המרחב הקיברנטי והשדה הביטחוני – מסגרת מושגית
משמעויות ביטחוניות לישראל

שמואל אבן ודוד סימן טוב

המונח "מרחב קיברנטי" מגדיר תופעה, שראשיתה בהמצאת הטלגרף בשנת 1844, שעיקרה ניצול השדה האלקטרומגנטי לצרכים אנושיים באמצעות טכנולוגיה. נקודת ציון מהותית בהתפתחות המרחב הקיברנטי הייתה המצאת המחשב הספרתי בשנת 1949. אבני דרך נוספות היו למשל: חיבור בין רשתות תקשורת לבין מחשבים ולמכונות שהחל בשנות השבעים של המאה העשרים; שימוש המוני ברשת האינטרנט ובמחשבים אישיים מאמצע שנות התשעים של המאה העשרים; אינטגרציה מקיפה בין מערכות מחשב למערכות תקשורת ולמכונות למיניהן (בתעשייה, בתחבורה ועוד), שימוש המוני במחשבי כף־יד סלולאריים, שגשוג הרשתות החברתיות באינטרנט ועוד, בעשור האחרון. כל אלה שינו את פני החברה והמשק.

טכנולוגיות המידע והמרחב הקיברנטי משנים במהירות גם את פניו של שדה הקרב המודרני. דוגמה אחת לכך היא הטכנולוגיות המתקדמות של שדה הקרב, כגון: מערכות בינה, שיתוף במידע, היתוך מידע, ניצול לוויינים בשדה הקרב, הפעלת כלים אוטונומיים, שילוב בזמן אמת של חיישנים המזהים מטרות עם מערכות אש ועוד. התפתחות המרחב הקיברנטי הביאה לסיקור אזרחי נרחב של זירת הלחימה, בין היתר באמצעות מכשירי סלולאר ניידים, המקנים לכל נוכח בזירה יכולת לתעד מידע, או לחלופין לבצע מניפולציות במידע. מידע זה מועבר מיידית ברשתות האינטרנט, מחולל דיונים ברשתות חברתיות ומשפיע על דעת קהל. כך נהפכו זירות לחימה למרחב שבו הציבור הוא שחקן מרכזי, המפעיל – יותר מבעבר – את השפעתו על עמדות מדיניות של ממשלות ושל מוסדות בינלאומיים, לעיתים על בסיס מידע מגמתי. לתופעה זו יש משמעויות מרחיקות לכת בכל הקשור להפעלת כוח צבאי. היא מגבילה את היכולת להפעיל כוח, אך גם יכולה לתרום לגיוס דעת קהל לשם הפעלת כוח.

הגדרות

למרחב הקיברנטי, המכונה גם מרחב הסייבר (Cyberspace), יש כמה הגדרות, שלהן רבדים משותפים.

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

סוכנות האו"ם ITU (International Telecommunication Union) מגדירה את המרחב הקיברנטי כדלהלן: המתחם הפיזי והלא פיזי, שנוצר או מורכב מחלק או מכל הגורמים הבאים: מחשבים, מערכות ממוכנות ורשתות, תוכנות, מידע ממוחשב, תוכן, נתוני תעבורה ובקרה והמשתמשים בכל אלה.[1]

מהגדרה זו עולה שהמרחב הקיברנטי מכיל שלושה רבדים התלויים זה בזה:

א. רובד אנושי: המשתמשים בתקשוב (תקשורת ומחשבים).[2]
ב. רובד לוגי: רובד התוכנות והביטים. אלה נעים במהירות האור ומייצגים מידע, הוראות, נכסים קיברנטיים (כגון תוכנות בעלות ערך, כסף אלקטרוני), תוכנות זדוניות (למשל סוסים טרויאניים) ועוד.
ג. רובד פיזי: הרכיבים הפיזיים של הרשת: חומרה, תשתיות ניידות ותשתיות נייחות; המצויים במרחבי היבשה, הים, האוויר והחלל (להלן "המרחבים הפיזיים").

למרחב הקיברנטי הגדרות נוספות. הגם שכולן מכירות בכל שלושת הרבדים (האנושי, הלוגי והפיזי) שלעיל, כל אחת מייחדת את הגדרת המונח "המרחב הקיברנטי" (Cyberspace) באמצעות חלק מהרבדים בלבד.

במסמכי צבא ארצות־הברית מוגדר המרחב הקיברנטי בהקשר לרובד השני (הלוגי) והשלישי (הפיזי), כדלהלן: "מרחב גלובלי בתוך סביבת המידע, המורכב מרשתות הנשענות על תשתיות טכנולוגיות המידע, התלויות אלה באלה, ובכלל זה האינטרנט, רשתות טלקומוניקציה, מערכות מחשבים, מעבדים, שבבים ובקרים". עוד נאמר, שהמרחב הקיברנטי הוא המרחב החמישי (נוסף על מרחבי היבשה, האוויר, הים והחלל), וכי בין המרחבים מתקיימים יחסי גומלין: המרחב הקיברנטי שוכן פיזית בכל אחד מהמרחבים האחרים, מקשר ביניהם ומעצים את יכולות הפעולה בהם, ואילו הפעילויות בהם מתבטאות במרחב הקיברנטי.[3]

משרד הקבינט הבריטי מגדיר (במסמך "אסטרטגיה של בריטניה לביטחון המרחב הקיברנטי") את המרחב הקיברנטי כך: "מרחב המקיף את כל צורות רשתות התקשורת והפעילות הדיגיטלית; בכלל זה הפעילות והתכנים המועברים ברשתות התקשורת הדיגיטליות".[4] הגדרה זו שמה במרכז את הרובד הלוגי.

משרד הפנים של גרמניה מגדיר (במסמך "האסטרטגיה של גרמניה לביטחון המרחב הקיברנטי") את המרחב הקיברנטי באופן מצומצם יחסית, כדלהלן: "המרחב הווירטואלי של כל מערכות המידע, המקושרות ביניהן ברמה הגלובלית. האינטרנט הוא הבסיס למרחב הקיברנטי, ואליו מקושרות רשתות נתונים נוספות". לפי הגדרה זו, מערכות מידע מבודדות אינן חלק מהמרחב הקיברנטי.[5]

בשונה מהגדרות הרואות את המרחב הקיברנטי כממד חמישי, קיימת גישה ולפיה המרחב הקיברנטי הוא אחד משבעה מרחבים, בצד האוויר, חלל, ים, יבשה, המרחב האלקטרומגנטי והמרחב האנושי. להבדיל מההגדרות הקודמות, גישה זו מבחינה בין המרחב הקיברנטי לבין המרחב האלקטרומגנטי ומונה את הרובד האנושי כמרחב בפני

עצמו.[6] המרחב הקיברנטי הוא מרחב מלאכותי הממומש באמצעות המרחב האלקטרומגנטי ומתממשק עם המרחבים הפיזיים באמצעות סנסורים (חיישנים) ואפקטורים (רכיבים מפעילים). ככזה, משמש המרחב הקיברנטי להעצמה פונקציונלית של מערכות אזרחיות וצבאיות הפועלות בכל המרחבים ובה בעת הוא חושף אותן לתקיפה קיברנטית.[7]

המכנה המובהק המשותף בין כל ההגדרות הוא הרובד הלוגי. השוני בין ההגדרות משקף כנראה את הדגשים של כל מדינה ושל כל ארגון בבואם להתמודד עם האתגרים במרחב הקיברנטי. נראה שההבדלים בהגדרות אינם משקפים הבנה שונה של התחום הקיברנטי, שכן כאמור כל בעלי ההגדרות מכירים בקיומם של שלושת הרבדים המופיעים בהגדרת האו"ם. אל רבדים אלו נתייחס בהמשך.

מאפייני המרחב הקיברנטי כמרחב לחימה

בכל אחד מהרבדים (האנושי, הלוגי והפיזי) המופיעים בהגדרת האו"ם קיימים סוגי פעולות ביטחוניות הנוגעות למרחב הקיברנטי. למשל:

א. פעולות במרחב הקיברנטי שמכוונות לרובד האנושי, ומטרתן לשנות את התנהגותו של האדם המשתמש. בין אלה העברת מסרי מידע (גלויים או סמויים) ליריב באמצעות המרחב הקיברנטי.

ב. חדירות לוגיות (באמצעות תוכנות) למטרות כגון ריגול, תקיפת מחשבים של היריב כדי למנוע את התועלת שהוא מפיק במרחב הקיברנטי ותקיפת מכונות ומתקנים במרחבים הפיזיים הנשלטים מהמרחב הקיברנטי. לדוגמה, שיבוש מנגנון בקרה תרמי, שיוביל לפיצוץ מפעל ביטחוני (אפקט במרחב היבשתי), או שיבוש מד גובה, שיוביל לפגיעה בכלי טיס (אפקט במרחב האוויר). במקרה זה המרחב הקיברנטי של היריב הופך כלי בשירות התוקף, ועל כן הוא עשוי להימנע מפגיעה במערכות התקשוב של היריב.

ג. ברובד הפיזי – פגיעה בחומרה, שעליה נשען הרובד הלוגי, וכן פעולות מחוץ למרחב הקיברנטי נגד תשתיות שהמרחב נשען עליהן. למשל, פעולות באש ולוחמה אלקטרונית שמטרתן לפגוע או לשתק רכיבי תקשורת ומערכות אנרגיה, שהמרחב הקיברנטי תלוי בהם.

על מאפייני המרחב הקיברנטי כמרחב לחימה אפשר ללמוד מהתייחסויות של בכירים במערכת הביטחון של ארצות־הברית. עם אלה נמנות: מאמר שפירסם סגן מזכיר ההגנה ויליאם לין באוגוסט 2010 בשם "אסטרטגיית המרחב הקיברנטי של הפנטגון"[8] והרצאה שנשא לין בוועידת RSA בסן פרנסיסקו בפברואר 2011;[9] עדות של גנרל קית' אלכסנדר באפריל 2010 בקונגרס, חודש לפני שמונה למפקד "פיקוד הסייבר" האמריקאי;[10] הרצאה של הגנרל בדימוס מייקל היידן (לשעבר ראש ה־NSA וה־CIA[11]) בכנס אבטחה Black Hat, שהתקיים בסוף יולי 2010 בלאס וגאס.[12] כמו כן, אפשר ללמוד על כך ממסמכים רשמיים שפירסמו הממסדים הביטחוניים בארצות הברית ובמערב אירופה, ממאמרים

אקדמיים ומהתבטאויות של בכירים ושל מומחים בכלי התקשורת. על סמך מידע ממקורות אלו וניתוח אירועים נסקור להלן את המאפיינים של מרחב הלחימה החדש.

יכולת פעולה במהירות הקרובה למהירות האור, כמעט ללא מגבלות גיאוגרפיות מסורתיות. תכונה זו מאפשרת לתוקפים לבצע תקיפות בטווחים ארוכים ובמהירות הבזק, בלא חיכוך עם היריב במרחבים הפיזיים. עם זאת, המרחב הקיברנטי מקיים תלות במרחבים אלה, הקשורה לפריסת תשתיות הרשת. בצד המתגונן, יכולת התקיפה המהירה מחייבת, בין היתר, התבססות על מערכות הגנה דינמיות, המגיבות אוטומטית נגד תוקף, בזמן אמת ובלי שיקול דעת אנושי.

יכולת פעולה חשאית. לקחי המתקפות שהתרחשו עד כה במרחב הקיברנטי והמידע על אודות אסטרטגיות לפעולה במרחב הקיברנטי מלמדים שלתוקף יש יכולת לפעול במרחב הקיברנטי בחשאיות וללא "חתימה" (הותרת סימני זיהוי) ולהסתתר מאחורי גורמים אחרים, כגון האקרים פרטיים, גורמים פליליים, ארגונים ומדינות זרות. כלומר, שימוש בתכונות המרחב הקיברנטי מאפשר לצמצם את החשיפה, את סבירות ההפללה ואת הסיכון לתגובת נגד. לראיה, באף אחת מההתקפות שאירעו במרחב הקיברנטי עד כה לא היה אפשר להפליל את המדינה החשודה. בשונה מהמלחמה בשדה הקרב הקינטי, שם ברור לרוב מי התחיל, מי פגע, איזה שטח נכבש וכו', אין כך הדבר במלחמה קיברנטית. לעניין זה עשויות להיות השלכות מנוגדות: מצד אחד הדבר עשוי לרסן תגובות נגד (אין כלפי מי להגיב), אך מצד אחר גדל הפוטנציאל להסלמה בלתי מבוקרת. למשל, אם יתרחשו התקפות שיגרמו נזקים כבדים ברכוש ופגיעה בנפש, יהיה לחץ פוליטי להגיב כלפי חשודים במעשה גם בלא עדויות מוצקות לגבי זהות תוקף.

נשק קיברנטי ניתן להפעלה גם כנשק אל־הרג. היכולת לגרום לפגיעה קשה בתפקוד של מדינה בלא להחריב תשתיות פיזיות או לקטול חיי אדם נחשבת ליתרון של נשק קיברנטי על פני תקיפות קינטיות (ב"אש") אסטרטגיות. עם זאת, כאמור, באמצעות תקיפות קיברנטיות אפשר לגרום גם הרס רב ופגיעה בחיי אדם באמצעות פגיעה במערכות המקושרות למרחב הקיברנטי והמצויות במרחבים הפיזיים.

המרחב הקיברנטי מאפשר נגישות ליעדים שקשה לפגוע בהם באמצעות תקיפה קינטית (תקיפה באש), כגון:

א. מתקנים ומערכות (תקשורת, שליטה ובקרה וכו') הנמצאים באזורים קשים לתקיפה קינטית (מרחק, הגנה קינטית חזקה, ריכוזי אוכלוסייה וכו').
ב. ענפי הבנקאות והפיננסים – אלה נחשבים כיום לתשתית לאומית קריטית החשופה לתקיפה במרחב הקיברנטי הן בשל התלות הרבה של המדינות במערכות הפיננסיות והן בשל התלות של המערכות הללו במרחב הקיברנטי. פגיעה במערכת הפיננסית עלולה למשל למנוע העברת שכר, להגביל סחר חוץ ואף לעצור את המשק.
ג. מערכות לוגיסטיקה ותחבורה, שכיום הן משובצות מחשב.
ד. מסדי נתונים של המדינה – משרדי הממשלה, מערכת המשפט, אוניברסיטאות ועוד.

סיכון נמוך לחיי אדם. בתקיפה במרחב הקיברנטי גלום סיכון נמוך לחיי אדם של התוקף לעומת תקיפה צבאית קינטית, שבה סיכון כוחות הוא אחד השיקולים העשויים למנוע התקפה. הדבר נכון גם בצד המתגונן. תכונה זו מקנה לצד המגן חופש פעולה רב למדי ואף יכולת להפעיל אמצעים אוטומטיים נגד תקיפה, בלא שיקול דעת אנושי ובלי להסתכן בפגיעה בחיי אדם, הן בצד התוקף והן בצד המגן. זאת להבדיל ממערכות הגנה קינטיות. בצד התוקף היא מאפשרת יותר העזה בקידום רעיונות התקפיים.

סלקטיביות. מאפיין זה אינו חד־משמעי. במתארי תקיפה מסוימים אפשר לתקוף מטרות ספציפיות בתוך מתחם מסוים בלי לפגוע בישויות נוספות. עם זאת, במתארי תקיפה אחרים קשה לשלוט בממדי התקיפה, וייתכן שהפגיעה תתפשט אל מעבר למתוכנן.

וירואליות. תכונה זו נוגעת לנטייה של "וירוסים" לשכפל עצמם בלא הפסק וליכולתם לנוע ברשת למקומות שונים. תכונה זו היא אתגר קשה לצד המגן, שעליו למנוע את התפשטות הווירוס לאזורים שונים. לתוקף זהו יתרון במתארים מסוימים של תקיפה רחבה. באמצעות מאמץ מוגבל הוא יכול ליצור אפקטים רבים. עם זאת, כאמור, תכונה זו עלולה להוות קושי לתוקף המעוניין במתאר של תקיפה ממוקדת וסלקטיבית ובשליטה הדוקה על תוצאות התקיפה.

סטנדרטיזציה של המרחב הקיברנטי. המרחב מבוסס בעיקרו על תשתיות של חברות גלובליות (מיקרוסופט, סיסקו, צ'ק פוינט וכו') המקושרות זו עם זו ומצויות בכל המדינות. אופיו האוניברסלי של המרחב ושימוש באותו ציוד (למשל במערכות ההפעלה windows/unix) משרתים אומנם את בוני המרחב הקיברנטי, אולם יש בכך סיכון רב לצד המגן. למשל, פריצה לתוכנת אבטחת מידע נפוצה או למאגר מידע טכנולוגי מסוים של חברה קיברנטית גלובלית עלולה לסכן את כל המקומות שבהם משתמשים בה. למשל, במרס 2011 הודיעה חברת אבטחת המידע RSA (בבעלות ענקית האחסון EMC), שהיא נפגעה ממתקפה מתוחכמת של האקרים, שהצליחו לגנוב מידע שנוגע להתקני Secure ID, המשמשים לאימות זהות העובדים בארגונים ובממשלות בכל רחבי העולם.[13] אירועים מסוג זה מעמידים בסיכון את יעילותם של מוצרי אבטחה הנפוצים בקרב תאגידים וממשלות.

חיבור בין המרחב הקיברנטי לבין מכשירים שפועלים במרחבים אחרים. למשל, באמצעות חיישנים ניתן להמיר מהמרחבים הפיזיים נתונים גיאוגרפיים, תרמיים, מכניים ואחרים לביטים ולהפך – באמצעות אפקטורים אפשר להמיר הוראות המועברות ברשת הביטים לפעולות במרחבים הללו. חיבור זה מאפשר לתוקף הקיברנטי לחולל אפקטים במרחבים הפיזיים באמצעות תקיפת מערכות המקושרות למרחב הקיברנטי, כגון מערכות משובצות מחשב (computer embedded system).

רוורסביליות – "יכולת לחזור לאחור בזמן". מבחינת המגן מדובר ביכולת התאוששות מהירה מהתקפה במרחב הקיברנטי באמצעות החזרת תצורת המחשוב לאחור ("חזרה בזמן"), בסיוע מערכות גיבוי. ככל שהגיבוי מקיף ורציף יותר כך ניתן לחזור לתצורה המקורית באופן מדויק יותר. בדרך כלל, השיקום מהתקפות קיברנטיות אמור להיות

מהיר וזול בהשוואה להרס פיזי, שגורמת תקיפה מסיבית באש. עם זאת, כאמור, גם התקפות קיברנטיות מסוימות עלולות לגרום לנזקים פיזיים ניכרים, שאינם ניתנים לשיקום כנ"ל. מבחינת התוקף: בצד היתרון, תכונה זו מאפשרת לו לגרום פגיעה מוגבלת וזמנית בתשתית המותקפת, להבדיל מהרס בלתי הפיך של תשתית במתקפה קינטית מסיבית, שלעיתים אינו רצוי, למשל כאשר מדובר בתשתית אזרחית. בצד החיסרון לתוקף – יכולת התאוששות של המגן ויכולתו לחסום נתיבים שהותקפו ולהתגונן מפני כלים שבהם הותקף בעבר (דבר ההופך במידה רבה את כלי הנשק הקיברנטיים לחד־פעמיים); אלה יקשו על תוקף ליצור נזק מצטבר ולשמור על רציפות ההתקפה ועל עוצמתה. זהו אתגר גדול לתוקף החותר להגיע להישגים אסטרטגיים באמצעות מתקפה קיברנטית ממושכת ורחבת היקף. בשל קושי זה יש חוקרים הסבורים כי פוטנציאל הנזק לאויב או ההישג לתוקף, המיוחסים להתקפות במרחב הקיברנטי, נמוכים משמעותית ממה שמעריכים ממסדים ומומחים רבים.[14]

יכולת שליטה אנושית גבוהה במרחב הקיברנטי. מאחר שהמרחב הקיברנטי הוא מרחב מלאכותי, יציר אדם, אמור המגן לשלוט במרחב שהוא בנה. הוא אמור לצפות את התנאים במרחב, להבדיל מקושי לחזות את התנאים במרחבים האחרים, כגון מזג האוויר. ביכולתו גם להשבית את המרחב או להגביל את השימוש בו. דוגמאות לניסיון להגביל את השימוש במרחב הקיברנטי ניתן למצוא בסין, במדינות ערב ובאיראן (ראו נספח ב'). נוסף על כך, קל יותר למגן לשקם במהירות רשת מאורגנת ומסודרת מלשקם רשת שאינה כזאת. מרחב זה מאפשר למשל לשני הצדדים (לתוקף ולמגן) להתאמן בקלות רבה ולבצע סימולציות. למרות האמור לעיל, מאותרים במרחב הקיברנטי אירועים מפתיעים, שבוני המרחב לא חזו מראש והם תולדה של אינטראקציות בין מחשבים או של העצמה של טעויות אנוש (למשל טעויות במתן הוראות בשוק ההון). תכונותיו של המרחב גם מעצימות את היכולות של "אנשי פנים" לבצע פעולות זדון באמצעותו (ראו נספח ג).

מרחב אזרחי־צבאי משולב. במקרים רבים תשתיות התקשורת הצבאיות קשורות לתשתיות אזרחיות. מכאן שהגנה על תשתיות אזרחיות חיונית גם לצרכים צבאיים. בה בעת, לצבאות יש יכולות קיברנטיות העשויות לסייע להגנת תשתיות אזרחיות. במדינות דמוקרטיות שילוב זה הוא אתגר משפטי למגן נוכח החקיקה המתקדמת בתחום זכויות הפרט, המקשה, בין היתר, על איסוף מידע והפעלת יחידות צבא במרחב הקיברנטי האזרחי.

קישוריות וניצול משאבי תקשוב של גורמים אחרים. עבור התוקף, רשתות התקשורת הגלובליות מאפשרות לחצות גבולות ולנוע במהירות אל יעדים המחוברים אליהן ואף להשתמש במשאבי התקשוב של היריב כדי לתקוף את מערכותיו. עם זאת, מאפשרת הקישוריות למגן להסתייע במדינות ידידותיות כדי לאתר התקפות ולסכלן לפני הגעתן למדינה.

תלות הדדית בין המרחב הקיברנטי למרחבים הפיזיים. המרחב הקיברנטי מקיים תלות דו־כיוונית עם המרחבים הפיזיים: מצד אחד הוא מעצים פעולות במרחבים אלו

ומצד אחר מאפשר לפגוע ביעדים במרחבים אלו באמצעותו. כלומר, פגיעה קינטית בתשתיות פיזיות, כגון במתקני תקשורת ותחנות כוח, עשויה לסייע למלחמה קיברנטית.

יכולת ייצור המוני של כלי נשק קיברנטיים במהירות ובעלות נמוכה מאוד. מרגע שיוצר נשק קיברנטי, כמו "תולעת" או תוכנת הגנה, אין מניעה לשכפלו בכמות גדולה, בלא מאמץ או עלות גבוהה, להבדיל מנשק קינטי. תכונה זו משרתת הן את המגן והן את התוקף.

ניצול משאבים מרחוק. המרחב הקיברנטי מאפשר להשתמש במשאבי כוח אדם ובמשאבי מחשוב באופן ייחודי, שאינו אפשרי במרחבים הפיזיים. בשונה משדה הקרב המסורתי, שבו נדרשו החיילים להגיע אל שדה הקרב, יכולים חיילים ומשאבי מחשוב, הפועלים בשדה הקרב הקיברנטי, להימצא במקומות שונים ולהיות זמינים לקרב במהירות רבה באמצעות טכנולוגיות המידע. הדבר משפר במידה רבה את היכולות להשתמש בכוחות מילואים במרחב הקיברנטי.

פחת טכנולוגי ומבצעי. פיתוח טכנולוגי ומציאת חולשות במערכים הקיימים מאלצים החלפה תדירה של כלי ההגנה. באופן דומה, פיתוח תדיר של יכולות הגנה וסגירת פרצות מחייבים לשכלל את כלי ההתקפה. עניין זה מהווה חיסרון גדול למגן משום שהוא צריך להחליף כמויות גדולות יותר של אמצעים שחלף זמנם.

"מדרגת כניסה נמוכה". מאפייני המרחב מציבים מגבלות מועטות לבנייה של יכולת התקפית קיברנטית לא מבוטלת, לעומת בניית צבאות המבוססים על כוחות קינטיים. להלן פירוט:

א. טכנולוגיה – קיימת זמינות גבוהה של אמצעים טכנולוגיים בשוק החופשי. התוקף אף יכול לרכוש מערכות הגנה שמצויות בשימוש היריב ולהשקיע בפיתוח יכולות תקיפה עד להשגת עליונות טכנית.

ב. ידע התקפי – ידע ניכר מצוי אף הוא בשוק החופשי. למשל, בידי האקרים וברשות חברות עסקיות המספקות שירותי תקיפה במרחב הקיברנטי, בעיקר לצורכי בדיקה ותרגול של מערכי הגנה של חברות ושל ארגונים.

ג. ההון הנדרש לפיתוח יכולות התקפיות נמוך בשיעור ניכר לעומת ההון הנדרש להקמת צבא קונוונציונלי מודרני.

לסיכום, מדינות יכולות להקים כוחות קיברנטיים בעלי יכולות תקיפה מתקדמות במחירים נמוכים לעומת אלה הדרושים לבניית כוחות קינטיים מתקדמים. ארגונים וקבוצות יכולים אף הם להצטייד ולהפעיל נשק קיברנטי. כל אלה יכולים לשכור אזרחים וחברות פרטיות שיפעלו בשבילם. כפי שאמר סגן מזכיר ההגנה של ארצות־הברית ויליאם לין: "כמה תריסרי מתכנתים מוכשרים יכולים לגרום נזק רב".[15] עם זאת, יש להבחין בין יכולות התקפיות העלולות לגרום נזקים מקומיים או זמניים, קשים ככל שיהיו, לבין יכולות לבצע מתקפה קיברנטית רחבה וממושכת על יעדים אסטרטגיים של אויב שיש לו יכולות הגנה מתקדמות. נראה כי מתקפה מהסוג השני דורשת יכולת השמורה לפי

שעה למדינות בעלות יכולת טכנולוגית גבוהה. מנקודת המבט של המתגונן במרחב, כלי הגנה קיברנטיים אומנם זמינים בשוק החופשי, אולם הגנה קיברנטית מקיפה מחייבת מתן מענה לקשת רחבה של סוגי איומים ושל גופים מוגנים, ולכך יש עלויות גבוהות.

המרחב הקיברנטי – מושגים ביטחוניים מסורתיים עם תוכן חדש

המרחב הקיברנטי שונה במובנים רבים מהמרחבים הפיזיים גם בהקשר הביטחוני. השוני הרב מחייב לבחון מחדש את תוקף המושגים האסטרטגיים המסורתיים וליצוק בהם תכנים חדשים. במסמכים של צבא ארצות־הברית מצויים מונחים אופרטיביים חדשים הנוגעים ללחימה במרחב הקיברנטי (ראו נספח א). עם זאת, נראה שהמונחים הראשיים הנמצאים בשימוש לגבי שדה הקרב המסורתי משמשים גם בשדה הקרב הקיברנטי: הרתעה, הגנה, התקפה, מרוץ חימוש וכו'. ייתכן שהמונחים הללו ימשיכו לשמש שנים רבות תוך כדי התאמתם למרחב החדש, וייתכן שזוהי תקופת מעבר, עד שיגובשו מונחים ומושגים חדשים בקרב הממסדים הביטחוניים.

הסביבה האסטרטגית[16]

הסביבה האסטרטגית הקיברנטית שונה מהסביבה האסטרטגית המסורתית, שבה נהוג בישראל לסמן מעגלי ייחוס (איום) גיאוגרפיים. הקשר בין המרחב הקיברנטי לגיאוגרפי נוגע לפריסה הגיאוגרפית של תשתית המחשבים והרשתות, כך שלמושג גיאוגרפיה משמעות שונה במרחב הקיברנטי. ההתייחסות הנדרשת לממד הזמן במרחב הקיברנטי שונה נוכח המהירות שבה נעים הביטים במרחב האלקטרומגנטי. כפועל יוצא מכך, המרחב הקיברנטי עלול להעצים יכולות של אויבים ותיקים, ועלולים להצטרף אליהם אויבים ושחקנים חדשים ושונים, שהתקשו ליטול חלק במערכות קודמות אם בשל מרחק ואם עקב בידול גיאוגרפי (מדינות שאינן גובלות עם המדינה). באותו אופן המרחב הקיברנטי יוצר הזדמנויות ביטחוניות חדשות ומאפשר להיעזר בבעלי ברית באופן שונה, בהתאם ליכולותיהם ולמקומם במרחב הזה. מסיבה זו, ובשל עדיפות שמדינות שונות יעניקו לפיתוח יכולות קיברנטיות, ייתכנו מאזני כוח חדשים בין מדינות או בין מדינות לבין ארגונים חוץ־מדינתיים (ארגוני טרור, קבוצות האקרים לאומניות או אנרכיסטיות). לפיכך, המרחב הקיברנטי יוצר סביבה אסטרטגית ייחודית ומרחיב את הסביבה האסטרטגית בכללותה.

בפעולות הביטחוניות נגד יריבים בסביבה האסטרטגית הקיברנטית מבחינים בשלושה תחומי פעילות:

א. חדירה למערכות התקשוב של האויב לצורכי ריגול. זו אינה בגדר לוחמה קיברנטית.
ב. לוחמה קיברנטית רכה (Soft Cyber Warfare) – פעולות במרחב הקיברנטי, שתכליתן לשבש את תפקוד האויב, כגון לוחמה פסיכולוגית, ולא לגרום במישרין להרס.

ג. לוחמה קיברנטית (Cyber War)[17] – פעולות במרחב הקיברנטי הכוללות התקפות המכוונות לגרום במישרין נזק או הרס לאויב, בכלל זה נזק למערכות תקשוב או ליעדים במרחבים הפיזיים, באמצעות פגיעה במכונות הנשלטות מהמרחב הקיברנטי או באמצעות הפעלתן באופן שיגרום נזק.

במדינות בעולם, הגופים האמונים על סוגי הפעולות הנ"ל הם גופים ביטחוניים – צבאות וארגוני מודיעין. עם זאת, בהגנת המרחב הקיברנטי מעורבים גם גופים רבים במגזר האזרחי ובהם משרדי ממשלה (דוגמת המשרד לביטחון המולדת בארצות־הברית) וחברות פרטיות (חברות אבטחה, טכנולוגיה ותקשורת). יצירת מערכת משותפת ומסונכרנת לכל הנוטלים חלק בהגנה והיזון הדדי בין המגינים לבין כוחות תוקפים מהווה אתגר מרכזי למעצבי אסטרטגיה קיברנטית ברמה הלאומית.

ריגול ולוחמה קיברנטית רכה

ריגול

ריגול הינה פעילות חודרנית (לא התקפית) נפוצה במסגרת משימותיהם של ממסדים ביטחוניים במרחב הקיברנטי. פעילות זו אינה מיועדת לפגוע במערכות האויב ולשבש אותן, ואף לא להשפיע עליו במישרין.[18] לשימוש במרחב הקיברנטי לצורכי איסוף מידע יש היסטוריה ארוכה, מאז שהוכנסו מחשבים ותוכנות לשימוש במערכות תקשורת למיניהן. בתחום זה ניתן להבחין בשלושה סוגי פעילויות:

א. איסוף מודיעין – על יכולות היריב ועל כוונותיו בעת שגרה ובמלחמה; זאת לצורכי הערכת מצב, גיבוש אסטרטגיות, קבלת החלטות, בניין כוח צבאי ולחימה.
ב. ריגול תעשייתי – בכלל זה גניבת סודות טכנולוגיים ועסקיים.
ג. ליקוט נכסים קיברנטיים של היריב, כגון גניבת תוכנות ומסדי נתונים, מתוך כוונה להשתמש בהם ללא היתר. עניין זה חורג מתחום איסוף מידע וקרוב יותר לשימוש בנשק שלל או לגניבת נכסים. עם זאת, אפילו גניבת נכס קיברנטי יכולה להיעשות בדרך של שכפול וללא הוצאתו מרשות היריב.

יש לציין כי בעולם שבו לעוצמות כלכליות וטכנולוגיות יש משמעויות מרחיקות לכת על מאזני הכוח האסטרטגיים, לאיסוף ולליקוט של מידע ושל נכסים קיברנטיים, טכנולוגיים וכלכליים עשויים להיות משמעויות ניכרות על הביטחון הלאומי של שני הצדדים. מידע ונכסים אלה עשויים לשפר את כושר התחרות של המדינה האוספת במשק העולמי ואת יכולותיה לצמצם פערים בתחום המחקר והפיתוח הביטחוני. באותה מידה עלולה המדינה הנחדרת לאבד את יתרונותיה האסטרטגיים. מדובר בתחום שבו פעולות האיסוף חורגות מהצורך המסורתי לאסוף מידע כדי להכיר את היריב ולעמוד על יכולותיו ועל כוונותיו.

ה"ניו־יורק טיימס" מציין אירוע שניתן לראותו כראשון בתחום הריגול במרחב הקיברנטי. בשנות ה־70 הצליחה רוסיה להתחבר ל־ARPANET (רשת תקשורת של הסוכנות האמריקאית לפרויקטים של מחקר מתקדם, שקדמה לאינטרנט). במסגרת פרויקט צבאי, שמימנו האמריקאים במרכז למחקרים מתמטיים בג'נבה, התגלה כי המודם של רשת התקשורת חובר למוסקבה וסיפק לרוסים נגישות לארצות־הברית באמצעות הרשת.[19]

דוגמה נוספת לאירוע חמור של ריגול קיברנטי הציג סגן שר ההגנה האמריקאי, ויליאם לין.[20] הוא מסר כי בשנת 2008 הצליחה סוכנות ביון זרה לחדור למערכות מחשוב מסווגות בארצות־הברית באמצעות שימוש בהתקן נתיק (כמו דיסק און קי) "באופן שחשבנו שהוא בלתי אפשרי". "היה זה התגשמות של הפחד העיקרי: תוכנה זדונית פועלת באופן שקט במערכות שלנו ומעבירה תוכניות אופרטיביות לידי האויבים". ייתכן שתיאור זה נוגע לחדירה המיוחסת לסין, שבמהלכה נגנבו תוכניות של מטוס הקרב העתידי F-35 Lightning II מתוצרת לוקהיד מרטין, לרבות תוכניות של מערכות האלקטרוניקה של המטוס המתקדם בעולם, שבפיתוחו הושקעו 300 מיליארד דולר.[21]

לין איפיין את תופעת הגניבה במרחב הקיברנטי כדלהלן: "בצד הביטחוני סוכנויות ביון זרות גנבו תוכניות צבאיות ותוכניות של כלי נשק. בצד המסחרי נגנבו תוכנות יקרות ערך וקניין רוחני מחברות עסקיות ומאוניברסיטאות. התקפות אלו אומנם אינן בעלות השפעות דרמטיות כמו התקפות קונוונציונליות, אולם לאורך זמן רב יש להן השלכות הרסניות, משום שהן שוחקות את היתרון של ארצות־הברית בתחום הטכנולוגיה הצבאית ופוגעות בכושר התחרות של ארצות־הברית בכלכלה העולמית".[22]

לוחמת מסרי מידע

לוחמת מסרי מידע היא לוחמה רכה העושה שימוש מניפולטיבי במידע. היא מהווה רכיב מרכזי בתחומים של לוחמה פסיכולוגית, של הונאה, של תעמולה ושל חשיפה של מידע שהיריב מעוניין להסתירו. מטרתה להשפיע על דעותיהם ועל התנהגותם של היריב ושל תומכיו באופן ההולם את מטרות הצד היוזם ובלא שימוש בכוח קינטי (באש). זאת להבדיל מפעולות ריגול. הצד האחר של משפחה זו הוא ההסברה, שתכליתה לספק מידע ולהציג את הגיונות הפעולה לקהל בית ולידידים, דבר שהוא חיוני בין היתר ללגיטימציה של הפעלת הכוח. מאז המעבר של תקשורת ההמונים לאינטרנט בשנות התשעים, חלה עלייה מתמדת בשימוש שנעשה במרחב הקיברנטי ללוחמת מסרי מידע, כמו גם להסברה.

ההבדל העיקרי בין לוחמת מסרי מידע במרחב הקיברנטי לבין תקיפה קיברנטית הוא הרובד הנתקף במישרין. מכאן גם השוני באופן שבו מאורגן המידע: לוחמת מסרי מידע משתמשת בדרך כלל במידע המאורגן והמוצג בדרך המובנת למשתמש הרגיל (מסר הוא מידע המובן לבני אנוש); להבדיל מתקיפה קיברנטית, הנעשית ברובד הלוגי או ברובד הפיזי, בשפות המובנות לאנשי תוכנה ואלקטרוניקה.

ארצות־הברית מכירה בעוצמה הרבה של תחום לוחמת מסרי המידע וביצעה בעיראק מלחמה פסיכולוגית מקוונת נגד אל־קאעדה. עתה פועלים האמריקאים להרחיבה במסגרת המלחמה בגורמים אסלאמיים עוינים בפקיסטן, באפגניסטן, באיראן וברחבי המזרח התיכון. כן פתחו האמריקאים במאמץ לשינוי דעת הקהל השלילית כלפיהם בקרב העולם המוסלמי. על כך אפשר ללמוד למשל מעדותו של גנרל דיוויד פטראוס, מפקד כוחות הקואליציה באפגניסטן, בקונגרס של ארצות־הברית במרס 2011. בעדותו דיווח פטראוס על המאמץ להגביר את פעולות הביון ברשתות החברתיות כדי להילחם באידיאולוגיה הקיצונית ובתעמולה המתנהלת נגד ארצות־הברית ונגד המערב. במסגרת מאמץ זה מפותחות תוכנות שיאפשרו להתערב בחשאי ברשתות החברתיות. למשל, חברה אמריקאית מקליפורניה זכתה במכרז של צבא ארצות־הברית לפיתוח שירותי ניהול מקוונים, שיאפשרו למפעיל אחד לנהל במקביל עשר זהויות בדויות באינטרנט. כל זהות תיבנה עם רקע היסטורי מפורט ובשימוש בשרתים מרחבי העולם כדי ליצור רושם שהמגיבים נמצאים במקומות שונים בעולם. התוכנה תאפשר התערבות של טוקבקיסטים ושל בלוגרים מתחזים בדיונים בערבית ובפרסית ובשפות אחרות המדוברות בפקיסטן ובאפגניסטן.[23]

עוד נודע, כי חיל האוויר של ארצות־הברית מצויד במטוסי הרקולס (C-130) המיועדים לבצע משימות של לוחמה פסיכולוגית כמו יכולת לחדור לשידורי הטלוויזיה והרדיו של מדינת אויב ולשדר מסרים נגד המשטר של המדינה או מסרים לתושבי המדינה; וכן לשמש ממסר שיאפשר להקים רשת לטלפונים סלולאריים, שתוכל להעניק לתושבי מדינה שירותי טלפון נייד ואינטרנט אלחוטי ואף לתקשר עימם, במקרה שהמשטר ינסה לנתק את אזרחיו. דהינו, להפקיע את השליטה בשדה האלקטרומגנטי ובמרחב הקיברנטי מידי המשטר לטובת קידום אינטרסים של היוזם.[24]

המחשה לעוצמה הרבה של לוחמת מסרי מידע אפשר לראות במהפכות המתחוללות במזרח התיכון בסיוע המרחב הקיברנטי. הצעירים המשתמשים במסרי מידע ובפונקציונליות קיברנטית כבר הצליחו לחולל מהפכי שלטון, למשל במצרים ובתוניסיה. מדובר במלחמה שבה המרחב הקיברנטי הוא תווך מסייע ומשפיע, אלא שבמקרה זה אויבי המשטרים האוטוריטריים הם אזרחי המדינה ולא אויבים מן החוץ (להרחבה בנושא ראו נספח ב).

תחום אחר של לוחמת מסרי המידע הוא חשיפה של סודות היריב במגמה לפגוע בו. מדובר בחשיפה של כוונות, של פעולות אסורות, של התבטאויות מביכות של מנהיגים וכד'. בתחום זה בולטת פעילות של יחידים ושל ארגונים פוליטיים נגד ממסדים מדינתיים (להרחבה בנושא ראו נספח ג).

סנקציות קיברנטיות

סנקציות הן לוחמה רכה, לא חשאית, שמטרתה להעניש את מפר הכללים (בראיית מפעיל הסנקציות) כדי לגרום לו לשנות את התנהגותו ולהרתיעו מלבצע את מעשהו פעם נוספת או להחלישו לקראת הפעלת מנופי כוח אחרים. קיימת קשת רחבה של סנקציות,

החל במניעת שיתוף פעולה וזכויות אחרות מהמדינה "הסוררת", עבור דרך נידוי וכלה בהטלת סגר על גבולותיה (דוגמת הסגר שהטילה קואליציה בראשות ארצות־הברית על עיראק בתקופת צדאם חוסין). המרחב הקיברנטי אטרקטיבי לסנקציות, שכן מבחינה טכנית מדובר בפעולות קלות יחסית לביצוע, כגון מניעת תקשורת עם חו"ל, שיש לה אפקט משמעותי. עם זאת, הטלת סנקציות קיברנטיות יעילות מחייבת קואליציה של מדינות רלוונטיות.

הטלת סנקציות קיברנטיות יכולה להיעשות במסגרת מכלול של סנקציות על מדינה "סוררת" או במסגרת גיבוש כללי משחק במרחב הקיברנטי. כך למשל סיפר מייקל היידן, כי בעבר שקל הממשל האמריקאי אפשרויות פעולה נגד מדינות שמתחומן יוצאות התקפות קיברנטיות על ארצות־הברית, בכלל זה סוגים של נידוי קיברנטי או תגובה שתאיים לפגוע או תפגע בזרימת התעבורה האינטרנטית של המדינה שממנה באה הפגיעה.[25]

לוחמה קיברנטית

התקפה קיברנטית

התקפה קיברנטית היא פעולת לוחמה במרחב הקיברנטי נגד אויב כדי לגרום לו נזק במטרה לפגוע בתפקודו ולגרום לו לנהוג על פי רצון התוקף. התקפה קיברנטית בפני עצמה אינה מסוגלת להביא לידי הכרעה או להביא הישגים אסטרטגיים כמו כיבוש שטחים בידי צבא יבשה, אך היא מסוגלת לפגוע ביעדים חיוניים של האויב וביכולותיו. בעדותו בקונגרס באפריל 2010 מנה מפקד פיקוד הסייבר האמריקאי סוגי מטרות המועדות להתקפה במרחב הקיברנטי ובהן: מערכות של הגנה אווירית, אמצעי לחימה ומערכות שליטה ובקרה של הצבא וכן תשתיות אזרחיות ובהן רשת החשמל, המערכת הפיננסית ומערכות תחבורה ותקשורת.

יש אפוא להניח שהתקפה קיברנטית עשויה להיות רכיב בכל מלחמה מודרנית בעתיד בצד מרכיבי כוח אחרים. התכונות הייחודיות של המרחב הקיברנטי עושות אותו אטרקטיבי ללחימה גם בתקופות שבין מלחמות קונוונציונליות. וכך עשויות התקפות קיברנטיות לשמש לתכליות האלה:

א. אמצעי להפעלת לחצים לשינוי מדיניות של היריב (כמו התקיפה המיוחסת לרוסיה באסטוניה) בתקופות שבין מלחמות קונוונציונליות.
ב. סיכול איומים ביטחוניים מתהווים כמו תקיפת סטאקסנט (Stuxnet) באיראן.
ג. בניית יכולת התקפה במסגרת מאזן הרתעה.
ד. תגובת נגד – פגיעה קיברנטית בתוקפים או במדינות שמהן יוצאות התקפות קיברנטיות.

אף שנושא ההתקפה במרחב הקיברנטי אינו מוסדר מבחינת המשפט הבינלאומי, עשויה פעילות קיברנטית התקפית להיחשב אקט מלחמתי, לעומת פעולות ריגול קיברנטי, שאין עמן נזק מיידי מוחשי, ואינן נחשבות אקט כזה.[26]

התקפה במרחב הקיברנטי נעשית בעיקר ברובד הלוגי, אך קיימת פעילות התקפית המסתייעת בחומרה. אפשר להבחין בשני סוגים של תקיפה. האחד, תקיפה במרחב הקיברנטי שמטרתה לשבש או לגרום נזק למרחב הקיברנטי של היריב (מחשבים, רשתות, בסיסי נתונים וכו'), באופן שימנע ממנו לנצל את המרחב הקיברנטי לתועלתו (למשל המתקפות המיוחסות לרוסיה באסטוניה ובגאורגיה); וסוג אחר – שימוש במרחב הקיברנטי לתקיפת מכשירים הקשורים אליו (מתקני תשתית, אמצעי לחימה וכו') כמו תקיפת סטאקסנט באיראן (ניתוח אירוע זה יוצג בהמשך).

בכירים אמריקאים מדגישים כי לתוקפים הקיברנטיים יש כיום יתרון על המגינים. לדברי סגן מזכיר ההגנה של ארצות־הברית, ויליאם לין, היתרון שיש כיום לתוקפים ברשת נובע מכך שהאינטרנט תוכנן ביסודו להיות פתוח ובנוי כדי להבטיח את זרימת המידע וכניסה של טכנולוגיות חדשות, בעוד תחום הביטחון ברשת היה בעל חשיבות משנית. עניינים מבניים אלה תרמו להתפתחות האינטרנט, אולם הם גם מספקים לתוקפים יתרון מובנה. לדבריו, אפשר לראות זאת באמצעות השוואה בין תוכנות אנטי־וירוס לתוכנות זדוניות. מערכת אנטי־וירוס מתוחכמת מריצה (פברואר 2011) כ־10 מיליון שורות קוד, לעומת מיליון שנה לפני כן. למרות זאת, תוכנת זדון של 125 שורות קוד, שאורכה כפי שהיה שנה לפני כן מסוגלת לחדור תוכנת אנטי־וירוס. ויליאם לין מבחין בין תקיפות קיברנטיות שתכליתן שיבוש מתוחם בזמן ובהיקף, כמו תקיפות האקרים או השבתה של אתר באמצעי תקיפה פשוטים למדי, לבין תקיפה שתכליתה לגרום נזק ולהרוס את התשתית הקיברנטית של היריב. תקיפות כאלה עדיין לא הופיעו בהיקף נרחב, אך טמון בהן פוטנציאל הרסני.[27]

אף על פי שאין האיום הקיברנטי דומה לאיום הקיומי שאיפיין את העידן הגרעיני, טוען ויליאם לין, שיש קווי דמיון ביניהם. המרחב הקיברנטי נותן בידי יריבים אפשרות וכלים קונונציונליים לאיים על ארצות־הברית. התקפה כזאת אומנם לא תגרום לנפגעים המוניים, אולם היא עלולה לשתק את החברה האמריקאית באופן דומה. וכן בטווח הארוך, חדירה מתמשכת ושיטתית של האקרים לאוניברסיטאות ולחברות עסקיות עלולה "לשדוד מארצות־הברית את קניינה הרוחני וליצור איום על יתרונה בכלכלה העולמית".[28]

במגוון שיטות ההתקפה הלוגיות מבחינים בין שיטות חודרניות, העושות שימוש בתוכנות זדוניות, לבין שיטות שאינן חודרניות באופיין, כמו התקפות מסוג "מניעת שירות" (DDoS).

תוכנות זדוניות (Malware) למיניהן מוחדרות בחשאי למחשבי היריב תוך ניצול נקודות חולשה במערכת האבטחה. החדירה יכולה להיעשות מבחוץ, דרך רשתות גלובליות אוניברסליות, או מבפנים, באמצעות סוכן הפועל בארגון, או בשילוב – חדירה לרשת מקומית בסיוע סוכנים. במשפחה זו של תוכנות זדוניות ישנם סוגים של תוכנות, כמו "תולעי מחשב" ו"סוסים טרויאנים" (Trojan horse), המאפשרים לחודר לבצע מגוון פעולות במשימות איסוף או למטרות לתקיפה, כגון: לאסוף מידע מודיעיני האגור במחשב היריב ("רוגלות"), לשבש את פעילות מחשב היריב, למחוק בו קבצים, להשתלט עליו

ולפעול באמצעותו נגד מחשבים ומכשירים אחרים המחוברים אליו ברשת. תוכנות זדוניות מכוונות לעיתים להתפשט למחשבים נוספים, לעיתים בשירות המפעיל ולעיתים באופן לא מבוקר. תוכנות זדוניות מסוימות יכולות להיות רדומות במחשבי היריב עד הפעלתן.

התקפות מסוג "מניעת שירות" (DDoS –Distributed Denial of Service) – מטרתן לשבש את המרחב הקיברנטי של היריב. בהתקפות מסוג זה מוצפים האתרים הנתקפים במספר גדול מאוד של פניות בו בזמן, עד שאינם יכולים לעמוד בעומס וקורסים. בהתקפות אלה נעשה שימוש בבידול טכני (שימוש בשרתים שאינם מזוהים עם הממסד התוקף) ויומינטי (שימוש בהאקרים) כדי למנוע הפללה. לדברי ויליאם לין, התקפות מסוג מניעת שירות, שנועדו לשבש מערכות מידע, היו עד כה קצרות טווח, בעלות ממדים צרים ולא מתוחכמות, אולם בעתיד יוכלו אויבים בעלי יכולות גבוהות יותר לבנות יכולת לשתק רשתות בהיקפים גדולים ולמשך זמן רב יותר. לדבריו, האפקט הטכני של התקפות אלה הוא אומנם הפיך, אולם לא כך הנזקים הכלכליים שנגרמו בעת ההתקפה ואובדן האמון במערכת. לין ציין שהתקפות של מניעת שירות כוונו גם נגד חברות מסחריות ובהן eBay ו־Paypal.[29] מייקל היידן ציין כי שימוש בהתקפת מניעת שירות הייתה אחת האפשרויות שאותן בחן הממשל האמריקאי כדי לפעול נגד מדינות שמהן יוצאות תקיפות כלפי ארצות־הברית, שכן תקיפה מסוג זה עומדת בהגבלות של אמנת ז'נווה.[30]

שימוש התקפי בחומרה הינו דרך נוספת לחדור למרחב הקיברנטי של היריב. סגן מזכיר ההגנה לין הדגיש שהאיום על המגן אינו נשקף רק מתוכנה אלא גם מחומרה, שיכולה לכלול מרכיבים סמויים שיפעלו בשירות מתקין החומרה, וזיהויה קשה בהרבה. לדבריו, חברות מחשבים ובהן מיקרוסופט החלו לבדוק ולנטר סוג זה של איומים, והן מציעות לגורמי ממשל לנקוט יוזמה דומה.[31]

הרתעה

קיימת הכרה בחולשת מושג מסורתי זה בהקשר של המרחב הקיברנטי הואיל ולא בכל מקרה ידוע מי אחראי לתקיפה, והתוקף עלול לעשות שימוש בתשתיות של צד שלישי. נוסף על כך, השגת הרתעה מחייבת הצגת יכולות מסווגות, שחשיפתן תגרום לאובדן הרלוונטיות שלהן. מפקד פיקוד הסייבר של ארצות־הברית, הגנרל אלכסנדר, העיד בקונגרס באפריל 2010 כי ארצות־הברית טרם גיבשה דוקטרינת הרתעה במרחב הקיברנטי נוכח הקושי לייצר הרתעה מסוג זה. לדבריו, "הדרך הטובה ביותר להרתיע היא באמצעות הגדלת רמת הביטחון ברשת שלנו".[32]

למרות האמור לעיל, אפשר לעשות פעולות הרתעה במרחב הקיברנטי. למשל, אזהרת מדינות תוקפניות, כגון האזהרה שהשמיעה מזכירת המדינה הילארי קלינטון כלפי סין,[33] ביצוע פעולות תקיפה מוגבלות על אויבים כדי להמחיש יכולת, ולו במחיר של חשיפת יכולות מסוימות. על אף הקושי לקיים הרתעה, ייתכנו מאזני הרתעה בין מדינות במרחב הקיברנטי.

הגנה במרחב הקיברנטי

התפתחות המרחב הקיברנטי כמרחב חיוני לתפקודן של מדינות מעוררת אצלן את הצורך להגן על מרחב זה ולמנוע פגיעה ביעדים שמחוץ למרחב הקיברנטי באמצעותו. ככל שמדינה מנצלת לתועלתה את המרחב הקיברנטי, כך היא חשופה יותר לפגיעה בו ולתשתיות הקשורות אליו. הדבר נכון גם לארגונים ביטחוניים. ככל שצבאות וארגוני ביטחון מסתמכים על המרחב הקיברנטי, כך גדלה תלותם בו לתפקודם, וגם החשיפה שלהם לפגיעה בו ובמערכות הקשורות אליו. פגיעותו הרבה של המרחב הקיברנטי נובעת גם מהישענותו על המרחב האלקטרומגנטי ועל תשתיותיו. ההגנה במרחב הקיברנטי אמורה להתמודד עם מגוון רחב של חדירות – החל בחדירות לצורכי איסוף וכלה במתקפות קיברנטיות. מגוון האויבים שעימם אמור מערך ההגנה להתמודד כולל: מדינות עוינות, ארגוני טרור, אנשי פנים המבצעים פעולות זדון, פושעים למיניהם, קבוצות האקרים הפועלות ממניעים אידיאולוגיים ואחרים ואירועי תקלה.[34]

למרות האמירה הרווחת, כאילו המרחב הקיברנטי הוא "מרחב ללא גבולות", יש להבחין בין המרחב הקיברנטי הגלובלי לבין המרחב הקיברנטי המדינתי. זה המדינתי משמעו מחשבים, מערכות ממוכנות ורשתות, תוכנות, מידע ממוחשב, תוכן, נתוני תעבורה ובקרה והמשתמשים של אלה (ראו הגדרת האו"ם לעיל), אשר בשימוש המדינה ותושביה.

הגנה במרחב הקיברנטי היא אתגר מסוג חדש, בין היתר נוכח היכולת של האויב לבצע מתקפה במהירות הבזק והקושי לזהות את התוקף. מפקד פיקוד הסייבר הגנרל אלכסנדר הסביר כי בעת גילוי החדירה הקיברנטית אין המגן יכול לקבוע בוודאות את תכליתה, ועל כן ההבחנה בין ריגול לבין ניסיון תקיפה במרחב הקיברנטי עשויה להיות קשה לביצוע (בשלב הראשון). הבחנה זו בין פעולת ריגול לפעולה התקפית חשובה בקשר לתגובת הנגד, שכן מדינות יוצאות למלחמות לאחר שהותקפו, אך לא יגיבו כך בעקבות ריגול משום שאינו נחשב אקט מלחמתי.[35] על כך יש להוסיף שדי בפרצה קטנה או בחוליה חלשה אחת – אנושית או טכנולוגית – כדי להביא לכישלון ההגנה. המרחב הקיברנטי מעצים גם יכולת של גורם עוין לנצל פרצות במערך ההגנה לתועלתו, ומערכות האבטחה הן לעיתים חסרות אונים נגד פעולות זדון של "אנשי פנים", שיש להם הרשאות לפעול במערכת (ראו נספח ג).

מסמך של צבא ארצות־הברית משנת 2010 מגדיר את מושג ההגנה הקיברנטית (Cyber defense) ברמה האופרטיבית.[36] לפי המסמך, הגנה קיברנטית היא מכלול פעולות המשלבות הגנה על רשתות מחשב והגנה על תשתית קריטית לכדי מערכה רחבה, שממנה אפשר גם להגיב במתקפת נגד או במתקפת מנע. במסגרת ההגנה במרחב הקיברנטי ננקטים, בין היתר, מגוון רחב של צעדים שמטרתם למנוע פגיעה ולהפחית סיכון ונזק לתשתיות תקשורת מחשבים המוגדרות חיוניות. בכך נכללות גם פעולות כמו יתירות (יכולות עודפות וגיבויים), בידוד מערכות מידע מסוימות, בידול בין מערכות, פריסת מערך אבטחת מידע קונוונציונלי בכמה שכבות, אבטחה פיזית של מערכות המידע נוהלי ביטחון מידע נוקשים ומשתנים ותרבות המשתמשים.

מענה (חלקי) לאתגר של מהירות התקיפה הקיברנטית נמצא בתפיסת ה"הגנה האקטיבית", שהיא אחד הרכיבים הבולטים של אסטרטגיית ההגנה הכוללת במרחב הקיברנטי של משרד ההגנה של ארצות־הברית (הפנטגון). תפיסה זו מתבססת על יכולות מודיעיניות מתקדמות לזיהוי פעולות ברשת, על מערכות הגנה ממוכנות לזיהוי תקיפה ולתגובה אוטומטית בלי מעורבות אנוש ועל יכולות התקפיות לצורכי סיכול.

מהאמור לעיל ברור שהמושג אבטחת מידע (שהרציונל שלו נוגע לשמירה על המידע מפני גנֵבה, השחתה ותקלה) אינו ממצה את תחום ההגנה על המרחב הקיברנטי עצמו ועל מערכות המחוברות אליו, כגון תשתית קריטית ומערכות לחימה. דווקא סוג הפעולות ההרסניות ביותר – שימוש במרחב כדי לגרום נזק למערכות כאלה – יכול להיעשות בלא פגיעה כלל בתצורת המחשב.

התרעה מודיעינית

השימוש במושג זה אינו דורש התאמה רבה למרחב הקיברנטי בנוגע להתרעה בסיסית, המבוססת על ניתוח של כוונות אסטרטגיות, של דרכי פעולה ושל כלים העומדים לרשות האויב. עם זאת, האתגר שונה בנוגע להתרעות אופרטיביות וטקטיות, שבהן נדרשת התייחסות לפרטי ההתקפה ולעיתויה. את ההכנות למתקפה במרחב הקיברנטי אפשר לערוך בחדרי חדרים, להבדיל מהכנות נרחבות הדרושות להכנת גייסות קונוונציונליים למלחמה, הכרוכות לרוב בדליפת מידע. לעיתים קשה לדעת בזמן אמת שהתקפה קיברנטית כבר החלה, בטרם נגלות תוצאותיה, ולעיתים תוצאותיה לא יתגלו כלל (ייחשבו לתקלה). שאלה אחרת היא תכליתה של התרעה במציאות שבה מתבצעת התקפה במהירות הבזק, ואילו צעדי הגנה אופרטיביים היא יכולה לשרת. הצורך של צבא ארצות־הברית להתבסס על מערכות הגנה דינמיות, המגיבות אוטומטית עם זיהוי התקיפה, מלמד על מצבים שבהם אי־אפשר להסתמך על התרעות טקטיות מסורתיות (כגון התרעות שמספקות תצפיות למפקדי יחידות שדה בדבר התקדמות כוחות אויב).

שילוב כוחות

סינרגיה ושילוב בין כוחות מסוגים שונים בלחימה מאפשרים להשיג אפקט מערכתי, שבו "השלם גדול מסך כל חלקיו". אופיו של המרחב הקיברנטי תואם מאוד רעיון זה. התקפה קיברנטית עשויה להשתלב עם לוחמה קינטית, עם לוחמה אלקטרונית ועם לוחמת מסרי מידע. במקרים מסוימים הלוחמה הקיברנטית עשויה להיות מגמה ראשית (מאמץ עיקרי), שרכיבי כוח אחרים יסייעו לה, ובמקרים אחרים יכולה להתבצע לוחמה קיברנטית בסיוע לרכיבי כוח אחרים.

שיתוף פעולה פנים־מדינתי ועם מדינות אחרות

שיתוף פעולה קיברנטי הוא עניין מרכזי לצורך ההגנה, שכן המרחב הקיברנטי חוצה גבולות, סקטורים וארגונים. נבחין בשני סוגים עיקריים של שיתופי פעולה.

שיתוף פעולה פנים־מדינתי – שיתוף פעולה במרחב הקיברנטי הוא ייחודי בתחום ההגנה. להבדיל מהתחום ההתקפי, המצוי ברשות כוחות הביטחון של המדינה, כינון מערכת הגנה אפקטיבית לאומית מחייב שיתוף פעולה עמוק בין המגזר האזרחי (הציבורי והפרטי) לצבאי, מאחר שקשה כאמור להפריד בין התשתיות הקיברנטיות האזרחיות לבין התשתיות הצבאיות, וחלק ניכר מהיכולות הקיברנטיות של המדינה נמצא בידיים פרטיות. עקב כך נדרש שיתוף פעולה רב־ממדי: על ציר אחד – שיתוף פעולה וסנכרון בתוך הסקטור הציבורי – בין המגזר האזרחי לביטחוני; ועל הציר האחר – שיתוף פעולה בין המגזר הציבורי והפרטי (חברות טכנולוגיות עילית, חברות תקשורת, חברות אבטחה, חברות תשתיות קריטיות ועוד).

שיתוף פעולה עם מדינות זרות הוא רכיב חשוב בהתמודדות עם האיומים החדשים נוכח אופיו האוניברסלי של המרחב הקיברנטי. לדוגמה: באמצעות רשתות ניטור משותפות ושיתוף פעולה מודיעיני אפשר לשפר את יכולת ההתרעה, העקיבות (traceability – היכולת לעקוב אחר נתיב התקיפה ולאתר את מקורה) והתגובה.

לוח 1: פעולות ביטחוניות במרחב הקיברנטי נגד יריבים ומאפייניהן

פעולות	מטרות ומאפיינים	דוגמאות לנזק מוגבל	דוגמאות לנזק רחב
1. ריגול			
א. איסוף מידע	א. השגת מידע לצורכי קבלת החלטות וביצוען והשגת עליונות במידע על היריב (לא לוחמה קיברנטית). ב. מאפיינים: פעולות חשאיות, בעיקר ברובד הלוגי. לא נועדו להשפיע על תצורת התקשוב, על בסיסי נתונים ועל המשתמש. ג. לא נחשב לאקט מלחמתי.	חשיפת סודות טקטיים או אופרטיביים נקודתיים אצל האויב.	חשיפת סודות אסטרטגיים (אובדן ההפתעה במלחמה). השגת עליונות מודיעינית על האויב.
ב. ליקוט (גנבת) קניין רוחני ונכסים קיברנטיים	א. פעולות איסוף להשגת יתרון טכנולוגי צבאי ועסקי (לוחמה קיברנטית רכה). ב. מאפיינים: בדומה לאיסוף מידע.	אובדן קניין רוחני ונכסים קיברנטיים מסוימים.	אובדן היתרון הטכנולוגי הצבאי והעסקי, פגיעה קשה בכושר התחרות.

פעולות	מטרות ומאפיינים	דוגמאות לנזק מוגבל	דוגמאות לנזק רחב
2. לוחמת מסרי מידע (לוחמה פסיכולוגית, תעמולה, חשיפת סודות)			
	א. שימוש במסרי מידע גלויים או סמויים כדי לגרום שינוי בהתנהגות של היריב או של גורמים המשפיעים עליו (לוחמה קיברנטית רכה). ב. מאפיינים: שימוש מניפולטיבי במידע כלפי רובד המשתמש במרחב הקיברנטי. לא נועדו לפגוע בתפקוד הפונקציונלי של מערכות התקשוב של היריב.	חשיפת סודות הגורמת נזק קצר טווח לתכנונים אופרטיביים. נזק מוגבל להסברה.	קורבן להונאה אסטרטגית, המשנה את פני המלחמה. פגיעה קשה בלגיטימציה של המדינה או של השלטון.
3. סנקציות קיברנטיות			
	א. נידוי קיברנטי של היריב כדי להביאו לשינוי בהתנהגותו (לוחמה קיברנטית רכה). ב. מאפיינים: הפסקת קשרים בתחומי השירותים וסחר במחשבים ותקשורת.	שיבושים בפעילות הקיברנטית.	שיתוק נרחב ולאורך זמן של המרחב הקיברנטי.
4. תקיפה קיברנטית (Cyber War)			
א. תקיפה קיברנטית בתוך המרחב הקיברנטי.	א. תקיפת מערכות תקשוב שברשות האויב במטרה לפגוע בתפקודו (לוחמה קיברנטית). ב. מאפיינים: פעולות אקטיביות, בעיקר ברובד הלוגי. ייתכנו פעולות גם בחומרה. ג. עשויות להיחשב לאקט מלחמתי.	נזקים מוגבלים לבסיסי נתונים ושיבוש זמני של המרחב הקיברנטי.	שיתוק נרחב של המרחב הקיברנטי לאורך זמן, אובדן בסיסי נתונים חיוניים בהיקף נרחב.
ב. תקיפה קיברנטית של מכשירים המחוברים למרחב הקיברנטי.	כנ"ל, אלא שהתקיפה יוצאת מגבולות המרחב הקיברנטי ומשפיעה במישרין על תפקוד מכשירים ומערכות שמחוץ למרחב.	פגיעה בתפקוד מפעלים בודדים. התאוששות מהירה.	פגיעה קשה בתשתיות, ביכולות צבאיות. נזק רב לרכוש ואף לנפש.

הערות

1 ITU Cybersecurity Gateway: www.itu.int.cybersecurity

ההגדרה מופיעה במסמך ITU מפברואר 2010 ITU Toolkit For Cybercrime Legislation

2 הגדרה המבליטה את הרובד האנושי־החברתי יש בערך "המרחב הקיברנטי" בוויקיפדיה (בעברית). לפי הגדרה זו, המרחב הקיברנטי הוא "מרחב מטפורי של מערכות מחשב ורשתות מחשב שבו נאגרים נתונים אלקטרוניים ומתבצעת תקשורת מקוונת ואינטראקטיבית ללא תלות במיקום הגיאוגרפי של המשתמשים בו. המונח הוטבע על ידי סופר המדע הבדיוני ויליאם גיבסון בשנת 1984 ברומן *Neuromancer*. מבחינה חברתית, המרחב הקיברנטי מאפשר למשתמשים בו לקיים אינטראקציה, להחליף רעיונות, לשתף מידע, לספק תמיכה חברתית, לקיים עסקים, ליצור אמנות, לשחק במשחקים, לעסוק בדיון פוליטי וכן הלאה. המונח מכוון פעמים רבות לאובייקטים ולזהויות הקיימות ברשת האינטרנט, כך שאפשר לומר, כי אתר אינטרנט נמצא במרחב הקיברנטי".

3 The United States Army's', *Cyberspace Operations Concept Capability Plan 2016-2028*, 22 February 2010.

4 Cabinet Office, "Cyber Security Strategy of the United Kingdom" (safety, security and resilience in cyber space), June 2009.

5 Federal Ministry of the Interior, *The new Cyber Security Strategy for Germany*, Berlin, February 2011.

6 Sebastian M. Convertino II, Lou Anne DeMattei, Tammy M. Knierim, *Flying and Fighting in Cyberspace*, Air University Press, Alabama, July 2007.

7 עמוס גרנית, **המרחב הקיברנטי כמרחב פעולה צבאי – באיזה מובן**, המכון לחקר המודיעין באמ"ן, מרס 2010.

8 William J. Lynn, "The Pentagon Cyber strategy", *Foreign Relations*, August 2010 [hereafter: Lynn, August 2010].

9 U.S. Department of Defense, Office of the Assistant Secretary of Defense, "Remarks on Cyber at the RSA Conference", As Delivered by William J. Lynn, III, San Francisco, California, February 15, 2011 [hereafter: Lynn, February 15, 2011].

10 "Advance Questions for Lieutenant General Keith Alexander", USA Nominee for Commander, United States Cyber Command, U.S. Senate, Committee on Armed Services, Washington, DC, April 15, 2010.

11 NSA (National Security Agency) – הסוכנות האמריקנית לביטחון לאומי, המצויה במשרד ההגנה של ארצות־הברית. הסוכנות ממונה על איסוף מודיעין סיגינט (Sigint – Signal Intelligence) כלומר, איסוף מידע מאמצעי התקשורת למיניהם ומאותות אלקטרוניים הנפלטים ממכשור זר (למשל מכ"מים), בדומה ליחידה 8200 בישראל.

12 מערכת אתר "אנשים ומחשבים", www.pc.co.il, "מנהל ה־CIA וה־NSA לשעבר: "אם לא ניזהר, המתקפות הקיברנטיות יהיו לפצצות האטום של המאה ה־21", www.pc.co.il, 2 באוגוסט 2010; William Jackson, "U.S. understanding of cyber war still immature, says former NSA director", *government computer news* (*GCN*). http://gcn.com July 29, 2010.
מייקל היידן היה המנהל של הסוכנות לביטחון לאומי – NSA (1999–2005) וראש ה־CIA (2006–2009). כיום הוא מנהל קבוצת האבטחה צ'רטוף (Chertoff), שהוקמה על ידי מייקל צ'רטוף, לשעבר השר לביטחון פנים והשר להגנה על תשתיות לאומיות בממשל הנשיא ג'ורג' בוש.

13 "תשתית המחשוב של RSA נפרצה; חשש לביטחון המידע של לקוחותיה", אתר TheMarker, 19 במרס 2011.

14 בהרצאה בכנס הרצליה בפברואר 2011 הדגיש ליביקי את הקלות היחסית שבה אפשר להתמודד עם תקיפות במרחב הקיברנטי, בין היתר באמצעות תיקון ושחזור מהיר. להערכתו, חולשת המתקפה הקיברנטית נובעת מאי־יכולתה לייצר אפקט קבוע. להתייחסות נוספת: Martin C. Libicki, *Cyberdeterrence and Cyberwar*, RAND, 2009.

15 Lynn, February 15, 2011.

16 הסביבה האסטרטגית – הסביבה הביטחונית והפוליטית המשפיעה על יכולתה של מדינה לממש את יעדיה הלאומיים. בכלל זה "השחקנים" הפועלים בה, הכלים שבידיהם ו"כללי המשחק".

17 ריצ'ארד קלארק, מומחה לביטחון, המצוטט בוויקיפדיה מגדיר CyberWar כך: "Actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption". Richard Clarke, *A Cyber War*, Harper-Collins, 2010.

18 פעילות שאינה משפיעה במישרין על היריב כל עוד אין הוא מודע לחשיפת סודותיו. יודגש כי פעולות ריגול, איסוף ומודיעין שינו את פני ההיסטוריה: פיצוח סודות מכונת הצופן הגרמנית "אניגמה" במלחמת העולם השנייה, גנבת סודות הגרעין של ארצות־הברית בידי ברית־המועצות ועוד.

19 John Markoff, "A Code for Chaos", *The New York Times*, October 2, 2010, based on Thomas C. Reed, a former secretary of the Air Force, in his book, *At the Abyss: An Insider's History of the Cold War,* Ballantine Books, 2004.

20 Lynn, February 15, 2011.

21 Siobhan Gorman, August Cole and Yochi Dreazen, "Computer Spies Breach Fighter-Jet Project", *Wall Street Journal*, April 21, 2009.

22 Lynn, February 15, 2011.

23 יצחק בן־חורין, "מלחמה ברשת: בלוגרים פיקטיביים בשירות ארצות־הברית", Ynet, 18 במרס 2011.

24 אנשיל פפר, "נשק נגד דיכוי: מטוס לחיבור לאינטרנט", **הארץ**, 9 בפברואר 2011.

25 דברי מנהל ה־CIA וה־NSA לשעבר, ראו לעיל הערה 12.

26 הבחנה זו ביו חדירה למטרות איסוף לבין חדירה למטרות תקיפה הוצגה בעדותו של גנרל אלכסנדר בקונגרס, ב־15 באפריל 2010. ראו לעיל הערה 10.

27 Lynn, February 15, 2011.

28 Lynn, August 2010.

29 Lynn, February 15, 2011.

30 מערכת אתר אנשים ומחשבים, ראו לעיל הערה 12.

31 Lynn, August 2010.

32 Keith Alexander, April 15, 2010.

33 אור הירשאוגה ואורי ברקוביץ', "הילארי קלינטון: מי שיפגע ברשת האינטרנט ויאיים על הכלכלה שלנו יישא בתוצאות", TheMarker, 21 בינואר 2010.

34 תאונה במרחב הקיברנטי. בדומה לסיכון הקיים בנשק ביולוגי, שבו עלולים לברוח מהמעבדה או משדה הקרב וירוסים קטלניים, שיתרבו ויתפשטו בלא יכולת בקרה, כך גם וירוסים קיברנטיים מעשה ידי אדם. לדברי לין, ב־15 בפברואר 2011, סוגים מסוימים של "תולעים רעילות" עלולות להשתחרר מידי יוצרן, להתפשט בעולם תוך דקות ולגרום בין היתר לשיבוש רשתות חיוניות. לפיכך אסטרטגיית הביטחון של הפנטגון במרחב הקיברנטי מניחה את התרחיש החמור של אפשרות זאת.

35 Keith Alexander, April 15, 2010.

36 The United States Army's, *Cyberspace Operations Concept Capability Plan 2016-2028*, February 22, 2010 (TRADOC Pamphlet 525-7-8).