# המרחב הקיברנטי והשדה הביטחוני – מסגרת מושגית
## משמעויות מערכתיות לישראל

שמואל אבן ודוד סימן טוב

### חשיבות טכנולוגיות המידע והמרחב הקיברנטי לישראל

לטכנולוגיות המידע ולמרחב הקיברנטי עצמו תרומה אסטרטגית לישראל. המשק הישראלי, בדומה למדינות המתקדמות ביותר בעולם, נשען במידה רבה על תשתיות המרחב הקיברנטי. ענפי טכנולוגיות המידע תורמים ישירות ובעקיפין לצמיחה הכלכלית בישראל, שהיא בין המדינות המובילות בעולם בפיתוח טכנולוגיות מידע. על פי מחקר של חברת הייעוץ הבינלאומית מקנזי,[94] "כלכלת האינטרנט" בישראל נחלקת לשני תחומים. חלק הארי הוא בתחום תעשיית טכנולוגיות מידע ותקשורת (ICT), והוא כולל פיתוח, ייצור ומכירה של ציוד, של תוכנות ושל שירותים. התחום הקטן יותר, שצומח במהירות, הוא תחום המסחר האלקטרוני אשר עוסק ברכישת מוצרים ושירותים באינטרנט. לפי המחקר, כלכלת האינטרנט בישראל (לפי הגדרת מקנזי) תרמה במישרין לתוצר של כ־50 מיליארד שקל בשנת 2009, כ־6.5% מהתוצר המקומי הגולמי (התמ"ג). נתון זה ממצב את ישראל כאחת מכלכלות האינטרנט המובילות בעולם. על פי המחקר, "כלכלת האינטרנט" הישראלית צפויה לצמוח בקצב שנתי של 9% – כפליים מקצב הצמיחה של המשק. בשנת 2015 צפויה התרומה של "כלכלת האינטרנט" הישראלית להסתכם בכ־85 מיליארד שקל, שיהוו כ־8.5% מהתמ"ג. לענפי טכנולוגיית המידע נודעת חשיבות מיוחדת משום שיש להם יכולת גבוהה להתחרות בשוק העולמי (חלק ניכר מהתוצר מופנה לחוץ לארץ) ומשום שהדרך היחידה של ישראל לצמוח במהירות היא הגדלת הייצוא.

ל"כלכלת האינטרנט" גם תרומה גבוהה לתעסוקה במשק, בייחוד לתעסוקת אקדמאים מתחומי הטכנולוגיה. נוסף על כך תורמים ענפי טכנולוגיות המידע תרומה ישירה ועקיפה לסקטור הביטחוני בישראל. ענפי טכנולוגיות מידע ותקשורת הם חלק חשוב מיכולותיה הטכנולוגיות של ישראל, הזוכות להערכה רבה של מומחים רבים מרחבי העולם,[95] וכך מחזקות את תדמיתה ואת מעמדה בעולם.

המרחב הקיברנטי מאפשר לישראל לפרוץ את בידודה הגיאוגרפי במזרח התיכון ולקיים קשרים הדוקים ושוטפים עם העולם. במרחב הקיברנטי טמון אף הפוטנציאל לחיזוק

מתוך: שמואל אבן ודוד סימן טוב, **לוחמה במרחב הקיברנטי: מושגים, מגמות ומשמעויות לישראל**, מזכר 109 יוני 2011

הקשר שבין הפריפריה למרכז המדינה. הוא משמש רכיב מרכזי בפעילות החברתית, והוא גורם חשוב בחיזוק הקשר שבין רשויות השלטון לאזרח.

## התארגנות ישראל להגנת המרחב הקיברנטי

בהתארגנות ישראל להגנת המרחב הקיברנטי ניתן למנות כמה נקודות ציון בולטות. בשנת 1997 הוקם פרויקט תהיל"ה (תשתית הממשלה לעידן האינטרנט). הפרויקט, שהוקם באגף החשב הכללי במשרד האוצר, נועד לספק שירותי גלישה מאובטחים למשרדי הממשלה ולמוסדותיה. על פי המדווח באתר האינטרנט של גוף זה, בתהיל"ה מצויה חוות שרתים שדרכה מקבלים מאות אלפי אזרחים בחודש שירותי ממשל זמין ומידע על פעולות משרדי הממשלה. תהיל"ה מפעילה אמצעים לשמירה על ביטחון הרשת הממשלתית באינטרנט, החל בצוות מומחי אבטחת מידע ותקשורת וכלה במוצרים וטכנולוגיות של חברות מובילות בעולם. בתהיל"ה הוקם "מרכז אבטחת המידע של ממשלת ישראל", שבין תפקידיו: לעקוב אחר אירועי אבטחת מידע בעולם עם תשומת לב להתקפות ברשת הנוגעות לישראל, לתאם בין גופים ממשלתיים לצורך פתרון בעיות אבטחה, לקשר בין גופים ממשלתיים לגופים חיצוניים ולערוך מחקרים בתחום. המרכז מוציא התראות אבטחת מידע לארגונים בתחום טכנולוגיות המידע המקיימים קשרים עם תהיל"ה או לגורמים ממשלתיים שאינם מסווגים. כן מקיים הגוף קשרים עם גורמים בינלאומיים כדי למגר התקפות ממוחשבות.[96] במסגרת זו פועל צוות Computer CERT (Emergency Response Team), שייעודו לתת מענה מיידי לאירועי אבטחת מידע בארגונים ממשלתיים או בגופים בסדר גודל בינלאומי. "נציגי ה־CERT מקיימים מוקד מענה זמין לתופעות של תקיפות ברשת, לניהול סיכונים, ליצירת נוהלי אבטחת מידע, בקרת תעבורה, להתפרצויות וירוסים, למניעת דואר זבל ופישינג, לפיראטיות ברשת, לזיוף זהות, לשמירה על פרטיות המידע, להעלאת המודעות לאבטחה; כן עוסק הצוות בשיתוף מידע ובעדכון מידע של ספקיות האינטרנט, של המשטרה ושל גורמי מערכת הביטחון".[97] אכן משימות נכבדות לקח הגוף על עצמו, אולם יש לזכור שהמנדט לפעילותו נוגע להספקת שירותי גלישה מאובטחים באינטרנט למשרדי הממשלה ולמוסדותיה, והמרכז אינו גוף אינטגרטיבי־אופרטיבי משותף לגופים האמונים על ביטחון המרחב הקיברנטי, כפי שראינו במדינות מערביות.

ב־27 במרס 2011 אישרה הממשלה את הקמת יחידת המנמ"ר (מנהל מערכות מידע) הממשלתי, גוף בין־משרדי שירכז את תחום התקשוב בממשלה. הגוף, הכפוף למנכ"ל משרד האוצר, אמור להנחות את יחידות התקשוב במשרדי הממשלה ולהיות אחראי במישרין לכל פרויקטי המחשוב הממשלתיים הרוחביים, ובכלל זה לפרויקט תהיל"ה.[98] ריכוז פרויקטי המחשוב של הממשלה במקום אחד הוא התקדמות רבה בהיערכות המדינה בתחום התקשוב, אולם מוטב שהגוף הממונה על ניהול ביטחון מערכות המידע יהיה מחוץ לגוף המקים והמפעיל תשתיות אלה.

בשנת 2002 הוקמה הרשות הממלכתית לאבטחת מידע בשירות הביטחון הכללי (השב"כ). "הרשות מופקדת על הנחיה מקצועית של הגופים המונחים שבאחריותה בתחום אבטחת תשתיות מחשב חיוניות מפני איומי טרור וחבלה בתחום אבטחת מידע מסווג ומפני איומי ריגול וחשיפה".[99] ההיגיון המקורי להיות הרשות יחידה בשב"כ קשור כנראה לאחריותו של השב"כ לסיכול ריגול וטרור. כיום אפשר להצביע על יתרונות ועל חסרונות למיקום הזה. יתרון חשוב הוא הקשר ההדוק בין הרשות לבין שאר היכולות והסמכויות של השב"כ (הכלולות בחוק השב"כ) ושל קהילת המודיעין, שבה השב"כ שותף. מנגד, גופים בסקטור הפרטי עלולים להירתע מחשיפה ליחידה בארגון האוחז במשימות ובסמכויות חריגות שאינן נוגעות רק לממד הזה.[100] נוסף על כך השב"כ מטבעו הוא גוף מבצעי העוסק בסיכול חשאי ואינו מופקד על משימות אחרות הדרושות כדי להתמודד עם האתגר הקיברנטי, כגון קשר הדוק עם הסקטור הפרטי, הגברת מודעות האוכלוסייה לאבטחה קיברנטית, טיפול בגופים שנפגעו במתקפה קיברנטית ועוד.

הרשות הממלכתית לאבטחת מידע בשב"כ מונחית על ידי ועדת היגוי להגנה על מערכות ממוחשבות במטה לביטחון לאומי (המל"ל), שבראשה עומד ראש המטה ללוחמה בטרור במל"ל.[101] תפקידה של ועדת ההיגוי לאשר לרשות לאבטחת מידע להרחיב את רשימת הגופים המונחים או המאובטחים שיידרשו להעמיק את הגנתם ולעמוד בהנחיות הרשות. על פי מאמרו של גבי סיבוני,[102] פעילות זו לא התבססה על תהליך סטטוטורי ושיטתי של איתור גופים אלה ואישורם; וכך יצא שחברות גדולות וחיוניות בסקטורים מסוימים כלולות ברשימה, ואילו חברות גדולות בסקטורים אחרים (למשל בתחומי המזון והתרופות) אינן ברשימה, על אף שתרומתן לתוצר, לתעסוקה ולמרקם החיים גדולה. ליקוי נוסף בשיטה הוא בכך שהיא מתמקדת בהנחיית חברות נבחרות בסקטורים מסוימים, מסייעת להגנה נקודתית ולא מספקת הגנה מערכתית, המחייבת כיסוי רחב יותר של גופים הקשורים לאותה מערכת חיונית. דוגמה לכך היא מערכת המים: "הגנה על תשתיות אספקת המים ואיכותם בישראל אינה נוגעת רק לתהליכים בחברת מקורות, המופיעה ברשימה, אלא גם לעשרות ספקי מים אחרים, אגודות, תאגידי מים, מתקני התפלה והולכה, מתקני טיפול בשפכים מתקני טיפול והולכת קולחים ועוד. חלקם הגדול של מתקנים אלה מופעל על ידי יזמים פרטיים, שההפעלה של מנגנוני הגנה אינה בראש מעייניהם. המצב הזה דומה בתחומים רבים נוספים".

לעומת זאת, דוגמה להכוונה, המשקפת מודעות גבוהה לביטחון מערכות המידע, מוצאים אצל הממונים על הגופים הפיננסיים במשרד האוצר ובבנק ישראל. משרד האוצר (אגף שוק ההון, ביטוח וחיסכון) הוציא הנחיות מפורטות לגופים פיננסיים – הנחיות העוסקות באבטחת מידע ובהגנה על מערכות המידע.[103] המפקח על הבנקים בבנק ישראל הוציא אף הוא חוזר מקיף ומפורט.[104] החוזר מדגיש בין היתר: "טכנולוגיית המידע היא מרכיב מרכזי בתפעול ובניהול תקין של תאגיד בנקאי, בהיות המידע, על כל היבטיו והשלכותיו, בעל השפעה מכרעת על יציבות התאגיד הבנקאי ועל התפתחותו".

הנחיה כזאת יכולה לשמש דוגמה למשרדי הממשלה האחרים ביחס לגופים שמולם הם פועלים במדינה.

**מטה הסייבר הצה"לי.** בשנת 2009 הגדיר הרמטכ"ל, רב־אלוף גבי אשכנזי, את המרחב הקיברנטי כמרחב לחימה אסטרטגי ואופרטיבי. בהתאם לכך הוקם "מטה הסייבר" הצה"לי, שנועד לשמש מטה מטכ"לי לתיאום ולהכוונה של פעולות הצבא במרחב הקיברנטי. המטה הוקם ביחידה 8200 באגף המודיעין (אמ"ן),[105] ושותפים בו נציגים מאמ"ן ומאגף התקשוב.[106] האלוף עמוס ידלין, בהיותו ראש אמ"ן, התייחס לנושא בהרצאה במכון למחקרי ביטחון לאומי בדצמבר 2009. הוא ציין את הפוטנציאל לפגיעות בישראל עקב פריצות למחשבים כאחד האיומים הלאומיים. לדבריו: "צה"ל מתכוון לספק הגנה טובה לרשתות, וגם להפעיל התקפות קיברנטיות משלו".[107] המטה הקיברנטי הצה"לי יכול להיות שותף בהגנת המרחב הקיברנטי של המדינה, בדומה לפיקוד הקיברנטי בארצות־הברית, אך גם הוא אינו הגוף המיועד לאינטגרציה לאומית להגנת המרחב הקיברנטי הלאומי.

## לוח 1: התארגנות במרחב הקיברנטי – השוואה בין ישראל לארצות־הברית

| | הקמת גופים העוסקים בקביעת מדיניות, בסנכרון ובתיאום מדינתי | הקמת גופים אופרטיביים |
|---|---|---|
| ארצות־הברית | מינוי עוזר מיוחד לנשיא ומתאם הגופים הפועלים לאבטחת המרחב הקיברנטי (2009). הוא אחראי לגיבוש, לתיאום ולסנכרון של מדיניות הממשל, לעבודה עם משרד האוצר ולניהול משברים. על משרדי הממשלה השונים הוטלה האחריות לקדם ולתאם את ההגנה על התשתיות החיוניות שבתחום אחריותם. במשרד החוץ מונה במאי 2011 מתאם למימוש האסטרטגיה הבינלאומית של ארצות הברית במרחב הקיברנטי. | הקמת מחלקת ביטחון הסייבר במשרד ביטחון המולדת (National Cyber Security Division) כפועל יוצא מהאסטרטגיה לביטחון המרחב הקיברנטי משנת 2003. הקמת פיקוד הסייבר של צבא ארצות הברית בשנת 2010. |
| ישראל | ההחלטה על הקמת מטה לאומי קיברנטי (מאי 2011). | הקמת תהי"ה (תשתית הממשלה לעידן האינטרנט) בשנת 1997.<br>הקמת הרשות הממלכתית לאבטחת מידע בשב"כ בשנת 2002.<br>הקמת "מטה הסייבר" בצה"ל (2009–2010). |

**מטה הסייבר הלאומי.** ב־18 במאי 2011 הכריז ראש הממשלה בנימין נתניהו על הקמת מטה סייבר לאומי. לפי הודעת משרד ראש הממשלה: "ייעודו העיקרי של המטה הוא להרחיב את יכולות ההגנה של המדינה על מערכות התשתיות החיוניות מפני התקפות טרור קיברנטי, המבוצעות הן בידי מדינות זרות והן בידי גורמי טרור."[108] המטה הוקם בעקבות המלצות צוות בראשות יו"ר המועצה הלאומית למחקר ופיתוח, האלוף במילואים יצחק בן ישראל. נתניהו הודיע כי אימץ את מלוא ההמלצות והסביר כי "בתחום ההגנתי

ישראל חשופה להתקפות סייבר שיכולות לשתק מערכות חיים שמפעילות את המדינה, כגון: חשמל, תקשרת, כרטיסי אשראי, מים, תחבורה. כל תחום הוא ממוחשב ולכן פגיע. יש צורך לגבש מענה הגנתי לאיום הזה". עוד דווח, כי המטה החדש צפוי לפעול לטיפוח חברות ישראליות המתמחות בהגנה על מרחב הסייבר, בניסיון לגזור נתח מהשוק הנרחב המתפתח בנושא ברחבי העולם.[109] הקמת המטה תהווה חידוש משמעותי משום שעד כה אין בישראל גוף שאמון על הטיפול בהגנת המרחב הקיברנטי בראייה הלאומית. הטיפול ההגנתי במרחב הקיברנטי בישראל התמקד ביחידות אופרטיביות (במשרד האוצר, בשב"כ ובצה"ל), אך חסר בדרג המדיני־האסטרטגי שמעליו (ראו לוח 1).

## המלצות לישראל

למדינת ישראל יש שלוש סיבות טובות להאיץ את התארגנותה הביטחונית במרחב הקיברנטי:

א. בדומה למדינות מערביות מפותחות אחרות, המרחב הקיברנטי חושף את ישראל לסיכונים בסיסיים ניכרים, ובהם סיכונים לפגיעה בתשתיות חיוניות, במערכת הביטחון, בתפקוד המשק וכו'.
ב. בשונה ממדינות רבות, ישראל ניצבת בפני אויבים שלהם מוטיבציות ברורות ומוצהרות לפגוע בה ככל הניתן. מדובר למשל באיראן, הפועלת להשיג גם יכולות קיברנטיות התקפיות.[110] כמו כן תיתכן כניסת ארגוני טרור לפעילות התקפית במרחב הקיברנטי אשר תופנה נגד ישראל.
ג. לישראל, שהיא בין המובילות בעולם בידע בתחומי טכנולוגיות המידע ובנוכחות במרחב הקיברנטי, ישנה האפשרות לפתח הגנה מתקדמת ולמצות את היתרונות שמגלם המרחב הקיברנטי בשדה הקרב.

במסגרת האצת ההתארגנות הישראלית נדרשים בין היתר הצעדים הבאים:

א. קביעת אסטרטגיה לאומית לביטחון המרחב הקיברנטי הישראלי ויישום האסטרטגיה בהובלת מטה הסייבר הלאומי.
ב. שילוב הלוחמה הקיברנטית כרכיב באסטרטגיית הביטחון של ישראל.[111]

החלטה על הקמת מטה הסייבר הלאומי הינה אומנם צעד חשוב נוסף בהתמודדות ישראל עם האתגר הקיברנטי, אולם יש להבטיח כי המטה יפעל על פי אסטרטגיה קיברנטית לאומית, שתגובש לשם כך. כמו כן, נוכח הפיגור של ישראל בתחום זה חשוב כי המטה יוקם במהירות[112] ויקבל אחריות וסמכויות הולמות כדי לסגור את הפער הקיים ברמה הלאומית בנוגע לניהול אסטרטגי ואינטגרציה בין כלל הגורמים האופרטיביים – האזרחיים והצבאיים – הפועלים במרחב הקיברנטי בהקשר ההגנתי.

## האסטרטגיה להגנת המרחב הקיברנטי של ישראל – הצעה

מוצע לישראל לגבש אסטרטגיה לאומית לביטחון המרחב הקיברנטי, אשר תביא להשגת המטרות האסטרטגיות במשאבים מינימליים ותשמש מסגרת לפעולה של כלל הגופים השותפים בהגנת המרחב הקיברנטי. האסטרטגיה תאושר בקבינט ותשמש קו מנחה הן לפעולה המשותפת של הגופים והן לפעולתו של כל גוף מתוקף אחריותו. להלן יעדי האסטרטגיה ועקרונות הפעולה הכלליים שלה.

יעדי האסטרטגיה:

א. לקיים בישראל מרחב קיברנטי בטוח, שיאפשר למדינה לממש את יעדיה הלאומיים בתחומי הממשל, הביטחון, המשק, החברה, החוץ, המדע ועוד.
ב. לחזק את הביטחון במרחב הקיברנטי הישראלי ולשמור על חופש הפעולה בו לרווחת כלל האוכלוסייה.

האסטרטגיה אמורה לקדם את השגת היעדים הללו באמצעות שילוב כוחות בין כל הגורמים הרלוונטיים במדינה, וזאת בהתאם לעקרונות הפעולה הבאים:

א. הכרה במרחב הקיברנטי כמרחב לאומי חדש, שיש להגן עליו באופן ייחודי (בשונה מהמרחבים המסורתיים), תוך ראייה כוללת ושיתוף פעולה בין כל הגורמים הנוגעים בדבר.
ב. כינון הנהגה ומנגנון מרכזי להגנה קיברנטית ברמה הלאומית (הקמת ארגון ברמה מדינתית).
ג. ניהול סיכונים מתוך ראייה כוללת ובכלל זה העמדת התשתיות הלאומיות הקריטיות ומערכות הביטחון בראש סדר העדיפויות, אך גם טיפול בהגנת רכיבים נוספים של המשק ושל החברה. למשל, הגנה על מאגרי ידע של האוניברסיטאות ושל מכוני מחקר, הגנה על חברות בעלות השפעה על המשק (שאינן בקטגוריה של תשתיות), הגנה על חברות הקשורות לחברות של תשתיות חיוניות ועוד.
ד. בניית מערך הגנה דינמי, אינטגרטיבי ומקיף ובכלל זה: שילוב בין מערכות הגנה פסיביות לבין מערכות הגנה אקטיביות (ראו אסטרטגיית הביטחון הקיברנטית של הפנטגון), שילוב בין הגנה על יעדים חיוניים לבין מרכיבי "הגנה מרחבית" (תעבורה הנכנסת למדינה, צומתי תקשורת), שיפור ארכיטקטורת רשתות, הידוק בין מנגנוני אבטחה פיזיים לאלה הקיברנטיים ועוד.
ה. שילוב כוחות במגזר הציבורי (הממשלתי) בין המגזר הביטחוני לבין המגזר האזרחי; וכן שיתוף פעולה ושילוב מאמצים בין יחידות בתוך כל אחד מהמגזרים הללו. למשל, שילוב מאמצים ושיתוף בידע בין הצבא לבין כוחות הביטחון האחרים.
ו. שיתוף פעולה הדוק בין הסקטור הממשלתי (הביטחוני והאזרחי) לבין הסקטור הפרטי בהגנה על המרחב הקיברנטי ובכלל זה שיתוף במידע וביכולות, כך שכל ארגון ממשלתי ופרטי מתאים יהיה מודע לסיכונים, לאירועי תקיפה וליכולות הגנה חדשות.

ז. שיתוף פעולה הדוק עם גורמי חוץ. למשל, בניית מערכות ניטור קולקטיביות עם בעלות ברית.
ח. חקיקה ואכיפה שיאפשרו פעולה הגנתית.
ט. סיוע לכלל האוכלוסייה בהתגוננות קיברנטית. למשל, הסברה להגברת מודעות הציבור לאיומים ולפתרונות, מתן תמריצים לעסקים ולתושבים ברכישת תוכנות הגנה, הגברת הפיקוח על חברות אבטחה ועל ספקי תקשורת לציבור בהיבט האמור.
י. בניית יכולת להתאוששות מהירה מהתקפה.
יא. שימוש בשיטות ובאמצעים הטכנולוגיים המתקדמים ביותר.
יב. גיבוש מדיניות הרתעה, סיכול תקיפות ותגובה כרכיבים משלימים לאסטרטגיה. בכלל זה: יכולת תגובה ישירה נגד מערכות קיברנטיות תוקפות[113] ויכולת פגיעה בתוקפן. על עניין זה ממונה מערכת הביטחון.

לצורך מימוש האסטרטגיה אנו מציעים לכלול, בין תפקידיו של מטה הסייבר הלאומי, את התפקידים הבאים:

א. סיוע לדרג המדיני בקבלת החלטות ובעיצוב מדיניות בתחום הגנת המרחב הקיברנטי הלאומי. בכלל זה, גיבוש הצעה לאסטרטגיה לאומית להגנת המרחב הקיברנטי בשיתוף עם הגורמים הרלוונטיים, אשר תאושר בקבינט המדיני־ביטחוני.
ב. הערכות סיכונים – שוטפות ועיתיות, בהסתמך על נתונים ועל הערכות, שיספקו גופי המודיעין והגופים האופרטיביים והטכנולוגיים הרלוונטיים.
ג. הערכות מצב – שוטפות ועיתיות, ובכלל זה המלצות לפעולה על סמך ניתוח חלופות.
ד. הוראת האסטרטגיה לגופים האזרחיים המשתתפים בהגנה על המרחב הקיברנטי ותיאום עם הגופים במגזר הביטחוני.
ה. תיאום הפעולות של כל הגורמים הממשלתיים והפרטיים הנוגעים לביטחון המרחב הקיברנטי. בכלל זה הטלת אחריות על משרדי הממשלה האזרחיים לקדם את הביטחון הקיברנטי בתחומם (כפי שעושים למשל משרד האוצר והמפקח על הבנקים בבנק ישראל כלפי גופים פיננסיים מוסדיים).
ו. הקמת מרכז אופרטיבי מדינתי ("מרכז מבצעים" קיברנטי) וניהולו. תפקידו יהיה ליצור תמונת מצב דינמית של איומים קיברנטיים, לשתף מידע בין כל הגופים הנוגעים בדבר ולסייע בניהול ההגנה.
ז. קביעת מערכות התשתית והגופים האזרחיים, שעל המדינה להנחותם או לאבטח אותם בתחום הקיברנטי, בהתאם לאסטרטגיה הלאומית.
ח. ייזום חקיקה ותקנות, החיוניות לפעולות לשם הגנת המרחב הקיברנטי בשגרה ובחירום.
ט. ייזום והובלה של פרויקטים ממשלתיים, למשל פרויקטים בנושאים האלה: שדרוג שיטות ואמצעי ההגנה על מערכות המידע (בכלל זה אבטחה פיזית), כינון מערכת ממוסדת להדרכה של עובדים בסקטור הממשלתי, שיפור יכולת ההתאוששות לאחר התקפה קיברנטית, ניהול תרגילי הגנה קיברנטיים ברמה הלאומית.

י. קביעת קריטריונים לפיתוח, לרכש ולהתקנה של אמצעי תקשוב בהיבטים של ביטחון קיברנטי.
יא. מתן אישורים להקמת תשתיות תקשוב בהקשר של השפעתן על ביטחון המרחב הקיברנטי הלאומי.
יב. ייזום והכוונה בתחום פיתוח אמצעי הגנה, הכשרת כוח אדם מקצועי ומחקר מדעי בהקשר של ביטחון המרחב הקיברנטי. בכלל זה הענקת תמריצים לגופי מחקר.
יג. ייזום שיתופי פעולה אסטרטגיים בין הסקטור הממשלתי לבין הסקטור הפרטי. בכלל זה שיתוף פעולה עם חברות תקשורת וטכנולוגיה בתחום התפעולי ובתחומי המחקר והפיתוח.
יד. ריכוז שיתוף פעולה עם מדינות אחרות בנוגע לביטחון המרחב הקיברנטי.
טו. בקרה על יישום האסטרטגיה ועל הפעילות בתחום הגנת המרחב הקיברנטי. וידוא קיום פיקוח ראוי על משרדי הממשלה השונים ועל הרשויות האזרחיות, פיקוח על ספקי תקשורת מבחינת ציוד ויישום כללי ביטחון קיברנטי.
טז. שיפור ההתגוננות של התושבים במדינה – באמצעות צעדי הסברה, מתן תמריצים להצטיידות בתוכנות הגנה (למשל, הקלות במס) ופיקוח על רמת השירות שנותנים ספקי תקשורת וחברות אבטחה לאוכלוסייה.
יז. להיות מרכז ידע לאומי בתחום הגנת המרחב הקיברנטי, המקושר אל מרכזי ידע בארץ ובחו"ל. בכלל זה למידה של דרכי ההתמודדות של מדינות אחרות עם האתגר הקיברנטי.

## שילוב המרחב הקיברנטי באסטרטגיית הביטחון של ישראל

הוספת מרחב לחימה חדש למרחבים המסורתיים (יבשה, ים, אוויר וחלל) מחייבת לשלב את המרחב הקיברנטי באסטרטגיית הביטחון או בתפיסת הביטחון[114] של ישראל. הצעה לתפיסת ביטחון מעודכנת הוכנה באפריל 2006, לפני מלחמת לבנון השנייה, על ידי ועדה בראשות מר דן מרידור, שמינה שר הביטחון עמיר פרץ. הוועדה הצביעה בין היתר על הרלוונטיות הנמוכה של מושג ההרתעה בהקשר למאבק בטרור, על הקושי ליישם את המשתמע ממושג ההכרעה והמליצה להוסיף את ההגנה כרכיב נוסף לשלושת הרכיבים המסורתיים (הרתעה, התרעה והכרעה).[115] האלוף עמוס ידלין, בהיותו ראש אמ"ן, אמר בדצמבר 2009, כי "תחום הלוחמה הקיברנטית תואם היטב לדוקטרינה ההתקפית של ישראל. זהו תחום שהוא כולו כחול־לבן, שאינו נשען על סיוע או טכנולוגיה זרים. ישראלים צעירים מכירים היטב את התחום הזה, שהרי ישראל הוכתרה באחרונה כמדינת הסטארט־אפים".[116]

בחינה של המושגים הרלוונטיים לתפיסת הביטחון של ישראל (כמפורט בפרק א) הראתה שתוכני המושגים של תפיסת הביטחון המסורתית אינם מתאימים למרחב הלחימה הקיברנטי. למשל, קשה מאוד ליישם הרתעה במרחב הקיברנטי, להתרעה

האופרטיבית אין משמעות ללא הגנה אקטיבית, והגנה קיברנטית מחייבת התאמה עמוקה לתכונות הייחודיות של המרחב. שיתוף הפעולה המתחייב להגנת המרחב הוא חסר תקדים בהשוואה לשיתופי פעולה אחרים בין הסקטור הביטחוני לאזרחי לצורך פעילות צבאית. זאת ועוד, לאור ההכרה במרחב הקיברנטי כמרחב לחימה, נדרש לבחון יכולות אסטרטגיות חדשות ואולי אף לחולל שינוי בסדר הכוחות, דהיינו להשקיע יותר בהקמת צבא קיברנטי.

**לסיום**, לישראל יש פוטנציאל להיות בין המדינות המובילות בעולם בתחום הביטחון הקיברנטי, בהתחשב בהון האנושי ובידע הטכנולוגי הגבוהים שבידיה. מיצוי פוטנציאל זה עשוי לתרום למדינה בתחומי הביטחון והכלכלה.

## הערות

94 נועה פלג, "צומחים בגדול, קוצרים בקטן", **גלובס**, 9 בנובמבר 2011.

95 דוגמה: בריאיון למגזין **פורבס** אמר ג'ורג' גילדר, מומחה אמריקאי נודע לטכנולוגיות המידע ולכלכלה: "הצלחת הקפיטליזם האמריקני הייתה ותמשיך להיות פונקציה של החדשנות הטכנולוגית, אנחנו במלחמת קיום מתמדת, כלכלית וביטחונית. ישראל היא הנכס האסטרטגי היחיד שלנו מחוץ לארצות־הברית. ישראל היא היחידה המובחרת שלנו. היא חלק אינטגרלי של כלכלת ארצות־הברית, שלוחה חיצונית שלנו ונכס אמיתי במזרח התיכון. שלמה גרינברג, "האם ישראל היא נכס אסטרטגי?", ביזפורטל, 17 בפברואר 2011.

96 אתר תהיל"ה: www.tehila.gov.il

97 אתר אבטחת המידע הממשלתי: www.cert.gov.il

98 אור הירשאוגה, "הממשלה אישרה הקמת יחידת מטה למנמ"ר הממשלתי", TheMarker.com 17 במרס 2011.

99 הקמת הרשות לאבטחת מידע היא תוצאה של החלטת הממשלה שהתקבלה בשנת 2002 (מספר ההחלטה ב־48). אתר השב"כ: www.shabak.gov.il

100 תת־אלוף ניצן נוריאל, ראש המטה ללוחמה בטרור (המשמש גם ראש ועדת ההיגוי להגנה על מערכות ממוחשבות במטה לביטחון לאומי) אמר כי גופים שונים בישראל ובהם חברות פרטיות גדולות לא הסכימו לקבל הגנה ממשלתית, עד שהמטה ללוחמה בטרור פרץ למערכות שלהם כדי להראות את הנזק הפוטנציאלי. המקור: ברק רביד, "רה"מ, בנימין נתניהו, הקים צוות שמטרתו היערכות ישראל למתקפה על רשתות מחשבים", **הארץ**, 3 באפריל 2011.

101 ניתן להניח כי המשימות שהוטלו על ראש הלוט"ר במל"ל בעניין הגנת המרחב הקיברנטי יועברו לראש מטה הסייבר הלאומי.

102 ד"ר גבי סיבוני, "הגנת נכסים ותשתיות קריטיות מפני תקיפה קיברנטית – הממד הסטטוטורי", **צבא ואסטרטגיה**, המכון למחקרי ביטחון לאומי, כרך 3, גיליון 1, מאי 2011.

103 **חוזר גופים מוסדיים**, 6-9-2006, 16 באוקטובר 2006.

104 **ניהול בנקאי תקין** [4] (09/03): ניהול טכנולוגיות המידע.

105 אמיר אורן, "זירת הלחימה החדשה של צה"ל נמצאת ברשתות מחשבים", **הארץ**, 2 בינואר 2010.

106 אגף התקשוב בצה"ל הוקם במרס 2003 על בסיס איחוד חיל הקשר וחטיבת התקשוב (תקשורת ומחשבים) ובכך נוסד גוף מטכ"לי האמון על קביעת מדיניות התקשוב בצה"ל (אתר אגף התקשוב).

107 נחמה אלמוג, "אלוף עמוס ידלין, ראש אמ"ן: ישראל מובילה בתחום הלוחמה הקיברנטית", אתר אנשים ומחשבים, 17 בדצמבר 2009.

108 דובר משרד ראש הממשלה, "ראש הממשלה הכריז על הקמת מטה סייבר לאומי", אתר משרד ראש הממשלה, 18 במאי 2011. עוד נאמר בהודעה על הקמת מטה הסייבר, כי "ראש הממשלה

הורה על הקצאת תקציב מיוחד (בסך מאות מיליוני שקלים – לפי **הארץ**, הערה 109 להלן) ליישום תוכנית החומש, אשר תציב את ישראל בחוד החנית העולמי של תחום הסייבר. התוכנית כוללת השקעה במחקר ופיתוח אקדמי, הקמת מרכז חישוב על (Super Computer) באחת האוניברסיטאות בישראל, הקמת מרכזי מצוינות אקדמיים, פעילות מאומצת להשבת חוקרים ואנשי אקדמיה לישראל, הגדלה משמעותית של מספר הסטודנטים לקיברנטיקה ושדרוג תשתיות המחקר באוניברסיטאות. כמו כן, התוכנית כוללת גם עידוד של המגזר העסקי, עם דגש על תחום ההיי־טק, במטרה לפתח טכנולוגיות כחול־לבן שיעניקו לישראל יתרון משמעותי בתחום. הממשלה תסיר חסמי ייצוא של פיתוחים קיברנטיים, ומערכת הביטחון תגדיל את מיקור החוץ של פיתוח טכנולוגיות קיברנטיות למגזר התעשייתי הפרטי על מנת לעודד מגזר זה".

109 יהונתן ליס, "ראש הממשלה בנימין נתניהו הכריז על הקמת מטה סייבר לאומי", **הארץ**, 18 במאי 2011.

110 Amy Kellogg, "Iran is Recruiting Hacker Warriors for its Cyber Army to Fight 'Enemies'", FoxNews.com, March 14, 2011.

111 העיתוי הנוכחי לעסוק בעניין מתאים גם לאור קביעת ועדת מרידור לתפיסת הביטחון של ישראל משנת 2006, כי "אחת לחמש שנים תיעשה בדיקה של הנחות היסוד בתפיסת הביטחון" (זאב שיף, **הארץ**, 24 באפריל 2006).

112 הלקח ההיסטורי מהקמת מטות במשרד ראש הממשלה בישראל, כמו המטה ללוחמה בטרור ומטה (בזמנו – המועצה) לביטחון לאומי, הוא שחולפות שנים רבות מרגע קבלת החלטה על ההקמה ועד להיות המטה אופרטיבי ובעל השפעה משמעותית, אם בכלל.

113 ראש המטה ללוחמה בטרור, תת־אלוף ניצן נוריאל, אמר בכנס הרצליה: "אני מוכן להשקיע הרבה כסף כדי שהמחשב של כל האקר שמתקיף את מדינת ישראל יישרף". ברק רביד, לעיל הערה 100.

114 "תפיסת ביטחון" – מושג קומפקטי המכיל את המושגים: הרתעה, התרעה, הכרעה, וכן את המושג הגנה (על פי הצעת ועדת מרידור). התפיסה מגלמת את הקשר בין המושגים הללו בהקשר להפעלת צה"ל ומגלמת בתוכה רכיבים אסטרטגיים חשובים ובהם עליונות אווירית ועליונות מודיעינית. עם זאת, תפיסת הביטחון אינה מכילה רכיבים אחרים של אסטרטגיית הביטחון של ישראל, כגון: הישענות על מעצמה דוגמת ארצות־הברית והסדרי ביטחון (פירוז, דילול כוחות, שימוש בכוחות בינלאומיים) במסגרת הסדרים מדיניים. אסטרטגיית הביטחון של ישראל אומנם לא כתובה, אבל היא נגלית במעשיה של ישראל.

115 שי שבתאי, "תפיסת הביטחון של ישראל – עדכון מונחי יסוד", **עדכן אסטרטגי**, כרך 13, גיליון 2, אוגוסט 2010.

116 נחמה אלמוג, לעיל הערה 107.

משרד ראש הממשלה
**המטה לביטחון לאומי**
*המטה ללוחמה בטרור*

'9/2011

לכל מאן דבעי,

הנדון: **מחקר "הלוחמה במרחב הקיברנטי -מושגים מגמות ומשמעויות לישראל" (מזכר 109)**

התחום הנדון הוא בעל חשיבות עולה לביטחון הלאומי של ישראל.

מבקש להביע הערכה רבה להנהלת המכון ולחוקרים על המחקר החדשני, המקיף, המעמיק והרלוונטי.

המזכר סייע לנו רבות בעת גיבוש ההצעה להחלטת הממשלה להקמת מטה קיברנטי לאומי ולקביעת תפקידיו, שהתקבלה ב-7 אוגוסט 2011.

בכוונתנו גם להעמיק גם הקשר שבין הלוחמה הקיברנטית לתפיסת הביטחון של ישראל, כפי שמציע המזכר.

נשמח לקבל תוצרים דומים בנושאי הביטחון הלאומי בעתיד.

בברכה,

תא"ל (מיל.) ניצן נוריאל
המטה ללוחמה בטרור