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 5

المقدمة 11

Foreword 112

ביקורות מערכתיות

ניהול סיכונים ממשלתי בתחום התקשוב 17

מדיניות פעם אחת - ביקורת מעקב 31

דואר ישראל

מערכות המידע בחברת דואר ישראל ובבנק הדואר 47

המוסד לביטוח לאומי

אבטחת המידע והגנת הסייבר במוסד לביטוח לאומי 59

פרויקט תבל לשדרוג מערך המחשוב במוסד לביטוח לאומי - ביקורת מעקב 69

תעשיות ביטחוניות ממשלתיות

הגנה בתחום הסייבר: היבטי אסדרה והגנה על המידע ומערכות המחשוב ברפאל מערכות לחימה מתקדמות בע"מ 81

דוח מיוחד

ההיערכות הלאומית בתחום הבינה המלאכותית 89

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

המקדמה

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 تنفيذ 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