דוח מבקר המדינה

סייבר ומערכות מידע
חלק שני

תקצירים

76ב חלק חמישי

סיוון התשפ"ו | יוני 2026

ירושלים

מס' קטלוגי 2026-A-005
ISSN 0334-9713

ניתן להוריד גרסה אלקטרונית של דוח זה
מאתר האינטרנט של משרד מבקר המדינה
www.mevaker.gov.il

תוכן העניינים

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

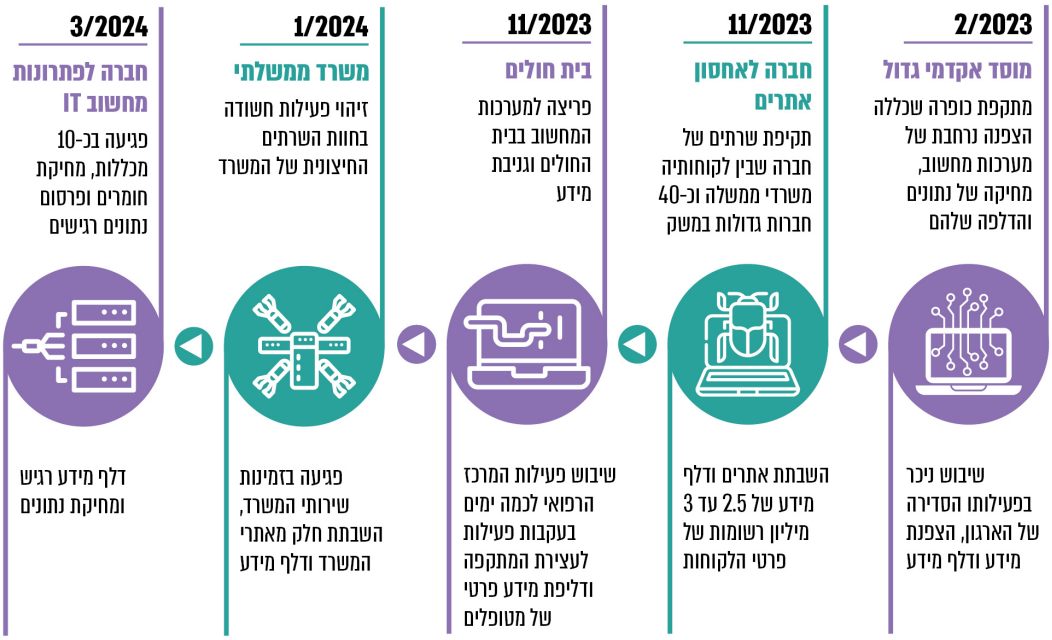
תקציר

רקע

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.

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. 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:

דוגמאות לגופים שהתמודדו עם מתקפת סייבר משמעותית, 2023 - 2024



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

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 הלאומי 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.

במאי 2024 פרסם מערך הסייבר דוח לפיו העלות הכלכלית המצטברת למשק הישראלי מנזקי מתקפות סייבר היא 12 מיליארד ש"ח בשנה[2]. 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.

תפקיד הגופים האסדרתיים המדינתיים בתחום הסייבר[4] - 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: (א) הגופים השונים (פרטיים וציבוריים) הפועלים במשק ונדרשים להעמיד הגנה עצמאית מול איומי הסייבר (הגופים במשק) (ב) 21 גופים בעלי חשיבות במשק שנבדקו בשאלון (ג) הגופים האסדרתיים המדינתיים הפועלים בתחום הסייבר (ד) הדרג המדיני.

להלן לוח המפרט את הגופים העיקריים המוזכרים בדוח זה:

שם הגוף	התיאור
מערך הסייבר הלאומי (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[5]. בהתאם לחוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח- 1998 (החוק להסדרת הביטחון), אחראי מערך הסייבר להנחיית מרבית הגופים שהם תשתיות מדינה קריטיות (גופי תמ"ק[6]) ולבקרה עליהם, ובהתאם להחלטת הממשלה 2443 מפברואר 2015, 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. זאת ועוד במסגרת תפקידו של המערך לסייע למשק הוא מפעיל בין היתר את האגף הארצי לניהול אירועי סייבר (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 (תורת ההגנה) - מדריך יישומי להגנת הסייבר בארגון.

[2] דוח אומדן הנזק הכלכלי של מתקפות סייבר בישראל.
[3] http://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide.
[4] הגופים האסדרתיים המדינתיים: מערך הסייבר הלאומי, שירות הביטחון הכללי, הרשות להגנת הפרטיות, יחידת ההגנה בסייבר במערך הדיגיטל הלאומי ויחידות מגזריות להכוונה מקצועית בתחום הסייבר.
[5] מתוך אתר המרשתת של מערך הסייבר - www.gov.il/he/pages/newabout.
[6] 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".

שם הגוף	התיאור
	מערך הסייבר הוקם במשרד רה"ם. הוא 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, התשמ"א-1981, ולתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017. הרשות להגנת הפרטיות היא יחידה במשרד המשפטים והיא עצמאית ובלתי תלויה בהפעלת סמכויותיה[7]. בראשה עומד עו"ד גלעד סממה שנכנס לתפקידו בנובמבר 2021 וכיהן בתפקיד במהלך עריכת הביקורת.
שב"כ	הארגון מנחה גופים מכוח החוק להסדרת הביטחון, חלקם גופי תמ"ק. השב"כ נתון למרות הממשלה וראש הממשלה ממונה עליו מטעם הממשלה. בראשו עמד מר רונן בר שנכנס לתפקידו באוקטובר 2021 וכיהן בתפקיד במהלך עריכת הביקורת. מר בר סיים את תפקידו ביוני 2025.
יה"ב (היחידה להגנת הסייבר בממשלה) במערך הדיגיטל	יחידת הכוונה והנחיה מקצועית בתחום הגנת הסייבר עבור משרדי הממשלה ויחידות הסמך[8]. היחידה הוקמה על פי החלטת הממשלה 2443. היא כפופה ארגונית למערך הדיגיטל 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 סייבר מגזריות	כיום פועלות 8 יחידות סייבר מגזריות שפועלות במסגרת משרדי ממשלה לשיפור הגנת הסייבר במגזרי המשק השונים. היחידות הוקמו בהתאם להחלטת ממשלה 2443 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. יחידות הסייבר המגזריות מנחות אלפי גופים ומסווגות אותם לפי רמת חשיבות להגנה בסייבר- C,B,A.
רשות חירום לאומית (רח"ל)	רח"ל הוקמה מכוח החלטת ועדת שרים לענייני ביטחון לאומי מס' ב/43 מדצמבר 2007 (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.

[7] בהתאם להחלטת הממשלה 1890 (2.10.22), ובמסגרת תיקון 13 לחוק הגנת הפרטיות.
[8] למעט "הגופים המיוחדים" שפורטו בהחלטה 3611 ועל פעולות גופים אלה באמצעות משרדי הממשלה במסגרת תפקידם ומשרד הביטחון.

שם הגוף	התיאור
המטה לביטחון לאומי (המל"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.
גוף תמ"ק (כמה עשרות גופים)	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 חיוניים (מאות גופים)	גופים ברמת החשיבות הגבוהה ביותר (גופי A), לדברי המערך יש כמה מאות גופים חיוניים. חלקם משויכים למגזרים שיש להם יחידות סייבר מגזריות והן מנחות אותן בתחום הסייבר ולחלקם אין גורם שמנחה אותם בתחום הסייבר.

נתוני מפתח

12 מיליארד ש"ח

העלות השנתית הכלכלית המצטברת למשק הישראלי מנזקי מתקפות סייבר בשנה

מאות

אירועי הסייבר בעלי פוטנציאל נזק משמעותי שאירעו בתקופת מלחמת חרבות ברזל (מ-7.10.23 עד 30.4.24)

חלק

מגופי תמ"ק, היו לפני פרוץ מלחמת חרבות ברזל ברמות הסמכה המשקפות יכולת התמודדות מוגבלת עם תוקפים. ביוני 2025 חל שיפור בציוני ההסמכה אולם עדיין היה קיים פער במועד זה

6 שנים

התקופה שבה, לפני פרוץ מלחמת חרבות ברזל, לא התקיים תרגיל סייבר לאומי. רק כשנה לאחר פרוץ המלחמה, בנובמבר 2024, התקיים תרגיל סייבר לאומי במתווה שולחני ולאחר מכן במרץ 2025 התקיים תרגיל לאומי שכלל תרחיש מלחמה ותרחיש סייבר

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 שבין נובמבר 2024 ועד יוני 2025. דוח זה כולל שלושה חלקים: **חלקו הראשון** של הדוח עוסק ברמת ההגנה והחוסן של המשק (עד כמה המגזרים במשק הישראלי ערוכים למנוע ולזהות מתקפות סייבר משמעותיות ולהגיב להן) כפי שהוצגה על ידי מערך הסייבר והשב"כ, כל אחד בתחום אחריותו, ואופן שיקופה לדרג המדיני לפני המלחמה ובמהלכה. **חלקו השני** עוסק בפעולות שנקטו הגופים האסדרתיים המדינתיים קודם המלחמה ובמהלכה כדי להעלות את החוסן של הגופים במשק. **וחלקו השלישי** של הדוח בוחן את ההיערכות של 21 גופים בעלי חשיבות במשק (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 אירועי סייבר לפני המלחמה ובמהלכה.

הביקורת נעשתה בגופים הבאים, חלקם גופים אסדרתיים מדינתיים בתחום הסייבר: משרד ראש הממשלה (רה"ם) - במערך הסייבר; במל"ל; בשב"כ; במשרד הביטחון - ברח"ל; במשרד המשפטים - ברשות להגנת הפרטיות; במשרד הכלכלה והתעשייה - במערך הדיגיטל (ביה"ב); במשרד האוצר - במינהל הרכש הממשלתי, באגף השכר והסכמי העבודה ובאגף התקציבים; בנציבות שירות המדינה (נש"מ); 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[9] ו-ISO27001) ובראשם תורת ההגנה 2.0 של מערך הסייבר. יצוין כי תמונת הרוחב אינה מבוססת על מדגם כמותי מייצג וכי 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 מיחידות הסייבר המגזריות), 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

[9] 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.

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.

משרד מבקר המדינה לא 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].

תמונת המצב העולה מן הביקורת

רמת ההגנה והחוסן של המשק בתחום הסייבר לפני המלחמה ובמהלכה ושיקופה לדרג המדיני

ממד הסייבר הוא אחד ממעגלי האיום המשמעותיים המשפיעים על החוסן הלאומי. כבר בהחלטת ועדת שרים ב/43 מדצמבר 2007 נקבע כי אחד הגורמים שעלולים להביא לידי מצב חירום במשק הוא טרור סייבר - שיבוש מערכות מידע הגורם לסיכון בנפש או לנזק לתשתיות.

החלטות הממשלה 3611, 2443, 2444, 219 הניחו מערך תפקודי שמכפיף את הטיפול באיומי הסייבר ברמה הלאומית-ממשלתית לראש הממשלה; זאת על ידי הגדרת ההגנה על תפקודו התקין והבטוח של מרחב 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.

רמת ההגנה בגופי תמ"ק - 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 של ציוני ההסמכה של גופי התמ"ק, שהעבירו מערך הסייבר ושב"כ, עולה כי לפני המלחמה (בשנת 2023), חלק מגופי התמ"ק היו בעלי רמות הסמכה המשקפות יכולת התמודדות מוגבלת למול תוקפים. ביוני 2025 חל שיפור בציוני ההסמכה אולם עדיין היה קיים פער במועד זה.

דיווחים חצי-שנתיים על מצב ההגנה של גופי תמ"ק לדרג מדיני ומקצועי - משנת 2020 ועד יוני 2025, מערך הסייבר לא העביר לראש ממשלה, למזכיר הממשלה, לראש המל"ל, לראש השב"כ וליו"ר ועדת חוץ וביטחון בכנסת 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 ולא התכנסה במשך שנה וחודשיים אחרי פרוץ המלחמה (עד דצמבר 2024). להלן פירוט המועדים שהוועדה התכנסה: בדצמבר 2020; בינואר ובדצמבר 2022; ביוני 2023 ובדצמבר 2024.

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. 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.

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.

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 סייבר למעט פגישה ייעודית 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. 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.

מדידת רמת ההגנה בגופים חיוניים - 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, אף שנושא זה נדרש ממנו בהחלטת הממשלה 2444 (15.2.15). 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.

☆

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 ובחלק 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.

פערים בפעולות הגופים האסדרתיים המדינתיים בתחום הסייבר קודם המלחמה ובמהלכה

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

- **אי-הצלחה לקדם הצעת חוק סייבר במשך כעשור** - 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[10] (ב) בהשוואה בין-לאומית שביצע מערך הסייבר עלה כי ישראל נמצאת בפיגור ניכר מבחינת מצב אסדרת הסייבר (ג) מספר דוחות מבקר המדינה שנכתבו בשנים האחרונות[11] 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 (עד אפריל 2024). למרות הפעולות הרבות שביצע מערך הסייבר יחד עם גופים נוספים לקידום החוק, נכון ליוני 2025, טרם הסתיים הליך גיבוש הצעת החוק[12], טרם לובנו כלל המחלוקות שעלו על ידי המשרדים השונים ואף לא נקבעו לוחות זמנים להגשת הצעת החוק.

- **איום ייחוס לאומי ומגזרי בתחום הסייבר** - במהלך השנים מערך הסייבר לא תיקף את איום הייחוס הלאומי כמתחייב בהחלטת ממשלה 3611. כמו כן ברמה המגזרית - 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.

- **תרגול לאומי ומגזרי לצורך היערכות וטיפול באירועי סייבר** - לפני מלחמת חרבות ברזל נמצאו פערים בביצוע תרגולים שנתיים הן ברמה הלאומית והן ברמה המגזרית כמפורט להלן. כמו כן נמצאו פערים בקיום תרגילי סייבר בשנים 2022-2023 בחלק מהגופים הרגישים המונחים על ידי מערך הסייבר, ובשנים 2021-2023 בחלק
מ-21 הגופים בעלי חשיבות למשק שנבדקו בשאלון. תרגולים אלו נדרשים כדי לוודא שהמדינה ערוכה להתמודד עם אירוע סייבר רב-מוקדי:

  - תרגול ברמה הלאומית - 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 לתכננו ונכח בו. יצוין כי אף שההגנה על מרחב הסייבר הוא יעד ביטחוני לאומי כפי שנקבע

---

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

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

12 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 מפעם לפעם).

בהחלטת הממשלה 2444, בתרגילי הסייבר הלאומיים שהתקיימו בשנת 2018, בשנת 2024 ובשנת 2025 לא השתתפו נציגים מהדרג המדיני - ראש הממשלה, חברי הקבינט המדיני-ביטחוני ושרים.

- תרגול ברמה המגזרית - 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.

👎 **תפיסה לאומית לניהול משבר סייבר** - אף שבהחלטת הממשלה 3611 מאוגוסט 2011 נקבע כי אחד מתפקידי מערך הסייבר הוא לגבש תפיסה לאומית לטיפול במצבי חירום בממד הסייבר, מערך הסייבר לא עדכן שנים רבות את מסמך "התפיסה הלאומית לניהול משבר סייבר" ותכולתה חסרה במספר היבטים: היא אינה כוללת התייחסות למדריכים ולהרחבות בנושא מוכנות ארגונים לתקיפת סייבר שפרסם המערך בשנים 2018 - 2023; היא אינה 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. כמו כן, מערך הסייבר לא הנחה את היחידות המגזריות לפעול לפי התפיסה גם לא בתקופת המלחמה. כמו כן מערך הסייבר לא הטמיע בשנים האחרונות את התפיסה הלאומית שפרסם ולכן השימוש בה בקרב הגופים המונחים מועט. בנוסף, נמצאו פערים בשיתוף הפעולה בין גופים רלוונטיים להתמודדות עם פשיעת סייבר ומתקפות סייבר ממניעים כלכליים.

👎 **פעולות מערך הסייבר לשיפור ההיערכות והכשירות של יחידות הסייבר המגזריות** - אף שבהחלטת הממשלה 2443 נקבע כי מערך הסייבר הוא המנחה המקצועי של יחידות הסייבר המגזריות והן המנחות המקצועיות של גופים חיוניים במגזר שלהן - לפני המלחמה מערך הסייבר לא קיים ליחידות סקירות מודיעין, הועלו פערים הנוגעים לאופן שבו מערך הסייבר משתף מידע מודיעיני עם יחידות הסייבר המגזריות, המערך לא הקים פורום לשיתוף מידע ביניהן ולא שיתף אותן באופן מספק בתכנון הכלים שהוא מפתח בין היתר עבורן. כמו כן, ההנחיות המקצועיות שהעביר להן אינן מחייבות (הן בגדר המלצה בלבד) ומערך הסייבר 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, נמצא פער ביכולת התפקודית של חלק מהיחידות וכמו כן רמת ההגנה בחלק מהמגזרים אינה מספקת ולכן יש חשיבות עליונה לכך שמערך הסייבר יחזק אותן באמצעות שיתוף ידע וכלים, הנחיה, פיקוח וטיפול בפערים.

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

👎 **מסגרות ארגוניות וכלים לטיפול בתחום הסייבר** - 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 ולטיפול בו: מינוי ממונה סייבר בארגון; מינוי צוות הנהלה לניהול משבר סייבר; קיום דיונים של ועדת היגוי סייבר לפחות בכל חציון, העסקת צוות טכנולוגי (פנימי או חיצוני) לאירוע סייבר (IR - Incident Response). היעדר המסגרות והכלים בגופים אלו מלמד על רמת מוכנות ארגונית נמוכה שלהם לאירוע משברי משמעותי. כמו כן 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.

👎 **מכרז מרכזי לשירותי תגובה לאירוע סייבר** - 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.

👎 **מודעות הנהלה להיבטי אבטחת מידע והגנת הסייבר בארגון** - לפני פרוץ מלחמת חרבות ברזל בידי שמונה (38%) מתוך 21 מנכ"לי הגופים שהשיבו על השאלון לא היו תמונות המצב ותשתית המידע הנחוצות (ציוניהם היו 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. כמו כן נמצא 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%).

ניתוח של איומים וסיכונים ותכנון ויישום של אמצעים טכנולוגיים לגילוי אירועי סייבר לפני מלחמת חרבות ברזל - 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. כמו כן בחלק מהגופים נמצאו פערים בנושא תכנון ויישום אמצעים טכנולוגיים לגילוי אירועי סייבר. יצוין כי חלק מהפערים תוקנו במהלך הביקורת.

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. כמו כן, ערב מלחמת חרבות ברזל, שניים (10%) מתוך 21 הגופים בעלי החשיבות במשק שענו על השאלון דיווחו כי כלל לא יושם בהם מערך ניטור אירועי סייבר וטיפול בהם (SIEM או SOC - Security Operation Center). הגופים דיווחו שבעקבות הביקורת הנושא תוקן.

שיעור העמידה של הגופים בקצב ההתרעות בספטמבר 2023 (לפני המלחמה) - בחלק מהגופים נמצאו פערים בנושא. יצוין כי חלק מהפערים טופלו במהלך הביקורת.

זמן הטיפול הראשוני בהתרעות סייבר בספטמבר 2023 (לפני המלחמה) - בחלק מהגופים נמצאו פערים בנושא. יצוין כי חלק מהפערים טופלו במהלך הביקורת.

תכנון של דרכי הטיפול באירועי סייבר ושל הטמעתן בתהליכי העבודה (לפני המלחמה) - דיווחיהם של 20 (95%) מתוך 21 הגופים בעלי החשיבות במשק שהשיבו על השאלון העידו כי ערב מלחמת חרבות ברזל היה פער אחד לפחות בתכנון דרכי הטיפול באירועי סייבר ובהטמעתן בתהליכי העבודה. היערכות לקויה עשויה לפגוע ביכולת של הגופים לטפל באופן המיטבי באירוע סייבר עם התרחשותו.

היערכות להתמודדות עם אירועי סייבר משמעותיים (לפני המלחמה) - דיווחיהם של חלק מתוך 21 הגופים בעלי החשיבות במשק שהשיבו על השאלון העידו על 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.

יישום לקחים מאירועי סייבר (לפני המלחמה) - בחמישה (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 העתידים יתרחשו בשל אותן הסיבות.

תמונת המצב בעניין יחידות הסייבר המגזריות (לפני המלחמה) - בחלק מהגופים נמצאו פערים בנושא. יצוין כי חלק מהפערים טופלו במהלך הביקורת.

מערך הסייבר הלאומי - תשתית לאומית לגילוי אירועי סייבר (לפני המלחמה) - נמצאו פערים בנושא זה וחלקם טופלו.

אירועים בעלי פוטנציאל נזק משמעותי שאירעו בתקופת מלחמת חרבות ברזל

מידע מהותי שחסר בניתוח של מאות אירועים בעלי פוטנציאל נזק משמעותי שאירעו בתקופת מלחמת חרבות ברזל במגזרים שונים (מ-7.10.23 עד 30.4.24) - בפירוט שיש בידי מערך הסייבר על האירועים חסר מידע חיוני הנדרש כדי לגבש תמונת מצב וסטטוס של האירועים, לתחקר אותם ולהפיק לקחים ותובנות מערכתיים כדי למנוע את הישנותם ולשפר תהליכים.

פעולות שביצע מערך הסייבר להעלאת החוסן בתקופת מלחמת חרבות ברזל - 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.

פעולות שנקט מערך הסייבר לצמצום הסיכון במגזרים מסוימים - בשנת 2023 הקים מערך הסייבר את יחידת ממשקים שפועלת לקדם ולשפר את מצב הגופים במגזרים אלו תוך הנחיה מרצון. יודגש כי מדובר בפתרון זמני ולא בפתרון המיטבי.

תקנות שעת חירום והוראות שעה להתמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה - חרבות ברזל), התשפ"ד - 2023 - בהיעדר חוק סייבר וכדי לצמצם את הסיכונים שהתגברו בעקבות מלחמת חרבות ברזל, מערך הסייבר פעל בשיתוף עם שב"כ ומלמ"ב להתקין תקנות חירום והוראות שעה שתוקפו במקור היה לשבעה חודשים, עודכן מספר פעמים ותוקפו הוארך עד לנובמבר 2025. עד סוף אוגוסט 2024 דיווח מערך הסייבר ליועצת המשפטית לממשלה ולוועדת החוץ והביטחון של הכנסת על מספר מקרים שבהם הייתה תקיפת סייבר חמורה והוא נתן לגופים הנחיות מחייבות לפי החוק.

פעולות הרשות להגנת הפרטיות לקידום תיקון 13 לחוק הגנת הפרטיות לצורך שיפור רמת ההגנה על מאגרי מידע אישי במשק - באוגוסט 2024 אישרה הכנסת את תיקון 13 לחוק הגנת הפרטיות. 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 ציין לחיוב שלוש יחידות סייבר מגזריות שהתבלטו בפעולתן כלפי המגזרים שלהן.

משרד מבקר המדינה ציין לחיוב בדוח גופים שנבדקו בשאלון וקיבלו ציון גבוה - 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; 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. ושמונה 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.

עיקרי המלצות הביקורת

רמת ההגנה והחוסן של המשק לפני המלחמה ובמהלכה ושיקופה לדרג המדיני

- 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.

- תמונת המצב שהציג מערך הסייבר הלאומי בנוגע לרמת ההגנה הלא מספקת של מגזרים מסוימים במשק הישראלי, לפני המלחמה ובמהלכה, מחייבת פעולה דחופה בשלושה מישורים: (א) 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 ולהביאה לאישור הממשלה. על הממשלה לבחון ולאשר את התוכנית לרבות אישור לוחות הזמנים והתקציב הנדרש ולעקוב אחר מימושה לפחות אחת לשנה; (ב) על ראש ממשלה 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. מומלץ כי פורום זה יקבל הכשרה רלוונטית לנושא (ג) מומלץ כי כל אחד מהשרים יקיים 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.

- 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.

- מומלץ כי מערך הסייבר ישלים את מדידת רמת ההגנה בכלל המגזרים, בשיתוף עם 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 סקר "בשלות הגנת הסייבר למדידת רמת ההגנה של הגופים" - כדי להבטיח את אמינותו.

פערים בפעולות הגופים האסדרתיים המדינתיים בתחום הסייבר קודם המלחמה ובמהלכה

מומלץ כי מערך הסייבר יגבש בשיתוף מנכ"לי משרדי הממשלה הרלוונטיים, וכן בשיתוף יחידות הסייבר המגזריות, ובשיתוף עם 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 יחידות הסייבר 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.

על ראש מערך הסייבר להשלים בהקדם את הכנת הצעת חוק הסייבר ולפעול יחד עם מל"ל ליישוב המחלוקות, זאת בהתאם להנחיות רה"ם. כמו כן לאור הכוונה להרחיב את סמכויות יחידות הסייבר המגזריות במסגרת חוק הסייבר, על מערך הסייבר לפעול כבר עתה לחיזוקן המקצועי והתפקודי, כדי להבטיח שאלו יוכלו לממש את אחריותן כפי שייקבע בחוק החדש - אם ינוסח ויתקבל. וכמו כן מומלץ כי ראש הממשלה, מר בנימין נתניהו, יעמוד על קידום תזכיר חוק הסייבר בהקדם ובהתאם להנחיותיו.

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.

מומלץ כי יתקיימו תרגילי סייבר ברמה הלאומית, ברמה המגזרית, בגופים רגישים המונחים על ידי מערך הסייבר ובגופים החיוניים:

- ברמה הלאומית - מערך הסייבר ורח"ל ישלימו את יישום המסקנות מתרגילי הסייבר הלאומי שהתקיימו 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.
- ברמה המגזרית - יחידות הסייבר המגזריות יקיימו תרגיל מגזרי כנדרש בהנחיות מערך הסייבר. מומלץ 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. מערך הסייבר יגדיר בשיתוף יחידות הסייבר המגזריות מנגנון שיאפשר להעביר לרח"ל סיכומי תרגילים ואת תכלול מוכנות העורף לחירום בתחום הסייבר בתהליך תקופתי סדור.
- בגופים רגישים המונחים על ידי מערך הסייבר - על מערך הסייבר והשב"כ לוודא מדי שנה שכל אחד מהגופים הרגישים שמונחים על ידם מבצע תרגיל סייבר שנתי. כמו כן מומלץ כי מערך הסייבר יהיה שותף בתכנון התרגיל, בפיקוח על אופן ביצועו, בתיקון הליקויים וביישום הלקחים בגופים המונחים על ידו.

- מומלץ שהמנכ"לים של גופים שנבדקו בשאלון 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.

מומלץ כי מערך הסייבר יעדכן, בשיתוף גופים 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.

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, יגבש דרכים להעשיר ולטייב את המידע המודיעיני שמועבר ליחידות.

ההיערכות והמוכנות של 21 גופים חיוניים ושל גופים אסדרתיים מדינתיים להתמודדות עם אירועי סייבר לפני המלחמה ובמהלכה

מומלץ כי המנכ"לים של הגופים שנבדקו ושנמצאו בהם פערים בהקמת המסגרות הארגוניות יקימו ויכנסו את המסגרות הארגוניות הנדרשות כדי שידונו בסיכונים שהארגון חשוף להם ויפעלו לצמצום הפערים. כמו כן, 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.

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).

מומלץ כי המנכ"לים של הגופים שנבדקו ונמצאו בהם פערים במודעות ההנהלה להיבטי אבטחת המידע והסייבר ילמדו את היבטי הסייבר ואת הסיכונים שהארגון שהם עומדים בראשו חשוף להם ויפעלו לצמצום הפערים.

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

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

- מומלץ כי הגופים החיוניים שבהם נמצא פער בתכנון דרכי טיפול באירועי סייבר ישלימו את התכנון והאישור של דרכי הטיפול שלהם באירועי סייבר.

- מומלץ כי הגופים שדיווחיהם מעידים על פערים בהיערכות לביצוע פעילויות להתמודדות עם אירועי סייבר משמעותיים ובהתאם לפער שנמצא אצלם יטפלו בפערים, כדי שביום שבו יתרחש האירוע הם יהיו ערוכים לכך באופן המיטבי.

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

- מומלץ כי כל הגופים בהם נמצאו פערים יפעלו לתיקונם.

אירועים בעלי פוטנציאל נזק משמעותי שאירעו בתקופת מלחמת חרבות ברזל

- 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 אירועי הסייבר 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 לטפל 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.

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 וכי השיפור 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 המשקפת 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. בנוסף 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 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 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 שבוצעו 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.

בראייה צופה פני עתיד, 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.
2. מערך הסייבר אשר אחראי להגנת ממד הסייבר הלאומי ופועל ברמת המדינה לחיזוק תמידי של רמת ההגנה של הגופים במשק.
3. יתר הגופים האסדרתיים המדינתיים בתחום הסייבר - שב"כ, רח"ל, יה"ב ויחידות הסייבר המגזריות.
4. הנהלות הגופים שנמצאו בהם פערים בדוח - על כל אחד מהגופים המבוקרים לפעול לתיקון הפערים שהתגלו במסגרתו.

לנוכח 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.

דוח מבקר המדינה

הגנת המידע הממוחשב בבית הנשיא - דוח מיוחד

▪ סיוון התשפ"ו ▪ יוני 2026

הגנת המידע הממוחשב בבית הנשיא - דוח מיוחד

תקציר

רקע

נשיא המדינה הוא ראש מדינה בלתי מפלגתי המייצג את המדינה כלפי פנים וכלפי חוץ. נשיא המדינה נבחר בידי הכנסת לתקופת כהונה של שבע שנים, וזאת מכוח חוק יסוד: נשיא המדינה. חלק גדול מסמכויות הנשיא הן סמכויות טקסיות באופיין, כגון חתימה על חוקים ואמנות עם מדינות חוץ, וחלק אחר מסמכויותיו הן ייחודיות, ובהפעלתן נתון לנשיא שיקול דעת, דוגמת הסמכות לחון עבריינים ולהקל בעונשם והסמכות להטיל את הרכבת הממשלה על אחד מחברי הכנסת. נוסף על כך, הנשיא מייצג את מדינת ישראל בפני הקהילה הבין-לאומית ויהדות התפוצות וכן עוסק במיסוד ובהובלה שותפויות מקומיות ובין-לאומיות בנושאים שונים, דוגמת התמודדות עם משבר האקלים. בית הנשיא, בהיותו מוסד של המדינה, הוא גוף מבוקר מכוח סעיף 9(2) לחוק מבקר המדינה, התשי"ח-1958 [נוסח משולב]. לשכת נשיא המדינה נכללת ביחידות שירות המדינה, ועובדיה הם עובדי מדינה.

פעילותו התקינה של בית הנשיא מושפעת ותלויה בין השאר ברמת הסודיות, השלמות, הזמינות והשרידות של המידע שברשותו, גם במערכות המחשוב המעבדות ומאכסנות אותו וברכיבי התקשורת של מערכות אלה. במערכות הממוחשבות של בית הנשיא אצור מידע רב, לרבות מידע בעל רגישות מיוחדת על קרוב ל-100,000 מבקשי חנינה. המידע ומערכות המחשוב בבית הנשיא הם נכס מרכזי וחיוני, ויש להגן עליהם ככל משאב אחר בעל ערך ארגוני. פגיעה בהם עלולה לגרום לנזקים בהיבטים תפעוליים, טכנולוגיים וכספיים, ואף לפגוע בצנעת הפרט ובסמל מרכזי של המדינה ובאופן שבו הוא נתפס בתודעה הלאומית והבין-לאומית. הדבר נכון בשגרה, ועל אחת כמה וכמה בעיתות מלחמה, כשכמות תקיפות הסייבר (סבר) מתגברת. בית הנשיא מפעיל כמה רשתות תקשורת.

נתוני מפתח

כמעט 100,000

מספר מבקשי החנינה שמידע רגיש לגביהם מצוי במאגר מידע של בית הנשיא. מאגר זה נוהל בידי בית הנשיא שלא על פי חלק מהוראות הדין החלות על גופים המחזיקים במאגרי מידע

בחלק

מהחשבונות הקיימים בבית הנשיא, נמצא ליקוי משמעותי מסוים בתחום הזדהות המשתמשים וניהול הרשאות

אין

לבית הנשיא תוכנית להתאוששות מאסון

ניטור

נמצאו ליקויים המתייחסים לעמידת בית הנשיא בדרישות הנוגעות לניטור מערכות מידע.

חלק

מהמערכות הממוחשבות בבית הנשיא הגיעו לסוף מחזור החיים שלהן

בחלק

מתחנות הקצה בבית הנשיא פעלו גרסאות שפג תוקפן ולכן הן היו חשופות לפגיעויות

פעולות הביקורת

בחודשים מרץ עד ספטמבר 2025 ביצע משרד מבקר המדינה ביקורת בנושא הגנת המידע הממוחשב בבית הנשיא. הביקורת התמקדה ברשת המרכזית, ונבדקו הנושאים האלה: ניהול העל של הגנת המידע; הזדהות המשתמשים וניהול ההרשאות; עדכניות הגרסאות של מערכות ההפעלה והתוכנה; תשתיות רשת בית הנשיא; אבטחת תחנות קצה; והגנת הפרטיות. בדיקת השלמה נערכה ביחידה להגנת הסייבר בממשלה שבמערך הדיגיטל הלאומי.

ועדת המשנה של הוועדה לענייני ביקורת המדינה של הכנסת החליטה שלא להניח על שולחן הכנסת ולא לפרסם נתונים מפרק זה לשם שמירה על ביטחון המדינה, בהתאם לסעיף 17 לחוק מבקר המדינה, התשי"ח-1958 [נוסח משולב]. חסיון נתונים אלה אינו מונע את הבנת מהות הביקורת.

תמונת המצב העולה מן הביקורת

עיקרי הליקויים שעלו בביקורת

ניהול העל של הגנת המידע בבית הנשיא

- **עד ספטמבר 2024 פעל בית הנשיא ללא גורם מנחה בתחום הגנת הסייבר במערכות המידע שנבדקו בביקורת** - משמעות הדבר היא שעד מועד זה לא הוחלו על בית הנשיא הכללים ודרכי הפעולה שהוחלו על משרדי הממשלה, שנועדו לשפר את רמת ההגנה בסייבר, להפחית את הסיכונים הנשקפים לנכסי המידע ולפעול בתחום זה על פי סטנדרטים בין-לאומיים. זאת, בשונה מתחומי ניהול ההון האנושי, הכספים והמשק, שלגביהם אימץ בית הנשיא זה מכבר את הכללים החלים על משרדי הממשלה, בשינויים המחויבים. בספטמבר 2024 אימץ בית הנשיא את הנחיות יה"ב[1] בתחום הגנת הסייבר ואבטחת המידע הבלתי מסווג.

- **עד יוני 2025 לא הוקמה בבית הנשיא ועדת היגוי לנושאי הגנת סייבר** - יצוין כי במהלך הביקורת, ביוני 2025, הוקמה לראשונה ועדת היגוי משרדית לנושאי הגנת הסייבר בבית הנשיא בראשות מנכ"ל בית הנשיא, ובתחילת יולי 2025 היא התכנסה לראשונה. נמצא כי משימות מרכזיות לא קודמו בבית הנשיא: הנהלת בית הנשיא לא העריכה נזקים ולא בחנה ואישרה את מפת הסיכונים המשרדית; לא גיבשה יעדים מדידים לבחינת יישום תשתית הגנת הסייבר; לא ביצעה סקרי הנהלה; ולא בדקה את ישימות הפעילויות המוגדרות למערכת ניהול הגנת הסייבר בבית הנשיא ואת ביצוען.

- **הנהלת בית הנשיא טרם גיבשה או אישרה מדיניות להגנת הסייבר גם לאחר שאימצה את הנחיות יה"ב המחייבות לעשות כך** - בית הנשיא פועל בתחום הגנת הסייבר ללא מסמך מדיניות מאושר, שנועד בין היתר להבהיר מהן המסגרות הארגוניות המיישמות את הגנת הסייבר במשרד, להגדיר את העקרונות שיאפשרו גיבוש נהלים ויתמכו בהמשכיות התפקודית ולהבטיח עמידה בהוראות הדין הנוגעות להגנת הסייבר.

- **נהלים** - בכל הנוגע לאבטחת המידע ברשת שנבדקה, בית הנשיא גיבש נהלים העוסקים רק בחלק מהנושאים הרלוונטיים, ואינם עוסקים בנושאי ליבה בתחום הגנת הסייבר, כגון במשתמשים ובהרשאות; בכללים לניטור של אירועים, חריגות ואיומים; במחזור חיי תוכנה; ובעדכוני מערכות הפעלה. הנהלים שגובשו לא אושרו כנדרש בהנחיות יה"ב.

- **הערכה ומיפוי של סיכוני סייבר** - סקר סיכונים הוא מרכיב מרכזי בהגנת המידע והסייבר. ביולי 2025 - במהלך הביקורת וכעשרה חודשים לאחר שבית הנשיא אימץ את הנחיות יה"ב, בית הנשיא עדכן כי הוא החל לראשונה בביצוע סקר סיכונים תשתיתי, ובמסגרתו מבוצע מבדק חדירה.

- **ביצוע מבדקי חדירה** - נמצא כי בית הנשיא ביצע מבדק חדירה תשתיתי חלקי בלבד.

  עוד נמצא כי בית הנשיא לא ביצע מבדק חדירה ליישומים המותקנים על גבי מערכות המחשוב שלו.

- **תוכניות עבודה שנתיות** - הנהלת בית הנשיא לא ניהלה במהלך השנים את פעילותה בתחום הגנת הסייבר בהתאם לתוכניות עבודה ייעודיות לתחום הגנת הסייבר. עם זאת, תוכניות העבודה הכלליות של בית הנשיא כללו גם משימות הנוגעות להגנת הסייבר. תוכנית העבודה לשנת 2025 כללה שתי משימות בלבד הנוגעות להגנת הסייבר. ציון שתי משימות בלבד בתכנית העבודה ל-2025 מעלה חשש כי חסרו בה משימות ליבה חיוניות בתחום הגנת הסייבר. כמו כן גם שתי המשימות שצוינו בתוכנית חסרות ציון של לוחות הזמנים לביצוע וציון הגורם האחראי לכך.

- **תחומי ליבה בתחום טכנולוגיות המידע -** תחומי ליבה של אחריות וסמכות בתחום הגנת הסייבר כפי שהוגדרו בידי נש"ם ויה"ב, לא הוטלו רשמית על ממלאי תפקידים בבית הנשיא, ובכלל זה: התכנון, הניהול והבקרה של מכלול היבטי הגנת הסייבר; גיבוש מדיניות הגנת הסייבר ותוכניות העבודה; ניתוח והערכה שוטפים של תוכנית הגנת הסייבר בהתאם לצרכים, לאיומים ולמענים; הכנת תוכנית תקציבית לטיפול

[1] יה"ב הוקמה מכוח החלטת ממשלה 2443 מפברואר 2015. על פי ההחלטה, ייעוד היחידה הוא לכוון ולהנחות מקצועית את משרדי הממשלה ויחידות הסמך בתחום הגנת הסייבר ולהקים מרכז שליטה ובקרה ממשלתי להתמודדות עם איומי סייבר (SOC ממשלתי).

בהגנת הסייבר ובקרה על היישום והניהול של תחום הגנת הסייבר; יישום מדיניות אבטחת המידע במערכות המידע, לרבות בקרה על פעילויות ממוחשבות לשם מניעת פרצות במערכות המחשוב; וכן ניהול תחום הגנת הסייבר והנחיה מקצועית בתחום זה.

- **הזדהות משתמשים וניהול הרשאות** - ממצאי הביקורת העלו ליקויים בעלי משקל בנושא הזדהות משתמשים וניהול הרשאות.

- **שימוש בתיבות דוא"ל אישיות** - בית הנשיא לא הקצה תיבות דוא"ל משרדיות לכל עובדי בית הנשיא העושים שימוש בדואר אלקטרוני במסגרת עבודתם השוטפת, ובכך למעשה יצר פתח לשימוש לא תקין בדוא"ל - שימוש של עובדים בתיבת דוא"ל פרטית לצורכי עבודה, דבר העלול לגרום לדלף מידע ולאובדן מידע וכן לפגוע ביכולתו של בית הנשיא לבצע בקרה על השימוש בתיבות הדוא"ל.

- **ניטור מערכות המידע ברשת בית הנשיא** - נמצאו ליקויים המתייחסים לעמידת בית הנשיא בדרישות הנוגעות לניטור מערכות המידע.

- **עדכניות הגרסאות של מערכות ההפעלה והתוכנה** - פגיעויות המתגלות במוצרי חומרה ותוכנה שבהם נעשה שימוש ברשת הארגון עלולות לחשוף את מערכות המידע בארגון לפעילות עוינת מצד תוקף פנימי או חיצוני, לרבות שימוש לא מורשה במידע בתוך הארגון, דליפת מידע אל מחוץ לארגון או חדירה של גורם עוין שעלולה לחבל במידע הארגוני או לפגוע בזמינותו. פגיעויות כאלה מתגלות חדשות לבקרים, וההתמודדות איתן מחייבת ניהול מדוקדק ומעקב אחר מחזור החיים של כלל המוצרים בארגון כדי לוודא שלא נעשה שימוש במוצרים שהגיעו לסוף מחזור החיים שלהם ואינם נתמכים עוד בידי היצרן, ושכל עדכוני האבטחה שמפרסמים יצרני המוצרים מותקנים במערכות הארגון.

  נמצא כי בבית הנשיא מצויות מערכות שאינן נתמכות עוד בידי היצרן. כמו כן בית הנשיא אינו מקפיד על התקנת כל עדכוני האבטחה המתפרסמים למוצרים השונים. משמעות הדבר היא שחלק מהמערכות הממוחשבות של בית הנשיא חשופות לפגיעויות שונות.

- **תשתיות רשת בית הנשיא ואבטחתה**

  - **ארכיטקטורת הרשת וניטורה** - נמצא כי האופן שבו בנויה רשת בית הנשיא אינו תואם את הנדרש על פי הנחיות יה"ב ובקרות תורת ההגנה בסייבר, ויוצר סיכון.
  - **מערכת הגנה להגבלת הגישה לרשת** - נמצא כי בית הנשיא לא עומד בהנחיות יה"ב שמטרתן הגבלת הגישה לרשת.
  - **מניעת דליפת מידע** - נמצא כי בית הנשיא לא עומד במלוא ההנחיות שנקבעו בהנחיות יה"ב ובתורת ההגנה בסייבר לצורך מניעת דליפת נתונים.

- **אבטחת תחנות הקצה** - תחנות הקצה בארגון הן יעד נפוץ לתקיפה באמצעות ניצול חולשות במערכת ההפעלה או ביישומים שונים המותקנים עליה. לפיכך מעקב שוטף אחר תחנות קצה חיוני כדי להבטיח שהן מאובטחות כנדרש וכדי לוודא שתחנות שאינן פעילות מנותקות מהרשת ולא משמשות יעד לתקיפה.

  נמצא כי בחלק מתחנות הקצה פעלו גרסאות של מערכות הפעלה שפג תוקפן והן היו חשופות לפגיעויות. ממצאים אלה משקפים היעדר שליטה של בית הנשיא בכל הנוגע לאבטחת תחנות הקצה.

- **ניהול המשכיות תפקודית בעת חירום** - לבית הנשיא אין תוכנית המשכיות עסקית ותפקודית ואין ברשותו תוכנית להתאוששות מאסון המבוססת על הערכת סיכונים. כמו כן בית הנשיא לא ביצע ניסוי (תרגיל) לבחינת מערך ההתאוששות שלו, כנדרש בהנחיות יה"ב. יוצא אפוא כי בית הנשיא לא נקט מבעוד מועד את הפעולות

הנדרשות כדי להבטיח שבעת חירום, עקב שיבוש תהליכים עסקיים קריטיים, פונקציות עסקיות יהיו זמינות, וכך יצומצם הנזק התפקודי והתדמיתי שעלול להיגרם לארגון.

הגנת הפרטיות בבית הנשיא - בית הנשיא, כגוף ציבורי, נדרש לעמוד בדרישות מחמירות בכל הנוגע לאבטחת המידע והגנת הפרטיות במאגרים שברשותו. דרישות אלו חלות בין היתר על מאגר החנינות, שבו מצוי מידע רגיש על קרוב ל-100,000 מבקשי חנינה, ועל מאגר התאמה הביטחונית, שבו מצוי מידע רגיש על מאות עובדי בית הנשיא בהווה ובעבר. נמצא כי בית הנשיא לא קיים חלק מהוראות הדין החלות על כלל הגופים המחזיקים במאגרי מידע: (א) לא מונה ממונה אבטחת מידע האמון על אבטחת המידע במאגרים; (ב) לא גובש מסמך הגדרות מאגר; (ג) לא מופו מאגרי המידע, ולא הוכנה רשימת מצאי של מערכות המאגרים; (ד) לא גובש נוהל אבטחה הכולל הוראות בדבר האבטחה הפיזית והסביבתית של אתרי המאגר והרשאות גישה אליהם; (ה) לא נקבעו הרשאות גישה של עובדים למאגרים ולמערכותיהם ולא נוהל רישום מעודכן של התפקידים והרשאות הגישה שניתנו לעובדים; (ו) אין בבית הנשיא מנגנון תיעוד אוטומטי המאפשר ביצוע בקרה על הגישה למערכות המאגרים, כנדרש בתקנות אבטחת מידע.

- **הסדרת הטיפול במאגר החנינות באמצעות ספק** - מאגר החנינות של בית הנשיא מכיל מידע רגיש של קרוב ל-100,000 מבקשי חנינה, לרבות נתונים רפואיים, סוציאליים וכלכליים. משנת 2019 קיבל בית הנשיא שירותים מספק חיצוני לצורך אספקת שירותי אפיון, פיתוח, תמיכה ותחזוקה של מאגר החנינות. בית הנשיא לא פעל כנדרש בתקנות אבטחת מידע בכל הנוגע לקבלת שירותים אלה מהספק: (א) הוא לא ביצע בדיקה מקדימה בנוגע לסיכוני אבטחת המידע הכרוכים בהתקשרות עם הספק החל בשנת 2019; (ב) בהסכם ההתקשרות עם הספק לא עוגנו הוראות בדבר המידע שהספק רשאי לעבד והמטרות שלשמן בלבד הוא רשאי להשתמש במידע שעיבד; (ג) בהסכם לא פורטו המערכות שהספק רשאי לגשת אליהן והפעולות שהוא מורשה לבצע; (ד) לא נקבע מנגנון להשבת המידע לבית הנשיא בסיום תקופת ההתקשרות; (ה) לא הוטלה על הספק החובה לדווח לבית הנשיא על עמידתו בהוראות תקנות אבטחת מידע, ואף לא על אירוע אבטחת מידע במאגר, אם התרחש; (ו) החל בשנת 2022 מקבל בית הנשיא שירותי תמיכה למאגר החנינות מספק שירותים חיצוני ללא הסכם תקף. לפיכך לא עוגנו בהסכם מחייב ההוראות הנדרשות להסדרת אופן ההתקשרות עם ספק חיצוני, שנועדו להתמודד עם האתגרים והסכנות הנוגעים לפגיעה בפרטיות וכרוכים בהתקשרות כאמור.

- **העברת מידע ממאגר החנינות לגופים ממשלתיים** - נמצא כי בית הנשיא מעביר למשרד המשפטים ולפרקליטות הצבאית בקשות חנינה המכילות מידע ממאגר החנינות, באמצעות דוא"ל, דהיינו דרך רשת האינטרנט - ללא הצפנה. בדרך הזו מועברים גם פריטי מידע בעל רגישות מיוחדת, כגון פרטים אישיים, נסיבות אישיות ומשפחתיות וכן נימוקים רפואיים, סוציאליים, כלכליים ושיקומיים. בכך פועל בית הנשיא שלא כנדרש בתקנות אבטחת מידע ותורת ההגנה בסייבר. כמו כן בית הנשיא שומר בקשות חנינה שהועברו למשרד המשפטים ולפרקליטות הצבאית בתיבת דוא"ל של הלשכה המשפטית בבית הנשיא לפרק זמן לא מוגבל. תיבת הדוא"ל אינה מתרוקנת באופן קבוע, ונשמרים בה פרטי בקשות חנינה ישנות, הכוללות מידע בעל רגישות מיוחדת. לכן גורם הניגש לתיבת הדוא"ל (כגון מנהל מערכת) נחשף לפרטים אישיים של מבקשי חנינות לאורך שנים רבות, בלי שהיה צורך בשמירתם.

יש לראות בחיוב את פנייתו של בית הנשיא ליה"ב בספטמבר 2024 בבקשה לקבל הנחיה בכל הנוגע להגנת הסייבר ואבטחת המידע הבלתי מסווג, את פעולותיו ליישום ההנחיות, את הקצאת התקציבים להגנת הסייבר וכן את כוונתו להמשיך ליישם את הנחיות יה"ב ולתקן ליקויים שעלו בביקורת.

יש לראות בחיוב את פעולות בית הנשיא לביצוע חלקים ראשונים בסקר סיכונים ובמבדק חדירה תשתיתי.

תקציב בית הנשיא להגנת הסייבר - בית הנשיא הקצה לתחום הגנת הסייבר כ-15% מתקציב תחום טכנולוגיית המידע הכולל שלו בשנת 2023; כ-5.8% בשנת 2024; ובשנת 2025 כ-11%. יש לראות בחיוב את הקצאת התקציב להגנת הסייבר בידי בית הנשיא בשנים 2023 ו-2025. עם זאת, בית הנשיא לא ניהל רישום נפרד של התקציבים המופנים באופן ייעודי לתחום הגנת הסייבר, כדי שניתן יהיה לבחון אם הוא עומד בהנחיית יה"ב.

עיקרי המלצות הביקורת

- על בית הנשיא לפעול על פי הנחיות יה"ב בתחום הגנת הסייבר ואבטחת המידע הבלתי מסווג.
- על מנכ"ל בית הנשיא, העומד בראש הנהלת בית הנשיא והמשמש יו"ר ועדת ההיגוי, לוודא כי הוועדה פועלת כנדרש בהנחיות יה"ב, ובכלל זה מאשרת את מיפוי נכסי המידע של המשרד; מאשרת מפת סיכונים ארגונית על סמך סקר סיכונים; פועלת להעלאת מודעות העובדים לסיכונים בסייבר; מקצה משאבים בהיקף הנדרש להגנה על הסייבר; ומתכנסת בתדירות הנדרשת. על ועדת ההיגוי של בית הנשיא לקבוע מדיניות להגנת הסייבר, בהתאם לנדרש בהנחיות יה"ב, ולתקפה בתדירות הנדרשת.
- על בית הנשיא להשלים את סקר הסיכונים ואת הטיפול בממצאיו, להשלים את סקרי הסיכונים במערכות המידע ולטפל בממצאיהם ולבצע סקרי סיכונים בתדירות הנדרשת על פי הנחיות יה"ב. כמו כן על בית הנשיא להשלים את מבדק החדירה התשתיתי, לבצע מבדקי חדירה יישומיים ולבצע מבדקי חדירה למערכות על בסיס תקופתי, כנדרש בהנחיות יה"ב.
- על בית הנשיא לבנות תוכניות עבודה שנתיות המתמקדות בתחום הגנת הסייבר, כנדרש בהנחיות יה"ב. כדי להבטיח את אפקטיביות תוכניות העבודה, יש לפרט בהן את לוחות הזמנים לביצוע ואת הגורמים האחראים לביצוע המשימות השונות ולעקוב אחר מימושן. כמו כן על בית הנשיא להשלים את החסר בנהלים מרכזיים ולגבש נהלים נוספים בתחום הגנת הסייבר, כנדרש.
- כדי להבטיח שבית הנשיא מקצה די משאבים להגנת הסייבר, עליו לנהל רישום נפרד של התקציבים המופנים לתחום זה. כמו כן, מומלץ לבית הנשיא להשלים הטלת תחומי האחריות והסמכות על בעלי תפקידים מתאימים בתחום הגנת הסייבר.
- על בית הנשיא לתקן את הליקויים ולעמוד במלוא הנחיות שנקבעו בעניין הזדהות משתמשים וניהול הרשאות.
- על בית הנשיא להקצות תיבות דוא"ל משרדיות לכל העובדים העושים שימוש בדוא"ל בשגרת עבודתם ולוודא כי לצורכי עבודה ייעשה שימוש אך ורק בתיבות דוא"ל משרדיות.
- על בית הנשיא לפעול לשיפור מערך הניטור על מערכות המידע שלו.
- על בית הנשיא לגבש מנגנון יעיל העוקב באופן שיטתי ולאורך זמן אחר מחזור החיים של המוצרים הפועלים במערכותיו ואחר פרסום עדכוני האבטחה הנוגעים להם, לוודא כי לא ייעשה שימוש במוצרים שהגיעו לסוף מחזור החיים שלהם ולהתקין בהם עדכוני אבטחה בהתאם להנחיות יה"ב ולתקנות אבטחת מידע, כדי להבטיח את הגנת המידע האצור במערכותיהם.
- על בית הנשיא להתאים את מבנה הרשת לנדרש על פי הנחיות יה"ב ובקרות תורת ההגנה בסייבר ולהתקין את מלוא מערכות ההגנה הנדרשות.
- על בית הנשיא לוודא כי הוא מנהל את כל תחנות הקצה בארגון, כנדרש בהנחיות יה"ב.
- על בית הנשיא לגבש תוכנית עסקית ותפקודית, הכוללת גם תוכנית להתאוששות מאסון, המבוססת על הערכת סיכונים ומפרטת את האמצעים שיש לנקוט בעקבות אירוע חירום המסכן את פעילות המשרד. תוכנית זו תכלול התייחסות לארבעה שלבים (שלב התגובה, שלב ההתאוששות, שלב השיקום ושלב התחקור), ותובא לדיון והחלטה בידי ועדת ההיגוי לנושאי הגנת הסייבר. כמו כן, על בית הנשיא לבצע ניסויים לבחינת מערך השיקום וההתאוששות שלו בתדירות הנדרשת בהנחיית יה"ב. כן מומלץ כי הנהלת בית הנשיא תשתתף בניסויים אלו.

על בית הנשיא לפעול על פי הוראות חוק הגנת הפרטיות ותקנות אבטחת מידע, ובכלל זה עליו למנות ממונה אבטחת מידע למאגרי המידע; לגבש מסמך הגדרות למאגרי המידע; למפות את מאגרי המידע; לגבש נוהל אבטחה לכל אחד ממאגרי המידע; ולקבוע את הרשאות הגישה שיקבל כל עובד בבית הנשיא למאגרי המידע ולמערכותיהם, כמו כן, עליו לערוך ביקורת על עמידה בהוראות תקנות אבטחת מידע על ידי גורם שאינו ממונה על אבטחת המידע בבית הנשיא, זאת לכל הפחות אחת ל-24 חודשים.

על בית הנשיא להיערך לביצוע הפעולות הנדרשות מגוף המחזיק במאגר מידע הטעון רמת אבטחה גבוהה בכל הנוגע למאגר החנינות; מאגר זה צפוי להכיל מידע על 100,000 אנשים ומעלה בתוך זמן קצר. כמו כן על בית הנשיא לפעול על פי תקנות אבטחת מידע: להעביר בקשות חנינה לגורם חיצוני, כגון משרד המשפטים, תוך שימוש בשיטות הצפנה מקובלות; וכן לצמצם את המידע הנשמר בידיו, לרבות בתיבת הדוא"ל, למינימום הנדרש בהתאם לתקנות ולהוראות הרשות להגנת הפרטיות.

על בית הנשיא לפעול על פי תקנות אבטחת מידע בכל הנוגע לקבלת שירותים מספק חיצוני המורשה לגשת למאגר מידע של בית הנשיא. כמו כן, עליו לעגן בהסכם ההתקשרות עם הספק את ההתניות והכללים הנדרשים על פי תקנות אבטחת מידע.

סיכום

פעילותו התקינה של בית הנשיא מושפעת ותלויה בין השאר ברמת הסודיות, השלמות, הזמינות והשרידות של המידע המצוי ברשותו, ובכלל זה במערכות המחשוב שלו. פגיעה במידע עלולה להוביל לנזקים בהיבטים תפעוליים, טכנולוגיים וכספיים, ואף לפגוע בצנעת הפרט ובשם הטוב ובתדמית של בית הנשיא ושל העומד בראש המדינה.

הביקורת על הניהול וההפעלה של רשת התקשורת המרכזית של בית הנשיא, המשמשת את כלל עובדיו לשם ניהול תחומי העשייה העיקריים של בית הנשיא, העלתה הליקויים בתחומים האלה:

1. **ההיבט הניהולי:** עד אמצע שנת 2025 פעל בית הנשיא ללא ועדת היגוי להגנת הסייבר וללא מדיניות מאושרת ויעדים מדידים בתחום הגנת הסייבר. החסר המהותי בהיבטי ניהול-העל בבית הנשיא ואי הטלת האחריות לתחומי ליבה על ממלאי תפקידים בבית הנשיא מובילים למסקנה כי תחומי הגנת הסייבר בבית הנשיא נזנחו במידה מסוימת ולא טופלו באופן ההולם את הסיכונים הנשקפים לגוף של המדינה.

2. **ההיבט האבטחתי:** הועלו ליקויים בעלי משקל בניהול אמצעי ההזדהות והחשבונות של המשתמשים ברשת; בית הנשיא לא הקצה תיבות דוא"ל משרדיות לכל עובדי הארגון העושים שימוש בדוא"ל במסגרת עבודתם השוטפת, ובכך יצר למעשה פתח לשימוש לא תקין בדוא"ל; נמצאו ליקויים המתייחסים לעמידת בית הנשיא בדרישות הנוגעות לניטור מערכות מידע; בבית הנשיא פועלות מערכות שאינן נתמכות עוד בידי היצרן, והוא אינו מקפיד על התקנת כל עדכוני האבטחה הנדרשים במערכותיו, ולכן חלק מהן חשופות לפגיעויות שונות; האופן שבו בנויה רשת בית הנשיא, אינו תואם את ההנחיות ויוצר סיכון; בית הנשיא לא התקין חלק ממערכות ההגנה הנדרשות; בית הנשיא לא פעל כנדרש להבטחת שליטה באבטחת תחנות הקצה של הרשת; והוא לא נקט מבעוד מועד את הפעולות הנדרשות להבטחת זמינות פונקציות עסקיות בעת חירום, עקב שיבוש תהליכים עסקיים קריטיים, באופן שהיה מצמצם את הנזק התפקודי והתדמיתי שנגרם לארגון.

3. **היבט ההגנה על הפרטיות:** בית הנשיא לא קיים חלק מהוראות הדין החלות עליו בכל הנוגע לאבטחת הפרטיות במאגרים שברשותו: לא מונה ממונה אבטחת מידע האמון על אבטחת המידע במאגרים; לא מופו מאגרי המידע, ולא הוכנה רשימת מצאי של מערכות המאגרים; לא גובש נוהל אבטחה, ולא נקבעו הרשאות גישה למאגרים; ואין מנגנון תיעוד אוטומטי של הגישה למערכות המאגר. ממצאים אלה עלו גם בנוגע למאגר החנינות של בית הנשיא, המכיל מידע רגיש על קרוב ל-100,000 מבקשי חנינה, לרבות נתונים רפואיים, סוציאליים וכלכליים. נוסף על כך, בית הנשיא קיבל שירותים מספק חיצוני לצורך הטיפול במאגר זה, אך לא נקט את הפעולות הנדרשות על פי

תקנות אבטחת מידע; בית הנשיא מעביר למשרד המשפטים ולפרקליטות הצבאית בקשות חנינה המכילות מידע המוגדר מידע בעל רגישות מיוחדת באמצעות דוא"ל וללא הצפנה, בניגוד לדרישות הדין; בית הנשיא שומר בקשות חנינה שהועברו לגופים אלה בתיבת דוא"ל לפרק זמן לא מוגבל, ואינו מצמצם את המידע הנשמר בידיו למינימום הנדרש.

יש לראות בחיוב את פנייתו של בית הנשיא ליה"ב בספטמבר 2024 בבקשה לקבל הנחיה בכל הנוגע להגנת הסייבר ואבטחת המידע הבלתי מסווג, את פעולותיו ליישום ההנחיות, את הקצאת התקציבים להגנת הסייבר וכן את כוונתו להמשיך ליישם את הנחיות יה"ב ולתקן ליקויים שעלו בביקורת.

על בית הנשיא כגוף ציבורי בעל חשיבות לאומית מהמעלה הראשונה, להמשיך לפעול לתיקון הליקויים שעלו בביקורת, במטרה להבטיח את הסודיות, השלמות, הזמינות והשרידות של המידע המצוי ברשותו, למנוע פגיעה בצנעת הפרט של תושבי המדינה ולמנוע פגיעה בשם הטוב ובתדמית של בית הנשיא.