קידום ההיערכות הלאומית להגנת מרחב הסייבר

הצעה להחלטה

הקדמה

האיומים במרחב הסייבר הופכים משמעותיים לביטחון הלאומי, לתפקוד התקין של המדינה והארגונים שבה, לסדר הציבורי ולפעילות המשק, ומצויים בעלייה מתמדת. כתוצאה מהיקף האיומים וחומרתם, עלול להיגרם נזק לרציפות במתן שירותים חיוניים, לחיי אדם, לפעילות המשק ולאינטרסים לאומיים חיוניים אחרים.

המענה המדינתי הנוכחי בתחום הגנת הסייבר אינו שלם ואף אינו מספק. הסנכרון בין כלל המאמצים והיכולות המדינתיות חסר, ויש צורך להעמיק את השותפות המתחייבת בין המגזר הביטחוני לבין המגזר האזרחי לצורך הגנה אפקטיבית.

לפיכך, נדרשת היערכות מדינתית כוללת שתוביל להעלאת רמת הגנת הסייבר ולהגדרת אחריות להגנת הסייבר ברמה הלאומית, זאת לצד שמירתו של הסייבר כמרחב פתוח המאפשר זרימה חופשית של ידע, הון ושירותים, מחולל חדשנות ותורם לרווחה חברתית, תוך שמירה על זכויות יסוד, ובהן הזכות לפרטיות וחופש הביטוי.

בהתאם לכך, ובהמשך להחלטת ממשלה מספר 3611 מיום 07.08.2011 בנושא "קידום היכולת הלאומית במרחב הקיברנטי" (להלן – החלטה 3611) בכלל, ולנספח ב' סעיף ה' בהחלטה 3611 בפרט:

מחליטים,

הגדרה:

הגנת הסייבר – מכלול הפעולות למניעה, לנטרול, לחקירה ולהתמודדות עם איומי סייבר ואירועי סייבר, ולצמצום השפעתם והנזק הנגרם מהם, וזאת בטרם התרחשותם, במהלכם ולאחריהם.

1. לקבוע כי ההגנה על תפקודו התקין והבטוח של מרחב הסייבר מהווה יעד ביטחוני לאומי חיוני של המדינה ואינטרס ממלכתי חיוני לביטחונה הלאומי.

2. לאמץ את עיקרי התפיסה הלאומית להגנת הסייבר (להלן – התפיסה) שגיבש המטה הקיברנטי הלאומי (להלן – המטה), כמפורט בנספח ב' פרק 1.

רשות לאומית להגנת הסייבר

3. להקים במשרד ראש הממשלה, כחלק ממימוש התפיסה, רשות לאומית להגנת הסייבר (להלן – הרשות), שייעודה הגנת מרחב הסייבר כמפורט בנספח ב' פרק 2, ושתפקידיה

העיקריים הינם:

א. לנהל, להפעיל ולבצע בהתאם לצורך את כלל מאמצי ההגנה האופרטיביים ברמה הלאומית במרחב הסייבר, בתפיסה מערכתית, לטובת מענה הגנתי שלם ורציף למול תקיפות סייבר, ובכלל זה טיפול באיומי סייבר ובאירועי סייבר בזמן אמת, גיבוש תמונת מצב שוטפת, ריכוז ומחקר מודיעין, ועבודה עם הגופים המיוחדים כמפורט בנספח ב' פרק 5.

ב. להפעיל מרכז לסיוע בהתמודדות עם איומי סייבר (להלן – ה-CERT הלאומי) עבור כלל המשק, ובכלל זה לפעול לשיפור החוסן ההגנתי בסייבר, לסייע בטיפול באיומי סייבר ואירועי סייבר, לרכז ולשתף מידע רלוונטי עם כלל הגורמים במשק ולהוות נקודת ממשק מרכזית בין גופי הביטחון לבין הגורמים במשק. ה-CERT הלאומי יפעל בהתאם לעקרונות שיגובשו על ידי המטה בתיאום עם היועץ המשפטי לממשלה בתוך 90 יום מהחלטה זו.

ג. לבנות ולחזק את החוסן של כלל המשק בסייבר באמצעות היערכות, כשירות ואסדרה, ובכלל זה העלאת הכשירות של מגזרים וגופים במשק, הנחיית המשק בתחום הגנת הסייבר, אסדרת שוק שירותי הגנת הסייבר, רישוי, תקינה, עריכת תרגילים ואימונים, מתן תמריצים וכלים נדרשים נוספים.

ד. לעצב, ליישם ולהטמיע תורה לאומית להגנת הסייבר.

ה. לבצע כל תפקיד אחר שיקבע ראש הממשלה, בהתאם לייעוד הרשות.

4. להקים את מערך הסייבר הלאומי, הכולל את הרשות והמטה כשתי יחידות סמך עצמאיות למשרד ראש הממשלה (להלן – המערך), כמפורט בנספח א' פרק 1, סעיף 1. ראש הרשות יישא באחריות המלאה למימוש ייעוד הרשות ותפקידיה, ובכלל זה פעילותה האופרטיבית, ניהול משימותיה ועובדיה. ראש המטה ימשיך בהובלת המדיניות והאסטרטגיה בתחום הסייבר ברמה הלאומית, בבניין הכוח הלאומי ובחיזוקה של מדינת ישראל כמובילה עולמית בתחום הסייבר, בהתאם לתפקידי המטה כאמור בהחלטה 3611 ולסעיף 11 להחלטה זו. ראש המטה ישמש גם כראש המערך ויופקד על אישור תכניות העבודה של הרשות, על אופן יישומן, ועל החלטות מדיניות עקרוניות בפעילותה.

5. להטיל על המטה, בתיאום עם משרד האוצר ונציבות שירות המדינה, להקים את הרשות במתווה תלת-שנתי בשנים 2015-2017, באופן שיאפשר מימוש הולם של ייעודה כגוף בעל מאפיינים אזרחיים ובטחוניים-אופרטיביים, כמפורט בהחלטה זו, ובפרט בנספח א' פרק 1 ונספח ב' פרק 3.

<u>פעילות לאומית לטובת הגנת הסייבר</u>

6. להטיל על המטה להקים תשתית טכנולוגית לאומית לגילוי, זיהוי, התרעה ושיתוף מידע, לצורך גילוי וזיהוי של תקיפות סייבר על מדינת ישראל, אשר תופעל על ידי הרשות, כמפורט בנספח ב' פרק 4. זאת בהתאם להמלצות שיגובשו כמפורט להלן ביחס להיבטים

הנוגעים להקמת תשתית זו שיש בהם כדי להשפיע על זכויות יסוד, ובכלל זה היקף המידע שייאסף, מתכונת השימוש בו, שמירתו ומסירתו. ההמלצות כאמור יגובשו על ידי המטה על יסוד איזון בין צורכי הגנת הסייבר לבין הגנה על זכויות יסוד כאמור לעיל, ויובאו לאישור היועץ המשפטי לממשלה בתוך 90 יום מהחלטה זו.

7. להטיל על הגופים המיוחדים לעבוד עם הרשות לטובת הגנת הסייבר, כל אחד במסגרת הדין החל עליו ועל פיו, ובהתאם לייעודו וסמכויותיו, כמפורט בנספח ב' פרק 5.

8. להקים פורום הגנת הסייבר, בראשות ראש הרשות, שמטרתו תיאום, בקרה והסדרה של הפעילות המשותפת לרשות ולגופים המיוחדים, כמפורט בנספח ב' פרק 6.

9. להטיל על המטה להציג לראש הממשלה בתוך חצי שנה, מתווה להעברת שטח הפעולה בתחום פעולות לאבטחת מערכות ממוחשבות חיוניות כהגדרתן בחוק להסדרת הביטחון בגופים ציבוריים התשנ"ח-1998 (להלן – מערכות ממוחשבות חיוניות), כמפורט בנספח א' פרק 2, משירות הביטחון הכללי לרשות, וזאת בתוך שנתיים מהקמתה. להטיל על המטה ועל הלשכה המשפטית במשרד ראש הממשלה, בשיתוף עם משרד המשפטים, להכין תזכיר לתיקוני החקיקה הנדרשים ליישום המתווה, אשר יובא לאישור ראש הממשלה באותו המועד.

10. לבטל את החלטת ועדת השרים לענייני ביטחון לאומי מספר ב/84 מיום 11.12.2002.

11. לשנות את החלטה 3611, כמפורט בנספח א' פרק 3.

12. יובהר כי החלטה זו אינה באה להסמיך את הרשות או את המטה לעסוק בעניינים שנמצאים בתחום סמכויותיו הסטטוטוריות של השב"כ.

13. להטיל על המטה ועל הלשכה המשפטית במשרד ראש הממשלה בשיתוף עם משרד המשפטים להכין את תזכיר חוק הגנת הסייבר, בהתאם לעקרונות החלטה זו, ובכלל זה לבחון את הצורך בתיקוני חקיקה נדרשים, ולהביאו לאישור ראש הממשלה בתוך חצי שנה מהחלטה זו.

14. להקצות תקציב ותקני ותקני כוח אדם למימוש החלטה זו, כמפורט בנספח ב' פרק 7.

<u>הערת מזכירות הממשלה:</u>

נספח ב' (פרקים 1-7) וחלק נוסף מדברי ההסבר וכן חוות הדעת המשפטית להחלטה זו הינם בסיווג "סודי" ונמצאים לעיונם של חברי הממשלה במזכירות הממשלה.

נספח א' פרק 1 – היבטים ארגוניים ברשות ובהקמתה

1. היבטים ארגוניים:

א. ראש הרשות יישא באחריות המלאה למימוש ייעוד הרשות ותפקידיה, כולל פעילותה האופרטיבית, ניהול משימותיה ועובדיה.

ב. ראש המטה ישמש גם כראש המערך.

ג. המטה והרשות, בהתייעצות עם נציבות שירות המדינה ומשרד המשפטים, יגבשו נוהל לחלוקת האחריות, הסמכות והתפקידים בין ראש המערך לבין ראש הרשות, באופן המבטא את האמור בסעיף 4 להחלטה זו.

ד. יחידת הסמך של הרשות תקום כיחידה עצמאית.

ה. המערך הכספי של מערך הסייבר הלאומי יוקם באופן הדרגתי ובתיאום בין אגף החשב הכללי במשרד האוצר לבין המטה.

ו. המבנה הארגוני ומרכיבי התפעול של המערך, יתוקצבו תוך היעדר כפילויות וצמצום משאבים ככל הניתן, למעט במקרים הכרחיים בלבד שיסוכמו בין המטה לבין אגף התקציבים במשרד האוצר.

ז. ראש הרשות:

1) ראש הרשות הלאומית להגנת הסייבר (להלן – ראש הרשות) יהיה בעל מומחיות, רקע וניסיון המתאימים לניהול הרשות.

2) שכרו ותנאי שירותו של ראש הרשות יהיו כשל מנכ"ל משרד ממשלתי.

3) בהתאם לסעיף 6(א)(2) לחוק נכסי המדינה התשי"א-1951 (להלן – חוק נכסי המדינה) להרשות את ראש הרשות לייצג את הממשלה בכל עסקה מהעסקאות שמדובר בהן בסעיפים 4 ו-5 לחוק נכסי המדינה, למעט עסקאות במקרקעין, בתחומי פעילותה של הרשות, עד לסכום של 1,000,000 ש"ח, ולחתום בשם המדינה על המסמכים הנוגעים לעסקאות האמורות. כמו כן, להרשות את ראש המערך כאמור בסעיף זה בתחומי פעילותו של המטה, ללא הגבלת סכום, ולחתום בשם המדינה על המסמכים הנוגעים לעסקאות האמורות. כל אחד מהם יחתום יחד עם החשב הרלוונטי או עם סגנו.

ח. עובדי הרשות:

1) המבנה הארגוני של הרשות ואופן איוש המשרות יסוכם בין המטה לנציבות שירות המדינה ויתואם עם אגף התקציבים במשרד האוצר בתוך 30 יום

מהחלטה זו באופן שישקף את ייעוד הרשות, תפקידיה, סמכויותיה, אופן פעילותה והדחיפות בהקמתה.

2) נציבות שירות המדינה והממונה על השכר במשרד האוצר יגדירו, בהתייעצות עם המטה, טבלאות שכר ייעודיות וכללי העסקה לעובדי הרשות, בהתאם למאפייני פעילותה הייחודים ולכוח האדם הייחודי הנדרש למימוש ייעודה, בשים לב להחלת חוק שעות עבודה ומנוחה.

3) לאור אופייה של הרשות כגוף בעל מאפיינים אזרחיים וביטחוניים-אופרטיביים, כמפורט בהחלטה זו, להטיל על המטה ועל הלשכה המשפטית במשרד ראש הממשלה, בשיתוף עם נציבות שירות המדינה, משרד המשפטים והממונה על השכר, לבחון את הצורך לאסור על עובדי הרשות להתאגד או לנקוט צעדים ארגוניים שעלולים לפגוע ברציפות פעילותה האופרטיבית, ובכלל זה תיקוני חקיקה נדרשים לכך.

ט. להנחות את שר האוצר לפעול להחלת תקנה 3(8)(א) לתקנות חובת המכרזים התשנ"ג-1993 על הרשות והמטה.

2. <u>היבטים בהקמה</u>:

א. <u>מתווה הקמה</u>:

1) הרשות תוקם במתווה תלת-שנתי החל מיום קבלת החלטה זו ובמשך השנים 2015-2017 (להלן – תקופת ההקמה).

2) הרשות תחל פעילותה בתוך 90 יום מיום מינוי ראש הרשות, ותממש את תפקידיה בהתאם לתכנית רב-שנתית שתגובש על ידי ראש הרשות בתקופה זו.

3) עד למינוי ראש הרשות יחלו כלל הגופים האמורים בחלטה זו לפעול למימוש ההחלטה מול המטה ומנהלת ההקמה כמפורט להלן, ובכלל זה העברת כלל המידע הרלוונטי להגנת הסייבר, כמפורט בנספח ב' פרק 5.

4) במהלך תקופת ההקמה ימשיך המטה ככל שיידרש בהקמת חלק מתחומי הביצוע של הרשות ובהפעלתם, עד להעברתם לרשות. עם איוש משרת ראש הרשות ייעשה הדבר בהתאם לתיאום בין ראש המטה לבין ראש הרשות, וזאת לא יאוחר מתום תקופת ההקמה.

ב. <u>מנהלת הקמת הרשות</u> (להלן – מנהלת ההקמה):

1) מנהלת ההקמה תפעל להקמת הרשות, ולמילוי תפקידיה עד לתחילת פעילות הרשות.

2) מנהלת ההקמה תוקם במסגרת המטה, על בסיס תקני הרשות, וזאת בהתאם לסיכום בין המטה לבין נציבות שירות המדינה, ובתיאום עם אגף התקציבים

במשרד האוצר.

3) לאחר תחילת פעילות הרשות, יוסבו תקני מנהלת ההקמה לתקני הרשות וזאת בהתאם לסיכום בין המטה לנציבות שירות המדינה.

ג. <u>דיור הרשות</u>:

1) אתרי הרשות ימוקמו באזור גוש דן ובבאר שבע.

2) להטיל על המטה ועל מנהל הדיור הממשלתי להקים את דיור הקבע של הרשות, בהתאם לצרכיה הביטחוניים והטכנולוגיים הייחודים, ובמידת הצורך להסדיר דיור ביניים.

המשך פרק זה הינו מסווג. הנוסח המלא שמור במזכירות הממשלה, בנספח ב' פרק 3.

<u>נספח א' פרק 2 – מערכות ממוחשבות חיוניות</u>

1. להקים ועדת היגוי להגנה על מערכות ממוחשבות חיוניות (להלן-ועדת ההיגוי), אשר תפקידה לעסוק במערכות ממוחשבות חיוניות ולאשר את הצעות השב"כ בדבר הוספה של גוף לתוספת הרביעית לחוק להסדרת הביטחון בגופים ציבוריים התשנ"ח-1998 או שינויה.

חברי הוועדה להגנה על מערכות ממוחשבות חיוניות:

א. ראש המטה הקיברנטי הלאומי – יו"ר

ב. ראש הרשות הלאומית להגנת הסייבר

ג. ראש רשות החירום הלאומית במשרד הביטחון

ד. שני נציגי צה"ל שימנה הרמטכ"ל

ה. ראש אגף סיגינט-סייבר בשירות הביטחון הכללי

ו. נציג היועץ המשפטי לממשלה

ז. ראש הרשות למשפט, טכנולוגיה ומידע במשרד המשפטים

ח. משתתפים נוספים על פי החלטת יו"ר הוועדה

2. עד לאישור ראש הממשלה את המתווה להעברת שטח הפעולה בתחום פעולות לאבטחת מערכות ממוחשבות חיוניות, כמפורט בסעיף 9 להחלטה זו, ימשיך שירות הביטחון הכללי לבצע את תפקידיו בהתאם לחוק להסדרת הביטחון בגופים ציבוריים התשנ"ח-1998 כמפורט להלן, בתיאום עם ראש המטה או עם מי שמינה לכך:

א. קיום הערכת מצב בתחום ההגנה על מערכות ממוחשבות חיוניות במדינת ישראל והגדרת איום הייחוס עליהן, באישור ועדת ההיגוי.

ב. הגשת הצעות לקביעת רשימת הגופים המונחים וסיווג המערכות הממוחשבות כחיוניות לאישור ועדת ההיגוי, וכן הצעות לשינויים בקביעה כאמור.

ג. ריכוז, עיבוד והערכת מודיעין וגיבוש תמונת מודיעין שוטפת ותקופתית לעניין האיום על מערכות ממוחשבות חיוניות.

ד. מתן הנחיות מקצועיות לגופים המונחים בנוגע למערכות ממוחשבות חיוניות, ובכלל זה:

1) קביעת מדיניות אבטחה של מערכות ממוחשבות חיוניות והעברת הנחיות ונהלי אבטחה לגופים המונחים.

2) הערכה וקביעת רמת האיום על המערכות הממוחשבות החיוניות בגופים המונחים.

3) הזרמת מידע לגופים מונחים בנושא הגנה על מערכות ממוחשבות חיוניות. קביעת דרישות מוקדמות ורמת ההכשרה בנוגע לכוח אדם המועסק במשימות

הגנה על מערכות ממוחשבות חיוניות בגופים המונחים.

4) אישור מינוי אחראים להגנה על מערכות ממוחשבות בגופים המונחים.

5) ביקורת ופיקוח על יישום הנהלים על ידי הגוף המונחה.

6) ייעוץ והכוונה לפתרון בעיות מקצועיות ואישור אמצעים טכנולוגיים לצורך הגנה על מערכות ממוחשבות בגופים מונחים.

3. להנחות את השב"כ להעביר לרשות את כלל המידע הנוגע למערכות ממוחשבות חיוניות והנחייתן, ובכלל זה, כלל הדו"חות בנושא, תמונת המצב, מידע על פעילות השב"כ ועל פעילות הגופים המונחים, וזאת בכפוף להוראות נספח ב' פרק 5.

<u>נספח א' פרק 3 – תיקון החלטה 3611</u>

1. בהמשך להקמת הרשות ובהתאם לתפקידיה, לשנות את נספח א' בהחלטה 3611, כך שתפקידי המטה ישונו כמפורט להלן:

א. לבטל את סעיפים: 2.ט., 2.י., 2.יא., 2.יב., 2.יג.

ב. לשנות את סעיף 1. כך שהמילים "ממליץ על" יוחלפו במילים "קובע את".

ג. לשנות את סעיף 2.ו. ובמקומו לכתוב "לקדם מחקר ופיתוח בתחום הסייבר".

ד. לשנות את סעיף 2.יד. ובמקומו לכתוב "לגבש אסטרטגיה לאומית לפיתוח ההון האנושי בתחום הסייבר ולקדם פרויקטים לאומיים ליישומה".

2. לשנות את שמו של המטה הקיברנטי הלאומי ל"מטה הסייבר הלאומי".

דברי הסבר

רקע כללי ולעניין סעיפים 1, 2 ו-3 ונספח ב' פרקים 1 ו-2

היווצרות מרחב הסייבר הינה תולדה של ההתפתחות הטכנולוגית המואצת של העשורים האחרונים, ותרומתו להתפתחות האנושית אינה ניתנת לערעור. מרחב זה מאפשר זרימה חופשית של ידע, הון ושירותים עם חסמי כניסה נמוכים מאד, ובכך הוא משפר את הרווחה החברתית ומעודד חדשנות. התבססותן של פעילויות מסורתיות רבות על מרחב הסייבר הולכת ועולה (דוגמת תשלומים דיגיטליים או שליטה ובקרה בתהליכי ייצור ותפעול), במקביל לפיתוח מתמשך של פעילויות מרכזיות חדשות באמצעותו (דוגמת מסחר מקוון ורשתות חברתיות). כתוצאה מכך ונוכח השפעתו הנרחבת על פעילותם של פרטים, ארגונים ומדינות, הופך מרחב הסייבר לבעל חשיבות אסטרטגית.

לצד זאת, מרחב הסייבר טומן בחובו משרעת איומים ייחודית בהיקפה, בהיותו תווך פוטנציאלי לפעילויות עוינות, מוכרות וחדשות כאחד, אשר עשויות להביא הן לפגיעה בתוך המרחב (למשל במידע או בתפקוד) והן לפגיעה היוצאת ממנו (למשל פיזית או תודעתית). בין היתר, איומים אלה כוללים: השחתת אתרים וחסימת שירותים, סחיטה והטרדה של פרטים וארגונים, פגיעה בפרטיות ע"י גניבת מידע אישי, ריגול מסחרי, שיבוש או השבתה של תהליכים ושירותים חיוניים לאזרחים ולמשק, גניבת סודות מדינה, פגיעה בתשתיות ובמערכות חיוניות למשק ולגופי הביטחון, פגיעה בחיי אדם ועוד. מגוון גורמים עוינים עשויים לממש איומים אלה – יחידים, אסופות האקרים, קבוצות פשיעה, ארגוני טרור, תאגידים ומדינות – וזאת מתוך שורה ארוכה של מניעים – אישיים, אידיאולוגיים, כלכליים, ביטחוניים ואחרים.

בשנים האחרונות ניכרת עלייה משמעותית בשכיחותם של אירועי סייבר ובחומרתם, בעולם כולו ובישראל בפרט. מגמה זו מיוחסת במידה רבה למאפיינים הייחודיים של המרחב אשר מקלים על הפעילות העוינת בתוכו: קבועי הזמן הקצרים המאפיינים את השתנות המרחב ואת הנעשה בו, חוסר הרלוונטיות של המרחק הפיזי לפעילות במרחב וכתוצאה מכך חשיפה לאיומים מכל העולם בסבירות דומה, האנונימיות היחסית המתאפשרת בו, היעדר כוח ביטחוני החוצץ בין התוקף לנתקף, מחירי הכניסה הנמוכים לפיתוח יכולות פעולה במרחב ועליית "שטח הפנים" לתקיפה כתוצאה מהתרחבותו המהירה. הסיכון האמור במגמה מדרדרת זו לפגיעה בביטחון האישי, בפעילות המשק ובביטחון המדינה, חייב התייחסות ברמה הלאומית.

בהחלטת ממשלה מספר 3611 בנושא "קידום היכולת הלאומית במרחב הקיברנטי" מיום 07.08.2011 (להלן – החלטה 3611), הוחלט על הקמת המטה הקיברנטי הלאומי (להלן – המטה) והוטל עליו, בין היתר, לגבש תפיסת הגנה לאומית במרחב הסייבר. תפיסה זו יועדה להחליף את התפיסה המצומצמת שניצבה בבסיס החלטת ועדת השרים לענייני ביטחון לאומי מספר ב/84 בנושא "אחריות להגנה על מערכות ממוחשבות במדינת ישראל" משנת 2002 (להלן – החלטה ב/84), שבה הוסדר הטיפול בהגנת מערכות ממוחשבות חיוניות בלבד – מערכות שהפגיעה בהן עלולה לגרום לנזק פיזי או כלכלי משמעותי מאד, לפגיעה בחיי אדם או לפגיעה באספקת שירות ציבורי חיוני. בהתאם לכך, למן הקמתו פעל המטה בשיתוף גורמי

המקצוע הרלוונטיים כדי לגבש את התפיסה ואת מתווה ההיערכות המדינתית למימושה.

העובדה כי הסייבר הוא מרחב אזרחי במהותו הייתה במוקד עבודת המטה המקיפה. הרי רובו המכריע של המרחב מבוסס על תשתיות, מערכות וטכנולוגיות אזרחיות, המופעלות ע"י פרטים וארגונים אזרחיים, ומכאן שמרבית האיומים במרחב מופנים כלפי המגזר האזרחי וברשותו מצוי גם רוב המידע אודות המתרחש במרחב. בנוסף, לא סביר כאמור כי גופי הביטחון יעמדו כחיץ, לא כל שכן הרמטי, בין הארגון לבין תוקפיו במרחב הסייבר. לאור זאת ומאחר שניהול הרשתות עומד בבסיס תהליכי הליבה של הארגון (עסקיים, תפעוליים או אחרים) – רק הארגון יכול לשאת באחריות להגן על עצמו. מנגד, מובן כי אין בכוחו של הארגון הבודד להעמיד את המומחיות והמשאבים הנדרשים כדי להתמודד עם מלוא משרעת האיומים שתוארה לעיל, בפרט כאשר הוא מודע רק למתרחש בגבולותיו.

מצב עניינים מורכב זה עמד בבסיס ההבנה היסודית כי שיתוף פעולה, בין הממשלה לבין הארגונים במשק ובין הארגונים לבין עצמם, יהווה מרכיב מרכזי בהגנה על מרחב הסייבר, וזו גם הגישה הרווחת בקרב רובן המוחלט של המדינות המפותחות.

המענה הנוכחי של מדינת ישראל לאיומים במרחב הסייבר אינו שלם ואף אינו מספק. עד כה, מענה זה התמקד כמעט בלעדית בהגנה איכותית על מערכות ממוחשבות חיוניות ועל גופי הביטחון. כעת נדרש מענה לאומי כולל, בדגש על המגזר האזרחי (לרבות הממשלתי), שיבסס את שיתוף הפעולה ההכרחי, ירתום את היכולות הלאומיות ויסנכרן את המאמצים הרלוונטיים.

להלן עיקרי המענה הלאומי הנדרש, שרובם ככולם אינם ממומשים היום, לא כל שכן כמכלול אינטגרטיבי: שיפור רמת הכשירות והמוכנות של הארגונים במשק באמצעות פעילויות אסדרה, תמרוץ, רישוי, הסמכה, תקינה, הסברה ותרגול; היתוך מידע ומודיעין מהסכמים מסחריים, מגופי הביטחון ומהארגונים עצמם, לטובת גילוי וזיהוי של איומי סייבר טרם התממשותם וגיבוש תמונת מצב לאומית; התמודדות בזמן אמת עם אירועי סייבר, לרבות סיוע לארגון בהכלת האירוע, בהתאוששות ממנו ובתחקורו; הפעלת יכולות ביטחוניות; עבודה שוטפת עם גופים מקבילים בעולם; פיתוח והטמעה של תהליכים ומנגנונים רוחביים לשיתוף מידע.

לאור כל זאת ובהסתכלות שאינה עוצרת בבעיות השעה, אלא צופה פני עתיד – תלות גוברת של החברה המודרנית במרחב הסייבר לצד התפתחותו כמרחב לחימה של ממש – מסקנה מרכזית הנובעת מעבודת המטה המעמיקה, היא שההגנה על מרחב הסייבר, במיוחד בראי אחריות המדינה כריבון, אינה נגזרת של דיסציפלינה ביטחונית קיימת, כי אם דיסציפלינה ייחודית ועצמאית. משמעות הדבר היא שייעוד זה הוא בלתי תלוי בייעודם של גופים אחרים, במניעי התוקף, בתבחינים טכנולוגיים למיניהם וכיוצא באלה.

לשם המחשה, ראוי לבחון את ההקבלה להגנה על המרחב האווירי, באשר ברור כי גורם ההגנה המרחבי נושא באחריות המלאה להתמודדות עם מגוון האירועים, בין אם מדובר בחדירת מטוס ריגול, מזל"ט מתאבד או מטוס קרב. זאת ועוד, במקרים רבים ייעוד זה גובר בחשיבותו על ייעודים קיימים אחרים. לדוגמה, במקרה של סחיטת תאגיד מרכזי בגין פרטי לקוחות שנגנבו ממנו (בפעולות שבוצעו במרחב הסייבר או באמצעותו), השאיפה לאתר את

העבריין ולמצות עמו את הדין עשויה ליפול בחשיבותה למול מניעת חשיפת המידע והפצתו באופן שיביא לנזק תודעתי, ביטחוני או כלכלי.

בהתאם לכך, שלושה עקרונות יסוד עומדים בבסיס החלטה זו:

1. אימוץ תפיסת הגנה לאומית שלמה המתייחסת באופן שיטתי ומדורג לכלל הארגונים והמגזרים במדינה, ובפרט לדומה ולשונה ביניהם, לכל סוגי מאמצי ההגנה הנדרשים, ולשיתוף הפעולה הייחודי הנדרש בין המדינה לבין המשק. במרכז המימוש של התפיסה עומדת הקמת הרשות הלאומית להגנת הסייבר בתור גוף ייעודי להגנה על מרחב הסייבר, ובכך תימדד הצלחתה. הרשות תיבנה כמוקד מרכזי של ידע ופעילות בתחום באמצעות מסה קריטית ייחודית של תשתיות, יכולות ומומחים.
2. הרשות תיעזר במידת האפשר ביכולות בלעדיות קיימות, החל מקהילת המודיעין וכלה ברגולטורים מגזריים, על מנת לרתום את מכלול המאמצים הנדרשים, אזרחיים וביטחוניים כאחד, למנף מוקדים קיימים של ידע ומומחיות ולאגם משאבים.
3. הרשות תעבוד "כתף אל כתף" עם הארגונים והמגזרים במשק, לטובת הגנתם, בהסכמתם ולכל הפחות בידיעתם. אבחנה ברורה זו ביחס לייעודים ממלכתיים אחרים תסייע בשמירה על זכויות הפרט ותעודד שיתוף פעולה מעמיק לאורך זמן.

<u>לעניין סעיף 9 להחלטה ולנספח א' פרק 2 – מערכות ממוחשבות חיוניות</u>

במסגרת כלל עבודות המטה שקדמו להחלטה זו התבססה תמימות דעים של כלל הגורמים המקצועיים בדבר הצורך לרכז בידי גוף אחד את האחריות להגנה על מרחב הסייבר (להוציא מערכות הגופים המיוחדים). בהתאם לכך, גם הטיפול בהגנת מערכות ממוחשבות חיוניות, אשר החל בשב"כ לפני יותר מעשור, יועבר לאחריות הרשות, לפי מתווה מיוחד שיהלום את רגישות הנושא ויוגש לאישור ראש הממשלה בתוך חצי שנה מהחלטה זו. עד להעברות אחריות זו לרשות, ימשיך השב"כ לשאת בה, כפי שמוגדר בחוק להסדרת הביטחון בגופים ציבוריים וכפי שהוגדר מחדש בהחלטה זו.

<u>לעניין סעיפים 4 ו-5, נספח א' פרק 1 ונספח ב' פרק 3 – הקמת הרשות</u>

הרשות מוקמת כיחידת סמך במשרד ראש הממשלה לצד המטה וכחלק ממערך הסייבר הלאומי. מבנה זה יאפשר לשמר את ההפרדה החיוניות בין פעילותה האופרטיבית של הרשות לבין פעילות המטה לקידום המדיניות הלאומית ובניין הכוח הלאומי בתחום הסייבר.

הקמת הרשות כיחידת סמך אזרחית-ביטחונית אופרטיבית תיתן בידיה את הכלים המנהליים הנדרשים למימוש ייעודה, לאור הדחיפות, הגמישות והרגישות המאפיינים את משימותיה בפרט ואת תחום פעילותה בכלל. בתוך כך ניתן למנות: ניהול עצמאי של העובדים, על ייחודיותם ומורכבות גיוסם, דרך עצמאות בנושאי המינהל השונים, וכלה בנושאים שהחלתם על הרשות מחייבת הגדרתה כיחידת סמך, לדוגמה פטור מתקנות חובת המכרזים או ועדת פטור משרדית נפרדת.

הרשות תקום במתווה תלת-שנתי במטרה לגשר בהקדם האפשרי על הפער ההגנתי הקיים. ראש הרשות יחל במימוש תפקידיה בהתאם לתכנית שיגבש במהלך 90 הימים הראשונים לעבודתו. בשנות ההקמה יסייע המטה בהקמת הרשות ובמימוש חלק מיכולותיה ותפקידיה, וזאת בתיאום עם ראש הרשות לאחר מינויו.

עובדי הרשות – לצורך מימוש ייעודה ועמידה במשימותיה, על הרשות לגייס כוח אדם ייחודי ואיכותי ובתנאים תחרותיים. לשם כך, ייבנו טבלאות שכר ייחודיות להעסקתם. בנוסף, ייבחן הצורך בקידום איסור התאגדות של עובדי הרשות כדי למנוע פגיעה בפעילותה כגוף אופרטיבי.

מנהלת ההקמה – מנהלת ההקמה של הרשות תוקם תחילה במסגרת המטה על מנת להתניע את פעילותה באופן מיידי. מנהלת ההקמה תכלול בעלי תפקידים מגוונים, כך שכבר בשנה הראשונה להקמתה תחל הרשות לפעול באופן משמעותי וכדי להשלים את הקמתה בתוך שלוש שנים מהחלטה זו. מנהלת ההקמה תמונה על בסיס תקני הרשות, ותקניה יוסבו לתקני הרשות עם תחילת פעילות הרשות.

דיור הרשות – הרשות תמוקם בגוש דן ובבאר שבע, כחלק מקריית הסייבר הלאומית, אשר הוקמה בהחלטת ממשלה מספר 1815 בנושא "הקמת קריית הסייבר הלאומית והטבת מס לחברות סייבר בקריה" מיום 06.07.2014. זאת בהתאם להחלטת ממשלה 1661 בנושא "העברת היחידות הארציות של הממשלה לירושלים" מיום 13.05.2007, סעיף א', לפיו ראש הממשלה יחליט על דיור יחידות במשרדו.

<u>לעניין סעיף 11 להחלטה ולנספח א' פרק 3 – שינויי החלטה 3611</u>

עם הקמת הרשות, קיים צורך לבטל תפקידים בעלי אופי אופרטיבי אשר הוטלו על המטה בהחלטה 3611, ולהטילם על הרשות. תפקידים אלו כוללים את האחריות לתרגילים, ריכוז תמונת המודיעין, ריכוז תמונת המצב, קידום והעלאת המודעות הציבורית לאיומים בסייבר, וגיבוש ופרסום אזהרות ומידע לציבור בנוגע לאיומים בסייבר. במקביל, יש לתקן את תפקידי המטה כך שיוכל לממש את ייעודו בקידום המדיניות הלאומית ובבניין הכוח הלאומי בתחום הסייבר, ובכלל זה גיבוש אסטרטגיה לאומית לפיתוח ההון האנושי בתחום הסייבר וכן קידום מחקר ופיתוח בתחום הסייבר.

מוצע לשנות את שמו של המטה הקיברנטי הלאומי ל"מטה הסייבר הלאומי". בשונה מהמונח "קיברנטי", המונח "סייבר" שגור זה תקופה ארוכה בשיח הציבורי, בממשלה, בתעשייה, באקדמיה ובתקשורת. יש לציין כי גורמים רבים העובדים עם המטה מכנים אותו כבר עתה "מטה הסייבר הלאומי".

לעניין סעיף 12 להחלטה – הכנת תזכיר חוק הגנת הסייבר

גיבוש מענה שלם לאתגרי הגנת הסייבר יחייב גם תיקוני חקיקה, בין היתר, כדי להסמיך את הרשות בביצוע פעולות מסוימות. המטה ומשרד המשפטים יפעלו להכנת תזכיר חוק הגנת הסייבר.

חלק מדברי ההסבר להחלטה זו מסווגים. הנוסח המלא שמור במזכירות ממשלה.

עמדת שרים אחרים שההצעה נוגעת לתחום סמכותם

שר הביטחון – תומך

שר האוצר – תומך

השר לביטחון פנים – תומך

שר המשפטים – תומך

השר לענייני מודיעין – תומך

החלטות קודמות של הממשלה בנושא

החלטת ממשלה מספר 3611 מיום 07.08.2011

החלטת ועדת השרים לענייני ביטחון לאומי מספר ב/84 מיום 11.12.2002

החלטת ממשלה מספר 1661 מיום 13.05.2007

עמדת היועץ המשפטי של המשרד יוזם ההצעה

חוות הדעת המשפטית להצעה הינה בסיווג סודי ושמורה במזכירות הממשלה.

סיווגים

סיווג ראשי: 01ביצועי

סיווג משני: 02הצהרתי

תחום פעולה עיקרי: 01חוץ וביטחון

מוגש על ידי ראש הממשלה

י' בטבת התשע"ה
01 בינואר 2015