לחימה במרחב הקיברנטי: מושגי יסוד

ליאור טבנסקי

מבוא

התפתחות המחשוב בעשורים האחרונים אפשרה שינויים מרחיקי לכת בכל תחומי החיים. ההתקדמות המהירה בקצב חסר תקדים בתחומי המחשוב, התקשורת והתוכנה הובילה להוזלה דרמתית[1] של ייצור, עיבוד והפצת מידע. ההתפתחות המדעית־טכנולוגית הנוגעת לעיבוד והפצת מידע, המכונה "מהפכת המידע", משפיעה גם על הביטחון הלאומי.

ההתמודדות האינטלקטואלית עם השלכות המעבר לעידן המידע על העיסוק הביטחוני הביאה בשנות התשעים של המאה הקודמת להתפתחות הרעיון של "המהפכה בעניינים צבאיים". רעיון זה נולד עקב שינויים מרחיקי לכת בתחום טכנולוגיות המידע, שגרמו לקפיצת מדרגה בזמינות ובאיכות המודיעין, בקצב העברת המידע ובדיוק הנשק.[2] ניצול הטכנולוגיות החדשות מאפשר יכולות שלא היו מוכרות קודם לכן, שיחד עם שיטות פעולה חדשות מביאות לשינוי איכותי במקצוע הצבאי.[3]

טכנולוגיות המידע ממשיכות להתפתח בקצב מהיר ומובילות לעידן חדש במהפכת המידע. צמיחה מהירה בתפוצת המחשוב והתקשורת ועלייה מהירה ומתמדת בביצועי המערכות הממוחשבות יוצרות מציאות חדשה: מרחב נוסף בעולם – המרחב הקיברנטי.

המרחב הקיברנטי טומן בחובו פוטנציאל ליתרונות עצומים, לצד סיכונים בלתי מוכרים. לאור החדשנות שבו – מרחב שלא נוצר בטבע אלא בידי בני אדם, וקיים כארבעים שנה בלבד – הבנתו והבנת השלכותיו נמצאות רק בראשיתן.

מאמר זה יתמקד בביטחון הלאומי לאור הופעת המרחב הקיברנטי. המפגש בין נושא חדשני, המאפשר יכולות חסרות תקדים ומהווה תחום טכני הדורש הבנה

ליאור טבנסקי, חוקר בתכנית לחקר לוחמה קיברנטית, הנתמכת על ידי קרן ג'וזף וג'נט ניובאוואר, פילדלפיה, ארצות הברית

מקצועית, ובין תקשורת ההמונים השרויה בתחרות על תשומת לבו של הצרכן, יוצר נטייה טבעית להפרזה. הדיון הציבורי בישראל בנושא הביטחון הקיברנטי, כמו בתחומים חדשניים ועתירי טכנולוגיה אחרים, לוקה בחסר.

המאמר נועד להמשיג את תחום העיסוק הקיברנטי וליצור שפה משותפת לדיון ציבורי פורה בישראל בנושא המתפתח של ביטחון קיברנטי. הוא ידון בתופעת המרחב הקיברנטי וביחסי הגומלין בינה ובין תחום הביטחון הלאומי של ישראל. במסגרת זאת יתייחס המאמר למאפייני המרחב הקיברנטי, לנקודות התורפה הקיימות בו ולאיומים האפשריים הקשורים בו. בהמשך יטפל המאמר בנושאי ההגנה, ההתקפה וההרתעה במרחב הקיברנטי. לאור חדשנות התופעה, המאמר יציע הגדרות אופרטיביות לנושאים הנדונים, תוך ניסיון להתמקד בהיבטי הביטחון הלאומי של ישראל.

המרחב הקיברנטי: יסודות ומאפיינים

המושג *cyberspace* – "מרחב קיברנטי" – הופיע לראשונה בספרות המדע הבדיוני; מרכיביו הלשוניים הם *space* + (*cyber*(*netics*).[5] המילה cyber מקורה במילה היוונית *kybernetes*, שפירושה "הגאי".[6] יישומה המודרני הופיע לראשונה במושג *cybernetics*, שהוצג על ידי המתמטיקאי נורברט וינר (Norbert Wiener) בספר שכתב ב־1948 כדי לתאר שליטה, בקרה ותקשורת בעולם החי או בעולם המכונות.[7] המילה *Space* היא בעלת משמעויות רבות בשפה האנגלית, ומתייחסת למאפיינים פילוסופיים, פיזיקאליים, מתמטיים, גיאוגרפיים, חברתיים, פסיכולוגיים ועוד. השימוש במילה "מרחב" ללא תיחום מדויק עשוי להוביל לפרשנויות מורכבות, ואכן כך קורה בהקשר למרחב הקיברנטי. ההגדרה הפשוטה ביותר של מרחב מתייחסת לציון מקום של אירוע או חפץ בעולם תלת־ממדי רציף.[8] הגדרה פשוטה זו מספיקה לניסיון היום־יומי של בני האדם, אך אינה מספיקה לתיאור ההתרחשות בעולם הממוחשב, השונה במהותו מהמרחב הפיזי.

החיבור הפשוט של שתי המילים "מרחב קיברנטי" אינו מעניק לנו הבנה מספקת של המושג. עלינו להגדיר את המושג בהתייחס לשימוש המיועד בו: הבנת התהליכים המתרחשים בעולם הממוחשב ויחסי הגומלין שלהם עם סוגיות הביטחון הלאומי.

בניגוד ליבשה, לים, לאוויר, לחלל או לספקטרום אלקטרומגנטי, המרחב הקיברנטי אינו חלק מהטבע. הוא נוצר בידי בני האדם ולא היה קיים ללא טכנולוגיות המידע שפותחו בעשרות השנים האחרונות. המרחב הקיברנטי מוחשי הרבה פחות מהמרחבים הטבעיים, ולפיכך הוא מחייב דיון מושגי זה.

המרחב הקיברנטי מורכב מכל הרשתות הממוחשבות בעולם ומכל נקודות הקצה שמחוברות אל אותן רשתות ונשלטות באמצעות פקודות העוברות בהן.

האינטרנט הציבורי המסחרי הפך בסוף העשור הראשון של המאה ה־21 לחלק בלתי נפרד מחיינו ומחיי ילדינו.[9] שני מיליארד איש ברחבי העולם היו מחוברים לרשת ברבעון הראשון של 2010. שיעור החדירה של האינטרנט במדינות המפותחות נע סביב 80 אחוזים.[10] הגישה לרשת האינטרנט עוברת במהירות מנקודות קצה נייחות ומתשתית פיזית קבועה להתקנים ניידים ולתשתית אלחוטית. מחיר השימוש באינטרנט ממשיך לצנוח, וממדי הרשת וסיבוכיותה הולכים ועולים.

כאשר מתחילים לדון במרחב הקיברנטי, הדיון נוטה להתמקד באינטרנט המסחרי. אולם, רשת האינטרנט הציבורי היא רק חלק מהמרחב הקיברנטי. מרחב זה כולל, לצד רשת האינטרנט, גם מגוון רשתות מחשב נוספות שאינן פתוחות לגישה באמצעות רשת האינטרנט, רשתות שרבות מהן עוצבו ונבנו כדי לבצע מטלה מוגדרת.[11] כל הרשתות הממוחשבות הללו, וגם רבות אחרות, הן חלק מהמרחב הקיברנטי. חלק מהרשתות הייעודיות בנויות מאותן אבני בניין כמו רשת האינטרנט הציבורית, אבל מופרדות ממנה. אחרות משתמשות בטכניקות שונות לחלוטין מזו של האינטרנט. המרחב הקיברנטי נוצר מחיבור מערכות ממוחשבות המתקשרות ביניהן.

המרחב הקיברנטי הוא תחום (כמו ים, יבשה, אוויר או חלל) שבו מתרחשות תופעות ובו פועלים בני האדם. אפשר לתאר את המרחב הקיברנטי כמורכב משלושה רבדים.[12] הרובד המוחשי ביותר, שהוא התשתית של העולם הקיברנטי, הוא הרובד הפיזי: אנרגיה חשמלית, מעגלים מוכללים, מעבדים, התקני אחסון, תשתיות תקשורת, כבלי נחושת וסיבים אופטיים, משדרים ומקלטים. כל אלה הם אבני הבניין המוחשיות של המרחב[13] – אבני בניין בעלות מאפיינים טבעיים: רוחב, גובה, עומק, מאסה, נפח.

הרובד השני הוא לוגיקה של תוכנה: מגוון מערכות של הוראות לפעולה ותגובה אשר תוכנתו על ידי בני האדם. הרכיבים הפיזיים נשלטים במידה רבה על ידי התוכנות השונות, והמידע המאוחסן במחשבים נתון לעיבוד באמצעות הוראות התוכנה. רוב המרחב הקיברנטי משתמש כיום בחומרה ובתוכנה סטנדרטיות.

הרובד השלישי של המרחב הקיברנטי הוא רובד הנתונים שהמכונה מכילה, היוצרים מידע. הרובד הזה הוא הפחות מוחשי מהשלושה, בעיקר לאור העובדה שמאפייני המידע שונים מאד ממאפייני האובייקטים הפיזיים.

מאפיינים ארגוניים של המרחב הקיברנטי

חלק גדול מהמרחב הקיברנטי מאורגן ומנוהל בידי ארגונים פרטיים ושיתופיים, שאינם חופפים מדינות או גבולות גיאוגרפיים. רשת האינטרנט, המהווה מרכיב מרכזי וצומח במרחב הזה, בנויה בצורה מבוזרת. האידיאולוגיה של יוצרי האינטרנט ומובילי הדעה בה היום מתנגדת לכל סוג של ניהול מדינתי.[14] ההתפתחות

המתמשכת של טכנולוגיות המידע מאפשרת יישומים חדשים ובלתי צפויים, המנצלים את התשתית הפתוחה של רשת האינטרנט. כך, למשל, התאפשרה העברת תוכן לא טקסטואלי (תמונה, קול, וידאו) על גבי תשתית האינטרנט, ותקשורת אלחוטית והוזלת כושר העיבוד מאפשרים להתקנים רבים (חפצים שהיו נטולי מחשוב, מכונות תעשייתיות, אביזרי עזר טכנולוגיים) לקבל יכולות קישוריות וחיבור אינטרנטי.

לאור המאפיינים המבניים והארגוניים הללו, המרחב הקיברנטי הוא בעל סיבוכיות גבוהה ונתון לשינויים תכופים ומשמעותיים. אולם, חשוב לציין שהמאפיינים הללו נאספו בשיטה אמפירית וכי במיוחד המאפיינים הארגוניים נגזרו מסיכום של תצפיות על המציאות הקיימת כיום. לאור בעיית האינדוקציה,[15] אין להסיק מכך שהמאפיינים הללו הם חלק הכרחי ומובנה מלכתחילה של מרחב קיברנטי, ולפיכך הם לא יופיעו בהגדרת התחום.

כאמור, מטרת מאמר זה היא לתרום לדיון הציבורי בסוגיות הביטחון הלאומי של ישראל במרחב הקיברנטי. הגדרת המושג "מרחב קיברנטי" חייבת, אפוא, לשקף נאמנה את המציאות הקיימת כדי להיות ישימה. הגדרה אופרטיבית למושג זה היא: רשתות הקשורות ביחס גומלין של תשתיות של טכנולוגיות מידע וכוללות את האינטרנט, רשתות "בזק", רשתות ייעודיות, מערכות מחשב ומערכות משובצות מחשב. המושג כולל גם את הסביבה הווירטואלית – המידע המאוחסן, המעובד והמועבר על גבי הרשתות הללו.[16]

המרחב הקיברנטי והביטחון הלאומי

הביטחון הוא אחד הצרכים העיקריים של בני אדם, חברות ומדינות. חלק ניכר מהעיסוק האנושי בכל המרחבים הטבעיים (יבשה, ים, אוויר, חלל, ספקטרום אלקטרומגנטי) נובע מסוגיות הביטחון. אולם הניסיון ההיסטורי, יחד עם ההגות הפילוסופית, מלמדים שאין בהתפתחות המדעית כדי לשנות את הטבע האנושי וכי סכסוכים בין אנשים וחברות ממשיכים ללוות אותנו.[17] כך גם המרחב הקיברנטי – מעשה ידי אדם – ינוצל בידי האדם למטרותיו ואפשר להניח בביטחון שגם במרחב הזה יהיו מאבקים וינוהלו סכסוכים.

מהותו של המרחב הקיברנטי גורמת לכך שמושגי יסוד מקובלים, כגון אלימות, זהות, מיקום, הגנה, התקפה ומהירות, אינם מתארים נכונה את ההתרחשויות בו. המאפיינים המיוחדים של המרחב הקיברנטי מחייבים, אפוא, עיסוק שונה ומקצועי בו.

ארצות הברית החלה להתייחס למרחב הקיברנטי בהקשר של הביטחון הלאומי כבר ב־1996.[18] תשומת הלב האמריקאית לנושא הביטחון במרחב הקיברנטי הלכה וגדלה מאז, ולאחרונה אף קיבלה ביטוי נשיאותי בדברי הנשיא אובמה: "It's now

clear that this cyber threat is one of the most serious economic and national security challenges we face as a nation. It's also clear that we're not as prepared as we should be, as a government or as a country".[19]

ההשקעה בתחום הביטחון הקיברנטי בארצות הברית לא מוגבלת לרמה ההצהרתית בלבד, אלא כוללת הפניית משאבים כספיים וארגוניים משמעותיים. מוסדות ממשל, צבא, אקדמיה ותעשייה אמריקאיים מובילים את העיסוק בתחום הביטחון הקיברנטי ומרבים לפרסם מחקרים וניירות עמדה בנושא זה. הדיון בשלבי התפתחותה של הגישה האמריקאית לנושא זה חורג מגבולות מאמר זה, ואזכורו כאן נועד להמחיש את העניין הרב שהוא מעורר בקרב חוגים רחבים בארצות הברית.

על אף גילו הצעיר של המרחב הקיברנטי, פוטנציאל השפעתו לא נעלם מעיני העוסקים בביטחון הלאומי גם במדינות אחרות ברחבי העולם, אולם ברוב המדינות עצם העיסוק בתחום זה ובתכניו לוטים בערפל ובמעטה של סודיות.

להלן תיאור היסודות הרעיוניים וביאור המונחים השגורים והמקובלים במרחב הקיברנטי, המאפשרים ליצור שפה משותפת בתחום זה בדיון הציבורי בישראל.

כלי הנשק

המרחב הקיברנטי תלוי בתשתיות פיזיות – מבנים המכילים מחשבים, מקורות חשמל, כבלי תקשורת, אנטנות, לוויינים. פגיעה קינטית בתשתית הפיזית תפגע ביכולות הקיברנטיות, אולם יש להבחין בין נשק קינטי מסורתי, גם אם הוא מכוון נגד מטרה קיברנטית, לבין התופעה החדשה של נשק קיברנטי. כלי הנשק הקיברנטיים מורכבים בעיקר מתוכנה ולעתים גם מחומרה.

אפשר למיין את כלי הנשק הקיברנטיים לשלוש קבוצות:

- כלי התקפה מובהקים: תוכנות זדוניות (Malware) לסוגיהן (וירוסים, תולעים, סוסים טרויאניים, פצצות לוגיות וכיו"ב)[20] ופעולות למניעת גישה ושירות (Denial of Service).
- כלים דו־שימושיים: אמצעים לסקירת מערכי ההגנה של רשתות מחשב (Network Monitoring); סקירת פגיעויות מוכרות (Vulnerability Scanning); בדיקות חדירה (Penetration Testing); הצפנה (Encryption); הסוואה של תוכן ותקשורת.
- כלי הגנה מובהקים: "חומת אש" (Firewall); מערכי התאוששות מאסון (Disaster Recovery).

תורפות

נקודת תורפה היא מאפיין מובנה של מערכת, שניתן להגדירה כמאפיין המבני או הארגוני החלש יותר מבין כלל מאפייני המערכת. המונח "תורפה", כמו הביטוי "עקב אכילס" המתייחס לפגיעות גופנית סמויה, משמש בהשאלה בניתוח מערכות הנדסיות וצבאיות, וגם לשיח היום־יומי. בניתוח סיכונים, תורפה היא חלק ממשוואת הסיכון: סיכון הוא מכפלה של תורפה באיום ובתוצאה הצפויה. ניתוח מאפייני המרחב הקיברנטי שנסקרו לעיל מצביע על כמה נקודות תורפה.

תרשים 1: המרחב הקיברנטי – נקודות תורפה

מאפיין	תורפה
שינוי בקצב מהיר	התיישנות מהירה של אמצעים, כולל מערכות הגנה.
הוזלה מהירה של האמצעים	סף כניסה נמוך מביא לריבוי שחקנים משמעותיים.
מבנה הפרוטוקול TCP/IP	קשה לזהות את מקור האות שהגיע ברשת.
שימוש רחב בציוד מסחרי סטנדרטי, "מן המדף"	צמצום פערי היכולות בין השחקנים השונים. פגיעות בחומרה ומערכות הפעלה זהות מסכנות קשת רחבה של מערכות.
רמת סיבוכיות גבוהה	קשה להבדיל בין תקלה לתקיפה. קשה מאד לקשר בין אירוע לתוצאה.
א־סימטריות	לא נדרשת השקעה רבה בפיתוח אמצעי הלחימה והפעלתם. לעומת זאת, הגנה מפני איומים קיברנטיים חייבת להקיף את כל אפיקי התקיפה ולהתעדכן בקצב גבוה. מחיר ההגנה הולך ועולה.
חוקים מעורפלים	אין בעולם הגדרה משותפת של "מלחמה קיברנטית". קיים שוני רב בתחומי החוק בין מדינות שונות בנוגע לפשיעה קיברנטית.

הגנה

ההגנה מפני איום קיברנטי נגזרת מהמכנה המשותף הרחב שלו, שהוא חדירה בלתי מורשית למערכת ממוחשבת. לפיכך, ההגנה ממוקדת במאמצים טכנולוגיים לזהות חדירה בלתי מורשית, לאתר את מקור הבעיה, להעריך את הנזק הנגרם, למנוע התפשטות הנזק בתוך הרשת, ובמידת הצורך לשחזר את הנתונים והמחשבים שנפגעו. ההגנה מנסה לעמוד בנתיב הפריצה, לזהות ניסיון כזה ולסכל אותו על ידי מניעתו. לשם כך מופעלות מערכות מחשבים לניטור פעילות, העברת התקשורת,

חסימת דרכי גישה, הגבלת הרשאות, וידוא זהות, הצפנה, גיבוי והתאוששות מאסון וכיוצא באלה.

לכאורה, מדובר במאמץ כדאי. עם זאת, יש להכיר במגבלות ההגנה במרחב הקיברנטי. נפח הפעילות עצמו מציב את המתגונן בעמדת נחיתות. הביזור של משאבי מחשוב ורשתות מאתגר כל ניסיון לזהות את גבולות תחומי האחריות. מצב העניינים ברשתות ממודרות פשוט יותר: הגוף הממודר יודע שהרשת נמצאת בשליטתו וכי עליו לתחזק אותה ולהגן עליה. ברם, רשתות מסוג זה הולכות ומתמעטות (זו אחת הסיבות שמאמר זה אינו עוסק בנושא הרשתות הצבאיות והלוחמה האלקטרונית). שיעור הולך וגדל של מערכות תעשייתיות מנצל את יתרונות המחשוב, ובכך פותח פתח לפגיעות. התשתיות החיוניות הוכנסו אל המרחב הקיברנטי, וגם כוחות הביטחון משתמשים בתשתיות המסחריות לרוב התקשורת שלהם. לפיכך, הנטל על ההגנה הפאסיבית הולך וגדל.

התקפה

מאפייני המרחב הקיברנטי של היום מעניקים יתרון ברור להתקפה על פני ההגנה.[21] התקפה קיברנטית אינה כוללת פגיעה קינטית בתשתית הפיזית שעליה בנוי המרחב הקיברנטי. התקפה במרחב הקיברנטי משתמשת בכלים קיברנטיים, וכלי הנשק שלה הם תוכנה וחומרה.

לאור מאפייני המרחב הקיברנטי שהוצגו לעיל, עצם זיהוי ההתקפה הקיברנטית אינו דבר פשוט. תסמינים זהים משותפים לתקלות ולתוצאות אפשריות של חדירה בלתי מורשית למשאבי המחשב. חדירה כזו משמשת לכל קשת האיומים הקיברנטיים, וגישה בלתי מורשית למשאב הממוחשב יכולה לשמש לכל סוגי הפעולות, כך שקשה מאד להעריך את זהות החודר ומטרתו. זיהוי של חדירה ופסילת האפשרות של תקלה טכנית אינם מספיקים.

מלחמה קיברנטית

מלחמות מלוות את המין האנושי משחר ההיסטוריה. הניסיון ההרסני המצטבר הביא לשורה של הבנות שנועדו לצמצם את זוועות המלחמה: הקמת מוסדות בינלאומיים, גיבוש אמנות בינלאומיות שונות המסדירות את גבולות המותר במלחמה, הקמת ארגוני סיוע הומניטרי ומערכת משפט נגד פושעי מלחמה.

החדשנות של המרחב הקיברנטי וחוסר התאמתו למושגי היסוד מהעולם הפיזי גרמו לכך שלא התגבשה עד היום הגדרה של מושג המלחמה במרחב הקיברנטי. עם זאת, מתקיימים בעולם הרחב, וגם בישראל, דיונים בנושאי המלחמה בעידן המידע, לוחמת מחשבים ולוחמת מידע.[22]

אפשר לדרג את הפעילות העוינת במרחב הקיברנטי לפי סוגיה והנזק שהיא גורמת. להלן מוצע מיון כזה, המסודר בסדר חומרה יורד:

א. התקפה על מטרות אזרחיות שונות, הגורמת לנזק פיזי.
ב. שיבוש ופגיעה בתשתיות מידע לאומיות חיוניות, הגורמים לנזק פיזי לרכוש ולפגיעה במטרות צבאיות בשטח הריבוני של המדינה.
ג. שיבוש ופגיעה במטרות צבאיות מחוץ לשטח הריבוני של המדינה.
ד. החדרת כלי תקיפה רדומים: סוס טרויאני או פצצה לוגית העלולים להיות הכנות לתקיפה.
ה. פשע פלילי, ריגול תעשייתי.
ו. שימוש בכלי נשק דו־שימושיים: איסוף מודיעין, חיפוש "חורי אבטחה", בדיקות חדירה.
ז. ניהול מערכה תקשורתית, תעמולה, נאצה, השחתת אתרי אינטרנט רשמיים ייצוגיים.

הקושי בדיון על מלחמה קיברנטית נגזר מהבעייתיות שבמושגי ההתקפה, ההגנה והאלימות במרחב הקיברנטי. כדי לקבוע שתקיפה קיברנטית היא חלק ממלחמה, יש לבחון קיומם של כמה מאפיינים:

א. מקור ארגוני וגיאוגרפי: האם מדינת לאום עומדת מאחורי הפעולה?[23]
ב. תוצאה: האם ההתקפה יכולה הייתה לגרום נזק, והאם אכן גרמה נזק ונפגעים?
ג. מניע: האם אפשר לזהות מניע אידיאולוגי־פוליטי, מקרו־כלכלי או דתי למתקפה?
ד. רמת המורכבות: האם המתקפה דרשה תכנון מורכב ומשאבים מתואמים, הזמינים בעיקר למדינות?

לאור מאפייני המרחב הקיברנטי של היום, קיים קושי רב להגיע לתשובות ברורות לשאלות אלו, לא כל שכן לתשובות המספיקות לקביעת מדיניות.

הרתעה

המחקר בנושא ההרתעה מעסיק חוקרים במדע המדינה, בלימודי ביטחון, בתורת המשחקים, בכלכלה ובפסיכולוגיה. העולם הצליח להתמודד עד כה עם כלי הנשק הגרעיניים המסוגלים להחריב את כדור הארץ באמצעות הרתעה המבוססת על מכת נגד הרסנית וודאית.

מודל ההרתעה שפעל היטב בתקופת המלחמה הקרה אינו ישים לשדה הקרב הקיברנטי. הסיבה העיקרית לכך היא המבנה של המרחב הקיברנטי היום, הגורם לחוסר יכולת לזהות בוודאות מקרה של תקיפה ולחוסר יכולת לאתר במהירות את

מקורו וזהותו של התוקף.[24] בהעדר יכולת ליצור הרתעה מפני תקיפה קיברנטית, המבוססת על גביית מחיר כבד מהתוקף, ההרתעה במרחב הקיברנטי צריכה להתבסס על מניעת הישג מהתוקף. לפיכך, חיוני להשקיע במחקר ממוקד בהרתעה מסוג זה כדי לצמצם את הסכנות לביטחון הלאומי.[25]

איומים: סקירה, מיון וניתוח

שחקנים רבים בעלי פוטנציאל של איום פועלים במרחב הקיברנטי. השחקנים שיוצגו להלן קיימים ופועלים מזה שנים במרחב זה:

א. Hacktivists. אלה יחידים התוקפים אתרי אינטרנט כדי להשתיל בהם מסר פוליטי, או פועלים לשבירת מנגנוני צנזורה וחשיפת סודות.

ב. פורצים (Hackers) – יחידים הפורצים מרחוק למערכת ממוחשבת באמצעות רשת תקשורת.

ג. כותבי תוכנה זדונית, מפיצי דוא"ל זבל ואוספי נתונים אישיים של משתמשים.

ד. מפעילי רשת של "מחשבים שבויים" (Botnet Herder). גם האקרים אלה פורצים מרחוק למחשבים באמצעות רשת תקשורת, אולם הם משיגים שליטה חלקית במחשבים רבים נוספים במטרה להפוך אותם בלא ידיעתם לכלים לביצוע משימה עתידית. בשנים האחרונות התפתחו והתרחבו יכולות התקיפה של רשתות עד כדי רבבות ואף מיליוני מחשבים.

ה. ארגוני פשע מאורגן משתמשים בהאקרים, ובעיקר במפעילי רשתות שבויות, למטרות רווח: גניבת זהות, הונאה, דואר זבל, פורנוגרפיה, הסוואת פעילות פלילית, הלבנות הון וכיו"ב.

ו. עובדים המשתייכים לחוגים הפנימיים של ארגון סגור (Insider Threat). רשתות המחשב של ארגונים ממודרים מופרדות מהרשת הכללית כדי להקשות על פריצה לתוכן. במצב כזה, גיוס עובד ממורמר הוא דרך טובה לחדור אל הרשת הממודרת. פורץ המזהה מכשולים טכניים עשוי לנצל עובדים תמימים של ארגון המטרה באמצעות מניפולציה חברתית (Social Engineering).

ז. שירותי ביטחון ומודיעין מאמצים כלים של המרחב הקיברנטי להשגת מטרתם. טכנולוגיות המידע מעניקות למרגלים מגוון רחב של אמצעים ודרכים לביצוע המשימה.

ח. גורמים חבלניים מנצלים גם את המרחב הקיברנטי כדי להעביר מסרים מוצפנים, לגייס תומכים, לרכוש מטרות, לאסוף מודיעין, להסוות פעילות וכיו"ב.

מהי מערכת חשובה לביטחון הלאומי? אין מדד טכני להערכת חיוניות של מערכת ממוחשבת ברמה הלאומית, שיכול להתקיים במנותק ממכלול הערכים, היעדים והכוחות החברתיים המשתמשים בה. לפיכך, מידת החשיבות היחסית של מערכת ממוחשבת, וכתוצאה מכך מידת ההשקעה הציבורית הנדרשת להגנתה,

נתונות לדיון ציבורי ולמאבק פוליטי. תשתיות לאומיות (ייצור ואספקת אנרגיה ומזון, תחבורה יבשתית ואווירית, משק מים וביוב, מערכות התקשורת וכיוצא באלה) היו קיימות בחברות המפותחות גם קודם להופעת המחשב ושימשו לרוב כמטרות אסטרטגיות בעימותים בינלאומיים. תשומת הלב לה הן זוכות בדיון על המרחב הקיברנטי נובעת משני גורמים עיקריים:

א. ראשית, עם חדירת המחשבים והתקשורת לכל תחומי החיים, המרחב הקיברנטי עצמו הפך להיות חיוני לתפקוד מלא של המדינות המפותחות. מרחב זה משול למערכת העצבים של הגוף. לפיכך, אבטחת פעולה תקינה ובלתי מופרעת שלו, יחד עם מתן יכולת גישה אליו לכל שכבות האוכלוסייה, הפכו להיות חיוניים.[26]

ב. שנית, עם התפתחות המחשוב שובצו המחשבים במערכות הייצור, השליטה והבקרה של התעשיות המסורתיות. השכבה הקיברנטית בעלת רמת הסיבוכיות הגבוהה נוספה על המערכות ההנדסיות המורכבות ממילא, והתשתיות הוותיקות הוכנסו אל תוך המרחב הקיברנטי.[27] בכך הן הפכו להיות פגיעות לנקודות התורפה של מרחב זה. לראשונה נוצר פוטנציאל להגיע אל היעדים המוגנים באמצעות ממד התקשורת והתוכנה, שאינו תלוי במיגון במרחב הפיזי. חיבור התשתיות החיוניות למרחב הקיברנטי חושף אותן לנקודות התורפה הקיברנטיות, ומכאן שנוצר פוטנציאל לפגוע ישירות במטרות החיוניות של המדינה על ידי ניצול נקודות התורפה הללו. האיום המהותי הוא פגיעה בתפקוד הפיזי של התשתיות החיוניות באמצעים קיברנטיים, תוך עקיפת מערכות ההגנה הצבאיות השומרות על המרחב הפיזי, הסתרת זהות המפַגע, ולבסוף הימנעות מתגובה ומעימות מזוין.

בנקודות התורפה של המרחב הקיברנטי, איום הוא מרכיב במשוואת הסיכון. איום מתאפשר על ידי ניצול נקודות תורפה ומכוון לשבש מערכת או לפגוע בנכסי האויב. כדי להבין טוב יותר את שדה הקרב הקיברנטי, ראוי לסקור גישות שונות להמשגת האיומים. אפשר להבחין בין איומים על המרחב הקיברנטי (risks *to* cyberspace), שנועדו לפגוע בתשתית הקיברנטית, ובין איומים שמשתמשים במרחב הקיברנטי אך לא פוגעים בו (risks *through* cyberspace).[28]

הגנה מפני הסוג הראשון של איום – על המרחב הקיברנטי – מכונה Critical Information Infrastructure Protection או "הגנה על תשתיות מידע חיוניות". "תשתית מידע חיונית" היא מערכת בעלת ממד ממוחשב, השולטת בתפקוד מערכת פיזית אחרת החיונית לתפקוד המשק ולביטחון המדינה. ההגנה על תשתיות מסוג זה מסתמנת כנדבך מרכזי בדיון על ההשלכות הביטחוניות של הופעת המרחב הקיברנטי. לעתים קרובות משמיטים את המילה "מידע" ומדברים על הגנה על "תשתית קריטית".

הסוג השני של איום – דרך המרחב הקיברנטי – כולל מגוון פעולות שהתאפשרו באמצעות מרחב זה: תקשורת מוצפנת להתנגדות פוליטית, להנחיית פעולות טרור או לפשע בינלאומי; פשיעה מסורתית (הונאה, גניבה, פדופיליה) המועצמת בידי רשתות המחשב; פשיעה חדשה הייחודית למרחב הקיברנטי: ריגול ממוחשב, פגיעה באספקת שירותי רשת, שימוש בתוכנות זדוניות למטרות מגוונות.

אפשר להבחין בין האיומים לפי מקורם הגיאוגרפי: מחוץ לגבולות המדינה או מתוכם, מחוץ לרשת המחשבים או מתוכה. המבנה הנוכחי של פרוטוקול התקשורת האינטרנטי, הארכיטקטורה הפתוחה של הרשת ופגיעויות מובנות בתוכנה ובחומרה, הופכים את מלאכת איתור המקור הגיאוגרפי לכמעט בלתי אפשרית. בדרך כלל, הנתיב של חבילות מידע המועברות ברשת אינו קבוע, והתחנות בדרך אינן נדרשות לבחון את תוכן המידע או את מקורו וגם לא לתעד את מסלול חבילות המידע. חשוב לציין שאין מדובר במאפיין הכרחי של המרחב הקיברנטי, אלא בתוצאה של מדיניות המעודדת פתיחות בגישה למידע ותקשורת חופשית. מדיניות זו מושרשת באידיאולוגיה ליברלית של חלוצי הרשת האמריקאיים. עם הפרטת תעשיות המידע ומסחורן, אידיאולוגיית השוק החופשי, הנרתעת מכל מעורבות מדינתית, מקשה על עצם הדיון בהסדרה טכנית ומשפטית שונה של המרחב הקיברנטי.

אפשר למיין את האיומים גם בהתאם למטרת המאיים: פשע, טרור, ריגול תעשייתי, ריגול צבאי ולוחמה קיברנטית. אלא שמיון כזה מתעלם מהעובדה ששיטת פעולה זהה יכולה לשמש למטרות רבות. בנוסף לכך, מיון כזה הוא בעייתי, לאור הקושי הרב להתחקות אחר מקור האות האלקטרוני שעובר במרחב הקיברנטי ואחר זהות שולחיו.

הערכת האיום הקיברנטי

הדיון בסוגי האיומים ובשיטות המיון שלהם מאפשר להבחין בקווים משותפים המאפיינים אותם: גישה בלתי מורשית למשאבי מידע ממוחשבים משותפת לכול סוג של איום קיברנטי. אולם החדירה הבלתי מורשית למשאבי מידע ממוחשבים פותחת קשת רחבה של תוצאות אפשריות, המעלות מצדן שורה של שאלות: מהי מידת האיום הנשקפת מהשחקנים השונים? האם כל השחקנים והאיומים רלוונטיים לביטחון הלאומי? כיצד נוכל להעריך את חשיבותם ולתעדף את מדיניות התגובה? כדי לספק תשובות רציניות לשאלות אלו יש צורך לא רק בדיון מושכל במושגים ובהבנה טכנית של עולם המחשוב, אלא גם בדיון ציבורי מעמיק.

הערכת סיכונים (Risk Assessment) היא תחום עיסוק רחב ומגוון, המשמש מקצועות שונים. דיון מקצועי בתחום זה חורג מגבולות המאמר. לצורך הדיון

בסוגיית האיום הקיברנטי נגדיר את הערכת האיום כמכפלה של סבירות התרחשות המאורע בהערכת הנזק הנגרם בו.

עיצוב מדיניות ציבורית מחייב להעריך את האיום, ולמעשה את התרחיש המעורר את הצורך במדיניות. אולם, לא קיימת אפשרות להערכה חד־משמעית, מדויקת ואובייקטיבית של איום כזה. הערכת האיום ברמה הלאומית מחייבת התייחסות לערכים החברתיים והתרבותיים של המדינה והחברה, המנחים את החשיבות היחסית של תרחישים ואיומים פוטנציאליים על אותה חברה. הערכה כזאת היא תמיד הערכה סובייקטיבית, אולם היא הדרך ההולמת ביותר לנהל תהליך של עיצוב מדיניות. במדינה דמוקרטית, המוסדות הייצוגיים והתקשורת משמשים אפיק לציבור להשמיע את קולו ולהשפיע על הביטחון הלאומי, על הרווחה ועל סוגיות נוספות.

חשוב לזכור כי בנושא הביטחון הלאומי הקיברנטי אין למומחים הטכניים בלעדיות על הערכת התרחישים וקביעת המדיניות. כפי שאין לתת לכלכלנים לקבוע את תקציב המדינה לבדם, כך אין להפקיד את הביטחון הקיברנטי אך ורק בידי אנשי המחשבים.

כאשר מנתחים את חשיבות המרחב הקיברנטי במסגרת רעיונית של מלחמה, היחס אליו ידמה מאד ליחס לכל מערכת נשק חדשה. כדי להעריך את משקלו היחסי של האיום הקיברנטי במסגרת המלחמה, יש לבחון את המשתנים הרגילים, כגון טווח יעיל, מידת ההרס של פגיעה, עלות השימוש, מגבלות פוליטיות על שימוש וכיו"ב.

לאיום הקיברנטי פוטנציאל להתממש במנותק מהמערכת המסורתית. המרחב הקיברנטי, כפי שהוא קיים כיום, מהווה שדה מערכה פרוץ. בניגוד לחלל, לאוויר, ליבשה או לים, ארגוני הביטחון הקיימים נמצאים רק בתחילת תפקודם במרחב הזה.

במרחב הקיברנטי קיים פוטנציאל קריטי לערער את הביטחון הלאומי, תוך עקיפה של מסגרות ההגנה הלאומיות המסורתיות ופגיעה ישירה במטרות חיוניות בעורף. עצם קיומו של המרחב הקיברנטי מאפשר העברת מידע ישירה, תוך התעלמות מגבולות מדיניים וגיאוגרפיים וממערכי ההגנה. בכך, המרחב הקיברנטי המתפתח יוצר שינוי אסטרטגי בעיסוק בביטחון הלאומי.

תרשים 2 מציע סיכום סכמטי של סוגי האיום הקיברנטי לפי רמת החדשנות, סבירות ההתרחשות ואפקט האיום.

תרשים 2: סוגי האיום הקיברנטי לפי רמת החדשנות, סבירות ההתרחשות ואפקט האיום

סוג האיום	רמת החדשנות	סבירות ההתרחשות	אפקט האיום
פגיעה ביכולת התפקוד של כוחות הביטחון	בינוני (איום ותיק יחסית)	עולה (אפשרויות טכנולוגיות נפוצות)	מועצם
ריגול ביטחוני	בינוני (איום ותיק יחסית)	סביר (אפשרויות טכנולוגיות נפוצות)	מועצם
ריגול תעשייתי, פיננסי, מדעי	בינוני (איום ותיק יחסית)	עולה (אפשרויות טכנולוגיות נפוצות)	מועצם (חשיבות גבוהה לחדשנות)
פגיעה ישירה בשירותי המדינה החיוניים	**חדש** (לא היה אפשרי בעבר)	עולה (אפשרויות טכנולוגיות חדשות)	**מועצם מאד**
מלחמה קיברנטית מלאה	חדש (לא היה אפשרי בעבר)	נמוכה (עלות־תועלת נמוכה לעומת מלחמה קינטית)	בינוני

סיכום: מאפיינים אסטרטגיים של ביטחון לאומי במרחב הקיברנטי

מאמר זה נועד להמשיג את תחום הביטחון הקיברנטי המתפתח וליצור שפה משותפת לדיון ציבורי פורה בישראל בתחום זה. לאור חוסר הבהירות המושגית, המאמר הציע ביאורים והגדרות אופרטיביות לנושאים החדשניים הקשורים במרחב הקיברנטי. נסקרו בו מאפייני המרחב, נקודות התורפה ואיומים קיימים, והוצגו בעיות ההגנה, ההתקפה וההרתעה הקיימות במרחב זה.

לוחמה קיברנטית מאפשרת לפגוע מרחוק במטרות טקטיות ואסטרטגיות, תוך סיכון נמוך לתוקף. הסיכון הנמוך לתוקף נובע ממאפייני המרחב הקיברנטי כיום: קושי להבדיל בין תקלה לתקיפה; קושי לקשר בין אירוע לתוצאה; קושי להתחקות אחר מקור הפגיעה ולזהות את התוקף; שימוש רחב בטכנולוגיות זולות "מן המדף"; פגיעוּיות רבות של מערכות ממוחשבות.

האיום הקיברנטי הוא א־סימטרי: לא נדרשת השקעה רבה בפיתוח אמצעי הלחימה והפעלתם. לעומת זאת, ההגנה מפני איומים קיברנטיים חייבת להקיף

את כל אפיקי התקיפה ולהתעדכן בפיתוחים חדשים. לפיכך, מחיר ההגנה מפני איומים קיברנטיים עולה כל הזמן.[29]

המאמר הציג כמה ממאפייני המרחב הקיברנטי בהקשר לביטחון הלאומי. האם האיומים הקיברנטיים שנסקרו מאיימים על הביטחון הלאומי של מדינת ישראל? חלק משמעותי מהתשובה נגזר מתפיסת תפקידו של מוסד המדינה וחורג ממסגרת מאמר זה, שלא נועד לספק תשובה לשאלות המהותיות והמטרידות המתעוררות עם התפתחות המרחב הקיברנטי. במדינה פתוחה ודמוקרטית, התשובות לשאלות מסוג זה מתגבשות באמצעות דיון ציבורי ותהליך פוליטי. המאמר נועד אכן לתרום לדיון ציבורי מושכל כזה בישראל, ולמקד את תשומת לבה של המערכת הפוליטית בסוגיות חדשות אלו בביטחון הלאומי.

המעט שניתן לומר בהקשר זה כבר עתה הוא, שעל המדינה מוטלת האחריות לביטחון לאומי גם כששדה המשחק מתפתח ומשנה צורה. עידן המידע גורם לשינויים מרחיקי לכת גם בהיבטי הביטחון הלאומי. כל מערכת מחשב חשופה לפגיעה. אין מערכת חסינה בפני פגיעה או תקלה, וחשוב להכיר בכך כדי להשתחרר משאיפה עקרה לביטחון מוחלט. עם זאת, הכרחי לשאוף לביטחון מיטבי, תוך התאמה למאפייני האיום והיעד.

מענה לאיום הביטחוני הקיברנטי ברמה הלאומית צריך להיות מותאם למאפייניו המיוחדים. כדי לעצב מדיניות ההולמת את צרכי המדינה, נדרשים דיון ציבורי ומחקר מקצועי. יש, אפוא, לרתום את שיטות העבודה המדעיות והארגוניות כדי שניתן יהיה לספק ביטחון בעידן המידע ולהתמודד בדרך הטובה ביותר עם האיום הקיברנטי.

הערות

1 ירידה בלפחות שלושה סדרי גודל בין ראשית שנות השבעים לאמצע שנות האלפיים. במדד מחיר ל־GigaFLOP, יחידה שעלתה 15 מיליון דולר ב־1984 עלתה 0.14 דולר ב־2009. במדד מחיר נפח האחסון על מדיה מגנטית, מחיר ל־Gigabyte ב־1993 היה 1,000 דולר וב־2009 – 0.02 דולר.

2 לדיון ב"מהפכה בעניינים צבאיים" (Information-Technology Revolution in Military Affairs – IT RMA) ראו: 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, D.C.: National Defense University Press, 1995;

3 יצחק בן־ישראל, "ביטחון, טכנולוגיה ושדה הקרב העתידי", בתוך: חגי גולן (עורך), **מרקם הביטחון**, תל אביב, מערכות, 2001, עמ' 269–327.

4 משחר ההיסטוריה שאפו בני האדם לשרוד ולהתפתח במרחבים הפיזיים הסובבים אותם, ובראש ובראשונה במרחב הפיזי המיידי: מביוּת החיות והחקלאות, דרך בנייה וכלה בשליטה בחומרי הגלם ועיבודם בשיטות מכאניות, כימיות וכד'. מאז המהפכה המדעית למדו החברות המפותחות לתמרן, ולעתים אף לשלוט, בסביבתן בסיוע השיטה המדעית. המרחב היבשתי משך באופן טבעי את מרב המאמצים. המרחב הימי נכבש בידי ציוויליזציות שונות לאורך ההיסטוריה, והמדינות שהשכילו לשלוט

ראשונות במרחב זה זכו לרווחה ולעדנה ארוכות שנים. המרחב האווירי נכבש במאה השנים האחרונות, וגם השולטים בו זכו ביתרון יחסי אדיר על פני מתחריהם. מאז שנות החמישים של המאה הקודמת ושיגור הלוויין הראשון ב־1957, מתקיימת תחרות בין המעצמות על פיתוח אמצעים להגעה ושהייה בחלל ובכוכבי הלכת הקרובים. ראו: יצחק בן־ישראל, "מלהב החרב אל זיכרון המחשב", **אודיסיאה**, גיליון 9, אוקטובר 2010.

5 Andrew M. Colman, *A Dictionary of Psychology*, "Cyberspace", Oxford University Press, 2009, *Oxford Reference Online*, Oxford University Press, http://www.oxfordreference.com/views/ENTRY.html?subview=Main&entry=t87.e2037

6 Julia Cresswell, *Oxford Dictionary of Word Origins*, "Cybernetics", *Oxford Reference Online*, Oxford University Press, http://www.oxfordreference.com/views/ENTRY.html?subview=Main&entry=t292.e1374 .

7 Norbert Wiener, *Cybernetics or Control and Communication in the Animal and the Machine*, New York: John Wiley and Sons, 1955.

8 *Encyclopædia Britannica 2010*, "Space", *Encyclopædia Britannica Online*, http://www.britannica.com/EBchecked/topic/557313/space.

9 האינטרנט הוא רשת פתוחה של נקודות קצה, התקנים ורשתות מחשב, המדברים ביניהם בפרוטוקול תקשורת IP או TCP. רשת האינטרנט בנויה בצורה פתוחה ומבוזרת, ומכל נקודת קצה בה ניתן לתקשר עם כל נקודת קצה אחרת. על גבי העיצוב הבסיסי הזה נוצרו אין ספור יישומים, ובתוכם גם כאלה שנועדו להגביל גישה ולוודא זהות, להצפין את המידע המועבר ברשת, לוודא קבלת המידע ועוד.

10 "World Internet Usage Statistics News and World Population Stats" .*ITU, Itu World, Telecommunication/Ict Indicators Database,* 2010

11 למשל: GPS, ACARS, SWIFT, GSM Cellular ועוד אלפי רשתות מחשב ייעודיות.

12 Martin C. Libicki, *Cyberdeterrence and Cyberwar*, RAND Corporation, Santa Monica, CA., 2009.

13 אלקטרוניקה היא התשתית של עולם המחשוב כיום. אולם לפני האלקטרוניקה היו מחשבים מכאניים. האלקטרוניקה לא חסינה בפני העתיד: הוכחה כבר האפשרות לנצל תשתיות ביולוגיות לצרכי המחשוב. מחשוב DNA משתמש בביולוגיה מולקולארית ו־DNA במקום הרכיבים האלקטרוניים. אפשרות נוספת היא מחשוב פֶּפְּטִידִי (Peptide): מחשוב ביו־מולקולארי המבוסס על תרכובת העשויה משתי חומצות אמינו לפחות.

14 החלוצים דוגמת ריינהולד או בארלו ראו ברשת האינטרנט מערכת פתוחה, לא היררכית, וגם אנטי־ממסדית. הם תלו בה תקוות שתאפשר קהילה וארגון שיתופיים ושוויוניים: John Perry Barlow, "A Declaration of the Independence of Cyberspace". לורנס לסיג מתאר את עקרון הפעולה של רשת האינטרנט כלהלן: "Like a daydreaming postal worker, the network simply moves the data and leaves interpretation of the data to the applications at either end. This minimalism in design is intentional. It reflects both a political decision about disabling control and a technological decision about optimal network design", Lawrence Lessig, *Code and Other Laws of Cyberspace*, New York: Basic Books, 1999.
המציאות הקיימת מורכבת יותר. לדיון במבנה השליטה ברשת האינטרנט ראו: Jack L. Goldsmith and Tim Wu, *Who Controls the Internet?: Illusions of a Borderless World*, New York: Oxford University Press, 2006.

15 האינדוקציה (הסקה מן הפרט אל הכלל) היא כלי נפוץ מאד, אך בעל מגבלה לוגית מובנית: תצפית על מאורע וחזרתו על עצמו אינה מאפשרת היסק לוגי תקף שהמאורע הזה מחויב המציאות. בעיית האינדוקציה היא שלהיסק מהפרט אל הכלל אין תוקף הכרחי.

16 קורא חד עין יכול לזהות דמיון בין ההגדרה שהצעתי כאן להגדרות המופיעות במסמכים רשמיים של זרועות הממשל השונות של ארצות הברית. הדמיון אינו מקרי: ארצות הברית וישראל חולקות ערכים משמעותיים, הן בעלות רמה מדעית וכלכלית דומה, ולכן גם רואות ומפרשות את המציאות בכלים דומים. ארצות הברית מובילה את המחקר והפיתוח המדעי־טכנולוגי העולמי, ובמקביל מובילה בעיסוק במדיניות בנושאים הקיברנטיים. מחקר השוואתי, הכולל מדינות כמו סין, רוסיה, הודו, צרפת ואחרות, יזהה הגדרות שונות עד מאד. אולם, מחקר כזה חורג מגבולות מאמר זה.

17 תוקידידס, **תולדות מלחמת פלופוניס**, ירושלים: מוסד ביאליק, 1988. התיאוריה הריאליסטית של יחסים בינלאומיים מגייסת את תולדות יוון העתיקה להבנת טבע האדם והאנרכיה הבינלאומית, המנחים את ההתרחשויות בנות זמננו: Steven Forde, "International Realism and the Science of Politics: Thucydides, Machiavelli and Neorealism", *International Studies Quarterly,* Vol. 39, No. 2, 1995; Azar Gat, *War in Human Civilization*, Oxford, New York: Oxford University Press, 2006.

18 ב־1996 נוסדה "המועצה הנשיאותית לתשתיות חיוניות" (The Presidential Critical Infrastructure Board).

19 President Barack Obama, May 29, 2009 http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/

20 להלן הצעת תרגום לעברית של המונחים האנגליים בתחום הלוחמה הקיברנטית: Malware– תוֹקעה: תוכנה זדונית המיועדת לשבש בסתר פעילות תקינה של מערכת ממוחשבת, וכך לפגוע בתהליך שמנוהל באמצעות אותה מערכת; Spyware – רוֹגלה: תוכנה זדונית המיועדת לאסוף נתונים בסתר ולעתים להעביר אותם ברשת; Phishing – דיוּג: תרמית מבוססת תוכנה והנדסה חברתית במטרה להשיג במרמה נתונים אישיים של משתמשים.

21 William Lynn III, "Defending a New Domain", *Foreign Affairs,* Vol. 89, No. 5, 2010.

22 יצחק בן־ישראל, "לוחמת מידע", **מערכות**, 369, פברואר 2000, עמ' 18–25.

23 לאחר פיגועי 11 בספטמבר 2001 בארצות הברית, סף התמיכה המדינתי הוּרד: כיום די בראיות נסיבתיות, כמו תמיכה אידיאולוגית באויב או מתן שירות לוגיסטי למחבלים.

24 Lynn III, Ibid.

25 Libicki, Ibid.

26 בצרפת, בפינלנד, באסטוניה וביוון הכירו מוסדות שלטוניים שונים בזכות הגישה לרשת האינטרנט כזכות יסוד.

27 יש לראות בכך תופעה צפויה: התפתחות טכנולוגיות המידע עשויה לשנות עד היסוד תחומי עיסוק קיימים. כפי שכותב העתידן והיזם ריי קורצוויל, בדרך זו השתנתה הפרדיגמה של המחקר הביולוגי מניסויים מסורתיים לחישוביות וסימולציה.

28 Ronald J. Deibert and Rafal Rohozinski, "Risking Security: Policies and Paradoxes of Cyberspace Security", *International Political Sociology,* Vol. 4, No. 1, 2010.

29 הטיעון של קושי ההגנה נגד איומים קיברנטיים דומה לטיעון נגד הגנה אקטיבית מפני טילים ולוויכוח בנושא "כיפת ברזל". הוא דומה גם לטיעון על עקרוּת ההגנה נגד מחבל מתאבד. על אף הטיעונים הללו, ההתפתחות המדעית מסייעת לייצר מענים לאיומים החדשים. ראו: ליאור טבנסקי, **המאבק בטרור בעידן המידע, "אינתיפאדת המתאבדים" וההתמודדות הישראלית עמה בסיוע טכנולוגיות עילית**, אוניברסיטת תל אביב, תל אביב, 2006.