השפעת התפתחות טכנולוגיית הלוחמה הקיברנטית על שינויים בבניין הכוח בישראל

גיל ברעם

בעשור האחרון חלו ההתפתחויות מהירות בתחומי המחשוב וטכנולוגיות המידע, שהובילו לשינויים מרחיקי לכת כמעט בכל תחומי החיים, ביניהם גם בתחום הצבאי־ביטחוני. בתחום זה התרחשו שינויים רבים במאפייני הלחימה ובבניין הכוח של צבאות, בין היתר בשל התפתחויות שחלו בדפוסי המחשבה האסטרטגית ובגיבוש הדוקטרינות הצבאיות שהותאמו למציאות המשתנה. ניסיונות שנעשו לבחון את השלכות המעבר לעידן המידע על העיסוק הביטחוני הובילו בשנות התשעים של המאה ה־20 להתפתחותו של רעיון "המהפכה בעניינים צבאיים". הרעיון נולד בעקבות ההמצאות הטכנולוגיות החדישות, שהובילו לעליית מדרגה בזמינות המודיעין ובאיכותו, בקצב זרימת המידע וביכולות הדיוק של כלי הנשק. בשנים הבאות, ובייחוד עם הכניסה למאה ה־21, התפתחו טכנולוגיות מתקדמות בתחום הלוחמה הקיברנטית, שהובילו לשינוי איכותי במאפייני שדה הקרב ובדפוסי פעילותם של הצבאות המודרניים.

הטכנולוגיה הקיברנטית המשמשת לצורכי לחימה משפיעה על דפוסי הלחימה כך שמדינה המחזיקה בה נהנית מעליונות בשדה הקרב, ממודיעין איכותי ומקיף, מיכולת תקיפה מדויקת ומהירה, מיכולות הגנה על תשתיות קריטיות, מיכולות שליטה ובקרה גבוהות ועוד. יכולות אלה תורמות לעוצמתה של המדינה ומחזקות את ביטחונה הלאומי. טכנולוגיית הלוחמה הקיברנטית טומנת בחובה פוטנציאל ליתרונות עצומים, לצד סיכונים חדשים ובלתי־מוכרים. לאור חדשנותו הרבה של תחום זה, הבנת טיבו והשלכותיו עודם מצויים בראשית הדרך.

בשנים האחרונות הגבירו מדינות רבות, ובראשן ארצות־הברית וישראל, את קצב פעילותן בזירה הקיברנטית. פעילות זו מהווה עבורן מקור עוצמה, אך

גיל ברעם היא תלמידה לתואר שני בתוכנית ללימודי ביטחון באוניברסיטת תל אביב, עמיתת מחקר בסדנת יובל נאמן למדע טכנולוגיה וביטחון.

גם חושפת את "הבטן הרכה". זאת משום שהתשתיות החיוניות לתפקודה של כל מדינה הפכו תלויות במחשבים. אופן ההתמודדות הרצוי עם האיום הנשקף כתוצאה מהתפתחות טכנולוגיית הלוחמה הקיברנטית הוא תחום עיסוק מרכזי שעמו מתמודדת מדינת ישראל בשנים האחרונות.[1]

האינטרס הלאומי של ישראל מתרכז בשמירה על ביטחונה מפני אלה המעוניינים לפגוע בה ומערערים על עצם קיומה. אינטרס זה, וכן מיקומה הגיאו־פוליטי של ישראל, מחייבים אותה ליצור עליונות בתחום הקיברנטי כחלק בלתי־נפרד מיכולתה להגן על עצמה מפני פגיעות קונוונציונליות וקיברנטיות, וכיכולת התקפית הרתעתית בזירת המזרח התיכון ומעבר לו.

ישראל נחשבת למובילה בעולם מבחינת יכולת התמודדותה עם תקיפות קיברנטיות: בדו"ח מקיף שבחן את מידת מוכנותן של 23 מדינות בתחום הקיברנטי קיבלה ישראל את הציון הגבוה ביותר – ארבעה כוכבים וחצי מתוך חמישה. מהדו"ח עלה כי ישראל נתונה בכל דקה תחת כאלף מתקפות קיברנטיות. נתון זה הרשים במיוחד את מחברי הדו"ח, ששיבחו את מערכות ההגנה הישראליות וציינו שישראל ערוכה היטב להתמודדות עם מתקפה קיברנטית נגדה.[2]

פיתוח יכולות הפעולה של ישראל בזירת הלוחמה הקיברנטית הוא מרכיב מרכזי בשמירה על חוסנה הלאומי. הכלכלה, התעשייה, הביטחון, החינוך והשמירה על קיומה כחברה דמוקרטית, פתוחה ומבוססת ידע תלויים, ברובם, ביכולתה להגן על רשתות המחשבים החיוניות שלה מפני פגיעה שעלולה להוביל לשיבוש אורח החיים התקין במדינה. ההישענות הגוברת על מערכות מחשב בארץ ובעולם הביאה עמה אתגרים חדשים, המצריכים מענה מיידי ברמה הלאומית.[3]

מטרת המאמר היא להציג את מקומה של טכנולוגיית הלוחמה הקיברנטית בתפיסת הביטחון הישראלית, ולבחון את ההיערכות שבוצעה בישראל במטרה להתמודד עם האיום הקיברנטי באמצעות בחינת שלושה תחומים מרכזיים: גיבוש אסטרטגיה סדורה להתמודדות עם האיום הנשקף כתוצאה מהתפתחות טכנולוגיית הלוחמה הקיברנטית; הקצאת משאבים ותקציבים; יצירת שינויים בבניין הכוח. ההנחה היא כי באמצעות בחינת הפרסומים הממשלתיים אפשר יהיה ללמוד על מידת חשיבות הנושא עבור מקבלי ההחלטות, ומכאן על המשאבים המוקצים להתמודדות איתו. כל זאת, מתוך כוונה להציג את המצב בישראל ולנסות להצביע על הפערים הקיימים בתחום.

המאמר מתבסס על ספרות עדכנית בנושא ועל מידע פומבי בלתי־מסווג הכולל קטעי עיתונות, הצהרות לתקשורת, מסמכי ממשל וראיונות עם אישים מרכזיים בתחום. יש לציין כי בישראל קטן מספרם של הפרסומים הרשמיים על אודות דרכי ההתמודדות עם האיום הקיברנטי, ובפרט ביחס ליכולותיה ההתקפיות בתחום.

על כן, סביר להניח שלאור אופייה הביטחוני של ישראל, מידע רב על פעולות המבוצעות בנושא ותקציבים המוקצים לתחום נותר חסוי.

ביצוע המחקר לווה במספר קשיים: כיוון שמדובר בתחום מחקר חדש יחסית, עדיין לא קיים מספיק ידע היסטורי בנושא השפעתה של התפתחות טכנולוגיית הלוחמה הקיברנטית על יצירת שינויים באסטרטגיות הקיימות ועל בניין הכוח. עם זאת, כיוון שמדובר בתחום בעל חשיבות רבה רצוי להתחיל להתעמק בו חרף פערי הידע הקיימים.

חשוב לציין כי המחקר מתמקד בתחום הלוחמה הקיברנטית, המורכב מהיערכותה של המדינה בתחומי ההגנה וההתקפה, ואינו עוסק בתחום השימוש במחשבים לצרכי תקשורת או ניהול לחימה. משום שהמחשבים משמשים כיום לביצוע פעולות רבות בתחומי התקשורת והלחימה, מדובר בתחום נרחב מאוד, החורג מהיקפו של מאמר זה.

מקומה של טכנולוגיית הלוחמה הקיברנטית בתפיסת הביטחון הישראלית

השינויים הרבים שחלו בתחום טכנולוגיות הלוחמה הקיברנטיות מאתגרים את התפיסות הביטחוניות הקיימות, ומחייבים בחינה מחודשת של מושגי היסוד. נוצר מצב שבו יש חשיבות ראשונה במעלה להגנה על התשתיות החיוניות של המדינה בתחומי האנרגיה, המים, המחשוב, התקשורת, התחבורה והכלכלה – הן במגזר האזרחי והן במגזר הביטחוני. על כן, יש לערוך את ההתאמות הנדרשות בתפיסת הביטחון על מנת שתוכל לספק מענה לאיומים החדשים.[4]

באפריל 2006 הוגשה לשר הביטחון דאז, עמיר פרץ, הצעה לתפיסת ביטחון מעודכנת. ההצעה הוכנה על ידי ועדה בראשות דן מרידור, שבין חבריה היו ראש המועצה לביטחון לאומי, ראש השב"כ, הממונה על הביטחון במערכת הביטחון ונוספים. מדו"ח הוועדה עלה שישראל נמצאת בעידן של שינויים אסטרטגיים גדולים ומהירים, ביניהם שינויים טכנולוגיים מרחיקי לכת.[5] בין היתר, המליצה הוועדה להוסיף את ההגנה כרכיב נוסף לשלושת הרכיבים המסורתיים (הרתעה, התרעה והכרעה),[6] ובפרט המליצה על הצטיידות בכלי־טיס בלתי־מאוישים ועל יצירת הגנה על מערכות המחשב הלאומיות מפני חדירת גורמים עוינים.[7]

בעקבות דיוני הוועדה עלתה האפשרות לצרף מונח יסוד רביעי ל"משולש הביטחון", והוא "התגוננות" או "הגנה".[8] ישראל אכן השקיעה חלק ניכר מתקציבה וממאמצי הביטחון שלה בהתגוננות פסיבית. רעיון ה"הגנה" הורחב, ונכללו בו, נוסף לכלי ההתגוננות הפסיביים, גם כלים התקפיים נקודתיים שמטרתם לסכל ירי תלול־מסלול או פיגועי טרור שמתחת לרף ההסלמה הרחבה.[9]

בתחום הלוחמה הקיברנטית קיימת חשיבות עליונה להגנה, כיוון שבאמצעות הגנה יעילה אפשר לוודא שמערכותיה החיוניות של המדינה ימשיכו לתפקד. נוסף על כך, יכולות קיברנטיות מתקדמות מאפשרות למדינה הגנה יעילה על התשתיות הקריטיות שלה וכך מספקות מענה לצורך בהגנה אקטיבית, כפי שהוצג בדו"ח ועדת מרידור.

במשך זמן רב נהוג היה לכנות את תחום ההגנה על מערכות ממוחשבות "אבטחת מידע", לפי התפיסה שהדבר המרכזי שעליו יש להגן הוא מידע רגיש (מידע מסווג או עסקי). עם השנים התפתחה גישה זו והקיפה איומים נוספים מלבד פגיעה במידע – מניעת שירות, השבתת תהליכים חיוניים מבוססי מחשב ועוד. ברמה הלאומית התרחב מושג ההגנה על מערכות ממוחשבות, ואפשר לכנותו "הגנה קיברנטית".[10] מאז פרסום הדו"ח חלה עלייה ניכרת בשימוש בטכנולוגיה קיברנטית לצורכי לחימה שונים בשדה הקרב. על כן, ראוי לבחון את מקומה של טכנולוגיית הלוחמה הקיברנטית בתהליכי עדכון תפיסת הביטחון של ישראל.

במבט היסטורי על מלחמות ישראל אפשר לראות שחשיבות הטכנולוגיה עלתה ממלחמה למלחמה, והשתכללה עם השנים. בין ישראל לבין מדינות ערב קיימים הבדלים בסיסיים, וכן קיימת א־סימטריה כמותית ברורה. אם שוקלים את הפערים הכמותיים הגדולים, בולט יתרונה היחסי של ישראל בהסטת המלחמה למישור הטכנולוגי: לישראל קל יותר להתמודד עם העולם הערבי בקרבות אוויר מתוחכמים או בביצוע פעולות קיברנטיות (על פי פרסומים זרים) מאשר בזריקת אבנים או בהתמודדות של חייל מול חייל. ככל ששדה הקרב רווי בטכנולוגיות מתקדמות, הולכים ומצטמצמים הפערים הכמותיים, וגדל ערכן של איכויות מערכות הנשק ושל כוח האדם. בצה"ל היטיבו לזהות את הפוטנציאל הרב הטמון במחשבים, וכבר משנות התשעים החל השימוש בלוחמת מחשבים (computer warfare) על סוגיה השונים.[11]

ההתמודדות עם האיום הנשקף כתוצאה מהתפתחות טכנולוגיית הלחימה הקיברנטית הולמת את תפיסת הביטחון הישראלית: מדובר בתחום המופעל ביכולות "כחול־לבן", שמסתמך על כושר הפיתוח וההמצאה "היהודי", בשילוב טכנולוגיות עולמיות. התחום מוכר היטב לישראלים הצעירים במדינה, שהוגדרה לאחרונה כ"מדינת סטארט־אפ"[12] ומתבסס על העיקרון של חשיבות האיכות על פני הכמות.

אפשר לראות ש"שלוש הרגליים" המקוריות של תפיסת הביטחון הישראלית המסורתית רלוונטיות עבור ההתמודדות עם האיום הקיברנטי:

1. הרתעה – יכולות קיברנטיות מתקדמות יאפשרו לישראל ליצור הרתעה מול אויביה. כדוגמה אפשר לראות את אירוע וירוס "סטקסנט" המיוחס לארצות־הברית ולישראל, שנתפס כעליית מדרגה בכל הנוגע ליכולות התקיפה

הקיברנטיות של מדינות ולעוצמת השפעתן, זכה לתהודה רחבת־היקף בתקשורת העולמית ותרם לחיזוק ההרתעה הישראלית.[13]

2. התרעה – היכולות הקיברנטיות מאפשרות לישראל לאסוף מידע רב על אויביה ובמקביל, למנוע מהם גישה למאגרי המידע שלה. כך תוכל המדינה להתריע באופן יעיל על כוונותיהם נגדה.
3. הכרעה – ישראל היא מהמדינות המובילות בעולם מבחינת יכולותיה הקיברנטיות. יכולות אלה מאפשרות לה להשיג יתרון בקרב, באמצעות שימוש בכלים קיברנטיים מתקדמים, ולהכריעו לטובתה. חשוב לציין כי מושג ההכרעה בתחום הקיברנטי, כמו למושג ההרתעה, הם מושגים חמקמקים שמשמעותם בהקשר הקיברנטי טרם מוצתה עד תום. עם זאת, כיום ברור כי עליונות קיברנטית בשילוב עם יכולות קינטיות מתקדמות עשויה להוביל להכרעת קרבות.

מקום המדינה ועד היום מושתתת תפיסת הביטחון על עקרון חשיבות האיכות על פני הכמות. טכנולוגיית הלחימה הקיברנטית עונה על עיקרון זה: באמצעות כלים קיברנטיים, שאינם דורשים הפעלת כוח פיזי רב אלא הכשרת כוח אדם מיומן, מתאפשרות פעולות המסייעות להגברת יכולת ההרתעה של ישראל ומקנות לה יוקרה רבה בזירה הבינלאומית.

לסיכום, נראה שאפשר לשלב את יכולות הלחימה הקיברנטית בתפיסת הביטחון הישראלית באופן פשוט יחסית, אם אכן זו תעודכן בקרוב. זאת משום שיכולות אלה עונות על שלושת העקרונות הבסיסיים שעליהם בנויה תפיסת הביטחון. כמו כן, פיתוח יכולות לחימה קיברנטיות עצמאיות וכלי לוחמה קיברנטיים מממשים בבירור את עקרון האיכות על פני הכמות: כל שנדרש הוא כוח אדם מיומן ברמה גבוהה לפיתוח מערכות המאפשרות ביצוע פעולות ביעדים רחוקים, מבלי לסכן חיי אדם ומבלי להזדקק למשאבים רבים.

גיבוש אסטרטגיה סדורה לתחום הקיברנטי

האיום הקיברנטי הוא פועל יוצא של תפקידן הקריטי של מערכות המחשב בתשתיות הלאומיות ובחיי היום־יום. מרחב וירטואלי זה נוצר מהתפתחות מבוזרת של מערכות ומגזרים שונים, כחלק מהתפתחות כלכלית וטכנולוגית מואצת, ללא הקשרים ביטחוניים מובהקים. כשעלה בשנים האחרונות הצורך לעסוק בהיבטים הביטחוניים של התחום הקיברנטי, נשאלה השאלה – מיהו "בעל הבית" והאחראי לביטחון בו?[14]

אבטחת מידע והגנה על תשתיות ממוחשבות אינם נושאים חדשים בישראל. ישראל הייתה מהמדינות הראשונות בעולם שהכירו בחשיבות ההגנה על מערכות ממוחשבות חיוניות. כבר בשנת 1996 קיבלה הממשלה החלטות באשר לדרך

ההתגוננות הרצויה מפני איומים קיברנטיים.[15] בשנת 1997 הוקם פרויקט תהיל"ה (תשתית הממשלה לעידן האינטרנט), שמטרתו להגן על חיבור משרדי הממשלה לאינטרנט ולספק שירותי גלישה מאובטחים למשרדי הממשלה.[16] בהמשך, בשנת 1998 חוקק "החוק להסדרת הביטחון בגופים ציבוריים", שעסק בהגדרת מערכות ממוחשבות חיוניות ובאבטחתן.[17]

ההחלטה על הקמת הרשות הממלכתית לאבטחת מידע

בישראל אין פרסום מוסדר של המדיניות הציבורית בתחום ההתמודדות עם האיום הקיברנטי, ומרבית המידע הקיים נסמך על פרסומים בתקשורת ומחקרים אקדמיים. עם זאת, מספר החלטות רשמיות שפורסמו שופכות אור על המצב: בפברואר 2002 התקבלה בוועדת השרים לענייני ביטחון לאומי ההחלטה בנושא "אחריות להגנה על מערכות ממוחשבות במדינת ישראל" (החלטה ב/84), שעיצבה את מתווה ההגנה על התשתיות הממוחשבות הקריטיות במדינה. ההחלטה משמשת בסיס להפעלת המענה הישראלי לאיום הקיברנטי על תשתיות מחשב לאומיות חיוניות. בהחלטה נקבעה הקמתם של שני גופים ייעודיים: האחד – ועדת היגוי עליונה שתבחן באופן שוטף את זהות הגופים הציבוריים והפרטיים החיוניים לתפקודה של מדינת ישראל; השני – יחידה ממלכתית להגנה על המערכות הממוחשבות.

ואכן, בהמשך להחלטת ועדת השרים הוקמה כבר באותה שנה ועדת היגוי בראשות ראש המועצה לביטחון לאומי, שמטרתה הייתה לגבש מכלול צעדים להגנה על מערכות המחשב החיוניות של המדינה. בוועדה נקבעו עקרונות תפיסת ההגנה, איומי הייחוס והגופים שיחויבו בצעדי הגנה.[18] כמו כן, היא פעלה כצוות היגוי המנחה את היחידה הממלכתית לאבטחת תשתיות ממוחשבות בשירות הביטחון הכללי (שב"כ).

באותה השנה הוקמה "הרשות הממלכתית לאבטחת מידע", הפועלת במסגרת חוק השב"כ. הרשות מנחה את הגופים שהוגדרו כחיוניים בנושאי ביטחון המחשוב והגנה על הרשתות, ומפקחת על ביצוע הנחיות אבטחת המידע והגנתו. כמו כן, היא מוסמכת לנקוט סנקציות נגד גופים המפרים את הנחיותיה. יש לציין כי גופי הביטחון השונים פועלים להגנה על תשתיותיהם הקריטיות באופן עצמאי, ללא הנחיה רשמית של הרשות לאבטחת מידע.[19]

ההחלטה על הקמת המטה הקיברנטי הלאומי

בנובמבר 2010 הטיל ראש הממשלה על יושב ראש המועצה הלאומית למחקר ולפיתוח, אלוף במיל' פרופסור יצחק בן ישראל, להציג תוכנית עבודה למיזם לאומי להתמודדות עם האיום הקיברנטי.[20] בין המלצותיו של צוות המיזם היו: המלצה 1 א' – הקמת מטה קיברנטי לאומי להגנה, שייעודו קידום הגנת המרחב

הקיברנטי בישראל. המלצה 1 ב' – הרחבת סמכויות שב"כ כגוף הביצוע לטיפול במרחב האזרחי.[21]

המסמך המרכזי בנושא הוא החלטת הממשלה מיום ה־7 באוגוסט 2011 בנושא "קידום היכולת הלאומית במרחב הקיברנטי".[22] החלטה זו היא תולדה של פעילות צוות המיזם. בהחלטה נקבעה הקמת המטה הקיברנטי הלאומי, ונקבע כי מטרתו היא "קידום היכולת הלאומית במרחב הקיברנטי ושיפור ההתמודדות עם האתגרים הנוכחיים והעתידיים במרחב הקיברנטי". אחד מתפקידיו של ראש המטה הוא "להמליץ לראש הממשלה ולממשלה על מדיניות קיברנטית לאומית, להנחות את הגורמים הרלבנטיים אודות המדיניות עליה הוחלט... ליישם את המדיניות ולבקר את יישומה".[23] ההחלטה על הקמת המטה, שפורסמה בפומבי, הייתה התקדמות משמעותית באופן טיפולה של הממשלה בנושא האיום הקיברנטי, והיוותה נקודת מפנה בתחום.

בעוד גופי הממשל, זרועות הצבא וגופי מערכת הביטחון מוגנים על פי חוק, מרבית המגזר העסקי והאזרחים מהשורה נותרו ללא הגנה מספקת בתחום. המגזר העסקי אינו נתון לפיקוח רשמי ואינו כפוף לגוף לאומי כלשהו, האחראי לבדוק את יכולות ההתמודדות עם פגיעה במערכות המחשב החיוניות שלו בשעת חירום. זוהי נקודת תורפה משמעותית של ישראל, שכלכלתה תלויה בכושר הייצור והייצוא של המגזר העסקי והתעשייתי.[24]

מקבלי ההחלטות בישראל צופים שבמלחמה הבאה ייעשה שימוש באמצעי לוחמה קיברנטיים, ואף על פי כן, אין כיום גוף רשמי בישראל שאחראי ישירות על הגנת המגזר העסקי. נכון הוא שרשות לאומית אינה יכולה להחליף את המנהלים האחראיים על עסקיהם, אך מאחר שחלק מהארגונים הפרטיים במשק מספקים שירותים החיוניים להמשך החיים התקינים בעורף, יש מקום להתערבות ממשלתית בהנחיות, בתקנות ובבקרה.[25]

עם הקמת המטה הקיברנטי הלאומי אמר ד"ר אביתר מתניה, ראש המטה, כי לתפיסתו קיימים חמישה היבטים שבהם על המדינה להתערב בהקשר הקיברנטי:

1. יצירת נקודת מבט כלל־מערכתית ברמה הלאומית: ההגנה הקיברנטית מחייבת בחינה רב־מערכתית, מאחר שקיימת תלות הדוקה בין המערכות הציבוריות למערכות הפרטיות והעסקיות.
2. "איגום" משאבים, פעולות ומידע: משמעות האיגום היא איחוד משאבים ממקורות שונים לגוף מתַכלל אחד, במטרה להתמודד בצורה טובה יותר עם האיומים הנשקפים לישראל.
3. יצירת שיתוף פעולה בינלאומי: על ישראל להוביל את נושא שיתוף הפעולה באופן יזום, וליצור שיתופי פעולה עם בעלות־ברית ברחבי העולם.

4. יצירת הסדרה לתחום הקיברנטי: ביצוע הסדרה תקינה, רישוי והסמכה, וכינון שיטה שבה ארגונים ופרטים יהיו מסוגלים להגן על עצמם על פי סטנדרטים מוגדרים וברורים.[26]
5. קידום תהליכים על ידי המדינה: כפי שפעלה המדינה בשנות השישים לקידום תחום התעופה בארץ, באמצעות הקמת הפקולטה לאווירונאוטיקה בטכניון, כך היא צריכה לספק כלים ומנופים על מנת לתמרץ פיתוחים אקדמיים ותעשייתיים בתחום הקיברנטי.[27]

לדברי מתניה, מטרת המטה הקיברנטי הלאומי היא תכנון כלל העשייה בתחום ההגנה הקיברנטית: חיזוק האבטחה בארגונים באמצעות יצירת הסדרה חוצת ענפים המותאמת למאגרי המידע, וכן הסדרה ענפית לכל תחום ותחום. נדבך נוסף הוא בניית תוכניות לאומיות, שיתוף פעולה ושיתוף המידע, במיוחד בקשר שבין המערכת הביטחונית והמערכת האזרחית.[28]

מהות פעילות המטה נוגעת להסדרה, לתִכלול ולקידום הפעילות הכלל־ממשלתית בתחום הקיברנטי בראייה רחבה, אזרחית וביטחונית כאחד. המטה פועל ברוח החלטת הממשלה, יחד עם הגופים הרלוונטיים, לגיבוש מדיניות הגנה ובניית תפיסת הגנה לאומית, וליצירת שיתופי פעולה בין כלל הגופים הפועלים בתחום. זאת לצד גיבוש תוכניות כוללות ובניית מנגנונים לטיפוח ההון האנושי בתחום הקיברנטי; פיתוח תשתיות טכנולוגיות ומחקריות באקדמיה ובתעשייה; קידום שיתופי פעולה בין המגזר הפרטי־עסקי, המגזר הממשלתי, התעשייה, האקדמיה ומערכת הביטחון; קידום המודעות הציבורית לאיום הקיברנטי ועוד.[29]

מהאמור לעיל אפשר לראות שישראל היטיבה לזהות את האיום הנשקף לתשתיותיה הלאומיות, ופעלה להקמת מערך הגנה ברמה הלאומית. שתי נקודות ציון מרכזיות הן: הקמת הרשות הממלכתית לאבטחת מידע (רא"מ) בשנת 2002; החלטת הממשלה מאוגוסט 2011 על "קידום היכולת הלאומית במרחב הקיברנטי" והקמת המטה הקיברנטי הלאומי. עם זאת, הממשל הישראלי טרם הפיץ לציבור אסטרטגיה מוסדרת ואחידה בנושא.

ישראל היא מהמדינות המובילות בעולם ביכולותיה הקיברנטיות, אולם, כנהוג בישראל, אין לכך ביטוי הולם בכל הנוגע לקביעת אסטרטגיה סדורה ולפרסום ברור של דרך הפעולה הרשמית בתחום. נראה כי בישראל טרם גובשה אסטרטגיה בתחום,[30] וכי עיקר המידע מגיע מהצהרות לעיתונות ומכתבות בתקשורת, ולא ממידע ממשלתי רשמי. אמנם קיימת החלטת ממשלה רשמית בנושא, אולם טרם פורסמה אסטרטגיה סדורה.

הקצאת תקציבים

בחלק זה ייבחנו התקציבים והמשאבים שהוקצו להתמודדות עם האיום הנשקף כתוצאה מהתפתחות טכנולוגיית הלוחמה הקיברנטית, מתוך הנחה שבחינת התקציבים תאפשר להקיש על מידת חשיבותו של הנושא עבור מקבלי ההחלטות בישראל.

המועצה הלאומית למחקר ופיתוח (המולמו"פ) יזמה בשנת 2007 ומימנה מחקר בנושא "מדדים למדע, לטכנולוגיה ולחדשנות בישראל", בשיתוף הלשכה המרכזית לסטטיסטיקה. מטרת המחקר הייתה לבחון את התקציבים המוקצים לנושאי מדע וטכנולוגיה בישראל. מהמחקר עלה שבעשור האחרון הוצאו בישראל מדֵי שנה כ־30 מיליארד ש"ח למחקר ופיתוח (מו"פ) אזרחי. בחינת האחוז מהתוצר הלאומי הגולמי המושקע במחקר ופיתוח הראתה שישראל מדורגת במקום הראשון בעולם – 4.3% בשנת 2009, לעומת 1.8% בממוצע במדינות הארגון לשיתוף פעולה כלכלי ולפיתוח (OECD). מרבית המימון בישראל, כ־79%, מגיע מהמגזר העסקי. הממשלה מממנת באופן ישיר כ־5 מיליארד ש"ח מהמו"פ האזרחי, נוסף על הכספים המוקצים למימון המו"פ בתחום הביטחוני.[31]

מהנתונים אפשר ללמוד שמדינת ישראל והמגזר העסקי שלה משקיעים סכומים לא־מבוטלים במחקר ופיתוח בתחום הטכנולוגי. לכך אפשר לצרף את התקציבים השונים שחולקו בשנה האחרונה למחקר ופיתוח בנושאים יישומיים ותיאורטיים בתחום הקיברנטי.[32] מצירוף הנתונים ניתן להניח שהתחום הקיברנטי מקבל תקצוב למטרות מחקר ופיתוח, מתוך הכרה בחשיבותו הגוברת לביטחון המדינה. התקצוב המדויק אינו מתפרסם ברבים.

אחת ההוצאות העיקריות בהצעת תקציב המדינה לשנים 2011–2012 יועדה ל"אשכול הביטחון והסדר הציבורי". מתוך הוצאה זו מוקצים כספים לגופי מערכת הביטחון השונים, האחראים על הטיפול בתחום הקיברנטי. סך התקציב שהופנה למימון האשכול עמד על סכום כולל של 61.8 מיליארד ש"ח בשנת 2011, וסכום כולל של 63.4 מיליארד ש"ח בשנת 2012. מתוך הסכומים האמורים, ההוצאות שהופנו לפעילות משרד הביטחון היו הגבוהות ביותר, ושיעורן עמד על כ־18% מסך ההוצאה התקציבית.[33] ניתן להניח שמשרד הביטחון משקיע סכומים לא־מבוטלים גם בפיתוח תחום הלוחמה הקיברנטית בגופים המצויים באחריותו.

המלצה נוספת של צוות המיזם הקיברנטי הייתה לייסד תוכנית מו"פ לאומית לבניית יכולות קיברנטיות, בשיתוף עם מערכת הביטחון, עם האקדמיה ועם התעשייה. התוכנית כללה המלצות להכוונת המשאבים הלאומיים הקיימים והוספת משאבים במידת הצורך. כל זאת במטרה להציב את ישראל בחמישייה המובילה של מדינות העולם מבחינת יכולותיה הקיברנטיות עד שנת 2015.[34] בהקשר זה חשוב לציין כי לא מדובר בהכרח רק בפיתוח יכולות צבאיות־ביטחוניות,

אולם סביר להניח כי לפחות חלק מהתקציב יוקצה לפיתוח ביטחוני בתחום הקיברנטי.

תקציב המטה הקיברנטי

בהחלטת הממשלה מאוגוסט 2011 שבה הוחלט על הקמת המטה הקיברנטי הלאומי, הוחלט להקצות למטה תקציב שיועבר למשרד ראש הממשלה ממקורות משרד האוצר.[35] התקציב המלא שהוקצה לפעולות המטה אינו מפורט בהחלטה, מלבד סכום קטן (כ־4.5 מיליון ש"ח) שהוקצה עבור "הקמת ותפעול המטה" לשנת 2011.

תקציב המטה הקיברנטי כיום הוא 2.5 מיליארד ש"ח לחמש השנים הבאות, כ־500 מיליון ש"ח בשנה. 100 מיליון מתוכם יוקצו כסכום ייעודי מתקציב המדינה עבור המטה הקיברנטי, ו־400 מיליון יינתנו לאחר תהליך "איגום" כספים ממקורות שונים.[36] לדבריו של רס"ן טל, ראש תחום בכיר במטה הקיברנטי, ראש הממשלה רואה בתחום הקיברנטי נושא בעל חשיבות עליונה ופועל רבות לקידומו. קיימת נכונות לפיתוח התחום והתקציבים ניתנים בהתאם. חשיבות האיום הקיברנטי צוברת תאוצה, ואף נבנתה תוכנית ארוכת־טווח שתבטיח את תקציביו.[37]

בישיבת ועדת הכספים מחודש מאי 2012 הוקצו באופן מפורש תקציבים להמשך קידום פעילותו של המטה, מעבר לסכומים שכבר הוקצו.[38] בקשת המטה, כפי שהובאה לאישור הוועדה, כללה כ־12 מיליון ש"ח למימון שני נושאים מרכזיים: הראשון – תקציב תפעול המטה, שכלל תשלום משכורות לעובדי המטה ויצירת תשתיות ממוחשבות ותשתיות אבטחה פיזיות עבור גופים מסווגים הנדרשים לתשתיות מסוג זה. השני – תחילת מימוש תקציב פעילותו השוטפת של המטה.[39]

מתוך הכרה בחשיבות הקשר בין האקדמיה, התעשייה והמטה הקיברנטי הוקצו על ידי המטה, בשיתוף משרד המדע, כ־50 מיליון ש"ח לשלוש שנים עבור מלגות ומחקרים בתחומי עיסוק שונים של תחום העיסוק הקיברנטי, במטרה למצב את ישראל כמובילה בעולם בתחום.[40] נוסף לכך, הכריזו המדען הראשי והמטה הקיברנטי על הקצאת 80 מיליון ש"ח עבור תוכנית קידמ"ה,[41] שמטרתה פיתוח המו"פ והיזמות בנושא ה־Cyber Security.[42] גם במקרה זה, סביר להניח שחלק מהמלגות יוקצו לתחומים הנוגעים ללוחמה הקיברנטית.

לנוכח מיעוט הפרסומים העוסקים בנושא התקציב, קשה לאמוד מהי ההשקעה הממשלתית המדויקת בהתמודדות עם האיום הקיברנטי בישראל. עם זאת, מהנתונים שהוצגו לעיל אפשר לראות שהאיום הנשקף כתוצאה מהתפתחות טכנולוגיית הלוחמה הקיברנטית לא נעלם מעיניהם של מקבלי ההחלטות במדינה, וכי הנושא זוכה למשאבים לא־מבוטלים.

החל משנת 2011 החלו להתפרסם בפומבי הקצאות תקציבים לתחום הקיברנטי. ניתן להניח במידה רבה של ודאות, שלאור העובדה שהטיפול בתחום הקיברנטי הובל בעשור האחרון על ידי מערכת הביטחון במעטה סודיות, תקציבים שונים שהוקצו לתחום זה אינם מפורסמים בגלוי. עם זאת, לאחר קבלת ההחלטה הרשמית על הקמת המטה הקיברנטי הלאומי באוגוסט 2011, החל להתפרסם בגלוי מידע על התקציבים המופנים להתעצמות ולנושאי מחקר ופיתוח בתחום.

שינויים בבניין הכוח

טכנולוגיית הלוחמה הקיברנטית יצרה שינוי במערכות הנשק של זירת הלחימה המודרנית, והפכה אותן למדויקות וליעילות יותר. בעקבות השינויים הרבים שחלו בסביבתה החיצונית של ישראל, גברו אתגרי הביטחון שמולם היא ניצבת, וגדלה מידת חשיבותו של המודיעין בתפיסת הביטחון הישראלית. כיום ניצבת ישראל בחזית הטכנולוגיה ומתמודדת עם האיומים הנשקפים לה, בסיוע כלים טכנולוגיים קיברנטיים המשולבים בכל זירות הלחימה.[43]

להתפתחויות מסוג זה הייתה השפעה לא־מבוטלת על עקרונות המלחמה ועל שינויים שחלו במבנה צבאות, ובכלל זה במבנה צה"ל. בבואו לבחון את מקומה של הטכנולוגיה לאורך מלחמות ישראל, טען פרופ' בן ישראל כי ככל ששדה הקרב מתקדם יותר מבחינה טכנולוגית, כך הגמישות והיכולת לאלתר ולשנות (changeability) תופסות חלק גדול יותר בלחימה המודרנית. למשל, מלחמת יום־הכיפורים הדגימה היטב שלא די לבנות מערכות לוחמה אלקטרונית נגד האיומים המוכרים של האויב, אלא יש צורך לבנותן כך שיוכלו להתמודד עם השינויים שיעשה האויב בפרמטרים האלקטרוניים של מערכותיו תוך כדי הלחימה.[44]

להלן ייבחנו השינויים המרכזיים שחלו בגופים הממשלתיים ובגופי מערכת הביטחון בישראל, לאור ההכרה הגוברת בסיכונים הנשקפים מהתפתחות האיום הקיברנטי ומכניסתה של הטכנולוגיה הקיברנטית לשדה הקרב.

המטה הקיברנטי הלאומי

באוגוסט 2011 הכריז ראש הממשלה על הקמת "המטה הקיברנטי הלאומי", שייעודו העיקרי הוא הרחבת יכולות ההגנה על מערכות התשתית החיוניות למדינה מפני התקפות טרור קיברנטי, העלולות להיגרם הן על ידי מדינות זרות והן על ידי גורמי טרור.[45] המטה, הפועל כשנה וחצי ומצוי בשלבי צמיחה, מורכב כיום מארבעה אגפים: האגף הביטחוני; האגף האזרחי; אגף המודיעין והערכת מצב; האגף לארגון ולמדיניות. נוסף לכך הוקם חדר מצב בירושלים, הפעיל 24 שעות ביממה שבעה ימים בשבוע, ומצוי בקשר רציף עם הגופים הביטחוניים העוסקים בתחום. חדר המצב מאפשר ראייה כוללת של סך האיומים ואפשרויות ההתמודדות,

כך שבשעת ביצוע תקיפה קיברנטית על גוף אחד, אפשר יהיה לדעת בזמן אמת על אילו גופים נוספים יש להגן.

שלושת הנושאים המרכזיים שעליהם אמון המטה הקיברנטי הם:

הראשון – גיבוש תפיסת ההגנה הרשמית של ישראל, זאת באמצעות שיתוף פעולה בין כלל הגופים האמונים על תחום ההגנה. נוסחה תפיסה הפועלת בשתי רמות: רמת האבטחה הכללית במשק ורמת האבטחה המדינתית.

השני – פיתוח התשתית וקידום המובילות הלאומית של ישראל בתחום הקיברנטי. בין היתר, באמצעות הרחבת ההון האנושי וקידום נושא המלגות למחקרים בתחום הקיברנטי.

השלישי – הובלת תהליכים לאומיים בתחום הקיברנטי, כמו יצירת הסדרה בשוק האבטחה; יצירת תשתית אבטחה מדינתית באמצעות חקיקה וביצוע תרגילי חירום; חיזוק קשרי החוץ עם מדינות שונות בעולם ועוד.[46]

ההחלטה על הקמת המטה הייתה צעד חשוב בהתמודדותה של ישראל עם האתגר הקיברנטי, אולם יש להבטיח כי המטה יפעל על פי אסטרטגיה לאומית שתגובש בהקדם. לנוכח פיגורה של ישראל בקביעת אסטרטגיה פומבית סדורה, יש חשיבות רבה לכך שהמטה יקבל סמכויות רחבות־היקף. רק כך אפשר יהיה להתחיל לצמצם את הפער שנוצר ברמה הלאומית בניהול האסטרטגי המקיף של כלל הגופים האזרחיים והצבאיים הפועלים בתחום הקיברנטי.[47]

הרשות הממלכתית לאבטחת מידע

הגוף הוותיק ביותר העוסק בנושא אבטחת המידע על היבטיו השונים הוא "הרשות הממלכתית לאבטחת מידע" בשב"כ. רשות זו צמחה מתוך יחידה שטיפלה במשך עשרות שנים בתחום אבטחת המידע הקלאסית, עד שקיבלה בשנת 2002 את האחריות על הנחיית כל גופי התשתיות הלאומיות האזרחיים להתגוננות מפני מתקפות סייבר אפשריות.

השב"כ קיבל סמכות על פי חוק להנחות גופים כגון חברת חשמל, מקורות, רכבת ישראל וחברות הגז. תחומי ההנחיה כוללים הוראות כמו כיצד למנוע השתלטות עוינת מרחוק, שעלולה לגרום פגיעה קשה במערכות קריטיות בלחיצת מקש, וכדומה. בשנים האחרונות התרחבה רשימת הגופים המונחים על ידי הרשות, מתוך הכרה לאומית באיום הקיברנטי הגובר.[48]

צפריר כץ, שכיהן עד לאחרונה כראש אגף הטכנולוגיה בשב"כ, העניק הצצה נדירה אל הנעשה בתחום הטכנולוגי בשב"כ ואמר כי כ־20% מאנשי השירות הם אנשים טכנולוגיים. השירות שינה את פניו לעומת שנות השמונים של המאה הקודמת, אז לא היה מוטה לכיוון הטכנולוגיה. היה צורך לפתח צורות העסקה

למספר שנים עבור אנשים צעירים. לתפיסתו, מדובר במהפכה הנמשכת לאורך כל העשור האחרון.[49]

צה"ל

בשנת 2009 הגדיר הרמטכ"ל דאז, רב־אלוף גבי אשכנזי, את המרחב הקיברנטי "כמרחב לחימה אסטרטגי ואופרטיבי עבור מדינת ישראל". בהמשך לכך הוקם "מטה הסייבר הצה"לי", שנועד לשמש מטה מטכ"לי לתיאום ולהכוונה של פעולות הצבא בתחום הקיברנטי. המטה הוקם ביחידה 8200 באגף המודיעין של צה"ל.[50]

בחיל התקשוב הוקמה מחלקת הגנה בסייבר, שפעילותה מסווגת ברובה. המחלקה מאפשרת לקיים פעילויות מבצעיות ביבשה, באוויר ובים, בעידן שבו הצבא נשען יותר מתמיד על טכנולוגיית מחשבים. המחלקה פועלת בשיתוף פעולה עם מרבית היחידות המובחרות של צה"ל, בעודה מפעילה אמצעים טכנולוגיים מתקדמים מגוונים על מנת לנטרל את התקיפות הקיברנטיות של האויב.[51]

במטרה להגן על מערכות המחשוב של צה"ל, פיתח חיל התקשוב תוכנית הכשרה המכונה "מסלול הגנת הסייבר". במאי 2012 הסתיים המחזור הראשון של קורס "מגן בסייבר" של החיל. לאחר מספר חודשי לימוד אינטנסיביים הוכשרו החיילים לבצע פעולות הגנה במרחב הממוחשב, על רקע המציאות הטכנולוגית המתפתחת.[52]

משרד הביטחון

בינואר 2012 פורסם כי משרד הביטחון עומד להקים מנהלת מיוחדת ללוחמה קיברנטית, שתרכז את כלל פעולות גופי הביטחון והתעשיות הביטחוניות העוסקים בפיתוח מערכות מתקדמות בתחום. במהלך שנת 2012 הוקמו מטות מיוחדים לעיסוק בלוחמה קיברנטית בתעשיות הביטחוניות המרכזיות, דוגמת אלביט מערכות, רפא"ל והתעשייה האווירית; גם התעשייה הצבאית שוקלת להיכנס לתחום[53]. טרם הוחלט מי יעמוד בראש המִנהלת החדשה, ואולם לדברי גורמים ביטחוניים, עצם ההחלטה להקים מנהלת חדשה "תיקח את העיסוק בתחום למקום חדש".[54]

הרשות למשפט וטכנולוגיה

בספטמבר 2006 הוקמה הרשות למשפט ולטכנולוגיה (רמו"ט) במשרד המשפטים. תפקידה הוא להגן על המידע האישי בישראל. יעדי רמו"ט הם חיזוק ההגנה על מידע אישי; הסדרת השימוש בחתימות אלקטרוניות ופיקוח עליו; הגברת האכיפה על עבירות פגיעה בפרטיות, בכלל זה עבירות המבוצעות במרחב הקיברנטי.[55] רמו"ט משמשת גם מרכז ידע בממשלה לחקיקה ולפרויקטים בעלי היבטים

טכנולוגיים, כגון ממשל זמין.[56] בימים אלה מטפלת הרשות בחקירת פרטי האירוע שבו פורסם באינטרנט מידע אישי רב, לרבות נתונים של כרטיסי אשראי, על ידי מי שהזדהו כהאקרים סעודיים.[57]

"ממשל זמין" – e-gov.il (תהיל"ה)

מערך "ממשל זמין" הוקם באגף החשב הכללי במשרד האוצר בשנת 1997 כיחידת תהיל"ה. מטרת פעילותו היא לאפשר לאזרחים לבצע מגוון פעולות רחב מול משרדי הממשלה ורשויות המדינה באמצעות האינטרנט, במקביל לשמירה על אבטחת המידע המועבר ועל פרטיות המשתמש. המערך מפעיל משאבים רבים לשמירת הפרטיות, החל בצוות מומחי אבטחת מידע וכלה בשימוש בטכנולוגיות אבטחה מהמובילות בעולם.[58]

סיכום

ישראל היטיבה לזהות את מאפייניו של האיום הנשקף כתוצאה מהתפתחות טכנולוגיית הלוחמה הקיברנטית, החלה לפעול ליצירת השינויים הנדרשים ונראה כי קיימת זיקה הדוקה בין אופן הטיפול באיום הקיברנטי לבין ביטחונה הלאומי של המדינה. אופן הטיפול מתרכז בשלושה נושאים: **הראשון** – ארגונים ביטחוניים, צה"ל, קהילת המודיעין והתעשייה הביטחונית, שבמצב הקיים פועלים להגן על מערכותיהם באופן עצמאי, ואינם מונחים על ידי השב"כ. **השני** – התשתיות הלאומיות הקריטיות שאפשר לתקוף אותן תקיפה קיברנטית, ומונחות על ידי הרשות לאבטחת מידע. **השלישי** – המגזר הפרטי, שבו פועלות חברות אזרחיות החשופות למתקפות קיברנטיות. שכבה זו מטופלת בחלקה על ידי רמו"ט, ובחלקה הגדול אינה מטופלת כלל.[59]

המלחמה הקיברנטית מתחוללת במלוא עוזה, וישראל היא שחקנית ראשית בה.[60] ניתן לבחון את העובדות היבשות ולהתרשם: הוקם מטה קיברנטי לאומי במשרד ראש הממשלה; מענקים בגובה מיליוני שקלים יוענקו בכל אחת מהשנים הבאות למחקרים ולפעילויות חינוך בתחום הקיברנטי; בצבא חולקה האחריות בתחום הקיברנטי בין אגף המודיעין (התקפה) ואגף התקשוב (הגנה); והרשות הממלכתית לאבטחת מידע צפויה להרחיב את פעילותה.[61] נראה שהטיפול בתחום הקיברנטי צובר תאוצה במספר היבטים מרכזיים: החל להתפרסם בגלוי מידע על אודות העיסוק הממשלתי באיום הקיברנטי, הוקצו תקציבים ייעודיים למחקרים בתחום ונעשה ניסיון לתקצב את פעילות המטה הקיברנטי הלאומי באופן שוטף. במקביל, גופים שונים הוקמו ו/או התפתחו מאוד במטרה להתמודד באופן מיטבי עם האיום הקיברנטי הגובר.

השינויים הטכנולוגיים המהירים שהתרחשו בשנים האחרונות השפיעו על סדר העדיפויות של מקבלי ההחלטות במדינה בדרכים שונות, ביניהן פרסום החלטות ממשלה רשמיות והקמת גופים ייעודיים להתמודדות עם האיום הקיברנטי. אף שבמבט ראשון נראה שישראל מתקדמת מאוד בדרך התמודדותה עם האיום הקיברנטי הגובר, עדיין יש מקום לנקיטת פעולות נוספות המגדירות בצורה ברורה יותר מהי המדיניות הרצויה לטיפול כולל בנושא.

הערות

1 דברי פרופ׳ יצחק בן ישראל ונוספים, מתוך: פרוטוקול מס׳ 95 – ישיבת וועדת המדע והטכנולוגיה: ״לוחמה קיברנטית – הערכות מדינת ישראל למתקפות על רשתות מחשבים ותקשורת״. יום שני, ב׳ תמוז תשע״א, (4 ביולי 2011), שעה 11:00. http://www.knesset.gov.il/protocols/data/html/mada/2011-07-04.html

2 לפי דו״ח של צוות חשיבה בינלאומי בנושא ביטחון – SDA (Security & Defense. Agenda) שנעשה בשיתוף חברת אבטחת המידע מקא׳פי (McAfee) שהתפרסם בפברואר 2012: Cyber-security: The vexed question of global rules. An Independent report on cyber-preparedness around the world. With the support of *McAfee*. SDA, Belgium. בדו״ח זה קיבלה ארצות־הברית ציון של ארבעה כוכבים. http://www.mcafee.com/hk/resources/reports/rp-sda-cyber-security.pdf
ראו גם: אהוד קינן, ״דו״ח: ישראל מוכנה יותר מארה״ב למתקפה מקוונת״. YNET, 31 בינואר, 2012. http://www.ynet.co.il/articles/0,7340,L-4183126,00.html

3 נייר מטה לדיון הוועדה העליונה למדע וטכנולוגיה בנושא: **המיזם הקיברנטי הלאומי.** הצעה להקמת תוכנית לאומית לבניית יכולות קיברנטיות בשילוב היבטי מו״פ, כלכלה, אקדמיה, תעשייה וצורכי הביטחון הלאומי. תל אביב, נובמבר 2012, עמ׳ 18.

4 שמואל אבן ודוד סימן טוב, **לוחמה במרחב הקיברנטי: מושגים, מגמות ומשמעויות לישראל**, המכון למחקרי ביטחון לאומי, מזכר 109, (תל אביב: המכון למחקרי ביטחון לאומי, 2011).

5 זאב שיף, ״דו״ח ועדת מרידור: חשש שמדינות מזרח־תיכוניות יצטיידו בגרעין בעקבות איראן״, **הארץ**, 24 באפריל, 2006. http://www.haaretz.co.il/misc/1.1100503

6 שי שבתאי, ״תפיסת הביטחון של ישראל – עדכון מונחי יסוד״, **עדכן אסטרטגי**, כרך 13, גיליון 2, (אוגוסט 2010), עמ׳ 8–10.

7 אמיר בוחבוט, ״משנים את תפיסת הביטחון״, **NRG מעריב**, 24 באפריל, 2006. http:// www.nrg.co.il/online/1/ART1/076/915.html

8 ההצעה לא אושרה באופן רשמי בממשלה, בשל חילוקי דעות בין קברניטים. עם זאת, מרכיב ההגנה הפך לחלק מתפיסת הביטחון של ישראל באופן בלתי־רשמי.

9 ״תפיסת הביטחון של ישראל – עדכון מונחי יסוד״. עמ׳ 8–10.

10 רמי אפרתי וליאור יפה, ״כך בונים הגנה קיברנטית לאומית״, **Israel Defense**, 11 באוגוסט, 2012. http://www.israeldefense.co.il/?CategoryID=512&ArticleID=2960

11 יצחק בן ישראל . ״לקחים טכנולוגיים״, **מערכות**, גיליון מספר 332, (1993). עמ׳ 13.

12 עמוס ידלין, ״הממד החדש של הלחימה – סייבר״. **מבט מל״מ**, (ינואר 2010). עמ׳ 4. http://www.intelligence.org.il/KotarPort.aspx#http://malam.barebone.kotar.co.il/KotarApp/Viewer.aspx?nBookID=94837032&sSelectedTab=tdBookInfo%231.undefined.3.fitwidth

13 סוכנות הידיעות "רויטרס", "סטוקסנט שפגע באיראן – רק אחד מ־5 וירוסים", YNET, 29 בנובמבר, 2011. http://www.ynet.co.il/articles/0,7340,L-4168852,00.html

14 "כך בונים הגנה קיברנטית לאומית".

15 ליאור טבנסקי, "הגנה על תשתיות קריטיות מפני איום קיברנטי", **צבא ואסטרטגיה**, כרך 3, גיליון 2, (נובמבר 2011). , ע' 72.
החלטות לדוגמה: החלטת ממשלה 1886 בק/9 מ־20 במרס 1997: הקמת ועדת היגוי לנושאי מחשוב בכל משרד ממשלתי; החלטת ממשלה 3582 בק/77 מ־16 במרס 1998: אחריות לנושא אבטחת מידע במשרדי הממשלה; החוק להסדרת הביטחון בגופים הציבוריים 1998.

16 לפירוט נוסף על תהיל"ה ראו פרק אחרון במאמר זה העוסק בנושא בניין הכוח.

17 "כך בונים הגנה קיברנטית לאומית".

18 "הגנה על מערכות משובצות מחשב".
http://www.nsc.gov.il/NSCWeb/Templates/CounterTerrorismActivities.aspx.

19 "הגנה על תשתיות קריטיות מפני איום קיברנטי", עמ' 72–73.

20 בנובמבר 2010 הנחה ראש הממשלה על הקמת צוות מיוחד, שיעסוק בגיבוש תוכנית לאומית להצבת ישראל בין חמש המדינות המובילות בתחום הקיברנטי. העבודה בנושא, שכונתה "המיזם הקיברנטי הלאומי", הובלה על ידי הוועדה העליונה למדע וטכנולוגיה, בראשות פרופ' בן ישראל. הצוות כלל נציגים מהגופים המרכזיים העוסקים בתחום הקיברנטי בישראל והורכב ממספר תת־צוותים שבחנו את המרכיבים החיוניים להתמודדותה של ישראל עם האיום הקיברנטי, וניתחו את התועלות הלאומיות בהיבטי הכלכלה, האקדמיה והביטחון הלאומי.

21 "המיזם הקיברנטי הלאומי", בתוך: **המועצה הלאומית למחקר ולפיתוח, דו"ח לשנים 2010–2011.** עמ' 10–17.
http://knesset.gov.il/committees/heb/material/data/mada2012-10-15.pdf

22 ההחלטה התקבלה בעקבות עבודת מטה מקיפה שבוצעה על ידי צוות לאומי בראשות יו"ר המועצה הלאומית למחקר ופיתוח , פרופסור יצחק בן ישראל.

23 "קידום היכולת הלאומית במרחב הקיברנטי". החלטת ממשלה מספר 3611 מיום 7 באוגוסט 2011.
http://www.pmo.gov.il/Secretary/GovDecisions/2011/Pages/des3611.aspx

24 "כך בונים הגנה קיברנטית לאומית".

25 יהודה קונפורטס, "דרושה: "כיפת ברזל" לסייבר שתגן על העורף", **אנשים ומחשבים,** 1 בפברואר 2012. http://www.pc.co.il/?p=79406

26 יוסי הטוני, "ד"ר אביתר מתניה: המרחב הקיברנטי מחייב התייחסות עסקית ולאומית־מדינתית; המסע לא קל", מתוך כנס CyberSec שהתקיים בפברואר 2012. **אנשים ומחשבים**, 12 בפברואר 2012. http://www.pc.co.il/?p=80025

27 שם.

28 דברי ד"ר אביתר מתניה, **כנס הסייבר הבינלאומי השני**, אוניברסיטת תל אביב, ב־9 ביוני 2012.

29 "כך בונים הגנה קיברנטית לאומית".

30 פרט לפרסום החלטת הממשלה על אודות הקמת המטה הקיברנטי הלאומי.

31 "מדיניות מו"פ לאומית כמערכת כלים שלובים", מסמך מסכם. מדברי פרופ' יצחק בן ישראל, כנס הרצלייה השנתי 2011. http://www.herzliyaconference.org/_Uploads/dbsAttachedFiles/OriSlonim2.pdf

32 "קול קורא למלגות בתחום: הגנת הסייבר ומחשוב מתקדם".
http://exactsci-info.tau.ac.il/exact_sciences/site/temp/cybersco.pdf

33 **תקציב המדינה – הצעה לשנות הכספים, 2011–2012 עיקרי התקציב ותוכנית תקציב רב־שנתית**. ירושלים, 2010. http://www.mof.gov.il/BudgetSite/StateBudget/Budget2011_2012/Lists/20112012/Attachments/1/Budget2011_2012.pdf

34 נייר מטה לדיון הוועדה העליונה למדע וטכנולוגיה בנושא: **המיזם הקיברנטי הלאומי.** הצעה להקמת תוכנית לאומית לבניית יכולות קיברנטיות בשילוב היבטי מו"פ, כלכלה, אקדמיה, תעשייה וצורכי הביטחון הלאומי. תל אביב, נובמבר 2012. ע' 20

35 "קידום היכולת הלאומית במרחב הקיברנטי", החלטת ממשלה מספר 3611, מיום 7 באוגוסט 2011. http://www.pm.gov.il/PMO/Secretarial/Decisions/2011/08/des3611.htm

36 מתוך ראיון עם פרופ' יצחק בן ישראל בנושא המיזם הקיברנטי. התקיים בתאריך 5 באוגוסט 2012, באוניברסיטת תל אביב.

37 מתוך ראיון עם רס"ן טל, ראש תחום בכיר במטה הקיברנטי. התקיים בתאריך 23 באוגוסט 2012, במטה הקיברנטי, רמת אביב. תוכנית התקצוב המוזכרת טרם פורסמה בפומבי.

38 שם.

39 **שינויים בתקציב לשנת 2012,** פרוטוקול מס' 1069, ישיבת ועדת הכספים. יום שני, א' באייר התשע"ב (1 במאי 2012), שעה 12:30. www.knesset.gov.il/protocols/data/rtf/ksafim/2012-05-01-02.rtf

40 "התקציב ותוכניות העבודה של מטה הסייבר הלאומי אושרו על ידי ראש הממשלה נתניהו". 6 ביוני 2012. http://www.pmo.gov.il/MediaCenter/Spokesman/Pages/spokecyber060612.aspx

41 ב־13 נובמבר 2012 הודיע ראש מטה הסייבר הלאומי על השקת תוכנית קידמ"ה – קידום מו"פ הגנת הסייבר. התוכנית היא פרי שיתוף פעולה בין המטה לבין המדען הראשי במשרד התמ"ת, שמטרתו לקדם את המו"פ והיזמות בתחום ה־Cyber-Security במטרה לשמר את הפוטנציאל התחרותי של התעשייה הישראלית בתחום זה בשוק העולמי, ואף להעצימו.

42 חוזר המדען הראשי: "תוכנית קידמ"ה (קידום מו"פ הגנת הסייבר) לקידום יכולות התעשייה הישראלית בתחום הגנת הסייבר". 21 בנובמבר 2012. http://www.moital.gov.il/NR/rdonlyres/89646959-5455-4A5A-99FD-C4B07D07E8E5/0/syber122012_3.pdf
ראו גם: "שמונים מליון ש"ח לקידום הסייבר", **IsraelDefenseTech**, 30 בדצמבר 2012, http://www.israeldefense.co.il/?CategoryID=760&ArticleID=3796

43 שמואל אבן ועמוס גרנית, "**קהילת המודיעין הישראלית – לאן? ניתוח, מגמות והמלצות**". מזכר מספר 97, תל אביב: המכון למחקרי ביטחון לאומי. מרס 2009. עמ' 64.

44 "יצחק בן ישראל, "לקחים טכנולוגיים", **מערכות,** גיליון מספר 332, (1993). עמ' 10.

45 כפי שפורט בהרחבה בפרק העוסק בקביעת האסטרטגיה.

46 מתוך ראיון עם רס"ן טל, ראש תחום בכיר במטה הקיברנטי. התקיים בתאריך 23 באוגוסט 2012 במטה הקיברנטי, רמת אביב.

47 מתוך דברי ראש הממשלה, מר בנימין נתניהו, **כנס הסייבר הבינלאומי הראשון**, אוניברסיטת תל אביב, 9 ביוני 2011.

48 עמיר רפפורט, "מתקפת סייבר על תשתיות לאומיות". **Israel Defense**, 8 בדצמבר 2011. http://www.israeldefense.co.il/?CategoryID=536&ArticleID=1421

49 עמיר רפפורט, "להגיב מהר כדי להיות רלוונטי", **Israel Defense**, 3 באפריל 2012, http://www.israeldefense.co.il/?CategoryID=512&ArticleID=2153

50 אמיר אורן, "זירת הלחימה החדשה של צה"ל נמצאת ברשתות המחשבים", **הארץ,** 1

בינואר 2010. http://www.haaretz.co.il/misc/1.1182490

51 "מקצועות המחשב מסלול מגן בסייבר", אתר חיל הקשר והתקשוב. http://www.tikshuv.idf.il/site/General.aspx?catId=60698&docId=76101

52 הדס דובדבני, "הסתיים קורס הסייבר הראשון בצה"ל. המטרה: שלושה מחזורים בשנה". אתר צה"ל. 3 במאי 2012. http://www.mako.co.il/pzm-soldiers/Article-595ec4bc4611731006.htm&sCh=3d385dd2dd5d4110&pid=1093150966

53 "חשיפה: מנהלת סייבר חדשה", **Israel Defense**, 12 בינואר 2012. http://www.israeldefense.co.il/?CategoryID=512&ArticleID=1657 – לא נמצאו פרסומים נוספים לגבי המִנהלת במשרד הביטחון, סביר להניח שמטעמי סיווג. ראו גם: "מתקפת סייבר על תשתיות לאומיות".

54 עמיר רפפורט, "חשיפה: תרגיל הגנת סייבר לאומי", **Israel Defense**, 19 בינואר, 2012. http://www.israeldefense.co.il/?CategoryID=512&ArticleID=1706

55 מתוך ראיון עם עו"ד יורם הכהן, ראש הרשות למשפט ולטכנולוגיה דאז, התקיים ב־5 בספטמבר 2012 בקריית הממשלה, תל אביב.

56 אתר הרשות למשפט, טכנולוגיה ומידע (רמו"ט) http://www.justice.gov.il/MOJHeb/ILITA/

57 הודעה לעיתונות בשם הרשות למשפט טכנולוגיה ומידע, משרד המשפטים, לשכת הדובר. http://www.justice.gov.il/NR/rdonlyres/4C39E414-E501-48C2-9C53-8EB533FD8B7D/32913/dover5.pdf

58 "אודות מערך ממשל זמין", http://e.gov.il/AboutUs/Pages/AboutUs.aspx

59 יוסי הטוני, "אל"מ (מיל') ד"ר גבי סיבוני: "יש שכבה שלמה של ארגונים שלא מוגנים מפני מתקפות סייבר", מתוך: כנס CyberSec 2012 המכון למחקרי ביטחון לאומי, ב־12 בפברואר 2012. **אנשים ומחשבים**, 15 בפברואר 2012. http://www.pc.co.il/?p=80466

60 אירועי ה־"סטקסנט", ה־"פליים" ונוספים, אשר על פי פרסומים זרים בוצעו על ידי ישראל.

61 "מתקפת סייבר על מתקני תשתית לאומית".