הכנסת
מרכז המחקר והמידע

י' באדר תשע"ז, 8 במרס 2017

הסדרת האחריות להגנת הסייבר בממשלה ובגופים הציבוריים

לקראת ישיבת ועדת המדע והטכנולוגיה של הכנסת, בנושא "הגנת הסייבר במרחב הממשלתי", יוצג להלן בקצרה מידע על הטיפול הממשלתי בנושא הגנת הסייבר. יצוין כי נושא הגנת הסייבר נידון לא אחת בוועדת המדע והטכנולוגיה של הכנסת.[1]

רקע[2]

אין כיום הגדרה בינלאומית אחת מקובלת ל"מרחב הסייבר" (Cyber space) . למרות הנטייה ליצור זהות בין "המרחב המקוון" ו"מרחב הסייבר", מרחב הסייבר איננו רק האינטרנט, וכולל בתוכו לא רק חומרה תוכנה ומערכות מידע אלא גם את בני אדם והאינטראקציות החברתיות שהם מבצעים באמצעות מערכות אלה.

מרחב הסייבר הוא חלק אינטגרלי מכל אחת מזירות החיים שלנו. כמעט כל שירות ציבורי ופרטי שאנו מכירים תלוי ו/או עושה שימוש במחשוב, תקשורת מחשבים ומערכות מידע ממוחשבות: שירותי הטלפוניה, התקשורת במדיות השונות, מערכות הפיננסים והבנקאות, התחבורה; תשתיות המים והחשמל ועוד. לצד היתרונות והייעול שמאפשרות המערכות הממוחשבות, הן יצרו גם איום חדש שמידת החשיפה לו גדלה ככל שההתפתחות הטכנולוגית גדולה יותר. לאיום הסייבר פנים שונות בתוכן: פשיעת סייבר, טרור סייבר, ריגול סייבר ולוחמת סייבר.

החוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998 קובע סמכויות ואחריות לאבטחה פיזית, אבטחת מידע ואבטחת מערכות מחשוב חיוניות של גופים ציבוריים שונים בתוכם הן גופי ממשלה והן גופים בבעלות פרטית.

הגדרת דפוסי הפעולה והסמכויות להגנה הסייבר של ישראל בדגש על תשתיות חיוניות, נקבעו בהחלטת ממשלה ב/84 משנת 2002 תחת הכותרת "אחריות להגנה על מערכות ממוחשבות במדינת ישראל" של ועדת השרים לענייני ביטחון לאומי. בהחלטה נקבע כי יש להקים ועדת היגוי עליונה שתפקידה לבחון אילו גופים מוגדרים כ"חיוניים" ולכן זקוקים להגנה קיברנטית. הגנה זו תסופק – כך על פי ההחלטה דאז, באמצעות יחידה ייעודית של שירות הביטחון הכללי – הרשות לאבטחת מידע (רא"מ).

מאז שנת 2011 קיבלה הממשלה מספר החלטות בנושא הסייבר ובשנת 2016 אף תוקן החוק להסדרת הביטחון בגופים ציבוריים באופן המשקף את כניסתו של מערך הסייבר הלאומי (המטה, ולעניין זה בעיקר - רשות הסייבר) לפעילות בתחומי ההגנה על הסייבר האזרחי.

[1] ועדת המדע והטכנולוגיה של הכנסת, "היערכות ישראל למתקפת סייבר וחשיבות ההגנה על תשתיות לאומיות", 20 ביולי 2015; "קידום ישראל כמובילה בתחום הסייבר", 13 במאי 2013, ועוד.

[2] מרכז המחקר והמידע של הכנסת, "המרחב הקיברנטי וההגנה על תשתיות חיוניות", רועי גולדשמידט, 12 במאי 2013.

להלן יוצגו בקצרה החלטות הממשלה בנושא, התיקון לחוק, סטאטוס יישום של עיקרי ההחלטות וסוגיות נוספות לדיון.

1. החלטות ממשלה

- **באוגוסט 2011 בעקבות המלצות של המועצה הלאומית למחקר ופיתוח (מולמו"פ), נתקבלה החלטת הממשלה על "קידום היכולת הלאומית במרחב הקיברנטי".** בין מטרותיה: קידום היכולת הלאומית במרחב הקיברנטי; שיפור ההתמודדות עם האתגרים במרחב הקיברנטי; שיפור ההגנה על תשתיות לאומיות חיוניות, קידום מעמדה של ישראל כמרכז לפיתוח טכנולוגיות מידע ועוד.

על בסיס החלטת הממשלה הוקם בראשית שנת 2012 "מטה הסייבר הלאומי". ייעודו של מטה הסייבר להמליץ לממשלה ולוועדותיה על מדיניות לאומית בתחום הקיברנטי ולפעול ליישומה של מדיניות זו. המטה פועל לקידום היכולת הלאומית במרחב הקיברנטי ולשיפור ההתמודדות עם האתגרים במרחב זה, בהם: הגנה על תשתיות חיוניות וקידומה של ישראל כמובילה במו"פ בתחום.[3]

- **בפברואר 2015 החליטה הממשלה להקים "רשות לאומית להגנת הסייבר".** על פי ההחלטה, מטה הסייבר והרשות יהוו יחד את **"מערך הסייבר הלאומי"** שבראשו יעמוד ראש מטה הסייבר. והן יוקמו כיחידות סמך עצמאיות תחת משרד ראש הממשלה.[4]

החלטת הממשלה על הקמת רשות הסייבר מפורטת וכוללת אלמנטים רבים שרק חלקם יוצגו להלן. תפקידי הרשות על פי ההחלטה כוללים בין השאר:

- לנהל להפעיל ולבצע את כלל מאמצי ההגנה האופרטיביים ברמה הלאומית במרחב הסייבר.
- להפעיל מרכז לסיוע בהתמודדות עם איומי סייבר (Cyber Event Readiness Team - CERT) עבור כלל המשק.
- חיזוק החוסן של כלל המשק בסייבר באמצעות היערכות, כשירות ואסדרה.

על מטה הסייבר הוטלה בהחלטה האחריות להקים את רשות הסייבר במתווה תלת שנתי בשנים 2015- 2017. בנוסף, הוטל על המטה להציג לראש הממשלה בתיאום עם ראש המטה לביטחון לאומי, מתווה להעברת הטיפול ב"אבטחת מערכות ממוחשבות חיוניות" משירות הביטחון הכללי לרשות הסייבר.

עוד נקבע בהחלטת הממשלה כי תוקם ועדת היגוי להגנה על מערכות ממוחשבות חיוניות שבין תפקידיה לקבוע אילו גופים יוגדרו כגופים חיוניים בהיבט של מערכות המחשוב שלהם ומתוקף החלטה זו תחת אילו מנגנוני הנחייה יופעלו.

על פי החלטת הממשלה בעניין **היה על מטה הסייבר והלשכה המשפטית במשרד ראש הממשלה בשיתוף עם משרד המשפטים להכין "תזכיר חוק הגנת הסייבר"** ולהביאו לאישור ראש הממשלה בתוך חצי שנה ממועד החלטת הממשלה.

---

[3] החלטת ממשלה מס' 3611, "קידום היכולת הלאומית במרחב הקיברנטי", 7 באוגוסט 2011.

[4] החלטת ממשלה מס' 2444, "קידום ההיערכות הלאומית להגנת הסייבר", 15 בפברואר 2015.

- **בפברואר 2015 החליטה הממשלה על "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר".**[5] בהחלטה נקבע בין השאר כי כחלק מרשות הסייבר תוקם **יחידה להסדרת שוק שירותי סייבר** שבין תפקידיה יהיה: קידום סטנדרטים של אנשי מקצוע; הכשרות, הסמכות והגדרת תחומי ידע נדרשים; יצירת ותפעול של מנגנון לאישור מוצרי הגנת סייבר ועוד.

כמו כן על פי ההחלטה ימונה על ידי המנכ"לים במשרדי הממשלה "ממונה הגנת סייבר" בכל משרד; כחלק מיחידת מערכות המידע במשרד ימונה "מנהל הגנת סייבר" ותוקם ועדת היגוי משרדית לנושא. בנוסף, יוקצה תקציב ייעודי לנושא הסייבר בשיעור שלא יפחת מ-8% מן התקציב שנקבע לתחום טכנולוגיית המידע במשרד, למעט באישור בנסיבות מיוחדות.

החלטת הממשלה כוללת גם הקמתן של עוד שתי מסגרות ארגוניות: **יחידה להגנת הסייבר בממשלה (יה"ב)** שמטרתה לספק הנחיה והכוונה ממשלתית בתחומי הגנת הסייבר עבור כלל משרדי הממשלה ויחידות הסמך; והקמתן של **יחידות להכוונה מקצועית מגזרית בתחום הגנת הסייבר במשרדי הממשלה** שמטרתן לספק הכוונה והנחיה מקצועית בתחום הגנת הסייבר בהתאם לסמכויות הרגולציה של המשרד או במסגרתו. על פי החלטת הממשלה הוטל על מטה הסייבר לסווג את הרגולטורים השונים בממשלה על פי סמכויותיהם והמגזר שבו הם פועלים ובהתאמה לקבוע את כוח האדם וגודל היחידה להכוונה מקצועית מגזרית הדרוש להם.[6]

לדברי ראש יה"ב ונציג ראש מערך הסייבר, יה"ב והיחידות להכוונה מגזרית פועלות בזירות שונות: בעוד יה"ב פועלת בהנחיה של משרדי הממשלה ויחידות הסמך שלה בפעילות הממשלתית הפנימית, הרי שהיחידות להכוונה מקצועית מגזרית פועלות להנחיית המשק האזרחי, כל אחת בתחום אחריותה לפי תחום פעילות המשרד או הרגולטור המגזרי.[7]

עוד נקבע בהחלטה, כי יוקם **מרכז שליטה ובקרה ממשלתי למול איומי סייבר** (SOC- Security Operation Center). מרכז השליטה והבקרה יוקם על פי ההחלטה על ידי מטה הסייבר והיחידה להגנת סייבר בממשלה - יה"ב.[8]

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

החוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998 קובע סמכויות ואחריות לאבטחה פיזית, אבטחת מידע ואבטחת מערכות מחשוב חיוניות[9] של גופים ציבוריים שונים בתוכם הן גופי ממשלה והן גופים בבעלות פרטית. (החוק מגדיר גוף ציבורי כך: "כל גוף המנוי בתוספות, ולגבי משרד ממשלתי המנוי בתוספות – לרבות יחידת הסמך שלו).

החוק תוקן לאחרונה בצורה מהותית בשנת 2016 ועיקרו של התיקון לחוק כלל למעשה את העברת האחריות לטיפול באבטחת מערכות ממוחשבות חיוניות של גופים אזרחיים מאחריות שירות הביטחון הכללי לאחריות הרשות הלאומית להגנת סייבר. לצורך העניין נוספה לחוק התוספת החמישית המפרטת גופים המונחים כאמור על ידי הרשות ביחס לאבטחת מערכות ממוחשבות חיוניות, והוצאתם של גופים

---

[5] החלטת ממשלה מס' 2443, "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר", 15 בפברואר 2015.

[6] שם.

[7] גדעון קונפינו, ראש היחידה להגנת הסייבר בממשלה, מכתב תשובה לפניית מרכז המחקר והמידע של הכנסת, 5 במרס 2017. אמרי קוזק, יועץ בכיר לראש מערך הסייבר הלאומי, מכתב תשובה לפניית מרכז המחקר והמידע של הכנסת, 7 במרס 2017.

[8] החלטת ממשלה מס' 2443, "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר", 15 בפברואר 2015.

[9] ההבחנה בין אבטחת מידע לאבטחת מערכות מחשוב חיוניות נועדה לענות על מקרים בהם המערכת איננה מערכת מידע אך היא מערכת מחשוב חיונית, לדוגמא מערכת מחשוב שמווסתת את תפעול שאיבת הגז או ייצור החשמל. עו"ד עידו בן יצחק, הלשכה המשפטית של הכנסת, פגישה, 5 במרס 2017.

אלה מן התוספת הרביעית. בהתאם לצו מתוקף החוק, מה-1 במארס 2017 הועברו לאחריות הרשות 11 גופים ציבוריים.[10] עם זאת, חברות תקשורת נותרו בתוספת הרביעית ואבטחת מערכות ממוחשבות חיוניות בחברות התקשורת נותרה תחת אחריות השב"כ.

יצוין, כי החוק איננו מגדיר מהן מערכות ממוחשבות חיוניות למעט באמירה כי המדובר ב"מערכות ממוחשבות שנקבעו כחיוניות על ידי הגוף שהסמיכה לכך הממשלה".[11]

החוק קובע בין השאר נושאים אלה: חובה למנות "ממונה ביטחון" בגופים האמורים; סמכויותיו של ממונה הביטחון; כפיפותו של הממונה לקצין מוסמך – נציג השב"כ, המשטרה, או הרשות הלאומית להגנת סייבר בהתאם לגוף הנידון; סמכותו של הקצין לתת הנחיות מקצועיות בנושאי אבטחה, אבטחת מידע ואבטחת מערכות מחשוב חיוניות; והכללים לערעור על ההנחיות המקצועיות.

לחוק חמש תוספות:

- **בתוספת הראשונה מנויים גופים שמונחים הן ביחס לאבטחתם הפיזית והן ביחס לאבטחת המידע שלהם בידי השב"כ**: משרד ראש הממשלה; משרד הביטחון; מפעלי מערכת הביטחון;[12] לשכת נשיא המדינה ומשרד החוץ.

  בהיבטים מסוימים של פעולתם מונחים גם: רשות שדות התעופה; חברות נמל[13]; חברות תעופה; חברות ספנות; גוף המפעיל מסוף מטענים מוטסים מישראל; מינהלת המעברים שבמשרד הביטחון.

- **בתוספת השנייה מנויים גופים שמונחים על ידי המשטרה ביחס לאבטחה פיזית ובידי השב"כ ביחס לאבטחת מידע**: משרדי ממשלה שלא מנויים בתוספת הראשונה; הסוכנות היהודית; רשות השידור; הרשות השנייה לטלוויזיה ורדיו; בנק ישראל; מקורות; חברת החשמל; בזק, החברה הישראלית לתקשורת בע"מ, חברת פלאפון תקשורת בע"מ, חברת סלקום ישראל בע"מ, חברת פרטנר תקשורת בע"מ, בזק בינלאומי, ברק אי.טי.סי (1955), החברה לשירותי בזק בינלאומיים, קווי זהב שירותי תקשורת בינלאומיים בע"מ, חברת מירס תקשורת בע"מ, וכן בעל רישיון כאמור בסעיף 13 לחוק התקשורת (בזק ושידורים), התשמ"ב-1982, אשר ניתנו לגביו הוראות כאמור בסעיף 13(ב) לחוק האמור; דואר ישראל; פי גלילות מסופי נפט וצינורות; קצא"א; חברת תשתיות נפט ואנרגיה; חברת בתי זיקוק לנפט; חברת פז בית זיקוק אשדוד; המוסד לביטוח לאומי; רשות מקרקעי ישראל; המרכז למיפוי ישראל; חברת רכבת ישראל; חברת נתיבי הגז הטבעי לישראל.

  בהיבטים מסוימים של פעולתם מונחים גם: רשות שדות התעופה; חברות נמל; חברות תעופה; חברות ספנות; גוף המפעיל מסוף מטענים מוטסים מישראל; מינהלת המעברים שבמשרד הביטחון; חברת נמלי ישראל.

---

[10] הגופים המנויים בצו: משרד האוצר; רשות האוכלוסין וההגירה; הרשות לניהול המאגר הביומטרי; רשות התקשוב הממשלתי-מערך ממשל זמין; מגן דוד אדום; מקורות חברת מים; נתיבי הגז הטבעי לישראל, רכבת ישראל, תשתיות נפט ואנרגיה, דנים וחומרים כימיים והלשכה המרכזית לסטטיסטיקה. בנוסף, על פי הצו, אמורה חברת החשמל לעבור גם כן לאחריות הרשות ב- 20 באפריל 2017.

צו להסדרת הביטחון בגופים ציבוריים (הוראת שעה) (קצין מוסמך לעניין גוף המנוי בתוספת החמישית לחוק), התשע"ז – 2016, מיום ה-25 בדצמבר 2016 פורסם ברשומות בקובץ התקנות 7750 מיום ה-29 בדצמבר 2016.

[11] על פי החלטת הממשלה מס' 2444, ועדת ההיגוי להגנה על מערכות ממוחשבות חיוניות – היא הגוף הממונה על ידי הממשלה להחליט אילו מערכות יוגדרו כך.

[12] הלכה למעשה שלושת הגופים האלה מוחרגים מאחריות השב"כ בהתאם לאפשרות הקבועה בחוק בסעיפים 21 ו-21 א. כאמור לעיל משרד הביטחון מונחה על יד המלמ"ב; המוסד וצה"ל עצמאיים כל אחד בתחומי פעולתו בהיבטים הקיברנטיים.

[13] בהתאם להגדרתם בחוק רשות הספנות והנמלים- התשס"ד 2004.

עם זאת, גופים המנויים גם בתוספת השנייה וגם בתוספת החמישית מונחים ביחס לאבטחת מידע בידי הרשות הלאומית להגנת הסייבר.[14]

- **בתוספת השלישית מנויים גופים המונחים רק בהיבט של אבטחה פיזית - על ידי המשטרה:** הקרן הקיימת לישראל; רשות העתיקות; רשות לשמירת הטבע והגנים הלאומיים; האוניברסיטה העברית; אוניברסיטת תל-אביב; אוניברסיטת חיפה; הטכניון; מכון וייצמן; אוניברסיטת בר-אילן; אוניברסיטת בן-גוריון; המרכז הארצי לפיתוח המקומות הקדושים. רשויות מקומיות – לעניין "אבטחת אישיות מאוימת" לפי סעיף 341א לפקודת העיריות וחברת נת"ע, נתיבי תחבורה עירוניים.

- **בתוספת הרביעית מנויים גופים המונחים בידי השב"כ בהיבט של אבטחת מערכות ממוחשבות חיוניות:** בזק החברה הישראלית לתקשורת; חברת מדיטרניאן נאוטילוס (ישראל); פלאפון תקשורת; סלקום ישראל; פרטנר תקשורת; 012 סמייל טלקום; 013 נטוויזין; בזק בינלאומי; הוט טלקום; מירס תקשורת.

- **בתוספת החמישית מנויים גופים המונחים על ידי הרשות הלאומית להגנת סייבר בהיבטי אבטחת מערכות ממוחשבות חיוניות:** משרד האוצר; רשות האוכלוסין וההגירה; הרשות לניהול המאגר הביומטרי; רשות התקשוב הממשלתי- מערך ממשל זמין; בנק ישראל; חברת בתי זיקוק לנפט; חברת פז בית זיקוק אשדוד; חברת החשמל לישראל; חברת קו צינור אילת אשקלון; מגן דוד אדום; מקורות חברת מים; נתיבי הגז הטבעי לישראל; רכבת ישראל; רשות שדות התעופה; תשתיות נפט ואנרגיה; הבורסה לניירות ערך; חיפה כימיקלים; דשנים וחומרים כימיים; בעלי החזקות כמשמעותן בחוק הנפט, התשי"ב-1952: I/10 "אשקלון", I/12 "תמר", I/13 "דלית", I/7, "נועה", I/14 "לוויתן צפון", I/15 "לוויתן דרום", לעניין המערכות הממוחשבות החיוניות המופעלות בקשר לחזקות אלה; חברת נמל אשדוד וחברת נמל חיפה; הלשכה המרכזית לסטטיסטיקה; חברת נת"ע, נתיבי תחבורה עירוניים.

3. דוח ועדת החוץ והביטחון של הכנסת בנושא בחינת חלוקת האחריות והסמכות בנושא הגנת הסייבר בישראל

באוגוסט 2016 פרסמה ועדת החוץ והביטחון של הכנסת דוח לא מסווג בנושא "בחינת חלוקת האחריות והסמכות בנושא הגנת הסייבר בישראל". להלן יוצגו בקצרה כמה סוגיות העולות מן הדוח שנכתב בעקבות דיונים של ועדת המשנה של ועדת החוץ והביטחון לנושא הגנה בסייבר.

- על פי הדוח הקמת הרשות הלאומית להגנת הסייבר "באה למלא חלל באזורים שלא טופלו עד היום, בעיקר במרחב האזרחי, ולשפר את התיאום בין כלל גורמי הסייבר". **למרות שהחלטת הממשלה קבעה כי לא תהיה פגיעה באחריות ובסמכות של השב"כ, כניסתה של הרשות "נוגסת" בתחומי האחריות והסמכות של השב"כ ומחייבת הסדרה, הן מערכתית והן מול כל אחד מגופי ההגנה בנפרד.**

[14] על פי סעיף 22 ב. לחוק, ההנחיה נעשית על ידי הרשות הלאומית להגנת הסייבר אך בהתאם לעקרונות של השב"כ (עד רמת סיווג "שמור"); ובהתאם להוראות של השב"כ (ברמת סיווג גבוהה משמור).

- מדוח הוועדה עולה כי בין חלק מן הגופים העוסקים בנושא הסייבר, בפרט רשות הסייבר והשב"כ נתגלעו מחלוקות מהותיות ביחס לדפוסי הטיפול בנושא שהגיעו עד לכדי היעדר שיתוף פעולה וחרמות הדדיות. עם זאת, לפי הדוח מאז גיבושו של מסמך הבנות בין הרשות לשב"כ ביוני 2016 חל שיפור בשיתוף הפעולה.

- הוועדה רואה חשיבות בהקמת רשות הסייבר הלאומית הן בשל תפקידה ביחס למגזר האזרחי-כלכלי שההגנה עליו, למעט בהיבטי תשתיות מחשוב קריטיות, הייתה חלקית, טרם הקמת הרשות, והן בשל הצורך ליצור חיבור בין הידע הביטחוני לידע האזרחי והכלכלי. לפי הוועדה רשות הסייבר הלאומית צריכה להיות הגורם האחראי על הגנת הסייבר במדינת ישראל.

- "**הוועדה לא השתכנעה בצורך בקיומן של שתי יחידות סמך עצמאיות במשרד ראש הממשלה העוסקות בתחום הסייבר- מטה הסייבר הלאומי ורשות הסייבר הלאומית המהוות יחדיו את מערך הסייבר הלאומי.**" לטענת הוועדה ישנם אזורי חפיפה בחלוקת הסמכויות ביניהן. עם זאת, ראש מערך הסייבר- ראש המטה הציג בפני הוועדה תפיסה לפי בעוד המטה עוסק בתכנון ארוך טווח (מו"פ, עידוד תעשייה ואקדמיה ועוד) ולא ממוקד בהיבטי הגנת סייבר, הרי שרשות הסייבר עוסקת בצד האופרטיבי של הגנה בסייבר. הוועדה סבורה שיש לבחון את מיקומו הנכון של מטה הסייבר הלאומי.

- דוח הוועדה מציין כי היבטי הריגול התעשייתי נעדרים כיום גורם אחראי. בנוסף, מצוין בדוח כי "**הוועדה התרשמה מחולשתה של המשטרה** (בהיבטי פעילותה בסייבר; ר.ג.), **בשל מגבלות חוקיות והיעדר משאבים מספיקים** והיא ממליצה להרחיב את הנושא כדי למצוא את האיזון המתאים בין הצורך לצמצם פגיעה בזכויות הפרט לבין שיפור האפקטיביות של פעולתה במרחב הסייבר. על מנת לחבר נכונה את הידע והיכולות הלאומיות עם הצורך המשטרתי להתמודד עם פשעי סייבר."

4. סטאטוס היישום של החלטות הממשלה ביחס להגנת הסייבר בממשלה וסוגיות נוספות

מרכז המחקר והמידע של הכנסת פנה אל התקשוב הממשלתי ואל ראש היחידה להגנת סייבר בממשלה (להלן, יה"ב) וכן אל ראש מערך הסייבר - ראש מטה הסייבר בשאלות ביחס למימוש החלטות הממשלה בנושא וכן ביחס למספר סוגיות עקרוניות. להלן יוצגו עיקרי תשובות הגופים.[15]

באשר ליישום החלטות הממשלה

- **לדברי ראש יה"ב, יה"ב הוקמה ולפעולתה הוקצו שבעה תקנים**. מתוך התקנים המוקצים, שלושה אוישו עד כה וארבעה מכרזים נכשלו ומתוכננים לצאת מחדש (כך במקור). בנוסף, ליחידה שלושה עובדים במיקור חוץ. **תקציב היחידה הוא כ-4 מיליוני ₪ לשנה (לא כולל הקמת ה-SOC הממשלתי)**.

[15] גדעון קונפינו, ראש היחידה להגנת הסייבר בממשלה, מכתב תשובה לפניית מרכז המחקר והמידע של הכנסת, 5 במרס 2017. אמרי קוזק, יועץ בכיר לראש מערך הסייבר הלאומי, מכתב תשובה לפניית מרכז המחקר והמידע של הכנסת, 7 במרס 2017.

- על פי תשובת נציג מערך הסייבר ותשובת ראש יה"ב, כאמור בהחלטת הממשלה 2443 **בכלל משרדי הממשלה מונה "ממונה הגנת סייבר".** גם ביחידות סמך, שבהן הוחלט כי יש להנחות את היחידה ישירות ולא באמצעות המשרד שתחתיו פועלת יחידת הסמך, מונה "ממונה הגנת סייבר" ליחידה. בנוסף, בכלל המשרדים ויחידות הסמך שבהם מונה ממונה הגנת סייבר, הוקמה והתכנסה "ועדת היגוי משרדית" בהשתפות נציג יה"ב.

- על פי תשובת נציג ראש מערך הסייבר הלאומי, ועדת ההיגוי לקידום ההובלה הממשלתית בהגנת הסייבר הוקמה והתכנסה עד כה שלוש פעמים (ואמורה להתכנס ב-8 במרס 2017 בפעם הרביעית).

- **לדברי ראש יה"ב ה-SOC (Security Operation Center) הממשלתי מוקם בעיר באר שבע במתקן ה- CERT הלאומי** (מרכז לסיוע בהתמודדות עם איומי סייבר)**, ושני משרדי ממשלה הוגדרו כפיילוט לפעולתו וחוברו אליו- משרד המשפטים ומשרד האוצר.** יצוין כי על פי תוכנית העבודה שפרסם מערך הסייבר, אמורים להתחבר ל- SOC בשנת 2017 עוד 6 גופי ממשלה ובשנת 2018 עוד 8 גופים, כך שעד לסוף שנת 2018 יהיו מחוברים אליו 16 גופים.[16]

- **באשר למיפוי שנדרש על פי החלטת הממשלה לשם הקמתן של יחידות מגזריות להגנת סייבר ציין נציג ראש מערך הסייבר כי, מיפוי כאמור בוצע, ובמסגרתו הוגדרו 15 מגזרים במשרדי הממשלה** כדלקמן: המגזר הפיננסי, מגזר התקשורת, מגזר התחבורה, מגזר התשתיות, האנרגיה והמים, מגזר הגנת הסביבה, מגזר הכלכלה והתעשייה, מגזר השלטון המקומי, המגזר לביטחון פנים, מגזר החינוך, מגזר הרווחה, המגזר לשירותי דת, מגזר החקלאות, מגזר המדע והטכנולוגיה ומגזר התרבות והספורט. ב-13 משרדים הושלמה או תושלם בקרוב הקמת היחידות המגזריות וב-2 משרדים מתבצע הליך מכרזי להקמת היחידה. באשר לגודל היחידות - שעל פי החלטת הממשלה אמור היה גם כן להיות ממופה ולכלול בין תקן למשרה אחת ביחידות קטנות לבין חמישה תקנים – ביחידה גדולה, על פי תשובת נציג ראש מערך הסייבר גודל היחידות המגזריות אינו לפרסום.

- ראש יה"ב ציין במכתבו כי עד כה ביצעה יה"ב את הפעולות הבאות:

-הנחיות ראש רשות התקשוב בנושאים: מדיניות ממשלתית להגנת סייבר; הגנה על מכשירים ניידים; אבטחת ענן;

- וועדה מייעצת למשרדי הממשלה ויחידות הסמך בנושא הגנת סייבר ואבטחת מידע בענן;

-פורום הגנת סייבר ממשלתי המתכנס מספר פעמים בשנה וכולל את ממוני הגנת הסייבר הממשלתיים ומנהלי אבטחת המידע;

- יצוין כי כאמור לעיל, **על פי החלטת הממשלה בעניין "קידום ההיערכות הלאומית להגנת הסייבר" מפברואר 2015 היה על מטה הסייבר והלשכה המשפטית במשרד ראש הממשלה בשיתוף עם משרד המשפטים להכין "תזכיר חוק הגנת הסייבר"** ולהביאו לאישור ראש הממשלה בתוך חצי שנה ממועד החלטת הממשלה. **עד כה טרם פורסם תזכיר חוק כאמור**, אך על פי תוכנית העבודה שפרסם מערך הסייבר הלאומי לשנים 2017- 2018 הצעת חוק הגנת סייבר אמורה להיות מונחת על שולחן הכנסת בשנת 2017.[17]

---

[16] ספר תוכניות העבודה לשנים 2017-8, "מערך הסייבר הלאומי: תוכנית עבודה לשנים 2017-8".

[17] ספר תוכניות העבודה לשנים 2017-8, "מערך הסייבר הלאומי: תוכנית עבודה לשנים 2017-8".

באשר לשאלות שהפנה מרכז המחקר והמידע של הכנסת ביחס להגנה על אתרי הממשלה ולאחסון האתרים, צוין בתשובת ראש יה"ב כי:

- כיום כ-1,300 אתרי ממשלה מתארחים בחוות השרתים הממשלתית וכ- 500 אתרים אינם מתארחים בחוות השרתים. **חוות השרתים בממשל זמין שתחת רשות התקשוב הממשלתית מארחת את מרבית אתרי הממשלה ופועלת להעביר את כל אתרי הממשלה כפי שנקבע בהחלטת הממשלה.** שירותי הממשלה עוברים לאירוח (hosting) באתר Gov.il החדש.

באשר לקיומו של DRP (Disaster Recovery Plan) לאתרי הממשלה ולתשתיות המחשוב החיוניות בממשל זמין[18], השיב ראש יה"ב כי תוכנית כאמור קיימת וכי ממשל זמין פועל בתוכנית רב שנתית להרחבת יכולותיו בתחום זה.

באשר לעילת מיקומה של יה"ב תחת אחריות התקשוב הממשלתי ולא בתוך הרשות הלאומית להגנת סייבר ציין ראש יה"ב כי "נושא ההגנה בסייבר הינו חלק אינטגרלי ומהותי בעולם מערכות המידע, לא ניתן לחשוב על האפשרות לפתח מערך מידע הכולל רכיבי תקשורת, שרתים, אחסון, תשתיות אפליקטיביות, יישומים וכו' שתחום ההגנה בסייבר אינו משולב בו משלב היזום. רשות התקשוב הממשלתי מנחה את משרדי הממשלה ואת יחידות הסמך בכל נושא התקשוב ובכלל זה בתחום הגנת הסייבר. מעבר לכך גם כל עולם הניטור של אירועי סייבר הינו חלק מתפיסה זו ולכן רשות התקשוב הממשלתי באמצעות היחידה להגנת הסייבר בממשלה היא הגוף המקים והמפעיל את ה – SOC הממשלתי."

נציג ראש מערך הסייבר השיב ביחס למיקומה של יה"ב תחת רשות התקשוב כי "יה"ב הינה הזרוע הקדמית של הרשות הלאומית להגנת הסייבר להנחיית משרדי הממשלה. יש הגיונות בהקמתה בתוך רשות התקשוב הממשלתי, כמו גם בתוך הרשות הלאומית להגנת הסייבר, והממשלה בחרה בחלופה הראשונה." עוד ציין נציג ראש מערך הסייבר, כי האחריות הכוללת על הגנת הסייבר במשרדי הממשלה היא על הרשות הלאומית להגנת סייבר והיא מיישמת אותה באמצעות היחידה להגנת הסייבר בממשלה- יה"ב, למעט בכל הנוגע לגופים שבהם מערכות ממוחשבות חיוניות המונחות במישרין על ידי הרשות או ראי"מ בשב"כ – בהתאם לחוק להסדרת הביטחון בגופים ציבוריים,תשנ"ח-1998.

באשר לטענות שהועלו בדוח ועדת החוץ והביטחון בדבר חולשתה של המשטרה בתחום הסייבר ובדבר היעדר אחראי על נושא הריגול התעשייתי, השיב נציג ראש מערך הסייבר כי "הרשות הלאומית להגנת הסייבר אחראית להגנת הסייבר במרחב האזרחי מכלל האיומים, וזאת מבלי לגרוע מאחריות המשטרה בתחומה." לא ברור לנו כיצד תשובה זו עונה על סוגיה אזרחית זו הדורשת בירור.

באשר לעמדת דוח ועדת החוץ והביטחון כי הוועדה לא השתכנעה בצורך בקיומם של מטה ורשות כשתי יחידות סמך עצמאיות במשרד השיב נציג ראש מערך הסייבר כי "עמדת המערך, כפי שהובעה עוד בשעת כתיבת הדוח של ועדת החוץ והביטחון, היא שעמדת הוועדה נובעת ככל הנראה מחוסר הבנה של תפקידי המערך, וההפרדה מצד אחד והסינרגיה מצד שני, בין תחומי המדיניות, בניין הכוח, הפעלת הכח ונושאים נוספים"

כתיבה: רועי גולדשמידט

אישור, יובל וורגן, ראש צוות

[18] הכוונה למערכת לגיבוי אתרי המשרדים במקרים של אסון או תקלה כוללנית, הכוללים הקמה של אתרים חלופיים ותשתיות חלופיות שיאפשרו המשכיות בתפעול האתרים ובנגישות למידע האצור בהם.