מרחב הסייבר והביטחון הלאומי

מבחר מאמרים | קובץ שני

גבי סיבוני, עורך

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

מרחב הסייבר והביטחון הלאומי

מבחר מאמרים | קובץ שני

גבי סיבוני, עורך

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

המכון למחקרי ביטחון לאומי (חל"צ)
חיים לבנון 40
ת.ד. 39950
תל־אביב 6997556

info@inss.org.il
http://www.inss.org.il

ISBN: 978-965-7425-50-3
מארס 2014 © כל הזכויות שמורות

הביא לדפוס: משה גרונדמן
עיצוב גרפי: מיכל סמו־קובץ, המשרד לעיצוב גרפי, אוניברסיטת תל־אביב

המכון למחקרי ביטחון לאומי (חל"צ)

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 המכון הוא דרג מקבלי ההחלטות, מערכת הביטחון, מעצבי דעת הקהל בישראל, הקהילה האקדמית העוסקת בתחומי הביטחון בישראל ובעולם, והציבור המתעניין באשר הוא.

תוכן

5 | **הקדמה**

7 | **תוכנית להרתעת סייבר: בניית יציבות באמצעות כוח**
פרנק ג'. צ'ילופו, שרון ל. קרדאש וג'ורג' ס. סלמואירגי

27 | **'דילמת דוקו': הנחת העמימות והשאיפה חסרת התוחלת למלחמת סייבר סטרילית**
מת'יו קרוסטון

39 | **השימושים האסטרטגיים בעמימות במרחב הקיברנטי**
מרטין ס' ליביקי

47 | **מבט בינתחומי על אתגרי הביטחון בעידן המידע**
יצחק בן־ישראל, ליאור טבנסקי

61 | **לוחמה קיברנטית והרתעה: מגמות ואתגרים במחקר**
אמיר לופוביץ

73 | **להגנת וירוס הסטקסנט**
ג'יימס א. לואיס

85 | **התרת אפקט ה־'סטקסנט': על המשכיות ושינוי בשיח על איומי הסייבר**
מרים דאן קוולטי

93 | **איום ארגוני הטרור במרחב הסייבר**
גבי סיבוני, דניאל כהן, אביב רוטברט

115 | **תוכנית הסייבר במכון למחקרי ביטחון לאומי**
עיקרי הפעילות

הקדמה

ההתפתחות המהירה של מדינת ישראל כגורם מוביל בתחום הסייבר מהווה מנוף לקידום המחקר בתחום זה בישראל בכלל ובמכון למחקרי בטחון לאומי, בפרט. כדי להעצים את המחקר ואת היקף הפעילות, מקדם המכון שיתוף פעולה בינלאומי עם גורמים רלוונטיים בתחום. אחד ממרכיבי שיתוף הפעולה הזה, הינו הכנס הבינלאומי בנושא מבצעי הגנה ומודיעין בסייבר שמקיימת תכנית הסייבר של המכון בשיתוף Cyber Security Forum Initiative (CSFI) – ארגון סייבר גדול וחשוב בקהילת הסייבר האמריקנית. הכנס השנה (2014) מתקיים בשיתוף עם גורמים שונים בישראל ובהם: המשרד למודיעין, המטה הקיברנטי הלאומי, אגף התקשוב של צה"ל והמדען הראשי במשרד הכלכלה.

התמקדות הכנס במבצעי הגנה ומודיעין מאפשר למכון למקד ולבדל את העשייה בתחום זה וכך לייצר השלמה למגוון הפעילויות המתקיימות בישראל ובעולם. לכנס השנה מספר מטרות ובהן: א. העמקת שיתוף הפעולה בין גורמי ממשל וארגונים העוסקים בתחום הסייבר בישראל ובארצות הברית. ב. חשיפת שוק הסייבר הישראלי לחברות טכנולוגיות אמריקניות המבקשות לפתח עסקים בישראל או המבקשות לחשוף יכולות וטכנולוגיות ישראליות בחו"ל. ג. הרחבת שיתוף הפעולה הבינלאומי עם מדינות ידידותיות בתחום הסייבר בעולם.

כמדי שנה, סמוך לכנס אנו מציעים לקהל שוחרי הסייבר פרסום ייחודי, המרכז מאמרים שפורסמו במסגרת תכנית הסייבר של המכון. המאמרים בחוברת זו – פרי עטם של חוקרי המכון ומחוצה לו – פורסמו לראשונה בכתב העת **צבא ואסטרטגיה,** שמפרסם המכון למחקרי ביטחון לאומי.

גבי סיבוני
ראש תוכנית הסייבר
המכון למחקרי ביטחון לאומי

תוכנית להרתעת סייבר:
בניית יציבות באמצעות כוח

פרנק ג'. צ'ילופו, שרון ל. קרדאש וג'ורג' ס. סלמואירגי

במובנים רבים, אין ספק שהרתעה בעולם הסייבר היא נושא מורכב הרבה יותר מאשר ההרתעה במלחמה הקרה. טבעו של מרחב הסייבר הוא הגורם לכך. גם התיאוריות המתוחכמות ביותר של ההרתעה הגרעינית יתגלו כבלתי־מספקות בהתמודדות עם מורכבותו של תחום זה, שהוא מעשה ידי אדם, ואשר מקיף מספר אינסופי כמעט של יכולות, גורמים ומניעים המשתנים בהתמדה.[1]

איומי סייבר מציבים בעיה אמיתית וגוברת, ועד היום, מאמציה של ארצות־הברית לתת להם מענה הולם משתרכים מאחור. אמנם, היכולת להתגונן מפני התקפה או פלישה חייבת להישמר, אך ארצות־הברית, ככל מדינה אחרת, תפיק תועלת רבה אם תצליח מלכתחילה להרתיע את אויביה מפעולה – לפחות ככל שהדבר נוגע לפעולות מהסוג החמור ביותר, דוגמת לוחמת סייבר. ברור לחלוטין שלא ניתן להרתיע את כל סוגי ההתנהגות העוינת, אך חשוב לזהות סדרי עדיפויות בנושא זה, ולקבוע מהי הדרך הטובה ביותר להתמודד עם האיומים המובילים. חרף דיונים נמרצים, גיבוש פתרון מקיף ואחיד נותר חמקני. אחת הסיבות לכך הוא טיבה המורכב והמקיף של הרתעת סייבר, המחייב פתרון מקיף ומגובש הכולל בעלי עניין במגזר הציבורי והפרטי גם יחד.

על מנת לסייע בהבניית הדיון ובקידום המטרה, אנו מציעים מסגרת עבודה שבוחנת את הסוגיה בצורה ביקורתית, ומבקשת להניא, להרתיע ולהכניע גורמים עוינים מדינתיים ולא־מדינתיים גם יחד. הצבת האיומים הפוטנציאליים בתבנית רעיונית זו מסייעת להבהיר מהם מקורות הסכנה, ומשמשת נקודת פתיחה לזיהוי האחראים ולשיוכם לפעולות עוינות שמתבצעות נגד מדינה כלשהי או נגד בעלות־בריתה. הדבר יאפשר לשחקנים הרלוונטיים, שהפכו מטרה לגורמים עוינים, להמשיך

פרנק ג'. צ'ילופו הוא ראש המכון למדיניות להגנת המולדת (HSPI) ומנהל משותף של מרכז הסייבר לביטחון לאומי וכלכלי (CCNES) באוניברסיטת ג'ורג' וושינגטון. שרון ל. קרדאש היא מנהלת משותפת של ה־HSPI וחברה ב־CCNES, ג'ורג' ס. סלמואירגי הוא עורך דין ויועץ ל־HSPI בוושינגטון.

מאמר זה ראה אור לראשונה ב**צבא ואסטרטגיה**, כרך 4, גיליון 3, דצמבר 2012, עמ' 3-21.

בפעולות ובדיונים הנחוצים על מנת להתוות ולהוציא לפועל אמצעי תגובה יעילים וראויים. יתרון נוסף של תבנית זו הוא סיוע בזיהוי תחומים ששיתוף פעולה בין הישויות המושפעות/המהוות יעד לפגיעה עשוי להועיל להם, או אפילו נדרש עבורם. לסיכום, מסגרת עבודה זו מספקת נקודת פתיחה לחקר הדרכים להרתעת גורמים עוינים, ובאופן זה מציעה נקודת מבט רעיונית בעלת ערך לארצות־הברית ולבעלות־בריתה גם יחד. פירוט מגוון הגורמים ופעילותם הפוטנציאלית שיובאו להלן אינו מתיימר להיות ממצה. נכון יותר יהיה לראות בו תמונת מצב או מעין טיוטה, שנועדה לתת מושג כללי במונחים של מי, מה, כיצד, מדוע וכדומה, וזאת כהקדמה לדיון מעמיק יותר על האסטרטגיה והמדיניות בתחום הרתעת סייבר.

גורמים מדינתיים

צבאות זרים עשויים להיות מעורבים ב"מתקפה על רשתות מחשב" או ב"ניצול רשתות מחשב" (CNA/CNE) כדי להגביל, לפגוע או להרוס יכולות של מדינה אחרת על מנת לקדם סדר־יום פוליטי. צבאות זרים משלבים יותר ויותר יכולות CNA/CNE במאמץ המלחמתי, בתכנון הצבאי ובדוקטרינה שלהם.[2] למאמצים כאלה יש יישומים קונבנציונליים בשדה הקרב (כלומר, שיפור במערכות נשק ופלטפורמות ו/או שיבוש מערכות אלה אצל אחרים) לצד יישומים בלתי־קונבנציונליים, ככל שמרחב הסייבר מותח את שדה הקרב וכולל בתוכו רכיבים חברתיים ואזרחיים. הפעילות במרחב הסייבר עשויה לכלול הכנות מודיעיניות של שדה הקרב, במטרה למפות תשתיות חיוניות של מי שנתפס כאויב.[3]

שירותי ביון ושירותי ביטחון: ניצול לרעה (Exploit) עשוי לכלול ריגול תעשייתי, כלכלי, צבאי ופוליטי, גניבת מידע ממשלה אחרת או על אודותיה, וכן גניבת קניין רוחני, טכנולוגיה, סודות מסחריים ועוד, שנמצאים בידי תאגידים פרטיים או אוניברסיטאות. שירותי ביון של מדינות רבות מעורבים בריגול תעשייתי בתמיכת חברות פרטיות.[4] מטרת־העל של פעילויות המתבצעות במסגרת זו היא השאיפה להשפיע על החלטות ועל מאזן הכוחות (האזורי והבינלאומי). כאן בולט שילוב של מודיעין טכני ואנושי, וכן איום מצד גורמים מבית ("insider").[5]

היבטים משולבים: ניתן לשלב רכיבים שונים ביכולתה של מדינה על מנת להשיג שלם הגדול מסכום חלקיו. בריתות (בין מדינות) יכולות להתגבש למטרה דומה. פעילות משותפת בהקשר זה עשויה לכלול איסוף מידע, שיתוף ממצאים שהשיג אחד הצדדים וביצוע משותף של מבצעים בשטח (מתקפות). מדינות יכולות גם לחפש ולגייס עזרה של גורמים לא־מדינתיים, כגון פצחנים (האקרים) להשכרה, שאינם חשים מחויבים או מוגבלים לנאמנות כלשהי.

גורמים לא־מדינתיים

ארגוני טרור לא־מדינתיים עלולים לבצע פעולות CNA/CNE כדי לקדם סדר־יום פוליטי מסוים. הם מייחסים חשיבות מרובה לאינטרנט (לצורכי גיוס, הדרכה, גיוס כספים, תכנון מבצעים וכדומה).[6] הצלחת מאמציהן של ארצות־הברית ובעלות־בריתה במלחמה בטרור בעולם הממשי עלולה להוביל ארגונים כמו אל־קאעדה ודומיו לחדור לעולם הסייבר באופן מעמיק יותר. אל־קאעדה אף עשוי לנסות להפיק לקחים מתוך פעילותם של ארגון "אנונימוס" ו"האקטיביסטים" (האקרים־אקטיביסטים) אחרים (או אפילו לחקות אותם), שעושים שימוש במרחב הסייבר על מנת למשוך תשומת לב למטרה שבה הם תומכים.

ארגוני פשע לא־מדינתיים מבצעים גניבת קניין רוחני, גניבת זהות וכן הונאות שונות, ומוּנָעים לרוב מתאוות בצע. הטכניקות והכלים הייחודיים לסייבר יכולים להניב תגמולים כספיים נכבדים. שוק עבריינות הסייבר העולמי הוערך ביותר מ־12.5 מיליארד דולר ב־2011,[7] אף על פי שהאומדנים משתנים (תוקף מתודולוגיות החישוב והאמינות של חלק מהמקורות נתון לוויכוח, וקשה להשיג הוכחה אמפירית).

היבטים משולבים: ניתן לצפות לבריתות מטעמי נוחות בין גורמים לא־מדינתיים (ארגוני טרור וארגוני פשע, ואפילו בין יחידים), במטרה לגשר על פערי יכולת כדי להשיג השפעה גדולה יותר. הסדרים דומים של נוחות הדדית אפשריים גם בין מדינה לבין ישויות שאינן מדינה (טרוריסטים, פושעים, האקרים יחידים). גורמים לא־מדינתיים יכולים להרחיב את היכולות והמיומנויות של המדינה, או לפעול כשלוחה שלה למטרות שונות. הסדרים כאלה הופכים את אתגר ייחוס האחריות (מי אחראי) למורכב עוד יותר, ומאפשרים למדינה ליהנות מיכולת הכחשה אמינה (plausible deniability).

השוואה בין הרתעת הסייבר להרתעה בתחום הגרעין[8] מעלה נקודות דמיון ושוני גם יחד.[9] מרחב הסייבר תובע במיוחד התמקדות בשחקנים ולא רק ביכולות/בנשק. לכן חיוני לסווג שחקנים אלה בהתאם להיקף, לעוצמה ולאופי האיום שהם נושאים. רק לאחר בחינה מדוקדקת שלהם נוכל לזהות את החשובים ביותר, ולהתמקד בהם באופן שמתעמת ומנטרל את הכוונות והיכולות הספציפיות שלהם.

הגנה והתקפה הן שני מרכיבים מכריעים בעמדה ובאסטרטגיה הרב־שכבתית האיתנה של ארצות־הברית, שנועדה להבטיח ביטחון לאומי. הרתעה יכולה לספק שכבת הגנה נוספת, באמצעות מניעת מהלכי פתיחה מצד בעלי אינטרסים עוינים כלפי ארצות־הברית. לכן, כדי לשמר ואף לקדם את הביטחון הלאומי/ביטחון המולדת, חשוב לשקול היטב, לפתח ולשמר לאורך זמן בתוך מערכת (טכנולוגית והגנתית/ביטחונית) מהירת צמיחה את היכולות האמריקאיות הנחוצות לתמיכה במדינה באופן אמין ויעיל, שיקנו לה מוכנות ויכולת להניא, להרתיע ולהכניע את

יריבה. אולם למרות מאמצים מרוכזים המכוונים למטרות אלה ולמערכות הגנה, אין לראות בגישה זו תחליף לבנייה ולאחזקת אמצעי שיקום משמעותיים נוספים, שמטרתם לאפשר התאוששות מהירה. אכן, יכולת התאוששות ושיקום כשלעצמה עשויה להיות הרתעה רבת־עוצמה. ברוח חוכמתו של סון צו (Sun Tzu), עצם היכולת להשתקם לאחר מכה, לצד מוכנות ברורה להגיב למתקפת סייבר, יפעלו לחיזוק מאמצי ההרתעה האמריקאית, ולכן ימנעו קרבות ושפיכות־דמים: "זכייה במאה ניצחונות במאה קרבות אינה שיא המיומנות. הכנעת האויב ללא קרב היא המיומנות בשיאה".[10]

קווי מתאר לאיום הסייבר

ארצות־הברית והאינטרסים שלה מצויים תחת איום סייבר יומיומי מגורמים מדינתיים ולא־מדינתיים גם יחד. המטרות האמריקאיות הפוטנציאליות רבות ומגוונות, ומתרחבות למגזרים חיוניים כמו מים, אנרגיה, כספים וטלקומוניקציה.[11] על פי דיווחי העיתונות המצטטים דובר של המִנהל הלאומי לביטחון גרעיני בארצות־הברית (NNSA) – "הארגון לביטחון גרעיני [של ארצות־הברית] חווה עד עשרה מיליון 'אירועי...ביטחון משמעותיים' בכל יום".[12] על פי חישובים של המשרד לביטחון המולדת של ארצות־הברית, מתגלות עשרות אלפי חדירות סייבר (ניסיונות ובפועל) בכל שנה, ועשרות מתקפות על מערכות תשתית חיוניות – כאשר מאז 2010 ועד 2012 חלה בהן עלייה בסדרי גודל.[13] טווח נושאי תפקידים בכירים בעבר ובהווה שהתריעו על כך הוא מרשים, וכולל את עוזר הנשיא לענייני ביטחון המולדת ומלחמה בטרור, ג'ון א. ברנן (John O. Brennan);[14] מנהל הסוכנות לביטחון לאומי וראש מטה הסייבר האמריקאי, גנרל קית' אלכסנדר (Keith Alexander); השר לשעבר לביטחון המולדת, מייקל צ'רטוף (Michael Chertoff); המתאם הלאומי לשעבר לענייני ביטחון ומלחמה בטרור ויועץ מיוחד לנשיא בנושא אבטחת סייבר, ריצ'רד קלארק (Richard Clarke); יו"ר ועדת הסנאט לביטחון המולדת, הסנטור ג'וזף ליברמן (Joseph Lieberman);[15] הנציג הבכיר בוועדת הסנאט לשירותים מזוינים, הסנטור ג'ון מקיין (John McCain), וראש ה־FBI רוברט מולר (Robert Mueller), שלאחרונה אף צפה שאיום הסייבר יחליף בעתיד את הטרור כאיום הראשי על המדינה.[16]

אחד הפרשנים תיאר זאת בבהירות רבה, כשאמר "מרגלים זרים ופשע מאורגן נמצאים כמעט בתוך כל רשת של חברה אמריקאית. בקרב היועצים הבכירים ביותר של הממשל בנושא אבטחת סייבר שוררת הסכמה רחבה, כי עברייני סייבר או טרוריסטים הפועלים בתחום הסייבר מסוגלים להשבית את התשתית החיונית במדינה בתחום הפיננסי ובתחום האנרגיה והתקשורת".[17] יחד עם זאת, נוסף לספיגת הפסדים כספיים שמוערכים על ידי הרשות הלאומית לריגול נגדי ופקידים

אמריקאיים נוספים במיליארדים, כתוצאה מניצול רשתות מחשב לגניבת קניין רוחני רב־ערך דרך פרצת אבטחה,[18] המדינה ניצבת נוכח מכה מאיימת יותר, עקב היותה מטרה למאמצי היריב לעסוק במה שמהווה המקבילה הסייברית להשגת מודיעין של שדה הקרב, דוגמת ניסיון מצד סין למפות תשתיות אמריקאיות חיוניות לאספקת מים ואנרגיה – שאותו הם עלולים למנף בהמשך כדי להניא, להתריע ולהכניע פעולה מצד ארצות־הברית.[19]

תעשיות חיוניות במדינות אחרות כבר חוו מתקפות סייבר. החברה הסעודית 'ארמקו' (Aramco) (חברה בבעלות המדינה ו"מפיקת הנפט הגדולה בעולם") סבלה מווירוס ממקור חיצוני שהדביק כ־30,000 מהמחשבים שלה באוגוסט 2012.[20] זמן קצר לאחר מכן, חברת RasGas מקטר ("המפיקה השנייה בגודלה בעולם של גז טבעי נוזלי") נפגעה אף היא.[21] דיווחי העיתונות מציינים כי "החברה הצרפתית Areva לתחנות כוח גרעיניות הייתה היעד למתקפת הסייבר בספטמבר [2011]".[22] והמגמה נמשכת.

מדינות מחזיקות ביכולות משתנות ברמה ובתחכום, ועשרות מהן מרחיבות את יכולת הסייבר שלהן, לרבות ארצות־הברית ובעלות־בריתה (ישראל היא שחקנית ראשית במרחב זה). אל מול ארצות־הברית, סין היא מקור מרכזי של "איום מתמיד ומתקדם", למרות שטביעות אצבע של המדינה הנותנת חסות אינן ניכרות תמיד על העכבר או על מסך המחשב. ייחוס האחריות קשה אף יותר כאשר נוצר שיהוי משמעותי בין האירוע לבין הדיווח או הבקשה לסיוע מצד הקורבן.[23] אולם עדות לכוונותיה של סין קיימת מזה כעשור: בשנת 1999 פרסמו שני קולונלים בצבא הסיני ספר תחת הכותרת "*Unrestricted Warfar*" ("לוחמה בלתי־מרוסנת"), שהדגיש אמצעים חלופיים להבסת יריב, שאינם פעולה צבאית ישירה ובעלת אופי מסורתי.[24]

גם רוסיה היא יריבה נחושה ומתוחכמת במרחב הסייבר. בעימות של 2008 בין רוסיה לגיאורגיה, תקפה רוסיה את רשת התקשורת הגיאורגית והרסה אותה. כפי שציין השגריר, דיויד סמית': "רוסיה שילבה פעולות סייבר בדוקטרינה הצבאית שלה", אם כי "בלא הצלחה מלאה... המתקפה המשולבת של רוסיה על גיאורגיה ב־2008 – מתקפה צבאית ומתקפת סייבר – הייתה המבחן המעשי הראשון של דוקטרינה זו... [ו]עלינו להניח שהצבא הרוסי למד מהלקחים שהופקו".[25] ב־2007, בנקים וממשל באסטוניה וכן גופים נוספים היו גם הם יעד ל"התקפות מניעת שירות (DDOS) נרחבות, מפוזרות וממושכות... רבות מהן – מקורן ברוסיה".[26] ממקום מושבם ברוסיה הצליחו האקרים ועבריינים להטביע את חותמם. מרחב הסייבר התגלה כמכרה זהב לעבריינים, שחדרו לעומקו ככל שההזדמנויות להרוויח בו המשיכו להכפיל את עצמן. ערך שוק עבריינות הסייבר העולמי הוערך ב־2011 בלמעלה מ־12.5 מיליארד דולר, כאשר הנתח של רוסיה בעוגה הוא כ־2.3 מיליארד

דולר (קרוב לכפול מערכו המוחלט בהשוואה לשנה הקודמת). כמו כן, ישנם סימנים לכך שגורמי פשע מאורגן במדינה החלו להצטרף "באמצעות שיתוף נתונים וכלים" כדי להגדיל את רווחיהם.[27]

הפוטנציאל לשיתוף פעולה בין ובקרב גורמים בעלי מניעים שונים לחלוטין מעורר חשש רציני. לדוגמה, מדינות שאין להן יכולות משלהן אך מבקשות להזיק לארצות־הברית או לבעלות־בריתה עשויות להצטרף, או פשוט לקנות/לשכור את השירותים והמיומנויות של עבריינים והאקרים, שיסייעו להן לתכנן ולבצע מתקפות סייבר. קל לאתר ערכות קוד בסגנון 'עשה זאת בעצמך' לניצול נקודות תורפה ידועות, ואפילו תולעת Conficker (שגרסאות שלה עדיין אורבות ומסוגלות ליצור בוטנט [botnet] מכ־1.7 מיליון מחשבים) נשכרה לשימוש.[28] לפיכך, היעדר גישה לתשתית או היעדר גיבוי ממעצמה אינם מכשול. גורמים שלוחים (פרוקסי) בעלי יכולות סייבר זמינים גם הם. קיים יריד חימוש לנשק סייבר. יריבים אינם זקוקים ליכולות, אלא רק לכוונה ולמזומנים.[29] זוהי תחזית מצמררת, אם זוכרים שארגון אל־קאעדה קרא למוג'אהידין ברשת לתקוף את ממשלת ארצות־הברית ותשתיות אמריקאיות חיוניות. סגן־אדמירל סמואל קוקס ממטה הסייבר ציין שפעילי ארגון אל־קאעדה מחפשים באופן פעיל אחר אמצעים לתקיפת רשתות אמריקאיות – יכולת שבאפשרותם לרכוש מהאקרים עבריינים.[30] כמו כן, בלי קשר לאופן השגתן, ליכולות סייבר יש פוטנציאל לשמש כמכפיל כוח במתקפה קונבנציונלית.

מוקדי דאגה אחרים הבולטים בהקשר זה כוללים את צפון־קוריאה ואיראן. את חוסר היכולת הקיימת, לפי שעה, משלימות שתי מדינות אלה בריבוי כוונות. איראן משקיעה משאבים נכבדים בהרחבה ובהעמקה של יכולות לוחמת הסייבר שלה.[31] היא גם מסתמכת זה מכבר על שלוחים כגון חזבאללה, שמתרבר עתה בארגון עמית בשם "סייבר חזבאללה" המיועד לפגוע במי שנתפס כאויב. גורמי אכיפת חוק מציינים כי היעדים והמטרות של "סייבר חזבאללה" כוללים הדרכה וגיוס אקטיביסטים בסייבר שהם תומכי משטר (כלומר, תומכי הממשל באיראן). אלה מצְדם מלמדים אחרים את הטקטיקות של לוחמת הסייבר. חזבאללה ממהר לנצל לרעה כלי מדיה חברתית דוגמת פייסבוק, כדי להשיג מודיעין ומידע, דבר שמייצר הזדמנויות נוספות לאיסוף עוד נתונים, במקביל לזיהוי יעדים פוטנציאליים חדשים ולפיתוח שיטות מותאמות ואמצעי גישה.[32]

נוסף לאלה, גורמים מתוך 'משמרות המהפכה' האיראניים עשו ניסיונות גלויים למשוך אליהם האקרים.[33] יש עדות לכך שבמוקד מאמצי הסייבר של 'משמרות המהפכה' פועלת קבוצת ההאקרים הפוליטית/עבריינית האיראנית "אשיאן" (Ashiyane).[34] משטרת הבאסיג', שמקבלת תשלום על ביצוע פעולות סייבר בשם המשטר, מספקת את מרבית כוח האדם לפעולת הסייבר של איראן.[35] במקרה של עימות במפרץ הפרסי, תוכל איראן לשלב שיטות ממוחשבות ואלקטרוניות

למתקפת רשת כדי לפגוע במערכות מכ"ם של ארצות־הברית ובעלות־בריתה, ולהקשות עליהן לבצע פעולות הגנה והתקפה גם יחד.[36] כחלק ממשימתו של ארגון חזבאללה עצמו להשיג הרתעה, הצהיר בגלוי מנהיגו, חסן נסראללה, שלא תהיה כל הבחנה בין ישראל לבין ארצות־הברית מבחינת פעולות נקם, אם תתקוף ישראל את איראן כדי לעכב את התקדמותה לעבר יכולת גרעינית: "אם ישראל תתקיף את איראן, אמריקה תישא באחריות".[37]

לסיכום, מדינות מנצלות לרעה את מרחב הסייבר כדי להשיג יתרון ולקדם את האינטרסים שלהן באמצעות איסוף מידע והשגת כושר פגיעה ביכולותיו של מי שנתפס כאויב. גם גורמים לא־מדינתיים, ארגוני טרור ועבריינים ממנפים את מרחב הסייבר למטרותיהם, ומפיקים תועלת מתחום שבו כולם ניצבים באותה נקודת זינוק, המתיר גם לשחקנים יחידים קטנים יותר להשפיע באופן שאינו יחסי לגודלם. אסימטריה זו מייצרת סביבה זרועת סכנות שונות, שבעבר לא משכו את תשומת הלב והאנרגיות של המעצמות. לפיכך, המעצמות חוששות מתרחישים מסוימים דוגמת אלה שצוינו לעיל, בשל יכולתם לערער באופן משמעותי ואף לחסל לחלוטין את האמון והביטחון במערכת (אמריקאית או אחרת).

איום זה אינו ייחודי לארצות־הברית. לוחמה אסימטרית היא כמובן אחת מהתכונות המאפיינות את ניסיונה של ישראל בשדה הקרב הממשי והווירטואלי גם יחד.[38] יש להביא בחשבון גם נפגעים ידועים פחות (לכאורה) של המאבק הסייברי. בהמשך לכך, הנה תיאור של הרשות הלאומית לריגול נגדי (Office of the National Counterintelligence Executive) – הגוף האמריקאי שמרכז את המלחמה בטרור – בדוח לשנת 2011 שהגיש לקונגרס:

> המשרד הפדרלי הגרמני להגנה על החוקה (BfV – Federal Office for the Protection of the Constitution) מעריך שחברות גרמניות הפסידו בין 28 ל־71 מיליארד דולר ובין 30 ל־70 אלף מקומות עבודה בכל שנה בעקבות ריגול כלכלי של גורמים זרים. כמעט 70 אחוזים מכל המקרים מערבים גורמי פנים (insiders).
>
> דרום־קוריאה מדווחת שהעלויות כתוצאה מריגול כלכלי של גורמים זרים ב־2008 עמדו על 82 מיליארד דולר, לאחר שכבר הגיעו ל־26 מיליארד דולר ב־2004. הדרום־קוריאנים מדווחים ש־60 אחוזים מהקורבנות הם עסקים קטנים ובינוניים, וכי מקורו של מחצית מהריגול הכלכלי הוא בסין.
>
> משרד הכלכלה, המסחר והתעשייה היפני ערך סקר בקרב 625 חברות יצרניות בשלהי 2007, ומצא כי יותר מ־35 אחוזים מהחברות המשתתפות דיווחו על אופן כלשהו של הפסד טכנולוגי. יותר מ־60 אחוזים מדליפות אלה היו קשורות לסין.[39]

הדברים שאמר הסנטור הצרפתי, ז'אן־מארי בוקל (Jean-Marie Bockel) – שתועדו ב'דוח מידע' של ועדת הסנאט הצרפתית לענייני חוץ, הגנה והכוחות המזוינים – מטרידים במידה דומה:

> בצרפת, רשויות מנהליות, חברות ומפעילי שירותים חיוניים (אנרגיה, תחבורה, בריאות וכד') נופלים קורבן מדי יום למיליוני מתקפות סייבר... המקור למתקפות סייבר אלה יכול להיות האקרים של מחשבים, קבוצות אקטיביסטיות, ארגוני פשע וכן חברות מתחרות, או אפילו מדינות אחרות. האצבע המאשימה מופנית לרוב כלפי סין או רוסיה, אם כי קשה מאוד לזהות במדויק את היוצרים שמאחורי כל מתקפה.[40]

וכך גם ההערכה שמספק ג'ונתן אוונס (Jonathan Evans), העומד בראש שירותי הביטחון בבריטניה:

> אסטרטגיית הביטחון הלאומי של בריטניה ממקמת בצורה ברורה את אבטחת הסייבר לצד הטרור, כאחד מארבעת אתגרי המפתח שניצבים בפני בריטניה. נקודות תורפה באינטרנט מנוצלות לרעה בצורה אגרסיבית לא רק על ידי עבריינים אלא גם על ידי מדינות, וההיקף הוא מדהים: מדובר בתהליכים בקנה־מידה תעשייתי המערבים אלפי אנשים, שעומדים מאחורי ריגול סייבר במימון מדינות ופשע סייבר מאורגן... חברה שעמה עבדנו, מהגדולות בלונדון, מעריכה שסבלה הפסדי הכנסות בסך 800 מיליון ליש"ט כתוצאה ממתקפת סייבר מצד מדינה, ולא רק כתוצאה מאובדן קניין רוחני, אלא גם בשל פגיעה ביתרון המסחרי שלה בעת ניהול משא־ומתן על כריתת הסכמים. אלה לא יישארו הקורבן התאגידי היחידי שסובל מבעיה זו. [41]

אוונס הוסיף ואמר את הדברים הבאים:

> עד כה, ארגוני טרור קיימים לא הציבו איום משמעותי בערוץ זה, אולם הם מודעים לפוטנציאל הקיים בניצול נקודות תורפה בסייבר כדי לתקוף תשתית חיונית, ואני צופה שהם ירכשו יכולות נוספות כדי לעשות זאת בעתיד.[42]

השאלה הנדרשת היא, לפיכך, מה צריך לעשות.

הרתעת סייבר ותגובה רב־ממדית

על רקע העדויות הרבות והמטרידות על יכולות הסייבר ועל כוונות עוינות מצד גורמים מדינתיים ולא־מדינתיים כאחד, חייבת ארצות־הברית להתוות ולגבש בקפידה מסלול התקדמות להתמודדות עוצמתית עם העובדות ועם המציאות המדאיגה המאפיינות את מרחב הסייבר כיום (ואשר לא סביר שייעלמו בקרוב). תהא זו נחמת שווא לחשוב שארצות־הברית או בעלות־בריתה יוכלו לפתור את הבעיה בעזרת 'חומות אש' (firewalls) בלבד. במקום זאת, על ארצות־הברית לנסח, להבהיר וליישם אסטרטגיה להרתעת סייבר, שתסייע בתמיכה ובחיזוק אבטחת הסייבר וההגנה על תשתיות חיוניות.

בתחומים מסוימים כבר מתקיים דיון נמרץ אך ראשוני בנושא זה, אולם בשל טבעו המורכב, חוצה המגזרים והרב־תחומי של האתגר, לא גובשה עד כה תגובה אסטרטגית משולבת. האיומים מתפתחים מדי יום ומוסיפים עוד נדבך של מורכבות, ולמרות הקצב והעוצמה של זרם האיומים, המגזרים השונים אינם משתפים ביניהם

בדרך כלל את המידע על האמצעים והכלים המשמשים את גורמי האיום, ואינם מפרסמים אותו. בעיקרון, שתיקה זו אינה חסרת הגיון, שכן הממשלה מבקשת להגן על חומר מסווג והתעשייה מעוניינת להגן על מידע קנייני. אולם בפועל, שתיקה כזו "תוקעת מקלות בגלגלים" שאמורים להניע תגובה ומאמצי מניעה.

על רקע דברים אלה, אין ספק שהיקף המשימה מעורר אימה, אולם ארצות־הברית צפויה להפיק תועלת מרובה מפיתוח ומיישום אסטרטגיה להרתעת סייבר, וממדיניות השואפת להניא, להרתיע ולהכניע – הן כגישה כללית והן באופן שמותאם במיוחד לגורם/יריב מסוים. עמדה כללית יציבה, כלומר, צעדי אבטחה בסיסיים (הגנה, היגיינה, טכנולוגיה), יכולה להוות 80 אחוזים מהפתרון ולנטרל את מרבית האיומים לפני שהם מתממשים במלואם. בכך ניתן יהיה לשחרר משאבים (אנושיים, כספיים וטכנולוגיים), שיוכלו להתמקד באופן תלוי־הקשר בשאר התחומים שמרכיבים את הבעיות והאיומים הקשים ביותר מבחינת רמת התחכום והנחישות. כדי להפוך המלצות אלה למעשיות, יש להתוות קווים ברורים. ראוי לשמור על הגמישות של תגובת ארצות־הברית באמצעות שמירה על מידת עמימות מסוימת באשר לאמצעים שברשותה, כל עוד הפרמטרים מובהרים היטב באמצעות הצבת סימני דרך ייעודיים או קווים אדומים נבחרים, שחצייתם לא תעבור בשתיקה.[43]

על מנת לייצר הרתעה אפקטיבית מול יחיד או ישות, ובכך למנוע מהם מלהשיג את מטרתם – ומוטב למנוע מהם לפעול מלכתחילה – הכרחי להבין באופן מוחלט מה בדיוק מנסה הצד היוזם להשיג. (הרעיון מבוסס על הנושא/העיקרון של האסטרטג הנודע, מיאמוטו מוסאשי (Miyamoto Musashi): "דע את אויבך, דע את חרבו"[44]). הבנה בסיסית זו מהווה את הצעד הראשון בדרך להניא את היריב מפעולה או להכניעו, ויישומה כרוך בבחינה יסודית של המצב מנקודת מבטו של הצד האחר. אמנם, כל מקורות האיום שצוינו לעיל עוסקים בריגול ובניצול של מידע ומערכות דרך אמצעי סייבר, אולם יש לזכור שלגורמים שונים יש יעדים שונים ומובחנים. למרות שהם עושים שימוש באמצעים וירטואליים ובמדיום וירטואלי, כל אחד מגורמים אלה שואף להשיג תוצאות מסוימות בעולם האמיתי, ובהתאם לכך יכוון את מעשיו.

מה חייבת ארצות־הברית לעשות כדי לשכנע גורמים מדינתיים להימנע מהפעלת שירותי המודיעין והצבא שלהם לצורך ניצול רשתות מחשב או לשם מתקפה על רשתות מחשב, בשם מטרות־על כלשהן? תגובת הסייבר של ארצות־הברית צריכה להיות תוצאה של אסטרטגיית הרתעה רחבה יותר ביחס לגורם נתון. במילים אחרות, הרתעת הסייבר תהיה תואמת ומשלימה לאסטרטגיית הרתעה אמריקאית מקיפה יותר. מדינות אחרות צריכות להבין ולהעריך את העובדה שארצות־הברית מסוגלת להטיל עונש מידתי אם תותקף במרחב הסייבר, וכי

התגובה האמריקאית עשויה בסופו של דבר להיות 'סייברית' או צבאית, כאשר כל האפשרויות מונחות על השולחן. לגבי תגובת סייבר, יש להפגין את יכולת ההתקפה באופן שלא יותיר ספק באשר להשלכות שיהיו לחציית קו אדום של ארצות־הברית. עם זאת, הפגנת היכולת חייבת להתבצע תוך הכרה מלאה בעובדה שניתן יהיה ללמוד ולשנות כל כלי, טכניקה, טקטיקה או הליך שייושמו, ולהשתמש בהם כדי לנקום בארצות־הברית ובבעלות־בריתה. התגובה בהקשר זה תלויה ביכולת לייחס את המתקפה לגורם ספציפי אחד או יותר (כוחות זרים).

מבחינת המודיעין, יש לזכור שמאז ומתמיד עסקו מדינות בגניבת סודות. אמנם הריגול הפך דיגיטלי, אך ממשלות זרות משתמשות באמצעי סייבר למטרה המקורית: להשיג מידע שיכול לשמש לעיצוב ולחידוד קבלת החלטות, ולשם כך הן מנסות להתאים את 'המקצוע העתיק בעולם' השני למאה ה־21. במילים אחרות, מדינות משתמשות באמצעי סייבר (דוגמת האקרים רוסיים וסיניים העובדים בשירות ממשלותיהם) כדי להגביר את יכולתן לאסוף מידע בעל ערך עבור קובעי המדיניות שלהן. השאלה היא, איזה מידע מעוניינים גורמים אלה להשיג, ומדוע? המידה שבה הממשלה שעל הכוונת (ארצות־הברית או בעלת־בריתה) תהיה מסוגלת להגן טוב יותר על המערכות שלה ולהתאים להן פעולות הרתעה תלויה ביכולתם של המומחים להרתעת סייבר להציג תובנות, ולנסח תשובות ברורות לשאלה זו.

ריגול תעשייתי הוא תת־קבוצה בסוג זה של פעילות המתקיימת בחסות מדינה. הכוונה היא להגביר את השגשוג הכלכלי או את יישומם של שיקולים עסקיים במדינה מסוימת. למרות שפעולת הריגול מוכוונת על ידי המדינה, הנהנים ממנה עשויים להיות גורמים פרטיים או פרטיים־למחצה. מצד אחר, מנקודת מבטו של יעד הריגול, ההשלכות של גניבת סודות מסחריים עלולות להיות מעמיקות ולהתרחב מעבר לאובדן הכלכלי, עד כדי פגיעה במעמדה של המדינה בעולם. על פי הערכתו של רוברט בראיינט (Robert "Bear" Bryant) מהרשות הלאומית האמריקאית לריגול נגדי, ריגול סייבר הוא "איום שקט על הכלכלה שלנו עם תוצאות ניכרות ביותר... סודות מסחריים שפותחו במשך אלפי שעות עבודה על ידי המוחות המבריקים ביותר שלנו נגנבים בשבריר שנייה, ומועברים למתחרים שלנו".[45] החדשנות והפריון של ארצות־הברית עלולים גם הם לסבול כתוצאה מכך, עם השלכות פוטנציאליות משניות נוספות על צמיחה ופיתוח עתידיים. אם מידע צבאי נחשף ונגנב, עלולות להיות לכך גם השלכות על הביטחון הלאומי. אין צורך בדמיון רב כדי לשער מה יכול לעשות גורם עוין עם טכנולוגיה אמריקאית גנובה בעלת פוטנציאל ליישום צבאי.[46]

בדומה למדינות, גם ארגוני טרור על־לאומיים מבקשים להשיג יתרון אסימטרי שאותו יוכלו למנף, בניסיון להנחיל את סדר־היום הפוליטי שלהם. עם זאת, בדרך

כלל מחזיקים ארגונים כאלה משאבים פחותים מאלה של מדינה, ומשתדלים להימנע ממעורבות בתהליך הפוליטי ולהעדיף שימוש באלימות להשגת מטרותיהם. מנקודת מבט זו, לא יהיה זה מאמץ גדול מדי עבורם להשיג תמורה נוספת להשקעתם, באמצעות שימוש באמצעים דיגיטליים כמכפיל כוח של פעולה צבאית. ככל שניתן יהיה ללמוד פרטים נוספים על הסייבר הטקטי ועל המטרות והשאיפות הפוליטיות והאסטרטגיות של ארגונים אלה, כך יתקבל חומר גלם מועיל יותר לעיצוב הרתעת סייבר שתמנע מהם לפעול.

ארגוני הטרור והפשע עשויים גם להתאחד וליצור איום משולב המתבסס על ברית מטעמי נוחות, שבה כל צד נשען על המיומנויות והנכסים של הצד השני כדי לקדם את מטרותיו בהתאם. בניגוד לארגוני הפשע שמקור הכנסתם העיקרי הוא הפשע בלבד, רווח כשלעצמו אינו המניע של ארגוני טרור. הבדל מהותי זה מהווה למעשה פתח שניתן לנצלו באמצעות תצוגה וביצוע מקצועיים של אסטרטגיית הרתעת סייבר מותאמת.

יש לזכור שהרתעה היא תת־קבוצה של הכנעה, שמטרתה לגרום לירי להימנע מפעולה על ידי כך שהיא גורמת לו להאמין שהסבירות להצלחתו קלושה, או שהנזק מהתגובה יהיה גדול ממה שיהיה מוכן לשאת.[47] בעבר נדרש שהרתעה תכלול "שלושה רכיבים גלויים: ייחוס, איתות ואמינות".[48] בהקשר הנוכחי, הרתעה מגלמת הנחה מוקדמת על כך שהקווים האדומים הכלליים של ארצות־הברית הובהרו ליריביה וכן לבעלות־בריתה, שהיא אותתה כי חציית גבולות אלה לא תעבור בשתיקה, וכי היא יכולה ומוכנה להטיל את ההשלכות של כל הפרה כזו על מי שחוצה אותם. התגובה האמריקאית הצפויה צריכה להיות מאיימת דיה על מנת להניא את הגורם המאיים הפוטנציאלי מביצוע הפעולה מלכתחילה.

כאשר ארצות־הברית מגדירה קווים אדומים במרחב הסייבר, עליה לפעול במחשבה תחילה ובזהירות ניכרת, ולזכור שפעילויות שמתקרבות לקווים אלה אך אינן חוצות אותם יגררו עונש מופחת, כפועל יוצא של הגדרת הגבולות. יש להעריך בהתאם פעילויות שאינן מבוצעות למטרה חיובית, כגון מאמצים למפות את התשתית החיונית בארצות־הברית. שום טובה לא תצמח מכך שלמדינה אחרת או לגורם לא־מדינתי זר יהיה ידע מפורט על מערכות אלה.

הייחוס הוא מכריע בביסוס ההרתעה. חשוב שניתן יהיה לדעת מי פעל, על מנת להטיל עליו את ההשלכות. עם זאת, קשה לאתר את "המקלדת המעשנת" במרחב הסייבר, שכן מרחב זה נוצר כך שיאפשר הכחשה אמינה. סדרי הגודל והמשמעות של אתגר הייחוס בהקשר של תגובה למתקפת סייבר זכו להדגשה מצד אנליסטים בכירים,[49] אם כי יש גם דעות מנוגדות.[50] אם נתעלם לרגע מהקושי לעשות זאת, היכולת לקשר בין הפעולה לבין הגורם לה תאפשר לצד המותקף להגיב. היכולת להגיב באותה מטבע מעלה את מספר האפשרויות שהצד המותקף יוכל להסתמך

עליהן בדיעבד, לרבות האפשרות להגיב בעוצמה רבה יותר מזו שהצד המותקף ספג. ראוי אפוא להשקיע זמן ומשאבים במאמץ מרוכז שתכליתו לפתח יכולת ייחוס משופרת, באמצעות טכנולוגיות ואמצעים אחרים.

היריבים חייבים גם הם להבין ולהעריך שארצות־הברית ערוכה ומוכנה להשתמש במלוא הכוח שברשותה – במגוון, בהיקף ובעומק – על מנת לאכוף כללים אלה. כדי לשדר מסר זה בצורה משכנעת ולהביא לכך שהוא יגיע ליעדו ולאוזניהם של בעלי הכוונות העוינות, חייב להתקיים מצג פומבי של היכולות באופן שיבהיר את המסר לאשורו, מבלי לחשוף יותר מדי ולאבד את היתרון בשל כך. למשל, עליו למנוע אפשרות שהאויב יוכל לבצע "הנדסה הפוכה" (או לחקות בדרך אחרת), ולהשתמש באותם אמצעים ושיטות של ארצות־הברית שהוצגו בפומבי, שמא יהיה זה "גול עצמי". היבט ה"מצג" של התרגיל הופך מתעתע אף יותר כאשר זוכרים שהחוקים השולטים בלוחמת הסייבר עדיין בשלבי התפתחות, ולכן אינם חד־משמעיים במידה מסוימת. נקיטת זהירות ותשומת לב נדרשים, אם כך, גם ברמה המשנית.

אף על פי שארצות־הברית נדרשת להפגין את ארגז הכלים שלה, המצויד בכל הנדרש כדי להילחם בגורמים עוינים בעת הצורך, עד היום לא הייתה הפגנה פומבית חד־משמעית כזו של עליונות סייבר, שארצות־הברית טענה באופן יזום והחלטי לבעלות עליה. על רקע זה, האם עליה לשקול ביצוע מקביל דיגיטלי של ניסוי גרעיני חי? יש להפנות שאלה זו לקובעי המדיניות, למומחים ולאנשי הטכנולוגיה האמריקאיים, המבקשים להגדיר את מסלול ההתקדמות ולפתח דוקטרינה ואסטרטגיה עבור מרחב הסייבר. האירוניה היא שאם תרגיל כזה יתבצע בזהירות (ההולמת את גודלו), הוא יוכל לפעול ביעילות להרתעת גורמים עוינים, כך שאין להוציא מכלל אפשרות שהוא יתרום למניעת מלחמה.

בניית יציבות באמצעות עוצמה

נהוג לומר שההגנה הטובה ביותר היא ההתקפה. על פי דיווחים ממקורות גלויים, ארצות־הברית מפתחת כללים למעורבות בכל הקשור למתקפות סייבר, ומשרד ההגנה חותר לחיזוק ארסנל נשק הסייבר שברשותו[51] (אם כי מתקפת סייבר עשויה להביא לתגובה צבאית או לתגובת סייבר). כפי שציין סגן יו"ר המטות המשולבים לשעבר, הגנרל ג'יימס אי. קרטרייט (James E. Cartwright), מאמצים והשקעה מהסוג שתואר כאן יסייעו להתאים מחדש את יחס ההגנה מול ההתקפה – שעד לאחרונה עמד על 90% מול 10% לערך לטובת ההגנה[52] – ויחזקו ויבנו אמון ביכולתה של ארצות־הברית להרתיע ביעילות פעולה עוינת במרחב הסייבר.

עם זאת, קהילת ביטחון הסייבר בארצות־הברית, כמו המקבילות לה אצל בעלות־בריתה, טרם השלימה את התהליך. עוד ארוכה הדרך עבור קהילה זו, בייחוד

בארצות־הברית, עד שתגיע לרמת המיומנות והבשלות שמציגות כיום הקהילות העוסקות במלחמה בטרור בארצות־הברית.[53] סנכרון סעיפים 10 ו־50 בחוק האמריקאי ששילב יחדיו פונקציות מודיעין וצבא מהווה פריצת דרך משמעותית בעידן שלאחר פיגועי ה־11 בספטמבר, שהביאה לשיפור ניכר במצבה הכולל של ארצות־הברית במלחמה בטרור. היא יכולה למנף הישג זה באמצעות התאמה והחלה של תפיסה דומה גם על הסייבר. עליה לחתור לכך תוך התייחסות לשני אתגרים (שעדיין יש לעמוד בהם): הסדרת החוקים העוסקים במעורבות וחתירה לעמדה יוזמת יותר.[54]

כדי להתקדם בחוכמה במרחב הסייבר, חייבות ארצות־הברית ובעלות־בריתה להפגין מנהיגות ולהציג חזון, לצד תוכנית פעולה מבוססת. זמן רב מדי הניעו התקריות את האסטרטגיה, למעשה, זוהי טקטיקה במסווה של אסטרטגיה. ארצות־הברית מחזיקה במספר יכולות ייחודיות, אך אלה לא ינוצלו במלואן עד שתגובש מסגרת אסטרטגית רחבה יותר שבתוכה ניתן יהיה לשבצן. בהמשך למסגרת הרעיונית שהוצגה כאן, עולים עקרונות מפתח מסוימים שיכולים לשמש בסיס לפיתוח וליישום אסטרטגיה, יכולת ועמדה להרתעת סייבר יעילה. עקרונות אלה מהווים את ראשיתה של תוכנית להרתעת סייבר, כדלקמן:

כיול במטרה לממש את החזון. בהקשר זה, יכולת תומכת באמינות. יש לשקול בזהירות את הכיול הקיים ולכוונו כנדרש, בהתאם להשקעות ולמאמצים המשקפים את היחס בין הגנה להתקפה – שחוסר איזון בו עלול להשפיע לרעה על הביטחון הלאומי. בהיותו דרישה מקדימה לאכיפת ההשלכות, כיול (או כיול מחדש) מתקיים בד בבד עם הרצון הפוליטי לפעול לאכיפת סנקציות בבוא העת.

התחלה ובנייה מעמדת כוח. כדי להרתיע ולהניא יריבים בהצלחה, נדרשת יכולת לשכנע אויבים פוטנציאליים שהמחיר של פעולה עוינת מצדם יעלה על התועלת שהם מייחסים לה. פיתוח של יכולת מכת פתיחה ואיתות נכון על קיומה הם, לפיכך, בסיסיים.

שימת הדגש על מהירות, הפתעה ויכולת תמרון. במרחב הסייבר, כל ננו־שנייה קובעת. לכן, היעד הוא להגיב בזמן אמת ככל האפשר. בעוד אין לפקפק בעיקרון שלכל חציית קו אדום יהיו השלכות, יש ערך לשמירה על מידה של עמימות באשר לטיבן המדויק של השלכות אלה, ועל ידי כך יישאר אותו גורם במצב של אי־ודאות תמידי. גמישות ובהירות נראות סותרות לכאורה, אך למעשה הן מייצרות אסטרטגיה שקולה.

אין להותיר אף אחד מאחור. יכולת של מכת פתיחה בלבד תותיר את המדינה פגיעה ובלתי־מוכנה לתגובה באותה מטבע, אם היריב מסוגל לכך. כמו בשלב המלחמה הקרה של עידן הגרעין, יידרשו תכנון מראש וזהירות בהפעלת יכולת מכה שנייה באופן שיבטיח הגנה על הכוח. שימור העליונות המדעית והטכנולוגית

הוא גורם מכריע, שכן ניתן להגיע לפתרונות טכניים לנוכח האתגרים המטרידים במרחב הסייבר.

דע את האויב. הביטוי אולי ישן ושחוק, אך הוא עדיין תקף. כדי להביס אויב פוטנציאלי נדרשת הבנה מעמיקה של מטרותיו ושאיפותיו הספציפיות. תובנה מעין זו תאפשר לבנות את האסטרטגיה והטקטיקה לאותו מקרה תוך התאמת הרכיבים ליריב הספציפי, ובכך למקסם את פוטנציאל הסיכול. הכלל שתקף כאן הוא מה שמכונה "לולאת OODA": התבונן, התכוונן, החלט ופעל (observe, orient, decide, and act).

הובלה שמהווה דוגמה. ברעיון של הרתעת סייבר איתנה טמונה הנחת המוצא, שהישות המנסה להרתיע מחוסנת מפני מה שהיא מנסה לעולל לאחרים (שכן תמיד קיימת האפשרות לאפקט בומרנג). כל דרך אחרת כמוה כקפיצה מהמטוס ללא מצנח. לכן, המסקנה המכרעת היא שעל ממשלת ארצות־הברית לשאוף תחילה לפתרון בעיותיה שלה, כדי להתמודד עם האיום. יתרה מכך, על הממשלה ליזום את הצעדים הדרושים להקלת שיתוף המידע, כך שעובדות חיוניות יגיעו לידי כל גורמי המפתח האחראיים להגנה על נכסים ומשאבים לאומיים, לרבות אלה שבבעלות המגזר הפרטי ובתפעולו (תשתית חיונית).

שותפים להצלחה. אין מרכיב יחיד בממשלה, גם לא הממשלה כגוף אחד, שיוכל להתמודד לבדו במרחב הסייבר. חיוני לכונן שותפויות אמת בתוך המגזרים השונים וביניהם. בתוך הממשל לדוגמה, סנכרון זהיר ושילוב של פונקציות מודיעין וצבא (סעיפי החוק 10 ו־50) למטרות הרתעת סייבר עשוי להתגלות כבעל ערך רב, כפי שהיה בהקשר של מלחמה בטרור. החשיבות של התגוננות מראש מתרחבת מעבר למגזר הציבורי, לעבר רשתות ומערכות חיוניות שמצויות בידיים פרטיות. בהתאם לכך, על המגזר הפרטי להתחייב לנקוט את הצעדים הדרושים לחיזוק הביטחון הלאומי. כדי להבטיח עמידה בסף זה, הרשויות הפדרליות צריכות להושיט יד למגזר הפרטי, בגישה שתשלב תמריצים חיוביים ושליליים להשגת התוצאה המבוקשת, בשיטת "המקל והגזר".

חשיבה ופעולה במושגים בינלאומיים. אתגרים חוצי־גבולות מחייבים פתרונות חוצי־גבולות, ומרחב הסייבר הוא חסר גבולות מטבעו. שותפים נאמנים ברמה הבינלאומית יכולים וצריכים לספק ערך רב בהקשר זה. יש להודות שאינטרסים לאומיים עלולים לפגוע ביכולת לשתף נתונים ומידע רגיש. יחד עם זאת, ההימנעות ממינוף יחסים בילטרליים ובריתות מרכזיות תהיה "גול עצמי", החל מהסכם שיתוף המודיעין "Five Eyes"(בין אוסטרליה, קנדה, ניו־זילנד, ארצות־הברית ובריטניה), דרך ברית נאט"ו ועד האיחוד האירופי, וכן שותפות אסטרטגיות נוספות כמו באזור המזרח התיכון ואסיה, הכוללות את ישראל, סינגפור, הודו ויפן.

עם מנהיגות מעוררת השראה בלוחמת הסייבר ברמה של דמויות המופת הצבאיות, בילי מיטשל (Billy Mitchell), ביל דונובן (Bill Donovan) או ג'ורג' פטון (George Patton) – שהיטיבו להבין את השימושים האסטרטגיים והטקטיים של חידושי טכנולוגיה ונשק – ארצות־הברית יכולה לעצב ולהוציא לפועל אסטרטגיית הרתעת סייבר רבת־עוצמה שמישירה מבט אל אויביה כשהיא מוכנה כיאות, בשאיפה שהאירועים שנכונו לה יישארו כרוכים בבייטים וביטים בלבד, במקום בכדורים, בפצצות ובשפיכות־דמים.

הערות

1 Eric Sterner, "Deterrence in Cyberspace: Yes, No, Maybe," in *Returning to Fundamentals: Deterrence and U.S. National Security in the 21st Century* (Washington, DC: George C. Marshall Institute, 2011), p. 27.

2 Bryan Krekel, Patton Adams, and George Bakos, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*, Prepared for the U.S.-China Economic and Security Review Commission by Northrop Grumman Corporation, March 7, 2012, p. 54, http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf.

3 Siobhan Gorman, "Electricity Grid in U.S. Penetrated By Spies," *Wall Street Journal*, April 8, 2009, http://online.wsj.com/article/SB123914805204099085.html; and Mark Clayton, "Exclusive: Potential China Link to Cyberattacks on Gas Pipeline Companies," *Christian Science Monitor*, May 10, 2012, http://www.csmonitor.com/USA/2012/0510/Exclusive-potential-China-link-to-cyberattacks-on-gas-pipeline-companies.

4 Office of the National Counterintelligence Executive (NCIX), *Foreign Spies Stealing US Economic Secrets in Cyber Space: Report to Congress on Foreign Economic Collection and Industrial Espionage 2009-2011* (October 2011), p. 4, http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf;

5 שם.

6 Eben Kaplan, *Terrorists and the Internet*, Council on Foreign Relations, January 8, 2009, http://www.cfr.org/terrorism-and-technology/terrorists-internet/p10005; and Special Report by the Homeland Security Policy Institute (HSPI) and the University of Virginia's Critical Incident Analysis Group (CIAG), *NETworked Radicalization: A Counter-Strategy* (Washington, DC: May 2007).

7 Group IB, *State and Trends of the Russian Digital Crime Market 2011*, p. 6, http://group-ib.com/images/media/Group-IB_Report_2011_ENG.pdf.

8 ראו:
Thomas C. Schelling's classic text, *Arms and Influence* (New Haven: Yale University Press, 1966).

9 ראו לדוגמה:
Martin C. Libicki, *Cyberdeterrence and Cyberwar* (RAND Corporation, 2009).

10 Sun Tzu, *The Art of War*, translated by Samuel B. Griffith (New York: Oxford University Press, 1963).

11 Ellen Messmer, "DHS: America's Water and Power Utilities under Daily Cyber-Attack," *Network World*, April 4, 2012, http://www.networkworld.com/news/2012/040412-dhs-cyberattack-257946.html?t51hb&hpg1=mp.

12 Jason Koebler, "U.S. Nukes Face up to 10 Million Cyber Attacks Daily," *US News & World Report*, March 20, 2012, http://www.usnews.com/news/articles/2012/03/20/us-nukes-face-up-to-10-million-cyber-attacks-daily.

13 Joe Lieberman, "Cyber Networks Sitting Ducks for Attacks" *Hartford* Courant, April 8, 2012, http://articles.courant.com/2012-04-08/news/hc-op-lieberman-cyber-security-biggest-national-th-20120408_1_cyber-attack-cyber-networks-cyber-threats

14 John O. Brennan, "Time to Protect against Dangers of Cyberattack," *Washington Post*, April 15, 2012, http://www.washingtonpost.com/opinions/time-to-protect-against- dangers-of-cyberattack/2012/04/15/gIQAdJP8JT_story.html.

15 Lieberman, "Cyber Networks Sitting Ducks for Attacks."

16 Jason Ryan, "FBI Director Says Cyberthreat will Surpass Threat from Terrorists," January 31, 2012, http://abcnews.go.com/blogs/politics/2012/01/fbi-director-says-cyberthreat-will-surpass-threat-from-terrorists/.

17 "המציאות היא שהתשתיות שלנו עוברות קולוניזציה", אמר טום קלרמן, לשעבר הממונה מטעם הנשיא אובמה על המועצה לאבטחת הסייבר. ראו: David Goldman, "Cybersecurity Bills Aim to Prevent 'Digital Pearl Harbor,'" April 23, 2012, http://money.cnn.com/2012/04/23/technology/cybersecurity-bills/?source=cnn_bin.

18 "בכיר במודיעין שתידרך עיתונאים בנושא האנונימיות ציין כמה מקרים שבהם ניתנו אומדנים כחלק מתביעות נגד ריגול כלכלי במהלך שש השנים האחרונות: מחקר של Dow Chemical על הדברת חרקים בשווי של 100 מיליון דולר, נוסחאות כימיות של DuPont בשווי של 400 מיליון דולר, נתונים קנייניים של מוטורולה בשווי 600 מיליון דולר, נוסחאות צבע של Valspar בשווי של 20 מיליון דולר". ראו :
Ellen Nakashima, "In a World of Cybertheft, U.S. names China, Russia as Main Culprits," *Washington Post*, November 3, 2011, http://www.washingtonpost.com/world/national-security/us-cyber-espionage-report-names-china-and-russia-as-main-culprits/2011/11/02/gIQAF5fRiM_story.html.

19 Nick Hopkins, "Militarisation of Cyberspace: How the Global Power Struggle Moved Online," *The Guardian*, April 16, 2012, http://m.guardian.co.uk/technology/2012/apr/16/militarisation-of-cyberspace-power-struggle?cat=technology&type=article; and Nick Hopkins, "US and China Engage in Cyber War Games," *The Guardian*, April 16, 2012, http://m.guardian.co.uk/technology/2012/apr/16/us-china-cyber-war-games?cat=technology&type=article.

20 Reuters, "Saudi Oil Producer's Computers Restored After Virus Attack" *New York Times*, August 26, 2012, http://www.nytimes.com/2012/08/27/technology/saudi-oil-producers-computers-restored-after-cyber-attack.html?_r=1.

21 Elinor Mills, "Virus Knocks out Computers at Qatari Gas Firm RasGas," *CNET News*, August 30, 2012, http://news.cnet.com/8301-1009_3-57503641-83/virus-knocks-out-computers-at-qatari-gas-firm-rasgas/.

22 Christopher Brook, "Report: French Nuclear Company Areva Hit by Virus" *ThreatPost*, October 31, 2011, http://threatpost.com/en_us/blogs/report-french-nuclear-company-areva-hit-virus-103111.

23 מייקל מק'קול (McCaul), יו"ר ועדת המשנה לנושאי ביקורת, חקירה וניהול של ועדת בית הנבחרים לביטחון המולדת, אמר: "איסוף המידע האגרסיבי ביותר על הכלכלה והטכנולוגיה של ארצות־הברית נעשה מצד סין...יכולות לוחמת הסייבר של סין ומבצעי הריגול שהיא מפעילה הם הנפוצים ביותר מבין הגורמים המדינתיים. סין יצרה קבוצות האקרים אזרחיות המעורבות בריגול סייבר, והקימה יחידות צבאיות ללוחמת סייבר". ראו:
NCIX, *Foreign Spies Stealing US Economic Secrets in Cyberspace*, p. 5;.
ראו גם:
Cindy Saine, "Experts Warn of Increased US Cyber Security Threat" *VOA News*, April 24, 2012, http://www.voanews.com/english/news/usa/Experts-Warn-of-Increased-US-Cyber-Security-Threat-148786975.html.

24 Qiao Liang and Wang Xiangsui, published by China's People's Liberation Army, Beijing.

25 David J. Smith, "How Russia Harnesses Cyberwarfare," *American Foreign Policy Council Defense Dossier* (August 2012), http://www.afpc.org/files/august2012.pdf.

26 Jason Healey and Leendert van Bochoven, "NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow" *Atlantic Council Issue Brief* (2011) p. 2, http://www.acus.org/files/publication_pdfs/403/022712_ACUS_NATOSmarter_IBM.pdf.

27 Group IB, *State and Trends of the Russian Digital Crime Market 2011*, p. 6, http://group-ib.com/images/media/Group-IB_Report_2011_ENG.pdf;
ראו גם:
http://group-ib.com/images/media/Group-IB_Cybercrime_Inforgraph_ENG.jpg (איור).

28 Frank J. Cilluffo, "The Iranian Cyber Threat to the United States," Testimony Before the House of Representatives Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence, and Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies, April 26, 2012, p. 4, http://www.gwumc.edu/hspi/policy/Iran%20Cyber%20Testimony%204.26.12%20Frank%20Cilluffo.pdf; and Conficker Working Group, *Conficker Working Group: Lessons Learned*, http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf.

29 Cilluffo, Testimony Before the House of Representatives, p. 4.

30 Jack Clohurty, "Virtual Terrorism: Al Qaeda Video Calls for 'Electronic Jihad'" *ABC News*, May 22, 2012, http://abcnews.go.com/Politics/cyber-terrorism-al-qaeda-video-calls-electronic-jihad/story?id=16407875#.UEieyEQrOlg.

31 Yaakov Katz, "Iran Embarks on $1b. Cyber-Warfare Program," *Jerusalem Post*, December 18, 2011, http://www.jpost.com/Defense/Article.aspx?id=249864.

32 Cilluffo, Testimony Before the House of Representatives, p. 6.

33 Golnaz Esfandiari, "Iran Says it Welcomes Hackers Who Work for Islamic Republic," Radio Free Europe, March 7, 2011, http://www.rferl.org/content/iran_says_it_welcomes_hackers_who_work_for_islamic_republic/2330495.html

34 Iftach Ian Amit, "Cyber [Crime/War]," paper presented at DEFCON 18 conference, July 31, 2010.

35 "The Role of the Basij in Iranian Cyber Operations," *Internet Haganah*, March 24, 2011, http://internet-haganah.com/harchives/007223.html.

36 Michael Puttre, "Iran Bolsters Naval, EW Power," *Journal of Electronic Defense* 25, no. 4 (2002): p. 24; Robert Karniol, "Ukraine Sells Kolchuga to Iran," *Jane's Defense Weekly* 43, no. 39 (September 27, 2006), p. 6; Stephen Trimble, "Avtobaza: Iran's Weapon in Alleged RQ-170 Affair?" *The DEW Line*, December 5, 2011, http://www.flightglobal.com/blogs/the-dewline/2011/12/avtobaza-irans-weapon-in-rq-17.html.

37 Reuters, "Nasrallah: Iran could Strike US Bases if Attacked," *Jerusalem Post*, September 3, 2012, http://www.jpost.com/IranianThreat/News/Article.aspx?id=283706.

38 Ilan Evyatar, "Falling into the Trap, Over and Over Again," *Jerusalem Post*, November 17, 2010, http://www.jpost.com/Features/InThespotlight/Article.aspx?id=195767; Dan Harel, "Asymmetrical Warfare in the Gaza Strip: A Test Case," *Military and Strategic Affairs* 4, no. 1 (2012): pp. 17-24, http://www.inss.org.il/upload/(FILE)1339053338.pdf; Yolande Knell, "New Cyber Attack Hits Israeli Stock Exchange and Airline," *BBC* News, January 16, 2012, http://www.bbc.co.uk/news/world-16577184; and Joshua Mitnick, "Israel's Businesses Losing the Cyber War," *Wall Street Journal*, July 25, 2012, http://online.wsj.com/article/SB10000872396390443477104577549262451192148.html.

39 NCIX, *Foreign Spies Stealing US Economic Secrets in Cyberspace*, p. 19.

40 Jean-Marie Bockel, Senator for Haut-Rhin, "Cyber Defence an International Issue, a National Priority," *Information report no. 681 – Committee on Foreign Affairs, Defence and Armed* Forces, July 18, 2012, http://www.senat.fr/rap/r11-681/r11-681-syn-en.pdf.

41 נאום בהרצאה השנתית על ביטחון והגנה ע"ש לורד מאיור, שנערכת בעיר לונדון, https://www.mi5.gov.uk/home/about-us/who-we-are/staff-and-management/director-general/speeches-by-the-director-general/the-olympics-and-beyond.html.

42 ראו:
Tom Whitehead, "Cyber Crime a Global Threat, MI5 Head Warns," *The Telegraph*, June 26, 2012, http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/9354373/Cyber-crime-a-global-threat-MI5-head-warns.html.

43 Cilluffo, *Testimony Before the House of Representatives*, pp. 7-8.
ראו גם:
Frank J. Cilluffo, "The U.S. Response to Cybersecurity Threats," *American Foreign Policy Council (AFPC) Defense Dossier* (August 2012), http://www.afpc.org/files/august2012.pdf; and Martin C. Libicki, "The Strategic Uses of Ambiguity in Cyberspace" *Military and Strategic Affairs* 3, no. 3 (2011): pp. 3-10, http://www.inss.org.il/upload/(FILE)1333532281.pdf.

44 *The Book of Five Rings.*

45 Nakashima, "In a world of cybertheft, U.S. names China, Russia as main culprits" [citing NCIX Bryant].

46 שם.

47 W. W. Kaufmann, "The Requirements of Deterrence," in W. W. Kaufman, ed., *Military Policy and National Security* (Princeton: Princeton University Press, 1956); Peter Marquez, "Space Deterrence: The Pret-a-Porter Suit for the Naked Emperor," in *Returning to Fundamentals*, pp. 9-10. אילוץ מבקש להשפיע על היריב לפעול

או להימנע מפעולה באמצעות איום, או בפועל, לגבות מחיר מהיריב כדי להגביל את אפשרויותיו ו/או את חישובי העלות־תועלת שלו כך שהיריב מחליט כי העלות של פעולתו המשוערת אינה מצדיקה את התועלת שתופק ממנה.

Marquez, "Space Deterrence" at p. 10, citing G. Schaub, Jr., "Deterrence, Compellence and Prospect Theory" *Political Psychology* 25, no. 3 (2004), pp. 389-411.

48 Marquez, "Space Deterrence," p. 10.

49 לדוגמה, ראו:

Yasmin Tadjdeh, "U.S. Military Overestimates Value of Offensive Weapons Cyberweapons, Expert Says," *National Defense*, September 13, 2012, citing Martin Libicki, senior management scientist at RAND Corp, http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=887.

50 F. Hare, "The Significance of Attribution to Cyberspace Coercion: A Political Perspective." Paper presented at the *Cyber Conflict (CYCON), 2012 4th International Conference* on June 5-8, 2012.

51 Federal News Radio, "DoD Hammering out Rules of Cyberspace," October 21, 2011, http://www.federalnewsradio.com/?nid=398&sid=2602063; and Ellen Nakashima, "Pentagon to Fast-track Cyber Weapons Acquisition," *Washington Post*, April 9, 2012, http://www.washingtonpost.com/world/national-security/pentagon-to-fast-track-cyberweapons-acquisition/2012/04/09/gIQAuwb76S_print.html.

52 Lolita C. Baldor, "Pentagon to Publish Strategy for Cyberspace War," *Navy Times,* July 14, 2011, http://www.navytimes.com/news/2011/07/ap-pentagon-publish-strategy-cyberspace-war-071411/;

ראו גם:

"A Conversation on Cyber Strategy with General James E. Cartwright," *Homeland Security Policy Institute (HSPI) Capstone Series on Cyber Strategy*, May 14, 2012, http://www.gwumc.edu/hspi/events/cartwrightCS501.cfm.

53 Frank Cilluffo and Andrew Robinson, "Analysis: While Congress Dithers, Cyber Threats Grow Greater," *Nextgov*, July 24, 2012, http://www.nextgov.com/cybersecurity/2012/07/while-congress-dithers-cyber-threats-grow-greater/56968/.

54 Cilluffo, *AFPC Defense Dossier*.

'דילמת דוקו':
הנחת העמימות והשאיפה חסרת התוחלת למלחמת סייבר סטרילית

מת'יו קרוסטון

הוויכוח סביב החלה או אי־החלה של הדין הבינלאומי בכל הנוגע למלחמת סייבר וסביב הצורך באמנת סייבר בינלאומית עשוי להתגלות כבלתי־רלוונטי. שני המחנות, התומכים והמתנגדים, מתווכחים האם יש צורך להחיל את דיני הלחימה, גם על תחום הסייבר, במקרה של מלחמת סייבר. במנותק מהדעה האם חוקי הלחימה חלים אם לאו, או האם יש לקדם אמנת סייבר בינלאומית, או שמא אמנה כזו תהיה חסרת משמעות, יש צורך אחד שנותר על כנו: השאיפה לחוקים שיפקחו על התנהלות מלחמת סייבר. אולם כל הצדדים מחמיצים את העובדה שמבנה תחום הסייבר מונע אסטרטגיה ש"תופסת טרמפ" על נורמות קונוונציונליות של מלחמה. נורמות אלה אפקטיביות בשל היכולת להבחין בין המגזר האזרחי למגזר הצבאי. לא ניתן ליישם הבחנה כזו בתחום הסייבר, בהיותו מאופיין במיזוג המשתתפים, המתקנים והיעדים לכדי ישות אחת, המשלבת באופן חסר־תקנה בין מוסדות אזרחיים לצבאיים. הסבר חשוב זה חסר ביחס לשאלה, מדוע מאמץ כלל־עולמי לשפר ולהבהיר נורמות סייבר נותר בלתי־מאוזן ובלתי־הולם.

וכך נוצרת 'דילמת דוקו': כל עוד המוקד הוא גיבוש יעדים לגיטימיים והצבת מגבלות על פעולה מורשית, ארצות־הברית ובעלות־בריתה חושפות את עצמן לפגיעויות, ובמקביל משקיעות מאמץ עקר שאינו מוביל לבקרת סייבר משופרת. בדיוק כמו הווירוס דוקו (Duqu) שכיכב בדיון הכלל־עולמי ב־2011, מתקפות הסייבר כיום יכולות להתבצע לצורך איסוף מידע **או** כפוטנציאל למתקפה פיזית; הן יכולות להיות יוזמה ממשלתית אך להתבצע דרך נכסים מסחריים חשובים; הן יכולת לכוון ליעדים מדיניים/צבאיים **ובמקביל** להסתייע בחדירה למערכות אזרחיות. יצירת כללי סייבר בדומה לנורמות קונוונציונליות היא לפיכך חסרת

ד"ר מת'יו קרוסטון (Matthew Crosston), אוניברסיטת Bellevue, ארצות־הברית

מאמר זה ראה אור לראשונה ב**צבא ואסטרטגיה**, כרך 5, גיליון 1, מאי 2013, עמ' 99-109.

תוחלת, שכן כללים אלה אינם ניתנים לאכיפה (כפי שיידון בהמשך). משום כך המאמצים הנוכחיים פשוט כובלים את ידי המדינות שומרות החוק. המסקנה היא שיש להקדיש מאמץ רב יותר ליצירת אסטרטגיה מונעת, שמקבלת את בעיית העמימות האזרחית/צבאית כמציאות קיימת. הנטייה של חוקרים וקובעי מדיניות לחתור ללוחמת סייבר 'סטרילית' באמצעות הגבלת הנזק שייגרם על ידי סיווג ברור של המטרה, פירושה שאסטרטגיית הסייבר סובלת מהיעדר כוח הרתעה אמיתי. בקצרה, מומחים להגנת סייבר רק מעצימים את הדילמה.

חוסר ההשפעה של הדין הבינלאומי

כפי שציין מכון המחקר East-West ב־2011, "קיים צורך דחוף לשיתוף פעולה בינלאומי בסוגיות אסטרטגיות אלה. אם ניכשל במשימה זו, האיום על היציבות הכלל־עולמית יהיה כאיומה של פצצה גרעינית".[1] נורמות בינלאומיות שגובשו באמנות האג וז'נבה הציבו קווי הגנה ברורים לאוכלוסיות אזרחיות בזמן שהמדינות מעורבות במלחמה. כבוד לחיי אזרחים והגנה עליהם נתפסים כיום כמקודשים, ללא קשר לצורה שבה מנוהלת המלחמה, ומכאן הציפייה שמרחב הסייבר יהיה כפוף לפיקוחן של הנורמות הקונוונציונליות.

היו שכינו סוגיה זו אחד מהקרבות הגיאופוליטיים החשובים שמתנהלים כיום, והרחיקו עד כדי האמירה שזהו ה'גראונד זירו' של הדיפלומטיה העולמית, של עבודת הביטחון הלאומי ושל המודיעין.[2] אכן, האופטימיים ביותר רוצים לראות הסכמים מרצון שמטילים מגבלות על פיתוח יכולות הסייבר, ולכאורה משפרים את ההתנהגות במרחב הסייבר. עם זאת, יש מי שהכירו בכך שקיימות סכנות פוטנציאליות בניסיון להגיע להישג כזה. סטיוארט בייקר (Stewart Baker), לשעבר יועץ כללי בסוכנות הביטחון הלאומי האמריקנית (NSA) ועוזר שר לענייני מדיניות במשרד לביטחון המולדת (DHS) בממשל הנשיא ג'ורג' וו. בוש, ניסח את החשש המובן מאליו: ארצות־הברית ובעלות־בריתה יצייתו לכללים, ובו־בזמן, אף לא אחד מיריביה יעשה כן.[3]

אולם הבעיה עלולה להיות אפילו קשה יותר מאשר אי־ציות לחוק: מרבית הרשתות הצבאיות שיכולות ליזום או לבצע מתקפת סייבר עובדות עם אינספור רשתות אזרחיות ותלויות בהן. נוסף לכך, רבים מהגורמים שהם חלק מהתכנון, היוזמה והפריסה של מתקפות סייבר אינם בהכרח גורמים צבאיים רשמיים, אלא עובדים אזרחיים של סוכנויות ממשלתיות. במילים אחרות, עולם לוחמת הסייבר אינו עולם של סיווג ברור אלא של עמימות מכוונת. למעשה, מגמות עתידיות מצביעות על כך שמיזוג זה רק יעמיק ויתחזק עם הזמן.

'הנחת עמימות' זו זכתה עד כה להתעלמות יחסית במהלך הוויכוחים השונים שהתקיימו סביב נושא הסייבר. במקום זאת, ויכוחים אלה התמקדו בשאלה עד כמה

משוחררים או נוקשים, רשמיים או לא־רשמיים, בינלאומיים או מקומיים אמורים להיות אותם קודים של מגבלות. רבים מהקודים המוצעים נועדו להגביל התנהלות בסייבר כך שתושג הגנה על בנקים, אנרגיה ורשתות אחרות של תשתית קריטית, 'למעט כאשר מדינות מעורבות במלחמה'.[4] בעיית העמימות, לעומת זאת, גורמת מבוכה למדינות: כיצד ניתן למתוח קו מפריד בין אזרחים לבין הצבא? הדילמה הגדולה ביותר, אפוא, היא לא הצלחה בזיהוי האחראי למתקפה (ייחוס נכון), אלא העמימות המובנית והמכוונת שמאפיינת את התשתית הקריטית המשמשת לפיתוח יכולות הסייבר של המדינה.

רבים מדיוני הסייבר העכשוויים לוקים באופן שבו הם מבקשים להקיש במשתמע מהלוחמה הקונוונציונלית ללוחמת הסייבר, ולראות במתקפות סייבר שוות־ערך למתקפות חמושות. אך כדי לעשות זאת, הדיון צריך לפנות להגדרות ולפרמטרים המשפטיים: מתי לוחמת סייבר עונה להגדרה של שימוש בכוח חמוש או מהלך רשמי של מלחמה? אילו פעולות ייחשבו כפשעי מלחמה? מה מידת הנזק המצדיקה תגובת נקם?[5] שאלות אלה קשות הרבה יותר למענה בזירת הסייבר בשל הסיוט הלוגיסטי שיוצרת הנחת העמימות. עובדה זו אינה מודגשת במחקרים ואינה זוכה למענה באסטרטגיה.

במקום זאת, מרבית השאלות עוסקות בהשוואה של מידת סכנת החיים, הערכות הנזק ובעיית הייחוס שהוזכרה לעיל. במידה מסוימת, כל הבעיות הללו נותרות בצל בעיית העמימות הצבאית/אזרחית. חוסר היכולת ליצור הפרדה זו פירושו שיכולת ההרס יכולה להיות קטלנית יותר, משום שהיא יכולה להתרחב מעבר לנפגעים צבאיים, הנזק יכול להיות הרסני יותר אם יקיף יותר מאשר מתקנים צבאיים, והייחוס עשוי אף להיות לא־רלוונטי כלל: השאלה **מי** עומד מאחורי המתקפה אינה הפתרון לבעיה, כל עוד ה**איך** שמאחורי ה**מי** משולב באופן שלא ניתן להפרדה לכדי ישות אחת של המגזר הממשלתי, הצבאי והאזרחי. במילים אחרות, רבים מניחים שההבנה **מי ומי** במלחמת סייבר תפתור את מרבית הבעיות המשפטיות, אך הנחת העמימות מציבה אזהרה: בסייבר, **מי** אף פעם אינו מובחן בקלות מ**איך** או חשוב יותר ממנו.

התסכול שבהצבת תנאים

חלק מהקושי להחיל את הדין הבינלאומי ביעילות על מרחב הסייבר קשור בכישלון נושן לתרגם מונחים ופרמטרים חיוניים לדבר שישפיע על התחום. ההתקדמות לפתרון בעיה זו הייתה מוגבלת ביותר, ואכן, די בהצצה חטופה בספרות של העשור האחרון על מנת להיווכח שמלחמת סייבר אינה חופפת בדיוק למסגרות המשפטיות הקיימות בנוגע למלחמה ולשימוש בכוח.[6] למרות מציאות זו, נעשו ניסיונות נמרצים להתגבר ביעילות על קשיים טרמינולוגיים ודוקטרינריים אלה,

ולהחיל אותם על זירת הסייבר. מאמר זה טוען שניתן לייחס את חוסר ההצלחה למיזוג הצבאי/אזרחי הטבוע בהנחת העמימות.

השאיפה לתנאים, לפרמטרים, להגדרות, לחוקים ולהסכמים מפורשים מבוססת בעיקר על החשש שכישלון ליצור מצבים מפורשים כאלה יותיר את מלחמת הסייבר מחוץ לגבולות המלחמה הקונוונציונלית. המסקנות נחשבות חמורות: תשתית אזרחית קריטית תהיה יעד, כמו גם צרכים בסיסיים כגון חקלאות, מזון, מים, מערכת הבריאות הציבורית, שירותי חירום, טלקומוניקציה, אנרגיה, בנקאות ופיננסים וכן הלאה. עם זאת, הנחת העמימות מבהירה את חוסר התכלית של היעד: מרבית יכולות הסייבר של מדינה, אם לא כולן, מנצלות תשתית אזרחית קריטית שמספקת גם פונקציות אזרחיות חשובות רבות, ותלויות בה. עד היום לא יצרה שום מדינה יכולות סייבר שהן נפרדות ומובחנות במלואן מרשתות ומתשתיות אזרחיות. במילים אחרות, פגיעה ביעדים "צבאיים" פירושה, למעשה, פגיעה ביעדים אזרחיים. נראה שהספרות המחקרית העכשווית עוקפת עובדה זו, וכתוצאה מכך עוסקת בחידה מדומה: ניסיון לכפות תשובה מדויקת תיאורטית על מציאות עם עמימות אמפירית. הוכחה נוספת להתעלמות זו היא הדרישה שחוקי מלחמת הסייבר **יאסרו** למעשה על פגיעה ביעדים שהם תשתית אזרחית טהורה – דרישה המציינת שגורמי סייבר חייבים לנסות לכבד את אמנות ז'נבה בדיוק כמו גורמים קונוונציונליים.[7] אולם במלחמת סייבר, תשתית אזרחית טהורה היא קטגוריה הדומה לפחיתת תשואה. לנוכח ההעצמה וההעמקה של המיזוג הצבאי והאזרחי, תשתית אזרחית טהורה תתגלה יותר כמיתוס מאשר כמציאות.

הכישלון לתת מענה למציאות מבנית זו דומה להדגשת יתר של הגורם הפועל (agency). ג'יימס לואיס (James Lewis) מהמרכז ללימודים אסטרטגיים ובינלאומיים (CSIS) מדגיש כיצד יכולה מדינה להפחית את הסיכונים לכל הצדדים באמצעות אכיפת סטנדרטים משותפים, בדומה למעבר מ'המערב הפרוע' לשלטון החוק.[8] יוג'ין ספאפורד (Eugene Spafford) מסכים עמו, כשהוא מציין כי אבטחת סייבר היא תהליך, לא טלאי, המחייב השקעה מתמדת לטווח הארוך לצד תיקון מהיר, שכן בלעדיו מדינות ימצאו עצמן מיישמות מאוחר מדי את הפתרונות לבעיות.[9] השניים נמנים עם השמות המכובדים והמבריקים ביותר בתחום חקר הסייבר. האזהרות שלהם אינן בלתי־רלוונטיות, אך הדגש על המדינה כסוכן פעולה, ובמקביל הפשל להכיר בהשפעה ובחשיבות של מבנה הסייבר הטבוע, מותירים פער רגיש בחשיבה האסטרטגית בנושא הסייבר. ההכרה בכך היא מכרעת, שכן מדינות מעמיקות במכוון את העמימות לצורכי יתרון אסטרטגי ויעילות כלכלית. לכן, האסטרטגיה אינה אמורה להתמקד בשאלה כיצד לאכוף הפרדה אזרחית/צבאית, אלא עליה לקבל את הנחת העמימות כמציאות לוגיסטית שיש להסתמך עליה.

כדי לקבל אישור אמפירי על חוסר התועלת בניסיון לתת מענה לבעיות אלה, אין צורך להרחיק מעבר לצבא ארצות־הברית במהלך שש השנים האחרונות: גנרל אלכסנדר (Alexander) ממפקדת הסייבר האמריקנית ציין שהושגה התקדמות, אך הסיכונים עדיין צומחים במהירות;[10] סגן־אדמירל מייקל רוג'רס (Michael Rogers), מפקד מפקדת הסייבר של הצי האמריקני, הודה בפני הקונגרס שלא הושג כל הסכם בין המפקדות השונות שיסדיר את דיני לוחמת הסייבר, אך הוא מקווה לראות התפתחויות חיוביות 'בשלב כלשהו בטווח הקרוב';[11] ואפילו הפנטגון הפיק דוח סייבר, שבסופו של דבר טען כי דיני הלחימה אכן חלים על מרחב הסייבר כשם שהם חלים על לוחמה מסורתית, אולם הודה שהמונחים הבסיסיים של 'פעולת מלחמה' ו'שימוש בכוח' עדיין **לוקים בהגדרתם** בתחום הסייבר.[12]

מלחמות מרות והליכה על חבל דק: דיון צבאי על פרמטרים של סייבר

בדיוק כמו חוקרים, קובעי מדיניות ודיפלומטים, גם הצבא מחויב בקביעות לגבש כללים נוקשים של התנהלות בסייבר, בדומה לכללי מלחמה קונוונציונלית.[13] כבר שנים אחדות תלוי ועומד תיקון לכללים הקיימים להתנהלות בעולם הסייבר.[14] נראה כי בעוד הצבא קיווה שקהילות החוקרים והדיפלומטים יוכלו לסייע, קהילות אלה עצמן קיוו לראות את הצבא מתווה את הדרך. חוסר הבהירות לגבי הנשיאה באחריות הוא עדות לבלבול הנוצר כל עוד הנחת העמימות הנוגעת למיזוג הצבאי/אזרחי אינה מטופלת.

גנרל אלכסנדר הצהיר כי בעת ניהול דיונים על כללי העימות בפעולות סייבר, ניסתה ארצות־הברית לעשות את הדבר הנכון.[15] אולם דיונים אלה נעו בין עמדות שרובן ככולן התעלמו מהעמימות המבנית העיקרית של תחום הסייבר. כתוצאה מכך, הצבא בזבז שש שנים בהבטחות להתקדמות שעתידה הייתה להגיע ולא התגשמה. אפילו הדוח הרשמי של הפנטגון תואר כ'חומק' מסדרה של שאלות מהותיות ובסיסיות חשובות, לרבות הצורך להגדיר מונחים כה בסיסיים כמו 'מלחמה', 'כוחות', ו'תגובה הולמת'.[16] נקודה זו מוזכרת לא על מנת ללעוג לצבא: לנוכח חוסר האונים של כל הצדדים הנוגעים בדבר בטיפול בהנחת העמימות, לצבא לא היה סיכוי רב להתקדם באופן מהותי במשימתו, ולהגדיר במדויק את הפרמטרים של פעולת סייבר.

כיצד, למשל, ניתן לצפות מ־USCYBERCOM לחבר את כל הנקודות, ולהיות הפוסק המתאים המכריע איזה אירוע הוא ראוי לפעולה, כאשר הוא עצמו מודה בקושי שיש לו אפילו לנסח מי בדיוק מרכיב את קבוצת לוחמי הסייבר שפועלת ומגִנה על רשתות הבית?[17] אם הסוגיות הנדונות לא היו כה חמורות ולא כל כך

מרחיקות לכת בנוגע לעתיד לוחמת הסייבר, זה היה כמעט משעשע. רק לאחרונה נראה היה שגופי הצבא הרלוונטיים מתחילים להפנים את הבעיות שנדונות כאן:

> למרות שננקטו כמה צעדים ראשונים ראויים לציון בהקמת מערך בינלאומי של נורמות סייבר – כפי שניכר בגופים דוגמת Convention on Cybercrime – כל מסגרת כלל־עולמית המפקחת על פעולות תגובה צבאית במרחב הסייבר צפויה לממש זאת בקצב איטי. אחרי הכול, כיצד ניתן להסב את כללי המלחמה, המבוססים על נוכחות פיזית של לוחמים וכלי נשק וטריטוריות ריבוניות, לעולם שבו ניתן לשגר באלפיות השנייה 'חיילים' ממספר רב של מדינות?[18]

הציטוט שלעיל תוחם לפחות את הדיון סביב אי־ההתאמה המובנית בין האופן שבו צפויה להתנהל מלחמה במרחב הסייבר, לבין האופן שבו התנהלו המלחמות בעבר. אולם עדיין, ציטוט זה מדגיש גורם פעולה על פני מבנה, ועוסק בהקמת מערך בינלאומי של נורמות סייבר, בעיקר על מנת לסמן רשמית את החלוקה בין נכסים צבאיים לאזרחיים, וכדי למתן פעולה שכבר מתבצעת. גישה זו יכולה להסביר מדוע מסמכי אסטרטגיה רשמיים מסיימים את דרכם כאוסף של אמירות שטחיות על האופן שבו ארצות־הברית מתכוונת להגן על עצמה. ראו לדוגמה את אסטרטגיית משרד ההגנה האמריקני לפעולה במרחב הסייבר, שפורסמה במחצית שנת 2011 :

> יוזמה אסטרטגית 1: יש להתייחס למרחב הסייבר כאל תחום מבצעי שיש לארגן, לאמן ולצייד, כך שמשרד ההגנה האמריקני יוכל לנצל את פוטנציאל מרחב הסייבר במלואו.
>
> יוזמה אסטרטגית 2: יש להפעיל תפיסות חדשות לתפעול הגנה, במטרה להגן על רשתות ומערכות מקומיות.
>
> יוזמה אסטרטגית 3: יש לחבור לשותפים נוספים במחלקות ובסוכנויות ממשלתיות וכן במגזר הפרטי, על מנת לבנות אסטרטגיית אבטחת סייבר כלל־ממשלתית.
>
> יוזמה אסטרטגית 4: יש לכונן קשרים איתנים עם בעלות־ברית של ארצות־הברית ועם שותפים בינלאומיים, על מנת לחזק אבטחת סייבר משותפת.
>
> יוזמה אסטרטגית 5: יש למנף את כושר ההמצאה של המדינה באמצעות כוח אדם ייחודי לסייבר וחדשנות טכנולוגית מהירה.

יש לנצל בצורה מלאה; להפעיל תפיסות חדשות; לחבור לשותפים; לכונן קשרים איתנים; למנף כושר המצאה – כל אלה סיסמאות נפלאות, אולם שום סיסמה אינה מלווה בחשיבה אסטרטגית חדשה ומפורשת שתוכל לגבש את היוזמות האמורות. כל ניסיון לאמץ אסטרטגיה קונוונציונלית חלקית ולאחר מכן לדחוק אליה את תחום הסייבר היה ויישאר פרויקט הנושא פירות דלים בלבד.

התמודדות עם העמימות: חשיבה אסטרטגית על המיזוג האזרחי/צבאי בסייבר

הצורך בגישה אסטרטגית חדשה מומחש בצורה הטובה ביותר בטיעונים של שניים מההוגים האסטרטגיים המכובדים ביותר, האחד צבאי והשני משפטי, שבמקרה גם מייצגים שתי עמדות מנוגדות בוויכוח הסייבר בנוגע לדיני לחימה (LOAC). שני הצדדים מתעלמים מהבעיה של מיזוג מבני צבאי/אזרחי בסייבר. דנלאפ (Dunlap) אמנם מסכים לצורך בשיפור, אך מאמין שעיקרי דיני הלחימה מספיקים על מנת לתת מענה לסוגיות החשובות ביותר של מלחמת סייבר.[19] נראה שבעיית ההבחנה בין מטרות צבאיות לגיטימיות לבין מטרות אזרחיות אינה מטרידה את דנלאפ כשהוא דן בהשפעה של החלת דיני הלחימה:

> דיני הלחימה מתירים 'פגיעות מקריות' באזרחים ובאובייקטים אזרחיים, כל עוד 'לא מדובר בהיקף רחב ביחס ליתרון הצבאי הישיר והממשי הצפוי'. בקביעה מהן פגיעות מקריות, נדרשים אסטרטגים של סייבר להביא בחשבון פגיעות שניתן להעריך במידה סבירה כי ייגרמו ישירות מהמתקפה. הערכה של השפעות 'מהדהדות' מדרגה שנייה או שלישית עשויה להיות שיקול מדיני נבון, אולם לא נראה שדיני הלחימה מחייבים כרגע ניתוח מתקדם מעין זה.[20]

הבחנה זו שעושה דנלאפ חשובה למדי לנוכח האקלים האינטלקטואלי הנוכחי: הוא הכניס לוויכוח את השימוש החיוני למדי בריאליזם, בכך שהוא מזכיר לאנשים שדיני הלחימה מעולם לא היו אסטרטגיה נטולת פגמים, שהגנה בצורה מושלמת על אזרחים ועל אובייקטים אזרחיים. אולם הבעיה שעולה מדבריו היא שחששותיו בנוגע להבחנה בין הצבאי לאזרחי מוטעים.

טיעונים אלה, שתומכים בדיני הלחימה, נבנו ביעילות סביב העובדה שמלחמת סייבר אינה אמורה להיות מושלמת בכל הקשור להגנה על אזרחים, כיוון שגם דיני הלחימה אינם עומדים בכך. אך טיעונים אלה מתייחסים כאל נתון לכך שמתווה כזה **אפשרי** בדרך כלל. אין זה סביר שמלחמת הסייבר תצליח בעתיד ליצור יכולת כזו, כיוון שהוכח זה כבר עד כמה הפונקציות הקריטיות, הנכסים, ספקי השירותים ושרשרות האספקה מסתמכים כולם בצורה ניכרת על רשתות ותעבורה אזרחיות.[21] בשל כך, אסטרטגיה חדשה צריכה להיות כזו שמונעת את השימוש בנשק סייבר בכללותו, משום שבעצם הפעלתו טמונה סבירות גבוהה לכך שייגרמו **בפועל** סיכון, נזק או אבדות לאזרחים. 'סטריליזציה' של השפעת נשק סייבר שכבר נעשה בו שימוש – באמצעות ניסיון לחייב בחירת מטרות – לא תצלח.

מחנה המתנגדים לדיני הלחימה שוגה באותה שגיאה כשהוא דן בשאלה, מדוע דיני הלחימה אינם יכולים להבהיר את מלחמת הסייבר:

> דיני הלחימה נועדו להבטיח שהצדדים בעימות יראו כמטרות את הלוחמים ולא את האזרחים, ואם אזרחים הופכים למטרות, עליהם להבטיח שגורמים כאלה

> יאבדו את מעמדם המוגן. כדי לקבוע האם מתקפות סייבר מבחינות כהלכה בין יעדים צבאיים לאזרחיים, נדרשת הבנה של ההבחנה.[22]

המחנה המתנגד נכשל בכך שהוא מאמין כי הבחנה כזו אפשרית בסייבר. הוא אינו רואה את ההשפעה האסטרטגית של הנחת העמימות, ובמקום זאת מתמקד בליקויים של דיני הלחימה ושאר הסכמים ונורמות עכשוויים. בקצרה, ההנחה שלו היא 'צרו חוקים טובים יותר ועולם הסייבר יציית להם'. אי לכך, מחנה זה רחוק אפילו יותר ממציאות הסייבר. בעיקרון, המחנה המתנגד נוקט גישה ליברלית יותר ביחס לעימות, משום שהיעד הסופי שלו הוא יצירת אווירה של אמון שיכולה למזער רמות גבוהות של אלימות ובגידה.[23] גישה זו מנוגדת למבנה הנוכחי והעתידי של מלחמת הסייבר אפילו יותר מזו של המחנה השני. שני המחנות מאמינים ביכולת לנטר, לפקח ולהגביל את מלחמת הסייבר לאחר תחילתה, כפי שנעשה לרוב במלחמה קונוונציונלית. זוהי תקוות שווא. הדרך הטובה ביותר להשיג יכולת לנטר, לפקח ולהגביל פעולת סייבר היא באמצעות אסטרטגיה שתחדיר פחד מראש, ולפיכך תגרום זהירות והיסוס. אסטרטגיות סייבר נוכחיות שמכוונות לאמון, להבחנה בין מטרות ולמזעור השפעה על מי שאינם לוחמים פשוט מתעלמות ללא הסבר מהאופן שבו מלחמת הסייבר מאורגנת, נבנית ומבוצעת.

הגישה הליברלית שולטת גם בקהילה המשפטית, ונשענת עליה רבות לצורך חשיבה אסטרטגית שנועדה לשלב פרויקטים משפטיים בתחום הסייבר:

> [פתרון אפקטיבי לאתגר הכלל־עולמי של מתקפות סייבר] לא יושג בידי מדינות יחידות הפועלות לבדן. הוא מחייב שיתוף פעולה כלל־עולמי. לפיכך פירטנו את מרכיבי המפתח של אמנת סייבר, כלומר, קיבצנו חוקים להגדרות ברורות של לוחמת סייבר ומתקפת סייבר, והצגנו קווים מנחים לשיתוף פעולה בינלאומי לאיסוף הוכחות ולתביעות פליליות – אשר יספקו פתרון מקיף וארוך־טווח לאיום הגובר של מתקפות סייבר.[24]

הסקירה שלעיל מציגה צד נוסף המתמקד במיתון הסיכונים ובהגבלת הנזק בתחום הסייבר **לאחר מעשה**. ללא קשר לעמדה פילוסופית, סדר־יום פוליטי או תבונה תיאורטית, דומה שכל צד שבוחן את בעיית הפרמטרים וההגדרות בתחום הסייבר שולל שיקולים של אסטרטגיה מונעת, המבוססת על הרתעה ועל שכנוע להימנע מפעולה. גנרל אלכסנדר, ראש מפקדת הסייבר האמריקנית, ציין את הצורך לסלול את נתיבי הדרך שבה יוכלו או לא יוכלו ממשלות ללכת, וכי סלילת הנתיבים היא השלב החיוני הראשון במתן מענה לאתגר של מתקפות סייבר.[25] המשותף לכל המחנות שנבחנו כאן הוא הנטייה לשלם מס־שפתיים לאסטרטגיה, ולאחר מכן להתמקד באופן בלעדי ב**פעולות לאחר מעשה** כדי להשיג התקדמות. אם ההתמקדות תמשיך להיות על פעולת הסוכן ולא על ליקוי מבני, ההתקדמות לא רק תואט, היא לא תתקיים.

ישנם ניצני התחלה בספרות, המעידים על ניסיון ראשוני להגדיר שינוי תודעתי זה ואת חשיבותו האסטרטגית. הם מתמקדים באופן שבו יש לפעול כדי שהיעד של מעצמות גדולות לא יהיה תקוות השווא לפתח מערכת הגנה מושלמת של הרתעת סייבר, אלא היכולת להחדיר בהדרגה הרתעה המבוססת על פחד הדדי מאיום של מתקפה. מעמדה של ארצות־הברית טוב יותר הודות להתרחבותה למדיניות פתוחה ושקופה, שחותרת ליצור הרתעה המבוססת על יעילות יכולות מתקפת הסייבר שלה.[26] נעשה גם ניסיון ראשוני, אם כי בקנה־מידה קטן אף יותר, להגדיר כיצד פועל כוח סייבר מרתיע למניעה, או כיצד נראית אסטרטגיה כזו. השאיפה היא שאסטרטגיית סייבר גלויה כזו תיצור אמינות לנשק וירטואלי ככזה שמפעיל השפעה משבשת מתגלגלת כה חזקה, עד כדי שלילת השימוש בו. המפתח יהיה בביסוס חשש סביר אצל היריב.

עקב הגילויים האחרונים על תולעת 'סטקסנט' ועל יעילות הווירוסים 'דוקו' **(Duqu)** ו'פליים' **(Flame)** – שסביר מאוד להניח כי התקדמו מעבר ליכולות סטקסנט – נשק סייבר צובר במהירות מוניטין של הפחדה, ולפיכך הרתעה באמצעות אסטרטגיית סייבר גלויה כבר אינה פנטזיה בלבד. זהו טיעון מאזן חשוב לפיתוח אסטרטגיה מקיפה ומלאה, שתאפשר עוצמת סייבר אמריקנית גלויה וסמויה גם יחד.[27] העיקרון הוא לגרום ליריב להאמין מתוך אינטרס עצמי רציונלי שהתנהגות טובה תימנע פגיעה מסיבית, והתנהגות רעה תגרור השלכות חמורות. באופן מעט אירוני, אפשר לומר שהמפתח לפיתוח אסטרטגיית סייבר גלויה של הרתעה מונעת כרוך בהסתמכות על אסטרטגיות ריאליסטיות של האסכולה הישנה, תוך התרחקות מהנורמות הריאליסטיות של אותה אסכולה ישנה ביחס ללוחמה קונוונציונלית. ספרות חדשה זו משפיעה על הנחת העמימות, משום שניתן לטעון כי שינוי תודעתי ואסטרטגי זה הוא ההתמודדות המפורשת ביותר עם 'דילמת דוקו': הדרך היחידה 'להתגבר' על העמימות היא להימנע מכניסה למצב עימות שמחייב להתמודד איתה. במילים אחרות, מציאות הסייבר הנוכחית, כמו גם העתיד הנראה לעין, הופכים אסטרטגיות שמסתמכות על פעולה **לאחר מעשה** לנחותות מטבען, בהשוואה לאסטרטגיות מונעות.

חשיבותה של 'דילמת דוקו'

הניתוח המוצג מצביע על ליקויים במאמצים הנוכחיים לגבש הגדרות ופרמטרים ברורים לפיקוח על כללי מלחמת הסייבר. הדגש שהושם כאן על קשיים מבניים מובְנים – כלומר, המיזוג הטבוע בין המגזר הצבאי לאזרחי בסייבר – מציג את ההשלכות החמורות הצפויות כתוצאה מאסטרטגיות שאינן מתמקדות במאמץ לעצור מראש פעולת סייבר. רק לאחרונה מתחילים להופיע ניתוחים משפטיים בודדים, שמציפים בעיות אלה:

> אין זה סביר שמדינה כמו ארצות־הברית תוכל לנקוט אמצעי הגנה נגד השפעתן של מתקפות על מטרות צבאיות באמצעות הפרדה בין יעדים צבאיים לבין אזרחים ואובייקטים אזרחיים במרחב הסייבר. זאת בשל התלות ההדדית הקיימת בין מערכות אמריקניות ממשלתיות ואזרחיות, כחלק מההסתמכות הממשלית המלאה־כמעט על חברות אזרחיות לצורכי אספקה, תמיכה ותחזוקה של יכולות הסייבר שלה... אומדנים של החלוקה היחסית עתידים להוכיח שקיים סיכון במיוחד במרחב הסייבר, בעוד התוצאות קשות יותר לחיזוי מאשר בעולם האמיתי: למתקפות פיזיות יש לפחות יתרון של התבססות על כללי הפיזיקה והכימיה. לדוגמה, כיוון שרדיוס הפיצוץ של פצצת חצי־טון הוא נתון ידוע, ניתן לדעת מראש ובוודאות מה יימצא מחוץ לרדיוס הפיצוץ ומה ייכלל בו. גבולות השגיאה ומתקפות הסייבר הרבה יותר רחבים ופחות מוּכרים...[מרבית הדוחות אינם מסבירים באיזה אופן] ניתן לכונן שותפויות ציבוריות־פרטיות אלה כך שיוכלו ליישם בצורה סבירה סוגיות של דיני לחימה, [והם] אינם נותנים מענה לשימוש הצפוי בהגנות אקטיביות מצד המגזר הפרטי.[28]

כפי שהודגם לעיל, סוגיה מבנית זו היא יותר מאשר סמנטיקה בלבד, היא כוללת הכול: מי מעורב במלחמת סייבר, מה ניתן להרוס במלחמה כזו, מי יכול להיחשב קורבן בעת מלחמת סייבר, ואפילו את השאלות הפילוסופיות והאתיות שיש לשאול על מלחמת הסייבר עצמה. 'דילמת דוקו' היא הפצרה להתרחק מיעדים בלתי־ניתנים להשגה ומחלומות אידאליסטיים, שמקורם בתקווה חסרת־שחר ליצור מלחמת סייבר סטרילית, בדומה להגבלות שנכפו על מלחמה קונוונציונלית. מלחמת סייבר לעולם לא תוכל להפוך לסטרילית באופן זה. משום כך, החשיבה האסטרטגית העכשווית ביחס לתחום הסייבר צריכה להכיר בכך שיש להפנות משקל רב יותר ל"הנחת העמימות", מאשר לבעיית הייחוס המוכרת.

הערות

1 Tom Leithauser, "Rules of War Should Apply to Cyber Conflict", *Cybersecurity Policy Report,* February 14, 2011.

2 Tom Gjelten,"Shadow Wars: Debating Cyber Disarmament", *World Affairs, 173;4,* November/December, 2010.

3 Ibid.

4 Aliya Sternstein, "Experts Recommend an International Code of Conduct for Cyberwar", *National Journal,* June 10, 2011.

5 Andrew Liaropoulos, "War and Ethics in Cyberspace: Cyber-conflict and Just War Theory", *European Conference on Information Warfare and Security, 177-XI,* (Reading, UK), July 2010.

6 Anatolin-Jenkins, Vida CDR, "Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?", *Naval Law Review*, *51:132,* 2005.

7 Don Tennant, "The Fog of (CYBER) War", *Computerworld, 43;16,* April 27, 2009.

8 James Fallows, "Cyber Warriors", *The Atlantic Monthly, 305;2,* March 2010.

9 Ibid.

10 John Curran, "Updated Rules for Cyber Conflict Coming Soon, Defense Officials

Say", *Cybersecurity Policy Report,* March 26, 2012.
11 Lolita Baldor, "Cyber Warriors", *Army Times,* August 6, 2012.
12 Gorman, Siobhan and Julian Barnes, "Rules for Laws of War: US Decides Cyber Strike Can Trigger Attack", *The Australian,* January 1, 2011.
13 Anonymous, "Military Ponders Cyber War Rules", *Los Angeles Times,* April 7, 2008.
14 Ellen Nakashima, "Pentagon Seeks to Engage Rules of Engagement in Cyber War", *The Herald,* August 10, 2012.
15 Ibid.
16 Ellen Nakashima, "Pentagon: Cyber Offense Part of Strategy", *The Washington Post,* November 16 2011.
17 Wesley Andrues, "What US Cyber Command Must Do", *Joint Forces Quarterly, Issue 59, 4th quarter,* 2010.
18 Ibid.
19 Charles Dunlap, "Perspectives for Cyber Strategists on Law for Cyberwar", *Strategic Studies Quarterly,* Spring 2011.
20 Ibid.
21 Erik Mudrinich, "Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem", *Air Force Law Review, 68,* 2012.
22 Michael Gervais, "Cyber Attacks and the Laws of War", *Journal of Law and Cyber Warfare, 30;2*, 2012.
23 Ibid.
24 Hathaway, Oona, et al, "The Law of Cyber-Attack", *California Law Review,* 2012.
25 Ibid.
26 Matthew Crosston, "World Gone Cyber M.A.D: How Mutually Assured Debilitation is the Best Hope for Cyber-deterrence", *Strategic Studies Quarterly,* Vol. 5, No. 1, Spring 2011.
27 Matthew Crosston, "Virtual Patriots and a New American Cyber Strategy: Breaking the Zero-sum Game", *Strategic Studies Quarterly*, Vol. 6, No. 4, Winter 2012.
28 Hannah Lobel, "Cyber War Inc: The Law of War Implications of the Private Sector's Role in Cyber Conflict", *Texas International Journal of Law, 47;3,* Summer 2012.

השימושים האסטרטגיים בעמימות במרחב הקיברנטי

מרטין ס׳ ליביקי

לעמימות אסטרטגית שמור מקום של כבוד במוסכמות המדינאות. חוסר הנכונות המכוונת של מדינות להצהיר על מעשיהן (או על מה שבכוונתן לעשות), בצד העדר הוכחה שהן עשו זאת משחררת מדינות אחרות. הן יכולות לטעון כי משהו נעשה, אך אם צורכיהן מכתיבים זאת, באפשרותן להעמיד פנים כי הדבר לא נעשה. דרגת הספק עשויה להשתנות: מספק מוחלט (איש אינו יודע מה קרה או מה עתיד לקרות) לספק קטן מאוד (לא "עובדים" על אף אחד). עם זאת, בכל אחד מהמקרים, מבצעי המעשה סיפקו עלה תאנה, שקוף ככל שיהיה, שמדינות אחרות יכולות לאמץ.

דוגמאות לעמימות אסטרטגית במרחב הפיזי

דוגמה אחת שכבר שנים שמור לה מקום של כבוד, היא סירובה של ישראל להודות (או להכחיש) שהיא מחזיקה בנשק גרעיני. לא יימצא פרשן ראוי לשמו המאמין באמת ובתמים שישראל אינה מחזיקה בנשק גרעיני. אך מאחר שישראל מעולם לא הצהירה שברשותה נשק גרעיני, מדינות אחרות חופשיות להעמיד פנים שישראל לא 'חצתה את הגבול' בתחום הגרעיני. מצב זה נוח למדינות שיהיו נתונות ללחץ של בני עמם להגיב בתוכניות גרעין משלהן במקרה שהמעמד הגרעיני של ישראל יֵצא לאור. מצב זה גם מסייע למדינות שלא היו יכולות לייצא פריטים מסוימים לישראל לו מעמדה הגרעיני היה גלוי יותר.[1] עם זאת, אין אף מדינה המתנהגת כאילו אין לישראל יכולת תגובה גרעינית.

עמימות דומה נוגעת לשימוש המשוער שעושה ארצות־הברית בכטב"מ (כלי טיס בלתי מאוישים) מסוג "פרדטור" ובטילי שיוט כדי לפגוע באנשי אל־קאעדה במדינות כמו תימן או פקיסטן. המדיניות הרשמית היא להכחיש את קיומן של

ד"ר מרטין ליביקי הוא מדען חבר בצוות הניהול הבכיר במכון ראנד, קליפורניה, ארצות הברית.

מאמר זה ראה אור לראשונה ב**צבא ואסטרטגיה**, כרך 3, גיליון 3, דצמבר 2011, עמ׳ 3–10.

טיסות כגון אלה. מנהיג תימן טען, שאלה היו מבצעים של תימן, מה שנשמע לא סביר, ורק פרשנים בודדים נפלו בפח והאמינו לטענות אלה. ואולם לפחות עד לאחרונה לא הודו ראשי המדינות האמורות בתקיפות שהתרחשו בשטחן, וכך לא נאלצו להתמודד עם הטענה בדבר פגיעה בריבונותן.

דוגמה אחרת היא מדיניות ארצות־הברית כלפי עצמאותה של טייוואן. ארצות־הברית הצהירה שהיא מתנגדת להכרזת עצמאותה של טייוואן וכן לכל ניסיון ליישב את עניין מעמדה של טיוואן בכוח. ארצות־הברית אינה מכירה בטייוואן כמדינה, ולפיכך אין לה הסכם סיוע הדדי איתה. לכן, נשאלת השאלה: האם במקרה שטייוואן תכריז על עצמאות וסין תחליט לכבוש את האי, ארצות הברית תתערב לטובתה של טייוואן? ברור שהאינטרס המובהק של ארצות־הברית הוא שסין תחשוב שזה אכן המצב כדי שלא תפתח במלחמה, וכמעט ודאי שהאינטרס של ארצות־הברית הוא, שגם טייוואן תחשוב שזהו המצב כדי שהיא עצמה לא תעודד את סין לפתוח במלחמה. הבה נניח שהסיכויים של התערבות ארצות־הברית משולים, פשוטו כמשמעו, להטלת מטבע, ונתפסים כך משני צדי המצָרים. בהתאם לכך, טייוואן עשויה להגיע למסקנה, שהערך הצפוי מהכרזת עצמאות הוא שלילי (הוא היה עשוי להיות חיובי אילו ידעה בוודאות שארצות־הברית תחוש לעזרתה) מאחר שארצות־הברית עשויה לא להתערב. בדומה לכך סין משיקולים שלה, עשויה להגיע למסקנה, שהערך הצפוי מפלישה וחציית המצָרים עלול להיות שלילי מכיוון שארצות־הברית עלולה לפעול. כל אפשרות עמומה פחות מזו עלולה לעודד צד זה או אחר לנקוט צעד טיפשי.

המרחב הקיברנטי מתאים לעמימות

מלחמה קיברנטית היא חשאית במהותה. כאשר פורצי מחשבים חודרים למערכת מחשב כדי לשבש את פעולתה, התוצאות הישירות הן על־פי־רוב בלתי נראות לעולם החיצוני. בהתאם לדרגת השיבוש במערכות האלה, גם התוצאות העקיפות עשויות להיות בלתי נראות לעין. תוצאות של מתקפת סייבר על רשת חשמל, הגורמת לכיבוי האורות, ניתנת לצפייה אפילו מהחלל; אבל בהעדר המשך חקירה וגילוי, לא יהיה ברור אם ההאפלה היא פועל יוצא של התקפה מכוונת, או של טעות אנוש, תוכנה לקויה, או (לעתים קרובות) של הטבע עצמו. גם אם יתברר שמערכת השתבשה בגלל התקפה, זהות התוקף עשויה להישאר אפופה במסתורין. לבסוף, אם עצם התקפת הסייבר וזהות מחולליה היו ברורים, מטרתה עשויה להיות מעורפלת ולא ברורה – אחרי הכול, מלחמה קיברנטית לבדה אינה יכולה להרוג איש, או אפילו להרוס יותר מדי (עיין ערך תולעת הסטקסנט – Stuxnet) ועוד פחות מכך לכבוש שטח או לשנות משטר (מלחמה קיברנטית אכן יכולה לאפשר שימושים אחרים בכוח, ושימושים אחרים אלה הם המוחשיים יותר). כמעט כל

הפריצות הקיברנטיות נועדו לגנוב מידע או לעשות שימוש במחשב המטרה (כמו ברובוט), ומעבר לכך להשאיר את המערכת כמות שהיא. אפשר לעצב התקפות כניסיונות להטעות בני אדם (למשל תמונות מכ"ם מסולפות) או את הציוד שלהם (ראו על תולעת הסטקסנט). במקרים האחרונים, המובן מאליו מטבע הדברים פועל כבומרנג; משעה שברור כי הצלחת להערים על מערכת, מנהלי המערכת אינם צפויים לאפשר לה לפעול כפי שפעלה בעבר.

האם תולעת הסטקסנט היא דוגמה יוצאת דופן?

אפשר היה לשער שמתקפת סייבר אשר שיבשה דבר מה בפועל עברה את השלב שבו הכול יכולים להצניע את קיומה. תולעת הסטקסנט התגלתה בחודש יוני 2010, ובספטמבר זוהתה מטרתה – מתקן גרעיני באיראן. החשדות המוקדמים ביותר סימנו את הכור בבושהר כיעד שלה,[2] אך איראן הכחישה שהכור ספג חבלה כלשהי. בתוך כמה שבועות זוהה מפעל הצנטריפוגות בנתנז כמטרת ההתקפה. הכחשות ראשוניות של איראן הופרכו בשלהי נובמבר 2010, ביום שבו חיסלו מתנקשים שני מדעני גרעין איראנים, וכאשר הודה אחמדינג'אד שהייתה תולעת שגרמה בעיות רבות, אך אלה תוקנו.[3] מהו הנזק הממשי שהסבה תולעת הסטקסנט לפיתוח הגרעין האירני? סטטיסטיקה של סבא"א (הסוכנות הבינלאומית לאנרגיה אטומית) מלמדת, כי ייתכן שהתולעת האמורה גרמה להתבלות מוקדמת של עשרה אחוזים מהצנטריפוגות של איראן, ולפיכך הקנתה ליוצרי התולעת כמה חודשי דחייה לכל היותר בלוח הזמנים המשוער שלפיו יהיה בידי איראן די חומר גרעיני לבניית הפצצה הראשונה שלה.[4] בדיווחים אחרים מצוטטים אישים בכירים, המתנבאים (נכון לינואר 2011) שהמועד המוקדם ביותר שבו איראן תוכל להרכיב התקן כזה הוא 2015, כלומר הושג עיכוב של כמה שנים.

רב הנסתר על הגלוי בכל הקשור לתולעת הסטקסנט (למעט מה שידוע שהיא הצליחה להשיג).[5] ראשית, לא ברור איך הצליחה התולעת לחדור למפעל ב־נתנז; דומה כי חשדות ולפיהם יוצרי התולעת קיבלו סיוע ביודעין או שלא ביודעין מקבלנים רוסים חיבלו ביחסי העבודה של האיראנים עם קבלנים אלה.[6] ומה שחשוב מכך – מי כתב את התולעת ומי שחרר אותה? האם היה זה אדם מסוים (התחכום שלה מרמז על אפשרות אחרת)? האם היו אלה ישראלים – כפי שאפשר לשער מכמה רמזים בקוד המקור – אך מי יידע אם רמזים אלה לא הושתלו כדי להטעות? האם היו אלה אמריקנים? האם מדובר בשיתוף פעולה – אמריקני־ישראלי?[7] האם היו אלה הסינים?[8] לנוכח העמימות הרבה, אין פלא שאיראן טרם הגיבה על האירוע הזה. גם סוריה לא הגיבה על ההתקפה על מה שנחשד כמתקן הגרעין שלה, ועיראק לא עשתה דבר חוץ מלהתלונן לאחר שהופצץ הכור שלה באוסיראק – ובשני המקרים הללו לא הייתה שום עמימות בנוגע למְבצעים. קשריה

האיתנים של איראן עם חמאס ועם חזבאללה מרמזים כי ייתכן שעמדו לרשותה כמה דרכים – שלא עמדו לרשותן של סוריה (בשנת 2007) או של עיראק (בשנת 1981) – להביע את חוסר הנחת שלה. יתרה מכך, איראן טרם עשתה "עניין גדול" מהתקרית, ואם לאחר חודשים של שתיקה והכחשות היא תראה בכך אקט של מלחמה, יהיה בכך משום תפנית של 180 מעלות.

יתרונות השימוש בתולעת הסטקסנט במקום בכוח אווירי לצמצום יכולתה הגרעינית של איראן, ברורים למדי (בהנחה שהתולעת אכן עשתה את מה שיוצריה ציפו): השפעה דומה, זריעת חוסר אמון בקרב קורבנותיה ואי־ודאות מי מבין הספקים או הציוד עדיין סובלים משיבושי התולעת, וכל זאת במידה פחותה בהרבה של גינוי (ואולי אף בהערצה כמוסה) ובפחות סיכונים אסטרטגיים מאלה הכורכים בהפעלת כוח אווירי.

שימושי העמימות

ההשערה המוצעת היא, שהתקפת סייבר המשמשת במקום שיטות קינטיות, יוצרת עמימות רבה יותר במונחים של תוצאות, מקורות ומניעים. לפיכך אם מתקפות סייבר פועלות בהצלחה – וסימן השאלה בעניין הזה הוא גדול – הן משנות את פרופיל הסיכון של פעולות מסוימות, כך ובדרך כלל בדרכים ההופכות אותן לחלופות מתאימות יותר. להלן כמה שימושים היפותטיים של מתקפות סייבר.

א. קורבן לתוקפנות בהיקף קטן עשוי להשתמש במתקפות סייבר כדי לבטא את אי־שביעות רצונו, אך הסיכון להסלמה קטן יותר לעומת זה הכרוך בתגובה פיזית. לדוגמה, בשלהי 2010 הפציצו כוחות צפון קוריאה אי בדרום קוריאה והרגו שני אזרחים ושני אנשי צבא. תגובה בדמות מתקפת סייבר, שנועדה לשבש מתקן תעשייה חשוב (אם מתעלמים מן העובדה שצפון קוריאה אינה ממוחשבת היטב ובעלת אפס חיבורי רשת לשאר העולם) הייתה עשויה להעביר את תחושת אי־שביעות הרצון של דרום קוריאה. לו רצתה צפון קוריאה להגיב היה עליה: (1) להודות שאחד ממתקניה נפרץ; (2) לנקוט צעדים שיוכיחו כי דרום קוריאה היא האחראית הבלעדית לכך (זו עשויה להיות ארצות־הברית או אפילו יפן, ואפילו סין). לחלופין, אם צפון קוריאה לא תגיב באופן פומבי, יש לה סיכוי טוב להגביל את מספר היודעים מדוע כמה ממתקניה חדלו מלפעול. תיאור זה מציג מאפיין חשוב נוסף של מלחמה קיברנטית, המעניק לה יתרון על פני לוחמה פיזית: אף־על־פי שהיותך מותקף עשוי להוות מקור לגאווה (תוכל לגלם את דוד לעומת האויב גוליית), העובדה שפרצו למערכות שלך פירושה שנכנסת למרחב הקיברנטי בלי לתת את הדעת על הגנה של מערכותיך. קורבנות איננה דבר הראוי להתגאות בו. לפיכך מומלץ למדינות היכולות להסתיר את העובדה שהותקפו לעשות זאת, וכך לשמור על כבודן – אך נתיב זה גם עושה את התגובה לאפשרית פחות. פתוחה

לפניהן הדרך להגיב באופן דומה, וכך מאבק של עין תחת עין שהחל בעולמות הפיזיים, עולה (או יורד) לעולם הקיברנטי. אך נתיב זה עשוי להיות בטוח יותר בכל ההיבטים לעומת הנחתת מכות פיזיות.

ב. מדינה עשירה בלוחמי סייבר עשויה להשתמש באיום בלוחמת סייבר להרתעה מפני הפיכתה למטרה אפשרית של אויביה. לדוגמה, באפשרותה של ישראל לאיים על איראן במתקפות סייבר אם תותקף על־ידי חזבאללה, ארגון בעל קשרים מוכחים עם איראן.[9] במצב עניינים שכזה, קיימת אפשרות שישראל לא תהיה מעוניינת לפרסם ברבים את האיום הזה. איום גלוי יאפשר לחזבאללה לכפות את רצונו על איראן בטענה שהוא מעוניין לתת ביטוי לסוג הפגיעה שתניע את ישראל לתקוף את איראן במרחב המדומה. אך יש מסלולים פרטיים להעברת האיום. יש היגיון באיום שכזה. הבעיה הרווחת בכל הנוגע להרתעת סייבר היא, שהייחוס של ההתקפה הפותחת מהווה בעיה, אך במקרה של התקפה פיזית – נניח, בדמות טילים של חזבאללה המשוגרים לעבר ישראל – יהיה קל מאוד לקבוע זאת. לחילופין, אף על פי שמדינה כמו איראן אינה עשויה בהכרח לחשוש מהתקפה ישראלית ישירה גם בתגובה להתקפה של חזבאללה, (התקפות שכאלה לא התממשו בשנת 2006, למשל), היא עשויה לחשוש ממתקפת־סייבר בהתחשב בעליונות הברורה של פורצי מחשבים ישראלים על פני עמיתיהם האיראנים. עליונות שכזו ממתנת (אם כי לא מבטלת) את החשש כי לאחר שהצהירה על הכוונה לבצע מתקפת־סייבר, לא יהיו לישראל מטרות נגישות באיראן. גם אם ההצלחה של מתקפה בודדה אינה ודאית, הסיכויים כי חלק מהן יצליחו ויגרמו נזק – טובים למדי. הפניית אצבע מאשימה של איראן כלפי ארצות־הברית לאחר מכן עלולה ליצור בעיה עבור ארצות־הברית, אך לעשות חיים קלים יותר עבור ישראל. הסלמה לאלימות איננה באמת אופציה עבור איראן בהתחשב בעליונותה של ישראל בתחום הלוחמה הקונבנציונלית (לפחות אם הקרב יהיה בסמוך לישראל). וליתר דיוק, כפי שצוין, איראן תיאלץ להודות כי המערכות שלה חובלו ולשכנע כי היא יודעת מי עומד מאחורי הפעולה. לבסוף, בעוד שישראל מרושתת יותר מאיראן, לאור יכולות הסייבר שלה, אולי לא יהיה בכך די כדי להטות את הכף לטובתה של איראן היה וזו תשיב מלחמה.

ג. מתקפות סייבר עשויות לשמש מדינה אחת כדי להשפיע על תוצאות סכסוך במדינה אחרת בלי שתצטרך להתחייב לכך בגלוי או אפילו במשתמע. לדוגמה, מלחמת האזרחים בלוב – אילו היה צבא לוב מחובר לאינטרנט באופן כזה שמתקפות סייבר היו יכולות להשפיע על ביצועיו,[10] אזי באמצעות נטרול כוחות הממשל המרכזי, היו פורצי מחשבים מן המערב יכולים להטות במידה ניכרת את כיוון המלחמה. אילו המורדים היו מנצחים, היו ממשלות המערב נשכרות מכך. אפשר שלא היה באפשרותם של כוחות המורדים לדעת שהם קיבלו סיוע, וייתכן

שהדבר היה רק לטובה (בייחוד אם מדובר במורדים בעלי נטייה ג'האדיסטית מבין המורדים בלוב, המקדמים בברכה את התערבות הכוחות האמריקניים). אפשרות אחרת היא לפזר רמזים (למשל, אם יכולת מסוימת תשותק מחר, אתם תדעו את הסיבה לכך). לחלופין, אילו ידה של הממשלה הייתה על העליונה, היא הייתה עשויה לחשוד שכוחות המערב חיבלו במערכות המידע שלה, אך הייתה מתקשה להוכיח זאת. היא הייתה עשויה להתלונן, אך היה צפוי מלוב להאשים את המערב במגרעותיה, ואז לתלונותיה, בהעדר הוכחות, לא היה ניתן לייחס חשיבות כלשהי. ליתר דיוק, היא לא הייתה רוצה לטעון כך אם רצונה היה להעמיד פנים לאחר מכן שאין לה כל סיבה לראות שוב במערב אויב. לו מלחמת האזרחים הייתה נמשכת, יכול היה המערב להעמיד פנים שהוא לא נתן סיוע לפני כן, וממילא גם לא התחייב להגדיל את הסיוע שלו (גם אם נשלחו רמזים למורדים, הם היו מתקשים מאוד להוכיח לאחרים שפורצי מחשבים מן המערב הציעו להם סיוע, שכן בשונה מהממשלה, אין לצפות שתהיה להם גישה למחשבים שחובלו). הבעיה הגדולה ביותר הטמונה בהצעת סיוע שכזה היא האפשרות של חשיפה, אבל אם היעד למתקפות שרוי בסכסוך עם שאר העולם, אין לצפות שהוא יזכה לסיוע ממשי באיתור התוקפים. סיוע שכזה הוא כה מושך (לפחות מנקודת המבט של נותן הסיוע), שהוא עשוי להפוך למאפיין שגרתי – משני הצדדים – בכל סכסוך שבו התוצאה אינה ודאית, ולרשתות יש חשיבות רבה במה שנוגע ליכולות לחימה. יודגש שוב, כי הודאה שהמערכות שלך נפרצו כרוכה תמיד במידה זו או אחרת של מבוכה.

ד. התקפות סייבר אינן צריכות להיות מכוונות בהכרח רק כלפי אויבים, אף־על־פי שהסיכונים שביצירת אויבים חדשים במקרה של חשיפת מקור המתקפות הם ברורים. דמיינו לעצמכם מצב שבו שתי מדינות ניטרליות מתקדמות באיטיות לעבר מלחמה. נניח שמדינה שלישית מסוגלת לגרום שיבושים במערכות המעקב, השליטה והבקרה של שני הצדדים, שיטילו ספק בדבר הצלחתן של שתי המדינות להתגבר על הסכסוך ביניהן. אם מערכות יוצאו מכלל שליטה, צפוי שכל אחת מהמדינות הללו תאשים תחילה את האחרת במקום לתלות את האשמה בצד שלישי. סביר ביותר שההנחה הראשונית – שהנזק נעשה על ידי הצד השני – תשפיע על התגובות ועל הפעילויות שלהן. יתר על כן, סיכוי גבוה הוא שהאשמה כזאת לא תוטח בפומבי עקב המבוכה הכרוכה בכך. עם זאת, תחבולות שכאלה עלולות להוביל מדינות למלחמה אם אחד הצדדים ישכנע את עצמו, למשל, שמתקפות הסייבר שמשגר כלפיו הצד האחר הן בגדר צעד מקדים להזזת כוחות מידית, או שהן מעידות שכוחות האויב אינם פרוסים במערך מסוים בלא סיבה.

ה. עמימות עשויה להועיל במדיניות הצהרתית, כזו המפרטת כיצד המדינה תגיב על מתקפת סייבר כנגדה. לעמימות יש חסרונות ויתרונות כאחד. החיסרון

הוא, שאחרים עשויים לחשוב שהם יכולים להתחמק מאחריות לביצוע התקפות שהם היו נמנעים מביצוען לו היה ברור להם שאלה יגררו פעולות תגמול. היתרון הוא, שסביר להניח שמדינת המטרה לא תרצה לתקוף בחזרה, בייחוד אם היא חוששת ליחס לעצמה את ההתקפה. מדינה הנמנעת מתקיפת־נגד מכיוון שאינה בטוחה, לא תאבד ממעמדה בעיניה שלה – ייחוס המעשה לצד מסוים הוא באמת משימה קשה. עם זאת, אם התוקף (ואחרים) יגיעו למסקנה שהמדינה האמורה ידעה מי התוקף אך העמידה פנים שאינה יודעת, מחשש להתלקחות מלחמה בהיקף מלא, אזי כל איום בנקמה מצדה יישמע לא אמין. אם מדינה ממהרת להבטיח פעולות תגמול בתגובה על מתקפות סייבר ואינה יכולה לעמוד בהבטחותיה, גם יכולתה לממש את איומיה האחרים, תוטל בספק.

מסקנות

העמימויות הטקטיות הרבות של לוחמת הסייבר מחזקות אסטרטגיה המבוססת על עמימויות אסטרטגיות. ייתכנו מקרים רבים שמדינה תוקפנית אינה מעוניינת לפרט מה היא עשתה. אפילו מדינת המטרה, במקרים מסוימים, עשויה להגיע למסקנה שלהעמיד פנים שלא הותקפה (אפילו אם עליה להעלים עין מהראיות) עדיף בעבורה מניסיון להבהיר עניינים.

ואולם יש גם חיסרון בעמימות אסטרטגית. מדינות עשויות ליטול על עצמן, שלא בדין, את הזכות לגרום סוגים שונים של נזקים במרחב הקיברנטי, בהניחן כי לעולם לא יידרשו לשאת באחריות על מעשיהן.. לעתים אין בכך הצדקה, והמדינה מרמה רק את עצמה; ואפילו אם יש הצדקה באי־לקיחת אחריות, היא מספקת לפורצי המחשבים דרגה של חופש שההיסטוריה מלמדת שהיא מסוכנת בפני עצמה.

הערות

1 בניגוד לכך היה צורך בחקיקה בשנת 2006, שתאפשר לארצות־הברית לשתף טכנולוגיה אזרחית עם הודו, שבדומה לישראל אינה חתומה על האמנה לאי־הפצת נשק גרעיני, אבל בשונה מישראל, היא מעצמה גרעינית מוצהרת. ראו: Peter Baker, "Signs India Nuclear Law: Critics Say deal to Share Civilian Technology could Spark Arms Race," Washington Post, December 19, 2006. www.washingtonpost.com/wp-dyn/content/article/2006/12/18/AR2006121800233.HTML

2 Robert McMillan, IDG News, "Was Stuxnet Built to Attack Iran's Nuclear Program?" taken from *PCWorld*, September 21, 2010.

3 William Yong, Alan Cowell, "Bomb Kills Iranian Nuclear Scientists," *New York Times*, November 30, 2010.

4 Joby Warrick, "Iran's Natanz nuclear facility recovered quickly from Stuxnet cyberattack," *Washington Post*, February 16, 2011. See also the report by the Institute for Science and International Security, http://media.washingtonpost.comqwp-srv/world/documents/stuxnet_

update_15Feb2011.pdf

5 הדבר הברור ביותר על תולעת הסטקסנט הוא אופן פעולתה מכיוון שהתולעת נתפסה "בחיים" כביכול, בטרם יכלה להשמיד את עצמה (פעולה שהיה עליה לעשות במקרה שלא יעלה בידה למצוא התקן לוגי מסוים ניתן לתכנות, שעמד בפרמטרים מסוימים קבועים מראש, הקשורים לסוג מסוים של צנטריפוגה).

6 www.economist.com/blogs/babbage/2010/09/stuxnet_worm

7 William Broad, John Markoff, David Sanger, "Israel Tests on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, January 15, 2011.

8 Jeffrey Carr, "Stuxnet's Finnish-chinese Connection", December 14, 2010, www.blogs.forbes.com/firewall/2010/12/14/stuxnets-finnish-chinese-connection/

9 משקיפים רבים חולקים על האפיון של חזבאללה כבובה של איראן. עם זאת, יש הבדל בין חזבאללה הפועל אך ורק בהתאם להוראות מאיראן, לבין מצב שבו לאיראן יש השפעה מספקת על חזבאללה כדי להניאו מלנקוט פעולות לא חכמות.

10 במאמר רב השפעה, שסקר את האפשרויות של התערבות המערב בלוב נזכר הנושא של לוחמה אלקטרונית בדמות שיתוק התקשורת, אך לא צוין דבר בנוגע ללוחמת סייבר:
Thom Shanker, "U.S Weighs Options, on Air and Sea," New York Times, March 6, 2011,
http://www.nytimes.com/2011/03/07/world/middleeast/07military.html

מבט בינתחומי על אתגרי הביטחון בעידן המידע

יצחק בן־ישראל, ליאור טבנסקי

מבוא

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

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

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

מאמר זה ראה אור לראשונה ב**צבא ואסטרטגיה**, כרך 3, גיליון 3, דצמבר 2011, עמ' 19–32.

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

הקדמה עיונית

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

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

טבלה 1: שלושת הגלים – לפי טופלר

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

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

שלושת העולמות של פופר

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

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

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

כלכלת עידן המידע

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

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

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

התמודדות אינטלקטואלית עם עידן המידע בתחום הביטחון הלאומי

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

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

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

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

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

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

המרחב הקיברנטי

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

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

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

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

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

טבלה 3 : מאפייני המרחב הקיברנטי ונקודות תורפה העולות מהם

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

מלחמת מידע ללוחמה קיברנטית

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

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

טבלה 4: נושאים הנכללים תחת הכותרת לוחמת מידע

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

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

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

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

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

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

התקפה והגנה במרחב הקיברנטי[21]

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

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

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

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

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

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

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

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

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

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

סוגיות מרכזיות בלוחמה קיברנטית

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

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

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

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

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

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

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

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

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

סיכום

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

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

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

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

הערות

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

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

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

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

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

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

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

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

National Defense University Press, 1995).

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

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

11 ראה לעיל על המושג מבית מדרשו של קרל פופר.

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

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

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

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

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

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

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

19 ראה טבלה 2 לעיל.

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

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

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

ברית המועצות, גרמה לפיצוץ אדיר בסיביר ב־1982
W. K. Clark and P. L. Levin, "Securing the Information Highway: How to Enhance the United States' Electronic Defenses," *Foreign Affairs,* Vol. 88, No. 6 (2009).

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

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

25 דיון מפורט בנושאים הללו חורג מגבולות המאמר.

26 "ניסוי אורורה" שנערך במעבדות הלאומיות באיידהו, ארצות הברית.
Lewis, James Andrew, "Thresholds for Cyberwar." Washington, DC: Center for Strategic and International Studies 2010.

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

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

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

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

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

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

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

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

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

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

לוחמה קיברנטית והרתעה: מגמות ואתגרים במחקר

אמיר לופוביץ

מבוא

בשנים האחרונות מספר הולך וגדל של חוקרים הרחיבו את הדיון באסטרטגיית ההרתעה כדי לבחון התמודדות עם מגוון של איומים "חדשים". בשונה מתקופת המלחמה הקרה שבה התמקד המחקר בהרתעה בין מדינות, בין מעצמות ובהרתעה גרעינית, אנו רואים בשנים האחרונות – ובייחוד מאז פיגועי ה־11 בספטמבר 2011 – מחקרים רבים הבוחנים את אסטרטגיית ההרתעה כלפי איומים נוספים, כמו טרור, מדינות סוררות וכלפי הרתעה בסכסוכים אתניים. למחקרים אלה יש כמה מאפיינים משותפים: הם מתבססים ברובם על ניסיון לבחון את רלוונטיות התנאים להצלחת הרתעה כפי שפותחו בהקשר של המלחמה הקרה, והם שמים דגש חזק למדי על המלצות מדיניות (policy oriented), ובעיקר על המלצות הנוגעות להתמודדות עם האתגרים הניצבים לפני ארצות־הברית.[1] מאפיינים מחקריים אלה בולטים מאוד גם בדרך שבה התפתח הדיון בקשר שבין הרתעה לבין לוחמה קיברנטית.[2] כך, רבים מהמחקרים העוסקים באסטרטגיית ההרתעה ולוחמה קיברנטית, יוצאים מנקודת המבט האמריקנית ובוחנים את האפשרות של ארצות־הברית ליישם אסטרטגיה של הרתעה כדי למנוע התקפות קיברנטיות עליה, או את הדרך שבה ארצות־הברית יכולה להשתמש בלוחמה הקיברנטית כדי להרתיע מגוון של איומים אותם היא מבקשת למנוע.[3]

ממחקרים אלו עולה, כי האפשרות להרתיע התקפות של לוחמה קיברנטית היא מוגבלת בכל אחד מהממדים הדרושים להפעלה מוצלחת של אסטרטגיה זו: הימצאות היכולת (אמצעי נשק), אמינות האיום והאפשרות להעביר את המסר המאיים למאתגר הפוטנציאלי.[4] עם זאת, יש כמה גורמים העשויים בתנאים מסוימים לשמש בסיס להרתעה מוצלחת גם של לוחמה קיברנטית. במאמר זה אסקור את ספרות המחקר ואציע כיוונים להמשך המחקר בסוגיות האמורות.

ד"ר אמיר לופוביץ' הוא מרצה בחוג למדע המדינה, אוניברסיטת תל־אביב

מאמר זה ראה אור לראשונה ב**צבא ואסטרטגיה**, כרך 3, גיליון 3, דצמבר 2011, עמ' 41–52.

בחלק הראשון של המאמר מוצגים התנאים להצלחת אסטרטגיית ההרתעה. בחלק השני נסקרים הטיעונים המרכזיים שהוצגו בנוגע לקשיים להפעיל הרתעה מוצלחת נגד לוחמה קיברנטית לגבי כל אחד מן התנאים הללו. החלק השלישי עוסק בכמה גורמים העשויים לחזק את ההרתעה כנגד לוחמה קיברנטית, ובמספר יתרונות וחסרונות שלהם. בחלק האחרון אצביע על החשיבות להמשיך את הדיון בקשרים שבין הרתעה ולוחמה קיברנטית, ואציע כיוונים אפשריים למחקר ולחשיבה בנושא.

התנאים להצלחת הרתעה

שחקנים יכולים לנסות לגרום ליריבם להימנע מפעולה לא רצויה במגוון דרכים. האסטרטגיה של הרתעה על־ידי איום בענישה (deterrence by punishment) היא אחת הנחקרות ביותר שבהן. סוג זה של הרתעה זכה למספר רב של ההגדרות,[5] כשביניהן הגדרתם של גורג׳ וסמוק זכתה לשימוש נרחב. לטענתם, הרתעה היא היכולת לשכנע יריב (פוטנציאלי) כי המחיר שהוא ישלם עקב ביצוע הפעולה הלא רצויה יעלה על כל רווח אפשרי.[6] סוג זה של הרתעה שונה מ**הרתעה על־ידי** מניעה (deterrence by denial),[7] המבוססת על הניסיון לשכנע תוקפן אפשרי שעליו להימנע מהפעולה מאחר שלא יצליח להשיג את מטרותיו.[8] המושג של הרתעה גם שונה מהמושג אכיפה (compellence), המבוסס על שימוש באיומים כדי לגרום ליריב לבצע פעולה, בעוד הדגש בהרתעה הוא כאמור לגרום ליריב להימנע מביצוע הפעולה הלא רצויה.[9]

סוגיה מרכזית שעסקו בה חוקרים שבחנו את אסטרטגיית ההרתעה על־ידי איום היא התנאים שבהם היא עשויה להצליח, כלומר לגרום ליריב פוטנציאלי להימנע מאתגור המגן. המחקר, שהתפתח ברובו בתקופת המלחמה הקרה ועסק בהרתעה בין מעצמות־העל, עמד על שלושה תנאים מרכזיים: יכולות המגן, אמינות האיום והעברת המסר של האיום למאתגר.

תנאי ראשון בכדי שהרתעה על־ידי איום בענישה תפעל, הוא שהמגן יוכל לגבות מחיר מהשחקן המאתגר. לא מפתיע אפוא שמחקרי ההרתעה התפתחו מאוד בעידן הגרעיני מאחר שנשק זה מאפשר להבהיר היטב את המחיר של מלחמה עתידית. הנשק הגרעיני נתן למנהיגים "כדור בדולח", שאפשר להם לראות את תוצאות המלחמה הגדולה הבאה, ולכן לנקוט משנה זהירות בהתנהגותם.[10] עם זאת חשוב להדגיש, כי אין מדובר רק ביכולת לא קונבנציונליות, וגם אמצעים קונבנציונליים עשויים לשמש לגביית מחיר ממאתגר.[11] יתרה מכך, חלק חשוב מממד היכולת הוא אמצעי העברה שיש בידי המגן, למשל מטוסים, טילים ואפילו כבישים או כלי רכב העשויים להיות חלק מנדבך היכולת בהקשר של הרתעה.

תנאי שני להצלחת הרתעה הוא אמינות האיום. כדי שאיום ההרתעה יהיה אפקטיבי, השחקן המגן צריך להיות נכון להשתמש באמצעים שברשותו. חוקרים הציגו מגוון גורמים העשויים להגביל נכונות זאת, למשל דעת קהל פנימית או בינלאומית, או אפילו יכולת ההרתעה של היריב עצמו (השחקן המאתגר).[12] המשותף לגורמים אלה הוא, שהם מעלים, כל אחד בדרכו, את המחיר של הפעולה ומקטינים את האמינות של השחקן להוציא לפועל את האיום אם יידרש לכך.[13]

התנאי השלישי הוא העברת המסרים למאתגר בדבר שני התנאים הקודמים — היכולות והכוונות. כלומר, על המאתגר להיות מודע לאמצעים שיש בידי השחקן המגן ולנכונותו להשתמש בהם. יש הטוענים שתנאי זה הוא החשוב ביותר, כפי שרמזו לכך חוקרים שפיתחו את הגישות הפסיכולוגיות להרתעה. לטענתם, לתפיסות ולעיוותי תפיסה של מקבלי החלטות יש השפעה ישירה על הצלחת הרתעה.[14] במובן זה, מה שחשוב זה לא היכולות של השחקן המגן וכוונותיו, אלא כיצד אלו נתפסים בעיני המאתגר הפוטנציאלי.

לבסוף, אסטרטגיית ההרתעה עשויה לשמש למניעת סוגים שונים של איומים. לכן קשה לדון באופן אחיד בתנאים להצלחת הרתעה, שכן אלו צריכים להיות מותאמים לא רק לשחקן המאתגר, אלא גם לסוג הפעולה שמנסים להניא אותו מלבצע. למשל, בעוד נשק גרעיני עשוי להיות אפקטיבי בהרתעה מפני מתקפה כוללת ("הרתעה כללית"), מידת יעילותו תהיה נמוכה יותר כלפי איומים מוגבלים יותר.[15]

הרתעה ולוחמה קיברנטית – הקשיים בהרתעה

חלק גדול מן המחקרים שבחנו את אסטרטגיית ההרתעה בהקשר של לוחמה קיברנטית, ביקשו ליישם את התיאוריות של המלחמה הקרה בכל הנוגע להצלחת ההרתעה. חוקרים בחנו את התנאים המרכזיים להצלחת הרתעה שהוצעו בספרות (ונידונו בחלק הקודם): יכולת המגן, אמינות האיום ותקשורת, כלומר האפשרות להעביר אל המאתגר את המסר בדבר היכולות ואמינות האיום. מרבית החוקרים סבורים על סמך בחינת התנאים האלה, שאסטרטגיית ההרתעה צפויה להיכשל לנוכח האיומים שיוצרת לוחמה קיברנטית.[16]

היכולת

קושי מרכזי בהרתעת לוחמה קיברנטית נובע מכך שסוג לוחמה זה מאפשר גם לשחקנים חלשים להעתיק את העימות למרחב שבו יוכלו למקסם את רווחיהם ובמידת סיכון נמוכה. למעשה, ככל ששחקן מפותח יותר מבחינה טכנולוגית, כך הוא פגיע יותר להתקפות של לוחמה קיברנטית.[17] גורם זה מקטין את אפשרות התגמול, ולכן את היכולת לבסס איום הרתעה אמין. כך למשל, קשה מאוד להרתיע

שחקנים, ובייחוד יחידים, שאין ברשותם מערכות מידע משל עצמם הניתנות לאיום בפגיעה בהן.[18] בעיה זו באה לידי ביטוי גם בהתמודדות עם מדינות שמידת ההתבססות שלהן על מערכות מידע היא נמוכה. במצבים כאלה האפשרות של איום אפקטיבי באמצעים של לוחמה קיברנטית בלבד היא מוגבלת.

האמינות

בעיה שנייה בהרתעת איומי לוחמה קיברנטית היא אמינות המגן. לפגיעות המגן עשויה להיות השפעה המגבילה את נכונותו להפעיל את יכולותיו עקב חששו כי תגמול עלול להוביל להסלמה. הבעיה של המגן היא, שהסלמה כזאת עלולה להיות מסוכנת לו יותר מאשר למאתגר, ועל כן עלול לגדול חוסר האמון של המאתגר בנכונותו של המגן לפעול.[19] הבעיה אף מועצמת מכך, שעל־פי־רוב לצד החלש השוקל שימוש בלוחמה קיברנטית יש חסמי כניסה נמוכים (low entry costs).[20] במילים אחרות, העלויות של מאתגר פוטנציאלי לעשות שימוש באמצעים של לוחמה קיברנטית הם במקרים רבים נמוכות, מה שמגדיל עוד את הקשיים בהצגת האיום ההרתעתי הנדרש כדי למנוע פעולה כזאת.

גם דעת קהל פנימית ובינלאומית עשויה להגביל את אמינות איום התגמול עקב המאפיינים של הלוחמה הקיברנטית. במצבים שיהיה קשה לבסס את זיהוי מקור הפגיעה (כפי שיתואר בהמשך),[21] יהיו מגבלות גם על היכולת להפעיל תגמול שיגרום נזק.[22] מגבלות אלה יכולות להיחשב בעיני מאתגר פוטנציאלי למערערות את אמינותה של ההרתעה. וכך תוקפן פוטנציאלי, המעריך כי קטנים הסיכויים שהמגן יממש את איומיו בגלל נזק שעשוי להיגרם לו עקב כך, תוקפן כזה יהיה נכון להסתכן ולפעול.

העברת האיום

הבעיה השלישית נובעת מהקושי של המגן להעביר למאתגר את המסר בדבר יכולותיו ובדבר אמינות התגובה שלו. מלבד הבעיות הבסיסיות בנוגע לכל אחד מן ההיבטים הללו, שתוארו לעיל, מאתגרים יכולים להיות לא רק אנונימיים אלא אפילו יחידים, שפעמים רבות אין להם כתובת פיזית הניתנת לזהוי.[23] כך למשל, לטענת ליביקי, עד היום לא לגמרי ברור מה המקור להתקפה על שרתי האינטרנט של אסטוניה בשנת 2007, והאם הייתה זו פעולה מכוונת מלמעלה של ממשלת רוסיה, כפי שטענו גורמים אחדים שבדקו את הנושא.[24] מקור הפגיעה יכול להיות מדינה אחרת, ארגונים או יחידים הפועלים בתוך מדינה אחרת, וכן ארגונים או יחידים הפועלים בתוך גבולות המדינה שאותה רוצים לתקוף. למעשה, מצב זה מבטא את הטשטוש הקיים בין פשיעה, טרור ולוחמה.

יתרה מכך, לצורך הרתעה לא מספיק זיהוי בדיעבד של הגורם המאתגר, אלא נחוץ זיהוי שלו מבעוד מועד, בטרם התקפה, כדי שיהיה אפשר להפנות אליו את האיום המרתיע. זוהי סוגיה מרכזית, שכן הרתעה מבוססת כאמור על כך שהמאתגר הפוטנציאלי יהיה מודע מראש ליכולתו של המגן ולנכונותו להפעיל את האמצעים שבידו. ואולם אם המגן מתקשה לזהות את מקור הפגיעה לאחר התרחשותה, קל וחומר שיתקשה בכך בטרם פגיעה. יתרה מכך, גם הפתרון של הצגת איומים כלליים שנועדו להקיף טווח רחב למדי של שחקנים שהמגן מעריך כמי שעלולים לנסות ולפגוע בו הוא מוגבל. זאת מכיוון שההרתעה יעילה יותר במקרה שהאיום, גם אם אינו מפורש לגמרי, מופנה לשחקן ספציפי ולא לשורה אנונימית ולא מוגדרת של שחקנים או סוגי שחקנים העלולים לנסות ולאתגרו.[25]

קושי אחר הקשור ישירות להעברת המסרים למאתגר נוגע לשאלת האמצעים להעברת מסרי האיומים לתוקף הפוטנציאלי.[26] קושי זה מתעצם משום ריבוי השחקנים היכולים ליצור איומים. שלא כמו בתקופת המלחמה הקרה, שבה מספר היריבים (שהיו מדינתיים) היה מוגבל ויכולותיהם היו ברורות למדי, בעידן המידע יש ריבוי של תוקפים אפשריים, מה שמקטין את האפשרות להציג הרתעה יציבה ואמינה.[27] במילים אחרות, בתקופת המלחמה הקרה — ובעימותים בין־מדינתיים מסורתיים בכלל — היריב היה ידוע, ולכן היה ברור מיהו הנמען של המסר ההרתעתי. מנגד, ריבוי האיומים של הלוחמה הקיברנטית וגיוונם יוצר זירה מורכבת יותר לפעולה, שבה לא ברור לגמרי כיצד יש להעביר את המסר המרתיע.

הרתעה ולוחמה קיברנטית – לעתים ההרתעה אפשרית

למרות הקשיים שצוינו, אין לפסול לגמרי את האפשרות שהרתעה כנגד לוחמה קיברנטית עשויה בתנאים מסוימים להצליח, חלקית לפחות. למשל, חוקרים הדגישו כי האיום בתגמול אינו חייב להיות מוגבל לחלל הקיברנטי, אלא יכול להיעשות באמצעים מסורתיים יותר. כך אם מדינה מאיימת לפעול באמצעים של לוחמה קיברנטית, האיום ההרתעתי כלפיה יכול להתבסס על קשת רחבה של אמצעים המצויים ברשותה של המדינה המבקשת להתגונן. איומים כלכליים, פוליטיים, דיפלומטיים או צבאיים עשויים להיות יעילים בהרתעת מדינה הרוצה להפעיל לוחמה קיברנטית נגד מדינה אחרת. בדומה, גם עם איומים שמציבים יחידים או ארגוני טרור המבקשים להפעיל לוחמה קיברנטית, יכולות מדינות – כפי שהציעו חוקרים (ואף כמה מקבלי החלטות) – להתמודד בעזרת אמצעי הרתעה שאינם מן המרחב הקיברנטי. למשל, איומים באמצעות מערכת המשפט (הפנימית והבינלאומית), ובאמצעות ארגונים לביטחון פנים, זאת למשל בשילוב עם איומים צבאיים מסורתיים.[28] באופן זה, אם יש שחקנים המעריכים שישיגו רווחים מהסטת העימות לחלל הקיברנטי, שבו הם נהנים מיתרונות, השחקנים

העלולים להיפגע יכולים לפעול בזירות הנוחות להם ולא להגביל את עצמם לתגובה במרחב הקיברנטי בלבד.

אמצעי אחר הוא הרתעה על־ידי מניעה. היתרון הטמון באסטרטגיה זו הוא אפשרות ביסוסה על אמצעים הגנתיים, וכך לא רק להניא יריב מפעולה, אלא גם לתת פתרון במקרה שהמאתגר החליט לתקוף. יתרה מכך, לדברי מורגן, התבססות על אמצעים הגנתיים מגוונים, שיסייעו לביסוס הרתעה על־ידי מניעה, יוכלו לסייע לזהות את התוקפן ולחזק את היכולת להפעיל תגובת־נגד, מה שעשוי לחזק גם את ההרתעה באמצעות ענישה.[29] עם זאת, הפעלת אסטרטגיה זו כרוכה בהתגברות על בעיות דומות לאלו הקשורות להפעלה מוצלחת של הרתעה על־ידי איום. בשני המקרים, מחיר הכניסה הנמוך שנדרשים מאתגרים לשלם כדי להפעיל לוחמה קיברנטית נותר קושי מרכזי. עוד מציע מורגן, כי הרתעה סדרתית (serial deterrence)[30] יכולה גם היא להיות מועילה להתמודדות עם איומים של לוחמה קיברנטית. לטענתו:

> attacks are very likely to turn out to be manageable cyber repeated serial deterrence, primarily through applications of harmful responses over an extended period, to induce either eventually permanent suspensions of the most temporary or bothersome attacks or of attacks by the most obnoxious opponents.[31]

בעוד שזוהי דרך מקורית להתמודד עם איומים במרחב הקיברנטי, ויש בה ניסיון מעניין להשתמש במושגים קיימים בדרך חדשנית, אין היא אינה חפה מאתגרים. ראשית, לא ברור שהיריב יכול להיות מושפע לאורך זמן מאותם ניסיונות, שכן אלו עלולים ללמד את המאתגר כי ההרתעה שמפעיל המגן אינה עובדת (ועל כן הוא נדרש לאותן פעולות חוזרות).[32]

בעיה נוספת הקשורה לאסטרטגיה המבוססת על הרתעה סדרתית היא חשיפת האמצעים שבידי המגן. הבעיה של חשיפת היכולת באה אומנם לידי ביטוי בכל אחת מצורות ההרתעה במרחב הקיברנטי (הרתעה על־ידי איום, הרתעה על־ידי מניעה); ואולם עקב אופיים של האמצעים שמשתמשים בהם במרחב זה, הבעיה חריפה במיוחד בכל הקשור לניסיונות הרתעה לאורך זמן, כמו הדרישות המתחייבות מאסטרטגיה של הרתעה סדרתית.[33] במצב זה, חשיפת היכולות ההתקפיות כפועל יוצא של התקיפות החוזרות ונשנות עשויה לשמש מקור לידע או השראה בעבור המאתגר.[34] מורגן עצמו התייחס לסוגיה זו וטען, כי חשיפת היכולות עלולה לא רק להעניק השראה ליריבים ומוטיבציה להשגת יכולות דומות, אלא גם עלולה לאפשר ליריב להתכונן לאיום העתידי ולפגוע ביעילותו של האיום הזה.[35]

כיוונים לחשיבה ולמחקר נוסף

אומנם כמה חוקרים כבר החלו להציע כיווני מחקר מגוונים לבחינת הרתעה במרחב הקיברנטי, אך אני מבקש להצביע כאן על שני כיוונים מרכזיים שבהם אפשר להרחיב עוד את הספרות בנושא. ראשית, יש מקום למקד יותר את המחקר העוסק באיומים במרחב הקיברנטי. נראה שקיים פער הולך וגדל בין הפרקטיקות בזירה הבינלאומיות וסוגי האיומים בה לבין הדרך שהמחקר בתחום בוחן את אסטרטגיית ההרתעה. פער זה קיים בתחומי מחקר נוספים של הרתעה, אך הוא בולט במיוחד בנוגע למרחב הקיברנטי, המכיל מגוון רחב של סוגי אינטראקציות בין סוגים שונים ומגוונים של שחקנים המאיימים בדרכים שונות. לכן יש להרחיב את הדיון בסוגי השחקנים והאיומים שהם יוצרים, ובדרכים להרתעת כל אחד מהם. זאת ועוד, בדומה למחקר הרחב בנוגע לאסטרטגיית ההרתעה, קיימת נטייה להתמקד בהרתעה של מדינות כלפי סוגים שונים של שחקנים (ארגוני טרור, מדינות סוררות וכו'),[36] בעוד חלק חשוב שאינו זוכה לתשומת לב מספקת נוגע להרתעה של אותם שחקנים את המדינות שאותן הם מבקשים לאתגר. בעיות אלה של הרתעה קיימות גם בלוחמה קיברנטית, ומעצימות את הקשיים של מדינות המתמודדות בזירה מורכבת בהרבה ממה שידעו בעבר.

בדומה, המחקר העוסק בלוחמה קיברנטית נוטה לעסוק בהיבטים קלאסיים של ביטחון, בעוד זירת האיומים מורכבת ומגוונת.[37] למשל, מדינות מוטרדות מאוד מכוחם העולה של שחקנים כלכליים (למשל גוגל), או אידיאולוגיים (למשל יחידים או קבוצות חברתיות המבקשים לקדם רפורמות שלטוניות), המשתמשים במרחב הקיברנטי. בלי להיכנס לשאלה, האם ההגדרות הקיימות ללוחמה קיברנטית מכילות את האינטראקציות עם שחקנים אלה, עשויה להיות תרומה חשובה לניתוח יחסים אלה באמצעות התיאוריות של ההרתעה. לדוגמה, אפשר לחקור באמצעות הכלים והמושגים של אסטרטגיית ההרתעה את האינטראקציות בין גוגל לבין סין בנוגע לאיומים המרומזים או הישירים שהציגו שחקנים אלה זה לזה בסוגית הצנזורה על התוצאות המוצגות במנוע החיפוש. בנוסף, פירוק המחקר של הרתעה ולוחמה קיברנטית לסוגים שונים של איומים (cyberwar, cybercrime, cyber-terror, internetwar) ולסוגי השחקנים המפעילים אותם (מדינות, יחידים, ארגונים כלכליים) עשוי להיות לא רק מדויק יותר ופורה, אלא גם להצביע על התנאים לקיום סיכויים רבים יותר להצלחתה של אסטרטגיית ההרתעה של כל אחד מן השחקנים המעורבים כלפי יריבו.

שנית, אני סבור כי יש להמשיך ולבחון בגישה ביקורתית ומקורית את הספרות האסטרטגית המסורתית בנושאי הרתעה. הדבר כבר נעשה במידה לא מבוטלת בכמה מן המאמרים שפורסמו בנושא, אך יש מקום להמשיך ולבחון מושגים נוספים לגבי אסטרטגיית ההרתעה, כמו "הרתעה מידית",[38] "הרתעה כללית" ו"הרתעה

מורחבת".[39] יש לנסות להבין את המשמעות והרלוונטיות של יישום פרקטיקות כאלה במרחב הקיברנטי.

בדומה אפשר להשתמש במושגים כמו "עמימות". מושג זה עשוי לשמש מסגרת חשיבה להתמודדות עם הדילמה הכרוכה מחד גיסא בצורך בחשיפת היכולות,[40] ומאידך גיסא החשש שהיריב יוכל לנצל חשיפה זו להגדיל את עוצמתו ואת חסינותו מפני איומי ההרתעה. שימוש בתובנות שפותחו בהקשרים שונים עשוי להיות בסיס מעניין לפיתוח רעיונות של עמימות במרחב הקיברנטי, לא רק לגבי הכוונות והנכונות להפעיל את האיומים, אלא בכלל ביחס לשאלת קיומן של היכולות. באור זה אפשר למשל לנתח את המאמצים שעושות מדינות בשנים האחרונות בתחום הלוחמה הקיברנטית. לא רק שאמצעים אלה שמפתחות מדינות עשויים לחזק את אסטרטגיית ההרתעה שלהן כלפי איומים אלה, אלא שעצם הבולטות שזכו לה מאמצים אלה יכולה לשמש ככלי הרתעתי. כך הגם שלהקמת פיקוד אסטרטגי לניהול לוחמה קיברנטית של ארצות־הברית יש מגוון מטרות ותפקידים,[41] עצם אזכורו והבולטות שקיבל מאפשרים לא רק את שיפור היכולת, אלא גם מדגימים את הנכונות להשקיע משאבים בצמצום האיומים והנזקים. ייתכן שהבלטת הרצון להשקיע באמצעים מעין אלו, וחשיפה של היקף התקציבים, המשאבים וכוח האדם המופנה לנושא — גם בלי פירוט מדויק של האמצעים הנרכשים ויכולותיהם — יוכלו לסייע בהגדלת אמינות המסר ההרתעתי נגד איומים במרחב הקיברנטי, במיוחד כלפי איומים הכרוכים ברמות גבוהות של אלימות מצדן של מדינות אחרות. במילים אחרות, חשיפה חלקית של היכולות תוך שמירה על ערפול ועמימות לגבי מהותן, מאפשרת לצמצם את אותן השפעות מזיקות שתוארו לעיל, אך גם להעביר מסר תקיף. עם זאת, אפשר לצפות כי סף הכניסה הנמוך לפעולה במרחב הקיברנטי, במיוחד כשמדובר בעימותים א־סימטריים, ימשיך להציב אתגר לביסוס אסטרטגיה של הרתעה המבקשת למנוע איומים במרחב הזה.

סיכום

המחקר העוסק בהרתעה של לוחמה קיברנטית דן בעיקר בקשיים הטמונים בהרתעת יריבים מלעשות שימוש באסטרטגיה זו. הגם שבתנאים מסוימים הרתעה עשויה להתקיים, בכל זאת הקשיים הנוגעים ליכולת המגן, לנכונות שלו להשתמש באמצעים אלה וליכולתו להעביר את המסר המרתיע למאתגר הפוטנציאלי מגבילים מאוד את האפשרות להפעיל הרתעה מוצלחת. עם זאת, בשל היתרונות הגלומים באסטרטגיית ההרתעה בהקטנת היקפי אלימות בסכסוכים, חשוב לנסות ולפתח עוד את המחקר העוסק בקשרים בין הרתעה לבין לוחמה קיברנטית. במאמר זה ביקשתי להצביע על שני כיוונים מרכזיים להמשך החשיבה והפיתוח של רעיונות אלה. ואולם, וכפי שטוען כאמור מורגן, יש לנהוג זהירות בתובנות

הקיימות, שכן נדרש עוד ידע אמפירי על מהותה של הלוחמה הקיברנטית, הן על הנזק שהיא גורמת, והן על הדרך שאפשר להשתמש בה.

הערות

1 Lupovici Amir, "The Emerging Fourth Wave of Deterrence Theory–Toward a New Research Agenda," *International Studies Quarterly* 54, no. 1 (2010): 705-732.

2 בלוחמה קיברנטית הכוונה היא לסוג מסוים של לוחמת מידע, הגם שלעתים המושג לוחמת מידע משמש כמושג חליפי למושג לוחמה קיברנטית. סוג לוחמה זה מבוסס על הניסיונות השונים למנוע, לשבש, לנצל או להשמיד את מערכות המידע של האויב, תוך הגנה על מערכות המידע של המגן מפני איומים דומים. ראו: Harknett J. Richard, "Information Warfare and Deterrence," *Parameters* 26, no. 3 (1996), pp. 93-97; Wheatley F. Gary and Hayes, E. Richard, Infor*mation Warfare and Deterrence*. (Washington DC: National Defense University Press, 1996), pp. v-vi, 5-6; Molander, C. Roger, Riddile, S. Andrew, and Wilson, A. Petter (1996). "Strategic Information Warfare: A New Face of War," *Parameters* 26 No. 3 (1996), pp. 83, 86-90. לסקירה מקיפה של מושגים מרכזיים על לוחמה במרחב הקיברנטי ראו: טבנסקי ליאור, "לחימה במרחב הקיברנטי: מושגי יסוד". **צבא ואסטרטגיה**, כרך 3, גיליון 1 (2011). עמ' 65–80.

3 על הנטייה הכללית של המחקר העוסק בלוחמת מידע וביטחון לבחון שאלות מדיניות, ולהמעיט בשילוב היבטים תיאורטיים כלליים יותר, ראו: Eriksson Johan and Giacomello Giampiero, "The Information Revolution, Security, and International Relations: (IR)relevant Theory?" *International Political Science Review* 27, no. 3 (2006), pp. 221-244.

4 במאמר זה אשתמש במונחים הרווחים לתיאור השחקנים הנוגעים לאסטרטגיית ההרתעה: השחקן המגן, השחקן המבקש להפעיל את אסטרטגיית ההרתעה כדי למנוע פעולה שאינה רצויה לו; והשחקן המאתגר, השחקן המבקש לפעול נגד המגן. השימוש במושגים החלופיים, השחקן המרתיע או השחקן המורתע, כפי שנעשה לעתים, הוא בעייתי, שכן הוא מרמז על הצלחת האסטרטגיה.

5 לסקירה מצוינת של הגדרות המושג הרתעה על־ידי איום ראו: Morgan, M. Patrick, *Deterrence Now* (NY: Cambridge University Press, 2003), pp 1-2.

6 George Alexander and Smoke Richard. *Deterrence in American Foreign Policy: Theory and Practice* (New York: Columbia University Press, 1974), p. 11.

7 חשוב להבהיר כי אסטרטגיה של הרתעה על־ידי מניעה גם שונה מאסטרטגיה של הגנה. אף שקיימת חפיפה ביניהן, הרי הגנה מבקשת לספק פתרון למקרה שאסטרטגיית ההרתעה תיכשל, ואילו הרתעה על־ידי מניעה מבקשת למנוע את הפעולה על־ידי כך שהמאתגר יבין שאין ביכולתו לבצע את הפעולה עקב יכולותיו של המגן.

8 להבחנה זו ראו: Snyder Glenn, *Deterrence and Defense* (Princeton: Princeton University Press, 1961). עם זאת, הרתעה על־ידי איום והרתעה על־ידי מניעה עשויות עקרונית לחזק זו את זו. אם מאתגר פוטנציאלי יידע לא רק שסיכויו להצליח נמוכים, אלא שגם ייגבה ממנו מחיר יקר, גדלים הסיכויים שהוא יימנע מפעולה.

9 Schelling Thomas, *Arms and Influence* (New Haven: Yale University Press, 1966), p. 69.

10 Carnesale Albert, Doty Paul, Hoffmann Stanley, Huntington, P. Samuel, Nye, Jr. S. Joseph, and Sagan D. Scott, *Living with Nuclear Weapons*. (Cambridge: Harvard University Press, 1983).

11 לדיון בהרתעה קונבנציונלית ראו למשל Shimshoni Jonathan, *Israel and Conventional Deterrence: Border Warfare from 1953 to 1970* (Ithaca: Cornell University Press, 1988); Mearsheimer J. John, *Conventional Deterrence* (Ithaca: Cornell University Press, 1983).

12 כך למשל נטען, שהתפתחות נורמות בינלאומיות הקוראות לאיסור השימוש בנשק גרעיני ודעת קהל בינלאומית התומכת בכך, מחלישות את אסטרטגיית ההרתעה הגרעינית מאחר שהן מעלות את מחיר מימוש האיום של המגן Paul T.V., "Nuclear Taboo and War Initiation in Regional Conflicts," *Journal of Conflict Resolution* 39, no. 4 (1995), pp. 699-700, 711.

13 חוקרים דנו בשאלה כיצד להגדיל את אמינות האיום, ואף הציעו אמצעים לכך, למשל "מסרים יקרים" (costly signals) Fearon James, "Domestic Political Audiences and the Escalation of International Disputes," *American Political Science Review* 88, no. 3 (1994), pp. 577–592. עם זאת, היו חוקרים שהטילו ספק באפקטיביות של חלק מן האמצעים האלה. לדיון בנושא ראו למשל Huth, Paul, "Reputations and Deterrence: A theoretical and Empirical Assessment," *Security Studies* 7, no. 1 (1997), pp. 72-99.

14 Morgan, *Deterrence Now*, pp. 15-16.

15 לסקירה מצוינת המדגימה היטב את הסוגים השונים של ההרתעה הישראלית ראו: בר־יוסף אורי, "50 שנות הרתעה ישראלית: לקחי העבר ומסקנות לעתיד". **מערכות**, גיליון 366–367, 1999, עמ' 12–29.

16 Harknett, Ibid, pp. 93-107; Berkowitz D. Bruce, "Warfare in the Information Age," In Athena's Camp: Preparing for Conflict in the Information Age. eds. John Arquilla and David F. Ronfeldt (Santa Monica, CA: RAND Corporation, 1997), pp. 183-184; Goldman O. Emily, "Introduction: Security in the Information Technology Age," In *National Security in the Information Age,* ed. Emily O. Goldman (London: Taylor & Francis, 2004), p. 3; Arquilla, John, "Thinking About New Security Paradigms," in National Security in the Information Age, ed. Emily O. Goldman (New York: Routledge, 2004), pp. 210-213. למסקנות דומות מגיע מורגן, הטוען כי היבטים שונים הנוגעים לפרקטיקות של ההרתעה מתקופת המלחמה הקרה ומבוססים הן על אסטרטגיה זו והן על גורמים תומכים כמו אמצעי בקרת נשק, רלוונטיים פחות להרתעה במרחב הקיברנטי. עם זאת, אין הוא פוסל על הסף את האפשרות של שימוש בסוגים שונים של אסטרטגיית ההרתעה להתמודדות עם איומים אלה Morgan, M. Patrick, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm," in *Proceedings of a Workshop on Deterring Cyberattacks*, eds. John D. Steinbruner et al., (Washington: The National Academies Press, 2010) pp. 55-76. נוכח מגבלות היכולת לבסס הרתעה כנגד לוחמה קיברנטית הוצע – במיוחד בעבור ארצות־הברית, שבה עוסק כאמור רובו של הדיון המחקרי – לנקוט אמצעים חלופיים לאסטרטגיה זו, למשל שימוש באמצעים הגנתיים. Adams James, Wheatley and Hayes, Ibid, p. 9; "Virtual Defense," *Foreign Affairs* 80 (2001), pp. 107-112.

17 Harknett, Ibid, pp. 96-97, 103-104; Wheatley and Hayes, Ibid, p. 9; Berkowitz, Ibid, pp. 183-184; Libicki C. Martin, *Conquest in Cyberspace* (Cambridge, UK: Cambridge University Press, 2007), p. 272. על הפגיעות של חברות (societies) למתקפות אלקטרוניות ראו: Deibert Ron, "Circuits of Power: Security in the Internet Environment," in *Information Technologies and Global Politics: The Changing Scope of Power and Governance*, eds. J.P. Singh and James N. Rosenau (NY: Suny Press, 2002), p. 115. על נקודות הרגישות לאיומים חיצוניים ופנימיים של מערכות

מידע, ראו: Libicki C. Martin, *Cyber Deterrence and Cyber War* (Santa Monica, CA: RAND Corporation, 2009), pp. 13-23. Available at: www.rand.org/pubs/monographs/2009/RAND_MG877.pdf.
עם זאת, חשוב לציין כי לטענת ליביקי היקף האיום שיוצרת לוחמה קיברנטית בתקופה הנוכחית אינו ברור או ודאי. לטענתו, סוגיית היקף הנזק שעשויה לוחמה קיברנטית לגרום היא מרכזית ועומדת בבסיס הוויכוח בדבר חשיבות אסטרטגיית ההרתעה כלפי סוג לוחמה זה Libicki, *Cyber Deterrence and Cyber War*, p. 36.
מסיבות דומות, הנוגעות למיעוט המידע הקיים וחדשנות הנושא, ממליץ מורגן להיזהר ממסקנות חפוזות בנוגע לאפשרויות ההרתעה של איומים במרחב הקיברנטי, Morgan, "Applicability of Traditional Deterrence Concepts", pp. 61-62.

18 Libicki, *Cyber Deterrence and Cyber War*, p. 26.

19 Harknett, Ibid, p. 104.

20 Molander et al., Ibid, p. 87.

21 על הקשיים בזיהוי מקורן של התקפות של לוחמה קיברנטית ראו גם: Libicki, *Cyber Deterrence and Cyber War*, pp. 44-45.

22 על דעת הקהל הפנימית והבינלאומית המגבילות את אפשרות השימוש בכוח, ובכך משפיעות על ההרתעה של השחקן המגן, ראו למשל: Jervis Robert, "Deterrence, Rogue States, and the Bush Administration," in Complex Deterrence, eds. T.V. Paul, Patrick Morgan, and James Wirtz (Chicago: University of Chicago Press), p. 153.

23 Hayes and Wheatley, Ibid, p. 9; Harknett, Ibid, p. 104; Berkowitz, 1997, pp. 183-184; Cordesman Anthony, and Cordesman, Justin, *Cyberthreats, Information Warfare, and Critical Infrastructure Protection: Defending the US Homeland*. (Westport: Praeger: 2001), p. 7; Arquilla, Ibid, pp. 210-211.

24 Libicki, *Cyber Deterrence and Cyber War*, pp. 1-3.

25 הסיבה לכך היא שהאיום המרתיע צריך להיות מותאם כאמור לסוג האיום ולסוג הגורם המפעיל אותו. לכן נטען כי קיימת חשיבות לבסס את ההרתעה על איום ממוקד כלפי מאתגר מסוים. למשל, הרתעה כלפי שחקן מדינתי הנהנה מריבונית בטריטוריה מסוימת ואשר יש לו "מטרות ערך", שונה מהרתעה כלפי שחקן שאינו מדינתי, המחייבת אפוא שימוש בסוגים שונים של איומים. סוגיה זו זוכה בשנים האחרונות לדיון נרחב בהקשר של הרתעה "תפורה" (tailored deterrence), בעיקר בהקשר של הרתעת טרור. לדיון במושג ראו: Lantis S. Jeffrey, "Strategic Culture and Tailored Deterrence: Bridging the Gap between Theory and Practice". *Contemporary Security Policy* 30, no. 3 (2009), pp. 469-471. לדיון במושג ביחס ללוחמה קיברנטית ראו: Kugler, L. Richard, "Deterrence of Cyber Attacks," in *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), pp. 331-333.

26 Harknett, Ibid, pp. 98-100.

27 Libicki, *Conquest in Cyberspace* p. 272. לדיון נוסף בהשפעת המהפכה בענייני צבא (RMA) על הרתעה ועל היכולת להרתיע ראו: Morgan, *Deterrence Now*, pp. 219-224.

28 ראו, Kugler, Ibid, p. 328. וכן ראו ב־ Hayes and Wheatley, Ibid, pp. 13, 19-20; Cordesman and Cordesman, 2002, p. 7.

29 Morgan, "Applicability of Traditional Deterrence Concepts", p. 59.

30 במושג דומה – הרתעה מצטברת (cumulative deterrence) – השתמש דורון אלמוג בנוגע לדרך להרתיע איומים של טרור שלא במרחב הקיברנטי, Almog Doron, "Cumulative Deterrence and the War on Terrorism," *Parameters* 34, no. 4

(2004-2005): pp. 4-19.

31 Morgan, "Applicability of Traditional Deterrence Concepts", p. 59.

32 Lupovici, Ibid, p. 722.

33 כך למשל עשוי המאתגר ללמוד על אמצעי הגנה (או לקבל השראה לאמצעים כאלה) מהאמצעים שמשתמש בהם השחקן המבקש להפעיל הרתעה על־ידי מניעה, וכך הוא עלול להגביל את היכולת להרתיע באמצעות אסטרטגיה זאת.

34 ביקורת דומה הועלתה לאחר הדיווחים על וירוס סטקסנט (Stuxnet), שעל פי הפרסומים שיבש את פיתוח הגרעין באיראן. החשש שהציגו מומחים לאבטחת מידע הוא, כי תקיפה קיברנטית זו תשמש לא רק השראה למה שאפשר לעשות באמצעות סוג לוחמה זה, אלא שחלקים מהקוד של הווירוס עצמו נחשפו ועלולים לסייע לשחקנים שונים לפגוע בתשתיות רגישות. ראו למשל: "Experts Fear Hackers Can Launch Stuxnet-Like Attacks on Power Plants, Prison Gates", *The Globe and Mail*, October 24, 2011.

35 Morgan, "Applicability of Traditional Deterrence Concepts", p. 63.

36 לאזכור של סוגיה זו בהקשר של לוחמת מידע ראו למשל: Goldman, 2004, p. 3.

37 לדיון במגוון איומים אלה ראו: טבנסקי 2011, ובעיקר עמ' 70, 75–77.

38 הבחנה בסיסית רווחת במחקר ההרתעה מבדילה בין הרתעה כללית, המבוססת על הניסיון למנוע מהיריב לשקול אפשרות של תקיפה (למשל כפי שבא לידי ביטוי בהרתעה גרעינית), לבין הרתעה מידית, הנוגעת למצב שבו שחקן מבקש לעשות פעולה (למשל מזיז כוחות) ובעזרת שימוש באיומים המגן מניא אותו מפעולה זאת. דיון חשוב ומעניין בהקשר זה יכול לעסוק במשמעות של כל אחת מצורות ההרתעה הללו במרחב הקיברנטי.

39 ליביקי, למשל, החל לבחון הרתעה מורחבת במרחב הקיברנטי, Libicki, *Cyber Deterrence and Cyber War,* pp. 104-106. ואפשר למקד ולפתח עוד את הדיון בסוגיות התיאורטיות שנידונו בנוגע לאסטרטגיה זו. לדיון במושג הרתעה מורחבת ראו למשל: Huth Paul, *Extended Deterrence and the Prevention of War* (New Haven: Yale University Press, 1988), pp. 15-27.

40 כאמור, הספרות בנושאי ההרתעה מדגישה את הצורך בהעברת המסר המאיים לצד היריב, ובכלל זה את המחיר שהוא יידרש לשלם. לכן מסרים לגבי יכולות המגן או חשיפת האמצעים שבידו הוזכרו כגורמים חשובים בהקשר הזה.

41 "ארצות־הברית מקימה פיקוד צבאי למלחמה בהאקרים", *Ynet*, 24 ביוני 2009, http://www.ynet.co.il/articles/0,7340,L-3736253,00.html

להגנת וירוס הסטקסנט

ג'יימס א. לואיס

גילויים חדשים על הווירוסים 'סטקסנט' (Stuxnet) ו'פליים' (Flame) עוררו שוב מקהלה של אזהרות דחופות מפני סכנות מלחמת סייבר והצורך בפעולה. אך השאלה המטרידה יותר שעולה בעקבות חשיפת הווירוסים היא – אם לוחמת סייבר היא נושא כה קריטי – מדוע אנשים כה רבים מחזיקים במידע כה שגוי לגביה? הדעה ש"'סטקסנט' או 'פליים' הגבירו את הסיכון מעידה על הבנה לקויה של מידת הסיכון שכבר קיימת במרחב הסייבר, של התדירות הגבוהה של פעולות סייבר זדוניות[1] שכבר מתקיימות בחסותן של מדינות ושל הצמיחה המהירה ביכולות הלוחמה של מדינות רבות. לכן, נכון יותר לראות את 'סטקסנט' ו'פליים' כפרק נוסף בתחרות המתמשכת בין ארצות־הברית, איראן ורוסיה.

האמונה ש'סטקסנט' מגביר את הסיכון לארצות־הברית או לבעלות־בריתה מתבססת על מספר הנחות מוצא שגויות. תפיסות הטוענות למכות נגד, נזק נלווה או פתיחת 'תיבת פנדורה' אינן מתקבלות על הדעת לאור היקף הפיתוח והשימוש בטכניקות מתקפת סייבר במהלך שלושת העשורים האחרונים. 'סטקסנט' לא חשף יכולת לוחמה חדשה שאחרים יזדרזו להעתיק. מתקפת סייבר היא יכולת מודיעינית וצבאית מוכרת שנמצאת בשימוש במשך שנים רבות. ההערכה היא שכארבעים מדינות מצטיידות ביכולות לוחמת סייבר או השיגו אותן כבר,[2] לרבות היכולת לשגר מתקפות סייבר. רוב התוכניות הלאומיות אפופות סודיות, ואין הסכמה בשאלה עד כמה החוק הבינלאומי הקיים, שתקף לעימות מזוין, אמור לחול על מצב ההתקפה החדש. עם זאת, כל צבא מתקדם כבר מצויד ביכולת לוחמת סייבר, ומדינות רבות אחרות שואפות להשיגה.

ההאשמה כלפי תפקידה של ארצות־הברית ב'סטקסנט' לא הייתה הפתעה מיוחדת. רוב המדינות כבר הגיעו למסקנה שארצות־הברית הייתה אחראית לכך, ולא נדהמו להיווכח שתוכנה הופכת לכלי התקפי ולאמצעי כפייה. השימוש

ג'יימס א. לואיס הוא חוקר בכיר ומנהל של תכנית למדיניות טכנולוגית ומדיניות ציבורית במרכז ללימודים אסטרטגיים ובינלאומיים – Center for Strategic and International Studies (CSIS).

מאמר זה ראה אור לראשונה ב**צבא ואסטרטגיה**, כרך 4, גיליון 3, דצמבר 2012, עמ' 57-67.

בטכניקות סייבר ככלי מודיעין החל בשנות השמונים. מתקפת סייבר מצד צבאות החלה בשנות התשעים.[3] פיתוח טכניקות סייבר התקפיות הואץ בשנות האלפיים, כאשר התרחבה זמינותן של רשתות גלובליות מהירות, והאינטרנט הפך מכלי עזר לתשתית מרכזית לפעילות כלכלית וממשלתית. בין אם מדובר בלוחמה שהיא "מוכוונת רשת" או לוחמה ב"תנאי מידוע" (informatized conditions – כפי שסין מגדירה זאת), מתקפת סייבר אינה חדשה למתכננים צבאיים.

מריגול למתקפה

למרות ש'סטקסנט' ו'פליים' התקבלו בהתלהבות כמבשרי עידן מלחמת הסייבר, גישה זו שגויה בכמה מישורים. מתקפת סייבר אינה דבר חדש, ולמרות שחבלה עשויה לערב שימוש בכוח, לא כל פעולת חבלה שקולה לפעולת מלחמה. ההתייחסות ל'סטקסנט' ו'פליים' כאל לוחמת סייבר מנציחה את ההנמקה האנלוגית השגויה והמוגזמת שדבקה בחקירת תחום אבטחת סייבר מראשית ימיה. יש לראות ב"מתקפת" סייבר ארסנל חדש של כלים לכפייה, לריגול ולמתקפה, יותר מאשר קטגוריית עימות ייחודית וחסרת־תקדים.

הקו המפריד בין ריגול למתקפה במרחב הסייבר הוא דק מאוד. יכולות החדירה לרשת והשליטה בה, שנדרשות לשם ריגול, עלולות לשמש לשיבוש שירותים חיוניים. יריב שמצליח להשיג גישה מבוקרת לרשת יכול גם לפגוע ואולי אף להרוס. אפשר לראות במתקפת סייבר סוג של "חימוש" ("weaponization") של מודיעין האותות (SIGINT) – המרת איסוף מידע פסיבי בשיבוש אקטיבי. פירוש הדבר הוא – אם למקם את המונח "פירוק נשק קיברנטי" בהקשרו הנכון – שאיסור על מתקפת סייבר יחייב גם איסור על ריגול – פעילות ששום מדינה לא תסכים לזנוח.

'פליים' היה רק אחד מבין תוכניות רבות לאיסוף מודיעין שנמצאות באינטרנט. כיום ידוע על כתריסר תוכניות דוגמת 'פליים' ששימשו לריגול סייבר. הטכנולוגיה שינתה את האופן שבו מדינות מרגלות זו אחר זו, וריגול סייבר הפך למרכיב מרכזי בתוכניות לאומיות לאיסוף מידע. האינטרנט יצר את מה שקציני מודיעין מכנים "תור הזהב" של הריגול.

"תור הזהב" הזה נכנס כבר לעשור השלישי שלו. בתחילת שנות השמונים השתמשו שירותי הביון הרוסיים בהאקרים (פצחנים) ממערב־גרמניה כדי לחדור לצבא ארצות־הברית, לחקור רשתות ולשאוב מידע. שירותי הביטחון הסיניים ניהלו מערכות ארוכות ומוצלחות נגד הרשתות של ארצות־הברית ובעלות־בריתה, והיו מעורבים בריגול תעשייתי נרחב בחסות המדינה. אם 'סטקסנט' הצביע לכיוון ארצות־הברית וישראל כמדינות שעשויות להפיק את הרווח הגדול ביותר משיבוש מאמצי הגרעין של איראן, ניתן לשאול איזו מדינה עשויה להרוויח מהשקעת משאבים עצומים במעקב אחר פעילי זכויות אדם בטיבט. ב־15 השנים האחרונות,

תוכניות איסוף רבות כמו 'פליים' הפכו ציבוריות. יש להניח שקיימות תוכניות נוספות המוסתרות טוב יותר. לצורכי ריגול, טכניקות סייבר הן במידה רבה הרחבה של יכולות מודיעין אותות מסורתיות, ומבחינתה של סין, מדובר בהרחבה של גישה מבוזרת העושה שימוש בסוכנים אזרחיים רבים, כפי שניתן לראות בתוכניותיה של סין לאיסוף מידע אנושי.

הן סין והן רוסיה משתמשות באקספלויטים (קודי מקור של פקודות תוכנה משבשות) בסייבר בדרכים שונות מאשר פעילויות הסייבר של שירותי המערב, מבחינת החשיבות והפוטנציאל שלהן לגרימת חוסר יציבות. שתי המדינות מסתמכות על גורמים שלוחים (פרוקסי) – פצחנים (האקרים) פרטיים הפועלים על פי הכוונת המדינה למטרות ממשלתיות. גורמים אלה מספקים דרגה קלושה למדי של יכולת הכחשה (במקרה שמשקיף רציני כלשהו אכן מאמין שסין ורוסיה אינן שולטות ברשתות שלהן), לצד חזית קדמית של תוקפים שיכולים לגונן על פעולות המדינה, ואם נדרש, גם "יקריבו" אותם על מנת לפייס מדינות אחרות. השלוחים הרוסיים התמקדו בפשעים פיננסיים, והסינים התמקדו בריגול תעשייתי. שתי המדינות מספקות רמה מסוימת של הדרכה ותמיכה לשלוחים שלהן, ומתעקשות רק על כלל מרכזי אחד – שלא יפעלו נגד יעדים מבית. כל עוד כלל זה נשמר, ובמקביל השלוחים מבצעים את המשימות שהמדינה מעבירה להם, הם חופשיים לפעול נגד מטרות בארצות אחרות. פצחנים רוסיים היו אחראיים לאקספלויטים נגד אסטוניה וגאורגיה (בגאורגיה היה תיאום מדויק עם תוכניות הצבא הרוסי), ואילו הסינים היו אחראיים לשאיבת נתונים מיעדים צבאיים וכלכליים רבים,[4] בארצות־הברית ובמדינות אחרות.

לעומת זאת, ארצות־הברית ובעלות־בריתה אינן עושות שימוש בשלוחים מטעמן לצורך מעורבות בפשעים פיננסיים בחסות המדינה, וארצות־הברית אינה מעורבת בריגול תעשייתי. הדוקטרינה האמריקנית לשימוש בטכניקות סייבר כהרחבה של אמצעי כפייה מסורתיים דוגלת בגישה שונה, אם כי בהחלט לא חסרת־תקדים.

מתקפת סייבר ותהליך ההתחמשות (Weaponization) של מודיעין האותות

יכולות כמו אלה של 'סטקסנט' משקפות שנים של פיתוח וניסויים בניצול רשתות דיגיטליות להשגת כוח צבאי. וירוס 'סטקסנט' צויד ביכולות הרס מתקדמות משום שתוכנן להשפיע על מערכות בקרה תעשייתיות – מחשבים ייעודיים המפעילים מכונות – אך למעשה הוא היה רק הרחבה ושיפור של טכניקות מתקפת תוכנה קיימות. היכולת להשתמש בתוכנה לשיבוש מערכות בקרה תעשייתיות ולגרום הרס פיזי הומחשה כבר בניסוי שנערך במעבדה הלאומית של איידהו (ארצות־

הברית) ב־2005. ההערכה היא שחמש מדינות מחזיקות ביכולת זו – ארצות־הברית, בריטניה, ישראל, רוסיה וסין, ומדינות רבות נוספות מנסות להשיג אותה. בהקשר זה ארצות־הברית יכולה להיחשב "ראשונה בין שוות", אך יש לה שותפים למעמד זה (או כמעט שותפים) בתחום מתקפת סייבר. 'סטקסנט' עשוי להיחשב ל"נשק" המתקדם ביותר מסוג זה (חותמת איכות אמריקנית נוספת), אך בשום אופן לא מדובר ביכולת ייחודית.

מתקפת סייבר היא אופציה נוספת הזמינה למתכננים צבאיים. במקרה של 'סטקסנט' למשל, המתכננים יכלו לשקול את היתרונות והחסרונות של מתקפת סייבר מול מתקפה אווירית, צוות מבצעי מיוחד, חבלנים או טילים. תורות הלחימה הקיימות הורחבו והותאמו למצב התקיפה החדש. מדינות יצרו יכולות מתקפת סייבר ופיתחו דוקטרינות ואסטרטגיות לשימושן. דוקטרינות לאומיות אלה אינן זהות בכל המדינות. אנו נמצאים בתקופת התנסות, שבה המדינות מעריכות יכולת צבאית חדשה זו וחוקרות מהי הדרך הטובה ביותר לנצל אותה. נוסף לשימוש שעשתה רוסיה ב"מתקפת" סייבר באסטוניה ובגאורגיה, והשימוש לכאורה שעשתה ישראל בסוריה, ראינו כיצד רוסיה וסין אוספות מידע לצורך מתקפות על תשתיות אמריקניות חיוניות (על פי ראש הסוכנות האמריקנית לביטחון לאומי),[5] ומשתמשות באיראן נגד ישראל ומדינות המפרץ. ארצות־הברית השתמשה במתקפות סייבר בשנות התשעים במהלך העימות עם סרביה, ונגד ההגנה האווירית של עיראק בין מלחמות המפרץ.

ארצות־הברית, רוסיה, סין ומדינות נוספות, כוללות בדוקטרינה שלהן לגבי שימוש צבאי במתקפת סייבר גם מתקפה על תשתיות חיוניות. הדוקטרינה הגלויה רומזת על כך שכל מדינה מקבלת החלטות על השימוש במתקפת סייבר באופן עקבי לתכנון השימוש שלה בסוגים אחרים של נשק ארוך־טווח – כגון שקלול יתרונות התקיפה, הסיכון בהסלמה והפוטנציאל לנזק נלווה. ניתן לראות בדוקטרינה האמריקנית כמה קוים מקבילים לחשיבה על הפצצה אסטרטגית ולשימוש בהפצצה אווירית להפחתת הנכונות והיכולת של האויב להתנגד, במקביל להימנעות מעימות ממושך עם כוחות צבאיים. הדוקטרינה הרוסית שמה דגש רב יותר על הפרת היציבות הפוליטית ועל שיבוש מערכות פיקוד צבאיות באמצעות טכניקות סייבר, בדומה לדוקטרינה הסובייטית שדגלה במכות פתיחה חזקות נגד נאט"ו באמצעות תקיפת תשתית חיונית. הדוקטרינה הסינית עמומה יותר, אך הדיון הציבורי מתמקד במתקפות על תשתיות במטרה לשבש יכולת אמריקנית להתערב במשברים אזוריים.[6]

כאשר בוחנים מתקפת סייבר בהקשר של קבלת החלטות צבאיות (בהנחה ששחקנים מדינתיים ושחקנים לא־מדינתיים חולקים לרוב תהליכי תכנון צבאי דומים), עולות ההשלכות של השימוש בה. הסבירות שמדינות ישגרו לעבר ארצות־

הברית או בעלות־בריתה מתקפת סייבר שתגרום נזק פיזי לא גברה בעקבות חשיפת 'סטקסנט', ובאותה מידה, אין סיכוי שמדינות אלה יפסיקו את השימוש בטכניקות סייבר לצורכי ריגול וכפייה פוליטית. הסיבה שאיננו עדים למתקפות שיכולות לגרום לארצות־הברית ולבעלות־בריתה נזק פיזי, הרס או נפגעים (בניגוד לריגול או לפשע) מצד המדינות שמחזיקות ביכולת כזו היא שמדינות אלה מעריכות שהסיכון לתגובה אלימה גבוה מדי. זו גם הסיבה שמונעת מהן לשגר מטוסים או טילים נגד ארצות־הברית. עם זאת, החוק והנוהג הבינלאומי אינם מצדיקים שימוש בכוח כתגובה לריגול ולפשע, וכך נעשה הסיכון לתגובה אלימה כזו נמוך וסביר.

הימנעות זו מתקיפה עשויה להשתנות ככל שמדינות אחרות, עם דרגת סובלנות אחרת כלפי סיכון, דוגמת איראן, ישיגו יכולות מתקדמות למתקפת סייבר, או כאשר גורמים שמעריכים באופן מופרז את יכולתם להישאר סמויים ישיגו יכולות מתקדמות. מה שאיננו יודעים הוא עד כמה התקדמו שחקנים לא־מדינתיים ביכולתם לפתח טכניקות הרסניות דומות. העובדה היחידה שאין עליה מחלוקת היא שעד היום לא ראינו שחקנים לא־מדינתיים המעורבים במתקפות כאלה. דבר זה עשוי לשקף היעדר מניע או יכולת, ולא ניתן להעריך באיזו מהירות עשויים גורמים אלה להשיג יכולת לבצע מתקפות דוגמת 'סטקסנט'.

לזכותם של מתכנני 'סטקסנט' ייאמר, שהוא נכתב בזהירות מספקת על מנת למנוע נזק נלווה. ייתכן שתוקפים אחרים לא יהיו כה זהירים, אך אין קשר בין עובדה זו לבין יכולת הגישה לקוד 'סטקסנט'. יריבים פוטנציאליים ממשיכים להתמודד עם אותם שיקולי בעד ונגד בהחלטתם האם להשתמש בכוח נגד ארצות־הברית, והם ימשיכו להירתע מהתגובה האפשרית של צבא ארצות־הברית לנוכח כל המשאבים הצבאיים שעומדים לרשותו מעבר למתקפת סייבר. אפשר שגורמים אלה יישענו על 'סטקסנט' כחלק מהצדקה ציבורית למתקפה, אך יהיה זה תירוץ בלבד ולא חלק מקבלת ההחלטות שלהם. הסיכוי שמדינות ישגרו מתקפת סייבר נגד ארצות־הברית או בעלות־בריתה בעקבות חשיפת 'סטאקסנט' אינו גבוה יותר מאשר הסיכוי שקדם לחשיפתו.

לאופן השימוש של צבאות בפוטנציאל של מתקפת סייבר יש השלכות המסבירות מדוע 'סטקסנט' ו'פליים' לא שינו באמת את מהלך העניינים. כמו לכל נשק, גם למתקפת סייבר יש מאפיינים משלה. מתקפות סייבר יכולות להיות מהירות וחשאיות ולהוות סיכון פוליטי מופחת בחלק מהתרחישים. החיסרון שלהן הוא תוצאה הרסנית פחות. מתכנן המתקפה ישקול היבטים אלה, ויעריך את הסבירות שמתקפת הסייבר תשיג את האפקט המבוקש ב"עלות" הנמוכה ביותר בהשוואה לאפשרויות מתקפה אחרות. בחלק מהתרחישים עדיפה מתקפת סייבר. החלופות ל'סטקסנט' כללו צוותי חבלה, התקפות אוויריות, ירי טילים או אפילו כיבוש שטח בידי כוחות קונבנציונליים. די ברשימה קצרה זו – שכל האפשרויות

בה כרוכות בסיכון רב יותר לאבידות, לאלימות ולהסלמה – כדי להראות מדוע מתקפת סייבר הייתה עדיפה.

יש מדינות שכבר עושות שימוש סדיר במתקפות סייבר בדרכים שמשרתות את צורכיהן. לאחרות יש יכולת להוציא לפועל מתקפה דוגמת 'סטקסנט', אך האסטרטגיה שלהן שמה דגש על יעדים אחרים, ועד היום לא היה להן עניין בגרימת נזק פיזי. רוסיה וסין הציגו יכולות מתקדמות, וביכולתן לשגר מתקפות דוגמת 'סטקסנט' אילו היה הדבר נתפס בעיניהן כמועיל. העובדה שהעימות בתחום סייבר נותר ברובו נסתר מעיני הציבור לפני 'סטקסנט', אין פירושה שהוא לא התקיים.

הנחה שגויה נוספת היא ש'סטקסנט' היה אירוע דוגמת הירושימה, בכך שהתיר את הרסן מכוח צבאי הרסני חדש וחסר־שליטה. אלא שכאן אין איש כאופנהיימר שידקלם בעקבות 'סטקסנט': "עתה הפכתי אני לכוח המוות, משמיד העולמות".[7] למרות הרצון המפתה לכאורה להשוות בין מתקפת הסייבר לנשק גרעיני, השוואה זו מופרכת מיסודה. גם לנשק גרעיני בקנה־מידה קטן ביותר יש כוח הרס עצום, אך למתקפות סייבר אין. הן מהוות נשק תמיכה, היעיל בעיצוב שדה הקרב לטובת המשתמש בו, אך השפעתן אינה כמו של הרס המוני או קטלני, ואין בכוחן להוות איום קיומי על מדינות. לכל היותר, ניתן להשוות מתקפת סייבר לטילים שמאפשרים מכה מהירה למרחק רב, עם מרכיב גדול יותר של סודיות (אולי), לצד תוצאה הרסנית פחות. יכולת הרס מוגבלת זו – אין פירושה שניתן לקדם בברכה שיבוש שנגרם מבהלה פיננסית מלאכותית או מהפסקת חשמל שנמשכת שבועות ארוכים, אך עלינו להימנע גם מהגזמה בהשפעה המיוחסת למתקפת סייבר.[8] 'סטקסנט' הפנה את תשומת הלב לפגיעותה של התוכנה המודרנית, אך הכוח ההרסני של מתקפת סייבר אינו קרוב כלל לזה של נשק גרעיני, או אפילו לזה של מתקפה בנשק קינטי.

התחרות האזורית

קוד 'סטקסנט' זמין עתה לציבור, ויש החוששים שיהיו מי שישתמשו בו שוב, אולם יש בכך התעלמות מאחת המגבלות העיקריות של מתקפת סייבר – בדרך כלל מדובר באקספלויט חד־פעמי. ברגע שהמתקפה חושפת שגיאות תֻכנות חדשות ("zero days") או אחרות במערכות ההפעלה או במערכות בקרה תעשייתית, הן לרוב מתוקנות. קוד 'סטקסנט' שנגיש לציבור היה חלק מאקספלויט גדול ומורכב יותר, שכלל מגוון טכניקות ריגול. הקוד היה רק חלק מהאקספלויט, ואינו מספיק כשלעצמו. אם 'סטקסנט' ישוגר שוב הוא לא יפעל. ההוכחה הטובה ביותר לכך היא שבעוד מערכות רבות ברחבי העולם נדבקו בווירוס, רק אחת ניזוקה – באיראן.

איראן עלולה לגלות רצון לנקום על 'סטקסנט', אך אין זה חדש לאיראנים שארצות־הברית ומדינות אחרות מעורבות במבצעים חשאיים שמיועדים לעכב

את תוכניתם הבלתי־חוקית לפיתוח נשק גרעיני, ובאותה מידה, האיראנים מעולם לא הסתירו את תמיכתם באלימות נגד ארצות־הברית או ישראל. איראן אחראית למותם של אנשי סגל אמריקניים בביירות, במפרץ הפרסי ובעיראק. 'סטקסנט' הוא פרק נוסף בעימות שמתקיים בחשאי ומתלקח מדי פעם בין ארצות־הברית לבין איראן, כבר למעלה משלושים שנה.

איראן לא היססה גם להביע איומים, ולא הסתירה את רצונה לפתח ולהשתמש בטכניקות מתקפת סייבר. רטוריקה ארסית מצד מנהיגי איראן נגד ישראל עשויה להיות התרברבות גרידא שנועדה לקהל הביתי, אך אין בכך כדי להצדיק אותה. למדינות יש אחריות על אמירות פומביות של מנהיגיהן. לנוכח האיומים שנשמעו, ועל רקע ההפרות החוזרות של המחויבות הבינלאומית ביחס לנשק גרעיני, יהיה זה תמוה לומר שפעולה סמויה הכרוכה בשימוש בתוכנה נגד תוכנית הגרעין האיראנית אינה ראויה, מה גם שלא נגרמו פגיעות בנפש או נזק נלווה.[9]

המסקנה שארצות־הברית הייתה מעורבת ב'סטקסנט' גם היא אינה מפתיעה. לארצות־הברית היסטוריה של נקיטת פעולות חשאיות נגד משטרים אגרסיביים ובלתי־דמוקרטיים. היכולת פותחה במלחמת העולם השנייה (בחסות הבריטים), ושוכללה והורחבה במהלך המלחמה הקרה. אולם ארצות־הברית מעולם לא השתמשה בכוח חשאי נגד מדינה דמוקרטית או נגד מדינה שאינה מהווה כל איום על השלום הבינלאומי. ניתן להטיל ספק ביכולתה של ארצות־הברית לזהות איומים על השלום, ואכן נעשו טעויות רבות בעבר, אך איראן אינה אחת מהן. במקרים רבים עדיפה פעולה חשאית על פני תגובות צבאיות אחרות, שכן היא מפחיתה את הסיכון לעימות ישיר או להרחבת הסכסוך. פעולה חשאית היא שביל הזהב בין הסכמה שבשתיקה לבין מלחמה גלויה, היא כלי לגיטימי נוסף להגנתה של מדינה, גם אם יש מי שיתנגדו לכך.

ארצות־הברית מצדיקה התערבויות אלה בכך שהיא מובילה קואליציה של מדינות המגֵנות על הדמוקרטיה – תפקיד שהוטל עליה בעקבות מלחמת העולם השנייה והמלחמה הקרה. תפקיד זה היה מקובל באופן כללי על הקהילה הדמוקרטית בין השנים 1941 ל־1990. גם אם איננו מקבלים את הטענה שארצות־הברית עדיין עומדת בראש קואליציה של מדינות להגנה על הדמוקרטיה, סיבה טובה המצדיקה נקיטת אמצעים אקטיביים כתגובה היא התנהגותה של איראן, המאיימת על ביטחונה של ארצות־הברית ועל שלום העולם.

היתרונות של 'סטקסנט' הם רבים, והצער היחידי שעלינו לחוש הוא שהתגלה מוקדם מדי. שיגור 'סטקסנט' הציב סיכון פוליטי נמוך הרבה יותר מאשר התקפות אוויריות. לא היה נזק נלווה, ולא שידור טלוויזיוני של בניינים עולים באש ואזרחים מבוהלים. לא הופל טייס ולא הוצעד ברחובות טהראן בדרך למתקן העינויים. הפיכת הקוד לנשק מלחמה עלתה הרבה פחות מאשר מטוס F16 אחד.

ההקשר הפוליטי החסר

הדגש שהושם על מלחמת סייבר בדיון הציבורי על 'סטקסנט' ו'פליים', הביא לכך ששאלות חשובות נותרו ללא התייחסות. כאשר אנו רואים שהיריב "חושף במקרה" פעולה חשאית ומורכבת, ובייחוד אם הדבר קורה יותר מפעם אחת, עלינו לשקול הסברים שאינם צירוף מקרים גרידא. ההשערה שכדאי להתעמק בה היא החיבור האפשרי בין חשיפת הווירוסים הללו לבין רוסיה. הגילויים בנוגע לוירוס 'פליים' שירתו סדר־יום פוליטי רוסי רחב יותר, שעניינו משילות אינטרנט (internet governance) ואבטחת סייבר. הצבת 'סטקסנט' ו'פליים' בהקשר של ריגול ופעולה פוליטית חשאית עשויה לספק הסבר טוב יותר מאשר ההתמקדות בלוחמה, בייחוד כאשר האופן שבו פורסם המידע על 'פליים' עולה בקנה אחד עם מניפולציה פוליטית שנועדה לזכות בתמיכה במפגשים רב־צדדיים בנושא משילות אינטרנט, שעתידים היו להתקיים במהלך 2012. רוסיה ומדינות אחרות רוצות שאיגוד הטלקומוניקציה הבינלאומי (ITU) ישחק תפקיד גדול יותר באבטחת סייבר ובמשילות אינטרנט. תפקיד גדול יותר של ה־ITU יחתור תחת כל מה שנתפס כ"הגמוניה" אמריקנית במרחב הסייבר, ואולי אף יפחית את הסיכון לרוסיה, כתוצאה מהגישה הבלתי־מוגבלת למידע שהאינטרנט מציע. רוסיה עשויה אף לחתור ל"הכפשת" השימוש במתקפות סייבר ולהשיג תמיכה רחבה באמנה האוסרת שימוש בנשק דוגמת 'סטקסנט', כחלק ממאמציה לערער תחום שנתפס כיתרון של הצבא האמריקני. מדובר בתכסיס ידוע ביחסים בינלאומיים – הצעת מגבלות המכרסמות ביכולתו של היריב יותר מאשר בזו של המציע (בדומה למאמצים בשנות השמונים לתמרן את פירוק הנשק הגרעיני באירופה כדי להפחית מיכולותיהן של מדינות נאט"ו יותר מאלה של החברות בברית ורשה).

בכל הקשור לנושא זה קיימים קישורים בלתי־שגרתיים: מנכ"ל החברה שחשפה את 'פליים' היה דובר לא־רשמי של ממשלת רוסיה בוועידת הסייבר בלונדון ב־2011. בנובמבר 2011 הכריזו החברה שלו ו־ITU על הקמת שותפות לקידום אבטחת סייבר גלובלית.[10] החברה טוענת שחשפה את 'פליים' לאחר ש־ITU ביקשה ממנה – בקשה שהייתה חסרת־תקדים כשלעצמה – לבחון פריצות נתונים במזרח־התיכון, ועל בסיס זה הכריזה ITU על אזהרה גלובלית של אבטחת סייבר, שגם היא הייתה חסרת־תקדים.[11] ייתכן שהדברים הם בדיוק כפי שהם, אולם השערה חלופית שלא ניתן לדחות אותה על הסף, היא שמדובר בתמרון פוליטי גדול יותר שתכננו הרוסים, על מנת להשפיע על השקפתן של מדינות מפתח. השימוש בגורם שלוח (פרוקסי) לפרסום מידע מזיק על היריב הוא טכניקת ביון מוכרת, ורוסיה נשענת באופן ניכר על גורמים שלוחים בשיטות ריגול הסייבר שלה. מצבים חריגים אלה מרמזים ומצביעים על השערות חלופיות, שהסבירה ביותר היא ששירותים

מערביים יצרו את 'פליים' כדי לרגל אחר איראן, וכי רוסיה ניצלה את החשיפה למטרות פוליטיות.

בשנים האחרונות החלו רוסיה וסין (לעתים דרך 'ארגון שנגחאי לשיתוף פעולה') לפתח אסטרטגיה בינלאומית שתיצור אינטרנט המותאם יותר לאינטרסים שלהן. הן מאמינות שהשליטה הדומיננטית של המערב במידע היא חלק מאסטרטגיה גדולה יותר של הגמוניה, ולא רק תהליך שצמח מתוך כישלון המדינה להחזיק בלעדית במדיה. בעוד הן יכולות לדכא את האזרחים שלהן, הן אינן יכולות לדכא מקורות מידע זרים. רוסיה וסין השקיעו רבות בצָנזור טכנולוגיות, אך גם ביקשו הסכמה בינלאומית להגדרת מידע כנשק שחובה לפקח עליו. האינטרנט יוצר לחצים פוליטיים שלא קל למשטרים רודניים לשלוט בהם, והוא יכול להוות איום עליהם (באיזה היקף – זוהי שאלה אחרת). מאמצים נרחבים אלה להגביל את הגישה למידע ולהחליש את ארצות־הברית הם ההקשר הפוליטי של 'פליים'.

באותו זמן לערך ש'פליים' ו'סטקסנט' משכו תשומת לב כה רבה, תוכנת ריגול נוספת הצליחה לחמוק בשקט. שירות פרוקסי פופולרי (שמאפשר למשתמשי אינטרנט לחמוק מפיקוח ממשלתי) נפגע כך שכל אדם שהוריד את תוכנת הפרוקסי הוריד גם תוכנה זדונית שסיפקה את שם המשתמש ואת שם המחשב, ותיעדה את כל הקשות המקלדת. התוכנה הזדונית Simurgh פגעה באלפי אנשים. החוקרים שאיתרו אותה – אנשי Munk Schoolשבאוניברסיטת טורונטו – מאמינים שהיא נועדה למתנגדי משטר איראניים וסוריים.[12] התוכנה הזדונית יצרה סיכון גבוה הרבה יותר מאשר 'פליים', אך לא זכתה להתייחסות כה מרעישה, וה־ITU לא הוציא אזהרה גלובלית בעקבותיו. הסבר אפשרי לחריגות זו הוא ש'פליים' מתאים לסדר־יום פוליטי רחב יותר מאשר Simurgh.

הקשר בין 'פליים' לבין משא־ומתן בינלאומי על אבטחת הסייבר (ומשילות אינטרנט), מספק רקע חשוב למאמצים הרב־צדדיים להפוך את מרחב הסייבר לבטוח יותר. אחד ההיבטים שלא זכו לתשומת לב בפרשנות הציבורית בנושא לאחרונה הוא שהסיכון החדש ממתקפת סייבר הפך לחלק מסדר־היום הבינלאומי בתחום האבטחה כבר לפני שנים אחדות, כאשר החלו לצוץ הסיכונים הביטחוניים והצבאיים מקישוריות גלובלית במהירות גבוהה. מרחב הסייבר, שכמעט אינו נשלט או מאובטח, הפך עתה מקור לחוסר יציבות בינלאומית. מדינות חוששות מהסלמה שתהפוך בהיסח הדעת לעימות קינטי (צבאי) נרחב יותר מאשר מההשפעה המעשית של מתקפת סייבר, בהתחשב בפוטנציאל המוגבל לנזק שהיא נושאת. דיאלוג רציני בנוגע לאפשרויות הפחתת הסיכון מתקיים לפחות מאז שרוסיה הפעילה טכניקות סייבר נגד אסטוניה ב־2007. ה"מתקפות" נגד אסטוניה ב־2007 היוו סכנה רבה יותר ליציבות הבינלאומית מאשר 'סטקסנט', שכן הן איימו לעורר עימות מזוין בין מדינות נאט"ו לבין רוסיה.

כתוצאה מכך, מתקיימים דיונים בפורומים רשמיים רבים בשאלה כיצד להפחית את הסיכון ולהגביר את היציבות, ביניהם קבוצת מומחי הממשל מטעם האו"ם (UN's Group of Government Experts), הארגון למען יציבות ושיתוף פעולה באירופה (Organization for Stability and Cooperation in Europe), הפורום האזורי של אסיה (Asian Regional Forum) וועידת לונדון (London Conference Process. ארגון מדינות אמריקה (Organization of American States) ערך מפגשים בנושא אבטחת סייבר. ארצות־הברית, רוסיה וסין מעורבות בדיאלוגים בנושא, וארצות־הברית משתתפת בדיונים דומים עם בעלות־בריתה הקרובות. תיאורם של 'סטקסנט' ו'פליים' כסכנה חמורה חדשה הוא אמצעי רטורי להשגת יתרון במשא־ומתן, יותר מאשר ניתוח רציני של מצב הביטחון הבינלאומי.

מסקנות

צבאות שמצטיינים בקדמה טכנולוגית יצרו טכניקות סייבר, ויעשו בהן שימוש כדי לקדם את האינטרסים שלהם. גם אם אין מדובר ב"לוחמה", בכל זאת קיים עימות. אם 'סטקסנט' ו'פליים' מהווים סיכון כלשהו, הסיכון הוא שחוסר ידע צבאי ורקע הולם למשא־ומתן על אבטחת סייבר, לצד מה שנראה כאמונות טפלות בנוגע למתקפת סייבר – הם אלה שיסכלו את המאמצים להפוך את מרחב הסייבר לבטוח ויציב יותר. 'סטקסנט' ו'פליים' לא היו אפוקליפטיים. למעשה הם אינם חדשים במיוחד, וודאי שאינם מבשרי עידן חדש של לוחמה. הטכנולוגיה מעצבת מחדש את הלוחמה מאז המהפכה התעשייתית. אולי הדבר אינו לרוחנו, אך נדיר שמדינות וארגונים חמושים ינטשו יכולת חדשה. מדינות עשויות לדחות נשק להשמדה המונית, אך למעט זאת הכל קביל, ומתקפת סייבר אינה יוצאת מכלל זה. מדינות ימשיכו לנהוג כפי שתמיד נהגו, ופשוט ינצלו טכנולוגיות חדשות להשגת מטרותיהן.

הערות

1 ניתן להגדיר פעולת סייבר זדונית כתוכנה שנשלחת באמצעות רשתות דיגיטליות להשגת גישה לא־חוקית למחשבי היעד, ומבצעת פקודות ללא הרשאת הבעלים.

2 James A. Lewis, Katrina Timlin, "Cybersecurity and Cyberwarfare," UNIDIR Resources, 2001, www.unidir.org/pdf/ouvrages/pdf-1-92-9045-011-J-en.pdf

3 ספרו של קליפורד סטול (Clifford Stoll): *The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage* (New York: Doubleday, 1989) מספק פרטים על ריגול סייבר סובייטי בשנות השמונים. אמנם התקיים דיון ציבורי מועט בלבד על מתקפות סייבר מצד ארה"ב נגד סרביה בשנות התשעים, אך פקידים אמריקניים סיפקו פרטים בראיונות.

4 US Cyber Consequences Unit, "Overview by the US CCU of the cyber campaign against Georgia," August 2009, http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf.

5 The Guardian, "Militarisation of Cyberspace: How the Global Power Struggle Moved Online," April 2012, http://www.guardian.co.uk/technology/2012/apr/16/militarisation-of-cyberspace-power-struggle

6 ראו לדוגמה:
Steve DeWeese, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, Northrop Grumman, October 2009.

7 רוברט אופנהיימר, המדען שעמד בראש פרויקט פיתוח פצצת האטום, ציטט משפט זה מתוך ה"בהגאוואד גיטה" (Bhagavad Gita), בעקבות הניסוי המוצלח הראשון.

8 תרחישי "סייבר־בדומה־לגרעין" כרוכים בשרשרת ארוכה של הנחות מפוקפקות על ההשפעה הפוליטית של מתקפה ועמידות המטרה. לדיון מפורט, ראו:
James Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats," CSIS, December 2002, http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf.

9 ראו לדוגמה:
Robert Wright, "How Obama's Cyberweapons Could Boomerang," *The Atlantic*, June 2012; Misha Glenny, "We will Rue Stuxnet's Cavalier Deployment," *Financial Times*, June 2012, http://www.ft.com/cms/s/0/6b674600-afc7-11e1-a025-00144feabdc0.html#axzz25KCLvt33;
או:
Jason Healy, "Stuxnets are not in the US National Interest: An Arsonist Calling for Better Fire Codes," Atlantic Council June 2012.
שימו לב שהאירוע שעורר זעקה זו לא היה המתקפה עצמה אלא סיפור חדשותי על המתקפה, שממחיש את תפקידה של המדיה בדיונים אלה. רעש תקשורתי אינו מדד טוב לסיכון ממשי.

10 "ITU Teams Up with Kaspersky Lab for ITU Telecom World 2012," http://www.kaspersky.com/about/news/business/2012/ITU_Teams_Up_with_Kaspersky_Lab_for_ITU_Telecom_World_2012.

11 Kaspersky Lab and ITU Research Reveals New Advanced Cyber Threat," http://www.kaspersky.com/about/news/virus/2012/Kaspersky_Lab_and_ITU_Research_Reveals_New_Advanced_Cyber_Threat/.

12 Munk School of Global Affairs, "Iranian Anti-Censorship Software 'Simurgh' Circulated with Malicious Backdoor," May 2012, https://citizenlab.org/2012/05/iranian-anti-censorship-software-simurgh-circulated-with-malicious-backdoor-2/.

התרת אפקט ה־'סטקסנט':
על המשכיות ושינוי בשיח על איומי הסייבר

מרים דאן קוולטי

מבוא

זה שנים אחדות שאיומי סייבר נמצאים על סדר היום הפוליטי והביטחוני. זמן לא רב לאחר שחוקרי מכון RAND, ג'ון ארקווילה ודויד רונפלדט, דיברו על כך ש"הלוחמה הקיברנטית (לוחמת סייבר) מגיעה!",[1] הפך צירוף המילים "לוחמת סייבר" לסיסמה הבולטת ביותר בשיח בנושאי מחשבים, ביטחון לאומי ומרחב קיברנטי (cyberspace). נתונה לחסדי האירועים וההתרחשויות שבכותרות, גברה ההתעניינות בנושא כל אימת שדווח באמצעי התקשורת על שימוש אגרסיבי במחשבים; היא שבה ודעכה כאשר נושאים אחרים תפסו את מרכז הבמה.

בשנת 2010 נפל דבר. הסטקסנט (Stuxnet), תולעת המחשב המתוחכמת שנוצרה כדי לחבל במערכות השולטות ומבקרות תהליכים תעשייתיים, הסעירה את הקהילה הבינלאומית במגוון דרכים והזניקה את נושא הסייבר אל מרחב החששות של הציבור ואל ראש רשימת האיומים. התוצאה היא, שעוד ועוד מדינות רואות במתקפות סייבר את אחד האיומים הביטחוניים העתידיים המרכזיים, אם לא הגדול שבהם. באיזו מידה מוצדקת ראייה זו, ומה באמת שינתה תולעת הסטקסנט בשיח?

מטרתו של מאמר זה לתת תמונה מאוזנת של תופעת לוחמת הסייבר. אדגים כיצד ומדוע התפתחה לוחמת הסייבר מהתפיסה הצרה, הנוגעת אך ורק לאינטראקציה צבאית, למשמעותה הרחבה, שנעשתה מנותקת ממלחמה במובנה הפשוט ומקיפה כמעט כל פעילות הנוגעת לשימוש אגרסיבי במחשבים. בעיקר תיעשה במאמר זה הבחנה בין צורות שונות של עימות סייבר, שתשמש בסיס להערכת סיכונים מיושבת ושקולה. בהמשך יודגם כיצד השיח על איומי הסייבר מתאפיין, ככל הנראה, בפחות מדי שינוי וביותר מדי המשכיות מכפי שנוטים

ד"ר מרים דאן קוולטי עומדת בראש יחידת המחקר 'הסכנה החדשה' במכון ללימודי ביטחון, ציריך, שוויץ.

מאמר זה ראה אור לראשונה ב**צבא ואסטרטגיה**, כרך 3, גיליון 3, דצמבר 2011, עמ' 11–18.

להודות כיום. דימוי האיום נשאר יציב משלהי שנות התשעים של המאה ה־20, ותולעת הסטקסנט לא חוללה שינוי משמעותי במצב הזה. הדבר נכון גם בנוגע לאמצעי־נגד מתוכננים או חזויים.

הֶקשרים ומשמעויות של לוחמת סייבר

חשיבותו של המושג לוחמת סייבר והשפעתו ניתנים להבנה בצורה הטובה ביותר בהקשר הרחב של מהפכת המידע, שעיצבה – ועדיין מעצבת – את התפיסות בדבר הזדמנויות וסכנות. בייחוד דומה כי הטכנולוגיות של מהפכת המידע וחידושים ארגוניים נלווים בשנות השמונים והתשעים שינו את אופי העימות ואת סוגי המבנים, הדוקטרינות והאסטרטגיות הצבאיות. לפיכך נראה כי מושג זה מרמז על הופעתה של לוחמה מסוג "חדש", שבה גורם המידע נהפך בהדרגה לחשוב יותר ויותר. התפתחות זו התאפשרה (אם לא הונעה) מסיומה של המלחמה הקרה וההגדרות המחודשות שבאו בעקבותיה למונחים כמו אויבים, מחשבה אסטרטגית והוצאה על ביטחון.

מלחמת המפרץ הראשונה, בשנת 1991, יצרה קו פרשת מים בכל הנוגע לחשיבה צבאית על לוחמת סייבר. עימות זה נתפס בעיני אסטרטגים צבאיים (בעיקר אמריקנים) כעימות הראשון בדור חדש של עימותים, שבהם הניצחון איננו מובטח רק בכוח הזרוע, והוא גם פועל יוצא של היכולת לנצח במלחמת המידע ולהבטיח "דומיננטיות של מידע". בעקבות מלחמה זו פורסמו אינספור ספרים בנושא,[2] והתגובה להתפתחויות הטכנולוגיות אחרי מלחמת המפרץ מצאה ביטוי גם במאמרי דוקטרינה חדשים שמיסדו את מרכיב המידע.

תחילה התאפיין השיח באופוריה רבה. אבל זמן קצר אחר־כך ניתנה תשומת לב רבה יותר לסיכונים הכרוכים בהתפתחות זו: גיבוש אסטרטגיות שלא מוקדו עוד ביכולת האויב, אלא סימנו את "זרימת המידע של היריב", הדגישו את הפגיעות הגבוהה יחסית של כוחות אמריקניים מרושתים. עם התקדמות הדיון על התקפות על מערכות מידע עוינות אפשריות, נידונו בהרחבה גם הסכנות האפשריות לרשתות נתונים אזרחיות. ארצות־הברית, כמעצמת־העל היחידה שנותרה, נתפסה כמי שנועדה מראש להפוך למטרה ללוחמה א־סימטרית. חשש נרחב קנה לו אחיזה בקרב הקהילה האסטרטגית, ולפיו אלו הצפויים לנחול כישלון נגד מכונת המלחמה האמריקנית עלולים לתכנן לפגוע קשות בארצות־הברית באמצעות תקיפת נקודות חיוניות שלה מבית, דהיינו תשתיות חיוניות[3]. המושג תשתית חיונית מכיל מגזרים כמו מידע וטלקומוניקציה, שירותים פיננסיים, אנרגיה ותשתיות, תחבורה ועוד רכיבים המשתנים ממדינה למדינה ובמהלך הזמן.[4] רוב המגזרים הללו מסתמכים על מרחב שלם של מערכות בקרה מבוססות תוכנה לפעולתם החלקה, האמינה והרציפה.

עם גידולן של רשתות מחשב והתרחבותן לעוד ועוד היבטים של חיי היומיום, השתנתה מטרת ההגנה ממה שנתפס כרשתות קנייניות מוגבלות (ממשלתיות, בעיקר צבאיות), אל החברה בכללותה – או ליתר דיוק, אל דרך החיים שלה, המתאפשרת באמצעות תת־המבנה הבלתי מופרע של הטכנולוגיה.[5] על בסיס זה התפתח איום הכולל שני צדדים הקשורים בקשר גומלין זה לזה. ראשית, פרספקטיבה פנימית, ולפיה עצם הקישוריות של מערכות תשתית מציבה סכנות מכיוון שהפרעות בתוכן עלולות להתפתח לאסונות גדולים במהירות רבה. חידושים בטכנולוגיית מידע ותקשורת הגבירו אפוא את הפוטנציאל לאסון של ממש בתשתיות חיוניות באמצעות הגדלה ניכרת באפשרות שסיכונים מקומיים יהפכו לסיכונים מערכתיים. שנית, פרספקטיבה עם מבט כלפי חוץ מתמקדת בהגברת הנכונות של שחקנים זדוניים לנצל נקודות תורפה בלא היסוס או מגבלות. מאחר שמערכות תשתית חיוניות משלבות ערכים סמליים ואינסטרומנטליים, התקפתן הופכת לחלק חשוב בהיגיון המודרני של השמדה, המבקשת להשיג השפעה מרבית.

ממד הסייבר גם מעצב מחדש את המרחב למשהו שאינו נטוע עוד במקום או בנוכחות. "האויב" הופך לישות מרוחקת ונטולת פנים, נעלם גדול שכמעט בלתי אפשרי לאתרו. מצב זה מוביל לשני מאפיינים חשובים של ייצוג האיום: ראשית, יכולת ההגנה על מרחב מתבטלת – אין מקום מוגן מפני התקפה או מפני התמוטטות קטסטרופלית. שנית, האיום הופך אוניברסלי כביכול משום שהוא נמצא כעת בכל מקום.

הפנומנולוגיה של הסייבר

לאור האמור לעיל, אין זה מפתיע לגלות, כי החשש מפני איומי סייבר הוא גדול כל כך. אך כל משקיף יוכל להיווכח עד כמה האיומים הם בלתי מוגדרים. לאחר שחרג מגבולותיו הצבאיים, הפך המושג מטושטש מאוד: לוחמת סייבר מתייחסת כעת לכל תופעה הכרוכה בשימוש הרסני או משבש בצורה מכוונת את עבודת המחשבים.

ערפול קונספטואלי שכזה מקשה עלינו להבין מה קורה בעימותים "סייבריים",[6] ואילו סוגים של אמצעי־נגד נדרשים להתמודדות עם אירוע ספציפי. ברוס שנייר (Bruce Schneier), טכנולוג אבטחה ומחבר בעל שם בינלאומי, מבחין בין סייבר־ונדליזם (cybervandalism), כלומר השחתה של אתר אינטרנט; סייבר־פשע (cybercrime), תופעה של גנֵבת קניין רוחני, סחיטה המבוססת על איום בתקיפה מסוג מתקפה מבוזרת למניעת שירות (DDoS), מרמה המבוססת על גנבת זהות וכיוצא באלה; סייבר־טרור (cyberterrorism), פריצה למערכת מחשב כדי לגרום להתכת כור גרעיני, לפתיחת סכר, או כדי לגרום להתנגשות בין שני מטוסים; ולוחמת סייבר (cyberwar).[7] שנייר משתמש במונח לוחמת סייבר במובן של

שימוש במחשבים לשיבוש פעילויות של מדינת אויב, ובייחוד התקפות המכוונות על מערכות תקשורת.

הסיווג של שנייר בונה מערך של איומי סייבר מתעצמים ומסלימים – משלב אחד בסולם לזה שבא אחריו, ההשפעות האפשריות וכן ההיקף והעוצמה מסלימים. בשנים האחרונות נוכחנו לגלות כי סייבר־ריגול (cyberespionage) וסייבר־חבלה (cybersabotage) נעדרים מהסולם. עם זאת יצוין, שקווי הגבול בין הפעילויות השונות מטושטשים מאוד. כאשר מתרחש אירוע שגרם נזק, קשה לקבוע אם הנזק הוא תוצאה של התקפה זדונית, פגם ברכיב מסוים או תאונה. על אף המטרות השונות, הכלים והטקטיקות המשמשים צבאות, ארגוני טרור ועבריינים במרחב הסייבר – דומים מאוד, אם לא זהים. פירוש הדבר, במקרה של התרחשות התקפה, קשה מאוד לזהות מי עומד מאחוריה ובאיזה סוג של תופעה מדובר.

יודגש שוב, הקושי בהבחנה בין התופעות השונות אין משמעו שההבחנה איננה נחוצה; ההפך הוא הנכון. **ראשית,** היתרון בתפיסה של "חומרת ההשפעות" שהיא מסייעת לקובעי מדיניות לתעדף בתיאוריה – דבר חשוב ביותר. רק התקפות מחשב שתוצאותיהן הרסניות או גורמות שיבושים חמורים צריכות להיחשב סוגיה של ביטחון לאומי, ולפיכך מחייבות תשומת לב הניתנת לאירועים שמהווים איום קיומי. מתקפות הגורמות לשיבוש של שירותים לא חיוניים, או שהן בעיקר מטרד יקר, אינן נכללות בקטגוריה זאת.[8] שנית, הגדרה צרה ומדויקת מסייעת לעקוף סכנות אחרות הטמונות בתיוג אירוע מסוים כ"מלחמה", למשל לפטור קורבנות של התקפה מאחריותם להשלכות הנובעות מרשלנותם שלהם בכל הנוגע לאבטחת מחשב או יצירת לחץ להשיב מלחמה נגד "פורצי מחשבים", אמיתיים או מדומים.[9] שלישית, הגדרת התופעות מדגימה בבירור היכן מרכז הכובד – בחקירות מחשב קפדניות. יש לחקור כל אירוע בקפדנות. כפי שמציין שנייר: "בדיוק כשם שכל מקרה של ירי אינו בהכרח פעולה מלחמתית, כך כל מתקפת אינטרנט מוצלחת, בלי קשר למידת חומרתה, אינה בהכרח פעולה של לוחמת סייבר. מתקפת סייבר המשתקת את רשת החשמל עשויה להיות חלק ממערכה של לוחמת סייבר, אך היא גם עשויה להיות פעולה של סייבר־טרור, סייבר־פשע או אפילו – אם היא מבוצעת בידי נער בן ארבע־עשרה שלא מבין באמת מה הוא עושה – סייבר־ונדליזם. הסיווג הספציפי מותנה במניעים של מחולל המתקפה ובנסיבות ההתקפה [...] בדיוק כמו בעולם האמיתי".[10]

הערכת סיכונים

הדברים לעיל מעלים את השאלה: עד כמה נמצאים אנו במצב של סכנה? עימותים במרחב המדומה הם בבחינת מציאות זה יותר מעשור – בכל עימות פוליטי, כלכלי וצבאי יש היבטים המתרחשים בתוך האינטרנט וסביבו. יתרה מכך, פעילויות

פליליות ופעילויות ריגול בעזרת טכנולוגיות מידע ותקשורת מתרחשות בכל יום. אך בכל ההיסטוריה של רשתות מחשבים, היו רק דוגמאות בודדות להתקפות חמורות שהיה להן הפוטנציאל לשבש או אף שיבשו בפועל – בצורה חמורה – פעילויות של מדינה. בודדות יותר הדוגמאות למתקפות סייבר שגרמו לאלימות פיזית נגד בני אדם או רכוש. הרוב המכריע של התקפות הסייבר הן מדרגה נמוכה וגורמות אי־נוחות, ולאו דווקא לשיבוש חמור או לשיבוש לטווח ארוך. למעשה ברור כיום, כי הסבירות להתרחשותה של לוחמת סייבר "טהורה" (או אסטרטגית) נמוכה ביותר, וסבירות גבוהה יותר מיוחסת למתקפות על מערכות מחשבים בשיתוף עם צורות התקפה אחרות, פיזיות.[11]

האם הערכה זו השתנתה בשנה החולפת? סיווג התולעת סטקסנט אכן מהווה אתגר. מסתובבים אלפי סיפורים והשערות על התולעת, על מקורותיה ועל כוונותיה.[12] סיפורים כתובים ברמה זו או אחרת, וכולם מכילים חלקי תצרף (פאזל) שאינם ניתנים לחיבור מלא ושלם. חלקי התצרף מרמזים על כך שרק למדינה אחת או לכמה מדינות – ההיגיון הרגיל של "מי צפוי להרוויח" מצביע על ארצות־הברית או על ישראל – היו היכולת והאינטרס לייצר ולשחרר את תולעת הסטקסנט כדי לחבל בתוכנית הגרעין של איראן. אף־על־פי שהעולם לא יידע כנראה לעולם לבטח מי עומד מאחורי קוד התוכנה הזה, מרבית המתכננים האסטרטגיים נכונים להאמין כי "מהלומה דיגיטלית ראשונה" התרחשה, ותיבת פנדורה הווירטואלית נפתחה.

עם זאת, גם אם נניח את התרחיש הקיצוני ביותר, ולפיו רוב המדינות בעולם פיתחו נשק סייבר יעיל ורב עוצמה, או יצליחו לפתח נשק מסוג זה בעתיד הקרוב (הנחה המוטלת בספק), עצם קיומן וזמינותן של יכולות כגון אלה אין פירושו שייעשה בהן בהכרח שימוש. נראה כי תחום הסייבר מוביל בני אדם להניח, כי מאחר שיש להם נקודות תורפה הן בהכרח ינוצלו. בכל זאת, בנושאי אבטחה וביטחון יש לבצע הערכת איומים קפדנית. הערכה כזאת מצריכה העמקה יסודית בשאלה: "למי יש האינטרס והיכולת לתקוף אותנו, ומה הוא צפוי להרוויח מכך?" בעבור מדינות דמוקרטיות רבות, הסיכון של מלחמה נדחק לשוליים. הסיכון של מתקפת סייבר בהיקפים החמורים ביותר צריך להישקל באותה הרצינות.

התרת אפקט תולעת ה'סטקסנט'

פרסום הקוד של תולעת הסטקסנט ופרטים רבים נוספים כבר הובילו להתקפות של מערכות מחשבים רבות נוספות. לפיכך מערכות SCADA – מערכות מחשב המנטרות ומפקחות על תהליכים תעשייתיים ותשתיתיים – צפויות לשמש מטרה לכל פורץ מחשבים בעתיד הנראה לעין. למצב זה נלווית סכנה אינהרנטית של תופעות מכוונות ולא מכוונות – אם כי חשוב לציין כי השיח בנושא תשתיות

חיוניות עוסק באיום על מערכות ה־SCADA זה יותר מעשור. כמו כן, מזה זמן רב מצפים מומחים לאירוע בסדר גודל רציני במרחב הסייבר. מנקודת מבט זו, תולעת הסטקסנט איננה הפתעה גדולה, אלא דווקא אישור למה שדנו בו וחששו מפניו במשך שנים. אף־על־פי שהיא מיקדה את תודעת הפוליטיקאים בשלבים היותר חמורים של איומי הסייבר, באופן זמני לפחות אין היא משנה את הסבירות להתרחשות אירוע של סייבר־טרור או לוחמת סייבר.

תולעת הסטקסנט גם אינה משנה את השיטות והכלים הזמינים להתמודדות עם איומי סייבר. הכוונה למשל לאמצעי אבטחת מידע, או לפעילויות המגוונות והרבות, המושגים והתהליכים הנכללים ב"הגנה על תשתיות חיוניות" (CIP). ההתייחסות ל־CIP דומה למדי במדינות רבות:[13] מבוקשות שותפויות הדוקות עם המגזר העסקי ועם שותפים בינלאומיים, בעיקר כדי להחליף מידע בנוגע לאיומים שונים ולמגוון סוגיות. לאחרונה גם ניכרת התרחקות מהמושג "הגנה", ומעבר לשימוש במושג "גמישות".[14] גמישות איננה מושג חדש כמובן, אך עלייתו הנוכחית מלמדת על שינוי חשוב בחשיבה. בעוד אמצעי הגנה נועדו למנוע התרחשות של שיבושים, הגמישות מקבלת את העובדה ששיבושים מסוימים הם בלתי נמנעים.

לחשיבה כזאת נודעת חשיבות רבה, ועליה להיות מושרשת בתודעת הפוליטיקאים ובתודעת כלל האוכלוסייה. רשתות מידע לעולם אינן יכולות להיות "מוגנות" מן ההיבט של הביטחון הלאומי. ההפך הוא הנכון: שומה על תקריות סייבר להתרחש, מכיוון שאין דרך להימנע מהן. במילים אחרות: אפילו ההגנות המושלמות ביותר לא יוכלו להבטיח ששום דבר חמור לא יתרחש בעולם המרושת.

מדינות נוטות להגיב בכוח לאתגר כזה ומנסות להגביר את רמת הביטחון בכל האמצעים. אך אין לטעות ולראות במרחב הסייבר עוד "תחום" שאפשר לנקוט בו פעולה צבאית לפי שיקול דעת. כדי שיהיה אפשר להמשיך ליהנות מיתרונותיו של עידן הסייבר, חשוב ללמוד באופן מעשי איך לחיות עם חוסר ביטחון. מלבד מגבלות משפטיות ואסטרטגיות, שיובאו ודאי בחשבון בכל התלבטות אם להשתמש במתקפות סייבר ככלי נשק אם לאו, המכשולים הגדולים ביותר צריכים להיות חששות מפני השלכות שליליות שאינן ניתנות לשליטה. ראשית, השלכות עלולות להיווצר ישירות עקב התלות ההדדית בין משאבים חיוניים שונים. שנית, השלכות שליליות עלולות להיות מורגשות באמצעות ההשפעה של אמון מעורער במרחב הקיברנטי, מה שיגרום להשלכות מזיקות לכלכלה העולמית.[15]

באמצעות העברת סוגיה מסוימת, במשתמע או במפורש, לתחום של ביטחון לאומי ופעולות צבאיות, נוטים להכפיף אותה לכללי משחק סכום אפס, שבהם הרווח של צד אחד הוא ההפסד של הצד האחר. עם זאת, ההיגיון של מרחב הסייבר הוא אחר. בדומה לפיקוח על החלל והימים, הפיקוח של מרחב הסייבר מחייב נורמות עולמיות מוסכמות. הדרכים הזמינות כיום ל"בקרת נשק" בזירה זו הן בעיקר

חילופי מידע וגיבוש נורמות, בעוד הניסיונות לאסור לחלוטין את האמצעים של לוחמת סייבר, או להגביל את הזמינות של נשק־סייבר צפויים להיכשל. הקשיים לא צריכים למנוע מהקהילה הבינלאומית לאמץ מגבלות אחראיות וריסון עצמי בשימוש בנשק הסייבר, ולחשוב על דרכים חדשות וחדשניות לשפר את ההגנה על רשתות מחשב חיוניות בלי להפריע ליכולתו של הציבור לחיות ולעבוד בביטחון באינטרנט.

הערות

1 John Arquilla and David F. Ronfeldt, "Cyberwar is Coming!", *comparative Strategy* vol. 12, no. 2 (1993), pp. 141-165.

2 Greg Rattray, *Strategic Warfare in Cyberspace*, Cambridge 2001; Michael O'Hanlon, *Technological Change and the Future Warfare*, Washington 1999.

3 Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*, London 2008.

4 Elgin Brunner and Manuel Suter, International CIIP Handbook 2008/2009, Zurich: Center for Security Studies, 2009.

5 Myriam Dunn Cavelty, "Cyber-Security", in Peter Burgess (ed.), *Routledge Handbook of New Security Studies*, London 2010, pp. 154-162.

6 Chris Demchak, "Cybered Conflicts as a New Frontier", *Atlantic Council*, October 28, 2010, http://www.acs.org/new_atlanticist/Cybered-conflict-new-frontier

7 Bruce Schneier, "Schneier on Security: A Blog Covering Security and Security Technology," Post: "cyberwar," June 4, 2007, http://www.schneier.com/blog/archives/2007/06/cyberwar.html

8 Cf. Clay Wilson, *Computer Attack and Cyber-terrorism: Vulnerabilities and Policy Issues for Congress, Congressional Research Report for Congress*, Washington 2003; Dorothy Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," in John Arquilla and David F. Ronfeldt (eds.), *Networks and Netwars: The Future of Terror, Crime and Militancy*, Santa Monica 2001, pp. 239-288.

9 Martin Libicki, *Defending Cyberspace and Other Metaphors*, Washington 1997, p. 38.

10 Schneier, http://www.schneier.com/blog/archives/2007/06/cyberwar.html

11 Peter Sommer and Ian Sommer, "Reducing Systemic Cybersecurity Risk, OECD/IFP Project on Future Global Shocks, 2011," www.oecd.org/dataoecd/3/42/46894657.pdf

12 שתי דוגמאות בולטות הן:
Mark Clayton, Stuxnet malware is 'weapon' out to destroy ... Iran's Bushehr nuclear plant? September 21, 2010, http://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant; William J. Broad, John Markoff and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, January 15, 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

13 Myriam Dunn Cavelty and Manuel Suter, "Public-Private Partnerships are no Silver

Bulled: An Expanded Governance Model for Critical infrastructure Protection", *International Journal of Critical Infrastructure Protection* Vol. 2, No. 4 (2009), pp. 179-187.

14 Christine Pommerening, "Resilience in Organizations and Systems: Background and Trajectories of an Emerging Paradigm", in *Critical Thinking: Moving from infrastructure Protection to infrastructure Resilience*, *CIP Program Discussion Papers Series*, (Washington 2007), pp. 9-22.

15 Andrew Rathmell, "Controlling computer Network Operations", *Information & Security: An International Journal* 7 (2001), pp. 121-144.

איום ארגוני הטרור במרחב הסייבר

גבי סיבוני, דניאל כהן, אביב רוטברט

מבוא

סרט הראינוע הראשון שהוצג בפני קהל נעשה על ידי האחים לומייר ב־1895. הסרט הראה רכבת נכנסת לתחנה, לכאורה לכיוון הצופים באולם. הצופים, שהיו משוכנעים שהרכבת מתקרבת אליהם, צרחו בבהלה וברחו מהבניין. בסרט הקולנוע הראשון שהוקרן אי פעם, נדמה היה לצופים שהם רואים מולם מציאות.[1]

איום טרור הסייבר הוא נושא בו מתערבבים לעיתים המציאות והדמיון. אם נבחן את אחת התפיסות המרכזיות במרחב הסייבר – ההתמודדות עם איומי טרור – ניווכח כי רציונל התפיסה (שהחלה להתפתח לאחר אירועים מעצבים מתחילת שנות האלפיים, כגון "באג המילניום" ופיגועי 11 בספטמבר 2001) הוא שהעולם נראה כבשיאו של תהליך הנמצא מעֵבר לעידן המודרני והטכנולוגי – עידן הנעדר גבולות מגוננים, ובו מדינות חדירות למידע, לרעיונות, לאנשים ולחומרים; בקיצור, עולם פתוח. הטרור שנלקח בחשבון באיום הייחוס בעולם כזה הוא טרור מסוג חדש: איום, בו טרוריסט הנמצא במרתף נידח בקצה העולם הוא בעל פוטנציאל נזק המשנה לחלוטין את מאזן הכוחות על ידי יכולת חדירה למערכות ביטחוניות או כלכליות חשובות בכל מדינה ומדינה ברחבי העולם והשגת מידע רגיש מהן, כמו גם יכולת לגרום להרס של מערכות.[2]

האם המציאות של 11 בספטמבר 2001, בה ארגון טרור התכונן במשך כשנתיים לפיגוע, כולל הכשרת טייסים בקורס טיס, שלבסוף השתמשו בסכינים יפניות פשוטות לבצע מגה פיגוע, יכול לחזור על עצמו במרחב הסייבר? האם תרחיש, בו ארגון טרור ישלח קבוצת טרוריסטים כסטודנטים לקורסים רלוונטיים במדעי

ד"ר גבי סיבוני הינו חוקר בכיר וראש תכנית לוחמת סייבר במכון למחקרי ביטחון לאומי. דניאל כהן הינו עמית מחקר ומתאם תכנית לוחמת סייבר במכון למחקרי ביטחון לאומי. אביב רוטברט הינו מלגאי תכנית ניובאוור במכון למחקרי ביטחון לאומי ותלמיד לתואר שלישי בבית הספר למדעי המחשב באוניברסיטת תל־אביב.

המחברים מבקשים להודות לנעם ק. מהמטה הקיברנטי הלאומי, לדורון אברהם וקרן ח'טקביץ, מתמחים בתכנית לוחמת סייבר במכון למחקרי ביטחון לאומי, על סיועם בהכנת מאמר זה.

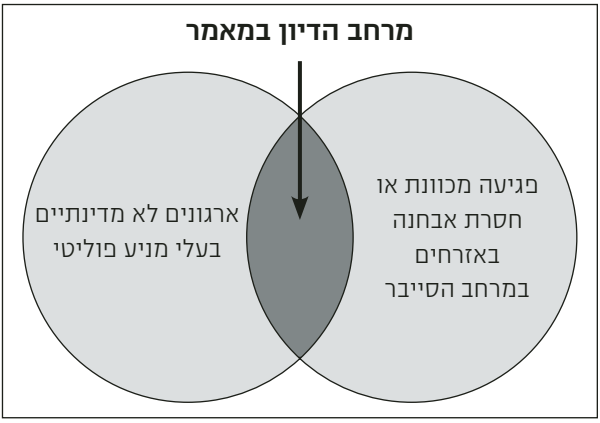
מאמר זה ראה אור לראשונה ב**צבא ואסטרטגיה**, כרך 5, גיליון 3, אפריל 2013, עמ' 3-25.

המחשב, יחמש אותם באמצעים טכנולוגיים נגישים לכל, ויבצע באמצעותם ובאמצעות היכולות שרחשו מגה פיגוע טרור במרחב הסייבר הוא מציאותי או דמיוני? כדי לתת מענה לשאלה זו יש לבחון, ראשית, מהן היכולות ששחקן לא מדינתי מסוגל להשיג והאם יכולות אלו עלולות להוות איום ממשי על ביטחונן הלאומי של מדינות. ניתוח האיומים העיקריים שבפניהם עומדת מדינה, בראייה רב־שנתית ולאור שינויים צפויים במאזן האסטרטגי שלה, מחייב הצגת הגורמים המאיימים על המדינה, תוך זיהוי שורשי האיום וסיבותיו.

אין עוררין על כך שגורמים לא מדינתיים, ארגוני טרור ועבריינים ממנפים את מרחב הסייבר למטרותיהם ומפיקים תועלת מתחום שבו כולם ניצבים באותה נקודת זינוק, תחום המאפשר גם לשחקנים יחידים קטנים להשפיע, ובאופן שאינו נמצא ביחס ישר לגודלם. אסימטריה זו מייצרת סביבה סכנות שונות, שבעבר לא משכו את תשומת הלב ואת האנרגיות של המעצמות. השאלה היא האם פעילותם של גורמים אלה במרחב הסייבר היא איום בעל פוטנציאל לנזק גדול ורחב היקף? ואם כן, מדוע הוא לא התממש עד כה?

מאמר זה יבחן האם התקפות של ארגוני טרור במרחב הסייבר, שהשפעתן עד היום היא בדרך כלל טקטית, יוכלו להשתדרג (ואולי כבר השתדרגו) לכלל יכולת להפעיל נשק סייבר בעל השפעות אסטרטגיות, נשק היכול לגרום נזק רחב היקף ו/או לאורך זמן, מהסוג ש"מוריד מדינות על ברכיהן" וגורם למערכות קריטיות לקרוס. מטרת מאמר זה היא לדון באיום הטרור במרחב הסייבר ולבחון את אמיתות התפיסות שהתגבשו בשנים האחרונות כלפי איום זה.

המאמר מתרכז בפעולות של ארגונים לא מדינתיים בעלי סדר יום ומטרות פוליטיות, גם אם אלה מופעלים או נתמכים לעיתים על ידי מדינות. זאת, כדי להבדיל בין אותם ארגונים לבין פעולות המבוצעות ישירות על ידי מדינות שאינן בתחום עיסוקו של מאמר זה, או על ידי ארגוני פשיעה או ארגונים אחרים בעלי מטרות שהן בעיקר בעלות אופי פלילי. לצורך המאמר, פעולת טרור של ארגון לא מדינתי במרחב הסייבר תוגדר כפעולה במרחב זה, שמטרתה לפגוע באופן מכוון או חסר אבחנה באזרחים. כך, לדוגמה, פעולה לשיבוש אתר אינטרנט של בנק מסחרי על ידי ארגון לא מדינתי, שלו מטרות פוליטיות, תוגדר כפעולת טרור במרחב הסייבר. לצורך המחשה ניתן להתבונן בתרשים הבא, המתאר את מרחב הדיון במאמר זה:



המתודולוגיה של המחקר

מספר אבני דרך נדרשו לצורך בחינת פעילותם של ארגוני הטרור במרחב הסייבר. הראשונה שבהן הייתה זיהוי המניעים לשימוש במרחב הסייבר במסגרת המאבק הפוליטי אותו מנהלים ארגוני הטרור. כך ניתן לזהות שני מניעים עיקריים לשימושים אלה: הראשון הינו השימוש במרחב הסייבר לצרכי תמיכה בפעילות הטרור, ובעיקר לצרכי גיוס כספים ופעילים, או לצורך הלבנת כספים לצרכי הפעילות; השני הינו השימוש בכלים במרחב הסייבר שיספקו את הפגיעה בפועל ביעדים שקבע לעצמו ארגון הטרור, וזאת לצד שימוש באמצעים אלימים אחרים. כאן נבחן שיתוף הפעולה שבין ארגונים לא מדינתיים לבין מדינות המפעילות אותם והתומכות בפעילות הטרור שלהם.

אבן הדרך השנייה של המחקר חייבה בחינה והבנת עומק של היכולות עליהן יכולים ארגוני הטרור להניח יד. זאת, מתוך הבנה שלא כל מפעיל מחשב, יהיה זה גאון טכנולוגי ככל שיהיה, יוכל לייצר פיגוע טרור אפקטיבי ומשמעותי, ותוך בחינת ההנחה שפגיעה משמעותית במרחב הסייבר תמשיך להיות נחלתן של מדינות עתירות טכנולוגיה ומחייבת משאבים לא מבוטלים – הן מודיעיניים והן טכנולוגיים. עם הבנת סל היכולות הטכנולוגיות והמודיעיניות הרלוונטיות של ארגוני הטרור, נדרש היה לבחון האם זוהו פעולות של ארגונים כאלה בפועל. לבסוף, נעשה ניתוח של כלל הממצאים במטרה לגבש תובנות והמלצות מסכמות כחלק מהמענה.

ניתוח יכולות

מרחב הסייבר מסייע להעמקת ידע ורכישת יכולות. בנוסף, הטכנולוגיה מסייעת ליצירת רשת תקשורת אנונימית.[3] כמו כן, מרחב הסייבר משמש מצע להרחבת

השותפים לפעילות טרור. לעומת גיוס פעילי טרור במרחב הפיזי, מרחב הסייבר מאפשר הגדלה משמעותית של מאתר המשתתפים בפעילות, גם אם במקרים רבים נעשה שימוש בשותפים "משוטים", המופעלים על ידי ארגונים ומדינות באצטלה של פגיעה בממסד. תופעות כאלו ניתן היה לראות באירועי התקיפה של האקרים על יעדים ישראליים ב־7 באפריל 2013,[4] כאשר חלק מהפעילים במתקפה קיבלו הכוונה, באמצעות אתרי אינטרנט בכיסוי, באשר לשיטות הפעולה וליעדים לתקיפה. שימוש בתחושות אנטי־ממסדיות של צעירים, כמו גם בתחושות כלליות נגד המערב או מדינת ישראל, מאפשר הרחבה משמעותית של מאתר הפעילים וכן מייצר מסה משמעותית המאפשרת את פעולת טרור הסייבר. לדוגמה, נטען שבמבצע "עמוד ענן" נרשמו יותר ממאה מיליון מתקפות סייבר על אתרים ישראליים,[5] וכי פעילים לא מעטים הופעלו במהלך אותו מבצע ובהתקפות המשך שלו, באמצעות הכוונה שמאחוריה עמדו ככל הנראה איראן וגרורותיה.[6]

סל היכולות והאמצעים של ארגוני טרור במרחב הסייבר מוגבל מצד אחד בשל קשר הדוק ונגישות טכנולוגית, שהינה בדרך כלל נחלתן של מדינות בעלות יכולות טכנולוגיות מתקדמות ושל חברות בעלות יכולות טכנולוגיות משמעותיות, ומן הצד השני – נגיש לשוק החופשי המאפשר מסחר בכלי נשק קיברנטיים ובמידע בעל ערך לתקיפה. גורם מסייע בבניית יכולות אלו הוא מדינות התומכות בטרור, המעוניינות להשתמש במתווך (Proxy) כדי להסתיר את זהותן כיוזמות תקיפה על יעד מסוים. בנוסף, נדרש ארגון הטרור להכשרת מומחים ולצבירת ידע על שיטות איסוף מודיעין, שיטות תקיפה ואמצעים להסוואת כלי תקיפה, כדי לחמוק ממערכות הגנה ביעד.

המחקר מראה שעד עתה אין לארגוני הטרור את התשתית המדעית והטכנולוגית העצמאית לפיתוח כלי סייבר בעלי יכולות לגרום נזק משמעותי, וכי הם חסרים את היכולת לבצע איסוף מודיעין איכותי למבצעים (מל"ם). היכולות של ארגוני הטרור לקיים פעילות פוגענית במרחב הסייבר ייבחנו, אפוא, תחת אילוצים אלה.

ככלל, יש להפריד בין שלושה מרחבי תקיפה בסיסיים: תקיפה של שער הארגון, בעיקר אתרי אינטרנט, וזאת באמצעות תקיפות, מניעת שירות או השחתה של אתרים; תקיפה של מערכות המידע הארגוניות;[7] ולבסוף, התקיפה המתוחכמת (והמורכבת) ביותר – תקיפת מערכות הליבה המבצעיות[8] של הארגון, הנוגעות לליבה התפעולית שלו, למשל מערכות בקרה תעשייתיות.[9] טרור הסייבר נגד מדינה ואזרחיה יכול להתבצע במספר רמות תחכום, כאשר בכל רמה נדרשות יכולות הן בהיבט הטכנולוגי והן בהיבטי ההשקעה בצד התוקף. הנזק שאפשר לגרום נמצא ביחס ישיר לרמת ההשקעה.

תקיפת שער הארגון

כאמור, ברמה הבסיסית ביותר ניתן לתקוף את שער הארגון, כלומר את אתר האינטרנט שלו, החשוף לציבור. הרמה הפשוטה ביותר של טרור קיברנטי מתאפיינת בהתקפות המונעות שירות, מפריעות לשגרת החיים, אך לא גורמות לנזק מהותי, בלתי הפיך או מתמשך. התקפות כאלו מכונות "התקפות מניעת שירות מבוזרות" (DDoS –Distributed Denial of Service), ומהותן היא גרימת עומס פניות אל מחשב או שירות אינטרנטי מסוים, באופן שחורג מסף היכולת שלו לספק מענה. בכך משיגים למעשה השבתה של השירות. פניות תמימות ואמיתיות לא ייענו, מכיוון שהשירות עמוס בהתמודדות שלו עם הפניות מצד התוקף.

התקפות DDoS אותן יבצע ארגון טרור[10] נדרשות להיות אפקטיביות ולהימשך פרק זמן סביר, כדי שמספר רב ככל האפשר של אנשים יבחינו במתקפה וייפגעו ממניעת השירות. יעדים מתאימים למתקפה כזו יכולים להיות, בין היתר, בנקים, שירותי סלולר, חברות טלוויזיה בכבלים ובלווין, ושירותי בורסה (מסחר וחדשות). לרשימה זאת ניתן להוסיף גם אפליקציות סלולריות נפוצות, ששיבוש הגישה אליהן יכול לגרום למטרד, דוגמת: WAZE, גישה לשירותי דואר אלקטרוני וליומן פגישות, וגם אפליקציות לשיחות על גבי רשת האינטרנט (Voice Over IP).

שיטה נוספת לתקיפת שער הארגון היא תקיפות על שרתי DNS – שרתים המשמשים לניתוב תעבורת האינטרנט. תקיפה כזו תביא לכך שאנשים המבקשים לגשת לאתר או לשירות מסוים יגיעו בפועל לאתר אחר, אליו התוקפים מעוניינים לנתב את התעבורה. תקיפה דומה אך פשוטה יותר יכולה להתבצע ברמת המחשב הבודד במקום ברמת שרת ה־DNS הכללי; כלומר, התקשורת ממחשב בודד תנותב לאתר של התוקף במקום לאתר האמתי אליו המשתמש מנסה לגלוש. הנזקים שתקיפות כאלו יכולות לגרום נעים מגניבת מידע, דרך מניעת שירות מלקוחות וכתוצאה מכך פגיעה עסקית בשירות שהותקף, ועד פגיעה תדמיתית בשירות: התוקף יכול להפנות את התעבורה אל דף המכיל תעמולה ומסרים אותם הוא רוצה להציג לציבור.

שיטה פופולרית ויחסית פשוטה לפגיעה תדמיתית בשער הארגון היא השחתת אתר האינטרנט שלו. ההשחתה (Defacement) כוללת שתילת מסרים פוגעניים בעמוד הראשי, הכנסת תעמולה שהתוקפים מעוניינים להפיץ לקהל רחב ופגיעה תדמיתית (ואולי גם עסקית) בארגון, הנתפס כלא מוגן ולא מאובטח מפני תוקפים פוטנציאליים.

תקיפת מערכות המידע של הארגון

רמת הביניים במדרג הפגיעה במרחב הסייבר מכילה תקיפות של מערכות המידע והמחשוב של הארגון, דוגמת שרתים, מערכות מחשב, מאגרי נתונים, רשתות

תקשורת ומכונות לעיבוד נתונים. התחכום הטכנולוגי הנדרש ברמה זו גבוה יותר מהנדרש לצורך תקיפת שער הארגון. רמה זו מחייבת השגה של נגישות למחשבי הארגון דרך עובדים בארגון או באמצעים אחרים. הנזק אותו ניתן לגרום בסביבה הווירטואלית כולל פגיעה בשירותים חשובים כמו בנקים, שירותי סלולר ודואר אלקטרוני.

קו ברור מפריד בין התקיפות המתוארות כאן ובין האיומים של הטרור הקיברנטי הפיזי: בדרך כלל לא ניתן לצפות בתקיפות אלו לנזק פיזי, אולם ההסתמכות על שירותים וירטואליים והנגישות אליהם עלולה בכל זאת לייצר פגיעה משמעותית. דוגמה לכך ניתן לראות בתקיפה באמצעות וירוס המחשבים Shamoon,[11] שפגע במחשבי חברת הנפט הסעודית ערמקו (Aramco) באוגוסט 2012. התקיפה, גם אם לא פגעה במערכות הליבה המבצעיות של החברה, הצליחה להשבית עשרות אלפי מחשבים ברשת הארגונית שלה, תוך גרימת נזק משמעותי באמצעות מחיקת מידע ממחשבי הארגון והאטת פעילותו לאורך זמן.[12]

תקיפת מערכות הליבה המבצעיות של הארגון

הרמה הגבוהה ביותר במדרג סיכון התקיפה הינה התקיפה של מערכות הליבה המבצעיות והתפעוליות של הארגון. לדוגמה, ניסיון פגיעה בתשתיות קריטיות פיזיות כמו תשתיות הולכת מים, חשמל, גז, דלק, מערכות בקרה על תחבורה ציבורית, או מערכות תשלומים בנקאיות. זאת, על ידי מניעת אספקת השירות החיוני לזמן מסוים, או במקרה החמור אף גרימה של נזק פיזי באמצעות פגיעה במערכות הפיקוד והבקרה של הארגון הנתקף.

מתקפה מוצלחת עלולה לגרום לשחרור חומרים מסוכנים לאוויר ולפגיעה פיזית באוכלוסייה גדולה. זוהי הנקודה בה פיגוע וירטואלי עלול לייצר נזק פיזי, וההשפעות עלולות להיות הרסניות. בעקבות חשיפת ה־Stuxnet עלתה המודעות לצורך להגן על מערכות בקרה תעשייתיות, אך מכאן ועד יישום בפועל של פתרונות הגנה עדיין הדרך ארוכה. את הפער הזה יכולים לנצל גורמי טרור, למשל על ידי יצירת קבוצת מומחים מתחומי המחשוב ואוטומציה של תהליכים, לצורך יצירת וירוס המסוגל לפגוע במערכות אלו.[13]

דרך נוספת להשגת נשק קיברנטי־פיזי עשויה להתפתח מהשוק השחור של נשק הסייבר ומהתרחבותו גם לתחום של תשתיות פיזיות, וזאת בנוסף על הנשק הווירטואלי אותו הוא מציע כבר היום. יש לציין כי עד כתיבת שורות אלו, תרחיש זה טרם התממש בפועל, אך מכיוון שמדובר בנשק קיברנטי מורכב ויקר, ייתכן והמסחר בו מתנהל במחשכי האינטרנט באופן חשאי.[14] זוהי, כאמור, המדרגה הגבוהה ביותר של פיגוע סייבר, והעלויות והנזקים הנגרמים ממנו הם גבוהים בהתאמה, כפי שניתן ללמוד מהתולעת Stuxnet.[15]

פיתוח יכולות תקיפה, בין של מדינות ובין של ארגוני טרור, מחייב תמהיל מתעצם של יכולות לפעולה במרחב הסייבר בשלושה מרכיבים עיקריים: יכולות טכנולוגיות, יכולת הכוונה מודיעינית לקביעת היעדים (ייצור מטרות) ויכולת מבצעית.

יכולות טכנולוגיות

אופייה המבוזר של רשת האינטרנט מקל מאד על הסוחרים בנשק קיברנטי. ואכן, האקרים וסוחרים רבים מנצלים את היתרונות הללו ומציעים כלי סייבר ושירותי תקיפה במרחב הסייבר לכל דורש. כך התפתח שוק מגוון ומשוכלל מאד של סחר במוצרי סייבר למגוון מטרות, כאשר טווח המחירים נע בין דולרים בודדים לתקיפה פשוטה וחד־פעמית של מניעת שירות, לאלפי דולרים עבור שימוש בחולשות שאינן מוכרות ויכולות לאפשר לתוקף דילוג לתוך מערכת מחשב מוגנת ביותר. שוק זה צומח בזכות מרחב הסייבר, על גבי תשתיות של רשתות חברתיות ופורומים המאפשרים תקשורת אנונימית בין סוחרים לקונים.[16] תופעה מעניינת לה אנו עדים בתקופה האחרונה היא יציאתם של סוחרים אלה ממחשכי הרשת האפלה אל האור. ניתן למצוא אותם ברשת החברתית הפופולרית ביותר, "פייסבוק".[17] בבלוג של חברת אבטחת המידע RSA[18] מתוארת מציאות חדשה, שבה הסוחרים מציעים את מרכולתם לא רק כמוצר, אלא כשירות שלם הכולל התקנת שרתי פיקוד ובקרה, הדרכה על השימוש בכלים ואפילו הנחות ומבצעים ואפשרות לרכוש רק מודולים מסוימים מתוך כלי התקיפה, כדי להוזיל את המחיר. במצב זה של פריחת השוק נשאלת השאלה, האם וכיצד ארגוני טרור יכולים לעשות שימוש לתועלתם בכל הידע והכלים שהצטברו בשוק הפשיעה הקיברנטי?

כדי לענות על שאלה זו, נצטרך לבחון את הפער בין שפע הכלים והיכולות המוצעים כיום למכירה חופשית באינטרנט, לבין הצרכים של ארגוני טרור. השוק של כלי התקיפה כיום מוכוון לארגוני פשיעה קיברנטית, ובעיקר לצרכי הונאות, גניבת כסף מחשבונות בנק תמימים והתחזות, תוך איסוף פרטים של כרטיסי אשראי, מספרי חשבון בנק, תעודות זיהוי וכתובות מגורים, סיסמאות כניסה לאתרים פיננסיים ועוד. כלים אלה לא מתאימים בהכרח לצרכי ארגון הטרור. עם זאת, ארגוני טרור רבים יכולים לכלול גם מרכיבים של ארגון פשיעה קיברנטי כדי לאסוף כסף למימון פעילות הטרור המרכזית שלהם. המטרה המרכזית של ארגוני הטרור – גרימת נזק משמעותי והפחדה – יכולה להתבצע במספר דרכים, בדרגות קושי וחומרה שונות. הכלים מעולם הפשיעה הקיברנטית יכולים לסייע רבות בתקיפות לשיבוש שירות (DDoS), או בגניבת כמויות גדולות של מידע רגיש מחברות שאינן מוגנות מספיק (למשל מידע על כרטיסי אשראי ממאגרי מידע לא מאובטחים) – דבר שיעורר, קרוב לוודאי, חרדה בציבור. יחד עם זאת, גרימת נזק

למערכות הבקרה דורשת כברת דרך נוספת מצדם של הטרוריסטים, שכן משימתם מורכבת הרבה יותר מגניבת כרטיסי אשראי וכלי הפשיעה הקיברנטיים לא משרתים אותה. באשר לרמת הביניים שתוארה לעיל, הנוגעת לפגיעה במערכות המידע של הארגון, נראה כי קיימים בעולם הפשיעה כלים היכולים לסייע לטרור הסייבר. אמנם, נדרשת התאמה מסוימת של כלים אלה, כמו למשל התאמה מגניבת מידע למחיקת מידע, אולם מדובר בכברת דרך קטנה יותר, שמַפתחי הווירוסים יסכימו, קרוב לוודאי, לבצע אותה עבור ארגוני טרור תמורת תשלום מתאים.

יכולת הכוונה מודיעינית

אחד המרכיבים המרכזיים בתהליך תכנון פיגוע קיברנטי הוא בחירת יעד או קבוצת יעדים שהפגיעה בהם תביא ליצירת האפקט הרצוי מבחינת ארגון הטרור. לצורך זה על גוף הטרור לרכז רשימת גופים המהווים פוטנציאל ליעדי פגיעה. כבר כיום קיימת טכנולוגיה חינמית שמספקת כלים המקלים על ביצוע משימה זו. למשל, באמצעות הרשתות החברתיות "פייסבוק" ו"לינקד־אין", ניתן לאתר מיהם העובדים באגפי המחשוב של חברות תשתית, חברות מזון ועוד. אם ניקח לדוגמה את חברת החשמל, מחקרים אקדמיים[19] מראים כי ניתן למפות ללא קושי רב את אגפי החברה, לאתר את העובדים במחלקות השונות ולברור את העובדים להם יש גישה למערכות המבצעיות של החברה.[20] אם עובדים אלה מודעים לחשיבותה של אבטחת המידע ולא ניתן בשל כך לתקוף אותם ישירות, אפשר לאתר בני משפחה וחברים שלהם באמצעות "פייסבוק" ולתקוף דרכם את היעד המבוקש. רשתות חברתיות מהוות מקור חשוב לריגול ואיסוף מידע עסקי ואישי על חברות וארגונים,[21] וארגוני טרור יכולים לעשות בקלות שימוש במידע המופץ בהן לתועלתם.

קיים גם צורך למפות את מערך המחשוב של הארגון המותקף, להבין אילו מחשבים מחוברים לרשת, אילו מערכות הפעלה ותוכנות הגנה מותקנות בהם, אילו הרשאות יש לכל מחשב, ודרך אילו מחשבים ניתן לשלוט במערכת הבקרה של הארגון. לדוגמה, אם ארגון טרור ירצה לשלוט על התפקוד של טורבינת ייצור חשמל, המשימה המוטלת עליו, אף על פי שהיא טכנית יותר וקשה יותר ממיפוי המבנה הארגוני של החברה, קלה היום במיוחד לאחר פרסום עבודתו של האקר "כובע לבן" שערך את "מפקד האינטרנט" הראשון בהיסטוריה.[22]

באמצעות רשת ענפה של רובוטים (תוכנות המושתלות על מחשבים וממתינות לפקודה ממרכז הפיקוד והבקרה איתו הן מתקשרות), ערך אותו האקר רשימה של 1.3 מיליארד כתובות IP הנמצאות בשימוש, ועל חלקן הוא פרסם גם נתונים טכניים, כמו סוג השערים הפתוחים, לאילו בקשות מגיבות הכתובות הללו ועוד. תוצאות המפקד מפורסמות באינטרנט באופן חופשי לכל דורש. עבור האקר בעל

כוונות זדון, אלה לפעמים כל הנתונים הנדרשים כדי לבצע תקיפה ולהשתלט על מערכת מחשב שלמה של אדם פרטי או ארגון. כך ניתן למפות מבנה ארגוני של חברה, ואם הרשת שלה אינה מוגנת מספיק – גם לדלות מידע על המחשבים הנמצאים בשימוש עובדי החברה.

הגנה טובה ומודעות לאבטחת מידע יכולות להקשות מאד על האקרים וטרוריסטים לבצע את הפעולות שתוארו לעיל. ארגונים להם מערכות מבצעיות קריטיות מפעילים לרוב שתי רשתות מחשוב: האחת חיצונית, המקושרת לאינטרנט, והשנייה פנימית, המנותקת פיזית מהאינטרנט ומחוברת למערכות הבקרה התעשייתיות של הארגון. מִפקד האינטרנט אינו מכיל נתונים על רשתות פנימיות מבודלות, מכיוון שהן לא נגישות דרך האינטרנט. תקיפה של רשתות אלו דורשת מודיעין, משאבים ומאמץ גדול מאד, וספק אם קיימים ארגוני טרור המסוגלים לבצע תקיפות כאלו. כאן באה לעזרתם של ארגוני הטרור עבודת מחקר נוספת שנערכה על ידי חוקרים מאוניברסיטת ברלין,[23] המציגה על גבי מפה של "גוגל" (שמציעה לחוקרים, כחלק משירות המפות שלה, להציג ולשתף מידע גיאוגרפי שאספו) מספר רב של מערכות בקרה תעשייתיות (ICS) הפרוסות בכל העולם ומחוברות לרשת האינטרנט. המידע המוצג במפה לקוח מתוך מאגר מידע עצום הנגיש בחינם לכל דורש דרך האתר Shodan,[24] אשר הופך את חייו של האקר טרוריסט לקלים יותר. שירות זה נעזר במידע אותו אספה חברת "גוגל" לצורך שירותי המיפוי והפרסום מבוסס־המיקום שלה, והפכה אותו לנגיש לציבור. ייתכן שהאקרים שפרצו לאחרונה לרשתות ביתיות של מאות ישראלים עשו שימוש בשירותיו של אתר Shodan כדי לאסוף מודיעין לתקיפה, ואולי גם כדי להשיג כלים (תחמושת קיברנטית) לביצועה בפועל.[25]

יכולת מבצעית

לאחר איסוף המודיעין וייצור או רכישה של הכלים הטכנולוגיים לקראת התקיפה, על מתכנני הטרור הקיברנטי לעבור לפעילות אופרטיבית. זהו השלב של ביצוע התוכנית בפועל, המנוהל באמצעות וקטור תקיפה.[26] הכוונה במושג זה היא לשרשרת פעולות המתבצעות על ידי התוקפים, כאשר כל פעולה מהווה מדרגה אחת בדרך ליעד הסופי וכוללת, בדרך כלל, שליטה מלאה או חלקית על מערכת מחשב או על מערכת בקרה תעשייתית. בווקטור תקיפה לא ניתן לדלג על מדרגות, וכדי להתקדם למדרגה מסוימת, יש לוודא שכל השלבים שלפניה הסתיימו בהצלחה.

השלב הראשון בווקטור תקיפה הוא, בדרך כלל, יצירת נגישות ליעד. שיטה נפוצה מאד ומוצלחת ליישומו במרחב הסייבר מכונה Spoofing[27] או זיוף. יש דרכים שונות לעשות שימוש בשיטה זו, כאשר המשותף לכולן הוא זיוף הזהות

של שולח הודעה כדי שנמען ההודעה יבטח בתוכן ולא יהסס לפתוח קישור בתוך ההודעה. למשל, קל מאד לשלוח דואר אלקטרוני לעובד בחברת החשמל, שהוזכרה לעיל, כאשר השולח המזייף משתמש בכתובת של עמית לעבודה, בן משפחה או אדם קרוב אחר. מטרת התוקף במקרה זה היא לגרום לנמען ההודעה לבטוח בתוכן ההודעה ולפתוח דבוקות המצורפות אליה, או להיכנס לכתובות אינטרנט המופיעות בתוכה.

זיוף דואר אלקטרוני הוא שיטת תקיפה הקיימת שנים רבות. בהתאם לכך גם פותחו אמצעי הגנה נגדה אלא שגם התוקפים צברו ניסיון. כיום ניתן להצביע על אירועים שבהם נשלח דואר אלקטרוני הנראה תמים לחלוטין, תפור לנמען ומכיל התייחסות אישית אליו, ובתוכו קיימים מסמכים הנוגעים ישירות לתחום עיסוקו. כתובת השולח במקרים אלה הייתה מזויפת והופיעה ככתובת של עמית לעבודה. ברגע שהנמען פתח את הדואר האלקטרוני, המחשב שלו נדבק בווירוס ללא ידיעתו.

שיטת הזיוף יכולה להועיל כאשר היעד הוא מחשב המחובר לרשת האינטרנט ויש אפשרות לשלוח אליו הודעות, אך במקרים מסוימים לא זה המצב. רשתות המוגנות ברמה גבוהה יהיו, בדרך כלל, מנותקות מהעולם החיצון באופן פיזי, כלומר לא יהיה קישור פיזי (גם לא אלחוטי) ביניהן ובין רשת בעלת רמת אבטחה נמוכה יותר. במקרה כזה יצטרך התוקף לנקוט צעד אחר או נוסף בווקטור התקיפה – הדבקת רשת היעד בווירוס באמצעות החדרתו על גבי מכשירים שפועלים גם ברשת הלא מוגנת וגם ברשת המוגנת. דוגמה לכך הם התקני Disk On Key, המשמשים כאחסון נייד ונוח של קבצים. כאשר התקפה כזו מצליחה, התוקף משיג גישה אל ציוד טכנולוגי השייך לקורבן (מחשב, מחשב כף יד, טלפון חכם), והשלב הראשון בווקטור התקיפה – יצירת נגישות ליעד – מסתיים. בתרחישים מסוימים הצעד הזה הוא החשוב והמשמעותי ביותר מבחינת התוקף. למשל, כאשר הושגה בדרך זו נגישות לרשת מבצעית של חברה, ומטרתו של הטרוריסט היא לחבל באותה הרשת ולמחוק מתוכה מידע, האתגר העיקרי הוא להשיג גישה ליעד. פעולת המחיקה והחבלה קלות יותר, בהנחה שהווירוס שהושתל ברשת מופעל ברמת הרשאות מספיק גבוהה. אך בתרחישים מורכבים יותר, כאשר הטרוריסט מעוניין לגרום נזק משמעותי ולהשיג אפקט הפחדה גדול יותר, נדרשת השקעה לא מבוטלת בצעדים הבאים בווקטור התקיפה.

חברת "לוקהיד־מרטין", שהייתה קורבן להתקפת סייבר, מציעה מתודולוגיה לניתוח פעולות התקפיות במרחב הסייבר, אותה היא מכנה "שרשרת הקטל הקיברנטית".[28] על פי מתודולוגיה זו, מתקפת סייבר מורכבת בנויה משבע אבני דרך, המקבילות לפעולות של הכנת המבצע ויצירת וקטור התקיפה. הצעד הראשון הוא איסוף מודיעין על היעד. לאחר מכן יש לבחור את כלי הנשק הקיברנטי המתאים לתקיפה, ואז לשגר אותו אל היעד. הצעד הבא כולל ניצול חולשה אצל מחשב

היעד, שתאפשר לשתול קובץ זדוני במערכת שלו, ולאחר מכן להתקין את הכלי באופן שיוכל לבצע פעולות בתוך המערכת. השלב הבא הוא יצירת תקשורת בין הכלי ובין שרתי הפיקוד והבקרה של התוקף, כדי שניתן יהיה להנחות את הכלי ולקבל ממנו דיווח על המתרחש במחשב הקורבן. השלב האחרון בשרשרת הקטל הוא ביצוע פעולות אקטיביות בתוך מחשב הקורבן, כמו מחיקה, התפשטות של הכלי, השתלטות על התקנים פיזיים הנגישים מהמחשב ועוד. המונח "שרשרת קטל קיברנטית" נבחר במטרה להדגיש כי כדי שהתוקף יצליח לבצע פיגוע קיברנטי, הוא צריך לצלוח את כל אבני הדרך מבלי להתגלות ומבלי שגישתו אל היעד תיחסם.

ארגון טרור המבקש לפגוע במערכות מבצעיות יצטרך לבצע את כל השלבים בשרשרת. אלו הן פעולות מתקדמות ומורכבות שארגוני טרור בדרך כלל לא ידעו לבצע בעצמם. אם היעד מוגן ברמה נמוכה מאד, לא תידרש יכולת טכנולוגית גבוהה מהתוקף כדי לייצר פגיעה או השחתה; אך ברוב המקרים יצטרכו הטרוריסטים לרכוש מוצרים או שירותים מהאקרים מומחים. במילים אחרות, הם יצטרכו לבצע "מיקור חוץ".

טרוריסטים ימצאו בשוק מוצרי הסייבר ההתקפיים יכולות נגישות ליעד שאינן בעלות רשת מבודלת. באותו שוק הם ימצאו גם מוצרי תקיפה, וניתן להניח שימצאו גם מוצרים לניהול מבצעים ברשת היעד (בדומה לממשק הניהול של הסוס הטרויאני SpyEye[29]). למרות כל זאת, טרם זוהו כלים זמינים ברשת המאפשרים תקיפה של המערכות המבצעיות של הארגון. הנגישות לכלים אלה אמנם אפשרית,[30] אך היא משימה הדורשת משאבי כוח אדם רב (מרגלים, פיזיקאים, מהנדסים), השקעה כספית (בפיתוח כלי תקיפה ובדיקתו בתנאי מעבדה על ציוד אמיתי) וזמן רב כדי לאתר חולשות ולבנות וקטור תקיפה מוצלח.

סוגי התקיפות במרחב הסייבר

ניתן לאפיין מספר סוגי תקיפה במרחב הסייבר, הן לפי רמת הנזק הצפויה והן לפי עוצמת ההשקעה המודיעינית, הטכנולוגית והמבצעית. ברוב המקרים קיימת הלימה בין שני המדדים. הסקירה להלן מציירת תמונה של יכולות ארגון שאינו מדינתי לפעול במרחב הסייבר.

תקיפה חובבנית

זוהי פעולה הנעשית באמצעות כלים המוכרים (ברוב המקרים) לחברות אבטחת המידע ומזוהים על ידי תוכנות ההגנה הסטנדרטיות. נגד כלים אלה פותחו הגנות ולפיכך הם עשויים להיות אפקטיביים רק מול מטרות שאינן מוגנות. שימוש בכלים כאלה נעשה, בדרך כלל, למטרות לימוד או משחק בלבד, מכיוון שרק במקרים

נדירים הם יכולים לשמש לגניבת מידע בעל ערך או לחבלה במערכות מחשב מוגנות. אמנם, יש להם יכולות ריגול וחבלה, אך אלו הן ברמת תחכום נמוכה.

תקיפה קלה

זוהי תקיפה שלא מושקעים בה מאמצים רבים, ועיקר הפעילות בה היא חיפוש כלים מוכנים ברשת האינטרנט או רכישתם מידי חברות המתמחות בכך. תקיפות מסוג זה בדרך כלל לא יצליחו לפגוע בגופים בעלי מודעות לאבטחת מידע (גופים מדינתיים, צבאיים, תעשיות מתקדמות), אבל יוכלו לחדור למחשבים פרטיים ולגנוב מהם מידע ואף לחבל בהם. תקיפות אלו הינן ברוב המקרים חד־פעמיות (גניבת קובץ חשוב, מחיקת כונן), אך לעיתים יכולות להיות חלק מתקיפה ארוכה יותר, כמו למשל במקרה של גניבת ה־DNS (Domain Name System) של המחשב המאפשרת מעקב אחר הפעילות שלו ברשת האינטרנט.

הכלים בהם ייעשה שימוש בתקיפה קלה לא יכללו מודולים שונים של תוכנה, אלא רכיב קוד אחד שעלותו זולה, המַבצע את כל הפעולות של הכלי. רכיב קוד זה יהיה כתוב בצורה שלא מאפשרת לשנות או להרחיב בקלות את יכולותיו ויהיה מוכוון מטרה. חיפוש באינטרנט ורכישה בסכומים שלא עולים על כמה אלפי דולרים יוכלו לספק לכל דורש נשק סייבר בעל יכולות מצומצמות.

בקטגוריה זו של תקיפה נכלל גם השימוש ברשת סוכני תוכנה (בוֹטְנֶט) לתקיפות DDoS. יצירת הרשת היא פעולה מורכבת יותר, אך מרגע שנוצרה, היא יכולה לשמש למבצעי DDoS רבים. ניתן גם להשכיר אותה לשימוש לכל דורש לצורך מניעת שירות מאתרים שונים שאינם מוגנים ברמה גבוהה מפני תקיפה כזו.

תקיפה בינונית

זוהי תקיפה המסוגלת לגרום נזק משמעותי, או לבצע פעולות ריגול מתקדמות, אבל בעלות נמוכה יותר מאשר תקיפה חמורה (ראו להלן). בפעולה כזאת לא יהיה, בדרך כלל, שימוש בחולשות ייחודיות חדשות (כיוון שהן יקרות מאד), אלא בחולשות מוכרות או מוכרות חלקית, שיעד התקיפה עדיין אינו מוגן מפניהן. הפעולה לא תכלול מודולים יקרים למימוש ובדיקה, דוגמת אה שפותחו עבור "סטוקסנט". יחד עם זאת, פעולה כזאת, באמצעות מודולים לתקיפה של מערכות מחשב (מחיקה, שיבוש) ומודולים לריגול, יכולה להיות יעילה מאד במסגרת תקיפה בטווחי זמן קצרים למטרות הרס (כי לא ייעשה מאמץ להסתיר את ההרס; הדבר יקר מדי), או לריגול נגד קורבן שלא מאבטח את מערכותיו ברמה גבוהה.

העלות של תקיפה בינונית פחותה משמעותית מעלותה של תקיפה חמורה: פחות שנות אדם, ללא ציוד חומרה ייחודי ויקר להשגה וללא רכישה של חולשות חדשות ויקרות, אלא של חולשות זולות יותר המספיקות לצורך חדירה למערכות

המחשוב של הקורבן, תוך ידיעה שהן עלולות להתגלות ולהיחסם בעתיד הלא רחוק. קטגוריית התקיפה הבינונית כוללת גם וירוסים המסוגלים להתפשט ברשת מחשבים (תולעים) ולהמתין לפקודה מהמפעיל שלהם. מודל תקיפה כזה שימושי במיוחד ליצירת רשת סוכני תוכנה רובוטיים, המשמשת למבצעי DDoS. כמו כן נכללת בקטגוריה זו תקיפת DDoS נגד אתרים מוגנים, הדורשת תחכום מצד התוקף והכרת מערכת ההגנה ביעד.

תקיפה חמורה

המדובר בפעולה שהושקעו בפיתוחה משאבים רבים של כוח אדם, מִחשוב וכסף, ואשר נבדקה באופן יסודי במעבדה קודם להפעלתה. פעולה כזאת מנצלת חולשות לא מוּכרוֹת (אשר יתנו למפעילי התקיפה טווח זמן רחב להפעלתה עד שיתגלו וייסגרו). בדרך כלל זו פעולה שתוּסווה כדי להותיר עקבות מעטות. כלי התוכנה יכיל מספר מודולים, שחלקם עשויים להיות מיועדים לחבל במערכות תוכנה או חומרה ייעודיות שנמצאות אצל הקורבן (למשל "סטוקסנט"), ולא יפעלו בשום מקרה אחר, כדי להפחית אפשרות לזיהוי.

פעולת תקיפה חמורה עשויה להכיל מגוון רחב מאד של מודולים, בהתאם למטרה שאותה היא נועדה לתקוף, כגון מודולי ריגול – חיפוש קבצים או מידע ושליחתו למפעיל; ומודולי תקיפה והסוואת התקיפה – חבלה בצנטריפוגות תוך כדי הטעייה של מערכת הבקרה כדי שתדווח שהן תקינות. העלות של תקיפה כזו תהיה שנות אדם רבות, מִחשוב מתקדם ולפעמים גם מערכות חומרה וציוד בדיקה שנועד לדמות את הזירה בה יפעל הקוד המפַגע, למשל צנטריפוגות עם מערכות בקרה של חברת "סימנס" במקרה של "סטוקסנט".

הטבלה הבאה מסכמת את ההבדלים בין תקיפות הסייבר השונות, וזאת באמצעות רשימת קריטריונים המאפשרת להבחין באופן ברור בין סוגי נשק סייבר על פי מדרג יכולות. הפרמטרים מתחלקים למספר קטגוריות: הראשונה כוללת את מעטפת נשק הסייבר ואת היכולת שלו להגיע אל יעדו ולפעול בו באופן חופשי מבלי שייחסם. שני הפרמטרים הראשונים נכללים בקטגוריה זו. חשיבותם היא בכך שהם מאפשרים סביבת עבודה נוחה לתוקף, היודע שהוא יכול לחדור אל יעדיו ולבצע בהם פעולות בזמן ובאופן הנדרש, מבלי לחשוש מסגירת היכולת או מחשיפה של הנשק והסרתו. שלושת הפרמטרים הבאים מהווים קטגוריה שנייה, המתייחסת ליכולת הנשק הקיברנטי לבצע את פעילותו העיקרית ביעד, בין אם מדובר בגניבת מידע, הריסתו, פגיעה ושיבוש אלקטרוניים או פיזיים. כלי הנשק השונים בקטגוריה זו נבדלים על פי האלגוריתמים שהם מיישמים לטובת ריגול ביעד ועל פי יכולותיהם לשבש מערכות ממוחשבות ופיזיות. יכולת פגיעה פיזית תהווה מדרגה עליונה בקטגוריה זאת. הקטגוריה האחרונה מייצגת שני פרמטרים

הקשורים להתנהלות הכלי בתוך רשת היעד, ומידת היכולת והחופש שהוא נותן למפעיליו לנהל את המבצע ביעד. יכולות גבוהות בקטגוריה זו נחשבות לכאלו שמאפשרות לעדכן את כלי הנשק על ידי שליחת מודולים מרחוק, שינוי הגדרות המשימה, שליחת פקודות לכלי והגדרת יעדים מודיעיניים חדשים עבורו. כמו כן, כלים מתוחכמים יידעו לנהל מבצע איסוף גדול ברשת היעד, על ידי התפשטות בין מחשבים שונים ואיסוף מרוכז ומתואם של מידע מתוכם.

ההבדלים בין תקיפות הסייבר

	תקיפה חמורה	תקיפה בינונית	תקיפה קלה	תקיפה חובבנית
יכולות חדירה למערכות	טובה מאד	טובה	טובה	נמוכה
יכולות הסוואת הפעילות	טובה מאד	טובה	בינונית	נמוכה
יכולות ריגול	טובה מאד	טובה מאד	טובה	בינונית
יכולות פגיעה במערכות מחשוב	טובה מאד	טובה מאד	טובה	נמוכה
יכולות פגיעה במערכות פיזיות המקושרות למערך המחשוב	טובה	נמוכה	נמוכה	נמוכה
יכולות התפשטות	טובה מאד	טובה	נמוכה	נמוכה
יכולות תקשורת מול שרת בקרה	טובה מאד	טובה	בינונית	נמוכה

ניתן ללמוד מהטבלה כי הקריטריונים המבדילים באופן משמעותי את יכולות התקיפה החמורה (המצויה בידי מדינות מעטות) משאר יכולות התקיפה בסייבר הם היכולת להתפשט ברשת, לקיים תקשורת מול שרת הבקרה ולפגוע במערכות פיזיות המקושרות למערכות המחשוב. אלו הן הפעולות הדורשות את התחכום הרב ביותר בייצור תקיפות סייבר. רק מדינות מעטות נגישות לידע וליכולת לייצר כלי נשק מסוג זה. העמודה "תקיפה קלה" בטבלה משקפת את מדרגת הכניסה הנמוכה למרחב הלחימה הקיברנטי. ניתן לראות כי גם כלי נשק קטנים המצויים בידי גורמים לא־מדינתיים מסוגלים לחדור למערכות מחשב בצורה טובה, לבצע ריגול ברמה טובה מאד, ואם הם מיועדים לכך – גם לחבל במערכות המחשב אליהן הם חדרו. מכיוון שיכולת ההסוואה שלהם היא בינונית, הם לא יוכלו לשהות במערכת המותקפת זמן רב כמו כלי נשק כבדים או בינוניים, ולכן יצטרכו להשיג את מטרותיהם בטווח זמן קצר.

פעילות במרחב הסייבר המיוחסת לארגוני טרור

פרק זה מפרט פעולות טרור במרחב הסייבר בהתאם לתיחום שפורַט לעיל, כלומר פעולות שמטרתן פגיעה מכוונת או חסרת אבחנה באזרחים, וזאת באמצעות פעולה במרחב הסייבר של ארגונים לא מדינתיים בעלי סדר יום ומטרות פוליטיות, גם אם אלה מופעלים או נתמכים לעיתים על ידי מדינות.

אחת ההתקפות המתועדות הראשונות של ארגון טרור נגד מערכות מחשוב מדינתיות התרחשה בסרי־לנקה על ידי לוחמי הגרילה "הנמרים הטמילים" ב־1998. שגרירויות של סרי־לנקה ברחבי העולם הוצפו במשך שבועיים בכ־800 הודעות דואר אלקטרוני ביום עם המסר: "אנחנו נמרי האינטרנט השחורים ואנחנו הולכים לשבש את מערכות התקשורת שלכם". יש הטוענים כי מסר זה השפיע על המקבלים אותו וזרע חשש ופחד בשגרירויות.[31] מספר שנים לאחר מכן, ב־3 במארס, 2003, כת יפנית בשם Aum Shinrikyo ("האמת העליונה") ערכה מתקפה קיברנטית מורכבת שכללה השגת מידע רגיש הנוגע למתקני גרעין ברוסיה, אוקראינה, יפן ומדינות נוספות, תוך ניסיון לתקוף את מערכות אבטחת המידע של המתקנים. המידע הוחרם וניסיון התקיפה נכשל לפני שהארגון הצליח לפעול.[32]

תקיפה באמצעות שליח התקיימה בינואר 2009 בישראל. באירוע זה התקיפו האקרים את תשתית האינטרנט של ישראל בתגובה למבצע "עופרת יצוקה" ברצועת עזה. התקיפה בוצעה על יותר מחמישה מיליון מחשבים. בישראל משערים שהיא נעשתה ממדינות שהיו חלק מברית המועצות לשעבר, בהוראה ובתשלום של גורמי חמאס וחזבאללה.[33] בינואר 2012, קבוצת האקרים פרו־פלסטיניים הקוראת לעצמה "Nightmare" הפילה למשך זמן קצר את אתר הבורסה לניירות ערך בתל אביב ואת אתר חברת "אל על" ושיבשה את פעילות אתר "הבנק הבינלאומי הראשון". בהתייחסות לכך מסר דובר חמאס ברצועת עזה כי "החדירה לאתרים ישראליים פותחת מרחב חדש של התנגדות ומלחמה אלקטרונית חדשה נגד הכיבוש הישראלי".[34]

מלחמת האזרחים בסוריה הביאה לפעילות התקפית ערה מצד ארגון "הצבא הסורי האלקטרוני" (Syrian Electronic Army – SEA) – קבוצה אינטרנטית המורכבת מהאקרים תומכי משטר אסד, התוקפת את קבוצות האופוזיציה הסוריות תוך שימוש בטכניקות של מניעת שירותים ומידע או פריצה לאתרים ושינוי תוכנם. הקבוצה הצליחה להוציא לפועל פעולות שונות הפוגעות בעיקר באתרי האופוזיציה הסורית, כמו גם באתרי אינטרנט מערביים. פעילות אחרונה זו שלה מכוונת בעיקר כלפי אתרי מדיה, תרבות וחדשות ברשתות מערביות. הקבוצה הצליחה לפרוץ ליותר מ־120 אתרים, ביניהם *The Financial Times, The Telegraph, The Washington Post, Al Arabia*.[35] אחת התקיפות המשמעותיות והאפקטיביות הייתה באפריל 2013, בעת ש"הצבא הסורי האלקטרוני" פרץ לחשבון הטוויטר של

Associated Press ושתל "ציוץ" מזויף, שבו נאמר שהבית הלבן הופצץ ושבאותה מתקפה נפצע נשיא ארצות הברית. המשמעות המיידית של הודעה זו הייתה צניחה חדה בשווקים הפיננסיים בארצות הברית ובמדד דאו ג'ונס למשך כמה דקות.[36] הארגון גם חשוד בניסיון חדירה למערכות שליטה ובקרה של מערכות מים. כך, למשל, ב־8 במאי 2013 פורסם בסוכנות ידיעות איראנית צילום מסך של מערכת ההשקיה של קיבוץ סער.[37]

במהלך מבצע "עמוד ענן" ברצועת עזה ב־2012 וכן בחודשים שלאחריו, ערכה קבוצת האקרים המכנה עצמה "OpIsrael" תקיפות[38] נגד אתרים ישראליים על רקע הסכסוך הישראלי־פלסטיני, בשיתוף עם "אנונימוס". בין היתר נפגעו אתר משרד ראש הממשלה, אתר משרד הביטחון, אתר משרד החינוך, אתר המשרד לאיכות הסביבה, אתר התעשייה הצבאית, אתר הלשכה המרכזית לסטטיסטיקה, אתר האגודה למלחמה בסרטן, האתר הרשמי של לשכת נשיא המדינה ועוד עשרות אתרים ישראליים קטנים. הקבוצה פרסמה כי הסיבות לתקיפה היו פגיעה בזכויות אדם של פלסטינים והפרת החוק הבין־לאומי על ידי ישראל.

באפריל 2013, קבוצת האקרים פרו־פלסטיניים, בשם "לוחמי הסייבר של עז א־דין אל קסאם" המזוהה עם הזרוע הצבאית של חמאס, לקחה אחריות להתקפה על אתר האינטרנט של חברת אמריקן אקספרס. אתר החברה ספג התקפת DDoS אינטנסיבית שנמשכה כשעתיים ושיבשה את האפשרות של לקוחות החברה להשתמש בשירותיו. בניגוד להתקפות DDoS טיפוסיות, כמו אלה שמבוצעות על ידי "אנונימוס" ומבוססות על רשת מחשבים שנפרצו ואוגדו לבוטנט הנשלט ע"י התוקף, ההתקפה של עז א־דין אל קסאם השתמשה בסקריפטים שהופעלו על גבי שרתי רשת פרוצים, יכולת המאפשרת גיוס רוחב פס גדול יותר לביצוע המתקפה.[39] אירוע זה שייך למגמה הכוללת התעצמות יכולות הסייבר של חמאס, בין השאר, בשכלול המערכה המודיעינית האיסופית כנגד צה"ל, ואיום השתלטות עוינת על מכשירי סלולר של אנשי צבא וחשיפת סודות באמצעותם.[40]

תקיפות סייבר עצמאיות של ארגוני טרור

ניתוח התקפות ארגוני הטרור במרחב הסייבר מראה שסף הכניסה הנמוך למתקפות מסוימות והנגישות לכלי תקיפה קיברנטיים לא הובילו למעבר של ארגוני הטרור לתקיפות בעלות פוטנציאל נזק גדול ומתמשך. ארגוני הטרור פעלו עד כה בעיקר בתקיפת שער הארגון. כלי התקיפה העיקרי היו מתקפות למניעת שירות והתקפות בסדר גודל של תקיפה חובבנית עד תקיפה בינונית. הסיבה העיקרית לכך היא שסל היכולות והאמצעים של ארגוני הטרור במרחב הסייבר הינו מוגבל, ועד עתה אין להם התשתית המדעית והטכנולוגית העצמאית לפיתוח כלי סייבר בעלי יכולות לגרום נזק משמעותי. בהתחשב בכך שארגוני הטרור חסרים את היכולת

לבצע איסוף מודיעין איכותי למבצעים (מל"ם), הסבירות לביצוע תקיפת סייבר משמעותית שלהם נראית נמוכה .

כדי שארגון טרור יוכל לפעול עצמאית ולהוציא לפועל פיגוע משמעותי במרחב הסייבר, יידרשו מגוון יכולות, בהן: יכולות איסוף מודיעין מדויק על היעד, רשתות המחשבים והמערכות שלו; רכישה או פיתוח של כלי סייבר מתאימים; מציאת קצה חוט לחדירה לארגון; הסוואת כלי התקיפה תוך כדי השתלטות על המערכת; ולבסוף – ביצוע המתקפה בזמן ובמקום אשר יפתיעו וישיגו תוצאה משמעותית. נראה שפעולה עצמאית של ארגון טרור, ללא גורם מדינתי התומך בו, אינה דבר מובן מאליו. אולם, אין לגזור מכך גזרה שווה באשר לארגונים הנתמכים ואף מופעלים על ידי מדינות בעלות יכולות משמעותיות.

קיימת אפשרות לתקיפות של ארגוני טרור תוך שימוש במיקור חוץ. אם נבחן את ארגוני הפשע, ניווכח כי ארגונים אלה עשו קפיצת דרך משמעותית בשנים האחרונות. מעבדת קספרסקי (Kaspersky) חשפה לאחרונה קבוצה חדשה של תוקפים, ככל הנראה בהזמנת ארגוני פשע או בהזמנה של מדינה על רקע ריגול תעשייתי. מדובר בקבוצה של האקרים בשם Icefog, המתמקדת בפגיעה בשרשרת האספקה של הארגון בצורה ממוקדת (בשיטת "תקוֹף ובְרח"), בעיקר במגזרי תעשיות צבאיות ברחבי העולם.[41] התפתחות נוספת חלה בתפוצת קודים זדוניים, תוך שימוש של מעבדות פשע ברשת השחורה (DarkNet), שהגבירה את הנגישות לקודים קיימים למטרות תקיפה. ארגוני פשע עושים כבר כיום שימוש בקודים קיימים לתקיפת מערכות פיננסיות על ידי שכפולם והפיכתם לקודי מוטציה.[42]

האפשרות שארגוני טרור יעשו שימוש ויקנו שירותי תקיפה מהאקרים שכירי חרב, וכן יעשו שימוש עתידי בקודי מוטציה, על בסיס וריאציה של קודים קיימים לתקיפת מטרות, היא ריאלית בעתיד הקרוב, ואין להתעלם ממנה בבניית איום הייחוס במרחב הסייבר לתקיפות שער הארגון ואפילו מערכות המידע שלו. לכן, ישנה סבירות גבוהה לכך שבשנים הקרובות תחול התקדמות ביכולות התקיפה הקיברנטית של ארגוני טרור, שיתבססו על רכישת יכולות מתקדמות יותר על ידיהם ותרגומן לתקיפות על מערכות המידע של ארגונים (ולא רק על שער הארגון).

יכולת לבצע מתקפה שתכלול חדירה למערכות המבצעיות ותפגע בהן היא מורכבת למדי. הצורך ביכולות מודיעין ויכולות החדרה ברמה גבוהה, שקיימות רק אצל מספר מדינות מצומצם, גורם לכך שפעולה התקפית תהיה מדינתית, ולכן לא נראתה עד היום התקפה מוצלחת של שחקן לא מדינתי על מערכות הליבה המבצעיות של ארגון כלשהו. אף שתקיפה כזו טרם זוהתה, ניתן לראות עלֶיה במגמת השיפור ביכולות הטכנולוגיות של שכירי החרב הפועלים במרחב הסייבר לצרכי פשיעה והונאה. מתוך כך ניתן להניח, שתמורת תגמול מתאים יסכימו גורמים טכנולוגיים פליליים לייצר כלים שיוכלו לבצע תקיפות על מערכות הליבה

המבצעיות של תשתיות קריטיות ושל חברות מסחריות. גורמים אלה יוכלו להעמיד את מרכולתם גם לטובת ארגוני טרור.

המלצות להתמודדות ברמה הלאומית

מגוון האיומים במרחב הסייבר הוא רחב. ההגנות הבסיסיות מפני איומים אלה לא צריכות להבדיל בצורה מהותית בין מקורותיו של האיום. לכן, המחשבה כי ניתן ליצור הגנה ייעודית במרחב הסייבר דווקא מול איומים של גורמי טרור, נראית לא מעשית. אדרבא, תפיסת המענה לאיומים לפגוע במרחב הסייבר על ידי ארגוני טרור אינה צריכה ואף אינה יכולה להיות שונה מהותית מתפיסת המענה הכוללת לאיומים במרחב זה.

תפיסת ההגנה היסודית בפני איומי הסייבר צריכה להתבסס על מספר מרכיבי יסוד: מודיעין; מענה הגנתי רב־שכבתי; מענה התקפי; הסברה; מענה אזרחי.

מודיעין

מרכיב היסוד הראשון בהתגוננות מפני איומי הסייבר הוא המודיעין, ובמסגרתו איסוף מודיעין שיתבסס על הכָּוונה לאור הערכות מצב. בהקשר זה קיימת חשיבות לזיהוי האיומים ולהכוונת גורמי האיסוף מול מידע הנוגע לגורמי טרור המבקשים לפעול במרחב הסייבר. כפי שנכתב לעיל, במקרים רבים עומדות מדינות מאחורי הפעילות של ארגוני טרור, ולכן מודיעין הנאסף בהקשר המדינתי יוכל לספק מידע גם בהקשר של ארגוני טרור המסונפים או מופעלים על ידי אותה מדינה.

תחום המודיעין מהווה נדבך חיוני מאין כמוהו בהתמודדות עם איומים במרחב הסייבר. היכולת לאסוף ולנתח מידע רב מאפשרת כיום לייצר מודיעין איכותי הן ברמה המדינתית והן, במקרים לא מעטים, ברמת ארגונים ועסקים המנטרים באופן קבוע את רשתות המידע והתקשורת. זאת, כדי לאתר התנהגויות אנומליות העשויות להעיד על תקיפה העתידה להתרחש, או ללמד על פעילות חריגה ברשת המחשבים. בהקשר זה ראוי להדגיש, כי העובדה שמדינה דוגמת איראן תומכת, ולעיתים אף מפעילה, ארגוני טרור, מחייבת את ארגוני המודיעין במערב לנטר לא רק את מדינת היעד אלא גם את הארגונים המסונפים לה. בהקשר של איראן המדובר בחזבאללה, בחמאס, וב"הצבא הסורי האלקטרוני".

מענה הגנתי הכולל מספר שכבות

המדובר בהגנה היקפית ובהגנה על נכסים חיוניים, הכוללת יכולות שימור פעולה גם אחרי חדירה של קוד מפַגע וסיכול מקדים של גורמים פעילים, למשל על ידי חשיפה של מידע מודיעיני לרשויות החוק במדינות בהן מתבצעת הפעילות וביצוע פעילות סיכול באמצעות כלים משפטיים במדינות אחרות. כך יתכן שיבוש של היכולת להפעיל את הקוד המפגע קודם שזה הופץ.

מענה התקפי לאיומים

מרכיב זה בהתמודדות עם איומי הסייבר כולל שני רבדים: הרובד הראשון נוגע ליכולת לפעול התקפית באמצעות מהלומה מקדימה, במרחב הסייבר ולעיתים גם מחוצה לו, כנגד משאבי הסייבר בארגון טרור (תשתיות, מימון, אתרים ופעילים). הרובד השני נוגע ליכולת לבצע פעולת תגמול אחרי התקיפה ואחרי זיהוי מסַפק של הגורמים לתקיפה. מהלומה זו לא חייבת להיות מתוחמת רק למרחב הסייבר ויכולה אף לכלול מרכיבים פיזיים של ממש. בחלק מהמקרים נדרשת הסדרה חוקית של הפעילות ההתקפית, כדי לאפשר אפקטיביות של המענה. במקרים לא מעטים ניתן לזהות את שרשרת הפעולה כאשר מדינות (דוגמת איראן) מפעילות ארגונים לא מדינתיים (דוגמת חזבאללה ו"הצבא הסורי האלקטרוני"), כשכולם יחד מפעילים גורמים בעלי עניין ואף גורמים משוּטים ברשת לצורך הגדלת יכולות התקיפה. הצורך להפעיל מערכת רחבה של תוקפים מחייבת הכְוונה במספר הקשרים: הראשון שבהם נוגע לקביעת המטרות אותן יש לתקוף; השני נוגע לעיתוי התקיפות; והשלישי נוגע לכלים לביצוע ההתקפות. כל אלה מחייבים הקמה של אתרים ופורומים ייעודיים אליהם מופנה המידע. פעילות זו יוצרת נקודת תורפה, מאחר וניתן לפעול לשיבוש ולשיטוי וכך לייצר בלבול, תוך הקהיה של עוקץ התקיפה שתוכנן על ידי מובילי התקיפה.

פעילות הסברה

ניתן להניח שפעילות הסברה לא תהייה אפקטיבית מול הגרעין הקשה של הפעילים בהתקפות הסייבר. לפעילות המניעה ההסברתית שתי מטרות: הראשונה היא הגדלת המוּדעות לאפשרות שתוקפים עלולים להיפגע כתוצאה מפעילות סיכול במדינה בה הם שוהים (למשל, חשיפה שלהם לגורמי האכיפה במדינה); השנייה היא החשיפה של העומדים מאחורי ההתארגנות. כאמור, במקרים רבים התוקפים המשוּטים לא יודעים כלל שהם מופעלים על ידי מדינות וארגוני טרור. לפיכך, באמצעות פעולות כאלו יתכן וניתן יהיה לצמצם במידה מסוימת את היקף התופעה.

ארגון המענה האזרחי במרחב הסייבר

נקודות התורפה של מערכת הסייבר האזרחית בישראל מהוות פְרצה הקוראת לגנב עבור ארגוני הטרור. ההגנות החלשות יחסית על מערכות אלו מאפשרות לארגוני הטרור לפעול באופן שאינו מסובך מול מטרות במרחב זה. מאחר ומערכת הסייבר האזרחית מייצרת חוּלשות מובנות, יש להסדיר את המענה האזרחי במרחב הסייבר, ויפה שעה אחת קודם. יש לציין, בהקשר זה, המלצה של המכון למחקרי

ביטחון לאומי לממשלת ישראל להסדיר את ההגנה של מרחב הסייבר האזרחי באופן שיוכל לספק מענה הולם לאיומים.[43]

ארגוני הטרור טרם חצו את הרף המבצעי והטכנולוגי המאפשר להם לפעול באופן עצמאי מול ישראל ומדינות אחרות במערב בתחום לוחמת הסייבר. אולם, התפתחות שוק התקיפה הפלילי עלולה ליצור יכולות תקיפה משמעותיות. התפתחות זאת, לצד המשענת וההכוונה המודיעינית והמבצעית של מעצמות טכנולוגיות דוגמת איראן, יכולה לגרום לפעילות מסוכנת בתחום הסייבר גם מצדם של ארגוני טרור. לכן, ראוי יהיה לא לזלזל באיום זה. אף שטרם נצפתה פעילות משמעותית של ארגוני טרור בתחום הסייבר, התפתחות האיום בתחום זה מחייבת התארגנות מתאימה.

הערות

1 מיכל אביעד, **קולנוע תיעודי**, תל אביב, חידקל, 2007, עמ' 5.

2 ראו למשל: חיים פס ודן מרידור (עורכים), **הקרב של המאה ה־21: דמוקרטיה נלחמת בטרור**, **פורום עיון**, המכון הישראלי לדמוקרטיה, ירושלים, תשס"ז–2006, עמ' 25.

3 ראו למשל TOR – תוכנה המסייעת ליצירת אנונימיות ברשת. כל שכבה מוצפנת וכל תחנה במסלול מקלפת את השכבה שלה ומעבירה לתחנה הבאה. עיקרון זה נקרא "ניתוב בצל" (The Onion Router – TOR), https://www.torproject.org/

4 Oded Yaron, "Hackers Plan Cyber Attack against Israeli Targets in April", *Haaretz*, March 14, 2013 http://www.haaretz.com/news/diplomacy-defense/hackers-plan-cyber-attack-against-israeli-targets-in-april.premium-1.509214 .

5 "שטייניץ: האיום הצבאי על ישראל הפך גם לאיום טרור סייבר", **גלובס**, 9 ביולי 2013, http://www.globes.co.il/news/article.aspx?did=100086069

6 ראו התבטאות של ראש הממשלה בנימין נתניהו בנושא זה: "נתניהו: גידול משמעותי במתקפות הסייבר מאיראן וגרורותיה", **גלובס**, 9 ביוני 2013, http://www.globes.co.il/news/article.aspx?did=1000851092

7 הכוונה היא לכל מערכת המאחסנת, משנעת או מעבדת מידע ארגוני, בין אם היא מקושרת לרשת האינטרנט ובין אם לא, ובין אם היא מהווה חלק מליבת העשייה העסקית של הארגון ובין אם לא.

8 מערכת ליבה מבצעית של הארגון היא החומרה שעל גביה והתוכנה אשר באמצעותה מנוהלים תהליכי הליבה של הארגון (בין אם הוא ארגון ביטחוני או ארגון עסקי אזרחי). זו מערכת ששיבוש או הריסה שלה יכולים להפסיק את פעילות הארגון או חלקים ממנו, עד כדי גרימה של נזק פיזי במקרים מסוימים.

9 מערכת בקרה תעשייתית (ICS) היא כלי המשלב רכיבי תוכנה וחומרה ונועד לפקח על תהליך פיזי של ייצור תהליכי. המערכת כוללת חיישנים לניטור התהליך המבוקר ופקדים לשליטה על תהליך זה. המערכת עשויה לכלול גם חיבור לרשתות מחשבים אחרות של הארגון ולעיתים אף לרשת האינטרנט.

10 סוג התקפות זה נעשה גם על ידי אקטיביסטים ואנרכיסטים בצורה עצמאית, או בשליחות והכוונה של ארגוני טרור.

11 "Shamoon Virus Targets Energy Sector Infrastructure", *BBC News Technology*, August 17, 2012, http://www.bbc.co.uk/news/technology-19293797

12 באירוע זה הוחדר קוד זדוני למערכת המחשוב של ערמקו, וכתוצאה מכך הושבתו

כ־30,000 מחשבים.

13 ראלף לנגר, הרצאה בנושא אבטחת מערכות בקרה תעשייתיות, ועידת הסייבר השנתית, המכון למחקרי ביטחון לאומי, 4 בספטמבר 2012, http://youtube/sBsMA6Epw78

14 "The Disturbing World of the Deep Web, Where Contract Killers and Drug Dealers Play their Trade on the Internet", *Daily Mail*, October 11, 2013, http://www.dailymail.co.uk/news/article-2454735/The-disturbing-world-Deep-Web-contract-killers-drug-dealers-ply-trade-internet.html .

15 Jesse Emspak, "Why We Won't Soon See another Stuxnet Attack", *Tech News Daily*, July 24, 2011, http://www.technewsdaily.com/7012-stuxnet-anniversary-look-ahead.html

16 Aditya K. Sood, Richard J. Enbody, "Crimeware-as-a-Service – A Survey of Commoditized Crimeware in the Underground Market", *International Journal of Critical Infrastructure Protection*, Volume 6, Issue 1, March 2013, http://www.sciencedirect.com/science/article/pii/S1874548213000036

17 עמוד ב"פייסבוק", בו מוצעים למכירה נשקי סייבר: https://www.facebook.com/groups/53807916899/

18 Limor Kessem, "Zeus FaaS Comes to a Social Network Near You", RSA, Speaking of Security, April 2013, http://blogs.rsa.com/zeus-faas-comes-to-a-social-network-near-you/

19 Michael Fire, Rami Puzis, Yuval Elovici, "Organization Mining Using Online Social Networks", http://arxiv.org/pdf/1303.3741v2.pdf

20 Aviad Elishar, Michael Fire, Dima Kagan, Yuval Elovici, "Homing Socialbots: Intrusion on a Specific Organization's Employee Using Socialbots", International Workshop on Social Network Analysis in Applications (SNAA), August 2013.

21 Fernando M. Pinguelo, Bradford W. Muller, Norris Mclaughlin, P.A. Marcus, "Is Social Media a Corporate Spy's Best Friend? How Social Media Use may Expose your Company to Cyber-Vulnerability", Bloomberg Law, http://about.bloomberglaw.com/practitioner-contributions/is-social-media-a-corporate-spys-best-friend/

22 Internet Census 2012, Carna Botnet, http://internetcensus2012.bitbucket.org/paper.html

23 מפת מערכות סקאדה בעולם: http://goo.gl/maps/nqnan

24 האתר Shodan, המכיל מידע שימושי להאקרים: http://www.shodanhq.com/

25 גילי כהן, "האקרים תקפו רשתות ביתיות של מאות ישראלים", **הארץ**, 11 בספטמבר 2013, http://www.haaretz.co.il/misc/2.444/.premium-1.2117098

26 וקטור תקיפה: http://searchsecurity.techtarget.com/definition/attack-vector

27 מתקפת זיוף: http://www.webopedia.com/TERM/S/spoof.html

28 Eric M. Hutchins, Michael J. Cloppert, Rohan M. Amin, "Intelligence-driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains", Leading Issues in Information Warfare & Security Research, 1 (2011), p. 80.

29 Doug Macdonald, "A Guide to SpyEye C&C Messages", Fortinet, February 15, 2011, http://blog.fortinet.com/a-guide-to-spyeye-cc-messages

30 Thomas Rid, "Cyber-Sabotage Is Easy", Foreign Policy, July 23, 2013. http://www.foreignpolicy.com/articles/2013/07/23/cyber_sabotage_is_easy_i_know_i_did_it?pa

31 Dorothy E. Denning, Cyberterrorism, Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Service, U.S House of Representatives, May 23, 2000, p. 269
http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

32 לכרונולוגיה של פעולות של Aum Shinrikyo ראו:
http://cns.miis.edu/reports/pdfs/aum_chrn.pdf

33 Paul Everard, "NATO and Cyber Terrorism", in: Center of Excellence Against Terrorism, *Response to Cyber Terrorism*, Ankara, Turkey, 2008, pp.118-126, http://www.nato.int/docu/review/2013/Cyber/timeline/EN/

34 דניאל כהן ואביב רוטברט, "תפוצת נשק קיברנטי במרחב הסייבר", **צבא ואסטרטגיה**, כרך 5, גיליון 1, מאי 2013.

35 Dylan Love, "10 Reasons To Worry About The Syrian Electronic Army", Business Insider, May 22, 2013, http://www.businessinsider.com/syrian-electronic-army-2013-5?op=1#ixzz2h728aL8P

36 Peter Foster, "'Bogus' AP tweet about explosion at the White House wipes billions off US markets", The Telegraph, April 23, 2013, http://www.telegraph.co.uk/finance/markets/10013768/Bogus-AP-tweet-about-explosion-at-the-White-House-wipes-billions-off-US-markets.html

37 יניר מגנה ועודד ירון, "מומחה ישראלי אמר ש'הצבא הסורי האלקטרוני' תקף בישראל – והכחיש", **הארץ**, 25 במאי 2013, http://www.haaretz.co.il/news/politics/1.2029071

38 אמיר בוחבוט, "מתקפת סייבר: הופלו אתרי משרד ראש הממשלה, הביטחון והחינוך", **וואלה חדשות**, 7 באפריל 2013, http://news.walla.co.il/?w=/90/2630896

39 נמרוד צוק, "פיגוע סייבר: לוחמי עז א דין אל קסאם הולמים באמריקן אקספרס", **כלכליסט**, 2 באפריל 2013,
http://www.calcalist.co.il/internet/articles/0,7340,L-3599061,00.html

40 לי ירון, "מחלקת ביטחון מתריעה: יכולות הסייבר של חמאס התעצמו", **במחנה**, 14 בנובמבר 2013, עמ' 19.

41 "Kaspersky Lab Exposes 'Icefog': a new Cyber-espionage Campaign Focusing on Supply Chain Attacks, September 26, 2013
http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_exposes_Icefog_a_new_cyber-espionage_campaign_focusing_on_supply_chain_attacks

42 להרחבה בנושא קוד מוטציה ראו: כהן ורוטברט, "תפוצת נשק קיברנטי במרחב הסייבר", **צבא ואסטרטגיה**, כרך 5, גיליון 1, מאי 2013.

43 גבי סיבוני, "מענה לאומי להגנה אזרחית בסייבר", מסמך עמדה למקבלי החלטות, המכון למחקרי ביטחון לאומי, אפריל 2013, http://heb.inss.org.il/index.aspx?id=4354&articleid=5904

תכנית הסייבר במכון למחקרי ביטחון לאומי – עיקרי הפעילות

המכון למחקרי ביטחון לאומי הוא מכון מחקר עצמאי במעמד של מוסד ללא כוונת רווח הפועל בישראל. המכון הוא גוף חיצוני של אוניברסיטת תל־אביב ועוסק בתחומי מחקר מגוונים, הקשורים בעיקר לביטחון הלאומי של מדינת ישראל. במסגרת פעולותיו מקיים המכון ימי עיון, פורומים וכנסים ומפיק פרסומים שונים, ביניהם ניירות עמדה למקבלי החלטות, מחקרים ושני כתבי עת. המכון נחשב כאחד המכונים המובילים בתחומו בעולם ומופיע בדירוגים כמכון המחקר המוביל בישראל בנושאי ביטחון לאומי.

תכנית הסייבר של המכון שמה לה למטרה לפתח את הידע ולהעמיק את הדיון והתובנות בנושא זה, תוך התמקדות בכמה היבטים: המשׂגה ויצירת שפה משותפת בהקשרי הביטחון הלאומי, פיתוח ובחינה של המדיניות הלאומית ואיתור קווים מנחים לדוקטרינה להגנה במרחב הקיברנטי, ברמה הלאומית והבין־ארגונית במדינת ישראל. התכנית נועדה לתרום לדיון המקצועי ולתובנות, ולסייע למקבלי החלטות לקדם מדיניות מושכלת ברמה הלאומית.

לצורך זה מתבצעות במכון פעילויות מחקריות שונות בנושאים הרלוונטיים לתחום הסייבר, ביניהן:

- פיתוח תפיסת ההגנה הלאומית במרחב הסייבר
- שיתוף ידע ומידע בין ארגונים ומגזרים שונים
- מודיעין ומבצעים במרחב הסייבר
- בחינת מודלים להתפשטות פוגענים במרחב הסייבר
- מעקב אחר ארגוני טרור וארגונים לא־מדינתיים בסייבר
- מעקב אחר פעילות של מדינות ושחקנים מרכזיים במרחב הסייבר
- היבטים חוקיים והיבטי רגולציה, ועוד.

בנוסף מפיץ המכון סקירה דו־שבועית בתחום המודיעין בסייבר, על בסיס חומר גלוי. סקירה זו יוצאת לאור באנגלית ומופצת באמצעות ארגון Cyber Security Forum Initiative (CSFI) ומערכי הפצה נוספים.

לצורך שיפור השפה המשותפת ופיתוח הידע, הוקם במסגרת התכנית **פורום לאומי** מקצועי המתמקד בפיתוח מדיניות וידע אסטרטגי בכל הקשור להגנה במרחב הקיברנטי. פורום זה מאפשר בנייה של ידע עדכני ומסייע לטווח קשרים בין הגורמים הרלוונטיים במשק, במגזר הפרטי והציבורי. בנוסף מספק הפורום למקבלי ההחלטות מצע מקצועי קבוע, תוך פיתוח ידע ופרסום ניירות עמדה בנושאים העומדים על הפרק. הפורום הוקם כדי לתת מענה לפער קיים בשיח בין

שתי סביבות: הסביבה הטכנולוגית, אשר בה פועלים גורמים רבים והתפתח ידע רב מאוד בישראל (ובעולם), והסביבה האסטרטגית, בדגש על מדינת ישראל והשיפור המשמעותי המתחייב ביחס למצב פיתוח הידע והמדיניות. כך נוצר במסגרת הפורום שיח מפרה וחיוני לשם השגת המטרה העליונה – **שיפור בר־קיימא של העמידות הקיברנטית של ישראל**. הפורום מקיים דיונים במועדים קבועים, בין היתר בנושאים הבאים:

- המשגה ויצירת שפה משותפת בהקשרי הביטחון הלאומי
- פיתוח ובחינה של המדיניות הלאומית להגנה במרחב הקיברנטי
- הממשקים בין התחום הטכנו־טקטי לבין התחום האסטרטגי
- בחינת הממשק בין המגזר הביטחוני והעסקי
- גבולות האחריות בין המדינה והמגזר הפרטי (ארגונים ויחידים)
- שיתוף ידע ורגולציה

בפורום חברים כעשרים וחמישה חברים בכירים משלושה מגזרים עיקריים: נציגים של גורמים רשמיים של ארגוני בטחון וארגוני המדינה, גורמי התעשייה הביטחונית, נציגי מרכזי הפיתוח של חברות הטכנולוגיה המובילות בתחום וגורמי אקדמיה. במהלך שנת 2013 הוציא המכון, בין היתר בעקבות תובנות שעלו בדיוני הפורום, מסמך המלצות למקבלי החלטות הנוגע לארגון ההגנה האזרחית בסייבר במדינת ישראל אחת ממטרות הפורום לשנת 2014 היא העמקת בחינת התפיסה הלאומית, בחינת היבטים של שיתוף ידע ורגולציה ומתן המלצות למקבלי ההחלטות בתחום.

צוות תכנית הסייבר

ראש התכנית – ד"ר גבי סיבוני
עמית מחקר ומתאם התכנית – דניאל כהן
מנהלת פורום הסייבר – הדס קליין

חוקרים

פרופ' אמיר אורבוך
ד"ר טל קורן
ד"ר יאיר אפנהיים
רס"ן מ' (אגף התקשוב)
הילה אדלר
כרמית ולנסי

עוזרי מחקר ומתמחים

רוקסנה בוגדנסקי
ג'ורג'יו בונדימן
עידו בר
קרן חטקביץ
שלומי יאס
שרה כהן
ניר כרמי
רן לוי
דניאל לוין
ג'רמי מקובסקי
סיימון צייפיס
סמי קרוננפלד
אמיר שטיינר