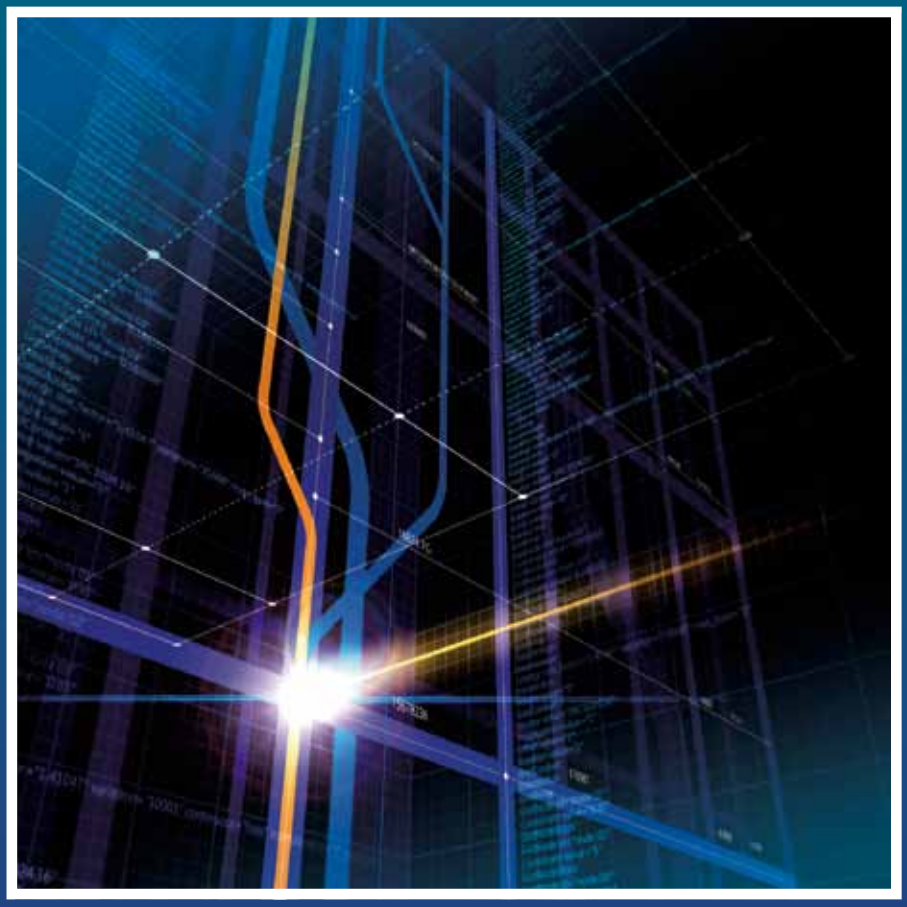
לוחמה במרחב הקיברנטי

מושגים, מגמות ומשמעויות לישראל

שמואל אבן ודוד סימן־טוב



מזכר
109

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
INCORPORATING THE JAFFEE CENTER FOR STRATEGIC STUDIES
TEL AVIV UNIVERSITY
אוניברסיטת תל-אביב

לוחמה במרחב הקיברנטי
מושגים, מגמות ומשמעויות לישראל

שמואל אבן ודוד סימן־טוב

המכון למחקרי ביטחון לאומי

המכון למחקרי ביטחון לאומי, המשלב בתוכו את מרכז יפה למחקרים אסטרטגיים, הוקם ב־2006.

מטרותיו של המכון למחקרי ביטחון לאומי, הן שתיים: הראשונה – לבצע מחקר בסיסי, העומד במבחן אמות המידה האקדמיות הגבוהות ביותר והעוסק בתחומי הביטחון הלאומי של ישראל, המזרח התיכון והמערכת הבינלאומית. השנייה – לתרום לדיון הציבורי ולעבודת הממשל בנושאים הנמצאים – או אמורים להימצא – בראש סדר היום הביטחוני של ישראל.

קהל המטרה של המרכז הוא: דרג מקבלי ההחלטות, מערכת הביטחון, מעצבי דעת הקהל בישראל, הקהילה האקדמית העוסקת בתחומי הביטחון, בישראל ובעולם, והציבור המתעניין באשר הוא.

שמואל אבן ודוד סימן־טוב

לוחמה במרחב הקיברנטי
מושגים, מגמות ומשמעויות לישראל

מזכר 109 יוני 2011

המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
INCORPORATING THE JAFFEE CENTER FOR STRATEGIC STUDIES
TEL AVIV UNIVERSITY אוניברסיטת תל-אביב

Cyber Warfare:
Concepts, Trends, and Implications for Israel

Shmuel Even and David Siman-Tov

המכון למחקרי ביטחון לאומי
חיים לבנון 40
ת.ד. 39950
תל־אביב 61398

טל': 03-640-0400
פקס: 03-744-7590

דוא"ל: info@inss.org.il
http://www.inss.org.il

ISBN: 978-965-7425-24-4

הביא לדפוס: משה גרונדמן
עיצוב גרפי: מיכל סמו־קובץ ויעל ביבר, המשרד לעיצוב גרפי
אוניברסיטת תל-אביב
עיצוב השער: מיכל סמו־קובץ
דפוס: קדם, תל־אביב

תוכן העניינים

פרק ד: משמעויות מערכתיות לישראל

נספחים

עיקרי הדברים

המרחב הקיברנטי הינו מרחב לחימה חדש, המצטרף למרחבי היבשה, הים האוויר והחלל בשדה הקרב המודרני. במזכר זה מתוארים מאפייניו הייחודיים של מרחב הלחימה החדש, מוצעים פירושים חדשים למושגים מסורתיים, ונסקרים האירועים וההתארגנויות בתחום הקיברנטי בעולם ובישראל. מחברי המזכר מציעים לישראל להאיץ את התארגנותה אל מול האתגר החדש כדי לשפר את ההגנה על המרחב הקיברנטי שלה.

מדינות מודרניות וצבאות מתקדמים בעולם מגבירים את פעילותם במרחב הקיברנטי, המהווה בעבורם מקור עוצמה, אך גם חושף "בטן רכה". למשל, התשתיות החיוניות לתפקוד המדינה (חשמל, תקשורת, מים, תחבורה, כספים ועוד) הנשענות על מרחב זה; רשתות הפיקוד, השליטה והבקרה הצבאיות תלויות במרחב הקיברנטי וכך גם הטכנולוגיות המתקדמות ביותר של שדה הקרב המודרני. עם אלה נמנות: מערכות איסוף, עיבוד והיתוך מידע; ניצול לוויינים בשדה הקרב; הפעלת כלי לחימה אוטונומיים; שילוב בין חיישנים המזהים מטרות לבין מערכות אש בזמן אמיתי ועוד.

למרחב הקיברנטי, כמרחב לחימה, יש תכונות ייחודיות המאפשרות לפעול במהירות של אלפיות השנייה נגד אויבים המצויים במרחק רב מן המדינה, ובלי לסכן לוחמים. התכונות הייחודיות של המרחב עושות אותו אטרקטיבי ללחימה גם בתקופות שבין מלחמות קונבנציונליות. אפשר להבחין בין עימותים המתרחשים במרחב הקיברנטי (כמו המתקפה המיוחסת לרוסיה על אסטוניה בשנת 2007) לבין מלחמות שבהן תקיפה במרחב הקיברנטי היא רכיב במלחמה בצד כוחות אחרים (כמו המתקפה של רוסיה על גאורגיה בשנת 2008). כמו כן אפשר להבחין בין תקיפות שנעשות בתוך המרחב הקיברנטי (פגיעה במערכות תקשוב) לבין שימוש במרחב כאמצעי על מנת לפגוע בתפקודן של מכונות הפועלות במרחבים הפיסיים. לדוגמה: תקיפה קיברנטית של פרויקט הגרעין של איראן, שהתרחשה בשנת 2009. אירוע זה ("סטאקסנט") המחיש את עוצמתו הפוטנציאלית הרבה של הנשק הקיברנטי ונחשב לאירוע מכונן בהתפתחות המרחב הקיברנטי כמרחב לחימה.

כמה מאירועי התקיפה הקיברנטיים ותהליכי התארגנות של מדינות במרחב הקיברנטי מעידים, שמירוץ החימוש הקיברנטי כבר החל! כחלק ממירוץ זה הוקמו בשנים האחרונות משרדים ומטות במדינות שונות, העוסקים במרחב הקיברנטי כמרחב

לחימה, וגובשו אסטרטגיות ביטחוניות לפעולה במרחב הקיברנטי (בארצות־הברית, בריטניה, צרפת, גרמניה, סין ועוד). נראה שמעתה עשויה לוחמה קיברנטית ליטול חלק בכל מלחמה מודרנית. יחד עם זאת, בפני מדינות ניצבים גם שיקולים מרסנים מפני ביצוע התקפות קיברנטיות, למשל: אי־ודאות לגבי תוצאות ההתקפה וסיכון לספוג התקפת נגד, בשעה שהגנתן עדיין אינה חזקה דיה. בנוסף, גופים חוץ־מדינתיים כארגוני טרור עלולים להשתמש במרחב הקיברנטי לביצוע התקפות, כאשר ישיגו יכולת לגרום נזק ניכר.

בה בעת מתפתחת הכרה בינלאומית, שיש להגן על המרחב הקיברנטי לטובת הכלל ולהסדיר את הפעילות בו, בדומה להסדרת הפעילות במרחבים האחרים; וזאת באמצעות שיתוף פעולה בין מדינות, התאמת כללי הדין הבינלאומי וגיבוש אמנה בינלאומית מחייבת. לפי שעה מתקדמת פעילות זו בעצלתיים ואינה מדביקה את קצב ההתפתחויות במרחב הקיברנטי.

בהקשר הישראלי. לטכנולוגיות המידע ולמרחב הקיברנטי תרומה מכרעת ליתרון האיכותי של ישראל בתחומי הביטחון והכלכלה. המרחב הקיברנטי חיוני לחברה, לקשר שבין הממשל לבין האזרחים ולקשרי ישראל עם העולם. ואף יותר מכך, יש לו חשיבות רבה לביטחון הלאומי של ישראל בהתחשב באיומים הקיברנטיים המתהווים, ביתרונה של ישראל בתחומי טכנולוגיות המידע ובפוטנציאל שמגלם המרחב הקיברנטי בשדה הקרב המודרני.

צה"ל עשה צעד חשוב בהכירו בשנת 2009 במרחב הקיברנטי כמרחב אסטרטגי ואופרטיבי חדש. בעקבות זאת הקים את "מטה הסייבר" המטכ"לי לתיאום ולהכוונה של פעולותיו במרחב (תהליך דומה היה בארצות־הברית, שהקימה את "פיקוד הסייבר" במשרד ההגנה). יחד עם זאת, נראה שהמושגים המסורתיים של תפיסת הביטחון של ישראל אינם מתאימים למרחב הלחימה החדש, ויש לעדכנם או לפתח מושגים מסדירים חדשים. למשל, "הסביבה האסטרטגית" במרחב הקיברנטי שונה מהמושג המקובל בישראל, המתבסס על מעגלי האיום הגיאוגרפיים המסורתיים. ההתייחסות ל"זמן ומרחב" במרחב הקיברנטי שונה, מאחר שמהירות הפעולה בו נמדדת באלפיות שנייה. המרחב הקיברנטי מעצים את יכולתם של שחקנים קיימים ומאפשר לשחקנים חדשים לבטא יכולת קיברנטית התקפית (כאלה שלא נטלו חלק במערכות קודמות בשל מגבלות גיאו־פוליטיות או נחיתות צבאית קונבנציונלית).

ההרתעה, שהיא יסוד ראשון בתפיסת הביטחון המסורתית של ישראל, קשה ליישום בייחוד במרחב הקיברנטי בשל הקושי לזהות מי אחראי לתקיפה, ומשום כך קשה שבעתיים לקבוע וליישם מדיניות תגובה מרתיעה. בנוסף, ההיסטוריה הקצרה של אירועי תקיפה קיברנטיים טרם סימנה "תגי מחיר", והשגת הרתעה מחייבת חשיפת יכולות קיברנטיות רגישות, שעלולה לגרום לאובדן ערכן.

הגנה היא אתגר מסוג חדש במרחב הקיברנטי, בין היתר נוכח היכולת של האויב לבצע מתקפה במהירות הבזק והקושי לזהות את התוקף. על מענה מסוים לאתגר זה יכולה ישראל ללמוד מתפיסת "ההגנה האקטיבית" הקיברנטית של ארצות־הברית. תפיסה זו מתבססת על יכולות מודיעיניות מתקדמות לזיהוי פעולות ברשת, על מערכות הגנה דינמיות (מערכות ממוכנות לזיהוי תקיפה ולתגובה אוטומטית בלי מעורבות אנושית) ויכולות התקפיות לצורכי סיכול. עם זאת, יודגש כי הגנה יעילה אינה מתבססת על טכנולוגיה מתקדמת בלבד, אלא גם על ארכיטקטורת רשת יעילה, נהלים, תרבות (מודעות לסיכונים, משמעת קפדנית וכו'), אבטחה פיסית, ובקרה אנושית.

התרעה מודיעינית היא אתגר שונה במרחב הקיברנטי לעומת התרעה מפני מלחמה קונבנציונלית. הכנות למתקפה קיברנטית עשויות להתנהל בחדרי חדרים על ידי צוותים קטנים וחשאיים, הרחק מהיעד, ועל כן קשה לצפות לדליפת מידע מוקדם, שישמש בסיס להתרעה, זאת לעומת הכנות למתקפה של צבא קונבנציונלי. לעתים אפילו קשה לדעת בזמן אמת שהתקפה כבר החלה. ואכן נראה שעד כה בוצעו ההתקפות הקיברנטיות המוכרות בהפתעה מוחלטת.

במישור הלאומי, ב־18 במאי 2011 הכריז ראש הממשלה בנימין נתניהו על הקמת **"מטה סייבר לאומי"**. לפי הודעת משרד ראש הממשלה: "ייעודו העיקרי של המטה הוא להרחיב את יכולות ההגנה של המדינה על מערכות התשתיות החיוניות מפני התקפות טרור קיברנטי, המבוצעות הן בידי מדינות זרות והן בידי גורמי טרור". המטה יוקם בנוסף ומעל הגופים הממלכתיים האופרטיביים האזרחיים הפועלים בתחום, כגון: "הרשות הממלכתית לאבטחת מידע" בשב"כ ופרויקט "תהיל"ה", המספק שירותי גלישה מאובטחים למשרדי הממשלה ומוסדותיה. טרם פורטו תפקדי מטה הסייבר העתיד לקום, סמכויותיו ומיקומו.

נראה כי האתגר העיקרי העומד לפתחו של מטה הסייבר הלאומי העתיד לקום הוא יצירת מערכת הגנה קיברנטית לאומית אינטגרטיבית. זהו אתגר החורג מהגנה על תשתיות לאומיות קריטיות מסורתיות והינו בעל רמת מורכבות גבוהה במיוחד. בשונה מתחומי לחימה אחרים ואף מהתחום ההתקפי הקיברנטי, המצויים בחצרה של מערכת הביטחון, כינון מערכת הגנה קיברנטית יעילה מחייב שיתוף פעולה בין המגזר האזרחי (הציבורי והפרטי) לבין המגזר הביטחוני, משום שבתחומים רבים קשה להפריד בין התשתיות הקיברנטיות האזרחיות לבין התשתיות הצבאיות. בד בבד נדרש שיתוף פעולה בין המגזר הציבורי (הצבאי והאזרחי) לבין המגזר הפרטי, שכן חלק ניכר מהיכולות הקיברנטיות של המדינה נמצא בידיים פרטיות, כגון חברות טכנולוגיה עילית, חברות תקשורת, חברות אבטחה, חברות תשתיות חיוניות ועוד. כן נדרש שיתוף פעולה עם מדינות אחרות. באמצעות רשתות ניטור משותפות ושיתוף

פעולה מודיעיני ניתן לשפר את יכולת ההתרעה, יכולת לעקוב אחר נתיב התקיפה ולאתר את מקורה, ויכולת התגובה.

לאור זאת, מציעים כותבי המזכר לכלול, בין תפקידיו של מטה הסייבר הלאומי, את התפקידים הבאים:

א. סיוע לדרג המדיני בקבלת החלטות ובעיצוב מדיניות בתחום הגנת המרחב הקיברנטי הלאומי. בכלל זה, גיבוש הצעה לאסטרטגיה לאומית להגנת המרחב הקיברנטי, בשיתוף עם הגורמים הרלוונטיים, אשר תאושר בידי הקבינט המדיני־ביטחוני.
ב. הערכות סיכונים – שוטפות ועיתיות, בהסתמך על נתונים והערכות, שיספקו גופי המודיעין והגופים האופרטיביים והטכנולוגיים הרלוונטיים.
ג. הערכות מצב – שוטפות ועִתיות, ובכלל זה המלצות לפעולה על סמך ניתוח חלופות.
ד. הוראת האסטרטגיה לגופים האזרחיים המשתתפים בהגנה על המרחב הקיברנטי ותיאום עם הגופים במגזר הביטחוני.
ה. תיאום הפעולות של כל הגורמים הממשלתיים והפרטיים הנוגעים לביטחון המרחב הקיברנטי. בכלל זה הטלת אחריות על משרדי הממשלה האזרחיים לקדם את הביטחון הקיברנטי בתחומם (כפי שעושים למשל משרד האוצר והמפקח על הבנקים בבנק ישראל כלפי גופים פיננסיים מוסדיים).
ו. הקמת מרכז אופרטיבי מדינתי ("מרכז מבצעים" קיברנטי) וניהולו. תפקידו יהיה ליצור תמונת מצב דינמית של איומים קיברנטיים, לשתף מידע בין כל הגופים הנוגעים בדבר ולסייע בניהול ההגנה.
ז. קביעת מערכות התשתית והגופים האזרחיים, שעל המדינה להנחותם או לאבטח אותם בתחום הקיברנטי, בהתאם לאסטרטגיה הלאומית.
ח. ייזום חקיקה ותקנות, החיוניות לפעולות לשם הגנת המרחב הקיברנטי בשגרה ובחירום.
ט. ייזום והובלת פרויקטים ממשלתיים, למשל פרויקטים בנושאים האלה: שדרוג שיטות ואמצעי ההגנה על מערכות המידע (בכלל זה אבטחה פיסית), כינון מערכת ממוסדת להדרכה של עובדים בסקטור הממשלתי, שיפור יכולת ההתאוששות לאחר התקפה קיברנטית, ניהול תרגילי הגנה קיברנטיים ברמה לאומית.
י. קביעת קריטריונים לפיתוח, לרכש ולהתקנת אמצעי תקשוב, בהיבטים של ביטחון קיברנטי.
יא. מתן אישורים להקמת תשתיות תקשוב, בהקשר להשפעתן על ביטחון המרחב הקיברנטי הלאומי.

יב. ייזום והכוונה בתחום פיתוח אמצעי הגנה, הכשרת כוח אדם מקצועי ומחקר מדעי בהקשר לביטחון המרחב הקיברנטי. בכלל זה הענקת תמריצים לגופי מחקר.

יג. ייזום שיתופי פעולה אסטרטגיים בין הסקטור הממשלתי לבין הסקטור הפרטי. בכלל זה שיתוף פעולה עם חברות תקשורת וטכנולוגיה בתחום התפעולי ובתחומי המחקר והפיתוח.

יד. ריכוז שיתוף פעולה עם מדינות אחרות בנוגע לביטחון המרחב הקיברנטי.

טו. בקרה על יישום האסטרטגיה ועל הפעילות בתחום הגנת המרחב הקיברנטי. וידוא קיום פיקוח ראוי על משרדי הממשלה השונים והרשויות האזרחיות, פיקוח על ספקי תקשורת מבחינת ציוד ויישום כללי ביטחון קיברנטי.

טז. שיפור התגוננות של התושבים במדינה – באמצעות צעדי הסברה, מתן תמריצים להצטיידות בתוכנות הגנה (למשל, הקלות במס), ופיקוח על רמת השירות שנותנים ספקי תקשורת וחברות אבטחה לאוכלוסייה.

יז. להוות מרכז ידע לאומי בתחום הגנת המרחב הקיברנטי, המקושר אל מרכזי ידע בארץ ובחו"ל. בכלל זה למידה של דרכי ההתמודדות של מדינות אחרות עם האתגר הקיברנטי.

לישראל יכולת להיות בין המדינות המובילות בעולם בתחום הביטחון הקיברנטי, לנוכח ההון האנושי והידע הטכנולוגי הגבוהים שבידיה. מיצוי היכולת עשוי לתרום למדינה בתחומי הביטחון והכלכלה.

המחברים מודים לד"ר עמוס גרנית, ראש המכון לחקר המודיעין באמ"ן, על הערותיו המועילות.

המזכר נכתב במסגרת תכנית המחקר לוחמה קיברנטית בראשות פרופ' יצחק בן ישראל וד"ר גבי סיבוני. התכנית נתמכת על ידי קרן ג'וזף וג'נט ניובאוואר, פילדלפיה, ארצות הברית.

מבוא

קפיצה לעתיד: מערכת ההתרעה הקיברנטית של ישראל זיהתה מתקפת "פצצות לוגיות" (תוכנות זדוניות), שכוונה לעבר שתי תחנות כוח. החיישנים הפעילו אוטומטית ובמהירות הבזק מערכות יירוט, ואלה נטרלו את רוב התוקפים (פעולות במרחב הקיברנטי נעשות במהירות של אלפיות השנייה ובקצב שמעורבות אנושית אינה רלוונטית).

כמה פצצות לוגיות חדרו בכל זאת את מערך ההגנה ופגעו במערכת הבקרה באחת התחנות. נגרם נזק לתוכנות, אך למרבה המזל הנזק טרם פרץ למרחבים הפיסיים. באותו רגע הופעל אוטומטית מנגנון ה־Roll Back של תחנת הכוח, והחזיר את תצורת המחשוב באלפית השנייה לאחור, למצבה כפי שהיה לפני פגיעתן של הפצצות הלוגיות (בהיותו וירטואלי, המרחב הקיברנטי הוא היחיד המאפשר "חזרה בזמן" – חזרה לתצורת העבר). בו בזמן הופעל מנגנון "ניתוק הזרם", המפסיק את פעולות מערכות התקשוב ביעדים אזרחיים חיוניים, שנקבעו מראש. באותו הזמן בקירוב הצליחה מערכת ההגנה האווירית ליירט טיל בליסטי, שכוון לחוות השרתים של חברת הטלפוניה הלאומית. כך ניצל המרחב הקיברנטי המדינתי, שקיומו תלוי בתשתיות תקשורת ובאנרגיה חשמלית. למרות זאת, חברת הטלפוניה המספקת שירותי תקשורת אישית (סלולארית, לווינית) לצבא נפגעה קשות. הדבר שיבש את תפקודו באופן חמור משהיה צפוי.

אירועים אלו היו חלק מהתרחישים שנבחנו בתרגיל לאומי להגנת המרחב הקיברנטי בשנת 2016. התרגיל צוין כהצלחה גדולה. הפעם, שלא כמו בתרגילים בשנים קודמות, חל שיפור ניכר בתפקודם של מנגנוני ההגנה המדינתיים, בהעברת מידע בין הגופים ובתיאום בין המערכות האזרחיות לצבאיות. עם זאת הודגש, שמערכת ההגנה הלאומית מספקת מענה להגנת תשתיות לאומיות חיוניות ולמערכת הביטחון, אך אינה נותנת מענה מספק לחלקו הגדול של המרחב הקיברנטי המדינתי, המצוי בידי המגזר הפרטי. ראש הממשלה שביקר בתרגיל אמר, שכל אזרחי המדינה זכאים להגנה ולחופש פעולה במרחב הקיברנטי, כפי שהמדינה מספקת הגנה במרחבים האחרים. לפיכך הוחלט להתקין על השרתים בכניסה למדינה מערכת הגנה המבוססת על השהיה רגעית של התקשורת הנכנסת (Delay line), כך שיתאפשרו סיכול והפעלת מנגנון ה־Roll Back ברמה הלאומית. כן הוחלט לשפר את מערכת הניתור המשותפת לישראל למדינות שמצויים בהן צומתי תקשורת המובילים אליה.

תרחיש זה אינו תחזית. הוא נועד להמחיש על קצה המזלג את אופיו המיוחד של המרחב הקיברנטי ואת האתגר הטמון בו למדינת ישראל – ובכך נעסוק בהרחבה במזכר הזה.

פרק א

המרחב הקיברנטי והשדה הביטחוני – מסגרת מושגית

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; שימוש המוני ברשת האינטרנט ובמחשבים אישיים מאמצע שנות התשעים; 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 הן 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 לידי סיקור 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 מידית 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 ומוסדות בינלאומיים, לעתים 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.

סוכנות האו"ם ITU (International Telecommunication Union) מגדירה את המרחב הקיברנטי כדלהלן: המתחם הפיסי והלא פיסי, 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 פיסי: הרכיבים הפיסיים של הרשת: חומרה, תשתיות ניידות ותשתיות נייחות; המצויים במרחבי היבשה, הים, האוויר והחלל (להלן "המרחבים הפיסיים").

למרחב הקיברנטי הגדרות נוספות. הגם שכולן מכירות בכל שלושת הרבדים (האנושי, הלוגי והפיסי) 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 (הפיסי), 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 פיסית 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

לוח 1: שלושת הרבדים במרחב הקיברנטי

הרובד	סוג פעילות ברובד ותכליתה	תוכן (דוגמאות)	מגמות התפתחות (דוגמאות)
1. רובד המשתמש			
א. הרובד האנושי	שימוש אנושי במוצרי תקשוב.	קריאה, סחר, השקעות, דליית מידע, חילופי מידע, קשר עם חברים, קשר בין אזרחים למשרדי ממשלה. פשיעה, לוחמה קיברנטית.	עלייה בתופעת קהילות משתמשים (WEB2), ובשימוש במכשור נייד ואינטגרטיבי (הטלפון החכם); תחילת שימושים מתוחכמים ברשת (WEB3).
2. הרובד הלוגי	פעולת תוכנות		
א. ממשק משתמש גרפי (GUI)	תרגום מידע משפת משתמש לשפת מחשב (מידע דיגיטלי), ובחזרה.	דפי טקסט, תמונות, סרטים, שמע, כפתורי הפעלה.	עלייה בסוגים וברמות האפליקציות המיוצגות בממשק. עלייה בייצוג הגרפי. מעבר ל-D3.
ב. תוכנות יישום	עיבוד מידע שמגיע מממשקי משתמש, תוכנות ניהול רשתות.	הוראות ותרשימי זרימה בשפת תכנות (אלגוריתמים).	יותר אפליקציות. יותר ויותר רובדי תוכנה בין החומרה לממשק המשתמש.
ג. מערכות הפעלה	"הרצת" תוכנות ותרגום משפת מחשב לשפת מכונה.	מידע בשפת תכנות הרלוונטית לשכבה.	
3. הרובד הפיסי			
א. חומרה	תשתית פיסית אלקטרומגנטית, שמבצעת פעולות מכונה.	שבבים, כרטיסים אלקטרונים וכו'. זרמים חשמליים.	גידול בנפח המידע על רכיבים אלקטרונים, מזעור, ניידות, זיכרון פלש (שבב השומר מידע ללא מתח חשמלי).
ב. מערכות תקשורת ואנרגיה (תשתית אלקטרומגנטית)	מספקות תנאים לקיום ופעילות התקשוב במרחב האלקטרומגנטי.	תשתית ותחזוקה. פריסת כבלים, אותות RF, גלי אור וחשמל.	גידול במגוון ופריסת מערכות תקשורת: תקשורת סלולאר, בלוטוס, ראוטר, לוויינית, כבלים ימיים. שיפור ניצול אנרגיה ומזעור.
ג. אמצעים נושאי חומרה ותוכנה	מספקים תנאים נוספים לקיום המרחב הקיברנטי במרחבי היבשה, הים, האוויר והחלל.		מחשבים וטלפונים חכמים; מתקנים, מערכות וכלים שמשובץ בהם מחשב; ציוד שמוטמעים בו מעבדים ובקרים; וכן אמצעים הנושאים אמצעי קלט (סורקים), סנסורים ואפקטורים. באזור זה מתרחש הקישור בין המרחב הקיברנטי לבין המרחבים הפיסיים.

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 הפיסיים 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 וארגון 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 והפיסי) 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 הפיסיים הנשלטים מהמרחב הקיברנטי. לדוגמה, שיבוש מנגנון בקרה תרמי, שיוביל לפיצוץ מפעל ביטחוני (אפקט במרחב היבשתי), או שיבוש מד גובה, שיוביל לפגיעה בכלי טייס (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 הפיסי – 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 שפרסם 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" האמריקני;[10] הרצאה של הגנרל בדימוס מייקל היידן (לשעבר ראש ה־NSA[11] וה־CIA) בכנס אבטחה Black Hat, שהתקיים בסוף יולי 2010 בלאס וגאס.[12] כמו כן, אפשר ללמוד על כך ממסמכים רשמיים שפרסמו הממסדים הביטחוניים בארצות־הברית ובמערב אירופה, ממאמרים אקדמיים ומהתבטאויות של בכירים ומומחים באמצעי 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 הפיסיים. 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 פיסיות 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 הפיסיים.

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 אוכלוסיה 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 מעבר למתוכנן.

ויראליות. 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 אמנם 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 הפיסיים 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 הפיסיים 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 פיסי, שגורמת תקיפה מסיבית באש. עם זאת, כאמור, גם התקפות קיברנטיות מסוימות עלולות לגרום נזקים פיסיים 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, שלעתים 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 ועוצמתה. זהו אתגר גדול לתוקף החותר להגיע להישגים אסטרטגים באמצעות מתקפה קיברנטית ממושכת ורחבת היקף. בשל קושי זה, יש חוקרים הסבורים, כי פוטנציאל הנזק לאויב או ההישג לתוקף, המיוחס להתקפות במרחב הקיברנטי, נמוך 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'). בנוסף, 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 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 לנוכח 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 שימוש במשאבי התקשוב של היריב כדי לתקוף את מערכותיו. עם זאת, מאפשרת הקישוריות למגן להסתייע במדינות ידידותיות, כדי לאתר התקפות ולסכלן טרם שהגיעו למדינה.

תלות הדדית בין המרחב הקיברנטי למרחבים הפיסיים. המרחב הקיברנטי מקיים תלות דו־כיוונית עם המרחבים הפיסיים: מצד אחד הוא מעצים פעולות במרחבים אלו ומצד אחר אפשר לפגוע ביעדים במרחבים אלו באמצעותו. כלומר, פגיעה קינטית בתשתיות פיסיות, 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 ומשאבי מחשוב באופן ייחודי, שאינו אפשרי במרחבים הפיסיים. 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 מחייבת 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 ההגנה 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 וארגונים.
ג. ההון הנדרש לפיתוח יכולות התקפיות נמוך בשיעור ניכר לעומת ההון הנדרש להקמת צבא קונבנציונלי 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 אמנם 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 הפיסיים, 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, מירוץ 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 ומקומם 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 לצרכי 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 לנזק או הרס לאויב. בכלל זה נזק למערכות תקשוב או ליעדים במרחבים הפיסיים, באמצעות פגיעה במכונות הנשלטות מהמרחב הקיברנטי או 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 המגנים 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 ולשבש את מערכות האויב, ואף לא להשפיע עליו במישרין.[18] לשימוש במרחב הקיברנטי לצרכי 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 וכוונותיו, בעת שיגרה ובמלחמה; זאת לצרכי 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 שיכפול וללא הוצאתו מרשות היריב.

יש לציין כי בעולם שבו לעוצמות כלכליות וטכנולוגיות משמעויות מרחיקות לכת על מאזני הכוח האסטרטגיים, לאיסוף ולליקוט של מידע ונכסים קיברנטיים טכנולוגיים וכלכליים עשויות 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 על תחום שבו פעולות האיסוף חורגות מהצורך המסורתי לאסוף מידע כדי להכיר את היריב ולעמוד על יכולותיו וכוונותיו.

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 למוסקווה, 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, תוך שימוש בהתקן נתיק (דוגמת 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."

יתכן שתיאור זה נוגע לחדירה המיוחסת לסין, שבמהלכה נגנבו תוכניות של מטוס הקרב העתידי F-35 Lightning II מתוצרת לוקהיד מרטין, לרבות תוכניות מערכות האלקטרוניקה של המטוס המתקדם בעולם, שבפיתוחו הושקעו 300 מיליארד דולר.[21]

לין אפיין 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 אמנם אינן בעלות השפעות דרמטיות כמו התקפות קונבנציונליות, 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, הונאה, תעמולה וחשיפה 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 וידידים, 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 הפיסי, 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 האמריקנים להרחיבה במסגרת המלחמה בגורמים אסלאמיים עוינים בפקיסטן, באפגניסטן, באיראן ובחבי המזרח התיכון. כן פתחו האמריקנים 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 והמערב. כחלק ממאמץ זה מפותחות תוכנות שיאפשרו להתערב בחשאי ברשתות

החברתיות. למשל, חברה אמריקנית 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, כגון 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 עמם, 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, כגון 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, פעולות אסורות, התבטאויות מביכות של מנהיגים וכד'. בתחום זה בולטת פעילות של יחידים וארגונים 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", 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 כחלק ממכלול של סנקציות על מדינה "סוררת", או כחלק מגיבוש כללי משחק במרחב הקיברנטי. כך למשל סיפר מייקל היידן, כי בעבר שקל הממשל האמריקני אפשרויות פעולה נגד מדינות שמתחומן יוצאות התקפות קיברנטיות על ארצות־הברית בכלל זה סוגים של נידוי קיברנטי, או תגובה שתאיים 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 כדוגמת כיבוש שטחים בידי צבא יבשה, אך היא מסוגלת לפגוע ביעדים חיוניים של האויב וביכולותיו. בעדותו בקונגרס באפריל 2010 מנה מפקד פיקוד הסייבר האמריקני 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 קונבנציונליות. וכך עשויות התקפות קיברנטיות לשמש לתכליות האלה:

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

למרות שנושא ההתקפה במרחב הקיברנטי אינו מוסדר מבחינת המשפט הבינלאומי, עשויה פעילות קיברנטית התקפית להיחשב אקט מלחמתי, לעומת פעולות ריגול קיברנטי, שאין עמן נזק מידי 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'), כגון תקיפת סטאקסנט באיראן (ניתוח אירוע זה יוצג בהמשך).

בכירים אמריקאים מדגישים, כי לתוקפים הקיברנטיים יש כיום יתרון על המגנים. 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 לפני שנה. למרות זאת, תוכנת זדון של 125 שורות קוד, שאורכה כפי שהיה אשתקד, מסוגלת לחדור תוכנת אנטי־וירוס. ויליאם לין מבחין בין תקיפות קיברנטיות שתכליתן שיבוש מתוחם בזמן ובהיקף, דוגמת תקיפות האקרים או השבתה של אתר באמצעי תקיפה פשוטים למדי, לבין תקיפה שתכליתה ליצור 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 שאפיין את העידן הגרעיני, טוען ויליאם לין, שיש קווי דמיון ביניהם. המרחב הקיברנטי נותן בידי יריבים אפשרות וכלים קונבנציונליים לאיים על ארצות־הברית. התקפה כזאת אמנם לא תגרום לנפגעים המוניים, אולם היא עלולה לשתק את החברה האמריקנית 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, כגון 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 אוניברסאליות, או מבפנים, באמצעות סוכן הפועל בארגון, או בשילוב – חדירה לרשת מקומית בסיוע סוכנים. במשפחה זו של תוכנות זדוניות ישנם סוגים של תוכנות, כגון "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, לעתים בשירות המפעיל ולעתים 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 אמנם הפיך, אולם לא כך הנזקים הכלכליים שנגרמו בעת ההתקפה ואובדן האמון במערכת. לין ציין, שהתקפות 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 האמריקני כדי לפעול נגד מדינות שמהן יוצאות תקיפות כלפי ארצות־הברית, שכן תקיפה מסוג זה עומדת בהגבלות של אמנת ז'נבה.[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 למרחב הקיברנטי הואיל ולא בכל מקרה ידוע מי אחראי לתקיפה, והתוקף עלול לעשות שימוש בתשתיות של צד שלישי. בנוסף, 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 אזהרה שהשמיעה מזכירת המדינה הילארי קלינטון כלפי סין,[33] ביצוע פעולות תקיפה מוגבלות על אויבים כדי להמחיש יכולת, ולו במחיר

לוח 2: סוגי ההתקפות במרחב הקיברנטי

התקפה	מאפיינים
1. שיבוש התקשוב של היריב.	התקפות שאינן משנות את תצורת המחשוב, אך יוצרות עומס מלאכותי על המערכת, הגורם שיתוק ושיבוש פונקציונאלי לפרק זמן מסוים. למשל, התקפות מסוג "מניעת שירות" (DDoS).
2. פגיעה בתקשוב של היריב.	התקפות הגורמות נזק והרס לתקשוב. הן משנות את תצורת התקשוב או את בסיסי המידע, ומונעת מהיריב לנצל את המרחב הקיברנטי לתועלתו.
3. שימוש במרחב הקיברנטי של היריב כדי לפגוע במכשירים המחוברים למרחב הקיברנטי או לגרום באמצעותם נזק והרס.	התקפות שאינן אמורות לשנות בהכרח את תצורת התקשוב משום שהן זקוקות למרחב הקיברנטי לצורך ההתקפה על מערכות משובצות מחשב (תשתיות חיוניות, אמצעי לחימה).

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 ותשתיותיו. ההגנה במרחב הקיברנטי אמורה להתמודד עם מגוון רחב של חדירות – החל בחדירות לצרכי איסוף וכלה במתקפות קיברנטיות. מגוון האויבים שעמם אמור מערך ההגנה להתמודד הוא: 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 לידי כישלון ההגנה. המרחב הקיברנטי מעצים גם יכולת של גורם עוין לנצל פרצות במערך ההגנה לתועלתו, ומערכות האבטחה הן לעתים 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 כגון: יתירות (יכולות עודפות וגיבויים), בידוד מערכות מידע מסוימות, בידול בין מערכות, פריסת מערך אבטחת מידע קונבנציונלי בכמה שכבות, אבטחה פיסית של מערכות המידע, ונוהלי ביטחון מידע נוקשים ומשתנים ותרבות המשתמשים.

מענה (חלקי) לאתגר מהירות התקיפה הקיברנטית נמצאת 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, דרכי פעולה וכלים העומדים לרשות האויב.

עם זאת, האתגר שונה בנוגע להתרעות אופרטיבית וטקטיות, שבהן נדרשת התייחסות לפרטי ההתקפה ועיתויה. את ההכנות למתקפה במרחב הקיברנטי אפשר לערוך בחדרי חדרים, להבדיל מהכנות נרחבות הדרושות להכנת גייסות קונבנציונליים למלחמה, הכרוכות לרוב בדליפת מידע. לעתים קשה לדעת בזמן אמת שהתקפה קיברנטית כבר החלה, בטרם נגלות תוצאותיה ולעיתים תוצאותיה לא יתגלו כלל (יחשבו כתקלה). 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, לוחמה אלקטרונית ולוחמת מסרי מידע. במקרים מסוימים הלוחמה הקיברנטית עשויה להיות מגמה ראשית (מאמץ עיקרי), שרכיבי כוח אחרים יסייעו לה, ובמקרים אחרים יכולה להתבצע לוחמה קיברנטית כמגמה מסייעת 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 לנוכח 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 3: 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.
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 השלטון.
3. סנקציות קיברנטיות	א. נידוי קיברנטי של היריב כדי להביאו לידי שינוי 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 וזמני 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.

פרק ב

אירועי תקיפה וגורמים מרסנים במרחב הקיברנטי

לאחר הכרת אופיו של שדה הקרב הקיברנטי ומושגיו, נסקור בקצרה את ההיסטוריה של תקיפות במרחב הקיברנטי המיוחסות למדינות. יוזכר שקטגוריה זו אינה כוללת אירועי חדירה קיברנטית לצורכי ריגול, לוחמה פסיכולוגית ופשיעה. מתברר כי רשימת אירועי התקיפה, המיוחסים למדינות היא קצרה ודלה. כמו כן, אף על פי שבמדינות המערב קיימת ציפייה דרוכה לטרור קיברנטי, עד כה לא ידוע על תקיפה קיברנטית משמעותית שביצע ארגון טרור.

הערכות המופיעות בפרסומים השונים בדבר זיהוי המדינה העומדת מאחורי מתקפה מסוימת, אינן נשענות על עדויות מוצקות אלא על הערכות מומחים, המבוססות על ניתוח מניעים, היקף הפעילות, תחכום האמצעים וכו'. עד היום אף מדינה או ארגון טרור לא קיבלו אחריות על תקיפה קיברנטית.

אירועי תקיפה בולטים במרחב הקיברנטי

האירוע הראשון של תקיפה קיברנטית מיוחס להחדרת תוכנה זדונית בידי ה־CIA של ארצות־הברית למערכת בקרה ממוחשבת מתוצרת ארצות־הברית, שנגנבה בידי רוסים והועברה מקנדה לברית־המועצות. מערכת הבקרה הותקנה בידי הסובייטים בצינור הגז הטרנס־סיבירי ביולי 1982. לאחר התקנתה אירע פיצוץ בצינור הגז, שנגרם בשל פעולת התוכנה הזדונית, וזה תואר כפיצוץ הלא־גרעיני האדיר ביותר שנצפה אי פעם מהחלל. על פי המדווח, מטרת המבצע הייתה לבלום את התופעה של גנבת טכנולוגיות וקניין רוחני בידי ברית־המועצות. ניתן לראות באירוע הזה ניצן ראשון של המלחמה במרחב הקיברנטי.[37]

אירועי התקיפה הראשונים המשמעותיים ברשת המודרנית מיוחסים לרוסיה. בשנת 2007 הותקפו אתרי אינטרנט ממשלתיים רבים באסטוניה ופעילותם הושבתה ליומיים. בתקיפה נעשה שימוש בשיטת "מניעת שירות" (DDoS). מבחינת אסטוניה, שהיא אחת המדינות המתקדמות בשימוש במחשבים ובאינטרנט, זו הייתה פגיעה של ממש ביכולת המשילות של השלטון. השימוש הניכר במחשבים התגלה כנקודת

תורפה נוכח ההתקפה הרחבה שהתרחשה כולה במרחב הקיברנטי.[38] העילה למתקפה הקיברנטית הרוסית הייתה העתקת אנדרטת זיכרון לחללי הצבא האדום ממלחמת העולם השנייה ממרכז הבירה טלין לפרברי העיר. בעקבות התקיפה חתמה נאט"ו על הסכם לשיתוף פעולה עם אסטוניה, החברה בארגון, שאמור לסייע לה במקרה שתותקף שוב.[39] התקיפה הגבירה את המודעות של חברות הברית לאיום הקיברנטי מצד מדינות יריבות והעלתה את תחום המלחמות הקיברנטיות לתודעה העולמית (התקיפה על אסטוניה מוזכרת כנקודת ציון במאמרים רבים).

בשנת 2008 הותקפה גאורגיה בתקיפה קיברנטית, וזו מיוחסת אף היא לרוסיה. גם בתקיפה זו נעשה שימוש בשיטת "מניעת שירות". התקיפה פגעה בשרתי אינטרנט ציבוריים רבים של המדינה והשביתה אתרים ממשלתיים. בשונה מהמתקפה על אסטוניה, המתקפה הקיברנטית על גאורגיה לא עמדה בפני עצמה אלא קדמה לפלישה של כוחות יבשה רוסיים למדינה. נראה שתכליתה הייתה לפגוע בקשר בין הממשל לאזרחים. מקרה זה הוא דוגמה להיות לוחמה קיברנטית מגמה מסייעת למאמץ הצבאי הכולל.

דוגמאות נוספות להתקפות שכללו שימוש בשיטת "מניעת שירות" או פריצה לאתרי אינטרנט:

א. תקיפות המיוחסות לצפון קוריאה. ביולי 2009 בוצעה התקפה על אתרים אמריקניים ובהם אתרי ממסד בארצות־הברית (למשל אתרים של CIA, FBI, NASA) ואתרים אזרחיים (בנקים, אמצעי תקשורת ומסחר). בד בבד הותקפו אתרי ממסד בדרום קוריאה. לא זוהה הגורם שעמד מאחרי ההתקפות. על פי החשד זו הייתה תגובה של צפון קוריאה על סנקציות שהופעלו עליה בתקופה ההיא.

ב. בנובמבר 2010 התקיימו קרבות דו־צדיים במרחב הקיברנטי בין האקרים מהודו להאקרים מפקיסטן, ואלה התבטאו בהתקפות הדדיות על אתרי אינטרנט ממשלתיים של שתי המדינות. בהתכתשות זו הותקפו 270 אתרי אינטרנט בהודו בתגובה על תקיפת 40 אתרים בפקיסטן.

ג. ישראל סבלה מהתקפות של האקרים מחזבאללה, מתורכיה, מצפון אפריקה, האקרים פלסטינים ואחרים על אתרים רשמיים ומסחריים (כגון אתר בנק ישראל, אתרי בנקים מסחריים, אתר עיריית ת"א ועוד). תדירות התקפות אלה עלה בעת אירועים ביטחוניים, כגון מלחמת לבנון השנייה, מבצע עופרת יצוקה ובלימת המשט לעזה. נזקן של התקפות אלה היה מועט.

תקיפת סטאקסנט באיראן מסמנת עידן חדש בלוחמה במרחב הקיברנטי. בספטמבר 2010 נודע כי מתקני גרעין באיראן הותקפו ונפגעו מ"תולעת" (סטאקסנט) שהוחדרה בקיץ 2009.[40] חברת האבטחה העולמית סימנטק, שפרסמה דוח מקיף בנושא, העריכה

שהתולעת הותאמה לפגוע בממירי תדר ספציפיים, המורכבים על מערכת הצנטריפוגות להעשרת האורניום באיראן.[41]

נשיא איראן אחמדינג'ד הודה בקיום ההתקפה, אך ניסה להמעיט בחשיבותה. לדבריו: "הם הצליחו לגרום נזק למספר מוגבל של צנטריפוגות, באמצעות תוכנה שהתקינו בחלקים האלקטרוניים. למרבה המזל, המומחים שלנו טיפלו בכך, והיום הם לא יכולים לחזור ולעשות את זה".[42] לאחר שנודע על חשיפת התקיפה הוציאה חברת סימנס ערכה לגילוי ולהסרת התולעת,[43] והאיראנים הקימו צוות להסרתה.[44] גם במקרה זה אין עדות על הגורם העומד מאחורי המתקפה. על סמך יעדי המתקפה ורמת התחכם הגבוהה, מצביעים פרסומים בתקשורת לכיוון ישראל וארצות־הברית,[45] שאותן מאשימה גם איראן.[46]

האירוע עורר את השיח בעולם בנושא הלוחמה במרחב הקיברנטי. קהילות האבטחה במרחב הקיברנטי רואות בתקיפת סטאקסנט אירוע מכונן. קיימת תמימות דעים שהתקיפה עשויה להביא לידי קפיצת מדרגה הן בתחום ההגנה והן בתחום פיתוח נשק להתקפה. להלן משמעויות שמייחסים מומחים בעולם לאירוע:

א. תקיפת סטאקסנט שונה מהתקיפות הקודמות, משום שזו תקיפה בכלי מתוחכם לאין שיעור, הממוקד ביעד ביטחוני מסוים, להבדיל מתקיפות קודמות המיוחסות בעיקר לרוסיה, שנעשו בכלים פרימיטיביים ובחזית רחבה.

ב. התקיפה היא אירוע ראשון בעידן הלוחמה הקיברנטית, שבו פעולה מסוג זה במרחב הקיברנטי גולשת לעולם הפיסי המקושר למרחב הזה. כלומר, התקיפה מגלמת את הרעיון של תקיפת מערכות הנמצאות מחוץ למרחב, באמצעות המרחב הקיברנטי. "הניו יורק טיימס" ציין, שזו הפעם הראשונה שעוברת תוכנה זדונית ממחשב שכיח (Windows-based computers) אל מערכת מקצועית ספציפית של בקרת ציוד תעשייתי, המצויה גם במערכות כגון: רשת חשמל, ציוד ייצור במפעלים, צינורות גז, סכרים ותחנות כוח. לפני כן התמקדו ההתקפות במרחב הקיברנטי באתרי אינטרנט, ברשתות של תאגידים וברשתות צבאיות בלבד.[47]

ג. האירוע ממחיש את פוטנציאל הנזק הגדול שעלולה לגרום מתקפה קיברנטית רחבה המבוססת על כלים מתוחכמים מסוג זה. כך למשל, באחד המאמרים מכונה תוכנות זדוניות מסוג סטאקסנט: "worms of mass destruction", ומודגש שזהו איום ממשי להבדיל מאיומים כגון "באג 2000" בשנת 1999, שלא התממשו.[48] שגריר רוסיה בנאט"ו טען, שתולעת הסטאקסנט הייתה עלולה לגרום אסון דוגמת צ'רנוביל.[49]

ד. התולעת או כלי נשק מסוגה עלולים ליפול לידי גורמים שיעשו בה שימוש נוסף. ב"ניו יורק טיימס" צוין, שבעקבות האירוע גבר החשש בארצות־הברית שהמחשבים בארצות־הברית פגיעים לתקיפה דומה.[50] כן הועלה חשש שתולעת הסטאקסנט תגיע לידי ארגוני טרור או לידי ארגוני פשע.[51]

ה. חשש לזליגה למדינות נוספות. חברת אבטחה מבלרוס, שגילתה את התולעת, טענה שזו חדרה ל־100,000 מחשבים, 60 אחוז מהם באיראן והשאר באינדונזיה ובהודו.[52]

תמונה זו משקפת אירועים מוכרים מרכזיים שפורסמו. עם זאת, ייתכן שברחבי העולם אירעו התקפות קיברנטיות שלא אובחנו ככאלה (אלא כתקלות) או שלא פורסמו. ייתכן גם שמדינות שונות התקינו יכולות תקיפה בדמות סוסים טרויאנים, או שהוחדרו יכולות מובנות סמויות במוצרי חומרה, שיופעלו "ביום פקודה".

גורמים נוספים שהעלו את המודעות ללוחמה הקיברנטית

למרות ההיסטוריה הדלה והקצרה למדי של מלחמות קיברנטיות, נראה שקיימת מודעות עמוקה הן לסיכונים הגוברים והן להזדמנויות החדשות העומדים לפתחן של מדינות בהקשר זה. למודעות זו תרמו גם גורמים שאינם קשורים לממסדים הביטחוניים, כגון:

א. פשעים באמצעות המרחב הקיברנטי (Cybercrimes) – אלה מספקים סיבות טובות להגן על מערכות המידע גם טרם בחינה של צורכי ההגנה הנדרשים אל מול מדינות עוינות. פעולות נפוצות בתחום זה הן: גנֵבת כספים, הונאה, הלבנת הון, גנבת סודות מסחריים, סחיטה, התחזות, שיבוש והשחתה של נתונים במערכות מידע. בכל אלה ממנף המרחב הקיברנטי יכולות של פושעים. נראה כי ארצות־הברית רואה בפשיעה קיברנטית את אחד הסיכונים לביטחון הלאומי (במובן הרחב של המושג), שכן פשיעה זו מאיימת על הפעילות העסקית והחברתית הגוברת במרחב הקיברנטי, נזקיה כבדים כבר כיום, וחברות מתקשות להתמודד עמה.[53] יש הערכות ולפיהן נזקי הפשעים הקיברנטיים בעולם כבר עולים על היקף הסחר בסמים של העולם התחתון.[54] סיכול פשיעה קיברנטית מעסיק במידה רבה גם ארגוני מודיעין כדוגמת ה־FBI בארצות־הברית.

ב. תקלות במרחב הקיברנטי – אלה ממחישים את פוטנציאל הנזק של תקיפות יזומות. לדוגמה: ב־6 במאי 2010 ביצעה קרן נאמנות, המשתמשת באלגוריתם מסחר ממוחשב, פקודת מכירה אחת של חוזים עתידיים בסך 4.1 מיליארד דולר. הפקודה גרמה לשרשרת של אירועים, שהובילו למפולת החדה ביותר שהתרחשה בשוק המניות בארצות־הברית (מדד דאו ג'ונס ירד בתוך דקות ביותר מ־9%).[55] אירוע זה מלמד על רגישות שוק ההון לפעולות מבוססות תוכנה. כמו כן, תקלות ונזקים הנובעים מהשבתת מערכות תקשוב אינם נדירים, והם ממחישים את התלות הגוברת של המשק ושל הציבור במרחב הקיברנטי. בישראל למשל יוזכרו תקלת תוכנה בבנק הפועלים בנובמבר 2008, שהשביתה את תפקוד הבנק, ותקלת תוכנה בחברת התקשורת סלקום בדצמבר 2010, שגרמה לקריסת התקשורת ברחבי הארץ.

ג. שיח ציבורי ותקשורתי נרחב – כתבות בתקשורת, כנסים אקדמיים ומאמרים מקצועיים בנושא. השיח מדגיש את התלות הגדלה של האוכלוסייה במרחב הקיברנטי בכל תחומי החיים ואת משמעות הפגיעה בו. יש אמנם מומחים הממעיטים בחומרת הסיכון הטמון בלוחמה קיברנטית, אך הם המיעוט.

ד. תרבות – סרטים, משחקי מחשב וספרים עתידניים, הממחישים את הפוטנציאל של מדיום זה כמרחב לחימה (לדוגמה, הסרט "מת לחיות 4" משנת 2007). נוכח ההתקדמות הטכנולוגית המהירה, חלק מהתרחישים המוצגים בסרטים משנים עברו נראים כיום ישימים בהחלט.

השימוש בנשק הקיברנטי – גורמים מרסנים

נוכח כוחה המאיים של התקפה קיברנטית, נשאלת השאלה כיצד להסביר את מיעוט מעשי התקיפה שנקטו מדינות עד כה? תחילה יצוין שלא לכל מדינה יש יכולת מספקת להשיג תוצאות ניכרות, יכולת שהיא תנאי הכרחי (אך לא מספיק) להחליט לפעול. אשר למדינות שיש להן היכולת, נראה שהפעלת מתקפה קיברנטית כרוכה בדילמות לא פשוטות: מצד אחד קיימת אי־ודאות מה יהיו הישגי ההתקפה, ומן הצד האחר יש סיכונים לא מבוטלים. זאת ועוד, הפעלת כוח קיברנטי מחייבת גם מניעים וגם נסיבות מדיניות. אשר לאי הוודאות בדבר ההישג ראוי לציין את הסיבות הבאות:

א. לא ברורה מידת האפקטיביות של התקפה קיברנטית, בין היתר בשל חוסר ידע וניסיון הנובעים מההיסטוריה הקצרה של הלוחמה הקיברנטית. לפעולות מסוימות עלולה להיות אפקטיביות מוגבלת ולאחרות השפעת יתר, כמו פגיעה לא רצויה במנגנונים אזרחיים. בעניין זה אמר מייקל היידן (בעבר ראש ה־NSA וה־CIA): "יש בעיה לצפות תוצאות של מתקפות קיברנטיות, הן קשות לחיזוי במידה רבה יותר מאשר נזקים הנגרמים ממתקפה פיסית. אינך יכול לעשות דבר בתחום זה בלי שמשהו יקפוץ בעולם הפיסי. בסופו של יום, אין זה משחק וידאו, ומשהו יקרה למישהו בעולם האמיתי".[56]

ב. קשה לתרגם מתקפה קיברנטית להישג מדיני. למשל, במתקפה כזאת אין כיבוש של שטחים או של יעדים שישמשו בסיס למשא ומתן מדיני בתום מלחמה, כפי שאפשר לעשות במלחמה יבשתית.

ג. קשה להבטיח רציפות של מתקפה ממושכת במרחב הקיברנטי. במקרים רבים יכול היריב לחסום את הפרצה ולשקם את מערכותיו במהירות גבוהה יחסית לשיקום נזקי תקיפה קינטית. על כן קשה גם ליצור אפקט של נזק מצטבר שיהווה לחץ מדיני, כמו למשל בסדרה של מתקפות אוויר אסטרטגיות. יש מומחים הרואים בתכונה זו חסרון גדול של הזרוע ההתקפית הקיברנטית, וסבורים שהציפיות ממנה מוגזמות.[57]

בד בבד קיימים סיכונים לתוקף, וגם הם בבחינת גורמים מרסנים:

א. סיכונים לתגובת נגד. התקפה קיברנטית עלולה לחשוף מדינה תוקפת למהלומת נגד, וייתכן שהתגובה תיעשה מחוץ למרחב הקיברנטי. סגן מזכיר ההגנה לין ציין (בפברואר 2011):

> עד כה פיתחו מדינות יכולות לחדור לרשתות מחשבים כדי לאסוף מידע ולא כדי לגרום להרס. יותר ממאה סוכנויות ביון זרות ניסו לחדור למערכת הביטחון האמריקנית, אך חדירות אלו היו מוגבלות לשם ריגול. אף על פי שאין לשלול התקפה של מדינה זרה על ארצות־הברית, לרוב המדינות אין אינטרס לעשות זאת יותר משיש להן אינטרס לבצע התקפה קונבנציונלית. הסיכון שלהן גדול אף הוא, שכן כוחה הצבאי של ארצות־הברית מספק הרתעה חזקה. אף על פי שמדינות הן השחקן בעל היכולות המשמעותיות ביותר לגרום נזק באמצעות התקפה קיברנטית, סביר פחות שהן ייזמו התקפה קטסטרופלית בנסיבות רגילות (להבדיל מארגוני טרור). ועם זאת, על ארצות־הברית להתכונן לאפשרות שלוחמה קיברנטית תהיה חלק מכל מלחמה קונבנציונלית בעתיד, ועליה להיות בעלת יכולת שתאפשר לה להתגונן מפני המדינה המתקדמת ביותר.[58]

נראה שכושר ההרתעה שמייחס לין לארצות־הברית הוא ייחודי מאחר שהיא היחידה שבידה יכולת להגיב בעוצמה בכל המרחב הגלובלי. כלומר, המרחק שמאפשר המרחב הקיברנטי לתוקף אינו מספיק כדי להגן עליו מפני תגובת נגד של ארצות־הברית, מה שאין כך לגבי רוב המדינות האחרות.

ב. "בית הזכוכית". הסיכונים למדינה תוקפת גבוהים יותר ככל שהיא נסמכת יותר על המרחב הקיברנטי לשימושה היא, וככל שמערך ההגנה שלה חלש יותר. המדינות המובילות ביכולות התקפה קיברנטיות מקיימות בעצמן תלות גבוהה במרחב הקיברנטי והן מעריכות שהגנתן אינה מספקת, ועל כן הן פגיעות מאוד בעצמן. מכאן שהגנה חזקה במרחב הקיברנטי עשויה להיות אחד התנאים החיוניים להתקפה, ולפחות בטווח הנראה לעין אמור להיות להן אינטרס לבלום את מירוץ החימוש הקיברנטי. עם זאת, נראה כי אי־האמון בין השחקנים הגלובליים והאמביציות של חלקם לפתח יכולות התקפיות, עשויות לגבור על אינטרס זה ולהוביל להאצת מירוץ החימוש הקיברנטי.

ג. סיכונים נגזרים מול צד שלישי (למשל, מדינה ניטרלית, חברת תקשורת בינלאומית). שימוש בתשתית של צד שלישי לצורך תקיפה עלול להיחשב לפגיעה באינטרסים שלו. סיכון אחר הוא פגיעה בנכסי צד שלישי עקב זליגה ויראלית. במקרים קשים עלול הדבר לגרום לתגובה שלו או של המערכת הבינלאומית.

ד. סיכונים נגזרים מול בריתות יריבות. לדוגמה: הפגיעה שפגעה רוסיה באסטוניה בשנת 2007 עוררה את המודעות ואת הצורך של נאט"ו להגן על חברי הארגון. כך גרמה מתקפה לא חשובה במיוחד של רוסיה להתעוררות קואליציה קיברנטית נגדה.

ה. סיכונים מול הקהילה הבינלאומית. אין עדיין הסדרה בינלאומית לפעולות במרחב הקיברנטי. עם זאת, ייתכנו תקיפות שיגרמו לפגיעה בחיי אדם או לנזק בתפקוד המדינה, שיתפרשו כאקט מלחמתי גם על פי החוק הבינלאומי הקיים. העמימות הקיימת כיום עשויה לפעול לשני כיוונים: אחדים עשויים לראות במצב הנוכחי "חלון הזדמנויות" לפעולות במרחב הקיברנטי, העלול להיסגר כאשר תהיה הסדרה כזאת. אחרים עשויים להגדיל את מרחבי הביטחון כדי להימנע מתגובה לא צפויה של יריבים ושל הקהילה הבינלאומית.

התוקף מתמודד עם שתי דילמות נוספות כמפורט לבלן:

א. חשיפת יכולות. תקיפה קיברנטית עלולה לחשוף יכולות רגישות לעיני כלל היריבים (לא רק אצל המותקף), ואלה יקדימו להתגונן מפניהן או אף ישתמשו בהן לצרכי תקיפה מצדם. לכן כלי נשק קיברנטיים רבים נתפסים כ"חד־פעמיים", כלומר מרגע שייחשפו יהיה קשה להסתמך עליהם לשם תקיפות נוספות.

ב. ניגוד עניינים לעומת פעולות איסוף במרחב הקיברנטי. בשירותי מודיעין עשויה פעילות תקיפה להיות על חשבון פעילות איסוף, הן מבחינת הקצאות המשאבים והן בדילמה בין איסוף מידע לבין תקיפת יעד, שהוא מקור המידע. בעוד תקיפה קיברנטית טומנת בחובה סיכונים לא מעטים, כפי שהוצג לעיל, התפתחות מואצת של המרחב הקיברנטי כשדה פעולה איסופי נעדרת כמעט לחלוטין דילמות אצל הצד האוסף. היא אינה אמורה להתגלות, ואין היא מתיימרת לשנות את המערכת היריבה ואינה אמורה לעורר תגובת נגד קשה גם אם תיחשף.

טרור קיברנטי

טרור קיברנטי הוא פעולת טרור המתבצעת במרחב הקיברנטי או באמצעותו. קיימת הסכמה בין מומחים שהמרחב הקיברנטי יכול להיות אטרקטיבי לפיגועי טרור (Cyber Terror). לדוגמה, ארגוני טרור עלולים לגרום למתקן חיוני, כמו בית זיקוק, להתפוצץ באמצעות פגיעה במנגנוני בקרה וויסות.[59] עם זאת, כיום ארגוני טרור, כדוגמת אל־קאעדה, עושים שימוש נרחב במרחב הקיברנטי לצורכי תקשורת פנימית ותעמולה, אך לא לתקיפה.

סגן מזכיר ההגנה לין אמר בפברואר 2011, שהדאגה הגדולה ביותר של ארצות־הברית היא מארגוני טרור שיגיעו ליכולות שיבוש והרס קיברנטיות המצויות כיום

בידי מדינות. לדבריו, אל־קאעדה הבטיח לשגר התקפות קיברנטיות אך טרם עשה זאת. לעתיד הוא הדגיש את הנקודות האלה: אפשר שארגוני טרור יפתחו כלי התקפה קיברנטיים או ירכשו אותם בשוק השחור, כמה תריסרי האקרים מוכשרים עלולים לגרום נזק רב (כלומר אפשר לבצע פיגועים גם בלא להגיע לסף היכולת הקיברנטית של מדינות), ובכל מקרה יהיה קשה לאתר קבוצות טרור הפועלות במרחב הקיברנטי.

מה מעכב ארגוני טרור מלבצע פיגוע באמצעות המרחב הקיברנטי? להלן כמה השערות:

א. אי־הבשלה של יכולת להשיג אפקטים המאפשרים לגרום נזק רב.[60]

ב. ארגוני טרור מעדיפים לפי שעה פעולות דמים של מחבלים מתאבדים, שתועלתן בעיניהם גבוהה בהרבה מהאלמוניות המאפיינת פעולות חבלה באמצעות המרחב הקיברנטי.[61]

ג. ניגוד עניינים: לארגוני הטרור אין בהכרח עניין לשנות את כללי המשחק במרחב הקיברנטי נוכח השימוש הרב שהם עושים בו לתועלתם, כגון: ניהול הארגונים, קשר בין הפעילים, פניה לקהלי יעד ולוחמת מסרי מידע.

ד. עלות־תועלת: פיתוח נשק קיברנטי איכותי אמנם זול מהקמת צבאות קונבנציונליים, אולם הוא יקר לאין שיעור לעומת ייזום פיגועי טרור.

בין ההשערות הללו נראה שאי־הבשלת יכולת מספקת לבצע פיגועים בעלי נזק גדול היא הגורם העיקרי המעכב עד כה פיגועי טרור קיברנטיים.

אמנה בינלאומית להסדרת הפעילות במרחב הקיברנטי

כדי להסדיר את הפעולות המותרות במרחב הקיברנטי ולהגן על התשתיות העולמיות ניכר מאמץ לגבש אמנה בינלאומית, אך לא ברור מתי זו תיחתם ועד כמה תהיה יעילה. את המאמץ לקידום האמנה מרכז ארגון התקשורת של האו"ם (ITU). ראש הארגון קרא בפברואר 2010 לקדם את האמנה לפני שתחול הידרדרות למלחמה קיברנטית.[62] לפי "הוושינגטון פוסט", באמצע יולי 2010 גובש באו"ם הסכם לעסוק בהפחתת איומי התקפות של רשתות מחשבים. ההסכם הוא רק בגדר הצעה וחתמו עליו נציגים מ־15 מדינות ובהן ארצות־הברית, סין ורוסיה.בין הצעדים שהמליצה עליהם הקבוצה: האו"ם ייצור כללי התנהגות מקובלים במרחב הקיברנטי; בין המדינות יתקיימו חילופי מידע על צעדי חקיקה ואסטרטגיות לביטחון המרחב הקיברנטי; תחוזק יכולתן של מדינות פחות מפותחות להגן על מערכות המחשב שלהן. ה"וושינגטון פוסט" הוסיף, כי בשנת 2005 נכשלה קבוצה זו להגיע להבנה משותפת; אבל הפעם, תוך שימוש בטקסט קצר ובו יסודות מוסכמים, הצליחה להגיע לנוסח מוסכם. לדברי פקיד בממשל האמריקני,

ההסכם משקף התקדמות בנוגע להבנת הצדדים את הצורך הבינלאומי להתמודד עם הסיכון.[63]

עם זאת, עקב חילוקי דעות בין המעצמות בדבר אופי האמנה ודרך אכיפתה קשה להשיג התקדמות ממשית יותר בכיוון של אמנה בינלאומית מפורטת ויעילה. על חילוקי הדעות אפשר ללמוד מעמדות שהציגו הצדדים בעבר. למשל, פקיד אמריקני הגדיר את המחלוקת בין ארצות־הברית לרוסיה כדלהלן: "הרוסים רוצים להגביל את ההתקפה, בעוד אנחנו רוצים להפליל את מי שמתקיפים אותנו מדי יום ביומו."[64] במקום אחר הוסבר שרוסיה רוצה אמנה בינלאומית כדי למנוע את "מירוץ החימוש הבא", ומבקשת לקיים מגבלות ופיקוח על התחום הקיברנטי ההתקפי בדומה לתחום הנב"ק (נשק בלתי קונבנציונלי). ארצות־הברית לעומתה אינה תומכת בהקמת מוסד בינלאומי נפרד להגבלת לוחמה קיברנטית וגורסת, שהדרך הכדאית ביותר היא שיתוף פעולה יעיל ואכיפת החוק הבינלאומי. האמריקנים רואים קושי באכיפת האמנה מאחר שבמרחב הקיברנטי כמעט בלתי אפשרי להבחין בין גורם התוקף בחסות ממסד ממשלתי לבין פעילות של אדם פרטי.[65] נראה שהם חוששים ממתכונת שתגביל את יכולתה העדיפה של ארצות־הברית במרחב הקיברנטי, אך לא תרסן את הפעילות העוינת נגדה.

מאזן ביניים של הגורמים המאיצים והגורמים המרסנים

המרחב הקיברנטי הוא שדה קרב אטרקטיבי כבר כיום, נוכח תכונותיו המיוחדות והתלות של מדינות וצבאות בו לתפקודם. ההיסטוריה הדלה יחסית של תקיפה במרחב הקיברנטי, המיוחסת למדינות, מוסברת בקיומם של רסנים המקשים להחליט לנצל את המרחב לתקיפה, ובהעדר מוכנות מספקת למלחמה כזאת. מוכנות כזאת מחייבת הן יכולות הגנתיות והן יכולות התקפיות גבוהות. כדי לחולל מלחמות במרחב החדש נדרשים גם ממסדים ביטחוניים מתאימים, שתפקידם לפתח את היכולות בתחום.

בשנים האחרונות מדינות מאיצות את התארגנותן ומקימות ממסדים ביטחוניים לפעולה במרחב הקיברנטי. התארגנות זו עשויה להעיד כי הן מניחות שהסרת הרסן בפני התקפות קיברנטיות הרסניות עשויה להיות רק עניין של זמן ושאין הן יכולות להסתכן באי־מוכנות למלחמה במרחב החדש. בכל מקרה, בניית יכולת עשויה בפני עצמה להאיץ את פיתוח המרחב הקיברנטי כמרחב לחימה צבאי.

דרך אחרת לעמוד על המשמעות של הקמת הממסדים הביטחוניים הקיברנטיים היא באמצעות אנלוגיה בין התפתחות המרחב הקיברנטי בעולם לבין התפתחות המרחב האווירי כמרחבי לחימה צבאיים. להלן בקצרה כמה ציוני דרך בהתפתחות המרחב האווירי מאז הופעת המטוס. בשנת 1908, חמש שנים לאחר טיסתם הראשונה, חתמו האחים רייט על הסכם לייצור מטוסים לצבא ארצות־הברית. במלחמת העולם הראשונה (1914–1918) הופיעו בנוף המלחמה מטוסי קרב חדשים מעל ראשי חילות

הפרשים הוותיקים. בשנת 1917, בעקבות כניסת ארצות־הברית למלחמה, הוקם בה "שירות האוויר" של הצבא, וזה סיפק הגנה וסיוע לכוחות הקרקע וזכה להצלחה בקרבות אוויר. באפריל 1918 הוקם חייל האוויר המלכותי הבריטי. במלחמת העולם השנייה (1939–1945) מילא חיל האוויר הבריטי תפקיד מרכזי בהגנה על בריטניה ובתוך כך נלחם בחיל האוויר של גרמניה על העליונות האווירית בשמי האי הבריטי ושימש זרוע ארוכה לתקיפות אסטרטגיות בעומק גרמניה במסגרת בעלות הברית. המרחב האווירי קיבל אפוא את חשיבותו האסטרטגית במהלך המחצית הראשונה של המאה ה־20 עם זיהויו כמרחב לפעולות צבאיות מסוג חדש, המאפשר בין היתר להגיע אל "הבטן הרכה" של האויב במהירות ובלא התכתשות עם כוחות היבשה שלו. תהליך התפתחות המרחב האווירי כמרחב אסטרטגי נבע משלושה גורמים: התפתחויות טכנולוגיות וניצולן לצרכים הצבאיים, אתגרים לאומיים ביטחוניים והקמת ממסדים ביטחוניים, שטיפלו ביישום אופרטיבי של הטכנולוגיה ומינופה לצרכים אסטרטגיים באמצעות משאבים לאומיים.

באנלוגיה למרחב האווירי ובהקשר להקמת הממסדים מצוי המרחב הקיברנטי בתקופה מקבילה לשלהי מלחמת העולם הראשונה. הקמת ממסדים ביטחוניים קיברנטיים עשויה לחולל מהפכה דומה בחשיבה ובעשייה הצבאית. במרחב הקיברנטי קיים פוטנציאל להתפתחות מהירה מזו שהייתה במרחב האווירי, אך מימושו תלוי במוטיבציה פוליטית המושפעת בין היתר מאירועים ביטחוניים. על כל פנים, בעתיד הקרוב יחתרו כנראה מדינות להשגת עליונות במרחב הקיברנטי שלהן ולהקמת "זרוע קיברנטית" שתפעל מעבר למרחב הזה, למימוש יעדים לאומיים באופן עצמאי או בשילוב עם כוחות אחרים, בדומה להתפתחות זרועות האוויר.

פרק ג

מבט מעבר לים – היערכות מדינות לאתגר הקיברנטי

פרק זה עוסק בהתארגנות של מדינות במרחב הקיברנטי ובכלל זה בתיאור אסטרטגיות הפעולה שלהן במרחב הקיברנטי ובגופים חדשים שהקימו כדי להתמודד עם האתגר. תחילה תוצג התארגנותה של ארצות־הברית, תוך מתן דגש לאסטרטגיה החדשה של משרד ההגנה שלה; בהמשך תוצג בקצרה התארגנותן של צרפת, גרמניה ובריטניה להגנה במרחב הקיברנטי, תוך מתן דגש להתארגנותו של המגזר האזרחי ברמה הלאומית; ואחר כך תוצג האסטרטגיה ההתקפית של סין. בפרק זה נראה בין היתר כיצד באים לידי ביטוי מעשי המאפיינים והמושגים שתוארו בפרק הקודם.

ארצות־הברית

האיום הקיברנטי על ארצות־הברית

בעשור החולף גברה מודעות ארצות־הברית לאיום הנשקף לה במרחב הקיברנטי (Cyber Threat), מצד מדינות, ארגוני טרור, פושעים ואחרים. מודעות זו הביאה לגיבוש אסטרטגיות פעולה קיברנטיות (Cyber Strategy) בפתח מסמך "האסטרטגיה הלאומית לאבטחת המרחב הקיברנטי" של ארצות־הברית (פברואר 2003), כתב הנשיא ג'ורג' בוש: "הדרך שבה נעשים עסקים, פועלות ממשלות ומנוהל הביטחון הלאומי – השתנתה. פעילויות אלה תלויות כיום בתשתיות של טכנולוגית המידע הנקראות המרחב הקיברנטי". מסמך זה, מטעם הבית הלבן, הצביע על עלייה דרמטית באיומים במרחב הקיברנטי ועל כיווני פעולה להתמודדות עם האיומים הללו.[66] מאז האיומים הקיברנטיים על ארצות־הברית רק התגברו.

באמצע שנת 2009 הגדיר הנשיא ברק אובמה את האיום הקיברנטי כאחד האיומים החמורים ביותר על הביטחון הלאומי של ארצות־הברית ועל כלכלתה. לדבריו: "התשתית הדיגיטלית, שבה אנו תלויים בכל יום, היא נכס לאומי אסטרטגי, ועל כן הגנה עליה צריכה להיות בראש סדר העדיפויות הלאומי". הוא הדגיש שארצות־הברית תלויה במרחב הקיברנטי, מהמערכות של הצבא ועד רשת החשמל, והביע דאגה

מהאפשרות שתתבצע התקפה על ארצות־הברית במרחב הקיברנטי. לדבריו: "השגשוג הכלכלי של אמריקה במאה ה־21 תלוי בביטחון המרחב הקיברנטי".[67]

מסמך "אסטרטגית הביטחון הלאומי" של הבית הלבן (מאי 2010) מדגיש את האיום הקיברנטי על ארצות־הברית וקובע: "היכולות של ארצות־הברית בחלל ובמרחב הקיברנטי – המעצימות את חיי היומיום שלנו והמאפשרות מבצעים צבאיים – פגיעות לשיבוש ולהתקפה".[68] כדוגמה לתלות הצבאית האסטרטגית במרחב הקיברנטי תצוין רשת ה־GIG (Global Information Grid) ובה מגוון רחב של אמצעי תקשורת (ובכלל זה לוויינים) בפריסה עולמית. הרשת מאפשרת לארצות־הברית להעביר מידע בין נקודות שונות על הגלובוס במהירות, באמינות ובביטחון. יכולת זו מאפשרת לארצות־הברית להעביר פקודות לכוחותיה, להנחות פצצות חכמות למטרות באמצעות GPS, לשלוט במטוסים ללא טייס מהקצה האחד של העולם למשנהו ועוד. אם תיפגע הרשת, עלולה ארצות־הברית לאבד מהדומיננטיות שממנה היא נהנית בשדות הקרב בעולם.

בפברואר 2010 מנה סגן מזכיר ההגנה לין שלושה סוגי איומים קיברנטיים: ריגול, שיבוש (כגון התקפות "מניעת שירות") והתקפות שמטרתן יצירת הרס. לדעתו, האיום האחרון הוא החמור ביותר והוא מתעורר רק עתה; הכלים כבר קיימים וניכר שגם קיימת היכולת למימושו. לדבריו: "אפשר לדמיין התקפות על הרשתות הצבאיות והתשתיות הקריטיות, כמו מערכת התחבורה וסקטור האנרגיה, שיגרמו נזק כלכלי חמור, הרס פיסי ואפילו אובדן חיי אדם". לדבריו, המעבר המסתמן במרחב הקיברנטי, משיבוש להרס, מבטא עלייה בסולם ההסלמה של האיומים. ככל שהאיום יתפתח כך יהיו דרכים רבות יותר לממשו:

> "אנו עומדים ברגע מכונן מבחינת האיום הקיברנטי – יותר כלי הרס מפותחים, אך טרם באו לידי שימוש, והשחקנים הזדוניים ביותר טרם הניחו את ידיהם על נשק קיברנטי בעל יכולות הרס גדולות. אולם מצב זה לא יארך לעד. ארגוני טרור או מדינות עוינות ישיגו יכולות כאלה. עלינו להקים יכולת הגנה בטרם זה קורה. כרגע יש חלון זמן, שמשכו לא ברור, לחזק את הרשתות שלנו נגד איומים מסוכנים".

לדעת לין, ייתכן תיאורטית שהתקפות הרסניות באמצעות המרחב הקיברנטי לעולם לא יבוצעו, אולם ההיסטוריה מלמדת שרק מעטים הם כלי הנשק שיוצרו ולא באו לידי שימוש. מסיבה זו על ארצות־הברית להיות מוכנה להתגונן מכל מגוון כלי הנשק הקיברנטיים האפשריים.[69]

ממסדים שהקימה ארצות־הברית לביטחון המרחב הקיברנטי

על הראייה הכוללת ועל האסטרטגיה של ארצות־הברית להגנה במרחב הקיברנטי ממונה הבית הלבן. לצדו של אובמה בית הלבן פועל הווארד שמידט (Howard Schmidt), "מתאם הפעולות לביטחון המרחב הקיברנטי ועוזר מיוחד לנשיא" (Cybersecurity

Coordinator and Special Assistant to the President). שמידט מונה בדצמבר 2009, והוא מופקד בין היתר על תיאום וסנכרון מדיניות הממשל ועל סיוע לנשיא בניהול משברים בתחום ביטחון המרחב הקיברנטי.

למשרד לביטחון המולדת תפקיד מרכזי ביישום האסטרטגיה לביטחון המרחב הקיברנטי. המחלקה לביטחון קיברנטי (National Cyber Security Division) היא הגוף הממונה במשרד על הנושא. המחלקה רואה את ייעודה "לפעול בשיתוף פעולה עם גורמים בסקטור הציבורי והפרטי ועם גופים בעולם כדי לאבטח (secure) את המרחב הקיברנטי ואת הנכסים הקיברנטיים של ארצות־הברית (America's cyber assets)".[70] מוקד עיסוקה נוגע לביטחון הרשתות הפדרליות ולהגנה (protection) על התשתיות החיוניות. המחלקה ממונה על יישום תוכנית לתגובה הגנתית כלפי התקפה (National Cyberspace Response System). התוכנית מרכזת את ענייני הניהול, התהליכים והפרוטוקולים אל מול אירועים חריגים המאותרים במרחב הקיברנטי. כמו כן אחראית המחלקה לתוכנית לניהול סיכונים (Cyber-Risk Management Programs), שנועדה למפות את הסיכונים ולצמצם אותם תוך שיקולי עלות־תועלת. המחלקה עוסקת בתיאום בין הרשויות הממלכתיות ובשיתוף מידע בין הגופים השונים (ובכלל זה שיתוף המגזר הפרטי), בין היתר בנוגע להתרעה מפני פעולות עוינות במרחב הקיברנטי. בתוך כך קיים שיתוף פעולה הדוק בינה לבין פיקוד הסייבר במשרד ההגנה.

משרד ההגנה (הפנטגון) ממונה על ההגנה וההתקפה הקיברנטיים בתחום הצבאי ועל סיוע לגופים האזרחים. לצורך זה הוקם במאי 2010 פיקוד הסייבר (Cybercom), כחלק מהפיקוד האסטרטגי במשרד ההגנה. מפקד הפיקוד, גנרל אלכסנדר, מסר בעדותו בקונגרס כי: "פיקוד הסייבר אחראי להוציא לפועל משימות קיברנטיות המוטלות עליו כדי להבטיח את חופש הפעולה במרחב הקיברנטי ולצמצם את הסיכונים לביטחון הלאומי". בין המשימות הקונקרטיות של הפיקוד (על פי דברי מפקד הפיקוד וסגן שר ההגנה):

א. הובלת ההגנה על רשתות הצבא ומשרד ההגנה.

ב. יצירת שרשרת פיקוד ברורה לקבלת החלטות בתחום הלוחמה הקיברנטית. השרשרת להפעלת פיקוד הסייבר היא: נשיא ארצות־הברית, מזכיר ההגנה, ראש הפיקוד האסטרטגי וראש פיקוד הסייבר.

ג. יצירת שיתוף פעולה עם גורמים מחוץ לצבא ומשרד ההגנה (משרדי ממשלה אחרים, מגזר פרטי) ומחוץ לארצות־הברית בהקשר ללוחמה קיברנטית.

ד. בהקשר המבצעי – אינטגרציה של משימות קיברנטיות וסנכרון אפקטים בסביבה הביטחונית הגלובלית; הכוונה של מבצעים ברשת המידע הגלובלית; הוצאה לפועל של מגוון מבצעים קיברנטיים.

ה. יצירת מודעות למבצעים קיברנטיים נגד ארצות־הברית והתרעה מפני אויבים.

ו. לשמש נציג הצבא בתחום הקיברנטי במגעים עם גורמים שונים ובהם סוכנויות ביטחוניות אחרות וחברות אמריקניות וזרות.

קהילת המודיעין האמריקאית היא רכיב חשוב במערך הביטחוני הקיברנטי. מסמך האסטרטגיה של קהילת המודיעין של ארצות־הברית מאוגוסט 2009[71] מראה, כי חיזוק היכולות הקיברנטיות היא אחת מחמש המשימות הראשונות במעלה של ארגוני המודיעין האמריקניים. המרחב הקיברנטי הוא כר נרחב לפעולת של ארגוני אלה בהקשרים של איסוף מודיעין, תקיפה וסיוע להגנה. גופי הקהילה האמריקניים, כגון ה־FBI, עוסקים גם בתחומים פליליים ובהם סיכול הונאות קיברנטיות. כן הוטל על ארגוני המודיעין להגביר את ניצול טכנולוגית המידע למינוף תפקודן הפנים־ארגוני. למשל, שיפור אינטגרציה של מידע וידע, ניהול משימות ארגוניות של הקהילה, מיכון תהליכי רכש ועוד. נראה שכיום הצבא וקהילת המודיעין מגבירים את מאמציהם לפתח יכולות לוחמה במרחב הקיברנטי. ייתכן שמגמה זו חייבה או תחייב הסדרה של חלוקת האחריות והסמכות ביניהם בתחום הלוחמה הקיברנטית. יוזכר כי ה־NSA מהווה חלק מקהילת המודיעין האמריקאית ובה בשעה גם חלק מהצבא וממשרד ההגנה האמריקאי.

האסטרטגיה של ארצות הברית לביטחון המרחב הקיברנטי

מטרת האסטרטגיה. במסמך *"האסטרטגיה הלאומית לאבטחת המרחב הקיברנטי"*, שפרסם הבית הלבן בפברואר 2003, נכתב כי מטרת האסטרטגיה:"לספק מסגרת להגן על התשתיות החיוניות לכלכלה, לביטחון ולדרך החיים האמריקנית". המסמך מגדיר את אבטחת המרחב הקיברנטי כאתגר אסטרטגי קשה ויוצא דופן, המחייב שיתוף פעולה בין השלטון המרכזי לשלטון המקומי, לסקטור הפרטי ולאזרחי המדינה. במסגרת זו הזמין נשיא ארצות־הברית דאז, ג'ורג' בוש, את הסקטור הפרטי להיות שותף של הממשל במימוש האסטרטגיה מאחר שרק פעולה משותפת יכולה לאפשר מרחב קיברנטי בטוח בעתיד. בראש סדר העדיפויות שהתוותה האסטרטגיה עומדים עניינים הנוגעים לביטחון הלאומי החשופים למרחב הקיברנטי, תשתיות לאומיות חיוניות, סקטורים פגיעים ומפעלים גדולים. עדיפות נמוכה יותר הוקנתה להגנה על עסקים קטנים ועל משקי הבית, ועדיפות אחרונה ניתנה לאבטחת המרחב הקיברנטי הגלובלי.[72]

האסטרטגיה הנ"ל נועדה לשמש מסגרת לשילוב כוחות ולחלוקת תפקידים בין כל הגופים האופרטיביים הפועלים לביטחון המרחב הקיברנטי של ארצות־הברית ובהם: משרד המתאם ועוזר הנשיא לביטחון המרחב הקיברנטי, המחלקה לביטחון קיברנטי במשרד לביטחון המולדת, פיקוד הסייבר במשרד ההגנה, שירותי הביון, גורמים במשרד

המשפטים ועוד. וכן הוטל על משרדי הממשלה לתאם בין כל הגורמים הרלוונטיים במדינה הגנה על התשתיות החיוניות בתחום אחריותם. למשל, משרד האוצר אחראי לאבטחת תשתיות חיוניות בשוק ההון, משרד האנרגיה אחראי לאבטחת מתקני אנרגיה חשובים וכו'.

ככלל, מטורת האסטרטגיה תקפים גם כיום. השינוי שחל הוא בקפיצת המדרגה שעשתה ארצות־הברית בשנים האחרונות בהתארגנותה למלחמה במרחב הקיברנטי, בין היתר עקב התממשות חלק מהאיומים. עוד שינוי משמעותי ניכר בהתייחסות האמריקאית להגנת המרחב הקיברנטי ממחוץ לגבולות ארצות הברית.

במאי 2011 השיק הבית הלבן את *"האסטרטגיה הבינלאומית למרחב הקיברנטי"*[73]. האסטרטגיה, שהוצגה על־ידי מזכירת המדינה, הילרי קלינטון, משלימה ומעדכנת את קודמתה בתחום הפעילות הקיברנטית מחוץ לארצות הברית, והיא מקנה חשיבות רבה לתחום זה במדיניות החוץ, הביטחון והסחר של ארצות הברית. לפי האסטרטגיה החדשה, ארצות הברית תפעל לקדם ולפתח תשתית מידע עולמית בטוחה, אמינה וחופשית, שתאפשר מסחר בינלאומי, חיזוק הביטחון הבינלאומי, עידוד חופש ביטוי וחדשנות; וזאת באמצעות בניית תרבות של התנהגות אחראית, הדרכת מדינות, יצירת שותפויות ותמיכה בשלטון החוק במרחב הקיברנטי. לארצות הברית יש לפחות שלושה שיקולים בולטים להגנה על המרחב הקיברנטי מחוץ לגבולותיה, שאותם אמורה האסטרטגיה לקדם:

א. הגברת הביטחון על ארצות הברית ובעלות בריתה. ארצות הברית מבינה, כי הביטחון במרחב הקיברנטי המדינתי לא יושג בלא שיתוף פעולה, שכן הרשתות מקושרות הדדית (גם רשתות ביטחוניות כמו בין חברות נאט"ו). במאפיין זה של המרחב הקיברנטי טמונים הזדמנויות (יכולת לקבל התרעה מוקדמות) אך גם סיכונים, שיש להתמודד עימם במשותף.

ב. לארצות הברית ולבעלות בריתה אינטרסים כלכליים, חברתיים, מדיניים וביטחוניים, התלויים ברשתות גלובליות. כך למשל, באמצעות אינטרנט בטוח יותר ושיתוף פעולה ניתן לקדם את הסחר האמריקאי ברחבי העולם, להגן על הקניין הרוחני, ולשפר את יכולתה של ארצות הברית להתמודד עם פשעים במרחב הקיברנטי ובאמצעותו.

ג. ארצות הברית חותרת לקדם את הערכים האמריקאים של חופש הביטוי וזכויות הפרט במרחב הקיברנטי ובאמצעותו. בפתיחת מסמך האסטרטגיה הנ"ל קובע הנשיא אובמה, כי "המרחב הקיברנטי והטכנולוגיות שהוא מאפשר מתירות לאנשים – מכל לאום, גזע, אמונה, והשקפה – לתקשר, לשתף פעולה ולשגשג יותר מאי־פעם".על יישום האסטרטגיה ממונים מספר משרדים: החוץ, הביטחון,

ביטחון המולדת, הסחר והמשפטים. במשרד החוץ האמריקאי מונה כריס פיינטר (Christopher Painter) כמתאם האסטרטגיה.[74]

האסטרטגיה הקיברנטית של משרד ההגנה האמריקאי ויישומה. "*אסטרטגית ההגנה הקיברנטית הכוללת של הפנטגון*" (*Cyber 3.0*) נמצאת בשלב סופי של בחינה, וחלקים ממנה כבר מיושמים. אסטרטגיה זו היא ייחודית וחדשנית ומוצגת על ידי האמריקאים באופן מפורט, שאין דומה לו במדינות אחרות. אסטרטגיה זו משתלבת באסטרטגיות של הבית הלבן שצוינו לעיל.

סגן מזכיר ההגנה לין מנה חמישה יסודות שעליהם מבוססת האסטרטגיה:[75]

א. משרד ההגנה הכיר (בשנת 2010) פורמלית במרחב הקיברנטי כמרחב לחימה, כמו היבשה, האוויר, הים והחלל. פירוש הדבר, הצבא חייב לפעול במרחב החדש בדומה למרחבי הלחימה המסורתיים כדי לשמור על הביטחון הלאומי. בהתאם לכך הצבא צריך להתארגן, להתאמן ולצייד את זרועותיו כדי לבצע משימותיו במרחב הקיברנטי. לשם כך הוקם פיקוד המרחב הקיברנטי וכל אחת מהזרועות הקימו ארגונים לפעולה במרחב הקיברנטי.

ב. רשתות הצבא ומשרד ההגנה מצוידות במערכות הגנה אקטיבית. להבדיל מהגנה פסיבית, הפועלת רק אחרי האפקט של האיתור (ומבוססת על "חומות הגנה"), הגנה אקטיבית מבוססת על גישה דינמית. היא פועלת במהירות הרשת תוך שימוש בסנסורים, בתוכנות ובמודיעין לגילוי תוכנות זדוניות ולהפסקת פעולתן לפני שהן מצליחות לגרום נזק. מאחר שחדירות מתוחכמות לא תמיד ייתפסו בגבולות המרחב הקיברנטי של המדינה, הגנה אקטיבית פועלת כדי לצוד תוכנות זדוניות במרחב. להערכת לין, אף על פי ששום רשת לא תהיה בטוחה במאת האחוזים, מערכת הגנה אקטיבית כבר שיפרה את הביטחון ברשתות משרד ההגנה. עוד ציין לין,[76] כי מערכת ההגנה הקיברנטית, שעליה מופקד משרד ההגנה, מושתתת על שלוש שכבות הגנה: השתיים הראשונות מתבססות על מערכות הגנה, שאותן מספקות חברות מסחריות באמצעות מכלול תוכנות הגנה למיניהן (כגון anti-virus, firewall), ואילו השכבה השלישית מבוססת על היכולות של גופי המודיעין הלאומיים. תפקידה של שכבה זו לספק "הגנה אקטיבית", להעביר מידע על תקיפות מסנסורים חיצוניים למנגנוני הגנה במרחב הקיברנטי הלאומי, לתאם בין הכוחות הפועלים במרחב הלאומי ולנהל את המערכה מתוך ראייה כוללת.

ג. אבטחת הגנתה של התשתית הקיברנטית החיונית במדינה, שגם הצבא נשען עליה, באמצעות שיתוף פעולה עם המגזר האזרחי. לין הדגיש את חשיבות ההגנה על התשתיות הקיברנטיות האזרחיות, שבלעדיהן רשת חשמל ושאר משרדי הממשלה לא יכולים לתפקד. לדבריו, מסיבה זו משימת המשרד לביטחון פנים במרחב

הקיברנטי היא קריטית ותפקידו של משרד ההגנה לסייע לו בעניין הזה. למשל, במהלך אסון טבע, כמו הוריקן, עושה הרשות הפדרלית לטיפול באסונות לאומיים (FEMA) שימוש בכוחות צבא. כך גם צריכות היכולות של הצבא במרחב הקיברנטי להיות זמינות למנהיגים האזרחיים כדי לסייע להגן על הרשתות ועל התשתיות החיוניות, ולתמוך בפעולות של גופי הממשלה. לין הדגיש, שבכל מקרה של סיוע שיגיש הצבא לרשויות האזרחיות יהיו המשאבים בשליטה אזרחית ויופעלו על פי החוקים האזרחיים. לצורך זה מוסדה שותפות פורמלית באוקטובר 2010 בין משרד ההגנה לבין המשרד לביטחון פנים בתחום הקיברנטי.

במסגרת ניסויית הועברו טכנולוגיות צבאיות ובכלל זה בתחום ההגנה האקטיבית לשימוש המשרד לביטחון פנים, כדי להגן על הרשתות הממשלתיות. כן מוסדו מסגרות לתכנון משותף ולחילופי כוח אדם בין המשרדים. להערכת לין, יוזמות אלה שיפרו באופן ניכר את היכולת של משרדי הממשלה להתמודד עם איומים קיברנטיים. מעדותו בקונגרס של מפקד הפיקוד הגנרל אלכסנדר עולה, שבעת מצב חירום מתרחבות סמכויות משרד ההגנה על חשבון המשרד לביטחון פנים בכל הקשור להגנה על האומה; ומשתמע מכך, שגם בתחום הגנת המרחב הקיברנטי האזרחי. האסטרטגיה מבוססת על ההבנה שהתשתיות הקיברנטיות האזרחיות חיוניות לתפקוד הצבא, ואי־אפשר להגן כראוי על התשתיות האזרחיות בלי מעורבות הצבא.

ד. בניית "הגנות קולקטיביות" ושיתופי פעולה עם בעלי ברית – מאפשרים לפקח באופן משותף על רשתות המחשבים מפני חדירה, בדומה למערכת הגנה אווירית משותפת, המאפשרת לקבל התרעה על התקפה אווירית. מסמך האסטרטגיה הבינלאומי למרחב הקיברנטי של הבית הלבן ממאי 2011 עוסק בין היתר בסוגיה זו. אחד מיעדי האסטרטגיה הנוגעים לתחום הצבאי הוא לבנות בריתות צבאיות ולשפר בריתות קיימות, כדי להתמודד עם איומים פוטנציאליים במרחב הקיברנטי. אחד הביטויים לכך הוא המאמץ של ארצות־הברית לקדם קואליציה קיברנטית בנאט"ו. מאמץ זה קיבל תנופה בוועידה שהתקיימה במטה הארגון בנובמבר 2010.[77] בוועידה הוסכם להקנות עדיפות גבוהה יותר להתמודדות עם האיומים הקיברנטיים, והוחלט להקדים את מועד הקמת מרכז התגובה הקיברנטי של הברית (NATO Cyber Incident Response Center) בשלוש שנים לעומת התכנון המקורי, כך שיהיה מבצעי כבר בשנת 2012.[78]

ה. שילוב הסקטור הפרטי. בדרך זו ניתן להבטיח שהמשאבים הטכנולוגיים והאנושיים הטובים ביותר של המדינה יופנו לתחום הגנת המרחב הקיברנטי, כפי שארצות־הברית עושה במרחבים אחרים (פירוט בהמשך).

בעדותו בקונגרס באפריל 2010 נשען הגנרל אלכסנדר גם על מסמך "האסטרטגיה הלאומית הצבאית למבצעים במרחב הקיברנטי" מסוף 2006,[79] שעל מימושה מופקד כיום פיקוד הסייבר. לדבריו, מטרת האסטרטגיה היא להשיג עליונות קיברנטית כדי להבטיח את חופש הפעולה של ארצות־הברית וכדי לשלול את חופש הפעולה מיריבים. מטרה זו יש להשיג באמצעות אינטגרציה של רשתות, הגנה, איסוף מידע והתקפה במרחב הקיברנטי. אלכסנדר סבור, שעליונות קיברנטית קשה להשגה בסביבה הנוכחית, אך עדיין אפשרית. לדבריו, אמנם בשלב הראשון יש לפתח את היכולת ההגנתית, אולם הפגיעות של ארצות־הברית אינה עומדת בסתירה ליעד של השגת עליונות קיברנטית (המחייבת גם פיתוח יכולות התקפיות). שאלות מעניינות של סנטורים, שאלכסנדר ענה עליהן בדלתיים סגורות, היו: האם יהיו בידי הפיקוד כלי התקפה משמעותיים במרחב הקיברנטי? האם קיומם יעודד אחרים לפתח כלים כאלה? באיזו רמת ביטחון עליו לקבוע את זהות התוקף לפני הפעלת מתקפת נגד?

שיתוף הפעולה בין הסקטור הביטחוני לבין הסקטור הפרטי הוא נושא מרכזי באסטרטגיה החדשה של הפנטגון להגנת המרחב הקיברנטי. לדברי לין, "האסטרטגיה הכוללת היא אמנם אבן דרך חשובה אולם הממשלה לא יכולה להגן על המדינה לבדה. ההגנה במרחב הקיברנטי אינה משימה צבאית, כמו הגנת החלל, שם כל האחריות מוטלת על הצבא. החלק המכריע של התשתיות הלאומיות הקריטיות, כולל האינטרנט, נמצאות בידיים פרטיות". אבטחת הרשת מחייבת אפוא שותפות בין הסקטור הציבורי לבין הסקטור הפרטי. הוא מנה שלושה מסלולים לשיתוף הפעולה בין הסקטור הציבורי לבין הסקטור הפרטי, שאותם יש לקדם כדי לשפר את ההגנה על ארצות־הברית במרחב הקיברנטי.

מסלול ראשון – שיתוף פעולה במידע. לספקי התקשורת והאינטרנט ראייה מצוינת על המתרחש ברשתות הגלובליות. ביכולתם לאתר את תנועת ההתקפות במערכות שלהם, במקרים רבים ביכולתם לספק ללקוחות התרעה מוקדמת, ובדרך כלל יש להם את היכולות התפעוליות הטובות ביותר להגיב על מצב כזה. הפנטגון עובד עם טכנולוגיות־מפתח וחברות ביטחוניות מהסקטור הפרטי, ומתקיימים חילופי מידע שישפרו את הביטחון ואת היכולת במרחב הקיברנטי. מנהלים בכירים מהחברות נפגשים עם בכירים ממשרד ההגנה, מהמשרד לביטחון פנים ומהמשרד של ראש קהילת המודיעין האמריקנית. השותפות הפרטית־הציבורית לא רק מסייעת לזהות נקודות תורפה ברשתות, אלא גם מעודדת פעולה בסקטור הממשלתי ומעוררת מומחים בתעשייה להתמודד עם הסיכונים הביטחוניים לפני שהנזק נגרם.

מסלול שני – שיתוף פעולה לחיזוק ארכיטקטורת רשת האינטרנט (מבנה, ארגון, היררכיה, כללים, מנגנוני הגנה וכו'). נוכח חוסר האיזון המובנה בין הגנה להתקפה ברשת ובמטרה להפחית את היתרון שיש כיום לפורצים ברשת, מבקש הפנטגון את

עזרת הקהילה המדעית כדי לחזק את ארכיטקטורת הרשת ובכלל זה לשבץ מנגנוני אבטחה ואימות ברמה גבוהה: בחומרה, במערכות ההפעלה ובפרוטוקולים של הרשת. לדברי לין: "האסטרטגיה הלאומית לזיהוי אמין ברשת", שהיא יוזמה של הבית הלבן, אמורה להניח אבן יסוד לעתיד בטוח יותר ברשת. אמנם התשתית הדיגיטלית לא תשתנה "בן לילה", אולם בתקופת זמן ארוכה אפשר להביא לידי שינוי הנדסי שיתקן את אחת מנקודת התורפה הבעייתיות ביותר של הטכנולוגיה כיום. לין מסר, ש"כדי לקדם את המאמץ, החליט משרד ההגנה של ארצות־הברית להוסיף חצי מיליארד דולר למימון מחקרים חדשים שיתמקדו בנושאים הנוגעים לביטחון המרחב הקיברנטי ובכלל זה מימון ראשוני לחברות פרטיות העוסקות בפיתוח טכנולוגיות דו־שימושיות, היכולות לשרת את צורכי הביטחון במרחב הקיברנטי". במקביל, מתבצע מאמץ להגדיל את ההיכרות של מערכת הביטחון עם הטכנולוגיות האלה. עוד ציין לין, כי הסקטור הממשלתי לוקה באיטיות. למשל, בימים אלה לוקח לפנטגון 81 חודשים לקלוט מערכת מחשב, בעוד ש ה־iPhone פותח ב־24 חודשים בלבד. לדבריו, יש לסגור את הפער בסיוע הסקטור הפרטי. כן חשף לין את דבר קיומן של תוכניות לחילופי מידע וכוח אדם בין הסקטור הממשלתי לבין תעשיית טכנולוגיות המידע. לדבריו, משרד ההגנה מעוניין לקבל מהתעשייה הזו מנהלים בכירים כדי לשלב בתוכו יותר יכולות המצויות בתעשייה, ולקבל מומחים מהתעשייה שיתמודדו ישירות עם האתגרים העומדים בפני משרד ההגנה. עוד הוכרז על תוכנית לניצול המומחיות הקיברנטית הקיימת בקרב אנשי המשמר הלאומי ומערך המילואים. חיילים רבים המשרתים במערכים אלו עובדים כאזרחים בתחום ה־IT בעולם. כדי לנצל ביעילות גדולה יותר את מומחיותם, יוקמו במערכים אלה יחידות שייועדו למשימות קיברנטיות.

מסלול שלישי – שבו מצפה לין לשיתוף פעולה בין הסקטור הממשלתי לפרטי – הוא הרחבת ההגנה האקטיבית גם לרשתות פרטיות, הקשורות לתשתיות חיוניות לצבא ולמשק. בשל היכולת המודיעינית של ארצות־הברית יש בידי הסקטור הממשלתי מידע מסווג על סיכונים קיברנטיים מסוימים. הטכנולוגיה שפיתח משרד ההגנה לצורך הרשתות הביטחוניות (המיועדת להתמודד עם סיכונים אלה) יכולה להעלות במידה ניכרת את האפקטיביות של הביטחון במרחב הקיברנטי בעבור הסקטור הפרטי. כבר עתה חולק משרד ההגנה מידע לא מסווג עם חברות ביטחוניות פרטיות, שהרשתות שלהן מכילות מידע רגיש, בנוגע לאיומים קיברנטיים עליהן. שאלה דחופה של מדיניות היא, כיצד לשתף במידע ובטכנולוגיה מסווגים חברות התומכות בצבא ובכלכלה כדי לשפר אצלן את הביטחון במרחב הקיברנטי? מדובר בזהות אינטרסים, שכן בעלים ומפעילים של תשתיות חיוניות יכולים להרוויח מההגנה האקטיבית שיקבלו, ואילו למשרד ההגנה יש את הטכנולוגיה והיכולת ליישם הגנה כזאת בהקשר האזרחי. אתגר חשוב הוא לפתח מסגרת של מדיניות וחוק שתאפשר זאת. לין ציין לחיוב את שיתוף

הפעולה בין הסקטור הציבורי לסקטור הפרטי לקראת באג 2000. יש דמיון באתגר, גם אז דובר באיום גלובלי הנוגע לכל דבר שהוא דיגיטלי, אולם שלא כמו באג 2000, עכשיו אנו עומדים מול איום של שחקנים זדוניים. לדעת לין, קידום המסלול השלישי הוא המאתגר ביותר.

נוצר הרושם שסגן שר ההגנה הציג את מעורבות משרד ההגנה בתחום האזרחי של המרחב הקיברנטי בזהירות רבה, בייחוד בדברו על מעורבות הצבא בהגנת תשתיות קריטיות אזרחיות ("היסוד השלישי" לעיל). זאת, כפי הנראה, נוכח מחלוקות שנתגלעו בעבר בעניין מעורבות הצבא במגזר האזרחי. כך למשל, סקירת סיכונים קיברנטיים, שביצעה ה־NSA בשנת 2009 לבקשת ממשל אובמה, עוררה התנגדות במשרד לביטחון הפנים. רוד בקסטרום, שהתפטר מתפקידו כמנכ"ל המרכז הלאומי לאבטחת מידע, אמר שהוא חושש שהסקירה תביא לידי כך שה־NSA יוכל לבחון כל דבר דוא"ל (דואר אלקטרוני), הודעת טקסט או חיפוש בגוגל שיעשה כל עובד ברשויות הממשל האמריקני. לדבריו, המודיעין האמריקני אמור לאסוף מידע על הנעשה מחוץ לארצות־הברית ולא צריך לקבל שליטה כה רבה על העברת המידע בתוך המדינה.[80] דוגמה נוספת, בעקבות הודעת שר ההגנה ביוני 2009 על הכוונה להקים את פיקוד הסייבר נשמעה בוושינגטון ביקורת על כך שגוף צבאי יטפל בהגנה על רשתות מחשב אזרחיות ותוכנן ייחשף בפניו. ביקורת מסוג אחר הייתה, שהפיקוד יקנה עדיפות להגנה על רשתות המחשב הצבאיות על פני הגנה על הרשתות אזרחיות.[81]

מקומה של התקפה באסטרטגיית ההגנה הקיברנטית של ארצות־הברית. המידע על האסטרטגיות של ארצות־הברית מבליט את האופי ההגנתי של התפיסה האמריקנית. זו נועדה לשמור על נכסיה הלאומיים ועל מעמדה כמעצמת־על, המתבססים גם על יתרונה הטכנולוגי כלפי אויבים או יריבים ומתחרים כדוגמת סין.[82] עם זאת, שדה הקרב הקיברנטי כולל פעולות הגנה והתקפה בו בזמן, ונראה שלארצות־הברית יש יתרון על כל מדינה אחרת ביכולת התקיפה ובנוכחות במרחב הקיברנטי. ההתקפה במרחב הקיברנטי היא חלק ממשימותיו של פיקוד הסייבר, שלא פורטו בידי בכירי מערכת הביטחון של ארצות־הברית, ומסיבות מובנות. בכנס האבטחה Black Hat, שהתקיים ביולי 2010 בלאס וגאס, אמר מייקל היידן, כנראה בנימה ביקורתית, כי בפיקוד הקיברנטי עוסקים רוב הזמן בפעילות הגנתית וצבא ארצות הברית אינו שוקל פעולות תקיפה חכמות, כדוגמת אלה שהוא עצמו הציע.[83]

בכנס הנזכר סיפר מייקל היידן על אפשרויות פעולה שנדונו בעבר בממשל כדי לרסן התקפות מצד מדינות, בין שאלה נעשות שלא בידיעתן ובין שהן נעשות באישורן, בעידודן ובמימונן. אחת הגישות שנדונו בממשל האמריקני היא לחדול מלשאול לגבי היכולת למצוא את התוקפים, ובמקום זה להטיל את האחריות על המדינה שממנה יצאה המתקפה ולפעול נגדה. לדבריו: "כל מיני סוגים של נידוי קיברנטי באים בחשבון,

או תגובה שתאיים ותפגע בזרימת התעבורה האינטרנטית של המדינה שממנה באה הפגיעה, למשל האטה של המסחר המקוון, ואף פגיעה ביכולות התקשורת של אותה מדינה". אחת האפשרויות לפעולה שנדונו הייתה התקפה של מניעת שירות, שכן היא עומדת בהגבלות של אמנת ז'נבה. לדבריו: "זהו כלי נשק זמין וקל. עלינו לגרום למדינות בוגרות להפנים שיש להן אחריות גם על המרחב הקיברנטי ומה שיוצא משם". היידן סיפר, שהועלו גם רעיונות של תחומים שאין לפגוע בהם, כגון רשתות תקשורת רגישות, ובהן רשתות חשמל ומערכות בנקאות. לדעתו "זהו פרדוקס מסוים, שכן במלחמה פיסית אלה יעדי תקיפה לגיטימיים".[84]

מדיניות תגובה במרחב הקיברנטי. לפי עדותו של הגנרל אלכסנדר בקונגרס, אם נשיא ארצות־הברית קובע שאירוע קיברנטי חוצה את הסף של שימוש בכוח, הוא גם רשאי לקבוע את מדיניות התגובה. קביעה זו נסמכת על שיקולים סובייקטיביים ואובייקטיביים, כגון הסתמכות על אמנת האו"ם המקנה זכות להגנה עצמית. כיום אין הגדרות מוסכמות בעולם וכל מדינה יכולה להגדיר לעצמה סף ייחודי לשימוש בכוח, בכפוף לחוקים בינלאומיים שאינם ספציפיים למרחב הקיברנטי.

מערב אירופה

צרפת

צרפת מכירה בחשיבות המכרעת של המרחב הקיברנטי לכלכלה, לחברה, לביטחון ולמרקם החיים. בשנת 2009 גובשה בצרפת אסטרטגיה להגנת המרחב הקיברנטי.[85] יעדי האסטרטגיה הם:

א. להיות מעצמה עולמית בתחום ההגנה על מערכות המידע. צרפת חותרת להשתייך לחוג המצומצם של אומות מובילות בתחום זה, ובכוונתה ליטול חלק פעיל בקבוצת המדינות המפותחות כדי לגבש מענה משותף לאיומים.

ב. לקיים מרחב מידע ביטחוני בטוח, שיאפשר לקבל החלטות ולהבטיח את תפקוד מנגנוני הפיקוד והשליטה במצבי שגרה וחירום.

ג. לחזק אבטחת רשתות חיוניות ויעדים חיוניים הנסמכים עליהם. צרפת הגדירה רשימה של תשתיות חיוניות לקיום האומה, שחלקן שייכות למגזר הפרטי. ההגנה עליהן מחייבת להכשיר את מגזר התעשייה במדינה.

ד. לאפשר מרחב קיברנטי בטוח. לשם כך יש לבנות הגנה מפני איומי תקיפה קיברנטיים, המופנים נגד גורמי הממשל, חברות פרטיות או אזרחים.

הדרך להשגת היעדים האסטרטגיים:

א. ניטור בזמן של התקפות קיברנטיות על צרפת ומתן מענה מהיר במקרה של התקפה.

ב. הגדלת הידע והיכולות המדעיות בתחום הקיברנטי ובכלל זה: שיפור המחקר על הסביבה הקיברנטית כדי לזהות מגמות טכנולוגיות הטומנות בחובן איומים פוטנציאליים. כן יוקם מרכז מחקר בשיתוף האקדמיה וגורמים פרטיים, שיתמקד בנושאים כמו הצפנה, ניתוח התקפות קיברנטיות ופיתוח תוכנות מאובטחות.
ג. אבטחת מערכות מידע של תשתיות חיוניות השייכות למדינה או לגורמים פרטיים. לצורך כך הוגדרה "האסטרטגיה הלאומית של צרפת לאבטחת מידע מסווג", והוקמה רשת אינטראנט מאובטחת של משרדי ממשלה.
ד. התאמת החקיקה להתפתחויות בתחום טכנולוגיות המידע והרשתות.
ה. פיתוח שיתוף פעולה בינלאומי בתחומים כגון אבטחת מידע והגנת מידע, מאבק בפשעים במרחב הקיברנטי.
ו. הגברת המודעות לנושא בקרב מקבלי ההחלטות והציבור הרחב בצרפת.

כדי לממש את האסטרטגיה הוקמו גופים ברמה הלאומית. במסגרת זו הוקמה המועצה האסטרטגית להגנת מערכות המידע הלאומיות, שבראשה עומד המנכ"ל למשרד ביטחון המולדת. חברי המועצה הם: הרמטכ"ל, ראשי ארגוני המודיעין האזרחיים, מנכ"ל משרד החוץ, מנכ"ל משרד הביטחון, נציג מיוחד לענייני חימוש, ובכירים בתחום התעשייה. תפקידה של המועצה לפרט את האסטרטגיה הלאומית להגנת מערכות המידע ולכוון את הסוכנות הלאומית לביטחון מערכות מידע.

הסוכנות לביטחון מערכות מידע (ANSSI), שהוקמה ביולי 2009, מאורגנת כדלהלן:
א. מרכז אופרטיבי לביטחון מערכות מידע (COSSI), הפועל ברציפות ואמור לנטר אירועי חדירה קיברנטיים ולהגיב בהתאם. המרכז מכיל את הפונקציות האלה: מרכז לקריפטולוגיה יישומית (צופן, זיהוי, הרשאות), מרכז לביקורות בתחום ביטחון מערכות מידע, מרכז לתגובה וטיפול בתקיפות קיברנטיות, מרכז ניטור, פונקצית תיאום, חדר מלחמה, משרד תכנון ותרגילים.
ב. אגף אסטרטגיה ורגולציה (SR), העוסק בגיבוש אסטרטגיה, בקביעת תקנות, בתיאום בין משרדי ובמעקב אחר התקדמות התחום בעולם.
ג. אגף סיוע, ייעוץ והכשרה (ACE).
ד. אגף מערכות מידע מאובטחות, העוסק בפיתוח ובאישור אמצעי תקשורת מאובטחים לשימוש הדרג המקצועי והמדיני (לא כולל מערכות תקשורת צבאיות).

גרמניה

בהתארגנות גרמניה להגנת המרחב הקיברנטי ברמה הלאומית יש מאפיינים דומים לאלה של צרפת ובכלל זה הקמת מועצה לאומית ומרכז אופרטיבי לתגובה לאירועי תקיפה. האסטרטגיה פורסמה במסמך "האסטרטגיה החדשה לביטחון המרחב

הקיברנטי הגרמני".[86] מסמך זה עוסק אמנם במגזר האזרחי, אולם מצוין בו שיש צעדים משלימים שאותם אמור הצבא הגרמני לנקוט כדי להגן על יכולותיו וכדי להגן על המרחב הקיברנטי הלאומי. בולטת במסמך האסטרטגיה החתירה לשיתוף פעולה בין המגזר הציבורי לבין המגזר הפרטי, וכן שיתוף בין גרמניה למדינות ומוסדות מחוץ למדינה.

האסטרטגיה עוסקת בעניינים האלה:

א. הגנה על תשתיות קריטיות.

ב. חיזוק אבטחת מערכות המידע במדינה. למשל, על ידי בקרה על ספקי תקשוב וחברות אבטחה לבל יחסכו באמצעי אבטחה ומתן תמריצים לאספקת מוצרי אבטחה לאזרחים (דוגמת Electronic proof of identity).

ג. חיזוק ביטחון התשתיות הקיברנטיות במשרדי הממשלה.

ד. הקמת מנגנון לתגובה מהירה להתקפות קיברנטיות (National Cyber Response Centre).

ה. הקמת מועצה לגיבוש מדיניות ולתיאום ברמה הלאומית (National Cyber Security Council).

ו. חיזוק יכולת רשויות החוק והאכיפה, בין היתר לשיפור יכולת ההתמודדות עם פשעים וריגול קיברנטיים.

ז. שיפור שיתוף הפעולה והתיאום עם מדינות אירופה ומדינות אחרות בעולם להגנת המרחב הקיברנטי.

ח. שימוש באמצעים אמינים של טכנולוגיית המידע.

ט. הכשרת עובדים והדרכה בתחום אבטחת מערכות המידע במגזר הממשלתי.

י. יכולת תגובה למתקפה קיברנטית. במסמך נכתב: "אם המדינה רוצה להיות מוכנה באופן מלא להתקפות קיברנטיות, יש ליצור ערכה מתואמת ומקיפה של כלים כדי להגיב על התקפות כאלה, בשיתוף פעולה עם רשויות המדינה המוסמכות".

בריטניה

לונדון מכירה אף היא בחשיבות המכרעת של המרחב הקיברנטי לכלכלה, לחברה, לביטחון ולמרקם החיים בממלכה. "העולם הדיגיטלי הוא מציאות כל החיים שלנו", כך נכתב בעיקרי מסמך "האסטרטגיה של בריטניה לביטחון המרחב הקיברנטי", שפרסם ביוני 2009 משרד הקבינט.[87] עוד נכתב במסמך:

> "כפי שהגנו על הימים במאה ה־19 לשם הביטחון הלאומי והשגשוג שלנו, ובמאה ה־20 היה עלינו להגן על המרחב האווירי, הרי במאה ה־21 עלינו להגן על המרחב הקיברנטי והיתרונות שהוא מקנה. האסטרטגיה הראשונה שלנו לביטחון המרחב הקיברנטי היא צעד חשוב להשגת מטרה זו".

האסטרטגיה הבריטית מבקשת ליצור מרחב קיברנטי בטוח באמצעות:

א. הפחתה של איומים של פעולות קיברנטיות (cyber operations) עוינות באמצעות הפחתה של מוטיבציות ויכולות של אויבים.

ב. הגנה על אינטרסים בריטיים מפני מבצעים קיברנטיים עוינים ועל יכולתה של בריטניה לנצל לתועלתה את ההזדמנויות הגלומות במרחב הקיברנטי. זאת באמצעות צמצום החשיפה, הפגיעות (vulnerability) וההשפעה (impact) של מבצעים קיברנטיים עוינים על אינטרסים בריטיים.

ג. איסוף מודיעין על איומים ושחקנים מאיימים, ופעולות נגד אויבים.

ד. שיפור הידע והמודעות, פיתוח דוקטרינה ומדיניות, פיתוח קבלת החלטות ומשילות בתחום הקיברנטי, מינוף יכולות טכנולוגיות ואנושיות.

ואלה כמה מהפעולות שהוחלט לנקוט לצורך זה ברמה הלאומית:

א. מיסוד תוכניות חוצות משרדי ממשלה לקידום יעדי האסטרטגיה. למשל, מתן תוספות מימון ליוזמות חדשניות לפיתוח טכנולוגיות עתידיות להגנה על הרשתות הבריטיות; וכן פיתוח וקידום מיומנויות קריטיות לצרכי הגנה קיברנטית.

ב. עבודה בצמידות עם כלל הסקטור הציבורי, התעשייה, קבוצות העוסקות בחירויות האזרח, הציבור ושותפים בינלאומיים. הממשלה בשיתוף עם התעשייה, כבר לקחה על עצמה מגוון פעילויות איכותיות בתחום הביטחון הקיברנטי. ועם זאת, על פי מסמך האסטרטגיה, האתגרים גדולים והמשימה כה חשובה, כך שנידרש לפתח אותן עוד יותר. אחד העקרונות הראשיים שחותרת אליהם האסטרטגיה הוא ליצור דפוסי שיתוף פעולה קבועים שיביאו לידי ביטוי את הידע והמומחיות המשותפים של הגופים הנ"ל להשגת המטרות.

שני משרדים הוקמו לצורך יישום האסטרטגיה: א. המשרד לביטחון קיברנטי (Office of Cyber Security (OCS. ה־OCS כפוף למשרד הקבינט (Cabinet Office). ייעודו לספק מנהיגות אסטרטגית קבועה ברמת הממשלה. המשרד אחראי על פיתוח האסטרטגיה להגנת המרחב הקיברנטי, על תיאום בין משרדי הממשלה ועל הגברת שיתוף הפעולה בין הממשל לבין הסקטור הפרטי. ב. מרכז ביטחון קיברנטי אופרטיבי Cyber Security Operations Centre (CSOC). מרכז אופרטיבי בין־תחומי שמשימותיו הן: לפקח באופן אקטיבי אחר הביטחון במרחב הקיברנטי, לתאם תגובות ומענה לאירועים, להשיג הבנה טובה ומהירה יותר של התקפות על הרשתות הבריטיות, ולספק ייעוץ ומידע בנוגע לסיכונים קיברנטיים למגזר העסקי ולציבור.

האסטרטגיה הקיברנטית הביטחונית של סין

בעוד באסטרטגיות של מדינות המערב יש דמיון רב בהיותן אסטרטגיות הגנתיות המכוונות כלפי איומים ואויבים דומים, הרי התפיסה של סין מזמנת ראייה אסטרטגית שונה של המרחב הקיברנטי – כמרחב של ההזדמנויות, שמימושן מחייב בין היתר יכולת חדירה לצורך איסוף אגרסיבי ולצורך התקפה.

ראייתה של סין את המרחב הקיברנטי כמרחב אסטרטגי

סין רואה בטכנולוגיות הדיגיטליות הזדמנות יוצאת דופן לקדם את יכולותיה האסטרטגיות, הכלכליות והצבאיות, ואת מעמדה כמעצמה המונה 1.35 מיליארד נפש. הדבר מתבטא בין היתר בהתפשטות המהירה של האינטרנט והתקשורת הסלולארית בסין. באמצעות טכנולוגיות מתקדמות מנסה סין לעבור בקפיצת מדרגה מחברה חקלאית (כמחצית מהסינים עדיין גרים ביישובים חקלאיים) לחברת המידע, תוך כדי דילוג מהיר ככל האפשר על שלב החברה התעשייתית. מה שלקח למדינות מערביות עשרות שנים מנסה סין לעשות בפרק זמן קצר בזכות טכנולוגיות דיגיטליות, שהשוק הסיני הגדול מאפשר את מימושן.[88]

במישור הביטחוני, מסוף שנות התשעים ועד כה התמקדה פעילות סין במרחב הקיברנטי בריגול במערב ובתקיפות מתנגדים פוליטיים ברחבי העולם. בשנים האחרונות בונה סין יכולת צבאית קיברנטית, שתכליתה לאפשר לה יתרונות אסטרטגיים התואמים את היותה מעצמת־על. כך עולה ממחקרים אמריקניים המנתחים את האסטרטגיה הקיברנטית של סין. סין רואה בפיתוח יכולתה הקיברנטית הצבאית רכיב אסטרטגי ההכרחי לאיזון נחיתותה האסטרטגית בתחום הקונבנציונלי לעומת ארצות־הברית. נראה שהיא רואה בפיתוח יכולת קיברנטית הזדמנות לזכות ביתרון אסטרטגי, שלא היה לה סיכוי להשיגו בעבר. הדברים אמורים הן בניצול המרחב הקיברנטי לשיפור תפקודו של צבא סין והן בחתירתה להשיג יכולת התקפית, שתקנה לה דומיננטיות במרחב הקיברנטי, וזו תתבטא גם במרחבים האחרים.

על פי פרסומים במערב, סין מהווה סיכון למערב בשלושה תחומים. האחד – איסוף מודיעין העשוי להביא יתרון צבאי. למשל, חשיפת נקודות תורפה של ארצות־הברית ותוכניות צבאיות, וכן איסוף סודות טכנולוגיים צבאיים ואזרחיים, שהם היתרון הגדול ביותר שיש לארצות־הברית, וגם גנבת נכסים קיברנטיים (תוכנות ובסיסי נתונים) לשימוש צבאי ואזרחי. להערכת מומחים במערב, הסינים פועלים, בעיקר כלפי יעדים בארצות־הברית ובאירופה, באמצעות חדירה מרחוק ובמגע קרוב, בכלל זה באמצעות אספקת רכיבי חומרה שמוצפנת בהם תוכנה זדונית. בשנת 2009 דווח על פריצה למחשבים בארצות־הברית, המיוחסת לסין, שבמהלכה נגנבו תוכניות של מטוס הקרב העתידי F-35 Lightning II. כמו כן מיוחסת לסין חדירה למחשביהן

של חברות מסחריות (כגון גוגל) לצורכי איסוף ולתקיפת מתנגדי המשטר ("מבצע אורורה" בשנת 2009).

תחום הסיכון השני הוא פיתוח יכולות התקפיות במרחב הקיברנטי, העלולות לאיים על התשתיות האזרחיות והצבאיות המפותחות של מדינות מערביות. היכולות הטכנולוגיות והאופרטיביות הגבוהות של סין בתחום האיסוף במרחב הקיברנטי עשויות ללמד גם על יכולותיה ההתקפיות.

תחום הסיכון השלישי הוא מאבק תרבותי – קריאת תיגר של סין על ערכי המערב כפי שארצות־הברית מנסה ליישמם במרחב הקיברנטי הגלובלי, כמו חופש מידע והגנה על זכויות קניין רוחני. כזכור, בעקבות התקפות האקרים מסין על ארצות־הברית והמשבר בין סין לגוגל הזהירה מזכירת המדינה הילרי קלינטון, ב־12 בינואר 2010, ש"ארצות־הברית תגן על הרשתות, ומי שיפגע בהן ויאיים על החברה האזרחית ועל הכלכלה שלנו יישא בתוצאות ויזכה לגינוי בינלאומי".[89]

עיקרי האסטרטגיה ההתקפית של סין

מסמך של תאגיד התעשיות הביטחוניות האמריקניות Northrop Grumman, מתאר את האסטרטגיה ההתקפית של סין כפי שרואים אותה האמריקנים.[90] על פי המסמך, צבא סין רואה ביכולתו הקיברנטית המתפתחת מכפיל כוח, הן לשם שיפור תפקודו המערכתי הפנימי והן לפעולה נגד אויבים. כחלק מתהליך המודרניזציה בצבא נעשה מאמץ לפתח ארכיטקטורת רשת, המסוגלת לתאם פעולות צבאיות בכל המרחבים. בה בעת, הסינים רואים בהשגת הדומיננטיות במידע רכיב מפתח בהשגת ניצחון בעימות. הם חותרים להשיג שליטה על זרימת המידע של היריב וכך להשיג דומיננטיות בשדה הקרב. לשם כך הם מפתחים יכולת לחדור למערכות המידע המתקדמות של היריב כדי לאסוף מודיעין, שעל בסיסו תושג הצלחה בעימותים עתידיים.

במסגרת תפיסתה ההתקפית, סין מפתחת יכולת לשלב בין מבצעי תקיפת רשתות מחשבים, לוחמה אלקטרונית ומהלומה קינטית ("אש"); זאת כדי לפגוע במערכות התקשורת של היריב (הצבאיות והאזרחיות) וליצור נקודות עיוורון, שאותן יוכלו הכוחות הסיניים לנצל בזמן אמת. כן מוזכרים מערכי פיקוד ושליטה ולוגיסטיקה כיעדים לתקיפה קיברנטית בשל תמיכתם הרבה בהשגת המטרות האסטרטגיות הצבאית. מבצעי תקיפה כאלה יפעלו בידי הסינים בשלבים מוקדמים של העימות ואולי אף כחלק של מכת מנע. פעולות אלו נחשבות לרכיב בהרתעה האסטרטגית של סין. לשיטתם: זו "מלחמה קטנה", לא אלימה, שאינה מחייבת בהכרח תגובה של היריב ועשויה למנוע את "המלחמה הגדולה". יש בצבא סין הסוברים, שלנשק קיברנטי יש פוטנציאל הרתעה השווה לזה של נשק גרעיני, ואף משופר יותר: אין הוא

גורם נזק פיסי, הנזק שהוא גורם נשלט וממוקד, והוא יכול להיות מופעל לטווחים כמעט בלתי מוגבלים.

מומחים בתחום הביטחון הקיברנטי סבורים, שסין נמצאת כיום בעיצומו של מאמץ לאיסוף מידע מסווג מהמערב, בטרם תתחזק יכולת אבטחת המידע שלו במרחב הקיברנטי, ובמאמץ זה משתתפים יחידות קיברנטיות של הממשלה, קבלני משנה סיניים וגורמים העוסקים בפשיעה קיברנטית. יש עדויות על זיקה בין גורמים סיניים בממסד לבין פעולות לוחמניות או איסופיות, שבוצעו על ידי האקרים נגד מטרות אמריקניות או זרות אחרות. יתרה מכך, היקף הפעילות, היכולת וסוג היעדים שהותקפו מעידים שזו פעילות מדינתית.[91]

על פי המסמך האמריקני, פעילות האיסוף המודיעיני של סין בארצות־הברית מאופיינת ברמה טכנולוגית גבוהה מאוד, בסימולטניות וביכולת לפעול פעולה ממושכת כלפי כמה יעדי איסוף במקביל. היעדים שכלפיהם פעלה סין בארצות־הברית באמצעות המרחב הקיברנטי היו: תשתיות הצבא, תעשיות ביטחוניות, תוכנית החלל, חברות טכנולוגיה עילית פרטיות שלהן זיקה לענייני ביטחון, גורמי הגנה קיברנטיים, מוקדי קבלת החלטות העשויים להיות קשורים לאינטרסים של סין ועוד.

לפי המסמך, בעימות עם ארצות־הברית סביר מאוד שסין תשתמש במרחב הקיברנטי כדי לתקוף תשתיות אזרחיות, שכן הן רלוונטיות לצבא, למשרד ההגנה ולחברות המועסקות בידי גורמי הביטחון. סין עשויה ככל הנראה לתקוף גם מדינות עמיתות לארצות־הברית כדי לעכב את הפרישה האמריקנית הצפויה באזורי עימות ולפגוע בהתנהלות הכוחות הנוכחים בזירה.

בהקשר ההגנתי, בשונה מארצות־הברית השואפת לספק חופש פעולה מלא לאזרחיה במרחב הקיברנטי, מקיימת סין שליטה הדוקה במרחב הקיברנטי הפנימי, בעיקר לשם מניעת חתרנות פוליטית, ועל כך היא רואה בחברות כמו גוגל יריב. בתחילת שנת 2011 אף הגבירה סין את הפיקוח על המרחב הקיברנטי בעקבות לקחים מהשימוש שעשו בו המתקוממים במדינות ערביות.[92] מבחינה זו יש לכוחות הביטחון של סין יתרון בהגנה מפני אויבים מבחוץ מכיוון שהם נהנים מחופש פעולה מלא במרחב הקיברנטי, בעוד כוחות הביטחון של ארצות־הברית כפופים לחוקים נוקשים הנוגעים לזכויות האזרח. מבחינה אחרת, תרומתו של מרחב קיברנטי מפוקח ומבוקר למשק עשויה להיות פחותה מזו של מרחב חופשי ופתוח לרעיונות.

מאפייני ההתארגנות של מדינות לפעולה במרחב הקיברנטי

עד השנים האחרונות, לא נדרשו מדינות להקמת מנגנונים מיוחדים לניהול מלחמה במרחב הקיברנטי, חוץ מרשויות לאבטחת מידע. נראה שהצבאות, ארגוני המודיעין ומשרדי ביטחון הפנים שאפו להכיל פעילות זו באמצעות הקמת גופים אופרטיביים

ביחידות קיימות אצלם. האירועים שחלו בשנים האחרונות והבנת הסיכונים וההזדמנויות הגלומים בשדה הקרב הקיברנטי שינו את התמונה ועוררו את הצורך בהתארגנות חדשה, שביטוייה ניכרים כיום במדינות שונות.

מעבר מגישה של אבטחת מידע לתפיסה של הגנה. בראשית שנות האלפיים הוקמו בכמה מדינות גופים לאומיים לביטחון מערכות מידע, שהיו באופיים גופי אבטחת מידע. לקראת סוף העשור חלה התפתחות ארגונית התואמת את היות המרחב הקיברנטי מרחב לחימה וגובשו אסטרטגיות להגנת המרחב הקיברנטי הלאומי.

המענה הארגוני לאתגר הקיברנטי, המשתקף בכמה מדינות, מורכב משתי קומות:

א. בקומה העליונה נמצא הדרג המדינתי העליון, שאותו מרכז גוף ברמה של משרד ממשלתי (בארצות־הברית ובבריטניה) או מועצה לאומית (בצרפת ובגרמניה). ברמה זו עוסקים בגיבוש אסטרטגיה וכללי מדיניות, ובתיאום וסנכרון בין כלל הגורמים במדינה העוסקים בביטחון המרחב הקיברנטי.

ב. בקומה מתחתיה פועלים יחידות או ארגונים ביטחוניים אופרטיביים, צבאיים (דוגמת פיקוד הסייבר בארצות־הברית) ואזרחיים (דוגמת מחלקת ביטחון הסייבר במשרד ביטחון המולדת בארצות־הברית).

קיימת הבחנה בין ההתארגנות ההגנתית, שהיא חוצת מגזרים, לבין התחום ההתקפי המצוי כולו בתחומם של ממסדים צבאיים וקהילות מודיעין (למשל בפנטגון וב־CIA בארצות־הברית). נראה שההחלטה על בניין היכולות ההתקפיות ועל הפעלתן מתקיימת דרך שרשרת הפיקוד הישירה בין גופי הביטחון הללו לבין הקברניטים. שרשרת הפיקוד בארצות־הברית כוללת כאמור את הנשיא, שר ההגנה, מפקד הפיקוד האסטרטגי ומפקד פיקוד הסייבר, ואינה עוברת דרך גופים אזרחיים, כמו המשרד לביטחון המולדת (אף שזה, משיקולי הגנה, אמור להיות מעודכן וערוך למתקפה של ארצות־הברית).

שילוב כוחות אופרטיבי בין הגופים האזרחיים לצבאיים. ההכרה בהיות המרחב הקיברנטי משותף למגזר הביטחוני ולמגזר האזרחי היא גורם מניע להתארגנות האופרטיבית המשותפת. אחד הביטויים לכך הוא הקמת "מרכזי מבצעים" משותפים (כגון בבריטניה, בצרפת ובגרמניה), שתכליתם לרכז את תמונת המצב ולסייע במענה הנדרש. עם זאת, במדינות הדמוקרטיות האלה ובארצות־הברית קיימת חלוקת עבודה ברורה למדי בין המגזרים. הגופים האזרחיים ממונים על עיקר הפעילות ההגנתית בתוך המדינה, ואילו הצבאות ושירותי המודיעין (שהם בעלי יכולת התקפית) מגנים על עצמם, מספקים למגנים מידע על יריבים, מסייעים ליחידות האזרחיות להגן על תשתיות חיוניות (בייחוד במצבי חירום, שבהם גדלות סמכויות הצבא), וממנפים את נוכחותם ואת יכולתם ההתקפית במרחב הקיברנטי לשיתוק מקורות ההתקפה ולתגובה נגד האויבים.

חתירה לשיתוף פעולה קיברנטי עם מדינות ידידותיות היא ממד בולט באסטרטגיה של מדינות המערב.

התארגנות גופי הלוחמה הקיברנטיים ליד ארגוני הסיגינט הלאומיים.[93] לפחות בחלק מהמקומות יש לגופים אלה מפקד אחד (מפקד פיקוד הסייבר בארצות־הברית הוא גם מפקד ה־NSA). נראה שהדבר נובע מכך, שלגופי הסיגינט תשתיות אנושיות וטכנולוגיות רלוונטיות להתמודדות עם לוחמה במרחב הקיברנטי, בנוסף על ניסיונם הרב בפעולה במרחב הקיברנטי בתחום האיסופי והכרתם את היריבים. במילים אחרות, נראה כי פעולה אפקטיבית במרחב הקיברנטי מחייבת שילוב של יכולות הסיגינט הלאומיות.

לסיכום פרק זה, נראה שהקמת המנגנונים הביטחוניים צפויה לחולל תהליך מתמיד של בניית כלים ותפיסות אופרטיביות ואף הקמת יחידות נוספות ללוחמה קיברנטית. התרחשויות ביטחוניות והיווצרות מניעים מדיניים להפעלת הכוח עשויות כמובן להאיץ תהליך זה. נוכח היכולות הקיברנטיות הנבנות, סביר כי מעתה עשויה לוחמה קיברנטית להוות חלק מכל מלחמה מודרנית. לגבי תדירות השימוש בלוחמה קיברנטית בתקופות שבין מלחמות קונבנציונליות, המסקנה היא פחות נחרצת, שכן בפני המעצמות הקיברנטיות ניצבים גם שיקולים מרסנים ולהפעלת נשק קיברנטי דרושים גם מניעים מדיניים. כך או אחרת, בכל הקשור לבניין הכוח, כאמור, מרוץ החימוש הקיברנטי בעולם כבר החל, בהובלת שלוש המעצמות – ארצות־הברית, רוסיה וסין – ובהשתתפות מדינות נוספות.

פרק ד

משמעויות מערכתיות לישראל

חשיבות טכנולוגיות המידע והמרחב הקיברנטי לישראל

לטכנולוגיות המידע ולמרחב הקיברנטי עצמו תרומה אסטרטגית לישראל. המשק הישראלי, בדומה למדינות המתקדמות ביותר בעולם, נשען במידה רבה על תשתיות המרחב הקיברנטי. ענפי טכנולוגיות המידע תורמים ישירות ובעקיפין לצמיחה הכלכלית בישראל, שהיא בין המדינות המובילות בעולם בפיתוח טכנולוגיות מידע. על פי מחקר של חברת הייעוץ הבינלאומית מקנזי,[94] "כלכלת האינטרנט" בישראל נחלקת לשני תחומים. החלק הארי הוא בתחום תעשיית טכנולוגיות מידע ותקשורת (ICT), והוא כולל פיתוח, ייצור ומכירה של ציוד, תוכנות ושירותים. התחום הקטן יותר, שצומח במהירות, הוא תחום המסחר האלקטרוני אשר עוסק ברכישת מוצרים ושירותים באינטרנט. לפי המחקר, כלכלת האינטרנט בישראל (לפי הגדרת מקנזי) תרמה במישרין לתוצר כ־50 מיליארד שקל בשנת 2009, כ־6.5% מהתוצר המקומי הגולמי (התמ"ג). נתון זה ממצב את ישראל כאחת מכלכלות האינטרנט המובילות בעולם. על פי המחקר, "כלכלת האינטרנט" הישראלית צפויה לצמוח בקצב שנתי של 9% – כפליים מקצב הצמיחה של המשק. בשנת 2015 צפויה התרומה של "כלכלת האינטרנט" הישראלית להסתכם בכ־85 מיליארד שקל, שיהוו כ־8.5% מהתמ"ג. לענפי טכנולוגית המידע נודעת חשיבות מיוחדת משום שיש להם יכולת גבוהה להתחרות בשוק העולמי (חלק ניכר מהתוצר מופנה לחוץ לארץ) ומשום שהדרך היחידה של ישראל לצמוח במהירות היא הגדלת הייצוא.

ל"כלכלת האינטרנט" גם תרומה גבוהה לתעסוקה במשק, בייחוד לתעסוקת אקדמאים מתחומי הטכנולוגיה. בנוסף תורמים ענפי טכנולוגיות המידע תרומה ישירה ועקיפה לסקטור הביטחוני בישראל. וענפי טכנולוגיות מידע ותקשורת הם חלק חשוב מיכולותיה הטכנולוגיות של ישראל, הזוכות להערכה רבה של מומחים רבים מרחבי העולם,[95] וכך מחזקות את תדמיתה ומעמדה בעולם.

המרחב הקיברנטי מאפשר לישראל לפרוץ את בידודה הגיאוגרפי במזרח התיכון ולקיים קשרים הדוקים ושוטפים עם העולם. במרחב הקיברנטי טמון אף הפוטנציאל

לחיזוק הקשר שבין הפריפריה למרכז המדינה. הוא משמש רכיב מרכזי בפעילות החברתית, וגורם חשוב בחיזוק הקשר שבין רשויות השלטון לאזרח.

התארגנות ישראל להגנת המרחב הקיברנטי

בהתארגנות ישראל להגנת המרחב הקיברנטי ניתן למנות כמה נקודות ציון בולטות. בשנת 1997 הוקם פרויקט תהיל"ה (תשתית הממשלה לעידן האינטרנט). הפרויקט, שהוקם באגף החשב הכללי במשרד האוצר, נועד לספק שירותי גלישה מאובטחים למשרדי הממשלה ומוסדותיה. על פי המדווח באתר האינטרנט של גוף זה, בתהיל"ה מצויה חוות שרתים שדרכה מקבלים מאות אלפי אזרחים בחודש שירותי ממשל זמין ומידע על פעולות משרדי הממשלה. תהיל"ה מפעילה אמצעים לשמירה על ביטחון הרשת הממשלתית באינטרנט, החל בצוות מומחי אבטחת מידע ותקשורת וכלה במוצרים וטכנולוגיות של חברות מובילות בעולם. בתהיל"ה הוקם "מרכז אבטחת המידע של ממשלת ישראל", שבין תפקידיו: לעקוב אחר אירועי אבטחת מידע בעולם עם תשומת לב להתקפות ברשת הנוגעות לישראל, לתאם בין גופים ממשלתיים לצורך פתרון בעיות אבטחה, לקשר בין גופים ממשלתיים לגופים חיצוניים ולערוך מחקרים בתחום. המרכז מוציא התראות אבטחת מידע לארגונים בתחום טכנולוגיות המידע המקיימים קשרים עם תהיל"ה או לגורמים ממשלתיים שאינם מסווגים. כן מקיים הגוף קשרים עם גורמים בינלאומיים כדי למגר התקפות ממוחשבות.[96] במסגרת זו פועל צוות CERT (Computer Emergency Response Team), שייעודו לתת מענה מידי לאירועי אבטחת מידע בארגונים ממשלתיים או בגופים בסדר גודל בינלאומי. "נציגי ה־CERT מקיימים מוקד מענה זמין לתופעות של תקיפות ברשת, ניהול סיכונים, יצירת נהלי אבטחת מידע, בקרת תעבורה, התפרצויות וירוסים, מניעת דואר זבל ופישינג, פיראטיות ברשת, זיוף זהות, שמירה על פרטיות המידע, העלאת המודעות לאבטחה; כן עוסק הצוות בשיתוף ועדכון מידע של ספקיות האינטרנט, המשטרה וגורמי מערכת הביטחון".[97] אכן משימות נכבדות לקח הגוף על עצמו, אולם יש לזכור שהמנדט לפעילותו נוגע לאספקת שירותי גלישה מאובטחים באינטרנט למשרדי הממשלה ומוסדותיה, והמרכז אינו גוף אינטגרטיבי־אופרטיבי משותף לגופים האמונים על ביטחון המרחב הקיברנטי, כפי שראינו במדינות מערביות.

ב־27 במרס 2011 אישרה הממשלה את הקמת יחידת המנמ"ר (מנהל מערכות מידע) הממשלתי, גוף בין־משרדי שירכז את תחום התקשוב בממשלה. הגוף, הכפוף למנכ"ל משרד האוצר, אמור להנחות את יחידות התקשוב במשרדי הממשלה ולהיות אחראי במישרין על כל פרויקטי המחשוב הממשלתיים הרוחביים, ובכלל זה על פרויקט תהיל"ה.[98] ריכוז פרויקטי המחשוב של הממשלה במקום אחד הוא התקדמות רבה

בהיערכות המדינה בתחום התקשוב, אולם מוטב שהגוף הממונה על ניהול ביטחון מערכות המידע יהיה מחוץ לגוף המקים והמפעיל תשתיות אלה.

בשנת 2002 הוקמה הרשות הממלכתית לאבטחת מידע בשירות הביטחון הכללי (השב"כ). "הרשות מופקדת על הנחיה מקצועית של הגופים המונחים שבאחריותה, בתחום אבטחת תשתיות מחשב חיוניות, מפני איומי טרור וחבלה בתחום אבטחת מידע מסווג, ומפני איומי ריגול וחשיפה".[99] ההיגיון המקורי להיות הרשות יחידה בשב"כ קשור כנראה לאחריותו של השב"כ לסיכול ריגול וטרור. כיום אפשר להצביע על יתרונות ועל חסרונות למיקום הזה. יתרון חשוב הוא הקשר ההדוק בין הרשות לבין שאר היכולות והסמכויות של השב"כ (הכלולות בחוק השב"כ) ושל קהילת המודיעין, שבה השב"כ שותף. מנגד, גופים בסקטור הפרטי עלולים להירתע מחשיפה ליחידה בארגון האוחז במשימות ובסמכויות חריגות שאינן נוגעות רק לממד הזה.[100] נוסף על כך השב"כ מטבעו הוא גוף מבצעי העוסק בסיכול חשאי, ואינו מופקד על משימות אחרות הדרושות כדי להתמודד עם האתגר הקיברנטי, כגון קשר הדוק עם הסקטור הפרטי, הגברת מודעות האוכלוסייה לאבטחה קיברנטית, טיפול בגופים שנפגעו במתקפה קיברנטית ועוד.

הרשות הממלכתית לאבטחת מידע בשב"כ מונחית על ידי ועדת היגוי להגנה על מערכות ממוחשבות במטה לביטחון לאומי (המל"ל), שבראשה עומד ראש המטה ללוחמה בטרור במל"ל.[101] תפקידה של ועדת ההיגוי לאשר לרשות לאבטחת מידע להרחיב את רשימת הגופים המונחים או המאובטחים, שיידרשו להעמיק את הגנתם ולעמוד בהנחיות הרשות. על פי מאמרו של גבי סיבוני,[102] פעילות זו לא התבססה על תהליך סטטוטורי ושיטתי של איתור גופים אלה ואישורם; וכך יצא שחברות גדולות וחיוניות בסקטורים מסוימים כלולות ברשימה ואילו חברות גדולות בסקטורים אחרים (למשל בתחומי המזון והתרופות) אינן ברשימה, על אף שתרומתן לתוצר, לתעסוקה ולמרקם החיים גדולה. ליקוי נוסף בשיטה הוא בכך שהיא מתמקדת בהנחיית חברות נבחרות בסקטורים מסוימים, מסייעת להגנה נקודתית ולא מספקת הגנה מערכתית, המחייבת כיסוי רחב יותר של גופים הקשורים לאותה מערכת חיונית. דוגמה לכך היא מערכת המים: "הגנה על תשתיות אספקת המים ואיכותם בישראל אינה נוגעת רק לתהליכים בחברת מקורות, המופיעה ברשימה, אלא גם לעשרות ספקי מים אחרים, אגודות, תאגידי מים, מתקני התפלה, והולכה, מתקני טיפול בשפכים מתקני טיפול והולכת קולחים ועוד. חלקם הגדול של מתקנים אלה מופעל על ידי יזמים פרטיים, שההפעלה של מנגנוני הגנה אינה בראש מעייניהם. המצב הזה דומה בתחומים רבים נוספים".

לעומת זאת, דוגמה להכוונה, המשקפת מודעות גבוהה לביטחון מערכות המידע, מוצאים אצל הממונים על הגופים הפיננסיים במשרד האוצר ובבנק ישראל. משרד

האוצר (אגף שוק ההון, ביטוח וחיסכון) הוציא הנחיות מפורטות לגופים פיננסיים העוסקות באבטחת מידע והגנה על מערכות המידע.[103] המפקח על הבנקים בבנק ישראל הוציא אף הוא חוזר מקיף ומפורט.[104] החוזר מדגיש בין היתר: "טכנולוגיית המידע היא מרכיב מרכזי בתפעול ובניהול תקין של תאגיד בנקאי, בהיות המידע, על כל היבטיו והשלכותיו, בעל השפעה מכרעת על יציבות התאגיד הבנקאי והתפתחותו". הנחיה כזאת יכולה לשמש דוגמה למשרדי הממשלה האחרים ביחס לגופים שמולם הם פועלים במדינה.

מטה הסייבר הצה"לי. בשנת 2009 הגדיר הרמטכ"ל, רב־אלוף גבי אשכנזי, את המרחב הקיברנטי כמרחב לחימה אסטרטגי ואופרטיבי. בהתאם לכך הוקם "מטה הסייבר" הצה"לי, שנועד לשמש מטה מטכ"לי לתיאום ולהכוונה של פעולות הצבא במרחב הקיברנטי. המטה הוקם ביחידה 8200 באגף המודיעין (אמ"ן),[105] ושותפים בו נציגים מאמ"ן ומאגף התקשוב.[106] האלוף עמוס ידלין, בהיותו ראש אמ"ן, התייחס לנושא בהרצאה במכון למחקרי ביטחון לאומי בדצמבר 2009. הוא ציין את הפוטנציאל לפגיעות בישראל עקב פריצות למחשבים כאחד האיומים הלאומיים. לדבריו: "צה"ל מתכוון לספק הגנה טובה לרשתות, וגם להפעיל התקפות קיברנטיות משלו".[107] המטה הקיברנטי הצה"לי יכול להיות שותף בהגנת המרחב הקיברנטי של המדינה, בדומה לפיקוד הקיברנטי בארצות־הברית, אך גם הוא אינו הגוף המיועד לאינטגרציה לאומית להגנת המרחב הקיברנטי הלאומי.

מטה הסייבר הלאומי. ב־18 במאי 2011 הכריז ראש הממשלה בנימין נתניהו על הקמת מטה סייבר לאומי. לפי הודעת משרד ראש הממשלה: "ייעודו העיקרי של המטה הוא להרחיב את יכולות ההגנה של המדינה על מערכות התשתיות החיוניות מפני התקפות טרור קיברנטי, המבוצעות הן בידי מדינות זרות והן בידי גורמי טרור."[108] המטה הוקם בעקבות המלצות צוות בראשות יו"ר המועצה הלאומית למחקר ופיתוח, האלוף במילואים יצחק בן ישראל. נתניהו הודיע כי אימץ את מלוא ההמלצות והסביר כי "בתחום ההגנתי ישראל חשופה להתקפות סייבר שיכולות לשתק מערכות חיים שמפעילות את המדינה, כגון: חשמל, תקשרת, כרטיסי אשראי, מים, תחבורה. כל תחום הוא ממוחשב ולכן פגיע. יש צורך לגבש מענה הגנתי לאיום הזה". עוד דווח, כי המטה החדש צפוי לפעול לטיפוח חברות ישראליות המתמחות בהגנה על מרחב הסייבר, בניסיון לגזור נתח מהשוק הנרחב המתפתח בנושא ברחבי העולם.[109] הקמת המטה תהווה חידוש משמעותי משום שעד כה אין בישראל גוף שאמון על הטיפול בהגנת המרחב הקיברנטי בראייה הלאומית. הטיפול ההגנתי במרחב הקיברנטי בישראל התמקד ביחידות אופרטיביות (במשרד האוצר, בשב"כ ובצה"ל), אך חסר בדרג המדיני־האסטרטגי שמעליו (ראו לוח 5).

לוח 4: התארגנות במרחב הקיברנטי – השוואה בין ישראל לארצות־הברית

	הקמת גופים העוסקים בקביעת מדיניות, סנכרון, ותיאום מדינתי	הקמת גופים אופרטיביים
ארצות־הברית	מינוי עוזר מיוחד לנשיא ומתאם הגופים הפועלים לאבטחת המרחב הקיברנטי (2009). הוא אחראי לגיבוש, תיאום וסנכרון של מדיניות הממשל, לעבודה עם משרד האוצר ולניהול משברים. על משרדי הממשלה השונים הוטלה האחריות לקדם ולתאם את הגנה על התשתיות החיוניות שבתחום אחריותם. במשרד החוץ מונה במאי 2011 מתאם למימוש האסטרטגיה הבינלאומית של ארצות הברית במרחב הקיברנטי.	הקמת מחלקת ביטחון הסייבר במשרד ביטחון המולדת (National Cyber Security Division) כפועל יוצא מהאסטרטגיה לביטחון המרחב הקיברנטי משנת 2003. הקמת פיקוד הסייבר של צבא ארצות הברית בשנת 2010.
ישראל	ההחלטה על הקמת מטה לאומי קיברנטי (מאי 2011).	הקמת תהיל"ה (תשתית הממשלה לעידן האינטרנט) בשנת 1997. הקמת הרשות הממלכתית לאבטחת מידע בשב"כ בשנת 2002. הקמת "מטה הסייבר" בצה"ל (2009 – 2010).

המלצות לישראל

למדינת ישראל יש שלש סיבות טובות להאיץ את התארגנותה הביטחונית במרחב הקיברנטי:

א. בדומה למדינות מערביות מפותחות אחרות, המרחב הקיברנטי חושף את ישראל לסיכונים בסיסיים ניכרים, ובהם סיכונים לפגיעה בתשתיות חיוניות, במערכת הביטחון, בתפקוד המשק וכו'.

ב. בשונה ממדינות רבות, ישראל ניצבת בפני אויבים שלהם מוטיבציות ברורות ומוצהרות לפגוע בה ככל הניתן. מדובר למשל באיראן, הפועלות להשיג גם יכולות קיברנטיות התקפיות.[110] כמו כן תיתכן כניסת ארגוני טרור לפעילות התקפית במרחב הקיברנטי אשר תופנה נגד ישראל.

ג. לישראל שהיא בין המובילות בעולם בידע בתחומי טכנולוגיות המידע ובנוכחות במרחב הקיברנטי, יש את האפשרות לפתח הגנה מתקדמת ולמצות את היתרונות שמגלם המרחב הקיברנטי בשדה הקרב.

במסגרת האצת ההתארגנות הישראלית, נדרשים בין היתר הצעדים הבאים:

א. קביעת אסטרטגיה לאומית לביטחון המרחב הקיברנטי הישראלי, ויישום האסטרטגיה בהובלת מטה הסייבר הלאומי.

ב. שילוב הלוחמה הקיברנטית כרכיב באסטרטגיית הביטחון של ישראל.[111]

החלטה על הקמת מטה הסייבר הלאומי הינה אמנם צעד חשוב נוסף בהתמודדות ישראל עם האתגר הקיברנטי, אולם יש להבטיח כי המטה יפעל על פי אסטרטגיה קיברנטית לאומית, שתגובש לשם כך. כמו כן, נוכח הפיגור של ישראל בתחום זה חשוב כי המטה יוקם במהירות[112] ויקבל אחריות וסמכויות הולמת, כדי למלא אחר הפער הקיים ברמה הלאומית בנוגע לניהול אסטרטגי ואינטגרציה בין כלל הגורמים האופרטיביים – האזרחיים והצבאיים – הפועלים במרחב הקיברנטי בהקשר ההגנתי.

האסטרטגיה להגנת המרחב הקיברנטי של ישראל – הצעה

מוצע לישראל לגבש אסטרטגיה לאומית לביטחון המרחב הקיברנטי, אשר תביא להשגת המטרות האסטרטגיות במשאבים מינימאליים ותשמש מסגרת לפעולה של כלל הגופים השותפים בהגנת המרחב הקיברנטי. האסטרטגיה תאושר בידי הקבינט ותשמש קו מנחה הן לפעולה המשותפת של הגופים והן לפעולתו של כל גוף מתוקף אחריותו. להלן יעדי האסטרטגיה ועקרונות הפעולה הכלליים שלה.

יעדי האסטרטגיה:

א. לקיים בישראל מרחב קיברנטי בטוח, שיאפשר למדינה לממש את יעדיה הלאומיים בתחומי הממשל, הביטחון, המשק, החברה, החוץ, המדע ועוד.

ב. לחזק את הביטחון במרחב הקיברנטי הישראלי ולשמור על חופש הפעולה בו לרווחת כלל האוכלוסייה.

האסטרטגיה אמורה לקדם את השגת היעדים הללו באמצעות שילוב כוחות בין כל הגורמים הרלוונטיים במדינה, וזאת בהתאם לעקרונות הפעולה הבאים:

א. הכרה במרחב הקיברנטי כמרחב לאומי חדש, שיש להגן עליו באופן ייחודי (בשונה מהמרחבים המסורתיים), תוך ראייה כוללת ושיתוף פעולה בין כל הגורמים הנוגעים בדבר.

ב. כינון הנהגה ומנגנון מרכזי להגנה קיברנטית ברמה לאומית (הקמת ארגון ברמה מדינתית).

ג. ניהול סיכונים מתוך ראייה כוללת ובכלל זה העמדת התשתיות הלאומיות הקריטיות ומערכות הביטחון בראש סדר העדיפויות, אך גם טיפול בהגנת רכיבים נוספים של המשק והחברה. למשל, הגנה על מאגרי ידע של האוניברסיטאות ומכוני

מחקר, הגנה על חברות בעלות השפעה על המשק (שאינן בקטגוריה של תשתיות), הגנה על חברות הקשורות לחברות של תשתיות חיוניות ועוד.

ד. בניית מערך הגנה דינמי, אינטגרטיבי ומקיף ובכלל זה: שילוב בין מערכות הגנה פסיביות לבין מערכות הגנה אקטיביות (ראו אסטרטגיית הביטחון הקיברנטית של הפנטגון), שילוב בין הגנה על יעדים חיוניים לבין מרכיבי "הגנה מרחבית" (תעבורה הנכנסת למדינה, צמתי תקשורת), שיפור ארכיטקטורת רשתות, הידוק בין מנגנוני אבטחה פיסיים לאלה הקיברנטיים ועוד.

ה. שילוב כוחות במגזר הציבורי (הממשלתי) בין המגזר הביטחוני לבין המגזר האזרחי; וכן שיתוף פעולה ושילוב מאמצים בין יחידות בתוך כל אחד מהמגזרים הללו. למשל, שילוב מאמצים ושיתוף בידע בין הצבא לבין כוחות הביטחון האחרים.

ו. שיתוף פעולה הדוק בין הסקטור הממשלתי (הביטחוני והאזרחי) לבין הסקטור הפרטי בהגנה על המרחב הקיברנטי ובכלל זה שיתוף במידע וביכולות, כך שכל ארגון ממשלתי ופרטי מתאים יהיה מודע לסיכונים, לאירועי תקיפה וליכולות הגנה חדשות.

ז. שיתוף פעולה הדוק עם גורמי חוץ. למשל, בניית מערכות ניטור קולקטיביות עם בעלות ברית.

ח. חקיקה ואכיפה, שתאפשר פעולה הגנתית.

ט. סיוע לכלל האוכלוסייה בהתגוננות קיברנטית. למשל, הסברה להגברת מודעות הציבור לאיומים ולפתרונות, מתן תמריצים לעסקים ולתושבים ברכישת תוכנות הגנה, הגברת הפיקוח על חברות אבטחה וספקי תקשורת לציבור בהיבט האמור.

י. בניית יכולת להתאוששות מהירה מהתקפה.

יא. שימוש בשיטות ובאמצעים הטכנולוגיים המתקדמים ביותר.

יב. גיבוש מדיניות הרתעה, סיכול תקיפות ותגובה כרכיבים משלימים לאסטרטגיה. בכלל זה: יכולת תגובה ישירה נגד מערכות קיברנטיות תוקפות,[113] ויכולת פגיעה בתוקפן. על עניין זה ממונה מערכת הביטחון.

לצורך מימוש האסטרטגיה, אנו מציעים לכלול, בין תפקידיו של מטה הסייבר הלאומי, את התפקידים הבאים:

א. סיוע לדרג המדיני בקבלת החלטות ובעיצוב מדיניות בתחום הגנת המרחב הקיברנטי הלאומי. בכלל זה, גיבוש הצעה לאסטרטגיה לאומית להגנת המרחב הקיברנטי, בשיתוף עם הגורמים הרלוונטיים, אשר תאושר בידי הקבינט המדיני־ביטחוני.

ב. הערכות סיכונים – שוטפות ועיתיות, בהסתמך על נתונים והערכות, שיספקו גופי המודיעין והגופים האופרטיביים והטכנולוגיים הרלוונטיים.

ג. הערכות מצב – שוטפות ועִתיות, ובכלל זה המלצות לפעולה על סמך ניתוח חלופות.
ד. הוראת האסטרטגיה לגופים האזרחיים המשתתפים בהגנה על המרחב הקיברנטי ותיאום עם הגופים במגזר הביטחוני.
ה. תיאום הפעולות של כל הגורמים הממשלתיים והפרטיים הנוגעים לביטחון המרחב הקיברנטי. בכלל זה הטלת אחריות על משרדי הממשלה האזרחיים לקדם את הביטחון הקיברנטי בתחומם (כפי שעושים למשל משרד האוצר והמפקח על הבנקים בבנק ישראל כלפי גופים פיננסיים מוסדיים).
ו. הקמת מרכז אופרטיבי מדינתי ("מרכז מבצעים" קיברנטי) וניהולו. תפקידו יהיה ליצור תמונת מצב דינמית של איומים קיברנטיים, לשתף מידע בין כל הגופים הנוגעים בדבר ולסייע בניהול ההגנה.
ז. קביעת מערכות התשתית והגופים האזרחיים, שעל המדינה להנחותם או לאבטח אותם בתחום הקיברנטי, בהתאם לאסטרטגיה הלאומית.
ח. ייזום חקיקה ותקנות, החיוניות לפעולות לשם הגנת המרחב הקיברנטי בשגרה ובחירום.
ט. ייזום והובלת פרויקטים ממשלתיים, למשל פרויקטים בנושאים האלה: שדרוג שיטות ואמצעי ההגנה על מערכות המידע (בכלל זה אבטחה פיסית), כינון מערכת ממוסדת להדרכה של עובדים בסקטור הממשלתי, שיפור יכולת ההתאוששות לאחר התקפה קיברנטית, ניהול תרגילי הגנה קיברנטיים ברמה לאומית.
י. קביעת קריטריונים לפיתוח, לרכש ולהתקנת אמצעי תקשוב, בהיבטים של ביטחון קיברנטי.
יא. מתן אישורים להקמת תשתיות תקשוב, בהקשר להשפעתן על ביטחון המרחב הקיברנטי הלאומי.
יב. ייזום והכוונה בתחום פיתוח אמצעי הגנה, הכשרת כוח אדם מקצועי ומחקר מדעי בהקשר לביטחון המרחב הקיברנטי. בכלל זה הענקת תמריצים לגופי מחקר.
יג. ייזום שיתופי פעולה אסטרטגיים בין הסקטור הממשלתי לבין הסקטור הפרטי. בכלל זה שיתוף פעולה עם חברות תקשורת וטכנולוגיה בתחום התפעולי ובתחומי המחקר והפיתוח.
יד. ריכוז שיתוף פעולה עם מדינות אחרות בנוגע לביטחון המרחב הקיברנטי.
טו. בקרה על יישום האסטרטגיה ועל הפעילות בתחום הגנת המרחב הקיברנטי. וידוא קיום פיקוח ראוי על משרדי הממשלה השונים והרשויות האזרחיות, פיקוח על ספקי תקשורת מבחינת ציוד ויישום כללי ביטחון קיברנטי.
טז. שיפור התגוננות של התושבים במדינה – באמצעות צעדי הסברה, מתן תמריצים להצטיידות בתוכנות הגנה (למשל, הקלות במס), ופיקוח על רמת השירות שנותנים ספקי תקשורת וחברות אבטחה לאוכלוסייה.

יז. להוות מרכז ידע לאומי בתחום הגנת המרחב הקיברנטי, המקושר אל מרכזי ידע בארץ ובחו"ל. בכלל זה למידה של דרכי ההתמודדות של מדינות אחרות עם האתגר הקיברנטי.

שילוב המרחב הקיברנטי באסטרטגיית הביטחון של ישראל

הוספת מרחב לחימה חדש למרחבים המסורתיים (יבשה, הים, אוויר וחלל) מחייבת לשלב את המרחב הקיברנטי באסטרטגיית הביטחון, או בתפיסת הביטחון,[114] של ישראל. הצעה לתפיסת ביטחון מעודכנת הוכנה באפריל 2006, לפני מלחמת לבנון השנייה, על ידי ועדה בראשות מר דן מרידור, שמינה שר הביטחון עמיר פרץ. הוועדה הצביעה בין היתר על הרלוונטיות הנמוכה של מושג ההרתעה בהקשר למאבק בטרור, על הקושי ליישם את המשתמע ממושג ההכרעה והמליצה להוסיף את ההגנה כרכיב נוסף לשלושת הרכיבים המסורתיים (הרתעה, התרעה והכרעה).[115] האלוף עמוס ידלין, בהיותו ראש אמ"ן, אמר בדצמבר 2009, כי "תחום הלוחמה הקיברנטית תואם היטב לדוקטרינה ההתקפית של ישראל. זהו תחום שהוא כולו כחול־לבן, שאינו נשען על סיוע או טכנולוגיה זרים. ישראלים צעירים מכירים היטב את התחום הזה, שהרי ישראל הוכתרה באחרונה כמדינת הסטארט־אפים".[116]

בחינה של המושגים הרלוונטיים לתפיסת הביטחון של ישראל (כמפורט בפרק א) הראתה, שתוכני המושגים של תפיסת הביטחון המסורתית אינם מתאימים למרחב הלחימה הקיברנטי. למשל, קשה מאוד ליישם הרתעה במרחב הקיברנטי, להתרעה האופרטיבית אין משמעות ללא הגנה אקטיבית, והגנה קיברנטית מחייבת התאמה עמוקה לתכונות הייחודיות של המרחב. שיתוף הפעולה המתחייב להגנת המרחב הוא חסר תקדים בהשוואה לשיתופי פעולה אחרים בין הסקטור הביטחוני לאזרחי לצורך פעילות צבאית. זאת ועוד, לאור ההכרה במרחב הקיברנטי כמרחב לחימה, נדרש לבחון יכולות אסטרטגיות חדשות ואולי אף לחולל שינוי בסדר הכוחות, דהיינו להשקיע יותר בהקמת צבא קיברנטי.

לסיום, לישראל יש פוטנציאל להיות בין המדינות המובילות בעולם בתחום הביטחון הקיברנטי, בהתחשב בהון האנושי והידע הטכנולוגי הגבוהים שבידיה. מיצוי פוטנציאל זה עשוי לתרום למדינה בתחומי הביטחון והכלכלה.

נספח א

המלחמה במרחב הקיברנטי - מילון מונחים[1]

התקפת רשתות מחשב – Computer network attack (CNA)

פעולות באמצעות שימוש ברשתות מחשבים, שמטרתן לשבש, להרוס או להשחית מידע הקיים במחשבים או ברשתות מחשבים או למנוע גישה אליהם; או פעולות שנועדו לשבש, למנוע, להרוס או להשחית את המחשבים ואת הרשתות עצמם (וכנראה גם מכשירים המחוברים למרחב הקיברנטי).

הגנת רשתות מחשבים – Computer network defense

צעדים הננקטים כדי להגן, לנטר, לנתח ולאתר פעילות לא מורשית המתקיימת בתוך מערכות המידע ורשתות המחשבים, ועל מנת להגיב אליה.

תגובה במסגרת הגנת מערכות התקשוב – Computer network defense response actions

צעדי הגנה מורשים* הננקטים כדי להגן על מערכות המחשב והרשתות המצויות תחת מתקפה, או על כאלה שבכוונת היריב לתקוף באמצעות מערכות מחשב ורשתות יריבות.

* בתזכיר עוזר מזכיר ההגנה של ארצות־הברית ("הנחיות בדבר צעדי התגוננות של רשתות מחשבים") מצוינים צעדי התגובה שנועדו לחזק את יכולות ההגנה של משרד ההגנה ברבדים העמוקים, ולשפר את יכולתו לעמוד בפני התקפות יזומות של יריבים.

איסוף מידע מרשתות מחשבים – Computer network exploitation

פעולות איסוף מידע – הננקטות באמצעות השימוש ברשתות מחשבים ממערכות מידע של יריבים או איסוף באמצעות מערכות ממוכנות על אודות יריבים.

מבצעי רשתות מחשבים – Computer network operations

פעילויות בתחומי ההתקפה על רשת מחשבים (CNA), הגנת רשתות מחשבים (CND) ואיסוף מידע מרשתות מחשבים (CNE).

---

1 המילון מבוסס על מסמך של צבא ארצות־הברית: *The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028*, 22 February 2010

אבטחה של תשתיות קריטיות – Critical infrastructure protection

צעדים הננקטים על מנת למנוע, או למתן את הסיכונים הנובעים מן הפגיעות או מהחשיפה של נכסי תשתית חיוניים, בהתאם לסוג הסיכון. צעדים אלה עשויים לכלול: שינויים בטקטיקות, טכניקות או נהלים; הוספת יתירות (גיבויים, מערכות כפולות), בידוד של רשתות או הקשחה של האבטחה.

התקפה קיברנטית – Cyber attack (CyA)

צעדי התקפה המשלבים התקפה על רשת מחשבים עם פעילויות מסייעות אחרות, כגון לוחמה אלקטרונית, התקפה פיסית, ואחרות.

ניהול תוכן קיברנטי – Cyber content management (CyCM)

ניהול תוכן קיברנטי מהווה את הטכנולוגיה, התהליכים והמדיניות הנדרשים על־מנת להעניק מודעות (ידע ונגישות) למידע רלוונטי ומדויק; גישה אוטומטית למידע חדש שהתגלה זה לא מכבר או למידע חוזר, כמו גם הענקת מידע במועד ובאופן יעיל ובטוח בפורמט שימושי.

ביון נגדי במרחב הקיברנטי – Cyber counterintelligence

צעדים שנועדו לזהות או לנטרל פעילות זרה, או לחדור אליה, העושה שימוש בכלים קיברנטיים כמתודולוגיה עיקרית. לחלופין, פעילות הננקטת כדי לזהות ולנטרל את מאמצי האיסוף של ארגוני מודיעין זרים העושים שימוש בשיטות מסורתיות כדי להעריך יכולת וכוונות קיברנטיות, או כדי לחדור למערכות קיברנטיות.

הגנה במרחב הקיברנטי – Cyber defense (CyD)

מכלול צעדים המשלבים ביטחון מידע, הגנה על רשתות מחשבים (בכלל זה צעדי תגובה) והגנה על תשתית קריטית עם יכולות מסייעות (כגון הגנה אלקטרונית, תמיכה בתשתית חיונית ואחרים). ההגנה במרחב הקיברנטי משולבת עם מרכיבי התגוננות דינמיים של לוחמה הקיברנטית.

ניהול פרויקטים קיברנטיים – Cyber enterprise management (CyEM)

ניהול הטכנולוגיה והתהליכים הנדרשים כדי להפעיל ביעילות מערכות ורשתות מחשב.

איסוף קיברנטי – Cyber exploitation (CyE)

איסוף מידע באמצעות ניצול רשת מחשבים (CNE) בשלוב עם יכולות מסייעות (כגון תמיכה בלוחמה אלקטרונית, מודיעין אותות ואחרים) למטרות מודיעין ומאמצים אחרים.

פעולות רשת במרחב הקיברנטי – Cyber network operations (CyNO)

פעולות ברשת, שעליהן מתבססות פעולות במרחב הקיברנטי שנועדו לשם תפעול, ניהול, אבטחה, הגנה, פיקוד ובקרה של תשתיות רשת השליטה ופיקוד של צבא ארצות־הברית בשדה הקרב.

מודעות מצבית קיברנטית – Cyber situational awareness

הידיעה המידית של מצב "כוחותינו" ושותפינו (כוחות ידידותיים) במרחב הקיברנטי, מידע על אודות היריב במרחב הקיברנטי וכל מידע רלוונטי אחר הנוגע לפעילות במרחב הקיברנטי ובאמצעותו, ובספקטרום האלקטרומגנטי. המודעות מושגת באמצעות מודיעין ופעילות מבצעית במרחב הקיברנטי, בספקטרום האלקטרומגנטי ובתחומים אחרים, הן באופן חד־צדדי והן באמצעות שיתוף פעולה עם שותפינו לפעילות אחידה, והשותפים הציבוריים־הפרטיים.

פעילות תומכת במרחב ובלוחמה הקיברנטית – Cyber support

סוג הפעילויות התומכות הנוצרות כדי לאפשר באופן ספציפי את פעילות הרשתות (CYNetOps) ואת הלוחמה הקיברנטית (CyberWar). פעולות אלה כוללות: הערכת פגיעות (חולשות), הערכת הביטחון התפעולי של המרחב הקיברנטי, מודיעין בנוגע למרחב הקיברנטי, מודיעין טכנולוגי המופק מתוכנות זדונית, מודיעין נגדי, היבטי חוק, זיהוי פלילי, בדיקה והערכה של מחקר ופיתוח, פיתוח לחימה ורכש.

מרחב קיברנטי – Cyberspace

מרחב גלובלי בתוך סביבת המידע, המורכב מרשתות הנשענות על תשתיות טכנולוגיות המידע, התלויות אלה באלה, לרבות האינטרנט, רשתות טלקומוניקציה, מערכות מחשבים, מעבדים, שבבים ובקרים.

פעולות ומבצעים במרחב הקיברנטי – Cyberspace operations

פעולות העושות שימוש ביכולות קיברנטיות, שהמטרה העיקרית היא העמידה ביעדים במרחב הקיברנטי ובאמצעותו. פעילות זו מכילה תפעול רשתות מחשבים ופעילות שנועדה להפעיל את רשת המידע הגלובלית (GIG) ולהגן עליה.

לוחמה קיברנטית – Cyberspace warfare (CyberWar)

מבצעים קיברנטיים חודרניים ("מעבר לגבולות בני ההגנה של רשת המידע הגלובלית"), שמטרתם לאתר, להרתיע ולהביס יריבים ולמנוע מהם גישה למידע. הלוחמה הקיברנטית שמה לעצמה למטרה רשתות מחשבים ותקשורת, כמו גם מעבדים ובקרים המוטמעים בציוד, מערכות ותשתיות. לוחמה קיברנטית עושה שימוש באיסוף קיברנטי, בהתקפה קיברנטית ובהגנה קיברנטית, וכן בכל הפעולות הנוגעות לתמיכה ביכולות הקיברנטיות.

הגנה דינמית במרחב הקיברנטי – Dynamic cyber defense (DCyD)

פעילות ההגנה הדינמית במרחב הקיברנטי משלבת בין היבטי מדיניות, מודיעין, חיישנים ותהליכים המבוססים על דרגת אוטומציה גבוהה כדי לזהות ולנתח פעילות זדונית, וכדי לזהות ולהוציא אל הפועל בו בזמן צעדים שאושרו מראש על מנת להביס התקפות עוד לפני שהן מצליחות לגרום נזק. ההגנה הדינמית במרחב הקיברנטי מתבססת על עקרונות ההגנה של הצבא בתחומי הביטחון, ההגנה לעומק והשימוש

המרבי בפעילות התקפית כדי להתמודד עם איומים קיברנטיים. הפעילות כוללת השגחה וזיהוי כדי שיהיה אפשר לספק אזהרה מוקדמת של פעילות אויב העומדת להתרחש. ההגנה הדינמית במרחב הקיברנטי משולבת עם ההיבטים ההגנתיים של מבצעי רשת כדי להעניק הגנה לעומק.

הערה: בטקסטים האמריקניים נמצאו שני מושגים בעלי דמיון רב: הגנה דינמית, כמופיע במילון הצבאי, והגנה אקטיבית כמופיע אצל סגן מזכיר ההגנה לין (לא נמצא במילון המונחים הצבאי).

ספקטרום אלקטרומגנטי – Electromagnetic spectrum

טווח התדרים של הקרינה האלקטרומגנטית, מאפס ועד אינסוף. הטווח מחולק לעשרים ושישה ערוצים בהתאם לאלף־בית הלטיני.

לוחמה אלקטרונית – Electronic warfare

פעילות צבאית הכוללת את השימוש באנרגיה אלקטרומגנטית ומכוונת לשלוט בספקטרום האלקטרומגנטי, או לתקוף את האויב. בלוחמה האלקטרונית שלושה רכיבים: התקפה אלקטרונית, הגנה אלקטרונית, ותמיכה בלוחמה האלקטרונית. התקפה אלקטרונית (Electronic attack) היא פעולה הכרוכה בשימוש באנרגיה אלקטרומגנטית, אנרגיה מכוונת או בנשק למניעת קרינה כדי לתקוף בני אדם, מתקנים או ציוד מתוך מטרה לפגום ביכולת הלחימה של האויב, לשתק אותה או להרוס אותה לחלוטין. ההתקפה האלקטרונית נחשבת לסוג של אש. הגנה אלקטרונית (Electronic protection) כוללת צעדים הננקטים כדי להגן על כוח אדם, מתקנים וציוד מפני כל השפעה של השימוש, אם בידי כוחותינו ואם בידי האויב, בספקטרום האלקטרומגנטי, המסוגל לפגום ביכולת הלחימה של כוחותינו, לנטרל או לחסל אותה.

רשת מידע גלובלית – Global information grid (GIG)

רשת המידע הגלובלית (GIG) ובה מערכות ושירותי תקשורת ומחשבים, תוכנה לרבות יישומים, נתונים, שירותי ביטחון, שירותים קשורים אחרים, וגם מערכות ביטחון לאומי. הרשת מבוססת על מכלול יכולות המידע הקשורות אלה באלה ברמה הגלובלית, כמו גם על התהליכים הקשורים בה, וכוח האדם העוסק באיסוף, בעיבוד, בשמירה, בהפצה ובניהול המידע על פי דרישה – עבור קובעי מדיניות, לוחמים וכוח אדם אחר בתפקידי תמיכה.

מידע – Information

עובדות, נתונים או הוראות בכל מדיה או צורה. הפירוש שאדם מעניק לנתונים באמצעות המוסכמות הידועות שבהן נעשה שימוש להצגתם.

אבטחת מידע – Information assurance

צעדים שנועדו להגן על מידע ועל מערכות מידע על ידי כך שמובטחים זמינותם, שלמותם, האימות שלהם, סודיותם ואי־ההתנערות מהם. פעילות זו כוללת את הדאגה לשחזורן של מערכות מידע על ידי הכללתן של יכולות הגנה, איתור ותגובה.

מסרי מידע – Information engagement

שימוש במידע למטרות הסברה, תעמולה ולוחמה פסיכולוגית. השימוש הכולל באמצעי הקשר הקיימים עם הציבור הרחב על מנת ליידע הן את הציבור האמריקני והן ציבור ידידותי אחר; מבצעים פסיכולוגיים, תיעוד מצולם של פעילות צבאית באוויר, בים וביבשה, תקשורת אסטרטגית של ממשלת ארצות־הברית ותמיכה בדיפלומטיה הציבורית, כמו גם אמצעים אחרים הנחוצים להשפיע על קהלי מאזינים זרים; בנוסף, מעורבות מנהיגים וחיילים שנועדה לתמוך בשני המאמצים דלעיל.

מבצעי מידע (שימוש אקטיבי במידע, סיגנלים וביטים) – Information operations

השימוש הכולל ביכולות הליבה של הלוחמה האלקטרונית, מבצעי רשתות מחשבים, מבצעים פסיכולוגיים, הונאה צבאית וביטחון מבצעי, בתיאום עם יכולות תמיכה ספציפיות ואחרות, כדי להשפיע על תהליך קבלת החלטות אנושי או אוטומטי, לפגוע בו, להרוס אותו או להשתלט עליו בכוח תוך הגנה עליו.

מודיעין – Intelligence

המוצר הנגזר מן האיסוף, עיבוד, האינטגרציה, הערכה, ניתוח ופרשנות של מידע זמין הנוגע למדינות זרות, או הנוגע לכוחות או רכיבים עוינים או עוינים באופן פוטנציאלי, או של מידע הנוגע לתחומי מבצעים המתנהלים בפועל או של מבצעים פוטנציאליים. מונח זה משמש גם לפעילות המובילה להיווצרותו של המוצר ולארגונים המעורבים בפעילות.

אינטרנט – Internet

רשת תקשורת אלקטרונית המחברת רשתות מחשבים ומתקני מחשוב סביב העולם.

רשת לשליטה ופיקוד בשדה הקרב – LandWarNet

תרומתו של הצבא לרשת המידע הגלובלית (GIG) המתבטאת במכלול יכולת המידע של צבא ארצות־הברית מקצה לקצה, הקשורות אלה באלה ברמה גלובלית, התהליכים הנלווים, וכוח האדם העוסק באיסוף, עיבוד, שמירה, הפצה וניהול המידע על פי דרישה, על מנת להעניק תמיכה ללוחמים, קובעי מדיניות, וכוח אדם האמון על תפקידי תמיכה. המונח מכיל מערכות ושירותי תקשורת ומחשבים בבעלות מלאה ובחכירה של צבא ארצות־הברית, וכן מערכות ושירותי תקשורת ומחשבים ממונפות ומשותפות של משרד ההגנה של ארצות־הברית, תוכנה לרבות יישומים, נתונים, שירותי ביטחון ושירותים קשורים אחרים. הרשת המאפשרת שליטה ופיקוד בשדה הקרב קיימת כדי לאפשר את הלחימה באמצעות הפיקוד על שדה הקרב.

מרכז משימתי ברשת – Network Enterprise Center

מרכז המאפשר גישה לרשתות, לשירותי רשת, לאמצעי תקשורת ולשירותי מידע ארגוניים ליחידות נייחות מקומיות (דואר, מחנה, בסיס).

פעולות לתפעול הרשת – Network operations (NetOps)

פעילות הננקטת כדי להפעיל את רשת תקשורת המידע הגלובלית (GIG), שבה משתמש צבא ארצות־הברית, ולהגן עליה.

מרכז שירות ברשת הגלובלית – Network service center

תפקידי הפעלת הרשת הגלובלית ונקודות תמיכה, שירותי מידע וקישוריות רשת באמצעות TNOSCs (מבצעי רשת בזירה ומרכזי ביטחון), מרכזי עיבוד מידע אזוריים, ונקודות קישור אזוריות.

סביבה אופרטיבית – Operational environment

מכלול התנאים, הנסיבות וההשפעות, המשליכים על השימוש ביכולות והמשפיעים על החלטותיו של המפקד.

אות אלקטרוני – Signal

כל סוג של אות חשמלי משודר, כפי שנעשה בו שימוש בתחום האלקטרוניקה. בהיבט התפעולי מדובר בסוג של הודעה שהטקסט שלה מורכב מסיגנל, אות, מילה, סימן, תצוגה חזותית או קול מיוחד, בודדים או אחדים מהם, בעלי משמעות שנקבעה מראש, והמועברים או משודרים באמצעים חזותיים, אמצעי שמע או באמצעים חשמליים.

מודיעין אותות אלקטרוניים (סיגינט) – Signals intelligence

קטגוריה של מודיעין ובה מודיעין התקשורת, המודיעין האלקטרוני ומודיעין האותות המבוסס על מכשור זר, אם כל אחד מאלה בפני עצמו ואם כולם במשולב, בלי קשר לאופן שבו הוא משודר. מודיעין הנגזר מתקשורת ומאותות המבוססים על מכשור אלקטרוני ועל מכשור זר.[117]

נספח ב

חשיפת סודות בסיוע טכנולוגיות המידע

חשיפת סודות והפצתם בסיוע טכנולוגיות המידע הוא תחום פעילות בולט בשנים האחרונות. עיקר הפעילות בתחום זה היא של ארגונים או של יחידים בעלי מניעים פוליטיים נגד ממסדים מדינתיים, בכלל זה במדינות דמוקרטיות. עם זאת, שיטה זו, שהיא חלק מלוחמת מסרי מידע, משמשת או עשויה לשמש כלי גם בשירותן של מדינות. כן היא מלמדת על תכונותיו של המרחב הקיברנטי ובכלל זה על הקלות היחסית שאפשר לדלות מידע מסווג ולהפיצו באמצעות טכנולוגיות המידע, כמו גם על יכולתו של המרחב להעצים את כוחם של שחקנים קטנים. מצד אחד זהו מאזן כוחות חדש, שבו המרחב הקיברנטי מפצה על א־סימטריה בין הכוחות, אך מצד אחר יש בידי מעטים כוח לגרום נזק לרבים.

אירוע ויקיליקס (WikiLeaks) בסוף שנת 2010 מדגים את הדרך שבה יכול המרחב הקיברנטי להעצים פעולות עוינות של חשיפת סודות מדינתיים. ב־28 בנובמבר 2010 פתח אתר ויקיליקס[117] בהדלפה הגדולה בהיסטוריה על בסיס מסמכים שהעביר אליו חייל בצבא ארצות־הברית, ברדלי מאנינג. האתר פרסם מאות אלפי מסמכים ובהם מסמכים מסווגים של משרד החוץ של ארצות־הברית, הנוגעים למפגשים בין דיפלומטים אמריקניים למנהיגים ופקידים בכירים של מדינות ברחבי העולם. מידע שהודלף מהאתר הופץ באמצעי תקשורת אחרים ואף הועבר לידיהם בידי מפעילי האתר למקרה שהאתר ייחסם. הפצת המסמכים אמנם לא חשפה סודות ביטחוניים גדולים, אך היא גרמה, ובמודע, נזק גדול ליחסי החוץ של ארצות־הברית עם מדינות ידידות.[118] נראה שמעתה מנהיגי עולם יחשבו היטב אם להיחשף בפני מערך החוץ האמריקני, מה שעלול לפגוע בתהליכי קבלת החלטות בארצות־הברית. לחשיפה גם עלולה להיות השפעה שלילית על מערך השגרירים ושיבוצם.

להלן מאפייני האירוע בהקשר הקיברנטי:

א. חדירה עוינת למרחב הקיברנטי מבפנים. זוהי חדירה של איש פנים למרחב הקיברנטי המדינתי החסוי, וגנבת מידע בדומה לריגול. האירוע ממחיש את הסיכון הגלום בחדירה קיברנטית יומינטית (בידי סוכן אנושי) בכלל ושל "איש פנים" בפרט, שהרי מערכות ההגנה הקיברנטיות כמעט אינן ישימות כלפיו.

ב. טכנולוגיות המידע מעצימות יכולת של איסוף מידע, גנבתו והדלפתו. הדלפות הן אמנם פעילויות חשאיות ותיקות, אולם באירוע זה וכדוגמתו יש מאפיינים הניתנים לביצוע רק באמצעות טכנולוגיות המידע והמרחב הקיברנטי. למשל, יכולת מהירה לאתר ולדלות כמויות גדולות מאוד של מידע, להעתיקו באיכות גבוהה ולהפיצו במהירות הבזק מעבר לגבולות המדינה. בעבר פעילות חשאית כזאת, בלא טכנולוגיות המידע, הייתה נתקלת בקשיים לוגיסטיים ניכרים (איתור מידע בתיקים, מיון, צילום, אחסנה, שינוע והפצה – והכול בחשאי), ועל כן לא הייתה מתקיימת בממדים כאלה, אם בכלל. כאמור, פעילות החייל האמריקני באירוע זה אינה שונה במהותה מריגול ולכן ממחישה את השינוי הדרמטי שחוללה טכנולוגיית המידע בתחום הריגול האנושי.

ג. מיזוג בין מדיות (אמצעים לתקשורת המונים) במרחב האלקטרומגנטי. אתרי אינטרנט, כמו ויקיליקס, משלימים את אמצעי התקשורת האחרים (טלוויזיה, עיתונות ורדיו) בהיותם מאגרי מידע הנגישים לקוראים בכל עת. השילוב העצים מאוד את חשיפת המידע באירוע, ולכן גם את הנזק שהוא גרם.

ד. יריבים חדשים ואי־סימטריה בסביבה האסטרטגית החדשה. מדובר בעימות במרחב הקיברנטי בין ארגון פוליטי חוץ־מדינתי שולי לבין המעצמה החזקה בעולם.

פרשה דומה במאפייניה הקיברנטיים אירעה בישראל בשנת 2008, ובמרכזה עמדה ענת קם. בהיותה חיילת בצה"ל בלשכת אלוף פיקוד המרכז, אספה קם אלפי מסמכים ומצגות מסווגים במחשב צבאי שהיה בשימושה. סמוך לשחרורה מהצבא העתיקה קם את המסמכים לשני דיסקים שהכילו יותר מאלפיים קבצים, ובהם גם מסמכים בסיווג סודי ביותר. המסמכים הכילו תוכניות למבצעים צבאיים, סיכומי דיונים בצה"ל, פרטים על פריסת כוחות הצבא, סיכומי תחקירים, הערכות מצב ויעדים שונים של צה"ל. בספטמבר 2008 העבירה קם כ־1,500 מסמכים לעיתונאי "הארץ" אורי בלאו. על פי כתב האישום נעשה הדבר "ממניעים אידיאולוגיים ולשם פרסום המסמכים בציבור". בפברואר 2011, בהתאם להסדר, הודתה קם והורשעה בעברות של ריגול חמור (איסוף והחזקת ידיעה סודית) ומסירת ידיעה סודית.[119] אירוע זה ממחיש אף הוא את הקושי של מנגנוני האבטחה הקיברנטיים להתמודד עם פעילות עוינת של אנשי פנים.

פרשה אחרת הקשורה לישראל היא מאות מסמכים שנגנבו מהרשות הפלסטינית ופורסמו בינואר 2011 ברשת אל־ג'זירה ובאתר האינטרנט של העיתון "גארדיאן" הבריטי. המסמכים כללו פרטים סודיים מהמשא ומתן שהתנהל בשנים האחרונות בין ישראל לרשות הפלסטינית, וניכר שההדלפה כוונה להביך את בכירי הרשות הפלסטינית. חבר צוות המשא ומתן הפלסטיני נביל שעת' האשים את אל־ג'זירה בניסיון לעשות דה־לגיטימציה להנהגה הפלסטינית. לדבריו, המסמכים שדלפו אמיתיים, אולם אלה

ניירות לא רשמיים, שאינם מחייבים את הפלסטינים.[120] אירוע זה, בדומה לאירוע ויקיליקס, ממחיש את השילוב ההדוק בין המרחב הקיברנטי לבין אמצעי התקשורת. כיום מסכי אתרי האינטרנט מוצגים בטלוויזיה, ואילו שידורי טלוויזיה ניתנים לצפייה באמצעות האינטרנט. בקרוב תמזג הטכנולוגיה את שני אלה, ולכן אין משמעות להבחנה היכן מוצג המידע המודלף.

אירוע אחר של חשיפת סודות הוא עימות בין קבוצת ההאקרים "אנונימוס" לבין חברת האבטחה HBGary בתחילת שנת 2011. "אנונימוס", היא קבוצה של האקרים אקטיביסטים ממדינות שונות. אחת ממטרותיה העיקריות היא לאפשר לציבור באמצעות הרשת נגישות למידע שהממסד מנסה להסתיר. בניסיון לעצור את הקבוצה איימה חברת האבטחה HBGary לחשוף את ראשי הקבוצה. ההאקרים של "אנונימוס" הגיבו בפריצה לאתר החברה ובפרסום פרטים מביכים ודיונים פנימיים בחברה, וכך הוכיחו שרמת האבטחה שמספקת החברה היא נמוכה.[121] ב־1 במאי 2011 הודיעה "אנונימוס" על פתיחת מערכה מקוונת נגד ממשלת איראן במחאה על הדיכוי במדינה, ובמסגרתה תתקוף את אתרי הממשל של איראן. בהודעת הקהילה נכתב, שאיראן עדיין סובלת מידיהם של האוחזים בשלטון, המנסים להשתיק את העם האיראני. פעילות הקבוצה גם היא דוגמה לשחקנים החדשים במרחב הגלובלי, הבאים לדי ביטוי במרחב הקיברנטי, נוסף על מדינות לאום, ארגונים בינלאומיים, ארגוני טרור ואחרים.[122]

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 בו 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 אומנות, 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 הרצלייה 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).

37 "Markof, "A Code for Chaos, ראו הערה 19.

"Cyberwar in the fifth domain", *The Economist*, July 1, 2010.

38 ד"ר יניב לווייתן, "כך נלחמנו במחשבים, על מחשבים ובאמצעות מחשבים בעשור החולף", מעריב באינטרנט, 31 בדצמבר 2009.

39 *The NATO Cyber War Agreement*, Strategy Page (www.strategypage.com) May 1, 2010.

40 William J. Broad, John Markoff and David E. Sanger, "Israeli Test on Worm Called Crucial In Iran Nuclear Delay", *The New York Times*, January 15, 2011.

41 מתן מיטלמן, "צעד נוסף לחשיפת המסתורין סביב סטוקסנט", TheMarker, 16 בנובמבר 2010.

42 "אחמדינג'ד מודה: וירוס פגע במחשבי הגרעין", וואלה, 29 בנובמבר 2010.

43 יוסי הנטוני, "המלחמה על האטום", אתר אנשים ומחשבים, 26 בספטמבר 2010.

44 ראו לעיל הערה 40 (*The New York Times*, January 15, 2011).

45 יוסי מלמן, "הערכה: התולעת פגעה בתוכנית הגרעין האיראנית בשני ראשי חץ דיגיטליים", אתר הארץ, 20 בנובמבר 2010.

46 "איראן מאשימה: ישראל וארצות־הברית יצרו את תולעת המחשבים סטוקסנט", אתר הארץ, 16 באפריל 2011.

47 *The New York Times*, January 15, 2011.

48 Harlan Ullman, "Outside View: Worms of mass destruction", *Space war*, October 13, 2010.

49 "רוסיה: התולעת כמעט גרמה לצ'רנוביל איראני", Ynet, 21 בינואר 2011.

50 *The New York Times*, January 15, 2011.

51 "איראן שיקמה את הכור הגרעיני לאחר תקיפת התולעת", **גלובס**, 16 בפברואר 2011.

52 *Space war*, October 13, 2010. לעיל הערה 48.

53 לדוגמה: ב־19 באפריל 2011 גילתה חברת סוני היפנית פריצה לשרתי רשת המשחק Sony PlayStation, שבמהלכה נחשפו לפורץ פרטי כרטיסי אשראי של 77 מיליון משתמשים. החברה השביתה את הרשת רק יממה לאחר מכן, ורק שבוע לאחר גילוי הפריצה הזהירה את הלקוחות, כי ייתכן שפרטיהם נגנבו. חברים בוועדת המשנה לסחר וייצור של הקונגרס של ארצות־הברית דרשו מהחברה הסברים לאירוע ולהתנהלות החברה במהלכו. בכוונתם להגיש הצעת חוק לאבטחת נתונים, בין היתר כדי למנוע אירועים דומים. המקור: "ארצות הברית: מנהלי סוני נדרשים לספק הסברים לקונגרס על הפריצה לרשת ה־PlayStation", אתר אנשים ומחשבים, 1 במאי 2011.

54 "Cyberwar: War in the fifth domain", *The Economist*, July 1, 2010.

55 ניו־יורק טיימס: "ממצאי חקירת מפולת 1,000 הנקודות בדאו־ג'ונס: האשמה באלגוריתם ובפקודת מכירה אחת", TheMarker, 1 באוקטובר 2010.

56 **אנשים ומחשבים**, 2 באוגוסט 2010. ראו לעיל הערה 12.

57 מרטין ליביקי, כנס הרצלייה, פברואר 2011.

58 Lynn, February 15, 2011.

59 *The Economist*, July 1, 2010.

60 Aki Peritz, "Fears aside, al-Qaeda ill-equipped for a major cyberattack", http://articles.philly.com, March 20, 2011.

61 *The Economist*, July 1, 2010.

62 "UN calls for global cyber treaty", www.cpccci.com/blog, February 2, 2010.

63 Ellen Nakashima, "15 nations agree to start working together to reduce cyberwarfare threat", *Washington Post*, July 17, 2010.

64 John Markoff and Andrew E. Kramer, *New York Times*, 28 June 2009.

65 "Us vs. Russia cyberspace dispute", *The New New Internet Cyber Frontier* (www.thenewnewinternet.com), 29 June 2009.

66 *The National Strategy to secure Cyberspace*, The White Hose, February 2003.

67 "President on cybercrime: It has happened to me", *THE OVAL*, May 29, 2009; "President Obama: focus on cybercrime", *Ecommerce journal*, June 9, 2009.

68 *US National Security Strategy*, The White House, May 2010.

69 Lynn, February 15, 2011.

70 Home Land Security office Website; National Cyber Security Division, March 2011.

71 *The National Intelligence Strategy of the USA*, DNI Office, August 2009.

72 *The National Strategy to secure Cyberspace,* The White House, February 2003.

73 *International Strategy for Cyberspace,* The White House, May 2011.

74 Christopher Painter, Coordinator for Cyber Issues, "Release of the Obama Administration's International Strategy for Cyberspace", U.S. Department of State, http://fpc.state.gov. May 18, 2011.

75 Lynn, February 15, 2011.

76 Lynn, August 2010.

77 Allied Command Operations (ACO), "NATO's 'Cyber Coalition' exercise a collaboration in cyber defence," www.aco.nato.int, November 18, 2010.

78 Spacewar, "US: NATO networks vulnerable to cyber threat", www.spacewar.com, January 25, 2011.

79 "National Military Strategy for Cyberspace Operations (NMS-CO)," Chairman of the Joint Chiefs Of Staff, Washington, December 2006.

80 מערכת אתר אנשים ומחשבים, "הבית הלבן סיים הכנת דו"ח על אבטחת המידע בממשל האמריקני", 19 באפריל 2009.

81 יוסי הטוני, "ארצות־הברית: הפנטגון יקים מטה ללחימה בטרור ובפשיעה המקוונת", אתר אנשים ומחשבים, 24 ביוני 2009.

82 תיאור האסטרטגיה ההתקפית של סין במסמך Northrop Grumman תורם גם להבנת האסטרטגיה האמריקנית מאחר שהוא ניתוח אמריקני של היריב, שאליו בין היתר מכוונת האסטרטגיה.

83 אתר אנשים ומחשבים, לעיל הערה 12.

84 שם.

85 "האסטרטגיה הצרפתית להגנת מערכות מידע", אתר הסוכנות הלאומית של צרפת לביטחון מערכות מידע (ANSSI). המסמך אינו עושה שימוש במונח מרחב קיברנטי ("סייבר") אלא במונח מערכות מידע. המחברים מודים ליונתן קלר על איתור ותרגום המידע.

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

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

88 סונג־לי, יזם אינטרנט סיני בסרט הדוקומנטרי "אסיה דיגיטלית", 2008. על פי הסרט, כחצי מיליארד סינים כבר מחוברים לרשת, ובכל יום נמכרים בסין מיליון טלפונים סלולאריים. בבייג'ין נמצא מרכז המחקר הגדול ביותר של מיקרוסופט.

89 TheMarker, 21 בינואר 2010. לעיל הערה 33.

90 *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, Northrop Grumman Corporation, Information Systems Sector, October 9, 2009.

91 "Chasing The Night Dragon," Strategy Page (www.strategypage.com) March 8, 2011.

92 Sharon LaFraniere and David Barboza, "China Tightens Censorship of Electronic Communications," *The New York Times*, March 21, 2011.

93 לעיל הערה 11. עם ארגונים אלה נמנה גם GCHQ בבריטניה.

94 נועה פלג, "צומחים בגדול, קוצרים בקטן", **גלובס**, 9 בנובמבר 2011.

95 דוגמה: בריאיון למגזין **פורבס** אמר ג'ורג' גילדר, מומחה אמריקני נודע לטכנולוגיות המידע ולכלכלה: "הצלחת הקפיטליזם האמריקני הייתה ותמשיך להיות פונקציה של החדשנות הטכנולוגית, אנחנו במלחמת קיום מתמדת, כלכלית וביטחונית. ישראל היא הנכס האסטרטגי היחיד שלנו מחוץ לארצות־הברית. ישראל היא היחידה המובחרת שלנו. היא חלק אינטגרלי של כלכלת ארצות־הברית, שלוחה חיצונית שלנו ונכס אמיתי במזרח התיכון. שלמה גרינברג, "האם ישראל היא נכס אסטרטגי?", ביזפורטל, 17 בפברואר 2011.

96 אתר תהיל"ה: www.tehila.gov.il

97 אתר אבטחת המידע הממשלתי: www.cert.gov.il

98 אור הירשאוגה, "הממשלה אישרה הקמת יחידת מטה למנמ"ר הממשלתי", TheMarker.com 17 במרס 2011.

99 הקמת הרשות לאבטחת מידע היא תוצאה של החלטת ממשלה ב־1984 משנת 2002. אתר השב"כ: www.shabak.gov.il.

100 תת־אלוף ניצן נוריאל, ראש המטה ללוחמה בטרור (המשמש גם כראש ועדת ההיגוי להגנה על מערכות ממוחשבות במטה לביטחון לאומי) אמר, כי גופים שונים בישראל ובהם חברות פרטיות גדולות לא הסכימו לקבל הגנה ממשלתית, עד שהמטה ללוחמה בטרור פרץ למערכות שלהם כדי להראות את הנזק הפוטנציאלי. המקור: ברק רביד, "רה"מ, בנימין נתניהו, הקים צוות שמטרתו היערכות ישראל למתקפה על רשתות מחשבים", **הארץ**, 3 באפריל 2011.

101 ניתן להניח כי המשימות שהוטלו על ראש הלוט"ר במל"ל בעניין הגנת המרחב הקיברנטי יועברו לראש מטה הסייבר הלאומי.

102 ד"ר גבי סיבוני, "הגנת נכסים ותשתיות קריטיות מפני תקיפה קיברנטית – המימד הסטטוטורי", **צבא ואסטרטגיה**, המכון למחקרי ביטחון לאומי, כרך 3, גיליון 1, מאי 2011.

103 **חוזר גופים מוסדיים**, 6-9-2006, 16 באוקטובר 2006.

104 **ניהול בנקאי תקין** [4] (09/03): ניהול טכנולוגיות המידע.

105 אמיר אורן, "זירת הלחימה החדשה של צה"ל נמצאת ברשתות מחשבים", **הארץ**, 2 בינואר 2010.

106 אגף התקשוב בצה"ל הוקם במרס 2003 על בסיס איחוד חיל הקשר וחטיבת התקשוב (תקשורת ומחשבים) ובכך נוסד גוף מטכ"לי האמון על קביעת מדיניות התקשוב בצה"ל (אתר אגף התקשוב).

107 נחמה אלמוג, "אלוף עמוס ידלין, ראש אמ"ן: ישראל מובילה בתחום הלוחמה הקיברנטית", אתר אנשים ומחשבים, 17 בדצמבר 2009.

108 דובר משרד ראש הממשלה, "ראש הממשלה הכריז על הקמת מטה סייבר לאומי", אתר משרד ראש הממשלה, 18 במאי 2011. עוד נאמר בהודעה על הקמת מטה הסייבר, כי "ראש הממשלה הורה על הקצאת תקציב מיוחד (בסך מאות מיליוני שקלים – לפי **הארץ**, הערה 109 להלן) ליישום תוכנית החומש, אשר תציב את ישראל בחוד החנית העולמי של תחום הסייבר. התוכנית כוללת השקעה במחקר ופיתוח אקדמי, הקמת מרכז חישוב על (Super Computer) באחת האוניברסיטאות בישראל, הקמת מרכזי מצוינות אקדמיים, פעילות מאומצת להשבת חוקרים ואנשי אקדמיה לישראל, הגדלה משמעותית של מספר הסטודנטים לקיברנטיקה ושדרוג

תשתיות המחקר באוניברסיטאות. כמו כן, התוכנית כוללת גם עידוד של המגזר העסקי, עם דגש על תחום ההיי־טק, במטרה לפתח טכנולוגיות כחול־לבן שיעניקו לשראל יתרון משמעותי בתחום. הממשלה תסיר חסמי ייצוא של פיתוחים קיברנטיים ומערכת הביטחון תגדיל את מיקור החוץ של פיתוח טכנולוגיות קיברנטיות למגזר התעשייתי הפרטי על מנת לעודד מגזר זה".

109 יהונתן ליס, "ראש הממשלה בנימין נתניהו הכריז על הקמת מטה סייבר לאומי", **הארץ**, 18 במאי 2011.

110 Amy Kellogg, "Iran is Recruiting Hacker Warriors for its Cyber Army to Fight 'Enemies'", FoxNews.com, March 14, 2011.

111 העיתוי הנוכחי לעסוק בעניין מתאים גם לאור קביעת ועדת מרידור לתפיסת הביטחון של ישראל משנת 2006, כי "אחת לחמש שנים תיעשה בדיקה של הנחות היסוד בתפיסת הביטחון" (זאב שיף, **הארץ**, 24 באפריל 2006).

112 הלקח ההיסטורי מהקמת מטות במשרד ראש הממשלה בישראל, כמו המטה ללוחמה בטרור ומטה (בזמנו – המועצה) לביטחון לאומי, הוא שחולפות שנים רבות מרגע קבלת החלטה על ההקמה ועד להיות המטה אופרטיבי ובעל השפעה משמעותית, אם בכלל.

113 ראש המטה ללוחמה בטרור, תת־אלוף ניצן נוריאל, אמר בכנס הרצלייה: "אני מוכן להשקיע הרבה כסף כדי שהמחשב של כל האקר שמתקיף את מדינת ישראל יישרף". ברק רביד, לעיל הערה 100.

114 "תפיסת ביטחון" – מושג קומפקטי המכיל את המושגים: הרתעה, התרעה, הכרעה, וכן את המושג הגנה (על פי הצעת ועדת מרידור). התפיסה מגלמת את הקשר בין המושגים הללו בהקשר להפעלת צה"ל, ומגלמת בתוכה רכיבים אסטרטגיים חשובים ובהם עליונות אווירית ועליונות מודיעינית. עם זאת, תפיסת הביטחון אינה מכילה רכיבים אחרים של אסטרטגיית הביטחון של ישראל, כגון: הישענות על מעצמה דוגמת ארצות־הברית, והסדרי ביטחון (פירוז, דילול כוחות, שימוש בכוחות בינלאומיים) במסגרת הסדרים מדיניים. אסטרטגיית הביטחון של ישראל אמנם לא כתובה, אבל היא נגלית במעשיה של ישראל.

115 שי שבתאי, "תפיסת הביטחון של ישראל – עדכון מונחי יסוד", **עדכן אסטרטגי**, כרך 13, גיליון 2, אוגוסט 2010.

116 נחמה אלמוג, לעיל הערה 107.

117 אתר ויקיליקס הוקם בשנת 2007 כדי לפעול נגד משטרים מדכאים ברחבי העולם באמצעות חשיפת מידע. הוא הציג ידיעות שהודלפו למערכת שלו בעילום שם, ללא הגבלת סיווג ביטחוני, צנזורה, והגנת הפרטיות.

118 Brian Krebs, "The cyberwar will not be streamed", *Computerworld*, December 20, 2010.

119 יובל יועז, "אושר הסדר הטיעון עם ענת קם; לא הורשעה בפגיעה בביטחון המדינה", **גלובס**, 6 בפברואר 2011.

120 "נביל שעת': המסמכים שבידי אל־ג'זירה אמיתיים", קול ישראל, רשת ב, 25 בינואר 2011.

121 דודי גולדמן, "מחתרת המסכה", **ידיעות אחרונות**, 25 במרס 2011.

122 "ארגון אנונימוס שם את איראן על הכוונת", מדור "קפטן אינרטנט", **הארץ**, 1 במאי 2011.