

בים, באוויר, ביבשה. ובסייבר?

רוני קציר¹

תוכן

- 1..... בים, באוויר, ביבשה. ובסייבר?
- 2..... מבוא
- 2..... מהי "לוחמה קיברנטית"?
- 4..... התפתחות המוסדות להגנה בסייבר בישראל
- 5..... הגנה במרחב הקיברנטי מול הגנה מפני לוחמה קיברנטית
- 6..... צבא ההגנה לישראל – הגנה גם בסייבר
- 7..... אחדות הפיקוד: בין סייבר לעורף
- 9..... הפלמ"ח והסייבר
- 10..... סיכום
- 11..... אחרית דבר
- 12..... רשימת מקורות

¹ סגן אלוף רוני קציר הוא ראש ענף זרועות במחלקת הייעוץ והחקיקה בפרקליטות הצבאית. המאמר נכתב במסגרת הקורס הכלל זרועי לפיקוד ולמטה (פז"ם) "אפק" מחזור ל".

מבוא

"קיבלתי החלטה לפתח רשות לאומית לנושא הסייבר שתסדיר וגם תדאג להגנת כלל מדינת ישראל בנושא הסייבר. כלומר, לא רק ההגנה על המתקנים החשובים וגופי הביטחון, אלא כיצד להגן על אזרחי ישראל מפני התקיפות הללו. זוהי רשות חדשה, זה בעצם להקים 'חיל אוויר' נגד אימים חדשים ... אנחנו בעולם חדש, אנחנו מתארגנים עם כוחות חדשים".²

במילים אלו פתח ראש הממשלה, מר בנימין נתניהו, את ישיבת הממשלה שבה הודיע על החלטתו להקים את "הרשות הלאומית להגנת הסייבר", אשר תהיה הזרוע הביצועית של המטה הקיברנטי. כמה חודשים לאחר מכן, התקבלה החלטת הממשלה המקימה את הרשות.³ ייעודה של הרשות יהיה להגן על המרחב הלאומי בסייבר (סב"ר).⁴ בכלל זה, היא תפעל לגיבוש תמונת המצב הלאומית בתחום, תידרש לזהות אימים ותקיפות, להתמודדות עם תקיפות ולטפל באירועים בזמן אמת. הכול בשיתוף פעולה עם הגורמים הביטחוניים הרלוונטיים. החלטה זו שמה קץ (לעת עתה) לוויכוח ממושך בין שירות הביטחון הכללי ובין המטה הקיברנטי הלאומי בשאלה מי יהיה הגורם האמון על הגנת המגזר האזרחי מפני אימים במרחב הקיברנטי. באופן תמוה, מהוויכוח נעדר קולו של צבא ההגנה לישראל. מההחלטה עולה כי צבא ההגנה לישראל לא יהיה הגוף שיישא באחריות (ובסמכות) להגן על גבולות ישראל מפני אימים במרחב הסייבר. "חיל הסייבר" יקום, אך בניגוד לחילות האוויר, הים והיבשה – הוא יקום ויתקיים מחוץ לצה"ל.

מאמר זה דן במשמעויות המעשיות הנובעות מהחלטת הממשלה להקים רשות לאומית להגנה בסייבר, ועל תפקידו של צה"ל בתחום זה. המאמר בוחן באופן ביקורתי את ההחלטה להפקיע את האחריות להגנה הלאומית במרחב הקיברנטי מידי צה"ל, ולהפקיד אותה בידי גוף חדש אשר אמור להיות אמון על הגנת האינטרסים האזרחיים במרחב הקיברנטי.

כדי לבחון את הסוגיה, נבחן תחילה את משמעות המונח "לוחמה קיברנטית" (cyber warfare) ונבין את סוג האיום על מדינת ישראל. בהמשך נסקור את ההתפתחות של המוסדות הישראליים העוסקים בתחום. הדבר ישמש לנו רקע לדיון בשאלה מי הגוף המתאים לשאת באחריות להגנה במרחב הקיברנטי, בהתייחס, בין היתר, לייעודו ולתפקידיו של צה"ל, ולקשיים הגלומים בהפעלת צה"ל על ידי גורם אזרחי.

מהי "לוחמה קיברנטית"?

האיום במרחב הקיברנטי נושא פנים רבות, ואולם נראה כי כדי לממש איום בקנה מידה אסטרטגי כלפי מדינה, אשר נהנית מהיערכות מתקדמת בעולם הקיברנטי כמו מדינת ישראל, נדרש שילוב של **כוונה** ושל **אמצעים**. מבלי להתייחס לכוונות ומתוך הנחה שהן קיימות, נציין כי אמצעים לפעולה בתחום זה נגד מדינה מתקדמת מצויים כיום בעיקר בידיהן של המעצמות. אולם אמצעים אלו עלולים להגיע לידי ארגוני טרור ומדינות התומכות בטרור נגד ישראל. על כן ברור כי האיום

² דברים מתוך ישיבת הממשלה מ-21 בספטמבר 2014. ראו: בסוק, "נתניהו: תוקם רשות לאומית להגנה אופרטיבית בסייבר", 21 בספטמבר 2014.

³ החלטה 2444 של הממשלה מ-15 בפברואר 2015.

⁴ האקדמיה ללשון העברית בשיתוף מכון התקנים הישראלי ומטה הסייבר הלאומי במשרד ראש הממשלה קבעו שהמונח העברי לסייבר הוא סב"ר – סביבה רשתית.

המרכזי גם במרחב הסייבר נותר עדיין האיום הביטחוני, או ליתר דיוק **איום "הלוחמה הקיברנטית"**.

הקשר בין התפתחות עולם הטכנולוגיה ובין התפתחותו של שדה הקרב המודרני, אינו מוטל בספק. הצפת המידע, הטכנולוגיות שחדרו לשדה הקרב, וההנגשה של יכולות תקיפת קיברנטיות לכל אדם אשר יש לו גישה למחשב אישי – כל אלו הביאו לשינוי מהותי במאפייני המלחמה,⁵ והולידו את המונח "לוחמה קיברנטית".

בשנות ה-90, התפתח לראשונה המושג "לוחמת מידע".⁶ הוגים צבאיים שונים ובראשם המלומדים אלווין והידי טופלר דנו בחשיבות המידע והשליטה במידע בשדה הקרב. באותה עת, ההנחה הרווחת הייתה שלוחמת מידע ולוחמה קיברנטית חד הם.⁷ הוויכוח המושגי התעורר כאשר פורסם מאמרם של ארקילה ורונפלדט, מומחים למדעי המדינה ממכון המחקר 'ראנד' (RAND), הנושא את הכותרת מברשת הטובות – "Cyberwar is coming!"⁸, וחווה שינוי עמוק במבנה הארגונים הצבאיים, לנוכח התרחשותה הצפויה של לוחמה קיברנטית, **המבוססת כולה על מידע שזורם באמצעים אלקטרוניים**.

מאותו רגע ואילך, נחלק העולם לשניים – "האלרמיסטים", רואי השחורות, המנבאים כי היכולות המתפתחות בעולם הקיברנטי עלולות למוטט מדינה מודרנית; והספקנים, אשר מבינים שקיים איום קיברנטי שאף עלול לפגוע באזרחים או בתשתיות לאומיות, אך רואים בו מטרד בלבד, אשר אינו איום לאומי.⁹ על גבי הציר הזה התפתח לאורך השנים הדיון על המדיניות האמריקנית להתמודדות עם איום הקיברנטי. עם זה, הניסיון שנצבר בשנים האחרונות הוביל להסכמה כללית אחת: בניגוד לתפיסה שביטאו ארקילה ורונפלדט, נוטים היום לחשוב **שהממד הקיברנטי אינו שדה לחימה עצמאי**. בדיוק כפי שלא סביר שבשדה הקרב המודרני, תתרחש מלחמה רק בממד אחד – באוויר, בים או ביבשה – כך גם לא סביר שתתרחש מלחמה רק בממד הקיברנטי. אירוע התקיפה באיראן, הידוע בשם 'סטוקנט' (Stuxnet), חיזק גישה זו. מתקפה זו נחשבת לאחת המתקדמות בתחום, והיא הייתה הראשונה אשר הסבה נזק פיזי של ממש.¹⁰ אולם, אף שניכר שהושקעו במתקפה מאמצים רבים, הרי שהתוצאה של התקיפה הייתה, לכל היותר, "מכה קלה בכנף" של תוכנית הגרעין האיראנית.¹¹ בהקשר הצבאי היכולות הקיברנטיות הן, אם כן, תוספת משוכללת לארסנל הכלים של הכוחות הלוחמים, כפי שהיו בעבר גם המטוס, הצוללת ופצצת הגרעין. הבנה זו של האיום הקיברנטי, ראוי שתעמוד בבסיס הדיון על האופן שבו יש להתגונן מפניו.

⁵ ראו למשל:

Hughes, "Towards a Global Regime for Cyber Warfare", pp. 106-117.

⁶ לניתוח המשמעויות של לוחמת המידע מנקודת המבט של סוף שנות ה-90, ראו: בן ישראל, "לוחמת מידע", עמוד 18.

⁷ ראו למשל: ברעם, "ההיערכות למלחמה קיברנטית", עמודים 22-27.

⁸ Arquilla and Ronfeldt, "Cyberwar is coming", pp. 141-165.

⁹ Sammaan, Cyber Command, The Rift in US Military Cyber Strategy, *Rusi journal*, 155: 16-21 (2010).
Ryan Singel, 'White House Cyber Czar: There Is No Cyberwar', *Wired.com*, 4 March 2010.

¹⁰ ראו למשל:

David Kushner, "The Real Story of Stuxnet", *IEEE spectrum*, (26 February 2013).

¹¹ על כך נכתב: "אומנם התקפות טריוויאליות הן פשוטות לביצוע במרחב הקיברנטי, אך אין להסיק מכך שהתקפות תשתית נרחבות אף הן פשוטות לביצוע".

Lindsay, "Stuxnet and the Limits of Cyber Warfare", 365-404.

התפתחות המוסדות להגנה בסייבר בישראל

מדינת ישראל הייתה מהראשונות לזהות את האתגרים המתפתחים במרחב הקיברנטי. עוד בשנת 1997 הוקם מיזם תהיל"ה (תשתית הממשלה לעידן האינטרנט), אשר היה אמון על הגנת החיבור של משרדי הממשלה למרשתת (אינטרנט). בשנת 2002 הוחלט על הקמת הרשות הממלכתית לאבטחת מידע בשב"כ.¹² תפקיד הרשות הוא הנחיה מקצועית בתחום אבטחת תשתיות המחשב, לגופים בעלי חשיבות לאומית מפני איומי טרור, ריגול וחשיפה.¹³ עם התגברות האיומים במרחב הקיברנטי¹⁴ הוקם בנובמבר 2010 צוות מיוחד שעסק בגיבוש תוכנית לאומית שתכליתה להציב את ישראל בין חמשת המדינות המובילות בעיסוק במרחב הקיברנטי. בעקבות עבודה זו, שכונתה "המיזם הקיברנטי הלאומי", החליטה הממשלה באוגוסט 2011 להקים מטה קיברנטי לאומי במשרד ראש הממשלה. ייעודו של המטה הקיברנטי הוא לגבש את תפיסת ההגנה של מדינת ישראל במרחב הקיברנטי, תוך יצירת שיתוף פעולה בין הגופים הממשלתיים, האקדמיה, התעשייה והמגזר הפרטי. כמו כן, אמון המטה על בניית תוכנית לפיתוח תשתיות טכנולוגיות ומחקריות בתחום.¹⁵ המטה הקיברנטי הוקם על פי המלצת צוות שבראשו עמד יו"ר המועצה הלאומית למחקר ולפיתוח, האלוף (במיל') פרופסור יצחק בן ישראל. הקמת המטה ביקשה לתת "גג אסטרטגי" לכלל היחידות האופרטיביות המספקות הגנה במרחב הקיברנטי (שב"כ, צה"ל, משטרת ישראל וכיו"ב).¹⁶

הצעד הבא בפיתוח התשתית הלאומית להגנה במרחב הקיברנטי, היה הקמת הרשות הלאומית להגנת הסייבר. בהמשך להכרזתו של ראש הממשלה שהובאה בראשית המאמר, ב-15 בפברואר 2015 קיבלה ממשלת ישראל החלטה שכותרתה "קידום היכולת הלאומית במרחב הקיברנטי". ההחלטה קובעת שבמשרד ראש הממשלה תקום "רשות לאומית להגנת הסייבר, שייעודה הגנת מרחב הסייבר". תפקידה המרכזי של הרשות 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...".¹⁷ עוד נקבע כי ברשות יפעל מרכז לסיוע בהתמודדות עם איומי סייבר (ה- CERT – Computer Emergency Readiness Team), אשר תפקידיו דומים לגופים מקבילים בעולם שהוקמו כדי לרכז את המידע הרלוונטי בתחום ההגנה בסייבר, ולשתף בו את כלל הגורמים במשק (לרבות גורמים אזרחיים) באופן שיטיב את המוכנות הלאומית להתמודדות עם מתקפות קיברנטיות. הרשות אמונה עוד על עיצוב, על יישום ועל הטמעת תורה לאומית להגנה בסייבר, וכן

¹² החלטת ועדת השרים לענייני ביטחון ב/84 מ-11 בדצמבר 2002.

¹³ סמכויות השב"כ בעניין זה הן מכוח החוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998.

¹⁴ החל משנת 2007 נצפו בעולם כמה תקיפות במרחב הקיברנטי במסגרת סכסוכים בין מדינות, כגון תקיפת רוסיה על אסטוניה ועל גאורגיה, התקפות סין בארה"ב והתקפת סטוקנט (Stuxnet) באיראן שהוזכרה לעיל. לאחרונה אף פרסמה חברת 'קספרסקי' תיעוד למתקפה שבוצעה נגד המדינות אשר היו מעורבות בחיפוש של המטוס המלזי, אשר נענתה באופן מיידי במתקפת נגד מצד אחת המדינות שהותקפו.

Raiu and Golovkin, "The Chronicles of the Hellsing APT: The Empire Strikes Back", **Securelist** (15 April 2015).

לסקירה מעמיקה של אירועי התקיפה שזכו לפרסום ראוי: אפק, "שוברים את הכללים וכולם משחקים", עמודים 45 – 75.

¹⁵ סקירה רחבה על התפתחות העיסוק בתחום הקיברנטי בישראל מופיעה במחקר צה"לי פנימי.

¹⁶ ראו גם: אבן וסימן טוב "לוחמה במרחב הקיברנטי, מושגים, מגמות ומשמעויות לישראל", עמוד 68.

¹⁷ החלטה 2444 של הממשלה מ-15 בפברואר 2015 (לטקסט הוספו הדגשות המחבר).

על היערכות ועל כשירות המשק בסייבר, ועל ביצוע אסדרה (רגולציה) שתאפשר הנחיה של המשק ושל שוק שירותי הגנת הסייבר.

משמעות ההחלטה היא שלצד המטה הקיברנטי תוקם **זרוע ביצועית**, אשר תישא באחריות, בסמכות וביכולות לבצע פעולות **זימות** במרחב הסייבר, לטובת ההגנה הלאומית. אחריות הרשות תתפרס על כלל מאמצי ההגנה במרחב הסייבר, ועולה מן ההחלטה כי יתר הגופים הפועלים במרחב זה, הגם שנשמרה עצמאותם בתחומים מסוימים, אמורים להתנהל על פי הנחיותיה ותורת הפעולה שתיקבע על ידה.

לצד הגופים הלאומיים, גם בצה"ל הוקמו גופים העוסקים בתחום הסייבר. אחד הגופים הוא מטה הסייבר, הכפוף ליחידה 8200. גוף זה אמון בעיקר על ההיבטים האופרטיביים של הלחימה בסייבר.¹⁸ גוף אחר הוא מחלקת ההגנה בסייבר, באגף התקשוב. משימתה המרכזית של מחלקה זו היא לסכל תקיפות מודיעיניות ולמנוע שיבוש במרכיבי מערכות המחשוב של צה"ל ופגיעה בהם, כדי להבטיח את רציפותם של תהליכי המחשוב, את זמינותם ואת מהימנותם. לגוף זה יש כיום יכולות טכנולוגיות מתקדמות ביותר, והוא פיתח תפיסות לחימה פורצות דרך שבאמצעותן הוא מממש את אחריותו. עם זה, מייעודה של המחלקה עולה כי היא מבצעת בעיקר משימות אשר מוגדרות בתורת הלחימה הצבאית כמשימות '**אבטחה**', **משל הייתה זאת הגנה על מחנות צה"ל**. לעומת זאת, המחלקה אינה עוסקת **בהגנה** מערכתית או לאומית, שמשמעה הוא שמירה על **גבולות המדינה ועל ביטחון אזרחיה** מפני איומי אויב.¹⁹

הגנה במרחב הקיברנטי מול הגנה מפני לוחמה קיברנטית

אפשר למצוא הגדרות רבות למונח המרחב הקיברנטי (מרחב הסב"ר). המכנה המשותף להגדרות אלו היא ההבנה שמדובר בממד סבוך ומתפתח, שהניסיון להגדירו כמעט שנדון לכישלון מראש. על כן במאמר זה לא נעסוק בהגדרת המרחב, אולם ננסה לבחון מהי ההגנה הדרושה במרחב הסייבר, ונבקש להבחין בין איומים על המרחב, ובין האיום שמקורו ב"לוחמה קיברנטית".

אחד המעצבים העיקריים של האסטרטגיות המדיניות במרחב הקיברנטי הוא ההכרה בכך שמחד גיסא, מדובר במרחב חיוני לשם התפקוד השוטף של המדינה המודרנית, ומאידך גיסא, המרחב חשוף לאיומים מגוונים, אשר בחלקם שונים מהאיומים הקלסיים המופנים נגד ישות מדינתית. כך למשל, מפגע אנונימי בודד הפועל במרחב הקיברנטי, ומנסה לפגוע במוסדות אזרחיים (כגון, בנקים) ממניעים פליליים, יכול לגרום למדינה שאינה מתגוננת כראוי לנזקים אסטרטגיים ואף לנזקים ביטחוניים של ממש. מכאן נובע כי היערכות נכונה להגנה מדינתית במרחב הקיברנטי, **מחייבת שילוב בין המערכות הממשלתיות למערכות האזרחיות, הן בהקמת מערכות ההגנה, הן באיסוף המידע, והן בהתמודדות עם איומים בזמן אמת.**

ניתן להבחין בין שלושה מרחבי הגנה בסייבר. מרחב ההגנה על התשתיות הקריטיות (אשר עליו אמון כיום השב"כ);²⁰ מרחב ההגנה הממשלתי-אזרחי, אשר מוגן כיום על ידי אגף התקשוב

¹⁸ כהן, "8200: לא מחפשים רק חננות עם משקפים".
¹⁹ כך למשל, "מבצעים הגנתיים" מוגדרים כ"בלימת התקפת האויב ומניעת כיבוש השטח המוגן..." (אמ"ץ, **תורה בסיסית מבצעים**, עמוד 77). צורת הקרב הגנה מוגדרת כ"צורת קרב טקטית שנועדה לבלום התקפת אויב ולמנוע את כיבוש השטח שמגנים עליו, או למנוע פגיעה באנשים ובציוד אשר נמצאים במרחב ההגנה ואשר המגן מופקד על ביטחונם..." (זרוע היבשה, **מבצעי כוחות היבשה**, כרך שלישי, מבצעים הגנתיים, עמוד 3).

²⁰ החלטת הממשלה קובעת כי האחריות במרחב זה תועבר תוך שלוש שנים מהשב"כ לרשות הלאומית להגנת הסייבר.

הממשלתי, ומרחב ההגנה הביטחוני, שבו כל ארגון ביטחוני "מגן בגזרתו". נוסף על כך, יש להיערך באופן ייעודי להגנה "חוצת מרחבים". לדוגמה, בתחום הפלילי נדרשת מעטפת הכוללת מניעה, חקירה ואכיפה של פשיעה בסייבר, וכיום האחריות לכך נתונה למשטרת ישראל. לעומת זאת, בתחום הביטחוני, הגנה "חוצת מרחבים" דורשת איסוף מודיעין לטובת התרעה וסיכול תוקפים ומרכז לאומי לניהול המערכה, זיהוי וחקירה. משימת איסוף המודיעין, יש לרכז באמצעות מחלקה ייעודית שתקום במטה הסייבר הלאומי. באשר למרכז הלאומי לניהול המערכה, ניתן לזהות עמדה הגורסת כי יש להקים בצה"ל "פיקוד סייבר", אשר ישמש כזרוע האופרטיבית בתחום הסייבר בעת התרחשות אירוע או מצב חירום. **הטעמים לכך הם פרקטיים בעיקרם.** ממד הסייבר הוא ממד של לחימה, וצה"ל הוא הארגון היחיד שבכוחו להציב במהירות וביעילות מענה לאיומים המתהווים, תוך ניצול משאביו התקציביים ואיכות כוח האדם העומד לרשותו. כמו כן, יש לצה"ל הגמישות האופרטיבית לפעול בכלל מרחבי הלחימה. **לצד זאת, משתקפת ההבנה כי האחריות להגנה על המגזר האזרחי, צריכה להיות בידי גורם אזרחי הפועל תחת המטה הקיברנטי הלאומי.**²¹

הקמת הרשות הלאומית להגנה בסייבר, שתפקידיה תוארו לעיל, מלמדת שהתפיסה שאימצה ממשלת ישראל היא לתת מענה אחד לאיום הביטחוני והאזרחי, באמצעות רשות אזרחית אחת, אשר מכווניה גם את פעולות כוחות הביטחון. הרשות נדרשת "לנהל, להפעיל ולבצע" את כלל הפעולות האופרטיביות בהגנה במרחב הקיברנטי. נראה כי הרשות המוקמת אמורה לפרוס כנפיה מעל כלל מעגלי ההגנה, **ואף להוביל את הטיפול בהגנה "חוצת המרחבים" – הן בהיבטי האיסוף והן בהיבטי ניהול המערכה.**²² המענה המוצע מצריך תפיסה הוליסטית (שלמה) של האיומים במרחב הסייבר והתשתיות הישראליות, והוא תואם את הגישה הרואה במרחב הקיברנטי **ממד לחימה חדש** אשר דורש מענה ייחודי.

צבא ההגנה לישראל – הגנה גם בסייבר

אחד הטעמים המרכזיים להקמת רשות אזרחית להגנה בסייבר הוא התובנה שחלק ניכר מתרחישי האיום כרוכים בתקיפה של מטרות אזרחיות. לפיכך, ובהתחשב באופיו של ממד הלחימה הקיברנטי, מימוש האחריות כרוך גם בהפעלת סמכות על גורמים אזרחיים.

ההבנה של המושג "לוחמה קיברנטית", כאמור, חותר תחת תובנות אלו. כל עוד המרחב הקיברנטי נתפס כמרחב לחימה ייחודי והוליסטי, יש יסוד לסברה שגם המענה לו צריך להיות שונה. אולם אם מקבלים את התפיסה שה"לוחמה הקיברנטית" אינה מושג עצמאי, אלא היא הרחבה של שדה הקרב הקיים, הרי שההתמודדות עם האיום צריכה להיות אף היא כחלק מההתמודדות עם מארג האיומים המופנים כלפי המדינה. תפיסה זו, משיבה למרכז הדיון את הגורמים הצבאיים.

במדינת ישראל, צה"ל הוא הישות האמונה על הגנת גבולות המדינה מפני איומים חיצוניים. מעמדו עוגן בחוק יסוד: הצבא, אשר קובע כי "צה"ל הוא צבאה של המדינה".²³ פקודת סדרי השלטון

²¹ מחקר פנימי צה"לי.

²² מחקר פנימי צה"לי.

²³ חוק יסוד: הצבא, התשל"ו-1976.

והמשפט מוסיפה וקובעת כי תפקידו של הצבא הוא "לעשות את כל הפעולות הדרושות והחוקיות לשם הגנת המדינה ולשם השגת יעדיה הביטחוניים לאומיים".²⁴ מכאן גם נגזר ייעודו של צה"ל הקובע כי "בכפופות לשלטונות המוסמכים של מדינת ישראל ולפי החלטותיה, צה"ל נועד . . . להגן על מדינת ישראל כפי שהוקמה, על השלמות הטריטוריאלית ועל הגבולות של שטחיה . . . על שלום אזרחיה, . . . וכל אינטרס לאומי אחר . . . מפני כל אויב ואיום חיצוניים ופנימיים".

דומה כי אין חולק שבמסגרת ייעודו ותפקידיו, צה"ל אחראי להגן גם על מוסדות אזרחיים, כגון חברת החשמל, חברת מקורות והבנקים, מפני איומים חיצוניים. ברור לכול, כי צה"ל הוא שאחראי על סיכול תקיפות מהאוויר, מהים ומהיבשה, גם כשאלו מכוונות כלפי אזרחים. **אם כן, במה שונה ממד הסייבר?** הבנה של ה"לוחמה הקיברנטית" כחלק ממארג הלחימה הקלאסי, תומכת במסקנה כי גם האחריות הכוללת להגנה מפני איומי סייבר ראוי שתינתן בידי צה"ל.

יתרה מזאת, לשם מימוש אחריותו, ניתנה בידי צה"ל הסמכות לפעול בשעת חירום גם מול אזרחים. לפיכך, בידי צה"ל נתונות עדיין סמכויות שמקורן בתקנות ההגנה, המאפשרות למשל לסגור שטחים בתוך מדינת ישראל (סמכות המופעלת כעניין שבשגרה), להרחיק אנשים ממקומות מסוימים, לסגור צירי תנועה ואף לתת הנחיות לאזרחים. על כן אין מניעה עקרונית לתת בידי צה"ל את הסמכויות הדרושות כדי לממש את האחריות במרחב הסייבר, וזאת גם אם מימושה כרוך בפגיעה מסוימת בחירויות הפרט.²⁵

הדין המסדיר את הקמתו של צה"ל ככוח המזוין היחידי במדינת ישראל, מעגן עיקרון דמוקרטי בסיסי שלפיו מחד גיסא, המדינה רשאית להגן על קיומה, לרבות באמצעות הפעלת כוח, ומאידך גיסא, הכוח המזוין מרוכז בידי **גורם אחד**, ומוגבל אך ורק לביצוע הפעולות "הדרושות" לשם הגנת המדינה. כמו כן, חוק יסוד הצבא מוסיף וקובע כי "אין להקים או לקיים כוח מזוין מחוץ לצבא הגנה לישראל אלא על פי חוק". משכך, דומה כי דווקא הכוונה להקים גוף אופרטיבי חדש, **אשר יידרשו לו סמכויות הכרוכות בהפעלת כוח גם כלפי גורמים זרים**, הוא שמעורר קושי חוקתי מהותי.

אחדות הפיקוד: בין סייבר לעורף

בחלקים הקודמים של המאמר הראיתי כי איום הסייבר הוא חלק מהמערכה הצבאית, ועל כן נכון שהמענה לו יינתן על ידי צה"ל. ישנה הטענה כי המאפיינים הייחודיים של הלחימה בסייבר, ובהם האנונימיות של התוקף, האפשרות של כל אדם עם מחשב לייצר תקיפה והתוצאות ה"וירטואליות" של התקיפה, מצדיקים הקמת רשות אזרחית, כאשר היכולות האופרטיביות וסמכות הפעלת הכוח, תיוותרנה בידי צה"ל, שיופעל במקרה הצורך על ידי הרשות.²⁶

אפשרות זו עלולה לפגוע בעקרון היסוד של הפיקוד, 'עקרון אחדות הפיקוד'. על פי עיקרון זה כל בעל תפקיד בצה"ל נתון למרותו של מפקד אחד בלבד. פיצול הפיקוד פוגע במשמעת הצבאית.

²⁴ פקודת סדרי השלטון והמשפט, התש"ח-1948.

²⁵ כאשר מובן שהדבר כרוך בביצוע איוון חוקתי בין התכלית שלשמה ניתנת הסמכות ובין עוצמת הפגיעה בפרט. אולם באיוון זה אין הבדל אם הסמכות היא גורם צבאי או גורם אזרחי. כך או כך, הפעלת הסמכות צריכה להיעשות לתכלית ראויה ובמידה שאינה עולה על הנדרש.

²⁶ סביר להניח כי זו אחת מדרכי הפעולה הנבחנות לקראת ביצוע ההחלטה על הקמת הרשות, ולו מהטעמים הפרקטיים שנמנו.

על פי עיקרון זה, אין לתת בידי רשות אזרחית סמכות פיקוד על חיילי צה"ל, אשר כפופים באותה עת גם לפיקוד צבאי.²⁷ אפשר להמחיש קושי זה באמצעות שני תרחישים אפשריים. התרחיש האחד הוא איום של תקיפת סייבר אקראית נגד תשתית אזרחית חיונית. כמענה לאיום, הרשות מורה על ביצוע פעולה מיידית על ידי היחידה הצבאית. מובן כי כל עוד היחידה נתונה לפיקוד צבאי, הוראה זו מעוררת קושי רב. כיצד "תבחר" היחידה בין המשימות שמטיל עליה הפיקוד הצבאי ובין המשימה ה"אזרחית"? מי יכריע מה קודם למה ולאיו משימה יוקצו המשאבים? אפשר לטעון כי קושי זה ייפתר, אם היחידה הצבאית תוכפף באופן מלא לרשות. פתרון זה מוביל לתרחיש השני, והוא השתלבות האיום הקיברנטי במלחמה כוללת. התקיפה בסייבר עשויה להיות למשל, מהלך מקדים לתקיפה קינטית. במקרה כזה, מיהו הגורם המוביל את הטיפול באירוע? הרשות – האחראית על ההגנה בסייבר, או צה"ל – האחראי על ההגנה ביתר המרחבים? כיצד ישולבו שני ה"כוחות המזוינים"? מי יכריע האם "לוחמי הסייבר", הכפופים לרשות, יופעלו לטובת מבצע הגנה או שמא דווקא למבצע תקיפה?

ניסיון דומה לפיצול הפיקוד נעשה לאחרונה בתחום העורף. עם הקמתו של המשרד להגנת העורף נעשה ניסיון להעניק בידיו סמכויות להפעיל ישירות את פיקוד העורף. עמדת צה"ל בעניין זה הייתה תקיפה וחד משמעית: למפקד פיקוד העורף יש מפקד אחד בלבד – הרמטכ"ל. עוד עמד צה"ל על כך שבעת חירום, אי אפשר להפריד בין חזית לעורף, ויש להעניק בידי משרד הביטחון וצה"ל את **הסמכות המלאה לנהל את אירועי החירום**. באשר למשרד להגנת העורף, הוצע כי הוא יעסוק בעיקר בתיאום בין הממשלה וגופים נוספים לבין הרשויות המקומיות ובהכנתן של הרשויות המקומיות לחירום.

ההיקש למשימותיו של פיקוד העורף מוליד שתי מסקנות חשובות. המסקנה האחת נוגעת לסוגיית האחריות. הרציונל שלפיו יש להעניק לצה"ל אחריות מלאה לנהל את אירועי החירום, מתקיים גם באירועי חירום במרחב הסייבר, קל וחומר כאשר מדובר באירועי לחימה משולבים. הדבר נכון גם בנוגע להנחיית האוכלוסייה. האחריות להנחיית אוכלוסייה בתחום העורף, ניתנה לצה"ל מפאת ההבנה שבדידו המידע והידע העדכניים ביותר בנוגע לטיב האיומים, סיכויי התרחשותם והדרך הנכונה להתגונן מפניהם. כמו כן, יש לצה"ל היכולת לקבוע, בכפוף להנחיה המדינית, אילו פעולות של האוכלוסייה ישרתו בצורה הטובה ביותר את המטרות של המערכה כולה. לא מן הנמנע שבמלחמות העתיד, שבהן תשולב גם לוחמה קיברנטית, יהיה צורך להנחות את האוכלוסייה כיצד להתנהג במרחב הקיברנטי (כגון, הנחיות על הגבלת השימוש במרשתת [אינטרנט] או הגבלות על שימוש במחשבים). ההכרה בכך שהמערכת הקיברנטית והמערכה הקינטית חד הן, תומכת במסקנה שגם אחריות זו ראוי שתהיה מוטלת על הגוף העוסק בניהול המערכה כולה, קרי – צה"ל.

המסקנה השנייה נוגעת לסוגיית הסמכות. אם נמצא שאפשר לתת לצה"ל את הסמכויות הדרושות כדי לעמוד במשימת ניהול העורף בחירום, משימה שמטבעה כרוכה בהפעלת סמכויות על אזרחים,²⁸ הרי שאין מניעה עקרונית להעניק לצה"ל סמכויות דומות כדי להתמודד עם איום הלוחמה הקיברנטית.

²⁷ כל זאת אף מבלי לדון בשאלה מהו מקור הסמכות של גורם אזרחי לפקוד על חייל, ומה תהיינה התוצאות של אי קיום פקודה במקרה זה.
²⁸ סמכויות פיקוד העורף מעוגנות בעיקר בחוק ההתגוננות האזרחית, התשי"א-1951.

הפלמ"ח והסייבר

לקראת סיום, נבקש להציג זווית התבוננות מעט אחרת על הסוגיה. ד"ר אלכסנדר ואקה (Alexander Vacca) – מומחה לאבטחת מערכות מידע והמנהל האסטרטגי של חברת האבטחה "Northrop Grumman" – טוען כי האופן שבו מתעצבת תורת לחימה מושפע מאוד מהתרבות של הארגון המעצב אותה.²⁹ התרבות הארגונית ניכרת בשפה ייחודית המשותפת לכלל החברים בארגון; במערכת של היקשים ומטפורות שבאמצעותם אפשר להבין מה מניע את החברים בארגון ואת ההקשרים הסיבתיים המסבירים תופעות ומסורות בארגון; ובעיקר – מעצבת את התהליכים לעיבוד של מידע חדש.

לפי גישתו של ואקה, טרם בשלה העת להגדיר את טיבו של האיום הקיברנטי, ולכן גם מוקדם מדי להכריע מהי הדרך הנכונה ביותר להתמודד מולו. הוא מציע, אם כן, את ה"כלי התרבותי" כאמצעי לחזות כיצד תפתח תורת הלחימה בעולם הסייבר, על פי הגוף המופקד על יישומה. באמצעות כלי זה הוא מנסה להסביר כיצד תפתח תפיסת הלחימה בפיקוד הסייבר שהוקם בחיל הים האמריקני (Navy), לעומת האופן שבו היא תפתח בפיקוד הסייבר שהוקם בחיל האוויר. תרבות הלחימה בחיל הים האמריקני מבוססת במידה רבה על כתביו של אלפרד מאהן, אדמירל חיל הים האמריקני, אשר היה גם היסטוריון והוגה צבאי זכה אף לכינוי 'האסטרטג האמריקני החשוב ביותר של המאה ה-19'. מאהן טען כי חיל הים הוא קריטי כדי לשמור על כוחות המסחר העולמיים ועל היכולת להניע כוחות צבאיים ממקום למקום, באופן המאפשר להתערב בסכסוכים צבאיים ולהגדיל את יכולת ההשפעה של הצבא, יותר מגודלו האמיתי. מכאן התפתחה תורת הלחימה של חיל הים האמריקני, המבוססת בין היתר על ספינות חזקות המאזנות בין התקפה להגנה – המסוגלות להביס כל אויב בים וקשות להכנעה; על גישה המעדיפה חתירה פעילה למגע על פני התפיסה הסבילה של יצירת הרתעה ועל התפיסה שלפיה הכרעת האויב בים תביא בעקיפין לניצחון במלחמה כולה. ואקה טוען, כי מאפיינים אלו יעצבו גם את תורת הלחימה של פיקוד הסייבר אשר תבסס על אבטחת המרחב הקיברנטי ושמירתו כאמצעי לסחר והעברת מידע צבאי.

לעומת חיל הים, תורת הלחימה של חיל האוויר מושפעת מכתביו של ההוגה הצבאי ג'וליו דואה, שהיה מראשוני ההוגים בתחום הפעלת הכוח האווירי, בראשית המאה ה-20. דואה האמין כי ההגנה הטובה ביותר היא ההתקפה, וראה בכוח האווירי מכונת תקיפה, אשר כוחה האדיר מייצר הרתעה אך יכול גם להכריע לבדו מלחמות, ולו באמצעות ההשפעה המוראלית הניכרת של התקיפה. בתוך התרבות הזו התפתחה, כצפוי, תפיסת לחימה קיברנטית המבוססת על יכולת תקיפה עוצמתית, המסונכרנת עם היכולות הקינטיות הקיימות, ואשר בכוחה לייצר אפקטים תודעתיים של ממש, אשר יסייעו להכניע את האויב.

ה"כלי התרבותי" עשוי לסייע גם בסרטוט גבולות האחריות להגנה במרחב הסייבר בישראל. אומנם, בשונה מהמצב בארה"ב, מגוון הגופים העוסקים בנושא אינו רב, ומן הסתם יהיה קשה להתחקות אחר ההגות הצבאית אשר עמדה בבסיס הקמתו של המטה הקיברנטי, או אחר ההגות אשר על בסיסה מוקם בימים אלו המבנה של הרשות הלאומית להגנה בסייבר. עם זה, אפשר בהחלט לנסות ולחזות באמצעות ה"כלי התרבותי" מה תהיינה התועלות (והמגרעות) שתנבענה

²⁹ Vacca, "Military Culture and Cyber Security", 159-176.

מהטלת האחריות להגנה בסייבר על צה"ל. קצרה היריעה מלדון במלוא ההשפעות האפשריות של התרבות הצה"לית על התפתחות תורת הלחימה בסייבר. אפשר רק לשער כי רוח הלחימה של צה"ל, עקרונות הלחימה, תורות הלחימה והערכים, הנטועים בארגון העברי הלוחם עוד מימי הפלמ"ח, כל אלו יתגלמו גם בתורת הלחימה בסייבר. בסביבה הקיברנטית המשתנה, שבה קשה לדעת מה ילד יום ומתי תרחש המתקפה הבאה וכיצד, נראה כי המטען הערכי האיתן שצה"ל נושא עימו יסייע ודאי לפתח במהרה את היכולות הנדרשות גם במרחב הקיברנטי.

סיכום

האיומים הלאומיים במרחב הקיברנטי הם שונים ומגוונים. החל מהאקר (פצחן) עצמאי הפורץ למחשבי הבנק וגונב מאגר של מספרי כרטיסי אשראי, דרך קבוצות מאורגנות הפועלות במרחבי הרשת כדי להשיג יעדים גלובליים וכלה בארגונים מדינתיים או מעין מדינתיים המשתמשים בעולם הסייבר כאמצעי לחימה לכל דבר ועניין. ממשלת ישראל קבעה לאחרונה כי המענה האופרטיבי לאיומים אלו, ראוי שיינתן על ידי "חיל סייבר אזרחי": רשות אופרטיבית שתפעל תחת המטה הקיברנטי הלאומי. רשות זו היא הזרוע הביצועית של המטה, ותפקידה הוא לבצע את כלל המשימות האופרטיביות להגנה על מרחב הסייבר ולנהלן. זאת מתוך ההכרה בצורך לתת מענה אחד וכולל לאיומים הייחודיים המופנים נגד מדינת ישראל במרחב זה.

המאמר הציג נקודת מבט אחרת, **המתבוננת על משימת ההגנה במרחב הסייבר מתוך האיום הביטחוני המרכזי, הוא איום ה"מלחמה הקיברנטית"**. איום זה אינו מתקיים לבדו, אלא הוא עוד נדבך ברשת האיומים הנובעים ממצב העימות שבו נמצאת מדינת ישראל מאז היווסדה.

הבנה זו של האיום הקיברנטי, מטילה ספק האם ההתמודדות עימו צריכה להיעשות באמצעות רשות אזרחית. כשם שהמצאת המטוס, הגרעין ופיתוח הצוללות דרשו היערכות מחדשת של הצבאות, לרבות במערכי ההגנה על מתקנים אזרחיים, אך לא הביאו ליצירתם של "צבאות אזרחיים", כך גם האיום הקיברנטי, קל וחומר במקרה הישראלי. בניגוד למדינות שבהן "מלחמת הסייבר" היא תצורה מודרנית של "מלחמה קרה", המתקיימת בין מעצמות שאין ביניהן עימות פיזי,³⁰ הרי שבישראל, האיום הקיברנטי הביטחוני מקורו בראש ובראשונה במדינות ובארגוני הטרור שערים אנו מצויים בעימות מזוין מתמשך.

לפיכך, ראוי כי **המענה למלחמה הקיברנטית** יינתן באופן שבו ניתן המענה ליתר האיומים הביטחוניים, קרי, בכוח הזרוע של צה"ל. הפקדת האחריות והסמכות בידי צה"ל עולה בקנה אחד עם העקרונות הדמוקרטיים שבבסיס הקמת צה"ל ככוח מזוין יחיד במדינה, היא מממשת נכון יותר את ייעוד צה"ל וחזונו, והיא מונעת התנגשות עם עקרון היסוד של אחדות הפיקוד. לצד כל אלה, עומדת גם המסורת הצבאית – המביאה עימה מורשת, תורות לחימה ותפיסות מגובשות, שיכולות לתרום לפיתוח מהיר של היכולות גם בתחום הסייבר. על כך אפשר להוסיף עוד יתרונות, אשר מפאת קוצר היריעה לא דנו בהן, כגון היתרון של צה"ל בגיוס ובפיתוח המשאב האנושי, והיתרונות המבניים והטכנולוגיים של צה"ל.

ההחלטה להקים רשות הגנה לאומית בסייבר היא ביטוי נוסף לאחריות שמגלה מדינת ישראל, אשר לאורך שנים היא מהמובילות בעולם בתחום זה. אולם אין בכך כדי לפתור אותנו מהשאלה,

³⁰ כגון, העימות בין ארה"ב לסין ורוסיה.

האומנם זהו המענה המתאים ביותר ל"מלחמה הקיברנטית" שעתידה להתרחש, והאם לא נכון לתת לצה"ל – המגן על גבולות המדינה באוויר, בים וביבשה, לעשות זאת גם במרחב הסייבר.

אחרית דבר

סמוך לפרסום המאמר, פורסמה החלטת הרמטכ"ל להקים בצה"ל את זרוע הסייבר.³¹ דומה כי החלטה זו מבטאת הבנה של קברניטי הצבא בדבר תפקידו של צה"ל, בין היתר, בהגנה על מדינת ישראל מפני איומי המלחמה הקיברנטית. עם זה, נראה שהחלטה זו אינה עולה בקנה אחד עם החלטת הממשלה, והיא מייצרת מאבק סמכויות בין "זרוע הסייבר" האזרחית, האחראית "לנהל, להפעיל ולבצע בהתאם לצורך את כלל מאמצי ההגנה האופרטיביים" במרחב האופרטיבי, לבין "זרוע הסייבר" הצבאית. נראה אם כן, שכדי להגשים את חזונו של הרמטכ"ל, יהיה צורך לבחון מחדש את תפקידיה ואת תחומי אחריותה של הרשות להגנה בסייבר, שזה עתה הוקמה.

³¹ זייתון, "הרמטכ"ל החליט להקים זרוע סייבר בצה"ל".

רשימת מקורות

- אבן, שמואל ודוד סימן טוב. "לוחמה במרחב הקיברנטי, מושגים, מגמות ומשמעויות לישראל". **המכון למחקרי ביטחון לאומי**, מזכר 109 (התשע"א-2011).
- אפק, שרון. "שוברים את הכללים וכולם משחקים – על המפגש בין המרחב הקיברנטי לבין כללי המשפט הבינלאומי". **בין הקטבים**, 2 (2014).
- בן ישראל, יצחק. "לוחמת מידע". **מערכות**, 369 (2000).
- בסוק, מוטי. "נתניהו: תוקם רשות לאומית להגנה אופרטיבית בסייבר". **The Marker** [21 בספטמבר 2014].
- ברעם, גיל. "ההיערכות למלחמה קיברנטית". **מערכות**, 456 (2014).
- זייתון, יואב. "הרמטכ"ל החליט להקים זרוע סייבר בצה"ל". **ynet** (15 ביוני 2015).
- החלטה 2444 של הממשלה מ-15 בפברואר 2015.
- החלטת ועדת השרים לענייני ביטחון ב/84 מ-11 בדצמבר 2002.
- חוק יסוד: הצבא, התשל"ו-1976.
- פקודת סדרי השלטון והמשפט, התש"ח-1948.
- כהן, שגיא. "8200: לא מחפשים רק חנוות עם משקפים". **ynet** (23 באוקטובר 2012).
- Hughes, Rex. "Towards a Global Regime for Cyber Warfare", in: Christian Czosseck and Kenneth Geers, eds., **The Virtual Battelfield: Prespective on Cyber-Warfare**. 2009.
- –Arquilla, John and David Ronfeldt, "Cyberwar is coming". **Comparative Studies**, 12: 141-165 (1993).
- Sammaan, Jean-Loup. "Cyber Command, The Rift in US Military Cyber Strategy". **Rusi journal**, 155: 16-21 (2010).
- Singel, Ryan. 'White House Cyber Czar: There Is No Cyberwar'. **Wired.com**, 4 March 2010.
- Kushner, David. "The Real Story of Stuxnet". **IEEE spectrum**, (26 February 2013).
spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.
- Lindsay, Jon R.. "Stuxnet and the Limits of Cyber Warfare". **Security Studies**. 22 (2013).
- Costin Raiu, Maxim Golovkin, "The Chronicles of the Hellsing APT: The Empire Strikes Back". **Securelist** (15 April 2015).
- Vacca, W. Alexander. "Military Culture and Cyber Security". **Survival** (53(6)), (2011–12), pp. 159–176.