דוח מבקר המדינה

# היערכות המדינה לאירועי סייבר ותפקודה במהלך מלחמת חרבות ברזל

▪ סיוון התשפ"ו ▪ יוני 2026

# היערכות המדינה לאירועי סייבר ותפקודה במהלך מלחמת חרבות ברזל

## מבוא

מלחמת חרבות ברזל הדגישה את ההכרח בהיערכותה ובמוכנותה של מדינת ישראל להתמודד עם אירוע חירום רב-זירתי. מאחר שממד הסייבר הוא אחד ממעגלי האיום שמולו נדרשת המדינה להיערך ולפעול, בדומה לזירות ולאיומים נוספים, הרי שרמת מוכנותה והיערכותה של המדינה בממד זה היא נדבך משמעותי בהיערכות הביטחונית הכוללת של ישראל ובחוסן הלאומי שלה.

בדוח זה מוצגים שלושה נושאים מרכזיים:

1. רמת ההגנה והחוסן של המשק (עד כמה המגזרים במשק הישראלי ערוכים למנוע ולזהות מתקפות סייבר משמעותיות ולהגיב להן) כפי שהוצגה על ידי מערך הסייבר הלאומי (להלן - מערך הסייבר) ושירות הביטחון הכללי (להלן - שב"כ), כל אחד בתחום אחריותו, ואופן שיקוף רמת ההגנה לדרג המדיני לפני המלחמה ובמהלכה.

2. הפעולות שנקטו הגופים האסדרתיים המדינתיים בתחום הסייבר קודם המלחמה ובמהלכה כדי להעלות את החוסן של גופים שונים במשק.

3. היערכות של 21 גופים בעלי חשיבות במשק (להלן - 21 הגופים שנבדקו בשאלון או 21 הגופים בעלי חשיבות במשק) בהם: גופים רגישים המונחים על ידי מערך הסייבר, משרדי ממשלה, גופים חיוניים, מוסדות להשכלה גבוהה, רשויות מקומיות וגופים מיוחדים שפועלים בהנחיה עצמית בתחום הסייבר, להתמודדות עם אירוע סייבר לפני מלחמת חרבות ברזל ובמהלכה.

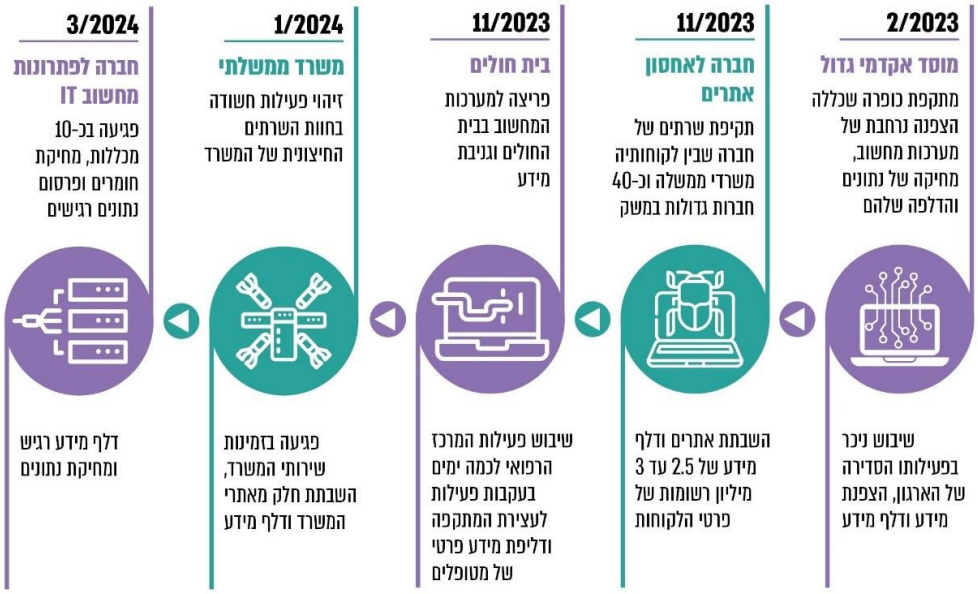
במהלך מלחמת חרבות ברזל חל גידול בהיקף ובעוצמה של מתקפות הסייבר נגד גופים במשק הישראלי שנועדו לפגוע בביטחון המדינה, בביטחון הציבור ובחוסן הלאומי, ולאסוף מידע לצרכי מודיעין. כך למשל מערך הסייבר הלאומי זיהה מספר קבוצות תקיפה הפועלות בממד הסייבר הישראלי המזוהות כמשויכות לאיראן, לחמאס ולחיזבאללה ומבצעות מגוון סוגי תקיפות נגד הנכסים בישראל.

למול התפתחות האיום לאחר פרוץ המלחמה נקטו הגופים האסדרתיים המדינתיים בתחום הסייבר בפעולות שונות להעלאת החוסן של גופים שונים ושל המשק כולו. כמו כן 21 הגופים שנבדקו פעלו להעלאת החוסן שלהם. עוד יצוין כי על פי התייחסויות שהתקבלו לדוח זה ממערך הסייבר ומשב"כ, מפרוץ המלחמה ועד מועד סיום עריכת הביקורת ביוני 2025, מדינת ישראל לא חוותה אירוע סייבר שפגע באופן משמעותי במשק. יחד עם זאת לדברי ראש מערך הסייבר דאז "לא לעולם חוסן" - השיפור הדרמטי בקצב וביכולות התקיפה מחייב נקיטת פעולות לחיזוק קו ההגנה ולהבטחת רציפות התפקוד ברמה המשקית והביטחונית.

נמצא כי ככל שהלחימה התמשכה, התעוזה והיצירתיות של התוקפים גברו: בתחילת המלחמה אירועי הסייבר התמקדו באירועי השפעה ומניעת גישה, בהמשך במתקפות לגרימת נזק (כגון מחיקת מידע) ובשנת 2024 זוהה מיקוד באיסוף מידע על יעדי איש, אזרחים ותהליכים בישראל[1]. לפי הערכת מערך הסייבר האיום ממתקפות הסייבר ימשיך ויתעצם. להלן דוגמאות לגופים שהתמודדו עם מתקפת סייבר משמעותית לפני המלחמה ובמהלכה:

[1] דוח סיכום שנת 2024 של מערך הסייבר, עמ' 3.

תרשים 1: **דוגמאות לגופים שהתמודדו עם מתקפת סייבר משמעותית, 2023 - 2024**




על פי דיווחים על אירועים במרשתת, בעיבוד משרד מבקר המדינה.

במאי 2024 פרסם מערך הסייבר דוח לפיו העלות הכלכלית המצטברת למשק הישראלי מנזקי מתקפות סייבר היא 12 מיליארד ש"ח בשנה[2]. כמו כן העלות המוערכת של נזקי פשיעת סייבר בעולם בשנת 2023 הייתה כ-8 טריליון דולר, גידול של כ-15% לעומת שנת 2022[3].

כל ארגון (או גוף או חברה) אחראי לטפל בסיכונים שהוא חשוף להם, לנהל אותם ולפעול להפחתתם. אירוע סייבר הוא סיכון מהותי לתפקודו התקין והרציף של ארגון ולעמידתו ביעדים שקבע לעצמו ובדרישות החוק לשמירה על מידע מסווג או פרטי. לכן כל ארגון נדרש לייצר מעטפת הגנה ויכולות התמודדות עם תרחישי האיום והסיכונים שהוא חשוף אליהם ואחראי לטפל באירוע סייבר המתרחש בחצרו בעיקר בשלבים האלו: ביצוע פעולות למניעת תקיפות סייבר, זיהוי וגילוי של אירועי סייבר מבעוד מועד (יכולות ניטור), חקירת האירועים, הכלה ומניעת התפשטות האירועים, הסרת האיום, תיקון ליקויים, השבת הארגון לתפקוד והפקת לקחים.

תפקיד הגופים האסדרתיים המדינתיים בתחום הסייבר - מערך הסייבר הלאומי, שירות הביטחון הכללי, הרשות להגנת הפרטיות, יחידת ההגנה בסייבר (להלן - יה"ב) במערך הדיגיטל הלאומי (להלן - מערך הדיגיטל) ויחידות מגזריות להכוונה מקצועית בתחום הסייבר (להלן - יחידות הסייבר המגזריות) (להלן - הגופים האסדרתיים המדינתיים) - הוא בעיקר לשפר את רמת ההגנה של הגופים המונחים על ידם בתחום הסייבר באופן שוטף, לחזק את החוסן שלהם ושל המשק בתחום זה ולאכוף בהתאם לסמכותם את עמידת הגופים בחוקים, בתקנות ובהנחיות הרלוונטיים. הם עושים זאת באמצעות הכוונה, הנחיה של הגופים ובקרה עליהם באופן שוטף וכן באמצעות חבירה עימם או סיוע להם בהתמודדות עם תקיפות סייבר שעשויות לסכן את המשק, או לפגוע במידע אישי.

עבודת ביקורת זו מתייחסת לכמה גורמים שיש להם תפקיד בהתמודדות עם תקיפות סייבר:

1. הגופים השונים (פרטיים וציבוריים) הפועלים במשק ונדרשים להעמיד הגנה עצמאית מול איומי הסייבר (להלן - הגופים במשק).
2. 21 גופים בעלי חשיבות במשק שנבדקו בשאלון.

---

2 דוח אומדן הנזק הכלכלי של מתקפות סייבר בישראל.

3 http://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide

3. הגופים האסדרתיים המדינתיים הפועלים בתחום הסייבר.
4. הדרג המדיני.

## פעולות הביקורת

בפברואר 2023 החל משרד מבקר המדינה לבדוק את נושא היערכות המדינה להתמודדות עם אירועי סייבר. לאחר פרוץ המלחמה ועד אוגוסט 2024 הרחיב המשרד את הבדיקה וכלל בה את בחינת תפקודה במהלך מלחמת חרבות ברזל. בדיקות השלמה נעשו בחלק מהנושאים בתקופה נובמבר 2024 עד יוני 2025.

הביקורת נעשתה בגופים הבאים, חלקם גופים אסדרתיים מדינתיים בתחום הסייבר: משרד ראש הממשלה (להלן - רה"ם) - במערך הסייבר; במטה לביטחון לאומי (להלן - המל"ל); בשב"כ; במשרד הביטחון - ברשות חירום לאומית (להלן - רח"ל); במשרד המשפטים - ברשות להגנת הפרטיות; במשרד הכלכלה והתעשייה - במערך הדיגיטל (ביה"ב); במשרד האוצר - במינהל הרכש הממשלתי, באגף השכר והסכמי עבודה ובאגף התקציבים; בנציבות שירות המדינה (להלן - נש"ם); ב-21 גופים בעלי חשיבות במשק שנבדקו בשאלון; בשבע יחידות סייבר מגזריות ובגופים נוספים.

במסגרת הביקורת הפיץ משרד מבקר המדינה שאלון בקרב 21 גופים ממגזרים שונים שהם בעלי חשיבות לרציפות התקינה של תפקוד המשק. בחירת הגופים נועדה לספק תמונה שתאפשר לבחון באופן רוחבי כיצד גופים ממגזרים ותחומים שונים במשק נערכו להתמודדות עם אירוע סייבר לפני מלחמת חרבות ברזל, ואת מידת המוכנות שלהם בהתאם לתקנות, להנחיות ולמתודולוגיות מקובלות בארץ ובעולם (כגון תקני NIST[4] ו-ISO27001) ובראשם תורת ההגנה 2.0 של מערך הסייבר. תמונת הרוחב אינה בגדר מדגם כמותי מייצג. כמו כן בניתוח המענה לשאלון לא הובאו בחשבון בקרות מפצות שאותן מיישמים הגופים כמענה לפער מסוים מטעמים מתודולוגיים שתכליתם להבטיח הערכה אחידה למול כל הגופים. בכך ניתן היה להבטיח בדיקה אחודה לכלל הגופים המאפשרת להשוות בין הגופים ביחס להיבטים שנבדקו.

כל הגופים ענו על השאלון, ובדיקתו כללה גם בדיקת מסמכים תומכים שהגופים התבקשו לצרף כתימוכין לתשובותיהם, ופגישות פרטניות שהתקיימו עם 11 מהגופים בהן נבדק המענה לעומק. בנוסף, כחודשיים לאחר פרוץ המלחמה נשלח לגופים אלו שאלון השלמה כדי לבחון אם חל שינוי במצבם בעקבות המלחמה, אם הותקפו, אם קיבלו הנחיות מיוחדות בתחום זה מהגופים האסדרתיים המדינתיים וכדי לקבל נתוני ניטור (SIEM) לצורך ניתוחם. כמו כן צוות הביקורת קיים מפגשי עומק עם יחידות הסייבר המגזריות (למעט אחת מהיחידות) על בסיס שאלון אחר שהן התבקשו למלא טרם המפגש וקיבל נתוני ניטור (SIEM) של גופי המגזר ככל שהיו כאלה.

בתשובת מערך הסייבר מינואר 2026 צוין כי קיים צורך משמעותי בשיפור רמת הגנת הסייבר הלאומית והוא מברך על כל מאמץ לשיפור הנושא אולם לעמדתו המקצועית קיים קושי באופן שבו בוצעה הבחינה, באופן הצגת הפערים ובאופן ניתוח השלכותיהם בדוח בהתייחס ל-21 הגופים שנבדקו בשאלון, תוך חשש להצגת תמונה כוללת שאינה מדויקת. זאת בין היתר, נוכח העובדה כי 21 הגופים האמורים לא מהווים מדגם מייצג; נוכח השונות המשמעותית הקיימת הן בפעילותם והן באסדרה המחייבת אותם; נוכח יצירת מדד עצמאי ותכלול הפערים שנמצאו ובחינת השפעתם על רמת ההגנה של הגופים, וזאת ללא ביצוע האבחנה הרגולטורית הנדרשת; ונוכח הצורך המקצועי לתת ולתכלל משקל מהותי לבקרות מפצות הננקטות ביחס לפערים משמעותיים, לצורך קבלת תמונת המצב המלאה הנדרשת.

---

[4] National Institute of Standards and Technology - NIST הוא מוסד ממשלתי אמריקאי במשרד הכלכלה של ארה"ב. מוסד זה מפרסם תקנים שארגונים מקצועיים ברחבי העולם מקבלים על עצמם כאמות מידה מקצועיות לתפקודם. מערך הסייבר הלאומי מקבל את תקינת NIST כתקינה מומלצת במסמכים מקצועיים שהוא מפרסם, והוא אף הסתמך על אחד מתקני NIST כבסיס מחייב בחוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה - חרבות ברזל), התשפ"ד-2023.

משרד מבקר המדינה אינו מקבל את טענת מערך הסייבר מאחר שתמונת המצב הרוחבית שהתקבלה מבוססת על גופים שונים ממגזרים שונים במשק, מבוססת על מתודולוגיות מקובלות ומציין כי מערך הסייבר עצמו השתמש בתקן NIST כמתודולוגיית בדיקה של רמת ההגנה של גופים במשק וכי גם בסקר שביצע מערך הסייבר בשנת 2023 בקרב מאות גופים חיוניים במשק לא ניתן ביטוי לבקרות מפצות כאמור מטעמים מתודולוגיים שתכליתם להבטיח הערכה אחידה למול כל הגופים. לא ניתן ביטוי לבקרות מפצות שכן הן מייצגות מעטפת הגנה חלופית ולא אחודה, להיעדר מענה מלא לעמידה בנורמות המקובלות שנבדקו. לדעת משרד מבקר המדינה ראוי להתייחס לתוצאות הבחינה הרוחבית שבוצעה כאל אבן בוחן להערכה כללית ומערכתית של ההיערכות של גופים שונים להתמודדות עם אירועי סייבר ולא כאל בחינה שתכליתה לעמוד על ציות של גופים לנורמות והוראות מחייבות, שכן ביסודה של בחינה זו מונחים כאמור גם תקנים מומלצים לחיזוק ההיערכות לאירועי סייבר. הרחבה בנושא השאלון, הגופים שנבדקו והתייחסות מערך הסייבר מובאת בפרק "ההיערכות והמוכנות של 21 גופים בעלי חשיבות במשק ושל גופים אסדרתיים מדינתיים להתמודדות עם אירועי סייבר לפני המלחמה ובמהלכה".

ועדת המשנה של הוועדה לענייני ביקורת המדינה של הכנסת החליטה שלא להניח דוח זה במלואו על שולחן הכנסת אלא לפרסם רק חלקים ממנו, לשם שמירה על ביטחון המדינה, בהתאם לסעיף 17 לחוק מבקר המדינה, התשי"ח-1958 [נוסח משולב].

## רקע על הגופים האסדרתיים המדינתיים ומתכונת האסדרה הקיימת

המחוקק התייחס לתחום אבטחת המידע והגנת הסייבר בחוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998[5] (להלן - החוק להסדרת הביטחון), בחוק הגנת הפרטיות, התשמ"א-1981 (להלן - חוק הגנת הפרטיות), ובתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן - תקנות אבטחת מידע)[6]. כמו כן הממשלה קיבלה כמה החלטות העוסקות בתחום זה (ב/84, 2443, 2444, 219, 3611)[7]. בהתאם להחלטות הממשלה ולחוק, הנחיית תחום אבטחת המידע והגנת הסייבר מוטלת על כמה גורמים. להלן רשימת הגופים האסדרתיים המדינתיים העיקריים בתחום הסייבר שאליהם מתייחס הדוח:

**מערך הסייבר:** גוף ממשלתי שאמון על הגנת ממד הסייבר הלאומי ופועל ברמת המדינה לחיזוק תמידי של רמת ההגנה של הגופים במשק והאזרחים, לטיפול בתקיפות סייבר וסילוקן ולהיערכות לשעת חירום[8]. בהתאם לחוק להסדרת הביטחון אחראי מערך הסייבר להנחיית מרבית גופי התמ"ק[9] ולבקרה עליהם, ובהתאם להחלטת הממשלה 2443 הוא אחראי להנחיה מקצועית של יחידות הסייבר המגזריות ושל יה"ב, ולפיכך נדרש לבצע בקרה על יישום הנחיותיו ליחידות. כמו כן, בהתאם להחלטת הממשלה 3611 הוא אחראי להמליץ לראש הממשלה על מדיניות קיברנטית (סייבר) לאומית, להנחות את הגורמים הרלוונטיים בעניין המדיניות שעליה הוחלט, ליישם את המדיניות ולבקר את יישומה. כמו כן, בתקופת המלחמה נחקק חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה), תשפ"ד-2023, שמאפשר למערך הסייבר לטפל בתקיפות סייבר חמורות במגזר השירותים הדיגיטליים (ראו בהרחבה פרק בנושא). זאת ועוד במסגרת תפקידו של המערך לסייע למשק הוא מפעיל בין היתר

---

5 החוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998.

6 תקנה 1, התוספת הראשונה והתוספת השנייה בתקנות אבטחת מידע.

7 החלטת הממשלה 3611, "קידום היכולת הלאומית במרחב הקיברנטי" (7.8.11), החלטת הממשלה 2443, "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" (15.2.15), החלטת הממשלה 2444, "קידום ההיערכות הלאומית להגנת הסייבר" (15.2.15), החלטת הממשלה 219, "בחינת רגולציה חכמה בסייבר וכללים והסמכות למתן הנחיות בזמן תקיפת סייבר שעודנה בעיצומה תוך שקילת שיקולים כלכליים" (1.8.21).

8 מתוך אתר המרשתת של מערך הסייבר - www.gov.il/he/pages/newabout.

9 גופי תמ"ק מוגדרים בחוק בהתאם לחוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998. המינוח בחוק הוא "מערכות ממוחשבות חיוניות", ואילו במתודולוגיה הייעודית המונח הוא "תשתיות מדינה קריטיות".

את האגף הארצי לניהול אירועי סייבר (להלן - CERT) המסייע לגופים השונים במשק כשיש חשש לאירוע סייבר שעשוי להסב להם או לארגונים אחרים נזק חמור, ומפרסם הנחיות שונות למשק שהן בגדר המלצה, לדוגמה: תורת ההגנה 2.0 (להלן - תורת ההגנה) - מדריך יישומי להגנת הסייבר בארגון. מערך הסייבר הוקם במשרד רה"ם, כפוף ישירות לראש הממשלה ובראשו עמד מר גבי פורטנוי שנכנס לתפקידו בפברואר 2022 וכיהן בתפקיד במהלך עריכת הביקורת. מר פורטנוי סיים את תפקידו במרץ 2025, ובמאי 2025 החליף אותו תא"ל (במיל') יוסי כראדי.

**הרשות להגנת הפרטיות:** הרשות להגנת הפרטיות היא מאסדרת של כלל המשק ומופקדת על הגנת הזכות לפרטיות ובכלל זה אבטחת המידע בכלל מאגרי המידע הכוללים מידע אישי בישראל. לשם כך הרשות מוסמכת לבצע אכיפה מינהלית ואכיפה פלילית על כלל המחזיקים במאגרי מידע (גופים פרטיים וגופים ציבוריים כאחד), בהתאם להוראות חוק הגנת הפרטיות ותקנותיו. לצורך הפקת תמונת מצב מגזרית בנוגע לעמידה בהוראות החוק והתקנות ולצורך איתור כשלים הטעונים אסדרה קיים בידי הרשות מנעד של כלים, ובהם פיקוח רוחב, הנעשה בעיקר במגזרים שיש בהם סיכון גבוה לפגיעה בפרטיות. הרשות להגנת הפרטיות היא יחידה במשרד המשפטים והיא עצמאית ובלתי תלויה בהפעלת סמכויותיה[10]. בראשה עומד עו"ד גלעד סממה שנכנס לתפקידו בנובמבר 2021 וכיהן בתפקיד במהלך עריכת הביקורת.

**שב"כ:** שב"כ מנחה גופים מכוח החוק להסדרת הביטחון, חלקם גופי תמ"ק. השב"כ נתון למרות הממשלה וראש הממשלה ממונה עליו מטעם הממשלה. בראש השב"כ עמד מר רונן בר שנכנס לתפקידו באוקטובר 2021 וכיהן בתפקיד במהלך עריכת הביקורת. מר בר סיים את תפקידו ביוני 2025.

**יה"ב (להלן - יה"ב או מערך הדיגיטל):** יחידת הכוונה והנחיה מקצועית בתחום הגנת הסייבר עבור משרדי הממשלה ויחידות הסמך[11]. היחידה הוקמה על פי החלטת הממשלה 2443 מפברואר 2015. היא כפופה ארגונית למערך הדיגיטל (בעבר רשות התקשוב הממשלתי) ופועלת בהנחיה מקצועית של מערך הסייבר. במסגרת פעילות מערך הדיגיטל הוא מפעיל את ה-SOC הממשלתי - מרכז שליטה ובקרה ממשלתי למול איומי סייבר. מערך הדיגיטל כפוף למשרד הכלכלה והתעשייה ובראשו עומדת גב' שירה לב עמי שנכנסה לתפקידה במאי 2022 וכיהנה בתפקיד במהלך עריכת הביקורת.

**יחידות הסייבר המגזריות:** כיום פועלות 8 יחידות סייבר מגזריות שפועלות במסגרת משרדי ממשלה לשיפור הגנת הסייבר במגזרי המשק השונים. היחידות הוקמו בהתאם להחלטת ממשלה 2443 מפברואר 2015 שהטילה על המנכ"לים של משרדי הממשלה לקדם את הטיפול בהיערכות לאיומי סייבר במסגרת המגזר שבו הם פועלים, על ידי הקמת יחידות להכוונה מגזרית והכנת עבודת מטה לבחינת התיקונים והשינויים המשפטיים הנדרשים על מנת שתהיה להן הסמכות הנדרשת להנחות בתחום הסייבר את הגופים במגזר. היחידות כפופות ארגונית למשרד הממשלתי שאליו הן שייכות ופועלות בהנחיה מקצועית של מערך הסייבר.

**רח"ל:** רח"ל הוקמה מכוח החלטת ועדת שרים לענייני ביטחון לאומי מס' ב/43 מדצמבר 2007 (להלן - החלטה ב/43), כגוף מטה שכפוף לשר הביטחון וייעודו לסייע במימוש אחריותו לטיפול בעורף בכל מצבי החירום, ובכללם טרור סייבר (שיבוש מערכות מידע הגורם לסיכון בנפש או נזק לתשתיות). זאת באמצעות תכנון, תיאום, הנחיה, הכוונה ובקרה של כלל המשרדים, הגופים הייעודיים, המערכות הלאומיות והרשויות המקומיות העוסקות במוכנות ובהכנה של המרחב האזרחי לחירום. כמו כן, מטרתה של רח"ל להביא למיצוי מרבי של המשאבים הלאומיים להבטחת הרציפות התפקודית במצבי משבר וחירום שונים. בראש רח"ל עמד תא"ל (מיל') יורם לרדו שנכנס לתפקידו באוקטובר 2020 וכיהן בתפקיד במהלך עריכת הביקורת. מר לרדו סיים את תפקידו באפריל 2025 ובאותו חודש נכנס לתפקידו אל"ם (מיל') איתן יצחק שהחליף אותו.

---

10 בהתאם להחלטת הממשלה 1890 (2.10.22), ובמסגרת תיקון 13 לחוק הגנת הפרטיות.

11 למעט "הגופים המיוחדים" שפורטו בהחלטה 3611 ועל פעולות גופים אלה באמצעות משרדי הממשלה במסגרת תפקידם ומשרד הביטחון.

**ה מ ל ״ ל :** המל״ל הוא גוף מטה לראש הממשלה ולממשלה בענייני חוץ וביטחון ופועל בהתאם לסמכויות המוקנות לו בחוק המטה לביטחון לאומי, התשס״ח-2008. היות שממד הסייבר הוא בעל השפעה ישירה על הביטחון הלאומי של מדינת ישראל, לרבות יחסי החוץ שלה, פועל המל״ל במסגרת סמכויותיו לקידום נושא הסייבר, זאת במסגרת סמכותו ובשיתוף פעולה עם משרדי הממשלה הרלוונטיים והסמכויות שנקנו להם מכוח הדין ומכוח החלטות הממשלה הרלוונטיות. למל״ל אין סמכויות אסדרתיות פורמליות בתחום הסייבר אך הוא מתכלל נושאים מסוימים שבהם מעורבים גופים אסדרתיים מדינתיים שונים בתחום הסייבר ומסייע להם בנושאים שיש להם הקשר לביטחון הלאומי. נושא הסייבר מרוכז במל״ל באמצעות עובד מושאל ממשרד הביטחון בדרגת ראש חטיבה. בראש המל״ל עמד היועץ לביטחון לאומי מר צחי הנגבי שנכנס לתפקידו בינואר 2023 וכיהן בתפקיד במהלך עריכת הביקורת.

**נוכח תפקידו של המל״ל לתכלל ולקדם נושאים בתחום הסייבר הנוגעים לביטחון הלאומי מומלץ כי ראש המל״ל יבחן אם קיים צורך לאייש באופן קבוע את המשרה העוסקת בתחום הסייבר וכן לעבות אותה בהתאם לסיכונים בתחום.**

## אסדרה בתחום הגנת הפרטיות

חוק הגנת הפרטיות מסדיר את הזכות החוקתית לפרטיות ואוסר את הפגיעה בה. כל הגופים במשק המחזיקים או מנהלים מאגרי מידע לפי הגדרתם בחוק הגנת הפרטיות, נדרשים לעמוד בהוראות חוק זה ובתקנותיו.

באוגוסט 2024 אישרה הכנסת את תיקון 13 לחוק הגנת הפרטיות והוא נכנס לתוקף שנה לאחר מכן באוגוסט 2025. התיקון מקנה לרשות להגנת הפרטיות סמכויות אכיפה מינהליות שלא היו בידה קודם. בין יתר הסמכויות הרשות מוסמכת להטיל עיצומים כספיים משמעותיים על הפרות של תקנות אבטחת מידע (עד כדי 320,000 ש״ח בגין כל הפרה, ופוטנציאל של מיליוני ש״ח לכל הליך אכיפה שיינקט על ידי הרשות).

תיקון החוק מוסיף נדבכים של אכיפה ובקרה שביניהם הרחבת אפשרויות מיצוי זכויות במישור המשפט האזרחי עקב הפרת חובות הקבועות בחוק הגנת הפרטיות; עדכון רשימת העבירות הפליליות; חובת מינוי ממונה הגנת פרטיות בכלל הגופים הציבוריים ובגופים בסקטור הפרטי בהתאם למאפייני מאגרי המידע שבשליטתם; מנגנון פיקוח מיוחד בגופים ביטחוניים על פי הגדרתם בחוק.

**משרד מבקר המדינה מציין לחיוב את פעילות הרשות להגנת הפרטיות לקידום תיקון 13 לחוק אשר מרחיב את סמכויות האכיפה של תקנות אבטחת מידע וקובע, בין היתר, סנקציות בגין הפרת תקנות אבטחת מידע לצורך שיפור רמת ההגנה על מאגרי מידע אישי במשק.**

## אסדרה בתחום הסייבר

חלק מהגופים במשק מונחים בתחום הסייבר באסדרה שאינה מחייבת אלא היא בגדר המלצה (מלבד החובה של כל המשק לקיים את חוק הגנת הפרטיות ותקנותיו), ראו תרשים ופירוט.

תרשים 2: **סמכות האסדרה בתחום הגנת הסייבר בגופים השונים**


הוכן בידי משרד מבקר המדינה.

להלן פירוט הגופים במשק וסוג האסדרה שחלה עליהם:

### 1. גופי תמ"ק

גופי ממשלה או גופים פרטיים שמנהלים מערכות ממוחשבות חיוניות שפגיעה בהן עלולה לגרום לנזק פיזי או כלכלי משמעותי מאוד, לפגיעה בחיי אדם או לפגיעה באספקת שירות ציבורי חיוני.

- **מספר הגופים:** כמה עשרות.
- **הגורם המנחה בתחום הסייבר:** מערך הסייבר או שב"כ, בהתאם לחלוקת האחריות הקבועה בחוק להסדרת הביטחון.
- **אופן הגדרת הגופים:** כמוגדר בחוק להסדרת הביטחון.
- **האסדרה וסמכות ההנחיה בתחום הסייבר:** הגופים מחויבים על פי החוק להסדרת הביטחון ליישם את הנחיות הגורם המוסמך (מערך הסייבר או שב"כ).
- **מתודולוגיית הסייבר:** מתודולוגיה ייעודית לגופי תמ"ק והנחיות משלימות של הגורם המוסמך.

### 2. משרדי ממשלה וגופי סמך

- **מספר הגופים:** כמה עשרות.
- **הגורם המנחה בתחום הסייבר:** יה"ב.
- **אופן הגדרת הגופים:** משרדי ממשלה ויחידות סמך.
- **האסדרה וסמכות ההנחיה בתחום הסייבר:** בהחלטת הממשלה 2443 נקבע שכל משרדי הממשלה ויחידות הסמך יהיו כפופים להנחיית יה"ב.

- **מתודולוגיית הסייבר:** משרדי הממשלה וגופי הסמך מחויבים לעמוד בהנחיות יה"ב ובתקן ISO 27001.

### 3. גופי מגזר שמונחים בידי יחידות הסייבר המגזריות

- **מספר הגופים:** אלפי גופים.
- **הגורם המנחה בתחום הסייבר:** יחידות הסייבר המגזריות.
- **אופן הגדרת הגופים:** יחידות הסייבר המגזריות מגדירות את הגופים המונחים לפי רמת חשיבות להגנה בסייבר - A, B, C - לדברי מערך הסייבר יש כמה מאות גופים בקטגוריה A (להלן - גופים חיוניים).
- **האסדרה וסמכות ההנחיה בתחום הסייבר:** לכל יחידה מגזרית יש סמכות שונה (מלאה, חלקית או לא קיימת) ולפיה היא מנחה את הגופים השונים במגזר.
- **מתודולוגיית הסייבר:** כל יחידה מגזרית מפרסמת הנחיות לגופים במגזר שלה.

### 4. גופים חיוניים ללא הכוונה בסייבר

- **מספר הגופים:** מאות גופים.
- **הגורם המנחה בתחום הסייבר:** אין.
- **אופן הגדרת הגופים:** מערך הסייבר.
- **האסדרה וסמכות ההנחיה בתחום הסייבר:** אין אסדרה מחייבת (למעט כאמור החובה של כל המשק לקיים את חוק הגנת הפרטיות ותקנותיו).
- **מתודולוגיית הסייבר:** אין מתודולוגיה מחייבת. גופים אלו פועלים לפי המלצת מערך הסייבר לפי תורת ההגנה בסייבר 2.0 ולפי הנחיות שונות של מערך הסייבר (בגדר המלצה).

### 5. יתר הגופים במשק

- **מספר הגופים:** מאות אלפי[12] עסקים בכל תחומי החיים, שלא הוגדרו על ידי יחידות הסייבר המגזריות ברמת חשיבות A,B,C להגנת הסייבר, ואין גורם אסדרתי מדינתי שיש לו סמכות להנחות אותם כיצד לפעול בנושא (למעט כאמור החובה של כל המשק לקיים את חוק הגנת הפרטיות ותקנותיו).
- **הגורם המנחה בתחום הסייבר:** אין.
- **האסדרה וסמכות ההנחיה בתחום הסייבר:** אין אסדרה מחייבת (למעט כאמור החובה של כל המשק לקיים את חוק הגנת הפרטיות ותקנותיו). הגופים פועלים לפי המלצות מערך הסייבר ואינם מחויבים ליישמן גם בעת אירוע סייבר משמעותי שמתרחש בהם, (למעט מגזר השירותים הדיגיטליים ושירותי האחסון שמחויב לפעול לפי חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי

[12] דמוגרפיה של עסקים של עצמאים בשנת 2022 ומאפייני בעלי העסקים:
www.cbs.gov.il/he/mediarelease/DocLib/2024/036/29_24_036b.pdf

האחסון (הוראת שעה - חרבות ברזל), התשפ"ד-2023, שנכנס לתוקף ב-6.12.23 ותוקפו במקור נקבע לשבעה חודשים[13]).

- **מתודולוגיית הסייבר:** אין מתודולוגיה מחייבת. הגופים פועלים לאור המלצת מערך הסייבר לפי תורת ההגנה בסייבר 2.0[14] ולפי המלצות שונות של מערך הסייבר (למעט הפעולות הנכללות בחוק האמור שהן בגדר חובה ובהתאם לקבוע באותו חוק).

## רמת ההגנה והחוסן של המשק לפני מלחמת חרבות ברזל ובמהלכה והפעולות שנקטו הגופים האסדרתיים המדינתיים כדי להעלות אותה

### החלטות ממשלה להעלאת רמת ההגנה והחוסן הלאומי בממד הסייבר

ועדת היגוי להגנה על מערכות ממוחשבות חיוניות (להלן - ועדת היגוי ב/84) פועלת בהתאם להחלטת ועדת השרים לענייני ביטחון לאומי, מס' ב/84 מדצמבר 2002 (להלן - החלטה ב/84), החלטת ממשלה 2444 מפברואר 2015, והחוק להסדרת הביטחון בגופים ציבוריים. תפקידה לעסוק במערכות ממוחשבות חיוניות בגופי תמ"ק ולאשר את ההוספה של גופי תמ"ק. בראש הוועדה עומד ראש מערך הסייבר וחברים בה ראש רח"ל, שני נציגי צה"ל, הקצין המוסמך לכך מטעם שב"כ, נציג היועץ המשפטי לממשלה, ראש הרשות להגנת הפרטיות, המשנה לראש המל"ל, נציג המשרד למודיעין ומשתתפים נוספים לפי החלטת ראש הוועדה. בהתאם להחלטה ב/84 על ראש הוועדה למסור אחת לחצי שנה לממשלה או לוועדת שרים שתיקבע לצורך כך דיווח על ביצוע החלטה ב/84 ועל מצב ההגנה על המערכות הממוחשבות במדינת ישראל (לרבות גופי תמ"ק).

החלטת הממשלה 3611[15] מאוגוסט 2011 הטילה על המטה הקיברנטי הלאומי (כיום מערך הסייבר) אשר הוקם על פי ההחלטה במשרד ראש הממשלה וכפוף ישירות לראש הממשלה, בין היתר, לקדם ולהעלות את המודעות הציבורית בנוגע לאיומים בממד הקיברנטי (להלן - סייבר) ולדרכי ההתמודדות עימם. בהחלטה נכתב כי ייעוד המטה הוא לשמש כגוף מטה לראש הממשלה, לממשלה ולוועדותיה אשר ממליץ על מדיניות לאומית ומקדם את יישומה בתחום הקיברנטי. בהחלטה מפורטים תפקידי המערך לרבות: להמליץ לראש הממשלה ולממשלה על מדיניות קיברנטית לאומית; לגבש תפיסה לאומית לטיפול במצב חרום במרחב הקיברנטי; ולקבוע ולתקף מידי שנה את איום הייחוס הלאומי.

החלטת הממשלה 2443[16] מפברואר 2015 אימצה, בין היתר, את עקרונות תפיסת האסדרה הלאומית להגנת הסייבר שמטרתה העלאה שיטתית ורציפה של רמת הגנת הסייבר במדינת ישראל באמצעות מימוש סטנדרטים מקצועיים בארגונים. כמו כן ההחלטה הטילה על משרד הכלכלה והתעשייה בתיאום עם מערך הסייבר ומשרד האוצר לגבש תוכנית סיוע ותמרוץ לשיפור המוכנות של גופים במשק לאירוע סייבר.

החלטת הממשלה 2444[17] מפברואר 2015 קבעה כי ההגנה על תפקודו התקין והבטוח של מרחב הסייבר היא יעד ביטחוני לאומי חיוני של מדינת ישראל ואינטרס ממלכתי חיוני לביטחונה הלאומי. על פי ההחלטה ראש הממשלה הוא האחראי על מערך הסייבר הכפוף לו ישירות ובסמכותו להטיל על מערך הסייבר לבצע כל תפקיד בהתאם לייעודו. יתרה מזאת ההחלטה מקימה ועדה מייעצת לראש הממשלה אשר חבריה ימונו ישירות על ידו ואשר תופקד על החלטות מדיניות עקרוניות בפעילותו. בהחלטה הוטל על מערך הסייבר (שהוקם באותה החלטה) לבנות ולחזק את

---

13 ב-23.7.24 נכנס לתוקף תיקון לחוק שבמסגרתו הוארך תוקפו עד 31.3.25, וב-31.3.25 נכנס לתוקף תיקון נוסף לחוק שבמסגרתו הוארך תוקפו עד 17.11.25.

14 תורת ההגנה בסייבר 2.0.

15 החלטת הממשלה 3611, "קידום היכולת הלאומית במרחב הקיברנטי" (7.8.11).

16 החלטת הממשלה 2443, "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" (15.2.15).

17 החלטת הממשלה 2444, "קידום ההיערכות הלאומית להגנת הסייבר" (15.2.15).

החוסן של כלל המשק בסייבר באמצעות היערכות, כשירות ואסדרה לרבות העלאת הכשירות של מגזרים וגופים במשק, הנחיית המשק, עריכת תרגילים ואימונים וכן מתן תמריצים וכלים נדרשים נוספים. כמו כן, בהחלטה הוטל על מערך הסייבר לנהל, להפעיל ולבצע בהתאם לצורך את כלל מאמצי ההגנה האופרטיביים ברמה הלאומית במרחב הסייבר, בהתאם לתפיסה מערכתית, לצורך מתן מענה הגנתי שלם ורציף על תקיפות סייבר, ובכלל זה לגבש תמונת מצב שוטפת.

בהחלטת הממשלה 219[18] מאוגוסט 2021 בנושא "בחינת רגולציה חכמה בסייבר וכללים והסמכות למתן הנחיות בזמן תקיפת סייבר שעודנה בעיצומה תוך שקילת שיקולים כלכליים" - הוחלט להקים צוות בין-משרדי בראשות מנכ"ל משרד רה"ם דאז (להלן - הצוות הבין-משרדי) שיבחן ויגיש בתוך 180 ימים המלצות בנוגע להתאמות הנדרשות להיערכות של ממד הסייבר האזרחי לאיומי סייבר. על הצוות הוטל לבחון, בין היתר, את הצורך ליצור אסדרה נפרדת לגופים שלא הוגדרו גופי תשתית מדינה קריטית ולקבוע את הכללים והסמכויות לגבי מתן הנחיות הנוגעות להיערכות למתקפת סייבר ולהתמודדות עם מתקפת סייבר שעודנה בעיצומה.

**החלטות הממשלה האמורות הניחו אפוא מערך תפקודי שמכפיף את הטיפול באיומי הסייבר ברמה הלאומית - ממשלתית לראש הממשלה; זאת על ידי קביעה שההגנה על תפקודו התקין והבטוח של מרחב הסייבר הוא יעד ביטחוני לאומי חיוני של המדינה, הקמת גוף לאומי ייעודי לנושא (מערך הסייבר) שכפוף ישירות לראש הממשלה ופועל במסגרת משרדו והענקת סמכויות ייעודיות לראש הממשלה בתחום זה.**

## מדידת רמת ההגנה בגופי תמ"ק ובגופים חיוניים

### מדידת רמת ההגנה בגופי תמ"ק

כאמור, גופי התמ"ק נדרשים לעמוד בדרישות של מתודולוגיה ייעודית לגופי תמ"ק שנכתבה בעבר. אחריות ההנחיה של מרבית גופי התמ"ק הועברה מהשב"כ למערך הסייבר בשנת 2017. מערך הסייבר ושב"כ מודדים אם גוף עומד במתודולוגיה לפי מאות בקרות ומדדים שנחלקים לחמש רמות הסמכה (להלן - מסמך הבקרות) (הרמה החמישית היא הגבוהה ביותר) והציון מבטא את רמת החוסן של הגוף.

**נמצאו פערים בתיקוף המתודולוגיה הייעודית שלפיה מחויבים גופי התמ"ק לפעול וזאת אף שבשנים אלו חלו שינויים טכנולוגיים נרחבים שהשפיעו על תחום הסייבר.**


**מומלץ כי מערך הסייבר ושב"כ ישלימו את הפערים שנמצאו בתחום המתודולוגיה הייעודית לגופי תמ"ק שלפיה מוסמכים הגופים ויפעלו להפיץ ולהטמיע אותה בקרב הגופים.**

### מדידת רמת ההגנה בגופים חיוניים

בהחלטת ממשלה 2444 מפברואר 2015 נקבע כי תפקיד מערך הסייבר הוא לנהל, להפעיל ולבצע בהתאם לצורך את כלל מאמצי ההגנה האופרטיביים ברמה הלאומית בממד הסייבר, בתפיסה מערכתית, לצורך מתן מענה הגנתי שלם ורציף מול תקיפות סייבר, ובכלל זה גיבוש תמונת מצב שוטפת.

מערך הסייבר מנחה ומכווין את יחידות הסייבר המגזריות, ואלו אחראיות להכווין את הגופים החיוניים במגזר שלהן. אגף הנחיה סקטוריאלית במערך הסייבר (לשעבר מרכז מגזרים), אחראי

[18] החלטת הממשלה 219, "בחינת רגולציה חכמה בסייבר וכללים והסמכות למתן הנחיות בזמן תקיפת סייבר שעודנה בעיצומה תוך שקילת שיקולים כלכליים" (1.8.21).

בין היתר על הנחיית והכוונת יחידות הסייבר המגזריות. שיטת ההנחיה של האגף מבוססת כאמור בעיקר על הצמדת מנחה מקצועי של המערך ליחידת הסייבר המגזרית וקבלת עדכונים ודיווחים שוטפים על מצב ההגנה שלהם ועל אירועי סייבר חריגים במגזר. בתפיסת ההפעלה של האגף במערך הסייבר נקבע כי אחת הפעולות שלו בעת שגרה הוא גיבוש תמונת מצב בארגונים השייכים למגזר.

בפגישות מאוגוסט 2023 עם מנהל אגף הנחיה סקטוריאלית במערך הסייבר עלה כי אין בידי מערך הסייבר תמונת מצב מלאה ועדכנית בנושא רמת ההגנה של המגזרים בתחום הסייבר הנשענת על מתודולוגיה סדורה למדידת רמת ההגנה של הגופים החיוניים בכל מגזר. עוד נאמר כי אפשר לייצר תמונת מצב מסוימת לפי צורך (למשל כפי שנעשה לקראת דיון בנושא עם שרת המודיעין דאז, גב' גילה גמליאל, ועם פורום השרים שהתכנס ביוני 2023 כפי שמפורט בהמשך), וכי נדרש שליחידות הסייבר המגזריות תהיה תמונת מצב בנושא הגנת הסייבר בגופים החיוניים שלהם.

במהלך הביקורת בספטמבר 2023 הציג אגף מודיעין והכוונה במערך הסייבר לצוות הביקורת מתודולוגיה, שהתגבשה מיוני 2023, למדידת מצב הגנת הסייבר במגזרים המורכבת ממדידת רכיבי ההגנה בגופים החיוניים ומבשלות הרגולציה בכל מגזר. כמו כן מערך הסייבר גיבש סקר בשלות הגנת הסייבר למדידת רמת ההגנה של הגופים (להלן - סקר), אולם הוא לא הופץ ולפיכך עם פרוץ מלחמת חרבות ברזל עדיין לא הייתה בידי מערך הסייבר תמונת מצב בנושא רמת ההגנה במגזרים שמבוססת על מדידה אחידה של הגופים.

לאחר פרוץ מלחמת חרבות ברזל (בנובמבר - דצמבר 2023) ביקש מערך הסייבר להאיץ את תהליך גיבוש תמונת המצב בנושא רמת ההגנה של המגזרים וגיבש סקר עדכני. במסמך הנלווה לסקר ציין מערך הסייבר כי הסקר מדגמי, אינו כולל את כל הפעילויות הנדרשות ליישום לטובת הגנת הסייבר בגוף, וניתוחו מבוסס על הערכה עצמית של הגופים, ללא בקרה של גורם בלתי תלוי.

הסקר הועבר על ידי מערך הסייבר לגופים במגזר מסוים ולכל יחידות הסייבר המגזריות והן התבקשו להעביר אותו לגופים המונחים שלהם. נכון לנובמבר 2024, הייתה בידי מערך הסייבר תמונת מצב בנוגע לחלק מהמגזרים (והוא הציג אותן בהערכות המצב שקיים בתקופת המלחמה). לדברי מערך הסייבר, תמונות המצב המגזריות אפשרו איתור של גופים המשמשים מרכזת (Hub) מול כמה ארגונים, ומולם בוצעה פעילות להעלאת החוסן. השלמת תמונת מצב של מערך הסייבר לכלל המגזרים תוכננה להסתיים עד סוף שנת 2024 אולם לא הושלמה. יצוין שלחלק מהיחידות המגזריות יש תמונת מצב שכל אחת מהן גיבשה בהתאם להנחיות שפרסמה לגופים המונחים שלה ולמדדים שהגדירה, אך זאת באופן שאינו מאפשר השוואה וניתוח של רמת ההגנה ושל הפערים בכלל המגזרים.


**אף שבהחלטת ממשלה 2444 מפברואר 2015 נקבע כי על מערך הסייבר לגבש תמונת מצב שוטפת ואף שבתפיסת ההפעלה של אגף במערך הסייבר נקבע כי אחת הפעולות שלו בעת שגרה היא גיבוש תמונת מצב בארגונים השייכים למגזר, נמצא כי עד פרוץ מלחמת חרבות ברזל מערך הסייבר לא ביצע מדידה סדורה ועקבית של רמת ההגנה במגזרים השונים ולא עקב לאורך שנים אחר מגמות ושינויים בה. רק במהלך המלחמה החל מערך הסייבר ליישם תהליך מדידה של רמת ההגנה במגזרים, באמצעות סקר ששלח לגופים. בנובמבר 2024 הייתה בידי המערך תמונת מצב של חלק מהמגזרים. ניתוח הסקר של יתר המגזרים תוכנן להסתיים עד סוף שנת 2024 אך לא הושלם. היעדר מדידה של הגופים החיוניים באופן שיטתי, אחוד ומובנה ולאורך שנים גורם לכך שאי-אפשר לנתח את המגמות, הפערים והאתגרים ולמקד את הטיפול בהם בטווח המיידי והארוך כמתחייב בהחלטות הממשלה 2443 ו-2444 משנת 2015 וכמוגדר בתפיסת ההפעלה של מערך הסייבר בנושא.**

בתשובת מערך הסייבר מינואר 2026 נמסר כי הוא רואה חשיבות בהערכת בשלות ההגנה ברמת ההגנה של מגזרי המשק ולצורך כך גיבש סקר עדכני אשר ייתן אינדיקציה לנושא מדידת הבשלות. השלמת תמונת המצב ברמת כלל מגזרי המשק הותנתה בהיענות הגופים למענה על הסקר. עוד ציין כי הוא פעל לאורך התקופה למיצוי שיעור ההיענות, באמצעות ליווי מקצועי, פניות יזומות ועבודה שוטפת מול הגופים והיחידות המגזריות. כתוצאה ממאמצים אלו התקבל שיעור היענות גבוה יחסית למקובל בסקרים מערכתיים דומים בעולם המאפשר זיהוי מגמות ביישום הגנות ומיקוד מאמצים בחלק ממגזרי המשק, גם אם לא הושגה תמונת מצב מלאה ביחס לכלל המגזרים.

בתשובת מגזר 2 מאוקטובר 2024 (להלן - תשובת מגזר 2) נמסר כי נכון לאוקטובר 2024 הוא העביר למערך הסייבר את הנתונים עבור גופי ה-A שבאחריותו, למעט חריג אחד, וטרם קיבל מהמערך את ממצאי הניתוח של תמונת המצב לגבי המגזר.

בתשובת מגזר 4 מנובמבר 2025 נמסר כי הסקר ששלח מערך הסייבר לצורך קבלת תמונת מצב לא זכה לשיתוף פעולה של הגופים המונחים, אולם היחידה המגזרית מחזיקה בנתונים עדכניים שניתן לשתף אותם עם מערך הסייבר במידת הצורך.

בתשובת מגזר 7 נמסר כי כחלק מתהליך המדידה והבקרה המתמשך שהוא מקיים מול גופי המגזר, הוחלט להפעיל סקר מגזרי חדש[19] לצורך מדידה עדכנית של גופי המגזר. כמו כן המשנה למנכ"ל המשרד פעל מול הגופים בדרישה לתיקון הליקויים. לדבריו פעילות זאת נושאת פרי וממצאים ראשונים של סקרים חוזרים מעידים על שיפור משמעותי. המשרד בוחן את התפיסה הקיימת לנוכח התקדמות הטכנולוגיה ובשנת 2026 תהיה התמקדות מיוחדת בנושא המדידה.

בתשובת מגזר 3 מנובמבר 2025 נמסר כי מאז המדידה של מערך הסייבר מנובמבר 2023 המגזר ביצע באופן עצמאי מדידה נוספת ומעמיקה יותר, המבוססת על מדד יה"ב, וציין כי לדעתו נדרש להגדיר מדד דומה עבור היחידות המגזריות.

בתשובת מגזר 6 מדצמבר 2025 נמסר כי באוקטובר 2024 מסרה יחידת הסייבר המגזרית למערך הסייבר תמונת מצב עדכנית בנוגע לרמת הבשלות של הגופים המונחים, וכי היא פועלת לפיה. עוד נמסר כי המשרד ומערך הסייבר מקיימים שיתוף פעולה מלא להשלמת מדידת רמות ההגנה בגופי המגזר.

**מומלץ כי מערך הסייבר ישלים את מדידת רמת ההגנה בכלל המגזרים, בשיתוף יחידות הסייבר המגזריות. מומלץ כי בשל ההתפתחויות הטכנולוגיות והשינויים השוטפים בגופים, המדידה תתוקף אחת לשנה, וכי בהתאם לתוצאותיה ולהתפתחות הסיכונים יפעלו מערך הסייבר ויחידות הסייבר המגזריות לטיפול בפערים שיועלו ולצמצומם. עוד מומלץ כי מערך הסייבר ויחידות הסייבר המגזריות יגבשו וישלבו תהליכי בקרה על תשובות הגופים על הסקר כדי להבטיח את אמינותו.**

## <u>רמת ההגנה בגופי תמ"ק לפני המלחמה ובמהלכה ושיקופה לדרג המדיני</u>

כאמור, גופי תמ"ק הם גופי ממשלה או גופים פרטיים שמנהלים מערכות ממוחשבות חיוניות שפגיעה בהן עלולה לגרום לנזק פיזי או כלכלי משמעותי מאוד, לפגיעה בחיי אדם או לפגיעה באספקת שירות ציבורי חיוני. גופים אלו הוגדרו בחוק להסדרת הביטחון. מערך הסייבר ושב"כ מנחים את גופי התמ"ק הכפופים להם לפעול לפי מתודולוגיה ייעודית לגופי תמ"ק ומודדים את עמידתו של הגוף במתודולוגיה לפי מאות בקרות ומדדים שמחולקים לחמש רמות הסמכה - חמש היא רמת ההסמכה הגבוהה ביותר.

[19] המשרד ביצע סקר מגזרי בשנת 2022.

יצוין שהעלאת רמת הסמכה של גוף תמ"ק היא תהליך מורכב שאורך זמן ודורש מהגוף להשקיע משאבים כספיים וארגוניים משמעותיים (לדוגמה בגיוס ובהכשרה של כוח אדם מקצועי, ברכש, בתחזוקת מערכות ושירותים להגנה מפני אירועי סייבר, לאיתורם ולטיפול בהם ובפעולות לחיזוק החוסן). כמו כן ביצוע שינויים משמעותיים במערכות ובתשתיות של גופים אלו צריך להיעשות במשנה זהירות כדי למנוע פגיעה ברציפות התפקודית שלהם.

מערך הסייבר מתקף את ציוני ההסמכה של הגופים אחת לשנתיים. במסמכי העוגנים השנתיים לשנת 2022 ולשנת 2023, שאותם שלח מערך הסייבר לגופי התמ"ק המונחים על ידו נקבע כי על כל גוף לקדם את רמת ההגנה ולהגיע לציון הסמכה גבוה יותר. בנוסף, גם בשנת 2024 הציב המערך יעד להעלות את ההסמכה של כל הגופים.

שב"כ מתקף בכל שנה את ציון ההסמכה של כל גוף תמ"ק שמונחה על ידו, קובע בכל שנה לכל אחד מהם את יעד ההסמכה שלו לאותה השנה ומודיע לו על כך.

כאמור תפקידה של ועדת היגוי ב/84 לעסוק במערכות ממוחשבות חיוניות בגופי תמ"ק ועל ראש מערך הסייבר (שמכהן כראש הוועדה) למסור אחת לחצי שנה לממשלה או לוועדת שרים שתיקבע לצורך כך דיווח על ביצוע החלטה ב/84 ועל מצב ההגנה על המערכות הממוחשבות במדינת ישראל (לרבות גופי תמ"ק). להלן מועדי ההתכנסות של הוועדה משנת 2020:

לוח 1: **מועדי התכנסות ועדת היגוי ב/84 משנת 2020 עד מאי 2025**

| השנה | מספר הפעמים שהוועדה התכנסה | מועדי ההתכנסות |
|---|---|---|
| **2020** | **1** | **דצמבר 2020** |
| **2021** | **0** | |
| **2022** | **2** | **ינואר 2022**<br>**דצמבר 2022** |
| **2023** | **1** | **יוני 2023** |
| **2024** | **1** | **דצמבר 2024** |
| **2025 (עד מאי)** | **0** | |

המקור: מערך הסייבר.

כנדרש בהחלטה ב/84 ראש מערך הסייבר דאז העביר לראש הממשלה, למזכיר הממשלה, לראש המל"ל, לראש השב"כ וליו"ר ועדת חוץ וביטחון בכנסת פירוט של פעילות הוועדה לשנת 2020 שכלל גם פירוט רמות ההסמכה של כל גופי התמ"ק לשנים 2017 - 2019 המייצגים את רמת ההגנה שלהם. עד יוני 2025 לא נשלחו סיכומי פעילות שנתיים נוספים. עם זאת, מערך הסייבר שלח העתק מסיכומי הדיון של ועדה ב/84 למשתתפים ולרשימת תפוצה הכוללת בין היתר את המזכיר הצבאי של שר הביטחון, לשכת ראש השב"כ, לשכת ראש המל"ל והמזכיר הצבאי של רה"ם. סיכומי הדיון כללו בין היתר התייחסות להסמכת גופים חדשים, והתייחסות לרמת ההגנה הכוללת של גופי התמ"ק (ממוצע הציונים).


**נמצא כי משנת 2020 ועד יוני 2025, מערך הסייבר לא העביר לראש ממשלה, למזכיר הממשלה, לראש המל"ל, לראש השב"כ וליו"ר ועדת חוץ וביטחון דיווחים חצי שנתיים של מצב ההגנה של המערכות הממוחשבות במדינת ישראל לרבות בגופי תמ"ק כנדרש בהחלטה ב/84. עוד נמצא כי ועדת ההיגוי ב/84, שתפקידה לעסוק במערכות ממוחשבות חיוניות בגופי תמ"ק ולאשר את ההוספה של גופי תמ"ק לא התכנסה בשנת 2021 וכן לא התכנסה במשך שנה וחודשיים אחרי פרוץ המלחמה (עד דצמבר 2024). להלן פירוט המועדים שהוועדה התכנסה: בדצמבר 2020; בינואר ובדצמבר 2022; ביוני 2023 ובדצמבר 2024.**

משרד מבקר המדינה קיבל את ציוני ההסמכה של מספר גופי תמ"ק שמונחים בידי מערך הסייבר ושל מספר גופים שמונחים בידי שב"כ, ציון ההסמכה משקף עד כמה הגופים מיישמים את הבקרות המגינות עליהם מפני תקיפה. הציון הוא בין 1 ל-5 ומבטא את רמת החוסן של הגוף.


**המגמה של התעצמות מתקפות הסייבר צפויה להתרחב בשנים הקרובות. גופי התמ"ק מנהלים מערכות ממוחשבות חיוניות שפגיעה בהן עלולה לגרום לנזק פיזי או כלכלי משמעותי מאוד, לפגיעה בחיי אדם או לפגיעה באספקת שירות ציבורי חיוני והם מוסמכים לפי 5 רמות הסמכה. מניתוח נתוני ההסמכה של גופי התמ"ק, שהעבירו מערך הסייבר ושב"כ, עולה כי לפני המלחמה (בשנת 2023), חלק מגופי התמ"ק היו ברמות הסמכה המשקפות יכולת התמודדות מוגבלת למול תוקפים. ביוני 2025 חל שיפור בציוני ההסמכה אולם עדיין היה קיים פער במועד זה.**

בתשובת מערך הסייבר נמסר כי ציון ההסמכה אינו משקף באופן מלא את רמת ההגנה בפועל של הגוף ואת הפעולות שמבצע המנחה מטעם המערך בגוף באופן שוטף לשיפור רמת ההגנה.

**על ראש מערך הסייבר לדווח אחת לחצי שנה לממשלה או לוועדת שרים שתיקבע לכך על פעילות ועדת היגוי ב/84 ועל מצב ההגנה על המערכות הממוחשבות במדינת ישראל (לרבות בגופי תמ"ק) כנדרש בהחלטה ב/84. מומלץ כי ראש הממשלה יזום ויקיים דיונים עתיים וסדורים בנושא רמת ההגנה של גופי תמ"ק לצורך קבלת החלטות בקבינט המדיני-ביטחוני או בוועדת שרים ייעודית שתופקד על הנושא. כמו כן, כחלק מתהליכי ההנחיה והבקרה שמערך הסייבר יקיים מול גופי התמ"ק עליו לגבש תוכנית פעולה שביסודה ייקבע עד איזה מועד יוסמכו כל גופי התמ"ק שבהנחייתו לרמה שנקבעה. עוד מומלץ שמערך הסייבר יגבש תוכנית ליווי לגופי תמ"ק חדשים כדי להבטיח צמצום פערים והעלאת רמת ההגנה שלהם באופן ממוקד ומהיר ויוודא כי ציון ההסמכה של גופי תמ"ק שבהנחייתו משקף את רמת ההגנה שלהם בפועל.**

## <u>רמת ההגנה והחוסן של גופים חיוניים ומגזרים במשק לפני מלחמת חרבות ברזל ובמהלכה, ושיקופה לדרג המדיני</u>

בהחלטת ועדת שרים ב/43 מדצמבר 2007 בה הוחלט על הקמת רח"ל נקבע כי טרור סייבר (שיבוש מערכות מידע הגורם לסיכון בנפש או נזק לתשתיות) עלול לגרום למצב חירום לאומי.

בהחלטת הממשלה 219[20] מאוגוסט 2021 בנושא "בחינת רגולציה חכמה בסייבר וכללים והסמכות למתן הנחיות בזמן תקיפת סייבר שעודנה בעיצומה תוך שקילת שיקולים כלכליים" - הוחלט להקים צוות בין-משרדי בראשות מנכ"ל משרד רה"ם (להלן - הצוות הבין-משרדי) שיבחן ויגיש בתוך 180 ימים המלצות בנוגע להתאמות הנדרשות להיערכות של ממד הסייבר האזרחי לאיומי סייבר.

מערך הסייבר הציג בשנה וחצי שלפני מלחמת חרבות ברזל את רמת ההגנה של המשק לפורומים ולגורמים שונים בדרג המדיני והמקצועי ובהם: לראשי ממשלה ולמנכ"לי משרדי ממשלה, לראש המל"ל, לשרת המודיעין דאז, לצוות הבין-משרדי ולפורום ממשלתי בראשות רה"ם שהתכנס באופן חד פעמי. רמת ההגנה של המשק שהציג מערך הסייבר התבססה בין היתר על רמת ההגנה של המגזרים השונים והיא מהווה נדבך משמעותי במוכנות המדינה להתמודד עם איום סייבר. רמת ההגנה של כל מגזר התבססה על רמת ההגנה של הגופים החיוניים השייכים לכל מגזר (למעט גופי תמ"ק שרמת ההגנה שלהם נסקרה לעיל). למשל: רמת ההגנה של מגזר הבריאות נגזרת מרמת ההגנה של בתי החולים וקופות החולים. להלן תמונת מצב שהוצגה בחלק מהפורומים:

**מאי-יולי 2022 - תמונת המצב שהוצגה בפני הצוות הבין-משרדי:**
בחודשים מאי - יולי 2022 הציג מערך הסייבר לחברי הצוות הבין - משרדי, סקירה על רמת ההגנה

[20] החלטת הממשלה 219, "בחינת רגולציה חכמה בסייבר וכללים והסמכות למתן הנחיות בזמן תקיפת סייבר שעודנה בעיצומה תוך שקילת שיקולים כלכליים" (1.8.21).

של המגזרים והמשק ועל איומי הסייבר. על פי הסקירה שהוצגה ישראל נמצאת בפיגור ניכר לעומת מדינות מפותחות בעולם בתחום האסדרה בסייבר וברמת ההגנה על גופים.

**פברואר-מרץ 2023 - תמונת המצב שהוצגה בפני שרת המודיעין דאז גילה גמליאל[21]:** בפברואר 2023 הציג מערך הסייבר לשרת המודיעין דאז מצגת ובה רמת ההגנה בסייבר לגבי כל אחד מהמגזרים המרכזיים במשק הישראלי לרבות התייחסות לרמת התפקוד של היחידה המגזרית שמנחה את המגזר. מהמצגת עולה תמונה ולפיה רמות ההגנה בחלק מסוים מהמגזרים (לא כולל את גופי התמ"ק) אינן מספקות.

בהמשך לסקירה שהוצגה לשרה כתב במרץ 2023 ראש מערך הסייבר דאז לשרה כי רמת ההגנה במשק הישראלי אינה מספקת בעיקר נוכח היעדר הפנמת הסיכון, וכי לנוכח התגברות האיומים, עוצמתם ומורכבותם, נדרשת חקיקה לאומית שתאפשר הגנת סייבר ראויה ושמירה על הרציפות התפקודית המשקית.

**יוני 2023 (כשלושה חודשים לפני פרוץ מלחמת חרבות ברזל) - תמונת המצב שהוצגה בפני ראש הממשלה, מר בנימין נתניהו, ופורום שרים:** באפריל 2023 העביר מערך הסייבר למזכיר הצבאי של ראש הממשלה נייר מדיניות המציג את הצורך והעקרונות בחקיקת חוק הסייבר ואת רכיביו העיקריים. כמה ימים לאחר מכן בפגישת עבודה עם מנכ"ל משרד ראש הממשלה דאז הציג לו ראש המערך מצגת ובה, בין היתר, התייחסות לרמת הגנת הסייבר במשק. במאי 2023 העביר מערך הסייבר למזכיר הצבאי דאז מצגת בנושא חוק הסייבר הכוללת פירוט נרחב יותר אודות רכיבי החוק המוצע.

בעקבות זאת, ביוני 2023 כינס רה"ם, באופן חד פעמי, פורום שרים מיוחד לדיון בנושא הסייבר והבינה המלאכותית. בפגישה[22] הציג ראש מערך הסייבר דאז, בין היתר את תמונת מצב ההגנה במגזרים; נדונו איומי הסייבר על גופים חיוניים שבאחריות המשרדים; הוצגה תמונת האיומים והסיכונים שהתגברו בשנים האחרונות בהיקף ובעוצמה (גידול של פי 2.5 בניסיונות למתקפות) והצורך במתן מענה לאיומים אלו באמצעות הסדרת התחום בחקיקה ראשית (להלן - הצעת חוק הסייבר). בפגישה לא הוצגה רמת התפקוד של כל יחידה מגזרית.

בפרקים הבאים בדוח ביקורת זה יוצג כי חלק מהנושאים שהוטלו על מערך הסייבר בהחלטות הממשלה 3611, 2444 ו-219 לא הושלמו; לדוגמה - הטיפול באסדרה, מימוש סטנדרטים מקצועיים מחייבים בארגונים, הגברת המודעות לאיומים, קיום תרגילים בתחום ההתמודדות עם אירועי סייבר, השתתפות דרג מדיני בתרגילים לאומיים ומגזריים, וחיזוק והעלאה של הכשירות של יחידות הסייבר המגזריות והגופים החיוניים.


**לפי מערך הסייבר רמת ההגנה של חלק מהמגזרים במשק לפני המלחמה הייתה לא מספקת: בהחלטת ועדת שרים ב/43 נקבע כי איום הסייבר (טרור סייבר) עלול לגרום למצב חירום לאומי. נמצא כי במהלך כשנה וחצי לפני פרוץ מלחמת חרבות ברזל, הציג מערך הסייבר במספר סקירות לרבות לצוות בין-משרדי, לשרת המודיעין דאז גב' גילה גמליאל ובאופן חד פעמי לפורום שרים בראשות רה"ם, מר בנימין נתניהו תמונת מצב ולפיה רמות ההגנה בתחום הסייבר בחלק מסוים מהמגזרים (לא כולל את גופי התמ"ק) אינן מספקות.**

**אוקטובר 2023 - פעולות שביצע מערך הסייבר להעלאת החוסן בתקופת מלחמת חרבות ברזל:** עם פרוץ מלחמת חרבות ברזל, התגברו והתעצמו באופן משמעותי ומיידי אתגרי הסייבר בישראל. לדברי מערך הסייבר הוא עבר לעבודה במתכונת חירום תומכת לחימה, שינה ומיקד את השקעת המשאבים ואת תיעדוף הפעילות בהתאם לאיומים, גייס אנשי מילואים לתגבור ופעל להאצתה ולשיפורה של ההגנה על ממד הסייבר של מדינת ישראל. עיקר המאמץ התמקד בתמיכה בצה"ל

---

21 כיהנה בתפקידה מינואר 2023 עד מרץ 2024.

22 www.gov.il/he/pages/spoke-cyber180623

בלחימה, בהגנה על גופי התמ"ק, בסיוע בהידוק הגנת הסייבר בגופי שרשרת האספקה הביטחונית, בסיוע בהגבהת חומות הגנת הסייבר בגופים חיוניים ושמירה על רציפות תפקוד המשק בחירום בהיבטי סייבר. פירוט בנושא מובא בהמשך.

**אוקטובר 2024 - תמונת המצב שהציג ראש מערך הסייבר דאז:** מאז פרוץ המלחמה חלה עליה דרמטית באיום הסייבר. בין היתר כמפורט:

1. גידול משמעותי במספר התוקפים וקבוצות התקיפה.
2. מצב רמת הגנת הסייבר במשק הישראלי: לפי ניתוח של מערך הסייבר מצב בשלות הגנת הסייבר במשק אינו מספק.
3. שיפור משמעותי ביכולות האויבים, בין היתר: נוכח השינויים הטכנולוגים ומהפכת ה-AI, קבוצות התקיפה משפרות את סל היכולות בקצב גבוה מהרגיל.
4. העלות השנתית לכלכלה הישראלית בגין תקיפות סייבר בשנה רגילה (ללא מלחמה) מוערכת בסכום של כ-12 מיליארד ש"ח בשנה, סגירת הפערים שתוארו צפויים להוריד דרמטית את העלות עד לכדי 50%.
5. השינויים האסטרטגיים ו"מחיר הטעות" למשק הישראלי, בפרט בתקופת מלחמה מחייבים מענה מבצעי מיידי כחלק מצרכי הביטחון של המלחמה לצורך הבטחת מרחב דיגיטלי אמין ובטוח ולצורך שימור חופש הפעולה בלחימה ותפקוד המשק.
6. "לא לעולם חוסן" - השיפור הדרמטי בקצב ויכולות התקיפה מחייב נקיטת פעולות לחיזוק קו ההגנה ולהבטחת רציפות התפקוד ברמה המשקית והביטחונית.
7. אנו מחויבים לפעול על מנת להבטיח שמדינת ישראל תשמר כמעצמת סייבר עולמית ותתמודד אל מול האיומים המתגברים.


**לפי מערך הסייבר רמת ההגנה של המשק באוקטובר 2024, שנה לאחר פרוץ המלחמה, הייתה לא מספקת ועלולה לא לעמוד בפני אתגרי העתיד: אומנם מאז פרוץ מלחמת חרבות ברזל ועד יוני 2025 מדינת ישראל לא חוותה אירוע סייבר שפגע באופן משמעותי בתהליכים עסקיים קריטיים שהשפיעו באופן מהותי על המשק. יחד עם זאת, באוקטובר 2024 דיווח ראש מערך הסייבר דאז כי מצב בשלות הגנת הסייבר במשק אינו מספק וכי השיפור הדרמטי בקצב וביכולות התקיפה מחייב נקיטת פעולות לחיזוק קו ההגנה ולהבטחת רציפות התפקוד ברמה המשקית והביטחונית. נוכח זאת ציין ראש המערך דאז כי יש חובה לפעול כדי להבטיח שמדינת ישראל תשמר כמעצמת סייבר עולמית ותתמודד עם האיומים המתגברים.**

**על מערך הסייבר, כמי שהוטל עליו בהחלטות ממשלה 2444 ו-2443 לבנות ולחזק את החוסן של כלל המשק בסייבר באמצעות היערכות, כשירות והסדרה ובכלל זאת העלאת הכשירות של מגזרים וגופים במשק וכמנחה המקצועי של יחידות הסייבר המגזריות - לגבש בשיתוף משרדי הממשלה ויחידות הסייבר המגזריות תוכנית פעולה לאומית-ממשלתית שתבטיח צמצום פערים ברמת ההגנה הן בטווח הקצר והן בטווח הארוך. תוכנית זו צריכה לעסוק במגוון נושאים שהוגדרו והוטלו על מערך הסייבר, על משרדי הממשלה ועל יחידות הסייבר המגזריות עוד בהחלטות הממשלה 3611, 2444 ו-219 ולא הושלמו, ובהם לדוגמה מימוש סטנדרטים מקצועיים מחייבים בארגונים, הגברת המודעות לאיומים, ביצוע תרגילים ואימונים בתחום ההתמודדות עם אירועי סייבר וכן חיזוק והעלאה של כשירות יחידות הסייבר המגזריות והגופים החיוניים וטיפול באסדרה ובמתן סמכויות הנחיה ואכיפה בתחומים שאלה אינם קיימים. על מערך הסייבר להביא**

**את התוכנית לאישור הממשלה. על הממשלה לבחון ולאשר את התוכנית לרבות אישור לוחות הזמנים והתקציב הנדרש ולעקוב אחר מימושה לפחות אחת לשנה.**

**נוסף על כך, מומלץ כי כל אחד מהשרים יקיים לפחות אחת לחצי שנה הערכת מצב מגזרית בתחום הסייבר אשר תשקף את רמת ההגנה, הפערים והסיכונים בפעילויות ובסמכויות בתחומי העיסוק של משרדו למול איום הייחוס העדכני, ויגדיר את תוכנית העבודה לטיפול.**

בתשובת מגזר 3 מנובמבר 2025 נמסר כי הוא מצטרף להמלצות המבקר בנוגע לצורך בגיבוש תוכנית פעולה לאומית ממשלתית שתבטיח צמצום פערים ברמת ההגנה בשל תוצאותיה האפשריות של התקפת סייבר ברמה הלאומית. עוד מסר כי הוא יכנס ועדות היגוי משרדיות ומגזריות אחת לשנה בראשות המשנה למנכ"ל וכן יבחן בחיוב את המלצת המבקר לגבי קיום הערכות מצב בראשות השר.

בתשובת השר האחראי למגזר 11 מדצמבר 2024 (להלן - תשובת מגזר 11) נמסר כי הוא פועל ליישום ההמלצה לקיים אחת לחצי שנה דיון בנושא הסייבר.

בתשובת מגזר 2 מאוקטובר 2024 נמסר כי המנכ"ל מכנס את ועדת ההיגוי המשרדית לפחות אחת לחצי שנה ובמסגרת דיוניה מוצגת גם תמונת הסייבר במגזר. כמו כן, בנובמבר 2025 מסר המשרד כי השר מקיים הערכות מצב עיתיות בעניין מוכנות המשרד בנושאים שונים לרבות בתחום הסייבר.

בתשובת מגזר 5 נמסר כי ההמלצה לקיים הערכות מצב תמומש, וכי תחום הסייבר מוצג לשר הן במסגרת אישורי תוכניות העבודה השנתיות והן בדיוני הבקרה הרבעוניים והחצי-שנתיים. כמו כן השר מעודכן בכל חשש ובכל אירוע משמעותי בזמן אמת. עם זאת ואף שלמשרד יש סמכות לתת הוראות בתחום הסייבר, הרי שבהיעדר תקציב מתאים, ליחידת הסייבר המגזרית אין את כל הכלים הנדרשים ליישום המלצת המבקר בנושא תוכנית העבודה.

בתשובת מגזר 6 מאוקטובר 2024 (להלן - תשובת מגזר 6) נמסר כי בחצי השנה האחרונה החלה היחידה המגזרית לקיים הערכות מצב מגזריות חודשיות ומשנת 2025 ישולב בהן מערך הסייבר. כמו כן תוכנן כי החל בשנת 2025 יתקיימו הערכות מצב חצי-שנתיות בראשות שר או מנכ"ל. בדצמבר 2025 עדכן המשרד כי במסגרת אישור תרחיש ייחוס סייבר למגזר בוצעה הערכת מצב בעניין מוכנות המשק, וכי ברבעון הראשון של שנת 2026 מתוכננת הערכת מצב ייעודית בראשות השר.

## <u>מעורבות הקבינט המדיני-ביטחוני בתחום הסייבר</u>

סעיף 6 לחוק הממשלה, התשס"א-2001, קובע כי בממשלה תפעל ועדת שרים לענייני ביטחון (להלן - הקבינט או הקבינט המדיני-בטחוני). חלק מסמכויות הקבינט נקבעו בחוק וחלקן בהחלטות ממשלה. החוק קובע את ההרכב היסודי של הקבינט ומאפשר לממשלה להוסיף חברים לפי הצעת רה"ם לעניין זה. הסמכות לקביעת סדר היום לישיבות הקבינט נתונה בידיו של ראש הממשלה כיו"ר הקבינט. בהחלטת ועדת השרים לענייני ביטחון לאומי, מס' ב/212 ממאי 2017 (להלן - החלטה ב/212), אישר הקבינט את המלצות[23] ועדת עמידרור להכשיר את חברי הקבינט החדשים, להכין אותם לדיונים ולעדכן אותם באופן שוטף וקבע מנגנונים לכך באמצעות הגדרת תפקידים ייעודיים במל"ל.

כאמור, החלטת הממשלה 2444 מפברואר 2015 קבעה כי ההגנה על תפקודו התקין והבטוח של מרחב הסייבר היא יעד ביטחוני לאומי חיוני של מדינת ישראל ואינטרס ממלכתי חיוני לביטחונה הלאומי.

---

[23] המלצות הוועדה לעניין עבודת הקבינט המדיני-ביטחוני.

משרד מבקר המדינה בחן[24] האם בעשור לפני פרוץ מלחמת חרבות ברזל ובמהלכה, התקיימו בקבינט המדיני בטחוני דיונים ייעודיים בנושא סייבר והאם הוצגה לקבינט (גם במסגרת דיונים שאינם ייעודיים לסייבר) תמונות מצב בתחום הסייבר אשר משקפות את רמת ההגנה והפערים והסיכונים למול איום הייחוס העדכני. להלן פרטים שרוכזו ממידע שהתקבל מהמל"ל באשר לעיסוק הקבינט בתחום הסייבר בתקופה זו[25]:

1. **דיונים ייעודיים בנושא סייבר:** ביוני 2018 התקיים דיון ייעודי יחיד בנושא סייבר. מאז לא התקיימו דיונים ייעודיים נוספים.

2. **העמקת ידע לחברי הקבינט בנושא סייבר:** בספטמבר 2021 התקיים מפגש העמקת ידע לשרי הקבינט בנושא מסוים במסגרתו הציג ראש מערך הסייבר דאז היבטים רלוונטיים בתחום הסייבר. לא התקיימו מפגשי העמקת ידע נוספים.

3. **הערכות מודיעין שנתיות:** הערכות מודיעין שנתיות (בשנים 2017, 2018 ו-2022) כללו התייחסות גם לנושא הסייבר.

4. **תמונת מצב רב-זירתית:** בשני דיונים שבהם ניתנה תמונת מצב רב-זירתית כוללת (דיונים שהתקיימו בשנים 2021 ו-2022) היה אזכור מסוים גם בנושא הסייבר.

5. **דיונים בנושא מסוים במהלך המלחמה:** בדיון אחד שהתקיים בנובמבר 2024 הייתה התייחסות גם לנושא הסייבר.


**אי-הצגת תמונת מצב בתחום הסייבר באופן שוטף לקבינט מדיני-ביטחוני: בעשור לפני המלחמה ועד יוני 2025, ראשי הממשלה לא יזמו ולא קיימו בקבינט דיונים ייעודיים בנושא הסייבר למעט פגישה ייעודית אחת שהתקיימה בשנת 2018. ועם זאת, נושא הסייבר הוזכר במסגרת דיונים שהנושאים שלהם היו רחבים יותר: הערכות מודיעין שנתיות, בחלק מהדיונים בנושא תמונת מצב רב-זירתית ובדיון אחד שהתקיים אחרי פרוץ המלחמה בנושא מסוים. זאת אף שהקבינט המדיני-ביטחוני מוסמך לעסוק בביטחון הלאומי ואף שההגנה על מרחב הסייבר הוא יעד ביטחוני לאומי כפי שנקבע בהחלטת הממשלה 2444. כתוצאה מכך, בתקופת הביקורת הקבינט לא נחשף למכלול הסיכונים בתחום הסייבר, לרמת ההיערכות ולנזקים הפוטנציאליים.**

בתשובת מערך הסייבר נמסר כי הקשר עם הדרג המדיני מבוצע באופן שוטף, בישיבות, בכתובים ובשיחות. התקיימו ישיבות שונות עם ראש הממשלה, שרת המודיעין דאז, מנכ"ל משרד רה"ם, המזכיר הצבאי וראש המל"ל, התקיים קשר רציף ושוטף בין לשכת ראש מערך הסייבר למזכיר הצבאי של ראש הממשלה לרבות העברת דיווח שבועי בכתב, העברת דיווחים עיתיים בעל פה ובכתב, עדכונים על אירועי אמת משמעותיים בזמן אמת.

**מאחר שאיום הסייבר מהווה איום משמעותי הולך ומתעצם שמולו נדרשת המדינה להיערך ולפעול, על ראש הממשלה ליזום דיונים סדורים בפורום מדיני קבוע וייעודי לנושא זה כמו קבינט מדיני-ביטחוני או ועדת שרים ייעודית שתופקד על הנושא, שעל שולחנו יונחו באופן עיתי וסדור (ולפחות אחת לחצי שנה) הערכות מצב בתחום הסייבר אשר ישקפו את רמת ההגנה, הפערים והסיכונים למול איום הייחוס העדכני והוא ידון בתפיסת הביטחון הכוללת בתחום הסייבר לצורך קבלת החלטות. עוד מומלץ כי פורום זה יקבל הכשרה רלוונטית לנושא.**

☆

[24] המידע התקבל ממל"ל וכן מרשימת הנושאים בהם דן הקבינט משנת 2017 ועד פרוץ מלחמת חרבות ברזל.

[25] יובהר לעניין זה כי לא נכללו בפירוט המובא התייחסויות אגביות שבהן הוזכרו ענייני סייבר אגב דיוניים שעסקו בנושאים אחרים.

**מהפרק עולה כי הנתונים שהציגו מערך הסייבר ושב"כ לפני המלחמה ובמהלכה שיקפו רמת הגנה שאינה מספקת של חלק מהמגזרים והגופים. כמו כן מהפרק עולה כי ראשי הממשלה לא יזמו ולא קיימו בקבינט דיונים ייעודיים בנושא סייבר למעט פגישה אחת שהתקיימה בשנת 2018. עם זאת, נושא הסייבר הוזכר במסגרת דיונים שהנושאים שלהם היו רחבים יותר: הערכות מודיעין שנתיות, בחלק מהדיונים בנושא תמונת מצב רב-זירתית ובדיון אחד שהתקיים אחרי פרוץ המלחמה בנושא מסוים. כתוצאה מכך הקבינט לא נחשף למכלול הסיכונים בתחום הסייבר, לרמת ההיערכות ולנזקים הפוטנציאליים.**

בתשובת גוף מסוים נמסר כי אין לו הערות למוצע.

# פערים בפעולות הגופים האסדרתיים המדינתיים בתחום הסייבר קודם המלחמה ובמהלכה

## <u>אסדרה בתחום הסייבר של מגזרים, גופים חיוניים, תשתיות תקשורת ותקשוב לאומיות וגופים נוספים</u>

### אסדרת המגזרים

כאמור בתחום האסדרה הלאומית בסייבר, החלטה 2443 הטילה על המנכ"לים של משרדי הממשלה שמפעילים סמכויות אסדרה כלפי גופים או פעילויות החשופים לאיומי סייבר לקדם את הטיפול בהיערכות לאיומי סייבר במסגרת המגזר[26] שבו הם פועלים, ובין היתר, להקים יחידות סייבר מגזריות שפועלות בהנחיה מקצועית של מערך הסייבר הלאומי, לקדם הגדרה של המדיניות ודרישות האסדרה שנדרשות לעבודתן ולבצע, בתיאום עם מערך הסייבר, עבודת מטה שתוגש לראש הממשלה, הבוחנת את התיקונים והשינויים הנדרשים מהבחינה המשפטית למימוש אפקטיבי של האמור.

לוח 2: **הנושאים שבטיפול או באחריות היחידות המגזריות לפי החלטת הממשלה 2443**

| | |
|---|---|
| **תפקיד יחידות הסייבר המגזריות** | • הכוונה והנחיה של הגופים במגזר בהיבטים של הגנת הסייבר, הגדרת המדיניות ודרישות האסדרה, ליווי מקצועי שוטף ומענה לפניות מקצועיות[27].<br>• בקרה על ביצוע הדרישות המקצועיות בהתאם לאסדרה ולרמה המקצועית הנדרשת.<br>• פיתוח והפעלה של תהליכי שיתוף מידע פנימיים וחיצוניים במגזר.<br>• ייזום ומימוש של פעולות רוחביות, לרבות הקמת תשתיות והפעלת מנגנונים לשיפור הגנת הסייבר במגזר (למשל הקמת SOC[28] מגזרי). |
| **סיווג היקף הפעילות** | החלטת הממשלה הטילה על מערך הסייבר לסווג את היקף הפעילות הנדרשת לכל יחידת סייבר מגזרית בהתאם לנזק הפוטנציאלי כתוצאה מפגיעה במערכות הממוחשבות של הגופים במגזר שעליו היא מופקדת על פי היקף הפעילות הנדרשת:<br>היקף גדול - חמישה עובדים;<br>היקף בינוני - שלושה עובדים;<br>היקף קטן - עובד אחד.<br>הממשלה הסמיכה את מערך הסייבר, את נש"ם ואת משרד האוצר בסיכום ביניהם לשנות את המפתחות האמורים. |

[26] כלל הגופים הפועלים במסגרת תחום מקצועי של משרד ממשלתי ובמסגרת אחריותו האסדרתית.

[27] בנושאים שחל עליהם החוק להסדרת הביטחון ובנושאים שחל עליהם חוק הגנת הפרטיות תתבצע ההנחיה בתיאום עם הגורם המוסמך לפי אותם חוקים.

[28] Security Operation Center - מרכז שליטה ובקרה לניטור, זיהוי ותגובה של אירועי סייבר.

| | |
|---|---|
| **התקצוב** | • בשנים 2015 - 2016 יתבסס התקציב לאיוש תפקידים על מקורות מערך הסייבר[29]<br>• בשנים 2017 - 2019 מחצית מהתקציב תתוקצב על ידי מערך הסייבר[30] ומחציתו ממקורות המשרד הממשלתי הרלוונטי. |
| **הפיקוח על יישום ההחלטה** | החלטת הממשלה הטילה על מערך הסייבר לבחון את מנגנון האיוש והתקצוב של התפקידים ביחידות אלו בתום חמש שנים מההחלטה (בשנת 2020) ולבצע בקרה על יישום ההחלטה[31] בנושא יחידות הסייבר המגזריות. |

על פי החלטת הממשלה 2443, בעיבוד משרד מבקר המדינה.

בהתאם להחלטת הממשלה 2443, בחודשים פברואר - יוני 2015 מיפה מערך הסייבר את פעילות משרדי הממשלה, גיבש רשימה של משרדים שנדרש להגדירם מגזרים לעניין סייבר וסיווג את היקף פעילותם. בספטמבר 2015 שלח ראש מערך הסייבר דאז מכתב בנושא למנכ"לי המשרדים שמופו, ובמהלך השנים 2015 - 2019 השתתף מערך הסייבר בתקצוב היחידות.

מילוי התפקידים של יחידות הסייבר המגזריות לאורך זמן מחייב את הקנייתן של סמכויות אסדרה ליחידות המגזריות ואת הקצאתם של כוח אדם ייעודי ותקציב פעולות:

1. אשר לסמכויות אסדרה - בהחלטת ממשלה 2443 נקבע כי מוטל על המנכ"לים של משרדי הממשלה לבצע, בתיאום עם מערך הסייבר, עבודת מטה שתוגש לראש הממשלה, הבוחנת את התיקונים והשינויים הנדרשים מהבחינה המשפטית למימושה.

2. אשר לתקציב היחידות - עלה כי בשנת 2020 הסתיים הסדר התקצוב שהוגדר בהחלטת הממשלה והיה על מערך הסייבר לבחון את מנגנון האיוש והתקצוב של התפקידים ביחידות. לדברי מערך הסייבר בכל שיח תקציבי אמר אגף תקציבים במשרד האוצר שהמערך אינו יכול לתקצב משרדי ממשלה.

3. אשר לתקני כוח אדם - בשנים 2021 - 2022 ראש חטיבת מערך ההגנה במערך הסייבר דאז השתתף בוועדה בנש"ם בראשות הממונה על מערכת הביטחון והחוץ בנש"ם שהסדירה במסגרת סמכותה את עבודת אגפי ביטחון, חירום וסייבר במשרדי הממשלה. במסגרת עבודת הוועדה הוסדר התקן של שני תפקידים הרלוונטיים לתחום הסייבר (ממונה ביטחון טכנולוגיות וסייבר ותפקיד ראש צוות ה-SOC) ביחידות הסייבר המגזריות הכפופות לאגף ביטחון, חירום וסייבר במשרדי הממשלה וביחידות הסמך שמוגדרות בחוק להסדרת הביטחון אולם הוועדה לא טיפלה בהסדרת התקנים ביחידות הסייבר המגזריות שאינן בסמכותה כיון שהן אינן כפופות לאגף ביטחון חירום וסייבר, לא הגדירה את המבנה הארגוני ואת התקנים הנדרשים בהן ולא סיווגה את היקף הפעילות בכל אחת מהן. נוסף על עבודת הוועדה ראש חטיבת ההגנה דאז וראש אגף הכוונה סקטוריאלית במערך הסייבר נפגשו עם חלק מהמנכ"לים ביחידות המגזריות ובהן הודגש שמחובת המשרד להקצות משאבים לטובת גיוס עובדי מיקור חוץ ביחידות המגזריות ועלה הצורך לחזק את כוח האדם ביחידות המגזריות.

מערך הסייבר מסר למשרד מבקר המדינה את תמונת מצב האיוש ביחידות הסייבר המגזריות הכוללת גם המלצה מעודכנת שלו למספר התקנים ביחידות הסייבר המגזריות נכון לשנת 2024 (לא כולל המלצה לצוותי ה-SOC). המלצה זו לא נמסרה ליחידות הסייבר המגזריות.

29 בסכום שלא יעלה על 500,000 ש"ח בשנה לתפקיד (אדם או יועץ).

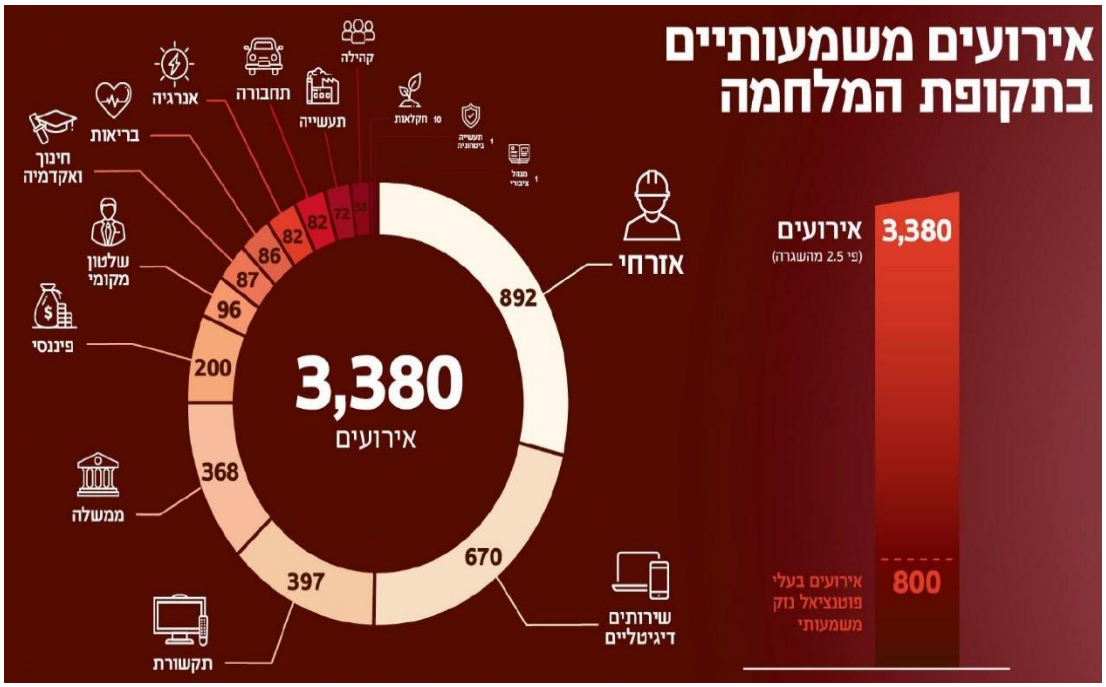
30 עד לתקרה של 500,000 ש"ח בשנה ליועץ.

31 בהחלטת הממשלה 2443 הוטל על מערך הסייבר לבצע בקרה על יישום נספח ד' בנושא יחידות להכוונה מקצועית מגזרית בתחום הגנת הסייבר במשרדי הממשלה.

**משרד מבקר המדינה מציין לחיוב את מערך הסייבר על שנקט פעולה לצמצום הסיכון במגזרים מסוימים והקים בשנת 2023 יחידת ממשקים שפועלת לקדם ולשפר את מצב הגופים במגזרים אלו תוך הנחיה מרצון יודגש כי מדובר בפתרון זמני ולא בפתרון המיטבי.**

בדוח לשנת 2023 פרסם מערך הסייבר תרשים המציג את אירועי הסייבר המשמעותיים לפי מגזרים מתחילת המלחמה ועד סוף שנת 2023.

תרשים 3 : **אירועים משמעותיים לפי מגזרים בתקופת המלחמה (אוקטובר-דצמבר 2023)**




המקור : סיכום שנת 2023, מערך הסייבר הלאומי[32].

בתשובת מגזר 6 נמסר כי הנתונים בתרשים 3 המתייחסים למגזר 6 אינם תואמים את המספרים הידועים לו, וכי בהנחה שהם נכונים הרי שמדובר באירועים שהיחידה המגזרית לא קיבלה ממערך הסייבר או מהגופים מידע עליהם.

**משרד מבקר המדינה מעיר למערך הסייבר כי עליו לעדכן את היחידות המגזריות הרלוונטיות באופן מידי בכל האירועים המשמעותיים הקשורים למגזר שלהם. כמו כן עליו להבטיח לפני פרסום מידע הקשור למגזרים כי הוא מתואם עם המגזר הרלוונטי והמידע מקובל עליו.**


**יחידות הסייבר המגזריות הן התשתית המקצועית והמעשית לקידום ההנחיה, ההכוונה, הפיקוח והבקרה בנוגע להגנת הסייבר במאות גופים ציבוריים ופרטיים המספקים שירותים חיוניים במגוון תחומים. בביקורת נמצא כי חלק ממערך יחידות הסייבר המגזריות מתאפיין בחולשה תפקודית משמעותית.**

בתשובת מערך הסייבר נמסר כי המערך פנה למשרדי הממשלה השונים כדי שיפעלו ליישום חובתם וציין כי סייע למשרדים באיוש חירום בתקופת חרבות ברזל. במקביל פועל המערך לעגן את תפקיד היחידה המגזרית במגזרים חיוניים במסגרת טיוטת חוק הסייבר שהוא מקדם בעת הזו.

---

32 סיכום שנת 2023 בסימן חרבות ברזל, עמ' 6.

בתשובת אגף השכר מספטמבר 2024 נמסר כי האגף מבין את הצורך בהיערכות המדינה לאירועי סייבר ומייחס לכך חשיבות רבה אולם במועד תשובתו עדיין לא התקבלו פניות בנושא מיחידות הסייבר המגזריות. עוד ציין האגף כי עם פרוץ מלחמת חרבות ברזל פנתה הנהלת מערך הסייבר לאגף השכר לנוכח הקושי בגיוס ובשימור של עובדים במערך הסייבר עצמו. כפועל יוצר מפנייה זו ולאחר בדיקת הדברים אישר אגף השכר מתווים למתן מענקי קליטה ולשימור של עובדים במערך הסייבר בהיקפים משמעותיים. אגף השכר ימשיך להיות מעורב בכל הנדרש והמצוי בתחומי אחריותו כדי לתמוך במערך הסייבר ולסייע בהיערכות המדינה לאירועי סייבר.

**על מערך הסייבר כגורם לאומי אחראי מהבחינה המקצועית ליחידות הסייבר המגזריות, המכיר את הפערים הרוחביים בתפקודן, לרכז ולכלול בפנייתו לאגף השכר גם את צורכי יחידות הסייבר המגזריות והפערים שקיימים כיום או לחלופין לכוון את היחידות לפנות לאגף השכר בנושא וזאת כדי להבטיח שגם יחידות אלו יקבלו את המענקים והכלים לגיוס ולשימור של עובדים שקיבל מערך הסייבר עצמו.**

בתשובת אגף תקציבים נמסרה עמדתו ולפיה רמת ההגנה בסייבר בענף או בסקטור מסוים נמצאת בסמכות ובאחריות של המשרד הרלוונטי ולכן צריכה להיות חלק מסדר העדיפויות של המשרד ולהיקבע בהתאם לשיקול דעתו. כמו כן ציין כי מטרת החלטת הממשלה 2443 נועדה להיות תמריץ זמני שפותח עם הזמן ומאפשר ליחידות המגזריות להיות חלק מסדר העדיפויות המשרדי והוסיף שבכל מקרה אין לתקצב בנפרד את אותן היחידות. לפיכך נקבע בהחלטת הממשלה שבשנים הראשונות התקציב יתקבל ממקור חיצוני ולאחר מכן יופחת בהדרגה.

**מומלץ כי מערך הסייבר יגבש, בשיתוף מנכ"לי משרדי הממשלה הרלוונטיים, וכן בשיתוף יחידות הסייבר המגזריות, אגף התקציבים, אגף השכר ונש"ם עבור כל יחידת סייבר מגזרית המלצה למבנה ארגוני, וכן הגדרת תפקידים, תחומי פעילות, שכר מתאים ותקציב הנדרש לביצוע משימותיה בהתאם לסיכונים, להיקף הפעילות ולמורכבות בכל מגזר. עוד מומלץ כי שותפים אלו יתכנסו באופן עיתי ויוודאו שהיחידות פועלות לפי האיוש והתקציב שהוגדרו, ואם יש צורך בכך - יעדכנו נתונים אלו בהלימה לסיכונים ולרמת ההגנה בכל מגזר.**

**עוד מומלץ כי מערך הסייבר בשיתוף היחידות המגזריות יציגו לקבינט המדיני-ביטחוני או לוועדת שרים ייעודית המופקדת על הנושא את הפערים התפקודיים, ואת ההשפעות והסיכונים הנובעים מפערים אלו על החוסן של המשק.**

## גופים ותשתיות לאומיות הפועלים ללא אסדרה בתחום הסייבר

כל גוף אחראי כאמור לטפל בסיכונים שהוא חשוף להם, לנהל אותם ולפעול להפחתתם. אירוע משמעותי בסייבר הוא סיכון מהותי לתפקודו התקין והרציף של ארגון ולעמידתו ביעדים שקבע לעצמו ובדרישות החוק לשמירה על מידע מסווג או פרטי. לכן כל גוף נדרש לייצר מעטפת הגנה ויכולות התמודדות עם תרחישי האיום והסיכונים שהוא חשוף אליהם ואחראי לטפל באירוע סייבר המתרחש בחצרו. תפקיד הגופים האסדרתיים המדינתיים בתחום הסייבר הוא בין היתר להביא לשיפור של רמת ההגנה של הגופים המונחים על ידם בתחום הסייבר, לחזק את החוסן שלהם ושל המשק בתחום זה ולאכוף, בהתאם לסמכותם, את עמידת הגופים בחוקים, בתקנות ובהנחיות רלוונטיים. הם עושים זאת באמצעות הכוונה, הנחיה של הגופים ובקרה עליהם באופן שוטף וכן באמצעות חבירה או סיוע להם בהתמודדות עם תקיפות סייבר שעשויות לסכן את המשק או לפגוע במידע אישי.

בפרק זה הוצג שיש גופים ופרויקטים לאומיים שחיוניים למשק ולמדינה, ואין לשום גוף אסדרתי מדינתי סמכות להנחות אותם בתחום הסייבר ולפקח עליהם בהתאם לסיכון ולנזק הפוטנציאלי כתוצאה מפגיעה במערכות הממוחשבות שלהם.

כאמור תפקידה של ועדה ב/84 לעסוק במערכות ממוחשבות חיוניות בגופי תמ"ק ולאשר את ההוספה של גופי תמ"ק או את ההחסרה שלהם (הוועדה לא עוסקת בגופים שאינם תמ"ק או בתשתיות מרכזיות).

**נמצא כי במדינת ישראל קיימים גופים שפגיעה בהם עלולה להוביל לפגיעה מעשית ותודעתית נרחבת, ולהשבתה של שירותים חיוניים. אמנם גופים אלו מחויבים לנהל את סיכוני הסייבר שלהם אך למרות חשיבותם אין כיום גוף אסדרתי מדינתי בתחום הסייבר שהוא בעל הסמכות להנחות אותם לעמוד ברמת ההגנה הראויה ההולמת את הסיכון הכרוך בהם, והכפפתם להנחיית הגוף האמור תלויה ברצונם.**

**מומלץ כי מערך הסייבר ויה"ב יבחנו את הצורך בהגדרת פרקטיקת ההנחיה מרצון. לעניין זה ניתן לתת את הדעת על היקף הליווי, הרגולציה והפיקוח הנדרשים במתווה זה.**

**מומלץ כי מערך הסייבר ימפה את הגופים ואת התשתיות הלאומיות בישראל בהתאם לסיכונים הלאומיים ולנזק הפוטנציאלי כתוצאה מפגיעה במערכות הממוחשבות, יבחן ויוודא שנוסף על המחויבות הבסיסית שלהם לנהל את סיכוניהם הם מקבלים ליווי והכוונה מגורם אסדרתי מדינתי בתחום הסייבר בהלימה לתחום פעילותם, לסיכון שבפגיעה בהם ולרמת ההגנה שלהם. עוד מומלץ כי תהליך המיפוי והבחינה יבוצע באופן עיתי אם במסגרת ועדת היגוי ב/84 שכוללת חברים מכל הגופים האסדרתיים המדינתיים או במסגרת ועדה אחרת.**

☆

**התמונה העולה מפרק זה משקפת פער בסמכויות וביכולת התפקודית של גופים אסדרתיים מדינתיים ובהם מערך הסייבר, יחידות הסייבר המגזריות ויה"ב להנחות ולפקח על חלק מהמשק ולהבטיח את עמידתו ברמת הגנה ראויה בסייבר.**

## <u>קידום הצעת חוק הסייבר</u>

זה שנים רבות קיימת הסכמה מקצועית במערכת הממשלתית ולפיה הטיפול בתחום הגנת הסייבר וההתמודדות עם האיומים הנשקפים לישראל ממרחב זה מחייבים הסדרה בחוק ייעודי. עד לפרוץ מלחמת חרבות ברזל ההסדרה החקיקתית בתחום זה הייתה קיימת רק לגופים המוגדרים בחוק להסדרת הביטחון (בין היתר גופי תמ"ק). במהלך השנים נתקל הטיפול בנושא בהתנגדויות ובחסמים בין היתר לנוכח החשש מהתערבות של המדינה בהתנהלותם של גופים פרטיים בדגש על גופים עסקיים.

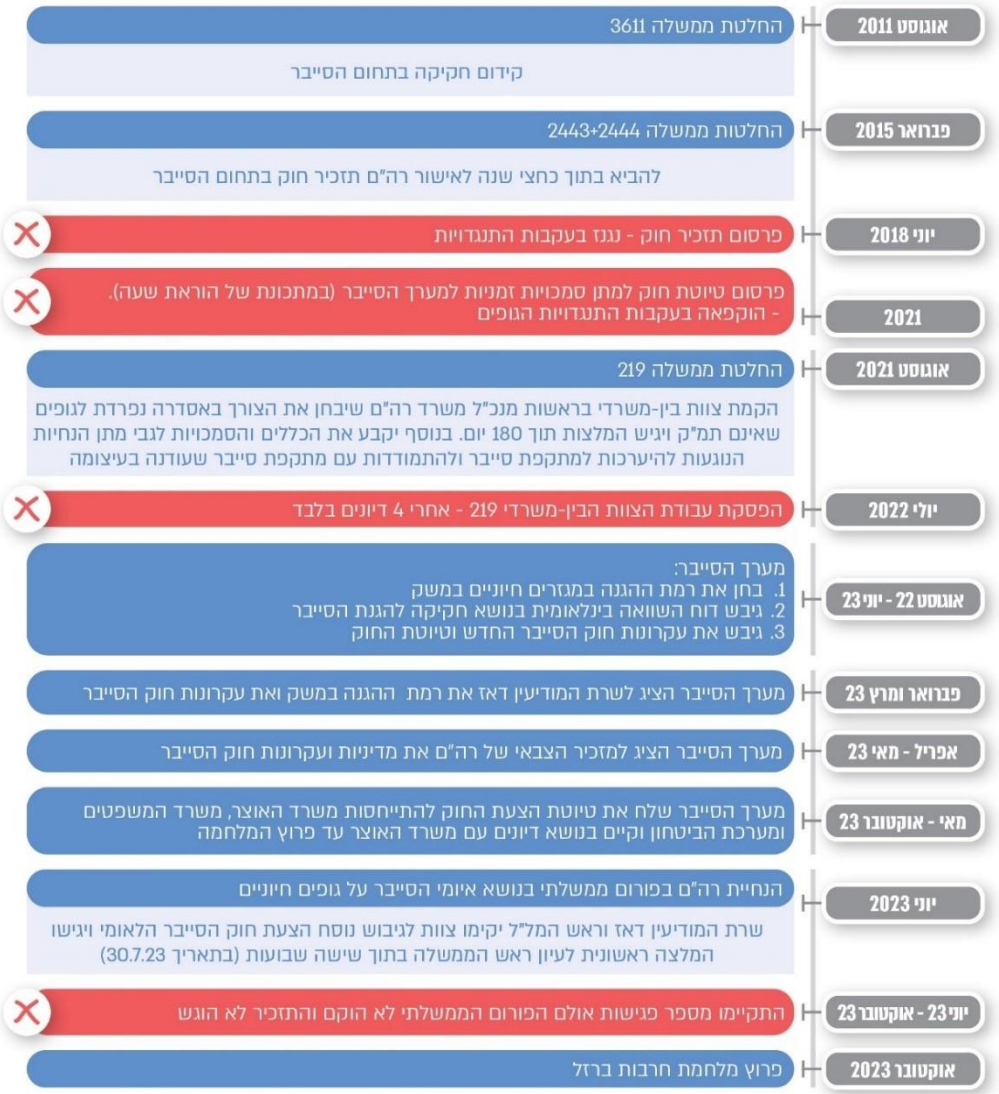
**במהלך המלחמה נעשתה אסדרה זמנית בחקיקה מוגבלת בזמן כלפי ספקי שירותי אחסון ו-IT כמפורט בהמשך.**

ולצד האמור, בנושא הגנת הפרטיות ואבטחת מאגרי מידע (כהגדרתם שם) קיימת אסדרה לכלל המשק. כל המחזיקים או המנהלים מאגרי מידע או מידע רגיש לפי הגדרתם בחוק הגנת הפרטיות, נדרשים לעמוד בהוראות חוק זה ובתקנותיו (לרבות תקנות בעניין אבטחת מידע במאגרי מידע). אסדרה זו אף חוזקה משמעותית בעקבות אישור תיקון 13 לחוק על ידי הכנסת באוגוסט 2024, חקיקה אשר קודמה במהלך תקופת מלחמת חרבות ברזל.

### פעולות מערך הסייבר לקידום חוק הסייבר לפני פרוץ מלחמת חרבות ברזל

בשנים 2011 - 2015 התקבלו כמה החלטות ממשלה שנועדו לשפר את רמת ההגנה בתחום הסייבר, בין היתר באמצעות חקיקה תומכת. להלן בתרשים החלטות הממשלה והפעולות שקידם מערך הסייבר לקידום החקיקה עד פרוץ מלחמת חרבות ברזל.

תרשים 4: **ציר זמן לקידום חקיקת חוק הסייבר משנת 2011 ועד לפרוץ מלחמת חרבות ברזל באוקטובר 2023**




**מהתרשים עולה כי משנת 2011 ועד פרוץ המלחמה ביצעו משרד רה"ם ומערך הסייבר פעולות שונות לקידום תזכיר חוק סייבר. חרף זאת נמצא כי במשך יותר מעשור לא הושלמו הפעולות לצורך חקיקה בכנסת של חוק ייעודי להסדרת תחום ההגנה בסייבר שישמש בסיס לאסדרה, הנחיה ופיקוח למול כלל המשק (ראו בהמשך).**

## פעולות הצוות הבין-משרדי שהוקם בעקבות החלטת הממשלה 219 מאוגוסט 2021

בהחלטת הממשלה 219 מאוגוסט 2021 הוחלט להקים צוות בין-משרדי בראשות מנכ"ל משרד רה"ם שיבחן ויגיש בתוך 180 ימים המלצות בנוגע להתאמות הנדרשות להיערכות של ממד הסייבר האזרחי לאיומי סייבר. על הצוות הוטל לבחון את הצורך ליצור אסדרה נפרדת לגופים שלא הוגדרו גופי תשתית מדינה קריטית ולקבוע את הכללים והסמכויות לגבי מתן הנחיות הנוגעות להיערכות למתקפת סייבר ולהתמודדות עם מתקפת סייבר שעודנה בעיצומה.

בחודשים מאי עד יולי 2022 נפגש הצוות הבין-משרדי ארבע פעמים. בפגישותיו הוצג הפער בין מצב האסדרה בתחום הגנת הסייבר בישראל לבין המצב במדינות העולם; הוצגה תמונת האיומים

הנשקפים לישראל; הוצגו שכבות ההגנה במשק; וכן הוצגו ממצאי השוואה בין-לאומית בתחום זה והתקיימו דיונים עם נציגי המשרדים להגנת הסביבה, התחבורה, הבריאות, האנרגיה והתקשורת, שהתמקדו בסמכויותיהם של המשרדים והגופים המונחים ובמודל ההפעלה.

ביולי 2022 פרש מנכ"ל משרד רה"ם דאז מתפקידו ובמקביל הופסקה פעילות הצוות הבין-משרדי שהוא עמד בראשו. לדברי מערך הסייבר הצוות הפסיק את הפעילות עקב הקדמת הבחירות לכנסת העשרים וחמש, וחלק ממשימותיו לא הושלמו. מאז סיום פעילות הצוות המערך מקדם חלק מפעולות אלו כמו קידום חוק הסייבר.

תרשים 5: **סטטוס הפעילויות שהוטל על הצוות הבין-משרדי לבצע**

| | הנושא | הסטטוס |
|---|---|---|
| 1 | בחינת רמת ההגנה בתחום הסייבר בגופים שונים במשק | בוצע |
| 2 | ביצוע השוואה בין-לאומית בין מצב האסדרה בתחום הגנת הסייבר בישראל ובין המקובל במדינות החברות בארגון לשיתוף פעולה ולפיתוח כלכלי (OECD) וממצאי ההשוואה ישמשו בסיס לגיבוש המלצות הצוות | בוצע חלקית ומערך הסייבר השלים את ביצוע ההשוואה במסגרת העבודה על הצעת חוק הסייבר |
| 3 | בחינת חלופות להעלאת רמת ההיערכות של מרחב הסייבר הישראלי לאיומי סייבר: | לא בוצע |
| | **3.1** פעילות הסברה | לא נדון |
| | **3.2** אימוץ וקידום של מודעות לתקינה וולונטרית בהתאם לסטנדרט הנהוג במדינות המפותחות | לא נדון |
| | **3.3** יצירת מרשם וולונטרי של העסקים העומדים בתקינה | לא נדון |
| | **3.4** יצירת אסדרה נפרדת לגופים שלא הוגדרו כגופי תשתית מדינה קריטית וקביעת הכללים והסמכויות למתן הנחיות הנוגעות להיערכות למתקפת סייבר ולהתמודדות עם מתקפת סייבר שעודנה בעיצומה | מערך הסייבר מקדם זאת באמצעות הצעת חוק הסייבר |
| 4 | בחינת המנגנון הקיים להמלצה בנוגע לשינוי גופי תשתית מדינה קריטית המונחים ע"י" מערך הסייבר הלאומי | לא נדון |

הוכן בידי משרד מבקר המדינה.

**נמצא כי הצוות הבין-משרדי בראשות מנכ"ל משרד רה"ם שהוקם כמתחייב מהחלטת הממשלה 219 מאוגוסט 2021 ופעל בשנת 2022 לגבש המלצות בנוגע להתאמות הנדרשות להיערכות של ממד הסייבר האזרחי לאיומי סייבר, הפסיק את פעולתו בלי להשלים את המשימות שהוטלו עליו, ומאז לא הוקם צוות חדש כנדרש. מאז הפסקת הפעילות בשנים 2022 - 2023 מקדם מערך הסייבר את הצעת חוק הסייבר ואת המשימות הרלוונטיות לחוק אולם בחלוף כארבע שנים החוק טרם נחקק ועדיין יש משימות נוספות שהוטלו על הצוות הבין-משרדי בהחלטת הממשלה 219 ואינן מקודמות: בחינת חלופות להעלאת רמת ההיערכות של מרחב הסייבר הישראלי לאיומי סייבר לרבות פעילות הסברה, אימוץ וקידום מודעות לתקינה וולונטרית בהתאם לסטנדרט הנהוג במדינות מפותחות, יצירת מרשם של העסקים העומדים בתקינה וכן בחינת המנגנון הקיים להמלצה בנוגע לשינוי גופי תשתית מדינה קריטית המונחים על ידי מערך הסייבר.**

**מומלץ כי מערך הסייבר יקדם את הפעילויות שהוטלו על הצוות הבין-משרדי בהחלטת הממשלה ולא הושלמו ויפעל לדווח לממשלה על ביצוען.**

### השוואה בין-לאומית בנושא חקיקת סייבר

לאחר שהצוות הבין-משרדי שהוקם במסגרת החלטת הממשלה 219 הפסיק את פעילותו, מאוגוסט 2022 פעל מערך הסייבר לקדם חקיקה בתחום הסייבר. לצורך זה הוא ביצע בין היתר השוואה בין-

לאומית בנושא חקיקה לאומית להגנת הסייבר בחמש המדינות האלו: בריטניה, גרמניה, אוסטרליה, הולנד וארצות הברית. הדוח גובש ביוני 2023 וההשוואה העלתה כי המדינות שנסקרו החילו, ככלל, שתי חובות עיקריות בנוגע לגופים קריטיים וחיוניים: חובת דיווח על אירוע סייבר משמעותי וחובת עמידה ברמת הגנה ראויה.

לוח 3: **ההשוואה הבין-לאומית שביצע מערך הסייבר ביוני 2023**

| המדינה | חובת דיווח על אירוע סייבר משמעותי | חובת ניהול הסיכון | סמכויות פיקוח ואכיפה | מועד הכניסה לתוקף של חוק לאומי להגנת הסייבר |
|---|---|---|---|---|
| גרמניה | ✓ | ✓ | ✓ | ✓ (2015) |
| האיחוד האירופי - NIS 1 | ✓ | ✓ | ✓ | ✓ (2016) כניסה לתוקף ב-2018 |
| בריטניה | ✓ | ✓ | ✓ | ✓ (2018) |
| אוסטרליה | ✓ | ✓ | ✓ | ✓ (2018) |
| ארצות הברית | ✓ | מוגבל | ✓ | ✓ (2022) |
| האיחוד האירופי - NIS 2 | ✓ | ✓ הרחבת מספר המגזרים | ✓ הרחבה משמעותית | ✓ (2022) |
| ישראל - המצב הנוכחי | ✗ | ✗ | ✗ | ✗ |

המקור: מערך הסייבר.

### הנחיית ראש הממשלה, מר בנימין נתניהו, ביוני 2023 בדבר הנחת תזכיר חוק

נוסף על ההשוואה הבין-לאומית ביצע מערך הסייבר בחינה של המצב הקיים בכל אחד מהמגזרים החיוניים במשק, ובמסגרת זו בחן את רמת ההגנה בכל מגזר ואת תמונת האיומים עליו. תוצרי הבחינה הראו כי חלק מהמגזרים סובלים מהגנה לא מספקת בסייבר. בהתאם לתובנות אלו מערך הסייבר גיבש עקרונות מרכזיים לטיוטת חוק סייבר, והוא החל לגבש את טיוטת החוק תוך היוועצות עם כמה גופים אסדרתיים וגופים נוספים ובהם משרד האוצר ויחידות הסייבר המגזריות. רמת ההגנה במשק ועקרונות החוק הוצגו כאמור בפברואר ובמרץ 2023 לשרת המודיעין דאז. נוסף על כך, באפריל 2023 העביר מערך הסייבר למזכיר הצבאי של רה"ם נייר מדיניות המציג את הרציונל של חוק הסייבר ואת רכיביו העיקריים, ובמאי העביר לו מצגת הכוללת פירוט נרחב יותר לגבי רכיבי החוק המוצע.

במאי 2023 שלח מערך הסייבר את טיוטת הצעת החוק שגיבש להתייחסות משרד האוצר, משרד המשפטים ומערכת הביטחון ועל בסיסה קיים עם משרד האוצר דיונים רבים, אך הם נעצרו לתקופה ארוכה אחרי פרוץ המלחמה.

כאמור, ביוני 2023 כינס רה"ם, פורום מצומצם של שרי ממשלה כדי לדון באיומי הסייבר על גופים חיוניים שבאחריותם. בפגישה הציג ראש מערך הסייבר דאז את תמונת האיומים והסיכונים שהתגברו בשנים האחרונות, ואת הצורך במתן מענה לאיומים אלה באמצעות חוק הסייבר. כמו כן הוצגו בדיון עיקרי החוק המוצע. בפגישה הנחה רה"ם את שרת המודיעין דאז ואת ראש המל"ל להקים צוות לגיבוש נוסח הצעת חוק הסייבר הלאומי בהשתתפות ראש מערך הסייבר והמזכיר הצבאי לרה"ם ולהגיש המלצה ראשונית לעיון ראש הממשלה בתוך שישה שבועות (עד 30.7.23). לפי תוכנית העבודה של מערך הסייבר ומשרד המודיעין לשנת 2023[33] (שנסגר בינתיים), תזכיר חוק הסייבר תוכנן להתפרסם בדצמבר 2023. לדברי מערך הסייבר, נוכח פרוץ מלחמת חרבות ברזל באוקטובר והצורך להתמקד במענה על אתגרי הלוחמה נדרש היה לשנות את תוכנית העבודה.

33 www.gov.il/he/departments/news/spoke-plans160723

**נמצא כי הצוות בראשות שרת המודיעין דאז וראש המל״ל ובהשתתפות ראש מערך הסייבר דאז והמזכיר הצבאי שעל הקמתו החליט ראש הממשלה ביוני 2023 לצורך גיבוש נוסח חוק הסייבר הלאומי, התכנס כמה פעמים, אולם גיבוש הצעת חוק הסייבר שתוכנן לדצמבר 2023 לא הושלם עד יוני 2025.**

בתשובת מל״ל נמסר כי מהפסקה משתמע כי היה עליו לגבש את נוסח חוק הסייבר הלאומי ולא כך הדבר, נוסח תזכיר חוק הסייבר המיועד לקדם הגנת סייבר מיטבית במרחב האזרחי מגובש ומקודם על ידי מערך הסייבר הלאומי האמון על הנושא. המל״ל מסייע למערך הסייבר ככל שזה פונה אליו אך המל״ל אינו אמון על גיבוש נוסח התזכיר.

בתשובת מערך הסייבר נמסר כי הוא ממשיך להשקיע תשומות משמעותיות כדי להשלים את גיבוש הצעת החוק בהקדם האפשרי ומקיים פגישות בנושא בדרג מקצועי ובדרגי מנכ״ל של משרדי ממשלה רלוונטיים וגופים נוספים.

## פעולות מערך הסייבר לקידום הצעת חוק הסייבר אחרי פרוץ מלחמת חרבות ברזל

במהלך המלחמה, ובמקביל לביצועה של ביקורת זו, האיץ מערך הסייבר את הפעולות לקידום הצעת חוק הסייבר ולטיפול בפערי האסדרה, כפי שיפורט בפרק זה ובתרשים 6.

תרשים 6: **ציר הזמן של קידום חקיקת חוק הסייבר מפרוץ מלחמת חרבות ברזל ועד מאי 2025**


על פי נתוני ממערך הסייבר, בעיבוד משרד מבקר המדינה.

## התקנת תקנות שעת חירום וחקיקה בהוראת שעה לאחר פרוץ המלחמה

עם פרוץ מלחמת חרבות ברזל ב-7.10.23 התעצמו תקיפות הסייבר בכלל, ובפרט נגד ספקי שירותי אחסון ונגד השירותים הדיגיטליים. לספקים אלו חיבוריות גבוהה לגופים רבים במשק הישראלי, ולכן בעיקר בתקופות מלחמה תקיפות סייבר חמורות נגדם עלולות להביא לפגיעה רחבה בביטחון המדינה ובביטחון הציבור וכן לפגוע באספקה ובשירותים החיוניים למשק. למרות הסיכונים לפני המלחמה לא הייתה לגופים אלו חובה לעמוד ברמת הגנה ראויה, ואין גורם שמנחה אותם באופן מחייב בתחום הסייבר. כמו כן לדברי מערך הסייבר לעיתים בעת אירוע סייבר הם אינם משתפים פעולה עם מערך הסייבר.

כדי להתמודד עם סיכונים אלו קידם מערך הסייבר, לאחר פרוץ המלחמה, תקנות שעת חירום (חרבות ברזל) (התמודדות עם תקיפת סייבר חמורות במגזר השירותים הדיגיטליים ושירותי

האחסון), התשפ"ד-2023, שנכנסו לתוקף ב-8.11.23 (ותוקפן היה לחודש), ובהמשך - ב-6.12.23 - התקבל בכנסת ונכנס לתוקף חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה - חרבות ברזל), התשפ"ד-2023, שתוקפו לשבעה חודשים. בתאריך 23.7.24 נכנס לתוקף תיקון לחוק שבמסגרתו הוארך תוקפו עד 31.3.25, וב-31.3.25 נכנס לתוקף תיקון נוסף לחוק שבמסגרתו הוארך תוקפו עד 17.11.25. לפי החוק, במקרה של "תקיפת סייבר חמורה" כהגדרתה בחוק בלבד, מוקנית למערך הסייבר, לשב"כ ולמלמ"ב[34] סמכות לתת הוראות לספקי שירותים דיגיטליים ולספקי שירותי אחסון לטיפול בתקיפה בתנאים שמוגדרים בחוק. עוד קובע החוק חובת דיווח ליועצת המשפטית לממשלה ולוועדת החוץ והביטחון של הכנסת, בין היתר, בדבר המקרים שבהם ניתנו הוראות לפי החוק על ידי הגורם המוסמך.

**עד סוף אוגוסט 2024 דיווח מערך הסייבר ליועצת המשפטית לממשלה ולוועדת החוץ והביטחון של הכנסת על מספר מקרים שבהם הייתה תקיפת סייבר חמורה וניתנו הנחיות מחייבות לפי החוק. לדברי מערך הסייבר, עד אפריל 2024, לא נדרש מערך הסייבר להפעלת סמכויות מחייבות מתוקף הוראת השעה, לדבריו מפני שעצם חקיקת החוק תרמה לשינוי.**

**מתחילת מלחמת חרבות ברזל נדרשת מדינת ישראל להתמודד עם מתקפות סייבר מורכבות יותר ועוצמתיות יותר. מציאות זו הדגישה את החסר בהסדר החקיקתי שיש בו כדי לאפשר לגורמים המדינתיים להנחות באופן מחייב את הגופים החיוניים במשק לעמוד ברמת הגנה ראויה, לדווח להם על תקיפות סייבר חמורות ולפעול בהתאם להנחיותיהם בעת תקיפת סייבר חמורה. כמו כן לעיתים הגופים אינם יודעים למי הם צריכים לדווח על תקיפת סייבר חמורה, ובהיעדר תשתית דיווח אחודה הדיווח לכל גוף אסדרתי אינו שלם.**

### הנחיית ראש הממשלה, מר בנימין נתניהו, מינואר 2024 בדבר הנחת תזכיר חוק סייבר

בעקבות בקשת ראש מערך הסייבר דאז מראש מל"ל ב-11.1.24 ובסיוע של מל"ל, פנה רה"ם בינואר 2024 לחלק משרי הממשלה במכתב בנושא קידום חוק הגנת הסייבר במרחב האזרחי, ובו הנחה את מערך הסייבר להגיש לאישור ועדת השרים לענייני חקיקה בתוך שלושה חודשים תזכיר חוק שיספק מענה לפערים הקיימים. כמו כן הוא ביקש מהשרים להנחות את הגורמים המקצועיים לתת עדיפות לסוגיה ולשתף פעולה עם מערך הסייבר תוך ביצוע הפעולות הנדרשות כדי לאפשר זאת ולהביא לידיעת המל"ל על מחלוקות או קשיים שעלולים לעכב את גיבוש תזכיר החוק.

לדברי מערך הסייבר מלחמת חרבות ברזל ממחישה את חשיבות ההגנה על ממד הסייבר הישראלי, וההגנה על תפקודו התקין והבטוח מהווה נדבך משמעותי בהגנה הלאומית. לאור זאת חשיבות חובות הארגונים החיוניים לביסוס רמת הגנת סייבר ארגונית ראויה קיבלה משנה תוקף לצד ביסוס יכולות סיוע לאומיות בנסיבות הנדרשות. מערך הסייבר הדגיש כי הוא מקדם טיוטת הצעת חוק שיסדיר רוחבית את הגנת ממד הסייבר הישראלי בראייה לאומית. במהלך הלחימה המשיך מערך הסייבר לקיים תהליכי למידה, הפקת לקחים וגיבוש תובנות מתקופת הלחימה ומתהליך החקיקה של הוראת השעה, וטיוטת החוק עודכנה בהתאם.

במרץ 2024 הפיץ מערך הסייבר את טיוטת חוק הסייבר לגורמים המעורבים בנושא, ובהם גופים אסדרתיים מדינתיים בתחום הסייבר, הרשות להגנת הפרטיות ויחידות הסייבר המגזריות, ופעל כדי לקבל את התייחסותם. בנוסף הפיץ את הטיוטה למל"ל כגוף שמסייע ליישוב מחלוקות. לדברי מערך הסייבר, לאחר המשך ליבון מעמיק של תובנות מהמלחמה וייישום הוראת השעה שפורסמה במהלכה, הוא הפיץ לגופים בנובמבר 2024 טיוטה מעודכנת. להלן עקרונות טיוטת החוק:

[34] הממונה על הביטחון במערכת הביטחון כמשמעו בסעיף 21 לחוק להסדרת הביטחון.

תרשים 7: **העקרונות המרכזיים המוצעים בטיוטת חוק הסייבר נכון למועד סיום הביקורת**


המקור: מערך הסייבר.

מהתרשים עולה כי במסגרת טיוטת החוק החדש מוצע בשלב זה לעגן הסדרה לאומית רוחבית בתחום הסייבר בחקיקה ראשית ובכלל זה לעגן את סמכויות יחידות הסייבר המגזריות כלפי הגופים המונחים.

לוח 4: **ההשפעות של היעדר הסדרה חקיקתית על ההיערכות למלחמה ועל מהלכה**

| הנושא שנכלל בטיוטת הצעת החוק | תיאור הבעיה בהיעדר חוק | ההשפעה של היעדר ההסדרה בחוק | האם טיוטת החוק מנובמבר 2024 נותנת מענה על הבעיה |
|---|---|---|---|
| דיווח של גוף חיוני על תקיפת סייבר חמורה[35] | 1. כיום לא כל הגופים החיוניים מחויבים[36] לדווח ליחידת הסייבר המגזרית ולמערך הסייבר על תקיפת סייבר חמורה.<br>2. יש גופים חיוניים שמחויבים לדווח בעת אירוע סייבר לשלושה גורמים אסדרתיים מדינתיים שונים: הרשות להגנת הפרטיות (במקרה של פגיעה במידע אישי השמור במאגר מידע), יחידת הסייבר המגזרית ומערך הסייבר הלאומי. | 1. אין לגופים האסדרתיים המדינתיים תמונת מצב מלאה על כלל תקיפות הסייבר החמורות בגופים החיוניים במשק. דבר זה מגביל ומצמצם את יכולתם לסייע לגופים ולמנוע זליגה של האירוע לגופים אחרים במגזר ובמשק.<br>2. לעיתים הגופים אינם יודעים למי הם צריכים לדווח על תקיפת סייבר חמורה והחוק צריך לכלול את כלל הגורמים שהגוף צריך לדווח | 1. כן<br>2. הפער נותר - עדין גופים ידרשו לדווח למספר גורמים במקביל. |

35 לרבות אירוע אבטחה חמור לפי הגדרתו בתקנות אבטחת מידע וכן אירועים שאינם נוגעים למידע אישי.

36 כלל הגופים במשק מחויבים לדווח באופן מידי לפי החוק רק לרשות להגנת הפרטיות על אירוע אבטחת מידע חמור במאגר מידע על פי ההגדרות שנקבעו בהקשר זה על פי חוק.

| הנושא שנכלל בטיוטת הצעת החוק | תיאור הבעיה בהיעדר חוק | ההשפעה של היעדר ההסדרה בחוק | האם טיוטת החוק מנובמבר 2024 נותנת מענה על הבעיה |
|---|---|---|---|
| | | אליהם או להפנות לחוקים אחרים בנושא. למשל: תקנות אבטחת מידע. כמו כן אין כיום תשתית דיווח אחודה ולכן עולה כי הדיווח לכל גוף אסדרתי אינו שלם. | |
| סמכויות יחידת הסייבר המגזרית כלפי הגופים המונחים וחובתם לעמוד ברמת הגה ראויה | לחלק מיחידות הסייבר המגזריות חסרה הסמכות להנחות גופים חיוניים במגזר שלהם באופן שוטף ולפעול בעת אירוע סייבר. | יש גופים חיוניים שאינם מחויבים ליישם את הנחיות היחידה המגזרית ולעמוד ברמת הגנה ראויה. | כן |
| מנגנון קביעת ארגון חיוני | כיום אין הגדרה מחייבת בחוק מהו ארגון חיוני. | כל יחידה מגזרית קובעת קריטריונים שונים, ואין הגדרה לאומית אחודה. | כן |
| הגדרת מגזרים חיוניים ומנגנון הוספת מגזרים | כיום אין הגדרה בחוק של מגזרים בתחום הסייבר. נדרשת הסדרה בנושא זה הכוללת מנגנון להוספה של מגזרים בהתאם לסיכונים המשתנים לאורך השנים. | כיום יש מגזרים ללא יחידות מגזריות שמנחות ומסייעות לגופים החיוניים במגזר. | כן |
| הגדרת הייעוד, הסמכות והתפקידים של מערך הסייבר | כיום, למעט גופי תמ"ק ובאופן זמני גופים שעונים להגדרות בחוק ספקי שירותי אחסון ושירותים דיגיטליים, אין חובה בחוק לגופים במשק לשתף פעולה עם מערך הסייבר גם בזמן תקיפת סייבר חמורה. | אין למערך הסייבר סמכות לפעול מול רוב הגופים במשק לרבות גופים חיוניים גם בזמן תקיפת סייבר חמורה. | כן - עבור גופים חיוניים |
| הכלים והסנקציות בנוגע לגופים שלא יפעלו כנדרש | כיום אין למערך הסייבר ולחלק מיחידות הסייבר המגזריות כלים וסנקציות בנוגע לגופים שאינם פועלים בהתאם להנחיות.<br><br>בתחום הגנת הפרטיות - תיקון 13 לחוק הגנת הפרטיות הקנה לרשות את הסמכות להטיל עיצומים כספיים בסך של עד כמה מיליוני שקלים, כדי להעלות את מידת הציות להוראות חוק הגנת הפרטיות ותקנותיו, וכפועל יוצא מכך - לחזק את ההגנה על מידע אישי השמור במאגרי מידע. | חלק מהגופים אינם מבצעים את ההנחיות ואין אפשרות להטיל עליהם סנקציות כלכליות.<br><br>. | כן |

על פי נתוני מערך הסייבר הלאומי, בעיבוד של משרד מבקר המדינה.

מערך הסייבר ריכז את התייחסויות הגופים לטיוטת תזכיר החוק שהעביר להם ופעל מולם ליישום ההערות ולצמצום המחלוקות. לדברי מל"ל המשרדים לא פנו אליו בנוגע למחלוקות והם רוכזו על ידי מערך הסייבר. לבקשת מערך הסייבר בדצמבר 2024 ובפברואר 2025 קיים מל"ל שתי פגישות עם גורמים ממערך הסייבר ועם גופים נוספים כדי לקדם טיפול במחלוקות שעלו מולם. אולם עד יוני 2025 טרם התקיימו פגישות עם כל הגורמים ולא יושבו כל המחלוקות. לדברי מערך הסייבר עיקר החסמים לקידום החוק הם: יצירת מכנה משותף רוחבי רחב למענה הלאומי מול 14 רגולטורים, בעלי ייחודיות ושונות וכן היבטי התקציב החיוניים לקידום החוק. מערך הסייבר לא העביר למבקר המדינה את ריכוז המחלוקות ואת סטטוס הטיפול בהן וטרם הוגדר לוח זמנים להמשך קידום הצעת החוק.


**זה שנים רבות קיימת הסכמה מקצועית במערכת הממשלתית ולפיה הטיפול בתחום הגנת הסייבר וההתמודדות עם האיומים הנשקפים לישראל מממד זה מחייבים הסדרה בחוק ייעודי שישמש בסיס להנחיה ולפיקוח של הגורמים המדינתיים על הגופים החיוניים במשק וידרוש מהם לעמוד ברמת הגנה ראויה, לדווח לגורמים המדינתיים על תקיפות סייבר חמורות ולפעול בהתאם להנחיותיהם בעת תקיפות אלו. אולם במשך יותר מעשור לא השלים משרד רה"ם את הפעולות לצורך חקיקה בכנסת של חוק ייעודי להסדרת התחום למרות היבטים אלה: (א) התקבלו כמה החלטות ממשלה בנושא בשנים 2011 - 2021 (החלטות ממשלה - 3611, 2444,2443 , 219) (ב) בהשוואה בין-לאומית בנושא חקיקה לאומית להגנת הסייבר שביצע מערך הסייבר בחמש מדינות (בריטניה, גרמניה, אוסטרליה, הולנד וארצות הברית) עלה כי ישראל נמצאת בפיגור ניכר מבחינת מצב אסדרת הסייבר ביחס למדינות שנסקרו (ג) מספר דוחות מבקר המדינה שנכתבו בשנים האחרונות[37] העלו פער בנושא קידום חוק הסייבר בישראל.**


**בשנים 2022 - 2025 פעל מערך הסייבר עם גופים נוספים לגיבוש טיוטת חוק סייבר חדש. לאחר פרוץ המלחמה, בינואר 2024, ולנוכח התגברות תקיפות הסייבר במרחב האזרחי והסיכון לפגיעה משמעותית ביותר בביטחון הלאומי של מדינת ישראל וכן לנוכח מרכיבו הקריטי של מרחב הסייבר בשימור חופש הפעולה בלחימה ובתפקוד המשק בשעת חירום וברציפות התפקודית של שירותים חיוניים בזמן שגרה, הנחה אותו ראש הממשלה, מר בנימין נתניהו, להגיש לאישור ועדת השרים לענייני חקיקה תזכיר חוק סייבר בתוך שלושה חודשים (אפריל 2024). למרות הפעולות הרבות שביצע מערך הסייבר יחד עם גופים נוספים לקידום החוק, נכון ליוני 2025 טרם הסתיים הליך גיבוש הצעת החוק[38], טרם לובנו כלל המחלוקות שעלו על ידי המשרדים השונים ואף לא נקבעו לוחות זמנים להגשת הצעת החוק.**

בתשובת מל"ל נמסר כי מערך הסייבר אמון על הנושא ואחראי לגבש ולקדם את הצעת החוק. בהתאם להנחיית ראש הממשלה התקיימו כמה פגישות משותפות של מל"ל עם מערך הסייבר כדי לנסות לסייע לו לקדם את טיוטת תזכיר החוק. לדבריו עד נובמבר 2024 מערך הסייבר לא ביקש את הסיוע של מל"ל היות והתקדם בשיח ישיר מול המשרדים והגופים הרלוונטיים. בהתאם להתקדמות הטיפול של מערך הסייבר עם הגופים ולפי בקשתו קיים מל"ל שתי פגישות ליישוב מחלוקות בדצמבר 2024 ובפברואר 2025 וכן פגישה נוספת בנובמבר 2025. בנוסף ציין שפעל יחד עם מס"ל לשקף לרה"ם את הצורך בקידום החוק, אולם מיוני 2023 לא התקיימו דיונים עם רה"ם בנושא.

בתשובת מערך הסייבר נמסר כי הוא ממשיך להשקיע תשומות משמעותיות להשלים את גיבוש הצעת החוק בהקדם האפשרי, וכי הוא מקיים פגישות בנושא בדרג מקצועי ובדרגי מנכ"ל של

---

37 מבקר המדינה, דוח שנתי בנושא סייבר ומערכות מידע (2022), "הגנת הסייבר במגזר התחבורה", עמ' 57 - 58, ודוח שנתי 69ב (2019), "היערכות גופים חיוניים להגנת הסייבר", עמ' 6 - 7.

38 לאחר פרוץ המלחמה קידם מערך הסייבר את חקיקת חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה - חרבות ברזל), התשפ"ד-2023 (נכנס לתוקף ב-6.12.23. תוקפו במקור נקבע לשבעה חודשים והוא הוארך בתקופת המלחמה מעת לעת).

משרדי הממשלה רלוונטיים וגופים נוספים. עוד נמסר בתשובתו כי לוחות זמנים להשלמת קידום החוק ייקבעו לאחר כניסתו של ראש המערך החדש לתפקיד במאי 2025.

**על ראש מערך הסייבר להשלים בהקדם את הכנת הצעת חוק הסייבר ולפעול יחד עם מל"ל ליישוב המחלוקות, זאת בהתאם להנחיית רה"ם. כמו כן מומלץ כי ראש הממשלה, מר בנימין נתניהו, יעמוד על קידום תזכיר חוק הסייבר בהקדם ובהתאם להנחיותיו.**

בתשובת מגזר 3 נמסר כי הוא תומך בקידום חוק הסייבר באופן שיקנה ליחידות המגזריות את הסמכויות לממש את אחריותן, ויפה שעה אחת קודם.

**לאור הכוונה להרחיב את סמכויות יחידות הסייבר המגזריות במסגרת חוק הסייבר, על מערך הסייבר, כמנחה המקצועי שלהן, לפעול כבר עתה לחיזוקן המקצועי והתפקודי, ובכלל זה לפעול מול גורמי הממשלה הרלוונטיים כדי להבטיח שאלו יוכלו לממש את אחריותן כפי שייקבע בחוק החדש - אם ינוסח ויתקבל.**

## <u>איום ותרחיש ייחוס לאומי בתחום הסייבר</u>

### איום ותרחיש ייחוס לאומי

**איום ותרחיש ייחוס מצרפי:** כאמור, בהחלטת הממשלה ב/43[39] מדצמבר 2007 נקבע כי תוקם רשות חירום לאומית שנועדה לשמש גורם מתאם ומתכלל של כלל הארגונים המטפלים בעורף בשעת חירום. בהחלטה נקבע כי אחד מתפקידיה של רח"ל הוא להכין ולהציג לאישורה של הממשלה, באמצעות שר הביטחון, את איום הייחוס ותרחיש הייחוס המצרפי (ניתוח האיומים והשפעתם הכוללת על המרחב האזרחי לרבות בתחום הסייבר). אישור איום הייחוס מתבצע בוועדת מל"ח עליונה בראשות שר הביטחון, ולאחר מכן איום הייחוס מועבר לאישור ועדת השרים לענייני ביטחון לאומי.

במסמך איום הייחוס המצרפי ("איום הייחוס הלאומי הרב שנתי למרחב האזרחי"), שמגבשת רח"ל בהתאם להחלטת הממשלה ב/43, מוגדרים מצרף האיומים המרכזיים (פעילות עוינת, אסונות טבע, תאונות, תקלות) על העורף, והוא משמש הבסיס לבניין הכוח ולהיערכות העורף לאיומים אלו. מטרתו לאפשר לממשלה לקבוע באופן ברור סדרי עדיפויות לעניין בניין הכוח, להכנתם ולהיערכותם של הגופים לקראת אירוע חירום, להיערכות ולתיאום בין-ארגוניים ולחלוקת משאבים ברורה המתבססת על ההחלטה. המסמך מחייב את הגורמים המכותבים להיערך לכתוב בו, ואת המוסדות השלטוניים לקבוע לפיהם את עיקרי האיומים הרלוונטיים עבורם ולגבש תרחישי ייחוס ענפיים שישמשו בסיס לבניין הכוח ולהיערכות שלהם - למשל מסמכי תרחיש ייחוס מצרפי למתאר מלחמה.

לדברי רח"ל, איום ותרחיש ייחוס מצרפי נקבעים לחמש שנים כיוון שכל שינוי בהם מחייב השקעה לא מבוטלת של הגופים הרלוונטיים בביצוע ההתאמות בתוכניות העבודה הרב-שנתיות שלהם. בתחום הסייבר קבעה רח"ל כי איום הייחוס ייקבע לתקופה של שלוש שנים בלבד, וזאת בשל השינויים התכופים וההתקדמות הטכנולוגית המהירה האופיינית בסייבר. בשני המקרים יש לתקף את איומי ותרחישי הייחוס אחת לשנה כדי להבטיח שאין שינוי מהותי או איום חדש שנדרש להיערך אליהם. למשל, לאחר פרוץ מלחמת חרבות ברזל פרסמה רח"ל עדכון למסמך איום הייחוס המצרפי עקב שינוי הפרדיגמה וההבנה שהמלחמה תהיה ארוכה.

איום הסייבר הוא אחד האיומים העיקריים שרח"ל מיפתה כמשפיעים על החוסן הלאומי ועלולים לגרום למצב חירום לאומי. לפיכך, בעבודת מטה משותפת שביצעה רח"ל עם מערך הסייבר שולב פרק סייבר במסמכי איום הייחוס המצרפי לשנים 2016 - 2020, לשנים 2021 - 2025 ובמסמכי

39 ועדת שרים לביטחון לאומי מתאריך 19.12.07.

תרחיש הייחוס המצרפי למתאר מלחמה (״תרחיש הייחוס המצרפי הרב-שנתי למתאר מלחמה למרחב האזרחי״) של אותן השנים.

**איום ותרחישי ייחוס לאומי בסייבר:** כאמור בהחלטת הממשלה 3611 מאוגוסט 2011[40] הוטל על המטה הקיברנטי הלאומי (לימים מערך הסייבר) אשר הוקם על פי ההחלטה במשרד ראש הממשלה וכפוף ישירות לראש הממשלה, לקבוע ולתקף מדי שנה את איום הייחוס הלאומי להגנה על ממד הסייבר ולהעלות את המודעות הציבורית לאיומים בממד הסייבר ולדרכי ההתמודדות עימם. כמו כן, לפי הנחיות מסמך האיום המצרפי, מערך הסייבר היה צריך לזהות ולקבוע את עיקרי האיומים הרלוונטיים ולגבש תרחישי ייחוס לתחום הסייבר שישמשו בסיס לבניין הכוח ולהיערכות שלו ושל הגופים הכפופים להנחייתו.

**לדברי מערך הסייבר, איום הייחוס הלאומי בסייבר נכתב לפני שנים רבות.**

בעקבות הנחיית ראש מערך הסייבר דאז, גיבש מערך הסייבר בדצמבר 2022, טיוטת איום ייחוס לאומי בסייבר בשיתוף פעולה עם גופי ביטחון ממלכתיים שעוסקים בהגנה לאומית בסייבר.

ראש מערך הסייבר דאז אישר את איום הייחוס הלאומי בסייבר בספטמבר 2023, כחודש לפני המלחמה.

שב״כ מגבש מדי שנה בשיתוף יחידות נוספות שאמונות על כך את איום הייחוס של היריב (גורמים עוינים). לאחר גיבושו, נקבעות בהתאם ההנחיות הרלוונטיות ומועברות בין היתר לגופי התמ״ק המונחים על ידו.

בתשובת מערך הסייבר נמסר כי הוא מקיים פגישות עבודה שוטפות עם ראש הממשלה, המזכיר הצבאי, רח״ל, פורום מנכ״לים וגורמים נוספים, ובהן הוצגו תמונת מצב ההגנה במשק ועיקרי תמונת המודיעין, לרבות במהלך מלחמת חרבות ברזל. כמו כן המערך מסר כי הוא מקיים הערכת מודיעין שנתית והציג את עיקרי איום הייחוס במופעים שונים בתוך מערך הסייבר, ליחידות המגזריות ולגופים מונחים. המערך פועל לתיקוף איום הייחוס בהתאם ללקחי המלחמה ויפעל לתקפו לאחר מכן אחת לשנה.


**עוד נמצא כי היחידה הסקטוריאלית במערך הסייבר, שתפקידה להנחות גופים מסוימים ואת יחידות הסייבר המגזריות, פעלה לאורך השנים האחרונות ללא איום ותרחישי ייחוס שאמורים לשמש מצפן למילוי תפקידה מול הגופים המונחים ולא השתמשה באיום הייחוס הלאומי שגיבש מערך הסייבר בעבודת ההנחיה שלה מול הגופים. נוכח זאת הגופים לא הונחו לפני המלחמה או במהלכה להתייחס בניתוח הסיכונים שלהם לאיומים הלאומיים האסטרטגיים שנקבעו באיום הייחוס בתחום הסייבר ולמקד את תוכניות העבודה ואת השקעת המשאבים שלהם בהתאם לכך.**

**לנוכח העובדה שבמהלך השנים מערך הסייבר לא תיקף את איום הייחוס הלאומי כמתחייב בהחלטת ממשלה 3611, על מערך הסייבר להקפיד לתקף ולאשר את איום הייחוס הלאומי שגיבש נוכח האיומים החדשים שעלו במלחמה בשיתוף רח״ל, שב״כ ויתר הגופים האסדרתיים המדינתיים ולהפיצם לגופים ולממשלה. כמו כן עליו להציג את איום הייחוס הלאומי לראש הממשלה מדי שנה.**

**איום ותרחישי ייחוס מגזריים**

לפי החלטת הממשלה 2443, מערך הסייבר הוא המנחה המקצועי של יחידות הסייבר המגזריות. כמו כן, בהחלטת הממשלה 2444 נקבע כי בין יתר תפקידי מערך הסייבר עליו לנהל, להפעיל ולבצע בהתאם לצורך את כלל מאמצי ההגנה האופרטיביים ברמה הלאומית במרחב הסייבר, בתפיסה

[40] www.gov.il/he/departments/policies/2011_des3611 (נספח א׳, סעיף 2 ה).

מערכתית, לטובת מענה הגנתי שלם ורציף על תקיפות סייבר, וכן לבנות ולחזק את החוסן של כלל המשק בסייבר באמצעות היערכות, כשירות ואסדרה, ובכלל זה העלאת הכשירות של מגזרים וגופים במשק, הנחיית המשק בתחום הגנת הסייבר, וכלים נדרשים נוספים.

לכל מגזר יש איום ותרחישי ייחוס סייבר שרלוונטיים לו בהתאם לפעילותו, למערכות ולארכיטקטורה הייחודיות שהוא מפעיל. איום ייחוס מגזרי בתחום הסייבר מדרג את מכלול איומי הסייבר המכוונים לפגיעה בתשתיות ובפעילויות הייחודיות של גופים במגזר לפי סיכויי התממשותם, והוא מאפשר לגופים במגזר למקד את מאמצי בניין הכוח, תוכניות העבודה והמשאבים בהגנה מפני איומי הסייבר המגזריים.

כמנחה המקצועי של יחידות הסייבר המגזריות, ראש אגף הנחיה סקטוריאלית במערך הסייבר מפרסם מדי שנה ליחידות הסייבר המגזריות את העוגנים לתכנון תוכניות העבודה לשנה העוקבת. מטרת העוגנים היא לסנכרן את העשייה הרוחבית בכל היחידות המגזריות ולאפשר את מדידת האפקטיביות והבשלות של היחידה המגזרית. ברשימת העוגנים שראש האגף פרסם ליחידות הסייבר המגזריות עבור השנים 2022, 2023 ו-2025 הוגדר העוגן הגדרת/כתיבת איום ייחוס מגזרי.

בתשובת רח"ל נמסר כי עקב חומרת איום הסייבר היא החליטה לסייע למערך הסייבר בגיבוש תרחישי איום מגזריים ונערכה לכך בתוכנית העבודה. בהתאם לתוכנית, רח"ל החלה בעבודת מטה לכתיבת איום ותרחישי ייחוס, ואף העסיקה לצורך כך יועץ מומחה בתחום. פריצת מלחמת חרבות ברזל באוקטובר עיכבה את תחילת העבודה. התהליך התבצע בשיתוף פעולה של רח"ל עם מערך הסייבר, עם המשרד הממשלתי האחראי למגזר ועם גורמים נוספים. הגורמים המאשרים שגם חותמים על האיום והתרחיש המגזרי הם: ראש מערך הסייבר - שהוא הגורם המנחה בתחום הסייבר; ומנכ"ל המשרד שאחראי למגזר - שהוא הגורם האחראי והמוסמך על פי דין והגורם שעליו חלה החובה להיערך להם.


**נמצא כי במהלך השנים שקדמו לפרוץ מלחמת חרבות ברזל יחידות הסייבר המגזריות ומערך הסייבר לא סיכמו ואישרו את איומי הייחוס ותרחישי הייחוס בתחום הסייבר של כל המגזרים שפועלים במסגרתם מאות גופים חיוניים אף שבשנים 2022 ו-2023 מערך הסייבר הנחה את היחידות לעשות זאת. עקב כך הגופים החיוניים שבכל מגזר לא הונחו למקד את תוכניות העבודה והשקעת המשאבים בהגנה מפני איומי ותרחישי הייחוס הרלוונטיים.**


**עוד נמצא כי הפעולות להכנה של איומי ותרחישי ייחוס מגזריים על ידי מערך הסייבר, רח"ל ויחידות הסייבר המגזריות, החלו בפועל רק לאחר פרוץ מלחמת חרבות ברזל, ונכון ליוני 2025, כשנה וחצי אחרי פרוץ המלחמה, עדיין לא הושלמו.**

**משרד מבקר המדינה מעיר למערך הסייבר כי לפי החלטות הממשלה 2443 ו-2444 הוא המנחה המקצועי של יחידות הסייבר המגזריות ועליו לבנות ולחזק את החוסן של כלל המשק בסייבר לרבות העלאת הכשירות של מגזרים וגופים במשק. לפיכך עליו להנחות את היחידות המגזריות, לפקח על יישום הנחיותיו ולסייע להן בין היתר בגיבוש איום ותרחישי ייחוס מגזריים. כמו כן הצורך בפעולתו בתחום איומי הייחוס המגזריים הינו יסודי ונחוץ כהמשך לתפקידו בגיבוש איומי ותרחישי הייחוס הלאומיים.**

**מומלץ כי מערך הסייבר ויחידות הסייבר המגזריות יגבשו תוכנית עבודה להשלמת גיבוש איומי הייחוס בכל המגזרים. עוד מומלץ כי מערך הסייבר ינחה את יחידות הסייבר המגזריות לתקף את איום הייחוס ותרחישי הייחוס המגזריים מדי שנה לנוכח השינויים הטכנולוגיים התכופים בתחום הסייבר וכדי לוודא שאין איום חדש שנדרש להיערך אליו. עוד מומלץ כי הוא ינחה אותן לעדכן אחת לשלוש שנים את האיומים ותרחישי הייחוס, יפקח על כך ובמידת הצורך יסייע להן בתהליך. זאת ועוד, מומלץ כי מערך הסייבר ויחידות הסייבר המגזריות יציגו מדי שנה את איומי**

**הייחוס ותרחישי הייחוס המגזרים העדכניים בפני השרים שאחראים לכל מגזר ולפני הפורום המדיני שיקבע.**

☆

**במהלך השנים מערך הסייבר לא תיקף את איום הייחוס הלאומי כמתחייב בהחלטת ממשלה 3611. הפעולות להכנה של איומי ותרחישי ייחוס מגזריים על ידי מערך הסייבר, רח"ל ויחידות הסייבר המגזריות החלו בפועל רק לאחר פרוץ מלחמת חרבות ברזל, ונכון ליוני 2025, כשנה וחצי אחרי פרוץ המלחמה, עדיין לא הושלמו.**

**על מערך הסייבר להקפיד לתקף ולאשר את איום הייחוס הלאומי שגיבש נוכח האיומים החדשים שעלו במלחמה - בשיתוף רח"ל, שב"כ ויתר הגופים האסדרתיים המדינתיים לרבות יחידות הסייבר המגזריות. בנוסף על מערך הסייבר ויחידות הסייבר המגזריות להשלים את גיבוש איומי הייחוס בכל המגזרים ולהנהיג תהליכי עבודה סדורים ושנתיים לעדכון ולתיקוף של איומי ותרחישי הייחוס הלאומיים והמגזריים, לשקפם מדי שנה לפני ראש הממשלה, לפני השרים שאחראים לכל מגזר ולפני הקבינט מדיני-ביטחוני או ועדת שרים ייעודית שתופקד על הנושא ולהטמיעם בגופים.**

## התפיסה הלאומית לטיפול במצבי חירום ובמשבר בממד הסייבר

בהחלטת הממשלה 3611 מאוגוסט 2011 נקבע כי אחד מתפקידי המטה הקיברנטי הלאומי (כיום מערך הסייבר) הוא לגבש תפיסה לאומית לטיפול במצבי חירום בממד הסייבר. כמו כן, בהחלטת ממשלה 2444 מפברואר 2015 נקבע כי תפקיד מערך הסייבר הוא לנהל, להפעיל ולבצע בהתאם לצורך את כלל מאמצי ההגנה האופרטיביים ברמה הלאומית בממד הסייבר, בתפיסה מערכתית, לצורך מתן מענה הגנתי שלם ורציף מול תקיפות סייבר, ובכלל זה טיפול באיומי סייבר ובאירועי סייבר בזמן אמת, גיבוש תמונת מצב שוטפת, ריכוז ומחקר מודיעין ועבודה עם הגופים המיוחדים.

כמענה על החלטות הממשלה 3611 ו-2444 פרסם מערך הסייבר למשק בשנת 2018 מסמך בנושא "תפיסה לאומית בסייבר להיערכות ולניהול מצבי משבר"[41] (להלן - התפיסה הלאומית למשבר סייבר) שנובעת מההבנה כי ההיערכות והניהול של מצבי משבר מחייבים שילוב כוחות, תיאום ושיתוף פעולה ברמה הלאומית. התפיסה היא המלצה לכלל המשק, וקהל היעד הנוסף שהוגדר בה הוא משרדי הממשלה, רגולטורים וארגונים ממלכתיים (למעט הגופים המיוחדים - צה"ל, משטרת ישראל, שב"כ, המוסד ומערכת הביטחון) שמובילים את המאמץ המדינתי להכלת התקיפות והשלכותיהן ומנחים ומכוונים את ארגוני המשק.

**מטרת התפיסה הלאומית למשבר סייבר:** לשמש מסמך יסוד המגדיר עקרונות ודרכים לפעולה בנושא היערכות למצבי משבר וניהולם בממד הסייבר האזרחי:

1. לייצר שפה משותפת ולהיות בסיס להעמקת שיתוף הפעולה והשיח בסייבר בנושא מצבי משבר, הן בין גורמים מדינתיים והן עם גורמים פרטיים.

2. לשמש עבור הארגונים כלי מסדיר ומכוון להקמת תוכנית להיערכות למצבי משבר בתחום הסייבר וניהולם.

3. לסייע להנהלות הארגונים לבחינת מידת ההיערכות הארגונית שלהם למצבי משבר בסייבר ולהתמקד בפערים.

4. לשמש עבור מערך הסייבר ועבור גורמים נוספים בסיס לפיתוח עזרים עתידיים בנושא היערכות למצבי משבר בסייבר וניהולם.

41 www.gov.il/he/departments/news/cybercrisispreparedness

**מעמד מסמך התפיסה הלאומית לניהול משבר סייבר:** מערך הסייבר הגדיר ופרסם את מסמך התפיסה הלאומית למשבר סייבר כמסמך המלצה והוא אינו מסמך מחייב.

## תכולת התפיסה הלאומית למשבר סייבר

לוח 5: **הנושאים העיקריים במסמך התפיסה הלאומית למשבר סייבר**

| | | |
|---|---|---|
| 1. | חשיבות מיפוי נכסי סייבר חיוניים ואופן מיפוים ברמה הארגונית וברמה הלאומית | |
| 2. | הגדרת מצבי הכוננות בסייבר ועקרונות לשינוי הכוננות | |
| 3. | עקרונות מרכזיים להיערכות ארגון למצבי משבר: | |
| | א. ידע מקצועי | • הטמעת התפיסה הלאומית למשבר סייבר.<br>• הטמעת תורת ההגנה בסייבר לארגון שפותחה במערך הסייבר<br>• הסתייעות בתורות, בנהלים ובשיטות עבודה מומלצות להיערכות למצבי משבר בתחום הסייבר ולניהולם |
| | ב. כוח אדם | • הקמת צוות הנהלה לניהול משבר סייבר<br>• הקמת צוות טכנולוגי לטיפול באירוע<br>• תכנון וטיפול הצבות כוח אדם בחירום, לרבות ריתוק משקי<br>• גיבוש עתודת מומחי סייבר לסיוע בעיתות שגרה וחירום |
| | ג. הצטיידות בטכנולוגיות ובאמצעים | • הצורך של ארגון להצטייד בטכנולוגיות ובאמצעים להעלאת רמת ההגנה בסייבר |
| | ד. הסתייעות בגורמים חיצוניים | • כלים מקצועיים של מערך הסייבר וגופי האסדרה השונים<br>• שירותים שניתנים על ידי חברות פרטיות |
| | ה. חשיבות ההכשרה והתרגול | גיבוש תוכנית הכשרות ותרגול שנתית להתמודדות הארגון במצבי משבר בסייבר. |
| 4. | אופן ניהול משבר סייבר | • מחזור חיים של אירוע סייבר<br>• תפיסת הניהול של אירוע סייבר בארגון<br>• פעולות בניהול משבר סייבר לפי מצבי כוננות |
| 5. | שאלון למיפוי נכסי הסייבר החיוניים | טבלה לסיוע במיפוי נכסי הסייבר התומכים בתהליכי הליבה והדורשים רמת הגנה גבוהה בסייבר |
| 6. | הערכת מצב בתחום הסייבר | טבלת נושאים לדיון בהערכת מצב בעקבות אירוע סייבר |
| 7. | "שאלון מידת היערכות למצבי משבר" | כלי עבודה שנועד לשמש את הנהלת הארגון לבחינת מידת ההיערכות הארגונית למצבי משבר בסייבר ולמיקוד הטיפול בפערים. |

על פי מסמך התפיסה הלאומית למשבר סייבר שפרסם מערך הסייבר, בעיבוד משרד מבקר המדינה.

במהלך השנים פרסם מערך הסייבר מדריכים והנחיות משלימות בנוגע להיערכות הארגונים ולמוכנותם להתמודדות עם אירועי סייבר ואירועי משבר. להלן דוגמאות למסמכים אלו.

לוח 6 : **דוגמאות למדריכים ולהנחיות משלימות שפרסם מערך הסייבר, 2018 - 2023**

| | |
|---|---|
| **2018** | מוכנות הארגון למשבר סייבר[42], אפיון ודרישות מצוות ניהול משבר ומצוות IR[43] |
| | היערכות והתמודדות עם אירוע כופרה (Ransomware) בארגון - דרכי פעולה מומלצות[44] |
| | מה לעשות במקרה של תקיפת סייבר? המדריך המלא למשתמש הביתי[45] |
| **2020** | בניית תוכנית היערכות לחירום וניהול משבר סייבר |
| | כיצד תוכלו לזהות במהירות הודעת דיוג[46] |
| **2021** | כיצד תוכלו להגן על הארגון שלכם ממתקפות פישינג?[47] |
| **2022** | תרגול בסייבר- בנייה ועריכה של תרגילי סייבר לארגון[48] |
| **2023** | רשימת תיוג לבחינת מוכנות ארגונית לתקיפת סייבר מסוג DDoS[49] |

המקור : מסמכים ופרסומים של מערך הסייבר הלאומי.

אירוע סייבר משמעותי עלול לפגוע קשות ברציפות התפקודית של כל ארגון, בתקינות ובשלמות של השירותים שהוא מספק, במוניטין ובנכסים שלו ואף לסכן את המשך קיומו. לכן כמו בכל משבר אחר שאליו ארגון עלול להיקלע, האחריות לניהול משבר סייבר מוטלת בראש ובראשונה על הנהלת הארגון שצריכה להתמודד עם ההשלכות שלו בהיבטים השונים - הארגוניים, הטכנולוגיים, העסקיים, הכלכליים, המשפטיים, הבטיחותיים, והתדמיתיים ולעמוד בקשר עם גופים שונים (פרטיים ומדינתיים) כדי למנוע התפשטות של האירוע, להכיל אותו, להתאושש ממנו ולחזור לשגרה.

**בפגישות שקיים צוות הביקורת עם ארגונים בתחומים מסוימים שחוו אירועי סייבר עלה כי בעת הטיפול באירוע היו סוגיות שנדרש היה לקבל החלטה בעניינן, אולם אין הנחיה סדורה לארגון ואין קווים מנחים ודרכי פעולה מומלצות ולא הוגדר הגורם המוסמך המדינתי לבצע כל פעולה.**

האחריות הממלכתית להגנה על ממד הסייבר הישראלי נחלקת בין כמה גופים אסדרתיים מדינתיים, כאשר מדובר באירועים משמעותיים יכולים לפעול מול הארגון הנתקף כמה גופים מדינתיים שיפעלו בהתאם לתפקידם, לסמכותם ולמיקוד של כל אחד מהם.

יצוין כי באירועי סייבר משמעותיים, בעיקר בעלי היבטים ביטחוניים או בעלי סיכון להשפעה על הביטחון הלאומי, מתקיים מנגנון לשיתוף פעולה וידע בין גופי האסדרה הביטחוניים למערך הסייבר לצורך הכוונת הפעילות האופרטיבית שלהם בעת הטיפול האירוע ולשם מניעת פעילויות מנוגדות במרחב. גופים מסוימים אינם נכללים במנגנון זה.

באירוע מסוים שבו נפגעו מספר גופים, כל גוף שנפגע נדרש לפעול עצמאית כדי לטפל בהשפעות האירוע על המערכות שלו ולסגור את הפערים שהיו. אולם לא היה גורם אסדרתי מדינתי שריכז את הנושא.


**אף שבהחלטת הממשלה 3611 מאוגוסט 2011 נקבע כי אחד מתפקידי מערך הסייבר הוא לגבש תפיסה לאומית לטיפול במצבי חירום בממד הסייבר נמצא כי מערך הסייבר לא עדכן שנים רבות את מסמך "התפיסה הלאומית לניהול משבר סייבר" ותכולתה חסרה במספר היבטים: היא אינה כוללת התייחסות למדריכים והרחבות בנושא מוכנות ארגונים לתקיפת סייבר שפרסם המערך בשנים 2018 - 2023; היא אינה**

42 www.gov.il/he/departments/news/cybercrisisforir
43 צוות תגובה טכנולוגי לאירוע סייבר (IR Incident Response).
44 www.gov.il/he/departments/general/rasomware_org
45 www.gov.il/he/Departments/General/fishingemails
46 www.gov.il/he/Departments/General/fishingemails
47 www.gov.il/he/departments/general/defend_your_organisation
48 www.gov.il/he/Departments/General/cyberexercise
49 www.gov.il/he/departments/general/ddos

**מפרטת את כל הגופים האסדרתיים המדינתיים בתחום הסייבר, את הסמכויות, תחומי האחריות והממשקים ביניהם; אין בתפיסה התייחסות לסוגיות שהעלו לפני צוות הביקורת ארגונים מסוימים שחוו בשנים האחרונות אירועי סייבר משמעותיים.**

בתשובת מגזר 6 נמסר כי יש נושאים נוספים שחסרים לגביהם מסמכי הנחיה בנושא התפיסה הלאומית לניהול משבר סייבר.

**על מערך הסייבר לעדכן את מסמך התפיסה הלאומית כנדרש בהחלטת הממשלה 3611 ולהשלים בה את הנושאים החסרים ואת התובנות העיקריות שעלו בשנים האחרונות מאירועי סייבר משמעותיים.**

**שימוש בתפיסה הלאומית על ידי קהל היעד שהוגדר:** כאמור, קהל היעד שהוגדר לתפיסה (בנוסף לכלל המשק) הוא משרדי הממשלה, רגולטורים וארגונים ממלכתיים שמובילים את המאמץ המדינתי להכלת התקיפות והשפעותיהן ומנחים ומכוונים את ארגוני המשק. למעט צה"ל, משטרת ישראל, שב"כ, המוסד ומערכת הביטחון. לדברי מערך הסייבר, הוא אינו מבצע מעקב אחר מידת השימוש במסמך התפיסה הלאומית ובשאלון אלא מנגיש אותם לכל הגורמים המקצועיים בארגון, והאחריות לעניין השימוש עצמו וכן ההחלטה בדבר השימוש בכלי הן בידי הארגון.

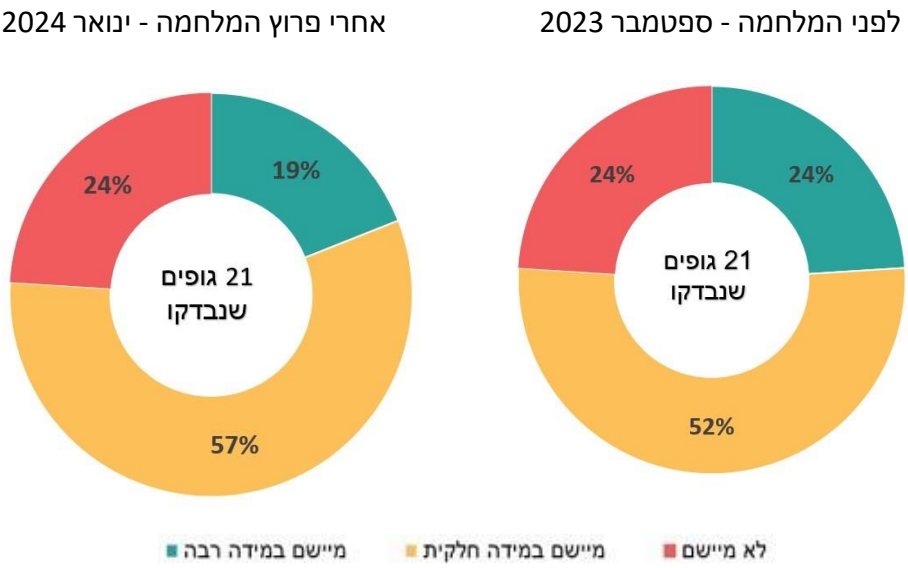
מערך הסייבר לא הנחה את היחידות המגזריות לפעול לפי התפיסה הלאומית לניהול משבר סייבר ולכן הן שילבו חלקים ממנה במסמכי הנחיות שלהם אבל לא הנחו את הגופים במפורש להשתמש בה. כמו כן גופי התמ"ק אינם מונחים לפעול לפי התפיסה הלאומית לניהול משבר סייבר כיוון שהם פועלים לפי מתודולוגיה ייעודית. כמו כן הרשות להגנת הפרטיות אינה משתמשת בתפיסה הלאומית לניהול משבר סייבר אלא פועלת על פי תפיסות הפעלה משלה.


**נמצא כי יה"ב ויחידות הסייבר המגזריות ממעטות להשתמש במסמך התפיסה הלאומית למשבר סייבר שגיבש מערך הסייבר בהתאם להחלטות ממשלה 3611 ו-2443, ומערך הסייבר לא הנחה את היחידות המגזריות לפעול לפי התפיסה, גם לא בתקופת המלחמה והן ממעטות להשתמש בה. כמו כן, הרשות להגנת הפרטיות אינה עושה בה שימוש.**

בתשובת מערך הסייבר מאפריל 2024 נמסר כי במהלך המלחמה הופצו ליחידות המגזריות הנחיות והמלצות ייחודיות להעלאת רמת הכוננות ולביצוע פעולות להעלאת חוסן שתואמות לאמירות המובאות במסמך התפיסה הלאומית בנושא משבר סייבר. עוד נמסר כי בהמשך לשיח עם משרד מבקר המדינה בנושא, יסב מערך הסייבר את תשומת ליבן של היחידות המגזריות למסמך שבאתר.

משרד מבקר המדינה בחן, באמצעות שאלונים שהפיץ ל-21 גופים בעלי חשיבות למשק, את מידת השימוש שלהם במסמך התפיסה הלאומית לניהול משבר סייבר לפני המלחמה וכן לאחר פרוץ המלחמה.

תרשים 8 : **מידת השימוש במסמך התפיסה הלאומית למשבר סייבר לפני המלחמה ובתקופת המלחמה**




על פי מענה הגופים על השאלונים, בעיבוד משרד מבקר המדינה.

**נמצא כי מערך הסייבר לא ביצע בשנים האחרונות פעולות להטמעה, לפרסום או לבדיקה של מידת השימוש במסמך התפיסה הלאומית לניהול משבר סייבר לרבות בתקופת מלחמת חרבות ברזל. וכי התפיסה אינה מונגשת לציבור באופן בולט באתר המרשתת (אינטרנט) של מערך הסייבר. עוד נמצא כי לפני מלחמת חרבות ברזל ואף בחודשים הראשונים לאחר שפרצה, חמש (24%) מתוך 21 הגופים שנבדקו בשאלון דיווחו כי הם לא מיישמים כלל את התפיסה הלאומית למשבר סייבר וכ-52% -57% מהגופים יישמו את התפיסה באופן חלקי.**

**מומלץ כי מערך הסייבר יעדכן, בשיתוף גורמים אסדרתיים מדינתיים נוספים, את התפיסה הלאומית למשבר סייבר, כנדרש בהחלטת הממשלה 3611 משנת 2011, כתפיסה מחייבת ואחודה עבור הגופים המונחים שלו וכי התפיסה תהיה בגדר המלצה לכלל המשק. עוד מומלץ כי התפיסה תכלול התייחסות מלאה לכלל ההיבטים העדכניים הכרוכים במוכנות הלאומית למשברי סייבר ובכלל זה תפרט את הגופים האסדרתיים המדינתיים, את תפקידם בהתרחש אירוע, את הממשקים ואת מנגנון קבלת ההחלטות ביניהם, וכי מערך הסייבר יפעל להטמיע תפיסה זו, לתרגלה ולבססה כתורה מקצועית שעל פיה ייערכו כלל הגופים במשק.**

## אסטרטגיה לאומית לפשיעת סייבר ופרויקט מתפ"ס (מרכז תיאום פשיעת סייבר)

בשנים האחרונות חל גידול משמעותי בהיקף מתקפות הסייבר המבוצעות ממניעים כלכליים, העלות המוערכת של פשיעת סייבר בעולם בשנת 2023 הייתה כ-8 טריליון דולר, גידול של כ-15% לעומת שנת 2022[50]. נוסף על כך כ-72% מהארגונים בעולם הושפעו בשנת 2023 מאירועי סייבר.

בדיון שקיים ראש חטיבת סייבר במל"ל באפריל 2022 סוכם כי פשיעת סייבר חמורה היא איום ממשי על הביטחון הלאומי, בשל הנזק הכספי המצרפי שנגרם בגללה למשק הישראלי ובשל השחיקה שהיא גורמת לאורך זמן ברציפות התפקודית, בחוסן הכלכלי, ביכולת להגן על הפרטיות ובאמון הציבור בשלטון החוק. כדי למזער את הסיכון, את היקף מתקפות הסייבר הכלכליות ואת

[50] www.statista.com/forecasts/1280009/cost-cybercrime-worldwide

הנזק הכלכלי שהן גורמות ברמה הלאומית הוסכם לקדם שתי יוזמות שיתכלל מערך הסייבר, האחת - גיבוש אסטרטגיה לאומית להתמודדות עם פשיעת סייבר ומתקפות סייבר ממניעים כלכליים, והשנייה - הקמת מרכז תיאום פשיעת סייבר (להלן - צוות מתפ"ס).

**אסטרטגיה לאומית להתמודדות עם פשיעת הסייבר:** לצורך גיבוש האסטרטגיה הוסכם על שיתוף פעולה של כלל הגופים בתחומים הרלוונטיים (מידע, טכנולוגיה, מודיעין, רגולציה, חקיקה ומשפט) ועל הקמת שלושה צוותי עבודה בנושאים האלה: קידום חוסן ומניעה בממד הסייבר הישראלי למול מתקפות פשיעת סייבר; התמודדות עם מתקפות, לרבות טיפול באירוע והכלתו, הדיווח עליו והחזרת יעדי המתקפה לרציפות תפקודית; התמודדות עם תוקפים. עוד סוכם כי מערך הסייבר הלאומי יתכלל את עבודת המטה הכרוכה באישור המלצות הצוותים, וכי העבודה תסוכם ותועבר עד סוף נובמבר 2022 לאישורם של ראשי מערך הסייבר הלאומי וראש המל"ל.

**לצורך גיבוש אסטרטגיה לאומית להתמודדות עם פשיעת הסייבר הוחלט באפריל 2022 על הקמת שלושה צוותי עבודה בריכוז של מערך הסייבר, וכן הוחלט כי המלצותיהם יסוכמו ויועברו עד לנובמבר 2022 לאישורם של ראש מערך הסייבר וראש המל"ל. נמצא כי עד אוגוסט 2024, רק צוות אחד סיים את עבודתו ואילו יתר שני הצוותים לא סיימו את עבודתם. נוכח זאת מערך הסייבר שהיה אחראי על עבודת המטה ועל הגשת ההמלצות לאישור ראש מערך הסייבר וראש המל"ל, לא השלים פעולות אלו.**

בתשובת מערך הסייבר נמסר כי הוא מכיר בצורך בעדכון עבודת האסטרטגיה בשותפות עם כל בעלי העניין הרלוונטיים.

**הקמת פרויקט מתפ"ס (מרכז תיאום פשיעת סייבר):** במסגרת הפרויקט תוכנן להקים מנגנון לתיאום פעולות של הרשויות נגד הפשיעה החמורה בממד הסייבר הלאומי, שבמסגרתו גופים רלוונטיים ישתפו פעולה בהתמודדות עם אירועים רלוונטיים משמעותיים ויפעלו בהתאם לסמכויות, ליכולות המודיעיניות והמבצעיות וליתרונות היחסיים של כל אחד מהם למקסום יכולות המדינה בהתמודדות עם אותם אירועים.

באוגוסט 2022 התקיים דיון התנעה של צוות מתפ"ס, ולאחר מכן החלה פעילות משותפת בין הגופים.

**נמצא כי אף שהוסכם על ידי הגורמים הרלוונטיים כי פשיעת סייבר חמורה היא איום ממשי על הביטחון הלאומי, נמצאו פערים בתיאום פעולות הרשויות כנגד הפשיעה החמורה בממד הסייבר הלאומי.**

**מומלץ כי הגופים הרלוונטיים יפעלו להשלמת הפערים בפעילותו של צוות מתפ"ס באירועי סייבר ובמידת הצורך יצרפו לצוות גם גורמים נוספים.**

☆

**מערך הסייבר לא עדכן במשך שנים רבות את מסמך "התפיסה הלאומית לניהול משבר סייבר" ותכולתה חסרה. בנוסף, מערך הסייבר לא הנחה את הגופים המונחים על ידו להשתמש בה ולא הטמיע אותה בשנים האחרונות ולכן השימוש בה בקרב הגופים המונחים מועט. בנוסף, נמצאו פערים בשיתוף הפעולה בין גופים רלוונטיים להתמודדות עם פשיעת סייבר ומתקפות סייבר ממניעים כלכליים.**

**מומלץ כי מערך הסייבר יעדכן, בשיתוף גופים אסדרתיים מדינתיים נוספים את התפיסה הלאומית למשבר סייבר כתפיסה מחייבת ואחודה עבור הגופים המונחים שלו וכי התפיסה תהיה בגדר המלצה לכלל המשק. עוד מומלץ כי התפיסה תכלול התייחסות להיבטים החסרים בה לרבות פירוט הגופים האסדרתיים המדינתיים, תפקידם בעת אירוע, הממשקים ומנגנון קבלת**

**ההחלטות ביניהם, ויפעל להטמיע תפיסה זו, לתרגלה ולבססה כתורה מקצועית שעל פיה יערכו כלל הגופים במשק.**

## <u>פעולות מערך הסייבר לשיפור ההיערכות והכשירות של יחידות הסייבר המגזריות</u>

כאמור, בהחלטת ממשלה 2443 מפברואר 2015 נקבע כי תוקם יה"ב ויוקמו יחידות סייבר מגזריות שתפקידן לקדם את הטיפול בהיערכות לאיומי סייבר במגזר, וכי הן יפעלו בהנחיה מקצועית של מערך הסייבר. כמו כן, לפי החלטת ממשלה 2444 מפברואר 2015 אחד התפקידים העיקריים של מערך הסייבר הוא לבנות ולחזק את החוסן של כלל המשק בסייבר באמצעות היערכות, כשירות ואסדרה, ובכלל זה העלאת הכשירות של מגזרים וגופים במשק, תקינה, קיום תרגילים ואימונים, מתן תמריצים וכלים נדרשים נוספים.

כאמור, תפקידם של יה"ב ושל יחידות הסייבר המגזריות הוא להכווין את הגופים במגזר שלהן, להנחותם ולסייע להם להעלות את רמת ההגנה שלהם ובכך לשפר את רמת ההגנה של המשק כולו. נוכח זאת חשוב שיחידות הסייבר המגזריות יהיו מקצועיות וחזקות. בביקורת נבדקו פעולות ההנחיה, ההכוונה והסיוע שמעניק מערך הסייבר ליחידות הסייבר המגזריות בעת שגרה, בעת אירוע סייבר ובמהלך מלחמת חרבות ברזל בכמה תחומים:

### שיתוף היחידות המגזריות במודיעין סייבר

מודיעין סייבר הוא מידע לגבי איומי סייבר, חולשות ידועות, התנהגות וכלים של קבוצות תקיפה, ומטרתו לאפשר לגוף לזהות איומים חדשים שרלוונטיים עבורו בהקדם האפשרי, באופן שיאפשר לו להגן על עצמו בעוד מועד.

מערך הסייבר מקבל מידע מודיעיני ממקורות שונים. כמו כן מערך הסייבר מפרסם תובנות והתרעות שונות לגופים המונחים ולמשק.

מערך הסייבר מעביר ליחידות הסייבר המגזריות, במקרים הרלוונטיים ובהתאם לצורך ולשיקול דעתו, מידע מודיעיני באופן שוטף. חלק מהמידע ממוקד ועוזר לסגור חולשות ולעצור התקפות, ועם זאת חלק מהמידע שמעביר מערך הסייבר מותמם, וזאת באופן שלעיתים המידע המותמם אינו מאפשר ליחידה המגזרית לפעול ולמנוע התקפה. כמו כן, מערך הסייבר מקיים הערכות מצב של תמונת המודיעין באופן עיתי. בתקופות שגרה לא הוצגו סקירות מודיעין ליחידות הסייבר המגזריות, ורק בתקופת מלחמת חרבות ברזל הוצגו להן סקירות מודיעין בלתי מסווגות.

**בפגישות שהתקיימו עם שבע מתוך שמונה יחידות סייבר מגזריות ויה"ב עלו פערים בתחום שיתוף במידע מודיעיני, כלהלן:**

1. **הועלו פערים הנוגעים לאופן שבו מערך הסייבר משתף מידע מודיעיני עם יחידות הסייבר המגזריות.**

2. **לפני המלחמה מערך הסייבר לא הציג ליחידות הסייבר המגזריות סקירות מודיעין. במהלך הביקורת ובתקופת מלחמת חרבות ברזל החל מערך הסייבר להציג באופן עתי ליחידות סקירות מודיעין בלתי מסווגות.**

3. **המידע המודיעיני שמערך הסייבר מעביר ליחידות מותמם ולעיתים מועבר ליחידות המגזריות באופן שאינו מאפשר להן טיפול באירוע.**

4. **בכמה מקרים מערך הסייבר דיווח על אירועי סייבר ישירות לגופים מבוקרים של היחידה המגזרית ואף הנחה אותם כיצד לפעול ללא התייעצות עם היחידה המגזרית או ללא שיתופה.**

5. **מערך הסייבר לא הציג ליחידות הסייבר המגזריות את איום הייחוס הלאומי שגיבש.**

בתשובת מערך הסייבר נמסר כי כחלק מתפיסת ההפעלה שלו, מועבר כל מידע מודיעיני רלוונטי באופן ישיר ובלתי אמצעי ליחידה המגזרית הרלוונטית, ושאר היחידות המגזריות מעודכנות במידת הצורך ובכפוף למגבלות המועברות למערך הסייבר.

בתשובת מגזר 7 נמסר כי המשרד רואה חשיבות עליונה בהקפדה על ערוץ תקשורת מסודר באמצעות היחידה המגזרית כנקודת התיאום היחידה מול הגופים במגזר. זאת כדי למנוע פגיעה במאמצי היחידה המגזרית ליצירת ערוץ תקשורת סדור וממוסד עם גופי המגזר וכדי להבטיח שהגופים ידעו מי הגורם האחראי לניהול האירוע וממי לקבל הנחיות רשמיות.

בתשובת מגזר 10 נמסר כי הוא מקיים שיח עם מערך הסייבר כדי לשפר את שיתוף המודיעין הרלוונטי עבור גופים במגזר בהתחשב בשיקולי ביטחון.

בתשובת מגזר 5 נמסר כי חשוב לפעול ליצירת ממשקי עבודה שוטפים לצורך קבלת מידע מודיעיני רלוונטי למגזר. ללא מודיעין איכותי יש קושי לפעול ולהיערך כנדרש.

בתשובת מגזר 2 נמסר כי החל מינואר 2023 מערך הסייבר משתתף בפורום אופרטיבי חודשי של היחידה המגזרית ומעביר במסגרתה סקירה מודיעינית. כמו כן, בנובמבר 2025 מסר המשרד כי שיתוף הפעולה של מערך הסייבר עם היחידה המגזרית בנושא דיווח על אירועי סייבר השתפר ומתקיימים ביניהם שיח ותיאום בנושא.

### פורום מקצועי ליחידות הסייבר המגזריות

בשנת 2023 יזמו והקימו באופן עצמאי ראשי יחידות הסייבר המגזריות פורום מקצועי. מטרת הפורום היא לייצר ליחידות הסייבר המגזריות ערך מוסף מהבחינה המקצועית. הפורום עוסק בתחומים האלו: שיתוף ידע ומודיעין בין היחידות; קידום מעמדו של מנהל אבטחת מידע וסייבר; קיום השתלמויות, כנסים וסיורים ביחידות השונות; פרסום והנגשה של מידע באמצעות מגזינים מקצועיים; דיווחים ישירים ואתר מרשתת של הפורום; השתתפות בתערוכות וכנסים בארץ ובחו"ל; חיזוק שיתוף הפעולה הבין-מגזרי להסרת פגיעויות ולחיזוק הגופים; שיתוף פעולה בין יחידות ה-SOC המגזריות ליצירת ערך לגופים.

משרד מבקר המדינה העביר למערך הסייבר במרץ 2024 את עיקרי הפערים המוצגים בתת-פרק זה. במהלך הביקורת במאי 2024 כינס מערך הסייבר לראשונה פורום של ראשי יחידות סייבר מגזריות שמטרתו שיתוף מידע בין המשתתפים ועדכונם בנושאים מרכזיים. בדיון עלו, בין היתר, הנושאים האלה:

1. הפורום יתכנס אחת לחודשיים.
2. על מערך הסייבר לשתף את היחידות המגזריות בחשיבה, בגיבוש תהליכים ובהערכות מצב.
3. על מערך הסייבר לשכלל את תהליך העבודה בעת חשד לאירוע סייבר.
4. מודיעין - על מערך הסייבר לשתף את יחידות הסייבר המגזריות במודיעין רלוונטי; ישנן פעמים שהפרפרזות לא רלוונטיות.
5. מערך הסייבר יעביר ליחידות הסייבר המגזריות סיכום הערכות מצב.

כמו כן במאי 2024 ערך מערך הסייבר כנס לממוני תמ"ק ולראשי יחידות הסייבר המגזריות בו הציג בין היתר סקירת מודיעין ואת יכולות המערך והכלים הטכנולוגים שהוא יכול לשתף עימם. ממאי 2024 עד סיום עריכת הביקורת ביוני 2025 מערך הסייבר המשיך לכנס את פורום ראשי יחידות מגזריות באופן סדור אחת לחודשיים.

**נמצא כי עד מאי 2024, מערך הסייבר לא פעל לשתף מידע באופן מיטבי עם היחידות המגזריות, ולא הקים קהילה או תשתית לשיתוף ידע מקצועי ומודיעיני בין יחידות הסייבר המגזריות. עקב**

**כך, בשנת 2023 יחידות הסייבר הקימו באופן עצמאי פורום מקצועי שמטרתו חיזוק יחידות הסייבר המגזריות. בעקבות הביקורת במאי 2024 הקים מערך הסייבר פורום מקצועי ליחידות הסייבר המגזריות שמאז מתכנס באופן סדור ומציג לראשי היחידות סקירת מצב מודיעינית ואת הכלים הטכנולוגים שהמערך יכול לשתף עימן.**

**מומלץ כי מערך הסייבר יגבש מחדש את תפיסת העבודה עם יחידות הסייבר המגזריות כשותפות אסטרטגיות וכסוכנות משמעותיות להעלאת רמת ההגנה במשק, ימשיך לכנס את הפורום של יחידות הסייבר המגזריות באופן שוטף, יציג לפניהן את הכלים שפיתח וישתף אותן בצוותי חשיבה. עוד מומלץ כי מערך הסייבר יציג לפניהן סקירת מודיעין מקיפה על האיומים הלאומיים ועל אלו הרלוונטיים לכל מגזר. עוד מומלץ כי מערך הסייבר יגבש דרכים להעשיר ולטייב את המידע המודיעיני שמועבר ליחידות.**

בתשובת מערך הסייבר נמסר כי הוא רואה ביחידות המגזריות שותפות אסטרטגיות וסוכנויות משמעותיות להעלאת רמת ההגנה במשק. הדבר מקבל ביטוי מפורש בהצעת החוק שמקדם מערך הסייבר, ובה הוא מבקש להקנות סמכויות רחבות ליחידות אלו ולחזק אותן במידה ניכרת.

**הנחיה מקצועית של יחידות הסייבר המגזריות על ידי מערך הסייבר:** כאמור, גופי התמ"ק מחויבים לפעול לפי הנחיית מערך הסייבר או לפי שב"כ בהתאם לחוק להסדרת הביטחון, ונוסף על כך מערך הסייבר ושב"כ מנחים אותם בנושאים שונים בהתאם לצורך. כמו כן, לפי החלטת הממשלה 2443 מערך הסייבר הוא הגורם המנחה המקצועי של יחידות הסייבר המגזריות ומשכך מוסמך להפיץ להם הנחיות מקצועיות. אגף הנחיה סקטוריאלית מתאים את ההנחיות שהוא מעביר לגופי תמ"ק ומעביר אותן כהמלצות בלבד ליחידות הסייבר המגזריות.

**נמצא כי באפריל 2023 הפיץ מערך הסייבר לגופי התמ"ק הנחיה בנושא "דיווחים הנדרשים מגופים מונחים" ולא הפיץ הנחיה מקבילה ליחידות הסייבר המגזריות.**

מערך הסייבר לא הגדיר מתודולוגיה אחודה שתשמש בסיס מינימלי מחייב שלפיו יחידות הסייבר המגזריות נדרשות לפעול ולהכווין את הגופים המונחים שלהן אלא פרסם להן המלצה ליישם את תורת ההגנה 2.0. כמו כן, כל ההנחיות שפרסם מערך הסייבר ליחידות הן בגדר המלצה בלבד. לצד זאת, לפי החלטת ממשלה 2443 אחד התפקידים של יחידות הסייבר המגזריות הוא הכוונה והנחיה של הגופים במגזר בהיבטים של הגנת הסייבר, לרבות הגדרת המדיניות. בהיעדר מתודולוגיה אחודה, כל יחידה מגזרית כתבה את כל ההנחיות לגופים המונחים שלה באופן עצמאי בהתאם לצרכיה, ליכולותיה, למשאבים העומדים לרשותה ובהתאם לייחודיות של כל מגזר ושילבה בהן חלקים מהנחיות מערך הסייבר כפי שמצאה לנכון.


**אף שבהחלטת הממשלה 2443 נקבע כי מערך הסייבר הוא המנחה המקצועי של יחידות הסייבר המגזריות, נמצא כי מערך הסייבר אינו מחייב אותן לפעול לפי מתודולוגיה אחודה ולפי הנחיות מחייבות שהוא מוסר להן כדי שישמשו בסיס מינימלי מחייב לכל הגופים המונחים, וכי הנחיותיו ליחידות המגזריות הן המלצות לפעולה. עקב כך כל יחידה מגזרית כתבה והגדירה בעצמה ובהתאם ליכולותיה המקצועיות, למשאביה ולצורכי המגזר את כל ההנחיות והנהלים שלפיהם הגופים במגזר שלה מונחים לפעול במקום להתבסס על הנחיות בסיסיות של מערך הסייבר ולבצע בהן התאמות בהתאם לכל מגזר. למערך הסייבר אין במצב הקיים סמכות לבקר את היחידות על יישום הנחיותיו שניתנו כהמלצות בלבד ואף אין ביכולתו למדוד את מצב המגזרים והמשק בהתאם לנורמה מחייבת ואחודה.**

בתשובת מערך הסייבר נמסר כי בהתאם להחלטת ממשלה 2443 היחידות המגזריות נדרשות ליישם את ההנחיות המקצועיות של המערך. עוד הוסיף המערך כי לתפיסתו גם כאשר מועברות המלצות מקצועיות נדרשות היחידות לבחון את התאמתן למגזר וליישמן בהתאם.

**מומלץ שמערך הסייבר יפעל כבר עתה לעדכון ההנחיות הרלוונטיות כהנחיות מחייבות.**

**השימוש של היחידות המגזריות בכלים ובשירותים שמספק להן מערך הסייבר:** בהחלטת הממשלה 2444 הוטל על מערך הסייבר להקים תשתית טכנולוגית וארגונית לאומית לגילוי, זיהוי, חקירה, התרעה ושיתוף מידע, בנוגע לתקיפות סייבר על מדינת ישראל.

מערך הסייבר מספק כיום ליחידות הסייבר המגזריות כמה כלים ושירותים טכנולוגיים. בשנים 2022 ו-2023 קידם מערך הסייבר הקמה של מגוון כלים ושירותים להגנת הסייבר ברמת המדינה.

מבדיקה שעשה מבקר המדינה מול ראשי יחידות סייבר מגזריות בנושא שימוש בכלים ושירותים שפיתח מערך הסייבר עלו פערים שונים. להלן יוצגו עיקריהם:

1. רשימת הגופים החיוניים (גופי ה-A) שהגדירו היחידות המגזריות שונה מהרשימה שקיימת בידי מערך הסייבר לפיכך יתכן כי המשאבים שמפעיל המערך אינם בהלימה לתיעדוף של היחידה המגזרית.

2. יחידות הסייבר המגזריות לא היו שותפות באיסוף הצרכים של הכלים הטכנולוגיים שמספק מערך הסייבר כך שיתאימו לצרכיהן ולכן יחידות הסייבר המגזריות ממעטות להשתמש בהם.

3. יחידות הסייבר המגזריות אינן מכירות את כלל השירותים שהמערך מספק.


**נמצא כי אין הלימה בין רשימות הגופים החיוניים הנמצאות בידי היחידות המגזריות ובין אלה הנמצאות בידי מערך הסייבר. מכאן משתמע כי המשאבים שמפעיל המערך אינם בהלימה לתיעדוף של היחידה.**

בתשובת מערך הסייבר נמסר כי רשימת הגופים החיוניים נקבעת על ידי היחידות המגזריות. לפיכך אם אין הלימה בין הרשימות במערך הסייבר לרשימות של היחידות המגזריות, על היחידות לעדכן אותו בשינויים. חוסר ההלימה נובע מהיעדר עדכון של היחידות המגזריות לגבי השינויים שנעשו.

בתשובת מגזר 6 נמסר כי הוא מספק ויספק למערך הסייבר כל מידע המצוי ברשותו לצורך עדכון רשימת גופי ה-A במגזר.

**מומלץ כי מערך הסייבר ינחה את היחידות המגזריות לעדכן אותו באופן שוטף בשינויים ברשימת גופי ה-A שלהן ויקיים תהליך עיתי סדור לעדכון ולהתאמה של הרשימות לאלו של היחידות.**

**נמצא כי יחידות הסייבר המגזריות לא היו שותפות לגיבוש הצרכים ולתכנון המערכות והכלים שמספק להן מערך הסייבר, ולכן חלק מהכלים אינם מתאימים לצורכיהן והן ממעטות להשתמש בהם, וחלק מהכלים אף אינם מוכרים להן, וזאת אף שיחידות הסייבר המגזריות מייצגות נתח משמעותי מהגופים במשק שעליהם נדרש להגן.**

בתשובת מערך הסייבר נמסר כי בכל מפגש של מערך הסייבר עם היחידות המגזריות הוא מציג להן מוצרים ופיתוחים מסוימים שהוא מקדם. במסגרת הטמעת יכולות טכנולוגיות המערך משתף אותן בביצוע פיילוט ובהעברת משובים על מוצרים.

בתשובת מגזר 2 מנובמבר 2025 נמסר כי הוא משתמש בפרויקט מסוים שמספק מערך הסייבר. ואף החל בחודשים האחרונים להשתמש ברכיב חדש שלו.

בתשובת מגזר 7 מנובמבר 2025 נמסר כי היחידות המגזריות מעריכות מאוד את המאמץ של מערך הסייבר לפתח מוצרים ולספק אותם לשימושן, ורואות בכך מהלך משמעותי שמגביר את החוסן הלאומי של מדינת ישראל. עוד נמסר כי איסוף דרישות ושיתוף יחידות הסייבר המגזריות בשלבים

הראשוניים של הפרויקטים יבטיחו שהמוצרים יהיו רלוונטיים, מותאמים ושקופים יותר לשימוש עבורן.

**מומלץ כי מערך הסייבר יקיים עם נציגי יחידות הסייבר המגזריות מפגשים עתיים ייעודיים להצגת כלל הכלים והשירותים שהוא מספק ולקבלת היזון חוזר בדבר אופן השימוש בהם. עוד מומלץ כי מערך הסייבר ימדוד באופן שוטף את מידת השימוש של היחידות בכלים אלו. כמו כן מומלץ כי ישלב גם נציגים של היחידות בצוותי העבודה של פרויקטי הפיתוח וההטמעה של הכלים והשירותים שהוא מספק.**

בתשובת מערך הסייבר מנובמבר 2025 נמסר כי כיום הדברים נלמדים ומקבלים ביטוי בעשיה השוטפת. כחלק מהפקת הלקחים של המערך הוא מקיים מפגשים עיתיים עם היחידות המגזריות, שולח להם דוחות ומקבל היזון חוזר. כמו כן המערך מספק כלים שונים.

☆

**אף שבהחלטת הממשלה 2443 נקבע כי מערך הסייבר הוא המנחה המקצועי של יחידות הסייבר המגזריות והן המנחות המקצועיות של גופים חיוניים במגזר שלהן, מהפרק עולה כי לפני המלחמה מערך הסייבר לא קיים סקירות מודיעין ליחידות הסייבר המגזריות והועלו פערים הנוגעים לאופן שבו מערך הסייבר משתף מידע מודיעיני עם יחידות הסייבר המגזריות. כמו כן הוא לא הקים פורום לשיתוף מידע ביניהן ולא שיתף אותן באופן מספק בתכנון הכלים שהוא מפתח בין היתר עבורן. כמו כן ההנחיות המקצועיות שהעביר ליחידות הסייבר המגזריות אינן מחייבות (הן בגדר המלצה בלבד) ולכן הוא אינו יכול לפקח על מידת יישומן. יצוין לחיוב כי במהלך הביקורת החל מערך הסייבר לטפל בחלק מהפערים, למשל באמצעות כינוס פורום מקצועי עם היחידות המגזריות והצגת סקירת מודיעין.**

**כאמור בפרקים קודמים נמצא פער ביכולת התפקודית של חלק מהיחידות וכי רמת ההגנה בחלק מהמגזרים אינה מספקת ולכן יש חשיבות עליונה לכך שמערך הסייבר יחזק אותן באמצעות שיתוף ידע וכלים, הנחיה, פיקוח וטיפול בפערים.**

בתשובת מגזר 3 נמסר כי אף שלא נפגש עם צוות הביקורת הוא תומך בכל ההמלצות בפרק זה. המגזר הוסיף כי מערך הסייבר נתן את הדעת על ממצאי הביקורת ובעקבות כך ניכר שיפור בפעילותו לשיתוף היחידות המגזריות.

בתשובת מגזר 6 נמסר כי הנושאים המובאים בפרק זה הם חשובים ויש ליישמם.

## <u>תרגול לצורך היערכות וטיפול באירועי סייבר</u>

### קיום תרגיל סייבר לאומי

כאמור, בהחלטה ב/43 של ועדת שרים לענייני ביטחון לאומי מדצמבר 2007 (להלן - החלטה ב/43) הוחלט על הקמת רח"ל[51], שנועדה לשמש גורם מתאם ומתכלל של כלל הארגונים המטפלים בעורף בשעת חירום, ונקבע כי אחד מתפקידיה הוא לתאם בין משרדי הממשלה וגופים אחרים אימונים ותרגילים משולבים לכלל הגורמים הפועלים בעורף. בדף המרשתת של רח"ל באתר של משרד הביטחון מצוין כי אחד מתפקידיה הוא עריכת תרגילי היערכות לחירום ומתן הוראה על עריכתם על ידי גופי החירום.

בהחלטת הממשלה 2444 נקבע כי ההגנה על תפקודו התקין והבטוח של מרחב הסייבר מהווה יעד ביטחוני לאומי חיוני של המדינה ואינטרס ממלכתי חיוני לביטחונה הלאומי. ההחלטה הגדירה

[51] www.mod.gov.il/Departments/Pages/rahel.aspx

את תפקידיו העיקריים של מערך הסייבר ובהם לנהל, להפעיל ולבצע בהתאם לצורך את כלל מאמצי ההגנה האופרטיביים ברמה הלאומית במרחב הסייבר, לבנות ולחזק את החוסן של כלל המשק בסייבר באמצעות היערכות, שמירה על כשירות ואסדרה, ובכלל זה עריכת תרגילים ואימונים.

תרגיל סייבר לאומי מיועד לבדוק ולשפר את היכולת של המדינה להתמודד עם אירועי סייבר משמעותיים שיגרמו לנזק רב-מערכתי לתשתיות ולשירותים חיוניים של המדינה. במסגרת התרגיל תיבדק יכולת התגובה של המדינה, בין היתר מהבחינה התפעולית, הטכנולוגית והביטחונית, ייבחנו ממשקי העבודה בין הגופים האסדרתיים המדינתיים, גופי הביטחון וגורמי ממשל, ותיבחן היכולת של המדינה לטפל באירוע ולהתאושש ממנו. מטרת התרגיל היא לאתר נקודות חולשה, לטפל בהן מבעוד מועד ולספק מענה וחלופות כדי לחזק את החוסן של המשק ולהבטיח את רציפות תפקוד השירותים החיוניים למשק.

רח"ל מבצעת ומתכללת תרגילים לאומיים רב-ארגוניים שנועדו לשפר את המוכנות הלאומית לאירועי חירום תוך מיקוד בתהליכים בין-ארגוניים. התרגילים מתקיימים בשיתוף עם כלל הגופים והארגונים הפועלים במרחב האזרחי, לרבות משרדי הממשלה, רשויות ייעודיות, צה"ל ופקע"ר, משטרת ישראל, כבאות והצלה לישראל, שירות בתי הסוהר ומד"א. הכנת תרגיל לאומי דורשת משאבים רבים. נושאי התרגיל נקבעים על בסיס תרחיש הייחוס הלאומי ונוגעים לארבעה נושאים מרכזיים - מלחמה, רעידת אדמה וצונאמי, סייבר ופנדמיה. כמו כן רח"ל מבצעת תרגילים בין-לאומיים בנושאים אלו וכן משחקי מנהלים, ימי עיון מקצועיים ואימונים. לדברי רח"ל תרגול תרחיש מסוים אפשרי כתרגיל ייעודי בתרחיש ממוקד או כשילוב של כמה תרחישים בתרגיל אחד. כאשר בכל שנת עבודה המרחב האזרחי שותף לשני תרגילים: האחד לאומי בעצימות גבוהה, והשני תרגיל צה"ל בעצימות נמוכה יותר. תפקידה של רח"ל הוא לספק למתורגלים "מגרש משחקים" לבחינת ההישגים הנדרשים שהוגדרו במטרות התרגיל.

בשנת 2014 קיים המטה הקיברנטי תרגיל סייבר לאומי ראשון: "מעגל קסמים 1". התרגיל התקיים במסגרת תוכנית תרגילים מקיפה שגיבש מטה הסייבר הלאומי, והשתתפו בו חלק מיחידות מערכת הביטחון, גורמי ממשלה ובנק ישראל[52]. בשנת 2015 תכננה רח"ל תרגיל סייבר המיועד לכלל המשק, אולם התרגיל לא יצא לפועל והוחלף בתרגיל מלחמה "נקודת מפנה 2015" - במסגרתו שולבו 18 אירועי סייבר שתוכננו והורצו על ידי מינהלת מטה הסייבר הלאומי.

בשנת 2018 התקיים תרגיל לאומי בהובלת מערך הסייבר ("מעגל קסמים 2"). בתרגיל השתתפו מערך הסייבר הלאומי, שמונה משרדי ממשלה, מל"ל, רח"ל, גופי תמ"ק, צה"ל, מלמ"ב ושב"כ, בנק ישראל ורשויות מקומיות. נציגים מהדרג המדיני (השרים של המשרדים שהשתתפו בתרגיל) לא השתתפו בתרגיל. מטרתו העיקרית של התרגיל הייתה לקדם את החוסן הלאומי בסייבר ומטרות המשנה שנקבעו לו היו: (א) בחינת תהליכי הליבה המבצעיים של מערך הסייבר הלאומי (ב) קידום המנגנונים המדינתיים לניהול משבר סייבר לאומי (ג) קידום שיתוף הפעולה הבין-ארגוני ברמה הלאומית בתחום הגנת הסייבר (ד) קידום תחום הדוברות וההסברה בהיבט של משבר סייבר לאומי.

צבא הגנה לישראל מקיים מדי שנה תרגיל מטכ"לי כולל. על פי אתר המרשתת של צה"ל, במאי 2023 התקיים תרגיל "אגרוף המחץ"[53] שנמשך שבועיים ודימה לחימה רב-זירתית באוויר, בים, ביבשה, בספקטרום ובתחום הסייבר. במסגרת התרגיל נבחנה כשירות צה"ל למוכנות ממושכת בכמה זירות, השתתפו בו כוחות צה"ל בסדיר ובמילואים, מכלל הפיקודים, הזרועות והאגפים, והם תרגלו התמודדות עם אתגרים ואירועים מתפרצים בכמה זירות בעת ובעונה אחת. במסגרת התרגיל הצבאי התקיים גם תרגיל הסייבר "כפפת מגן", שהתמקד בבחינת היכולת המדינתית לספק במצב לחימה מענה מבצעי על אירוע סייבר במשק שיש לו השפעות על הביטחון הלאומי בשים דגש על רציפות התפקודית המשקית ותוך בחינת שיתוף הפעולה של מערך הסייבר עם גופי

52 www.pc.co.il/featured-news/157286

53 האימון המטכ"לי המרכזי של צה"ל.

הביטחון המדינתיים ועם רח"ל בתרגיל (בסיוע נציגות של משרדי ממשלה נבחרים). נציגים של גופים אלו סייעו בגיבוש התרגיל והשתתפו בו. פעילות התרגול תוכננה לשלוש זירות, ובכל אחת מהן הוגדר המתורגל הראשי: בזירה הצבאית - צה"ל, בזירת המשק - רח"ל ובזירת מרחב הסייבר הלאומי - מערך הסייבר. יצוין כי זהו אינו תרגיל סייבר לאומי היות שהוא לא כלל את כלל המגזרים, לא השתתפו בו נציגים של יחידות סייבר מגזריות, גופי תמ"ק או גופים מיוחדים.

לדברי מערך הסייבר, קיום תרגילים לאומיים מחייב הובלה ושותפות של הגורמים בעלי הסמכות הרלוונטית, כדוגמת רח"ל והמל"ל. כמו כן, תקופת הקורונה ומלחמת חרבות ברזל גרמו לביטול של מופעי תרגול רבים ולדחייתם של אחרים.

מערך הסייבר ונציגי רח"ל סיכמו ביניהם במאי 2023 כי יש צורך לקיים תרגיל סייבר לאומי "נקודת מפנה 24", התרגיל התקיים בנובמבר 2024 במתווה של תרגיל שולחני, והשתתפו בו נציגי רח"ל, מל"ל, מערך הסייבר, יה"ב, שב"כ, הרשות להגנת הפרטיות ועשרות גופים נוספים ממגזרים שונים בהם משרדי ממשלה, גופי תמ"ק, ושולבו בו לראשונה גם אנשי הסייבר, החירום והדוברים אך לא השתתפו בו מנכ"לים או נציגי דרג מדיני.

במהלך מלחמת חרבות ברזל, במרץ 2025, קיימה רח"ל תרגיל לאומי נוסף, "נקודת מפנה 25", שבו תורגלו תרחיש מלחמה ותרחיש סייבר. לדברי רח"ל מערך הסייבר היה שותף לתכנון התרגיל. כמו כן ציינה רח"ל כי לא השתתפו בתרגיל נציגים מהדרג המדיני.

רח"ל מסרה שאין הנחיה המגדירה מי הגורמים שצריכים להשתתף בתרגול לאומי ובפרט המשתתפים מהדרג המדיני, והיא אינה יכולה לחייב שום גורם להשתתף בתרגילים. עם זאת, מנכ"לים ושרים משתתפים בתרגילים שונים בהתאם לתחומי האחריות והסמכות של המשרדים השונים אך לא בתרגילים שולחניים. יצוין כי לדברי ראש אגף ההנחיה הסקטוריאלית במערך הסייבר הציפייה היא שבתרגילי ההנהלה ישתתפו מנכ"ל או סמנכ"ל, ובתרגילים מגזריים ישתתף השר. מכאן שקל וחומר שנחוצה השתתפות דרג מדיני בתרגילים לאומיים.


**אף שבשנים האחרונות נצפתה "קפיצת מדרגה" ביכולת של תוקפים וחלה עלייה במספר אירועי הסייבר, בחומרתם, בנזק שנגרם ובהשפעה שלהם על המשק ואף שתרגיל סייבר לאומי הוא בעל חשיבות רבה לחיזוק החוסן של כלל המשק בסייבר ולהיערכות הלאומית שכן הוא מדמה אירוע סייבר לאומי רב-מוקדי בהשתתפות משרדי ממשלה, גופי תמ"ק, מגזרים, גופים מיוחדים וגופי ביטחון - בשש השנים שקדמו למלחמה (משנת 2018) רח"ל ומערך הסייבר לא ערכו תרגיל סייבר לאומי, ורק כשנה לאחר פרוץ המלחמה, בנובמבר 2024, התקיים תרגיל סייבר לאומי במתווה שולחני. ולאחר מכן במרץ 2025 קיימה רח"ל תרגיל לאומי שכלל תרחיש מלחמה ותרחיש סייבר אשר מערך הסייבר היה שותף לתכנונו ונכח בו. עוד נמצא כי אף שההגנה על מרחב הסייבר הוא יעד ביטחוני לאומי כפי שנקבע בהחלטת הממשלה 2444, בתרגילי הסייבר הלאומיים שהתקיימו בשנת 2018, בשנת 2024, ובשנת 2025 לא השתתפו נציגים מהדרג המדיני - ראש הממשלה, חברי קבינט מדיני-בטחוני ושרים נוספים.**

בתשובת רח"ל מספטמבר 2024 נמסר כי בהחלטת הממשלה ב/43 הוטל עליה לבצע תרגילים ואימונים משולבים, כי בחמש השנים שקדמו למלחמת "חרבות ברזל" ביצעה רח"ל כשישה תרגילים לאומיים בתרחישים שונים שאינם סייבר, וכי משנת 2020 התחוללה בישראל ובעולם מגפת הקורונה, ועקב כך לא היה אפשר לקיים תרגילים או כל התקהלות אחרת. עם היציאה מהקורונה בשנת 2022 העדיפות העליונה הייתה לתרגל תרחיש מלחמה, ותרגול זה התקיים במסגרת התרגיל הצה"לי בשנת 2023, ובמסגרתו תורגל גם תחום הסייבר. יש תרחישים רבים שנדרש לתרגל ואין יכולת מעשית לתרגל כל תרחיש בכל שנה. התרחישים שבגינם נשקף לישראל איום ברמה גבוהה הם: מלחמה, רעידת אדמה, פנדמיה של שפעת וסייבר. על כן נקבעה מחזוריות רב-שנתית לביצוע כלל התרגילים ובהתאם לה מומלץ לקיים תרגיל סייבר לאומי אחת ל-3 שנים. תרגול לאומי אינו מחליף או מבטל תרגול של כל אחד מהגופים בתחומו. יתר על כן, במסגרת

מימוש אחריותו של כל גוף מוסמך עליו לתכנן לעצמו מתווה תרגילים משל עצמו ללא קשר למתווה הלאומי של רח"ל.

בתשובת מערך הסייבר נמסר כי תרגיל לאומי בסייבר מבוצע בהובלת רח"ל בתיאום עם מערך הסייבר הלאומי בהתאם להחלטת ב/43. קיום תרגיל לאומי מחייב את הפלטפורמה של רח"ל לצורך ביצועו, ומערך הסייבר הינו חלק בלתי נפרד מתרגילים כאמור המתקיימים בנושא סייבר.

**על מערך הסייבר ורח"ל להשלים את יישום המסקנות מתרגילי הסייבר הלאומי שנערכו בשנת 2024 ובשנת 2025. כמו כן לאור העלייה באיומים בתחום הסייבר וכדי לתרגל את המשק באופן רציף, מומלץ כי מערך הסייבר יבצע תרגיל לאומי או רב-מגזרי בסייבר אחת לשנה, וכי אחת לשלוש שנים התרגיל יתבצע בהובלת רח"ל. עוד מומלץ כי מערך הסייבר ינחה מי הגורמים שצריכים להשתתף בתרגילים אלו לרבות דרג מדיני ומנכ"לי המשרדים הרלוונטיים.**

בתשובת מגזר 10 מנובמבר 2025 נמסר כי היחידה המגזרית השתתפה בתרגיל והחלה ביישום הלקחים ממנו.

### קיום תרגילי סייבר למגזרים

כאמור, יחידות הסייבר המגזריות מנחות את הגופים החיוניים במגזר שאליו הם שייכים כדי לשפר את ההגנה שלהם ולחזק את חוסנם. אירוע סייבר שיפגע במספר גופים חיוניים במגזר עלול לשבש את פעולתם התקינה ולפגוע בשירותים חיוניים שהמגזר מספק לציבור ואף לסכן אותו.

כאמור, בשנת 2023 רח"ל ומערך הסייבר החלו להכין, בשיתוף יחידות הסייבר המגזריות, תרחישי ייחוס מגזריים בתחום הסייבר.

מערך הסייבר לא פרסם ליחידות המגזריות הנחיה מפורטת בנושא קיום תרגילי סייבר מגזריים באופן שוטף. עם זאת, בעוגנים השנתיים שהוא פרסם ליחידות המגזריות בשנים 2022, 2023 ו-2024 נקבע שעל היחידות המגזריות לבצע תרגיל סייבר מגזרי שנתי. בתשובת מערך הסייבר נמסר כי במהלך הביקורת, ולאחר שבחן את הסוגיה מבחינה מקצועית, לרבות לנוכח מורכבות התרגיל המגזרי והצורך בהקצאת משאבים רבים עדכן את מסמך העוגנים לשנת 2025 והנחה את היחידות לבצע תרגיל סייבר מגזרי אחת לשנתיים.

לדברי ראש אגף ההנחיה הסקטוריאלית הציפייה היא שבתרגילי ההנהלה ישתתפו מנכ"ל או סמנכ"ל, ובתרגילים מגזריים ישתתף השר, אולם הדבר נתון לשיקול הדעת של היחידות המגזריות, בין השאר בהתאם לסוג התרגיל.


**נמצאו פערים בקיום תרגילי סייבר מגזריים בשנים 2022-2023, אף שמערך הסייבר הגדיר ליחידות הסייבר המגזריות כעוגן שנתי לקיים תרגיל מגזרי פעם בשנה בשיתוף עימו.**


**עוד נמצא כי מערך הסייבר לא פרסם ליחידות הסייבר המגזריות הנחיה מפורטת בדבר הצורך לקיים תרגיל סייבר מגזרי ופירוט של תדירות ביצוע התרגיל, העקרונות שתרגיל מסוג זה אמור להתבסס עליהם ושל הגורמים שנדרשים להשתתף בו ובכלל זה גם הצורך שישתתף דרג מדיני.**

**על יחידות הסייבר המגזריות לקיים תרגיל מגזרי כנדרש בהנחיות מערך הסייבר ומומלץ כי מערך הסייבר יגבש עבור יחידות הסייבר המגזריות הנחיה מפורטת ומחייבת בדבר קיום תרגיל סייבר מגזרי לפחות אחת לשנתיים בהשתתפות השר הממונה, יפקח על יישומה, יסייע ליחידות בתכנון התרגילים וישתתף בהם.**

**עוד מומלץ כי מערך הסייבר ינחה את יחידות הסייבר המגזריות לתכנן את התרגילים המגזריים, בהלימה עם תרחיש האיום המגזרי ועם התייחסות לתקיפות חדשות. על מערך הסייבר להגדיר בשיתוף יחידות הסייבר המגזריות מנגנון שיאפשר להעביר לרח"ל סיכומי תרגילים רלוונטיים ואת תכלול מוכנות העורף לחירום בתחום הסייבר בתהליך תקופתי סדור.**

## קיום תרגילי חירום בגופים רגישים

כאמור, תרגיל סייבר מאפשר לארגון להבין טוב יותר את מכלול הסיכונים הטכניים והארגוניים, לזהות פערים, תקלות וחולשות, למקד את המאמץ ולשפר את המוכנות לאירוע סייבר. בתרגיל נבחנים בין היתר מוכנות בעלי התפקידים להתמודד עם מצב חירום בתחום הסייבר, משמעויות ארגוניות, עסקיות ותפעוליות ותיקוף הנהלים. ומתורגלים בו הצוות שאחראי לטיפול בחירום (בהשתתפות חברי הנהלה), הדרג הטכני וגורמים ארגוניים נוספים.

משרד מבקר המדינה קיבל ממערך הסייבר ומשב"כ פרטים על קיום תרגילי סייבר שנתיים בגופים רגישים שכפופים להנחייתם ובדק את עמידתם בהנחיה לקיים תרגיל סייבר בכל שנה.


**נמצאו פערים בקיום תרגילי סייבר בשנים 2022-2023 בחלק מהגופים הרגישים המונחים על ידי מערך הסייבר.**

**מניתוח הנתונים שהעביר שב"כ על קיום תרגילי סייבר שנתיים נמצא כי בשנת 2022 בוצעו תרגילי סייבר בכל הגופים המונחים על ידי השב"כ, ואילו בשנת 2023 בוצעו בחלקם. לדברי שב"כ הגופים תכננו את התרגיל לרבעון האחרון של שנת 2023 אולם דחו את התרגילים בגלל מלחמת חרבות ברזל. יצוין כי חלק מהגופים השלימו את התרגיל בשנת 2024.**

בתשובת שב"כ נמסר כי שניים מהגופים שדחו את התרגיל עקב המלחמה השלימו אותו בשנת 2024.

**על מערך הסייבר והשב"כ לוודא מדי שנה שכל אחד מהגופים הרגישים שמונחים על ידם מבצע תרגיל סייבר שנתי, וכן מומלץ כי מערך הסייבר יהיה שותף בתכנון התרגיל, בפיקוח על אופן ביצועו, בתיקון הליקויים וביישום הלקחים בגופים המונחים על ידו.**

## קיום תרגילים בגופים החיוניים שהשיבו על השאלון

לפי התפיסה הלאומית לניהול משבר סייבר, משבר סייבר צריך להיות מנוהל על ידי צוות ניהול משבר שחברים בו גורמים בכירים בהנהלת הארגון והוא מנחה ומכוון את פעילות הגורמים הרלוונטיים האחרים בארגון[54]. לתרגול יש חשיבות רבה בהיערכות ארגונים למצבי משבר ולהעלאת חוסנו של הארגון. התרגול צריך להיכלל בתוכנית העבודה השנתית, להקיף בעלי תפקידים רבים ככל האפשר לרבות נציגים בדרג ההנהלה וחברי צוות ניהול המשבר.

לצד תורת ההגנה 2.0 פרסם מערך הסייבר קובץ אקסל המכיל בקרות על תורת ההגנה 2.0 (גרסה 1.3) (להלן - בקרות תורת ההגנה) אשר מכיל רשימה של נושאים בתחום אבטחת מידע שארגון יכול לבדוק את עצמו לפיהם. הבקרות מאפשרות לארגון ליישמן בארבע רמות שונות של בשלות (בקרה ברמה בסיסית - 1, בקרה ברמה מתפתחת - 2, בקרה ברמה מתקדמת - 3, בקרה ברמה חדשנית - 4). כל ארגון יכול לבדוק כיצד הוא עומד בנורמות המובאות בהגדרת "עומק היישום" ו"ראיות נדרשות" ובהגדרות שנקבעו לרמות היישום (1 - 4) המוגדרות לכל בקרה.

[54] מתוך מסמך התפיסה הלאומית לניהול משבר סייבר.

היות שתורת ההגנה 2.0 ובקרות תורת ההגנה פורסמו על ידי מערך הסייבר והן מומלצות לכל הארגונים במשק, קל וחומר חשוב שהן ייושמו בגופים חיוניים ובגופי התמ"ק שרמת ההגנה שלהם נדרשת להיות גבוהה יותר מיתר הגופים במשק.

משרד מבקר המדינה בחן באמצעות שאלון שהפיץ ל-21 גופים שהם בעלי חשיבות למשק, אם במהלך השנתיים הסמוכות לתחילת המלחמה (יוני 2021-יולי 2023) הם קיימו מדי שנה את תרגילי הסייבר המפורטים ומוגדרים בבקרות תורת ההגנה 2.0. פירוט בנושא זה ראו להלן במבוא לפרק "ההיערכות והמוכנות של 21 גופים בעלי חשיבות במשק ושל גופים אסדרתיים מדינתיים להתמודדות עם אירועי סייבר לפני המלחמה ובמהלכה". יובהר כי בבדיקת תשובות הגופים תרגול נחשב לכל אחד מאלה: תרגיל מעשי, תרגיל יבש, סימולציה, אימונים ומבדקי כשירות. להלן הסברים מפורטים מתורת ההגנה על כל אחד מהנושאים שנבדקו:

1. תרגיל לצוות הנהלה לניהול משבר סייבר - בקרה מספר 10.3 (רמה1) - "הארגון וידא כי הוא תרגל את ההנהלה (Top Table Exercise) אחת לשנה לפחות".

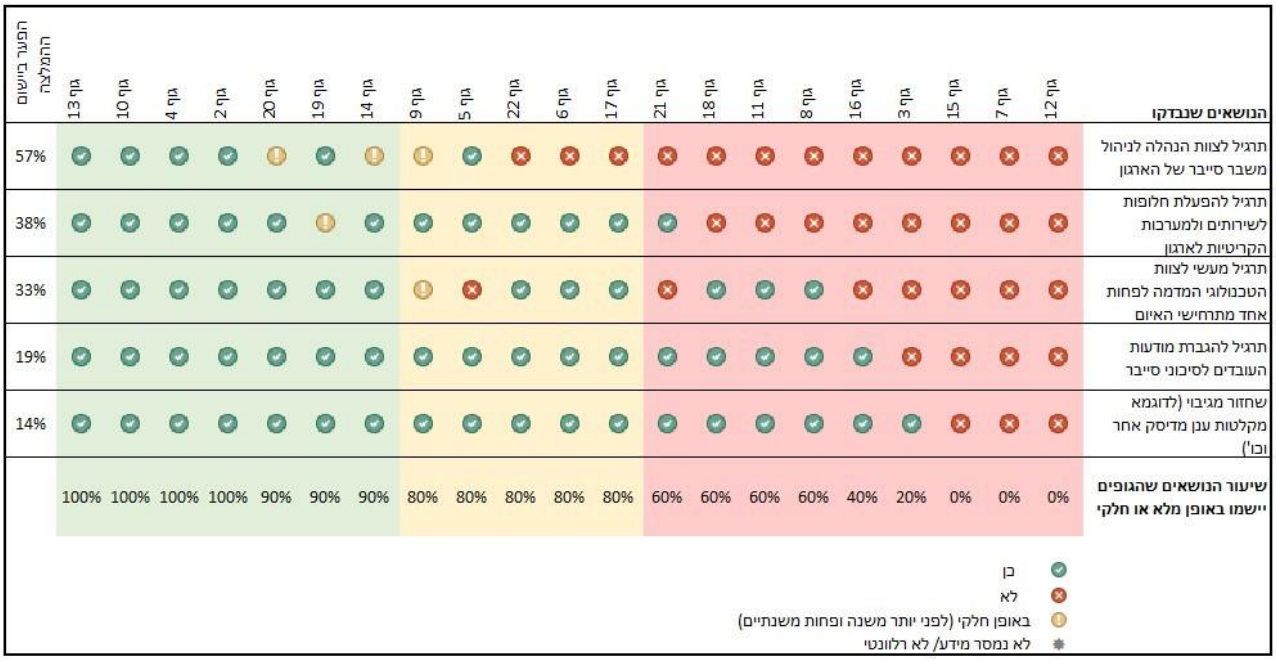
2. תרגיל להפעלת חלופות לשירותים ולמערכות הקריטיות של הארגון - בקרה מספר 19.1 (רמה 3) - "הארגון וידא כי הוא אחת לשנה לפחות מבצע מבדק כשירות ומוכנות לעבודה באתר חלופי (DR), וזאת ע"י דילוג חלק מתהליכי ליבה לעבודה באתר החלופי" ובקרה מספר 19.4 (כללי - הוכחות ליישום בקרה) - "על הארגון לוודא כי יש תכנית הדרכה ותרגולים שנתית בנושא המשכיות עסקית, הכוללת התייחסות לסוגיות רלוונטיות. וכי קיימת בה התייחסות לתרגול אתר החלופי (DR Site) באופן המאפשר בדיקה ממשית של עדכניות, רלוונטיות והבטחה לעמידה במדדים שהוגדרו (דוגמת RTO, RPO) לרבות עמידה בנפחי העבודה הרצויים, זמינות שטחי אחסון ויכולת גדילה עתידית וכד'".

3. תרגיל מעשי לצוות הטכנולוגי, המדמה לפחות אחד מתרחישי האיום: בקרה מספר 10.3 (רמה 2) - "הארגון יוודא כי צוות התגובה עבר פעם אחת לפחות בשנה מבדק כשירות, וזאת תוך שילוב אמצעי סימולציה מקובלים", ובקרה מספר 16.6 (רמה 2) - "הארגון וידא כי הוא ביצע תרגול חצי שנתי של מערך הניטור ע"י 'צוות סגול' (Purple Team) מטעמו לשם בחינת איכות תהליך הניטור וביצוע פעולות תגובה בהתאם ל-Playbooks מוגדרים".

4. תרגיל להגברת מודעות העובדים לסיכוני סייבר - בקרה מספר 19.4 (רמה 2) - "הארגון וידא כי עובדי הארגון עברו פעם אחת לפחות בשנה מבדק כשירות, וזאת תוך שילוב אמצעי סימולציה מקובלים".

5. שחזור מגיבוי (לדוגמה מקלטות, מענן, מדיסק אחר וכו'): בקרה מספר 19.3 (רמה 1) - "הארגון וידא כי האתר החלופי עומד בדרישות הכשירות ע"י ביצוע מבדקים עיתיים לדוגמא בדיקת תקינות שחזור אחת לחודש של יעדי הגנה".

תרשים 9: **ביצוע תרגילי סייבר בשנתיים שלפני מלחמת חרבות ברזל (יוני 2021 - יולי 2023)**[55]




המקור: שאלון גופים.

**נמצא כי בשנתיים שלפני פרוץ מלחמת חרבות ברזל (יוני 2021- יולי 2023), תשעה (43%) מתוך 21 הגופים שנבדקו בשאלון קיבלו ציון של 60 ומטה במדד שמשקף קיום של חמישה סוגי תרגילי סייבר שנתיים שמערך הסייבר ממליץ לקיים במסגרת הבקרות של תורת ההגנה 2.0. תרגילים אלו נועדו לוודא כי ההנהלה ויתר הגורמים בארגון ערוכים ומתורגלים להתמודד עם אירוע סייבר משמעותי וכי יש ברשותם כלים שיסייעו להם להגיב במהירות ולהתגבר עליו. עוד נמצאו שני פערים רוחביים: 57% מהגופים לא ביצעו תרגול צוות הנהלה וכמו כן 38% מהגופים לא ביצעו תרגול להפעלת תהליכים חלופיים לשירותים ולמערכות קריטיות.**

בתשובת גוף 3 נמסר כי בספטמבר 2024 הוא ביצע אימון הנהלה להתמודדות עם משבר סייבר, כי תרגיל להגברת מודעות אבטחת מידע לעובדים נמצא בשלב הטמעה ומתוכנן להתבצע ברבעון הרביעי בשנת 2024, וכי תרגיל להפעלת חלופות לשירותים ומערכות קריטיות ותרגיל מעשי לצוות הטכנולוגי יתווספו לתוכנית העבודה לשנת 2025 כתלות בתקצוב.

בתשובת גוף 7 מספטמבר 2024 (להלן - תשובת גוף 7) נמסר כי לאחר פרוץ מלחמת חרבות ברזל הוא קיים תרגיל הנהלה, תרגילי פישינג ושחזור מגיבוי וכן תרגול מגזרי בהשתתפות גורמים נוספים במגזר ובמערך הסייבר. הגוף ציין כי הוא מאמץ את ההמלצה ומתעתד לבצע תרגילי סייבר במסגרת תוכניות עבודה שנתיות.

בתשובת גוף 8 נמסר כי לאחר פרוץ המלחמה, באוגוסט 2024, השתתפה ההנהלה בתרגול מגזרי בהובלת מערך הסייבר, ובספטמבר 2024 קיימה תרגיל DR.

בתשובת גוף 9 נמסר כי הוא ערך תרגיל הנהלה נוסף בדצמבר 2024. התרגיל התקיים בראשותו של המנכ"ל והשתתפה בו ההנהלה הבכירה בחברה. את התרגיל הובילה חברה חיצונית המתמחה בניהול משברים בתחום הסייבר.

55 הציון חושב באופן הבא: כן - עבור דיווח שהתרגיל התקיים לפני פחות משנה; ביצוע חלקי - עבור דיווח שהתרגיל בוצע לפני שנה-שנתיים; לא - עבור דיווח שהתרגיל התקיים לפני יותר משנתיים או לא בוצע.

בתשובת גוף 12 נמסר כי בעקבות הדוח הוא קיים תרגיל סייבר בשיתוף מערך הסייבר וכן ביצע תרגול להגברת מודעות העובדים לסיכוני סייבר (קמפיין פישינג).

בתשובת גוף 15 מספטמבר 2024 (להלן תגובת גוף 15) נמסר כי אחרי פרוץ המלחמה, במהלך שנת 2024, הגוף ביצע את התרגילים האלה: תרגיל הנהלה, תרגיל הפעלת תהליכים חלופיים, שחזורים מגיבוי והדרכות להגברת המודעות ההנהלה והעובדים.

בתשובת גוף 18 מאוקטובר 2024 (להלן - תשובת גוף 18) נמסר כי הוא מתכנן תרגיל הנהלה במתכונת "שולחן עגול" ומתכוון להשלימו עד סוף שנת 2024.

בתשובת גוף 14 נמסר כי הוא קיים בספטמבר 2023 תרגיל הנהלה לניהול משבר סייבר.

בתשובת גוף 19 נמסר כי בכוונתו לערוך תרגיל לאחר מעבר מתוכנן של הארגון לבניין חדש. עם זאת ציין כי לאחר פרוץ המלחמה הוא ערך בדיקה במערכות המעורבות כדי לוודא את מוכנותן לאירוע סייבר או לכשל פיזי.

בתשובת גוף 21 מאוקטובר 2024 נמסר כי הנהלת המשרד אישרה לצאת לפרויקט תרגיל סייבר מקיף בנושא מוכנות למשבר לסייבר, וכי הפרויקט נמצא בשלב אישורי רכש.

בתשובת גוף 17 מאוקטובר 2024 נמסר כי לאחר הביקורת ולאחר פרוץ מלחמת חרבות ברזל, בפברואר 2024 הוא ביצע תרגיל הנהלה לניהול משבר סייבר.

**מומלץ כי המנכ"לים של הגופים שנבדקו ונמצאו בהם פערים יפעלו לקיום התרגילים הנדרשים מדי שנה באופן סדור, לתיקון הליקויים ולשיפור המוכנות של הגופים. כמו כן, על הגופים האסדרתיים המדינתיים שמנחים גופים אלה לסייע לגופים שבהם נמצאו הפערים ולהגביר את הבקרה בנושא.**

בתשובת גוף נמסר כי ביצע תרגיל הנהלה במרץ 2022. בנוסף, בספטמבר 2023 ביצע תרגיל הנהלה בהשתתפות כלל הגורמים הנדרשים. תרגיל זה התקיים לפני המלחמה אולם לא בטווח התאריכים שבדק משרד מבקר המדינה. בנוסף ציין כי הוא מקבל את הערת המבקר ויקיים תרגיל נוסף על התרגיל שבוצע בשנת 2023.

בתשובת גוף ממאי 2024, מיולי 2024 ומדצמבר 2025 נמסר כי הוא תכנן תרגיל הנהלה לדצמבר 2023 אולם הוא נדחה עקב המלחמה והתקיים בדצמבר 2024. עוד מסר הגוף כי במרץ 2023 ההנהלה תורגלה במסגרת תרגולים אחרים ובנוסף ציין כי פעילות ההנהלה נבחנה גם באירועי אמת.

**משרד מבקר המדינה מציין לחיוב שבעה גופים שקיבלו ציון 90 ומעלה במדד שמשקף קיום של חמישה סוגי תרגילי סייבר שנתיים שמערך הסייבר ממליץ לקיים אותם במסגרת הבקרות של תורת ההגנה 2.0.**

☆

**לפני מלחמת חרבות ברזל נמצאו פערים בביצוע תרגולים שנתיים הן ברמה הלאומית (התרגיל הלאומי האחרון התקיים כשש שנים לפני המלחמה בשנת 2018) והן ברמה המגזרית כפי שפורט. תרגולים אלו נדרשים כדי לוודא שהמדינה ערוכה להתמודד עם אירוע סייבר רב-מוקדי ולכן על מערך הסייבר להנחות מי הגורמים שצריכים להשתתף בתרגילים אלו לרבות דרג מדיני ומנכ"לי המשרדים הרלוונטיים. בנוסף גם ב-21 הגופים שנבדקו בשאלון נמצאו פערים בנושא תרגולים.**

## מסגרות ארגוניות, מודעות הנהלה וכלים לטיפול בתחום הסייבר

כדי שארגון יוכל לבצע את הפעולות הנדרשות בזמן ניהול משבר סייבר, עליו להיערך להן כבר בשלב שגרת ההגנה. נוסף על בדיקת ביצוע תרגילי סייבר בגופים כאמור, משרד מבקר המדינה בדק את ההיערכות והמוכנות הארגונית של גופים להתמודד עם אירועים ומשברים בתחום הסייבר בהיבטים האלה: מינוי והפעלה של המסגרות הארגוניות הנדרשות להתמודדות עם אירוע סייבר ומידת המודעות והמעורבות של הנהלת הגופים לנושאים מהותיים בהיערכות הארגון לאירוע סייבר.

בהחלטת הממשלה 2443 הוטל על המנכ"לים של משרדי הממשלה ומנהלי יחידות הסמך לפעול לשיפור רמת הגנת הסייבר ולשם כך עליהם למנות ממונה הגנת הסייבר, להקים ועדת היגוי משרדית, להסדיר את העסקת אנשי המקצוע בתחום הגנת הסייבר המועסקים במשרד, להקצות תקציב ייעודי להגנת הסייבר במסגרת התקציב הקיים של המשרד ולקדם את העמידה של המשרד בתקני אבטחת מידע ארגוניים.

### קיום מסגרות ארגוניות להתמודדות עם אירוע סייבר

משרד מבקר המדינה בחן באמצעות שאלון שהפיץ ל-21 גופים בעלי חשיבות במשק אם הם הקימו והפעילו לפני פרוץ מלחמת חרבות ברזל מסגרות ארגוניות הנדרשות לניהול סיכוני הסייבר ולהיערכות לאירועי סייבר משמעותיים ולטיפול בהם. להלן יפורטו המסגרות הארגוניות שלגביהן נעשתה הבדיקה:

1. **ממונה הגנת הסייבר:** בהחלטת הממשלה 2443 הוטל על המנכ"לים של משרדי הממשלה למנות ממונה הגנת הסייבר. הממונה אחראי להבטיח כי התכנון והניהול של מכלול היבטי הגנת הסייבר במשרד, והבקרה בנושא יתבצעו כנדרש. נוסף על כך, לפי בקרה 1.4 בבקרות תורת ההגנה יש לוודא כי הנהלת הארגון מינתה גורם המשמש "ממונה על הגנת המידע והסייבר" מטעם הארגון.

2. **ועדת היגוי לנושאי הגנת סייבר שמתכנסת אחת לחציון:** בהחלטת הממשלה 2443 נקבע כי על משרדי הממשלה להקים מסגרת ארגונית, בראשות המנכ"ל, האחראית ליישום המדיניות בנושאי הגנת המידע והסייבר, וכי הוועדה תתכנס לפחות פעם בחציון. בהנחית יה"ב 5.1 בנושא "מדיניות להגנת הסייבר בממשלה" נכתב כי ועדת ההיגוי בכל משרד אחראית לגיבוש עקרונות המדיניות, להתוויית אסטרטגיות לפעילות, לאישור של תוכנית האב ותוכניות העבודה השנתיות, לביצוע הערכת נזקים בעקבות תקלות ולגיבוש המלצות לטיפול על פי מסמך עקרונות המדיניות. כמו כן, בבקרות תורת ההגנה מוזכרים תפקידי הוועדה בבקרות מספר 6.10, 6.11, 18.1.

3. **צוות לניהול משבר סייבר ברמת ההנהלה:** על פי מסמך התפיסה הלאומית לניהול משבר סייבר[56] שפרסם מערך הסייבר הלאומי, על ארגון להקים צוות היערכות וניהול משבר סייבר, ומכיוון שהנהלת הארגון מחזיקה באחריות הכוללת להיערכות למצבי משבר בתחום הסייבר, והיא תנהל את המשבר אם יתממש, מומלץ כי בראש הצוות יעמוד מנכ"ל הארגון או סגנו, וכי נוסף להם הצוות יכלול גורמים בדרגה ניהולית בכירה, שמכירים את תהליכי העבודה בארגון זמן רב ומגיעים מתחומי ידע שונים, למשל: מנהל אבטחת מידע וסייבר, סמנכ"ל תפעול, סמנכ"ל כספים, יועץ משפטי. מדובר בצוות ניהולי שבזמן שגרה אחראי להיערכות הארגון למשבר סייבר ובזמן משבר אחראי לניהולו בכל ההיבטים, לרבות: ריכוז וביצוע של הערכת מצב, הכרזה על מצב הכוננות ושינוי רמת הכוננות, ביצוע פעולות לנוכח מצב הכוננות, עבודה מול גורמים בתוך הארגון ומחוץ לו, ולבסוף התאוששות, חזרה למצב שגרה, הפקת לקחים והטמעתם.

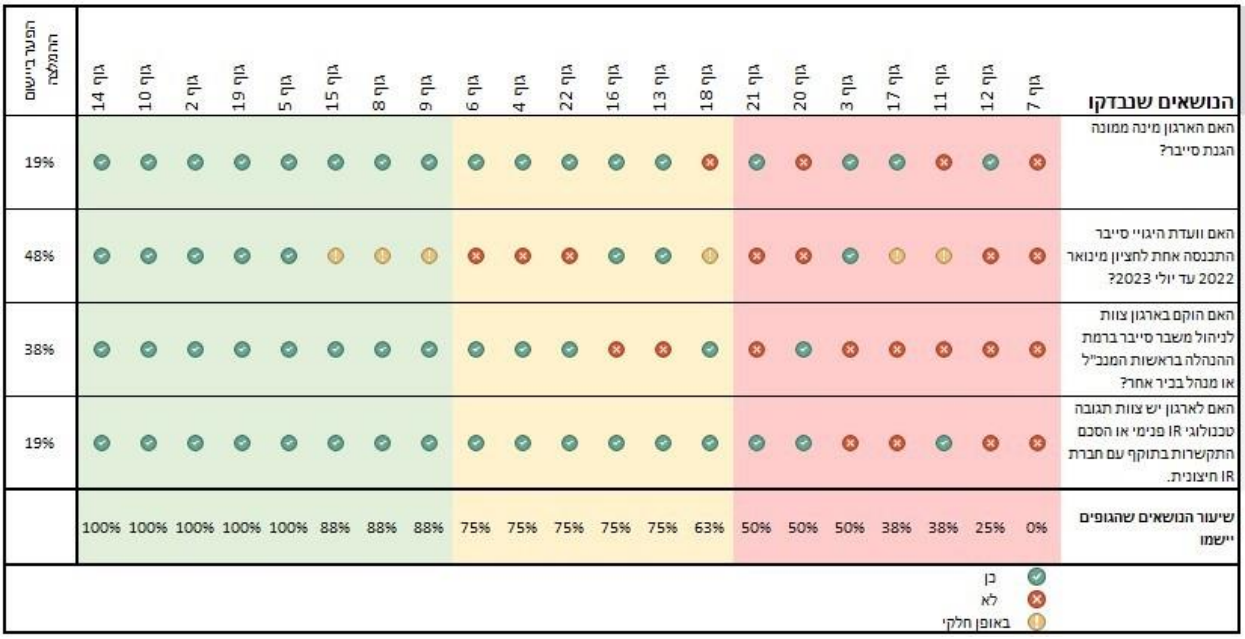
---

56 התפיסה הלאומית לניהול משבר סייבר - עמ' 21 פסקה א.

4. **צוות תגובה טכנולוגי (פנימי או חיצוני) לאירוע סייבר (IR Incident Response):** על פי מסמך התפיסה הלאומית לניהול משבר סייבר על ארגון להקים צוות תגובה טכנולוגי מקצועי[57] שייעודו מניעה של אירוע סייבר, זיהויו, התמודדות עימו, טיפול בו והתאוששות מנזקיו. צוות זה כולל גורמי אבטחת מידע וסייבר וגורמי IT, ויכולים להשתתף בו עובדי הארגון או מומחי חוץ שבהם הארגון בוחר להסתייע. תפקידיו העיקריים של הצוות הם להשיב את הארגון לשגרת עבודה, מלאה או חלקית, מנקודת מבט ניהולית ותפעולית, להשיג שליטה על המערכות והתשתיות שנפגעו, לצמצם את הנזק ולמנוע את התפשטות האירוע. לכן חשוב שהם יתחילו בעבודה מהר ככל שאפשר בעת חשד לאירוע או גילוי אירוע.

5. **ביטוח סייבר:** בעשור האחרון גובר הביקוש לכיסוי ביטוחי בפני תקיפות סייבר, שנותן מענה להוצאות כגון הוצאות שבוצעו בעקבות אירוע סייבר; הוצאות רגולטוריות משפטיות; הוצאות הקשורות לרכיבי אבטחת מידע; הוצאות על ביצוע מחקר בנוגע לזהות התוקף; פגיעה בפרטיות; נזקי פגיעה בפעילות העסקית של הארגון; נזקי פגיעה במערכות הארגון והחזר כספי בהתרחש מתקפת כופר. כמו כן, בעת אירוע סייבר חברת הביטוח שולחת לארגון הנתקף צוות ניהול אירוע וצוות תגובה מקצועי מטעמה, שתפקידו צמצום של הפגיעה והנזק.

תרשים 10: **מסגרות ארגוניות וכלים להתמודדות עם אירוע סייבר לפני מלחמת חרבות ברזל**




על פי תשובות הגופים על השאלון, בעיבוד משרד מבקר המדינה.

**נמצא כי לפני פרוץ מלחמת חרבות ברזל, 7 (33%) מתוך 21 הגופים שנבדקו בשאלון קיבלו ציון 60 ומטה במדד שמשקף הפעלה של מסגרות ארגוניות וכלים נדרשים שאמורים לשמש את התשתית הארגונית להתמודדות עם אירוע סייבר משמעותי ולטפל בו: מינוי ממונה סייבר בארגון; מינוי צוות הנהלה לניהול משבר סייבר; קיום דיונים של ועדת היגוי סייבר לפחות בכל חציון, העסקת צוות תגובה IR פנימי או רכישת שירותי צוות תגובה IR חיצוני. היעדר המסגרות והכלים בגופים אלו מלמד על רמת מוכנות ארגונית נמוכה שלהם לאירוע משברי משמעותי. עוד נמצא כי יש פערים רוחביים בנושאים האלו: לארבעה (19%) מהגופים אין צוות פנימי או חיצוני, ב-48% מהגופים ועדת היגוי סייבר לא התכנסה כנדרש בשנה וחצי שלפני מלחמת חרבות ברזל, ב-38% מהגופים לא הוקם צוות הנהלה לניהול משבר סייבר ול-90.5% מהגופים אין ביטוח סייבר.**

גבוה

[57] התפיסה הלאומית לניהול משבר סייבר - עמ' 21 פסקה ב.

**מומלץ כי המנכ"לים של הגופים שנבדקו ונמצאו בהם פערים יקימו ויכנסו את המסגרות הארגוניות הנדרשות כדי שידונו בסיכונים שהארגון חשוף להם ויפעלו לצמצום הפערים.**

בתשובת גוף 3 נמסר כי צוות לניהול משבר סייבר נקבע במסגרת האימון שנערך בספטמבר 2024 להנהלת המשרד, וכי במכרז לספק מחשוב חדש נוספה הדרישה לצוות IR פנימי.

בתשובת גוף 4 מאוקטובר 2024 (להלן - תשובת גוף 4) נמסר כי הפער הושלם, וכי חודד נושא מועדי הכינוס של ועדת ההיגוי (שהייתה קיימת) והיא מתכנסת כנדרש.

בתשובת גוף 7 נמסר כי ה-CISO הארגוני (מנהל אבטחת מידע) אחראי לאבטחת מידע. כמו כן ציין כי בכוונתו להתקשר עם גוף חיצוני אשר יסייע לו בהתרחש אירועי סייבר.

בתשובת גוף 8 נמסר כי לאחר העברת המענה על שאלון מבקר המדינה, החל מינואר 2024 מוסדה תדירות ההתכנסויות של ועדת ההיגוי בקביעות מדי רבעון.

בתשובת גוף 9 מינואר 2024 נמסר כי ועדת ההיגוי שלו התכנסה בדצמבר 2024.

בתשובת גוף 13 מדצמבר 2024 (להלן - תשובת גוף 13) נמסר כי לאחר פרוץ המלחמה הוא רכש שירות IR חיצוני. כמו כן, לגבי צוות ניהול משבר סייבר יש נוהל שמסביר מיהם הגורמים המעורבים, אבל לא מונו אנשים ספציפיים לצוות. הגוף מקבל את המלצת המבקר למינוי שמי של חברי הצוות.

בתשובת גוף 17 נמסר כי לאחר הביקורת ולאחר פרוץ מלחמת חרבות ברזל הוא טיפל בליקויים כמפורט: ביוני 2024 הוא הקים צוות תגובה טכנולוגי פנימי, ביולי 2024 הוא פרסם מכרז קבלת שירותי צוות תגובה מחברה חיצונית לשירותי IR למתן מענה על אירועי סייבר, ובאוקטובר 2024 סוכם בוועדת היגוי סייבר בראשות המנכ"ל שיוקם צוות הנהלה לניהול משבר סייבר וייקבעו תפקידיו וסמכויותיו.

בתשובת גוף 12 נמסר כי הוא משתמש בשירותי ה-IR החיצוני של המגזר ומסתמך על יכולותיו ועל יכולות היחידה המגזרית כצוות IR פנימי. עוד ציין כי בעקבות הדוח הוקמה ועדת היגוי סייבר. כמו כן נמסר שוועדת ההיגוי שהוקמה קיימה שני מפגשים.

בתשובת גוף 5 מספטמבר 2024 נמסר כי אומנם אין לו הסכם עם חברת IR חיצונית, אולם בעת אירוע הוא מקבל שירות זה מהיחידה המגזרית, וכי הוא נעזר בשירות זה באירוע שהתרחש.

בתשובת גוף 22 נמסר כי הוא מקיים הערכות מצב שוטפות בתדירות גבוהה, ומאז פרוץ מלחמת חרבות ברזל אף הוגברה התדירות. הערכות המצב מתקיימות בראשות מנכ"ל הגוף או סגנו, ובהשתתפות נציגים נוספים.

בתשובת גוף 20 נמסר כי נושא ביטוח הסייבר נבחן באמצעות פיילוט שהוא היה שותף בו, וכי ממצאי הפיילוט הצביעו על ישימות נמוכה של הנושא בצורה רוחבית בממשלה.

גוף 14 מינה לאחר הביקורת צוות לניהול משבר סייבר.

בתשובת מגזר 7 מספטמבר 2024 (להלן - תשובת מגזר 7) נמסר כי הוא מספק מנגנון התקשרות עם צוותי IR מקצועיים עבור כלל הגופים במגזר ולכן לדעתו אין צורך בהתקשרויות עצמאיות של הגופים במגזר.

**על הגופים האסדרתיים המדינתיים שמנחים גופים אלה לסייע לגופים שבהם נמצאו הפערים ולהדק את הבקרה בנושא. עוד מומלץ כי מערך הסייבר כמנחה מקצועי של המשק יגבש מדיניות**

**לגבי ביטוח סייבר בפרט עבור גופים חיוניים וגופי תמ"ק או ייתן להם מענה אחר ברמה הלאומית.**

**משרד מבקר המדינה מציין לחיוב שמונה גופים שקיבלו ציון 88 ומעלה במדד שנבחן - ציון שמעיד כי הגופים הפעילו את המסגרות הארגוניות והכלים הנדרשים שאמורים לשמש התשתית הארגונית להתמודדות עם אירוע סייבר משמעותי ולטיפול בו.**

**מכרז מרכזי לשירותי תגובה לאירוע סייבר**

בהחלטת הממשלה 2443 הוגדר, בין היתר, כי אחד מהתפקידים של יה"ב הוא היערכות להתמודדות עם אירועים, לרבות ניהול אירועים, תהליכי התאוששות ושיקום.

בשנת 2021 זיהה יה"ב כי קיים פער בממשלה בנושא זה. ראש מערך הדיגיטל (בעבר נקרא ראש רשות התקשוב) דאז, פנה לדבריו למינהל הרכש ונענה שלא מתוכנן פרסום מכרז מרכזי בנושא. בהתאם לכך החל לקדם כתיבה ופרסום של מכרז עצמאי לשירותי IR עבור מערך הדיגיטל. עוד לדבריו התכנון היה שגם המשרדים יוכלו לרכוש את שירותי ה-IR באמצעות המכרז, אולם מינהל הרכש לא אישר זאת אלא הורה שהמכרז יוכל לשמש רק את מערך הדיגיטל.

בתשובת מינהל הרכש מאוקטובר 2024 נמסר כי הוא לא קיבל ממערך הדיגיטל או ממערך הסייבר בקשה לפרסום מכרז מרכזי לצוות IR ולכן לא פרסם מכרז כזה. כמו כן ציין כי בהתאם לתקנות חובת המכרזים, התשנ"ג-1993 - הסמכות לבצע מכרז מרכזי נתונה לחשב הכללי בלבד, ומשרדי ממשלה אינם רשאים ליצור התקשרויות רכש על בסיס מכרזים שפורסמו על ידי משרדים אחרים. ולכן למינהל הרכש הממשלתי ולחשב הכללי לא הייתה הסמכות לאשר למשרדים לבצע רכש בהתאם לתנאי המכרז של מערך הדיגיטל הלאומי.

בינואר 2024, בעקבות הצורך שעלה במלחמת חרבות ברזל להגיב על אירועי סייבר, קידם מערך הדיגיטל רכש חירום דחוף בפטור ממכרז למשך שנה. באוגוסט 2024 פרסם מערך הדיגיטל מכרז לרכש שירותי IR. לדברי מערך הדיגיטל, משרד אשר יבחר להשתמש בשירות זה יוכל לעשות כן, בכפוף לאישורו ובתנאי שהאירוע ינוהל על ידו.

**נמצא כי מערך הסייבר ומערך הדיגיטל לא פעלו לקדם מול מינהל הרכש פרסום מכרז מרכזי לשירותי תגובה על אירוע סייבר (IR - Incident Response) ואין מכרז מרכזי בנושא - אף שמערך הדיגיטל זיהה עוד בשנת 2021 כי יש צורך במשרדים בשירות זה. עוד נמצא כי ל-4 (19%) מתוך 21 הגופים שנבדקו בשאלון אין צוות תגובה כלל (פנימי או חיצוני). בעקבות הצורך שעלה במלחמת חרבות ברזל להגיב על אירועי סייבר, קידם מערך הדיגיטל רכש חירום דחוף בפטור ממכרז למשך שנה לשירות זה עבור מערך הדיגיטל.**

**מומלץ כי מערך הסייבר, יה"ב ומינהל הרכש יתכללו את הצרכים של המשרדים ושל יחידות הסייבר המגזריות ויגבשו מכרז מרכזי למתן שירותי תגובה על אירוע סייבר (IR) וכן יבחנו אם נדרשים מכרזים מרכזיים נוספים להיערכות לקראת אירועי סייבר, למניעתם ולניהולם (לדוגמה, הכשרה, קיום תרגילים).**

בתשובת מערך הדיגיטל ומערך הסייבר נמסר כי ההמלצה נבחנת מול מינהל הרכש. בתשובת מגזר 2 נמסר כי הוא מסכים עם ההמלצה היות שנחוץ מאוד לבצע את המכרז, וכי ראוי שבמכרזים טכנולוגיים ישתתפו כמה ספקים כדי "לפזר" את הסיכון. כמו כן, בתשובת מגזר 6 נמסר כי הוא מסכים עם ההמלצה ומבקש לוודא שהמכרז יכלול דרישות מקצועיות כדי להבטיח שהזוכים יהיו בעלי הידע והכלים הרלוונטיים לפעילות הייחודית של המגזר שלו.

בתשובת מינהל הרכש נמסר כי הוא מאגם את צורכי כלל משרדי הממשלה ומבצע בחינה להצדקת ביצועו של מכרז מרכזי. המינהל, בהתייעצות עם הגופים המאסדרים בענייני סייבר במדינת ישראל, יבחן את היתרונות שבעריכת מכרז מרכזי בתחום ה-IR וכן יבחן חלופות נוספות

שבאמצעותן ניתן לסייע למשרדים להתקשר לרכישת שירותי IR, והכול בהתאם לסדר העדיפויות של המשימות.

**מודעות הנהלה להיבטי אבטחת המידע והגנת הסייבר בארגון**

כאמור, בהחלטת ממשלה 2443 הוטל על המנכ"לים של משרדי הממשלה ויחידות הסמך לפעול להעלאת רמת הגנת הסייבר בארגון שלהם. לשם כך הם נדרשים בין היתר להכיר את הנכסים של הארגון, את רמת ההגנה בו ואת הסיכונים הנשקפים לו, וזאת הם עושים בין היתר באמצעות השתתפות בוועדת היגוי סייבר שהם צריכים לעמוד בראשה וכן באמצעות השתתפותם בצוות הנהלה לניהול משבר סייבר. כמו כן, אחד העקרונות של תורת ההגנה הוא שהאחריות להגנה על המידע מוטלת בראש ובראשונה על הנהלת הארגון, וכי על ההנהלה להבין את הסיכונים שאורבים לארגון במרחב הסייבר ולגבש תוכנית עבודה לצמצום פערי ההגנה.

בשאלון שהופץ ל-21 גופים בעלי חשיבות למשק נבדק אם הוצגו למנכ"לי הגופים באופן אישי או באמצעות ועדת היגוי סייבר הנושאים האלה, שנכללים בבקרות תורת ההגנה שפרסם מערך הסייבר. להלן פירוט הבקרות הרלוונטיות:

1. **סיכוני הסייבר הארגוניים (תרחישי איום, נזקים וסבירויות):** בקרה מספר 1.1 - "דירקטוריון הארגון אישר את מדיניות הגנת המידע והסייבר הארגונית ואת מפת הסיכונים, והקצה משאבים בהתאם".

2. **מדיניות אבטחת מידע וסייבר של הארגון:** בקרה 1.1.

3. **תחקירים של אירועי סייבר מהותיים מהשנתיים האחרונות:** בקרה מספר 1.1 (דגשים) - "ודאו כי קיים פרוטוקול ישיבת דירקטוריון המכיל התייחסות לאירועי סייבר שהתרחשו, ומעקב אחר ביצוע פעולות מתקנות".

4. **הגדרת צוות הנהלה לניהול משבר סייבר וקביעת תפקידיו וסמכויותיו:** בקרה מספר 18.1 (רמה 2) - "מנהל צוות ניהול משברים הינו מנכ"ל או המשנה למנכ"ל".

5. **עקרונות הטיפול באירועי סייבר - כמוגדר בנוהל לטיפול באירועי סייבר (השלבים, החומרה, הסמכויות, חובת הדיווח, התיעוד והתחקור):** בקרה מספר 18.1 (שם הבקרה) - "הארגון וידא כי הגדיר תוכנית לטיפול באירועי הגנת מידע וסייבר"; (ראיות לבקרה) - "ודאו כי לפחות אחת בשנה ועדת היגוי להגנת מידע וסייבר מבצעת מעקב אחר מימוש תוכנית לטיפול באירוע הגנת מידע וסייבר"; (רמה 1) - "הארגון וידא כי ברשותו תוכנית תגובה לניהול אירועי הגנת מידע וסייבר הכוללת בין השאר התייחסות להגדרת המשאבים ותמיכת הנהלה הנדרשים לתחזוקה ושיפור יכולת התגובה לאירועי סייבר, מנהל צוות ניהול משברים הינו מנכ"ל או המשנה למנכ"ל".

6. **עקרונות תוכנית העבודה בתחום הגנת הסייבר של הארגון:** בקרה 1.1 (דגשים) - "ודאו כי בשנה האחרונה תועדו בפרוטוקול ישיבות דירקטוריון אשר כללו הצגה של מפת הסיכונים, תוכנית העבודה, אישור התקציב השנתי, וכן מעקב תקופתי אחר היישום בפועל".

7. **תוכנית התאוששות מאירועי סייבר הכוללת קביעת סדרי עדיפויות להעלאת מערכות ומדדים להתאוששות:** בקרה 19.1 (רמה 1) - "הארגון וידא כי הנהלת הארגון הגדירה ואישרה את תוכנית ההתאוששות מאסון (DRP)"; "הארגון וידא כי אחת לשנה לפחות הנהלת הארגון עורכת דיון בנושא המשכיות עסקית בהיבטי הגנת מידע וסייבר".

8. **הפקת הלקחים מתרגולים שביצע הארגון בתחום הסייבר בשנתיים האחרונות:** בקרה 10.3 (רמה 1) - "ודאו כי ברשות הארגון תכנית עבודה סדורה לביצוע תרגולים בשנה הקרובה ושהארגון השלים את ביצוע התרגילים בשנה החולפת. ודאו יישום לקחים אשר הופקו מהתרגיל לשם שיפור רמת הגנת הסייבר של הארגון".

9. **ממצאי מבדקי חדירה מהשנתיים האחרונות (השנתיים שקדמו למלחמת חרבות ברזל) בחומרה קריטית וגבוהה (אם נעשו):** בקרה 19.1 (רמה 1) - " הארגון וידא כי אחת לשנה לפחות הנהלת הארגון עורכת דיון בנושא המשכיות עסקית בהיבטי הגנת מידע וסייבר וזאת תוך התייחסות לנושאים מקובלים כגון הצגת ממצאי מבדקי כשירות ומוכנות והצגת פערים והמלצות ליישום".

10. **דוחות שנתיים מה-SOC הארגוני:** בקרה 16.4 (ראיות) - "ודאו כי החלטת הנהלת ארגון בדבר הקמת מערך ניטור מרכזי עוגנה בפרוטוקול סדור, תוך הצגת הנימוקים להצגת הצורך בהקמתו"; ודאו כי הנהלת הארגון וידאה כי הגדירה תקציב המאפשר לארגון להקים מערך ניטור המספק מענה לפרופיל הסיכון של הארגון"; "ודאו כי הוגדרו מדדים לבחינת אפקטיביות מערך הניטור וזאת בהתאם לצורכי הארגון".

תרשים 11: **מודעות ההנהלה להיבטי אבטחת המידע והסייבר בארגון**

| הנושאים שנבדקו | גוף 20 | גוף 12 | גוף 11 | גוף 21 | גוף 18 | גוף 17 | גוף 8 | גוף 3 | גוף 5 | גוף 6 | גוף 15 | גוף 19 | גוף 7 | גוף 10 | גוף 22 | גוף 9 | גוף 13 | גוף 4 | גוף 2 | גוף 14 | גוף 16 | שיעור הפער |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| סיכוני הסייבר הארגוניים (תרחישי איום, נזקים וסבירויות) | ✗ | ✗ | ◐ | ✓ | ◐ | ✓ | ✓ | ✓ | ◐ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | 17% |
| עקרונות תוכנית העבודה בתחום הגנת הסייבר של הארגון | ✗ | ✗ | ◐ | ✓ | ✗ | ✓ | ✓ | ✓ | ◐ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | 19% |
| מדיניות אבטחת מידע וסייבר של הארגון | ✗ | ✗ | ◐ | ✓ | ✗ | ✓ | ✓ | ✓ | ◐ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | 29% |
| תחקירים של אירועי סייבר מהותיים שהתרחשו בארגון בשנתיים האחרונות | ✗ | ✗ | ✓ | ✗ | ◐ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ | ✓ | ✓ | - | - | ✓ | ✓ | - | ✓ | 26% |
| הגדרת צוות הנהלה לניהול משבר סייבר וקביעת תפקידיו וסמכויותיו | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | 38% |
| עקרונות הטיפול באירועי סייבר- כמוגדר בנוהל לטיפול באירועי סייבר (השלבים, החומרה, הסמכויות, חובת הדיווח, התיעוד והתחקור) | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✓ | ✓ | ◐ | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ◐ | ✓ | 48% |
| תוכנית התאוששות מאירועי סייבר הכוללת קביעת סדרי עדיפויות להעלאת מערכות ומדדים להתאוששות | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✓ | ✗ | ✓ | ✓ | ✗ | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | 52% |
| הצגת הפקת הלקחים מתרגולים שביצע הארגון בתחום הסייבר בשנתיים האחרונות והתובנות שעלו מהם | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✓ | ✗ | ✓ | ✗ | ✓ | ✗ | ◐ | ✓ | ✓ | ✓ | ✓ | ✓ | 55% |
| ממצאי מבדקי חדירה מהשנתיים האחרונות בחומרה קריטית וגבוהה (אם נעשו) | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ◐ | ✓ | ✓ | ✗ | - | ✓ | ✓ | ✓ | ✓ | - | ✓ | - | ✓ | 40% |
| דוחות שנתיים מה SOC הארגוני | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✓ | ◐ | ✗ | ✗ | ◐ | - | ✓ | ✓ | ✗ | - | ✗ | ✓ | - | ✓ | 52% |
| שיעור הנושאים שהגופים יישמו באופן מלא או חלקי | 0% | 0% | 30% | 30% | 35% | 40% | 50% | 60% | 65% | 70% | 70% | 70% | 75% | 80% | 80% | 83% | 88% | 89% | 90% | 93% | 100% | |

✓ כן
◐ לא
✗ באופן חלקי
- לא רלוונטי

על פי תשובות הגופים על השאלון, בעיבוד משרד מבקר המדינה.

גבוה

**נמצא כי לפני פרוץ מלחמת חרבות ברזל בידי שמונה (38%) מתוך 21 מנכ"לי הגופים שהשיבו על השאלון לא היו תמונות המצב ותשתית המידע הנחוצות (קיבלו ציון 60 ומטה) להיערכות הארגון שלהם לטיפול באירוע סייבר וכן לרמת ההגנה הקיימת ולפערים בה. לדוגמה, לא הוצגו להם סיכוני הסייבר הארגוניים; מדיניות אבטחת המידע והסייבר של הארגון; עקרונות הטיפול באירוע סייבר; תוכנית התאוששות עסקית; הפקת לקחים מתרגולים שביצע הארגון וממצאי תחקירים של אירועי סייבר משמעותיים. נוכח זאת קיים חשש כי המנכ"ל לא יכיר את האתגרים העומדים לפני הארגון ולא ישקיע את המשאבים הנדרשים כדי להגן על הארגון כראוי.**


**עוד נמצא כי יש פער רוחבי בהצגת הנושאים האלה למנכ"לים: תוכנית התאוששות מאירועי סייבר (52%); הצגת הפקת הלקחים מתרגולים (55%); ממצאי מבדקי חדירה בדרגת חומרה קריטית וגבוהה (40%) ודוחות שנתיים מה-SOC הארגוני (52%).**

בתשובת יה"ב נמסר כי זיהתה פערים אלו בגופים שבהנחייתה והחלה ליזום תרגילי הנהלה בקרב המשרדים. כמו כן, אחת המטרות המרכזיות של ועדות ההיגוי היא הצגת תמונת מצב בנושאים אלו להנהלת המשרד, תוך שיקוף הפערים והמשאבים הנדרשים לצמצומם.

בתשובת גוף 3 נמסר כי צוות החירום הארגוני שאחראי להמשכיות העסקית בעת חירום קיבל הכשרה לטיפול במשבר סייבר במסגרת תרגיל הנהלה שהתקיים בספטמבר 2024. כמו כן נמסר כי הפקת הלקחים מתרגילי סייבר בוצעה בשנת 2024.

בתשובת גוף 7 נמסר כי לאחר פרוץ המלחמה, בספטמבר 2024, הגוף קיים תרגיל הנהלה המדמה אירוע סייבר, ומסקנותיו הועברו לגורמים המעורבים.

בתשובת גוף 8 נמסר כי לאחר פרוץ המלחמה, בדצמבר 2023, מונה צוות הנהלה לניהול משבר סייבר, ובמאי 2024 הוצגו בוועדת ההיגוי עקרונות הטיפול באירועי סייבר. כמו כן בכוונת הגוף להציג לפני הוועדה לקחים שהופקו מתרגול שקיים וממצאי מבדקי חדירה.

בתשובת גוף 10 נמסר כי עד סוף שנת 2024 יושלם עדכון מדיניות אבטחת המידע הארגונית ויתקבל אישורה על ידי המנכ"ל או ועדת ההיגוי הקרובה.

מתשובת גוף 14 מאוקטובר 2024 נמסר כי מנכ"ל החברה מעורב בכל תהליכי העבודה בחברה, וביתר שאת אחרי פרוץ המלחמה, וכי המנכ"ל מעורב בנושא באופן שוטף, מכיר כל מערכת ומשתתף בתרגילי הסייבר וההיערכות לחירום. כמו כן תוצאות מבדקי החדירה ותובנות מניטורי ה-SOC מוצגות למנכ"ל החברה ולוועדת ההיגוי.

בתשובת גוף 16 מספטמבר 2024 (להלן - תשובת גוף 16) נמסר כי בספטמבר 2024 הוא הציג לוועדת ההיגוי אירועי סייבר משנת 2024.

בתשובת גוף 17 נמסר כי לאחר הביקורת ולאחר פרוץ מלחמת חרבות ברזל, בפברואר 2024, הגוף ביצע תרגיל הנהלה והמנכ"ל סיכם אותו. כמו כן, באוקטובר 2024 סוכם בוועדת היגוי בראשות מנכ"ל שיוקם צוות הנהלה לניהול משבר סייבר וייקבעו תפקידיו וסמכויותיו.

בתשובת גוף 18 נמסר כי אחרי פרוץ המלחמה, במסגרת דיון ועדת ההיגוי העליונה להגנת הסייבר שהתקיימה בספטמבר 2024, הוצגו אירועי סייבר שנוהלו במהלך 2024.

בתשובת גוף 19 נמסר כי בשנה שאחרי פרוץ מלחמת חרבות ברזל הוצג למנכ"ל סטטוס אבטחת מידע אולם לא עלו בתקופה זו ממצאים ברמת חומרה גבוהה וקריטית. כמו כן הוצגו לו עיקרי נוהל הטיפול באירוע סייבר והוא הנחה להשלים את גיבוש הנוהל הסופי.

בתשובת גוף 15 נמסר כי לאחר פרוץ המלחמה, בשנת 2024, בוצע תרגיל מודעות הנהלה לאבטחת מידע וסייבר ותואמה ישיבת היערכות ליישום הפקת לקחים מהתרגיל. כמו כן מסר הגוף כי בכוונתו להציג למנכ"ל החל ממועד התכנסותה של ועדת ההיגוי הקרובה פירוט נוסף של תוצאות דוחות מה-SOC. עוד נמסר כי המנכ"ל מקיים פגישות קבועות עם מנהל אגף מחשוב ומערכות מידע וצוותו ומכיר היטב את הנושא וכן מתודרך ופועל בהתאם לכך.

בתשובת גוף 22 נמסר כי לאחר תקופת הביקורת הוא עדכן את מסמך ההתאוששות מאסון, וכי הוצגו למנכ"ל בוועדת ההיגוי התרגילים שנערכו וסוגיהם.

**מומלץ כי המנכ"לים של הגופים שנבדקו בשאלון ושנמצאו בהם פערים ילמדו את היבטי הסייבר ואת הסיכונים שהארגון שהם עומדים בראשו חשוף להם ויפעלו לצמצום הפערים.**

בתשובת גוף 7 מספטמבר 2024 נמסר כי הוא מקבל את ההמלצה ובכוונתו לשכלל את לימוד היבטי הסייבר השונים - בכלל זה יידוע והעברת המידע לגורמים הרלוונטיים מקרב ההנהלה והעובדים, לרבות הצגת הסיכונים, דרכי ההתגוננות ודרכים לצמצום הפערים.

בתשובת גוף 11 מאוקטובר 2024 נמסר כי הוא יקיים הליך שבמסגרתו יילמדו היבטי הסייבר של הארגון והסיכונים שהוא חשוף להם, וכי הוא יפעל לצמצום הפערים.

**משרד מבקר המדינה מציין לחיוב שמונה גופים שקיבלו ציון 80 ומעלה במדד שבחן אם למנכ"ל יש תמונת מצב ותשתית המידע הנחוצות להיערכות הארגון לטיפול באירוע סייבר, המשקפת את רמת ההגנה בסייבר, את הפערים ואת תוכניות הטיפול בהם.**

## פעולות שביצע מערך הסייבר להעלאת החוסן בתקופת מלחמת חרבות ברזל

עם פרוץ מלחמת חרבות ברזל, התגברו והתעצמו באופן משמעותי ומיידי אתגרי הסייבר בישראל. לדברי מערך הסייבר הוא עבר לעבודה במתכונת חירום תומכת לחימה, שינה ומיקד את השקעת המשאבים ואת תיעדוף הפעילות בהתאם לאיומים, גייס אנשי מילואים לתגבור ופעל להאצתה ולשיפורה של ההגנה על ממד הסייבר של מדינת ישראל. עיקר המאמץ התמקד בתמיכה בצה"ל בלחימה, בהגנה על גופי התמ"ק, בסיוע בהידוק הגנת הסייבר בגופי שרשרת האספקה הביטחונית, בסיוע בהגבהת חומות הגנת הסייבר בגופים חיוניים ושמירה על רציפות תפקוד המשק בחירום בהיבטי סייבר. להלן הפעילויות העיקריות שמערך הסייבר מסר שהוא ביצע מאז תחילת המלחמה:

1. **הערכות מצב וצוותי משימה:** בחודשי המלחמה הראשונים התקיימו הערכות מצב יומיות בפורומים שונים כולל השתתפות גורמים ביטחוניים ולאומיים. בפגישות נסקרו בין היתר מצב הלחימה, אירועי הסייבר, תמונת מצב גופי התמ"ק והמגזרים, מודיעין, מגמות ואתגרים. בהתאם לסיכונים ולצורך מונו צוותי משימה ממוקדים שפעלו למנוע או לצמצם תקיפות בתחום הסייבר ולטפל בפערים שעלו.

2. **שרשרת אספקה:** מופו גופי שרשרת אספקה ומערכות שתומכים בפעילות של צה"ל, בפעילות הממשלה ובתפקוד התקין של המשק ובוצעו מולם פעולות להעלאת החוסן נוכח אתגרי המלחמה.

3. **פעולות להעלאת החוסן של גופי תמ"ק:** בוצעה פעילות פרטנית מול גופי תמ"ק להעלאת החוסן, למניעת אירועי סייבר ולסיוע בטיפול בהם. כמו כן, אחת לחודש התקיימה הערכת מצב בהשתתפות כל ממוני התמ"ק בגופים.

4. **פעולות להעלאת חוסן מול יחידות סייבר מגזריות:** בתחילת המלחמה הופצו ליחידות הנחיות והמלצות להעלאת החוסן והחלה, כאמור, פעילות למדידת חוסן של שני מגזרים; התקיימו כחמש פגישות הערכת מצב עם ראשי יחידות הסייבר המגזריות; ראש מערך הסייבר דאז נפגש עם מנכ"לים לצורך העלאת המודעות לאיומי הסייבר במגזר והצורך לחזק את היחידות המגזריות.

5. **פעולות להעלאת החוסן של גופים במשק בגופי שרשרת אספקה, בגופי תמ"ק, בגופים חיוניים ובגופים אחרים, בהתאם לסיכונים ולצורך שזיהה המערך**

6. **חקיקה:** כאמור, הותקנו תקנות שעת חירום ובהמשך נחקק חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה - חרבות ברזל).

7. **מערכות לטיפול באתגרי רוחב:** בוצע טיפול ממוקד בנושאי רוחב שאינם נמצאים באחריות גוף או מגזר מסוים.

8. **קמפיין מרחב תודעתי מוגן:** בוצע קמפיין תקשורתי לציבור לזיהוי ולאימות של הודעות וקישורים שנועדו להונאות ולפרסום דיס-אינפורמציה.

**מפרוץ המלחמה ועד יוני 2025 מדינת ישראל לא חוותה אירוע סייבר שפגע באופן משמעותי בתהליכים עסקיים קריטיים שהשפיעו באופן מהותי על המשק. יחד עם זאת, לפי דברי ראש מערך הסייבר דאז באוקטובר 2024, ישנה עליה דרמטית באיום הסייבר ולא לעולם חוסן - השיפור הדרמטי בקצב ויכולות התקיפה מחייב נקיטת פעולות לחיזוק קו ההגנה ולהבטחת רציפות התפקוד ברמה המשקית והביטחונית.**


**דוח זה מציג כי לפני המלחמה רמת ההגנה בתחום הסייבר בחלק מסוים מהמגזרים (לא כולל את גופי התמ"ק) לא הייתה מספקת. מערך הסייבר מסר לצוות הביקורת כי עם פרוץ המלחמה הוא נקט פעולות מיידיות לזיהוי ולצמצום של פערים קריטיים ולחיזוק ההגנה על ממד הסייבר של מדינת ישראל, ולצורך כך הסיט משאבים ושינה סדרי עדיפויות. משרד מבקר המדינה מציין לחיוב את המאמץ שהשקיע מערך הסייבר הלאומי בתחילת המלחמה ובמהלכה כדי להעלות את רמת החוסן של הגופים במשק. עם זאת אין בפעולות אלו כדי לתת מענה מלא על הפערים אשר פורטו בדוח זה והתחדדו במלחמה, ובעניינם של פערים אלו נדרשות פעולות נוספות רבות.**

**נוכח הפערים שהוצגו בדוח, ונוכח השיפור הדרמטי בקצב וביכולות התקיפה וכדי להתמודד עם אתגרי העתיד, על מערך הסייבר לגבש מפת דרכים ותוכנית עבודה כוללת לפעילות שהוא אחראי לה בהתאם לסיכונים שעלו במלחמה ולתובנות שהופקו, וכן עליו לפקח על כך שגופי התמ"ק והיחידות המגזריות מיישמים תוכנית זו.**

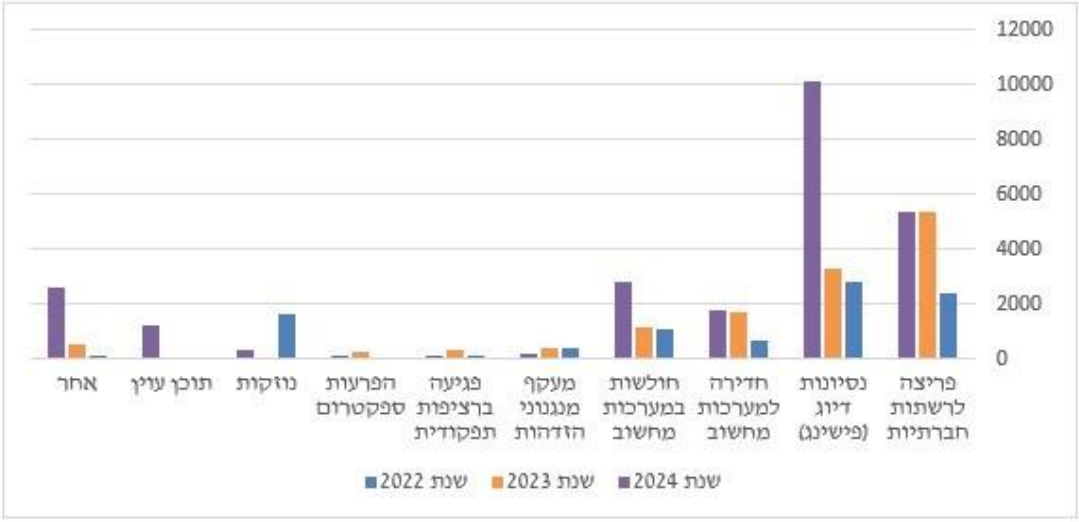
## <u>אירועים עם פוטנציאל נזק משמעותי למשק וביצוע תחקירים</u>

### דיווחים למערך הסייבר על אירועים שהתרחשו לפני מלחמת חרבות ברזל ובמהלכה

מנתוני מערך הסייבר[58] עולה כי בשנת 2023 חל גידול של 43% במספר האירועים שדווחו על ידי אזרחים וארגונים ואומתו כאירועי סייבר לעומת שיעורם בשנת 2022 (13,040 לעומת 9,108). חלק ניכר מהגידול בשנת 2023 נובע מהתגברות התקיפות במהלך המלחמה (ברבעון זה התרחשו 68% מהאירועים). גם בשנת 2024 חל גידול של 24% בתקיפות ביחס לשנת 2023. להלן תרשימים המציגים את התפלגות סוגי האירועים.

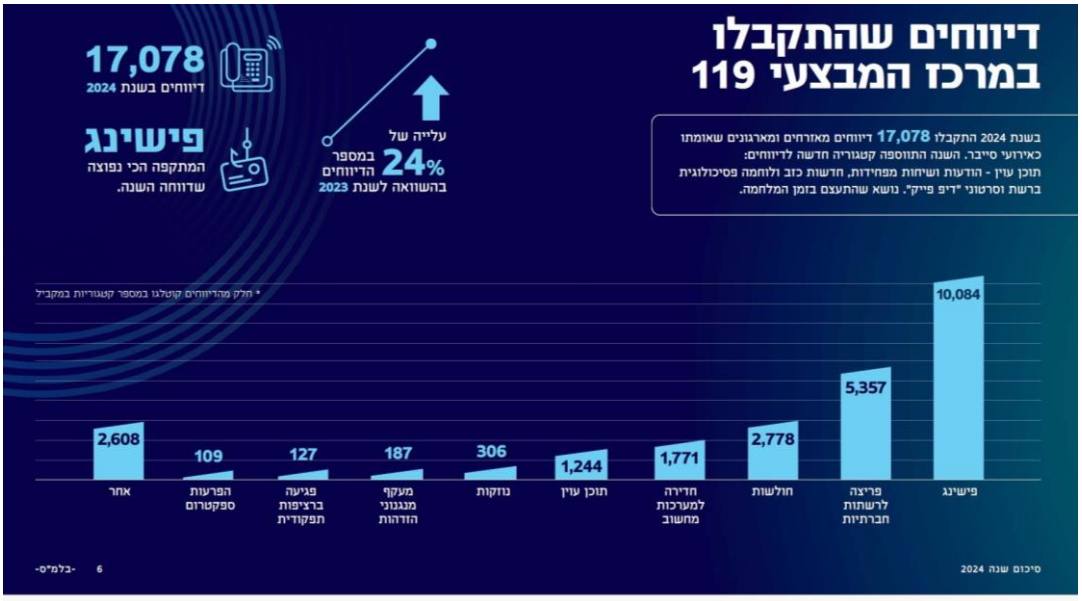
[58] מערך הסייבר הלאומי - סיכום שנתי 2022 בסייבר וכן הדוח השנתי של מערך הסייבר לשנת 2023.

תרשים 12 : **מספר הדיווחים המאומתים למערך הסייבר על אירועי סייבר, לפי נושאים, 2022 - 2024**




על פי נתוני מערך הסייבר, בעיבוד משרד מבקר המדינה.

תרשים 13 : **מספר הדיווחים המאומתים למערך הסייבר על אירועי סייבר בשנת 2024**




על פי נתוני מערך הסייבר.

**מהתרשימים עולה כי ניסיונות דיוג (פישינג) ופריצה לרשתות חברתיות הם שני התחומים שבהם נצפו האירועים הרבים ביותר (כמחצית מהאירועים) בשנים 2022 - 2024. כמו כן בשנת 2023 נצפה גידול בחדירה למערכות המחשוב ובשנת 2024 נצפה גידול בחולשות סייבר[59]. כיום מערך הסייבר מטפל באירועי פריצה לרשתות חברתיות ודיוג באמצעות פעולות להעלאת מודעות: פרסום מידע והמלצות לאזרח ופונה לחברות האחסון ולגורמים הרלוונטיים לפי הצורך כדי לצמצם פגיעה בציבור.**

[59] נקודות תורפה במערכות מחשב, תוכנה וחומרה, שיכולות להיות מנוצלות על ידי תוקפים כדי לחולל תקיפת סייבר.

**נוכח הגידול המתמשך במספר אירועי הסייבר מסוג דיוג ופריצה לרשתות חברתיות, מומלץ כי מערך הסייבר יבחן את אפקטיביות הטיפול שלו בנושא זה ואת מידת התאמת המענה שהוא מספק לתופעות אלו ויפעל לשפר אותו.**

### אירועים בעלי פוטנציאל נזק משמעותי

בהחלטת הממשלה 2444 נקבע כי על מערך הסייבר הלאומי לבנות ולחזק את החוסן של כלל המשק בסייבר, להפעיל מרכז לסיוע בהתמודדות עם איומי סייבר עבור כלל המשק, לסייע בטיפול באיומי סייבר ובאירועי סייבר, לרכז ולשתף מידע רלוונטי עם כלל הגורמים במשק ולשמש נקודת ממשק מרכזית בין גופי הביטחון לבין הגורמים במשק.

לפי דיווחי מערך הסייבר, בשנת 2022 התרחשו 1,044 אירועי סייבר בעלי פוטנציאל נזק משמעותי. במהלך מלחמת חרבות ברזל (בין שבעה באוקטובר 2023 עד אפריל 2024) התרחשו מאות אירועי סייבר בעלי פוטנציאל נזק משמעותי, ולדבריו שיעורם גדול פי 2.5 מהמספר המקביל בתקופת שגרה.

**משרד מבקר המדינה ביקש ממערך הסייבר להעביר לידיו את ממצאי התחקירים שביצע בנושא אירועים בעלי פוטנציאל נזק משמעותי שאירעו במשק בשנים 2023 - 2024 וקיבל מתוך אלפי האירועים שהתרחשו רק שישה תחקירים.**

בתשובת מערך הסייבר נמסר כי בעת שגרה יש מעבר על פרטי כל האירועים המשמעותיים על ידי דרג מקצועי בכיר, לצורך בחינת תובנות ולקחים בשים לב לצורך המבצעי, ובמיוחד נוכח היקף האירועים שלהם מסייע מערך הסייבר. תחקירים מעמיקים נערכים רק בנסיבות שבהן נמצא צורך מקצועי לעשות כן, כגון באירועים מורכבים וייחודיים, ומופקות תובנות רוחביות במגוון שיטות ולא בהכרח בתחקירי עומק.

**מומלץ כי מערך הסייבר יגדיר קריטריונים שבהם יבצע תחקירים של אירועי סייבר משמעותיים ויפיץ את התובנות למשק, למגזרים ולגופים רלוונטיים.**

כמו כן משרד מבקר המדינה ביקש ממערך הסייבר פירוט ותחקירים, אם התבצעו, הנוגעים למאות האירועים שהתרחשו לאחר פרוץ מלחמת חרבות ברזל וסווגו על ידו כבעלי פוטנציאל נזק משמעותי. לגבי כל אחד מהאירועים העביר מערך הסייבר נתונים מסוימים.


**על פי הדיווח שהעביר מערך הסייבר למשרד מבקר המדינה, בשנת 2023 התרחשו מספר אירועים בעלי פוטנציאל נזק משמעותי ששויכו ל-21 הגופים שנבדקו בשאלון בדוח זה: לגבי חלק מהאירועים חסר פירוט הנדרש להבנת התמונה המלאה של הטיפול בהם.**

בתשובת מערך הסייבר נמסרה התייחסות לחלק מהאירועים.


**משרד מבקר המדינה מעיר למערך הסייבר כי בפירוט שיש בידו על מאות האירועים שאירעו בתקופת מלחמת חרבות ברזל (בין שבעה באוקטובר 2023 עד אפריל 2024) שהם בעלי פוטנציאל לנזק משמעותי חסר מידע חיוני הנדרש כדי לגבש תמונת מצב וסטטוס של האירועים, לתחקר אותם ולהפיק לקחים ותובנות מערכתיים כדי למנוע את הישנותם ולשפר תהליכים.**

**לפי החלטת הממשלה 2444 על מערך הסייבר לבנות ולחזק את החוסן של כלל המשק בסייבר, להפעיל מרכז לסיוע בהתמודדות עם איומי סייבר עבור כלל המשק, לסייע בטיפול באיומי סייבר ובאירועי סייבר, לרכז ולשתף מידע רלוונטי עם כלל הגורמים במשק. נוכח זאת על מערך הסייבר להגדיר מה המידע הנדרש לו כדי לגבש תמונת מצב על כל האירועים המשמעותיים במשק, לתעד את המידע ולהפיק מתמונת מצב זו תובנות מערכתיות. כמו כן עליו להציג תובנות מרכזיות**

**לדרגים שונים בממשלה, לגופים אסדרתיים מדינתיים מקבילים (יה"ב, שב"כ, הרשות להגנת הפרטיות, משטרת ישראל, יחידות הסייבר המגזריות) ולגופים במשק ולהנחות את הגופים כיצד עליהם להיערך ולטפל באירועים. בנוסף, עליו לוודא כי גופים בהנחייתו שבהם התרחשו אירועי סייבר משמעותיים או אירועים שסווגו כבעלי פוטנציאל נזק משמעותי פועלים יחד עם המנחה מטעם המערך לתיקון הליקויים.**

לדברי מערך הסייבר בתקופת הביקורת הוא יישם חלק מהנושאים המובאים בהמלצה: הוא הפיק תובנות מאירועי הסייבר בתקופת המלחמה ופרסם לציבור מידע והמלצות.

## ההיערכות והמוכנות של 21 גופים בעלי חשיבות במשק ושל גופים אסדרתיים מדינתיים להתמודדות עם אירועי סייבר לפני המלחמה ובמהלכה

### <u>רקע</u>

בחלק זה של הדוח מוצגת תמונת מצב רוחבית[60], לפני המלחמה ובמהלכה, בנוגע להיערכות של 21 גופים בעלי חשיבות במשק להתמודדות עם אירוע סייבר ממגזרים שונים בהם גופים רגישים המונחים על ידי מערך הסייבר, משרדי ממשלה, גופים חיוניים - גופי A, מוסדות להשכלה גבוהה, רשויות מקומיות וגופים מיוחדים. אלה הפעולות העיקריות שבמסגרתן הופקו הנתונים שעליהם מתבססת תמונת המצב הרוחבית:

1. **ה ש א ל ו ן :** ניתוח מענה הגופים[61] לשאלון ששלח להם משרד מבקר המדינה. השאלון נשלח לגופים עוד טרם המלחמה (מרביתם ענו עליו ערב המלחמה - בספטמבר 2023). להלן הפרטים:

   א. מדובר ב-21 גופים בעלי חשיבות במשק שאינם כפופים לאסדרה אחודה בתחום ההגנה בסייבר שכן הם משויכים למגזרים ולמערכים שונים ומשום כך רמת ההגנה הנדרשת מכל אחד מהם שונה. ברוב המקרים הגופים נדרשים לעמוד בכמה נורמות או באסדרות של גופים אסדרתיים מדינתיים שונים. נוכח זאת גיבש משרד מבקר המדינה את השאלון בהתבסס על תקנות אבטחת מידע, הנחיות של גופים אסדרתיים מדינתיים בתחום הסייבר ומתודולוגיות מקובלות בארץ ובעולם בתחום הגנת הסייבר (כגון תקני NIST ו-ISO27001) ובראשם תורת ההגנה 2.0 של מערך הסייבר, הנחיות שחלקן חלות על הגופים באופן מחייב וחלקן הן בגדר המלצה.

   ב. בשאלון נכללו כ-110 שאלות ב-17 נושאים הנוגעים לנדבכים יסודיים בהיערכות של כל גוף ואשר העמידה בהן יכולה לשקף כאמור תמונה בנוגע למוכנות הגוף להתמודדות עם אירוע סייבר.

   ג. בניתוח המענה לשאלון של 21 הגופים לא הובאו בחשבון בקרות מפצות שאותן מיישמים הגופים כמענה לפער מסוים מטעמים מתודולוגיים שתכליתם להבטיח הערכה אחידה למול כל הגופים. בכך ניתן היה להבטיח בדיקה אחודה לכלל הגופים המאפשרת להשוות בין הגופים ביחס להיבטים שנבדקו.

   ד. בתשובת מערך הסייבר צוין כי קיים צורך משמעותי בשיפור רמת הגנת הסייבר הלאומית והוא מברך על כל מאמץ לשיפור הנושא אולם לעמדתו המקצועית קיים קושי באופן שבו בוצעה הבחינה, באופן הצגת הפערים ובאופן ניתוח השלכותיהם בדוח בהתייחס ל-21

---

60 כאמור תמונת הרוחב אינה מבוססת על מדגם כמותי מייצג

61 כולל מסמכי תמך

הגופים שנבדקו בשאלון, תוך חשש להצגת תמונה כוללת שאינה מדויקת. זאת בין היתר, נוכח העובדה כי 21 הגופים האמורים לא מהווים מדגם מייצג; נוכח השונות המשמעותית הקיימת הן בפעילותם והן באסדרה המחייבת אותם; נוכח יצירת מדד עצמאי ותכלול הפערים שנמצאו ובחינת השפעתם על רמת ההגנה של הגופים, וזאת ללא ביצוע האבחנה הרגולטורית הנדרשת; ונוכח הצורך המקצועי לתכלל ולתת משקל מהותי לבקרות מפצות הננקטות ביחס לפערים משמעותיים, לצורך קבלת תמונת המצב המלאה הנדרשת. עוד ציין המערך כי הוא פועל כיום במסגרת הכלים הקיימים לו למיפוי רמת ההגנה בסייבר של מגזרי משק שונים, תוך שכלול שוטף של שיטת הבחינה, המדידה והניתוח, לצד שילוב אומדני מומחים המבוססים על אינדיקציות לחוסן בפועל.

2. **בדיקות העמקה:** בדיקות העמקה ב-11 גופים לגבי סוגיות שהועלו בשאלון ובמסגרתן נבחנו פערים ספציפיים שעלו בכל גוף. נוכח זאת מוצג בדוח מידע נוסף על פערים ייחודיים שנמצאו בחלק מהגופים בבדיקות ההעמקה האמורות.

3. **ניתוח נתונים:** ניתוח של נתוני התרעות ממערכות ה-SIEM[62] בגופים שנבדקו, ביחידות המגזריות ובמערך הדיגיטל מספטמבר 2023 (לפני המלחמה) עד נובמבר 2023 (במהלך המלחמה), שמהם ניתן ללמוד בצורה אמפירית בין השאר על כמות ההתרעות אודות חשד לאירועי סייבר ועל הקצב והיעילות של הטיפול בהן על ידי הגופים.

לדעת משרד מבקר המדינה ראוי להתייחס לתוצאות הבחינה הרוחבית המובאת בפרק זה כאל אבן בוחן להערכה כללית ומערכתית של ההיערכות של גופים שונים להתמודדות עם אירועי סייבר ולא כאל בחינה שתכליתה לעמוד על ציות של גופים לנורמות והוראות מחייבות, שכן ביסודה של בחינה זו מונחים כאמור גם תקנים מומלצים לחיזוק ההיערכות לאירועי סייבר.

תרשים 14: **מרכיבי הביקורת שעליהם נשענים ממצאי חלק זה של הדוח**


הוכן בידי משרד מבקר המדינה.

הממצאים והפערים המשמעותיים שמועלים בחלק זה של הדוח, העוסק בהיערכות גופים בעלי חשיבות במשק וגופים אסדרתיים מדינתיים להתמודדות עם אירועי סייבר, מציפים סוגיות הדומות במאפייניהן לכאלה שמסתמן כי אפשרו את התרחשותה של מתקפת הטרור בשבעה באוקטובר והביאו להחמרת הנזק שנגרם בגינה. במובן זה יש לראות בממצאים, בפערים ובתובנות משום נורת אזהרה ויש לתת עליהם את הדעת. להלן הסוגיות:

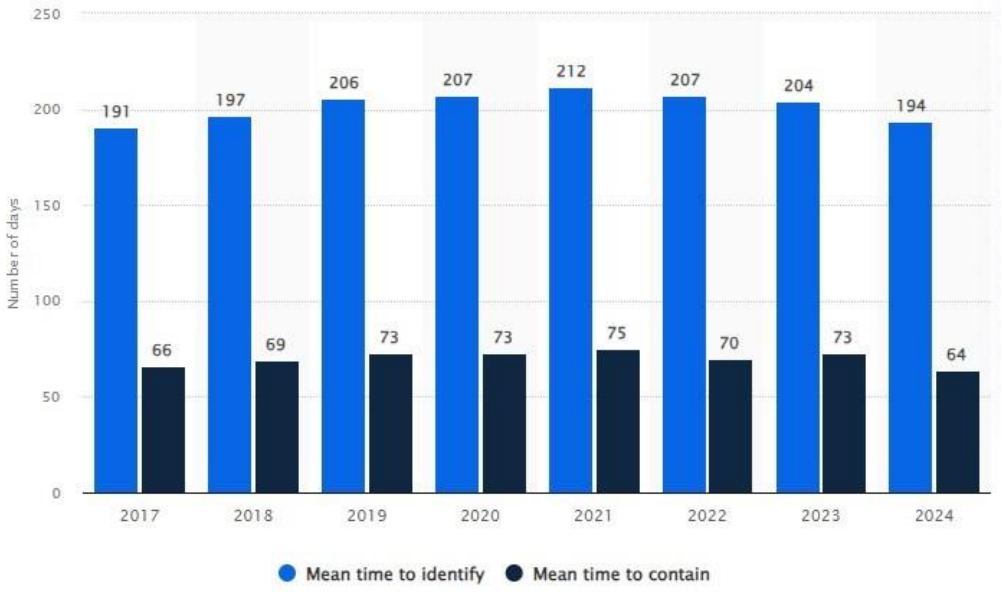
62 Security Information and Event Management - SIEM, ראו הרחבה נוספת בהמשך.

1. כיצד התייחסו הגופים להתרעות על אירועי סייבר, ואיזה מענה נתנו עליהן?[63]
2. האם הגופים מדווחים לגופים האסדרתיים המדינתיים על התרעות שקיבלו?[64]
3. באיזו מידה הדרגים השונים יכולים לייצר תמונת מצב מדינתית על תקיפת סייבר נרחבת ומורכבת שמתרחשת?[65]
4. האם ההיערכות ההגנתית של גופים אלה הייתה מותאמת לתרחישי איום הייחוס?[66]
5. כיצד גופים אלה נערכו להתמודדות עם מתקפות סייבר על "קו המגע הסייברי" בחגים ובסופי שבוע?[67]
6. כיצד גופים אלה נערכו למתן מענה מיידי בקרות התקפת סייבר נרחבת ומורכבת?[68]

המענה על שאלות אלו רלוונטי ביותר להתמודדות עם סיכונים משולבים אפשריים בזירת הסייבר. למשל, הסיכון כי גופים בעלי חשיבות במשק מותקפים כבר בעת הזו או יותקפו בעתיד באופן שעלול להשבית או לשבש את פעילותם או לגרום לדלף המידע האגור והמטופל בהם; התרחשותן בהווה של תקיפות סייבר שקטות (שלא התגלו); הפעלת התקיפות השקטות בזמן מלחמה או חירום והעצמת התקיפות בזמן מלחמה או חירום; שימוש של האויב בידע וביכולות סייבר מתקדמים המתקבלים ממדינות בעלות יכולות מעצמתיות.

**בבדיקה שביצע מבקר המדינה בעניין זה במקורות גלויים נמצא דוח של חברת Statista[69] שממנו עולה כי נכון לשנת 2023, תוקף נמצא ברשת בממוצע 204 ימים לפני הזיהוי שלו על ידי גורמי ההגנה בסייבר. נכון לשנת 2024 נתון זה עומד על 194 ימים בממוצע. בפרק זמן זה יכול התוקף להכיר את הרשת, את חולשותיה ואת פרצות האבטחה בה, להדליף מידע, לשבש מידע או לבצע כל פעולה אחרת.**

תרשים 15: **הזמן הממוצע לזיהוי ולהכלה של תקיפות סייבר ברחבי העולם, 2017 - 2024 (בימים)**




המקור: statista.com.

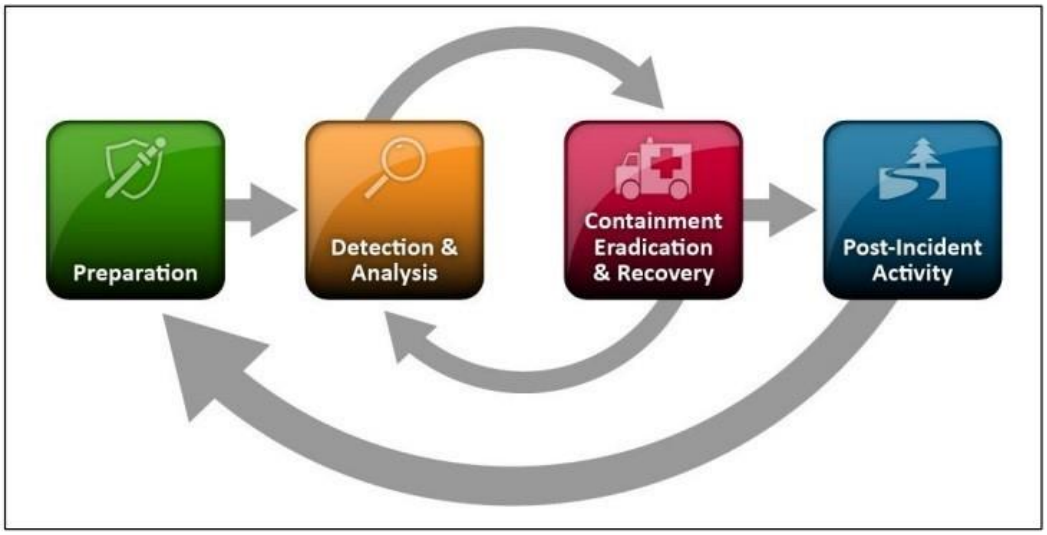
63 ראו סעיף "תהליכים אופרטיביים של מעקב אחר התרעות ושל קבלת החלטות בדבר דרך הטיפול בהן".
64 ראו סעיפים "היכרות יחידות הסייבר המגזריות עם תמונת המצב בנושא אירועי הסייבר בגופים" ו-"מערך הסייבר הלאומי - תשתית לאומית לגילוי אירועי סייבר".
65 ראו סעיפים "היכרות יחידות הסייבר המגזריות עם תמונת המצב בנושא אירועי הסייבר בגופים" ו-"מערך הסייבר הלאומי - תשתית לאומית לגילוי אירועי סייבר".
66 ראו סעיף "הכוונת מאמץ ההיערכות לאירועי סייבר".
67 ראו סעיף "היערכות הגופים החיוניים לניטור התרעות סייבר לאחר שעות הפעילות, בסופי שבוע ובחגים".
68 ראו סעיף "היערכות לביצוע פעילויות כדי להתמודד עם אירועי סייבר משמעותיים".
69 www.statista.com/statistics/1417455/worldwide-data-breaches-identify-and-contain

ההתייחסות להתרחשות כלשהי כאל אירוע סייבר יכולה להיות שונה מגוף לגוף. אחד המאפיינים הבולטים המשפיעים על ההכרה בהתרחשות כאירוע סייבר הוא העצימות של אותה התרחשות. ככל שהעצימות של ההתרחשות גבוהה יותר, גוברת הסבירות שהיא תוכר כאירוע סייבר. בחלק זה של הדוח נבחנים ההיערכות והמענה של הגופים והמאסדרים לאירועי סייבר במובנם הרחב ביותר תוך התייחסות להתרחשויות בעצימות נמוכה יחסית כאל אירועי סייבר פוטנציאליים לכל דבר ועניין.

## מערך ההגנה וההיערכות הארגונית להתמודדות עם אירועי סייבר

הקמת מעטפת הגנה על ארגון מתאפיינת ביצירת כמה מעגלי הגנה[70], בהסתמך על הנחת היסוד כי "קו המגע לעולם ייפרץ"[71]. נהוג להתייחס לקו ההגנה הראשון כאל מנגנון שמהותו מניעת תקיפה: יישומם של אמצעים טכנולוגיים, תהליכיים או אנושיים שמטרתם למנוע מהתוקף להשיג גישה למערכות התקשוב של הארגון. ההנחה שביסוד קו ההגנה השני היא כי ייתכן שהתוקף יצליח להתגבר על מאמץ המניעה ולהשיג גישה מְפַגַּעַת. לכן מטרות קו ההגנה השני הן לגלות את התקיפה זמן קצר ככל שאפשר לאחר שאירעה (באמצעות יכולות גילוי), לנתח ולחקור את האירוע, לנסות למנוע את התפשטותו (להכיל אותו), להסיר את האיום, לתקן ליקויים, להתאושש ממנו ובמידת הצורך להשיב את הארגון לתפקוד. בסוף התהליך על הארגון להפיק לקחים (שלב העמידות), ראו את התרשים שלהלן.

תרשים 16: **שלבי ההתמודדות של ארגון עם אירוע סייבר**




המקור: תקן NIST SP 800-61r2[72].

## המערך המשמש את הגופים לגילוי אירועי סייבר ולטיפול בהם

כאמור, האחריות לגילוי אירוע סייבר ולטיפול בו היא בידי הגופים שאחראים להגן על נכסי המידע שלהם, לנוכח ההבנה שאירוע סייבר עלול לפגוע ביעדים שהם מחויבים לעמוד בהם ולנוכח מחויבותם לקיום החוקים בתחום אבטחת המידע, לעמידה ברגולציות ולשמירה על מידע מסווג או פרטי. יתרה מזו - גופים אלה הם המנהלים את מערכות התקשוב שבשימושם, ולכן הם מיטיבים להכיר, יותר מכל גורם אחר, את אותן מערכות ואת הכלים המתאימים לניהולן. תפקיד הגופים האסדרתיים המדינתיים בתחום הסייבר הוא, בין היתר, להנחות את הגופים שלהם

---

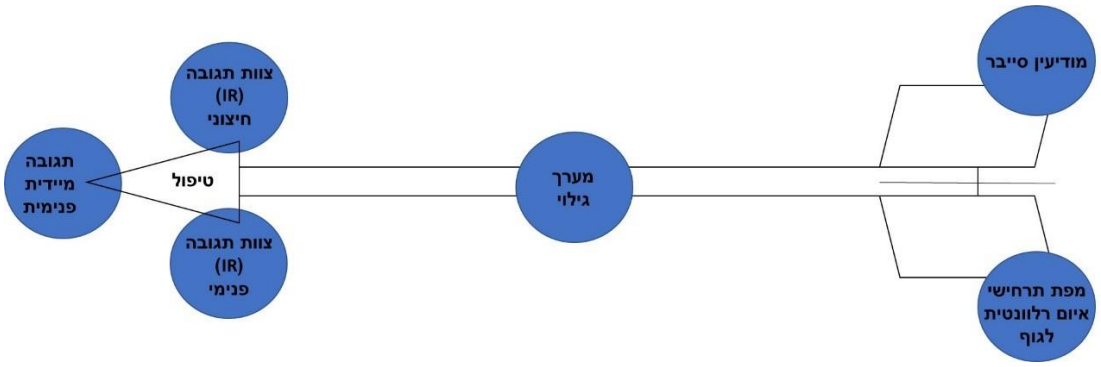
70 יגאל אונא; מאי 2019; "הגנת מרחב הסייבר הלאומי"; **סייבר, מודיעין וביטחון**, כרך 3, גיליון 1.

71 הרצי הלוי; אוקטובר 2020; "הגנה רב-ממדית"; **בין הקטבים - עליונות צבאית ותר"ש "תנופה"** 28 - 30.

72 nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

בתחום הסייבר, לפקח על רמת העמידה שלהם בדרישות הסייבר החלות עליהם, לגבש תמונת מצב מדינתית ולסייע לגופים בעת תקיפת סייבר חמורה בהתאם לקריטריונים ולסדר עדיפות.

תרשים 17: **מבנה מערך לגילוי אירועי סייבר בארגון ולטיפול בהם**




הוכן בידי משרד מבקר המדינה.

## מתודולוגיות ותקנים רלוונטיים

כאמור, הביקורת שממצאיה מפורטים בחלק זה של הדוח מבוססת על מתודולוגיות, תקנים והנחיות מקובלים בארץ ובעולם. בלוח שלהלן מוצגים לצד כל הנחיה הפרקים הרלוונטיים בדוח וכן אם היא מחייבת את הגופים שנבדקו בדוח:

לוח 8: **מתודולוגיות, תקנים ומסמכי הנחיה מרכזיים הרלוונטיים לבדיקות הביקורת**

| שם הנורמה | סוג המסמך | הפרקים בדוח שנעשה בהם שימוש בנורמה |
|---|---|---|
| תורת ההגנה 2.0, כולל מסמך הבקרות בגרסה 1.3 | מסמך תורתי-לאומי שפרסם מערך הסייבר כהמלצה לכלל המשק | הכוונת מאמץ ההיערכות לאירועי סייבר |
| | | תכנון ויישום של אמצעים טכנולוגיים לגילוי אירועי סייבר ולהתרעה עליהם |
| | | תהליכים אופרטיביים של מעקב אחר התרעות ושל קבלת החלטות בדבר דרך הטיפול בהן |
| | | תכנון של דרכי הטיפול באירועי סייבר ושל הטמעתן בתהליכי העבודה |
| | | היערכות לביצוע פעילויות כדי להתמודד עם אירועי סייבר משמעותיים |
| | | תחקור אירועי סייבר והפקת לקחים מהם |
| ISO 27001-2013 | תקן בין-לאומי שמחייב את משרדי הממשלה | הכוונת מאמץ ההיערכות לאירועי סייבר |
| הנחיית יה"ב 5.3 | הנחיה מגזרית שמחייבת את משרדי הממשלה | הכוונת מאמץ ההיערכות לאירועי סייבר |
| NIST SP-800-30r1 | פרסום של ארגון תקינה אמריקאי מקובל[73] | הכוונת מאמץ ההיערכות לאירועי סייבר |

[73] National Institute of Standards and Technology - NIST הוא מוסד ממשלתי אמריקאי במשרד הכלכלה של ארה"ב. מוסד זה מפרסם תקנים שארגונים מקצועיים ברחבי העולם מקבלים על עצמם כאמות מידה מקצועיות לתפקוד. מערך הסייבר הלאומי מקבל את תקינת NIST כתקינה מומלצת במסמכים מקצועיים שהוא מפרסם ואף הסתמך על אחד מתקני NIST כבסיס מחייב בחוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראה שעה - חרבות ברזל), התשפ"ד-2023.

| שם הנורמה | סוג המסמך | הפרקים בדוח שנעשה בהם שימוש בנורמה |
|---|---|---|
| CK&ATT MITRE | פרסום של ארגון תקינה אמריקאי מקובל[74] | הכוונת מאמץ ההיערכות לאירועי סייבר |
| NIST SP-800-61r2 | פרסום של ארגון תקינה אמריקאי מקובל | תכנון ויישום של אמצעים טכנולוגיים לגילוי אירועי סייבר ולהתרעה עליהם |
| | | תכנון של דרכי הטיפול באירועי סייבר ושל הטמעתן בתהליכי העבודה |
| | | היערכות לביצוע פעילויות כדי להתמודד עם אירועי סייבר משמעותיים |
| | | תחקור אירועי סייבר והפקת לקחים מהם |
| NIST SP-800-53r5 | פרסום של ארגון תקינה אמריקאי מקובל | תכנון ויישום של אמצעים טכנולוגיים לגילוי אירועי סייבר ולהתרעה עליהם |
| | | תהליכים אופרטיביים של מעקב אחר התרעות ושל קבלת החלטות בדבר דרך הטיפול בהן |
| | | תכנון של דרכי הטיפול באירועי סייבר ושל הטמעתן בתהליכי העבודה |
| הנחיית יה"ב 5.4 | הנחיה מגזרית שמחייבת את משרדי הממשלה | תהליכים אופרטיביים של מעקב אחר התרעות ושל קבלת החלטות בדבר דרך הטיפול בהן |
| מדד יה"ב 2.0 | כלי בקרה מגזרי המחייב את משרדי הממשלה | תכנון ויישום של אמצעים טכנולוגיים לגילוי אירועי סייבר ולהתרעה עליהם |
| הנחיית יה"ב 5.22 | הנחיה מגזרית שמחייבת את משרדי הממשלה | תכנון של דרכי הטיפול באירועי סייבר ושל הטמעתן בתהליכי העבודה |
| | | תחקור אירועי סייבר והפקת לקחים מהם |
| תפיסה לאומית בסייבר להיערכות ולניהול מצבי משבר | מסמך תורתי-לאומי שפרסם מערך הסייבר כהמלצה לכלל המשק | הכוונת מאמץ ההיערכות לאירועי סייבר |
| | | תהליכים אופרטיביים של מעקב אחר התרעות ושל קבלת החלטות בדבר דרך הטיפול בהן |
| | | היערכות לביצוע פעילויות כדי להתמודד עם אירועי סייבר משמעותיים |

הוכן בידי משרד מבקר המדינה.

## הכוונת מאמץ ההיערכות להתמודדות עם אירועי סייבר

הכוונת מאמץ ההיערכות של גוף לאירועי סייבר נועדה מחד גיסא למקד את הגוף בפעילויות הנדרשות ומאידך גיסא לוודא כי הגוף נותן מענה מקיף על הסוגים השונים של אירועי הסייבר העלולים להתרחש בו. הכוונה זו נבחנה בביקורת לפי אופן ביצועם של התהליכים העיקריים האלה:

1. קבלת מודיעין סייבר מגופי האסדרה המדינתיים (מערך הסייבר ויחידות הסייבר המגזריות).

2. גיבוש מפת איומים וסיכונים רלוונטית.

[74] MITRE הוא ארגון אמריקאי ללא כוונות רווח העוסק במחקר ופיתוח במימון פדרלי. עם תחומי המחקר שלו נמנים טכנולוגיית מכ"ם, סייבר, GPS. מערך הסייבר הלאומי הצטרף בשנת 2021 לתוכנית של הארגון לרישום פגיעויות במוצרים טכנולוגיים (www.gov.il/he/pages/cve_cna).

### קבלת מודיעין מגופי האסדרה

**נמצא כי כל הגופים בעלי החשיבות במשק שמילאו את השאלון דיווחו כי הם מקבלים מודיעין סייבר מגופי האסדרה המדינתיים. עם זאת כאמור יחידות הסייבר המגזריות שנבדקו בדוח ציינו כי המודיעין שמעביר להם מערך הסייבר לוקה בחסר (בעניין זה ראו לעיל).**

### גיבוש מפת איומים וסיכונים רלוונטית

תהליך גיבוש מפת איומים וסיכונים נועד למקד את אמצעי ההגנה ולנהל אותם ביעילות. ניתוח זה מתחיל במיפוי נכסי המידע של הארגון, כגון מערכות המידע ומאגרי המידע של הארגון, ובהגדרת רמת הערכיות שלהם בהתאם לתהליכים בארגון וממשיך בניתוח של הסיכונים ותרחישי האיום הנוגעים לנכסי המידע. על פי המלצות מסמך "תורת ההגנה 2.0", על הנהלת הארגון מוטלת האחריות להבנת הסיכונים ולניהולם, ולכן יש חשיבות לקיום תהליכים שבמסגרתם יוצגו להנהלה נושאים מרכזיים לצורך אישורה ולצורך קבלת דירקטיבות (מיפוי וסיווג נכסי מידע, הגדרת התהליכים העסקיים הקריטיים, ניתוח איומים וסיכונים, סטטוס הטיפול בסיכונים וכו'). תהליך הניתוח של איומים וסיכונים מפורט בתקנים מקובלים ובהם NIST, כמפורט בתרשים שלהלן.

תרשים 18: **מודל דוגמה לניתוח איומים וסיכונים**

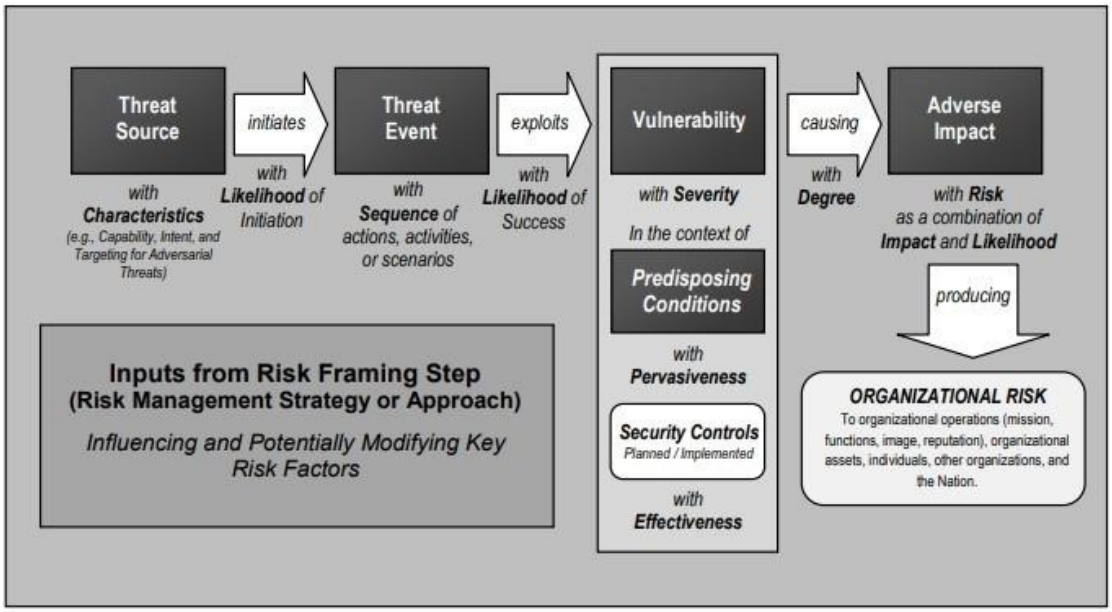
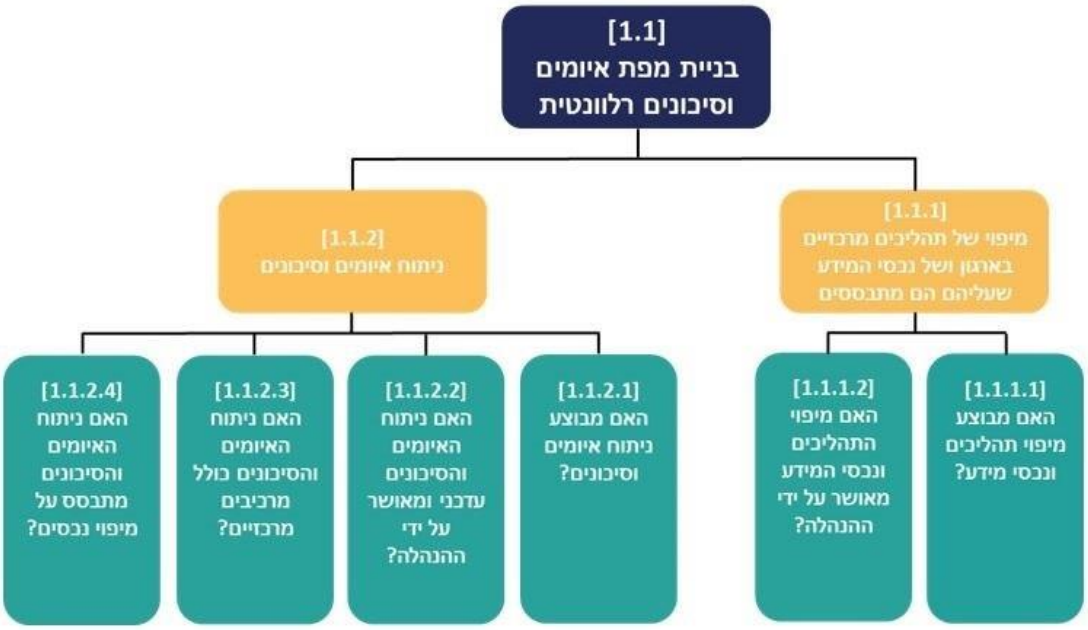



FIGURE 3: GENERIC RISK MODEL WITH KEY RISK FACTORS

המקור: תקן NIST SP 800-30r1[75].

[75] nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

תרשים 19 : **גיבוש מפת איומים וסיכונים רלוונטית - מרכיבי בדיקת משרד מבקר המדינה**

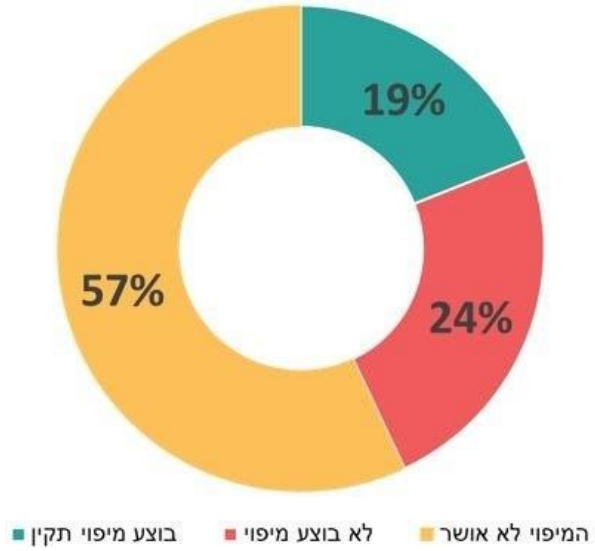



הוכן בידי משרד מבקר המדינה ; מבוסס בין היתר על תורת ההגנה 2.0, סעיף 2.1 ונספח ב' וכן על בקרות תורת ההגנה בסייבר 2.0, גרסה 1.3, סעיפים 1.2 ו-2.1.

## מיפוי של תהליכים מרכזיים ושל נכסי המידע בגופים בעלי חשיבות במשק

בביקורת נשאלו 21 הגופים שנבדקו, לפני מתקפת הטרור בשבעה באוקטובר, אם במהלך השנתיים האחרונות (יוני 2021 עד יולי 2023) הם מיפו תהליכים ונכסי מידע, מהי מידת העדכניות של המיפוי והאם ההנהלה אישרה אותו.

תרשים 20 : **פילוח הגופים שנבדקו על פי תשובותיהם על השאלון בנושא מיפוי תהליכים מרכזיים ונכסי מידע, יוני 2021 עד יולי 2023, לפני מתקפת הטרור בשבעה באוקטובר**




על פי מענה הגופים על השאלונים, בעיבוד משרד מבקר המדינה.

**נמצא כי 5 (24%) מתוך 21 הגופים בעלי החשיבות במשק שהשיבו על השאלון דיווחו כי בין יוני 2021 ועד יולי 2023 ולפני מתקפת הטרור בשבעה באוקטובר לא ביצעו מיפוי של תהליכים מרכזיים ושל נכסי מידע שעליהם התהליכים מתבססים. עוד נמצא כי 12 (57%) מ-21 הגופים דיווחו כי ההנהלה לא אישרה בתקופה זו את המיפוי שבוצע, כל זאת באופן שאינו עולה עם תקנים, מדיניות והנחיות המקובלים בתחום. נוכח זאת, ייתכן שמעטפת ההגנה שהוקמה בגופים אלו אינה מגינה על חלק מנכסי המידע המרכזיים הקיימים בארגון והדבר פוגע ביכולתם לגלות ולסכל אירועי סייבר במהירות ובאופן מקיף.**

בתשובות אחד הגופים נמסר כי מאחר שמדובר בגוף קטן, המנכ"ל מכיר את נכסי המידע של החברה.

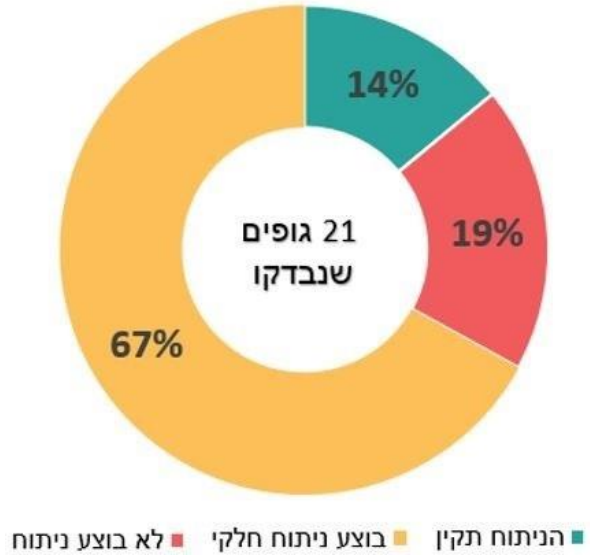
**על הגופים שדיווחו כי לא ביצעו מיפוי לבצע מיפוי עדכני ומלא של תהליכים מרכזיים בארגון ושל נכסי מידע שעליהם התהליכים מתבססים. כמו כן על הגופים שדיווחו כי לא קיבלו מההנהלה אישור למיפוי להשלים את התהליך ולקבל את האישור הדרוש בכתב.**

בתשובות חלק מהגופים נמסר כי הפער יטופל וחלק מהגופים כבר פעלו לביצוע המיפוי.

### ניתוח של איומים וסיכונים

בביקורת נשאלו 21 הגופים שנבדקו, לפני מתקפת הטרור בשבעה באוקטובר, האם במהלך השנה וחצי האחרונות (ינואר 2022 עד יולי 2023) ביצעו תהליך של ניתוח איומים וסיכונים, ואם כן - האם הניתוח עדכני, מלא[76] ומאושר על ידי ההנהלה.

תרשים 21: **פילוח הגופים שנבדקו לפי תשובותיהם על השאלון בנושא ניתוח איומים וסיכונים, ינואר 2022 עד יולי 2023, לפני מתקפת הטרור בשבעה באוקטובר**



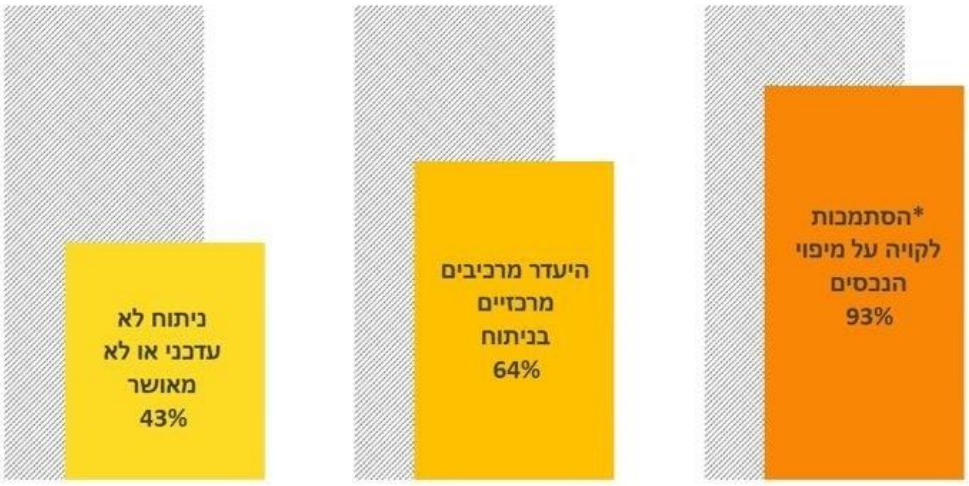

על פי מענה הגופים על השאלונים, בעיבוד משרד מבקר המדינה.

**נמצא כי דיווחיהם של 18 (86%) מתוך 21 הגופים בעלי החשיבות במשק שהשיבו על השאלון מעידים כי בין ינואר 2022 ועד יולי 2023 ולפני מתקפת הטרור בשבעה באוקטובר היה אצלם פער בנושא ניתוח האיומים והסיכונים: 14 מהגופים (67%) ביצעו את ניתוח האיומים והסיכונים באופן חלקי, וארבעה גופים אחרים (19%) דיווחו כי לא ביצעו כלל תהליך זה, זאת אף שניתוח**

[76] ניתוח מלא - על פי תקנים מקובלים בתחום, כגון NIST SP 800-30r1.

**כאמור הוא הבסיס המומלץ להקמת מעטפת הגנה מתאימה לארגון, לניהול יעיל שלה ולהשקעת משאבים יעילה, ובלעדיו ייתכן שחלק מתרחישי האיום לא יזוהו ולא יטופלו.**

תרשים 22: **האופנים שבהם ניתוח האיומים והסיכונים היה חלקי כפי שעלה מתשובותיהם של 14 הגופים שבהם נמצא פער זה**




על פי מענה הגופים על השאלונים, בעיבוד משרד מבקר המדינה.
* ניתוח האיומים לא התבסס על מיפוי נכסים או התבסס על מיפוי נכסים חסר או לא עדכני.

**אותם 14 גופים שתשובותיהם מעידות על ניתוח חלקי של איומים וסיכונים דיווחו באופן המצביע על אחת או יותר מהאפשרויות הבאות כסיבות לכך: (א) ב-6 גופים (43%) הניתוח לא היה עדכני או שלא היה מאושר בידי ההנהלה בשנה וחצי האחרונות (ב) ב-13 גופים (93%) הניתוח לא הסתמך כלל על מיפוי הנכסים או הסתמך על מיפוי נכסים חסר או לא עדכני (ג) ב-9 גופים (64%) הניתוח לא כלל מרכיבים מרכזיים שנדרשים במתודולוגיות מקובלות, ובהם הגדרת יעדי ההגנה, הגדרת תרחישי איום מרכזיים והערכת רמות האיום, זיהוי נכסי המידע החשופים לאיום וחישוב רמות הסיכון המוערכות.**

בתשובות חלק מהגופים נמסר כי הם פועלים לשיפור ניתוח האיומים. כך לדוגמה: אחד הגופים מבצע תיקוף והעמקה של ניתוח האיומים בשיתוף הגורם המנחה; אחד הגופים מיפה את הנכסים, ובהמשך ניתוח הסיכונים הוא יתמקד בנכסים בהתאם לרמת החיוניות שלהם; ואחד הגופים ביצע בשנת 2024 תהליך של ניתוח איומים וכתיבת תוכנית להפחתת הסיכונים.

**נוכח הפערים הרוחביים שנמצאו באופן ובאיכות של כתיבת ניתוח האיומים והסיכונים ונוכח חשיבות מסמכים אלו לבניית מעטפת הגנה ראויה בארגונים, מומלץ כי ברמה הלאומית יגדיר מערך הסייבר האחראי להנחיית גופים במשק[77] קווים מנחים לאופן הביצוע והכתיבה של ניתוח איומים וסיכונים. קווים אלו יגדירו, בין היתר, את המרכיבים המרכזיים הנדרשים להיכתב בניתוח ואת רמת הפירוט הנדרשת (למשל בהתאם לתקן NIST 800-30r1 או תורת ההגנה 2.0 של מערך הסייבר) ואת המדדים והיעדים לגבי אופן ניתוח האיומים והסיכונים. למשל: מידת התאמת התרחישים לאיום הייחוס הלאומי או המגזרי; מידת התאמת התרחישים לתרחישים מקובלים כמו MITRE ATT&CK; תדירות העדכון של ניתוח האיומים. כמו כן מומלץ כי מערך הסייבר יצרף תבנית של מסמך ודוגמאות לניתוח איומים.**

**נוסף על כך, נוכח העובדה ש-43% ממסמכי ניתוח האיומים שנבדקו לא היו עדכניים או לא אושרו על ידי ההנהלה, מומלץ כי מערך הסייבר יפעל לטיפול בפער זה במסגרת סמכויותיו בתחום ההנחיה והבקרה כדי לוודא שממוני אבטחת המידע בגופים במשק יציגו בישיבות ועדת היגוי**

77 החלטת הממשלה 2444 מגדירה את אחד מתפקידיו של מערך הסייבר הלאומי כהנחיית כלל המשק בתחום הגנת הסייבר (סעיף 2.ג) וכן מגדירה הנחיה עקיפה לגופים שונים באמצעות יה"ב ויחידות הסייבר המגזריות.

**סייבר להנהלות שלהם את ממצאי ניתוח האיומים ואת מידת העמידה של הארגון ביעדים שהוגדרו, וכן יעבירו נתונים אלה ולגופים האסדרתיים המדינתיים הרלוונטיים לצורך גיבוש תמונת מצב לעניין היערכות הגופים לאירועי סייבר.**

**מומלץ כי הגופים בעלי החשיבות במשק שדיווחו כי לא ביצעו ניתוח איומים וסיכונים מלא ומפורט של התהליכים המרכזיים בארגון ושל נכסי מידע שעליהם התהליכים מתבססים, שאותם מיפו ואישרו יבצעו את המיפוי והניתוח באופן מלא ומפורט ויביאו את אופן ביצועם לאישור ההנהלה.**

בתשובות חלק מהגופים נמסר כי הפער יטופל.

## <u>גילוי אירועי סייבר</u>

יכולתם של גופים לגלות אירועי סייבר בשלב מוקדם היא הבסיס למניעת התפשטות האירועים, לצמצום חומרת הנזק בגינם ולחזרה מהירה לשגרה. יכולת הגילוי של הגופים נבחנה בביקורת לפי אופן ביצועם של שני התהליכים העיקריים האלה:

1. תכנון ויישום של אמצעים טכנולוגיים לגילוי אירועי סייבר ולהתרעה עליהם.

2. תהליכים אופרטיביים של מעקב אחר התרעות והחלטה בדבר דרך הטיפול בהן.

### תכנון ויישום של אמצעים טכנולוגיים לגילוי אירועי סייבר ולהתרעה עליהם

**בחלק מהגופים נמצאו פערים בנושא. יצוין כי חלק מהפערים טופלו במהלך הביקורת.**

**מומלץ כי ברמה הלאומית יגדיר מערך הסייבר לגופים במשק מדדים ויעדים (KPI[78]) לבקרה על מערכות הגילוי שלהם ויגבש תמונת מצב בעניין מידת עמידתם של הגופים ביעדים.**

### תהליכים אופרטיביים של מעקב אחר התרעות ושל קבלת החלטות בדבר דרך הטיפול בהן

**בחלק מהגופים נמצאו פערים בנושא. יצוין כי חלק מהפערים טופלו במהלך הביקורת.**


**נמצא כי במועד האמור (ערב מלחמת חרבות ברזל), שניים מהגופים בעלי החשיבות במשק שענו על השאלון (10%) דיווחו כי כלל לא יושם בהם מערך ניטור אירועי סייבר וטיפול בהם (SIEM או SOC). הגופים דיווחו שבעקבות הביקורת הנושא תוקן.**

בתשובת אחד הגופים נמסר כי הוא רכש לאחרונה מערכת SIEM לניטור כל מקורות המידע באופן מרוכז כדי לאפשר מעקב קבוע ורצוף של התרעות והוא נמצא בשלבי הטמעה, וכי הוא נמצא בשלבי הטמעת ניטור מלא 24/7 באמצעות צוות SOC.

בתשובת אחד הגופים נמסר כי מאז הביקורת הוא עושה שימוש בשירות מנוהל (SOC, IR, PT וכו') לרשת הגוף באופן קבוע 24/7.

### שיעור העמידה של הגופים בקצב ההתרעות

**בחלק מהגופים נמצאו פערים בנושא. יצוין כי חלק מהפערים טופלו במהלך הביקורת.**

78 KPI - Key Performance Indicator.

**זמני הטיפול הראשוני בהתרעות**

**בחלק מהגופים נמצאו פערים בנושא. יצוין כי חלק מהפערים טופלו במהלך הביקורת.**

☆

גבוה

**מהנתונים שהוצגו עד כה ניתן להבחין כי לפני מתקפת הטרור בשבעה באוקטובר, ב-18 (86%) מ-21 הגופים בעלי החשיבות במשך שנבדקו היה פער בניתוח תרחישי האיום הנשקפים להם בממד הסייבר ושל הסיכונים הנובעים מהם.**

## טיפול באירועי סייבר

עם קבלת התרעה על חשד לאירוע סייבר נדרש הארגון להתחיל בטיפול בו. מהירות התגובה והאיכות שלה יקבעו את מידת הנזק שייגרם לארגון בגין האירוע. ניתן ללמוד מכך על החשיבות הרבה של היערכות מקדימה לשלב הטיפול, כדי שבקרות אירוע יתקצרו זמני התגובה. יכולות הגופים נבחנו בביקורת לפי אופן ביצועם של שני התהליכים העיקריים האלו:

1. תכנון דרכי הטיפול באירועי סייבר והטמעתן בתהליכי העבודה.
2. היערכות לביצוע פעילויות להתמודדות עם אירועי סייבר משמעותיים.

### תכנון של דרכי הטיפול באירועי סייבר ושל הטמעתן בתהליכי העבודה

תרשים 23: **פערים בתכנון דרכי הטיפול באירועי סייבר ובהטמעתן בתהליכי העבודה, יוני 2021 עד יולי 2023, לפני מתקפת הטרור בשבעה באוקטובר**


על פי מענה הגופים על שאלונים, בעיבוד משרד מבקר המדינה.

גבוה

**נמצא כי דיווחיהם של 20 מתוך 21 הגופים בעלי החשיבות במשך שהשיבו על השאלון (95%) העידו כי ערב מלחמת חרבות ברזל היה פער אחד לפחות באחת מהקטגוריות שנבדקו בעניין תכנון דרכי הטיפול באירועי סייבר ובהטמעתן בתהליכי העבודה. נוסף על כך בכל אחת מהקטגוריות שנבדקו נמצאו פערים בקרב 57% - 95% מהגופים. היערכות לקויה עשויה לפגוע ביכולת של הגופים לטפל באופן המיטבי באירוע סייבר עם התרחשותו.**

**מומלץ כי הגופים שבהם נמצאו הדיווחים המעידים על הפערים ישלימו את התכנון והאישור של דרכי הטיפול שלהם באירועי סייבר.**

בתשובות חלק מהגופים נמסר כי הפערים נמצאים בטיפול.

**היערכות להתמודדות עם אירועי סייבר משמעותיים**

ככלל, גופים מקבלים באופן שוטף התרעות שווא (False Positives) וכן הם מקבלים התרעות על אירועי סייבר בקנה מידה מצומצם, ואלה מטופלים במהירות. אירועים נפוצים פחות, אם כי מספרם אינו מבוטל, הם אירועי סייבר בקנה מידה גדול יותר (כגון אירוע הכופרה בבית החולים הלל יפה ואירוע הכופרה בטכניון). הגופים נדרשים לקיים היערכות נרחבת יותר לאירועים משמעותיים אלה, שכן בקרות אירוע הם נדרשים להפעיל צוותים רבים, ובהם צוות תגובה טכנולוגי חיצוני וצוות ניהול משבר סייבר ברמת ההנהלה, לקיים פעילות של הדוברות ולהסתייע בגופי האסדרה המדינתיים בתחום הסייבר.


**נמצא כי דיווחיהם של חלק מתוך 21 הגופים בעלי החשיבות במשק שהשיבו על השאלון העידו כי ערב מלחמת חרבות ברזל, היה פער לפחות באחת משלוש הקטגוריות שבחנו את אופן היערכותם לביצוע פעילויות כדי להתמודד עם אירועי סייבר משמעותיים. הדבר עלול לגרום לכך שגופים אלה יתקשו להתמודד באופן המיטבי עם אירועי סייבר משמעותיים וכתוצאה מכך הנזק יגדל.**

**מומלץ כי הגופים שדיווחיהם מעידים על פערים ובהתאם לפער שנמצא אצלם יטפלו בפערים, כדי שביום שבו יתרחש האירוע הם יהיו ערוכים לכך באופן המיטבי.**

בתשובות חלק מהגופים נמסר כי הפערים מטופלים.

**נוכח הפער שנמצא בחלק מ-21 הגופים בעלי החשיבות במשק שנבדקו מומלץ כי מערך הסייבר ויחידות הסייבר המגזריות יבדקו את המצב בכלל הגופים המונחים שלהם ויפעלו לתיקון הפערים ככל הנדרש.**

בתשובת אחת היחידות המגזריות נמסר כי ההמלצה מוטמעת בתוכנית העבודה של המגזר מול הגופים.

בתשובת אחת היחידות המגזריות נמסר כי היחידה מיישמת אמצעים למניעת משבר סייבר באמצעות דרישה רגולטורית לניהול סיכוני סייבר והתמודדות עם תקיפות סייבר. עוד נמסר כי היחידה אוכפת על הגופים המונחים את הדרישות ומפקחת על עמידתם בדרישות אלה.

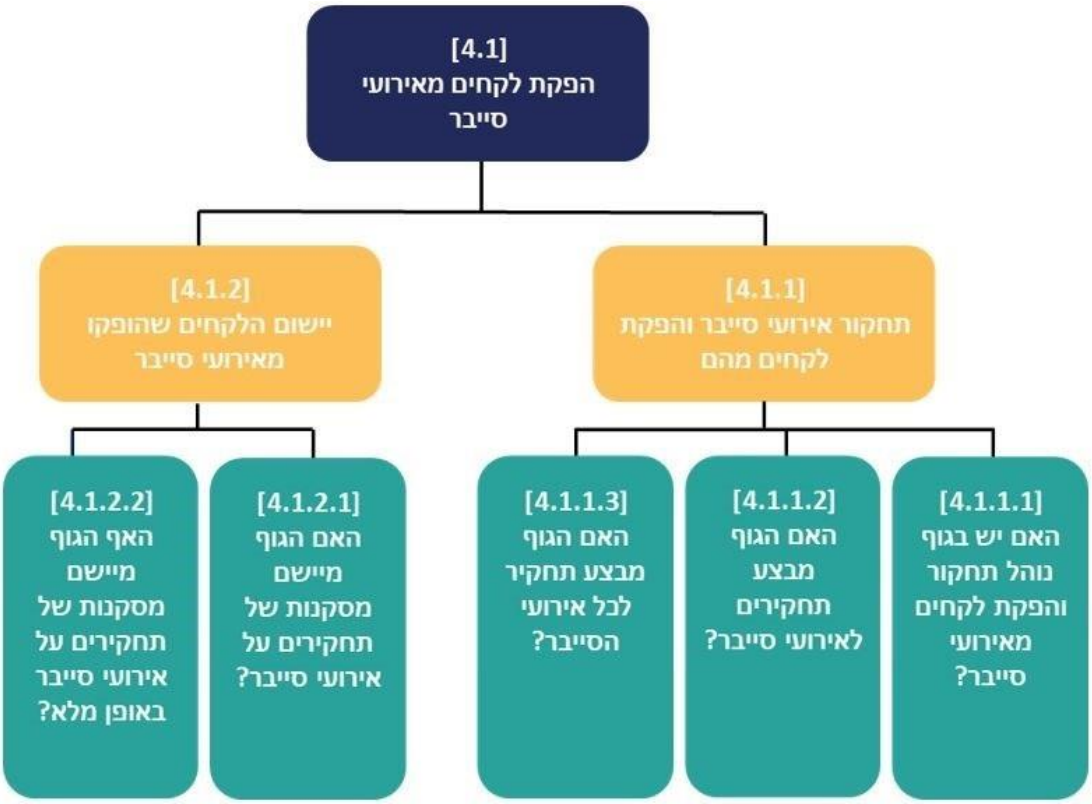
בתשובת אחת היחידות המגזריות נמסר כי היא מקיימת באופן קבוע בדיקה בכלל הגופים המונחים על ידה, בוחנת את הפערים ומחדדת הנחיות בהתאם.

## <u>הפקת לקחים מאירועי סייבר</u>

לאחר סיומו של אירוע סייבר על הארגון לזהות את הגורמים לאירוע ואת נקודות התורפה שאיפשרו את התרחשותו, וכן עליו להפיק לקחים בעניין האירוע וליישם אותם. בשאלונים שמשרד מבקר המדינה שלח לארגונים הם התבקשו לדווח על שלושת אירועי הסייבר המשמעותיים ביותר שהם חוו בשנים 2021 - 2023, והביקורת התבססה על דיווחיהם בשאלונים. במסגרת שלושת האירועים האמורים התמקדה הביקורת בשני התהליכים האלו:

1. תחקור אירועי סייבר והפקת לקחים מהם.
2. יישום הלקחים שהופקו מאירועי סייבר.

תרשים 24 : **הפקת לקחים מאירועי סייבר - מרכיבי בדיקת משרד מבקר המדינה**




הוכן בידי משרד מבקר המדינה; מבוסס בין היתר על בקרות תורת ההגנה 2.0, גרסה 1.3, סעיפים 18.2, 19.1.

## תחקור אירועי סייבר והפקת לקחים מהם

במסגרת הביקורת נשאלו 21 הגופים שנבדקו אם יש בידם נוהל לתחקור אירועי סייבר ולהפקת לקחים מהם וכן אם הם מבצעים תחקור של אירועי הסייבר שהתרחשו אצלם ומפיקים מהם לקחים.

**נמצא כי שניים (9%) מתוך 21 הגופים בעלי החשיבות במשק שהשיבו על השאלון דיווחו כי אין בידם נוהל תחקור והפקת לקחים מאירועי סייבר. כל הגופים שהשיבו על השאלון וציינו כי חוו אירוע סייבר משמעותי בשלוש השנים האחרונות דיווחו כי ביצעו תחקור של אירועים אלו.**

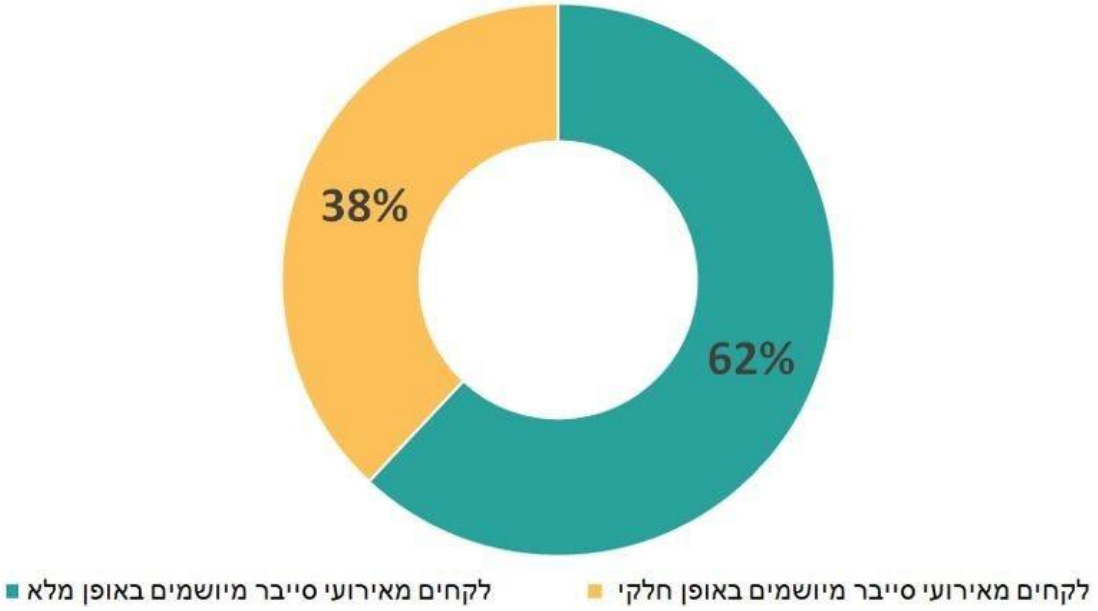
**מומלץ כי הגופים שבהם נמצא פער יכינו נוהל תחקור אירועי סייבר.**

בתשובת גוף מסוים נמסר כי פער זה נמצא בתהליכי השלמה.

### יישום הלקחים שהופקו מאירועי סייבר

במסגרת הביקורת נבדק אם 13 הגופים שנבדקו שדיווחו בשאלון כי חוו אירועי סייבר דיווחו על יישום מלא של הלקחים מהם.

תרשים 25: **פילוח הגופים שהשיבו כי חוו אירועי סייבר לפי המידה שבה יישמו את הלקחים שהפיקו מהם**




על פי המענה של הגופים על השאלונים, בעיבוד משרד מבקר המדינה.


**נמצא כי חמישה (38%) מתוך 13 הגופים בעלי החשיבות במשק שהשיבו כי חוו אירועי סייבר דיווחו כי הם מיישמים באופן חלקי לקחים מאירועים אלה. ייתכן כי בגופים אלה אירועי הסייבר אינם מטופלים כנדרש, ולכן האירועים העתידיים יתרחשו בשל אותן הסיבות.**

בתשובת אחד הגופים נמסר כי הטכנולוגיות הרלוונטיות נרכשו, ויישומה המלא של הפקת הלקחים מבוצעת בהתאם להערכת הסיכון ולחומרתו.

בתשובת אחד הגופים נמסר כי לקחי תחקירים מיושמים במסגרת המשאבים והכלים העומדים לרשותו ככל שניתן.

בתשובת אחד הגופים נמסר כי יישום לקחים מתחקירים מבוצע בתהליך ניהול סיכונים על בסיס בחינת היתכנות, יכולת ותיעדוף משאבים.

**מומלץ כי גופים שדיווחו כי יישמו באופן חלקי לקחים מאירועי סייבר יישמו באופן מלא לקחים מאירועים אלה.**

בתשובת גוף מסוים נמסר כי מושקעים משאבים רבים ביישום לקחים מאירועי סייבר, אך לנוכח המגבלות השונות לא תמיד מגיעים ליישום מלא.

## <u>תמונת המצב בעניין יחידות הסייבר המגזריות</u>

**בחלק מהגופים נמצאו פערים בנושא. יצוין כי חלק מהפערים טופלו במהלך הביקורת.**

## מערך הסייבר הלאומי - תשתית לאומית לגילוי אירועי סייבר

**נמצאו פערים בנושא זה וחלקם טופלו.**

## סיכום

**במהלך מלחמת חרבות ברזל חל גידול בהיקף ובעוצמה של מתקפות הסייבר נגד גופים במשק הישראלי שנועדו לפגוע בביטחון המדינה, בביטחון הציבור ובחוסן הלאומי ולאסוף מידע לצרכי מודיעין. אמנם מפרוץ המלחמה ועד יוני 2025 מדינת ישראל לא חוותה אירוע סייבר שפגע באופן משמעותי בתהליכים עסקיים קריטיים שהשפיעו באופן מהותי על המשק - יחד עם זאת, על פי מערך הסייבר באוקטובר 2024 מצב בשלות הגנת הסייבר במשק לא היה מספק והשיפור הדרמטי בקצב וביכולות התקיפה חייב נקיטת פעולות לחיזוק קו ההגנה ולהבטחת רציפות התפקוד ברמה המשקית והביטחונית.**

**מתקפת שבעה באוקטובר המחישה את ההשפעה הדרמטית שיש להיערכות המוקדמת ולטיפול בסימני האזהרה שקדמו לה. ניתן להצביע על חמש שאלות עיקריות הנוגעות גם להיערכות המוקדמת בתחום הסייבר ושנמצאו בהם פערים משמעותיים בדוח זה:**

1. **האם הוגדר איום ייחוס, ואם כן - מה הייתה מידת ההלימה בינו ובין המצב בפועל?**

2. **מה הייתה רמת ההגנה של המדינה ורמת מוכנותה להתמודדות עם איום הייחוס ערב המלחמה?**

3. **איזה מידע הוצג לפני הממשלה ומקבלי ההחלטות בנוגע לרמת ההגנה ולרמת מוכנותה של המדינה להתמודדות עם האיום ואילו פעולות בוצעו בנושא?**

4. **אילו התרעות הועברו לדרג המדיני ולדרג מקצועי ואילו פעולות בוצעו בנושא?**

5. **האם מפרוץ המלחמה בוצעו הפעולות הנדרשות לצמצום הפערים ולתיקון הליקויים, והאם ההתנהלות של הדרג המדיני, הגופים האסדרתיים המדינתיים, הגופים המונחים והמשק הייתה מספקת?**

**החלטות הממשלה מזה כעשור הניחו מערך תפקודי שמכפיף את הטיפול באיומי הסייבר ברמה הלאומית-ממשלתית לראש הממשלה; זאת על ידי הגדרת ממד הסייבר כיעד חיוני לביטחונה הלאומי של המדינה, הקמת גוף מטה ייעודי לנושא (מערך הסייבר) שכפוף ישירות לראש הממשלה ופועל במסגרת משרדו והענקת סמכויות ייעודיות לראש הממשלה בתחום זה.**

**מערך הסייבר אמון על הגנת מרחב הסייבר הלאומי ועל הקידום והביסוס של עוצמתה של ישראל בתחום זה, והנהלת כל גוף אחראית להגנת הסייבר בתחום אחריותה.**

**להלן פירוט פערים מערכתיים ומסקנות ביקורתיות העולות מממצאי דוח זה:**

1. **לפי מערך הסייבר רמת ההגנה של חלק מהמגזרים במשק לפני המלחמה ובמהלכה הייתה לא מספקת ועלולה לא לעמוד בפני אתגרי העתיד: בהחלטת ועדת שרים ב/43 נקבע כי איום הסייבר (טרור סייבר) עלול לגרום למצב חירום לאומי.**

   א. **במהלך כשנה וחצי לפני פרוץ מלחמת חרבות ברזל, הציג מערך הסייבר במספר סקירות לרבות לצוות בין- משרדי, לשרת המודיעין דאז גב' גילה גמליאל ובאופן חד פעמי לפורום שרים בראשות ראש הממשלה בנימין נתניהו תמונת מצב ולפיה רמות ההגנה בתחום**

**הסייבר בחלק מסוים מהמגזרים במשק הישראלי (לא כולל גופי התמ"ק) אינן מספקות. בנוסף לפני המלחמה (בשנת 2023), חלק מגופי התמ"ק היו ברמות הסמכה המשקפות יכולת התמודדות מוגבלת עם תוקפים.**

**ב. באוקטובר 2024, שנה אחרי פרוץ מלחמת חרבות ברזל, ראש מערך הסייבר דאז דיווח כי מצב בשלות הגנת הסייבר במשק אינו מספק וכי השיפור הדרמטי בקצב וביכולות התקיפה מחייב נקיטת פעולות לחיזוק קו ההגנה ולהבטחת רציפות התפקוד ברמה המשקית והביטחונית. ביוני 2025 חל שיפור בציוני ההסמכה של גופי התמ"ק אולם עדיין היה קיים פער במועד זה.**

**2. אי-הצגת תמונת מצב בתחום הסייבר באופן שוטף לקבינט מדיני-ביטחוני: בעשור לפני מלחמת חרבות ברזל ועד יוני 2025, ראשי הממשלה לא יזמו ולא קיימו בקבינט דיונים ייעודיים בנושא הסייבר למעט פגישה ייעודית אחת שהתקיימה בשנת 2018. ועם זאת, נושא הסייבר הוזכר במסגרת דיונים שהנושאים שלהם היו רחבים יותר: הערכות מודיעין שנתיות, בחלק מהדיונים בנושא תמונת מצב רב-זירתית ובדיון אחד שהתקיים אחרי פרוץ המלחמה בנושא מסוים. זאת אף שהגנה על מרחב הסייבר הוא יעד ביטחוני לאומי כפי שנקבע בהחלטת הממשלה 2444. כתוצאה מכך, בתקופת הביקורת הקבינט לא נחשף למכלול הסיכונים בתחום הסייבר, לרמת ההיערכות ולנזקים הפוטנציאליים.**

**3. איומי ותרחישי ייחוס ברמה הלאומית והמגזרית לפני פרוץ המלחמה: במהלך השנים מערך הסייבר לא תיקף את איום הייחוס הלאומי כמתחייב בהחלטת ממשלה 3611. ערב המלחמה, ועד יוני 2025, הפעולות להכנה של איומי ותרחישי ייחוס מגזריים לא הושלמו.**

**4. התרגול שהתקיים לפני פרוץ המלחמה להתמודדות עם אירועי סייבר היה לא מספק בכל הרמות שנבדקו בדוח: ברמה הלאומית - משנת 2018 ועד נובמבר 2024 לא התקיים תרגיל סייבר לאומי ייעודי. בתרגיל שבוצע בשנת 2018 ובתרגילים שהתקיימו החל משנה אחרי פרוץ המלחמה, בנובמבר 2024 ובמרץ 2025 לא השתתפו נציגים מהדרג המדיני - ראש הממשלה, קבינט מדיני-ביטחוני ושרים; ברמה המגזרית - בחלק מהמגזרים נמצאו פערים; בחלק מ-21 הגופים שנבדקו - נמצאו פערים; בחלק מהגופים הרגישים המונחים על ידי מערך הסייבר - נמצאו פערים בשנים 2022 - 2023.**

**5. חולשה תפקודית של יחידות סייבר מגזריות: יה"ב (מערך הדיגיטל) ויחידות הסייבר המגזריות הן התשתית המקצועית והמעשית לקידום ההנחיה, ההכוונה, הפיקוח והבקרה בנוגע להגנת הסייבר במאות גופים ציבוריים ופרטיים המספקים שירותים חיוניים במגוון תחומים. בביקורת נמצא כי חלק מסוים ממערך יחידות הסייבר המגזריות מתאפיין בחולשה תפקודית משמעותית. עם זאת שלוש יחידות סייבר מגזריות התבלטו בפעולתן כלפי המגזרים שלהן.**

**6. ניתוח איומים וסיכונים כבסיס להכוונת ההיערכות להתמודדות עם אירועי סייבר: רוב הגופים שנבדקו (86%) אינם מבצעים ניתוח יסודי של תרחישי איום כבסיס לתכנון של מעטפת ההגנה שלהם בתחום הסייבר.**

**7. יישום התפיסה הלאומית לניהול מצבי משבר במרחב הסייבר: התפיסה הלאומית בנושא "טיפול במצבי חירום ובמשבר במרחב הסייבר" אינה עדכנית במשך שנים, תכולתה חסרה, מערך הסייבר לא הנחה את יחידות הסייבר המגזריות לפעול לפיה ולא פעל להטמיעה ולכן השימוש בה מועט.**

8. **תכנון דרכי טיפול באירועי סייבר והיערכות להתמודדות עם אירועי סייבר משמעותיים: בגופים שנבדקו נמצא פער משמעותי לעניין תכנון דרכי הטיפול באירועי סייבר וביצוע פעולות ההיערכות הנדרשות.**

9. **השלמת חקיקת חוק הסייבר: במשך יותר מעשור לא השלים משרד רה"ם את הפעולות לצורך חקיקה בכנסת של חוק ייעודי להסדרת תחום הסייבר. בשנים 2022 - 2025 פעל מערך הסייבר רבות יחד עם גופים נוספים לקידום החוק, אולם נכון ליוני 2025 טרם הסתיים הליך גיבוש הצעת החוק, טרם לובנו כלל המחלוקות שעלו על ידי המשרדים השונים ואף לא נקבעו לוחות זמנים להגשת הצעת החוק.**

**עם פרוץ המלחמה נקט מערך הסייבר פעולות מיידיות לזיהוי ולצמצום של פערים קריטיים ולחיזוק החוסן של המשק בתחום הסייבר, לרבות בתחום שרשרת האספקה הביטחונית. כמו כן המערך קידם אסדרה זמנית בחקיקה מוגבלת בזמן כדי להתמודד עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה - חרבות ברזל), ולצורך כך הסיט משאבים ושינה סדרי עדיפויות. עם זאת, אין בפעולות אלו שביצע המערך כדי לתת מענה מלא לפערים. על כן קיים הכרח בנקיטת פעולות נוספות כדי להתמודד עם התעצמות יכולות התקיפה ועם אתגרי העתיד.**

**על הגורמים הבאים לפעול להבטחת המענה לפערים המועלים בדוח זה ולתיקון הליקויים המפורטים בו, כל אחד בתחום אחריותו כמפורט להלן:**

1. **ראש הממשלה אשר אחראי להגנה בסייבר ברמה הלאומית הן כעומד בראש הקבינט המדיני ביטחוני והן באמצעות מערך הסייבר הלאומי והשב"כ הכפופים לו, ובנוסף לו גם העומדים בראש כל מגזר במשק.**

1. **מערך הסייבר אשר אחראי להגנת ממד הסייבר הלאומי ופועל ברמת המדינה לחיזוק תמידי של רמת ההגנה של הגופים במשק.**

2. **יתר הגופים האסדרתיים המדינתיים בתחום הסייבר - שב"כ, רח"ל, יה"ב ויחידות הסייבר המגזריות.**

3. **הנהלות הגופים שנמצאו בהם פערים בדוח - על כל אחד מהגופים המבוקרים לפעול לתיקון הפערים שהתגלו במסגרתו.**

**לאור ממצאי הדוח, על כלל הגורמים האמורים לראות בליקויים התרעה כוללת ומשמעותית המחייבת נקיטת פעולות, חלקן דחופות, ולפעול בהקדם לתיקונם. על מערך הסייבר בשיתוף משרדי הממשלה ויחידות הסייבר המגזריות לגבש תוכנית פעולה לאומית-ממשלתית שתבטיח צמצום פערים ברמת ההגנה הן בטווח הקצר והן בטווח הארוך ולהביאה לאישור הממשלה. מומלץ כי ראש הממשלה יזום ויקיים דיונים סדורים לצורך הצגת תמונת מצב היערכות המדינה לאירוע סייבר ופערים בה לצורך קבלת החלטות בקבינט המדיני-ביטחוני או בוועדת שרים ייעודית שתוקם לנושא זה וזאת באופן תקופתי ולפחות אחת לחצי שנה וכן מומלץ כי משרד ראש הממשלה והעומד בראשו יפעלו להשלמת חקיקת חוק הסייבר.**