היבטים בהיערכות המדינה
להגנת המרחב הקיברנטי

תקציר

רקע כללי

המרחב הקיברנטי (להלן גם - מרחב הסייבר) מורכב מהגורמים האלה: מערכות ממוכנות ממוחשבות, רשתות מחשבים ותקשורת, תכנות, מידע ממוחשב, תוכן שהועבר באופן ממוחשב, נתוני תעבורה ובקרה והמשתמשים של כל אלה. בשנת 2011 החליטה הממשלה להקים מטה קיברנטי לאומי במשרד ראש הממשלה (להלן - משרד רה"מ) שישמש גוף מטה לראש הממשלה (להלן - רה"מ) ולממשלה אשר ימליץ על מדיניות לאומית בתחום הקיברנטי ויקדם את יישומה (להלן - ההחלטה מ-2011)[1]. עוד החליטה הממשלה להסדיר את האחריות לטיפול בתחום הקיברנטי ולקדם את יכולת ההגנה על המרחב הקיברנטי בישראל.

בהמשך להחלטה מ-2011 קיבלה הממשלה בפברואר 2015 שתי החלטות: החלטה מספר 2443 - "קידום אסדרה [רגולציה] לאומית והובלה ממשלתית בהגנת הסייבר" (להלן - ההחלטה בעניין האסדרה), והחלטה 2444 - "קידום ההיערכות הלאומית להגנת מרחב הסייבר" (להלן - ההחלטה בעניין ההיערכות). בהחלטות אלו הוחלט על הקמת רשות לאומית להגנת הסייבר (להלן - הרשות) וגופים נוספים המיועדים לטיפול באסדרה של שוק הסייבר ושל הארגונים הפועלים במרחב הסייבר האזרחי.

פעולות הביקורת

מספטמבר 2013 עד יולי 2015, לסירוגין, עשה משרד מבקר המדינה ביקורת בנושא היערכות המדינה להגנת המרחב הקיברנטי. הנושאים שנבדקו הם כדלהלן: גיבוש תפיסת הגנה כוללת על המרחב הקיברנטי; הסדרת האחריות לטיפול בתחום הקיברנטי ומימושה; האסדרה של שוק הסייבר; הגדרת הגופים והמערכות שיש להגן עליהם ורמת ההגנה הנדרשת; מצב ההגנה על מערכות המחשוב שאינן תשתיות מדינה קריטיות; מצב ההגנה על מערכות מחשוב שהן תשתיות מדינה קריטיות. הביקורת נעשתה במטה הקיברנטי הלאומי שבמשרד רה"מ (להלן - מטה הסייבר או המטה); בשירות הביטחון הכללי (להלן - שב"כ); ובמספר משרדי ממשלה וגופים נוספים. בדיקות השלמה נעשו בספטמבר 2015.

1 החלטה מספר 3611 שנושאה הוא "קידום היכולת הלאומית במרחב הקיברנטי". הגדרת המרחב הקיברנטי לקוחה מהחלטה זו.

ועדת המשנה של הוועדה לענייני ביקורת המדינה של הכנסת, בהתייעצות עם מבקר המדינה, החליטה להטיל חיסיון על חלקים מפרק ביקורת זה לשם שמירה על ביטחון המדינה, בהתאם לסעיף 17 לחוק מבקר המדינה, התשי"ח-1958 [נוסח משולב].

הליקויים העיקריים

הסדרת האחריות לטיפול בתחום הקיברנטי

הממשלה אישרה את הסדרת האחריות לטיפול בתחום הקיברנטי בחלוף כשלוש שנים ממועד קבלת ההחלטה מ-2011. עובדה זו עיכבה את קידום השינויים בחקיקה ומרבית השינויים הארגוניים האחרים החיוניים לצורך מתן הסמכות, האחריות והמשאבים הנחוצים להעמקת הפעילות בתחום הגנת הסייבר ולהרחבתה לחלקים נוספים במרחב הקיברנטי האזרחי בישראל. התמשכות ההליך של הסדרת האחריות לטיפול בתחום הקיברנטי במשך שנים ואי-העמידה בלוח הזמנים שקבעה הממשלה בשנת 2011 לגיבוש תפיסת ההגנה הכוללת אינן עולות בקנה אחד עם התגברות האיום על מדינת ישראל.

בעבודת המטה ובתהליך קבלת ההחלטות הנוגעים להסדרת האחריות לטיפול בתחום הקיברנטי במדינת ישראל נפלו כמה ליקויים, בין היתר בהליך גיבוש ואישור מסמך תפיסת ההגנה. כן נמצאו הליקויים הבאים: (1) במסמכים שהוגשו לשרי הממשלה, טרם ישיבת הממשלה, לא הוצגה חלופה נוספת. (2) בעבודת המטה לא פורטה העלות של החלופות באשר לגורם שיישא באחריות להגנה על המרחב הקיברנטי של מדינת ישראל. (3) בהצעות ההחלטה לממשלה ובדברי ההסבר להן לא פורטו מלוא ההוצאה התקציבית הכרוכה ביישומן והמשמעויות של היישום על משק המדינה.

המטה לא הציג לרה"מ, את המתווה להעברת שטח הפעולה בתחום הפעולות לאבטחת מערכות ממוחשבות חיוניות כהגדרתן בחוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998 (להלן - החוק להסדרת הביטחון), מהשב"כ לרשות, אף שהיה אמור לעשות זאת עד אוגוסט 2015.

עד תחילת 2016 לא הושלמה הכנת תזכיר חוק הגנת הסייבר, שלפי האמור בהחלטת הממשלה בעניין ההיערכות היה צריך להיות מוגש לרה"מ עד אוגוסט 2015.

המטה הציג דרישה למבנה מינהלת ההקמה עוד בדצמבר 2014, אולם מבנה כזה טרם אושר סופית. נוסף על כך, עד ינואר 2016 לא הציג המטה הצעה למבנה ארגוני שלם של הרשות, אף שעל פי ההחלטה בעניין ההיערכות, מבנה זה היה אמור להיות מסוכם עם נציבות שירות המדינה ואגף התקציבים במשרד האוצר עד מרץ 2015. ראש הרשות מונה בחלוף כמעט שנה ממועד קבלת ההחלטה בעניין ההיערכות.

> התמשכות ההליך של הסדרת האחריות לטיפול בתחום הקיברנטי במשך שנים ואי-העמידה בלוח הזמנים שקבעה הממשלה בשנת 2011 לגיבוש תפיסת ההגנה הכוללת אינן עולות בקנה אחד עם התגברות האיום על מדינת ישראל

ועדת השירות בנציבות שירות המדינה המליצה על מתן פטור ממכרז פומבי למשרות מקצועיות ברשות, בשל דחיפות האיוש והסיווג הביטחוני של בעלי התפקידים המיועדים לעבודה ברשות, והממשלה אישרה מתן פטור זה. בהחלטתה זו לא נתנה ועדת השירות משקל ראוי למאפיינים האזרחיים של הרשות ולמשך הזמן הארוך שנקבע לאיוש רוב המשרות ברשות.

האסדרה של שוק הסייבר

סקר תקני אבטחת מידע וסייבר בחו"ל בוצע באיחור משמעותי מלוחות הזמנים שנקבעו לכך. גם בחינה וקידום של מיסוד מנגנונים לאישור ולהסמכה של מוצרי הגנת הסייבר בישראל בהתאם לתקינה בין-לאומית למוצרי אבטחת מידע ומחשוב נמצאים בפיגור לעומת לוח הזמנים המקורי. השירותים המקצועיים בתחום הגנת הסייבר כוללים, בין היתר, ביצוע של סקרי סיכונים, מבדקי חדירה, סיוע בניהול אבטחת המידע בארגון והכנה לקראת הסמכה לתקני אבטחת מידע (להלן - שירותי הגנת הסייבר). נמצא כי עד מועד סיום הביקורת לא עמד המטה במשימה של הגדרת מנגנון למדרוג שירותי הגנת הסייבר. במצב דברים זה, חל עיכוב באסדרת מקצועות הסייבר והעוסקים בתחום זה.

קביעת הגופים והמערכות שיש להגן עליהם

נמצאו שני גופים, שהיה מקום ליזום את בחינת הגדרתם כגוף ציבורי כהגדרתו בחוק להסדרת הביטחון מבחינת מהות פעילותם וחשיבותה, אולם בחינתם לא נעשתה או שנעשתה בשלב מאוחר יחסית.

תהליך המיפוי של המרחב הקיברנטי הישראלי לא הסתיים וגם לא נקבעה תכנית עבודה ולוח זמנים לסיומו. לפיכך לא היה בידי מטה הסייבר מיפוי שיאפשר לקבוע מי הם הגופים במרחב הקיברנטי האזרחי הטעונים הגנה בהתאם להיררכיה פירמידלית של כלל הגופים במדינה ועל פי רמות הסיכון שלהם וסוגי המערכות הממוחשבות שבהם.

ההיערכות להגנת מערכות מחשוב שאינן תמ"ק[2]

אף שהמטה המליץ עוד באוגוסט 2012 להסתייע ביכולות ובסמכויות של משרדי הממשלה המשמשים מאסדרים (רגולטורים) כלפי הגופים שבמגזרם לצורך קידום האסדרה בתחום ההגנה על הסייבר, לא הופעלו, עד מועד סיום הביקורת, חלק מהמאסדרים המגזריים בתחום הסייבר. כמו כן טרם אוישו משרות מנהלי היחידות

> תהליך המיפוי של המרחב הקיברנטי הישראלי לא הסתיים... לפיכך לא היה בידי מטה הסייבר מיפוי שיאפשר לקבוע מי הם הגופים במרחב הקיברנטי האזרחי הטעונים הגנה

2 תשתיות מחשוב קריטיות.

להכוונה מקצועית מגזרית בתחום הגנת הסייבר, בניגוד למה שנקבע בהחלטת הממשלה בעניין האסדרה.

המטה הקיברנטי והשב"כ קיימו, כל גוף בנפרד, פעילות של סיוע וחיזוק המאסדרים המגזריים. לא נמצא שהמטה תיאם עם השב"כ את הפעילות בתחום המאסדרים המגזריים והסתייע בו לקידום פעילות זו.

ההגנה על תשתיות מחשוב קריטיות

כמה גופים מונחים אינם עומדים בקצב הראוי ביישום התכנית הרב-שנתית להטמעת דרישות האבטחה של השב"כ, ביניהם גם גופים הנמצאים זמן ממושך יחסית בהנחיית השב"כ.

על אף האמור בהחלטה מ-2002[3], עד דצמבר 2014 לא דיווחו ראשי ועדת ההיגוי העליונה להגנה על מערכות ממוחשבות חיוניות לממשלה או לוועדת שרים על מצב ההגנה של המערכות הממוחשבות כנדרש בהחלטה.

ההמלצות העיקריות

הסדרת האחריות לטיפול במרחב הסייבר, הקמת הרשות והסדרת שיתוף הפעולה בינה ובין הגופים הפועלים במרחב הסייבר ובראשם השב"כ, היא תהליך מורכב ורגיש הכולל היבטים מבצעיים, תקציביים, טכנולוגיים ומשפטיים. את התהליך שעליו החליטה הממשלה יש לתכנן בקפדנות כך שיובטח כי הרשות תקבל את כל הידע הנדרש למימוש אחריותה. אשר על כן, יש להחיש את סיום הפעולות שעליהן החליטה הממשלה.

על המטה לסיים בהקדם את הכנת תזכיר חוק הגנת הסייבר בהתאם לנדרש בהחלטת הממשלה.

מן הראוי שאיוש המשרות ברשות ייעשה, ככל הניתן, באמצעות תהליכים תחרותיים ושוויוניים אשר יגשימו את עקרון שוויון ההזדמנויות לכל הקבוע בחוק שירות המדינה (מינויים), התשי"ט-1959. תהליכים אלה, גם יגדילו את האוכלוסייה שממנה יהיה אפשר לגייס את המועמדים המתאימים ביותר.

על המטה לבחון את האופן שבו הוא קובע מסגרת עבודה מפורטת ומחייבת למילוי מכלול משימותיו ברמה השנתית והרב-שנתית. נוסף על כך, נוכח העיכוב שחל משך שנים בקידום הטיפול בתחום האסדרה של שוק הסייבר והדחיפות שיש להנחת הבסיס לאסדרת הנושא, יש חשיבות רבה לכך שתכנית העבודה של

3 החלטת ועדת השרים לענייני ביטחון לאומי בנושא "אחריות להגנה על מערכות ממוחשבות" משנת 2002.

המטה תגדיר אבני דרך וכן את המועד הסופי שבו אמורות להיות מושלמות כל המשימות שייקבעו בתחום זה.

מן הראוי שוועדת ההיגוי העליונה תקבע מתכונת לאיתור גופים פוטנציאליים להגדרה כגופים מונחים ועל בסיסה תיזום תהליך בחינה של כלל המגזרים והגופים במשק כדי להמליץ על גופים נוספים הראויים להכרה כגופים מונחים או לחלופין על הוצאת גופים מסטטוס זה. כמו כן, מן הראוי ליצור מנגנון מסודר שיבטיח כי ככל שמתעוררים קשיים בהגדרת גוף כגוף מונחה, יובא הדבר לידיעת ועדת ההיגוי העליונה מבעוד מועד, ובמקרה שהבעיה אינה נפתרת על ועדת ההיגוי יהיה לדווח על כך לממשלה או לוועדת שרים.

מתוקף אחריותו של המטה היה עליו לוודא כי יוגדר היקף הבעיה שעמה יש להתמודד בתחום ההגנה על מרחב הסייבר האזרחי, ייקבע מה הם התחומים והגופים במשק שיש להגן עליהם, מה המענה שצריך להינתן ואילו משאבים יושקעו בכך. לצורך כך על המטה להחיש את פעילותו בנושא ולפעול, בעצמו או באמצעות אחרים, לקידום מיפוי מלא של המרחב.

מן הראוי להחיש את הפעולות לשם הקמת היחידות להכוונה מקצועית מגזרית וחיזוק המאסדרים המגזריים. על המטה גם להגדיר את הגורם ברשות שיפעל מול המאסדרים המגזריים, ייעודו, תפקידיו, סמכויותיו ומבנהו הארגוני ולקדם את הקמתו ואיושו.

על ועדת ההיגוי העליונה להמשיך ולעקוב אחר התקדמות יישום דרישות האבטחה של השב"כ בגופים המוגדרים כתשתיות מדינה קריטיות ולבחון, בשיתוף השב"כ, דרכי פעולה לשיפור מהיר של המצב בתחום.

על ועדת ההיגוי העליונה לבחון מתכונת דיווח לממשלה על מצב ההגנה על המרחב הקיברנטי הישראלי בכלל, ועל תשתיות קריטיות בפרט, ובכלל זה על תהליכי המיפוי וההגדרה של גופים במשק כתשתיות מידע קריטיות. רצוי כי דיווח כזה יכלול מדדים כמותיים כך שיתאפשר לממשלה לבחון את מצב ההגנה גם על בסיס מדדי תפוקה ותוצאה רלוונטיים.

על השב"כ לבחון את הצורך בדיווח למועצות המנהלים של התאגידים שיש בהם תשתיות מחשוב קריטיות על אי-עמידה בהנחיותיו המציבה בסיכון תשתית מדינה חיונית או את הפעילות העסקית של אותו תאגיד.

על המטה הקיברנטי והשב"כ, בשיתוף משרד המשפטים וגורמים ממשלתיים נוספים הנוגעים בדבר, לבחון דרכים לאכוף על הגופים הציבוריים כהגדרתם בחוק להסדרת הביטחון, המוגדרים תשתיות מדינה קריטיות, את מילוי הנחיות השב"כ, ולשקול את עיגונן של דרכי האכיפה בדין.

נוכח הליקויים שהועלו בדוח זה בתחום הליך קבלת ההחלטות, על כל הגורמים הנוגעים בדבר להפיק לקחים ולמנוע הישנותם של פגמים כאלה בהחלטות עתידיות בכלל, ובתחום ההיערכות הלאומית להגנת המרחב הקיברנטי בפרט.

סיכום

התלות של ארגונים רבים במערכות הממוחשבות שלהם גדלה והולכת. האירועים אשר מתרחשים במרחב הסייבר הכלל-עולמי מלמדים על מגמת העלייה הדרמטית באיום הנשקף במרחב הסייבר הן במספר האירועים והתקיפות הצפויים והן במורכבותם. החלטת הממשלה מ-2011 הביאה להקמת המטה הקיברנטי הלאומי בתחילת שנת 2012 והטילה עליו להסדיר את האחריות לטיפול במרחב הקיברנטי ולהגיש הצעה לתפיסת הגנה כוללת לממשלה תוך 120 יום מהקמתו. הקמת מטה הסייבר הלאומי הרחיבה והעמיקה את הפעילות הממשלתית בתחום הסייבר. עם זאת, ממצאי דוח זה מלמדים על כך שקיימים פערים בין עצמת האיום על כלל המרחב הקיברנטי האזרחי ובין קצב ההתארגנות והמענה מבחינת ההיערכות המדינתית להגנתו, להוציא תחומים ומגזרים מעטים כמו תשתיות מדינתיות קריטיות.

בפברואר 2015, בחלוף כשלוש שנים וחצי מאז הקמת מטה הסייבר, קיבלה הממשלה שתי החלטות בנושא. נוסח החלטת הממשלה העוסקת בהסדרת האחריות לפעולה במרחב הסייבר אינו בהיר דיו, בכל הקשור לסמכות ולאחריות הגופים העוסקים בנושא, וגם בהליך גיבוש ואישור מסמך תפיסת ההגנה נפלו כמה ליקויים.

הסדרת האחריות לטיפול במרחב הסייבר, הקמת הרשות והסדרת שיתוף הפעולה בינה ובין הגופים הפועלים במרחב הסייבר הן פעולות מורכבות ורגישות הכוללות היבטים מבצעיים, תקציביים, טכנולוגיים ומשפטיים. תכליתו של דוח זה להעלות את הנושא למסילה של יישום מיטבי. על כן יש לתת את הדעת לממצאי הדוח, ולפיהם בעבודת המטה ובתהליך קבלת ההחלטות על הסדרת האחריות לטיפול בתחום הקיברנטי במדינת ישראל נפלו ליקויים מהותיים. יש ללמוד ממצאים אלה הן לצורך הפקת הלקחים הנדרשת לעניין הליכי התכנון וההחלטה ברמה הלאומית בעתיד, והן לצורך קידום המשימות הנדרשות בתחום ההיערכות לאבטחת המרחב הקיברנטי.

קיימים פערים בין עצמת האיום על כלל המרחב הקיברנטי האזרחי ובין קצב ההתארגנות והמענה מבחינת ההיערכות המדינתית להגנתו