ההיערכות למלחמה קיברנטית

כיום ניתן לפגוע בתשתיות צבאיות ואזרחיות באמצעות מחשבים הנמצאים אלפי קילומטרים מהיעדים המותקפים. ההתפתחות הזאת מחוללת שינויים מרחיקי לכת בבניין הכוח של הצבאות המודרניים

הלוחמה הקיברנטית של היום כבר אינה מוגבלת רק לתחום המידע ולוחמת המידע, ועניינה המרכזי הוא לוחמה פיזית והסבת נזק פיזי באמצעות שימוש ביכולות קיברנטיות

גיל ברעם
חוקרת בסדנת יובל נאמן למדע, לטכנולוגיה ולביטחון שבאוניברסיטת תל־אביב

מבוא

כניסתן של טכנולוגיות הלוחמה הקיברנטיות לשדה הקרב המודרני הובילה להרחבת מושג המלחמה כפי שהיה מוכר עד היום. אמצעי לחימה חדשים, שלא היו קיימים קודם לכן, נכנסו לשדה הקרב והביאו לשינוי במאפייני המלחמה ובמשמעותה.

בשנים האחרונות התרחש מעבר מלוחמת מידע ללוחמה קיברנטית, בלי שהושם דגש במידה מספקת על סוגיית המעבר ועל השינוי שהתרחש. תופעה כזאת מאפיינת רעיונות חדשים בראשית התפתחותם, כשמשמעויותיהם המלאות אינן ברורות עדיין. במאמר מוצגת סקירה תמציתית של תהליך המעבר מלוחמת מידע ללוחמה קיברנטית, ומתוארים ניסיונותיהם של הממשל האמריקני ושל הממשל בישראל להתמודד עם האיום שנשקף. בסוף המאמר נידון הקושי הרב לגלות מי עומד מאחורי מתקפות קיברנטיות.

המעבר מלוחמת מידע ללוחמה קיברנטית

כדי לעמוד על המשמעות של הרחבת מושג המלחמה יש להזכיר את ההבדלים בין שני המונחים "לוחמת מידע" ו"לוחמה קיברנטית". אלווין טופלר דיבר על חשיבותו של המידע בלחימה ועל היכולת לשלוט במידע ולנצלו לצרכים שונים.[1] בראשית הדרך, קרי בשנות ה־90 של המאה הקודמת, נוצר בלבול מסוים בין לוחמה פסיכולוגית לבין לוחמת מידע, ועיקר העיסוק בנושא התבטא בתדרוך אנשי צבא בנוגע להתנהלותם מול התקשורת, שכן ההנחה הייתה שכניסת כלי התקשורת לשדה הקרב משנה את פני המערכה. בהמשך התפתחה ההבנה בנוגע לחשיבות הרשתות החברתיות, והן גויסו כדי להשפיע על תודעת ההמונים. ההנחה הרווחת הייתה שלוחמה קיברנטית היא לוחמת מידע.

אולם מאז שכתבו בני הזוג טופלר את ספרם "מלחמה ואנטי מלחמה" התקדם העיסוק במידע על היבטיו השונים. ההתקדמות הרבה שחלה ביכולות הטכנולוגיות בתחום המחשוב הובילה להיווצרותו של המרחב הקיברנטי. אנשי הצבא ואנשי האקדמיה התייחסו לטכנולוגיה הקיברנטית כאל מרחב לחימה חדש בעל מאפיינים משלו וכללי פעולה שייחודיים לו. בשל העיסוק הרב בנושא המידע הגיעה רק בשלב מאוחר יותר ההבנה שהטכנולוגיה הקיברנטית משולבת למעשה בכל אחד מתחומי הלחימה המוכרים והיא כמעט שאינה עומדת בפני עצמה, לא כל שכן שהיא אינה מרחב לחימה חדש. במקביל התפתחה גם ההבנה כי שימוש במחשבים יכול לגרום לנזק פיזי ממשי.

> כיום מאפשרת טכנולוגיית הלוחמה הקיברנטית לבצע מגוון רחב של פעולות החורגות מתחום העיסוק במידע ומתמקדות בתחום ההגנה, ההתקפה וגם איסוף המודיעין

הלוחמה הקיברנטית של היום כבר אינה מוגבלת רק לתחום המידע ולוחמת המידע, ועניינה המרכזי הוא לוחמה פיזית והסבת נזק פיזי באמצעות שימוש ביכולות קיברנטיות. אפשר לתאר את השינויים שהתחוללו בלוחמה הקיברנטית באמצעות תרשים זרימה (איור 1). כיום מאפשרת טכנולוגיית הלוחמה הקיברנטית לבצע מגוון רחב של פעולות החורגות מתחום העיסוק במידע ומתמקדות בתחום ההגנה, ההתקפה וגם איסוף המודיעין. ההכרה בכך שהמחשב הוא נקודת תורפה הובילה ליצירתן של מערכות לוחמה קיברנטית המאפשרות לפגוע בנכסי המידע של הצד האחר וכן לגרום לפגיעות פיזיות חמורות. כל זאת בלי שיהיה צורך להפעיל לשם כך כלי נשק קונוונציונליים או לא־קונוונציונליים.

> מדינה יכולה לגרום נזק פיזי למדינה אחרת באמצעות כלים קיברנטיים, אך יהיה קשה מאוד להוכיח שהיא עמדה מאחורי האירוע

ההתפתחות בטכנולוגיית הלוחמה הקיברנטית הובילה להרחבה ניכרת של יכולותיהן המודיעיניות והצבאיות של מדינות. דוגמה בולטת לכך היא אירוע ה"סטוקסנט" (Stuxnet) שפגע בפעילותן התקינה של הצנטריפוגות באיראן ויצר מצב שבו הצנטריפוגות נפגעו פגיעה פיזית באמצעות שימוש בכלים קיברנטיים. דוגמה נוספת היא פרשת "פלֵיים" (Flame): בסוף מאי 2012 האשימה איראן את ישראל בהפעלת קוד עוין חדש - שהכינוי שלו היה "פליים" - במערכות המחשב שלה. גורמי מחקר וחברות אבטחה שבדקו את הנושא, ובהם גוף התקשורת של האו"ם וגוף אבטחה מרכזי באיראן, אמרו כי מדובר בתוכנה מהמתוחכמות שבהן נתקלו אי פעם וכי מהנתונים שבידיהם נראה כי מדובר בווירוס שיצרה מדינה בעלת ידע רב בתחום הלוחמה הקיברנטית.[3]

אירועים כאלה מעידים על עלייה ברורה ביכולות הלחימה של מדינות בתחום הלוחמה הקיברנטית: פותחו יכולות טכנולוגיות שמאפשרות לאסוף מידע מרחוק ולגרום נזק פיזי באמצעות פגיעה במערכות מחשב.

חשיבות הנושא מתחדדת במיוחד לאור היעדרם של כללי פעולה ברורים בתחום הלוחמה הקיברנטית ולאור העובדה שלרוב לא ניתן לדעת מאיזו טריטוריה נעשתה התקיפה.[4] במילים אחרות: מדינה יכולה לגרום נזק פיזי למדינה אחרת באמצעות כלים קיברנטיים, אך יהיה קשה מאוד להוכיח שהיא עמדה מאחורי האירוע. בהקשר הזה יש לציין שמדינות כמעט שאינן מפרסמות את יכולותיהן בתחום הלחימה הקיברנטית, ומעט המידע שקיים מבוסס על פרסומים בתקשורת.

נראה שמקבלי ההחלטות עדיין לא הפנימו כראוי את העוצמה הגלומה בלוחמה קיברנטית. ניתן ללמוד על כך ברגע שבוחנים מיהם הגורמים המופקדים על התחום הזה. בניין הכוח בתחום הקיברנטי שייך באופן מסורתי למודיעין. בארה"ב קיבלה הסוכנות לביטחון לאומי (NSA) את האחריות לפיקוד הסייבר, ובישראל אגף המודיעין הוא האחראי העיקרי לטיפול בתחום. תפקידם של גופי המודיעין הוא לאסוף מידע, ומשום שהתפיסה המקובלת היא שהעיסוק בתחום הקיברנטי קשור בעיקר למידע, קיבלו גופי המודיעין את האחריות לתחום החדש הזה.

בשנים האחרונות, לאחר שהחלה לחלחל אט־אט ההכרה ביכולות הגלומות באמצעי הלוחמה הקיברנטית, החלו עוד ועוד גופים ביטחוניים לעסוק בתחום הזה.

יתר על כן, הטיפול באיום הנשקף מהלוחמה הקיברנטית הולך ותופס מקום יותר ויותר חשוב בסדר היום של ארה"ב ושל ישראל והוא משפיע ישירות על הקצאות התקציבים ועל הכנסת שינויים בבניין הכוח של הצבאות. עם זאת, משמעותם הכוללת של השינויים האלה והשלכותיהם טרם הובנו לעומק.

התמודדות הממשל האמריקני עם האיום הקיברנטי

טכנולוגיית הלוחמה הקיברנטית מאפשרת לצבא ארה"ב למלא רבות ממשימותיו באמצעות "שלט רחוק": לתקוף יעדים מרוחקים, להשיג מודיעין בזמן אמת וכן לנהל מבצעים ומרכזי פיקוד ושליטה ברחבי העולם. עשיית הפעולות האלה נשענת על מערכות התקשורת הגלובליות של הצבא הכוללות כ־15 אלף רשתות וכ־7 מיליון מכשירים ממוחשבים הפרוסים במאות אזורים בעולם.[5] עם זאת, רמה גבוהה כל כך של מחשוב גם חשופה להתקפות־נגד: בעשור האחרון גברה תדירות הניסיונות לחדור למחשבים של ארה"ב ושל בעלות בריתה.

כדי להשיג יתרון על פני אויביה חייבת ארה"ב להיות המובילה בתחום הפיתוח הטכנולוגי וההגנה על רשתותיה. לשם כך יש צורך בהשקעות גדולות ובעיצוב הכוח הצבאי בהתאם למדיניות ההשקעות החדשה. ארה"ב אכן משקיעה משאבים רבים בתחום הזה ונחשבת למובילה בעולם בתחום היכולות הקיברנטיות: בדו"ח שבחן את מידת מוכנותן של 23 מדינות בתחום הקיברנטי קיבלה ארה"ב ציון גבוה מאוד: ארבעה כוכבים מתוך חמישה.[6]

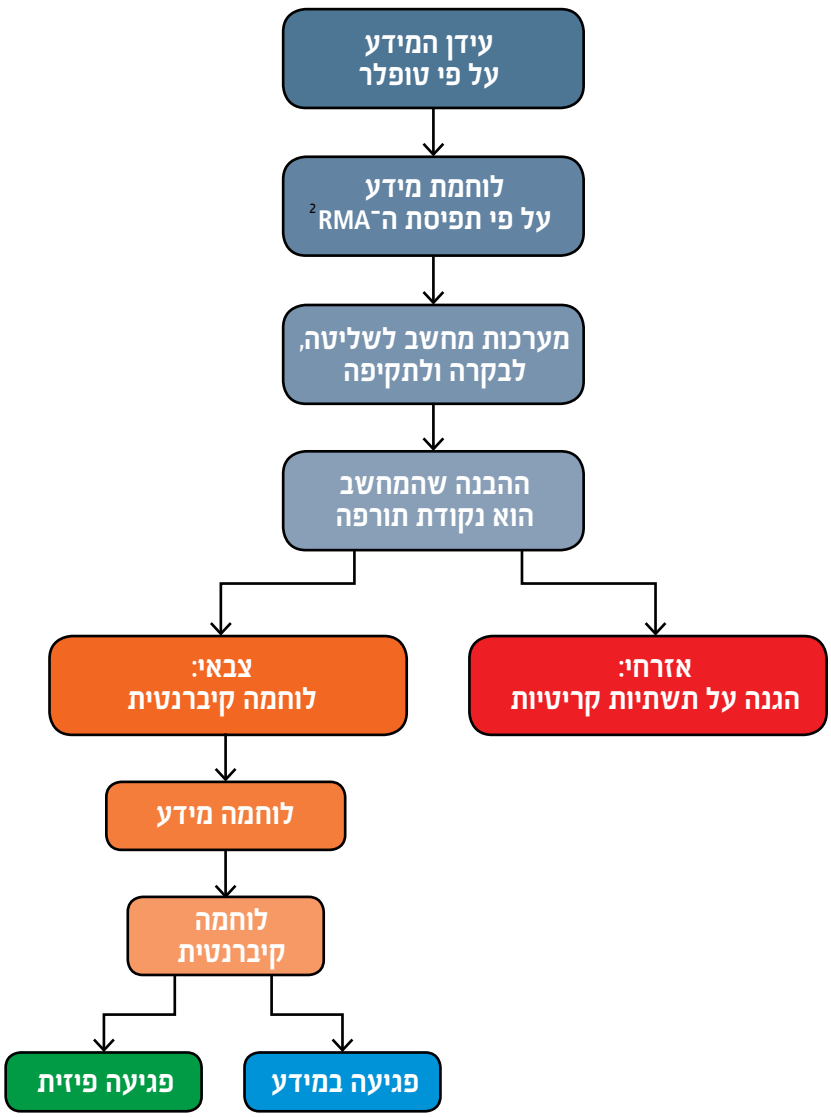
ארה"ב פעילה בתחום הקיברנטי בכמה מישורים, שהחשובים שבהם הם: פרסום מסמכי מדיניות ברורים, הקצאות תקציביות ושינויים בבניין הכוח.

בעשור האחרון פירסם הממשל האמריקני מסמכים רשמיים שפירטו את מדיניותו הסדורה בנוגע לדרכי ההתמודדות עם האיום הקיברנטי. כבר בנובמבר 2002 חתם הנשיא ג'ורג' בוש הבן על מסמך פעולה[7] שהנחה את גופי הממשל לפתח - לראשונה - כללים ברמה הלאומית שיקבעו מתי ובאילו תנאים תוכל ארה"ב לבצע תקיפות קיברנטיות משטחה.[8] בפברואר 2003 פירסם הבית הלבן מסמך בשם "האסטרטגיה הלאומית לביטחון המרחב הקיברנטי" שבו נקבע כי הביטחון הקיברנטי הוא נושא המצוי באחריותו של המשרד לביטחון המולדת. מטרת המסמך הייתה "ליצור את מסגרת הפעולה להגנה על התשתיות החיוניות לכלכלה, לביטחון ולדרך החיים האמריקנית". המסמך כולל מגוון רחב של פעולות שנועדו להגן על ביטחונה הלאומי של ארה"ב באמצעות הגנה על תשתיותיה הקריטיות.[9]

במאי 2011 פירסם הבית הלבן את המסמך "האסטרטגיה הבין־לאומית למרחב הקיברנטי"[10] שהניח את היסודות לדרכי פעולה ברורות להתמודדות עם האיום הקיברנטי. בין היתר כלל המסמך הנחיות להכנסת שינויים בכל משרדי הממשל כדי להתאים את דרכי הפעולה של רשויות הממשל השונות לאופיו של האיום הקיברנטי.[11]

ביוני 2011 הכריז הממשל על גיבוש קווים מנחים (Cyberwar Guidelines) המגדירים את "ההתנהלות של ארה"ב במהלך מלחמת סייבר עתידית". המסמך מגדיר את הרשאותיהם של מפקדי כוחות הסייבר לביצוע פעולות קיברנטיות מורכבות העלולות להקשות על ארה"ב מהבחינה הדיפלומטית, כמו הדבקת מחשבי האויב בקוד עוין וביצוע פעולות שונות

התפתחות הלוחמה הקיברנטית



שיגרמו להפלת רשת החשמל של הירי.[12]
בשעת הצורך יהיו הכוחות האמריקניים רשאים לחסום תקיפות קיברנטיות שיבוצעו נגדם, בין היתר באמצעות נטרול השרתים המרכזיים של המדינה התוקפת. כמו כן יהיו הכוחות רשאים לתקוף מחשבים צבאיים של מדינות שיתקפו את ארה"ב. לחלופין שומרת לעצמה ארה"ב את הזכות להגיב תגובה קונוונציונלית נרחבת יותר על תקיפות קיברנטיות שיבוצעו נגדה.
בפברואר 2013 חתם הנשיא אובמה על צו נשיאותי (Presidential Policy Directive 20) שמטרתו להביא לשיפור ההגנה על התשתיות החיוניות של המדינה מפני התקפות קיברנטיות. הצו מאפשר לנשיא ליישם תהליכים ואף לכפות תקנות כדי לבסס את האבטחה המקוונת על אתרי הסוכנויות הפדרליות בארה"ב.[13]
במקביל לפרסום מסמכי המדיניות הוקצו תקציבים ניכרים לבניית מערכי התמודדות בכל גופי הביטחון המרכזיים - במשרד ההגנה, בכל אחת מזרועות הצבא, בסוכנות לביטחון לאומי, במשרד לביטחון פנים - וכן במשרד המשפטים.
בשני העשורים האחרונים היו מתכנני המדיניות האמריקנית עדים להתרחשותה של "המהפכה בעניינים צבאיים". המהפכה הזאת השפיעה רבות על מבנה הצבא ועל עיצוב דרכי פעולתו.[14]
ארה"ב השקיעה סכומים גדולים במחקר ובפיתוח בתחום הטכנולוגיה הקיברנטית, בהתאם לאסטרטגיות הממשלתיות שגובשו בנושא. התוספות התקציביות שניתנו לתחום הזה הובילו לשינויים רבים בבניין הכוח: החל מתקציב 2010 הוקצו סכומים ייעודיים להקמתו של פיקוד הסייבר האמריקני, והוקצו תקציבים להקמתם של מטות סייבר ייעודיים בזרועות הצבא השונות. תפקיד המטות האלה הוא להתמודד עם האיום הקיברנטי.
בדצמבר 2009 מונה מתאם לנושא הקיברנטי המשמש יועץ לנשיא. תפקידו העיקרי של המתאם הוא להוביל מהלכי תיאום וסנכרון של מדיניות הממשל ולסייע לנשיא בניהול משברים בתחום של ביטחון המרחב הקיברנטי.[15] תחת משרד ההגנה הוקם "פיקוד הסייבר האמריקני", שלפי פרסומי המשרד הגיע למוכנות מבצעית מלאה בנובמבר 2010. הנחת העבודה שעמדה בבסיס הקמת הפיקוד היא שהאיום הקיברנטי הוא האיום העיקרי

טכנולוגיית הלוחמה הקיברנטית מאפשרת לצבא ארה"ב למלא רבות ממשימותיו באמצעות "שלט רחוק": לתקוף יעדים מרוחקים, להשיג מודיעין בזמן אמת וכן לנהל מבצעים ומרכזי פיקוד ושליטה ברחבי העולם

לפעילותן של מערכות ממשלתיות וצבאיות מסווגות ולא מסווגות החיוניות לשמירה על ביטחונה הלאומי של ארה"ב. פיקוד הסייבר "אחראי להנחיית הפעולות ברשתות המחשבים של משרד ההגנה ועל הגנת רשתות המחשבים הממשלתיות בעזרת שיתוף פעולה עם הסוכנויות הממשלתיות השונות".[16]

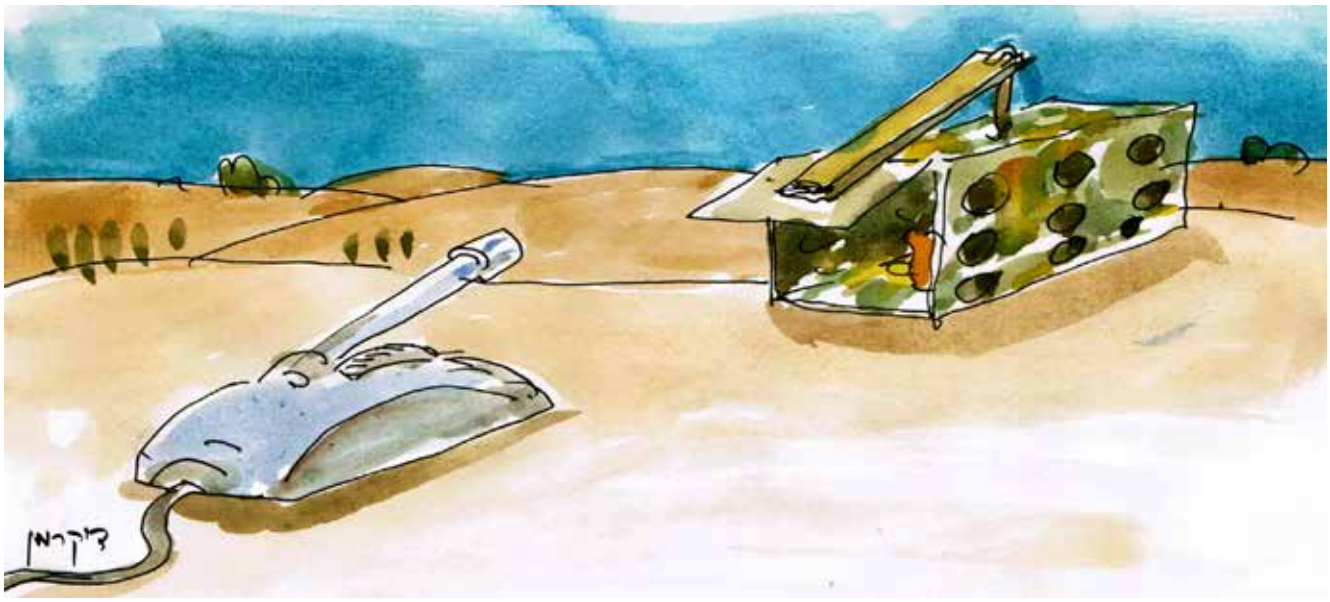
אחד ממסמכי היסוד של צבא ארה"ב, המגדיר את המבנה של צבא ארה"ב ואת מטרותיו לעשור הקרוב, קובע שהשגת עליונות בתחום של טכנולוגיות המידע היא אחת ממטרות־העל של הצבא

אחד ממסמכי היסוד של צבא ארה"ב, Joint Vision 2020, המגדיר את המבנה של צבא ארה"ב ואת מטרותיו לעשור הקרוב, קובע שהשגת עליונות בתחום של טכנולוגיות המידע היא אחת ממטרות־העל של הצבא: "מידע, עיבוד מידע ורשתות תקשורת מצויים בליבה של כל פעולה צבאית. במהלך ההיסטוריה ראו מנהיגים צבאיים בהשגת עליונות בתחום המידע את המפתח להשגת ניצחון... מהפכת המידע יוצרת שינוי איכותי וכמותי בסביבת המידע - שינוי שעד 2020 יוביל לשינויים עמוקים בביצוע מבצעים צבאיים".[17]

בשנים האחרונות החלו הפנטגון והמשרד להגנת המולדת לפעול להגנה על רשתות ממשלתיות ועל תשתיות קריטיות בשיתוף עם בעלות בריתה של ארה"ב. שיתוף הפעולה איפשר להרחיב את מעטפת ההגנה גם ברמה הבין־לאומית

במרוצת השנים חלו שינויים רבים במבנה הגופים המתמודדים עם האיום הקיברנטי, וכמעט בכל היחידות הצבאיות האמריקניות ננקטו מהלכים שונים כדי להתמודד בהצלחה עם ההתפתחויות המהירות ועם האיומים המתרבים. בצבא ארה"ב הוקמו פיקודי סייבר בזרועות השונות, ובאחריותם לשלב יכולות לוחמה קיברנטית ביכולות הלוחמה הקיימות של כל זרוע וזרוע. המהלך הזה מעיד שהיכולות הקיברנטיות חדרו עמוק לגופי הצבא השונים והפכו לחלק בלתי נפרד מפעולות הלחימה.
בזרוע האוויר והחלל הוקמה יחידה מיוחדת ללוחמה קיברנטית (24th Air Force) שהוכרזה מבצעית בראשית 2011; בזרוע היבשה החל לפעול באוקטובר 2010 פיקוד הסייבר של זרוע היבשה (Army Cyber Command/2nd Army Plans) שמטרתו להגן על כוחות היבשה של ארה"ב מפני לוחמה קיברנטית.
זרוע הים האמריקנית החלה להפעיל בשנים האחרונות יחידה ייעודית שמטרתה להקנות לחיל עליונות בתווך הקיברנטי באמצעות כוחות הסייבר של הצי (Navy Cyber Forces). בגוף הזה משרתים יותר מ־14 אלף חיילים ואזרחים הפועלים בתחומי המחשוב והטלקומוניקציה וכן אחראים למגוון רחב של פעולות ברשתות המחשבים שמיועדות להגן על רשתות הצי.[18]
בשנים האחרונות החלו הפנטגון והמשרד להגנת המולדת לפעול להגנה על רשתות ממשלתיות ועל תשתיות קריטיות בשיתוף עם בעלות בריתה של ארה"ב. שיתוף הפעולה איפשר להרחיב את מעטפת ההגנה גם ברמה הבין־לאומית.
אפשר אפוא להצביע על תהליכים אחדים שהתרחשו בעקבות ההכרה באיום הנובע מהתפתחותה של טכנולוגיית הלוחמה הקיברנטית:

1. הסטת תקציבים לתחום הביטחון הקיברנטי. משרדים רבים מציינים זאת במפורש בבקשות התקציב השנתיות.
2. הקמת גופים ייעודיים שתפקידם לאפשר לארה"ב להיערך טוב יותר וביעילות רבה יותר להתמודדות עם האיומים הקיברנטיים וכן לאפשר יכולות הגנה והתמודדות בהתאם. דוגמה לגוף כזה היא הקמתו של פיקוד הסייבר.
3. יצירת שינויים מבניים בזרועות הצבא: הקמת גופים האחראים לתחום הקיברנטי בכל זרוע - גופים שיאפשרו היערכות יעילה להתמודדות עם האיומים הקיברנטיים הנוגעים להן.



המצב בישראל

גם בישראל לא נעלמה חשיבותה של טכנולוגיית הלוחמה הקיברנטית מעיניהם של העוסקים בביטחון הלאומי. גופי הביטחון עוסקים בתחומים האלה כבר שנים רבות. מטבע הדברים, התכנים אפופים במעטה סודיות.

ישראל היא מהמדינות המובילות בעולם בפיתוח טכנולוגיות קיברנטיות, אולם נראה שהיא מצויה בפיגור מסוים בכל הנוגע לפרסום אסטרטגיה סדורה בתחום. בעשור האחרון - כפי שפורט לעיל - פורסמו בארה"ב פרסומים ממשלתיים רשמיים בתדירות גבוהה שפרסו בצורה ברורה את דרכי הפעולה של הממשל להתמודדות עם האיום הקיברנטי. בישראל, לעומת זאת, עיקר המידע מגיע מפרסומים בתקשורת ומיעוטו ממידע ממשלתי רשמי.

המסמך המרכזי בנושא הזה הוא החלטת הממשלה בנוגע ל"קידום היכולת הלאומית במרחב הקיברנטי" מ־7 באוגוסט 2011[19] - בין היתר באמצעות הקמת המטה הקיברנטי הלאומי שמטרתו "לפעול לקידום היכולת הלאומית במרחב הקיברנטי ולשיפור ההתמודדות עם האתגרים הנוכחיים והעתידיים".[20]

המדינה זיהתה את מאפייני האיום הקיברנטי, החלה להיערך לקראתו וליצור את השינויים הנדרשים. ההיערכות מתרכזת בשלושה תחומים:

1. גופי מערכת הביטחון, צה"ל והתעשיות הביטחוניות, שמוגנים היטב מפני מתקפות קיברנטיות.
2. התשתיות הלאומיות הקריטיות שמוגנות על ידי הרשות הממלכתית לאבטחת מידע.
3. המגזר האזרחי, שבו פועלות חברות אזרחיות. המערכות שלהן מוגנות פחות מאלה של מערכת הביטחון. השכבה הזאת מטופלת בחלקה על ידי הרשות למידע ולטכנולוגיה במשרד המשפטים (רמו"ט).[21]

בשל העובדה שישראל היטיבה לזהות את מאפייניו של האיום הקיברנטי, היא ערכה שינויים בבניין הכוח בהתאם. השינוי החשוב ביותר הוא הקמת המטה הקיברנטי הלאומי. כמו כן הוקמה (כבר ב־2002) הרשות הממלכתית לאבטחת מידע שאחראית להגנת התשתיות הלאומיות הקריטיות וכן הוקמה, כאמור, רמו"ט האחראית לשמירת ביטחון המידע הפרטי ברשת.

ישראל היא מהמדינות המובילות בעולם בפיתוח טכנולוגיות קיברנטיות, אולם נראה שהיא מצויה בפיגור מסוים בכל הנוגע לפרסום אסטרטגיה סדורה בתחום

בצבא חולקה האחריות לביטחון הקיברנטי בין אגף המודיעין (התקפה) לבין אגף התקשוב (הגנה): צה"ל הקים ביחידה 8200 שבאגף המודיעין את מטה הסייבר הצה"לי, ובאגף התקשוב הוקמה מחלקת "הגנה בסייבר" המופקדת על הגנת הרשת הצה"לית.[22] ההגנה על משרדי הממשלה ועל התשתיות הלאומיות הקריטיות מוטלת - על פי החוק - על השב"כ. מאמץ רב מושקע להגברת התיאום בין כל הגופים האלה. מענקים ממשלתיים בגובה מאות מיליוני שקלים מועניקים מדי שנה למחקרים בתחום הקיברנטי.[23]

השינוי ביכולות ההרתעה - בעיית הייחוס

אחת הבעיות שעימן מתקשות ארה"ב וישראל להתמודד היא סוגיית ההרתעה הקיברנטית ובעיית הייחוס (Problem of Attribution), דהיינו הקושי לזהות מי עומד מאחורי ההתקפות הקיברנטיות. כך, למשל, בארה"ב משוכנעים שמדינות כמו רוסיה, אירן וסין עומדות מאחורי תקיפות סייבר רבות נגדה, אך מתקשים להביא לכך הוכחות חד־משמעיות. הסיבה: המדינות האלה פועלות בתחום הקיברנטי באמצעות ארגוני האקרים שפועלים בחשאי כארגוני טרור בחסות הממשל. מדינות כאלה יכולות להתנער מפעולות הלוחמה הקיברנטיות ולטעון שנעשו ללא ידיעתן.[24]

מאחר שהתקפות קיברנטיות ניתן לבצע באנונימיות מוחלטת ובלי להשאיר עקבות כלשהן, נשאלת השאלה כיצד ניתן להרתיע את האויב מלהוציאן אל הפועל. סביר להניח

שאם תימצא דרך להרתיע, היא תהיה שונה מההרתעה הצבאית המוכרת לנו מהעבר.[25] לא תהיה זאת הרתעה באמצעות הצגתן של יכולות פיזיות שנראות לעין כמו מטוסים, טנקים וכלי נשק מתקדמים מסוגים שונים.

בשנים האחרונות נעשו בארה"ב ניסיונות להתאים את מושגי המלחמה המסורתיים לעולם הקיברנטי. גנרל קית' אלכסנדר, שעמד בראש פיקוד הסייבר האמריקני ומונה לאחר מכן לעמוד בראש הסוכנות לביטחון לאומי, העיד בקונגרס באפריל 2010 וציין שארה"ב טרם גיבשה דוקטרינת הרתעה לתחום הקיברנטי נוכח הקשיים לייצר הרתעה כזאת. לדבריו, "הדרך הטובה ביותר להרתיע היא באמצעות הגדלת רמת הביטחון ברשת שלנו". עם זאת, אפשר להעלות על הדעת פעולות הרתעה נוספות בתחום הקיברנטי. לדוגמה, ניתן להזהיר באופן פומבי מדינות תוקפניות, כפי שעשתה בינואר 2010 מזכירת המדינה האמריקנית דאז, הילארי קלינטון, בהזהירה את סין שתשים קץ לאלתר לתקיפות הקיברנטיות שהיא יוזמת נגד ארה"ב. שלוש שנים מאוחר יותר, במרס 2013, השמיע הנשיא אובמה אזהרה דומה.[26]

ניתן להרתיע גם באמצעות ייזום תקיפות מוגבלות כדי להמחיש יכולות קיברנטיות, גם אם ייחשפו כתוצאה מכך יכולות אמריקניות מסוימות במהלכן.[27]

בתקשורת העולמית מיוחסות לישראל ולארה"ב פעולות קיברנטיות שונות שגרמו נזקים משמעותיים למדינות יריבות. במרבית המקרים אין לפרסומים האלה אישור רשמי, אולם אי־אפשר להתעלם מההד התקשורתי הרב שיצרו. גם זוהי דרך ליצור הרתעה.[28] סביר להניח שמדינה תהסס לתקוף מדינה אחרת בסייבר, אם תדע שהיא עלולה לספוג כתוצאה מכך נזקים כבדים. אבל גם יכולת תקיפה קיברנטית אינה תחליף למערך הגנה פעיל, בעל יכולות מתקדמות ונראות לעין.

סיכום

העיסוק בתחום הלוחמה הקיברנטית מעלה כמה שאלות חשובות, ובהן: כיצד אפשר לדעת שהתרחשה תקיפה? כיצד אפשר לזהות את התוקף או את מקור התקיפה? כיצד ניתן לדעת מהי מטרת התקיפה? האם ניתן לראות בהתקפה קיברנטית הכרזת מלחמה ולהגיב

העיסוק בתחום הלוחמה הקיברנטית מעלה כמה שאלות חשובות שעליהן עוד אין תשובות חד־משמעיות. סביר להניח שאלה יינתנו בהדרגה, ככל שהעיסוק בלוחמה הקיברנטית יילך ויגדל

עליה במלחמה מ"הסוג הישן": באמצעות מטוסים, טנקים ואוניות? מתי יש להשתמש בלוחמת מחשבים נגד תקיפה קיברנטית או פיזית? כיצד מעריכים את תוצאות התקיפה? כיצד מונעים פגיעה עצמית? מהו מעמדו של לוחם במרחב הקיברנטי, האם מדובר בלוחם לכל דבר?[29] כיצד יש להתייחס לסוגיה של איסוף מידע על מדינות ידידות בתחום הקיברנטי? על השאלות האלה ועל רבות אחרות עוד אין תשובות חד־משמעיות. סביר להניח שאלה יינתנו בהדרגה, ככל שהעיסוק בלוחמה הקיברנטית יילך ויגדל.

הערות

1. אלווין והיידי טופלר, **מלחמה ואנטי מלחמה**, מעריב, אור יהודה, 1994
2. Revolution in Military Affairs - בשלהי שנות ה־80 של המאה הקודמת החל להתגבש שינוי רעיוני בולט בחשיבה הצבאית - שינוי שצבר תאוצה עם פרוץ המלחמה בעיראק ב־1991. השינוי הרעיוני הזה מכונה "המהפכה בעניינים צבאיים" ומתייחס לארבעה תחומים שבהם חל או יחול שינוי מהפכני לעומת מלחמות העבר: תקיפה מדויקת, תמרון דומיננטי, ניצול החלל ולוחמת מידע. להרחבה ראו: יצחק בן ישראל, "ביטחון, טכנולוגיה ושדה הקרב העתידי", **מרקם הביטחון**, עורך: חני גולן, מערכות, תל־אביב, 2001; דימיטרי אדמסקי, **תרבות אסטרטגית וחדשנות צבאית**, מערכות, תל־אביב, 2012
3. "Kaspersky Lab and ITU Research Reveals New Advanced Cyber Threat", **Kaspersky Lab**, May 28, 2012, http://goo.gl/UVSj0, "The Flame Cyber Espionage Attack: Five Questions We Should Ask", **Forbes**, June 4, 2012, http://goo.gl/7yv2fG, גילי כהן ועודד ירון, "שר הביטחון הודה לראשונה בפעילות סייבר התקפית של ישראל", **הארץ**, 6 ביוני, 2012, http://goo.gl/9d5Pdp
4. הניסיון העיקרי ליצירת הסדרה חוקית בתחום לוחמת הסייבר הוא "מדריך טאלין למשפט הבין־לאומי הרלוונטי ללוחמה קיברנטית" (Tallinn Manual on the International Law Applicable to Cyber Warfare, 2013) שפורסם במרס 2013. את המדריך כתבו מומחים בתחום, והוא כולל הצעה ל־95 חוקים בנושא המלחמה הקיברנטית וקביעת האחריות של המדינות.
5. William Lynn, "Defending a New Domain: The Pentagon's Cyberstrategy", **Foreign Affairs**, September 2010, http://goo.gl/Hlep
6. לפי דו"ח של צוות חשיבה בין־לאומי בנושא ביטחון - Security & Defense Agenda (ובקיצור: SDA) שהוכן בשיתוף עם חברת אבטחת המידע מקאפי (McAfee) והתפרסם בפברואר 2012 Cyber-security: The vexed question of global rules. An Independent report on cyber-preparedness around the world, http://goo.gl/0fVTw1
7. National Security Presidential Directive 16 - To Develop Guidelines for Offensive Cyber-Warfare
8. **National Security Presidential Directives** [NSPD] George W. Bush Administration, http://goo.gl/JnD9bq
9. **The National Strategy to Secure Cyberspace**, President Bush, Washington, February 2003, http://goo.gl/O1kggv
10. President Obama, The White House, **International Strategy for Cyberspace - Prosperity, Security and Openness in Networked World**, May 2011, pp. 3-5, http://goo.gl/H42MH
11. **Ibid**.
12. Lolita C. Baldor, "Pentagon gets cyberwar guidelines", **The Washington Times**, June 22, 2012, http://goo.gl/pKX4Eq
13. Glenn Greenwald, Ewen MacAskill, "Obama orders US to draw up overseas target list for cyber-attacks", **The Guardian**, June 7, 2013, http://goo.gl/gwuUpN, http://goo.gl/cJXJhA
14. Eliot A Cohen, "A Revolution in Warfare", **Foreign Affairs**, Vol. 75, No.2, March-April 1996, pp. 37-38
15. **Office of the Coordinator for Cyber Issues**, http://goo.gl/L0i1MB
16. **US Department of Defense - US Cyber Command Fact Sheet,** May 25, 2010, http://goo.gl/Fmw5ok. יש לציין שראש הסוכנות לביטחון לאומי הוא כיום גם ראש פיקוד הסייבר הצבאי, וכי הנשיא אובמה שקל להפריד בין התפקידים.
17. Joint Chiefs of Staff, **Joint Vision 2020**, Washington DC, June 2000
18. http://goo.gl/2FUM2m, http://goo.gl/2qYdx , http://goo.gl/RKtTXt
19. ההחלטה התקבלה לאחר עבודת מטה מקיפה שעשה צוות לאומי בראשות פרופסור יצחק בן ישראל.
20. "קידום היכולת הלאומית במרחב הקיברנטי", החלטת ממשלה מספר 3611 מיום 7 באוגוסט, 2011, **אתר משרד ראש הממשלה**, http://goo.gl/8Eaf71
21. גבי סיבוני, **המענה הלאומי להגנה האזרחית בסייבר: המלצות למקבלי החלטות - נייר עמדה**, אוגוסט 2013, http://goo.gl/JA8dCn
22. "מחלקת ההגנה בסייבר", **אתר חיל הקשר והתקשוב**, http://goo.gl/ZqWQW9
23. להרחבה ראו: נתי כהן, "הממד החמישי - היערכות ישראל למתקפת סייבר נרחבת", **מערכות** 452, דצמבר 2013, עמ' 10-17, http://goo.gl/wfC5hf
24. לדוגמה, בדו"ח ועדת המודיעין של הסנאט האמריקני **Worldwide Threat Assessment of the US-Intelligence Community** - ממרס 2013 מצוין שסין, איראן ורוסיה מפעילות יכולות קיברנטיות משמעותיות וכי התפיסה שלהן בנוגע ללוחמת הסייבר שונה מאוד מתפיסתה של ארה"ב, http://goo.gl/KCyRT
25. להרחבה ראו: אמיר לופוביץ', "לוחמה קיברנטית והרתעה: מגמות ואתגרים במחקר", **צבא ואסטרטגיה**, כרך 3, גיליון 3, דצמבר 2011, http://goo.gl/FeM1Jb
26. BBC News, "President Obama upbraids China over cyber attacks", 13 March 2013, http://goo.gl/U7tho
27. שמואל אבן ודוד סימן־טוב, **לוחמה במרחב הקיברנטי - משגים, מגמות ומשמעויות לישראל**, מזכר 109, המכון למחקרי ביטחון לאומי, יוני 2011, עמ' 30, http://goo.gl/Qrr4HU
28. Martin C. Libicki, **Cyber Deterrence and Cyberwar**, Project Air Force - Rand Corporation, 2009, p. XIV, http://goo.gl/kkz2tN
29. בעז זלמנוביץ, "מיהו לוחם?", **מערכות** 455, יוני 2014, עמ' 58-59, http://goo.gl/d2VSut