דוח מבקר המדינה

סייבר ומערכות מידע

ת ק צ י ר י ם

ירושלים | חשוון התשפ"ה | נובמבר 2024

מס' קטלוגי - 2024-S-008

ISSN 0793-1948

דוח זה מובא גם באתר המרשתת של
משרד מבקר המדינה
www.mevaker.gov.il

עיצוב גרפי: צוות אי.אר דיזיין

תוכן העניינים

תקצירים

פתח דבר

דוח זה, המונח על שולחן הכנסת, מציג את תוצאות הביקורת בתחומי הגנת הסייבר וטכנולוגיות המידע. במקבץ זה כלול גם דוח מיוחד בנושא ההיערכות הלאומית בתחום הבינה המלאכותית.

מאוקטובר 2023 נמצאת מדינת ישראל במלחמת חרבות ברזל, בצפון ובדרום, בעקבות מתקפת הפתע הרצחנית של ארגון הטרור חמאס על יישובי עוטף עזה והסביבה בשמחת תורה התשע"ד, שבעה באוקטובר 2023. כפי שהודעתי בעבר, משרדנו מקיים ביקורת מקיפה בנושאים הנוגעים לטבח בשבעה באוקטובר ולמלחמת חרבות ברזל. לדידי, קיימת חובה ציבורית וערכית לקיום ביקורת על אופן תפקודם של כלל הדרגים ביום הטבח, בתקופה שלפניו ובתקופה שלאחריו. בד בבד עם הביקורת בנושא המלחמה משרדנו ממשיך לעשות ביקורת גם בתחומים אחרים.

בשנים האחרונות, ובפרט במהלך המלחמה, אנו עדים לעלייה בתקיפות הסייבר שמבצעות מדינות ומעצמות נגד מדינת ישראל במטרה לגרום נזק ולהשבית ארגונים. עלויות הטיפול בתקיפות סייבר בישראל בשנת 2024 מוערכות על ידי מערך הסייבר הלאומי בכ-12 מיליארד ש"ח.

עם תחילת כהונתי כמבקר המדינה ונציב תלונות הציבור הגדרתי את תחום הסייבר כאחד מנושאי הליבה שבהם תעסוק ביקורת המדינה. זאת במטרה לבחון את היערכותם ומוכנותם של הגופים המבוקרים להתמודדות עם הסיכונים המשמעותיים במרחב הקיברנטי, עם האיומים האסטרטגיים ועם אתגרי הסייבר העתידיים המונחים לפתחם. מהביקורות של משרדי בתחומי הסייבר ומערכות המידע עולה כי חסרה אסדרה בתחום הסייבר המחייבת את הארגונים להגן על עצמם; הגופים החיוניים במשק נדרשים להיות ערוכים להתמודד עם תקיפות ברמה של מדינה או של מעצמה; ומקבלי ההחלטות בממשלה צריכים להיות מודעים לרמת ההגנה במשק ולליקויים בה. דוח זה עוסק כולו בתוצאות ביקורת המדינה בתחום הגנת הסייבר ומערכות המידע. ואלה פרקי הדוח:

- **ניהול סיכונים ממשלתי בתחום התקשוב**
- **אבטחת המידע והגנת הסייבר במוסד לביטוח לאומי**
- **מערכות המידע בחברת דואר ישראל ובבנק הדואר**
- **הגנה בתחום הסייבר: היבטי אסדרה והגנה על המידע ומערכות המחשוב ברפאל מערכות לחימה מתקדמות בע"מ**
- **פרויקט תבל לשדרוג מערך המחשוב במוסד לביטוח לאומי - ביקורת מעקב**
- **מדיניות פעם אחת - ביקורת מעקב**

יובהר כי הפרק בנושא אבטחת המידע והגנת הסייבר במוסד לביטוח לאומי והפרק בנושא הגנה בתחום הסייבר: היבטי אסדרה והגנה על המידע ומערכות המחשוב ברפאל מערכות

לחימה מתקדמות בע"מ עברו תהליך חיסיון, וכי ועדת המשנה של הוועדה לענייני ביקורת המדינה של הכנסת החליטה שלא להניחם במלואם על שולחן הכנסת אלא לפרסם רק חלקים מהם, בהתאם לסעיף 17 לחוק מבקר המדינה, התשי"ח-1958 [נוסח משולב].

להלן סקירה של חלק מפרקי הדוח:

- הטרנספורמציה הדיגיטלית, שהשתלבה ברוב תהליכי העבודה בממשלה, מביאה עימה הזדמנויות לשיפור ולייעול של עבודת הממשלה ולמתן שירותים מתקדמים לציבור, לצד אתגרים וסיכונים חדשים. היקף הפעילות הכספית בתחום התקשוב הממשלתי עמד בשנת 2022 על 4.8 מיליארד ש"ח. חשוב אפוא מאוד לנהל את הסיכונים בתחום זה בצורה סדורה ומתודולוגית. הביקורת בנושא **ניהול הסיכונים הממשלתי בתחום התקשוב** מלמדת על פערים ניכרים בתחום ניהול סיכוני התקשוב בממשלה, ובהם היעדר ריכוז תמונת המצב הממשלתית בדבר סיכוני התקשוב; אי-נקיטת פעולות של מערך הדיגיטל להפחתת סיכונים רוחביים; דיווח חסר של משרדי הממשלה בנוגע לסיכוני התקשוב העיקריים שהם צריכים להידרש להם; והיעדר פעולה מרכזית, סדורה ושיטתית לניהול סיכוני התקשוב במשרדי הממשלה, הכוללת הן נדבך של ניהול סיכונים בפרויקטי תקשוב והן נדבך של ניהול סיכוני תקשוב משרדיים-רוחביים - כמו מחסור בכוח אדם וקושי בגיוסו ושימורו, שבגללם 80% מהעובדים בתחום התקשוב בממשלה הם נותני שירותים (3,993 מתוך 5,308 עובדים בשנת 2022).

  על מערך הדיגיטל הלאומי להידרש לממצאי ביקורת זו ולמפת החום הממשלתית של תחומי הסיכון בתחום התקשוב המוצגת בדוח הביקורת, כדי למקד את הפעילות הממשלתית בתחום ולהבטיח כי ניהול הסיכונים בתחום מאתגר ודינמי זה ייעשה באופן מתודולוגי ומיטבי ויאפשר להיערך לאתגרים מבעוד מועד ולתת מענה לשינויים החלים בסביבת הפעילות הממשלתית.

- חברת דואר ישראל הייתה חברה ממשלתית בבעלות מלאה של מדינת ישראל (עד להפרטתה במאי 2024), המספקת שירותי דואר וכן נותנת שירותים בנקאיים באמצעות חברת הבת שלה - בנק הדואר. נכון לסוף שנת 2023, לחברת הדואר ולבנק הדואר 400 יחידות דואר, 650 מרכזי מסירה וכ-60 מרכזי דוורים אזוריים. כ-11.9 מיליון לקוחות החברה והבנק קיבלו שירות ביחידות הדואר בשנת 2023. בחברת הדואר 55 מערכות מידע, שחלקן נחלקות לתתי-מערכות, ובבנק הדואר יש 16 מערכות נוספות, שחלקן נחלקות לתתי-מערכות, והממוצע השנתי של הוצאות התפעול וההשקעות של אגף מערכות מידע הוא 124 מיליוני ש"ח. מערכות אלו מבוססות על טכנולוגיות שונות ונתמכות על ידי יותר מ-20 ספקים. הביקורת בנושא **מערכות המידע בחברת דואר ישראל ובבנק הדואר** העלתה ליקויים בתחומי מערכות המידע ואבטחת המידע בחברת הדואר ובבנק הדואר, ובהם ניהול לקוי של תהליך ביטול ההרשאות לעובדים וליקויים בבקרה על תהליך זה - כך, 85 (3%) מבעלי ההרשאות למערכת מסוימת אינם מוגדרים במערכת משאבי אנוש כ"פעילים" ואף 79 מתוכם לא אותרו בבקרות הממוחשבות בחברה, ו-780 (כ-13%) מבעלי ההרשאות הפעילות במערכת הניהול המרכזי של הרשת הם עובדים שאינם נכללים ברשימת העובדים הפעילים במערכת משאבי אנוש בחברה; שימוש בציוד ממוחשב מיושן הפוגע הן בשירות ללקוחות החברה והבנק והן באבטחת המידע - כך, אף שפרויקט החלפת הציוד הממוחשב הוגדר פרויקט אסטרטגי כבר בשנת 2019, רק בתחילת שנת 2022 החלו בחברת הדואר להחליפו. עד מרץ 2024 רק 683 מ-1,850 מחשבים הוחלפו או שודרגו; היעדר תוכנית עבודה

רב-שנתית לאגף מערכות מידע; היעדר מעקב אחר ביצוע תוכניות העבודה; ריבוי מערכות שמקשה את העברת המידע ביניהן ומצריך ביצוע הליכים ידניים והשקעת משאבים כדי לפצות על כך.

על אגף מערכות המידע בחברת הדואר לקבוע תוכנית פעולה סדורה הכוללת פיתוח של מערכות המידע בראייה עתידית, שדרוג מערכות ישנות ומיטוב של המערכות הקיימות ושל האינטגרציה ביניהן; כל זאת תוך הקפדה על הגנת הסייבר וצמצום החשיפה לסיכונים שמקורם בהיבטים שונים של שימוש שאינו מורשה. על חברת הדואר לפעול, במסגרת שיפור אבטחת המידע - ובייחוד לנוכח אירוע סייבר שהתרחש בה באפריל 2023 - לשיפור הבקרה על ניהול ההרשאות בחברה. על החברה לבחון את הליקויים שהועלו בביקורת בנושא זה ולגבש דרכים לתיקונם המיידי.

- הדוח כולל פרק בנושא **הגנה בתחום הסייבר: היבטי אסדרה והגנה על המידע ומערכות המחשוב ברפאל מערכות לחימה מתקדמות בע"מ.** בשנת 2022 התקציב של מחלקת אבטחת טכנולוגיות והגנה בסייבר ברפאל היה 10% מתקציב המחשוב של מינהל טכנולוגיות מידע ותהליכים ברפאל; ושיעור אירועי הסייבר מסוג דיוג שדווחו למערך הסייבר הלאומי (מס"ל) בשנת 2022 היה 31% מ-9,108 אירועי הסייבר שדווחו לו. בביקורת עלו ליקויים הנוגעים בין היתר לאי-הסדרת יחסי העבודה בין מס"ל לממונה על הביטחון במערכת הביטחון (מלמ"ב) וליקויים הנוגעים להגנה על המידע ומערכות המחשוב ברפאל. על הנהלת רפאל ודירקטוריון רפאל לפעול לתיקון הליקויים ולוודא בשיתוף מלמ"ב כי רפאל מיישמת את הנחיות מלמ"ב כנדרש, שכן פעילות רפאל היא מרכיב משמעותי בבניית עוצמתה הצבאית וחוסנה של המדינה.

- משרדי מקפיד לבצע ביקורת מעקב כדי לבדוק אם הליקויים שעליהם הצבענו בדוחות הביקורת תוקנו. דוח זה כולל תוצאות של ביקורות מעקב בשני נושאים: **פרויקט תבל לשדרוג מערך המחשוב במוסד לביטוח לאומי -** בביקורת המעקב עלה כי מרבית הליקויים הליבתיים שעלו בביקורת הקודמת לא תוקנו או תוקנו במידה מועטה. זאת אף שעד מועד סיום הביקורת הושקעו בפרויקט תבל כספי ציבור בסך של יותר ממיליארד ש"ח (יותר מפי שניים מהתקציב הכולל הראשוני של הפרויקט). עוד עלה שהמטרה של שיפור השירות לציבור וסיוע לציבור במיצוי זכויותיו מושגת באופן חלקי בין היתר עקב צמצום בתכולות הפרויקט; **מדיניות פעם אחת -** בביקורת המעקב, עלה כי אף שממועד הביקורת הקודמת חלה התקדמות ניכרת בפעולה מקדמית שנחוצה לצורך יישום מדיניות פעם אחת - לא תוקנו מרבית הליקויים שהועלו בביקורת הקודמת בדבר היקף מיפוי השירותים הממשלתיים הניתנים לציבור וניתוח מאפייניהם. התוכנית הממשלתית שעליה החליטה הממשלה עוד בשנת 2016 עדיין לא עלתה, גם בחלוף שמונה שנים, על מסילת יישום ממשית, והשלמת התהליך בכללותו אינה נראית באופק של השנים הקרובות. נראה כי בעיית השורש בעניין זה היא מגבלת יכולתו של מערך הדיגיטל לנקוט פעולות ליישום התוכנית, שכן עיקר פעילותו מול הגופים הממשלתיים אינה נשענת על סמכויות שיש בהן כדי לחייב את משרדי הממשלה לבצוע את הנחיותיו. חולשה זו בד בבד עם היעדר הירתמות של הגופים הממשלתיים והציבוריים ליישום ההחלטה והנחיות מערך הדיגיטל בנושא מובילים למימוש מצומצם של מדיניות פעם אחת.

- נוסף על פרקי הדוח שפורטו לעיל, במקבץ זה כלול גם דוח מיוחד בנושא **ההיערכות הלאומית בתחום הבינה המלאכותית.** שימור עליונותה של מדינה ישראל בתחומי

המדע והטכנולוגיה הוא אחד מעמודי התווך של ביטחונה הלאומי, חוסנה הכלכלי ורווחת אזרחיה. זוהי דרך אסטרטגית לפצות על היעדר משאבי טבע ועל משאבי אנוש מצומצמים ביחס למדינות אחרות בעולם. מהפכת הבינה המלאכותית כבר איננה טכנולוגיה עתידנית - היא טכנולוגיית ליבה חדשנית המשפיעה בהדרגה על מרבית היבטי החיים בהווה ואף תופסת מקום מרכזי ומשמשת מוקד לתחרות בזירה הבין-לאומית במגוון תחומים: מדע, כלכלה, תעשייה, ביטחון, בריאות, חינוך ותעסוקה.

דוח זה מצביע על כך שמדינת ישראל זיהתה כבר בשנת 2018 כי התחום הטכנולוגי מצוי בפתחה של מהפכה של ממש, ושראש הממשלה הבין כבר אז את ההכרח שבהכנה וביישום של תוכנית לאומית מקיפה וכוללת בנושא. ולמרות זאת לא השכילה הממשלה להוביל וליישם מהלכים לאישור תוכנית לאומית רחבה, כוללת וארוכת טווח ולהעלותה לנתיב של יישום ממשי, ובפועל מיצובה של ישראל במדדים הבין-לאומיים המצביעים על מוכנותה בתחום הבינה המלאכותית נשחק. ניתן לקבוע כי המדינה איתרה את הצורך במועד וניתחה אותו, ואולם זה כמה שנים היא אינה צולחת את שלבי קבלת ההחלטות ההכרחיות ואת שלבי יישומן.

כדי לשמר את עליונותה הטכנולוגית והמדעית של ישראל בתחום הבינה המלאכותית, שהוגדרה בעלת עדיפות לאומית, על משרד החדשנות להוביל את מדיניות הממשלה בתחום ולפעול בהתאם להחלטת הממשלה ולסיכום של שרת החדשנות, המדע והטכנולוגיה דאז עם המועצה לביטחון לאומי (המל"ל). במסגרת זו עליו להשלים את גיבוש התוכנית האסטרטגית הלאומית שהחל בהכנתה כבר בשנת 2022. כמו כן על המשרד לקבוע מתווה הן לבחינה עיתית של מידת העמידה ביעדים שנקבעו בתוכנית והן לבחינה פרטנית של כיווני הפעולה שהוגדרו בה ולעדכונם במידת הצורך. עוד עליו לבחון את הדרך שבה מנוהל כיום מימוש הפעימות שאושרו בהחלטות הממשלה - בידי גורמים המבצעים זאת באופן וולונטרי ובלא שניתנה להם סמכות תקציבית. בעת הזו נדרש ממשרד החדשנות, המדע והטכנולוגיה לממש את אחריותו ובאופן זה תקוים החלטת הממשלה כלשונה. הובלה ברורה של תוכנית לאומית משמעותית הכרחית לשמירה על יכולותיה הטכנולוגיות ועל יתרונה היחסי אל מול יתר מדינות העולם. כל סטייה מנתיב היישום האמור של ההחלטה יחייב עדכון של הממשלה בנושא לצורך בחינת מצב הדברים ולצורך מתן מענה שיבטיח את מימוש היעד של קידום תחום הבינה המלאכותית על ידי הממשלה. מוצע כי ראש הממשלה - אשר כבר בשנת 2018 יזם מהלך לקידום התוכנית הלאומית בתחום הבינה המלאכותית כבסיס להחלטת הממשלה בנושא - יעקוב באמצעות מל"ל אחר התקדמות הטיפול הממשלתי בנושא ויבטיח כי תוכנית לאומית משמעותית מיושמת הלכה למעשה.

לסיום, חובה נעימה היא לי להודות לעובדי משרד מבקר המדינה, הפועלים במסירות לביצוע ביקורת באופן מקצועי, מעמיק, יסודי והוגן ולפרסום דוחות ביקורת אובייקטיביים, אפקטיביים ורלוונטיים.

משרד מבקר המדינה מתחייב להמשיך ולבקר את עמידת הגופים המבוקרים בפני סיכונים עכשוויים ועתידיים ולעסוק בתחומי הגנת הסייבר, טכנולוגיות המידע והגנת הפרטיות, לטובת אזרחי ישראל.

נמשיך להתפלל ולייחל לניצחון צה"ל ומערכת הביטחון במלחמה קשה זו שנכפתה עלינו על ידי המרים שבשונאינו, המבקשים להשמידנו כעם וכמדינה, לחזרת החטופים לבתיהם, לחזרת תושבי הדרום והצפון לבתיהם, להחלמת הפצועים ולימים שקטים ושלווים.

מתניהו אנגלמן
מבקר המדינה
ונציב תלונות הציבור

ירושלים, חשוון התשפ"ה, נובמבר 2024

المقدمة

يعرض هذا التقرير المطروح على طاولة الكنيست نتائج الرقابة في مجالات الحماية السيبرانية وتكنولوجيا المعلومات. كما تتضمن هذه المجموعة تقرير خاص عن الاستعداد الوطني في مجال الذكاء الاصطناعي.

منذ أكتوبر 2023، تخوض دولة إسرائيل حرب السيوف الحديدية، في الشمال والجنوب، في أعقاب الهجوم القاتل المفاجئ الذي شنته منظمة حماس الإرهابية على بلدات غلاف غزة والمنطقة المحيطة بها في اخر يوم من ايام عيد العُرش (سمحات توراة)، السابع من أكتوبر 2023. وكما أعلنت سابقًا، فإن مكتبنا يجري مراجعة شاملة للقضايا المتعلقة بمجزرة السابع من أكتوبر وحرب السيوف الحديدية. في رأيي، هناك واجب عام وأخلاقي لإجراء مراجعة على طريقة عمل جميع المستويات يوم المجزرة، في الفترة التي سبقتها والفترة التي تلتها. بالتوازي مع الرقابة في موضوع الحرب، يواصل مكتبنا عملية الرقابة في مجالات أخرى أيضًا.

خلال السنوات الأخيرة، وخاصة خلال الحرب، نشهد زيادة في الهجمات السيبرانية التي تنفذتها دول وقوى عُظمى ضد دولة إسرائيل بهدف إلحاق ضرر بمؤسسات وتعطيلها. وتقدر تكاليف التعامل مع الهجمات السيبرانية في إسرائيل في عام 2024 من قبل الهيئة الوطنية للأمن السايبراني بحوالي 12 مليار ش.ج.

عندما توليت منصبي كمراقب الدولة ومفوض شكاوى الجمهور، قمت بتعريف المجال السيبراني كأحد القضايا الأساسية التي ستتعامل معها رقابة الدولة. وذلك بهدف فحص جاهزية واستعداد الهيئات الخاضعة للرقابة للتعامل مع المخاطر الكبيرة في الحيز السيبراني والتهديدات الاستراتيجية والتحديات السيبرانية المستقبلية الماثلة أمامها. تظهر الرقابات التي أجراها مكتبي في مجالات السايبر ونُظم المعلومات أن هناك نقصًا في قواعد التنظيم او التقنين في المجال السيبراني الذي يُلزم المؤسسات بحماية نفسها؛ يتعين على الهيئات الأساسية في الاقتصاد أن تكون مستعدة للتعامل مع هجمات على مستوى دولة أو قوة عالمية؛ وعلى أصحاب القرار في الحكومة أن يكونوا على دراية بمستوى الحماية في الاقتصاد وأوجه القصور فيه. يتناول هذا التقرير بأكمله نتائج رقابة الدولة في مجال الحماية السيبرانية ونظم المعلومات. فيما يلي فصول التقرير:

- **إدارة مخاطر حكومية في مجال معالجة البيانات عن بعد**
- **أمن المعلومات والحماية السيبرانية في مؤسسة التأمين الوطني**
- **أنظمة المعلومات في شركة بريد إسرائيل وبنك البريد**
- **الحماية في المجال السيبراني: جوانب تنظيم وحماية المعلومات وأنظمة الحاسوب في شركة رفائيل لأنظمة القتال المتقدمة م.ض.**
- **مشروع تيفيل لتحسين نظام الحوسبة في مؤسسة التأمين الوطني - رقابة متابعة**
- **سياسة المرة الواحدة - رقابة متابعة**

نُنوه أن الفصل الخاص بأمن المعلومات والحماية السيبرانية في مؤسسة التأمين الوطني والفصل الخاص بالحماية في المجال السيبراني: جوانب تنظيم وحماية المعلومات وأنظمة الحاسوب في شركة

رفائيل لأنظمة القتال المتقدمة م.ض. مروا بعملية السريّة، وأن اللجنة الفرعية للجنة شؤون رقابة الدولة في الكنيست قررت عدم طرحهما بالكامل على طاولة الكنيست، بل نشر أجزاء منهما فقط، بموجب مادة 17 من قانون مراقب الدولة لعام 1958 [نسخة مدمجة].

فيما يلي استعراض لبعض فصول التقرير:

- إن التحول الرقمي، الذي تم دمجه في معظم إجراءات العمل في الحكومة، يجلب معه فرصًا لتحسين وتنجيع العمل الحكومي وتقديم خدمات متقدمة للجمهور، إلى جانب تحديات ومخاطر جديدة. في عام 2022، بلغ حجم النشاط المالي في مجال معالجة البيانات الحكومي عن بعد الحكومي 4.8 مليار ش.ج.، لذلك من المهم جدًا إدارة المخاطر في هذا المجال بطريقة منظمة ومنهجية. تظهر رقابة موضوع إدارة المخاطر الحكومية في مجال معالجة البيانات عن بعد فجوات كبيرة بهذا المجال في الحكومة، بما في ذلك غياب صورة مركزة للوضع الحكومي فيما يتعلق بمخاطر معالجة البيانات عن بعد؛ عدم اتخاذ الهيئة الرقمية إجراءات للحد من المخاطر العَرْضيّة؛ إبلاغ غير كامل للوزارات الحكومية عن المخاطر الرئيسية لمعالجة البيانات عن بعد التي يتعين عليها التعامل معها؛ الافتقار إلى إجراء مركزي، منظم ومنهجي لإدارة مخاطر معالجة البيانات عن بعد في الوزارات الحكومية والذي يتضمن طبقة إدارة مخاطر في مشاريع معالجة البيانات عن بعد وطبقة إدارة مخاطر وزارية عرْضية في معالجة بيانات عن بعد - مثل نقص القوى العاملة وصعوبة توظيفها والحفاظ عليها، حيث أن 80% من العاملين في مجال معالجة البيانات عن بعد في الحكومة هم من مقدمي الخدمات (3,993 من أصل 5,308 موظف في عام 2022).

  يجب على الهيئة الرقمية الوطنية التطرق لنتائج هذه الرقابة ولخريطة الحرارة الحكومية لمجالات المخاطر في مجال معالجة البيانات عن بعد في تقرير الرقابة، وذلك لتركيز العمل الحكومي في المجال وللتأكد من ان إدارة المخاطر في هذا المجال المليء بالتحديات والديناميكية تطبق بطريقة منهجية ومثالية وتمكّن من الاستعداد للتحديات في وقت مبكر وتقديم رد للتغيرات التي تحصل في بيئة العمل الحكومي.

- كانت شركة بريد إسرائيل شركة حكومية بملكية دولة إسرائيل الكاملة (حتى خصخصتها في أيار 2024)، والتي تقدم خدمات بريدية وتقدم أيضًا خدمات مصرفية من خلال شركة تابعة لها - بنك البريد. حتى نهاية عام 2023، كان لدى شركة البريد وبنك البريد 400 وحدة بريدية، 650 مركز تسليم وحوالي 60 مركز بريد إقليمي. تلقى حوالي 11.9 مليون عميل للشركة والبنك خدمة في وحدات البريد في عام 2023. تمتلك شركة البريد 55 نظاماً للمعلومات بعضها ينقسم إلى أنظمة فرعية، كما يمتلك بنك البريد 16 نظاماً إضافيّاً بعضها ينقسم إلى أنظمة فرعية، ويبلغ المتوسط السنوي لمصاريف التشغيل والاستثمار لقسم نظم المعلومات 124 مليون ش.ج. تعتمد هذه الأنظمة على تقنيات مختلفة ويتم دعمها من قبل أكثر من 20 مورد. كشفت الرقابة المتعلقة بأنظمة المعلومات في شركة بريد إسرائيل وبنك البريد عن أوجه قصور في مجالات نظم المعلومات وأمن المعلومات في شركة البريد وبنك البريد، بما في ذلك خلل في إدارة عملية إلغاء أذونات الموظفين وفي الرقابة على هذه العملية - وبالتالي، فإن 85 (3٪) من أصحاب الأذونات لنظام معين لم يتم تعريفهم في نظام الموارد البشرية على أنهم "نشطون" وأنَّ الرقابات المحوسبة التي اجرتها الشركة لم تستطع ايجاد 79 منهم ، 780 (حوالي 13%) من أصحاب الأذونات النشطة في نظام الإدارة المركزية للشبكة هم موظفون غير مدرجين في قائمة الموظفين النشطين في نظام الموارد البشرية بالشركة؛ استخدام معدات محوسبة قديمة التي تضر بكل من خدمة عملاء الشركة والبنك وأمن المعلومات - وبالتالي، على الرغم من تعريف مشروع استبدال المعدات المحوسبة كمشروع استراتيجي في عام 2019، فقط في بداية عام 2022

بدأت شركة البريد في استبداله. حتى آذار 2024، تم استبدال أو ترقية 683 حاسوب فقط من أصل 1850. عدم وجود خطة عمل متعددة السنوات لقسم نظم المعلومات؛ عدم متابعة تنفيذ خطط العمل؛ كثرة الأنظمة الذي يصعب نقل المعلومات فيما بينها ويُلزم القيام بإجراءات يدوية واستثمار موارد للتعويض عن ذلك.

يجب على قسم نظم المعلومات في شركة البريد إقرار خطة عمل منظمة تتضمن تطوير نظم المعلومات برؤية مستقبلية، ترقية الأنظمة القديمة وتحسين الانظمة الحالية وتحسين التكامل بينها؛ كل هذا مع الحرص على حماية سيبرانية وتقليل الانكشاف للمخاطر الناشئة عن جوانب مختلفة من الاستخدام غير المصرح به. يجب على شركة البريد أن تعمل، في إطار تحسين أمن المعلومات - وخاصة على ضوء الحدث السيبراني الذي تعرضت له في نيسان 2023 - لتحسين الرقابة على إدارة الأذونات في الشركة. يجب على الشركة فحص أوجه القصور التي وُجدت في الرقابة في هذا الموضوع وصياغة سبل لتصحيحها على الفور.

- يتضمن التقرير فصل حول **الحماية في مجال السايبر: جوانب تنظيم وحماية المعلومات وأنظمة الحاسوب في شركة رفائيل لأنظمة القتال المتقدمة م.ض.** في عام 2022، بلغت ميزانية قسم الأمن التكنولوجي والحماية السبرانية في شركة رفائيل 10% من ميزانية الحوسبة لشعبة تكنولوجيا المعلومات والعمليات في رافائيل، وفي عام 2022 بلغ معدل الحوادث السيبرانية من نوع التصيد التي تم الإبلاغ عنها إلى الهيئة الوطنية للأمن السايبراني 31٪؛ من أصل 9,108 حدث سيبراني تم إبلاغها به. وكشفت المراجعة عن أوجه قصور المرتبطة، من بين أمور أخرى، بعدم تنظيم علاقة العمل بين الهيئة الوطنية للأمن السايبراني ومسؤول الامن في جهاز الامن وأوجه قصور المتعلقة بحماية المعلومات وأنظمة الحوسبة في رفائيل. يجب على إدارة رافائيل ومجلس إدارة رفائيل العمل على تصحيح أوجه القصور والتحقق بالتعاون مع مسؤول الامن في جهاز الامن من تطبيق رفائيل لتوجيهاته كما يجب، حيث أن عمل رفائيل يشكل جزء هام في بناء القوة العسكرية للبلاد ومتانتها.

- يحرص مكتبي على إجراء مراقبة متابعة لفحص ما إذا تم تصحيح أوجه القصور التي أشرنا إليها في تقارير المراقبة. يتضمن هذا التقرير نتائج رقابات المتابعة في موضوعين: **مشروع تيفيل لترقية نظام الحوسبة في مؤسسة التأمين الوطني -** كشفت رقابة المتابعة أن معظم أوجه القصور الجوهرية التي وُجدت في الرقابة السابقة لم يتم تصحيحها أو تم تصحيحها قليلًا. وذلك على الرغم من أنه بحلول موعد انهاء عملية المرقابة، كان قد تم استثمار أموال عامة بلغ مجموعها أكثر من مليار ش.ج. في مشروع تيفيل (أكثر من ضعف الميزانية الإجمالية الأولية للمشروع). كما تبين أن هدف تحسين الخدمة للجمهور ومساعدة الجمهور في تحصيل حقوقه يتحقق جزئيا، من بين أمور أخرى، بسبب تقليص محتويات المشروع؛ سياسة المرة الواحدة - تبين خلال رقابة المتابعة أنه على الرغم من إحراز تقدم كبير في الإجراءات الأولية اللازمة لتنفيذ سياسة المرة الواحدة منذ موعد الرقابة السابقة - إلا أن معظم أوجه القصور التي وُجدت في الرقابة السابقة فيما يتعلق بحجم مسح الخدمات الحكومية المقدمة للجمهور وتحليل خصائصها لم تصحح. كما أن الخطة الحكومية التي قررتها الحكومة عام 2016، لم تنتقل، حتى بعد مرور ثماني سنوات، إلى مسار التنفيذ الفعلي، ولا يبدو اكتمال العملية برمتها في أفق السنوات القليلة المقبلة. يبدو أن أصل المشكلة في هذا الأمر هو محدودية قدرة الهيئة الرقمية على اتخاذ الإجراءات اللازمة لتنفيذ الخطة، حيث أن الجزء الرئيسي من نشاطه تجاه الجهات الحكومية لا يستند على صلاحيات التي من شأنها إلزام الوزارات الحكومية على تنفيذ توجيهاتها. ويؤدي هذا الضعف مع عدم التزام الجهات الحكومية والعامة بتنفيذ القرار وتوجيهات الهيئة الرقمية حول الموضوع إلى محدودية تطبيق سياسة المرة الواحدة.

- بالإضافة إلى فصول التقرير المفصلة أعلاه، تتضمن هذه المجموعة أيضًا تقرير خاص حول موضوع **الاستعداد الوطني في مجال الذكاء الاصطناعي.** إن الحفاظ على تفوق دولة إسرائيل في مجالات العلوم والتكنولوجيا هو أحد ركائز أمنها القومي، متانتها الاقتصادية ورفاهية مواطنيها. إنها طريقة استراتيجية لتعويض النقص في الموارد الطبيعية والموارد البشرية المحدودة مقارنة بدول العالم الأخرى. لم تعد ثورة الذكاء الاصطناعي تكنولوجيا مستقبلية فحسب - بل هي تكنولوجيا أساسية مبتكرة تؤثر تدريجيًا على معظم جوانب الحياة في الوقت الحاضر، بل وتحتل مكانة مركزية وهي بمثابة محور منافسة على الساحة الدولية في مجالات متنوعة: العلوم، الاقتصاد، الصناعة، الأمن، الصحة، التعليم والعمل.

يشير هذا التقرير إلى أن دولة إسرائيل أيقنت بالفعل منذ عام 2018 بأن المجال التكنولوجي على أعتاب ثورة حقيقية، وقد فهم آنذاك رئيس الحكومة ضرورة إعداد وتطبيق خطوات للمصادقة على خطة وطنية شاملة وواسعة النطاق حول هذا الموضوع. رغم ذلك، لم تتمكن الحكومة من قيادة وتطبيق خطوات للمصادقة على خطة وطنية واسعة، شاملة وطويلة الأمد ووضعها على مسار التطبيق الفعلي، وعلى أرض الواقع تآكل موقع إسرائيل الذي يشير إلى جاهزيتها في مجال الذكاء الاصطناعي على الصعيد الدولي. ويمكن القول أن الدولة حددت الحاجة في الموعد وعالجتها، لكنها منذ بضع سنوات لم تتجاوز مراحل اتخاذ القرارات اللازمة ومراحل تطبيقها.

للحفاظ على التفوق التكنولوجي والعلمي لإسرائيل في مجال الذكاء الاصطناعي، والذي تم تحديده كأولوية وطنية، يجب على وزارة الابتكار قيادة سياسة الحكومة في هذا المجال والتصرف وفقًا لقرار الحكومة وملخص وزيرة الابتكار، العلوم والتكنولوجيا آنذاك مع مجلس الأمن الوطني. في إطار ذلك يتوجب عليها استكمال صياغة الخطة الاستراتيجية الوطنية، التي بدأت في إعدادها فعليا في عام 2022. كذلك، يجب على الوزارة وضع مخطط إجمالي سواء لفحص دوري لدرجة الالتزام بالأهداف المحددة في الخطة أو لفحص فردي لتوجيهات العمل المحددة فيها وتحديثها إذا لزم الأمر. كما يجب عليها فحص الطريقة التي يتم فيها حاليًا إدارة تطبيق المراحل المصادق عليها في إطار قرارات الحكومة – من قبل جهات التي تقوم بذلك طوعيا ودون منحهم صلاحية بما يخص الميزانية. في الوقت الحالي، مطلوب من وزارة الابتكار، العلوم والتكنولوجيا تتنفيذ مسؤوليتها وبهذه الطريقة سيتم تطبيق قرار الحكومة بحذافيره. إن القيادة الواضحة لخطة وطنية ضرورية للحفاظ على قدراتها التكنولوجية وتفوقها النسبي مقارنة بدول العالم الأخرى. يتطلب ابلاغ الحكومة عن أي انحراف عن مسار التطبيق المذكور للقرار لغرض دراسة الوضع ولغرض تقديم رد يضمن تحقيق هدف تعزيز مجال الذكاء الاصطناعي من قبل الحكومة. يُقترح أن يتابع رئيس الحكومة – الذي بادر بالفعل في عام 2018 لتعزيز الخطة الوطنية في مجال الذكاء الاصطناعي كأساس لقرار الحكومة بشأن هذه القضية – من خلال مجلس الأمن الوطني التقدم المحرز في تعامل الحكومة مع القضية وأن يضمن تطبيق خطة وطنية هامة بالفعل.

في الختام، من حُسن الواجب أن أشكر موظفي مكتب مراقب الدولة، الذين يعملون بكل تفان لإجراء عمليات الرقابة بطريقة مهنية، متعمقة، شاملة وعادلة ولنشر تقارير رقابة موضوعية، فعّالة وذات صلة.

نحن في مكتب مراقب الدولة نلتزم بمتابعة الرقابة وفحص متانة الهيئات الخاضعة مقابل المخاطر الحالية والمستقبلية وتناول مجالات حماية السايبر، تقنيات المعلومات وحماية الخصوصية، لصالح مواطني إسرائيل.

سنواصل الدعاء وتمني انتصار جيش الدفاع الإسرائيلي والجهاز الأمني في هذه الحرب الصعبة التي فرضها علينا من يكرهوننا، والذين يسعون إلى ابادتنا كشعب وكدولة، من أجل عودة المختطفين إلى منازلهم، من أجل عودة سكان الجنوب والشمال إلى منازلهم، من أجل شفاء الجرحى ومن اجل أيام هادئة وساكنة.

متنياهو انجلمن
مراقب الدولة
ومفوض شكاوى الجمهور

القدس، تشرين الثاني 2024

דוח מבקר המדינה - סייבר ומערכות מידע |
חשוון התשפ"ד | נובמבר 2024

ביקורות מערכתיות

ניהול סיכונים ממשלתי בתחום התקשוב

ניהול סיכונים ממשלתי בתחום התקשוב

רקע

הטכנולוגיות הדיגיטליות במשרדי הממשלה הן תשתית ליבה לכלל הפעילות הממשלתית ואמצעי מרכזי לניהול ולתפעול של המשרדים ולמתן שירות לציבור. משרדי הממשלה חשופים לסיכונים שונים, ובהם סיכוני תקשוב[1], אשר יכולים להשפיע על פעילותם ועל יכולתם לממש את יעדיהם.

הצורך בניהול סיכוני תקשוב בממשלה מעוגן בהחלטת ממשלה משנת 2014[2], בהנחיות מערך הדיגיטל[3], בהוראות התכ"ם (תקנון כספים ומשק) של החשב הכללי במשרד האוצר[4] ובמתודולוגיות בין-לאומיות.

יישום הליך סדור ושיטתי לאיתור מוקדי סיכוני התקשוב שהמשרד חשוף להם, הערכת השלכות הסיכונים וההסתברות להתרחשותם, לצד הכנת תוכנית מתאימה למניעת הסיכון או לצמצומו ויצירת מערך בקרה שיתריע על התממשות אפשרית של סיכונים אלו – כל אלה הכרחיים על מנת למזער את הסיכונים הפוטנציאליים או את סבירות התממשותם ואף למנוע את חלקם.

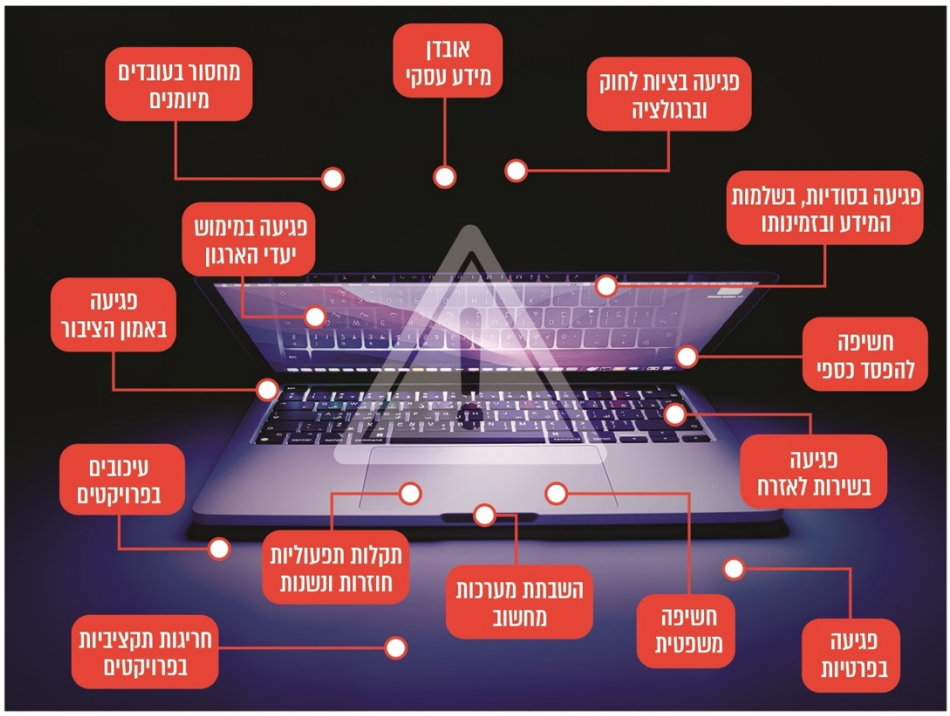
1 סיכון תקשוב - חשיפת תשתיות התקשוב, תהליכי התקשוב או פרויקטי התקשוב לאירוע כשל אשר עלול לפגוע בארגון וביעדיו, לפגיעה במידע, לפגיעה ברמת השירות או לאי-עמידה בתקנים מחייבים.

2 החלטת ממשלה 2097 (10.10.14).

3 נכון לשנת 2023, 48 גופים - משרדי ממשלה ויחידות סמך - מונחים על ידי מערך הדיגיטל הלאומי (להלן - משרדי ממשלה).

4 הוראת תכ"ם 5.2.1, "עקרונות לניהול סיכונים תפעוליים בחטיבות מטה באגף החשב הכללי ובחשבויות משרדי הממשלה".

נזקים פוטנציאליים של התממשות סיכונים בתחום התקשוב



נתוני מפתח

4.8 מיליארד ש"ח
היקף הפעילות הכספית של התקשוב בממשלה בשנת 2022

80%
מהעובדים בתחום התקשוב בממשלה הם נותני שירותים (3,993 מתוך 5,308 עובדים בשנת 2022). מדובר בשיעור שמציב סיכונים שונים הנוגעים לגיוס ושימור כוח אדם

X
מערך הדגיטל לא גיבש תמונת מצב ממשלתית של סיכוני התקשוב ולא עשה פעולות להפחתת הסיכונים הרוחביים

במשך כ-2.5 שנים
לא מונה מנהל סיכוני תקשוב ראשי על ידי מערך הדיגיטל (2021 - 2023)

כ-65%
ממשרדי הממשלה שדיווחו במערכת "איתם"[5] בשנת 2022 (24 מ-37 משרדים) דיווחו על נושא ההון האנושי כסיכון מרכזי

כ-57%
ממשרדי הממשלה שדיווחו במערכת "איתם" בשנת 2022 (21 מ-37 משרדים) דיווחו על נושא התקציב כסיכון מרכזי

8 משרדים
מתוך 13 משרדים שנבדקו (62%) לא מינו נכון ליולי 2023 מנהל סיכוני תקשוב משרדי

8 משרדים
מתוך 13 משרדים שנבדקו (62%) לא ביצעו סקר סיכונים ארגוני מקיף

פעולות הביקורת

בחודשים נובמבר 2022 עד אוגוסט 2023 בדק משרד מבקר המדינה את ניהול הסיכונים בתחום התקשוב בממשלה. נבדקו בעיקר הנושאים האלה: פעולות מערך הדיגיטל הלאומי לניהול סיכוני תקשוב בממשלה; מיפוי סיכוני התקשוב ברמה הלאומית; וניהול סיכוני התקשוב במשרדי הממשלה וביחידות הסמך. הביקורת נעשתה במערך הדיגיטל הלאומי במשרד הכלכלה והתעשייה. בדיקות השלמה נעשו באגפי טד"ם (אגפי טכנולוגיות דיגיטליות ומידע) ב-13 משרדים ויחידות סמך המונחים על ידי מערך הדיגיטל: משרד האוצר, משרד המשפטים, משרד החינוך, משרד הבריאות, משרד החוץ, המשרד להגנת

5 מערכת מידע מרכזית לניהול תהליכי משילות טכנולוגית שפיתח מערך הדיגיטל הלאומי.

הסביבה, משרד התקשורת, משרד החקלאות ופיתוח הכפר, משרד הרווחה והביטחון החברתי, רשות האכיפה והגבייה, רשות האוכלוסין וההגירה, משרד הכלכלה והלשכה המרכזית לסטטיסטיקה.

יצוין כי הביקורת התמקדה בבחינת תהליכי ניהול הסיכונים בתחום התקשוב הנוגעים לפיתוח יישומים מרכזיים, תפעול ותחזוקה של מערכות, מתקנים ותשתיות פיזיות, רכש ציוד ותוכנה והון אנושי בתחום התקשוב (המהווה את החלק העיקרי של הפעילות הכספית בתחום התקשוב - 92%). בדוח זה לא נבדק נושא ניהול הסיכונים בתחום אבטחת המידע והגנת הסייבר[6].

תמונת המצב העולה מן הביקורת

- **מינוי מנהל סיכוני תקשוב ראשי במערך הדיגיטל -** מסוף שנת 2020 ועד לאוגוסט 2023 לא אייש מערך הדיגיטל את תפקיד מנהל סיכוני תקשוב ראשי, כמתחייב מהחלטת הממשלה משנת 2014. כתוצאה מכך נפגעה יכולתו של המערך לקדם במהלך תקופה זו משימות שתכליתן להוביל ולהנחות את אגפי טד"ם במשרדי הממשלה בנושא ניהול סיכוני תקשוב, ולסייע להם בהנעת סקרי סיכוני תקשוב וביישום תכניות להפחתתם. אי מינוי מנהל סיכוני תקשוב ראשי פגע גם ביכולת לגבש תמונת מצב ממשלתית של סיכוני התקשוב, בהטמעת המתודולוגיה לניהול סיכוני תקשוב במשרדי הממשלה ובקידום פעילות רוחבית להפחתת הסיכונים.

- **ריכוז תמונת מצב ממשלתית בדבר סיכוני התקשוב וייזום פעילות רוחבית להפחתת הסיכונים -** הגם שבהחלטת ממשלה משנת 2014 נקבע כי מערך הדיגיטל הלאומי יהיה אחראי על ריכוז תמונת מצב ממשלתית בדבר סיכוני התקשוב ועל ייזום פעילות רוחבית להפחתתה, נמצא כי:

  - מערך הדיגיטל לא גיבש במהלך השנים 2021-2023 תמונת מצב ממשלתית רוחבית של סיכוני התקשוב, זאת על אף שחלק מהמשרדים דיווחו במערכת "איתם" בשנים אלה על סיכוני התקשוב המרכזיים שלהם. כמו כן, על פי המידע המצוי במערך הדיגיטל, משנת 2014 - מיפוי סיכוני תקשוב רוחביים בוצע פעם אחת בלבד, בשנת 2019.

  - חסרה פעולה של מערך הדיגיטל למעקב אחר התפתחות הסיכונים הרוחביים בממשלה במהלך השנים, לרבות רמתם ושינויים שחלו בעניינם.

6 על פי החלטת הממשלה מ-2014, בכל הנוגע להיבטי הגנה בסייבר, יונחה מנהל סיכוני התקשוב הראשי מקצועית על ידי היחידה להגנת הסייבר בממשלה (יה"ב).

- מערך הדיגיטל לא ביצע פעולות להפחתת סיכונים רוחביים בשנים 2022 - 2023, על אף החובה שהוטלה עליו בעניין זה בהחלטת הממשלה ואף שחלק מהמשרדים העבירו אליו, דיווחים בדבר סיכוני התקשוב העיקריים העומדים בפניהם.

- שימור הידע במערך הדיגיטל בתחום ניהול סיכוני התקשוב הרוחביים בממשלה לוקה בחסר.

דיווח של משרדי הממשלה על סיכוני תקשוב משרדיים-רוחביים - בעת גיבוש תוכניות העבודה הונחו אגפי טד"ם במשרדי הממשלה על ידי מערך הדיגיטל לפרט במערכת "איתם" שלושה עד חמישה סיכונים עיקריים המשליכים על יכולתם לממש את יעדיהם. הועלה כדלהלן:

- בשנים 2022 ו-2023 כ-20% מתוך 48 המשרדים המונחים על ידי מערך הדיגיטל הלאומי כלל לא דיווחו על סיכוני התקשוב המשרדיים-רוחביים העומדים בפניהם: בשנת 2022 היה שיעור המשרדים שכלל לא דיווחו 23% (11 משרדים); ובשנת 2023 היה שיעור זה 19% (9 משרדים).

- חלק ממשרדי הממשלה דיווחו דיווח חלקי בלבד - על סיכון אחד או שניים: בשנת 2022 היה שיעור המשרדים שדיווחו דיווח חלקי 40% (19 משרדים); ובשנת 2023 גדל שיעור המשרדים שדיווחו דיווח חלקי ל-50% (24 משרדים).

עולה אפוא כי בשנים 2022 ו-2023 לא דיווחו כנדרש (לא דיווחו בכלל או דיווחו דיווח חלקי) 63% מהמשרדים (30 משרדים) ו-69% מהמשרדים (33 משרדים), בהתאמה, על סיכונים משרדיים-רוחביים בתחום התקשוב במערכת "איתם". היעדר דיווח מלא של מרבית המשרדים בדבר סיכוני התקשוב פוגע באפשרות של מערך הדיגיטל לגבש תמונת מצב ממשלתית מלאה בנוגע לסיכוני התקשוב, לנתח את השלכותיהם ולגבש פעולות וצעדים רוחביים להפחתתם.

דיווח מערך הדיגיטל על סיכונים ברמה רוחבית-משרדית - מערך הדיגיטל הוא היחיד מבין 48 המשרדים שלא דיווח במערכת "איתם" ולו פעם אחת בשנים 2021 - 2023, על סיכוני תקשוב משרדיים-רוחביים העלולים לפגוע ביכולתו לממש את יעדיו, אף שהוא אמון על פיתוח שירותים דיגיטליים ותשתיות טכנולוגיות ברמה הלאומית ואף שהוא גורם מנחה שאמור לשמש דוגמה למשרדי הממשלה.

דיווח על סיכונים ברמת הפרויקט - נמצא כי בשנים 2021 - 2023 שניים עד 11 משרדים מתוך 48 משרדים בכל שנה לא דיווחו על סיכונים ברמת הפרויקט.

בחינת תמונת המצב הממשלתית של סיכוני התקשוב - מאחר ומערך הדיגטל לא גיבש תמונת מצב עדכנית של סיכוני התקשוב, ערך משרד מבקר המדינה ניתוח של הסיכונים על בסיס המידע (החלקי) שהתקבל מדיווחיהם של 37 משרדי ממשלה במערכת "איתם" כדי לבדוק אילו סיכונים משרדיים-רוחביים דווחו בשנת 2022 ומהי תמונת המצב העולה מדיווחים אלה:

- **שכיחות הדיווח על כל אחד מתחומי הסיכון:** נכון לשנת 2022 תחום הסיכון המשרדי-רוחבי בתחום התקשוב שעליו דיווחו מרבית המשרדים היה ההון האנושי,

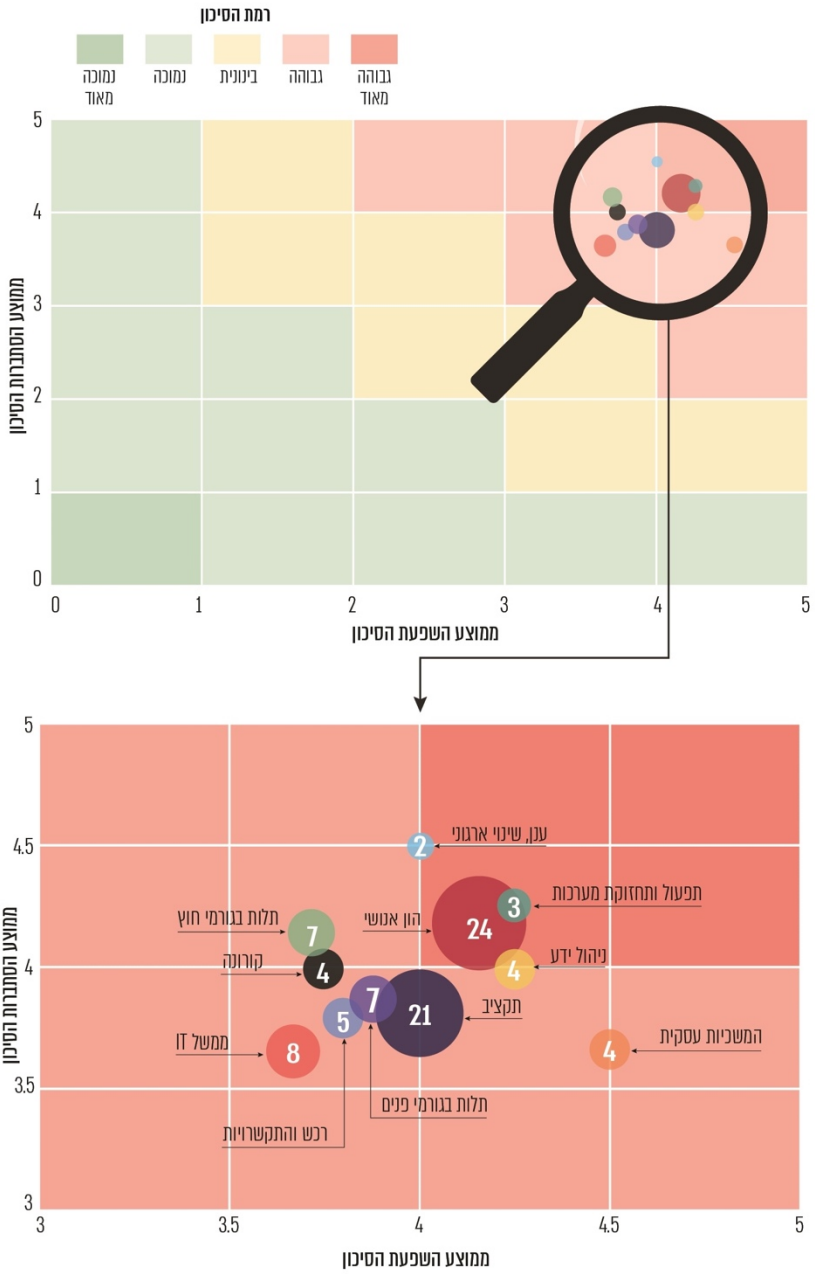
שעליו דיווחו 65% מהמשרדים (24 משרדים). תחום זה כולל מחסור בתקנים, מחסור בכוח אדם, היעדר מיומנות של העובדים, קושי בשימור עובדים וקושי בגיוס עובדים. תחום סיכון נוסף שעליו הצביעו יותר ממחצית המשרדים (57%, 21 משרדים) הוא נושא התקציב, הכולל למשל היעדר תקציב מדינה מאושר, תיקצוב פרויקטים באופן חלקי ושלא בבסיס התקציב. סיכון נוסף, שעליו הצביעו כ-20% מהמשרדים, נוגע לממשל IT, הכולל לדוגמה פערים בין תוכניות העבודה של אגף טד"ם ובין הצרכים העסקיים של הארגון.

- **רמת הסיכון שדווחה לגבי כל אחד מתחומי הסיכון:** עלה כי תחום סיכון ההון האנושי דווח 22 פעמים ברמת סיכון גבוהה וגבוהה מאוד, רמה המתארת פוטנציאל לנזק בעל השפעה גבוהה והסתברות גבוהה להתממשות הסיכון; תחום סיכון התקציב דווח 13 פעמים ברמת סיכון זו.

לשם הצגת הסיכונים באופן ויזואלי, הציב משרד מבקר המדינה את תחומי הסיכון על מפת חום. הצבעים במפה מסמלים את רמות הסיכון: סיכון גבוה מסומן בצבע אדום, סיכון בינוני בצבע צהוב, וסיכון נמוך בצבע ירוק. כל עיגול בתרשים מתאר קטגוריית סיכון; המיקום על ציר ה-X מתאר את ממוצע ההשפעה של הסיכון; המיקום על ציר ה-Y מתאר את ממוצע ההסתברות של הסיכון להתממש; וגודל העיגול והמספר שבתוכו מתארים את מספר המשרדים שדיווחו על הסיכון.

החלק העליון של מפת החום שלהלן משקף את מיקומם של הסיכונים על גבי מפת החום. בחלק התחתון של התרשים יש מיקוד של מפת החום באופן שמאפשר לראות אילו תחומי סיכון נמצאים ברמת סיכון גבוהה עד גבוהה מאוד וכמה משרדים דיווחו עליהם.

מפת החום הממשלתית של תחומי הסיכון בתחום התקשוב, על פי הדיווחים שנעשו בשנת 2022 במערכת "איתם"



על פי דיווחי המשרדים במערכת "איתם", בניתוח ועיבוד משרד מבקר המדינה.

ממפת החום עולה שכל הסיכונים מצויים ברמת סיכון גבוהה עד גבוהה מאוד. מדובר ברמה המתארת פוטנציאל לנזק בעל השפעה גבוהה והסתברות גבוהה להתממשות הסיכון. עוד עולה כי תחומי ההון האנושי והתקציב הם תחומי הסיכון הבולטים ביותר, לא רק בשכיחות הדיווחים עליהם, אלא גם ברמת הסיכון הגבוהה שדווחה לגביהם. מפת חום זו, המתבססת על הדיווחים החלקיים של המשרדים עשויה לשמש למצער כנקודת פתיחה למיקוד פעילות המערך ומשרדי הממשלה בתחום סיכוני התקשוב ולתיעדוף הפעולות והקצאת המשאבים להפחתתם על בסיס רמת הסיכון.

- **מינוי מנהלי סיכוני תקשוב במשרדים -** נכון ליולי 2023, 8 מבין 13 משרדי ממשלה (62%) שנבדקו לא קבעו את זהות מנהל סיכוני התקשוב המשרדי (להלן - לא מינו מנהל סיכוני תקשוב משרדי). מדובר במשרד החינוך, רשות האוכלוסין, משרד החקלאות, משרד התקשורת, משרד החוץ, משרד הכלכלה והתעשייה, המשרד להגנת הסביבה, ומשרד הרווחה - שלא פעלו בעניין זה כמתחייב בהחלטת הממשלה מ-2014 ומהנחיות מערך הדיגיטל. כמו כן, נכון למועד זה לא היה למערך הדיגיטל מידע בנוגע למינוי מנהלי סיכוני תקשוב במשרדים, אף שתפקידו להיות בקשר רציף עימם ולקבל מהם דיווחים על ממצאי סקרי הסיכונים, על הסיכונים המהותיים ועל התקדמות בביצוע תוכניות הטיפול.

- **ביצוע סקר סיכוני תקשוב משרדי מקיף -** בדיקה שנעשתה ב-13 משרדים בנוגע לביצוע סקר סיכוני תקשוב משרדי מקיף, הממפה את הסיכונים העיקריים בפעילות התקשוב של המשרד ומתעדף את הטיפול בהם, העלתה כי:

  - שלושה משרדים - משרד המשפטים, משרד הבריאות[7] ומשרד החינוך - שלפי הנחיות מערך הדיגיטל מחויבים לבצע סקר סיכוני תקשוב ארגוני מקיף בשל היקף הפעילות הכספית השנתית שלהם בתחום התקשוב שעולה על 250 מיליון ש"ח[8] - לא ביצעו סקר כזה בארבע השנים האחרונות. נכון לשנת 2022 היקף הפעילות הכספית של משרד הבריאות בתחום התקשוב עמד על 550 מש"ח; היקף הפעילות הכספית של משרד המשפטים עמד על 466 מש"ח; היקף הפעילות הכספית של משרד החינוך עמד על 358 מש"ח.

    - משרד המשפטים - עלה כי משרד המשפטים מתמודד עם סיכוני תקשוב מהותיים הנוגעים בין היתר למעבר לענן, לשימור וגיוס כוח אדם ולתקציב. לסיכונים אלו יש השפעה על השגת היעדים של אגף טד"ם, החל בנזק נקודתי ברמת היחידה הארגונית וכלה בהשפעה על השגת יעדי המשרד בכללותו. משרד המשפטים הציג בפני משרד מבקר המדינה את ריכוז הסיכונים ופעולות מסוימות שנעשו להפחתת חלק מהם, אך אין בדברים שהוצגו כדי לייתר את החובה לבצע סקר סיכוני תקשוב משרדי מקיף כנדרש בהנחיות מערך הדיגיטל, ולקיים על בסיסו של סקר זה החלטות בדבר נקיטה בפעולות להפחתת סיכונים שלגביהם יוחלט כי אין להותיר את החשיפה להם.

7 הבדיקה במשרד הבריאות אינה כוללת את חטיבת המרכזים הרפואיים.

8 על פי נתוני מערך הדיגיטל, "מבט על פעילות התקשוב הממשלתי 2022".

- משרד החינוך - עלה כי משרד החינוך נדרש להתמודד עם כמה סיכוני תקשוב מהותיים, בהם סיכונים הנוגעים להון האנושי, למעבר לענן ולתחזוקת מערכות ליבה מיושנות. כאמור, אף שעל פי הנחיות מערך הדיגיטל משרד החינוך נדרש לבצע סקר סיכונים ארגוני מקיף, הוא לא ביצע בשנים האחרונות סקר סיכונים כזה. אף שנעשו פעולות הפחתה מסוימות להתמודדות עם חלק מהסיכונים הידועים, אין הדבר מייתר את הצורך בביצוע סקר סיכוני תקשוב משרדי מקיף לזיהוי ולמיפוי סיכונים מהותיים נוספים לצד תוכנית הפחתה מפורטת לטיפול בהם.
- משרד הבריאות - עלה כי בפני משרד הבריאות עומדים סיכונים מהותיים ואתגרים ארגוניים בתחום התקשוב, ובכלל זה בנושא ההון אנושי, המעבר לענן, מערכות מיושנות, תקציב ועוד. משרד הבריאות הכין תוכנית אסטרטגית המתייחסת לחסמים העומדים בפניו אך אין בתוכנית זו ניתוח מפורט של הסיכונים ומשמעותם, וגם לא פעולות הפחתה ולוחות זמנים ברורים לטיפול בהם. כאמור, משרד הבריאות לא ביצע בשנים האחרונות סקר סיכונים ארגוני מקיף אף שהוא נדרש לבצע זאת על פי הנחיות מערך הדיגיטל.

- מבין עשרה משרדים נוספים שנבדקו, שהיקף פעילותם הכספית השנתית בתחום התקשוב אומנם קטן מ-250 מיליון ש"ח, אך עומד על עשרות מיליוני ש"ח, חמישה משרדים (50%) - משרד הרווחה, משרד האוצר, משרד הכלכלה, משרד החקלאות ומשרד התקשורת - לא ביצעו בשנים האחרונות סקר סיכוני תקשוב ארגוני מקיף, אף שהדבר מומלץ על פי הנחיות מערך הדיגיטל לכל יחידה, ללא תלות בהיקף פעילותה הכספית.
- נכון לאוגוסט 2023 לא היה בידי מערך הדיגיטל מיפוי של משרדי הממשלה ויחידות הסמך שביצעו סקר סיכונים משרדי מקיף, אף שבהנחיותיו נקבע כי על המשרדים לדווח למנהל סיכוני התקשוב הראשי על ממצאי סקרי הסיכונים, על הסיכונים המהותיים ועל התקדמות בביצוע תוכניות הטיפול.

ניהול סיכונים בפרויקטים - עלה כי ניהול סיכוני התקשוב במשרדי הממשלה שנבדקו אינו נעשה תמיד בהתאם להנחיות מערך הדיגיטל בצורה סדורה ושוטפת לאורך כל מחזור חיי הפרויקט וכי לעיתים חסרים בו מרכיבים מהותיים, דוגמת קביעת רמת הסיכון והשלכותיו, לוח זמנים לביצוע פעולות ההפחתה ומעקב ממנו ניתן ללמוד אם הסיכון צומצם/התרחב ואם צעדי ההפחתה הועילו אם לאו.

ניהול סיכונים במערך הדיגיטל - עלה כי מערך הדיגיטל לא ביצע סקר סיכוני תקשוב ארגוני מקיף כנדרש בהנחיותיו, אף שהדבר נדרש מתוקף ההיקף הגבוה של פעילותו הכספית בתחום התקשוב - 446 מיליוני ש"ח בשנה ומתוקף היותו אחראי על ניהול מערכות ליבה קריטיות מרכזיות בתחום התקשוב בממשלה.

גיבוש מדיניות ומתודולוגיה לניהול סיכוני תקשוב וסיוע בהטמעתן - מערך הדיגיטל פעל במהלך השנים לשם קביעת מדיניות לניהול סיכוני תקשוב והטמעת המתודולוגיה בעניינה, ובכלל זה פרסום הנחיות וביצוע הדרכות למשרדים. בקרה שביצע מערך הדיגיטל העלתה כי היישום של ההנחיות והמתודולוגיה במשרדים אינה מספקת. במטרה להבטיח כי ניהול סיכוני התקשוב במשרדי הממשלה ייעשה באופן מיטבי מומלץ כי המערך ימשיך ביישום פעולותיו בתחום ההדרכה וההטמעה ויבחן באילו פעולות נוספות יש לנקוט על מנת להטמיע יישום תהליכי ניהול סיכוני תקשוב במשרדים.

הקמת מערכת "איתם" - מערך הדיגיטל פעל להקמת מערכת "איתם" - מערכת מידע מרכזית לניהול תהליכי משילות טכנולוגית. המערכת כוללת מודול לניהול סיכוני תקשוב שבמסגרתו מיושמת מתודולוגיית ניהול סיכונים, הכוללת שימוש בבנק סיכונים מרכזי הכולל רשימת סיכוני תקשוב אופייניים ורלוונטיים למשרדי הממשלה. מטרת הבנק לזהות בצורה יעילה, שלמה ומהירה את סיכוני התקשוב; לסייע בשמירה על אחידות במיפוי הסיכונים ולאפשר ביצוע ניתוחי רוחב לסיכוני התקשוב במשרדי הממשלה.

עיקרי הממצאים הביקורת

- על מערך הדיגיטל למפות ולנתח את סיכוני התקשוב הרוחביים ולוודא כי מצויה בידו מפה עדכנית של סיכוני התקשוב ברמה רוחבית-ממשלתית ולעקוב אחר התפתחות רמת הסיכונים באופן מתמשך. מומלץ כי מפה זו תשולב בתמונת המצב הכלל-ממשלתית על הפעילות בתחום התקשוב שהוא מפרסם מדי שנה בשנה. נוסף על כך, על מערך הדיגיטל ליזום פעילות רוחבית להפחתת הסיכונים הרוחביים ולשקף למשרדי הממשלה את פעולותיו להפחתת כל סיכון וסיכון.

- כדי שמערך הדיגיטל יוכל לפעול בהתאם להחלטת הממשלה, לגבש תמונת מצב ממשלתית מלאה בדבר סיכוני התקשוב ולפעול להפחתתם, עליו לנקוט פעולות שיבטיחו שכל המשרדים ידווחו במערכת "איתם" בהתאם לנדרש, הן על הסיכונים המשרדיים-רוחביים והן על סיכונים בפרויקטים. בכלל זה עליו לחדד ולהבהיר למשרדים את ההנחיות כדי להבטיח שתהיה בידיו תמונת מצב מלאה.

- על המשרדים שלא מינו מנהל סיכוני תקשוב משרדי לפעול בהקדם למינוי בעל תפקיד זה. נוסף על כך, על מערך הדיגיטל לעקוב אחר הנושא כדי להבטיח כי בכל המשרדים ימונו בעלי תפקידים כאמור.

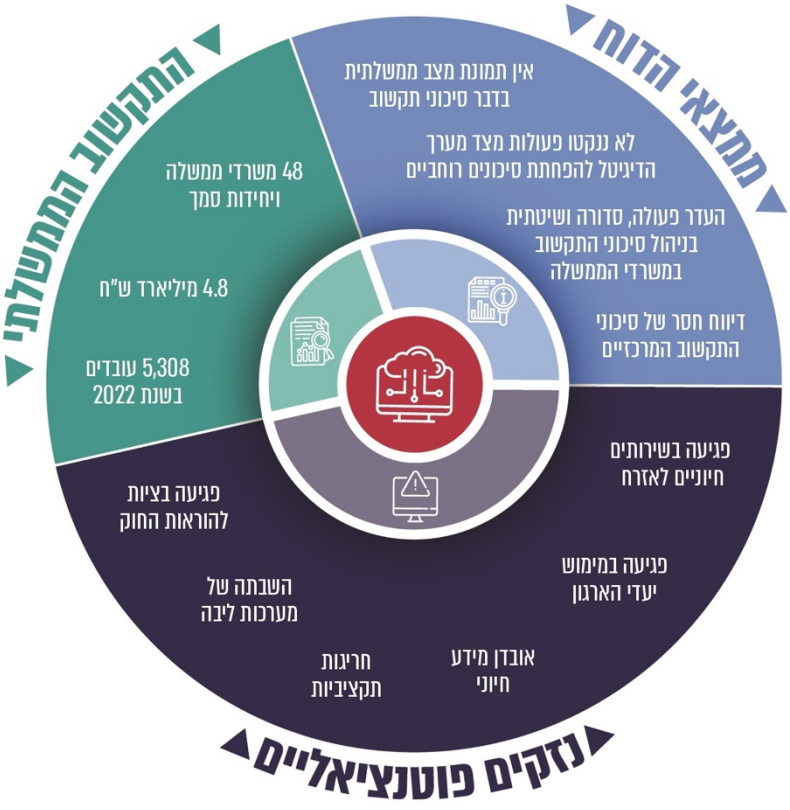
- על מנהלי סיכוני התקשוב המשרדיים לקיים שגרת ניהול סיכונים סדורה, הכוללת תוכנית עבודה לביצוע סקרי סיכונים וגיבוש תוכנית עבודה שנתית לניהול סיכוני התקשוב.

- מומלץ כי מערך הדיגיטל יבצע בקרה על פעולות המשרדים בביצוע סקרי סיכונים ומעקב אחר יישום תוכניות ההפחתה שנקבעו בהם. עוד מומלץ כי מערך הדיגיטל יבחן אם יש מקום להוריד את הרף שנקבע ולפיו רק משרדים שהיקף פעילותם הכספית השנתית בתחום התקשוב גבוה מ-250 מיליון ש"ח מחויבים לבצע סקר סיכוני תקשוב ארגוני.

- מומלץ כי מערך הדיגיטל יפעל למיפוי ולניתוח של סיכונים מערכתיים הנוגעים לכלל עולמות הטכנולוגיה והטרנספורמציה הדיגיטלית בממשלה, לרבות בחינה של הסיכונים הכרוכים באי-הכנסת טכנולוגיות חדשות[9], ויגבש מדיניות ארוכת טווח לניהולם, לצד מיפוי סיכוני תקשוב רוחביים שמעלים משרדי הממשלה.

- מומלץ כי מערך הדיגיטל יגביר את פעילותו להטמעת המתודולוגיה בתחום ניהול סיכוני תקשוב בקרב המשרדים.

ניהול סיכונים ממשלתי בתחום התקשוב - תרשים מסכם



9 RONI - Risk of Not Investing

סיכום

הטרנספורמציה הדיגיטלית והשתלבותה ברוב תהליכי העבודה בממשלה מביאות עימן הזדמנויות לשיפור ולייעול של עבודת הממשלה ומתן שירותים מתקדמים לציבור, לצד אתגרים וסיכונים חדשים. לפיכך חשוב מאוד לנהל את סיכוני התקשוב בממשלה בצורה סדורה ומתודולוגית.

ממצאי דוח זה מלמדים על פערים ניכרים בתחום ניהול סיכוני התקשוב בממשלה, ובהם היעדר ריכוז תמונת מצב ממשלתית בדבר סיכוני התקשוב; אי-נקיטת פעולות של מערך הדיגיטל להפחתת סיכונים רוחביים; דיווח חסר של משרדי הממשלה בנוגע לסיכוני התקשוב העיקריים שהם צריכים להידרש להם; והיעדר פעולה מרכזית, סדורה ושיטתית בניהול סיכוני התקשוב במשרדי הממשלה, הכוללת הן נדבך של ניהול סיכוני תקשוב משרדיים-רוחביים והן נדבך של ניהול סיכונים בפרויקטי תקשוב.

על מערך הדיגיטל הלאומי להידרש לממצאי דוח זה ולמפת החום הממשלתית של תחומי הסיכון בתחום התקשוב המוצגת בו כדי למקד את הפעילות הממשלתית בתחום ולהבטיח כי ניהול הסיכונים בתחום מאתגר ודינמי זה ייעשה באופן מתודולוגי ומיטבי, ויאפשר להיערך לאתגרים מבעוד מועד ולתת מענה לשינויים החלים בסביבת הפעילות הממשלתית.

דוח מבקר המדינה - סייבר ומערכות מידע |
חשוון התשפ"ד | נובמבר 2024

ביקורות מערכתיות

מדיניות פעם אחת - ביקורת מעקב

מדיניות פעם אחת - ביקורת מעקב

רקע

הרשות המבצעת, על כל זרועותיה, מספקת אלפי שירותים שונים לציבור. אחת הדרכים לייעול השירותים שמשרדי הממשלה ויחידות הסמך מעניקים לציבור היא מתן שירותים במתכונת דיגיטלית מלאה מקצה לקצה, במקום אחד, באופן ידידותי ונגיש, תוך יישום **"מדיניות פעם אחת" (מדיניות פעם אחת), שמשמעה קבלת מידע[1] מהאזרח פעם אחת בלבד ושיתופו בין גופי ממשלה לצורך מתן שירותים שונים בלי שהאזרח יידרש למוסרו בכל פעם מחדש.**

בשנת 2016 החליטה הממשלה[2] לאמץ את מדיניות פעם אחת במשרדי הממשלה וביחידות הסמך, לשם שיפור השירות הממשלתי הניתן לציבור והפחתת הנטל הבירוקרטי המוטל עליו (החלטה 1933). על פי ההחלטה, חלה חובה על משרדי הממשלה להעביר ביניהם את המידע הנדרש לצורך שיפור השירות לציבור בהתאם למגבלות ולהוראות שנקבעו באותה החלטה ועל פי דין. כך למשל נקבע כי שיתוף המידע ייעשה תוך איזון בין החובה לשתפו לצורך מתן השירות המיטבי לאזרח ובין החובה לשמור על הפרטיות בהתאם לחוק הגנת הפרטיות, התשמ"א-1981, בין היתר מתוך תשומת לב לרגישות המידע, להיקפו ולתועלת לציבור שיש בשיתופו. בשנת 2020, בעיצומו של משבר הקורונה, החליטה הממשלה[3] על תוכנית להאצת השירותים הדיגיטליים לציבור (החלטה 260) שבמסגרתה הוחלט להטיל על משרד הדיגיטל דאז ועל כ-40 משרדים וגופים ציבוריים נוספים לקדם שינוי עומק בתהליכים בירוקרטיים, תוך שימוש באמצעים דיגיטליים מתקדמים ופלטפורמות טכנולוגיות רוחביות, ובכלל זה לבצע צעדים להקלת הנטל הבירוקרטי באמצעות מדיניות פעם אחת.

כדי שיהיה אפשר לממש את מדיניות פעם אחת במסגרת מתן שירותי הממשלה בהיקף רחב, יש לזהות ולמפות את השירותים שכל משרד נותן; לתקפם - לנתח את מאפייני השירות כגון האסמכתאות הנדרשות והגופים המעורבים; להוסיפם למאגר המקטלג את כלל השירותים הממשלתיים; לחברם לתשתית הטכנולוגית הממשלתית המאפשרת שיתוף מידע; לאשר את העברות המידע בין הגופים בוועדות להעברות מידע[4]. בהתאם להחלטה 1933 הקים מערך

1 נתונים השמורים במאגר ממשלתי או אישור שהנפיק משרד ממשלתי.

2 החלטת הממשלה 1933, "שיפור העברת המידע הממשלתי והנגשת מאגרי מידע ממשלתיים לציבור" (30.8.16).

3 החלטת הממשלה 260, "תוכנית להאצת השירותים הדיגיטליים לציבור ולקידום הלמידה הדיגיטלית ותיקון החלטת ממשלה" (26.7.20).

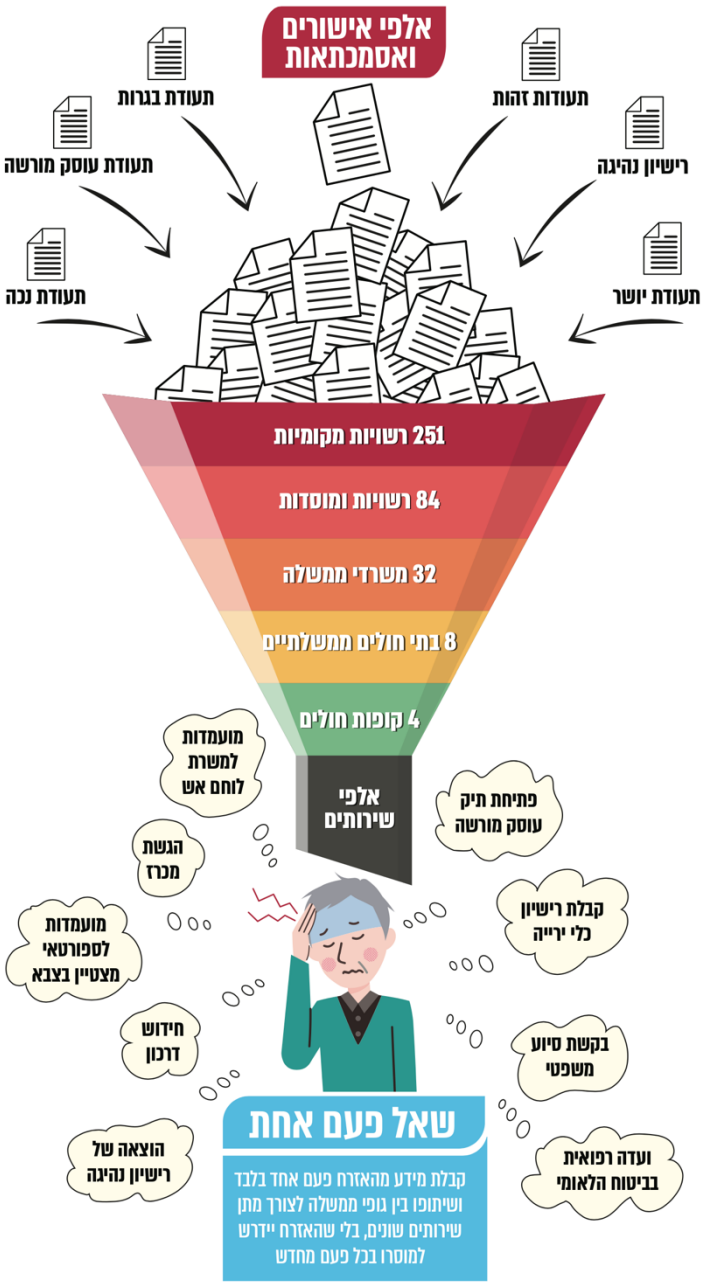
4 על פי תקנה 3א לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017, כל גוף ציבורי אשר מוסר או מקבל מידע נדרש למנות ועדה שמתפקידה לדון בבקשות למסירת מידע מן המשרד לגופים הציבוריים או בבקשות המשרד לקבלת מידע מאת גוף ציבורי אחר ולשקול אם לאשר בקשות אלה.

הדיגיטל[5] את שדרת המידע כתשתית ממשלתית מאובטחת להעברות מידע בין משרדי הממשלה והגופים הציבוריים ואת "מערכת ועדות" (מערכת מוע"ד) לסיוע בניהול ובאישור של תהליכי העברות מידע אלו.

דוח זה נכתב בין היתר בראי מלחמת "חרבות ברזל" (מלחמת חרבות ברזל) והמענה האזרחי לאוכלוסייה במהלך חודשי המלחמה מאז שבעה באוקטובר. החשיבות והתרומה שבמתן שירותים דיגיטליים לאזרחים רבות בעת שגרה, ורבות אף יותר בעת חירום. העברת מידע בין גופים ציבוריים היא ציר מרכזי בהתנהלות הממשלה והשירות הציבורי באירועי חירום, ובפרט לצורך מתן שירותים שחלקם קריטיים ומצילי חיים. במהלך מלחמת חרבות ברזל נזקקו מאות אלפי אזרחים ועסקים לשירותים שונים מהממשלה, כגון שירותים וסיוע למשפחות החטופים, הנעדרים והחללים; שירותים וסיוע למי שרכושם נפגע; שירותים וסיוע למפונים מבתיהם; שירותים למי שנפגעה פרנסתם; רישוי כלי ירייה. שירותים מקוונים יעילים יכולים לצמצם במעט את עוגמת הנפש של מי שחרב עליהם עולמם ולחסוך זמן ומשאבים הן בהגשת הבקשות ומיצוי הזכויות על ידי האזרחים והן במהלך הטיפול עצמו במשרדי הממשלה השונים.

5 מערך הדיגיטל הלאומי הוקם בשנת 2021 במסגרת איחוד רשות התקשוב הממשלתי ומטה המיזם הלאומי ישראל דיגיטלית (ישראל דיגיטלית).

המחשה של מדיניות פעם אחת



נתוני מפתח

?

בחלוף כשמונה שנים ממועד קבלת החלטת הממשלה בעניין יישום מדיניות פעם אחת בממשלה וביחידות הסמך, עדיין אין למערך הדיגיטל נתונים ביחס להיקף השירותים שבהם מיושמת מדיניות זו

רק ב-9%

מהשירותים הממשלתיים (350 שירותים מתוך 3,888) שדרת המידע[6] משמשת לצורך העברות מידע בין משרדי הממשלה והגופים הציבוריים

342 ימים

בממוצע נדרשו בשנת 2023 לאישור או דחייה של בקשה להעברת מידע בין גופים ציבוריים. כמעט פי שישה (570%) מהזמן שהוגדר בהחלטת הממשלה - 60 יום

240,000

בקשות לרישוי כלי ירייה המתינו לבחינת המשרד לביטחון לאומי בתקופת המלחמה (נכון לדצמבר 2023). למרות היקפי הבקשות, רק באפריל 2024 הוקם בין צה"ל לבין המשרד לביטחון לאומי ממשק דיגיטלי להעברת המידע הנדרש ביניהם לקידום בחינת הבקשות

0

מתוך 480 השירותים הניתנים על ידי משרד החינוך תוקפו, ולפיכך לא ניתן לדעת אילו מהם מתאימים ליישום מדיניות פעם אחת

0

התכנסויות של ועדת ההיגוי לעניין העברות מידע בין גופים ציבוריים בשנים 2021 - 2023

0

מהשירותים של משרד הביטחון הרלוונטיים למשפחות השכולות ולנכי צה"ל ממומשים באמצעות שדרת המידע

רק 20%

מהבקשות (209 מתוך יותר מ-1,000) להעברות מידע שהגישו גופים לרשות האוכלוסין מנוהלות במערכת הייעודית (מוע"ד) שבה אמורים לנהל את תהליכי העברות המידע בין הגופים

6 שדרת המידע היא תשתית מרכזית הנותנת מענה רוחבי אחיד המבוסס על פיתוח ממשקים סטנדרטיים להעברה מאובטחת של מידע בין משרדי הממשלה וגופים ציבוריים.

פעולות הביקורת

בשנת 2021 פרסם משרד מבקר המדינה דוח בנושא יישום מדיניות פעם אחת[7] (הדוח הקודם או הביקורת הקודמת). הנושאים העיקריים שנבדקו במסגרת הביקורת הקודמת הם הליך מיפוי השירותים הממשלתיים; קביעת יעדים לצמצום היקף המידע והאישורים הנדרשים מהציבור לקבלת שירות; פיתוח מערכת לניהול עבודת הוועדות להעברת מידע (מערכת מוע"ד); הקמת שדרת המידע הממשלתית (שדרת המידע או השדרה).

בחודשים יוני עד דצמבר 2023 ערך משרד מבקר המדינה ביקורת מעקב ממוקדת על ממצאים משמעותיים שעלו בביקורת הקודמת. ביקורת המעקב התמקדה בפעילות מערך הדיגיטל ליישום מדיניות פעם אחת ולקידום התשתיות התומכות ובמערכת מוע"ד. יודגש כי בביקורת זו נבדקו היבטים נוספים שלא נבדקו בביקורת הקודמת; ממצאים שעלו במסגרת בדיקות אלה שולבו בדוח הנוכחי בציון "בביקורת הנוכחית".

תמונת המצב העולה מן הביקורת

- **מיפוי ותיקוף של השירותים - בביקורת הנוכחית** נמצא כי 12 גופים כלל לא תיקפו את השירותים שהם מציעים, ובכללם 480 שירותים במשרד החינוך ו-129 שירותים בבתי הדין הרבניים. כמו כן עלה כי שמונה שנים אחרי שהממשלה קיבלה החלטה בנושא, מערך הדיגיטל לא קבע מדיניות לעניין המיפוי והתיקוף של השירותים, בכלל זה לעדכון ולטיוב של מאגר השירותים, ואין למערך תמונת מצב מלאה ועדכנית של כלל השירותים הממשלתיים, בכלל זה המידע והאישורים הנדרשים לשם אספקתם.

- **הרחבת הגופים הממופים - בביקורת הקודמת** הומלץ שרשות התקשוב וישראל דיגיטלית יבחנו את האפשרות לשלב במיפוי גופים ציבוריים נוספים הנותנים שירותים רבים לציבור כגון רשויות מקומיות, בתי חולים וקופות חולים. **בביקורת המעקב עלה כי הליקוי לא תוקן**, וכי על אף המלצת מבקר המדינה בדוח הקודם, הבחינה לא נעשתה וממילא טרם מופו ותוקפו שירותים הניתנים על ידי גופים ציבוריים שאינם גופים ממשלתיים. מצב זה פוגע בתהליכי שיפור השירות לציבור ובצמצום העומס הבירוקרטי המוטל עליו ואינו עולה בקנה אחד עם התוכנית להאצת השירותים הדיגיטליים הניתנים לציבור, שעליה החליטה הממשלה בשנת 2020.

- **שימוש משרדי הממשלה בשדרת המידע -** בביקורת הקודמת עלה כי שלושה גופים (צה"ל, רשות המיסים והמוסד לביטוח הלאומי) שעל פי החלטת הממשלה היו אמורים עד אפריל 2021 להטמיע את השימוש בשדרת המידע לצורך שיתוף מידע עם גופים אחרים לא

7 ראו מבקר המדינה, **דוח שנתי 72א** (2021), '"מדיניות פעם אחת' לשיפור השירות הממשלתי הדיגיטלי לציבור".

עשו כן. **בביקורת המעקב עלה כי הליקוי לא תוקן,** וכי צה"ל, רשות המיסים והמוסד לביטוח לאומי טרם התחברו לשדרת המידע, שלא בהתאם להחלטת הממשלה, המלצת מבקר המדינה בדוח הקודם ותוכנית הפריסה של רשות התקשוב דאז לחיבור הגופים לשדרת המידע. **עוד נמצא בביקורת הנוכחית** כי שלושה גופים אחרים הצורכים מידע שנמצא ברשות גופים אחרים: משרד הביטחון, משרד האנרגייה והתשתיות ורשות העתיקות, טרם התחברו לשדרת המידע על אף החלטת הממשלה בעניינם ותוכנית הפריסה של רשות התקשוב דאז. כמו כן, **בביקורת הנוכחית נמצא** כי בחלוף כשמונה שנים מקבלת החלטת הממשלה המנחה את משרדי הממשלה ויחידות הסמך להשתמש בתשתית הטכנולוגית הממשלתית לצורך שיתוף מידע (שדרת המידע), בתשתית זו (ובתשתיות מיושנות יותר שקדמו להחלטת הממשלה) נעשה שימוש לגבי פחות משליש מכלל השירותים (1,178 מתוך 3,888 שירותים), כך שבמרבית השירותים (70%) משרדי הממשלה משתמשים בתשתיות מקומיות, בדואר האלקטרוני או שהאזרח נדרש להעביר בעצמו את המידע הנדרש. היעדר השימוש בשדרת המידע פוגע במיצוי היתרונות האמורים ומונע את שיפור השירות לציבור ואת יישום מדיניות פעם אחת, שמטרתה לצמצם את הטרחה הנגרמת לאזרח בשל הדרישה להעברת אותו מידע לגופי ממשלה שונים.

שימוש משרד הביטחון בשדרת המידע - נמצא כי משרד הביטחון אינו מקבל אישורים שונים ממשרדי הממשלה באופן ישיר באמצעות שדרת המידע, ובמקום זאת דורש לקבל אישורים אלו מבני המשפחות השכולות ונכי צה"ל. משרד מבקר המדינה העיר למשרד הביטחון כי בפעילותו האזרחית הוא אינו שונה מכלל משרדי הממשלה במתן שירות לציבור באמצעות התווך הדיגיטלי המאובטח המוצע על ידי מערך הדיגיטל. מצופה היה כי דווקא בתקופת מלחמת חרבות ברזל, שבה נוספו אלפי בני משפחות למעגל השכול וכן אלפי נכים, ישפר המשרד את השירות לאוכלוסיות אלו באמצעות חיבור לשדרת המידע תוך יישום מדיניות פעם אחת, ולא יטריח אוכלוסיות אלו להמצאת אישורים ואסמכתאות ממשרדים שונים שלא לצורך.

מימוש מדיניות פעם אחת - ביקורת הקודמת עלה כי לא הייתה תמונת מצב שלמה ומפורטת על שיעור היישום של מדיניות פעם אחת במשרדי הממשלה, והומלץ לרשות התקשוב וישראל דיגיטלית לקבוע יעדים פרטניים ברמת המשרדים וברמת השירותים, בכלל זה לוח זמנים רב-שנתי להתקדמות, כדי להבטיח את ההגעה ליעדים שנקבעו בהחלטת הממשלה. **בביקורת המעקב נמצא כי הליקוי לא תוקן,** וכי בחלוף שמונה שנים מהחלטת הממשלה וארבע שנים מהביקורת הקודמת, למערך הדיגיטל עדיין אין מידע או נתונים בנוגע להיקף שירותי הממשלה המממשים את מדיניות פעם אחת ולהיקף שירותי הממשלה הפוטנציאליים למימוש מדיניות זו. למערך הדיגיטל גם אין מנגנונים לניטור מימוש מדיניות פעם אחת במשרדי הממשלה ולבקרה בנושא. עוד נמצא כי מערך הדיגיטל לא קבע בשנים 2021 - 2023 יעדים פרטניים, ברמת המשרדים וברמת השירותים, לשילוב השירותים הממשלתיים במסגרת שדרת המידע וליישום מדיניות פעם אחת. כמו כן נמצא שלא נקבע לוח זמנים רב-שנתי להתקדמות כדי להבטיח הגעה ליעדים שנקבעו בהחלטות הממשלה 1933 ו-260 בכל הנוגע למימוש מדיניות פעם אחת ולהרחבת השירותים הדיגיטליים הניתנים לציבור, אין תהליך בקרה ופרסום לציבור על העמידה בהחלטות אלו.

העברת מידע בין גופים ו"מערכת ועדות" לניהול עבודת הוועדות להעברת מידע (מערכת מוע"ד)

- **בביקורת הקודמת** הומלץ כי בדיווח השנתי שרשות התקשוב מגישה לממשלה בנוגע לעבודת הוועדות להעברת מידע ייכללו נתונים בנוגע לזמני הטיפול בבקשות בכל שלב לרבות לגבי צווארי בקבוק עיקריים בתהליך והסיבות לעיכובים. **בביקורת המעקב נמצא כי הליקוי לא תוקן**, וכי מאז שנת 2020 לא הפיק מערך הדיגיטל דוחות שנתיים לממשלה וממילא לא העביר לה דוחות כאמור. עוד נמצא שוועדת ההיגוי שהוקמה על פי החלטת ממשלה לצורך מעקב אחר יישום ההחלטה בכל הנוגע להעברות מידע בין משרדים לשם קידום מדיניות פעם אחת לא התכנסה כלל בשנים 2021 - 2023 כך שלמעשה פעולתה נפסקה. זאת, אף שהממשלה דרשה מוועדת ההיגוי בראשות המערך לדווח לה מדי שנה על סטטוס יישום ההחלטה לעניין העברות המידע. היעדר התכנסות ועדת ההיגוי ופרסום המידע לציבור פגעה בבקרה על יישום ההחלטה. חסר זה בבקרה בולט במיוחד לנוכח ממצאי הביקורת לעניין היקפי השימוש במערכת מוע"ד ופרקי הזמן הממושכים לטיפול בהעברות המידע בין המשרדים.

- **בביקורת הקודמת** נמצא כי רק כ-9% מכלל הבקשות שטופלו בוועדות להעברות מידע בין גופים ציבוריים בשנת 2019 נוהלו באמצעות מערכת מוע"ד. **בביקורת המעקב נמצא כי הליקוי לא תוקן** וכי למערך הדיגיטל אין נתונים בנוגע להיקפי הבקשות להעברות מידע שאינן מטופלות במערכת מוע"ד, וכי להערכת המערך בקשות רבות אינן מנוהלות במערכת מוע"ד. כך עלה כי בשנים 2021 - 2023 הוגשו לרשות האוכלוסין 209 בקשות באמצעות מערכת מוע"ד, שהן כחמישית (כ-20%) בלבד מכלל הבקשות להעברות מידע שהועברו לרשות בתקופה זו.

- **בביקורת הנוכחית עלה** כי בשנים 2018 - 2023, בממוצע, הוחזקה בקשה בטיפול הגוף מחזיק המידע 277 ימים, לעומת 60 ימים שהוגדרו לכך בהחלטת הממשלה. זמן הטיפול בבקשות להעברת מידע ארך אפוא יותר מפי ארבעה מהמתחייב על פי החלטת הממשלה. משך טיפול בבקשה להעברת מידע האורך כתשעה חודשים ואף יותר מרגע הגשת הבקשה להעברת המידע עד אישורו פוגע בשירות לציבור, משקף חוסר יעילות, גורם עומס בירוקרטי ובזבוז של משאבים וקשב ניהולי לעיסוק המתמשך. יודגש כי התמשכות התהליך להעברת המידע פוגעת ביישום מדיניות פעם אחת, המבוססת על העברות המידע בין המשרדים.

העברת מידע בין משרדים במהלך מלחמת "חרבות ברזל" - רישוי כלי ירייה בין צה"ל ובין המשרד לביטחון לאומי התנהל זה שנים משא ומתן להקמת ממשק מקוון להעברת נתונים בין הגופים. ואולם, מאחר שעד לאפריל 2024 לא הוקם ממשק כזה, לרבות באמצעות שדרת המידע, האזרח מגיש הבקשה לקבלת רישיון לכלי ירייה נדרש להגיש בד בבד גם בקשה לצה"ל לקבלת אישור על שירות בצבא (טופס 830). לאחר קבלת האישור מצה"ל נדרש המבקש להעביר אותו למשרד לביטחון לאומי. **בביקורת הנוכחית עלה כי** נוכח ההיקף החריג של בקשות לקבלת רישיון כלי ירייה מאז פרוץ המלחמה, פנה המשרד לביטחון לאומי לצה"ל באוקטובר 2023 בבקשה לקדם בהקדם את הקמת הממשק בין שני הגופים, ובחודשים נובמבר ודצמבר 2023 שלח בקשות רשמיות לקבלת המידע הנדרש להחלטת הוועדה להעברת מידע, וזאת בהתאם לתקנות הגנת הפרטיות. רק באפריל 2024,

שישה חודשים לאחר תחילת המלחמה, הממשק המקוון של צה"ל מול המשרד לביטחון לאומי לטובת רישוי כלי ירייה עלה לאוויר והופעל. זאת, על אף העומס שנכון לדצמבר 2023 הסתכם בכ-240,000 פניות שטרם טופלו, והנחיצות בהעברת מידע יעילה ובטווח זמנים קצר מצה"ל למשרד לביטחון לאומי, לצורך בחינה מהירה של הבקשות לרישיונות לכלי ירייה בתקופת המלחמה. דוגמה זו ממחישה את הנזק שבאי-ציות להחלטות הממשלה בדבר השימוש בשדרת המידע ומימוש מדיניות פעם אחת.

מיפוי ותיקוף של השירותים - בביקורת הקודמת עלה כי רק לגבי 933 (26%) מכלל 3,545 השירותים לציבור שמופו נעשה הליך הכרחי של ניתוח ותיקוף של מאפייני השירות (כגון האסמכתאות הנדרשות והגופים המעורבים) על ידי המשרדים נותני השירותים בשיתוף מערך הדיגיטל. בהיעדר ניתוח ותיקוף של מאפייני השירות קשה לקבוע אילו שירותים מתאימים ליישום מדיניות פעם אחת או באילו מהם מיישמים אותה בפועל באופן המביא לחיסכון בירוקרטי ניכר, ולפיכך קשה לפעול מול המשרדים הרלוונטיים לשם אכיפת החלטת הממשלה. כמו כן, הומלץ לקבוע לוחות זמנים ויעדים להתקדמות בפעולות ליצירת מאגר שירותים ולתיקופו מול המשרדים, לעקוב אחר מידת עמידתם של המשרדים בלוחות הזמנים וביעדים ולדווח לממשלה בהתאם לכך ולבחון דרכים לעדכון עיתי ואפקטיבי של המידע ולטיוב שלו. **בביקורת המעקב נמצא כי הליקוי תוקן במידה רבה**, וכי מתוך 3,888 שירותים שמופו, מערך הדיגיטל תיקף מול משרדי הממשלה 2,742 שירותים (70%).

העברת מידע בין גופים - בביקורת הקודמת הומלץ להשלים את הפעולות לפיתוח טופס מקוון שיאפשר ממשק עבודה יעיל במוע"ד עם גופים ציבוריים חיצוניים. **בביקורת המעקב נמצא כי ההמלצה יושמה,** וכי מערך הדיגיטל מעמיד לרשות הגופים הציבוריים החיצוניים, גופים שאינם מחוברים למערכת מוע"ד, טופס מקוון המקושר למערכת מוע"ד.

עיקרי המלצות הביקורת

על מערך הדיגיטל לקבוע תוכנית עבודה מפורטת לקידום מדיניות פעם אחת, לרבות לוחות זמנים שיחייבו את כלל משרדי הממשלה, יחידות הסמך והגופים הציבוריים שטרם מיפו ותיקפו את השירותים הניתנים על ידם או גופים שלא התחברו לשדרת המידע הממשלתית ואינם משתמשים בה לצורך העברת המידע בין גופים - כל זאת כדי שפעולות אלו ישמשו תשתית מתאימה ליישום מדיניות פעם אחת. אם למערך הדיגיטל אין סמכות מספקת בכל הנוגע לקידום פעולת הגופים כמתחייב מהחלטת הממשלה הרי שעליו לפעול להסדרת ההרחבה של סמכות ההנחיה שלו באמצעות החלטת ממשלה או בכל דרך אחרת שתיקבע. כמו כן, מוצע כי המערך יבחן את האפשרות לעגן את כלל לוחות הזמנים בהחלטת ממשלה מחייבת.

- על משרד החינוך, המשרד להגנת הסביבה, בתי הדין הרבניים, רשות המיסים בישראל, שירות התעסוקה, משרד הפנים ומשרד התרבות והספורט, בשיתוף פעולה עם מערך הדיגיטל, להשלים את מיפוי השירותים שהם נותנים לציבור ואת תיקופם.

- על צה"ל, רשות המיסים, המוסד לביטוח לאומי, משרד הביטחון, משרד האנרגייה והתשתיות, רשות העתיקות והלשכה המרכזית לסטטיסטיקה, להשלים את הפעולות הנדרשות לשם חיבורם לשדרת המידע. על גופים אלו ליישם את העברות המידע מהם ואליהם באמצעות השדרה תוך ניצול יתרונותיה, כדי לממש את מדיניות פעם אחת במתן שירות לציבור בכלל, ובפרט באירועי החיים שצוינו בהחלטות הממשלה: לידה, מעבר דירה, מעבר בין עבודות, נכות, הזדקנות לסיעוד, פטירה, פתיחת עסק וייבוא מסחרי.

- על משרד הביטחון ליישם לאלתר את החלטת הממשלה ואת הערת מבקר המדינה בדוח הקודם לעניין החיבור לשדרת המידע, וכפועל יוצא מכך לתת שירות בהתאם למדיניות פעם אחת.

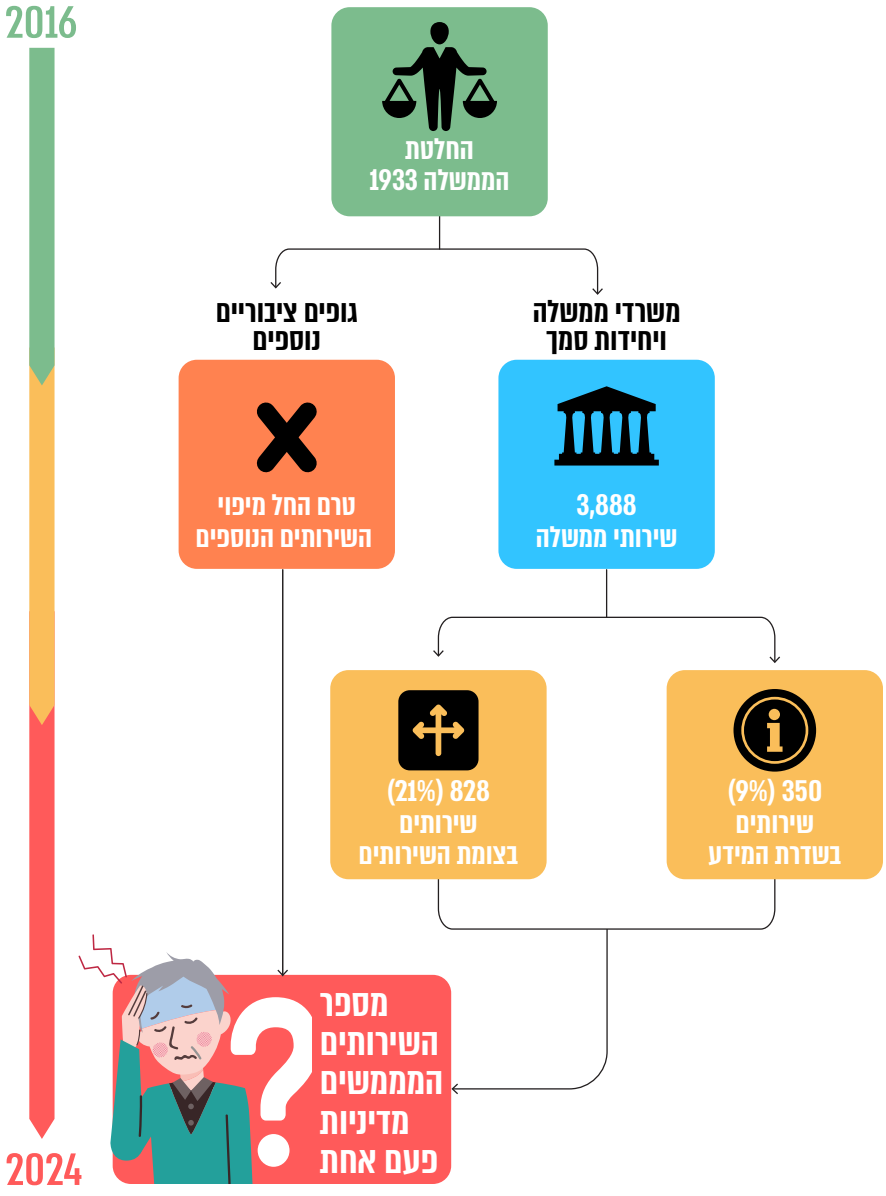
- על מערך הדיגיטל לפעול מול כלל הגופים הממשלתיים שטרם השלימו את מחויבויותיהם להתחברות ושימוש בשדרת המידע על פי החלטת הממשלה, כדי לוודא שהגופים פועלים למימושה, לעדכן בהתאם את תוכנית הפריסה של שדרת המידע ולכלול בה לוחות זמנים מחייבים לחיבור הגופים הרלוונטיים לשדרת המידע, בהתאם להחלטת הממשלה. עוד מוצע כי המערך יגדיר ממדי הצלחה ויעקוב אחר מימושם. כמו כן, על כלל המשרדים והגופים הציבוריים הרלוונטיים, המציעים שירותים לציבור להתחבר לשדרת המידע ולהציע באמצעותה את השירותים שהם נותנים לציבור. מוצע כי מדדי ההצלחה ועמידת משרדי הממשלה ביעדים אלו ידווחו לממשלה ולציבור במסגרת הדוח השנתי של המערך.

- על ראשת מערך הדיגיטל לחדש את פעילות ועדת ההיגוי לעניין העברות מידע ולכנסה לצורך פיקוח על עבודת משרדי הממשלה והגופים הציבוריים לשם השגת תכלית מדיניות פעם אחת, וכן לעקוב אחר כשלים ביישום המדיניות כאמור בהחלטת הממשלה, כל זאת לשם שיפור השירות הממשלתי לציבור והפחתת הנטל הבירוקרטי המוטל עליו. כמו כן, על הוועדה לדווח לממשלה על מימוש ההחלטה, לרבות לעניין זמני העברת המידע בין גופים בפועל. כמו כן עליה לחדד לכלל הגופים הציבוריים את חובתם לנהל את תהליכי אישור העברות המידע ביניהם ולממשן בפועל ביעילות ובמהירות באמצעות תשתיות שהמערך מעמיד לטובת תהליכים אלו, ובכללן שדרת המידע ומערכת מוע"ד, זאת לשם ייעול ושיפור השירות לציבור.

- על משרד המשפטים להשלים את עבודת הצוות הבין-משרדי לשיפור תחום העברות המידע ולהעביר את כל התהליך שינוי משמעותי, בהתאם להחלטת הממשלה ובאופן שיבטיח קיצור ניכר בתהליך האישור ובמשכי העברות המידע בין הגופים. על מערך הדיגיטל להשלים את יישום תהליכי שיפור לעבודת הוועדות המשרדיות להעברת מידע בין גופים, כולל יישום אוטומציה ותהליכים דיגיטליים לניהול התהליך הכולל במערכת החדשה - מערכת צ'יטה[8], כדי לסייע בצמצום משך הטיפול מהגשת הבקשה עד ההחלטה הסופית בעניין לפחות מ-60 יום בהתאם לפרק הזמן שהוגדר לשם כך בהחלטת ממשלה.

8 מערכת מידע חדשה המוקמת על ידי מערך הדיגיטל לניהול הליכי העברות מידע בין משרדים.

מספר השירותים המממשים את מדיניות פעם אחת, שמונה שנים לאחר קבלת החלטת הממשלה בעניין



על פי נתוני מערך הדיגיטל, בעיבוד משרד מבקר המדינה.

סיכום

כדי לצמצם את הנטל הבירוקרטי ולשפר את השירות שהממשלה נותנת לציבור, החליטה הממשלה בשנת 2016 לממש את מדיניות פעם אחת בשירות הציבורי. על פי מדיניות זו, אם מידע שגוף ציבורי אחד זקוק לו לשם מתן שירות לאזרח או לעסק נמצא בידי גוף ציבורי אחר, אין לבקשו מהאזרח או מהעסק מקבל השירות, ויש לקבל את המידע מאותו גוף המחזיק בו. בשנת 2020 החליטה הממשלה על האצת מתן השירותים הדיגיטליים לציבור, בין היתר באמצעות מימוש מדיניות פעם אחת. מלחמת חרבות ברזל המחישה ואף העצימה את החשיבות שבמתן שירותים דיגיטליים לציבור תוך יישום מדיניות פעם אחת.

משרד מבקר המדינה פרסם בשנת 2021 דוח ביקורת בנושא יישום החלטות הממשלה בנושא. מהדוח הקודם עלה כי עוד ארוכה הדרך ליישום של החלטת הממשלה שקבעה כי החל משנת 2021 משרד ממשלתי לא יבקש מהציבור, לשם מתן שירות, אישור שהנפיק משרד ממשלתי אחר. ארבע שנים לאחר החלטת הממשלה עדיין לא הייתה תמונת מצב בנוגע לשיעור היישום של מדיניות פעם אחת במשרדים. נוכח זאת, לא ניתן היה לקיים הליך של הצבת יעדים להמשך מימוש המדיניות, לרבות קביעת אבני דרך להתקדמות ומעקב אחר ביצוען. דוח מעקב זה בחן את תיקון הליקויים העיקריים שעלו בביקורת הקודמת.

בביקורת המעקב, שמונה שנים לאחר קבלת החלטת הממשלה הראשונה בנושא, ואף שחלה התקדמות ניכרת בפעולה מקדמית שנחוצה לצורך יישום מדיניות פעם אחת ביחס לדוח הביקורת הקודם - בהיקף מיפוי השירותים הממשלתיים הניתנים לציבור וניתוח מאפייניהם, מרבית הליקויים שהועלו בדוח הקודם לא תוקנו: שיעור השירותים בשדרת המידע - תשתית טכנולוגית שהוקמה לצורך מתן מענה רוחבי מאובטח להעברת מידע בין כלל משרדי הממשלה - הוא 9% בלבד מהשירותים הממשלתיים, היעדים שנקבעו בהחלטות הממשלה רחוקים מהשגה, ולמערך הדיגיטל אין יעדים ותוכניות מפורטות למימושם. כמו כן, אין מעקב ובקרה בנושא הקידום והיישום של מדיניות פעם אחת: למערך הדיגיטל אין נתונים ביחס להיקף השירותים הממשיים והפוטנציאליים ליישום מדיניות פעם אחת; הוא אינו מעביר דיווחים עיתיים לממשלה בנוגע לסטטוס העמידה בהחלטות הממשלה; ועדת ההיגוי הבין-משרדית שהוקמה כדי לעקוב אחר יישום ההחלטות אינה מתכנסת.

העברת מידע בין המשרדים היא ציר מרכזי ליישום מדיניות פעם אחת. ממצאי דוח זה מלמדים שמשרדי הממשלה מתנהלים שלא בהתאם להחלטות הממשלה ולהנחיות מערך הדיגיטל, בין היתר בכך שמשכי הזמן לטיפול בהעברות המידע ביניהם עולים לכדי חריגה של 300% ומעלה ממשך הזמן שקבעה הממשלה - זמן ההעברה הממוצע היה כתשעה חודשים למול 60 ימים שנקבעו בהחלטת הממשלה. ממשכי זמן הטיפול הארוכים וממספר השירותים הגדול שטרם תוקפו וטרם חוברו לשדרת המידע, ניכרת מחויבות נמוכה של משרדי הממשלה ויחידות הסמך ליישום החלטות הממשלה.

במהלך מלחמת חרבות ברזל, ולנוכח ההיקף החריג של כ-240,000 בקשות חדשות לקבלת רישיון כלי ירייה שהמתינו לבחינת המשרד לביטחון לאומי נכון לדצמבר 2023, העביר המשרד לביטחון לאומי לצה"ל בקשה לקבלת מידע בממשק מקוון. רק באפריל 2024, כשישה חודשים מתחילת המלחמה, הוקם והופעל הממשק המקוון בין צה"ל ובין המשרד לביטחון לאומי, זאת על אף הנחיצות שבהעברת מידע יעילה ומהירה מצה"ל למשרד לביטחון לאומי לצורך בחינה

של הבקשות לרישיונות לכלי ירייה בתקופת המלחמה.

עולה אפוא כי התוכנית הממשלתית שעליה החליטה הממשלה עוד בשנת 2016 עדיין לא עלתה, גם בחלוף שמונה שנים, על מסילת יישום ממשית, וכי השלמת התהליך בכללותו אינה נראית באופק של השנים הקרובות. נראה כי בעיית השורש בעניין זה היא מגבלת יכולתו של מערך הדיגיטל לנקוט פעולות ליישום התוכנית, שכן עיקר פעילותו מול הגופים הממשלתיים אינה נשענת על סמכויות שיש בהן כדי לחייב את משרדי הממשלה לביצוע בפועל. חולשה זו בד בבד עם היעדר הירתמות של הגופים הממשלתיים והציבוריים ליישום ההחלטה והנחיות מערך הדיגיטל בנושא מובילים למימוש מצומצם של מדיניות פעם אחת.

כדי להאיץ את מימוש המדיניות, על מערך הדיגיטל לאמץ ראייה מערכתית ומתכללת לשם טיפול בכל המרכיבים התורמים למימושה, זאת בד בבד עם ההירתמות הנדרשת מכלל משרדי הממשלה ויחידות הסמך, ליישם את התהליכים התורמים ליישום מדיניות פעם אחת. בכלל זה נדרשת פעולתם של מערך הדיגיטל והמשרדים, כל אחד בתחומו, בסוגיות האלה: מיפוי ותיקוף של השירותים הניתנים לציבור, חיבור המשרדים לשדרת המידע והקמת הפורטלים התומכים, קידום ושיפור של תהליכי העברות המידע בין המשרדים, בכלל זה באמצעות מערכת מוע"ד. מוצע כי המערך יפעל לקדם את מדיניות הממשלה האמורה גם בקרב גופים ציבוריים נוספים ובכללם השלטון המקומי ומערך הבריאות. מתן מענה לפערים שעלו בביקורת הקודמת ובביקורת המעקב יאפשר שיפור וייעול של השירות לציבור ושל עבודת הממשלה. אם לצורך המימוש האמור יידרשו למערך סמכויות נוספות, עליו לפנות לממשלה להסדרתם.

על מערך הדיגיטל לשקף לממשלה ולציבור בדוחותיו השנתיים את מידת המימוש של החלטות הממשלה, הן בנוגע למדיניות פעם אחת והן לעניין העברות המידע בין הגופים. היעדר שינוי משמעותי בקצב יישום מדיניות פעם אחת יחייב את מערך הדיגיטל להביא את הנושא לפני הממשלה, כדי שהיא תבחן את האפשרות לעדכן את החלטות הממשלה ולכלול בהן לוחות זמנים מחייבים ליישום הפעולות על ידי משרדי הממשלה והגופים הציבוריים.

על שר הכלכלה הממונה על מערך הדיגיטל לעקוב אחר מימוש החלטות הממשלה בעניין מדיניות פעם אחת ולהציג לפני הממשלה, מדי פעם בפעם, את סטטוס מימוש המדיניות. על הצוות הבין-משרדי, בראשות משרד המשפטים, להשלים את דיוניו ולהציג לממשלה מתווה להסרת חסמים ולקידום תהליכי העברת מידע יעילים ומהירים בין משרדי הממשלה והגופים הציבוריים, כל זאת לשם מימוש החלטות הממשלה לשיפור השירות לציבור ולהפחתת הבירוקרטיה.

מידת תיקון עיקרי הליקויים שעלו בדוח הקודם

פרק הביקורת	הגוף המבוקר	הליקוי בדוח הביקורת הקודם	מידת תיקון הליקוי כפי שעלה בביקורת המעקב			
			לא תוקן	תוקן במידה מועטה	תוקן במידה רבה	תוקן באופן מלא
העברת מידע בין גופים ומערכת מוע"ד	רשות התקשוב	על רשות התקשוב להשלים את הפעולות לפיתוח טופס מקוון שיאפשר ממשק עבודה יעיל במוע"ד עם גופים ציבוריים חיצוניים.				←
מיפוי ותיקוף של השירותים הניתנים לציבור	רשות התקשוב, ישראל דיגיטלית, משרדי הממשלה ויחידות הסמך	משרדי הממשלה ויחידות הסמך בשיתוף מערך הדיגיטל תיקפו רק כ-26% מכלל השירותים שמופו (933 שירותים מתוך 3,545). בהיעדר תיקוף מלא של השירותים שמופו, לא הייתה לרשות התקשוב ולישראל דיגיטלית תמונה שלמה ומהימנה על מספר השירותים הכולל שכל משרד נותן לציבור, על שדות המידע והאישורים הנדרשים לקבלת כל שירות ועל גוף המקור המנפיק כל אישור.			←	
מיפוי ותיקוף השירותים הניתנים לציבור	רשות התקשוב וישראל דיגיטלית	הומלץ שרשות התקשוב וישראל דיגיטלית יבחנו את האפשרות לשלב במיפוי שנעשה לצורך בחינת האפשרות למימוש מדיניות פעם אחת גופים ציבוריים נוספים הנותנים שירותים רבים לציבור, כגון רשויות מקומיות, בתי חולים וקופות חולים.	←			

פרק הביקורת	הגוף המבוקר	הליקוי בדוח הביקורת הקודם	מידת תיקון הליקוי כפי שעלה בביקורת המעקב			
			לא תוקן	תוקן במידה מועטה	תוקן במידה רבה	תוקן באופן מלא
שימוש משרדי הממשלה בשדרת המידע	רשות המיסים, המוסד לביטוח לאומי, משרד הביטחון	שלושה גופים שנדרשו בהחלטת הממשלה 260 משנת 2020 להחצין מידע בשדרת המידע עד אפריל 2021 עדיין לא הטמיעו את המערכת - רשות המיסים, המוסד לביטוח לאומי ומשרד הביטחון.	←			
מימוש מדיניות פעם אחת	רשות התקשוב	באוגוסט 2020 לא הייתה בידי רשות התקשוב תמונה שלמה ומפורטת של שיעור היישום של מדיניות פעם אחת במשרדים, על כל נדבכיה, וכן לא היה אפשר לקיים הליך מיטבי של הצבת יעדים למימוש המדיניות, לרבות קביעת אבני דרך להתקדמות ולמעקב אחר ביצוען.	←			
העברת מידע בין גופים ומערכת מוע"ד	רשות התקשוב	הומלץ לכלול בדיווח השנתי שרשות התקשוב מגישה לממשלה בנוגע לעבודת הוועדות נתונים בנוגע לזמני הטיפול בבקשות בכל שלב, לרבות בנוגע לצווארי בקבוק עיקריים בתהליך אישור הבקשות ולסיבות לעיכובים. זאת כדי לשקף תמונה מלאה של תהליך העברת המידע הן בצד מבקש המידע והן בצד המחזיק בו ושל השלבים בתהליך הדורשים שיפור.	←			
העברת מידע בין גופים ומערכת מוע"ד	רשות התקשוב ומשרדי הממשלה הרלוונטיים	רק כ-9% מכלל הבקשות שטופלו בוועדות להעברות מידע בין גופים ציבוריים בשנת 2019 נוהלו באמצעות מערכת מוע"ד. על רשות התקשוב והגופים שטרם התחברו למוע"ד לנקוט את הצעדים הנדרשים לצורך חיבורם למערכת.	←			

דוח מבקר המדינה - סייבר ומערכות מידע |
חשוון התשפ"ד | נובמבר 2024

דואר ישראל

מערכות המידע בחברת דואר ישראל ובבנק הדואר

מערכות המידע בחברת דואר ישראל ובבנק הדואר

רקע

חברת דואר ישראל היא חברה ממשלתית בבעלות מלאה של מדינת ישראל, המספקת שירותי דואר וכן מפעילה שירותים בנקאיים באמצעות חברת הבת שלה - בנק הדואר. נכון לסוף שנת 2023, לחברת הדואר ולבנק הדואר 400 יחידות דואר, 650 מרכזי מסירה וכ-60 מרכזי דוורים אזוריים. כ-11.9 מיליון לקוחות החברה והבנק קיבלו שירות ביחידות הדואר בשנת 2023.

חברת הדואר מספקת ללקוחותיה מגוון שירותים, כגון שירותי דואר בישראל, משלוח מסמכים וסחורות בין ישראל לחו"ל והפעלת רשת מוקדי שליחים המספקת שירותי הפצה ללקוחות עסקיים ופרטיים בכל רחבי הארץ.

בנק הדואר מספק שירותים פיננסיים ללקוחות עסקיים, לגופי ממשלה ולכלל הציבור. בנק הדואר הוא בבעלות ממשלתית ונתון לפיקוח משרד התקשורת, כמו חברת דואר ישראל. שירותי בנק הדואר ניתנים באמצעות כ-400 סניפים של חברת הדואר והם כוללים שירותי אשנב בנקאיים. בבנק הדואר כ-510,000 חשבונות בנק, שיעור הפיקדונות הכולל בבנק זה הוא כ-4.7 מיליארד ש"ח, מתבצעות בו כ-22 מיליון פעולות של לקוחות מזדמנים בשנה ומספר לקוחותיו הכולל הוא כמיליון.

בחברת הדואר ובבנק הדואר יש מגוון רחב מאוד של מערכות מידע, ובכלל זה מערכות תפעוליות המשמשות לצרכים אלה: יצוא ומכס, שירותי דיגיטל, שירותי שליחים, בנק וקמעונאות, מטה, תשתיות ואבטחת מידע, הפעלה וטלפוניה.

באפריל 2023 התגלתה תקיפת סייבר במערכות המידע של הדואר. בבדיקה שביצעו צוותי אבטחת מידע וסייבר של אגף מערכות מידע בדואר ישראל ב-2.4.23 התגלתה פעילות חשודה במערכות המידע של הדואר. ב-5.4.23 הופעל צוות IR[1] של חברה חיצונית שנותנת שירותי הגנת סייבר לדואר ישראל. בחברה הוחלט כצעד מניעתי לנתק את מערכות הדואר מרשת האינטרנט. החברה החיצונית זיהתה עדות לפעילות התוקף במערכות החברה החל מיולי 2022. החברה החיצונית לא הצליחה לזהות את התוקף, והתוקף הצליח להוציא מהארגון את מאגר המשתמשים והסיסמאות. כתוצאה מכך הושבתו שירותים רבים של החברה. בין היתר, לא ניתן היה לבצע תשלומים מקוונים, העברת בעלות רכב, תשלומים להוצאה לפועל והעברות לקופות חולים. כמו כן, חלו עיכובים בשחרור פריטים המגיעים מחו"ל. עם התקדמות עבודת צוות החברה החיצונית הופעלו השירותים בהדרגה.

1 צוות תגובה לאירועי סייבר.

נתוני מפתח

124 מיליוני ש"ח
ממוצע שנתי של הוצאות התפעול וההשקעות של אגף מערכות מידע בשנים 2019 - 2022

55
מספר מערכות המידע בחברת דואר ישראל. בבנק הדואר יש 16 מערכות מידע נוספות

48.75%
שיעור הירידה של תקציב ההשקעות המתוכנן באגף מערכות מידע מ-64.2 מיליוני ש"ח בשנת 2019 ל-32.9 מיליוני ש"ח בשנת 2022

64%
שיעור הפניות בנושא תקלות חומרה מסך הפניות הקשורות לתקלות שגרמו להשבתת תחנות קצה ביחידות הדואר

683
מחשבים בלבד הוחלפו או שודרגו מסך של 1,850 אשר נדרש להחליפם או לשדרגם ל-WIN 10

85
בעלי ההרשאות למערכת ג'[2] (ששיעורם 3% מכלל בעלי ההרשאות במערכת זו) אינם מוגדרים במערכת משאבי אנוש כעובדים פעילים בחברה, נכון לינואר 2024

780
מבעלי ההרשאות הפעילות במערכת הניהול המרכזי של הרשת[3] (המהווים כ-13% מכלל בעלי ההרשאות במערכת זו) הם עובדים שאינם נכללים ברשימת העובדים הפעילים במערכת משאבי אנוש בחברה

449
בעלי הרשאות פעילות מתוך 780 בעלי ההרשאות הפעילות אשר אינם מופיעים כ"פעילים" במערכת משאבי אנוש לא התחברו למערכת הניהול המרכזי של הרשת מתחילת שנת 2024

פעולות הביקורת

בחודשים יוני 2023 עד מרץ 2024 בדק משרד מבקר המדינה את פעולותיה של חברת דואר ישראל ובנק הדואר בתחום מערכות המידע. הביקורת בוצעה בחברת הדואר ובבנק הדואר. בין יתר הבדיקות משרד מבקר המדינה ביצע בדיקה על אופן ניהול הרשאות המשתמשים בדואר והבקרה עליו. בדיקות השלמה נעשו במשרד התקשורת.

2 המערכת המרכזית לניהול תהליכי אשנב המשמשת גם קופה של דואר ישראל לצורך כל הפעולות הכספיות המבוצעות בסניפים ובסוכנויות.

3 מערכת כלים ייעודית המשמשת לניהול מרוכז של רשתות מחשבים בארגונים.

תמונת המצב העולה מן הביקורת

- **חיבור ה-SOC של חברת הדואר ל-SOC המגזרי של משרד התקשורת -** כלי חשוב הנכלל במערך ההגנה על נתונים ומשאבים ארגוניים הוא SOC (SECURITY OPERATION CENTER). זהו מרכז פעולות אבטחה המדווח על פעולות חריגות, איומים פוטנציאליים, תובנות על בסיס ממצאי החקר שבוצע בעקבות אירוע ועוד. חברת הדואר מפעילה SOC באחריותו של אגף מערכות מידע בחברת הדואר. שירותי ה-SOC מושכרים מחברה פרטית. בביקורת עלה כי אף שבשנים 2022 - 2023 היחידה המגזרית במשרד התקשורת, המפעילה SOC מגזרי הממומן על ידי משרד התקשורת ומערך הסייבר הלאומי, פנתה כמה פעמים לחברת הדואר בבקשה לחבר את חברת הדואר ל-SOC של משרד התקשורת, במועד סיום הביקורת חברת הדואר טרם התחברה ל-SOC של משרד התקשורת. בכך החברה אינה מנצלת את היתרונות הגלומים בחיבור ל-SOC של משרד התקשורת, ובהם בקרה חיצונית נוספת בעת התרחשותן של תקיפות סייבר.

- **תוכניות עבודה שנתיות ורב-שנתיות בתחום מערכות המידע -** אף שהיקף תקציב אגף מערכות מידע בחברת הדואר הוא מהותי ונע בין כ-102 מיליוני ש"ח לכ-136 מיליוני ש"ח ושיעור תקציב האגף מסך תקציב החברה נע בין 17.2% עד 19.6% (כ-102 מיליוני ש"ח מסך תקציב של כ-592 מיליוני ש"ח בשנת 2022 וכ-136 מיליוני ש"ח מסך תקציב של כ-693 מיליוני בשנת 2020), אין לחברה ולבנק הדואר נוהל להסדרת נושא תוכניות העבודה, ואף בשנים 2019 - 2023 לא הייתה תוכנית עבודה רב-שנתית בתחום מערכות המידע. תהליך גיבוש תוכנית העבודה עד לתום שנת 2023 אינו כולל בחינת חלופות בראייה אגפית, אלא מתבסס בעיקר על תקציב קבוע ומוגדר מראש. לא מתבצע מעקב אחר יישום תוכנית העבודה, ונבצר מהנהלת החברה לדעת בכל רגע נתון מה היא תוכנית העבודה ואילו שינויים בוצעו בה. כמו כן, לא ניתן לעקוב אחר תקציבים שהוסטו ממשימה למשימה, ואף הנהלת אגף מערכות מידע אינה יודעת להעריך כמה שעות עבודה הושקעו בכל משימה. יצוין כי בשנת 2024 החברה הטמיעה תוכנה ייעודית לניהול הצוותים והפרויקטים.

- **תקלות במערכות מידע בדואר ובבנק הדואר -** בשנת 2018 הציג אגף מערכות מידע במצגת את הצורך בהחלפת ציוד מחשוב מיושן ביחידות הקצה, ואת בשל תקלות חומרה רבות. על פי נתוני החברה, מ-1.4.22 עד 21.7.23 הגישו משתמשי המערכות 46,349 פניות אשר סווגו כתקלות חומרה. מספר הפניות על תקלות בשל בעיות חומרה הוא הגדול ביותר ושיעורו כ-35% מסך הפניות בחברה. בתקופה זו כ-64% מהפניות הקשורות לתקלות שגרמו להשבתת תחנה בנקודת קצה עסקו בתקלות חומרה, שהן 3,306 פניות מתוך 5,178 פניות שנבחנו, וכ-32% מהתקלות שגרמו להשבתה מלאה של יחידות דואר בתקופה הנבדקת היו תקלות חומרה, שהן 525 תקלות מתוך 1,618 תקלות שנבחנו. כמו כן, כ-80% מכלל תקלות החומרה שבגינן הושבתו תחנות קצה וכ-92% מתקלות החומרה שגרמו להשבתה של יחידות דואר הן תקלות בציוד ממוחשב אשר בשנת 2018 חלקו כבר הוגדר כציוד שנדרש להחליפו. מנתונים אלה אפשר ללמוד על היקף הפגיעה של חומרה מיושנת בתפקוד של יחידות הדואר, וכפועל יוצא מכך על פגיעתן בשירות שניתן ללקוחות.

- **פרויקט החלפת ציוד ממוחשב מיושן בחברת הדואר ובבנק הדואר -** פרויקט החלפת הציוד[4] אושר בתוכניות העבודה לשנים 2019 - 2023. בד בבד עם החלפת המחשבים החל גם שדרוג מערכות ההפעלה למערכות הפעלה WIN-10. פרויקט החלפת הציוד הממוחשב הוגדר כפרויקט אסטרטגי כבר בשנת 2019. על אף האמור, רק בתחילת שנת 2022 החלו בחברת הדואר ברכישת ציוד מחשוב חדש. נכון למועד סיום הביקורת, יותר מארבע שנים לאחר שעלה הצורך בהחלפת ציוד מחשוב מיושן, תקלות רבות נגרמות בשל אי-החלפתו, והדבר מחזק את הצורך הדחוף בהחלפת הציוד. עד מרץ 2024 החברה החליפה ושדרגה רק 683 מחשבים (כ-37%) מכלל 1,850 המחשבים שיש לשדרגם ל-WIN-10 ולהחליפם; שדרגה רק 196 (כ-56%) מכלל 350 מחשבי הפלזמה שיש לשדרג ל-WIN-10; וכן שדרגה רק 136 (כ-68%) מכלל 200 המערכות לניהול תורים שיש לשדרג. כמו כן בביקורת נמצא כי הפחת השנתי על מחשבים וציוד נמוך במעט מרכישות של אלה ברוב השנים. סך רכישות המחשבים והציוד ההיקפי בשנים 2019 - 2022 הוא 39.8 מיליוני ש"ח, וסך הפחת השנתי לשנים אלה הוא 37.4 מיליוני ש"ח (כ-94%). מנתונים אלה עולה כי השקעות החברה ברכש תוכנה ומחשבים וציוד היקפי גבוהות רק במעט מהפחת על ההשקעות שנעשו בשנים קודמות, ובשנת 2022 ההשקעה ברכש תוכנה ומחשבים וציוד היקפי הייתה נמוכה מהפחת על ההשקעות שנעשו בשנים קודמות. ניתן להסיק כי החברה שומרת על המצב הקיים ולא דואגת לשיפור מתמיד בתחום מערכות המידע.

- **מערכת ניהול תורים ממוחשבת -** בשנת 2007 החלו חברת הדואר ובנק הדואר להפעיל מערכות לניהול תורים בחלק מיחידות הדואר על ידי שימוש ב"תוכנת מדף". בביקורת נמצא כי המערכת הקיימת אינה מאפשרת ללקוחות החברה להזין מידע על השירות שלשם קבלתו קבעו את התור[5], ואינה מקצה ללקוח זמן נדרש בהתאם לצרכיו. פרק הזמן שנדרש להקצות ללקוח המגיע לאשנב לצורך פתיחת חשבון בנק בבנק הדואר הוא לרוב ארוך בהרבה מפרק הזמן שנדרש להקצות ללקוח המגיע לאסוף חבילת דואר. עקב כך לעיתים עלול להיווצר בסניפי בנק הדואר תור ארוך, והשירות עלול להינתן ללקוחות זמן רב לאחר המועד שנקבע להם. המערכת אינה מאפשרת הזנה של מידע על השירות שלשם קבלתו נקבע התור ואינה מזהה את הפעולות שהלקוח רוצה לבצע. זיהוי מוקדם של הפעולות יכול היה לסייע לעדכון הלקוח מראש במסמכים הנדרשים או בהכנות הנדרשות לקבלת השירות. כמו כן, לקוח יכול לבטל תור ביוזמתו. עם זאת, המערכת אינה שולחת הודעות ללקוחות כדי לוודא שהם מגיעים לסניף לקבלת השירות בתור שנקבע או לחלופין לביטול התור שנקבע. חוסר התאמה של המערכת לניהול תורים לאופי פעילות החברה ולצורכי החברה מקשה את ניהול התורים באופן יעיל ואפקטיבי וגורם לפגיעה בשירות ללקוח.

- **ריבוי מערכות והיעדר ממשק ביניהן -** במועד סיום הביקורת מופעלות בחברת הדואר 55 מערכות מידע, שחלקן נחלקות לתתי-מערכות, ובבנק הדואר יש 16 מערכות נוספות שחלקן נחלקות לתתי-מערכות. למערכות אלו יש יותר מ-20 ספקים שונים, והן מבוססות על טכנולוגיות שונות. ריבוי המערכות והיעדר ממשק ביניהן מובילים לפגיעה באינטגרציה בין המערכות, בחוסר אחידות בנתונים ובקושי בניהול תהליכים. בשל היעדר האינטגרציה בין המערכות בחברה ובבנק נוצר קושי בסנכרון נתונים בין מערכות, והדבר עלול לגרום לטעויות. לפיכך, החברה משקיעה בתשומות כוח האדם או בפיתוח תהליכים ידניים מפצים,

4 מחשבים, מדפסות, עמדות ממוחשבות לניהול תורים, מסכי מחשב וציוד חומרה נוסף.

5 מלבד העברת בעלות רכב.

כגון תהליכים ליצירת התאמה בין המערכות או תהליכים לפיתוח מערכות נוספות. כך לדוגמה, למערכת מידע משאבי אנוש אין ממשק ממוחשב עם מערכת המחשב המרכזי[6] של הבנק. לצורך ביטול הרשאות של עובד[7] במערכת המחשב המרכזי נעשות פעולות ידניות מפצות: נשלח דוא"ל מאגף משאבי אנוש לבעלי תפקידים במערכת המחשב המרכזי בבקשה לבטל את הרשאות העובד במערכת. נדרשת פעולה של ביטול ההרשאות. נוסף על כך, פעם בחודש מתבצע תהליך של בקרה מפצה הכולל הפקת דוח חריגים בעניינם של כל העובדים שפרשו או עזבו וטרם נותקו ממערכת המחשב המרכזי, ובדיקה ידנית של המקרים החריגים. הערך החד-ערכי במערכת המידע של אגף משאבי אנוש שונה מהערך החד-ערכי במערכת המחשב המרכזי. כמו כן, בשל הבדלים ברישום העובדים בשתי המערכות, יצרה החברה טבלת המרה ידנית, וזאת כדי לקשר בין מספר הזהות של העובד לשם המשתמש במערכות הבנק. טבלת ההמרה אמורה להתעדכן ידנית כפתרון המפצה על חוסר ההתאמה בנתונים.

- **סקירת הרשאות תקופתית בחברת הדואר -** פעמיים בשנה, בינואר ובאוגוסט, החברה מבצעת סקירת הרשאות ידנית של 17 מערכות ליבה. עם זאת, ביתר המערכות בחברת הדואר לא מתבצעת סקירת הרשאות, כנדרש בנוהל משתמשים והרשאות. כמו כן, לא מתבצע תהליך המציג את החריגות שנמצאו במהלך הבדיקה, אף שהדבר היה יכול לסייע בזיהוי של מערכות או אגפים אשר יש בהם באופן קבוע מספר חריגות רב ולתת להם מענה בהתאם לכך. כמו כן, לא מתבצע תהליך בקרה ממוחשב נוסף הבוחן את מידת התאמתן של ההרשאות לבעלי ההרשאה. למשל, ייתכן שעובד יחליף תפקיד עם עובד אחר במחלקה ולצורך תפקידו החדש נדרש לבצע שינוי בהרשאות המוקצות לו, אך המנהל העסקי המבצע את הסקר לא יהיה ער לשינוי הנדרש.

- **בדיקת הרשאות במערכת ג' בחברת הדואר -** בבדיקת צוות הביקורת נמצא כי נכון לינואר 2024, 85 מבעלי ההרשאות למערכת ג' (ששיעורם 3% מכלל בעלי ההרשאות במערכת זו) אינם מוגדרים במערכת משאבי אנוש כ"פעילים". כלומר, הרשאתם של עובדים שעזבו או פרשו מהחברה לא נותקה, ולחלופין מעמדם לא עודכן במערכת משאבי אנוש. עוד נמצא כי למרות ביצוע בקרות אוטומטיות מפצות על ידי החברה, חלו שגיאות בתהליך הבקרה הממוחשבת האוטומטית. ממצאי הביקורת העלו כי לא אותרו בבקרה האוטומטית 79 עובדים שלהם הרשאות פעילות ומנגד אינם "פעילים" במערכות משאבי אנוש.

- **הרשאות במערכת הניהול המרכזי של הרשת בחברת הדואר -** ממצאי הביקורת העלו כי נכון לדצמבר 2023, 780 (כ-13%) מבעלי ההרשאות הפעילות במערכת הניהול המרכזי של הרשת הם עובדים שאינם נכללים ברשימת העובדים הפעילים במערכת משאבי אנוש בחברה. 449 (כ-58%) מתוך 780 עובדים בעלי הרשאות שאינם מוגדרים כ"פעילים" לא התחברו למערכת הניהול המרכזי של הרשת מתחילת שנת 2024 ואילך. אין מידע על תאריך ההתחברות האחרונה של 196 (כ-25%) מבעלי ההרשאות, וידוע כי מועד ההתחברות האחרונה של 135 (כ-17%) מהעובדים היה בשנת 2024. ניתן להסיק כי עובדים שלא התחברו לאחר שנת 2023 וכן עובדים שאין מידע לגבי מועד התחברותם האחרונה הם עובדים שעזבו את החברה אך לא בוטלו הרשאותיהם. עובדים אשר התחברו לאחרונה

6 מחשב מרכזי המשמש להפעלת יישומים רבים בעת ובעונה אחת, תוך שימוש בעיבוד נתונים בהיקף רחב.

7 בשל עזיבה או פרישה.

בשנת 2024, שהם ככל הנראה עובדים פעילים בחברה, עדיין הופיעו במערכת כוח האדם כעובדים שאינם "פעילים". 70 מ-80 העובדים בעלי ההרשאות הפעילות שנכללו במדגם שדגם צוות הביקורת[8] כלל אינם עובדים בדואר. הרשאותיהם של שישה מהעובדים, שעזבו את חברת הדואר כבר בשנת 2020, עדיין לא בוטלו במועד המדגם, יותר משלוש שנים לאחר עזיבתם. כמו כן לא בוטלו ההרשאות של עובד אחר, שעזב את החברה כבר בשנת 2021, ושל שלושה עובדים שעזבו בשנת 2023. אי-ביטול הרשאות לעובדים שאינם "פעילים" עלול לגרום למצב שבו בלתי מורשים עושים שימוש בהרשאותיהם התקפות לצרכים זדוניים ולפגיעה בחברה.

בדיקת ההרשאות במחשב המרכזי בבנק הדואר - נמצא כי 35 (כ-2%) מתוך 1,794 ההרשאות הפעילות במחשב המרכזי של בנק הדואר שייכות לעובדים שאינם מוגדרים כפעילים במערכות כוח האדם. אומנם לרוב המשתמשים נדרשים תחילה להיכנס למערכת הניהול המרכזי של רשת הבנק כדי להתחבר למחשב המרכזי, אולם ממצאים אלה חמורים בשל חשיבות רמת אבטחת המידע הגבוהה בבנק. הותרת הרשאות פעילות למערכות הבנק לעובדים שאינם מועסקים בחברה עלולה לאפשר פגיעה באבטחת המידע.

בדיקת ההרשאות במערכת הניהול המרכזי של רשת בנק הדואר - נמצא כי 67 משתמשים בעלי הרשאות פעילות אינם מוגדרים כ"פעילים" במערכות משאבי אנוש או שלא ניתן לאתרם. לאחר בחינת כלל העובדים נמצא כי 58 מהם הם אנשי מערכות מידע שהם עובדים פעילים חיצוניים. בדיקת תשעת המשתמשים הנוספים העלתה כלהלן: הרשאותיהן של שלוש עובדות ששהו בחופשת לידה לא בוטלו אף שעל פי נוהל ניהול הרשאות עובדים יש לבטל הרשאות לעובדים הנעדרים מהעבודה למשך יותר מחודש ימים קלנדרי. עובד נוסף פרש מהבנק כבר ב-30.6.23 ולאחר מכן חזר לעבוד אך אינו מוגדר כעובד פעיל באגף משאבי אנוש. עובדת נוספת פרשה מהבנק אך עדיין יש לה הרשאות, ושלושה עובדים נוספים הם עובדים פעילים אך אינם מוגדרים ככאלה במערכות משאבי אנוש, אף ששמותיהם ומספר הזהות שלהם נכללים בטבלת ההמרה. כמו כן, נמצא כי שם המשתמש של עובד אחר שעזב עדיין משמש עובדים אחרים. עקב אי-ביטול הרשאותיהם של עובדים שאינם פעילים למערכות בנקאיות רגישות נפגעת אבטחת המידע של הבנק, ונשקף סיכון לחדירת גורמים לא מורשים למערכותיו.

תהליך איסוף המאזנים מסניפי הדואר - מדי יום נהגי החברה אוספים את האסמכתאות הפיזיות לפעולות הבנקאיות ביחידות הקצה לשקים (מאזנים[9]) ומעבירים אותם למטה בנק הדואר שבמרכז המיון במודיעין. נמצא כי החברה אינה עומדת ביעדים שקבעה לעצמה (85% מהמאזנים מגיעים ביום למוחרת) ורק 70% מהמאזנים מגיעים למטה הבנק בתוך יומיים. הבקרה והמעקב בנוגע להגעת המאזנים למטה בנק הדואר אינה מלאה, והמעקב היומי אינו מתבצע אחר מאזנים שאינם מיום העסקים הקודם, כך שלא ניתן לדעת אם מאזן כאמור הגיע לדואר אלא רק בבדיקה החודשית. כמו כן, לא מתבצע מעקב המשך לאחר בדיקה זו. עוד נמצא כי המאזנים הושארו במשך שעות ממושכות באולם המיון ללא השגחה

8 80 מסך 780 בעלי הרשאות פעילות במערכת הניהול המרכזי של הרשת שאינם נכללים ברשימת העובדים הפעילים במערכת משאבי אנוש בחברה.

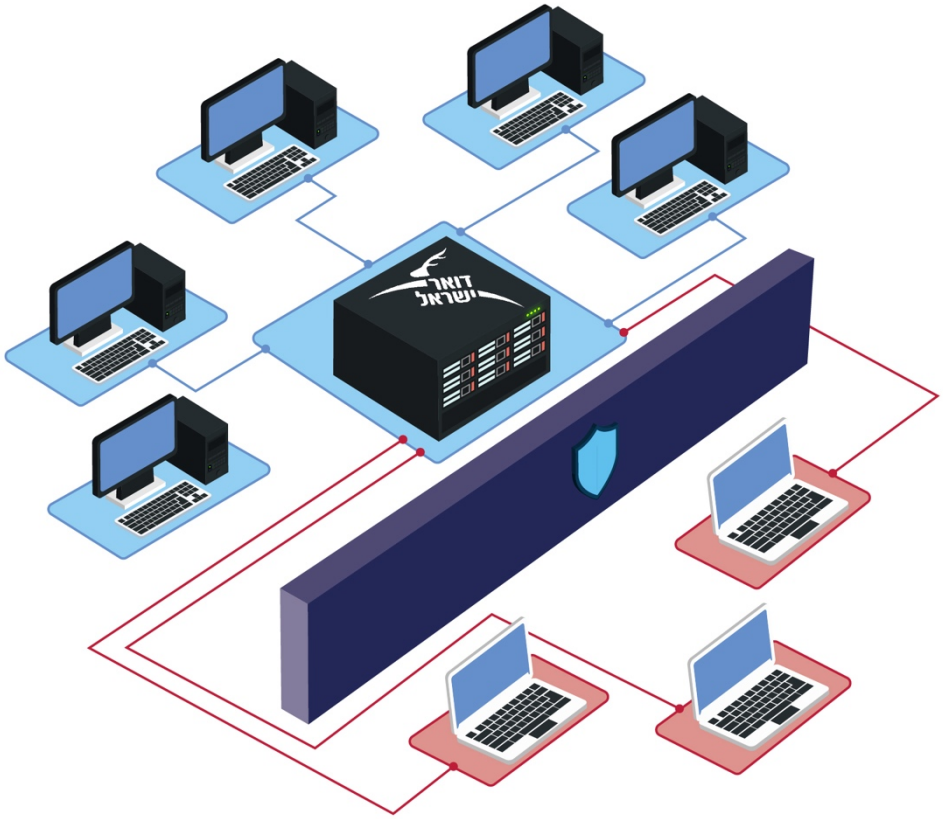
9 מאזנים אלו כוללים בין היתר, המחאות, שוברים, טפסים בנקאיים והמחאות למשמרת.

ותוך סיכון ממשי לגניבתם או לחשיפתם בפני גורמים שאינם מורשים לכך. תופעה זו נמשכה שנים.

עיקרי המלצות הביקורת

- על החברה לגבש נוהל להסדרת נושא תוכניות העבודה השנתיות והרב-שנתיות ולוודא את יישום הנוהל תוך הקפדה על בחינת חלופות, מעקב אחר יישום תוכנית העבודה וניהול תוכנית העבודה בצורה המאפשרת להנהלת אגף מערכות מידע ראייה כוללת בכל רגע נתון על המשימות המתבצעות, עלותן והיקפן.
- על החברה לפעול להשלמה של פרויקט החלפת הציוד המיושן ביחידות החברה בהקדם, וזאת כדי לצמצם סיכונים ולשפר את השירות הניתן ללקוחות.
- על החברה לפעול למימוש ההמלצה שבתוכנית האב משנת 2021 למניעת כפילויות ופעילויות מיותרות באמצעות תכלול, גיבוש והבניה של פעולות ותהליכי עבודה לפיתוח מסגרות משותפות ואחודות באמצעות טכנולוגיות דיגיטליות ומידע.
- על החברה לבצע בדיקת הרשאות שגרתית במערכת הניהול המרכזי של הרשת כדי למזער את הסיכון הכרוך במתן הרשאות לעובדים שאינם זכאים לכך וכדי שיתאפשר ניהול ההרשאות של מערכות רבות. כמו כן, על החברה לבחון את תהליך בדיקת ההרשאות במערכת ג' ובכלל המערכות הנבדקות כדי לאתר כשלים בתהליך איתור העובדים שאינם "פעילים", בין היתר במסגרת סקירת ההרשאות הידניות. נוסף על כך, על החברה לאתר את כלל העובדים שמוגדרים כמשתמשים לא פעילים ויש להם הרשאות במערכות השונות ולבחון לעומק את מנגנון הבקרה על הרשאות המשתמשים ולשפרו בהתאם לממצאים.
- על החברה לעבות את הבקרות הנערכות בבנק הדואר ולהשוות באופן שוטף את נתוני בעלי ההרשאות התקפות אל מול נתוני אגף משאבי אנוש. כמו כן, עליה לפתח תהליכים אוטומטיים לניתוק הרשאות ממערכות הבנק ולבצע בקרות על הרשאות אלה.

ממצאי הביקורת בבדיקת הרשאות במערכת הניהול המרכזי של הרשת בחברת הדואר



780

מבעלי ההרשאות הפעילות במערכת הניהול המרכזי של הרשת אינם נכללים ברשימת העובדים הפעילים בחברה.

סיכום

בחברת הדואר 55 מערכות מידע שחלקן נחלקות לתתי-מערכות, ובבנק הדואר יש 16 מערכות נוספות שחלקן נחלקות לתתי-מערכות. למערכות אלו יש יותר מ-20 ספקים שונים, והן מבוססות על טכנולוגיות שונות.

דוח זה מעלה ליקויים בתחומי מערכות המידע ואבטחת המידע בחברת הדואר ובבנק הדואר, ובהם ניהול לקוי של תהליך ביטול הרשאות לעובדים וליקויים בבקרה על תהליך זה; שימוש בציוד ממוחשב מיושן הפוגע הן בשירות ללקוחות החברה והבנק והן באבטחת המידע; היעדר תוכנית עבודה רב-שנתית לאגף מערכות מידע; היעדר מעקב אחר ביצוע תוכניות העבודה; ריבוי מערכות שמקשה את העברת המידע בין המערכות ועקב כך מעורר צורך בביצוע הליכים ידניים ובהשקעת משאבים בחברה כדי לפצות על כך.

על אגף מערכות המידע בחברת הדואר לקבוע תוכנית פעולה מוסדרת הכוללת פיתוח מערכות מידע בראייה עתידנית, שדרוג מערכות ישנות ומיטוב של המערכות הקיימות ושל האינטגרציה ביניהן, כל זאת תוך הקפדה על הגנת הסייבר וצמצום החשיפה לסיכונים שמקורם בהיבטים שונים של שימוש שאינו מורשה.

על החברה לפעול, במסגרת שיפור אבטחת המידע, ובייחוד - לנוכח אירוע סייבר שהתרחש בה באפריל 2023 - לשיפור הבקרה על ניהול ההרשאות בחברה. על החברה לבחון את הליקויים שהועלו בביקורת בנושא זה ולגבש דרכים לתיקונם המיידי.

דוח מבקר המדינה - סייבר ומערכות מידע |
חשוון התשפ"ד | נובמבר 2024

המוסד לביטוח לאומי

אבטחת מידע והגנת הסייבר במוסד לביטוח לאומי

אבטחת מידע והגנת הסייבר במוסד לביטוח לאומי

רקע

המוסד לביטוח לאומי (בט"ל) מחזיק במאגר גדול, המכיל מידע מארגונים וגופי ממשל רבים וגודלו טרה-בייט (TB) רבים. המאגר גדל בכ-10% בכל שנה. המאגר כולל מידע על כל תושבי מדינת ישראל מיום הלידה ועד יום הפטירה. המאגרים של בט"ל נדרשים לרמת אבטחה גבוהה לפי תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017[1].

ביולי 2023 החליטה ועדת היגוי עליונה להגנה על מערכות ממוחשבות במדינת ישראל[2] כי בט"ל עונה על התבחינים הנדרשים, וכי יש מקום להנחותו כגוף תשתית מדינה קריטית (גוף תמ"ק). לפיכך המליצה הוועדה על הוספת בט"ל לתוספת החמישית לחוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998, כדי שבט"ל יהיה מונחה לפי חוק זה על ידי מערך הסייבר הלאומי (מס"ל). נכון לאפריל 2024, מועד סיום הביקורת, טרם התקבל אישור להוספת בט"ל לתוספת החמישית לחוק להסדרת הביטחון. במסגרת הפיכתו לגוף תמ"ק החל בט"ל לבצע פעילות יזומה לשיפור רמת ההגנה שלו, בהתאם למתודולוגיה הייעודית של גופי תמ"ק.

נכון לפברואר 2024, מתבצעים בכל יום עשרות אלפי ניסיונות לתקיפת סייבר נגד בט"ל. אירוע סייבר בבט"ל עלול לגרום לפגיעה חמורה בפרטיות של מיליוני אזרחים ותושבים המקבלים שירות מבט"ל, וכן עלול לגרום לפגיעה בעבודת בט"ל ואף לשיתוק של העבודה, ובעקבות כך לפגיעה ביכולת לשלם קצבאות (זקנה, נכות, קיום, אבטלה תגמולי מילואים). להלן דוגמה לאירוע אבטחת מידע חמור בבט"ל כהגדרתו בתקנות: בפברואר 2022 דווח על אירוע גניבת זהות שבעקבותיו מידע אישי על 2,000 אזרחים היה חשוף ונגיש למי שאינו מורשה לכך.

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

2 החלטת הממשלה ב/84 משנת 2002 שבה נקבע כי יש להקים ועדת היגוי עליונה להגנה על מערכות ממוחשבות במדינת ישראל, שתפקידה לבחון אילו גופים יוגדרו "חיוניים", ולכן זקוקים להגנה קיברנטית. האחריות להגנה זו הוטלה על שב"כ. בשנת 2016, במסגרת תיקון לחוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998, עברה אחריות זו מהשב"כ למס"ל.

נתוני מפתח

10 שנים

לא עודכנה מדיניות הגנת הסייבר של בט"ל, אף שחלו שינויים משמעותיים מאז. 50% מהנהלים שלפי תקנות אבטחת מידע נדרש לכלול בנוהל אבטחת מידע של כל ארגון, אינם קיימים בבט"ל

עשרות אלפים

מספר ההתרעות להתקפות סייבר על בט"ל ביממה הדורשות תחקור על ידי אנליסט בודד שמאייש את מרכז שליטה ובקרה לטיפול באירועי סייבר (SOC) של בט"ל

יותר משנתיים

פרק הזמן שבו לא התכנסה ועדת היגוי סייבר בראשות מנכ"ל - מראשית שנת 2022 עד לינואר 2024

0

מבדקי חדירה התבצעו לגבי המערכת המרכזית של בט"ל

87%

מתקנות אבטחת מידע מקוימות בבט"ל באופן חלקי בלבד. לא מתבצעת כלל ביקורת תקופתית על עמידה בתקנות

גופים רבים

מקבלים מידע מבט"ל באמצעות מערכות שיתוף מידע שהתגלו בהן פערי אבטחת מידע

פעולות הביקורת

בחודשים יולי 2023 עד אפריל 2024 בדק משרד מבקר המדינה את נושא אבטחת המידע והגנת הסייבר בבט"ל ואת העמידה שלו בתקנות אבטחת מידע. בביקורת נבדקו בין היתר הנושאים האלו: המדיניות והנהלים בתחום הגנת הסייבר; ניהול הסיכונים; העברת מידע מבט"ל לגופים חיצוניים; הגנה לוגית; הגנה פיזית; המשכיות עסקית; התמודדות עם אירועי סייבר; ושרשרת האספקה. הביקורת נעשתה בבט"ל, במשרד ראש הממשלה - במערך הסייבר ובמשרד המשפטים - ברשות להגנת הפרטיות.

ועדת המשנה של הוועדה לענייני ביקורת המדינה של הכנסת החליטה שלא להניח על שולחן הכנסת ולא לפרסם חלקים מפרק זה לשם שמירה על ביטחון המדינה, בהתאם לסעיף 17(א) לחוק מבקר המדינה, התשי"ח - 1958 (נוסח משולב).

תמונת המצב העולה מן הביקורת

- **מדיניות אבטחת מידע והגנת הסייבר -** בט"ל לא עדכן את מדיניות אבטחת המידע והגנת הסייבר שלו במשך כעשר שנים, משנת 2014, זאת אף שמאז הסיכונים בתחום השתנו במידה ניכרת, ואף שהדבר מנוגד למדיניות בט"ל, ולפיה מדיניות אבטחת מידע תידון ותתוקף מדי שנה בשנה. בעת ביצוע הביקורת עודכן מסמך המדיניות לרמה של טיוטה ואושר במרץ 2024 בידי ממלא מקום מנכ"ל בט"ל, אולם טרם התקיים דיון בוועדת ההיגוי לאבטחת מידע בנוגע למדיניות כנדרש במסמך המדיניות. כמו כן במסמך המדיניות חסרה התייחסות מפורשת לנושאים שנדרשת להם התייחסות לפי תקנים מקובלים, כמו ניהול וסיווג של נכסים והמחויבות לבצע בקרות על עמידה בתקנות אבטחת מידע.

- **נוהלי אבטחת מידע -** בט"ל לא התייחס בנוהל אבטחת מידע של הארגון ל-6 (50%) מ-12 הנושאים שנקבע בתקנות אבטחת מידע כי נדרש להסדיר אותם במסגרת נוהל אבטחת מידע. לגבי ארבעה (33%) מ-12 הנושאים, הנהלים הקיימים בעניינם לא עודכנו עשר שנים; ולגבי שניים (17%) מ-12 הנושאים לא צוין המועד האחרון שבו עודכנו הנהלים בעניינם.

- **ועדת היגוי להגנת סייבר -** ועדת היגוי סייבר בראשות המנכ"ל לא התכנסה מתחילת שנת 2022 ועד ינואר 2024, ואת בניגוד למדיניות בט"ל המחייבת כינוס של הוועדה בכל חצי שנה. מכיוון שהוועדה לא התכנסה בפרק הזמן האמור, לא היה בפרק זמן זה בבט"ל גורם שיאשר את מדיניות הגנת הסייבר, יאשר את תוכניות העבודה השנתיות ויבצע מעקב אחר יישומן ויציג את רמת ההגנה בסייבר לראש הארגון, לרבות פערים, אירועים משמעותיים ואיומים. כמו כן, גם בדיון הראשון של ועדת ההיגוי בינואר 2024 לא הוצגה רמת ההגנה בסייבר לממלא מקום מנכ"ל בט"ל, לא אושרה טיוטת המדיניות, ולא הוצגו נושאים מרכזיים אחרים שהוגדרו בכתב המינוי של הוועדה.

- **ניהול סיכונים -** בט"ל אינו מנהל רשימת מצאי של כלל הנכסים והתהליכים העסקיים שלו ואינו מסווג אותם לפי רמת הקריטיות שלהם לארגון כנדרש בתקנות אבטחת מידע ובנורמות מקובלות בתחום הסייבר, ובהן הנורמות הכלולות בתורת ההגנה[3]. בט"ל בחר חלק מהמערכות החשובות והקריטיות מתוך כלל המערכות הקיימות בבט"ל, ומהן מופו כשליש מהמערכות שהוגדרו החשובות ביותר, ונקבע שמערכות אלה ייבחנו בסקר. קיום הליך של ניהול סיכונים שלא על בסיס מיפוי מלא של כלל נכסי הארגון מעלה חשש כי ניהול הסיכונים לא ישקף בצורה מיטבית את הסיכונים העיקריים שאליהם חשוף הארגון, וכי המשאבים והפעולות המופנים להתמודדות עם סיכונים אינם מוקצים בהלימה לרמת הסיכון הנשקפת לנכסי הארגון. כמן כן, בט"ל אינו מבצע סקרי סיכונים אחת ל-18 חודשים לגבי מאגרי המידע שלו, כנדרש מארגונים שיש להם מאגרי מידע שחלה עליהם רמת אבטחה גבוהה.

3 מערך הסייבר הלאומי, מדריך יישומי להגנת הסייבר של הארגון גירסה 2.0 (יוני 2021).

- **מבדקי חדירה -** בט"ל אינו מבצע מבדקי חדירה לגבי מאגרי המידע שברשותו, כמתחייב מתקנות אבטחת מידע וכן ממסמך המדיניות שלו. כך, רק כ-7% מהמבדקים שבוצעו היו על מערכות שמקושרות למערכת המרכזית, אשר בה נמצאים כל מאגרי המידע של בט"ל. כמו כן, בט"ל אינו עוקב אחר תיקון הליקויים שנמצאו במבדקים, ונמצאו ליקויים חוזרים וליקויים רוחביים ברמת חומרה גבוהה שלא תוקנו, דבר החושף את בט"ל לסיכון. זאת ועוד, בט"ל אינו מבצע מבדקי חדירה למערכת המרכזית וקיים חוסר במידע וידע אודות ביצוע מבדקים מסוג זה בבט"ל ובמס"ל.

- **הגנה לוגית -** נמצאו פערים בהגנה הלוגית בבט"ל במספר נושאים.

- **זיהוי אירועי סייבר וטיפול בהם -** נמצאו פערים ביכולת של בט"ל לזהות אירועי סייבר ולטפל בהם: אין בבט"ל צוותים ייעודיים לניהול משבר - צוות ניהול אירוע (IR) וצוות לביצוע חקירה פורנזית (DFIR) ; צוות הנהלה לניהול אירוע סייבר שהוקם בסוף ינואר 2024 לא התכנס, לא הוכשר ולא תורגל; נמצא פער בהפעלת ה- SOC; הצוות שמאייש את ה-SOC לא עבר הכשרה ייעודית לנושא; ה-SOC אינו נמצא באחריות חטיבת אבטחת מידע, אלא באחריות אגף תשתיות; יש חוסר הלימה בין הצורך בתחקור עשרות אלפי ההתרעות ביממה, ובין איוש ה-SOC באנליסט אחד בלבד. נוכח זאת קיים חשש כי לא מתאפשר לזהות את אירועי האמת בזמן סביר או בכלל.

- **המשכיות עסקית -** נמצאו פערים ביכולת ההמשכיות העסקית של בט"ל בנושאים שלהלן: טיוטת נוהל התאוששות עסקית שקיימת בבט"ל איננה כוללת נושאים הנדרשים כחלק מתוכנית המשכיות עסקית, ובהם מיפוי עדכני של התהליכים החיוניים והסיכונים הכרוכים בהם, הגדרת יעדי התאוששות מדידים והקצאת משאבים ותשומות נדרשים. כמו כן, טיוטת הנוהל כוללת סדרי עדיפות להתאוששות משנת 1991, אשר אושררו בשנת 2013 ואינם עדכניים. נוסף על כך, בט"ל לא ביצע תרגול של תוכנית התאוששות מאסון בשלוש השנים האחרונות; נמצאו פערים ביכולת לשחזר מידע מגיבויים.

- **ניהול הסיכונים מצד שרשרת האספקה -** לבט"ל אין נוהל בנושא שרשרת אספקה, ואין לו מיפוי של כלל ספקי התקשוב שלו והסיווג שלהם לפי רמת הסיכון הנשקף מהם. כמו כן, במכרזים של בט"ל אין נספח אבטחת מידע שמחייב עמידה של הספק בבקרות התואמות את הנדרש במתודולוגיית שרשרת האספקה. זאת ועוד, בט"ל אינו מבצע ביקורות על ספקי התקשוב שלו. נוכח זאת קיים סיכון לפגיעה בבט"ל באמצעות פגיעה באחד הספקים המהותיים שלו. במספר מקרים מצומצם שבהם ביצע בט"ל ביקורות התגלו ליקויים.

- **העברת מידע מבט"ל לגופים חיצוניים -** בט"ל מעביר לגופים חיצוניים רבים מידע באמצעות מערכות לשיתוף מידע שהתגלו בהן פערי אבטחת מידע. כמו כן, בט"ל אינו מבצע בקרה על התאמת המידע שמועבר לגופים ציבוריים למידע שאישרה הוועדה להעברת מידע למסור. זאת ועוד בט"ל אינו מקיים בקרות עיתיות על תפוגת תוקף הממשק להעברת המידע ואינו מפסיק את העברת המידע לאחר חמש שנים כנדרש לפי נהליו.

- **עמידה בדרישות החוק והתקנות -** נמצא כי אין בידי בט"ל תוכנית לבקרה שוטפת על העמידה של מאגרי המידע בדרישות תקנות אבטחת מידע, כנדרש בתקנה 3 לתקנות אלה. מאגר המידע של בט"ל, הנחשב למאגר גדול וכולל מידע רגיש בנפח של טרה-בייט (TB) רבים, מחייב קיום תוכנית סדורה כזו, כדי להבטיח רמת אבטחה נאותה. עוד נמצא כי רובן

המכריע של תקנות אבטחת מידע (13 מ-15 תקנות - 87%) מקוימות בבט"ל באופן חלקי בלבד.

צוות מבדקי חדירה פנימי - בט"ל מעסיק צוות בודקי חוסן מיומנים במשרה מלאה, אשר מבצע באופן שוטף מבדקי חדירה תשתיתיים ואפליקטיביים למערכות ויישומים. כאמור, לא מתבצעים מבדקים על המערכת המרכזית.

שרשרת האספקה - במכרזים החדשים בט"ל הוסיף בפרק אבטחת מידע נושאים כמו ביקורות אצל ספקים וחובת הדיווח שלהם על אירועים.

מלחמת חרבות ברזל - במהלך מלחמת חרבות ברזל נדרש בט"ל לבצע פעולות דחופות לטיפול בנפגעי פעולות האיבה, במשפחות החטופים, במשפחות המפונים ובמשרתי המילואים. פעולות אלו כללו בין היתר פיתוח שירותים חדשים לטיפול באוכלוסיות אלו; פיתוח ממשקים להעברת מידע לגופים אחרים; ומציאת פתרונות חדשים המאפשרים עבודה מהבית של עובדי בט"ל, כדי שהשירות לא יפגע.

אתר הגיבוי (DR) - משרד מבקר המדינה מציין לחיוב את בט"ל על העתקת אתר הגיבוי (DR) למקום החדש במרץ 2024, במהלך הביקורת.

עיקרי המלצות הביקורת

- על בט"ל לעדכן את מסמך מדיניות אבטחת המידע והגנת הסייבר שלו בנושאים שנדרשת להן התייחסות לפי תקנים מקובלים ולהציגו בוועדת ההיגוי לאבטחת מידע, וכן עליו לוודא כי המסמך יעודכן באופן עיתי ובהתאם לסיכונים המשתנים בתחום כפי שמתחייב במדיניות אבטחת המידע והגנת הסייבר של בט"ל.
- נוכח החשש כי נושאים עיקריים באבטחת המידע של בט"ל אינם מטופלים בהתאם לשינויים בסביבה הארגונית, לאיומי הסייבר החדשים ולסיכונים, על בט"ל לעדכן את נוהל אבטחת המידע שלו כך שיכלול את הנושאים שנדרשים לפי תקנות אבטחת מידע. אשר לנהלים הקיימים, יש לעדכן את הנושאים שלא עודכנו בשנתיים האחרונות.
- נוכח חילופי ממלא מקום המנכ"ל בבט"ל לאחר כינוס ועדת היגוי סייבר בראשונה ונוכח העובדה שבדיון הוועדה לא הוצגו נושאים משמעותיים כמו רמת ההגנה בסייבר של בט"ל, מומלץ כי בט"ל יכנס בהקדם את ועדת היגוי סייבר, כדי להציג לפניה את נושא רמת ההגנה בסייבר ונושאים מרכזיים אחרים שנכללו בכתב המינוי של הוועדה ולאשר את טיוטת המדיניות.
- על בט"ל לערוך מיפוי של כלל הנכסים והתהליכים העסקיים שלו ולסווג אותם לפי רמת הקריטיות שלהם לארגון וזאת בהתאם לנדרש בתקנות אבטחת מידע.

- מומלץ כי בט"ל, בהנחיית מס"ל, יבצע תהליך סדור של סקרי סיכוני אבטחת מידע בהתאם למתודולוגיות מקובלות, כמו תורת ההגנה, ויוודא כי בסקרי הסיכונים יובאו בחשבון סיכונים הנשקפים לגופי תמ"ק ברמה הלאומית. עוד מומלץ כי ממצאי הסקר והתוכנית לתיקון הליקויים שעלו בו יועברו למס"ל המשמש כמנחה מקצועי של בט"ל.

- מומלץ כי בט"ל ייעזר במומחי תוכן בנושא המערכת המרכזית לצורך ביצוע מבדקי חדירה למערכת המרכזית. היות שחלק מגופי התמ"ק מחזיקים גם הם במערכות דומות, מומלץ כי מס"ל יקים פורום לשיתוף ידע בין הגורמים הרלוונטיים, שבין היתר יבחן מענה מערכתי לאומי לביצוע מבדקים על מערכות אלו.

- מומלץ כי בט"ל יקים צוותים ייעודיים לניהול משבר: צוות ניהול אירוע (IR) וצוות לביצוע חקירה פורנזית (DFIR). עוד מומלץ כי בט"ל יפעל לכנס ולתרגל את צוות ההנהלה לניהול אירוע סייבר.

- מומלץ כי בט"ל, בשיתוף מערך הסייבר, ישפר את היכולות של ה-SOC לגלות ולזהות אירועי סייבר וכן יפעל לסגירת הפער בהפעלת ה-SOC. עוד מומלץ כי מערך ה-SOC יהיה כפוף לחטיבת אבטחת מידע.

- מומלץ כי בט"ל, בליווי ובסיוע של מס"ל, יבצע מיפוי מלא של כל הספקים שלו, כנדרש בהנחיית מס"ל בנושא. עוד מומלץ כי בט"ל יגבש תבנית של נספח אבטחת מידע במכרזים שכוללת את המחויבויות של הספק במסגרת ההתקשרות ואת הדרישות ממנו לעמידה בבקרות, בהתאם למתודולוגיית שרשרת האספקה של מערך הסייבר.

- על בט"ל לערוך סקרי סיכונים ומבדקי אבטחת מידע למערכות שיתוף המידע הפעילות. במידה ויתגלו במערכות אלו פערי אבטחת מידע, על בט"ל להטמיע בקרות מפצות.

- על בט"ל לבצע בהקדם ביקורת על מידת העמידה של המאגרים המשמעותיים שברשותו בתקנות אבטחת מידע וזאת כנדרש בתקנות. בנוסף עליו לבצע את הביקורת באופן עתי.

מידת עמידתו של בט"ל בתקנות אבטחת מידע

הנושא	ממצאי הביקורת
מסמך הגדרות המאגר	קיים חלקית
ממונה על אבטחת מידע	קיים חלקית
נוהל אבטחה	קיים חלקית
מיפוי מערכות המאגר וביצוע סקר סיכונים	קיים חלקית
אבטחה פיזית וסביבתית	קיים
אבטחת מידע לגבי ניהול כוח אדם	קיים חלקית
הגנה לוגית - נושא 1	קיים חלקית
הגנה לוגית - נושא 2	קיים חלקית
הגנה לוגית - נושא 3	קיים חלקית
תיעוד של אירועי אבטחה	קיים חלקית
התקנים ניידים	קיים חלקית
ניהול מאובטח ומעודכן של מערכות המאגר	קיים חלקית
אבטחת תקשורת	קיים חלקית
מיקור חוץ	קיים חלקית
ביקורת תקופתית	לא קיים

הוכן בידי משרד מבקר המדינה.

סיכום

בט"ל מחזיק במאגר גדול, בנפח של טרה-בייט (TB) רבים, הכולל מידע על כל תושבי מדינת ישראל מיום הלידה ועד יום הפטירה. מאגר זה נדרש לרמת אבטחה גבוהה בהתאם לחוק הגנת הפרטיות ולתקנות אבטחת מידע, וכן משום שהוא יעד מרכזי לניסיונות תקיפה (עשרות אלפי חשדות לאירועים ביממה), ופגיעה בו עלולה להיות קריטית בייחוד בתקופה זו של מלחמת חרבות ברזל, שבה ממלא בט"ל תפקיד חיוני בטיפול בנפגעים, במפונים ובאנשי המילואים.

ביוני 2023 הוגדר בט"ל כתשתית מדינה קריטית (גוף תמ"ק) והחל בתהליכי אסדרה של הגנת הסייבר בהתאם לתו"ל ייעודי לגופי תמ"ק, בהנחיית מערך הסייבר. במהלך מלחמת חרבות ברזל נדרש בט"ל לבצע פעולות דחופות לטיפול בנפגעי פעולות האיבה, במשפחות החטופים, במשפחות המפונים ובמשרתי המילואים. פעולות אלו כללו בין היתר פיתוח שירותים חדשים לטיפול באוכלוסיות אלו; פיתוח ממשקים להעברת מידע לגופים אחרים; ומציאת פתרונות חדשים המאפשרים עבודה מהבית של עובדי בט"ל, כדי שהשירות לא ייפגע.

ממצאיו של דוח זה משקפים פערים ניכרים בכל הנוגע לניהול אבטחת המידע בבט"ל ולהיערכותו לאיומי סייבר. פערים רבים עלו בנוגע למכלול תחומי הפעילות הרלוונטיים לאבטחת המידע וביניהם: פערים בגילוי אירועי סייבר ובטיפול בהם; ליקויים ברמת האבטחה הלוגית; תוכנית המשכיות עסקית שאינה עדכנית; ויכולת התאוששות נמוכה במקרה של אסון. הממצאים שהועלו בדוח זה, כמכלול, וכל ממצא בפני עצמו מהווים סיכון לפגיעה בסודיות, באמינות ובזמינות של המידע שבמאגרי בט"ל.

הדוח כולל ממצאים נוספים הנוגעים לקיום חלקי ביותר של תקנות אבטחת מידע ולחוסר יכולת של חטיבת אבטחת מידע בארגון למלא חלק מתפקידיה.

על ממלא מקום מנכ"ל בט"ל, הנהלת בט"ל וועדת היגוי סייבר, בשיתוף מס"ל, כמנחה מקצועי, לפעול בהקדם למיפוי סיכוני הסייבר המהותיים הניצבים בפני הארגון ולגבש תוכנית עבודה לטיפול בפערי אבטחת המידע, ובהם הפערים שצוינו בדוח זה.

דוח מבקר המדינה - סייבר ומערכות מידע |
חשוון התשפ"ד | נובמבר 2024

המוסד לביטוח לאומי

פרויקט תבל לשדרוג מערך המחשוב במוסד לביטוח לאומי - ביקורת מעקב

פרויקט תבל לשדרוג מערך המחשוב במוסד לביטוח לאומי - ביקורת מעקב

רקע

בשנת 2009 יזם המוסד לביטוח לאומי (הביטוח הלאומי) את פרויקט "תבל" לשדרוג מערך המחשוב ("תבל" או הפרויקט), אשר היעד המרכזי שלו הוא מימוש עקרון "המבוטח במרכז", המתמקד במיצוי זכויותיו. הפרויקט נועד לשדרג בהדרגה את מערכות הליבה ומערכות המטה המרכזיות בביטוח הלאומי, ובסך הכול 48[1] מערכות ותת-מערכות, ולהקים תשתית טכנולוגית מודרנית. על פי המתוכנן הפרויקט היה אמור להימשך 11 שנים (מתחילת שנת 2010 ועד סוף שנת 2020) ותקציבו הכולל היה אמור להסתכם בכ-477 מיליון ש"ח.

בשנת 2015 פרסם מבקר המדינה דוח העוסק בשלב א' של הפרויקט[2] (דוח המבקר מ-2015). בדוח האמור צוין בין היתר כי לנוכח החריגות מתקציב הפרויקט ומלוח הזמנים שלו מתחייבת נקיטת פעולה תכליתית לתיקון הליקויים, כדי להבטיח כי בשנים הבאות יימשך יישומו של הפרויקט על פי התוכניות והתכולות שאושרו. עוד צוין בדוח האמור כי היות שאחד היעדים העיקריים של הפרויקט הוא להעמיד במרכז את המבוטח ואת מיצוי זכויותיו, נודעת חשיבות רבה להשלמתו של הפרויקט בלא עיכובים נוספים. בשנת 2017, נקבע בדוח יועצים ששכר הביטוח הלאומי כי הדרך שנבחרה למימוש הפרויקט לא הייתה נכונה, ונוסף על כך יש כשל כולל בניהול התוכנית. ההמלצה העיקרית של היועצים הייתה שיש להמשיך ביישום תוכנית הפרויקט תוך גידורה לתכולה חלקית יחסית לתכולת התוכנית המקורית.

בשנת 2020 פרסם משרד מבקר המדינה דוח נוסף על פרויקט "תבל"[3] (הדוח הקודם או הביקורת הקודמת), ובו ביקורת על ניהול התכולות של הפרויקט, על תקציבו ועל תוכנית העבודה שלו, לרבות על תיקון הליקויים שמבקר המדינה התריע עליהם בדוח המבקר מ-2015. בדוח זה נקבע כי אף שהביטוח הלאומי יישם במסגרת הפרויקט כמה מערכות חשובות ומתקדמות והן תרמו לשדרוג תהליכי העבודה בביטוח הלאומי ולשיפור השירות למבוטח, מערכות אלו הן רק חלק קטן מהמערכות שתוכננו בשנת 2009, והדרך ליישום מלא של היעד העיקרי של הפרויקט - מימוש תפיסת "המבוטח במרכז" - עוד ארוכה. ההמלצה העיקרית בדוח הייתה שעל הביטוח הלאומי לבחון לעומקם את הליכי ההערכה והתכנון בפרויקט ולנהל מעקב הדוק אחר התקדמות העמידה באבני הדרך שלו בכל שלב ושלב כדי למנוע עיכובים נוספים ביישומו.

1 בדוח הקודם צוינו 31 מערכות ליבה. לנוכח גודלם והיקפם של המודולים של מערכת ועדות רפואיות (כגון מערכת ועדות נפגעי עבודה, מערכת ועדות נכות כללית), הם נספרים בדוח זה כמערכות נפרדות ולפיכך מדובר בסך הכול ב-38 מערכות ליבה. פרט למערכות הליבה, הפרויקט המקורי כלל גם מערכת ERP עם עשרה מודולים בתחומי המטה. סה"כ 48 מערכות ותת-מערכות.

2 ראו מבקר המדינה, **דוח שנתי 65ג** (2015), "פרויקט תבל לשדרוג מערך המחשוב במוסד לביטוח לאומי", עמ' 1289 - 1331.

3 ראו מבקר המדינה, **דוח שנתי 70ג** (2020), "פרויקט תבל לשדרוג מערך המחשוב במוסד לביטוח לאומי".

בשנת 2021 הוחלט לצמצם עוד את הפרויקט ולהתמקד רק בחלק מתחום הגמלאות - סוגי גמלאות אשר במסגרת אישורן יש לכנס ועדות רפואיות, וכן הוחלט להקפיא את הטיפול בשאר מערכות הליבה. בהמשך אותה שנה שכר הביטוח הלאומי יועץ נוסף לבחינת המשך דרכו של הפרויקט. היועץ ציין כי הפרויקט סובל מפיגור גדול בלוחות הזמנים ובפער גדול בעלויות למול המתוכנן; לצד זאת הוא ציין כי חל שיפור בניהול הפרויקט. היועץ המליץ להמשיך בפרויקט בדגש על חיזוק תהליכי הבקרה התקציבית.

נתוני מפתח

14 שנים

חלפו מתחילת הפרויקט שהחל בשנת 2010 ותוכנן להסתיים בשנת 2020. במועד סיום התוכנית הרב-שנתית הנוכחית (בשנת 2025) הפרויקט יהיה בפיגור של חמש שנים ואין צפי למועד השלמתו

1 מיליארד ש"ח

החריגה הצפויה בעלות הפרויקט עד מועד סיומה של התכנית הרב שנתית הנוכחית. חריגה זו צפויה לגדול במאות מיליוני ש"ח נוספים עד להשלמת הפרויקט

200%

הגידול הצפוי בעלות הפרויקט יחסית לתקציבו המקורי עד למועד סיומה של התכנית הרב שנתית הנוכחית. מתכנון של 477 מיליון ש"ח לצפי של 1.5 מיליארד ש"ח

50%

ממערכות הליבה (19 מערכות מתוך 38) הוצאו מתכולת הפרויקט ומימושן הוקפא, כגון המערכות המטפלות בגמלאות זקנה ושאירים, מילואים וילדים

51 שנים

גיל מערכת המידע המטפלת בגמלאות זקנה ושאירים. מערכת זו ומערכות נוספות שפותחו לפני עשרות שנים, הוצאו מתכולת הפרויקט

270,000

מבוטחים טופלו באמצעות מערכת "תבל" בשנת 2022, כמו כן הוגשו 140,000 תביעות והתקיימו 50,000 ועדות רפואיות באמצעות המערכת

רק 10 מערכות

מתוך 38 מערכות הליבה שפיתוחן תוכנן במקור להסתיים בשנת 2020 מומשו עד למועד הביקורת הנוכחית (26%)

116 מיליון ש"ח

התקציב השנתי הממוצע של פרויקט "תבל" בשנים 2019 - 2023

פעולות הביקורת

בחודשים יוני עד ספטמבר 2023 ערך משרד מבקר המדינה ביקורת מעקב ממוקדת על הממצאים העיקריים שעלו בביקורת הקודמת על פרויקט "תבל". ביקורת המעקב נעשתה במוסד לביטוח לאומי והתמקדה בתקציב הפרויקט, בלוחות הזמנים למימושו ובתכולותיו. כמו כן נבדקו תוכניות העבודה הרב-שנתיות והשנתיות והבקרה עליהן וכן הבקרה התקציבית על הפרויקט.

תמונת המצב העולה מן הביקורת

תיחום הפרויקט והתכולות שיושמו - בביקורת הקודמת עלה כי הביטוח הלאומי יישם במסגרת הפרויקט חלק קטן מהמערכות שתוכננו להיכלל בפרויקט בשנת 2009. בביקורת המעקב נמצא כי הליקוי **תוקן במידה מועטה**. הביטוח הלאומי החליט לגרוע מהפרויקט 19 (50%) מתוך 38 מערכות הליבה שתוכננו בתכולה המקורית ואלו לא יבוצעו (6 מערכות מתוכן נגרעו מאז הביקורת הקודמת). תשע מערכות נוספות שתוכננו (כ-24%) טרם מומשו. 7 מערכות מומשו באופן מלא: 3 מערכות חדשות ועוד 4 שפעלו באופן חלקי בביקורת הקודמת. בסך הכול במסגרת הפרויקט מומשו באופן מלא רק 10 (כ-26%) ממערכות הליבה. עוד נמצא כי לא בוצעו שישה מתוך עשרה מודולים במסגרת פרויקט ה-ERP. כמו כן, אין לביטוח הלאומי תוכנית להשלמת המערכות הנוספות המתוכננות במסגרת הפרויקט, מעבר לשנת 2025.

הביטוח הלאומי החליט כאמור לגרוע מפרויקט "תבל" ולא לשדרג כ-50% ממערכות הליבה המתוכננות, מרביתן בתחום הגמלאות, בלא שיש לו תוכנית חלופית למתן מענה טכנולוגי למערכות אלו. המערכות שהוחלט לגרוע מהפרויקט עסקו בין היתר בתחומים אלה: גמלת זקנה ושאירים, גמלת מילואים, גמלת אבטלה, גמלת ילדים וגמלת שאירים, מערכות שבאמצעותן משלם הביטוח הלאומי עשרות מיליארדי שקלים למעל מיליון מבוטחים מדי שנה. מדובר במערכות שפותחו לפני עשרות שנים (מערכת זקנה ושאירים פותחה בתחילת שנות השבעים של המאה הקודמת) על תשתיות וטכנולוגיות מיושנות, והיכולת הטכנולוגית וזמינות אנשי המקצוע להמשיך ולתחזקן הולכת ומצטמצמת. החלטה זו מובילה הלכה למעשה לשינוי ייעודו המקורי של הפרויקט ולפיו יש לחדש את מערך המידע של הביטוח הלאומי, להסיר חסמים טכנולוגיים ותהליכיים, לשפר את הניהול והבקרה של הביטוח הלאומי וכן את היכולת להתאים במהירות את מערכות המידע ואת תהליכי העבודה לשינויים בחוקים, באסדרה (רגולציה) ובמדיניות הביטוח הלאומי.

לוחות הזמנים של הפרויקט - במועד סיום הביקורת, 14 שנים לאחר תחילת ביצועו של הפרויקט, ועל אף צמצום תכולות הפרויקט לכמחצית מהתכנון המקורי, ניתן לקבוע כי הפיגור הגדול בלוחות הזמנים והצמצום המתמשך והנרחב בתכולותיו משקפים תהליך עקבי

ורב-שנתי של התרחקות מהתכנון המקורי של הפרויקט עד לכדי ויתור על נדבכים שלמים בו. מגמה זו שנמשכת כבר כמה שנים לא הובילה לעמידה בלוחות הזמנים ביישום התכולות של הפרויקט לאחר צמצומו. נכון למועד ביצוע ביקורת זו השלמת התוכנית הרב-שנתית המאושרת למימוש עד לשנת 2025 (תוכנית הכוללת 15 מתוך 38 [40%] מערכות הליבה שתוכננו מלכתחילה) תהיה בחריגה של 5 שנים (כ-45%) מלוח הזמנים המקורי. נוסף על כך אין לביטוח הלאומי תוכנית להשלמת יתרת התכולה המצומצמת שאושרה, ולפיכך החריגה מלוח הזמנים צפויה לגדול עוד יותר.

תקציב הפרויקט - בביקורת הקודמת עלה כי על אף היישום החלקי של תכולות הפרויקט יחסית לתכנון המקורי, שיעור ביצועו של התקציב עד יולי 2019 היה גדול בכ-58% מהתקציב המקורי שאושר לפרויקט. בביקורת המעקב נמצא כי **הליקוי לא תוקן,** ואף שהתכולות המקוריות של הפרויקט צומצמו במידה ניכרת (בכמחצית), עד למועד ביקורת המעקב הוצאו כ-1.2 מיליארד ש"ח המהווים כ-260% מהתקציב המקורי שאושר לתכנית בסך 477 מיליון ש"ח. ההערכה היא שעד לסיום מימושה של התוכנית הרב-שנתית הנוכחית בשנת 2025, עלויות הפרויקט יגדלו ביותר מ-200% מהתקציב המקורי, חריגה של יותר ממיליארד ש"ח. יודגש כי לביטוח הלאומי אין הערכה לגבי העלות הצפויה של התוכנית הרב-שנתית הבאה, ולפיכך אין לביטוח הלאומי הערכה בנוגע לעלותו הכוללת הצפויה של הפרויקט במועד סיומו.

הכללת עלות העסקתם של עובדים בתקן של הביטוח הלאומי בתקציב הפרויקט - בביקורת הקודמת עלה כי נתוני תקציב הפרויקט אינם כוללים את עלות העסקתם של עובדים בתקן של הביטוח הלאומי המשולבים בפרויקט והומלץ כי עלות העסקתם תיכלל בתקציב הפרויקט. בביקורת המעקב נמצא כי **הליקוי לא תוקן**, וכי אף שהנהלת הביטוח הלאומי מסרה שהיא תפעל ליישום ההמלצה, עלויות כוח האדם של עובדי התקן לא שויכו לתקציב הפרויקט. עלויות אלו מוערכות בכ-5 מיליון ש"ח לשנה, כלומר כ-4% מתקציב הפרויקט השנתי.

תכנון הפרויקט לעומת ביצועו והבקרה התקציבית עליו - בביקורת הקודמת עלה כי צוות הפיקוח התקציבי של הביטוח הלאומי התקשה לבצע בקרה מלאה על תקציב הפרויקט לעומת התכולות המתוכננות, בשל היעדר נתוני תכנון מפורטים, מלאים ומעודכנים. בביקורת המעקב נמצא כי **הליקוי** בהליכי הבקרה התקציבית **תוקן במידה מועטה.** בביקורת זו עלה כי בתהליך בקרת סטטוס המשימות הביטוח הלאומי מעדכן בדיעבד את השעות המתוכננות לביצוע של כל משימה שהסתיימה, בהתאם לשעות הביצוע בפועל. עדכון בדיעבד זה גורם למעשה למחיקת תקציב השעות המתוכננות לביצוע הפרויקט, שבמסגרתו מנוהלות מאות משימות. כפועל יוצא מפרקטיקה זו, בתום תהליך עדכון נתוני הביצוע של המשימה, נתוני התכנון של הקצאת המשאבים בפרויקט (מספר שעות הפיתוח) מוצגים כזהים לנתוני הביצוע בפועל.

הפרקטיקה של מחיקת נתוני התכנון משקפת ליקוי ממשי שיש לו השפעות משמעותיות ביותר על כל תחום הפיקוח והבקרה על התנהלות הפרויקט. בהיעדר בקרה שוטפת על פערים בין התכנון לבין הביצוע בפועל, לא ניתן לעמוד על בעיות באופן הקצאת המשאבים בפרויקט (מאות אלפי שעות פיתוח בהיקף כספי של עשרות מיליוני ש"ח בשנה). כמו כן, מאחר שדוח הפיקוח התקציבי שמוצג לחשב אחת לרבעון מתבסס על נתוני התכנון מהמערכת לניהול הפרויקטים, שכאמור מתעדכנים בדיעבד בהתאם לביצוע בפועל, הרי

שדוח זה אינו משקף את התכנון המקורי, ולא ניתן להסתמך עליו לצורך בקרה על הביצוע ולצורך קבלת החלטות. בהיעדר דיווח אמין על נתוני התכנון, לא ניתן לבצע בקרה תקציבית ותהליכית אפקטיבית, וההחלטות המתקבלות על בסיס דיווחים אלו עלולות להיות שגויות.

ביצוע תחקיר בסיום כל גרסה - נמצא שלאחר ההשלמה של כל גרסה או סבב פיתוח לא מבוצעים תחקירים ותהליכי הפקת לקחים מעמיקים כדבר שבשגרה. הביטוח הלאומי מסתפק בביצוע תחקירים נקודתיים בעניינם של אירועים ספציפיים, שאינם מספקים את המענה על הצורך בקיום תהליך הפקת לקחים שבמסגרתו ייבחן מחזור החיים של הגרסה בכללותה, החל בשלב איסוף הדרישות, עבור דרך תהליכי האפיון והפיתוח, ניהול השינויים והבדיקות וכלה בשלב העלייה לאוויר. הלקחים נדרשים הן לצורכי שינוי ושיפור והן לצורכי שימור, גם בעת שגרסה עולה באופן מוצלח לטובת שכפול הצלחות בעתיד, ואי-יישומם גורם לפגיעה ביכולת הביטוח הלאומי לשפר את תהליכי הפיתוח באופן סדור ומתמשך.

מנגנוני המשילות בפרויקט - משרד מבקר המדינה מציין לחיוב את פעולות הביטוח הלאומי לקיום עבודה שוטפת של ועדת ההיגוי וועדת הכספים וכן את הפגישות העיתיות בראשות החשב וסמנכ"ל תקשוב, ובכלל זאת את העובדה שהתוכנית מוסכמת על כלל הגורמים המעורבים בביצועה.

עיקרי המלצות הביקורת

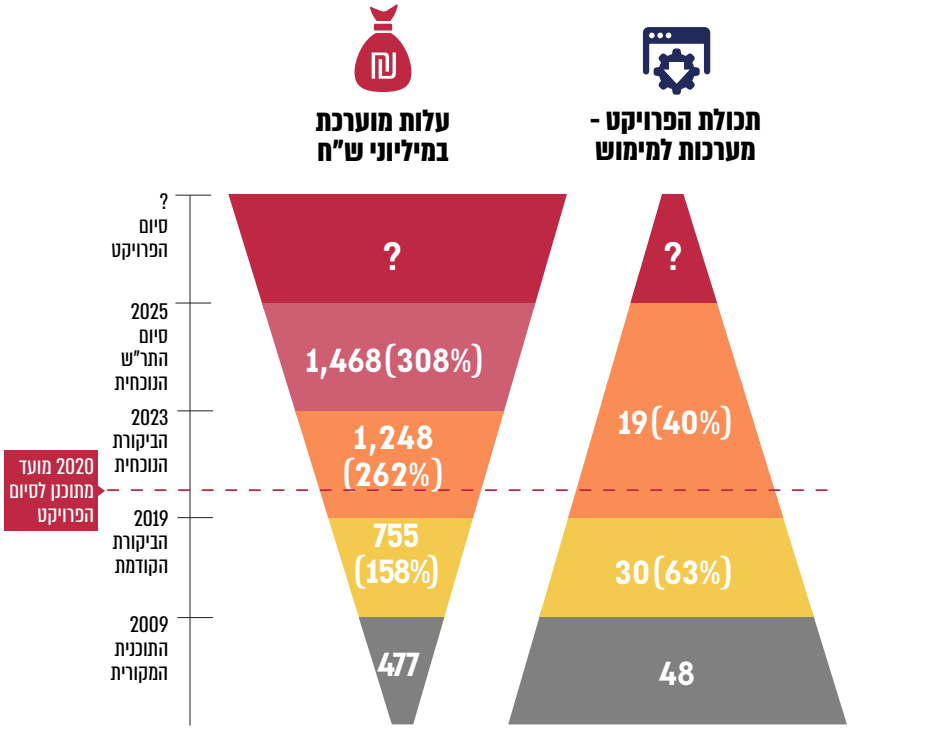
על הביטוח הלאומי להבנות תוכנית סדורה אשר תכלול לוח זמנים סופי להשלמת הפרויקט על כל רכיביו שאושרו על ידו. כמו כן, עליו לקבוע מנגנוני בקרה עיתיים כדי לוודא שהתוכנית שתיקבע תמומש הלכה למעשה. כל זאת על מנת להשיג את היעד העיקרי של הפרויקט – העמדת המבוטח ומיצוי זכויותיו במרכז.

על הביטוח הלאומי לבחון את עתיד המערכות שהוצאו מתכולת הפרויקט, ובכלל זה את איכות המענה הקיים ואת הישימות הטכנולוגית להמשך פעולתן בתצורה הטכנולוגית הקיימת לאורך זמן ובהתאם לגבש תוכנית רב-שנתית לשם שדרוגן והשגת היעד המרכזי של מימוש עקרון המבוטח במרכז, המתמקד במיצוי זכויות, זאת במקביל להמשך פיתוח המערכות הקיימות בתכולת פרויקט "תבל".

נוכח החריגה המשמעותית והמתמשכת מתקציב הפרויקט, על הביטוח הלאומי לבצע תחקיר מעמיק בנושא, לזהות ולנתח את הגורמים לחריגה זו ולקבוע באילו דרכי פעולה ניתן למנוע חריגות נוספות בפרויקט זה ובפרויקטי מחשוב אחרים שמנהל הביטוח הלאומי. על בסיס תחקיר זה, על הביטוח הלאומי לקבוע תקציב סופי להשלמת הפרויקט על כל תכולותיו וגורם שיהיה אחראי לעמידה בתקציב זה.

- על הביטוח הלאומי לכלול בתקציב הפרויקט את כלל הוצאות הפרויקט ובכללן את עלויות העסקתם של עובדי התקן.
- על הביטוח הלאומי ליישם תהליכי בקרה כמקובל, שבמסגרתם ייבחן התכנון המקורי לעומת הביצוע בפועל, ובכלל זה ינותחו החריגות, הן הערכות היתר והן הערכות החסר, כך שניתן יהיה ללמוד ולהפיק לקחים מבוססים ואמינים בנוגע לעלויות בפועל וכן בנוגע ליעילות עבודתם של צוותי האפיון, הפיתוח והבדיקות.
- על הנהלת הפרויקט לאמץ תהליך מובנה ושיטתי של הפקת לקחים בסיום כל גרסה.

הצמצום בתכולות פרויקט "תבל" למול הגידול בעלויותיו



*בסוגריים: שיעור מהתוכנית המקורית

סיכום

פרויקט "תבל" הוא פרויקט הדגל הדיגיטלי של המוסד לביטוח לאומי שהוחל בביצועו לפני למעלה מעשור כדי להסיר חסמים טכנולוגיים ותהליכיים ולממש את חזון הביטוח הלאומי להנגיש את מכלול השירותים של הביטוח הלאומי לציבור ולאפשר את שקיפות הנתונים. זאת במסגרת תפיסת הביטוח הלאומי לשים את המבוטח במרכז ולמצות את זכויותיו. נכון למועד ביקורת המעקב הביטוח הלאומי השקיע כ-1.2 מיליארד ש"ח בפרויקט והשלים עשר (רבע) מתוך 38 מערכות הליבה שתוכננו להיכלל בפרויקט.

משרד מבקר המדינה פרסם שני דוחות ביקורת בנושא יישום הפרויקט: האחד בשנת 2015 והשני בשנת 2020. דוח מעקב זה נועד לבחון את אופן תיקון הליקויים העיקריים שעלו בביקורת הקודמת.

בביקורת המעקב עלה כי מרבית הליקויים הליבתיים שעלו בדוח הקודם לא תוקנו או תוקנו במידה מועטה. כך עלה כי החריגה בלוחות הזמנים נמשכת, וכי אין לביטוח הלאומי צפי של מועד השלמת הפרויקט. כמו כן, במקביל לכך שהביטוח הלאומי צמצם את תכולות הפרויקט עד לכדי מחציתו, במועד הביקורת עלות הפרויקט הצפויה הנוכחית עומדת על כ-1.5 מיליארד ש"ח, חריגה המסתכמת בכמיליארד ש"ח מהתקציב המקורי שעמד על כ-477 מיליון ש"ח (חריגה של כ-200%), ועד להשלמת הפרויקט חריגה זו צפויה לגדול במאות מיליוני ש"ח נוספים. חריגות מתמשכות אלו בלוחות הזמנים ובעלויות הפרויקט פוגעות ביכולת לספק שירות מיטבי לציבור המבוטחים. הדוח אף מצביע על פרקטיקה של עדכון בדיעבד של נתוני התכנון, אשר פוגעת פגיעה יסודית ביכולת לקיים הליכי פיקוח ובקרה נאותים על תקציבי הפרויקט ועל בחינת המשאבים שהוקצו בפועל למול אלו שתוכננו ואושרו מלכתחילה. אשר למעורבות הגורמים הרלוונטיים בפרויקט, נמצא כי הביטוח הלאומי תיקן את הליקוי שעלה בדוח הקודם ובכלל זה החל לכנס ישיבות של ועדות היגוי וכן פגישות בקרה עיתיות של נציגי הנהלת הביטוח הלאומי.

אף שעד מועד סיום הביקורת הושקעו בפרויקט "תבל" כספי ציבור בסך של יותר ממיליארד ש"ח (למעלה מפי שניים מהתכנון הראשוני והכולל של הפרויקט), המטרה של שיפור השירות לציבור וסיוע לציבור במיצוי זכויותיו מושגת באופן חלקי בין היתר עקב צמצום בתכולות הפרויקט.

החריגות המהותיות בפרויקט מחייבות את הנהלת הביטוח הלאומי להפגין מעורבות ניכרת בניטור הגורמים שהביאו לחריגות אלו, להבנות מנגנונים לצמצומן ולקבוע באופן סופי ומחייב את מועד השלמת הפרויקט ואת תקציבו. הנהלת הביטוח הלאומי נושאת באחריות לוודא כי כספי הציבור שהיא משקיעה בפרויקט ינוצלו ביעילות, ולפיכך מוצע כי הביטוח הלאומי יחיל את התובנות שיופקו מתיקון הליקויים העולים מדוח זה גם על כלל הפרויקטים שבניהולו. בד בבד נדרשת הנהלת הביטוח הלאומי לבחון, נוכח קצב היישום של פיתוח המערכות, כפי שהתקדם ב-14 השנים האחרונות, את הצפי להשגת שיפור המענה התקשובי בכלל המערכים של הביטוח הלאומי, ובמיוחד באלו שפיתוחם הוצא מתיחום הפרויקט, ולקיים דיון מעמיק ואסטרטגי בנושא לאור תוצאות בחינה זו.

מידת תיקון עיקרי הליקויים שעלו בדוח הקודם

פרק הביקורת	הגוף המבוקר	הליקוי בדוח הביקורת הקודם	מידת תיקון הליקוי כפי שעלה בביקורת המעקב			
			לא תוקן	תוקן במידה מועטה	תוקן במידה רבה	תוקן באופן מלא
ניהול תוכנית העבודה השנתית של הפרויקט	הביטוח הלאומי	במחצית הראשונה של שנת 2019 התקדם הביטוח הלאומי ביישום הפרויקט בלי שהושגה הסכמה בין הגורמים המעורבים בו בנוגע לקיומה של תוכנית עבודה שנתית מפורטת.				←
תכולת הפרויקט	הביטוח הלאומי	רק חמש מ-38 המערכות העיקריות בתחום הליבה שנכללו בתכולה המקורית של הפרויקט משנת 2009 יושמו עד לאוגוסט 2019, ואף זאת באופן חלקי יחסית לתכנון המקורי. מתוך 10 מודולים בתחום המטה (מערכת ERP) יושמו רק שניים באופן מלא ואחד באופן חלקי.		←		
תקציב הפרויקט	הביטוח הלאומי	אף שהביטוח הלאומי הקים בשנת 2018 צוות לפיקוח תקציבי והוא התכנס באופן שוטף, התקשה הצוות לבצע בקרה מלאה על תקציב הפרויקט בשנת 2019 לעומת התכולות המתוכננות, בשל היעדר נתוני תכנון מפורטים, מלאים ומעודכנים.		←		
תקציב הפרויקט	הביטוח הלאומי	על אף היישום החלקי של תכולות הפרויקט יחסית לתכנון המקורי, ביצוע התקציב עד יולי 2019 היה גדול בכ-58% מהתקציב המקורי שאושר לפרויקט בשנת 2009 (כ-755 מיליון ש"ח לעומת התקציב המקורי שהיה 477 מיליון ש"ח).	←			

פרק הביקורת	הגוף המבוקר	הליקוי בדוח הביקורת הקודם	מידת תיקון הליקוי כפי שעלה בביקורת המעקב			
			לא תוקן	תוקן במידה מועטה	תוקן במידה רבה	תוקן באופן מלא
תקציב הפרויקט	הביטוח הלאומי	נתוני הביצוע של תקציב הפרויקט אינם כוללים את כל העלויות הישירות המשויכות לפרויקט, כגון עלות שכרם של 15 עובדי מינהל תקשוב ומערכות מידע המועסקים בפרויקט.	←			

דוח מבקר המדינה - סייבר ומערכות מידע |
חשוון התשפ"ד | נובמבר 2024

תעשיות ביטחוניות ממשלתיות

הגנה בתחום הסייבר: היבטי אסדרה והגנה על המידע ומערכות המחשוב ברפאל מערכות לחימה מתקדמות בע"מ

הגנה בתחום הסייבר: היבטי אסדרה והגנה על המידע ומערכות המחשוב ברפאל מערכות לחימה מתקדמות בע"מ

רקע

בהחלטת הממשלה מאוגוסט 2011[1] נקבע כי מרחב הסייבר האזרחי הישראלי כולל את כלל הגורמים הממלכתיים והפרטיים במדינת ישראל, למעט הגופים המיוחדים[2]. דהיינו, מרחב הסייבר הישראלי כולל את המרחב האזרחי, הממשלתי והביטחוני. הפעילות הגוברת במרחב הרשתי מאפשרת חדשנות טכנולוגית ופיתוחים לאדם ולסביבתו. ואולם לצד היתרונות שמאפשרות מערכות ממוחשבות במרחב הרשתי, הן יצרו גם איום חדש ההולך ומתעצם: איום הסייבר. אירוע סייבר הוא התרחשות אשר מעידה על פגיעה אפשרית בפעילותה התקינה של מערכת מחשוב. רפאל מערכות לחימה מתקדמות בע"מ (רפאל) היא מרכיב משמעותי בבניית עוצמתה הצבאית וחוסנה של המדינה. החברה כפופה בין היתר להוראות חוק החברות הממשלתיות, התשל"ה-1975, והחוק להסדרת הבטחון בגופים ציבוריים, התשנ"ח-1998 (החוק להסדרת הביטחון). הממונה על הביטחון במערכת הביטחון (מלמ"ב) מנחה את מפעלי מערכת הביטחון ומפעלים המייצרים מוצרים עבור מערכת הביטחון[3]. רשות החברות הממשלתיות מפיצה חוזרים לחברות הממשלתיות ולחברות בנות ממשלתיות בנושאים שונים בהתאם לסמכותה בחוק החברות הממשלתיות, התשל"ה-1975, ובכלל זה לגבי ניהול הסיכונים התאגידי.

בשנת 2022 דווחו למערך הסייבר הלאומי (מס"ל) על ידי כלל הגורמים במדינה 9,108 אירועי סייבר. כ-31% מהם נבעו ממתקפות דיוג[4].

1 החלטת הממשלה 3611 (7.8.11).

2 בהחלטת הממשלה 3611 (7.8.11) הוגדרו גופים מיוחדים כדלקמן: צה"ל, משטרת ישראל, שירות הביטחון הכללי (שב"כ), המוסד למודיעין ולתפקידים מיוחדים (המוסד) ומערכת הביטחון באמצעות הממונה על הביטחון במערכת הביטחון (מלמ"ב); וכמו כן הוגדרה מערכת הביטחון כדלקמן: הגופים המונחים על ידי מלמ"ב מכוח החוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1988, וכן ספקים ומפעלים המפתחים או המייצרים ציוד ביטחוני עבורם.

3 מערכת הביטחון - צה"ל ומשרד הביטחון (משהב"ט), לרבות יחידות הסמך שלו.

4 phishing - מתקפת סייבר שבה התוקף מתחזה לגורם אמין כדי להונות אנשים ולגרום להם לחשוף מידע רגיש.

נתוני מפתח

10%

בשנת 2022: התקציב של מחלקת אבטחת טכנולוגיות והגנה בסייבר ברפאל מתוך התקציב בנושא מחשוב של מינהל טכנולוגיות מידע ותהליכים ברפאל

12 שנים

לא יישמו מס"ל ומלמ"ב את החלטת הממשלה בנושא קידום היכולת הלאומית במרחב הקיברנטי, בכל הנוגע לקביעת הסדרים מיוחדים לקידום ההגנה במרחב הסייבר

31%

שיעור אירועי הסייבר מסוג דיוג שדווחו למערך הסייבר הלאומי (מס"ל) בשנת 2022 מתוך כלל אירועי הסייבר

פעולות הביקורת

בתקופה נובמבר 2022 עד יולי 2023 ביצע משרד מבקר המדינה ביקורת בנושא ההגנה בסייבר בכמה היבטים הנוגעים לאסדרה ולהגנה על מידע ומערכות המחשוב ברפאל. בביקורת נבדקו הנושאים האלה: הסדרת יחסי העבודה בין מס"ל למלמ"ב; סמכויות ההנחיה והפיקוח של מלמ"ב; תפיסת ההגנה בסייבר במלמ"ב; מדיניות אבטחת המידע ברפאל; ניהול הסיכונים הארגוני ברפאל; תוכניות העבודה ותקציב ההגנה בסייבר של רפאל; ההגנה על רשת מחשוב מסוימת ומערכות מידע מסוימות ברפאל ובקרות על אבטחת המידע המיושמות בהן; ומיגון תשתיות מסוימות ברפאל. הביקורת נערכה במלמ"ב וברפאל. בדיקות השלמה נערכו בתעשייה האווירית לישראל בע"מ (התע"א), בחברת החשמל לישראל בע"מ ובמס"ל.

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 ועל יחסי מסחר בין-לאומיים של המדינה, בהתאם לסעיף 17 לחוק מבקר המדינה, התשי"ח-1958 [נוסח משולב].

תמונת המצב העולה מן הביקורת

- **הסדרת יחסי העבודה בין מס"ל למלמ"ב -** אף שעברו כ-12 שנים ממועד החלטת הממשלה מאוגוסט 2011 בעניין קידום היכולת הלאומית במרחב הקיברנטי, מס"ל ומלמ"ב לא קבעו הסדרים מיוחדים הנוגעים לקידום ההגנה על המרחב הקיברנטי ולקידום המחקר והפיתוח בתחום המרחב הקיברנטי כנדרש בהחלטת הממשלה.

- **סמכויות ההנחיה והפיקוח של מלמ"ב -** בחוק להסדרת הביטחון משנת 1998 לא הוקנו למלמ"ב סמכויות ברורות בכל הנוגע לביצוע פעילות טכנולוגית אופרטיבית ולא הוקנתה למלמ"ב סמכות הנחיה מקצועית לגבי רשתות מסוימות.

- **תפיסת ההגנה בסייבר במלמ"ב -** תורת ההגנה בסייבר שהכינה חטיבת תורה והגנה (תוה"ג) ביחידה הטכנולוגית במלמ"ב אינה כוללת תקן למרכז ניטור של ארגון, על אף היותו של מרכז ניטור כזה אחד ממרכיבי ההגנה החשובים ביותר של ארגון. כמו כן חטיבת תוה"ג לא פרסמה לגופים המונחים הנחיה לגבי ההיערכות הנדרשת לניהול אירוע סייבר ולגבי ניהול האירוע עצמו, הנוגעת לנושאים, כגון תהליכי ניטור, זיהוי אירוע סייבר, תגובה עליו, התאוששות ממנו, תחקורו, הפקת לקחים ממנו, תרגול אירועי סייבר, הגורמים הפנימיים המשתתפים בניהול אירוע סייבר והממשקים ביניהם, והפעילויות הנדרשות של הגוף המונחה מול גורמים חיצוניים.

- **ניהול הסיכונים הארגוני ברפאל -** במאי 2023, בעת הביקורת, כשלוש שנים וחצי לאחר פרסום חוזר רשות החברות הממשלתיות בנושא ניהול סיכונים תאגידי מינואר 2020, אישרה הוועדה הארגונית לניהול סיכונים ברפאל מסמך אסטרטגיית סיכון כוללת לחברה ומדיניות לניהול סיכונים. ואולם הנהלת רפאל לא העלתה לאישור הדירקטוריון את האסטרטגיה והמדיניות האמורות, והדירקטוריון לא אישר אותן. נכון ליולי 2023 מדיניות ניהול הסיכונים לא כללה התייחסות למנגנוני דיווח לגורמים חיצוניים לרפאל. כמו כן רפאל לא דיווחה לרשות החברות הממשלתיות כנדרש ממנה. כל זאת שלא בהתאם לאמור בחוזר רשות החברות הממשלתיות לגבי ניהול סיכונים תאגידי מינואר 2020.

- **מיגון פיזי של תשתיות מסוימות -** עלו פערים בתחום זה.

- **ביטוח מפני אירועי סייבר -** ביולי 2023, בעת הביקורת, לחברת החשמל לישראל בע"מ היו שתי פוליסות ביטוח המכסות נזקים לרכוש ותביעות צד ג' בגין אירועי סייבר, ואילו לתעשייה האווירית לישראל בע"מ (התע"א) ולרפאל[5] לא היו פוליסות ביטוח כאמור. רפאל לא רכשה ביטוח מפני אירועי סייבר בעיקר מהסיבות שלהלן: רמת ההגנה על הסייבר ברפאל גבוהה; רכישת הביטוח אינה יעילה כלכלית; לא יהיה ניתן לתבוע מחברת הביטוח פיצוי בגין פגיעה בתפוקה או במחזור המכירות; לא ניתן לחשוף מידע מסווג לחברת הביטוח בעקבות נזק בגין אירוע סייבר, ומגבלה זו מקשה לממש את הביטוח בקרות אירוע; וניתן

5 למעט ציוד תקשוב ומערכות ממוחשבות ברפאל המבוטחות בגין אירוע סייבר שמקורו בטעות או במחדל.

לרכוש ביטוח המכסה נזק של עד עשרה מיליוני דולרים בלבד, סכום שאינו מהותי לפעילותה של רפאל.

- **פערי דיווח ברפאל -** רפאל לא דיווחה לדירקטוריון בישיבותיו על כמה אירועי סייבר כנדרש.
- **תחקור אירועי סייבר -** הנהלת רפאל לא תחקרה את ניהול אירועי הסייבר שהתרחשו בשנים 2020 - 2022 בהיבטים מסוימים הנוגעים לתפקוד הנדרש של רפאל.
- **תוכנית מפורטת לניהול אירועי אבטחת מידע -** הוראת מטכ"ם מפברואר 2023 אינה מפרטת את תהליך ההתאוששות מאירוע סייבר מסוים או מפנה לתוכנית מסוימת ואינה כוללת הפניות למסמכים מסוימים.
- **הפקת לקחים מאירועי סייבר מסוימים -** כמה מסמכי תחקור אירועים לא התייחסו להפקת הלקחים הנדרשים.
- **סקרים ומבדקי חדירה -** רפאל לא קבעה את התדירות לביצוע סקרים ומבדקי חדירה הנדרשים. כמו כן, עלו פערים בתחום זה.

עיקרי המלצות הביקורת

- על מס"ל ומלמ"ב לקיים את החלטות הממשלה בכל הנוגע להסדרת שיתוף הפעולה ביניהם באמצעות המנגנונים שנקבעו בהחלטות.
- מומלץ כי מלמ"ב יפעל להסדיר ככל הנדרש את הסמכויות הנדרשות לצורך מימוש ייעודו.
- מומלץ כי היחידה הטכנולוגית במלמ"ב תפעל להשלים את תורת ההגנה בסייבר, ובכלל זה להכין את התקן למרכז הניטור ואת ההנחיות הנדרשות לגבי היערכות לניהול אירועי סייבר ולניהול האירועים, תחקורם והפקת הלקחים בנושא.
- על הנהלת רפאל לדווח לדירקטוריון כנדרש לגבי אירועי סייבר.
- מומלץ כי הנהלת רפאל תמשיך לבחון מדי שנה בשנה את גודל התקציב הנדרש להגנת הסייבר בהתייחס לפוטנציאל הנזק, למחזור המכירות השנתי ולרווח התפעולי השנתי שלה.
- על הנהלת רפאל לתחקר את ניהול אירועי הסייבר בהתאם לנדרש. על רפאל להשלים את ההוראה בנושא ניהול אירועי אבטחת טכנולוגיות והגנת סייבר במערכות המחשב כנדרש.
- מומלץ כי רפאל תפעל לתיקון הפערים שעלו בתחום הסקרים ומבדקי החדירה.
- על רפאל לפעול לתיקון הליקויים שעלו בדוח זה.

סיכום

רפאל היא מרכיב משמעותי בבניית עוצמתה הצבאית וחוסנה של המדינה. בביקורת עלו ליקויים הנוגעים בין היתר לאי-הסדרת יחסי העבודה בין מערך הסייבר הלאומי (מס"ל) למלמ"ב ולהגנה על המידע ומערכות המחשוב ברפאל. על הנהלת רפאל ודירקטוריון רפאל לפעול לתיקון הליקויים ולוודא בשיתוף מלמ"ב כי רפאל מיישמת את הנחיות מלמ"ב כנדרש.

דוח מבקר המדינה - סייבר ומערכות מידע |
חשוון התשפ"ד | נובמבר 2024

דוח מיוחד

ההיערכות הלאומית בתחום הבינה המלאכותית

ההיערכות הלאומית בתחום הבינה המלאכותית

רקע

בינה מלאכותית (Artificial Intelligence) היא שם גג לטכנולוגיות המיועדות לאפשר למכונות לבצע משימות שדורשות אינטליגנציה אנושית (בינה מלאכותית). מהפכת הבינה המלאכותית המתרחשת בשנים האחרונות היא בגדר "חדשנות משבשת[1]" (Disruptive Innovation), והיא צפויה לשנות מהותית תחומי חיים וענפי תעשייה רבים. משרד החדשנות, המדע והטכנולוגיה (משרד החדשנות) הגדיר את המונח בינה מלאכותית כ"יכולת של מכונה ללמוד לבצע פעולה אנושית ולטייב את ביצועה, בהסתמך על נתונים, דוגמאות וניסיון פעולה, ובאופן רחב יותר, לכלל הפעולות הטכנולוגיות למיצוי מידע ולהפקת תובנות ממאגרי נתונים".

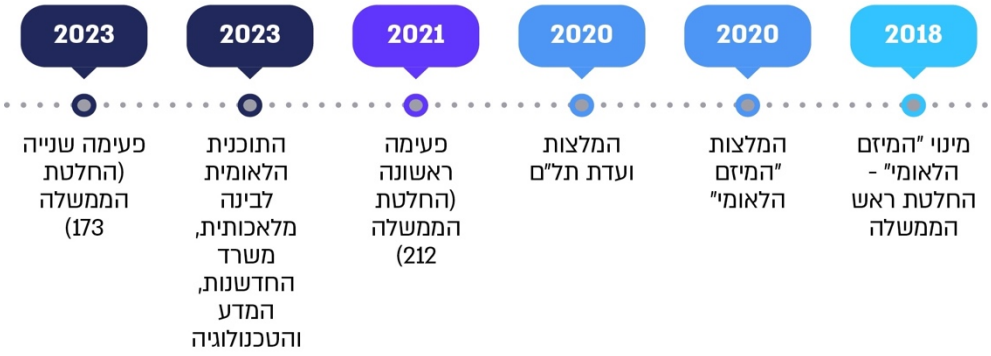
המחקר האקדמי בתחום הבינה המלאכותית החל כבר בשנות החמישים של המאה העשרים, אך בשנים האחרונות, ובייחוד מאז יציאתם לשוק של אמצעים ויישומונים (אפליקציות) הזמינים לשימוש במגוון תחומים, אנו עדים לקפיצת מדרגה משמעותית ביכולות השילוב בין האדם למכונה, אשר יש המגדירים אותה כמהפכה של ממש. תחום הבינה המלאכותית משולב למשל בפיתוח כלי רכב עצמאיים (אוטונומיים), בפיענוח תצלומי רנטגן, בהערכת סיכוני אשראי, במסחר בניירות ערך ובבחינת מועמדים לתעסוקה. מערכות בינה מלאכותית משולבות גם ביחסים בין צרכנים לעסקים, בין עסקים לעסקים אחרים, בין בעלי מקצוע ללקוחות, ביחסי עבודה, בין גופים במגזר הציבורי ובין המגזר הציבורי לכלל הציבור.

הבינה המלאכותית נמצאת בשימוש נרחב גם במהלך מלחמת "חרבות ברזל". מלבד השימוש המבצעי בה, היא סייעה בחלק מפעולות הזיהוי והאיתור של החטופים והחללים. בתחום ההסברה משמשת הבינה המלאכותית, בין היתר, ליצירת סרטונים במגוון שפות כדי להנגיש את המידע לאוכלוסיות רבות ברחבי העולם באמצעות שכפול קול, הנפשה, דיבוב, כתוביות ותרגום. כמו כן, במהלך המלחמה בלט השימוש בטכנולוגיית "deepfake" - יישום טכנולוגי מבוסס בינה מלאכותית, שבו השתמשו גורמים שונים לתעמולה ולהפצת מידע כוזב.

במאי 2018 מינה ראש המטה לביטחון הלאומי דאז (המל"ל), בהתאם להחלטת ראש הממשלה, את ראשי המיזם לגיבוש תוכנית לאומית להעצמת החוסן המדעי-טכנולוגי כמרכיב מרכזי בביטחון הלאומי של ישראל ("המיזם הלאומי"). מטרת המיזם הייתה להעמיד את מדינת ישראל בחמישייה המובילה של מדינות העולם בתחומי הליבה הטכנולוגיים, ובהם בינה מלאכותית ומדעי הנתונים. דוח המיזם הוגש לראש הממשלה ופורסם בספטמבר 2020.

1 חדשנות פורצת דרך שמחוללת שינוי מהותי ולא פעם מאיימת על הקיים.

אבני דרך בתחום הבינה המלאכותית בישראל 2018 - 2023



בפברואר 2020 מינה יושב ראש פורום תשתיות לאומיות למחקר (פורום תל"ם[2]) ועדת בדיקה מקצועית בראשות ד"ר ארנה ברי לבחינת הצורך בהתערבות ממשלתית לשם האצת התפתחות תחום הבינה המלאכותית ומדע הנתונים (ועדת תל"ם). הוועדה הונחתה בכתב המינוי להתמקד בהיבטי הון אנושי, תשתיות פיזיות, הנגשת מאגרי מידע והעברת הידע מהאקדמיה לתעשייה. דוח הוועדה פורסם בדצמבר 2020. באוגוסט 2021, במסגרת החלטת ממשלה 212, אישרה הממשלה את המלצות ועדת תל"ם ליישום הפעימה הראשונה בהיקף תקציבי של כ-550 מיליון ש"ח לשנים 2021 - 2023.

ביולי 2022 השיקה שרת החדשנות דאז "תוכנית לאומית לבינה מלאכותית". התוכנית גובשה על ידי צוות בין-משרדי ופורסמה על ידי משרדה בינואר 2023 (התוכנית הלאומית של משרד החדשנות).

בפברואר 2023 אישרה הממשלה בהחלטה 173 הרחבה לפעימה הראשונה, שאושרה כאמור באוגוסט 2021 (הפעימה השנייה). במסגרת ההחלטה הונחה משרד האוצר להקצות תקציב הרשאה להתחייב שלא יעלה על 500 מיליון ש"ח, אשר ימומש על ידי גופי פורום תל"ם בשנים 2023 - 2026.

דוח ביקורת זה נועד לבחון את ההיערכות הלאומית בתחום הבינה המלאכותית, כיצד יוזמת ומיישמת ממשלת ישראל אסטרטגיה לאומית שתבטיח את השתלבותה של מדינת ישראל בשורת המדינות המובילות בעולם והאם פעולותיה בתחום הבינה המלאכותית יניחו בסיס רחב ואיתן להתפתחותה והובלתה של ישראל כמעצמה מדעית-טכנולוגית. הליכי ההערכות, ההחלטה והיישום של תכנית ממשלתית בתחום הבינה המלאכותית החלו בשנת 2018 ונמשכו במהלך תקופת הביקורת.

2 מסגרת פעולה וולונטרית אשר נועדה לתאם ולאגם משאבים בין כל הגופים הלאומיים שתשתית מחקרית גדולה יכולה לשמש אותם (מפא"ת, ות"ת, משרד האוצר, רשות החדשנות ומשרד החדשנות).

נתוני מפתח

0

לא קיימת בישראל **אסטרטגיה לאומית ארוכת טווח** בתחום הבינה המלאכותית. כמו כן הממשלה לא אישרה **תוכנית אב כוללת ופרטנית ליישום.** תחת זאת אישרה הממשלה תוכניות בתחום לאורך השנים בפעימות, מימושן איטי, חסר, ואינו עומד בלוחות הזמנים שנקבעו.

רק מיליארד ש"ח

הסכום שאישרה הממשלה בשתי פעימות, כאשר מרבית הסכום טרם מומש. התקציב המאושר הוא כחמישית מהתקציב שהומלץ בוועדת תל"ם בדצמבר 2020 וכעשירית מההמלצה של "המיזם הלאומי" מספטמבר 2020.

ירידה מהמקום ה-5 למקום ה-9

במדד Tortoiseמתוך 83 מדיניות בין השנים 2019 - 2024. מדד זה הוא מדד בין-לאומי בתחום הבינה המלאכותית, שדירוגו מתבסס על שלושה תחומים - השקעה, חדשנות ויישום.

ירידה מהמקום ה-20 למקום ה-30

במדד Oxford מתוך 193 מדיניות בין השנים 2020 - 2023. מדד זה הוא מדד בין-לאומי בתחום הבינה המלאכותית העוסק במוכנות הממשלתית לבינה מלאכותית. במדד משנה, המודד את אסטרטגיית הבינה המלאכותית של הממשלה ואת יכולותיה בתחום הדיגיטל ישראל ירדה בשנים אלו 33 מקומות (ממקום 35 ל-68).

40% בלבד

מתקציב הפעימה הראשונה שאושר בממשלה לשנים 2021 - 2023 מומש (220 מלש"ח מתוך כ-550 מלש"ח). שיעור המימוש מתייחס להתקשרויות שנחתמו, ועשרות מלש"ח מתוכן טרם בוצעו או הושלמו בפועל.

רק 11%

שיעור מימוש הפעימה הראשונה בתחום מחשוב עתיר ביצועים (מחשב-על) כ-30 מיליון ש"ח מתוך 270 מיליון ש"ח שאושרו.

55%

מהתקציב שהוקצה בפעימה הראשונה עבור תחום ההון האנושי מומש (כ-34 מלש"ח מתוך 62 מלש"ח), במיקוד בצורכי האקדמיה ללא מתן מענה על צורכי התעשייה.

76%

שיעור מימוש התקציב בתחום עיבוד שפה טבעית בעברית וערבית. עם זאת, שיעור המימוש כולל הסכם למודול שפה שבגינו קיימת התחייבות תקציבית שטרם מומשה בפועל.

פעולות הביקורת

בחודשים יוני 2023 - מרץ 2024 בדק משרד מבקר המדינה את ההיערכות הלאומית בתחום הבינה המלאכותית, את דירוגה הבין-לאומי של ישראל בתחום זה ואת פעולות הממשלה ומשרדי הממשלה לקידום תוכנית לאומית לבינה מלאכותית. הביקורת נעשתה במשרד החדשנות, ברשות החדשנות, במשרד הביטחון, בוועדה לתכנון ולתקצוב, במשרד האוצר ובמטה לביטחון לאומי במשרד ראש הממשלה. בדיקות השלמה נעשו במערך הדיגיטל הלאומי שבמשרד הכלכלה והתעשייה.

תמונת המצב העולה מן הביקורת

היעדר גורם ממשלתי מתכלל האמון על הובלת תוכנית לאומית בתחום הבינה המלאכותית - בהתאם להחלטת הממשלה ולסיכום בין שרת החדשנות לראש המל"ל, ביולי 2022 גיבש משרד החדשנות, בהובלת השרה דאז, תוכנית לאומית לבינה מלאכותית. אולם נמצא כי לאחר חילופי הממשלה בינואר 2023, משרד החדשנות לא פעל כפי שנקבע בהחלטת הממשלה לקידום ולהובלה של תחום הבינה המלאכותית, התוכנית שהשיק המשרד, לא עלתה לאחר הקמת הממשלה ה-37 על מסילת יישום ממשית, ולפיכך אף לא באה לכדי מימוש וממילא לא קודמו אבני הדרך שנקבעו בתוכנית. נמצא כי מאז חילופי הממשלה, המשרד צמצם את פעילותו לנושאים ספציפיים בתחום הבינה המלאכותית בישראל ולא הוביל את קידום התחום ברמה הלאומית.

שש שנים לאחר שהתקבלה החלטת ראש הממשלה לקדם את תחום הבינה המלאכותית ולהגישה כתוכנית לאישור הממשלה עדיין לא אושרה בממשלה תוכנית לאומית כוללת לקידום התחום, למעט שתי פעימות מתוך תוכנית תל"ם, נמצא כי התוכנית הלאומית שהשיקה שרת החדשנות דאז ביולי 2022 נותרה "אות מתה" מאחר שלא יושמה לאחר חילופי הממשלות. הצורך בכך שהטיפול הממשלתי בנושא הבינה המלאכותית יובל על ידי גורם ממשלתי מתכלל שנושא באחריות כוללת ליישום התוכנית הממשלתית מודגש ביתר שאת לנוכח שורה של סיבות: חשיבות תחום זה לכלכלת המדינה ולחוסנה; ריבוי משרדי הממשלה והגופים הציבוריים הפועלים לקידום טכנולוגיית הבינה המלאכותית ולהטמעתה במגזר הממשלתי; חשיבות מיצובה של ישראל כמובילה עולמית במהפכה טכנולוגית זו; הסמכות שניתנה למשרד החדשנות בהחלטת הממשלה להוביל את הטיפול הממשלתי בנושא. בפועל, נכון למועד הביקורת, לא היה גורם ממשלתי מתכלל, הנושא באחריות כוללת שאמון על גיבוש הובלת תוכנית לאומית, על איגום תקציבים ועל בקרה ופיקוח על היישום וההתקדמות של התוכנית.

נסיגה בדירוג של ישראל בתחום הבינה המלאכותית - ישראל שואפת להיות מדינה מובילה בתחומי הטכנולוגיה וההיי-טק. בביקורת עלה כי בשנים 2019 - 2024 ירד מקומה

של ישראל בדירוג העולמי בפעילותה והשקעתה בתחום הבינה המלאכותית - במדד Tortoise ירידה מהמקום ה-5 מתוך 62 מדינות למקום ה-9 מתוך 83 מדינות, במדד Oxford ירידה ממקום 20 ל-30 מתוך 193 מדינות ובמדד החדשנות ירידה מהמקום 10 למקום ה-15 מתוך 133 מדינות. נסיגה זו מוסברת בין היתר בממצאים שמפורטים בדוח זה בכל הנוגע לפעולותיה של הממשלה באישור, הובלה ויישום של תוכנית לאומית רחבה בתחום הבינה המלאכותית. יצוין כי מנתוני מדדי המשנה של Tortoise לשנת 2024 עולה כי בעוד שלישראל חוזקות בקטגוריית ההון האנושי, במחקר ופיתוח ובמסחר, היא חלשה - באסטרטגיה ממשלתית (מקום 32); בתשתיות (מקום 26); ובסביבה תפעולית (מקום 65). הירידה של ישראל בדירוגים הבין-לאומיים בשנים 2019 - 2024, ומקומה היחסי של ישראל בתחום היהערכות והמוכנות הממשלתית, משקפות מגמה שמחייבת את הממשלה לבחון את מדיניותה בנושא.

- **דיון בהמלצות "המיזם הלאומי" בממשלה -** "המיזם הלאומי" הוקם במינוי המל"ל על פי החלטת ראש הממשלה. טיוטת דוח המיזם הוצגה לראש הממשלה במאי 2019, וטיוטה סופית הוצגה לראש המל"ל בדצמבר אותה שנה. לאור חילופי הממשלות בשנים אלו, הדוח הסופי נשלח לכלל משרדי הממשלה ופורסם לציבור בספטמבר 2020 וכלל תוכנית מקיפה להבניית מענה לאומי אסטרטגי לתחום הבינה המלאכותית ולפרויקטים ממשלתיים בהיקף כספי של 10 מיליארד ש"ח. בדוח נקבע, על סמך חוות דעתם של מאות מומחי ידע שפעלו בהתנדבות במשך כשנתיים, כי קידום תחום הבינה המלאכותית חיוני לחוסנה של ישראל בתחומים קריטיים (מדע, כלכלה, ביטחון, בריאות ועוד). בביקורת נמצא כי המלצות המיזם לא הוגשו לממשלה ולא נדונו בה וכן לא נדונו בשום פורום ממשלתי כלשהו שמוסמך לקבל החלטות בנושא, וממילא הן גם לא תוקצבו ולא הבשילו לכדי מימוש. זאת הגם שהיה על המל"ל לבחון את עבודת "המיזם הלאומי" בסמוך לאחר השלמתה ולהביא את הפעולות הנדרשות למימוש המלצותיו לבחינת הגורם המוסמך שאישר את המינוי. כמו כן, בהתאם לסיכום עם היועצת המשפטית למשרד רה"ם, היה על המל"ל להקים את הצוות הבין-משרדי ולהגיש את המלצותיו לראש הממשלה ולממשלה בסמוך להשלמת עבודת "המיזם הלאומי" ולא רק כשנה וחצי לאחר מכן.

משעה שראש הממשלה, הממשלה או כל גורם ממשלתי אחר הטילו על גורמים מקצועיים לקיים עבודת מטה ולהניח דוח המתבסס על המלצותיהם של 14 צוות מקצועיים ומאות מומחי ידע, שאמור לשמש בסיס לקבלת החלטה אופרטיבית בנושא מסוים, הרי שלאחר השלמת עבודת הצוותים והנחת הדוח המסכם את עבודתם היה על ראש המל"ל לפעול להשלמת ההליך עד לדיון של הממשלה בהמלצות, אולם הדבר לא קרה. אי העברת מסקנות דוח "המיזם הלאומי", אשר ישב על המדוכה במשך שנתיים, לממשלה, מטעמים מינהליים אשר אינם נוגעים לתוכן עבודת המיזם, פגעה ביכולתה של הממשלה להפיק את התועלת המרבית מתוצרי עבודתם של מאות מומחי ידע מהשורה הראשונה אשר מונו על פי החלטת ראש הממשלה.

- **דיון בהמלצות ועדת בינה מלאכותית ומדע הנתונים (ועדת תל"ם) בממשלה -** ועדת תל"ם מונתה על ידי יו"ר פורום תל"ם לבחינת הצורך בהתערבות ממשלתית לשם האצת התפתחות תחום הבינה המלאכותית ומדע הנתונים. נמצא כי בדומה להמלצות "המיזם הלאומי", שנועדו לשמש בסיס להחלטת ממשלה בנושא, גם תוכנית זו, אשר גובשה והושלמה בדצמבר 2020 כבסיס להחלטת ממשלה, לא נדונה בממשלה במתכונתה המלאה אלא במתכונת מצומצמת במסגרת שתי פעימות שתוקצבו על ידי הממשלה בהיקף

תקציבי של כחמישית מהתקציב שהומלץ בוועדה, כמיליארד ש"ח, ולפיכך גם לא אושרה כתוכנית אב כוללת לתחום ולא תוקצבה בראייה פרוייקטלית ארוכת טווח.

- **אסדרה (רגולציה)** - למרות הסיכונים הקיימים בטכנולוגיית הבינה המלאכותית והצורך להסדיר את השימוש בה באופן אחראי תוך שמירה על זכויות היסוד, נמצא כי נכון למועד סיום הביקורת הפעילות המשותפת של משרד החדשנות ומשרד המשפטים לקידום האסדרה בתחום הבינה המלאכותית והעקרונות שגובשו במסמך עקרונות המדיניות טרם אושרו על ידי הממשלה, וכי ישראל נמצאת בפיגור בהשוואה להתקדמות האסדרהבאיחוד האירופי שבו כבר קיימת חקיקה שמסדירה את השימוש בבינה מלאכותית לפי רמות סיכון. היעדר אסדרה בישראל בתחום הבינה המלאכותית טומן בחובו סיכונים שונים אשר מעלים סוגיות משפטיות ורגולטוריות חדשות. נדרש לוודא כי על אף התקדמות הטכנולוגיה יישאר האדם במרכז קבלת ההחלטות, וכי פיתוח הבינה המלאכותית והשימוש בה יבוצעו באופן אחראי ומאפשר מתוך הקפדה על שמירת זכויות יסוד ואינטרסים ציבוריים; על כבוד האדם ופרטיותו; על שוויון ומניעת אפליה; ועל שקיפות מלאה.

- **מחשוב עתיר ביצועים (מחשב-על) HPC** - אף שכבר בשנת 2020 זוהה הצורך בתשתיות חישוב-על כתנאי בסיסי והכרחי לביסוס מעמדה של מדינת ישראל כמדינה מובילה בתחום הבינה המלאכותית, במועד עריכת הביקורת, כחמש שנים לאחר מכן, תשתיות החישוב הקיימות מוגבלות ואינן מספקות לעניין קידום המחקר והתעשייה בישראל. היעדרה של תשתית חישוב מספקת מעכב את יכולות המגזר הציבורי, האקדמיה והתעשייה לקדם ולפתח את תחום הבינה המלאכותית.

- **תשתית לאימון מודלים גדולים** - נמצא כי נכון לסוף דצמבר 2023, מועד תום הפעימה הראשונה, מפא"ת לא ביצעה את חלקה בהסכם השותפים להסדרת תשתית לאימון מודלים גדולים, ורשות החדשנות לא הסדירה תשתית של חישובים מורכבים לשימוש מדעי, שמעמידות שתיהן בסיס לקידום טכנולוגיית הבינה המלאכותית. לפיכך שיעור מימוש הפעימה הראשונה בתחום זה לטובת קידום הבינה המלאכותית היה 11% בלבד, כ-30 מיליון ש"ח מתוך 270 מיליון ש"ח שאושרו.

- **עיבוד שפה טבעית NLP** - ועדת תל"ם קבעה כי קיימת חשיבות עליונה לפיתוח תחום עיבוד השפה הטבעית, וכי תחום זה מהותי לשימוש ביכולות בינה מלאכותית במשרדי הממשלה ובתעשיות נוספות. על כן התוכנית הגדירה כמטרה מרכזית את צמצום הפער הטכנולוגי הניכר בין היכולות הזמינות בתחום עיבוד השפה באנגלית ובשפות לטיניות אחרות לבין היכולות המקבילות הקיימות בעברית ובערבית. בעניין זה נמצא כלהלן:

  - רק ב-31.12.23, היום האחרון שהוגדר ליישום הפעימה הראשונה, חתמה מפא"ת על הסכם התקשרות בהיקף כספי כולל של 37 מיליון ש"ח למימוש פרויקט מודל שפה בעברית וערבית עם חברה בין-לאומית, והמודל הראשון צפוי להיות מיושם רק לקראת אמצע שנת 2025, שנה וחצי לאחר תום הפעימה הראשונה. היקפו הכספי של ההסכם הוא כרבע מההתחייבות בתחום עיבוד השפה במסגרת הפעימה הראשונה. העיכוב הניכר של מפא"ת בקידום המענה למודל שפה גדול (LLM) בעברית ובערבית עלול לפגוע באופן משמעותי בקידום המענה המסופק על ידי גופי הממשלה לאזרחים, שכן מודל עיבוד שפה גדול בעברית ובערבית אמור להזניק את הטרנספורמציה הדיגיטלית

של המשק הישראלי בכלל ובמגזר הציבורי בפרט באמצעות שימוש בכלי בינה מלאכותית.

- במועד תום הפעימה הראשונה לא היה בישראל מודל שפה בעברית וערבית לשימוש גופי הממשלה ואזרחיה. סך המימוש התקציבי בתחום עיבוד שפה טבעית לפיתוח יכולות עיבוד עבור עברית וערבית - אשר נדרש לצמצום הפער הטכנולוגי הניכר הקיים בתחום למול יכולות העיבוד באנגלית ובשפות לטיניות אחרות - היה 76% מהתקציב שאושר לרכיב זה (138 מתוך 180 מיליון ש"ח). שיעור מימוש זה כולל כאמור את ההסכם למודל שפה אשר בגינו קיימת רק התחייבות תקציבית למול החברה בסך 37 מיליון ש"ח, אך הוא טרם מומש בפועל.

- **הון אנושי -** נמצא כי גם בתחום ההשקעה בהון האנושי לקידום הבינה המלאכותית, היישום של ות"ת למימוש תוכנית תל"ם במסגרת הפעימה הראשונה שאושרה על ידי הממשלה היה חלקי, נכון לסוף שנת 2023 - מועד תום הפעימה הראשונה - מימוש תקציב תחום ההון האנושי בפעימה זו היה כ-34 מיליון ש"ח מתוך 62 מיליון ש"ח, כמחצית (55%) מהתקציב שהוקצה עבורו, וגם זאת מתוך התמקדות בצורכי האקדמיה וללא מתן מענה על צורכי התעשייה.

- **העסקת חוקרים וסגל בכיר באקדמיה -** נמצא כי אף שבהסכם השותפים של הפעימה הראשונה תכולת פרק ההון האנושי בתוכנית כללה כ-24 מיליון ש"ח שהוקצו לקליטת אנשי סגל באקדמיה וכ-20 מיליון ש"ח שהוקצו להענקת מענקי מחקר ייעודיים לחוקרים בתחומי AI CORE, רכיבים אלו לא יושמו על ידי ות"ת עד תום הפעימה הראשונה. עוד עלה כי לוות"ת ולרשות החדשנות אין מידע עדכני ומדויק על מספר החוקרים הקיים. חוסר במידע יסודי זה מצביע על היעדר הקשב המספק לקידום הכשרת ההון האנושי הנדרש בתחום הבינה המלאכותית, אף שהדבר נדרש למימוש היעד שהוגדר.

- **היקף המלגות -** נמצא כי היקף המלגות שהעניקה ות"ת בשנים 2021 - 2023 במסגרת מימוש תקציב הפעימה הראשונה שאושרה על ידי הממשלה, היה כ-50 מלגות מתוך כ-1,000 מלגות (5%) שעליהן המליצה ועדת תל"ם. עוד נמצא כי היקפן הכספי הממוצע היה כ-10 מיליון ש"ח לשנה, מתוך 100 מיליון ש"ח לשנה שהומלצו על ידי הוועדה. עולה אפוא כי היקף המלגות שניתנו במסגרת הפעימה הראשונה היה כ-10% מהתקציב שהומלץ. עוד עלה בביקורת כי אין לרשות החדשנות ולוות"ת מידע על מידת ההשפעה של חלוקת מלגות אלו על קידום ההון האנושי באקדמיה בתחום הבינה המלאכותית.

- **מימוש תקציב הפעימה הראשונה -** נכון לתום מועד הפעימה הראשונה, דצמבר 2023, המימוש התקציבי של הפעימה הראשונה היה חסר וכלל רק כ-40% מסך הסכום שאושר בממשלה, שהם 220 מיליון ש"ח מתוך כ-550 מיליון ש"ח. סכום זה הוא בבחינת מימוש בהיקף של כ-5% בלבד מהתוכנית המלאה שגובשה על ידי ועדת תל"ם אך כאמור לא נדונה בממשלה במתכונתה המלאה ולא תוקצבה. יודגש כי שיעור המימוש האמור מתייחס להתקשרויות שנחתמו, אך עשרות מיליוני ש"ח מתוכן טרם בוצעו או הושלמו בפועל.

- **הפעימה השנייה -** בביקורת נמצא כי בפברואר 2023 אישרה הממשלה תקציב לפעימה השנייה ביישום תוכנית תל"ם בהיקף של עד 500 מיליון ש"ח, למימוש בשנים 2023 - 2026, אך רק בספטמבר 2024, יותר משנה וחצי לאחר החלטת הממשלה האמורה, נחתם הסכם השותפים של פורום תל"ם לפעימה זו למימוש בשנים 2024 - 2027. מצב הדברים האמור,

שבו בהסכם השותפים שנחתם נקבע כי הפעימה השנייה תמומש כשנה לאחר מועד המימוש שנקבע בהחלטת הממשלה, משקף פער משמעותי ביישום החלטת הממשלה בכל הנוגע לפעימה השנייה. זאת בין היתר לנוכח ההערכה כי בשנה הראשונה והשנייה מתוך הארבע שעליהן החליטה הממשלה ימומשו במסגרת ההסכם בסך הכול רק כ-10% מהתקציב הכולל שנקבע בהחלטת הממשלה.

יצוין כי סך התקציב שאושר לפעימה הראשונה והשנייה הוא כמיליארד ש"ח, כחמישית מהתקציב שעליו המליצה ועדת תל"ם בדצמבר 2020.

אוריינות נתונים - נמצא כי אף שאוריינות הנתונים היא מיומנות חיונית הצפויה להידרש בכל תחום ובכל מגזר, הפעימה הראשונה שאושרה על ידי הממשלה וכן הסכם השותפים בפעימה השנייה לא כללו התייחסות לתחום זה. עוד נמצא כי משרד החינוך לא שולב כחלק מהסכמי השותפים לקידום הבינה המלאכותית. היעדר הקניית אוריינות הנתונים כבר בגילאים הצעירים עלולה לפגוע במוכנות ובהשתלבות של הדור הבא בעולם הטכנולוגי, שכן בינה מלאכותית נוגעת לכל תחומי החיים וצפויה להיות בשימוש יום-יומי על ידי כלל הציבור.

הקמת מוקד ידע במשרד החדשנות - משרד מבקר המדינה מציין לחיוב את פעולות משרד החדשנות, לרתימת הגופים לקידום עקרונות הרגולציה ולהקמת מוקד ידע ותיאום לרגולציה ולאתיקה של בינה מלאכותית.

עיקרי המלצות הביקורת

על משרד החדשנות, לפעול בהתאם להחלטת הממשלה ולסיכום של השרה דאז עם המל"ל ולהוביל את מדיניות הממשלה בתחום הבינה המלאכותית. במסגרת זו עליו להשלים את גיבוש התוכנית האסטרטגית הלאומית שהחל בהכנתה עוד בשנת 2022. על תוכנית זו לכלול, בין היתר: חזון, אבני דרך, תוכנית פעולה מפורטת הכוללת הגדרה של הגורם הממשלתי האחראי לכל כיוון פעולה, לוחות זמנים למימושה ותוכנית תקציבית התואמת לתוכנית שתיקבע. כמו כן עליו לקבוע מתווה לבחינה עיתית של מידת העמידה של המדינה ביעדים שנקבעו בתוכנית, וכן מתווה לבחינה פרטנית של כיווני הפעולה שהוגדרו בה, לרבות עדכונם במידת הצורך. בעת הזו נדרש ממשרד החדשנות, המדע והטכנולוגיה לממש את אחריותו ובאופן זה תקום החלטת הממשלה כלשונה. הובלה ברורה של תוכנית לאומית משמעותית הכרחית לשמירה על יכולותיה הטכנולוגיות ועל יתרונה היחסי אל מול יתר מדינות העולם. כל סטייה מנתיב היישום האמור של ההחלטה יחייב עדכון של הממשלה בנושא לצורך בחינת מצב הדברים ולצורך מתן מענה שיבטיח את מימוש היעד של קידום תחום הבינה המלאכותית על ידי הממשלה. מוצע כי ראש הממשלה - אשר כבר בשנת 2018 יזם מהלך לקידום התוכנית הלאומית בתחום הבינה

המלאכותית כבסיס להחלטת הממשלה בנושא - יעקוב באמצעות המל"ל אחר התקדמות הטיפול הממשלתי בנושא ויבטיח כי מיושמת תוכנית לאומית משמעותית הלכה למעשה.

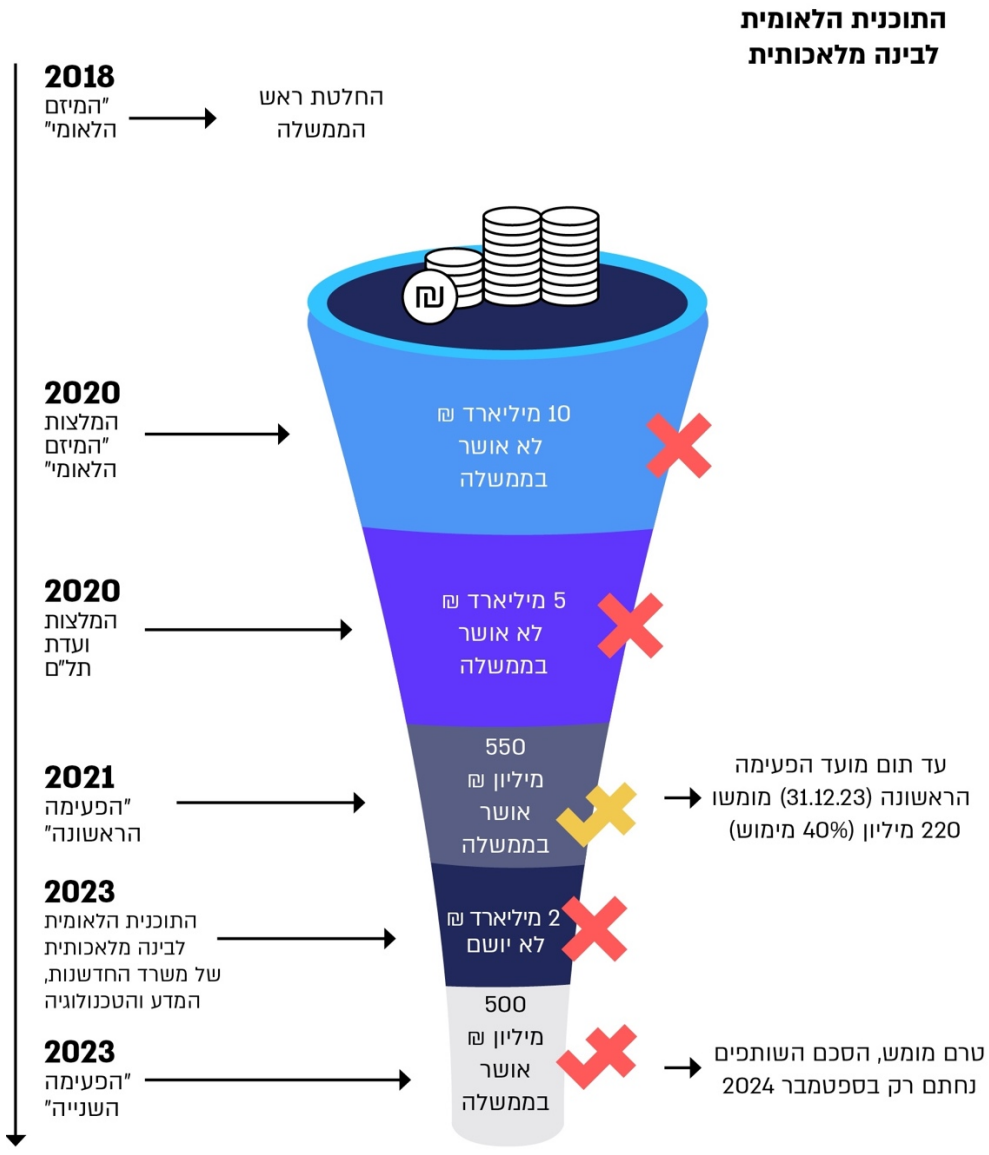
- על משרד החדשנות לפעול בשיתוף עם רשות החדשנות ולקדם את חתימת ההסכמים הנדרשים לקידום התשתית המחשובית הנדרשת לקידום הבינה המלאכותית בישראל.
- לאור חשיבות קידום מודל שפה גדול בעברית וערבית, מוצע כי משרד החדשנות יפעל בשיתוף רשות החדשנות, מפא"ת ומערך הדיגיטל, לקידום הפרויקט ולהטמעתו במשרדי הממשלה ובמגזר הציבורי.
- לנוכח עמדת הגופים כי אין ביכולתה של תוכנית המענקים לפתור את בעיית ההיצע בקליטת אנשי סגל חדשים בתחום הבינה המלאכותית, מומלץ כי לאחר קביעת מספר החוקרים הנדרש, ות"ת תבחן חלופות נוספות לקליטת סגל אקדמי בתחום, וכי היא תממשן, בהתאם לממצאי הבחינה, במסגרת הפעימות הנוספות.
- על רשות החדשנות וות"ת להפעיל מנגנוני בקרה בדגש על איסוף וניתוח של נתונים כדי לבחון את השפעת חלוקת המלגות ויעילותן על קידומו והרחבת היקפו של ההון האנושי בתחום הבינה המלאכותית.
- מוצע כי משרד החדשנות, יבחן את הסיבות להיקף המימוש המצומצם של מרכיבי הפעימה הראשונה של התוכנית בתחום ההון האנושי וינקוט בפעולות ממשיות על מנת להבטיח מימוש מלא בהמשך היישום של התכנית. כמו כן, לנוכח העובדה כי החסם המרכזי במיצוי היכולות בתחום הבינה המלאכותית הוא ההון האנושי, מוצע כי משרד החדשנות בשיתוף ות"ת יבחנו מתווה מוסכם ומתכלל להגדלה של היקף המחקר ושל מספר חברי הסגל והחוקרים בתחום הבינה המלאכותית.
- על משרד החדשנות ומשרד המשפטים לפעול לעדכון עקרונות האסדרה בהתאם להתפתחויות הטכנולוגיות ולעקרונות שנקבעו באמנה הבין-לאומית שנחתמה, ולהביאם לאישור הממשלה. כמו כן, עליהם לבחון את הצורך בקידום חקיקה כפי שנעשה באיחוד האירופי, או לחלופין בקידום אסדרה ברמה הסקטוריאלית בהתאם לסיכון קונקרטי, כמקובל בארצות הברית, בבריטניה, באוסטרליה ועוד. מכל מקום, אסדרה באחת הדרכים נדרשת לצורך הגנה על בטחון המדינה ואזרחיה מפני שימוש לרעה ביכולות הבינה המלאכותית.
- על משרד החדשנות, אשר קיבל מהממשלה את הסמכות והאחריות להוביל ולקדם את תחום הבינה המלאכותית בישראל, לפעול למימוש הפעימה השנייה כפי שנקבעה בהחלטת הממשלה. כמו כן עליו לעקוב אחר לוחות הזמנים של מימוש הפעימה ואחר תכולות ביצועה. זאת בשיתוף פעולה עם פורום תל"ם ויתר המשרדים והגופים הממשלתיים העוסקים בקידום ובהטמעה של תחום זה בישראל.
- מומלץ כי משרד החדשנות בשיתוף משרד החינוך ישלבו את תחום החינוך בתוכנית הלאומית לבינה מלאכותית באמצעות הבניית תוכניות לקידום ולחיזוק של אוריינות הנתונים כמקצוע בתוכניות הלימודים. עוד מומלץ כי לאחר השלמת עבודת ועדת המשנה שמונתה על יד מנכ"ל משרד החינוך לקידום תחום הבינה המלאכותית, משרד החינוך יאסדר את הנושא באמצעות חוזר מנכ"ל ויגבש תוכנית רב-שנתית להטמעת התחום בתוכנית הלימודים בכלל מוסדות החינוך.

סטטוס מימוש הפרויקטים העיקריים של הפעימה הראשונה

עיבוד שפה טבעית	מחשוב עתיר ביצועים (מחשב-על)	הון אנושי	רגולציה (אסדרה)
מפא"ת מודל שפה גדול בעברית ובערבית- (LLM')	**מפא"ת** תשתית אימון מודלים גדולים	**ות"ת** מלגות לדוקטורנטים	**משרד החדשנות, המדע והטכנולוגיה** מסמך עקרונות מדיניות, רגולציה ואתיקה
רשות החדשנות קול קורא למאגרי מידע, מודלים וכלים בתחום עיבוד השפה	**רשות החדשנות** תשתית חישוב מדעי	**ות"ת** מלגות למסטרנטים	
מפא"ת תרגום עברית-ערבית	**רשות החדשנות** תשתית מעבדתית למחקר ופיתוח	**ות"ת** קליטת סגל בתחומי CORE AI	
משרד החדשנות, המדע והטכנולוגיה מחקר יישומי באקדמיה		**ות"ת** הענקת מענקי מחקר ייעודיים לחוקרים בתחומי CORE AI	
רשות החדשנות TRUST AI			

✓ בוצע ✓ בוצע באופן חלקי ✗ לא בוצע

ההתפתחות התקציבית והמהותית של הרשות הלאומית לבינה מלאכותית



סיכום

ההובלה המדעית והטכנולוגית של מדינת ישראל היא אחד מעמודי התווך של ביטחונה הלאומי, חוסנה הכלכלי ורווחת אזרחיה. הובלתה של ישראל בתחומים אלו היא דרך אסטרטגית לפצות על היעדר משאבים טבעיים ועל משאבי אנוש מצומצמים ביחס למדינות אחרות בעולם. מהפכת הבינה המלאכותית כבר איננה טכנולוגיה עתידנית - היא טכנולוגיית ליבה חדשנית המשפיעה בהדרגה על מרבית היבטי החיים בהווה ואף תופסת מקום מרכזי ומשמשת מוקד לתחרות בזירה הבין-לאומית במגוון תחומים, ובהם : מדע, כלכלה, תעשייה, ביטחון, בריאות, חינוך ותעסוקה.

דוח זה מצביע על כך כי אף שמדינת ישראל זיהתה כבר בשנת 2018 כי התחום הטכנולוגי מצוי בפתחה של מהפכה של ממש, ואף שראש הממשלה הבין את ההכרח שבהכנה וביישום של תוכנית לאומית מקיפה וכוללת בנושא, הרי שמאז לא השכילה הממשלה להוביל וליישם מהלכים לאישור תוכנית לאומית רחבה, כוללת וארוכת טווח ולהעלותה לנתיב של יישום ממשי, תוך קיום בקרה שוטפת שתבטיח את מסלול ההתקדמות הנחוץ. ובפועל מיצובה של ישראל בממדים הבין-לאומיים נשחק.

נמצא כי על אף החלטת ראש הממשלה משנת 2018 לאשר את הקמת "המיזם הלאומי", ואף שוועדת תל"ם, ועדה בדיקה מקצועית שמונתה לבחינת ההאצה הנדרשת להתפתחות תחום הבינה המלאכותית,קבעה בשנת 2020 כי קיומה של תוכנית לאומית בתחום הבינה המלאכותית ומדע הנתונים קריטי וחיוני לחוסנה של מדינת ישראל, נכון לשנת 2024 לא קיימת תוכנית לאומית מאושרת ומתוקצבת על ידי הממשלה. תחת זאת, בשנים 2018 - 2023 גובשו שתי תוכניות מרכזיות לקידום התחום ברמה הלאומית - "המיזם הלאומי" ותוכנית ועדת תל"ם - אך תוכניות אלה נזנחו או קודמו באופן חלקי ביותר. בביקורת עלה כי גם הסיכום בשנת 2021 בין ראש המל"ל לשרת החדשנות דאז כי יוענקו למשרדה אחריות וסמכות כוללות לניהול התוכנית הלאומית ולתכלול פעולות הממשלה בנושא, סיכום שעוגן בהחלטת הממשלה, לא יושם. נוסף על כך עלה כי התוכנית הלאומית שגובשה על ידי משרד החדשנות נותרה בגדר "אות מתה" וכי מאז חילופי הממשלה בדצמבר 2022, משרד החדשנות לא ראה עצמו מחויב למינוי האמור אלא לקידום תחומים ספציפיים בלבד.

יוצא אפוא כי כשש שנים לאחר שהתקבלה החלטת ראש הממשלה ולמרות העובדה שטכנולוגיית הבינה המלאכותית מתקדמת בקצב מהיר בזירה הבין-לאומית, לא קיימת בישראל אסטרטגיה לאומית ארוכת טווח, והממשלה לא אישרה תוכנית אב כוללת ופרטנית ליישום. אישור הממשלה של תוכניות בתחום לאורך השנים התבצע בפעימות, מימושן איטי, חסר ואינו עומד בלוחות הזמנים שנקבעו. כמו כן, עקרונות המדיניות, הרגולציה והאתיקה בתחום הבינה המלאכותית שגיבשו משרד החדשנות ומשרד המשפטים טרם אושרו בממשלה ולפיכך אף לא עוגנו רבדים חיוניים בחקיקה או באסדרה סקטוריאלית.

ניתן אפוא לקבוע כי המדינה איתרה את הצורך במועד וניתחה אותו, ואולם זה כמה שנים היא אינה צולחת את שלבי קבלת ההחלטות ההכרחיות לנוכח הצורך ואת שלבי יישומן.

כדי לשמר את עליונותה הטכנולוגית והמדעית של ישראל בתחום הבינה המלאכותית, שהוגדר כבעל עדיפות לאומית, על משרד החדשנות, להוביל את מדיניות הממשלה בתחום ולפעול בהתאם להחלטת הממשלה ולסיכום של השרה דאז עם המל"ל. במסגרת זו עליו להשלים את

גיבוש התוכנית האסטרטגית הלאומית שהחל בהכנתה כבר בשנת 2022. על תוכנית זו לכלול, בין היתר: חזון, אבני דרך, תוכנית פעולה מפורטת הכוללת הגדרה של הגורם הממשלתי האחראי לכל כיוון פעולה, לוחות זמנים למימושה ותוכנית תקציבית התואמת לתוכנית שתיקבע. כמו כן על המשרד לקבוע מתווה הן לבחינה עיתית של מידת העמידה של התוכנית ביעדים שנקבעו בה, והן לבחינה פרטנית של כיווני הפעולה שהוגדרו בה ובכלל זה עליו לעדכנם במידת הצורך. במסגרת זו עליו לבחון בין היתר את המבנה הניהולי הקיים למימוש הפעימות שאושרו בהחלטות הממשלה, הפועל במועד סיום הביקורת באופן וולונטרי וללא סמכויות תקציביות.

בעת הזו נדרש ממשרד החדשנות, המדע והטכנולוגיה לממש את אחריותו ובאופן זה תקוים החלטת הממשלה כלשונה. הובלה ברורה של תוכנית לאומית משמעותית הכרחית לשמירה על יכולותיה הטכנולוגיות ועל יתרונה היחסי אל מול יתר מדינות העולם. כל סטייה מנתיב היישום האמור של ההחלטה יחייב עדכון של הממשלה בנושא לצורך בחינת מצב הדברים ולצורך מתן מענה שיבטיח את מימוש היעד של קידום תחום הבינה המלאכותית על ידי הממשלה.

מוצע כי ראש הממשלה - אשר כבר בשנת 2018 יזם מהלך לקידום התוכנית הלאומית בתחום הבינה המלאכותית כבסיס להחלטת הממשלה בנושא - יעקוב באמצעות המל"ל אחר התקדמות הטיפול הממשלתי בנושא ויבטיח כי מיושמת תוכנית לאומית משמעותית הלכה למעשה.

We will continue to pray and hope for the victory of the IDF and the Defense System in this difficult war forced upon us by our most bitter of enemies seeking to destroy us as a nation and as a state, for the return of the hostages to their homes, the return of residents from affected areas in the south and the north to their homes, the recovery of the injured and for peaceful and routine days.

Matanyahu Englman
State Comptroller and
Ombudsman of Israel

Jerusalem, November 2024

readiness in the artificial intelligence. While the state has identified and analyzed the need in time, for several years it has failed in the decision-making and implementation stages.

To preserve Israel's technological and scientific superiority in the artificial intelligence, deemed a national priority, the Ministry of Innovation, Science, and Technology must guide the government's policy in this field under the government's resolution and the conclusions of the former Minister of Innovation, Science, and Technology in collaboration with the National Security Council. This includes, formulation of the national strategic plan, which was initiated in 2022. Additionally, the Ministry must establish a framework for periodic evaluation of compliance with the established goals in the plan, alongside individual assessments of the defined action directions and necessary updates. Moreover, it is imperative to examine the current management of implementing the approved measures under government resolutions, by parties acting voluntarily and without designated budgetary authority. At this juncture, the Ministry of Innovation, Science, and Technology must assume its responsibilities to ensure that the government's resolution is carried out as required. A clear leadership approach for a significant national program is crucial to maintain technological capabilities and relative advantages over other nations. Any deviation from the prescribed implementation path will necessitate a government update to assess the situation and provide responses to advance artificial intelligence as a government priority. It is recommended that the Prime Minister, who initiated the promotion of a national program in artificial intelligence already in 2018 as a basis for the government's resolution, monitor the government's progress through the National Security Council to ensure the practical implementation of a significant national plan.

It is my pleasant duty to thank the employees of the Office of the State Comptroller, who work devotedly in conducting an audit professionally, intensively, thoroughly and fairly and in the publication of objective, effective and relevant audit reports.

The State Comptroller's Office undertakes to continue auditing the audited bodies' compliance with current and future risks and engaging in cyber defense Information technologies and privacy protection for the benefit of Israeli citizens.

Rafael. It is imperative that Rafael's management and board of directors address these deficiencies and collaborate with the Director of Security of the Defense System to ensure compliance with its directives, as required, given that Rafael's operations are a significant component for the enhancement of the country's military strength and resilience.

- My office conducts follow-up audits to examine whether the deficiencies indicated in the audit reports have been rectified. This report includes the follow-up audits regarding: **The Tevel Project for Upgrading the Computing Systems in the National Insurance Institute** – the follow-up audit indicated that the majority of the core deficiencies that arose in the previous audit had not been rectified or had been slightly rectified. This is notwithstanding that until the completion of the audit, public funds had been invested in the Tevel Project at more than NIS one billion (more than twice as much as the Project's initial overall budget). It was further found that improving the service provided to the public and assisting the public in ensuring its rights had been achieved only partially, among other things due to a reduction in the Project's capacities; **Ask Once Policy** – the follow-up audit found that although since the completion of the previous audit there had been progress in the preliminary activity required for the implementation the Ask Once Policy – most of the deficiencies found in the previous audit had not been rectified with regard to the mapping of the government services provided to the public and an analysis of their characteristics. Although eight years have passed, the government plan resolved upon by the government in 2016 has not yet been fully implemented and the completion of the process is not expected in the next few years. The root of the problem is that the Digital Agency lacks the authority to oblige the government ministries to implement its directives. This, alongside with the lack of engagement of the government and public bodies in implementing those directives, lead to a partial implementation of the Ask Once Policy.

- In addition to the previously detailed chapters of the report, it includes a special report on **The National Preparedness in the Artificial Intelligence**. Preserving the State of Israel's supremacy in the domains of science and technology is a fundamental pillar of its national security, economic resilience, and the well-being of its citizens. This approach strategically compensates for the lack of natural resources and limited human resources compared to other countries. The artificial intelligence revolution is no longer a futuristic concept – it is an innovative core technology that increasingly influences various facets of contemporary life and emerges as a central element of competition in the international arena across a variety of fields: science, economy, industry, security, health, education, and employment.

  The report indicates that the State of Israel already recognized in 2018 that the technological sector is on the brink of a significant revolution, and the Prime Minister acknowledged the necessity of preparing and implementing a comprehensive national plan on the subject. However, the government has not succeeded in leading and executing a broad, comprehensive, and long-term national plan, and implement it, resulting in a decline in Israel's position in international benchmarks attesting to its

has 16 additional systems, some of which are divided into sub-systems, and the annual average of the operational expenses and the investments of the Information Systems Department is NIS 124 million. These systems are based on various technologies and supported by over 20 suppliers. The audit on the f **Information Systems in the Israel Postal Company and the Postal Bank** found deficiencies in the information systems and data protection in the Postal Company and the Postal Bank, including poor management of the procedures for revoking authorizations for employees and its monitoring – thus, 85 (3%) of authorizations holders for a particular system are not defined in the human resources system as "active" and also 79 of them were not located in the Company's computerized controls, 780 (about 13%) of the holders of the active authorizations in the network's central management system are employees who are not included in the list of active employees in the Company's human resources system; the use of outdated automated equipment which is detrimental to both the service provided to the Company's customers and the Bank and the data protection – thus, despite the project for replacing the automated equipment being already defined as a strategic project in 2019, the Postal Company started to replace it only at the beginning of 2022. Until March 2024, only 683 out of 1,850 computers had been replaced or upgraded; the lack of a multi-year work plan for the Information Systems Department; the lack of monitoring and follow-up of the performance of the work plans; the multiplicity of information systems that makes it difficult to transfer the information between those systems and requires the performance of manual procedures and the investment of resources to compensate for this.

The Information Systems Department at the Postal Company must determine a methodological plan that includes the development of the information systems from a future standpoint, the upgrading of old systems and the optimization of the existing systems and the integration between them; while ensuring cyber protection and the reduction of exposure to risks originating in the various aspects of unauthorized use. The Postal Company must, as part of the process improve data protection – and in particular in light of the cyber incident that occurred there in April 2023 – to improve the control over the of Company's authorization management. The Company must examine the deficiencies that were raised in the audit and immediately rectify them.

- The report includes a chapter on the **Cyber Protection: Aspects of Regulation and Protection of the Information and Computer Systems at Rafael Advanced Defense Systems Ltd.** In 2022, the budget allocated to the Cyber and Technology Protection Department at Rafael constituted 10% of the computing budget of the Information Technologies and Processes Administration. Additionally, the rate of phishing incidents reported to the Israel National Cyber Directorate in 2022 represented 31% of the total 9,108 cyber incidents recorded to it that year. The audit identified several deficiencies, including the lack of regulation of the working relationship between the National Cyber Directorate and the Director of Security of the Defense System, as well as deficiencies pertaining to the protection of information and computer systems at

- **The Tevel Project for Upgrading the Computing Systems in the National Insurance Institute – Follow-Up Audit**
- **Ask Once Policy – Follow-Up Audit**

It should be noted that regarding the chapter on the Cyber and Data Protection in the National Insurance Institute and the chapter on the Aspects of Regulation and Protection of the Information and Computer Systems at Rafael Advanced Defense Systems Ltd. confidentiality measures were taken by the Knesset's State Control subcommittee, which decided not to submit them in their entirety before the Knesset but rather publish only parts thereof, under paragraph 17 of the State Comptroller Law, 1958 [Consolidated Version].

The following is an overview of several chapters of the report:

- The digital transformation, which has been integrated into most of the government's work processes, presents opportunities to improve the effectiveness of the government's work and the provision of advanced services to the public, alongside new challenges and risks. During 2022, the scope of the financial activity in the government ICT was NIS 4.8 billion. Therefore, it is essential to manage the risks in this field in an organized and methodological manner. The audit on the subject of **the Government Risk Management in the ICT** indicates considerable gaps in the ICT risk management by the government, including the lack of an overall governmental overview regarding ICT risks; the failure of the National Digital Agency to reduce broad risks; partial reports by government ministries concerning their main ICT risks; and the absence of a main organized and systematic program for ICT risk management in the government ministries, including aspects of risk management regarding projects and broad and cross-cutting risk management – such as a shortage of manpower and difficulty in recruiting and retaining staff. As a result, 80% of the employees in the ICT in the government are freelancers (3,993 out of 5,308 employees during 2022).

  The Israel National Cyber Directorate must address the findings of this audit and the government heat map of the areas of risk in the ICT presented in the audit report, to focus the government activity in this field and ensure that the risk management in this challenging and dynamic field is performed methodologically and optimally and allows preparation for the challenges in advance, providing a solution for the changes occurring in the environment of the government activity.

- The Israel Postal Company was a government company under the full ownership of the State of Israel (until it was privatized in May 2024), providing postal services as well as banking services via its subsidiary – the Postal Bank. As of the end of 2023, the Postal Company and the Postal Bank have 400 postal units, 650 collection centers and about 60 regional postal centers. During 2023, about 11.9 million customers of the Company and the Bank received services in the postal units. The Postal Company has 55 information systems, some of which are divided into sub-systems, and the Postal Bank

Foreword

This report, which is placed on the Knesset's table, presents the results of the audit in the fields of Cyber and Information Technology protection. It also includes a special report on the National Preparedness in the Artificial Intelligence.

Since October 2023, the State of Israel is engaged in the Swords of Iron War, in the north and in the south, following the surprise murderous attack by the Hamas terrorist organization on the communities near the Gaza Strip and the surrounding area on Simchat Torah (celebrating the completion and rebeginning of the reading of the Torah) October 7th, 2023. As I have previously announced, our office is conducting a comprehensive audit on the matters concerning the massacre on October 7th and the Swords of Iron War. In my opinion, it is a public and moral duty to conduct an audit on the manner in which all the echelons functioned on the day of the massacre, during the period preceding it and during the period following it. Alongside with the audit on the war, our office is continuing to conduct audits in other areas as well.

In recent years, and in particular during the course of the war, we are witnessing an increase in cyber-attacks against the State of Israel carried out by states and great powers to damage and disable organizations. The Israel National Cyber Directorate has estimated the costs of dealing with the cyber-attacks in Israel during 2024 at about NIS 12 billion.

When I first took office as the State Comptroller and Ombudsman, I identified and defined the field of cyber as one of the core subjects that the State Audit will deal with. This is with the aim of examining the preparedness and readiness of the audited bodies to deal with the significant risks in the cyberspace, the strategic threats and future cyber challenges. My office's audits in of cyber and information systems indicate the lack of relevant regulation in the cyber field, necessary to oblige organizations to take protection measures; the essential entities in the economy should be prepared to deal with attacks by states or great powers; and the decision makers within the government must be aware of the level of protection in the economy and its deficiencies. This report deals entirely with the results of the State Audit in the cyber and information systems protection. The chapters of the report are as follows:

- **The Government Risk Management in the ICT**
- **Cyber and Data Protection in the National Insurance Institute**
- **The IT Systems in the Israel Postal Company and the Postal Bank**
- **Cyber Protection: Aspects of Regulation and Protection of the Information and Computer Systems at Rafael Advanced Defense Systems Ltd.**

State of Israel

Report of the State Comptroller

Cyber and Information Systems

November 2024

Jerusalem | State Comptroller and Ombudsman