מבט בינתחומי על אתגרי הביטחון בעידן המידע

יצחק בן־ישראל, ליאור טבנסקי

מבוא

התפתחות האלקטרוניקה והמחשב מאז מלחמת העולם השנייה השפיעה על מגוון תחומים רחב ויצרה את "עידן המידע". מאמר זה עוסק ביחסי הגומלין בין טכנולוגיות המידע, עידן המידע והביטחון, ומתמקד בתופעות החדשניות.

חלק ניכר מהדחף לפיתוח עולם המחשוב נגזר מהיישומים הצבאיים. במקביל התפתחה גם החשיבה על השפעת השינוי הטכנולוגי על סוגיות הביטחון. אולם, עידן המידע שממשיך להתפתח במהירות, וכך תקשורת המחשבים ושיבוץ המחשב בכל תחומי החיים יצרו מרחב קיברנטי. נראה שהשינויים מאתגרים את התפיסות הקיימות ומחייבים בחינה מחדש של מושגי יסוד. המאמר נועד לתרום לדיון בסוגיות הביטחון הלאומי הנובעות מהתפתחות טכנולוגיות המידע. הצורך בדיון ציבורי מושכל ובעיצוב מדיניות החלטי מתחזק לאור העובדה כי הסיכון כבר התממש. מספיק להזכיר את האירועים שקרו באסטוניה באביב 2007, ופרשת Stuxnet.[1] במקרה הראשון, אורח החיים של המדינה נפגע בעקבות התקפה פשוטה מבחינה טכנית אך מסיבית על שירותים מבוססי אינטרנט. במקרה השני נראה שהיה שימוש בנשק קיברנטי מורכב מאוד מבחינה טכנית, שעוצב כדי לפגוע במדויק במערכת בקרת תהליך תעשייתי במתקן מאובטח להעשרת דלק גרעיני באיראן. עיצוב הנשק ושיטת הפעלתו כללו הסוואת הפעילות לאורך זמן. נראה שהפעלת הנשק הקיברנטי הזה גרמה לנזקים פיסיים מצטברים בעלי משמעויות אסטרטגיות. בשני המקרים יש הסכמה רחבה שמדינות עמדו מאחורי ההתקפות הקיברנטיות; ובשני המקרים אין ראיות חד־משמעיות.

פרופ' יצחק בן ישראל עומד בראש סדנת יובל נאמן למדע, טכנולוגיה וביטחון, אוניברסיטת תל אביב
ליאור טבנסקי הוא חוקר בתכנית לחקר לוחמה קיברנטית, הנתמכת על ידי קרן ג'וזף וג'נט ניובאוואר, פילדלפיה, ארצות הברית

הבנת הבסיס העיוני של עידן המידע חיונית לליבון סוגיית הביטחון הקיברנטי. במאמר נשתמש בהגותם של הפילוסוף קרל פופר, הסוציולוגים העתידנים אלווין והיידי טופלר, והכלכלן פול רומר לביאור המאפיינים של עידן המידע, ולבירור סוגיות ביחסי הגומלין בין ההתפתחות הטכנולוגית לביטחון הלאומי. בהמשך ננתח את מאפייני המרחב הקיברנטי של היום, ונדון במשמעויות לענייני הביטחון הלאומי. בחלק השלישי נסקור את התחום המוכר כ"לוחמת מידע" ונתמקד בתופעה החדשנית: לוחמת המחשבים במרחב הקיברנטי. בהמשך המאמר נסקור את כלי הנשק הקיברנטיים ושיטות הלחימה, נדון בהגנה, בהתקפה, ובהרתעה. נציג סוגיות מרכזיות העולות בתחום הביטחון הקיברנטי. נראה שעל מנת לשמור על הביטחון והשלום, נדרשת בחינה רב־תחומית של הסוגיות והאתגרים החדשים.

הקדמה עיונית

השינוי הטכנולוגי מעסיק הוגים רבים שמתחבטים בהבנתו ובבחינת ההשפעות החברתיות שלו. נזכיר שלושה הוגים הרלוונטיים להבנת המציאות המשתנה, אולם מפאת מסגרת הפרסום לא נוכל להרחיב את הדיון בנושא.

המונח הגל השלישי לקוח מבית מדרשם של זוג הסופרים שחיבוריהם הם רבי־מכר, אלווין והיידי טופלר מתאר תקופה. לטענתם, אנו נמצאים בעיצומו של המעבר לגל השלישי, אשר בו מבוססת הכלכלה על ידע ושליטה במידע,[2] במקום על ייצור תעשייתי המוני.

טבלה 1: שלושת הגלים – לפי טופלר

	משאב עיקרי	מיהו עשיר?	סמל	כלי מלחמה	דרך המלחמה
הגל הראשון	חקלאות מאורגנת	בעל אדמות	מגל	חרב	קרב פנים אל פנים בטווח אפס; כיבוש (אדמה)
הגל השני מאמצע המאה ה־17 עד סוף המאה ה־20	תעשיה ממוכנת, ייצור המוני	תעשיין	מכונות של קווי יצור המוני	טנק, מטוס	קרב באמצעות מכונות, מטווח בינוני־רחוק; דיוק נמוך; ניסיון לפגוע בכושר הייצור
הגל השלישי מסוף המאה ה־20 ואילך	ידע	ביל גייטס	מחשב	לוחמת מחשב Cyber Warfare	ניסיון לפגוע במידע באמצעים ממוחשבים. פגיעה מרחוק בכושר התפקוד, מבלי להגיע פיסית אל היעד

גם צורת המלחמה משתנה. שם המשחק יהיה השגת מידע על האויב ומניעת מידע על עצמך. מי שישלוט בטכנולוגיות המידע ינצח במלחמה, גם אם יעמדו מולו כלים רבים שייפלטו מקווי הייצור של הגל השני.

שלושת העולמות של פופר

בנוסף לשימוש בתזה של הזוג טופלר, נעזר בכמה מושגים מבית היוצר של הפילוסוף **קרל פופר** אשר הלך לעולמו ב־1994. פופר בחן את עולם הידע כמושג הקיים נוסף על עולם החומר ועולם הרוח.[3] לטענתו, קיים "עולם" שלם של ידע אנושי (פופר מכנה אותו עולם־3) המאוכלס ב"יצורים" שהם תוכן אובייקטיבי של מחשבה, כמו משפט פיתגורס וחוקי הפיסיקה, שאינם "חומר" ואינם "חוויות מנטליות" סובייקטיביות. מרגע שנוצר משפט פיתגורס הוא אמת אובייקטיבית, שאינה תלויה עוד ברוח שיצרה (או גילתה) אותו. הידע הוא אובייקטיבי אף שהוא תוצר של הרוח האנושית (הסובייקטיבית).

טבלה 2: שלושת העולמות של פופר והמרחב הקיברנטי – מאפיינים עיקריים

	תכולה	מעמד	דוגמאות	דוגמה במרחב הקיברנטי
עולם – 1	חומר	אובייקטיבי	שולחנות, מטוסים	חומרה
עולם – 2	חוויות מנטליות	סובייקטיבי	כאב, שמחה	תצוגות (חוויית משתמש)
עולם – 3	ידע	אובייקטיבי	מתמטיקה, פיסיקה	תוכנה

כלכלת עידן המידע

שלא כמו בחומר, אפשר להשתמש בידע שוב ושוב, ולחלק אותו לצרכנים רבים בלי שהוא יתמעט. הידע הוא "סחורה" בלתי־נדלית. הכלכלן פול מ' רומר, ממובילי המחקר בתורת הצמיחה החדשה, דן בהשלכות הכלכליות של ידע, ובמאמרו בו הוא מניח יסודות לכלכלה "אחרת", מבוססת ידע.[4] מתברר שהכלכלה, הבסיס לעוצמה ולשגשוג, צומחת לא רק כתוצאה משינויי הון וכוח האדם, והתפתחות הידע היא מקור חדש לצמיחה. אופי הצמיחה מבוססת הידע שונה מהמוכר לכלכלה המסורתית.

אם ננסה לאחד עתה את הבסיס המטאפיסי של פופר עם הסוציולוגיה של טופלר ועם תורת הכלכלה של רומר, נוכל לטעון כי מלחמות הגל השני והראשון התנהלו בעיקר בעולם־1 ("חומר"). במלחמות אלו ניצח מי שהשכיל להעמיד

צבא גדול וחזק יותר, ומי שידע לגייס לעזרתו ולטפח את הגורמים המנטליים (עולם־2) של גייסותיו (כמו רוח־קרב, מוטיבציה, אומץ לב וכו'). לפי תיאור זה, מלחמות העתיד יתפשטו גם לעולם־3, עולם המידע. מבלי להפחית בערכם של גורמים אלו גם בעתיד, הרי בעוד מלחמות העבר (הגל הראשון) נשענו על כוח הזרוע, ומלחמות ההווה (הגל השני) נשענות על כוח המכונות, ישענו מלחמות העתיד יותר ויותר על כוח המוח.

התמודדות אינטלקטואלית עם עידן המידע בתחום הביטחון הלאומי

סמלו המובהק של עידן המידע – המחשב האלקטרוני – נבנה עם סיום מלחמת העולם השנייה כדי לעזור לצבא ארה"ב בחישובים בליסטיים לארטילריה. בשישים השנים שלאחר מכן, בייחוד אחרי המצאת הטרנזיסטור והמעגל המוכלל, הלכו מימדי המחשב וקטנו בהתמדה. גורדון מור, ממייסדי יצרנית המעבדים "אינטל", העריך בשנת 1965, שבכל שנה עד שנתיים יכפיל מספר הטרנזיסטורים את עצמו בשבב המוכלל, בעוד שהמחיר יישאר קבוע.[5] משהתברר שאכן הדבר מתקיים בתחום המוליכים למחצה, הניבוי זכה לכינוי "חוק מור". העתידן ריי קורצוויל מציג טיעונים משכנעים בעד הרחבת "חוק מור" לטכנולוגיות המידע בכללותן.[6]

עם התפתחות המחשב והקטנת ממדיו, עסקו מוסדות הביטחון בשיפור הביצועים של מערכות רבות באמצעות שיבוץ מחשב. התרומה המרכזית התבטאה במהפכת הדיוק של החימוש, וראשיתה בכוח האווירי. תחילה תרמו המחשבים לשיפור בתכנון המבצעים. כשהתאפשר להכניס מחשב למטוסי קרב, נרתם כוח החישוב למשימות התקיפה. שינוי אסטרטגי של ממש התחולל כאשר מימדי המחשב ומחירו קטנו עד שאפשר היה להכניסם לחימוש עצמו. כך נולד עידן "החימוש החכם", חימוש מונחה מדויק, שאומץ תחילה בחימוש אווירי. התוצאות המבצעיות היו מרחיקות לכת. מה שמסוגל לעשות כיום מטוס עם חימוש חכם, בתקיפת מטרת נקודה דוגמת טנק, שקול למה שיכלו לעשות 15 מטוסים לפני 30 שנה או 60 מטוסים לפני 40 שנה.[7] אין פלא כי למהפכה הטכנולוגית הזו יש השפעה מכרעת על תורת הלחימה.

כדי להתאים את אומנות המלחמה לטכנולוגיות המידע, פותחה בראשית שנות התשעים של המאה העשרים תורת לחימה חדשה, "המהפכה בעניינים צבאיים" (Revolution in Military Affairs – RMA). התפישה עומדת על ארבעה יסודות: תקיפה מדויקת; חלל; שליטה בתמרון; לוחמת מידע.[8] לוחמת מידע נוגעת לכמה היבטים שונים: לוחמת מחשבים (שהם האמצעי הטכנולוגי העיקרי לאחסון ושינוע מידע), לוחמה אלקטרונית (בעיקר נגד מערכות קשר ותקשורת), לוחמה פסיכולוגית וטיפול באמצעי תקשורת (החל מתדרוך עיתונאים, דרך עיתונאים

המשובצים בכוחות הלוחמים וכלה במניפולציה במידע המשוחרר לציבור). חשוב לדייק במושגים ולהבין היטב למה מתכוונים במונח "לוחמת מידע", וכפי שנראה בהמשך, המושגים הללו השתנו עם הופעתו והתפתחותו של המרחב הקיברנטי.

התוצאה הישירה של ה־RMA היא עליונות צבאית מוחלטת של צבאות המדינות המפותחות בשדה הקרב[9] – כפי שזו באה לידי ביטוי במלחמות ארצות־הברית בעיראק ואפגניסטן, ובמלחמות ישראל בלבנון ונגד ארגוני הטרור. תוצאה נוספת של ה־RMA היא היכולת חסרת התקדים לנהל לחימה בעצימות נמוכה מדויקת ויעילה, ואף היכולת לגבור על טרור באמצעים צבאיים – בלי לגרום נזק סביבתי רחב.[10]

ואולם התפתחות המחשוב ממשיכה, ומחייבת שינוי תפיסתי מתמשך. החלק הבא במאמר נועד לספק בסיס לתפיסה מעודכנת של הביטחון הלאומי במציאות הכוללת מרחב קיברנטי חדש.

המרחב הקיברנטי

התפוצה המתמשכת של המחשוב ורשתות התקשורת יצרה בראשית המאה ה־21 מצב חדש: שכבה ממוחשבת נוספה על המערכות הקיימות הוותיקות, והיא שולטת למעשה בתפקודן. תפוצת המחשבים, שיבוצם בהתקנים שונים וחיבורם ברשתות התקשורת – כל אלה יוצרים את המרחב הקיברנטי. המושג מאפשר לנו להבין את המתרחש בעולם־3,[11] תוך מיקוד ביחסי הגומלין עם סוגיות הביטחון הלאומי: רשתות הקשורות ביחסי גומלין של תשתיות טכנולוגיות מידע הכוללות רשתות בזק, רשתות ייעודיות, האינטרנט, מערכות מחשב ומערכות משובצות מחשב. המושג כולל גם את הסביבה הווירטואלית – המידע המאוחסן, המעובד והמועבר על הרשתות הללו וביניהן.[12]

שלא כמו יבשה, ים, אוויר, חלל או ספקטרום אלקטרומגנטי, המרחב הקיברנטי אינו תוצר הטבע. המרחב הקיברנטי נוצר בידי בני האדם, ולא היה קיים בלא טכנולוגיות המידע שפותחו בעשרות השנים האחרונות. הידע – שהוא אולי המרכיב החשוב ביותר במרחב הקיברנטי – הוא תוצר של פעילות אנושית מצטברת.[13] המבנה והעיצוב של המרחב הקיברנטי כפי שהוא היום טומנים בחובם השלכות משמעותיות לענייני הביטחון הלאומי.[14]

אפשר לתאר את המרחב הקיברנטי כמורכב משלושה רבדים.[15]

1. הרובד המוחשי ביותר, המשמש היום תשתית של עולם המחשוב, הוא הרובד הפיזי. הרכיבים הפיסיים הם אבני הבניין המוחשיים של המרחב הקיברנטי, אבני בניין עם מאפיינים טבעיים: רוחב, גובה, עומק, משקל, נפח.[16] הרובד החומרי – חופף את "עולם־1" בתפיסה של פופר.

2. הרובד השני הוא לוגיקה של תוכנה: מגוון מערכי הוראות שתוכנתו בידי בני אדם. הרכיבים הפיזיים נשלטים במידה רבה על־ידי התוכנה, והמידע המאוחסן במחשבים נתון לעיבוד באמצעות הוראות התוכנה. רובד התוכנה הוא בחלקו "פיסי" (עולם־1) ובחלקו "לוגי", דהיינו, שוב, עולם־3.
3. הרובד השלישי של המרחב הקיברנטי הוא רובד הנתונים שהמכונה מכילה ומעבדת. הנתונים ועיבודם יוצרים מידע וידע. הרובד הזה הוא הפחות מוחשי מהשלושה, בעיקר משום שמאפייני המידע שונים מאוד ממאפייני האובייקטים הפיזיים. זהו רובד השייך במובהק לעולם־3 של פופר.

טבלה 3 : מאפייני המרחב הקיברנטי ונקודות תורפה העולות מהם

מאפיין	תורפה
שינוי בקצב מהיר	התיישנות מהירה של אמצעים, כולל של מערכות הגנה.
מבנה הפרוטוקול TCP/IP	קשה להתחקות אחר האות ברשת ולזהות את מקורו.
רמת סיבוכיות גבוהה	קשה מאוד לקשר בין אירוע לתוצאה; קשה להבדיל בין תקלה לתקיפה.
שימוש רחב בציוד מסחרי סטנדרטי, מן־המדף	צמצום פערי היכולות בין שחקנים קטנים לגדולים. פגיעות של חומרה ומערכות הפעלה זהות מסכנת קשת רחבה של מערכות.
אמצעי הלחימה הבסיסיים – זולים יחסית	מחיר ההגנה הולך ועולה.
סביבה משפטית מעורפלת	"תחום אפור" עם סיכוי נמוך לענישה– מעודד חוסר יציבות.

מלוחמת מידע ללוחמה קיברנטית

בספרות המקצועית האמריקנית והאירופית,[17] לוחמת המידע נתפסת כמאפיין מובהק של עידן המידע. בעגה הצבאית האמריקאית מכונה לוחמת המידע בשם Information Operations. החלק הממוחשב שלה קרוי Computer Network Operations (CNO).[18]

מבט בטבלה 4 מגלה שלמעשה אלו נושאים "קלאסיים", שהעיסוק בהם ימיו כימי המלחמה עצמה. במרוצת ההיסטוריה פותחו כמה שיטות לוחמה קלאסיות ל"לוחמת מידע", החל באיסוף מודיעין באמצעות "חיישנים" אנושיים (ראה פרשת המרגלים בימי יהושע בן־נון) וכלה בפיתוח טכנולוגיות איסוף מיוחדות (כמו חיישני מודיעין מוטסים, לוויינים וכו'). גם בתחום המניעה פותחו שיטות קלאסיות בלוחמת מידע, כמו הסוואה, דמיים ומיסוך, שיבוש וחסימה, הונאה והטעייה, תעמולה ועוד.

טבלה 4: נושאים הנכללים תחת הכותרת לוחמת מידע

נושא	מערכות וטכנולוגיות רלוונטיות
איסוף מידע	חיישנים שונים בכל תחומי הספקטרום האלקטרו־מגנטי
שינוע מידע לעיבוד ולצרכן	תקשורת רחבת סרט, דחיסה, הצפנה
אחסון ושליפה	בסיסי נתונים, De-Duplication, דחיסה
עיבוד וסינון מידע	עיבוד אותות דיגיטאלי (DSP), אלגוריתמים לזיהוי אוטומטי (ATR), מיזוג נתונים (Data Fusion), אינטליגנציה מלאכותית (AI)
הנגשת מידע	תקשורת רחבת סרט; מערכות תצוגה וממשק אדם־מכונה
מניעת מידע	הסתרה, שיבוש, לוחמה אלקטרונית (ל"א), הצפנה, הטעיה
הגנה על מידע	מניעת גישה למידע שלך מבלתי מורשים, הצפנה

עיון בטבלה 4 לעיל מוביל למסקנה, שהחידוש הכמעט יחיד בתחום זה הוא התלות הגוברת והולכת של מערכות המידע במחשב. במילים אחרות, בעוד שלוחמת מידע אינה תחום חדש, הרי שאין הדבר כך לגבי מערכות המידע משובצות המחשב. המרחב הקיברנטי מאפשר להגדיר מטרות, כלי נשק ושיטות לחימה חדשים. מה שייחודי למלחמת הגל השלישי, מלחמה בעידן המידע, אינו לוחמת מידע לכשעצמה אלא לוחמת מחשבים. משום כך ראוי לצמצם את תחום הדיון ולהתמקד בלוחמת מחשבים במרחב הקיברנטי. החדשנות במרחב הקיברנטי כה רבה, עד שמושגי היסוד כגון "מלחמה", "נשק", "התקפה" ו"הגנה" זקוקים לביאור מחודש.

לוחמת מחשבים במרחב הקיברנטי היא חדירה בלתי מורשית למערכות המחשב של היריב לשם איסוף מודיעין, שיבוש, הטעיה, מניעת שימוש והשהיית המידע. זאת במקביל למניעת הישג דומה של היריב במערכות המחשב שלנו. גם תקיפה מסורתית (הפגזה, הפצצה, חבלה פיזית) של מערכות מחשב תגרום ודאי שיבוש, מניעה והשהיית המידע. אולם תקיפה פיזית כזאת אינה נכללת בלוחמה קיברנטית.

מאפייני המרחב הקיברנטי[19] מגדירים גם את הלוחמה בתחום הזה. מאפייני המרחב הקיברנטי מקשים על ההבחנה בין פגיעה מכוונת לתקלה, ומקשים על האפשרות לייחס פעולה לגורם מסוים (attribution), ולכן גם מקשים להגיב על תקיפה. מאפייני המרחב הקיברנטי היום מעצימים שחקנים שוליים ומקנים יתרון לתוקף לעומת המגן.

בשנים האחרונות מתפתח דיון בפגיעות שנוצרה לאור חיוניות המרחב הקיברנטי לכל תהליכי החיים בחברה המפותחת.[20] לוחמת מחשבים אינה מוגבלת

למערכים צבאיים; עם תפוצת המחשוב ורשתות התקשורת היא הפכה ישימה בכל תחומי החיים. רוב המערכות במשק האזרחי – תלויות היום במחשבים ומחוברות למרחב הקיברנטי. עובדה זו יוצרת פגיעות, הפותחת אפשרויות חדשות ללחימה ודורשת הערכות הגנתית גם של המדינות המפותחות.

התקפה והגנה במרחב הקיברנטי[21]

כלי הנשק הקיברנטי הוא תוכנה זדונית או חומרה מזיקה, הפוגעת במשאב הממוחשב של הקורבן וגורמת לשיבוש נתונים, הטעיה, מניעת שירות או איסוף והעברת מודיעין. אנו מציעים תרגום עברי למונחים האנגליים בתחום:

malware– תוֹקעה. תוכנה זדונית שמיועדת לשבש בסתר פעילות תקינה של מערכת ממוחשבת, וכך לפגוע בתהליך שמנוהל באמצעות אותה מערכת.

spyware– רוֹגלה. תוכנה זדונית שמיועדת לאסוף נתונים בסתר ולעתים להעביר אותם ברשת;

phishing – דיוּג. תרמית מבוססת תוכנה והנדסה חברתית על מנת להשיג במרמה נתונים אישיים של משתמשים ופרטי הזדהות.

השתלת חומרה יכולה להיעשות בהוספת רכיב אלקטרוני נוסף ליחידה קיימת או תוספת בתוך מעגל משולב. ההשתלה יכולה להתבצע בשלב הייצור, ההובלה, התפעול תחזוקה ותיקון.[22] השימוש בתוכנה כנשק לוגי נפוץ מהשימוש בחומרה. אפשרות זו מאפשרת את שיטות הלחימה החדשניות ביותר. הידע והטכנולוגיה הם מוצרים בלתי־נדלים, ובכך חשיבותם העצומה בכל הנוגע ללוחמת המידע, ולא כל ההשלכות כבר הובררו במלואן.[23]

בשעה שמתבסס החשד שמתרחשת התקפה קיברנטית, קשה מאוד לזהות את מקורה ואת זהות התוקף. כל הגורמים הפועלים במרחב הקיברנטי משתמשים באותם הכלים והשיטות. פעמים רבות קיים שיתוף פעולה מסחרי, מעין "מיקור חוץ", בין הגורמים הטכניים בעלי יכולת התקיפה (מתכנתים, פורצי הצפנה, בעלי רשתות שבויות), למזמיני שירותים (חוקרים פרטיים, פשע מאורגן, ארגוני ביון). כדי לקבוע שתקיפה קיברנטית היא מעשה מלחמתי, יש לבחון כמה מאפיינים:

- **מקור ארגוני וגיאוגרפי**: האם מדינה עומדת מאחורי הפעולה?[24]
- **מניע**: האם אפשר לזהות מניע אידיאולוגי, פוליטי, כלכלי, דתי למתקפה?
- **רמת המורכבות**: האם המתקפה דרשה תכנון מורכב ומשאבים מתואמים, אשר זמינים בעיקר לגופים מדינתיים?
- **תוצאה**: האם ההתקפה גרמה לנזק ונפגעים? האם הייתה גורמת נזק לולא פעולות ההגנה?

מאפייני המרחב הקיברנטי מקשים לתת תשובות לשאלות הללו, ודאי לא תשובות המספיקות לקביעת מדיניות.

כדי להתגונן צריך לזהות שמתרחשת מתקפה, וכאמור הדבר אינו פשוט כלל במרחב הקיברנטי. ככל שהחדרת כלי הנשק תעשה מוקדם יותר, ובייחוד לפני גיבוש תוכניות בדיקה, הסיכוי לגילוי קטן. ככל שהנשק הקיברנטי יהיה מדויק יותר, כך הוא יגרום פחות נזק סביבתי ויפחית הסיכוי שהמותקף יגלה את דבר ההתקפה. פעילות ההתגוננות מכילה שלושה מעגלים:[25]

1. **הגילוי**: זהו "עקב אכילס" של התחום – כיצד נדע שהתרחשה תקיפת מחשבים?
2. **המניעה**: הפעלת אמצעים לעצירת התוקף בשלב החדירה.
3. **התגובה**: בכלל זה אמצעי התאוששות לצמצום הישג התוקף, אמצעי זיהוי פלילי ואף "פעולת תגמול".

סוגיות מרכזיות בלוחמה קיברנטית

השינוי הטכנולוגי, הנמצא ביסוד מעבר ל"גל השלישי", להרחבה מהירה של "עולם־3" ולהתפתחות "כלכלת המידע", מעלה שאלות חדשות. אחת המרכזיות היא שאלת ההגנה על תשתיות חיוניות. בשנים האחרונות אנו עדים לדיון מתפתח על ההגנה על התשתיות חיוניות, המונחות ביסוד החברה המודרנית. היתכנות האיום הוצגה בניסויים, למשל מתקן לייצור חשמל הוצא מכלל שימוש והתפוצץ באמצעות שידור הוראות למערכת השליטה והבקרה.[26] נראה שהאיום התממש בפרשה שנתגלתה בקיץ 2010: וירוס תולעת המכונה Stuxnet התפשט במחשבי "חלונות" וחיפש בינם מחשבים המריצים תוכנת שליטה ובקרה תעשייתית תוצרת "סימנס" מסוג מסוים, המחוברים לבקר תעשייתי מדגם מוגדר. כאשר איתר את המחשבים הרלוונטיים, הפעיל הווירוס קוד תוכנה ששיבש את פעילות הבקר הממוחשב תוך הסתרת השינוי מתוכנת השליטה וממפעילי הציוד. נטען כי בסופו של דבר, פגע סטאקסנט בהפעלה התקינה של הצנטריפוגות להעשרת אורניום באיראן. משך התקיפה ומקורה – אינם ידועים.[27]

תשתיות חיוניות של המדינה הן יעד מתבקש במהלך סכסוך. מדוע אפוא עלה כעת החשש הזה, ודווקא במדינות החזקות ביותר? ארצות הברית שנהנית ממעמד של מעצמת־העל היחידה בעולם – היא החלוצה והמובילה בדיון על פגיעותה הקיברנטית.[28] התשובה נעוצה במעבר מ"מלחמות הגל השני" של טופלר אל מלחמות "הגל השלישי", גל המידע. הדיון המחודש בהגנה על התשתיות החיוניות נעוץ בהופעת איום חדש, שלא היה בר ביצוע לפני כן. התפתחות המרחב הקיברנטי מאפשרת, לראשונה בהיסטוריה, לתקוף מערכות תשתית חיוניות במרחב הקיברנטי, בלי להגיע פיזית אל מקום הימצאותן ובלי להיחשף במהלך התקיפה. נניח שיום אחד יתמוטטו מערכות המחשבים של הבנקים בישראל. נניח גם כי נצליח לקבוע בוודאות כי הנזק העצום נגרם במכוון, בחדירה מכוונת, ונניח שנצליח לאתר את התוקף בשטחה של מדינה שכנה. האם זו תקיפה מלחמתית?

לכאורה הנזק שנגרם הוא "רק" כלכלי ולא נפגעו חיי אדם (ישירות). פעמים רבות מדינות הבליגו על תקיפות מסורתיות שגרמו נזק כלכלי אך לא פגעו בחיי אדם.[29] אבל נזק כלכלי עלול לגרום לשיתוקה של מדינה שלמה. נושא ההגנה על תשתיות מידע לאומיות חיוניות הוא אחד המרכזיים בדיון על ביטחון קיברנטי. נושא ההגנה על תשתיות חיוניות חורג מגבולות מאמר זה, וראוי לטיפול ממוקד.[30]

"מלחמה מידע" מעלה מיד הרהור על מושג המלחמה עצמו: האם תקיפה קיברנטית של המידע הממוחשב, ללא שימוש באש – היא "מלחמה"? מהי מטרה לגיטימית במלחמה כזאת? השימוש הצבאי הנרחב בתשתיות אזרחיות (בעיקר לתקשורת) מקשה על ההבחנה בין מטרה צבאית לאזרחית. כך, תשתית המחשוב של משרד ההגנה האמריקני מורכבת מ־15,000 רשתות ושבעה מיליון התקנים הפזורים ברחבי העולם. אולם רוב התקשורת של משרד ההגנה מנותב ברשתות אזרחיות מסחריות.[31] אזרחים (גם ילדים ונשים) יכולים להיות יעילים כלוחמי מחשבים לא פחות מחיילים. האם זה הופך אותם מטרות פוטנציאליות לתגובה? כיצד יש לפעול במקרה של נזק כלכלי רחב? כיצד אומדים את הנזק העקיף שהתקיפה גרמה? נניח שתקיפה קיברנטית גרמה לשיבושים ממושכים באספקת חשמל. נניח שאחת התוצאות היא כיבוי מערכות התאורה והרמזורים בכביש, ושבעלטה אירעה תאונות דרכים קטלנית. האם להתייחס לקורבן התאונה כחלל במלחמה קיברנטית? כיצד יש להגיב: באש ובתמרון, או במכת־נגד קיברנטית? הבעיה סבוכה יותר מהתרחיש שתיארנו, משום שתקיפת מחשבים אינה זקוקה לבסיס מדינתי, והיא יכולה להיעשות גם על ידי ארגונים ואף יחידים.

לוחמת מחשבים מתנהלת גם בין מדינות ידידותיות בתחרות להשיג למודיעין דיפלומטי וכלכלי. האם ראוי לקרוא לזה "לוחמה"? האם ראוי להפעיל לוחמת מחשבים בימי שלום למטרות כאלה?

הבעיה המיוחדת בנושא הלוחמה הקיברנטית היא זיהוי התקיפה: בניגוד לתקיפה מסורתית המתרחשת בעולם־1, שהוא עולם החומר, איתור הפגיעה וזהות התוקף אינם בהכרח נחשפים לאחר התקיפה. ללוחמת מחשבים גם אין "קו חזית" מוגדר ואין בה כמעט משמעות למרחקים גיאוגרפיים. נוכח מאפייני המרחב הקיברנטי, עצם זיהוי התקיפה אינו מובן מאליו: לתקיפה ולתקלות יש תסמינים דומים. עם השתכללות עולם המחשבים, המתבטאת בריבוי התוכנות והיישומים, ובריבוי מספר הטרנזיסטורים בכל רכיב – הסבירות לתקלה אינה יורדת. ההסתברות הסטטיסטית לשגיאת תכנות (Bug) בתוכנה היא קבועה, וערכה הנומינלי עולה עם ריבוי המורכבות של תוכנות.[32]

כאמור, היכולת לזהות שהמחשבים שלך הותקפו ונפגעו, ולא התקלקלו באופן "טבעי" – לוקה בחסר. בלי היכולת להבחין בזמן אמת בין מתקפה לתקלה, נדרשת השקעה כבדה ב"כוננות קיברנטית" מתמדת. ההגנה מפני איומים קיברנטיים

חייבת להקיף את כל אפיקי התקיפה, להתעדכן עם פיתוחים חדשים, ומחיר ההגנה הולך ועולה. הטיעון על קושי ההגנה דומה לטיעון נגד הגנה אקטיבית נגד טילים, ולטיעון על עקרות הגנה נגד מחבל מתאבד. עם זאת, ניתן לייצר מענה לאיומים החדשים.[33] על ההגנה מוטלת מעמסה רבה מכיוון שבמאפייני המרחב הקיברנטי של היום יש יתרון ברור להתקפה על פני ההגנה.[34] תחום ההצפנה הוא אחד הבודדים במרחב הקיברנטי שבו המגן נהנה בינתיים מיתרון על התוקף.[35] בהינתן הקושי לזהות את עצם התקיפה, מקורה הגיאוגרפי וזהות התוקף, מתקבל מצב של חוסר וודאות המקשה על תגובה מסלימה. טבלה 3 לעיל מסכמת את המאפיינים ואת נקודות התורפה הרבות היוצרים את "בעיית הייחוס": קשה לדעת את מקור התוקף וזהותו, בשליחות מי פעל, וודאי שקשה להוכיח אשמה. בתחום הביטחון המסורתי מוקדש מאמץ רב לנושא המודיעין, ההתרעה, וההרתעה, כדי לצמצם ככל האפשר משאבים המופנים לקיום כוננות מתמדת. נושא ההרתעה הוא בעייתי במיוחד במרחב הקיברנטי בעיקר עקב בעיית הייחוס.[36] אם מתגברים עליה, ומוציאים לפועל תקיפה קיברנטית, מאפייני המרחב הקיברנטי מעלים בעיות נוספות. כיצד לזהות שהמחשבים שניסית לתקוף, בתגובה על מתקפה קיברנטית שאיתרת, אכן נפגעו? כדי שיהיה אפשר להסתמך על התקפה קיברנטית נדרשת בקרת תוצאות (battle damage assessment). מבחינה זו, לתקיפה המבוצעת "בחוג פתוח", כלומר כזו שלא ידוע אם הצליחה, יש תועלת מוגבלת. בעיה זו חריפה במיוחד בתקיפה קיברנטית.

בלוחמה קונבנציונלית התפתחו "חוקי משחק" המעוגנים באמנות בינלאומיות. אמנות אלו נוסחו לפני הופעת המרחב הקיברנטי, והן עוסקות ב"מאבק מזוין", ב"עימות פיזי", ב"פגיעה טריטוריאלית" וכדומה. המושגים האלה אינם רלוונטיים ללוחמת מחשבים, והאמנות הקיימות דורשות התאמה ללוחמה קיברנטית, מלחמה ב"גל השלישי". על אף המחקר הענף בתחום, סביר להניח שבחינת הסוגיות מזווית המשפט תמשך שנים רבות. העדר "חוקי משחק" מקשה על התמודדות היומיומית עם הבעיות המיוחדות של הלוחמה הקיברנטית. הסוגיות שסקרנו אינן משפטיות גרידא, אלא סוגיות מדיניות הכרחיות לקבלת החלטות ולביצוען. כך בימים אלה (סתיו 2011) שוקדים בנאט"ו על גיבוש מסגרת משפטית שתאפשר לארגון להגיב על מתקפות קיברנטיות בשיטות שחוקיותן מעורפלת במצב המשפטי הקיים. הבנת היסודות העיוניים של התחום חיונית לשיפור יכולת ההתמודדות.

סיכום

המרחב הקיברנטי הוא תוצר חדש למדי של עידן המידע. ביטחון קיברנטי הוא חלק מסוגיה חדשה: המעבר לעידן המידע. על מנת להתמודד עם השינוי המאתגר, יש לאמץ פרספקטיבה רב תחומית. לכן הצגנו בתחילת המאמר מקורות עיוניים

אחדים של עידן המידע. בחרנו לגייס למשימה מרעיונותיהם של הזוג טופלר, ושל קרל פופר ופול רומר, אולם ברור לנו שיש עוד מקורות, ואנו בטוחים שנראה מחקר בינתחומי נוסף בנושא "עידן המידע". לאחר מכן סקרנו את רכיבי הלוחמה הקיברנטית: נשק, הגנה, התקפה, מלחמה, תוך נגיעה הכרחית ביסודות הטכניים מתחום המחשבים.

הבעייתיות בהתמודדות עם אתגרי ביטחון נובעת ממאפייני המרחב הקיברנטי: מהירות הפעולה, קצב השינוי, מורכבות וסיבוכיות. ההגנה וההתקפה הקיברנטית מתרחשים בעולם־3, עולם הידע. יש לחקור לעומק את ההשלכות המהותיות הנובעות מהסוגיות המרכזיות של לוחמה קיברנטית, שתוארו בפרק האחרון במאמר.

החידוש המרכזי אינו "לוחמת המידע" אלא לוחמת המחשבים במרחב הקיברנטי. הדיון בפתרונות ל"ענייני מחשבים" נוטה להתרכז בתחום הטכני, המרוחק מהדיון הציבורי וממרחבי עיצוב המדיניות הציבורית. ברור שדרושה הבנה מקצועית בתחום הנדון, והוא מציב אתגרים כבירים הדורשים מענה ברמת המדיניות הציבורית הלאומית. סקירת הסוגיות המרכזיות של לוחמת המידע מציגה תמונה מורכבת, אל מעבר למקצועות המחשב. לפיכך כדי לספק ביטחון לאומי בסביבה המשתנה של עידן המידע, ראוי להשתמש בתשומות מכל תחום ידע רלוונטי: כלל מדעי החברה, פסיכולוגיה ופילוסופיה. אנו מקווים שהמאמר יעודד מחקר בינתחומי של אתגרי הביטחון הקיברנטי, יתרום לפיתוח מדיניות ביטחון לאומית מושכלת ובסופו של דבר יתרום לביטחון ושגשוג בעידן המידע.

הערות

1 "The Meaning of Stuxnet: A sophisticated "cyber-missile" highlights the potential—and limitations—of cyberwar," *Economist (GBR) Economist* 397, no. 8702 (2010). September 30, 2010, from the print edition.

2 ניתן להבחין בין מידע (Information) או נתונים (Data) ובין ידע (Knowledge) המחייב גם המשגה והבנה של המידע הגולמי. לצורך המאמר, ההבחנה אינה מהותית.

3 K. Popper, *Objective Knowledge - An Evolutionary Approach*, Oxford University Press, 1972. פרקים 3–4.

4 Paul M. Romer, "Endogenous Technological Change", *Journal of Political Economy*, 1990, Vol. 86, no. 5, pt 2, pp. S71-S102.

5 Mollick, E. "Establishing Moore's Law." *Annals of the History of Computing, IEEE* Vol. 28, no. 3 (2006), pp. 62-75.

6 Ray Kurzweil, "The Law of Accelerating Returns" (2001).

7 יצחק בן־ישראל, "מלהב החרב אל זיכרון המחשב" **אודיסאה** 9, אוקטובר 2010.

8 לקורא המתעניין ב־RMA בהקשר של טכנולוגית המידע מומלצים הספרים הבאים: Michael E. O'Hanlon, *Technological Change and the Future of Warfare*. (Washington, D.C.: Brookings Institution Press, 2000). Stuart E. Johnson and Martin C. Libicki, *Dominant Battlespace Knowledge: The Winning Edge*. (Washington, DC:

National Defense University Press, 1995).

9 עליונות שהביאה לנסיגת האויבים לאסטרטגיה של הישרדות ולחימה א־סימטרית.

10 היכולת הוצגה לראשונה בניצחונה של ישראל על "אנתפאדת המתאבדים" הפלסטינית בשנים 2000–2005. ראה: ליאור טבנסקי, **המאבק בטרור בעידן המידע: 'אינתיפאדת המתאבדים' וההתמודדות הישראלית עמה בסיוע טכנולוגיות עילית.** אוניברסיטת תל אביב, תל־אביב (2007).

11 ראה לעיל על המושג מבית מדרשו של קרל פופר.

12 הדמיון הרב להגדרות אמריקניות מקורו בדמיון בין ארצות הברית וישראל בכל הקשור לערכים ולרמה מדעית וכלכלית. סין, רוסיה, הודו, צרפת ואחרות – מגדירות את המרחב הקיברנטי והאיומים הקיברנטיים בצורות שונות. אולם, העיסוק בנושא זה חורג מגבולות עבודה זו.

13 הדיון על מעמד הידע מופיע אצל קרל פופר, ומוזכר בפרק הקודם.

14 לדיון על המרחב הקיברנטי בהקשר לביטחון הלאומי ראו: ליאור טבנסקי, "לחימה במרחב הקיברנטי: מושגי יסוד", **צבא ואסטרטגיה**, כרך 3, גיליון 1, אפריל 2011.

15 Martin C. Libicki, "Cyberdeterrence and Cyberwar," (Santa Monica, CA: RAND Corporation, 2009).

16 אלקטרוניקה היא התשתית של עולם המחשוב היום. לפני האלקטרוניקה היו מכונות חישוב מכאניות. ובעתיד? כבר כיום הוכחה האפשרות לנצל תשתית ביולוגיות לצורכי המחשוב. מחשוב DNA משתמש בביולוגיה מולקולארית ו־DNA במקום הרכיבים האלקטרוניים. אפשרות נוספת היא מחשוב פפטידי Peptide: מחשוב ביו־מולקולארי המבוסס על תרכובות העשויה חומצות אמינו.

17 השווה ההגדרות של משרד ההגנה אמריקאי: "Joint Publication Jp 3-13: Joint Doctrine for Information Operations". edited by United States Department of Defense. Washington, DC, 2006.
לאלה של האיחוד האירופי כפי שמוגדרים במכרז של רשות ההגנה האירופית EDA Study "Computer Network Operations (CNO) for EU led military operations", 10-CAP-OP-37 (EU milops CNO Capability) - Annex, August 16, 2010.

18 שכוללת הגנה (Computer Network Defense (CND, ניצול Computer Network Exploitation (CNE) והתקפה Computer Network Attack (CNA). הבסיס הטכני לשלוש סוגי הפעולה הוא זהה.

19 ראה טבלה 2 לעיל.

20 ראה למשל: Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do about It*. New York: Ecco, 2010; Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz. *Cyberpower and National Security*. Washington, DC: Center for Technology and National Security Policy; National Defense University Press: Potomac Books, 2009; Lynn III, William. "Defending a New Domain", *Foreign Affairs* Vol. 89, no. 5 (September-October 2010); Coward, Martin. "Network-Centric Violence, Critical Infrastructure and the Urbanization of Security." *Security Dialogue* 40, no. 4-5 (2009), pp. 4-5; Sharp, Walter Gary. "The Past, Present, and Future of Cybersecurity", *Journal of National Security Law & Policy* 4, no. 1 (2010).

21 לדיון בסוגיות הטכניות ראה: Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld*. (O'Reilly Media 2009).
Lehtinen, Rick, Deborah Russell, and G. T. Gangemi. *Computer Security Basics*. Sebastopol, CA: O'Reilly & Associates, 2006.

22 נטען כי חומרה פגומה שהשתיל ה־CIA בציוד לבקרת מערכת הובלה של גז שרכשה

ברית המועצות, גרמה לפיצוץ אדיר בסיביר ב־1982

W. K. Clark and P. L. Levin, "Securing the Information Highway: How to Enhance the United States' Electronic Defenses," *Foreign Affairs,* Vol. 88, No. 6 (2009).

23 למשמעויות הכלכליות ראה הדיון אצל פול רומר, שהוזכר לעיל.

24 לאחר פיגועי 11 בספטמבר 2001, סף התמיכה המדינתי הורד: לעיתים, די בראיות נסיבתיות כמו תמיכה אידיאולוגית באויב או מתן שירות לוגיסטי למחבלים.

25 דיון מפורט בנושאים הללו חורג מגבולות המאמר.

26 "ניסוי אורורה" שנערך במעבדות הלאומיות באיידהו, ארצות הברית.

Lewis, James Andrew, "Thresholds for Cyberwar." Washington, DC: Center for Strategic and International Studies 2010.

27 ראה הערה 1. Chen, T. "Stuxnet, the Real "The Meaning of Stuxnet." *Economist*. Start of Cyber Warfare?" *IEEE Network* Vol. 24, no. 6 (2010).

28 United States. President's Commission on Critical Infrastructure, Protection. *Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection*. Washington, DC: US GPO, 1997.

29 כך נהגו ממשלות ישראל לאורך שנים, כאשר אלפי רקטות "טפטפו" מרצועת עזה ופגעו בשטחים פתוחים במערב הנגב.

30 ראה: ליאור טבנסקי, הגנה על תשתיות קריטיות מפני איום קיברנטי, **צבא ואסטרטגיה,** כרך 3, גיליון 2, נובמבר 2011. Myriam Dunn, "Securing the Digital Age: The Challenges of Complexity for Critical Infrastructure Protection and Ir Theory," in Johan Eriksson and Giampiero Giacomello, (eds.), *International Relations and Security in the Digital Age* (Routledge, 2007).

31 Lynn III, William. "Defending a New Domain".

32 אחד המדדים למורכבות התוכנה הוא מספר שורות הקוד Source Lines of Code (SLOC). "**חלונות** 3.1NT", מערכת ההפעלה מבית **מיקרוסופט**, יצאה לאור ב־1993 וכללה 4.5 מיליון שורות. "**חלונות** XP" יצאה לאור ב־2001 וכללה 45 מיליון שורות. הפצת לינוקס Fedora 9, כוללת 204 מיליון שורות קוד.

33 ראה: ליאור טבנסקי, **המאבק בטרור בעידן המידע**. (2007)

34 ראה לעיל, וגם: Lynn III, William. "Defending a New Domain"

35 שיטות ההצפנה הקיימות מבוססות על עקרון מתמטי הבא לידי ביטוי בקושי לפרק לגורמים מספר המורכב ממספרים ראשוניים. למחשוב קוונטי מאפיינים שיבטלו לחלוטין את היתרון של שיטות ההצפנה הקיימות. כאשר ייבנה מחשב קוונטי – תחום הביטחון יעבור זעזוע עקב התיישנות יסודות ההצפנה.

36 Libicki, Martin C. "Cyberdeterrence and Cyberwar." Santa Monica, CA., RAND Corporation, 2009. ראה גם מאמר של אמיר לופוביץ' בגיליון זה.