מבט על, גיליון 856, 18 בספטמבר 2016

התארגנות ישראל להגנה בסייבר: תמונת מצב ומשמעויות

שמואל אבן, דוד סימן טוב וגבי סיבוני

באפריל 2016 החלה הרשות הלאומית להגנת הסייבר ("הרשות") לפעול באופן רשמי. תפקידה הראשון והעיקרי הוא: "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" (החלטת ממשלה מספר 2444 מ-15 פברואר 2015). ראש הרשות כפוף לראש מטה הסייבר הלאומי, שמוגדר כראש מערך הסייבר הלאומי.

ההיגיון שהנחה את הקמת הרשות הוא כי לשם ההגנה בסייבר נדרש שיתוף פעולה הדוק עם כל גורמי המשק ועל כן נדרש להקים רשות אזרחית, שעיסוקה בתחום הגנת סייבר בלבד ואשר תיטול על עצמה בעתיד גם חלק מהפעילות שביצע השב"כ בהקשר להגנה על תשתיות לאומיות חיוניות. סביב הקמת הרשות נסובו מחלוקות ומתחים אשר לחלוקת האחריות בין הגופים. ב-9 ביוני 2016 גובש מסמך הבנות בין הרשות לשב"כ במטרה להסדיר את הפעילות, אולם מדובר במתח מובנה שעתיד ללוות את הפעילות.

במקביל חלו התפתחויות תפיסתיות וארגוניות בצה"ל. ביוני 2015 החליט הרמטכ"ל, ראי"ל גדי איזנקוט, להקים זרוע סייבר עצמאית אשר תוביל בצה"ל את פעילות ההגנה וההתקפה בממד הזה. כשלב מקדים הוקמו מטה סייבר במטכ"ל, הוקמה חטיבת הגנה באגף התקשוב ובוצעו שינויים ארגוניים באגף המודיעין.

באוגוסט 2016 פרסמה ועדת החוץ והביטחון של הכנסת דוח בנושא "בחינת חלוקת האחריות והסמכות בנושא הגנת הסייבר בישראל". הדוח הוא פרי עבודתה של ועדת משנה לנושא ההגנה בסייבר בראשות ח"כ אבי דיכטר, ראש השב"כ לשעבר. מטרת הוועדה היא "ללמוד ולפקח על אופן ההיערכות המדינתית להגנת הסייבר, ולבחון את משמעויות החלטת הממשלה על הקמת הרשות ואופן מימושה". המסמך הופץ בפומבי, ולפיכך מזמין דיון ציבורי.

לפי דוח הוועדה: "תהליכי העבודה, כפי שהוצגו לוועדה, מייתרים הלכה למעשה את משמעות כפיפותו של ראש הרשות לראש המערך. שכן, ראש הרשות הינו עצמאי, בליבת עשייתו, ההגנה בסייבר, ולא מחויב לקבל אישור מראש המערך להחלטותיו ולפעולותיו בתחום". "הועדה לא השתכנעה בצורך בקיומן של שתי יחידות סמך עצמאית במשרד ראש הממשלה העוסקות בתחום הסייבר". משמעותם של דברים אלה היא כי הוועדה סבורה שיש לבחון את מקומו הארגוני הנכון של מטה הסייבר הלאומי וסימנה יעד זה לבחינה בהמשך עבודתה.

להלן מסקנות נוספות, שאליהן הגיעה הוועדה:

- אין להפוך את הרשות להגנת הסייבר לסוכנות איסוף מודיעין נוספת. עליה להתבסס על מידע שיאספו גורמי קהילת המודיעין ועל חומר גלוי.
- הוועדה קובעת שנוסח חוק הסייבר המתגבש חייב להיכתב בשיתוף ומעורבות כל הגורמים הרלוונטיים במערכת הביטחונית והאזרחית. כן יש להבטיח שהמגבלות שחלות על השב"כ מבחינת זכויות הפרט ייחולו גם על הרשות.
- הוועדה התרשמה מחולשת המשטרה בתחום הסייבר, הנובעת ממגבלות חוקיות והעדר משאבים, והמליצה להרחיב את הדיון בנושא.
- במצב מלחמה, הוועדה רואה חשיבות בהעברת האחריות לתכלול ולניהול ההתמודדות במרחב הסייבר לגורם המוביל את המערכה (צה"ל/שב"כ), בהתאם למתאר העימות, כאשר "פורם ההגנה של הרשות" ימשיך לפעול באופן שיאפשר לה להשפיע באופן ישיר ובאמצעות נציגות במכלול המלחמתי בהובלת צה"ל.
- הוועדה ממליצה לשוב ולבחון באופן עתי, במהלך חמש השנים הקרובות, את ההסדרה בתחום הסייבר, נוכח עוצמת האיום והניסיון המועט יחסית של ההתמודדות עמו.

<u>משמעויות והמלצות</u>

ראשית, חיוני להבהיר כמה מושגי יסוד: "הסייבר", "ביטחון הסייבר" ו"הגנת הסייבר". הסייבר הוא שם כללי למכלול פעילויות, תופעות ותפוקות שיוצרות מערכות ממוכנות ממוחשבות, רשתות מחשבים ותקשורת וכו' (ראו: הגדרת מרחב הסייבר בהחלטת ממשלה מ-7 בנובמבר 2011). על כן, חברות הסייבר הן כל חברות הטלפוניה, המחשוב, ספקי האינטרנט, לווייני תקשורת, וגם חברות העוסקות בהגנת ובאבטחת הסייבר. ביטחון הסייבר הוא תחום מצומצם יותר אך רחב דיו, העוסק ביציבותו ובהתנהלותו הסדירה של מרחב הסייבר הלאומי, למשל מידת תלותה של ישראל בלווייני תקשורת, בחברות הסלולר וכו'. תחום הגנת הסייבר הוא חלק מתחום ביטחון הסייבר, ורק עליו ממונה הרשות (למעט הגנה על גופים ביטחוניים, גופים המונחים על ידי הממונה על הביטחון במערכת הביטחון (מלמ"ב) וגורפים אחרים שהוחרגו מאחריותה של הרשות). לאור זאת, ישראל זקוקה לאסטרטגיית סייבר לאומית על כל היבטיה, ובכלל זאת כדי לשפר את ביטחון הסייבר ואת ההגנה בסייבר. גיבוש אסטרטגיית הסייבר הלאומית, כמו גם אסטרטגיה לביטחון הסייבר, צריך להיות באחריות מטה הסייבר הלאומי, לקבל את אישור הקבינט והממשלה ועל עיקריה להתפרסם בציבור.

מושג חיוני נוסף הוא "אירוע סייבר", המופיע בהחלטת ממשלה מפברואר 2015. נכון להגדיר מושג זה כאירוע שיש עמו סיכון או פגיעה בסייבר, מכל סיבה שהיא: תקלה, שריפה, אסון טבע, מעשה פלילי ופגיעה קינטית – ולא רק כתוצאה מתקיפות סייבר לוגיות של אויבים. אפשרויות אלה אינן ברורות בהחלטת הממשלה ובדוח הוועדה. אם מקובלת הגדרה זו של המושג, הרי שעל הרשות החדשה לתת מענה לכל סוגי הסיכונים והאירועים הללו.

לאור הקמת הרשות, מוצע כי מרכז הכובד של מטה הסייבר יעבור בהדרגה לנושאים הקשורים לתחום הסייבר הלאומי בכלל (פיתוח התעשייה, עידוד המחקר והפיתוח, בניית ההון האנושי, העמקת החינוך והמשילות באמצעות הסייבר, ועוד), ובפרט לנושאים הנוגעים לביטחון הסייבר הלאומי – כגון מבנה, יציבות ושרידות מרחב הסייבר הלאומי בשגרה ובחירום – בתחומים שמעבר לתחום עיסוק הרשות ואשר יוגדרו בבהירות. לאחר שהרשות תתבסס במשרד ראש הממשלה, יש לשקול את העברתה למשרד ממשלתי מתאים יותר.

אשר לשינויים הארגוניים, יש להגדיר את הממשקים ותחומי האחריות והסמכות בין הרשות, צה"ל וקהילת המודיעין. למשל, הרשות נדרשת לעסוק גם בניתוח ומחקר מודיעיני וגם באיסוף ממקורות במערכת האזרחית בישראל ומחוצה לה (מידע מהשטח, מחברות אזרחיות ומעמיתים בחו"ל). עניין זה מעורר למשל את השאלה כיצד תתגבש בישראל תמונת מודיעין אחודה כאשר סימנים על תקיפה כלשהי יהיו בחצרה של הרשות, שאינה חוקרת את היריב על רוב היבטיו, ואילו והמידע והידע המסבירים את סימני התקיפה (מי האויב, מה כוונתו וכו') יהיו בחצרה של קהילת המודיעין. לכן, מומלץ להגדיר בראייה מערכתית את חלוקת האחריות ושיתוף הפעולה בין כלל הגופים העוסקים בלוחמת סייבר בהקשרי מודיעין, הגנה, התקפה וניהול מערכה משולבת. למשל, יש להגדיר מי מספק את תמונת המודיעין וההתרעות, ומי יפקד על המערכות בסייבר על כול היבטיהן.

מומלץ להסדיר את תפקידו של צה"ל בחירום ובמלחמה בהקשר להגנת מרחב הסייבר, ואת הממשקים בינו לבין הרשות ובין השירותים החשאיים למשטרה. תהליכי הסדרה ראשוניים כבר הותנעו, אולם יש עוד כברת דרך רבה ללכת. הצעת הוועדה כי צה"ל יהיה אחראי על הובלת הגנת הסייבר במדינה במלחמה אינה הולמת את המציאות הקיימת, בעיקר בשל העובדה שמי שאינו מצוי ופועל לעומק במרחב הסייבר המדינתי בשגרה יתקשה לקחת אחריות אפקטיבית על המשימה עם המעבר למצב חירום.

ולבסוף, שינוים ארגוניים, מורכבים ככל שיהיו, אינם מעידים על יכולות ועל שיפור יכולת ההתמודדות ההגנתית בסייבר. לפיכך, מומלץ לבחון ולקבוע קריטריונים ומבחנים מעשיים לכושר העמידה של מערך ההגנה בסייבר, שיאפשרו להעריך את המצב הקיים ואת התרומה הנוספת של העשייה בעתיד.