



דוח מבקר המדינה - סייבר ומערכות מידע
אייר התשפ"ג | מאי 2023

המשרד לביטחון לאומי -
שירותי בתי הסוהר

טכנולוגיות דיגיטליות ואבטחת המידע והסייבר בשירות בתי הסוהר



טכנולוגיות דיגיטליות ואבטחת המידע והסייבר בשירות בתי הסוהר

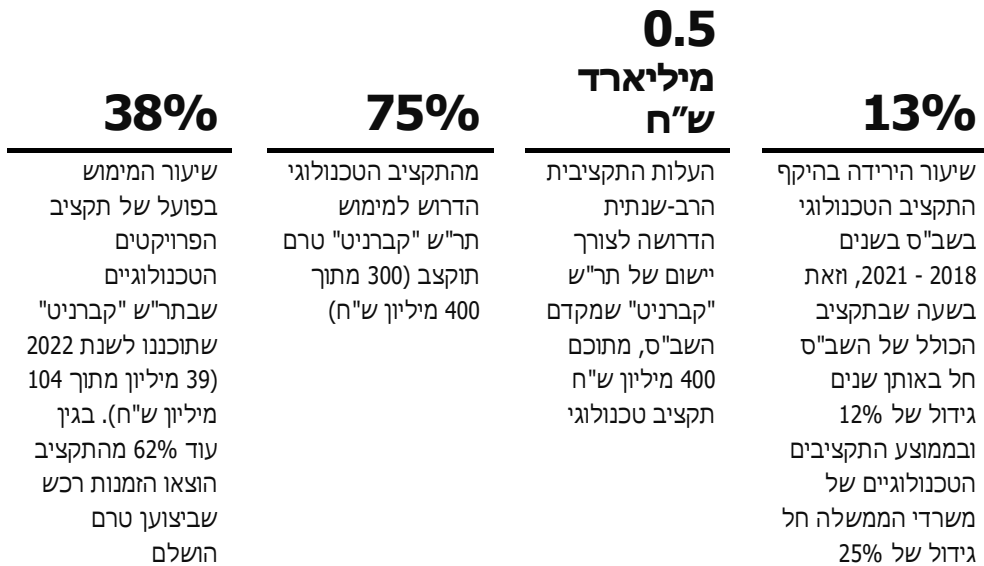
רקע

שירות בתי הסוהר (השב"ס) הוא ארגון הכליאה הלאומי, גוף ביטחוני הנכלל במערכת אכיפת החוק וכפוף למשרד לביטחון לאומי. השב"ס הוקם בשנת 1949 ובשנת 2006 הוכר כארגון הכליאה הלאומי של מדינת ישראל. השב"ס מחזיק במשמורתו כ-14,000 אסירים ועצורים פליליים, ביטחוניים ומינהליים (ועוד כ-5,200 אסירים ועצורים בחלופות מאסר ופיקוח באחריות השב"ס) לשם הגנה על שלום הציבור וביטחונו. נכון לתחילת שנת 2022 השב"ס מנהל 30 מתקני כליאה בפריסה ארצית (22 בתי סוהר ושמונה בתי מעצר), בחלוקה לשלושה מחוזות פיקוד - צפון, מרכז ודרום, ומעסיק 9,200 עובדים. תקציבו השנתי ל-2022 עמד על 4.6 מיליארד ש"ח.

במסגרת פעילותו של השב"ס למימוש יעדיו ניצבים לפניו אתגרים טכנולוגיים רבים וכדי להתמודד עם אתגרים אלה הוא מפעיל באמצעות החטיבה הטכנולוגית עשרות מערכות ארגוניות ממוחשבות: מערכות ליבה מבצעיות לניהול האסירים ולמודיעין; תחומי רפואה ושיקום; מערכות לניהול תחומי כוח האדם, ההדרכה והלוגיסטיקה; מערכות אבטחה מגוונות המותקנות במתקני הכליאה ומשמשות להגנה עליהם; מערכות אבטחת מידע והגנת הסייבר; ומערכות ממוחשבות בתחום התשתיות, לרבות חוות שרתים ואתר גיבוי. בשנים 2006 - 2014 קידם השב"ס פרויקט לפיתוח מערכת תקשוב ארגוני (פרויקט "קידמה") אשר נכשל והופסק לאחר שהושקעו בו 144 מיליון ש"ח. החל משנת 2021, בהובלת נציבת השב"ס וראש החטיבה הטכנולוגית, החל השב"ס בביצועו של מהלך אסטרטגי שנועד להוביל לקפיצת מדרגה טכנולוגית בשב"ס. מהלך אסטרטגי זה התבטא בגיבוש התוכנית הרב-שנתית "קברניט" (תר"ש "קברניט"), אשר יישומה החל בראשית שנת 2022. תוכנית זו היא תוכנית פעולה פנימית אשר נועדה, לדברי השב"ס, לעצב ולהוביל את דרכו החדשה של השב"ס כארגון ביטחוני מרכזי, חדשני ומתוחכם, ובין היתר, לבסס סביבת עבודה מתקדמת וחדשנית עבור הסגל תוך הגברת השימוש בטכנולוגיה, בדיגיטציה ובחדשנות.



נתוני מפתח



פעולות הביקורת

בחודשים מרץ-דצמבר 2022 בדק משרד מבקר המדינה את נושא טכנולוגיות דיגיטליות והגנת הסייבר בשב"ס. הביקורת כוללת שלושה נדבכים כלהלן:

1. טכנולוגיות דיגיטליות ומערכות המידע בשב"ס. במסגרת חלק זה נבדקו בין היתר תקציב תחום הטכנולוגיה והמשילות הטכנולוגית בשב"ס.
2. ביטחון מידע, אבטחת המידע והגנת הסייבר בשב"ס.
3. הרציפות התפקודית של המערכות הטכנולוגיות בשב"ס והשפעותיה על תפקוד בתי הסוהר בהתרחש אסון.

הביקורת נעשתה בנציבות השב"ס ובבתי סוהר שונים. ביקורת השלמה נעשו במשרד לביטחון לאומי, במערך הדיגיטל הלאומי במשרד הכלכלה והתעשייה, במערך הסייבר הלאומי (מס"ל) במשרד ראש הממשלה, באגף התקציבים במשרד האוצר ובשירות הביטחון הכללי (שב"כ). משרד מבקר המדינה ערך מבדקי חוסן במערכות השב"ס וממצאיו הועברו לגופים. משרד מבקר המדינה ערך בעבר ביקורות על היבטים שונים בפעילות השב"ס: "הקמת מערכת מידע בשירות בתי הסוהר - פרויקט קידמה"; "המערך הרפואי לטיפול בכלואים בשירות בתי הסוהר"; "מעצרים פליליים בישראל"; ו"שיקום אסירים בישראל". ממצאי הביקורות והמלצות המבקר פורסמו בכמה דוחות שנתיים.



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

חלק א' - טכנולוגיות דיגיטליות ומערכות מידע בשב"ס

תמונת המצב העולה מן הביקורת



הפקת לקחים מפרויקט קידמה - במהלך שמונה השנים מאז כישלון פרויקט קידמה, פרויקט תקשוב ארגוני שכשל לאחר שהושקעו בו 144 מיליון ש"ח, נציבות השב"ס והמשרד לבט"פ לא ביצעו תחקור בנושא נסיבות הכישלון ולא הפיקו לקחים שעשויים היו לשמש את השב"ס בבואו לנהל פרויקטי מחשוב עתידיים וטרם המימוש של פרויקט תקשוב ארגוני חדש בשנת 2022 - תר"ש "קברניט".



מערך התקשוב של השב"ס והמשילות הטכנולוגית - תמונת המצב של תחום טכנולוגיות המידע בשב"ס לאחר כישלון פרויקט קידמה התאפיין בשנים 2014 - 2021 בעיסוק מצומצם של הנהלת הארגון בנושא התקשוב. בשנים 2018 - 2021 חלה ירידה בהיקף התקציב הטכנולוגי בשב"ס (-13%) וזאת בשעה שבתקציב הכולל של השב"ס חל באותן שנים גידול של 12% ובממוצע התקציבים הטכנולוגיים של משרדי הממשלה חל גידול של 25%. תקופה זו התאפיינה באיוש חלקי של תפקידי ליבה (ראש החטיבה הטכנולוגית וראש מחלקת התקשוב בחטיבה). כמו כן נמצא פער טכנולוגי מהותי הנובע מתשתיות תקשוב חסרות שלא איפשרו מתן מענה לצרכים ולאתגרים התפקודיים של הארגון. בשל הפער הטכנולוגי הזה חלק גדול מהתהליכים בשגרת הניהול של בתי הסוהר נעשו באופן ידני; מערכות השליטה של הארגון לא סיפקו מענה לצרכים המבצעיים והניהוליים שלו; אמצעי זיהוי האסירים, מערך המצלמות והתשתית הטכנולוגית שעליה התבסס הארגון היו מיושנים. מצב זה פגע בתפקודו של השב"ס וביכולתו לעמוד ביעדיו.



אישור תר"ש "קברניט" ותקציבה - השב"ס החל ביישום תר"ש "קברניט" בלא שאושר תקציבה הכולל המסתכם בכחצי מיליארד ש"ח, ובלא שניתן אישור של המשרד לבט"פ והשר לבט"פ דאז למימושה המלא. עולה אפוא כי השב"ס החל ביישום תוכנית תקשובית מקיפה, שעה שניתן לה אישור תקציבי של כ-20% מהעלות התקציבית הכוללת של התכנית המסתכמת ב-532 מיליון ש"ח (מתוכם כ-400 מיליון ש"ח מרכיב טכנולוגי), וללא אישור הדרג הממונה לתכנית בכללותה. מצב זה מציב סיכון להשלמת התוכנית בשנים הבאות. השב"ס החליט להתחיל במימוש התר"ש על אף היעדר מקור תקציבי ובלא שמשרד האוצר והמשרד לבט"פ התחייבו להקצות לתוכנית את התקציב שיבטיח את מימושה.



מימוש תקציבי החטיבה הטכנולוגית בתר"ש "קברניט" ועמידה בלוחות הזמנים לשנת 2022 - נכון לסוף דצמבר 2022 השב"ס נמצא בפיגור במימוש הפרויקטים שבתר"ש "קברניט" שתוכננו לשנת 2022. נמצא כי במועד זה, מתוך תקציב של 104 מיליון ש"ח מומשו בפועל כ-39 מיליון ש"ח המהווים 38% בלבד מתקציב תר"ש "קברניט"; אשר לכ-63 מיליון ש"ח המהווים כ-62% מהתקציב הוצאו הזמנות רכש אך לא הושלמה המשימה. בחלוקה לפי פרויקטים נמצא כי מתוך 31 פרויקטים טכנולוגיים בתר"ש "קברניט" 24 פרויקטים מבוצעים כמתוכנן ו-7 פרויקטים נמצאים בפיגור בלוח הזמנים בין היתר, בשל אי-קבלת התקציב ממשד האוצר בעוד מועד. בין הפרויקטים העיקריים שביצועם מתעכב: פרויקט שכר וכוח אדם, חוות שרתים, תיק אסיר ממוחשב, היועדות חזותית עם בתי המשפט, מערכת שו"ב.

סקר סיכוני תקשוב - על אף המורכבות הטכנולוגית של תחום התקשוב בשב"ס, היקף מערכות המידע והממשקים שלהן עם גופים ממשלתיים, לא ביצע השב"ס מיפוי של נכסי המידע, מאגרי הנתונים, התשתיות והפרויקטים, וכן לא ביצע סקרי סיכונים שוטפים ומקיפים. עוד נמצא כי השב"ס לא ביצע ניהול סיכונים כולל בעניין תוכנית "קברניט" כדי להתמודד עם סיכונים מערכתיים בתחומי התקציב, לוחות הזמנים, ממשקים, תשתית, טכנולוגיה, כוח אדם, אבטחת מידע, הטמעה והתלות ההדדית בין מרכיבי התוכנית. מנהל סיכוני תקשוב ייעודי גויס רק בראשית שנת 2023.



השקעה בקידום טכנולוגי - לאחר תקופה ארוכה של קיפאון טכנולוגי, החל משנת 2021 משקיע השב"ס ובייחוד החטיבה הטכנולוגית מאמץ ניכר להשלמת פערי הטכנולוגיה באמצעות ייזום ומימוש פרויקטים לקידום הדיגיטציה בליבה המבצעית והניהולית של הארגון.

שינוי ארגוני ותוספת כוח אדם טכנולוגי - במסגרת תר"ש "קברניט" בוצע שינוי ארגוני בחטיבה הטכנולוגית. כמו כן בשנת 2022 הוחל בגיוס כוח אדם, והגיוס הושלם ברובו והוביל להכפלת כוח האדם בחטיבה, מ-100 ל-199 עובדי קבלן.

מימוש ושילוב טכנולוגיות במערכות הליבה המבצעיות - במהלך שנת 2022 ביצעה החטיבה הטכנולוגית, כחלק מתר"ש "קברניט", הטמעה של מערכות טכנולוגיות חדשות כגון יומנים דיגיטליים, תיק אסיר דיגיטלי ומערכות לניטור רב-ממדי כחלק מהמעבר ל"בית סוהר חכם".


עיקרי המלצות הביקורת


מוצע כי השב"ס יטמיע מתודולוגיה ארגונית של תחקור והפקת לקחים בעניין פרויקטי מחשב, ומומלץ שתהליך זה יתקיים גם בנוגע לתוכנית "קברניט" בכללותה, בהתחשב בעלותה ובמורכבותה. על המשרד לביטחון לאומי להיות מעורב בתהליכים אלו כגורם הממונה על השב"ס ומנחה אותו.

מומלץ כי המשרד לביטחון לאומי והשר הממונה יבחנו את תר"ש "קברניט" בכללותה לצורך אישורה לרבות התקציב הרב-שנתי למימושה. עוד מומלץ כי המשרד יקבע הסדר

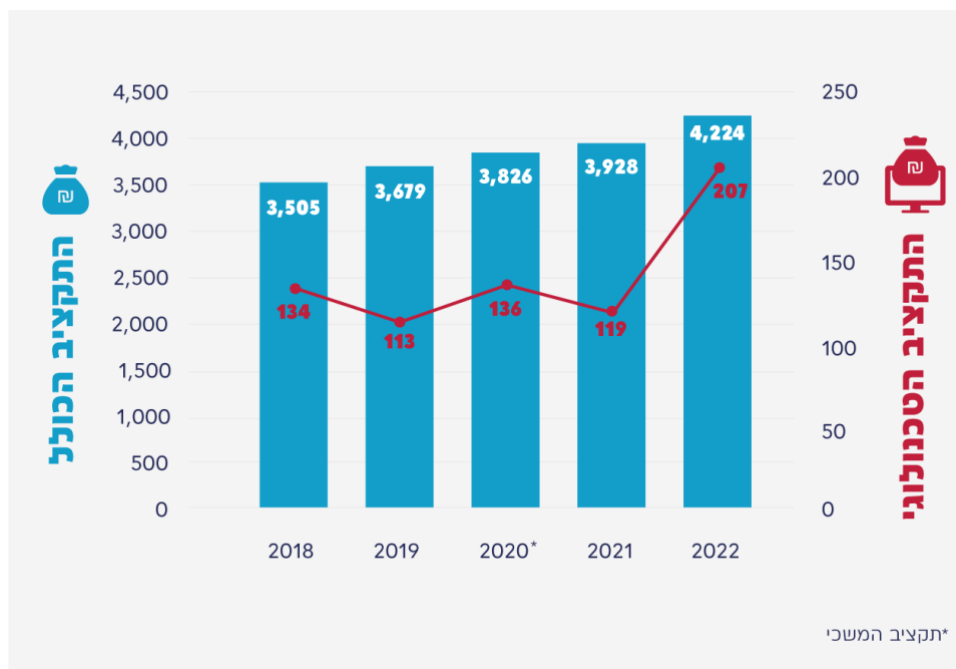


קבוע ושוטף לביצוע בקרה על יישום פרויקטי הליבה של התוכנית לרבות יעדיהם, תכולותיהם, לוחות הזמנים לביצועם והביצוע התקציבי שלהם. יישום תוכנית "קברניט", שהינה תוכנית רב-שנתית ועתירת משאבים, מחייב את השב"ס לפעול בנושא לאחר שקיבל אישור של המשרד לביטחון לאומי והשר לביטחון לאומי לתוכנית בכללותה.

על השב"ס ליישם את הנחיית מערך הדיגיטל הלאומי ולבצע סקר סיכונים מקיף ושוטף הנוגע לכלל פעילותו, ובכלל זה לתוכנית "קברניט" שבוצעה במועד הביקורת, ולהשלים את איוש המשרות בתחום ניהול הפרויקטים. 

מומלץ כי משרד האוצר יעביר תקציבי פיתוח מבעוד מועד ולא בסוף שנת התקציב, על מנת שגופים ממשלתיים ובכללם השב"ס יוכלו לנצל תקציבי פיתוח אלו ולהוציא הזמנות בגינם באותה שנה, מבלי שיושת עליהם קיצוץ תקציבי בשל היותם "עודפים מחוייבים". עוד מוצע למשרד האוצר, למשרד לביטחון לאומי ולשב"ס לבחון את מכלול המשמעויות של תקציב תר"ש "קברניט" ושל תקציב הטכנולוגיה של השב"ס, בהתחשב בין היתר באתגרי התקציב במועד הביקורת, כל זאת על מנת להבטיח את מימוש תר"ש "קברניט", לנוכח חשיבות השלמתה, כאמור. 

התקציב הטכנולוגי של השב"ס בהשוואה לתקציב הכולל של השב"ס על שינויו, 2018 - 2022 (במיליוני ש"ח)



על פי נתוני השב"ס ומשרד האוצר, בעיבוד משרד מבקר המדינה.



חלק ב' - ביטחון מידע, אבטחת המידע והגנת הסייבר בשב"ס

הממצאים בפרק ביקורת זה אינם מתפרסמים לציבור מטעמים של שמירה על ביטחון המדינה.

השב"ס, ארגון הכליאה הלאומי האמון על 30 מתקני כליאה, הוא גוף ביטחוני המחזיק במשמורת אלפי אסירים פלילים וביטחוניים. המידע על אסירים אלו, לרבות מידע ביטחוני מסווג ומידע אישי ורגיש בתחום הרפואי, הביומטרי והמודיעיני, מנוהל במערכות המידע של הארגון. נוסף על כך במחשבי השב"ס שמור מידע רב על שיטות פעולה, מבצעים, חקירות ומידע על מערכות ההגנה והביטחון בשב"ס. נוסף על המידע שמקורו בארגון, השב"ס מקבל מידע מסווג, מבצעי ומודיעיני מהמשטרה ומגורמים נוספים. חשיפתו של מידע זה לגורם שאינו מוסמך עלולה לגרום, בין היתר: לנזק למדינה; לסיכון חיי אדם; לחשיפת ידיעות, שיטות פעולה וחקירות חשאיות; ולהכשלת מבצעים.

בשנים האחרונות מסתמן גידול ניכר במספרם של אירועי סייבר המשבשים את פעילותם התקינה של ארגונים בארץ ובעולם. כמו כן מסתמנת עלייה ניכרת בחומרתם של אירועים אלה.

תמונת המצב העולה מן הביקורת

אסדרת ההנחיה המקצועית בתחום אבטחת המידע והסייבר



הגוף המנחה את השב"ס בתחום אבטחת מידע והגנת הסייבר - השב"ס הינו גוף ביטחוני ובמערכתיו מצוי מידע מסווג ברמות סיווג שונות. נמצא כי השב"ס, המשרד לבט"פ ומס"ל לא היו מודעים במהלך השנים לכללי השב"כ שנקבעו בשנת 2004 על ידי ראש הממשלה דאז, אשר הטילו על השב"ס את האחריות לקבוע לעצמו את דרכי אבטחת המידע המסווג בהתאם לעקרונות שהוגדרו. לפיכך בכל הנוגע לתחום המסווג, המגלם את הסיכון הגבוה ביותר, השב"ס לא פעל על פי הכללים המחייבים ולא הניח את הבסיס הנדרש לטיפול בתחום רגיש זה. כמו כן השב"ס לא קיבל ליווי והנחיה בתחום המסווג, זאת אף שבכל הנוגע לתחום הלא מסווג, המגלם סיכון נמוך יותר, הוא זכה לליווי ולהנחיה של היחידה המגזרית במשרד לבט"פ. כמו כן, על אף היותו של השב"ס גוף ביטחוני, ועל אף המידע הרגיש הנמצא ברשותו, ועדת ההיגוי העליונה להגנה על מערכות ממוחשבות (ועדת ב/84), לא דנה בעניין השב"ס ולא בחנה אם ראוי להגדירו גוף "חיוני" הזקוק להגנה קיברנטית.



מדיניות הגנת הסייבר - השב"ס היה מחויב לפרסם מדיניות הגנת סייבר ארגונית מכוח החלטת הממשלה בשנת 2015. עלה כי בתום הביקורת, בדצמבר 2022 אושרה המדיניות לפרסום בארגון על ידי סגן הנציבה כתורה נושאת ארגונית אך טרם אושרה על ידי היחידה המגזרית במשרד לביטחון לאומי. כמו כן, מסמך המדיניות המגזרית המאושרת, שאותו פרסם המשרד לבט"פ ואשר מיועד, בין היתר, להכווין ולהנחות את הגופים שתחת אחריותו



בהיבטי הגנת הסייבר, הוא חלקי ואינו כולל הנחיות מפורטות, המותאמות לנורמות מקובלות בתחום הגנת הסייבר, עבור הגופים שתחת אחריותו. החסר בהנחיות אלה פוגע ביכולת להבטיח מוכנות נאותה של השב"ס להתמודדות עם מתקפות סייבר.

ניהולו ואבטחתו של מידע ביטחוני מסווג - אחד העקרונות המנחים בכל הנוגע לאבטחת מידע ומסמכים מסווגים הוא שיש צורך ממשי באמצעי מידור ואבטחה כדי למנוע חשיפת מידע רגיש מהבחינה הביטחונית לפני גורם בלתי מוסמך. מידת הרגישות הביטחונית של המסמך נקבעת על פי רמת הסיווג שלו. ארבע רמות הסיווג הן: סודי ביותר, סודי, שמור ובלתי מסווג (להלן - בלמ"ס).

דוגמאות למידע ברשתות השב"ס





משרד מבקר המדינה בדק שורה של היבטים הנוגעים לניהולו ואבטחתו של מידע ביטחוני מסווג. בבדיקה זו הועלו פערים משמעותיים, העומדים בניגוד לפרקטיקה המחייבת בגופים מקבילים. פערים אלו נמצאו בכל אחד מהתחומים המפורטים להלן:

1. טיפול במידע דיגיטלי מסווג ובמסמכים מסווגים.
2. הסדרת הטיפול במידע ביטחוני מסווג באמצעות נוהלי אבטחה, שמירה וסיווג של מסמכים.
3. טיפול במידע מסווג המתקבל מגורמים חיצוניים.
4. הסדרת הסיווג הביטחוני של עובדים בשב"ס.
5. שימוש באמצעי תקשורת.

הגנה על מערכות ותשתיות תקשוב



משרד מבקר המדינה בדק שורה של היבטים הנוגעים להגנה על מערכות ותשתיות תקשוב בשב"ס. כמו כן בוצעו מבדקי חדירה בשילוב סקר הערכת פגיעויות בנוגע לרשתות בשב"ס. בבדיקה שבוצעה הועלו פערים משמעותיים, העומדים בניגוד לפרקטיקה המחייבת בגופים מקבילים. הפערים נמצאו בכל אחד מהתחומים המפורטים להלן:

1. הגנת הסייבר על חלק מהמערכות.
2. ביצוע סקרי סיכונים באבטחת מידע וסייבר וביצוע מבדקי חדירה.
3. היערכות לניהול אירועי סייבר.
4. ניהול משתמשים והרשאות.
5. תהליכי הפיתוח של רשת מחשב מסווגת.



יצוין לחיוב כי בשנים האחרונות בוצעה פעילות נרחבת במחלקת הגנת הסייבר בשב"ס ליישום ארכיטקטורה מאובטחת ופתרונות הגנה, זאת חרף המשאבים המצומצמים אשר עמדו לרשות השב"ס. פעילות זו הביאה לשיפור ניכר בתחום אבטחת המידע.

כמו כן, בכל אחת מהשנים 2021 - 2022 הקצה השב"ס לתחום הגנת הסייבר מעל 8% מסך תקציב טכנולוגיות המידע השנתי בארגון, ובכך עמד בשיעור המינימלי שנקבע בהחלטת הממשלה.



עיקרי המלצות הביקורת

פרק זה העלה פערים משמעותיים בניהולו של מידע ביטחוני מסווג ואבטחתו במערכות המחשוב של השב"ס. כמו כן, הדוח חושף מציאות רבת שנים לפיה תחומי האחריות והסמכות של השב"ס ושל הרגולטורים בתחום אבטחת המידע המסווג והסייבר, ובתחום טכנולוגיות דיגיטליות ומערכות מידע אינם מיושמים, הלכה למעשה, באופן תקין וכנדרש. מומלץ כי ראש הממשלה בהתייעצות עם השר לביטחון לאומי יבחנו את סוגיית אבטחת המידע והסייבר בשב"ס בכללותה ובפרט את סוגיית אבטחת המידע המסווג. עד להכרעת ראש הממשלה נדרש כי השב"ס יפעל בהתאם לכללי השב"כ.

תחומי הפערים העיקריים בתחום ביטחון המידע, אבטחת המידע והגנת הסייבר



על פי ממצאי הביקורת, בעיבוד משרד מבקר המדינה.









חלק ג' - הרציפות התפקודית של המערכות הטכנולוגיות בשב"ס והשפעותיה על תפקוד בתי הסוהר בהתרחש אסון

הממצאים בפרק ביקורת זה אינם מתפרסמים לציבור מטעמים של שמירה על ביטחון המדינה.

הרציפות התפקודית של השב"ס במגוון תהליכים ניהוליים ומבצעיים קריטיים, ובהם אבטחת בתי הסוהר, על כל רבדיה, ובכלל זה ניהול מערך המודיעין, ניהול שגרת היום-יום בבית הסוהר לרבות ספירת האסירים, חלוקת תרופות לאסירים, ניהול כוח אדם, תלויה במערכות הטכנולוגיות. רציפות זו עלולה להיפגע מאסון או ממשבר חמור, בין שמדובר במשבר שלעיתים ניתן לצפות אותו (כדוגמת סופה עזה או מזג אוויר קיצוני), ובין שמדובר במשבר לא צפוי (כדוגמת הפסקת חשמל, רעידת אדמה, אירוע טרור, מלחמה או תאונה) המשבש את מהלך הפעילות הרגיל של הארגון. אירועים אלו עלולים גם לפגוע פגיעה חמורה במערך הטכנולוגי של הארגון וליצור בו כשלים. פגיעה חמורה במערך הטכנולוגי יכולה להיווצר גם מפגיעה פיזית (בתום לב או בזדון) או מהתקפות סייבר על תשתיות ומערכות טכנולוגיות של הארגון. מאחר שהשב"ס נדרש להמשיך להחזיק אסירים במשמורת בטוחה גם בעת אירוע חירום או אסון, עליו להיות ערוך ומוכן למצבי החירום השונים ולתת מענה של רציפות תפקודית בכל תנאי.

האסונות המרכזיים שבבסיס איום הייחוס של שב"ס

 <p>רעידת אדמה</p>	 <p>תקיפת סייבר</p>	 <p>מלחמה</p>
 <p>דליפת חומרים כימיים</p>	 <p>שיטפון</p>	 <p>הפסקת חשמל</p>



תמונת המצב העולה מן הביקורת




משרד מבקר המדינה בדק שורה ארוכה של היבטים העוסקים ברציפות התפקודית של המערכות הטכנולוגיות בשב"ס והשפעותיהם על תפקוד בתי הסוהר בהתרחש אסון. בבדיקה זו הועלו פערים משמעותיים, העומדים בניגוד לפרקטיקה המקובלת לעניין זה. הפערים נמצאו בכל אחד מהתחומים המפורטים להלן:

1. המענה הטכנולוגי לאיום הייחוס.
2. תוכנית ההמשכיות העסקית והרציפות התפקודית בשב"ס.
3. תוכנית התאוששות מאסון של השב"ס.
4. הגנה על אתר רגיש של השב"ס ותפעולו.
5. שיחזור נתונים ומערכות מידע מגיבוי.
6. הרציפות התפקודית של בתי הסוהר.



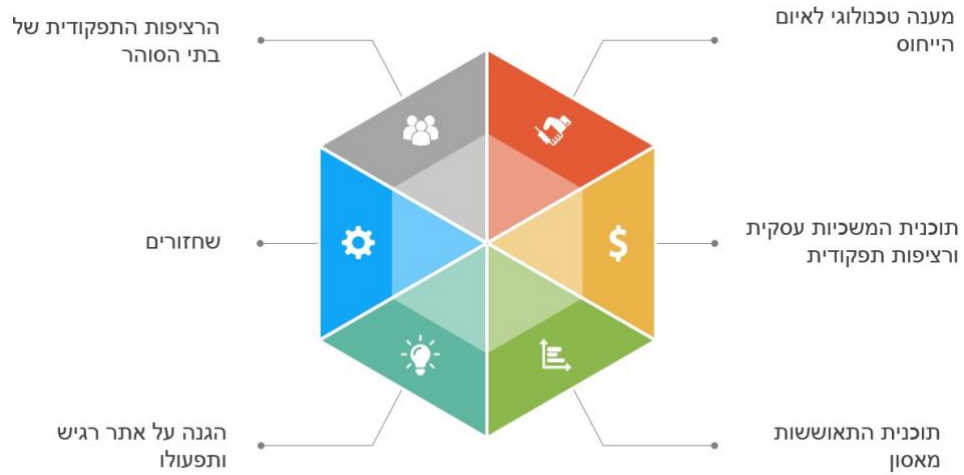
יצוין לחיוב המאמץ שנעשה בשב"ס לקדם ולתעדף את הקמת חוות השרתים החדשות.

עיקרי המלצות הביקורת

לרציפות התפקודית של השב"ס יש חשיבות אסטרטגית הן בהיבט חיי אדם של האסירים המוחזקים במשמורתו והסוהרים האמונים על שמירתם והן בהיבט הביטחוני והחברתי. על השב"ס והמשרד לביטחון לאומי לפעול לתיקון הפערים שהועלו בפרק זה וליישם את ההמלצות המפורטות כל זאת על מנת להבטיח שרציפות זו לא תיפגע בקרות אירועי אסון העלולים לסכן את יציבותו ותפקודו של מערך הכליאה הלאומי. 



תחומי הפערים העיקריים בתחום הרציפות התפקודית של המערכות הטכנולוגיות בשב"ס והשפעותיה על תפקוד בתי הסוהר בהתרחש אסון



על פי ממצאי הביקורת, בעיבוד משרד מבקר המדינה.



סיכום

תפקידו של השב"ס לספק משמורת בטוחה של אסירים ועצורים פליליים וביטחוניים, וזאת בתנאים נאותים תוך שמירה על כבודם ולצד שיקומם לקראת ההשתלבות בחברה לאחר שחרורם. מערכות טכנולוגיות מתקדמות תומכות במערכי כליאה הפועלים בעולם למימוש ייעודם של ארגונים אלו. תפקידו של השב"ס, מימוש ייעודו ואופיו הביטחוני מחייבים אותו, בדומה לגופי כליאה בעולם, לעשות שימוש במערכות טכנולוגיות מתקדמות.

תמונת המצב של תחום טכנולוגיות המידע בשב"ס התאפיינה בעיסוק מצומצם של הנהלת הארגון בנושא, בתקצוב טכנולוגי בשיעור נמוך, באיזש חלקי של תפקידי ליבה ובפער טכנולוגי מהותי. מצב זה פגע בתפקודו של השב"ס וביכולתו לעמוד ביעדיו. בשלהי שנת 2021, נמצא השב"ס בפיגור טכנולוגי מהותי וזאת בניגוד לתמורות הגלומות באמצעים טכנולוגיים ככלי לשיפור תפקודו השוטף הן בפן המינהלי והן בפן המבצעי. בשנת 2022 חלו שינויים אשר מטרם לאפשר לארגון לצמצם את הפערים ולבצע קפיצת מדרגה טכנולוגית. השב"ס בראשות הנציבה אימץ תוכנית מקיפה רב-שנתית לשיפור המערך הטכנולוגי ואף החל ביישומה בשנת 2022 תוך קבלת גיבוי תקציבי חלקי מהמשרד לבט"פ וממשרד האוצר. אולם, התוכנית המוגדרת כתוכנית רב-שנתית לא קיבלה את אישור השר לבט"פ דאז, ותקצבה רק לשנתה הראשונה מבלי שניתנה התחייבות של משרד האוצר והמשרד לבט"פ להמשך תקצובה בשנים הבאות ולהבטחת מימושה המלא.

המשרד לביטחון לאומי והשר העומד בראשו נושאים באחריות לתפקוד מערך הכליאה בישראל ובמסגרת זו עליהם להבטיח כי השב"ס ממלא תפקידו באמצעות תשתית טכנולוגית מתאימה וכי בניין הכוח בתחום זה מנוהל בראייה ארוכת טווח ובמתווה תקציבי המבטיח את מימושו. על השב"ס בשיתוף המשרד לביטחון לאומי ומשרד האוצר להמשיך לפעול יחד לצמצום הפערים הטכנולוגיים הקיימים ולהציב את השב"ס ברמה טכנולוגית מתקדמת התואמת את אחריותו וייעודו כארגון ביטחוני. על השב"ס לבצע תהליך סדור להפקת לקחים מכישלונות העבר בתחום זה, לנהל את סיכוני התקשוב בכלל ובת"ר"ש "קברניט" בפרט, ולהעמיד סביבה ניהולית מקצועית תומכת למימושו.

דוח זה גם מעלה פערים חמורים בניהולו של מידע ביטחוני מסווג ואבטחתו במערכות המחשוב של השב"ס. על אף היות השב"ס גוף ביטחוני, התשתית המיחשובית אינה תואמת את הסטנדרטים המחויבים בגופי ביטחון. הדוח חושף מציאות רבת שנים ולפיה תחומי האחריות והסמכות של השב"ס ושל הרגולטורים בתחום אבטחת המידע המסווג והסייבר, ובתחום טכנולוגיות דיגיטליות ומערכות מידע אינם מיושמים, הלכה למעשה, באופן תקין וכנדרש. דוח זה מהווה תמרור אזהרה לכלל הגופים המעורבים בתחום אבטחת סודות מדינה, אבטחת מידע והגנת הסייבר, ומחייב פעולות מהירות לתיקון הפערים שעלו בדוח זה. מומלץ כי ראש הממשלה בהתייעצות עם השר לביטחון לאומי יבחנו את סוגיית אבטחת המידע והסייבר בשב"ס בכללותה ובפרט את סוגיית אבטחת המידע המסווג. עד להכרעת ראש הממשלה נדרש כי השב"ס יפעל בהתאם לכללי השב"כ.

לרציפות התפקודית של השב"ס יש חשיבות אסטרטגית הן בהיבט חיי אדם של האסירים המוחזקים במשמורתו והסוהרים האמונים על שמירתם והן בהיבט הביטחוני והחברתי. על



השב"ס והמשרד לביטחון לאומי לוודא שרציפות זו לא תיפגע בקרות אירועי אסון העלולים לסכן את יציבותו ותפקודו של מערך הכליאה הלאומי.

דוח זה העוסק בשב"ס, מומלץ שיילמד ושיופקו ממנו לקחים לגופים נוספים במערכת הממשלתית הנושאים אופי דומה בכל הקשור לביטחון מידע, אבטחת מידע וסייבר וכן בהיבטי רציפות תפקודית של המערכות הטכנולוגיות ומוכנות לאסון.

