול רק מקום שם הסיכון הלאומי גבוה. בנוסף, נזכיר כי הרגולטור המגזרי רשאי לפטור ארגון חיוני מדרישות רמת ההגנה, בכפוף לתנאים המנויים בחוק, אם זה הוכיח (באמצעות הערכה של צד שלישי) עמידה בתקנים מחמירים ביחס לשירותי הליבה שלו.

2. **טענה: האסדרה המוצעת מתעלמת מהסטנדרט הבינלאומי ומותירה פתח ליצירת רגולציה ייחודית לישראל; קיים חשש כי שינויים בתקנות ייעשו באופן שרירותי, ללא התראה וללא התחשבות בשיקולים מסחריים.**

מענה:

א. עקרון הבנצ'מארק הבינלאומי כבסיס: דוח זה הראה כי ההשוואה הבינלאומית הייתה אבן הראשה של עבודת המטה. החל מההחלטה על מודל האסדרה ועד לפרטי חובות הדיווח וניהול הסיכונים – הכל נגזר מהמתרחש בעולם. זאת במקביל לשינויים מתחייבים כתוצאה מהצרכים הייחודיים במדינת ישראל.

ב. החובה בחוק להיצמד לסטנדרט מערבי בנוגע לרמת הגנה: תזכיר החוק קובע במפורש כי ההוראות יתבססו על כללים הנהוגים ב"מדינות מפותחות עם שווקים משמעותיים" למעט במקרים בהם קיימות נסיבות מיוחדות המצדיקות אחרת, כפי שמורה חוק עקרונות האסדרה. משמעות הדבר היא שהרגולטורים חייבים, ככלל, לפעול בהקשרים אלו לפי הסטנדרט העולמי, וזוהי הדרך הטובה ביותר למנוע שרירותיות.

ג. אימוץ בפועל של רגולציית NIS2 האירופית : ברמה המעשית, דרישות ניהול הסיכון להגנה נדרשת בהצעת החוק הישראלי נוסחו בהתאמה מלאה לעקרונות ההגנה של דירקטיבת 2NIS האירופית ולמסמכי היישום של סוכנות הסייבר האירופית (ENISA) . התאמה זו מבטיחה כי ככלל, ארגון שפועל בזירה הגלובלית לא יידרש לבצע התאמות ייחודיות ברמת ההגנה הנדרשת עבור השוק הישראלי.

ד. "נמל מבטחים" – הכרה בתקנים קיימים: בניסיון לצמצם נטל רגולטורי, החוק מורה לארגונים לעמוד בחובותיהם לעניין רמת הגנה נדרשת באמצעות עמידה בהוראות הרלוונטיות בתקנים בינלאומיים מובילים, כגון ISO 27001 , מסגרת העבודה של NIST (CSF) או NIST SP 800-53. מודל זה מתמרץ את השוק לאמץ סטנדרטים בינלאומיים, ומבטיח כי עבור חברות שכבר פועלות לפי סטנדרט גבוה – תוספת הנטל הרגולטורי תהיה מינימלית.

3. טענה: התבחינים להגדרת "ארגון חיוני" עמומים, אינם מספקים ודאות למשק, ואינם נצמדים לסטנדרט הבינלאומי המקובל.

<u>מענה</u>:

א. מידתיות (הימנעות מהרחבת יתר): הדרישה להיצמד לבנצ'מארק הבינלאומי העדכני (NIS2) הייתה מחייבת להחיל את החוק על כל עסק בינוני ומעלה במדינת ישראל (על בסיס גודל מחזור וכמות עובדים). לגישתנו, זהו צעד לא מידתי בעת הזו. לכן, בחר המערך לדבוק בשיטת "התבחינים המגזריים" (הבוחנת את מהות העיסוק וחיוניות עיסוקו), שיטה שהייתה נהוגה באירופה בדור הראשון של חקיקת הסייבר.

ב. עיגון בחקיקה: אומץ מנגנון הקובע כי התבחינים, ככל שישונו, ייקבעו על בסיס אמות מידה מקצועיות המיושמות במדינות מפותחות. כלומר, החוק יוצר עוגן מקצועי מחייב המונע קביעת תבחינים שרירותיים, למעט במקרים החריגים בהם הוחלט כי קיים בכך צורך – אז שומה על הגורם המבקש להוכיח צורך כאמור.

ג. המודל הבריטי – ריסון כוחו של הרגולטור: לצד ההכרה בהכרח לייצר מסלול חריגים לארגונים חיוניים, הצעת החוק אימצה את המודל הבריטי המגביל את שיקול הדעת של הרגולטור. על פי מודל זה, בבואו להכריז על ארגון כ"חיוני" שלא על פי התבחינים המנויים, הרגולטור מחויב לשקול שורת שיקולים שפורטו בחוק וכן להיוועץ בוועדה ייעודית. במקרה זה, לארגון קיימת גם זכות שימוע בה יוכל להציג טענותיו טרם קביעת המאסדר.

4. טענה: האסדרה המוצעת עלולה לפגוע באקלים העסקי ולהרחיק השקעות חיצוניות, בשל הענקת סמכויות לא-מידתיות והיעדר חובה לשקול שיקולים מסחריים וכלכליים.

<u>מענה</u>

א. סמכויות סטנדרטיות (השוואה לרגולטורים אחרים): סמכויות הפיקוח המוקנות לעובד המוסמך בחוק (כגון הסמכות להיכנס לחצרים או לדרוש מסמכים) הן סמכויות סטנדרטיות ומקובלות במשפט המנהלי הישראלי. אין בהן כל חריגה מהנורמה, והן חיוניות לביצוע פיקוח אפקטיבי. לראיה, סמכויות אלו מוקנות כיום בחקיקה ראשית לשורה ארוכה של רגולטורים, שכן מדובר בחלק אינטגרלי בארגז הכלים של הרגולטור הישראלי. סמכויות דומות מוענקות לרגולטורים בבנצ'מארק הבינ"ל.

ב. חובה מפורשת לשקול עלויות: הצעת החוק מחייבת את הרגולטור באופן מפורש לשקול שיקולים כלכליים ומסחריים בעת מתן הוראות להתמודדות עם תקיפת סייבר חמורה, כך למשל: "במתן הוראות... ישקול העובד המוסמך... את העלות הכלכלית המוערכת של יישום ההוראות והשפעתן האפשרית על הרציפות התפקודית של הארגון החיוני". יתרה מכך, אם הארגון הגיש הערכת עלויות מטעמו – החוק מחייב את הרגולטור להתחשב בה. חובה זו חלה באופן מלא גם על עובדי מערך הסייבר.

5. טענה: חובת הדיווח המוצעת מחמירה באופן קיצוני ביחס לבנצ'מארק הבינלאומי, הן בהיקף האירועים המדווחים והן בלוחות הזמנים.

<u>מענה</u>

א. צמצום התחולה ל"תקיפות" בלבד (הקלה רגולטורית): בניגוד לנטען, חובת הדיווח בחוק הישראלי דווקא מקילה ביחס למקובל במדינות ההשוואה (ובכלל זה בדירקטיבת NIS 2 האירופית). בעוד שבעולם חובת הדיווח חלה על כל "אירוע סייבר" (Incident) – כולל תקלות טכניות, טעויות אנוש וכשלים לוגיים – החוק הישראלי מחייב דיווח אך ורק על "תקיפות סייבר" (קרי, אירועים שמקורם זדוני). צמצום זה מפחית באופן דרמטי את כמות הדיווחים הנדרשת ואת הנטל הרגולטורי על הארגונים, וממקד את המאמץ הלאומי באיומים זדוניים בלבד.

ב. הגדרת "אירוע משמעותי" – יישור קו עם העולם: הטענה בדבר היעדר הגדרה ברורה לתקיפה משמעתית המחייבת דיווח אינה מדויקת. בדומה לרוב מדינות ההשוואה, החוק אינו נוקט דרך של הגדרה ייחודית ("Definition"), אלא קובע מנגנון אופרטיבי: ניסוח תנאים וקריטריונים <u>שבהתקיימם</u> האירוע (או התקיפה, בנוסח הישראלי) הופך לבר-דיווח. גישה זו תואמת את הנעשה בעולם:

- בבריטניה: החובה לדווח נגזרת מ"השפעה משמעותית" של אירוע סייבר על השירות - מספר המשתמשים שהושפעו, משך השיבוש והאזור הגיאוגרפי שנפגע;
- בגרמניה: חוק ה-BSIG והמסמכים הנלווים אליו קושרים את חובת הדיווח לקיומו של "כשל IT" הפוגע בזמינות, במהימנות או בסודיות של תשתית קריטית.
- באוסטרליה: אין הגדרה נפרדת לאירוע בר-דיווח, אלא חובת דיווח שקמה כאשר לאירוע יש "השפעה משמעותית" (ישירה או עקיפה) על זמינות הנכס.

ג. לוחות הזמנים לדיווח (מידיות): הדרישה לדיווח מיידי הכרחית לאור אופי האיום. נוכח הסיכונים בישראל, ומאחר והחוק הישראלי עוסק בתקיפות (זדון) ולא בתקלות סתם, חלון הזמן לתגובה אפקטיבית, סגירת מעגל ומניעת התפשטות הוא קצר ביותר. דיווח שאינו נעשה בסמוך לגילוי שומט את הקרקע תחת היכולת המבצעית של המערך לסייע לארגון ולהזהיר את המשק. מבחינה השוואתית, הדרישה לדיווח מהיר (12-24 שעות) מקובלת בעולם, והולכת ומתקצרת (בריטניה – ירידה מ-72 ל-24 שעות). ראו לעניין זה פירוט מלא בפרק ג' לעיל. עוד יש לציין, כי גם תקנות אבטחת המידע בישראל מחייבות דיווח באופן מיידי.

ד. מתן פטור מחובת דיווח למי שעומד בתקינת סייבר מחמירה: בדיונים על הוראת השעה למגזר השירותים הדיגיטליים ושירותי האחסון עלתה הדרישה לפטור חברות העומדות בתקינת סייבר בינ"ל איכותית מחובת הדיווח. מעבר לתפקידה בידוע הרגולטור, חובת הדיווח נועדה לאפשר למערך הסייבר לייצר תמונת מצב ברמה הלאומית, להצליב מידע ובמידת הצורך להתריע בפני גופים אחרים. עמידת ארגון זה או אחר בתקן מחמיר של הגנת סייבר אינה מחליפה את

הצורך של המדינה לדעת על התקיפה, ולכן פטור מדיווח אינו מוצדק, ונראה שגם אין לכך תקדים בבנצ'מארק הבינ"ל.

6. **טענה: רגולציה ודרישות הגנה מחמירות על המגזר הציבורי עלולות לייצר "חסמי כניסה" שיפגעו ביכולת להתקשר עם עסקים קטנים וחדשניים (סטארט-אפים), ואף יובילו להתייקרות רוחבית של המכרזים והרכש הממשלתי.**

<u>מענה</u>

א. חובת הממשלה כנאמן הציבור: גם תחת המסגרת החוקית הקיימת, הממשלה רשאית ואף מחויבת לקבוע דרישות סף מקצועיות לספקים שלה. כגוף המחזיק במידע הרגיש ביותר של אזרחי ישראל, חזקה על הממשלה שהיא מעוניינת להתקשר רק עם ספקים אחראיים המנהלים סיכונים כראוי. ההחלטה שלא להתפשר על אבטחת המידע, גם במחיר של סינון ספקים שאינם עומדים ברף, היא החלטה ניהולית וציבורית מתבקשת לשם הגנה על הציבור.

ב. מגמה עולמית – הממשלה כמודל: בחינת הנעשה בעולם מראה כי דווקא במדינות המערב המתקדמות, הדרישות כלפי ספקי הממשלה הולכות ומחמירות, מתוך תפיסה שהממשלה צריכה לשמש מודל לחיקוי לכלל המשק ולהעלות את הסטנדרט בשוק.

- ארה"ב (שרשרת אספקה ופיתוח מאובטח): הצו הנשיאותי 14028 מנחה את הממשל הפדרלי לאמץ ארכיטקטורת "אפס אמון" (Zero Trust) ולהקשיח את דרישות הרכש. בהמשך לכך, מזכר M-22-18 של ה-OMB מחייב סוכנויות פדרליות לרכוש תוכנה רק מיצרנים העומדים בתקן ה-SSDF (הנחיות לפיתוח תוכנה מאובטח של מכון NIST). רגולציה זו מחייבת בפועל כל חברת טכנולוגיה שרוצה לעבוד עם הממשל האמריקאי ליישר קו עם סטנדרט אבטחה מחמיר.
- גרמניה (בדיקת מוצרים): סעיף 3 לחוק הגרמני מעניק למשרד הפדרלי לאבטחת מידע (BSI) סמכות נרחבת לבצע בדיקה, הערכה ואישור של מערכות IT המיועדות לעיבוד מידע בגופים פדרליים.

7. **טענה: סמכויות ההתערבות של הרגולטורים והמערך בעת תקיפה חמורה נשענות על קריטריונים עמומים (כגון "בטחון הציבור"), המותירים פתח לשיקול דעת רחב מדי, ועוקפים את סמכות הרגולטור המגזרי ואת האוטונומיה של הגוף הנתקף.**

מענה המערך

א. ודאות משפטית וסטנדרט בינלאומי: המונח "בטחון הציבור" האו מונח מקובל בחקיקה; זהו מונח שזכה לפרשנות ענפה וברורה בפסיקה הישראלית לאורך השנים. יתרה מכך, השימוש במונחי שסתום כגון "ביטחון המדינה" או "יציבות המשק" הוא כורח המציאות כשעוסקים בהגנה מפני איומים לאומיים דינמיים, חמורים ומשתנים. סקירה משווה מגלה כי המחוקק המערבי משתמש במינוחים רחבים דומים בדיוק כדי לא לכבול את ידי המדינה בעת חירום.
באוסטרליה, לדוגמא, החוק מעניק לשר האחראי סמכויות נרחבות להכריז על נכס כ"קריטי" (גם אם אינו עומד בתבחינים כלשונם) או להורות על התערבות, כל עוד הדבר נדרש ל"יציבות

החברתית או הכלכלית", ל"הגנת המדינה" או ל"ביטחון הלאומי". החוק אף מאפשר במקרים מסוימים הכרזה חשאית על נכס קריטי מטעמי ביטחון לאומי[156].

ב. מתן הזדמנות לפעולה עצמאית (איזונים ובלמים): טיוטת החוק מעגנת חובה לאפשר לארגון לפעול בעצמו ו/או להשמיע את טענותיו בטרם ינתנו לו הוראות לטיפול בתקיפה (למעט במקרים דחופים ביותר). זהו המנגנון המאפשר לארגון להשמיע את קולו, להציג חלופות או להביע הסתייגות בטרם תתקבל החלטה.

ג. הבחנה בין "רגולציה" ל"תגובה מבצעית": יש להבחין בין אסדרה (רגולציה) לבין התערבות בזמן אמת. בעוד שאסדרה עוסקת באכיפת נורמות וכללים בשגרה, התערבות בעת תקיפה חמורה היא אקט מבצעי שנועד לבלום נזק מתגלגל. מכל מקום, החוק קובע מנגנוני ריסון גם בהליך זה: במקרה שמתן ההוראות מבוצע ע"י מערך הסייבר הדבר נעשה תוך יידוע הרגולטור המגזרי הרלוונטי (כך שהוא אינו "נעקף"); ובכל מקרה ההוראות ניתנות רק לאחר שהעובד המוסמך שקל שיקולים רחבים – כולל משמעויות כלכליות ועלויות לארגון – בטרם מתן ההוראות.

8. **טענה: אין הצדקה להטיל רגולציה על החברות הגדולות והמבוססות, ובכלל זה במגזר הטכנולוגיה, שכן הן ממילא מחויבות לסטנדרטים גבוהים ומנהלות את הגנת הסייבר שלהן באופן עצמאי.**

<u>מענה</u>

א. היעדר עלות נוספת: המשוואה פשוטה; אם חברות גדולות כבר מקיימות פרקטיקות הגנה מחמירות העולות על דרישות הסף של החוק – הרי שהחוק לא ייצר עבורן עלות נוספת. החוק נועד ליישר קו עבור מי שאינו מוגן, ולא להפריע למי שכן. חובת הדיווח יוצרת אמנם נטל מסוים – אך הוא שולי ביותר מבחינת עלויות, נחוץ מבחינת האינטרס הלאומי, ומקובל באירופה, אוסטרליה וארה"ב.

ב. המגמה העולמית – רגולציה ספציפית ומהודקת: עם כניסתה של דירקטיבת NIS 2 לתוקף באירופה, הורחבו הוראות ניהול הסיכון לגופים חיוניים במגזרי התשתיות הדיגיטליות, ספקי שירותים דיגיטליים וספקי שירותי ICT. הנציבות האירופית אף פרסמה לאחרונה תקנות יישום (Implementing Regulation)[157] ייעודיות, הכוללות נספח עם פירוט דקדקני של אופן מימוש חובת ניהול הסיכונים ספציפית למגזרים אלה. העובדה שהרגולטור האירופי בחר לפרסם הוראות טכניות פרטניות דווקא למגזר זה, מעידה על הצורך באסדרה חיצונית גם עבור שחקנים טכנולוגיים חזקים.

ג. הכרה בשונות והקלות: יחד עם זאת, מערך הסייבר מכיר בשונות הגדולה הקיימת בין ארגונים חיוניים שונים, הכוללים בין היתר גם חברות מבוססות בעלות רמה נאותה של הגנת סייבר. עבור קבוצה זו, מוצע לאפשר לרגולטור, בכפוף לתנאים שנקבעו בחוק, לפטור ארגון מעמידה בדרישות רמת ההגנה וכן ממתן הוראות בעת תקיפה חמורה, ובלבד שיוכיח (באמצעות הערכה של צד שלישי) עמידה בתקנים מחמירים על שירותי הליבה שלו. **מודל זה מאזן היטב בין האינטרס הלאומי בהגנה על ארגונים לחיוניים, לבין היכולת של חלק מהארגונים המפוקחים להגשים את אותו אינטרס באמצעים אחרים.**

---

[156] סעיפים 9 (f)(1)ו-9(3) לחוק ה SOCI-האוסטרלי; וכן סעיפים 51A ו-51, 35AB(1), 35AA.

[157] תקנות היישום של הנציבות האירופית (Implementing Regulation) בנוגע לניהול סיכונים בתשתיות דיגיטליות: https://digital-strategy.ec.europa.eu/en/library/nis2-commission-implementing-regulation-critical-entities-and-networks

נספח ב': תקיפות סייבר בולטות מן השנים האחרונות

להלן כמה דוגמאות לתקיפות סייבר משמעותיות אשר הביאו לפגיעה ניכרת בנכסים, תשתיות ו/או ארגונים חיוניים בעולם. דוגמאות אלה ממחישות את החשיבות של נקיטת אמצעי הגנה בסיסיים, בפרט בארגונים המשתייכים לקטגוריות אלה.

- **Synnovis** - ב-3 ביוני 2024, נפלה שותפות המעבדות הבריטית Synnovis קורבן למתקפת כופרה שגרמה לשיבושים נרחבים ולירידה משמעותית ביכולת לעבד דגימות מעבדה. המתקפה השפיעה ישירות על בתי חולים של ה-NHS ועל שירותי רפואה קהילתית במספר רבעים בלונדון, ואילצה את הצוותים לבטל ולדחות טיפולים רפואיים ולעבור לפרוטוקולים ידניים מבוססי נייר. תהליך ההתאוששות המורכב, שכלל בנייה מחדש של למעלה מ-60 מערכות IT מקושרות, נמשך חודשים ארוכים[158].

- **מתקפת Snowflake (אפריל–יוני 2024)** - המתקפה יוחסה לקבוצת התקיפה UNC5537 (המקושרת לקבוצת Scattered Spider). הקורבן הישיר היה פלטפורמת אחסון ועיבוד הנתונים בענן Snowflake, אך דרכה הותקפו מעל 160 לקוחות ארגוניים, בהם ענקיות כמו AT&T (גניבת 50 מיליארד רשומות שיחות), Ticketmaster (דליפת פרטי 560 מיליון לקוחות) ובנק Santander. הנזק כלל גניבת כמויות עתק של מידע רגיש, פגיעה במוניטין ועלויות שיקום וחקירה שנאמדו במאות מיליוני דולרים. הארגונים חזרו לפעילות הדרגתית תוך ימים עד שבועות, אך הליכי הטיפול בדליפות המידע נמשכים עד היום.[159]

- **Change Healthcare** - ב-21 בפברואר 2024, הותקפה חברת Change Healthcare, חברת בת של UnitedHealth Group, המהווה צומת מרכזי לעיבוד עסקאות במערכת הבריאות האמריקאית. התקיפה בוצעה על ידי קבוצת כופרה בשם ALPHV BlackCat. על פי הדיווחים היא שיתקה פונקציות קריטיות כגון אימות זכאות לביטוח, הנפקת מרשמים וביצוע תשלומים, ופגעה בתיעוד הרפואי של אחד מכל שלושה מטופלים בארה"ב. האירוע הוגדר כפריצת המידע הגדולה ביותר בהיסטוריית הבריאות של ארה"ב, לאחר שנגנב מידע רפואי מוגן של כ-100 מיליון אמריקאים. השפעת המתקפה הייתה כה נרחבת עד שהיא איימה על היציבות הכלכלית של ספקי שירותי בריאות רבים ברחבי המדינה ואילצה בתי חולים להסתמך על תהליכים ידניים יקרים ולא יעילים[160].

- **CyberAv3ngers** – ב-1 בדצמבר 2023 פרסמה CISA, סוכנות הגנת הסייבר של ארה"ב הודעה משותפת עם ה-FBI, מערך הסייבר, וכמה סוכנויות אמריקאיות נוספות, המזהירה מפני פעילות סייבר זדונית שמקורה במשמרות המהפכה של איראן. לפי ההודעה, קבוצת התקיפה CyberAv3ngers שמה לה ליעד לפגוע בתעשיות המים, האנרגיה והמזון בארצות הברית.

[158] עדכונים רלוונטיים באתר Synnovis: https://www.synnovis.co.uk/cyberattack-information-centre.
[159] https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion
[160] https://www.aha.org/system/files/media/file/2025/02/Change-Healthcare-Cyberattack-Underscores-Urgent-Need-to-Strengthen-Cyber-Preparedness.pdf

המתקפות נעשות באמצעות פגיעה במוצרים של החברה הישראלית יוניטרוניקס, שמפתחת ומייצרת בקרים מתוכנתים (PLC) המשמשים לשליטה ובקרה של מכונות המבצעות פעולות אוטומטיות (כגון מערכות ייצור) – לרבות באותם מגזרים הנמצאים תחת איום. בסיום ההודעה נכתב כי "הסוכנויות דוחקות בכל הארגונים, במיוחד ארגוני תשתית קריטיים, ליישם את ההמלצות המפורטות כדי להפחית את הסיכון לתקיפה..."[161]

- **Colonial Pipeline** - ב-7 במאי 2021 התרחשה מתקפת סייבר נגד חברת הנפט האמריקאית קולוניאל פייפליין, המספקת נפט ומזוט בעיקר לדרום-מזרח ארצות הברית. יממה קודם לכן נגנבו נתונים בנפח 100 ג"ב משרתי החברה. המתקפה בוצעה באמצעות תוכנת כופר ששיתקה את ציוד המחשוב המנהל את צינור הנפט המרכזי של החברה. כתוצאה מכך, החברה עצרה את כל פעולותיה למשך מספר ימים. המתקפה גרמה למחסור בדלק מטוסים בכמה נמלי תעופה, וכן לשינוי זמני ומסלולי טיסות בחברת תעופה אחת לפחות. ב-9 במאי הכריז נשיא ארצות הברית ג'ו ביידן על מצב חירום, המאפשר הובלת דלק ללא מגבלות כדי להתגבר על המחסור. מאחורי המתקפה עמדה קבוצת ההאקרים Darkside[162]. לפי מנכ"ל החברה בעדותו בפני הסנאט האמריקאי, החדירה לארגון בוצעה באמצעות מערכת VPN **ללא דרישה להזדהות כפולה**. כך, **פעילות החברה שותקה באמצעות גניבתה של סיסמא אחת בודדה ע"י התוקפים**[163].

- **עיריית בולטימור** – במאי 2019, מתקפת כופר מסוג RobbinHood שבוצעה על ידי האקרים (טרם יוחסה רשמית למדינה) נגד **עיריית בולטימור**. המתקפה השביתה את רוב מערכות ה IT-העירוניות, כולל דוא"ל, תשלומי חשבונות ומכירות נדל"ן. הנזק הישיר והעקיף נאמד ב-18.2 מיליון דולר. השלכות הרוחב כללו קריאה ארצית בארה"ב להפסיק תשלום כופר מצד רשויות מקומיות. העירייה חזרה לפעילות הדרגתית לאחר **חודש**, ותהליך השיקום המלא נמשך חודשים ארוכים[164].

- **WannaCry** – במאי 2017 אירעה אחת מתקיפות הסייבר הגדולות בהיסטוריה, כשקבוצת האקרים בשם Shadow Brokers עשתה שימוש בכלי תקיפה שפיתחה סוכנות הביון האמריקאית (NSA) בארה"ב, שהתבסס על חולשת אבטחה במערכת ההפעלה Windows. על אף שמייקרוסופט פרסמה עדכון אבטחה לחולשה, ארגונים ואנשים פרטיים רבים לא התקינו אותו, וכך הותירו את מערכותיהם חשופות. ההאקרים שלחו אימייל הכולל את הנוזקה, ועם פתיחתו היא השתלטה על המחשב והצפינה את המידע שבו. **לפחות 16 בתי חולים ציבוריים בבריטניה נפגעו במתקפה, מה שהוביל לעצירת טיפולים ודחיית ניתוחים**. עוד נפגעו חברת חברות שליחויות, בנקים, מפעילות תקשורת, מערכות רכבות, מספר אוניברסיטאות ועוד [165].

---

[161] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a ; https://www.calcalist.co.il/calcalistech/article/bkthcu00bp

[162] https://crsreports.congress.gov/product/pdf/IN/IN11667 ; https://www.energy.gov/ceser/colonial-pipeline-cyber-incident/

[163] https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/

[164] https://en.wikipedia.org/wiki/2019_Baltimore_ransomware_attack

[165] https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf