מרחב הסייבר והביטחון הלאומי

מבחר מאמרים | קובץ שלישי

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 שלישי

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: 978-965-7425-78-7

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

הקדמה

ההתפתחות המהירה של מדינת ישראל כגורם מוביל בתחום הסייבר מהווה מנוף לקידום המחקר בתחום בישראל בכלל ובמכון למחקרי בטחון לאומי בפרט. כדי להעצים את המחקר ואת היקף הפעילות, ובשל העובדה שמרחב הסייבר אינו מכיר בגבולות שבין מדינות וארגונים, החלטנו במכון למחקרי בטחון לאומי להעמיק את פעילות התכנית ולקיים את הכנס השנתי לביטחון סייבר בארצות הברית. כנס DCOI העוסק בהגנה ומודיעין בסייבר מביא לדיון את נושאי הליבה הנוגעים לביטחון והגנת מרחב הסייבר ולהיבטי המודיעין בו. הכנס שמתקיים השנה בוושינגטון, ארצות הברית, אורגן בשיתוף עם מגוון גורמים מישראל, מארצות הברית וממדינות נוספות.

התמקדות הכנס במבצעי הגנה ומודיעין מאפשרת למכון לבדל את העשייה שלו בתחום זה וכך לייצר השלמה למגוון הפעילויות המתקיימות בישראל ובעולם. לכנס השנה מספר מטרות ובהן: פיתוח השיח בתחום ביטחון מרחב הסייבר, הן במרחב התאגידי והפיננסי והן במרחב התשתיות הקריטיות; העמקת שיתוף הפעולה בין גורמי ממשל וארגונים, העוסקים בתחום הסייבר בישראל ובארצות הברית; חשיפת שוק הסייבר והטכנולוגיה הישראלית לחברות טכנולוגיה אמריקניות ומדינות אחרות בעולם, המבקשות לפתח עסקים בישראל או המבקשות לחשוף יכולות וטכנולוגיות ישראליות בחו"ל; העמקת שיתוף הפעולה הבין לאומי עם מדינות ידידותיות בתחום הסייבר בעולם.

כמידי שנה, סמוך לכנס, אנו מציעים לקהל שוחרי הסייבר פרסום ייחודי המרכז חלק מתוצרי המחקר ומאמרים שפורסמו במסגרת תכנית הסייבר של המכון. המאמרים בחוברת זו פורסמו בכתב העת **צבא ואסטרטגיה** והינם פרי עטם של חוקרי המכון ושל חוקרים מחוץ למכון שהשתלבו במסגרת תכנית המחקר במכון.

בברכה,

גבי סיבוני, עורך
ראש תוכנית ביטחון סייבר
המכון למחקרי ביטחון לאומי

האסטרטגיה של דאע"ש במרחב הסייבר

גבי סיבוני, דניאל כהן, טל קורן

הצלחותיו של ארגון דאע"ש ("המדינה האסלאמית") כוללות שילוב של מרכיבים הקשורים זה לזה, באופן שמסייע לו לבסס את שליטתו באזורים נרחבים ולשמש כראש החץ הנוכחי של הג'יהאד העולמי. כמו כן יוצר דאע"ש איום הנובע מהעובדה שפעילי הארגון המחזיקים באזרחות של אחת ממדינות המערב עלולים לשוב למולדתם ולבצע שם פיגועי טרור. איום נוסף של דאע"ש קיים באפשרות של הפעלת "זאבים בודדים" לביצוע פיגועי טרור ביעדים ברחבי העולם המערבי. מטרתו של מאמר זה היא לבחון מהו מודל ההצלחה של דאע"ש – ארגון שהשתלט כאמור על אזורים גיאוגרפיים רבים, ותופס מקום מרכזי בתודעה הציבורית ברחבי העולם. המאמר ינסה להעריך את האסטרטגיה הייחודית של הארגון, המשַלבת שני מרכיבים מרכזיים הקשורים ביניהם: שימוש נרחב במדיה החברתית מצד אחד ואכזריות קיצונית ומוחצנת מצד שני.

מילות מפתח: המדינה האסלאמית, דאע"ש, מדיה חברתית, עיראק, סוריה, טרור.

הקדמה

בחודש מאי 2004 פרסם אתר אינטרנט אסלאמי קלטת וידאו בה נראית הוצאתו להורג בבגדאד של האזרח האמריקאי ניק ברג. בסרטון נראה ברג כשהוא לבוש בבגדי אסיר כתומים (כמדי האסירים בכלא גואנטנמו) ומוּצא להורג על ידי עריפת ראשו בידי מנהיג "אל־קאעידה" בעיראק, אבו מוסעב א־זרקאווי. סרטון זה קיבל משמעות היסטורית מצמררת עשר שנים לאחר מכן, עם פרסום הקלטת שתיעדה

ד"ר גבי סיבוני הינו חוקר בכיר וראש תכנית ביטחון סייבר במכון למחקרי ביטחון לאומי. דניאל כהן הינו עמית מחקר ומתאם תכנית ביטחון סייבר במכון למחקרי ביטחון לאומי. ד"ר טל קורן הינו חוקר בתכנית ביטחון סייבר במכון למחקרי ביטחון לאומי.

מאמר זה ראה אור לראשונה ב**צבא ואסטרטגיה**, כרך 7, גיליון 1, מארס 2015, עמ' 117-133.

את הוצאתו להורג בעריפת ראש של האמריקאי ג'יימס פולי, הפעם על ידי פעיל דאע"ש – הארגון שהמשיך את דרכו של א־זרקאווי. ההבדלים המרכזיים בין שני הסרטונים הם שעורף ראשו של ג'יימס פולי מדבר במהלך הסרטון באנגלית רהוטה, שהסרטון על הריגת פולי הוא ברמה גבוהה ושנעשה שימוש במדיה ובמדיה החדשה להפצת המסר שבו בצורה ויראלית לכל קצות העולם. כך נוצרה בעיני המתבונן במדינות המערב תחושה של זעזוע ממראה השבוי המובל לשחיטה. התברר שלא רק הקורבן יכול להיות "השכן ממול", אלא גם השוחט.

ארגון דאע"ש עושה שימוש במאפייני עידן המידע ו"הכפר הגלובלי", בהם טושטשו המחיצות בין מציאות לדמיון, וכן באמצעים הטכנולוגיים הנגישים כיום לכל. זאת, הן כדי לקרוא לתומכיו במערב לקיים את ההיג'רה (הגירה למדינה האסלאמית) והן כדי לעודד אותם לג'יהאד, או, כפי שהתבטא לוחם הארגון ממוצא קנדי: "לארוז את המזוודות או להכין את מטעני החבלה".[1]

לוחמה פסיכולוגית בשירות ארגוני הטרור אינה תופעה חדשה. קרלוס מָרִיגֶלָה, מאבות הטרור המהפכני המודרני, פרסם בשנות השישים של המאה העשרים את "המדריך הזעיר למלחמת גרילה", בו התייחס למלחמת העצבים וללוחמה הפסיכולוגית. לטענתו, ממשלות יהיו תמיד בעמדת נחיתות בהתמודדות עם לוחמה פסיכולוגית אותה מפעיל ארגון טרור, וזאת כתוצאה מהשקעה של משאבים רבים בסיכול ובצנזורה. על פי מריגלה, השקעה זו נדונה לכישלון.[2] האתגרים והאיומים בעידן הדיגיטלי והמדיה החדשה משתנים כתוצאה מהמרחבים החדשים בהם יכול ארגון הטרור לפעול לקידום מטרותיו הפוליטיות. ארגון דאע"ש, כדוגמה, פועל בצורה רחבה במרחב הווירטואלי, תוך שימוש בפלטפורמות מדיה חדשה המקשות על צנזורה מדינתית. המדינה הבאה להתגונן מפני התופעה של שימוש במדיה החדשה למטרות טרור נמצאת בעמדת נחיתות, ולכן המענה שלה לאיום חייב להיות בכלים חדישים ועדכניים.

גל הפיגועים הספונטניים של "זאבים בודדים" בארצות הברית, קנדה, אוסטרליה, מדינות אירופה וישראל ממחיש את הקשר הסימביוטי הנרקם בין קריאת דאע"ש לגיוס לשורותיו, התעמולה שהוא עושה ופעולות הטרור שלו נגד אזרחי המערב, ובין פלטפורמות התקשורת השונות אותן מאפשר המרחב הווירטואלי. קשר זה ניכר היטב ומתמזג בצורה ישירה בפעולות טרור של "בוגרי סוריה ועיראק" ששירתו בדאע"ש, השבים למדינות האם שלהם. דוגמה לכך היא הפיגוע במוזיאון היהודי בבריסל במאי 2014, שבו נרצחו בני הזוג הישראליים מירה ועמנואל ריבה על ידי מהדי נמוש, אזרח צרפתי ממוצא אלג'ירי שחזר למדינת האם שלו לאחר לחימה בשירות הג'יהאד בסוריה. קשר זה מתבטא גם בפעולות טרור מקומיות לא מאורגנות הנעשות בהשפעת דאע"ש ובהשראתו. דוגמאות לפעולות

כאלו הם פיגועי דריסה וירי שנעשו בקנדה וניסיונות לפיגועים באמצעות עריפת ראשים שנעשו באוסטרליה ובארצות הברית.

דאע"ש מפעיל מנגנוני הסברה, גיוס ותעמולה במרחב הווירטואלי, כולל הוצאה לאור של מגזינים וסרטונים המופקים ברמה גבוהה, מאפשר סיקור תחת מגבלות על ידי המדיה הבין־לאומית ומוֹכֵר ברשת מותגים עם סמל הארגון. פעילי דאע"ש אף מתעדים ומשתפים את רשמיהם ברשתות החברתיות. שיטת פעולה זו, הכוללת שקיפות ומוחצנות, משתלבת במהלך האסטרטגי הנוכחי של הארגון – הכנה לפעילות טרור גלובלי על ידי גיוס פעילים זרים והקמת תאי טרור חדשים ברחבי העולם.[3]

בדומה לטקטיקה ארוכת ימים אותה אימצו קבוצות מהפכניות, גם ארגון "המדינה האסלאמית" אימץ את הרעיון של תעמולה על ידי מעשה, שבה אלימות ותקשורת מוזגו לצורך השגת אפקט מרבי של תעמולה ואלימות, וכל זאת לשם העברת מסר פוליטי. הייחוד של דאע"ש הוא בשילוב בין פלטפורמות הפצה במדיה ובמדיה החדשה להצגת אכזריות קיצונית ומוחצנת.[4] פלטפורמות אלו מהוות ספקטרום חדש של "מלחמה רשתית" המנצל את מהפכת המידע לתועלת ארגון הטרור. דאע"ש עושה שימוש גם ב"תעמולה הופכית" (reciprocal propaganda), וכולל בה תמונות זוועה המתעדות את מעשה הטרור (דוגמת סרטוני עריפות הראשים) ונועדות ליצור פחד וחרדה בציבור הרחב. כן הוא משתמש בסוג זה של תעמולה ככלי להשפעה על מקבלי החלטות במערב.

מאמר זה מנסה לבחון את האסטרטגיה הייחודית של ארגון דאע"ש, המשלב שני מרכיבים מרכזיים הקשורים זה בזה: שימוש נרחב במדיה החברתית מצד אחד ואכזריות קיצונית מוחצנת מצד שני – מרכיבים שבעזרתם הוא הצליח לכבוש בהצלחה אזורים גיאוגרפיים רבים ולחדור לתודעה הציבורית העולמית באופן חסר תקדים.

הצלחותיו של דאע"ש, שהתבסס בשנה האחרונה בעיראק ובסוריה והקים תשתית ארגונית בצפון אפריקה ובחצי האי סיני, כוללות שילוב של מרכיבים הקשורים זה לזה, באופן שמסייע לארגון לבסס את שליטתו באזורים נרחבים ולשמש כראש החץ של הג'יהאד העולמי. הארגון מהווה איום על יציבותם של משטרים ערביים במזרח התיכון, כמו סעודיה, ירדן ולבנון, ולצד זאת הוא מהווה איום באמצעות פעיליו המחזיקים באזרחות של מדינות המערב ועלולים לשוב למולדתם ולבצע בה פיגועי טרור, וכן על ידי עידוד מַפגעים ספונטניים לבצע פעולות טרור ביעדים במערב. המדיה והאלימות משמשות את דאע"ש בערבוביה, הן להפחדה של אויבים הנמצאים בקִרבה למרחב הפעילות שלו והן לגיוס פעילים ותומכים. ההפחדה ומאמצי הגיוס מתרחשים על רקע קִרבה פיזית למדינות הדמוקרטיות במערב, וכוללים שימוש נרחב במדיה החברתית ובאמצעי התקשורת,

לצד הפגנת אכזריות קיצונית מוחצנת בממדים שלא נודעו כמותם עד היום. כאמור, מרכיבים אלה משולבים זה בזה, אולם הפנִיה לקהל יעד מערבי והקִרבה אליו, הן בממד הפיזי (הקִרבה לאירופה) והן בפנִיה לגיוס תומכים מאותן מדינות, יוצרות משוואה המשלבת תחושת פחד פרימיטיבי עמוק בקרב כלל הציבור מצד אחד, עם משיכה רבה בקרב קהל התומכים הפוטנציאלי מצד שני.

מאמר זה טוען, כאמור, שההצלחה הרשתית של דאע"ש נובעת מתוך הקֶשר בין השימוש באכזריות קיצונית מוחצנת ובין השימוש במרחב הקיברנטי להפצת מסרים פנימה (למרחב השליטה וההשפעה שלו) והחוצה (למדינות המערב), לצורכי גיוס והפחדה. כל זאת, כפי שצוין לעיל, על רקע קִרבה פיזית למערב ויצירת תחושות פחד עמוקות מפני הצפה של המדינות המערביות במפַגעים ובתומכי הג'יהאד העולמי.

השימוש המושכל שעושה דאע"ש ברשתות החברתיות נועד להעביר מסרים ממוקדים לקהלי יעד ספציפיים. קהלי יעד חשובים בראיית הארגון הם קהילות מוסלמיות במדינות המערב ובאסיה. האסטרטגיה התקשורתית של דאע"ש הצליחה למצב את הארגון כאויב המרכזי של המערב, למתג אותו כראש החץ במאבק של הג'יהאד העולמי ולזכות בתמיכה בקרב ציבורים ערביים ומוסלמים, ארגונים ג'יהאדיסטיים וקהילות מוסלמיות במערב.[5]

מערכת התעמולה והגיוס של דאע"ש

ארגון דאע"ש, בדומה לארגון "אל־קאעידה" בתחילת דרכו, הכיר בעובדה כי הוא חייב לפעול במספר חזיתות בו־זמנית במלחמתו נגד "הכופרים". הארגון רואה את השימוש באסטרטגיה התקשורתית "כמייצגת שני שלישים מהקרב",[6] ובמלחמה על התודעה – מהלך חיוני ומשלים לפעילותו.[7] החשיבות של המדיה על צורותיה השונות כאמצעי להשפעה ולהשגת תמיכתם ואהדתם של מיליוני מוסלמים ברחבי העולם ניכרת היטב בפעולותיו של דאע"ש ובמשאבים הרבים שהוא משקיע לשם כך. האינטרנט והרשתות החברתיות הם האמצעי העיקרי להפצת האידיאולוגיה והמסרים הפוליטיים של הארגון, וכן לגיוס מתנדבים זרים ומימון, וכל זאת תוך שליטה מוקפדת על המידע המתפרסם מאזורי הקרבות ושחרורו בצורה מבוקרת.

דאע"ש עושה שימוש במספר פלטפורמות מקוונות,[8] דוגמת "מוסד אל־פרקאן להפקה הסברתית",[9] המשמש כזרוע התקשורתית הרשמית של הארגון ומנהיגיו, וכן "סוכנות אל־אִעתִצָאם להפקת מדיה", הפועלת בשנתיים האחרונות להפקת סרטונים של דאע"ש ולהפצתם ברשתות החברתיות. זרוע תקשורתית נוספת של דאע"ש הוא אתר אינטרנט הנקרא "מרכז אל־חיאת לתקשורת", הפונה בעיקר לקהל יעד מערבי. "מרכז אל־חיאת לתקשורת" מחזיק חומר רב על דאע"ש, ובו נאומים וסרטונים המתורגמים ליותר מעשר שפות. האתר, שכאמור פונה למערב

ולקהל יעד שאינו דובר ערבית, משלב תכנים וחומרים מגוונים בקטעי וידאו חדשים ומוסיף כתוביות לקטעי וידאו קיימים. כן יש בו מאמרים, דיווחי חדשות ותרגום מסרי ג'יהאד. איכות האתר גבוהה והוא נבנה ככל הנראה על ידי צוות המנוסה בהפקת חומרי תקשורת לקהל מערבי.

כאמור, דאע"ש מפיץ ברשת סרטי תעמולה רוויים בדם, שבהם הוא מציג לראווה את הטקטיקות האכזריות שבהן הוא עשה שימוש במהלך כיבושיו בסוריה ובעיראק, תוך התרברבות על אוזלת ידם של אויביו. אחד מסרטי התעמולה של דאע"ש, שפורסם בספטמבר 2014 כסרט תיעודי וערוך בצורה מקצועית, הוא "להבות המלחמה: המאבק רק החל" (*Flames of War*),[10] שמטרתו היא להעביר מסר ברור שנועד להרתיע פעילות של ארצות הברית נגד הארגון. הסרט בן 55 הדקות עושה שימוש בדימויים רומנטיים המעוצבים בקפידה, תוך שילוב אלמנטים של פיצוצים, קרבות, חיילים אמריקאיים פצועים וכאלה שעומדים להיהרג, רטוריקה אנטי אמריקאית, קטעים ערוכים בהילוך איטי של הוצאות להורג וקטעי ארכיון של מנהיגי המערב. לצד האלמנטים המתוחכמים המשולבים בסרט, כלולים בו כאלה שמטרתם היא ליצור אשליות (גודל, תמונות מעוותות, העצמת הנואמים, נאום לאור לפידים), והם מזכירים במידת מה את סרט התעמולה שהופק בגרמניה הנאצית כסרט דוקומנטרי על ידי לני ריפנשטאהל ב־1934 – "ניצחון הרצון" (*Triumph des Willens*).[11]

הסרט "להבות המלחמה" אינו היחיד שהופק על ידי דאע"ש. הוא מצטרף לשורה ארוכה של סרטים של הארגון הערוכים באופן מקצועי ומתעדים פיגועי תופת, התקפות טרור והתנקשויות באנשי ממשל, צבא וכוחות הביטחון בעיראק. דוגמה לכך היא הסדרה הפופולרית בת ארבעה חלקים, שחלקה הראשון הופץ כבר ביוני 2012, בשם "צחצוח החרבות" (*The Clanging of the Swords*), הזוכה לחשיפה רבה בפלטפורמות המקוונות של תומכי הג'יהאד העולמי ובאמצעי המדיה השונים (טוויטר, פייסבוק).[12] ניתוח מקיף של החלק הרביעי של "צחצוח החרבות" (שפורסם ב־17 במאי 2014) נעשה על ידי ניקו פְּרוּצָ'ה וארי פישר באתר *Jihadica*. הניתוח מציג את רמת התחכום של דאע"ש בשימוש במדיה החברתית ובטכנולוגיות להפצת מידע בפלטפורמות שונות: טלפונים סלולריים (שהם הפלטפורמה המועדפת על הארגון, במיוחד השימוש באפליקציה Twitter for Android), טאבלטים, פייסבוק ואתרים לשיתוף קבצים (archive.com, justpaste.it). זאת, תוך שימוש בגודל ובפורמט שונים, באיכות משתנה של הסרט ובמגוון שפות (ערבית, אינדונזית, אנגלית, גרמנית, יפנית). אין זה מפתיע שהחלק הרביעי של "צחצוח חרבות" שוחרר לפרסום ביום שבת, מתוך כוונה שהאתרים השונים יתקשו לחסום את הפרסום בשל כך שמרבית עובדי החברות יהיו ביום מנוחה

מעבודה.. ואכן ב־24 השעות הראשונות לאחר פרסום הסרטון היו קרוב ל־60,000 צפיות בו (הזמן הממוצע לצפייה היה 17 דקות).[13]

בנובמבר 2014 פורסם סרטון על עריפת ראשיהם של 22 שבויים סוריים. ניתוח הסרטון, שנעשה על ידי ארגון *TRAC* וגוף המחקר *Quilliam*, מצביע על כך שהפקת הסרטון נעשתה בצורה מקצועית, כולל שעות צילום רבות, שימוש במצלמות HD ועריכה מהוקצעת. הערכת מבַצעי הניתוח היא שעלות הפקת סרטון כזה היא כ־200,000 דולר.[14] הפקת הסרטון מצביעה על רמת האכזריות והתחכום של העושים במלאכה בארגון דאע"ש: הסרטון אינו תיעוד גרידא של הוצאה להורג, אלא תוכנית "ריאליטי" של הוצאה להורג המונית, המבוצעת כולה על ידי לוחמי "חוץ" שהתגייסו לארגון, המוציאים להורג את "הניצבים" תוך כדי מהלך הסרטון. שיטה זו מצביעה פעם נוספת על החשיבות שדאע"ש מקנה לשימוש במדיה ואת ההבנה העמוקה של הארגון את מידת ההשפעה שיש לסרטון כזה על צופים משני סוגי האוכלוסיות שתוארו לעיל – במערב ובקרב המועמדים לגיוס: יצירת תחושה של משיכה "רומנטית" אצל מתגייסים פוטנציאליים ויצירת תחושות של פחד ובעתה בקרב אזרחי מדינות המערב.

בארגון דאע"ש מבינים שאין להסתמך רק על התכנים האלימים, אלא יש להראות גם פנים נוספות של החיים בצִלה של המדינה האסלאמית. מכיוון שחלק מהפרסומים של הארגון נועד לגייס מתנדבים חדשים לאזורי הלחימה ממדינות המערב וממדינות לא ערביות אחרות, עושה דאע"ש שימוש ב"מרכז אל־חיאת לתקשורת" להפצת סרטונים מקוריים תחת הכותרת "*Mujatweets*", שמטרתם היא להראות כי החיים תחת המדינה האסלאמית הם שלווים ונורמליים. זאת, כאמור, כדי להקנות לדאע"ש פן חיובי שיטשטש את התדמית הנוקשה שלו כארגון רצחני, וכן למשוך קהלים נוספים להצטרף לשורותיו.[15]

בנוסף לכך ניתן למצוא באתר של "מרכז אל־חיאת לתקשורת" סדרה של מאמרים המפורסמים כמסמכי PDF, המזכירה את המגזין המקוון *Inspire* של "אל־קאעידה". תכליתם של מאמרים אלה היא להראות ולהדגיש את הצלחת דאע"ש בשדה הקרב ולהציג לוחמים בולטים של הארגון. חלק מקטעי הווידאו המופיעים באתר נועדו להשפיע על דעת הקהל, בין השאר באמצעות סצנות של חלוקת מזון, טיפול רפואי ומתן צדקה. הסרטים כוללים כתוביות באנגלית ומיועדים לבעלי מקצוע מערביים הנקראים לבוא ולסייע בהקמת המדינה האסלאמית. דאע"ש גם מוציא לאור פרסום בשם *IS Report*, המתאר, בין השאר, הקמה של מערך להכשרת אימאמים וכולל מאמרים באנגלית, פסקי הלכה, תמונות של הוצאות להורג ותמונות של ניצחונות בשדה הקרב.[16]

בנוסף לגופי התקשורת של דאע"ש המפיצים את פרסומי הארגון באינטרנט, מפיץ הארגון מספר מגזינים אינטרנטיים, שהחשוב והעיקרי ביניהם הוא כתב העת

"דאביק" (*Dabiq*),[17] הדומה בעיצובו למגזין *Inspire* של "אל־קאעידה". הגיליון הראשון של "דאביק" פורסם ביולי 2014 במגוון שפות וכולל חמישים עמודים. חלקו העיקרי, "The Return of the Khilafah", נועד לשכנע את קוראיו בלגיטימיות של החליפות שעליה הכריז מנהיג דאע"ש אבו בכר אל־בגדאדי, תוך שהוא קורא למוסלמים מכל העולם לבוא "למדינתם הטבעית" ולחיות תחת הנהגתו. שלושת הגיליונות הנוספים של כתב העת פורסמו במהלך החודשים ספטמבר–אוקטובר 2014, וכוללים ציטוטים והתבטאויות של בכירי דאע"ש, חדית'ים הנותנים לגיטימציה לעבדות של מי שנתפסו כ"שלל מלחמה", מידע על בניית המדינה האסלאמית, קריאה להרג "צלבנים", הצדקה של הוצאות להורג ועוד.

פעילות הסברתית נוספת של דאע"ש, שנועדה לקהילות מוסלמיות המתגוררות מחוץ לאזורי הלחימה בסוריה ובעיראק, מוצאת ביטוי במגזין החדשות האינטרנטי "חדשות המדינה האסלאמית", המתפרסם בשפה האנגלית וכולל דיווחים שוטפים על הארגון ודברי הגות אסלאמית סָלָפִית־ג'יהאדיסטית.[18] בנוסף לכך, דאע"ש מנהל פורומים ואתרי חדשות רשמיים באינטרנט בשפה הערבית, דוגמת "במת דבר הג'יהאד" ("אל־מַנְבַּר אל־אעלאמי אל־ג'יהאדי"),[19] הכוללים תכני תעמולה שונים הנוגעים לדאע"ש.

השימוש של דאע"ש ברשתות חברתיות מאפשר לארגון לגייס תמיכה רחבה של ציבור רדיקלי מוסלמי צעיר בארצות המוצא שלו, וכן במערב, וזאת באמצעות העברת מסרים ממוקדים. בעוד שהתקשורת והעברת המסרים בין ארגוני הג'יהאד העולמי ותומכיהם, דוגמת "אל־קאעידה", נעשו לרוב במחשכים וברשת שאינה נגישה לכל, וכן במסגדים, בהפצת עלונים ובאתרי אינטרנט המיועדים לכך,[20] דאע"ש בחר לפעול בגלוי בערוצי המדיה החברתית, לרבות יוטיוב, טוויטר ופייסבוק, וכן ברשתות חברתיות אחרות, פחות ידועות, הפונות לקהל יעד מערבי ולקהילות מוסלמיות במערב (למשל, האתרים: VK, Diaspora).

דאע"ש מציף את הרשתות החברתיות בחומרים גרפיים אכזריים במיוחד, הכוללים עינויים, הוצאות להורג המוניות, עריפת ראשים, צליבת אנשים ועוד. כאמור, זהו רק חלק מהתמונה הרחבה, והשימוש שעושה הארגון ברשתות החברתיות משרת מספר מטרות נוספות, כגון: לוחמה פסיכולוגית ויצירת אפקט של הרתעה הן על קהל היעד הספציפי באזורי הקרבות והן על דעת הקהל המערבית; הפגנת נוכחות ודימוי של גודל כדי ליצור מצג כאילו הארגון גדול יותר משהוא למעשה; הפצת אידיאולוגיה; גיוס מימון; קריאה למתנדבים להצטרף לג'יהאד, תוך שימוש בסרטונים ובראיונות עם מוסלמים מאוסטרליה, מאירופה ומארצות הברית.

השימוש של דאע"ש ברשתות החברתיות מגיע לרמת תחכום גבוהה, והמסרים האכזריים והתעמולתיים שלו נעשים באופן הדוחק הצדה את המאמצים

התקשורתיים של הארגונים המתחרים, דוגמת "אל־קאעידה" ונגזריו. כך, למשל, דאע"ש השתמש באפליקציה הפועלת ברשת טוויטר בשם "שחר הגאות השמֵחה" (Dawn of Glad Tidings). אפליקציה זו הייתה עד לא מזמן נגישה להורדה בחנות היישומים של גוגל (Google Play Store) ואפשרה הצגת פוסטים אוטומטיים של חשבונות של תומכי הארגון. אמצעי נוסף בו עושה דאע"ש שימוש הוא האשטאגים (Hashtag) למיניהם, הנמצאים ברשתות החברתיות טוויטר, גוגל ופייסבוק.[21] דאע"ש משתמש ב"Hahstag Hijacking", שהינה שיטה פשוטה יחסית לשתול מילים פופולריות, ובכך הוא מבקש לזכות בתשומת הלב של אנשים המחפשים תוכן מסוים. דוח מיוחד שפרסמה לאחרונה חברת *ZeroFox* מצביע על כך שדאע"ש עושה שימוש בטכנולוגיות מתקדמות כדי לנצל רשתות מחשבים שבהן הוא מחדיר נוזקות (בוטים) כדי לקדם קמפיינים שלו. בנוסף לכך, דאע"ש מפיץ משחקי מחשב הכוללים אימונים והכנות לשדה הקרב, שנועדו לגייס מתנדבים ותומכים בארגון. כזה הוא, למשל, הקדימון למשחק מחשב הקרוי *Jihad Simulator*, בו המשַחקים מדמים חטיפה של כלי רכב צבאיים ופיצוצם, וכן ירי לעבר בתי ספר.[22] המִשחקים מאפשרים רמת תקשורת גבוהה (ניהול שיחות באמצעות טקסטים, מצלמות רשת, אוזניות ומיקרופונים) ויוצרים תשתית גיוס ואימון נוחה ורחבת היקף.[23] ניסיונות של מדינות במערב לסגור חשבונות של דאע"ש ותומכיו ולצנזר את תוכן הפרסומים של הארגון ברשתות החברתיות כמעט ואינם מצליחים. רשת הטלוויזיה *CNN* פרסמה לפני מספר חודשים ידיעה לפיה הרשת החברתית פייסבוק פועלת לעצור את השימוש של דאע"ש בה, אך עד כה ללא הצלחה.[24]

דאע"ש יוזם קמפיינים תקשורתיים גדולים כחלק ממסע תקשורתי ממומן ומתוזמן היטב שנועד לעודד הצטרפות לשורותיו ולאיים על ארצות הברית ובעלות בריתה לבַל יתערבו בנעשה בעיראק. כזה הוא הקמפיין בעל הכותרת "מיליארד מוסלמים תומכים במדינה האסלאמית", שיזם דאע"ש ב־19 ביוני 2014 באמצעי המדיה השונים. הקמפיין זכה להצלחה ולגילויי תמיכה ברחבי העולם, שפורסמו על רקע צילומים של אתרים שונים ובהם הר הבית בירושלים, מגדל אייפל בצרפת, ה"ביג בן" בלונדון ובירות שונות בצפון אמריקה, באירופה ובאסיה. דאע"ש גם מוכר מזכרות (חולצות, מחזיקי מפתחות, חיילי צעצוע וחפצים אישיים) המשמשות אותו למטרות תעמולה וכמקור הכנסה נוסף.

לוחמה פסיכולוגית

"תיאטרון הטרור" האכזרי, בו עושה שימוש ארגון דאע"ש כחלק מהסימביוזה המסוכנת בין הטרוריסטים תאבי ההכרה והחשיפה ובין התקשורת רודפת הרייטינג והלהוטה אחרי המחזות האלימים והמרתקים שיוצרים אירועי הטרור,[25] אינו תופעה חדשה. הוא חלק מאסטרטגיה רציונלית שתכליתה הוא להעביר מסר

שעיקרו פסיכולוגי. במובן זה, השימוש של דאע"ש וארגונים דומים לו בטרור נגד אזרחים בריטיים ואמריקאיים הוא "בעיקר סמלי ותעמולתי".[26] מאפייניו במקרה זה שונים ממה שהורגלנו עד כה, וזאת לאור האכזריות הרבה והלא אנושית אותה נוקט דאע"ש והשימוש המקיף שלו במרחב הקיברנטי (הרשתות החברתיות) להפצת תכנים אלה. מִטבע הדברים, אכזריות זו של הארגון יוצרת אווירה של עניין ומודעות בין־לאומית מתמשכת, מעבירה מסרים, מעלה אותם לסדר היום של הציבור ושל מקבלי ההחלטות, מסייעת לקידום תדמיתו של דאע"ש ויוצרת אהדה למניעיו, תוך הצטיירותו כצד הקורבן, ולעתים תוך יצירת מראית עין של כוח רב יותר מכוחו האמתי.

השימוש שעושה דאע"ש באמצעי התקשורת כדי לקדם את מטרות הטרור שלו שונה במהותו מהשימוש שעשו ארגוני טרור אחרים בתקשורת בפיגועים קודמים שלהם, שגם הם זכו לחשיפה תקשורתית בין־לאומית רחבה – משבר בני הערובה באיראן (1979–1981), הפיגוע במגדלים התאומים בניו יורק (2001) ומשבר בני הערובה בתיאטרון במוסקבה (2002).[27] נושא השימוש במדיה על ידי טרוריסטים נחקר רבות,[28] תוך ניסיון להבינו בהקשר של תקשורת מבוססת סמלים (Symbolic Communication Theory). אצל דאע"ש, הקורבן אינו חסר חשיבות. אדרבא, הארגון מייחס חשיבות רבה לקורבנות (ילדים, עיתונאים, עובדי סיוע, נשים), ולכן בחירתם נעשית בדרך שנועדה לפגוע בבטן הרכה של דעת הקהל ומקבלי ההחלטות במערב. משאבים רבים משקיע דאע"ש בעיתונאים חטופים למטרות תעמולה.

שינוי אסטרטגי ביעדי הטרור

דאע"ש הכניס במהלך שנת 2014 מספר שינויים אסטרטגים ביעדי הטרור שלו ובאופן שבו הוא התנהל במרחב הלחימה. בשלב הראשון התמקד הארגון ביצירת תשתית שתאפשר לו להתבסס באזורים השונים בסוריה ובעיראק. במסגרת זו הוא התמקד בביצוע פעולות טרור אכזריות נגד אוכלוסיות סוניות מקומיות וסמלי שלטון ובטיהור אתני על רקע דתי. דוגמה בולטת לכך הם מעשי הטבח של דאע"ש במיעוט היזידי באזור ארביל, הרי סנג'אר ואזור סכר מוסול. תהליך זה היה מלווה באיומים תקשורתיים נגד המערב ונמשך עד שלהי קיץ 2014. לאחרונה פרסם "המרכז הסורי לזכויות אדם" מסמך המתעד הוצאתם להורג של 1,429 בני אדם בסוריה מאז יוני 2014, שמחציתם הם אזרחים ומחציתם חברי השבט השיעי שעיטאת, תושבי המחוז דיר א־זור שבמזרח סוריה.[29]

השלב השני של השינוי האסטרטגי ביעדי הטרור של דאע"ש החל במהלך חודש אוגוסט 2014, במקביל לגיבוש הקואליציה בראשות ארצות הברית ללחימה בארגון. השינוי העיקרי שביצע דאע"ש בשלב זה היה הצבת המערב בכלל, וארצות הברית בפרט, כיעד מרכזי לפעולות טרור. במסגרת זו הוציא הארגון להורג בצורה

ברוטלית, על ידי עריפת ראשים, מספר עיתונאים ועובדי סיוע חטופים (אמריקאים, בריטים וצרפתים), תוך עשיית שימוש מניפולטיבי בתקשורת. ההוצאות להורג גרמו לזעזוע רב בקרב דעת הקהל המערבית ובעולם הערבי המתון. ברמה התקשורתית, הן היו מתוזמנות היטב ובוצעו על ידי לוחם דאע"ש ממוצא בריטי לבוש שחורים המכונה "ג'ון הג'יהאדיסט" ונראו כתסריט מוכן מראש. ההוצאות להורג הוצגו כ"מסר לאמריקה", ונעשה בהן שימוש באמצעי צילום מתקדמים ובצילומים ערוכים היטב. במסרים שהתלוו להן נקבע שהאחריות להוצאות להורג מוטלת על ממשלות ארצות הברית וקנדה, ואף צורף אליהן איום לפיו כל התערבות של ממשלות המערב תוביל לפגיעה באזרחים חפים מפשע. על פי "ניו יורק טיימס", במהלך החודשים נובמבר 2012–ינואר 2014 חטף דאע"ש לפחות 23 בני אדם מ־12 מדינות שונות, שחלקם שוחרר תמורת כופר.[30]

השלב השלישי בשינוי האסטרטגיה של דאע"ש החל באמצע ספטמבר 2014 בקריאה של הארגון לפגוע באזרחי המדינות השונות במערב הלוקחות חלק בקואליציה שהתגבשה נגדו. כך, למשל, אחד ממנהיגי דאע"ש, אבו מוחמד אל־עדנאני א־שאמי, קרא להרוג "כופרים" במדינות מערביות,[31] וקלטת אודיו שהופצה על ידי הארגון קראה לפגוע באזרחי המערב ובכוחות הביטחון שלהם.[32] קריאה זו חזרה גם בגיליונו הרביעי של "דאביק" מחודש אוקטובר 2014. קריאת דאע"ש להריגת אזרחים מערביים הניבה תוצאות, שסימנים ראשונים להן ניתן לראות בסיכול הכוונה לבצע פיגוע הרג נגד אזרחים באוסטרליה, בפיגועי דריסה וירי בקנדה, בתקיפת שוטרים בגרזן ברובע קווינס בניו יורק, בהנחת מטענים בווינה ועוד.[33]

ארסנל הטרור הרצחני של דאע"ש כולל אמצעים מזוויעים, ובהם כאמור עריפת ראשים, וזאת כאסטרטגיה מחושבת היטב שהלכה וצברה תאוצה בעקבות התקיפות האוויריות של ארצות הברית על יעדי הארגון. תכליתן של עריפות הראשים המתוקשרות היא כפולה: מצד אחד, ליצור לחץ של דעת הקהל, בעיקר נגד ממשלות בריטניה, ארצות הברית וצרפת, ובמקביל לבדל את דאע"ש מיתר הארגונים באכזריותו חוצת הגבולות; ומצד שני, להיות כוח משיכה למגויסים פוטנציאליים על ידי פנייה לתחושות האסלאמיות הבסיסיות, במסגרת החזרה ליסודות האסלאם והכפירה במוסר המערבי המודרני. רציחתו בעריפת ראש של העיתונאי ג'יימס פולי ב־19 באוגוסט 2014 נועדה להעביר מסר של איום לארצות הברית ("מסר לאמריקה"), לפיו כל החלטה לפעול נגד המדינה האסלאמית תוביל לפגיעה באזרחים אמריקאיים, תוך האשמת הממשל האמריקאי בלא פחות מאשר באחריות לרצח פולי. גם הרצח של העיתונאי סטיבן סוטלוף על ידי דאע"ש ב־2 בספטמבר 2014 נועד להעביר מסר תקיף לארצות הברית ("מסר שני לאמריקה") נגד המשך התקיפות האוויריות של כוחותיה על יעדי הארגון: "כל עוד הטילים

שלך ימשיכו לתקוף את האנשים שלנו, הסכין שלנו תמשיך לתקוף את הצוואר של אנשיך".[34]

עריפת הראשים פונה לשני קהלי יעד – מקומי וגלובלי. הפנייה לקהל היעד המקומי, כוללת סרטוני תעמולה שלרוב ערוכים ומתוזמנים בצורה בסיסית, כחלק מהרצון ליצור לוחמה פסיכולוגית נגד המתנגדים "מבית". קהל היעד השני, המשמעותי יותר, הוא העולם המערבי, ובפרט ארצות הברית, בריטניה ואוסטרליה. סרטים אלה ערוכים ומתוזמנים היטב, מתוך הרצון של דאע"ש להשיג הישגים פוליטיים ותעמולתיים, כמו השפעה על דעת הקהל באמצעות הטלת אימה וגיוס פעילים פוטנציאליים. כך, למשל, במהלך החודשים ספטמבר–אוקטובר 2014 פרסם דאע"ש מספר סרטונים שבהם נראה העיתונאי הבריטי ג'ון קנטלי מדווח מאזורי הקרבות בעין אל־ערב (העיירה קובאני) על "המניפולציה של התקשורת המערבית" וכיצד "המערב נגרר למלחמה שהוא אינו יכול לנצח בה, נגד אלפי חמושים".[35] דיווחים אלה נראו במובהק כתעמולה של דאע"ש.

לדברי ראמי עבד א־רחמן, ראש "המרכז הסורי לזכויות אדם", המספר הרב של חיילים שנרצחו על ידי עריפת ראשיהם והנחתם במקום ציבורי נועד ליצור טרור ופחד מפני הארגון.[36] יש לציין כי התופעה של רצח בני ערובה באמצעות עריפת הראש אינו דבר חדש, וניתן למצוא לו דוגמאות משנים קודמות: הוצאתו להורג של דניאל פרל ב־2002 על ידי "התנועה הלאומית לשיקום הריבונות הפקיסטנית", עריפת ראשים של רוסים אתניים ושל זרים על ידי טרוריסטים צ'צ'ניים, ופעולות דומות של גורמי טרור אחרים, כגון ארגון "אבו סייף" בפיליפינים, קבוצות טרור אלג'יריות וארגון הטליבאן.

סיכום ותובנות

ארגון "המדינה האסלאמית" פיתח בחודשים האחרונים יכולת שליטה במדיה החברתית, תוך שהוא רואה בה כלי נשק לגיטימי במלחמתו נגד מתנגדיו בארצות המוצא של הארגון ונגד המערב (ארצות הברית, בריטניה, אוסטרליה). דאע"ש עושה זאת על ידי שימוש בתכנים פשוטים המבהירים היטב את מטרותיו ואת המסר שהוא רוצה להעביר, שמטרתו העיקרית היא ליצור פחד, תוך "ניהול מחושב של האכזריות" והיעדר רחמים.[37] הקמפיין הוויראלי של עריפת ראשים, צליבות, שריפות והוצאות להורג המוניות, הזוכה לתפוצה באמצעי התקשורת השונים, נעשה באופן ברוטלי ובאכזריות חסרת תקדים.

טרור הוא סוג של תעמולה, וככל שהוא מכיל אלמנטים אכזריים יותר, ההשפעה שלו רבה ומשאירה חותם גדול יותר. התיאור הגרפי המצמרר של עריפת הראש, תוך התמקדות בפרט הבודד חסר ההגנה, משפיע יותר מתעמולה המושגת באמצעים כגון מכוניות תופת ופעולות טרור "קונוונציונליות", גם אם מספר מקרי המוות בהם

גבוה יותר.[38] דאע"ש מנצל את הפוטנציאל הטמון בגלובליזציה הרשתית ומפעיל בצורה סימולטנית מנגנוני השפעה המוניים שונים ומגוונים, חלקם מבוססי משחקי מחשב ורשת וחלקם קונוונציונליים יותר, מבוססי רשתות חברתיות.[39] מהלכים אלה אפשרו לדאע"ש ליצור מסע תעמולה מקוון, מתוחכם ומתוזמן היטב.

מכונת התעמולה של דאע"ש והשימוש שהארגון עושה במדיה החברתית ובאמצעי התקשורת ממלאים שתי פונקציות חשובות, הנבדלות זו מזו באופן מהותי בתכליתן ומסתמכות על פלטפורמה תקשורתית שלא הייתה קיימת לפני כעשור. הפונקציה הראשונה היא לוחמה פסיכולוגית, שנועדה לפגוע במורל חיילי היריב. אסטרטגיה זו אינה חדשה. כבר סון דזה ("החכם סון") כתב כי הכרעה מושגת ברובה על ידי "עריפת ראשן של מטרות צבאיות וחברתיות באופן סלקטיבי ומידי, במטרה להשיג הלם ומורא", וזאת על ידי שימוש באמצעים אכזריים וחסרי רחמים כגון עריפת ראשים.[40] "מלחמת הבזק" במלחמת העולם השנייה ביטאה תפיסה דומה, שהתבססה על הפחדה של האויב באמצעות לוחמה פסיכולוגית. זו כָּללה פיזור עלונים מהאוויר, השמעת מסרים באמצעות רמקולים רבי עוצמה וכדומה.

הפונקציה השנייה של מכונת התעמולה של דאע"ש נוגעת להשגת תמיכה מצד גורמים אסלאמיים מערביים, תוך הבאת לוחמיו של ארגון "המדינה האסלאמית" להתאחד תחת מטרה אחת וקורת גג אחת. הדרך לעשות זאת היא קריאה לחזרה אל שורשי האסלאם ומתן הכשר למתגייסים לבצע מעשי אלימות, ללא צורך לתת על כך דין וחשבון.

השילוב של אכזריות מצד אחד עם שימוש במדיה החברתית מצד שני הוכיח עד כה הצלחה רבה ומשמש כלי רב עוצמה בידי דאע"ש, המשתלב בארסנל הצבאי שלו. הצלחה זו של הארגון הביאה את ממשלת עיראק, בצעד יוצא דופן, לאסור ביוני 2014, במהלך הלחימה בארגון, על שימוש במדיה חברתית במשך 17 יום. במסגרת זו נחסמו יותר מעשרים אתרי חדשות, כולל אתר "אל־ערביה", מתוך כוונה להפריע לתקשורת בין חברי דאע"ש.

ארגון דאע"ש פועל בצורה שונה מארגון "אל־קאעידה", שנמנע ככל שניתן מפגיעה באזרחים מוסלמים חפים מפשע כדי לא לאבד את תמיכת האוכלוסייה. מנהיג "אל־קאעידה", איימן א־זוואהירי, קבע כי עדיף להרוג בני ערובה בירייה ולהתמקד במתקפות על הכוחות האמריקאיים והעיראקיים: "אתה לא צריך להיות מרומה על ידי דברי השבח והחנופה של הצעירים הפנטיים המתארים אותך כראש וראשון לטובחים". א־זוואהירי הוסיף את תובנותיו לגבי חשיבותה של התקשורת: "אנו נמצאים במאבק, ויותר מחצי ממאבק זה מתרחש בשדה הקרב של התקשורת. קרב זה הוא בעצם תחרות על לֵבם ומוחם של אנשינו".[41]

דאע"ש, בניגוד ל"אל־קאעידה", אינו בוחל באמצעים ופוגע באופן אלים גם באוכלוסייה מוסלמית מקומית, תוך יישום אידיאולוגיה רצחנית. אידיאולוגיה זו גורסת כי הגשמת החזון של המדינה האסלאמית ייעשה על ידי פרובוקציות, דוגמת פיגועים באתרים אסטרטגיים ותשתיות לאומיות.[42] דאע"ש רואה בשימוש באלימות אכזרית (rough violence) דבר הכרחי, וחשיבות דומה הוא מייחס לשימוש במדיה, אותה הוא רואה כצעד הכרחי ליצירת תעמולה אפקטיבית.

הצלחת האסטרטגיה של דאע"ש מוצאת את ביטויה במספר מאפיינים עיקריים המייחדים את פעילות הארגון בהשוואה לארגוני טרור אחרים ומהווים קריטריונים להצלחתו: כיבוש שטחים נרחבים תוך פרק זמן קצר יחסית בסוריה ובעיראק, ביסוס שלטונו בהם והקמת החליפות האסלאמית. דאע"ש, שהוקם כשלוחה של "אל־קאעידה" בעיראק, התפשט למזרח סוריה ולצפונה, תוך שהוא מנצל את חולשת המשטר העיראקי. כיום הוא שולט על אוכלוסייה של 10–12 מיליון איש ועל כשליש משטחה של עיראק וכשליש משטחה של סוריה – שטח השווה בהיקפו כמעט לכל שטחה של בריטניה.

התמודדות עם דאע"ש מחייבת לפעול במספר רבדים, בנוסף לפעילות הצבאית של כוחות הקואליציה. הרובד הראשון נוגע לאיתור ולפגיעה ב"נתיב הכסף" – המסלול דרכו מצליח הארגון להפעיל מערכת פיננסית ענפה לצרכיו. פעולה זו מחייבת מאמץ מודיעיני ומאמץ של לוחמה כלכלית חובקי עולם, במטרה לזהות ולנטרל את הגורמים המעורבים במימון הארגון ובסחר עִמו. לצד מאמץ זה יש להפעיל מאמץ מדיני משלים, בעיקר מול טורקיה וקטר, שבתמיכתן באסלאם הקיצוני ובהתעלמות ממעבר מתנדבים לדאע"ש דרך הגבול המשותף בין טורקיה לסוריה מנסות לאחוז את המקל משני קצותיו. במקביל יש לפתוח במאבק מודיעיני ומבצעי במרחב הקיברנטי. מאבק זה נוגע לשני רבדים נוספים: הרובד הראשון עוסק בצמצום החשיפה של הארגון ברשת, על ידי הורדה של אתרים ותכנים המשמשים את דאע"ש לצורך גיוס פעילים, ליצירת פיגועי השראה, לגיוס כספים וללוחמה פסיכולוגית. כדי למנוע זאת יש ליצור תשתית משפטית ולהגיע להבנה עם ענקי אינטרנט, שלהם יש אינטרסים מסחריים. היכולת הטכנולוגית לביצוע צעדים מעשיים כאלה קיימת, אולם ללא הקמה של צוות משימה בין־לאומי, שיפעל מידית להסרה אפקטיבית של תכנים פוגעניים מהרשת, יקשה להתמודד עם תופעה זאת. צוות כזה יוכל, בנוסף, לפעול לקעקוע הנרטיב של דאע"ש באמצעות קמפיינים נגדיים ברשתות החברתיות, בבחינת "לחימה באש באמצעות אש".

הרובד השני הוא ההתמודדות עם פיגועים ספונטניים במדינות המערב. בשל בשל העובדה שלרוב פיגועים אלה אינם מחייבים תשתית ארגונית במדינה בה נעשה הפיגוע, נדרש ליצור כלי התמודדות מתאימים למאבק זה. אחד הכלים הוא היכולת לייצר פרופיל של מַפגעים פוטנציאליים. פרופיל זה ייבנה מתוך

מגוון מקורות, שהעיקרי בהם הוא ניתוח של מאפייני הפעולה ברשת האינטרנט של אוכלוסיות המוּעדות לפורענות. במקרים רבים ניתן למצוא בדיעבד סימנים מעידים לרצון לבצע פיגוע. גם במקרה זה נדרש להקים צוות משימה בין־לאומי, שיוכל לגבש את המתודולוגיה לבניית פרופיל של מַפגעים פוטנציאליים ולבנות את הכלים לזיהוּיָם, וזאת על בסיס ניתוח של נתוני Big Data שייאספו באופן קבוע. האתגר המרכזי בגישה זו נוגע להבניה של מאפייני הפרופיל של מַפגעים פוטנציאליים יותר מאשר להיבטים הטכנולוגיים של מערכות הניתוח. ארגוני הביטחון במדינות המערב חולקים אותו אינטרס, ולכן הם יוכלו לשתף פעולה בבניית היכולת האמורה, ובכך לאגד יכולות ולזרז את יישום התפיסה.

דעא"ש פועל באופן שיטתי במרחב הקיברנטי ויצר לעצמו מודל מוצלח של שימוש במרחב זה לקידום מטרותיו. מדינות המערב, בהובלת ארצות הברית, חייבות לעשות מאמץ משולב כדי להתמודד עם התופעה בטרם יהיה מאוחר מדי. המדובר בפעולה מדינית, משפטית, כלכלית, מבצעית וטכנולוגית. רק שילוב של מכלול פעולות זה, לאורך זמן, יוכל לאפשר מאבק אפקטיבי בארגון "המדינה האסלאמית" ובתופעות הג'יהאד בעולם המערבי.

הערות

1 "Canadian ISIS Fighter To Muslims In Canada: You Have A Religious Duty To Either Emigrate To The Islamic State, Or Else Carry Out Attacks In Canada," MEMRI, December 8, 2014, http://www.memrijttm.org/canadian-isis-fighter-to-muslims-in-canada-you-have-a-religious-duty-to-either-emigrate-to-the-islamic-state-or-else-carry-out-attacks-in-canada.html

2 Carlos Marighella, *Minimanual of The Urban Guerrilla*, 1969, http://www.marxists.org/archive/marighella-carlos/1969/06/minimanual-urban-guerrilla/ch32.htm

3 דניאל כהן, "להילחם בדאע"ש גם ברשת", **הארץ**, 4 בספטמבר 2014, http://www.haaretz.co.il/opinions/.premium-1.2424714.

4 Neville Bolt, *The Violent Image: Insurgent Propaganda and the New Revolutionaries* (London: Hurst & Company, 2012).

5 **דאע"ש: דיוקנו של ארגון טרור**, מרכז המידע למודיעין ולטרור על שם אלוף מאיר עמית, 26 בנובמבר 2014, http://www.terrorism-info.org.il/he/article/20733

6 "Antiterrorism Seminar Discusses Media Role", *A-sharq Al-Awsat*, November 25, 2005, http://www.aawsat.net/2005/11/article55268813

7 Angela Gendron, "Al Qaeda: Propaganda and Media Strategy," *ITAC Trends in Terrorism Series* 2, 2007, http://www.itac.gc.ca/pblctns/index-en.php?id=07

8 להרחבה על מנגנוני ההסברה של דאע"ש ראו: **דאע"ש: דיוקנו של ארגון טרור**.

9 התרגום המילולי של "אל־פרקאן" הינו "הבחנה", קרי הבחנה בין אמת לשקר.

10 Ryan Mauro, "ISIS Releases 'Flames of War' Feature Film to Intimidate West," *The Clarion Project*, September 21, 2014, http://www.clarionproject.org/analysis/isis-releases-flames-war-feature-film-intimidate-west

11 Brad Conley, "Leni Riefenstahl – Triumph Des Willens [1935] [HD]," February 25,

2014, https://www.youtube.com/watch?v=rclIE-_VZ5g

12 'מוסד אל־פורקאן להפקה הסברתית' מציג סרט חדש של דאע"ש –"Online Jihad Exposed," 18 במאי 2014, http://www.onlinejihadexposed.com/2014/05/4.html

13 Nico Prucha, "Is this the Most Successful Release of the Jihadist Video Ever? (Part 1)," *Jihadica*, May 19, 2014, http://www.jihadica.com/is-this-the-most-successful-release-of-a-jihadist-video-ever; Nico Prucha, "Is this the Most Successful Release of the Jihadist Video Ever?, Ideological Trends, Iraq, Social Media", May 19, 2014, http://www.jihadica.com/is-this-the-most-successful-release-of-a-jihadist-video-ever, /عبار لا-مراوصلا-لبلصـ-part-2-the-release-of

14 Terrorism Research & Analysis (TRAC) Press Room, http://www.trackingterrorism.org/content/trac-press-room.

15 "New ISIS Media Company Addresses English, German And French-Speaking Westerners," *MEMRI: Jihad & Terrorism Threat Monitor*, June 23, 2014, http://www.memrijttm.org/new-isis-media-company-targets-english-german-and-french-speaking-westerners.html

16 ראו לדוגמה: https://azelin.files.wordpress.com/2014/06/islamic-state-of-iraq-and-al-shc481m-22islamic-state-report-122.pdf

17 כתב העת "דאביק" קרוי על שם המקום בצפון סוריה המוזכר בחדית' על אחרית הימים, שבו צפוי להתקיים קרב גדול בין האסלאם ובין הכופרים. בקרב זה המוסלמים עתידים לנצח.

18 ראוי לציין שבאוקטובר 2014 הוציא ארגון "אל־קאעידה" לאור את המגזין החדש "התעוררות" (*Resurgence*) לאחר דחיה מחודש מארס. המגזין שפורסם באנגלית, מתמקד בנושאי ג'יהאד כלליים וכולל, בנוסף לכך, תכנים עכשוויים על פעילות הארגון בתת־היבשת ההודית.
http://www.longwarjournal.org/archives/2014/10/al_qaedas_resurgence.php

19 אתר שיתוף תוכן של תנועת הג'יהאד העולמי:
Al-Platform Media: alplatformmedia.com/vb

20 *Summary of Information on Jihadist Websites*, ICT Jihadi Monitoring Group Periodic Review: Bimonthly Report, International Institute for Counter-Terrorism (ICT) at the Interdisciplinary Center at Herzliya, February 2014, http://i-hls.com/wp-content/uploads/2014/06/JWMG122014.pdf

21 האשטאג ("Hashtag") נמצא בשימוש ברשתות חברתיות כדי לתייג פוסט כלשהו כחלק מנושא מסוים, וזאת על ידי הוספת סולמית לפני הנושא. כך ניתן למצוא תכנים בנושא מסוים באופן יעיל.

22 David Shamah, "Video Games, Twitter Tricks: How ISIS Pulls in the Kids," *The Times of Israel*, September 21, 2014, http://www.timesofisrael.com/video-games-twitter-tricks-how-isis-pulls-in-the-kids-2

23 על שימוש בפלטפורמות המדיה השונות, ובפרט על השימוש במשחקי מחשב, ניתן לקרוא במחקר מעמיק שפורסם ב"מרכז דדו לחשיבה צבאית בינתחומית". ראו: דניאל ברן ויוסי לוי, "תופעת המדינה האסלאמית – מה המערב לא מבין?", **בין הקטבים**, גיליון 3, ינואר 2015.

24 Samuel Burke, "Facebook Looks to Block ISIS Clothing Sales," *CNN*, June 25, 2014, http://edition.cnn.com/2014/06/24/world/isis-facebook-merchandise

25 Gabriel Weinmann and Conrad Winn, *The Theater of Terror: The Mass Media and International Terrorism* (New York: Longman Group, 1993).

26 Stephen L. Carter, "Boston and the Terrible Theater of Terrorism," *Bloomberg*, April 18, 2013, http://www.bloombergview.com/articles/2013-04-18/boston-and-the-terrible-theater-of-terrorism

27 Gabriel Weinmann, "The Role of the Media in Propagating Terrorism," in: *Countering Terrorism: Psychological Strategies*, eds. Updesh Kumar and Manas K. Mandal (London: SAGE Publications, 2012), pp. 182-203.

28 בועז גנור, **אסטרטגיית הטרור המודרני ותפקידה של התקשורת** (הוצאה לאור מטח: המרכז לטכנולוגיה חינוכית והמרכז הבינתחומי הרצליה, המכון למדיניות נגד הטרור, 2007); בועז גנור, **מבוך הלוחמה בטרור: כלים לקבלת החלטות** (הוצאת מפעלות המרכז הבינתחומי הרצליה, 2003), עמ' 207–213.

29 "בחמישה חודשים: דעא"ש הוציא להורג 1,500 איש בסוריה", *NRG*, 17 בנובמבר 2014, http://www.nrg.co.il/online/1/ART2/646/773.html

30 Karen Yourish, "The Fates of 23 ISIS Hostages in Syria," *The New York Times*, November 17, 2014, http://www.nytimes.com/interactive/2014/10/24/world/middleeast/the-fate-of-23-hostages-in-syria.html?_r=0

31 Robert Spencer, "Islamic State: 'We Will Conquer your Rome, Break your Crosses, and Enslave your Women, by the Permission of Allah,'" *Jihad Watch*, September 21, 2014, http://www.jihadwatch.org/2014/09/islamic-state-we-will-conquer-your-rome-break-your-crosses-and-enslave-your-women-by-the-permission-of-allah

32 את הקלטת ניתן לשמוע בקישור: http://ent.siteintelgroup.com/Statements/is-spokesman-had-called-for-lone-wolf-attacks-in-australia-in-september-2014-speech.html

33 לדוגמה: Perry Chiaramonte, "Citizen Jihadists: ISIS Uses 'Lone Wolves' to Mount Cheap, Effective Attacks on US Soil," *FOX News*, October 25, 2014, http://www.foxnews.com/world/2014/10/25/citizen-jihadists-isis-uses-lone-wolves-to-mount-cheap-effective-attacks-on-us/

34 *Islamic State Beheads American Journalist Steven Sotloff,* graphic video, http://leaksource.info/2014/09/02/graphic-video-islamic-state-beheads-american-journalist-steven-sotloff/.

35 "דאע"ש פרסם סרטון חטוף: 'אחשוף את האמת'", *YNET*, 18 באוגוסט 2014, http://www.ynet.co.il/articles/0,7340,L-4572689,00.html

36 "Over 1,400 People Executed in Syria by ISIS in 5 Months: Monitor", November 19, 2014, http://khabarsoutheastasia.com/en_GB/articles/apwi/articles/newsbriefs/2014/11/19/newsbrief-01

37 Alastair Cooke, "The ISIS's 'Management of Savagery' in Iraq," *The World Post*, updated August 30, 2014, http://www.huffingtonpost.com/alastair-crooke/iraq-isis-alqaeda_b_5542575.html

38 Shashank Joshi, "Where does the Islamic State's Fetish with Beheading People Come from?," *The Telegraph*, September 14, 2014, http://www.telegraph.co.uk/news/worldnews/middleeast/syria/11071276/Where-does-the-Islamic-States-fetish-with-beheading-people-come-from.html

39 ברן ולוי, "תופעת המדינה האסלאמית – מה המערב לא מבין?", עמ' 18.

40 Harlan K. Ullman and James P. Wade, *Shock and Awe, Architecting Rapid Dominance*

(NDU Press Book, December 1996), http://www.globalsecurity.org/military/library/report/1996/shock-n-awe_ch2.html

41 Craig Whitlock, "Keeping Al-Qaeda in his Grip," *The Washington Post*, April 16, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/04/15/AR2006041501130.html

42 Abu Bakr Naji, *The Management of Savagery: the Most Critical Stage through which the Umma Will Pass,* trans. William McCants (Cambridge: The John M. Olin Institute for Strategic Studies at Harvard University, May 23, 2006).

חשיפת המשק הישראלי לריגול סייבר עסקי

שחר ארגמן וגבי סיבוני

מרחב הסייבר מתאים במיוחד לגניבת מידע עסקי ולריגול. הנגישות למידע לצד היכולת לשמור על אנונימיות, תוך טשטוש עקבות, מאפשר לגורמים שונים לעסוק בגניבת מידע בעל ערך, שנזקה עלול להיות רב. תופעה זו רלוונטית מאוד גם למדינת ישראל, החשופה במידה ניכרת לאיומי הסייבר בשל היותה עתירת טכנולוגיה מתקדמת כשחלקה של התעשייה מבוססת החדשנות והנשענת על קניין רוחני ייחודי, הוא רב מאוד. המאמר בוחן את היקף התופעה בעולם תוך נסיון לאמוד את היקף נזקיה הכספיים במדינות העולם ואף בישראל במסגרת הבהרת המורכבות של אומדנים אלה. מחברי המאמר מנסים להעלות את המודעות של הגורמים הרלוונטיים בישראל ובעולם להיקף התופעה תוך נסיון לתת המלצות באשר לכיווני ההתמודדות איתה.

מילות מפתח: סייבר, ריגול, ריגול עסקי, קניין רוחני, פשיעת סייבר, גניבת סייבר, טכנולוגיה

"There are two types of companies: companies that have been breached and companies that don't know they've been breached [...] the vast majority of companies have been breached"
Shawn Henry[1]

"The price tag for intellectual property theft from U.S. companies is at least $250 billion a year [...] it's the greatest transfer of wealth in history"
Gen. Keith B. Alexander[2]

שחר ארגמן הוא ראש אגף במטה הסייבר הלאומי.
אל"ם (מיל') ד"ר גבי סיבוני הוא ראש תוכנית צבא ואסטרטגיה וראש תוכנית לוחמת סייבר במכון למחקרי ביטחון לאומי.

מאמר זה ראה אור לראשונה ב**צבא ואסטרטגיה**, כרך 6, גיליון 1, מארס 2014, עמ' 39-52.

רקע

המרחב הקיברנטי הוא תולדה של ההתפתחות הטכנולוגית המואצת בעשורים האחרונים. תחילה חוברו להן יחדיו מערכות תקשורת ומערכות ממוחשבות שפעלו כרשתות מקומיות. לאחר מכן חוברו הרשתות אלו לאלו לכדי מרחב פעולה והוויה גלובלי. מאז הולך המרחב הקיברנטי ומתפתח במספר מישורים: בעושר אמצעי המחשוב המקושרים ביניהם, במספר הרשתות ובסוגיהן, בנפחי התעבורה של המידע, ברמת הקישוריות, במגוון היישומים ובמידת התלות הכלכלית והחברתית בו.

בד בבד עם היתרונות העצומים הגלומים במרחב הסייבר, טומן מרחב זה בחובו איומים חדשים וחמורים, ההופכים אותו לתווך חדש לפעילות עוינת. פעילות כזו עלולה להתבטא הן בפגיעה בידע ובתפקוד בתוך מרחב הסייבר והן בפגיעה במרחב הפיזי דרך מרחב הסייבר.[3] לצד התרחבות השימוש הכולל במרחב הסייבר, גם הפעילות העוינת המתקיימת בו נמצאת בעלייה מתמדת.[4] מגוון האיומים בסייבר הוא רחב ביותר.

הוא כולל מניעת שירות, השחתת אתרים, חשיפת פרטים לצורך הפחדה והשפעה, פשיעה מסוגים שונים, ריגול מסחרי וביטחוני ופגיעה בתשתיות לאומיות אסטרטגיות, במאגרי מידע, במערכות שליטה ובקרה ואף במערכות נשק.

מרחב הסייבר מהווה, מעצם טבעו, ממד מתאים במיוחד לפעילות ריגול בכלל ולריגול עסקי בפרט. ריגול בין חברות מסחריות אינו תופעה חדשה, אולם השימוש במרחב הסייבר מאפשר יצירת נגישות למידע רב באופן פשוט יותר, תוך שמירה על חשאיות ברמה טובה. הנזק כתוצאה מריגול עסקי קיבל בימינו ממדים חדשים ומאיימים כתוצאה מהתאמתו האופטימלית של מרחב הסייבר לפעילות מסוג זה. מרחב הסייבר הפך לתווך מרכזי לביצוע פעולות ריגול גם בשל העובדה שגופי מודיעין מדינתיים פועלים בו כדי להשיג מטרות מדינתיות – פוליטיות, ביטחוניות, טכנולוגיות וכלכליות. זאת, לצד פעילות של ארגוני פשיעה, העושים זאת למען בצע כסף. מהמידע הרב המתפרסם לאחרונה על העיסוק של מדינות בריגול במרחב הסייבר, ובפרט על מאבקי הסייבר בין ארצות הברית לסין, עולה כי הריגול העסקי הפך לכלי מרכזי בין מדינות בכלל ומעצמות בפרט, כחלק ממלחמה כלכלית ביניהן וממאמציהן להשגת דומיננטיות גלובלית.

מדינת ישראל חשופה במידה ניכרת לאיומי הסייבר עקב היותה עתירת טכנולוגיה מתקדמת. הידע הרב שנוצר בארגונים כלכליים, מדעיים ואחרים במדינת ישראל נשמר, משונע ומנוהל במרחב הסייבר, ועל כן הוא נגיש לגורמי תקיפה שונים. בנוסף, חלקה של התעשייה מבוססת החדשנות והקניין הרוחני הייחודי בתוך כלכלת ישראל הוא משמעותי מאד. תעשיית חברות ההזנק הישראלית היא מהמובילות בעולם, וגם נתון זה מגביר כמובן את המוטיבציה לריגול עסקי בישראל.

בשל העובדה שמערכי ריגול ייעודיים מתקדמים (APTs – Advanced Persistent Threats) כמעט ואינם מתגלים על ידי אמצעי ההגנה הסטנדרטיים שבהם נעשה שימוש לצרכי אבטחה בחברות מסחריות, ניתן להניח שחברות ישראליות, במיוחד כאלו המפַתחות ידע ייחודי, מהוות יעד לריגול מסחרי ולגניבת קניין רוחני, כמו במדינות מתקדמות אחרות.

מטרת מאמר זה היא לבחון את השימוש במרחב הסייבר לצורך ריגול עסקי וגניבה של קניין רוחני. בנוסף מבקש המאמר להציף את המורכבות של הערכת היקף התופעה והנזקים הכספיים שהיא גורמת, ולבסוף – לנתח את היקף הריגול המסחרי בישראל. זאת, כדי להגביר את המודעות אליו בשיח הציבורי, ובעקבותיה – את הפעילויות הנדרשות לצמצום התופעה ונזקיה.

הסייבר כתווך לריגול עסקי

ריגול עסקי קיים אמנם משחר ההיסטוריה, אולם עם מעבר העולם העסקי לפעילות ענפה בסייבר, התפתח מאד גם הריגול העסקי במרחב זה. מרחב הסייבר מתאים מעצם טבעו לפעילות ריגול, ובמיוחד לריגול עסקי. הוא מאפשר פעילות אנונימית באופן יחסי, לרבות העברה נוחה ובטוחה של כמויות מידע עצומות בלי תלות במרחק ובגבולות. במקביל, הוא מקשה מאד על קורבן הריגול – יהיה זה ארגון מסחרי או ממשלתי – להבחין בעצם פעילות הריגול. אפילו אם הנתקף הבחין בתקיפה וזיהה את הכלים ששימשו לביצועה (Spyware), יש לו קושי לשייך את הפעולה הזדונית שהתגלתה לגורם המבַצע ולבסס האשמה אמינה לגבי זהות הגורם התוקף.

הריגול המסחרי בסייבר מתאפשר בעלות נמוכה מאד בהשוואה לדרכי איסוף מודיעיני אחרות, ובסיכונים מבצעיים נמוכים. כך, לדוגמה, פעילות ריגול במרחב הסייבר מצמצמת מאד את הצורך בסוכנים ביעד. תודות למצב עניינים זה, יכולים היום גורמי ביון ברחבי העולם להעצים את יכולותיהם, הן באיסוף המתבצע כולו במרחב הסייבר[5] והן על ידי שילוב כלי ריגול "קלאסיים" עם היכולות החדשות במרחב זה. כך, פעילות הריגול הופכת לפשוטה יותר לַתוקף ומסוכנת יותר לנתקף. לדוגמה, פעילות ריגול בה מעורב סוכן העובד בארגון המותקף, הופכת לפשוטה יותר בעידן הסייבר: העברת המידע הגנוב קלה יותר, וקשה יותר לשייכה לגורם המבַצע. גם יחסן של רשויות החוק לפשיעה בסייבר מקל ומצמצם את הסיכון לעוסקים בריגול המסחרי. כך, פורץ שייתפס בפריצה פיזית לחברה מסחרית לצורך גניבת מידע, צפוי לשלם על כך מחיר גבוה הרבה יותר מעמיתו השולח את ידו להשגת אותו מידע דרך המקלדת.

ריגול עסקי יוגדר כהוצאה לא ברשות של מידע עסקי חסוי שאינו נחלת הכלל, שמטרתה השגת יתרון טכנולוגי ו/או רווחים כלכליים. מידע כזה כולל נתונים

בתחומי האסטרטגיה, התכנון, החדשנות הטכנולוגית, תהליכי פיתוח מוצרים, תהליכי ייצור ושיווק, תוכניות פרסום, מצב פיננסי, סוגיות משפטיות, אנשי מפתח, נתוני שכר, נתוני מכרזים ועוד. הגניבה יכולה להיעשות לא רק מארגונים מתחרים אלא גם מגופים דוגמת מכוני מחקר אקדמיים, שבהם יש מידע רב ערך.

השגת המידע כרוכה, במקרים רבים, בעבירה על החוק, להבדיל מאיסוף מידע עסקי ממקורות גלויים. פעילות זו היא ענף אחד במשפחה רחבה של "פשיעה כלכלית", הכוללת מעילות והונאות, גניבות, הרס ושיבוש פעילות עסקית ועוד. ריגול עסקי המבוצע בידי מדינה נעשה, בדרך כלל, במטרה לחזק את הכלכלה המקומית, כדי ליצור יתרון לכלכלת אותה מדינה או לסקטור מסויים בכלכלתה ביחס לכלכלות מתחרות בעולם.

העלייה בהיקף הריגול העסקי המבוצע במרחב הסייבר משקפת את השינויים הטכנולוגיים, הכלכליים והחברתיים שמתרחשים בשנים האחרונות באופן שבו מידע נוצר, משונע, נאגר ומנוהל בארגונים כלכליים ומדעיים ובגופים רגישים אחרים. כמעט כל הרשומות המסחריות והמדעיות, אפילו הרגישות ביותר, נשמרות באופן דיגיטלי ונגישות דרך רשתות מחשב ברחבי העולם. לאור זאת, ולאור העדיפות שנותנים כיום תוקפים מתוחכמים דוגמת גופי מודיעין מדינתיים או ארגוני פשע מתוחכמים, מתאפשר לגופים אלה לעשות שימוש במרחב הסייבר לביצוע גניבת מידע מסחרי ועסקי. גניבות אלו הן בשיעור גדול משמעותית מכל ריגול עסקי שהיה מוכר בעבר, הן במידת החשיבות והרגישות של המידע הגנוב לבעליו והן בכמותו.

הניסיון מראה שרק חברות מעטות מסוגלות לזהות תקיפות מתוחכמות המבוצעות על ידי ארגון ביון מדינתי או ארגון פשיעה מתקדם, ומעטות עוד יותר מסוגלות להתגונן בפניהן באופן יעיל.[6] ישנן דוגמאות רבות המצביעות על כך, שגם החברות הרגישות ביותר בתעשיות הביטחון בארצות הברית היו טרף קל יחסית לריגול מסחרי (או ביטחוני) דרך הרשת שבוצע על ידי ארגונים מדינתיים, כנראה מתוך מוטיבציה מסחרית.[7]

דוח של המשרד הלאומי למניעת ריגול בארצות הברית (ONCIX), שהוגש לקונגרס האמריקאי,[8] כולל התייחסות לאיום גניבת המידע המסחרי וליריבים המרכזיים המבצעים פעילות זו בארצות הברית. סין ורוסיה נזכרות בדוח כבעלות היכולות הגבוהות ביותר בתחום זה, ומאופיינות בו כמדינות "האגרסיביות ביותר באיסוף של מידע מסחרי וטכנולוגי אמריקאי".[9] בדוח נוסף של אותו גוף לקונגרס האמריקאי, מיולי 2012,[10] מצוטטים דברי גנרל ג'יימס קְלָפֶּר,[11] בעדותו בפני הקונגרס על הערכת האיומים הלאומית של קהילת המודיעין האמריקאית. קלפר העיד כי גופי מודיעין של מדינות יריבות מפתחים באופן עקבי מתודולוגיות וטכנולוגיות המאתגרות את יכולותיהם של גופי הממשל והסקטור הפרטי בארצות הברית להגן

על הסודות הלאומיים והמסחריים שלה.[12] ואכן, דוח הערכת האיומים האמריקאי לשנת 2013 מצביע על עלייה של איום הסייבר לראש רשימת האיומים על ארצות הברית,[13] לפני איומי הטרור והפצתו של נשק להשמדה המונית.

מורכבות הערכת הנזק של הריגול המסחרי

מטֶבע הדברים, יש קושי רב להעריך את מידת הנזק הנגרם כתוצאה מריגול מסחרי. הסיבות העיקריות לקושי זה נוגעות למגוון היבטים, בהם הקושי המתודולוגי לכמת את היקף הנזק הנגרם ליריב כתוצאה מאובדן הקניין הרוחני, ובשל העובדה שרק חלק מזערי מכלל פעילויות הריגול המתקדם מתגלה. ריצ'ארד ביטליך, מנהל האבטחה בחברת Mandiant, המתמחה בתחקור אירועי תקיפה בסייבר, העיד בפני ועדה ממשלתית בארצות הברית כי מתוך סך אירועי התקיפות המתוחכמות לצרכי ריגול שמקורן בסין, אותם תחקרה החברה, רק שישה אחוזים מהאירועים שהתגלו היו ידועים לחברות המותקפות. נתון זה מצביע על פער גדול מאד בין עוצמת התופעה לבין הבנת המחיר הכבד שהמשק משלם כתוצאה מריגול מסחרי.[14] בנוסף, פעילות הריגול המסחרי בסייבר, המבוצעת על ידי ארגונים מתקדמים, ממומשת בכלים ייעודיים לריגול, שכלי ההגנה הסטנדרטיים בהם עושים שימוש מרבית הארגונים אינם מסוגלים לזהות, לחסום או לנטרל. יש לזכור כי במרחב הסייבר קיים היום יתרון מובהק לתוקף.

ארגוני ביון רבים עושים שימוש בסייבר כזירה מרכזית לאיסוף ידיעות, ויכולות שפותחו לצורך כך בגופים ביטחוניים משיגות את המענה ההגנתי הנוכחי לאיומים אלו. זאת ועוד, התוקף הייעודי הממוקד נהנה גם מהיתרון שהוא יכול ללמוד על כלי האבטחה של המגן ואף להצטייד בהם,[15] וכך לבצע סימולציות המאפשרות לו למצוא את התנאים לא להתגלות על ידי כלי האבטחה בהם עושה הנתקף שימוש.[16] בנוסף לכך, פעילות הריגול המדינתית מבוצעת על ידי גופי מודיעין המאורגנים לצורך זה, בעוד שהיערכות להגנה מחייבת התארגנות מדינתית כוללת, המערבת גופים ביטחוניים וגופים מהמגזר הממשלתי שאינו ביטחוני וכן מהמגזר הפרטי – התארגנות שמטֶבעה היא מסורבלת ואיטית יותר.

ארגון ה־FBI העריך כי מול כל אירוע בו חברה אמריקאית זיהתה שרשתות המחשב שלה נפרצו, התרחשו כמאה אירועים דומים, בהם חברות שרשתות המחשב שלהן נפרצו לא הבחינו בכך.[17] דוח של חברת האבטחה האמריקאית Mandiant, שפורסם בפברואר 2013,[18] קובע כי תכליתו של מערך התקיפה הסיני היא ריגול מסחרי וכי הוא תקף באותה שנה 141 חברות מערביות, בעיקר בארצות הברית. זוהי דוגמה לפעילות ריגול מסחרי המבוצעת על ידי גוף מדינתי, שהתנהלה במשך שנים ולא עלתה כלל לתודעה הציבורית עד לפרסום הדוח.[19] אפשר להקיש מדוגמה זו על כך שחברות אחרות, הנתקפות על ידי מערכי תקיפה מתקדמים,

אינן מצליחות במרבית המקרים להבחין בתקיפה. גם במקרים המעטים שבהם הן מצליחות לזהות שהן הותקפו, הנושא אינו מגיע לידיעת הציבור, והמשמעויות הכלכליות והאבטחתיות לא נלמדות בהקשר המדינתי הכולל.

במקרים המעטים שחברות וארגונים מצליחים להבחין בקיומה של פעילות ריגול המתבצעת נגדם, ואף מאתרים תוכנת ריגול שהותקנה במחשבי הארגון, הם מתקשים להעריך את היקף וסוג המידע שכבר דלף מתוך רשתותיו. הכישלון בהגנה על נכסי החברה או הארגון גורם לכך שאחראֵי האבטחה בהם נוטים לעתים להעריך בחסר את הנזקים שגרמה פעילות הריגול.

הנטייה הטבעית כשמתגלה כלי תוכנה לא מוכר – תוכנה זדונית במחשבי החברה – היא להסיר אותו ולוודא שהמערכות ממשיכות לעבוד. רק במקרים מעטים מאד נערכת חקירה פורֶנזית מקיפה שמטרתה היא להבין את מהות התקיפה ולאתר את הכלים ששימשו למימושה, וזאת בשל עלותה הגבוהה הן בהיבט הכספי והן במשך הזמן הנדרש לביצוע החקירה הפורֶנזית שבמהלכה נפגע המענה התיקשובי בחברה. גם אם מתבצעת חקירה פורנזית מלאה ומקצועית, וזו מצליחה לחשוף את העובדות כהווייתן, וגם כאשר הנהלת החברה מקבלת תמונה מלאה ואמינה בנוגע לגניבת המידע המסחרי, ישנם מקרים רבים בהם הארגון מעדיף שלא לחשוף את הגניבה, או לכל הפחות לצמצם את הערכת הנזק, מתוך תקווה להקטין בכך את ממדי הפגיעה במוניטין שלו כתוצאה מפרסום האירוע. הפגיעה במוניטין עלולה, כמובן, לסכן את היחסים עם בעלי המניות, ציבור המשקיעים, הספקים, הלקוחות ובעלי עניין אחרים.

לבסוף, קיים קושי מובנה להעריך את ההיקף הכספי של הקניין הרוחני. ברור שערכו של הקניין הרוחני אינו משתקף בהכרח בערכה של ההשקעה שבוצעה כדי ליצור אותו. זו, כנראה, האמירה ההחלטית ביותר שניתנת להיאמר בעניין: לדוגמה, שווי התשואות העתידיות שיימנעו מהחברה כתוצאה מגניבת מידע עסקי דרך המרחב הקיברנטי הוא נתון סובייקטיבי המוּעד לספקולציות.

לאור סיבות אלו ונוספות, יש קושי רב לאמוד את הנזק המצטבר הנגרם לארגון כתוצאה מהריגול המסחרי בסייבר. קושי זה גובר כאשר מנסים לאמוד את הנזק הכלכלי הנגרם מתופעה זו למדינה. כתוצאה מכך, ההערכות המתפרסמות על מידת הנזק המדינתי הנגרם מגניבת מידע מסחרי ברשת נעות על פני מנעד רחב מאד.

שיטות הערכת הנזק המסחרי בעולם

מחקרים שונים, הדנים בתופעת הריגול המסחרי ועלותו, מנסים להציע מתודולוגיה לביצוע הערכת הנזק. פערי המידע המשמעותיים בנושא זה, הנובעים מהסיבות שהוזכרו לעיל, והקושי המובנה לתת להם מענה, מהווים אבן נגף להערכת היקף התופעה.

מקובל לחלק את עלות הפשיעה הקיברנטית לשלוש קבוצות עיקריות:[20] **עלות היערכות**, כמו מאמצי אבטחה, התאמה לתקני אבטחה נדרשים והוצאות ביטוח; **עלות נזק ישיר**, כמו פגיעה בתפקוד, תיקון הפגיעה, עלויות זמן עבודה, סגירת פרצות ושחזור מידע, הפסדים ישירים לעסק, פיצוי לקוחות, קנסות וסוגיות משפטיות; **אומדן נזק עקיף**, כמו אובדן אמון הלקוחות, אובדן עסקאות והכנסות עתידיות, פגיעה במותג וכדומה.

הגישות השונות להערכת הנזק מתבססות על סקרים וניתוח תיאורטי. במחקרים מבוססי סקרים מתבקשים מנהלים ומומחי IT בחברות מסחריות לאמוד את הנזק. מתוך אומדני קבוצת המדגם מתבצעת הרחבה אל הכלל. דא עקא שקיים פער עמוק בין הבנת התופעה אצל הנשאלים בקבוצת המדגם ובין היקף התופעה בפועל. פער זה מתעצם לאור העובדה שקבוצת המדגם צפויה להיות מוּטָה: אלה שחוו תקיפות כואבות אינם נוטים להתנדב ולספר על כך, ולפיכך אין זה צפוי שייקחו חלק במחקרים כאלה. לאור כל זאת, נדרשים מחקרים אלה לבצע תיקון מתאים של ממצאיהם. עניין זה כשלעצמו משפיע באופן דרמטי על הבנת היקף התופעה.

שיטת הניתוח התיאורטי מבוססת על מודל חישוב הנסמך על נתונים גלויים, השערות והערכות מומחים לאבטחת מידע, אנשי עסקים, כלכלה וגורמי אכיפה. גם מודל זה סובל מהפער בין איכות המידע הזמין ובין נתוני האמת וההתבססות על הערכות. דוגמה למחקר מסוג זה היא הערכת הנזק שנגרם כתוצאה מגניבה מסחרית בסייבר באנגליה, שנעשתה על ידי חברת Detica.[21]

הערכת סיכון ומדידתו חיוניים להבנת התופעה של גניבה במרחב הסייבר ולחלוקת משאבים אופטימלית להתגוננות מפניה. יש לכן עניין רב לארגונים ומדינות לאמוד את העלות הנגרמת להם כתוצאה מגניבת מידע. גנרל קית אלכסנדר, מפקד פיקוד הסייבר האמריקאי והעומד בראש הסוכנות לביטחון לאומי (NSA), טען בסימפוזיון על האיומים המתהווים בסייבר כי חברות אמריקאיות מאבדות כ־250 מיליארד דולר בשנה כתוצאה מגניבה של קניין רוחני.[22] הוא ציטט את הדוח של חברת "סימנטק", המעריך את "הנזק השנתי הישיר מפשיעת סייבר ב־114 מיליארד דולר, אולם הנזק המוערך הזה יכול לעלות ל־388 מיליארד דולר אם כוללים בו את הזמן וההזדמנויות העסקיות שאבדו".[23] דוח ועדה לבחינת גניבת קניין רוחני אמריקאי מעריך שהנזקים הנגרמים כתוצאה מגניבה כזאת עולים על 300 מיליארד דולר בשנה.[24]

מדינות נוספות על ארצות הברית מנסות גם הן להעריך את היקף התופעה: המשרד הפדרלי הגרמני להגנה על החוקה מעריך שלחברות גרמניות נגרם הפסד שנתי הנאמד בין 28 ל־71 מיליארד דולר וכי בין שלושים לשבעים אלף מקומות עבודה אובדים עקב ריגול כלכלי זר. דרום קוריאה דיווחה שהעלויות שנגרמו לה

כתוצאה מריגול כלכלי שבוצע על ידי גורמים זרים בשנת 2008 היו 82 מיליארד דולר, לעומת 26 מיליארד דולר ב־2004. לפי דיווח זה, שישים אחוזים מהקורבנות היו עסקים קטנים ובינוניים, ומקורן של מחצית מתקיפות הריגול המסחרי הוא בסין. משרד הכלכלה, המסחר והתעשייה של יפן ערך ב־2007 סקר בקרב 625 חברות יצרניות ומצא כי יותר מ־35 אחוזים מהחברות שנטלו בו חלק דיווחו על הפסד טכנולוגי כלשהו וכי יותר משישים אחוזים מהמקרים המדווחים היו קשורים לסין. גורמים בריטיים רשמיים העריכו כי ההתקפות על מערכות מחשב, כולל ריגול תעשייתי וגניבה של מידע מסחרי של חברות, עולות למגזר הפרטי הבריטי 34 מיליארד דולר לשנה. יותר מארבעים אחוזים מסכום זה נגרמים מגניבה של קניין רוחני, כמו מִפרטים, נוסחאות וסודות של חברות.[25]

טבלה 1: סיכום הערכות הנזקים כתוצאה מריגול כלכלי במדינות שונות בעולם

מדינה	הערכת הנזק השנתי כתוצאה מגניבת מידע מסחרי וקניין רוחני (במיליארדי דולר)	מידת הנזק כחלק מהתמ"ג (באחוזים)
ארצות הברית	300–250	2.0–1.67
דרום קוריאה	82	7.3
גרמניה	71–28	2.0–0.8
אנגליה	34	1.4

יש לציין כי המעריכים השונים לא נתנו הסבר לאופן שבו הם הגיעו להערכת עלות הנזק – ככל הנראה בשל הקשיים להעריך את הנזקים הישירים, ובמיוחד העקיפים, מפשיעת הסייבר. לקשיים אלה ניתן אולי להוסיף אינטרסים שונים של הגופים החוקרים, בעיקר של חברות אבטחת מידע מסוימות, החשודות בכך שיש להן עניין בניפוח ממדי התופעה.

מחקר שפורסם על ידי קבוצת המחקר של חברת McAfee,[26] ביולי 2013, מנסה להתמודד עם מורכבות ההערכה של עלות הפשיעה בסייבר. המחקר מציב סימני שאלה על אומדני העלות המתפרסמים במאמרים שונים ומנמיך את הערכות הנזק למשק האמריקאי המושמעות על ידי גופים רשמיים. המחקר לא קובע הערכות מוחלטות של עלויות הנזק, אך מראה למשל כי גבול הנזק העליון למשק האמריקאי נע על פי שיטת הערכה אחת בין 0.5 ל־2.0 אחוזים מהתמ"ג,[27] בעוד שעל פי שיטה אחרת הוא לא עולה על אחוז אחד מהתמ"ג.[28]

ריגול מסחרי בישראל

מדינת ישראל רגישה מאד לאיומי סייבר בכלל ולריגול מסחרי בפרט, עקב היותה מדינה עתירת טכנולוגיה מתקדמת. חלק ניכר מהייצוא של ישראל נשען על חברות שיש להן תלות רבה בקניין רוחני, וניתן לפיכך להניח שהיא מהווה יעד לגניבת קניין זה. בנוסף, חלקה של התעשייה המבוססת חדשנות וקניין רוחני ייחודי בכלכלת ישראל הוא משמעותי מאד: תעשיית חברות ההזנק הישראליות היא מהמובילות בעולם, וגם מצב זה מגביר את המוטיבציה לריגול עסקי בישראל. על אלה יש להוסיף את המודעות הנמוכה בקרב המגזר העסקי בישראל לסיכוני הריגול בסייבר, המביאה להעדפה של נוחות עבודה וניצול הזדמנויות עסקיות על פני אבטחה. ניתן אפוא להניח, שכמו במדינות מתקדמות אחרות, כך גם בישראל, חברות מסחריות, במיוחד אלו המפתחות ידע ייחודי, מהוות יעד לריגול מסחרי ולגניבת קניין רוחני. מבין 141 חברות מסחריות שהותקפו על ידי מערך התקיפה APT1, כמתואר על ידי חברת Mandiant, שלוש היו חברות ישראליות.[29]

מדינת ישראל הייתה בין המדינות המובילות בעולם בהפנמת איום הסייבר לתשתיותיה הקריטיות, אך לא בהפנמת איום הריגול העסקי. כבר ב־2003 הוקמה הרשות לאבטחת מידע – רא"ם[30] – שייעודה הוא אבטחת התשתיות הקריטיות של מדינת ישראל מפני תקיפות המבוצעות בתווך הקיברנטי ומאיימות לפגוע בתשתיות אלה, ומפני גניבת סודות מדינה. המגזר העסקי הפרטי והציבורי בישראל לא זכה למענה דומה, ואין כיום גוף בעל אחריות להגנת מגזר זה מפני ריגול מסחרי בסייבר. כתוצאה מכך, ישראל נמצאת כיום בפיגור בנוגע להגנת המגזר העסקי ביחס למדינות רבות בעולם, ובהן ארצות הברית. במדינות אלו התגבשה ההבנה שיש חשיבות להגנה מדינתית על הנכסים המסחריים הלאומיים וכי המדינה אחראית למתן נדבכי הגנה מדינתיים מפני האיומים בסייבר למשק בכלל ולמגזר הפרטי בפרט. הבנה זו הביאה להטלת אחריות לנושא על גוף או גופים מדינתיים, שמתפקידם להוביל את פעילות ההגנה המדינתית בסייבר במטרה לחזק את ההגנה הכוללת בתחום זה.[31]

קיים קושי רב להעריך את הנזק הנגרם למשק הישראלי מהריגול המסחרי. בישראל אין חובת דיווח על מציאת כלי איסוף במחשבי חברה, למעט הנחיות מינימליות בנוגע למידע הקשור למרשם האוכלוסין ולרגולציה במגזרים ייחודיים דוגמת הבנקים והגופים מפוקחי הרשות לאבטחת מידע והממונה על הביטחון במערכת הביטחון. גם אין בישראל חובה חוקית לפרסם אובדן מידע עסקי רגיש של חברה,[32] ואין בה גוף האחראי להגנת המגזר המסחרי בסייבר, שמתוקף תפקידו לרכז מידע מסוג זה ולעשות בו שימוש להפקת לקחים ולחיזוק מענה הגנתי כולל. לאור זאת, הסיכוי לאיתור ריגול מסחרי בסייבר בישראל הוא נמוך מאד. זו כנראה הסיבה לדיווחים המעטים הנוגעים לגניבת ידע מסחרי וקניין רוחני מחברות ישראליות.

למרות המגבלות והקושי בהערכת הנזק מתקיפות סייבר, ניתן להניח שארגונים עסקיים ואחרים בישראל חשופים לגניבות מסחריות בהיקפים שאינם נופלים מאלה של מדינות מתקדמות אחרות. זאת, הן בשל הדימוי של ישראל כמובילה בעולם בפיתוח ידע חדשני והן לאור הליקויים בהגנה שהוזכרו לעיל. אם מתבססים על ההנחות השמרניות, לפיהן נזקי הגניבה המסחרית בסייבר מגיעים לאחוז אחד מהתמ"ג הלאומי, הנזק השנתי מגניבות כאלו בישראל מגיע לכ־2.5 מיליארד דולר. עבודת מחקר ראשונית להערכת נזקי הריגול העסקי בישראל, שנעשתה עבור מטה הסייבר הלאומי על ידי חברת המחקר Meidata, אומדת את הנזק השנתי למשק הישראלי מריגול עסקי בין מיליארד לשלושה מיליארד דולר. אין ספק שנזק בסדר גודל כזה, שעולה בהתמדה משנה לשנה, מחייב היערכות לאומית ומצדיק השקעה משמעותית בהתגוננות אצל חברות וגופים נתקפים, המשלמים את המחיר העיקרי של תופעת הריגול העסקי.

תובנות מסכמות

מדינת ישראל, בה קיימת תודעה ביטחונית גבוהה, הייתה מן המדינות החלוצות בהבנת הסיכונים הביטחוניים המתפתחים במרחב הסייבר המתהווה עוד לפני שאותרה פגיעה כלשהי בתשתית קריטית בישראל. יחד עם זאת, הסיכון הטמון בגניבת סודות מסחריים וקניין רוחני של חברות כלכליות ישראליות לא מזוהה גם כיום כאיום משמעותי לחוסנה של המדינה. זאת, גם לאחר הצגת עדויות ברורות לכך שמדינות וארגוני פשע עושים שימוש רב במרחב הסייבר לביצוע ריגול עסקי, שיש לו השפעות כלכליות ניכרות על חברות מסחריות ועל מדינות, תוך שימוש בכלים מתקדמים ביותר.

האיום הכלכלי על חברות מסחריות כתוצאה מריגול עסקי מוגדר על ידי ראש קהילת המודיעין הלאומית האמריקאית כאיום המוחשי הראשון במעלה על ארצות הברית וממוקם לפני איום טרור והפצתו של נשק להשמדה המונית. עלות הנזק הנגרם כתוצאה מריגול עסקי בסייבר היא משמעותית, ונמצאת במגמת עליה, ומשלם אותה, בראש ובראשונה, המגזר העסקי. על פי מחקרים שונים, מרכיב העלות של הריגול המסחרי הוא הדומיננטי ביותר בתוך סך סוגי הפשיעה בסייבר.[33] מדינת ישראל, שכלכלתה מוכוונת ידע חדשני, חשופה גם היא לפשיעה קיברנטית, ובכלל זה לריגול עסקי.

קיים קושי רב לאמוד את הנזק מריגול מסחרי במרחב הסייבר. לכן, ניתן לראות מִנעד רחב של אומדנים בדוחות שונים. הקושי להעריך באופן אמפירי את הנזקים, ומרכזיותן של הערכות מומחים הבאות לתת מענה לפער באיכות הנתונים שנאספים, מהווים אבן נגף בכל השיטות לאומדן הנזקים הנגרמים מריגול מסחרי. זהו המקור לפערים הגדולים בהערכות של נזקים אלה. למרות

הקשיים, הם אינם מייתרים את הצורך בהערכות הנוגעות להבנת המשמעות של תופעת הריגול העסקי; הערכות כאלו הן הבסיס להבנתן של מדינות את התופעה ולהיערכותן אליה.

מוצע לפעול לפיתוח מתודולוגיה יציבה, שתוכל לספק כלים להערכה אמינה של הנזקים שבהם עסק מאמר זה. כך תגדל המודעות לשיפור ההגנה מול האיום ומול הנזקים שהוא גורם. כדי לקדם את הנושא, יש לשפר בראש ובראשונה את היכולת לאסוף מידע אמין על התופעה באמצעות מנגנונים לדיווח על אירועי סייבר. לצידם יש לפתח כלי הערכה משופרים שיתנו מענה לפערי המידע הקיימים בין הדיווחים וההערכות של הסקרים לגבי מספר האירועים והערכת הנזק שהם גורמים מצד אחד ובין התמונה בפועל מצד שני. זהו פער מובנה, בשל העובדה שבמרבית המקרים, המותקפים כלל אינם מודעים לכך שהותקפו וכי מידע עסקי שלהם נגנב, ולפיכך אינם מסוגלים, גם בדיעבד, לקשר בין נזק עסקי לבין גניבת מידע עסקי מהארגון, שכאמור, הם אינם יודעים דבר עליה. בנוסף לכך, שיפור המענה האזרחי הכולל במרחב הסייבר בישראל, תוך קביעת גורם אחראי בעל סמכות מתאימה, יוכל לאפשר פיתוח של תפיסת התמודדות מקיפה עם הגניבות המסחריות במרחב הסייבר, מתוך ראייה לאומית רחבה.

כאמור, מטרת מאמר זה היא להאיר את תופעת הריגול העסקי המתבצע בתווך הקיברנטי ואת הנזקים שנגרמים למשק הישראלי בעטיה. בהיעדר מחקרי עומק על התופעה, קשה להצביע על היקפה המדויק, אולם ניתן להעריך שהוא משמעותי לכלכלה הישראלית ומצוי במגמת עליה ניכרת. המענה לתופעה זו צריך להכיל מגוון פעילויות, וביניהן: מחקרים ממוקדים על היקפה ופילוחה בסקטורים שונים; שיפור האבטחה במגזר העסקי; פיתוח תעשיית ביטחון הסייבר; מהלכים מדינתיים שיוכלו לתת מענה לריגול העסקי המדינתי המתבצע במרחב הסייבר, לרבות שיתופי פעולה והסְדרות מול מדינות עמיתות הסובלות גם הן מהתופעה.

המענה לתופעת הריגול העסקי במרחב הסייבר הוא מורכב ועתיר משאבים. נדמה שהגדלת המודעות אליה, הן בקרב הגורמים העסקיים והן בקרב מקבלי ההחלטות בישראל, היא תנאי הכרחי לתחילת פעילות לצמצום נזקי הפשיעה הקיברנטית בכלל ונזקי הריגול המסחרי בפרט. זאת, כדי להביא את יכולת ההגנה הישראלית בסייבר למיצוי נכון אל מול כלל האיומים.

הערות

1 Nicole Perlroth, "Study May Offer Insight into Coca-Cola Breach", *The New York Times*, November 30, 2012, http://bits.blogs.nytimes.com/2012/11/30/study-may-offer-insight-into-coca-cola-breach/?_r=0 .

2 גנרל אלכסנדר הוא מפקד פיקוד הסייבר האמריקאי ועומד בראש הסוכנות לביטחון לאומי (NSA) בארצות הברית. ראו:

Carrie Lukas, "It's Time for the U.S. to Deal with Cyber-Espionage – Adversaries draining intellectual property from American companies must come to an end", *US News*, June 4, 2013, http://www.usnews.com/opinion/articles/2013/06/04/chinas-industrial-cyberespionage-harms-the-us-economy.

3 למשל, הפעלת מערכות שליטה ובקרה, השולטות על בַּקָרים ממוחשבים לתהליכים תעשייתיים, באופן שונה מהתהליך הסדור, כך שייגרמו נזק לתהליך התעשייתי או הרס של המערכות התעשייתיות עצמן.

4 Francois Paget, "2014 Threats Predictions: Cybercrime and Hacktivism Will Continue to Grow", McAfee Labs, January 8, 2014, http://blogs.mcafee.com/mcafee-labs/2014-threats-predictions-cybercrime-and-hacktivism-will-continue-to-grow.

5 הדוגמה הבולטת למעקב המבוצע כולו במרחב הסייבר העולמי היא מערכת המעקב העולמית PRISM של ה־NSA, שנחשפה מתוך הדלפותיו של אדוארד סנודן. המעקבים במרחב הסייבר שביצע ה־NSA נעשו לכאורה לצורך שמירה על ביטחונם של אזרחים אמריקאים. אולם, ישנם דיווחים שמעקבים כאלה בוצעו גם אחר תעשיות שעניינו את ארצות הברית, בעיקר בתחום היכולות הביטחוניות המתקדמות. ראו:
Glenn Greenwald and Ewen MacAskill, "NSA Prism Program Taps in to User Data of Apple, Google and Others", *The Guardian*, June 7, 2013. http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data;
Scott Shane, "No Morsel Too Minuscule for All-Consuming N.S.A.", *The New York Times*, November 2, 2013, http://www.nytimes.com/2013/11/03/world/no-morsel-too-minuscule-for-all-consuming-nsa.html?pagewanted=1&_r=0.

6 Mandiant Report, "APT1 Exposing One of China's Cyber Espionage Units", February 2013. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

7 ראו כדוגמה את תקיפת הסייבר המוצלחת ב־2011 על חברת "לוקהיד מרטין" לצורך גניבת תוכניות מטוס החמקן המתקדם F–35.

8 Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace, Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011, Annex B – West and East Accuse China and Russia of Economic Espionage*, October 2011, http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

9 **שם,** עמ' 4.

10 *Foreign and Economic Espionage Penalty Enhancement Act of 2012*, House of Representatives Report 112-610, 2012, http://www.fas.org/irp/congress/2012_rpt/ecoesp.pdf.

11 קלפר הוא ראש קהילת המודיעין הלאומית האמריקאית (DNI – Director of National Intelligence).

12 James R. Clapper, Director of National Intelligence, "Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence", January 31, 2012, p. 8, http://www.intelligence.senate.gov/120131/clapper.pdf.

13 James R. Clapper, Director of National Intelligence, "Statement for the Record on the Worldwide Threat Assessment of the Us Intelligence Community, Senate Select Committee on Intelligence", March 12, 2013, http://www.intelligence.senate.gov/130312/clapper.pdf.

14 Devlin Barrett, "U.S. Outgunned in Hacker War", *Wall Street Journal*, March 28, 2012, http://online.wsj.com/article/SB10001424052702304177104577307773326180032.html.

15 ברוב המקרים, כלי האבטחה הם כלים מסחריים סטנדרטיים.

16 ראו דוח מפורט בהקשר זה ב:
Mandiant Report, "APT1 Exposing One of China's Cyber Espionage Units".

17 IBTimes Staff Reporter, "America's Top Cyberwarrior Says Cyberattacks Cost $250 Billion A Year", July 13, 2012, http://www.ibtimes.com/americas-top-cyberwarrior-says-cyberattacks-cost-250-billion-year-722559.

18 Mandiant Report, "APT1 Exposing One of China's Cyber Espionage Units".

19 החברה מזכירה בדוח כי היא חקרה עשרות מערכי תקיפה מתקדמים, יותר מעשרים מתוכם מערכים בעלי מאפיינים דומים, שמקורם בסין. החברה בחרה, מסיבות משלה, לפרסם בדוח התייחסות למערך אחד בלבד.

20 R. Anderson, C. Barton, R. Böhme, R. Clayton, M. van Eeten, M. Levi, T. Moore and S. Savage, "Measuring the Cost of Cybercrime", in: *Workshop on the Economics of Information Security*, WEIS, 2012. http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

21 Detica, *The Cost of Cyber Crime*, A Detica Report in partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office, UK, 2011, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60942/THE-COST-OF-CYBER-CRIME-SUMMARY-FINAL.pdf.

22 IBTimes Staff Reporter, "America's Top Cyberwarrior Says Cyberattacks Cost $250 Billion A Year".

23 Emil Protalinski, "NSA: Cybercrime is the Greatest Transfer of Wealth in History", *ZDnet*, July 10, 2012. http://www.zdnet.com/nsa-cybercrime-is-the-greatest-transfer-of-wealth-in-history-7000000598/.

24 The IP Commission Report, *The Report of the Commission on the Theft of American Intellectual Property*, http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.

25 Office of the Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace*.

26 McAfee, *The Economic Impact of Cybercrime and Cyber Espionage*, Center for Strategic and International Studies, July 2013, http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf.

27 **שם**, עמ' 14.

28 **שם**, עמ' 15.

29 Mandiant Report, "APT1 Exposing One of China's Cyber Espionage Units".

30 הרשות הלאומית לאבטחת מידע – רא"ם – כפופה לשב"כ. היא הוקמה מכוח החלטת ממשלה מדצמבר 2002.

31 האחריות הכוללת לתחום ההגנה הלאומית על המשק האמריקאי מוטלת על המשרד להגנת המולדת, הפועל בשיתוף פעולה הדוק עם משרד ההגנה (המכיל גופי מודיעין, דוגמת "הסוכנות לביטחון לאומי" ו"הסוכנות הלאומית למניעת ריגול", שפעילים מאוד בתחום ההגנה מפני מתקפות בסייבר וריגול מסחרי), "לשכת החקירות הפדרלית" (FBI)

ומשרד המשפטים.

32 כשמדובר באירוע פריצה בסייבר לחברה ציבורית בישראל, שעלול להשפיע על פעילותה או על נכסיה, יתכן שתהיה חובה לדווח עליו לבורסה, משום שעלולה להיות לו השפעה על שיקול הדעת של משקיע סביר ביחס לקניה או מכירה של מניית החברה.

33 Detica, *The Cost of Cyber Crime*, p. 3.

ניתוח רב ממדי של שיתוף מידע סייבר ארגוני

אבירם זרחיה

התפתחות איום הסייבר מחייבת ארגונים לשנות דפוסי חשיבה ומערכי הגנה בהיבטים רבים. אחד מהם נוגע למדיניות הארגון באשר לשיתוף מידע סייבר עם גורמים חיצוניים ומעבָר מתפיסה של ארגון ממודר לתפיסה של ארגון משתף. השיתוף יוצר בעיה מורכבת ומרובת פנים בתחומי הטכנולוגיה, המשפט, התרבות הארגונית ואף הפוליטיקה. הקמת מערך שיתוף משרתת גורמים רבים, ובהם גופי הרגולציה, הממשל, רשויות החוק והביון, יצרני הפתרונות והשירותים ואף הארגונים עצמם, אך גם מעוררת התנגדות מצד גורמים פנים ארגוניים וארגוני ההגנה על הפרטיות.
מטרת המאמר היא להציג את נושא שיתוף המידע בסייבר על היבטיו ואתגריו השונים, לחשוף את הקורא לעולם המושגים המקיף אותו ולהציג תובנות ותחזיות באשר להתפתחות המגמה בעתיד.

מילות מפתח: סייבר, שיתוף מידע, פרטיות, רגולציה, אבטחת מידע, אמון.

מבוא

אחד האתגרים המשמעותיים של ארגונים בעידן הנוכחי הוא ההתמודדות עם איום הסייבר. השימוש המוגבר בטכנולוגיה במגוון ארגונים – ממשלתיים, ציבוריים ופרטיים – הופך אותם למטרה להתקפות המכוונות לאסוף מידע, לפגוע במידע או להשבית שירותים. התקפות על ארגונים מסחריים עלולות לפגוע במוניטין הארגון, לסכן את נכסיו הרוחניים והפיזיים ולגרום לעלויות כספיות כבדות. התקפות על גופים ותשתיות ממשלתיים וציבוריים עלולות, בנוסף, לפגוע בשגרת החיים של מדינה ואף בבריאות תושביה וביטחונם.

אבירם זרחיה הוא מומחה טכנולוגי להגנה בסייבר בחברת ג'וניפר נטוורקס, מרצה בתחום הסייבר ומתמחה בתוכנית לביטחון סייבר במכון למחקרי ביטחון לאומי.

מאמר זה ראה אור לראשונה ב**צבא ואסטרטגיה**, כרך 6, גיליון 3, דצמבר 2014, עמ' 55–70.

במהלך העשור האחרון זלג עולם הפשיעה המסורתי למרחב הסייבר. השכלול בכלי הפריצה ודרכי התקיפה הוביל להיווצרות כלכלת פשיעה חדשה, מפותחת ומשוכללת, בסייבר. תהליך דומה עבר על מרחב הלוחמה בין מדינות, ורבים רואים בסייבר את ממד הלחימה החמישי של שדה הקרב המודרני, בנוסף ליבשה, אוויר, ים וחלל.

ההתמודדות עם איום הסייבר מחייבת השקעה בתשתיות אנושיות וטכנולוגיות בהתאם למדיניות ניהול הסיכונים הארגונית או הלאומית. איכות של מערך אבטחת מידע ארגוני מושפעת מגורמים שונים, שאחד המרכזיים בהם הוא יכולת איסוף וניתוח מידע הן על תעבורת משתמשים לגיטימית והן על התקפות, בין אם הצליחו ובין אם נכשלו. באמצעות יכולת זו ניתן לאתר מראש פרצות במערך האבטחה ולחסום אותן, וכן לזהות התקפות ולהגיב עליהן באופן יעיל ומהיר, ובכך לחסוך מהארגון התמודדות עם תוצאותיהן, או לפחות להקטין את השפעתן.

שיתוף מידע סייבר ארגוני הוא תקשורת של מידע הנוגע לאבטחת הארגון אל ישות חיצונית, במטרה להשיג תועלות הן לארגון המשתף והן לארגון המקבל. שיתוף כזה יוצר בעיה מורכבת ומרובת פנים ומהווה שינוי פרדיגמה בעולם טכנולוגיות המידע (IT). מודל השיתוף יכול להתקיים בתוך אותו מגזר שוק, בין חברות ממגזרים שונים, ואף בין ארגונים ובין גופי ממשל ובין ממשלות שונות. בשנתיים האחרונות נראה כי מתחזקת מגמת השיתוף וכי גופי רגולציה ואכיפת חוק, מקומיים ובין־לאומיים, מקדמים מגמה זו באמצעות הנחייה, עידוד או חקיקה. במקביל מתפתחת תעשייה של פתרונות אבטחה, המבוססת על שיתוף מידע בין גופים.

מטרת המאמר היא להציג את אתגר השיתוף על היבטיו השונים ולחשוף את הקורא לעולם המושגים המקיף את הנושא. המאמר מתבסס על מגוון מקורות אקדמיים, מחקריים, ממשלתיים, טכנולוגיים ועיתונאיים. הוא מציג תחילה את המצב הנוכחי והבעייתיות הנובעת ממנו, ממשיך בניתוח היבטים מעשיים של שיתוף ואופני מימושם, כולל נגיעה ברקע התאורטי של נושא האמון בין גופים, מפרט את התועלות והאתגרים לארגון, מתאר את מרחב ההזדמנויות העסקי, סוקר היבטי חוק, רגולציה ופרטיות, ומציע לסיכום מספר תובנות. רוב הדוגמאות במאמר לקוחות מארצות הברית, שבה מיזמי השיתוף, מאמצי התקינה, פעולות הממשל וסוכנויות הביון ותהליכי החקיקה חשופים ונמצאים במרכז הדיון הציבורי. תהליכים דומים עוברים על מדינות אחרות ובהן ישראל, גם אם אלה אינם חשופים במלואם לעיני הציבור.

ממידור לשיתוף

איום הסייבר מתקיים כממד פשיעה ולחימה משוכלל ומורכב, שהתפתח בשנים האחרונות בשני אפיקים מקבילים: **מרחב האיום** ו**חומרת האיום**. בהיבט **מרחב האיום**, ארגונים נדרשים להגן כיום לא רק על מערכות המחשוב והמידע הפנים ארגוניות, אלא גם על אמצעי הקצה המגוונים שברשות המשתמשים, כגון טלפונים חכמים ומחשבים ניידים, וכן על מערכות תשתית, כגון חשמל ומיזוג אוויר. כל זאת, באופן רציף, בדרך שתאפשר לספק שירותים מכל מקום ובכל זמן, כפי שמצופה מארגון בעידן הנוכחי.

בהיבט **חומרת האיום**, ההתקפות הופכות לקשות יותר לאיתור וכוללות גם אופני תקיפה שאינם מתועדים או ידועים ליצרניות פתרונות האבטחה. כאלה הם, למשל, "מתקפות יום אפס" (Zero Day Attacks)[1] והאקרים המשתפים ביניהם מידע באופן שוטף ובזמן אמת ויוצרים מצב בו כל נקודת תורפה שמתגלה במערכות, או נוזקה (Malware), ניתנות לשכפול ולמימוש כמתקפה בצדו האחר של העולם באופן כמעט מיידי. מחקר של מכון RAND שנערך לאחרונה בנושא זה,[2] מספק ניתוח של האופן בו "השווקים השחורים" של עולם הסייבר בנויים ומתפקדים כמערכת משולבת (Eco-System) בעלת תשתית ומבנה ברורים.

התפתחויות אלו יצרו קושי לארגונים להילחם לבדם את מלחמת הסייבר, וכתוצאה מכך הֵחל תהליך של שינוי בתפיסת ההגנה שלהם. ברוב הארגונים, למעט אלה הכפופים לרגולציה ומערכות צבאיות־ממשלתיות, תפיסת ניהול אבטחת המידע התאפיינה בנתק מוחלט מארגונים אחרים, הן בהיבט הטכנולוגי של מערכות המידע ואבטחת המידע והן בהיבט של שיתוף מידע על אירועי סייבר ואבטחה. המידע על התקפה או ניסיון התקפה, וכן תוצאות הניתוח שלו, נשמרו בתוך הארגון, סווגו והופצו לתפוצת נמענים פנים ארגונית מוגבלת בלבד. גילוי המידע לצד שלישי נתפס כסיכון לארגון, העלול להוביל לפגיעה במוניטין, לחשיפה משפטית ועוד.

לאחרונה אנו עדים לשינוי התפיסה, כאשר ארגונים ורשויות רבים שוקלים לנטוש את אסטרטגיית הארגון הממודר[3] לטובת מודל של שיתוף מידע עם גופים אחרים (Information Sharing). שיתוף מידע סייבר בין גופים, בדומה לזה המתקיים בין האקרים בצד ההתקפי, יצור מצב בו, למשל, מעטפת הגנה שנוצרה בארגון מסוים כדי להתמודד עם איום שהתגלה, תופץ כחיסון לארגונים אחרים, או לפחות כמידע שיעלה את רף הערנות והמודעות שלהם לאיום הספציפי.

העלויות הגבוהות המושתות על הארגון כדי שיוכל לעמוד ברף הנדרש להספקת מעטפת הגנה יעילה במשאבי זמן, אנשים וטכנולוגיה, יוצרות אינטרס ארגוני לשיתוף מידע והעברת חלק מהעלויות הללו לצד שלישי. מחקר שנערך בארצות הברית בנושא זה,[4] מנתח את הקשר בין שיתוף מידע סייבר ובין עלויות

האבטחה הארגוניות. ממצאי המחקר מראים כי חברות ששיתפו מידע נדרשו להשקעה כספית קטנה יותר במערך האבטחה, כדי להגיע לרמת הגנה זהה לזו של חברות שלא שיתפו מידע. מכאן שניתן להגיע לחיסכון כספי ישיר לארגון, בין היתר כתוצאה מהשיתוף. המדובר, לדוגמה, באיסוף ובהזנת מודיעין פרואקטיבי על חולשות והתקפות צפויות, בחיסון מפני התקפה שהתרחשה בארגון אחר, בשימוש באנשי מקצוע שיעזרו בניתוח אירועי אבטחה, ועוד.

סיבה נוספת לשינוי התפיסה הארגונית ביחס לשיתוף מידע הן התועלות העסקיות הישירות והעקיפות הנובעות מעמידה בסטנדרטים ורגולציות. במגזרים חיוניים מסוימים, כמו פיננסים, בריאות, אנרגיה ותקשורת, נדרשים ארגונים, כולל פרטיים, לאפשר למדינה פיקוח טוב יותר על התנהלותם, וזאת במספר היבטים. ברוב הרגולציות נכללת, בין היתר, דרישה לשיתוף מידע בין הארגון ובין רשות מפקחת כלשהי בכל הנוגע לאירועי סייבר או ניסיונות תקיפה. בצד החובות, ישנן גם תועלות ישירות ועקיפות לארגון מהרגולציה: ארגון פיננסי הפועל תחת רגולציית באזל III[5] – תקינה המתייחסת לגופים פיננסיים ומחייבת, בין היתר, שקיפות של סיכונים תפעוליים ובהם גם אירועי אבטחה מול הרגולטור – מחויב בהקצאת הון בהתאם לרמת הסיכונים שלו[6], ויכול לשפר רווחיות על ידי הקטנתם. דוגמה לתועלת עקיפה ניתן למצוא בארגון המספק שירותים, שמתאפשר לו להתמודד במכרז ממשלתי המחייב עמידה בתקינת ISO-27032,[7] הכולל אף הוא מתווה לשיתוף מידע.

עקרונות טכנולוגיים בשיתוף מידע

שיתוף מידע בין ארגונים באופן מאובטח הוא אתגר טכנולוגי ותפעולי בהיבטים רבים, החל מרמת הגדרת המטרות והמדיניות וכלה ברמת המימוש והשימוש. מתודות לפתרון האתגר צריכות לכלול איזון בין המרכיבים הבאים: היכולת לתמוך במספר גדול של ארגונים ולהוסיף אותם בקלות למיזם השיתוף (Scalability); היכולת לעשות שימוש במידע לאחר בדיקת מִתאם (קורלציה) וניתוחו קרוב לזמן אמת במטרה להפיק תועלת מרבית ממנו (Usability); מערך בקרות המבטיחות את קיום שלושת העקרונות הבאים: סודיות, שלמות וזמינות (Confidentiality, Integrity, Availability – CIA).[8] השלבים בבניית מערך לשיתוף מידע כוללים, בין היתר, הגדרת המטרות והמשתתפים, זכויות וחובות הארגונים החברים במיזם, ארכיטקטורה טכנולוגית, מודל אמון ובקרות ותהליכי עבודה.

שיתוף המידע בין ישויות שונות מחייב יצירת מערכת אמון ביניהן, כדי שניתן יהיה להבטיח כי המידע נכון ושלם וכי ניתן להפיק ממנו תועלת. זהו הבסיס האקדמי והתיאורטי לכל המודלים השימושיים והדוגמאות הנדונים במאמר. מרחב הדיון והפתרונות בנושא האמון משתרע בין רמת הרכיבים בתוך מוצר כמו

מחשב, דרך שילוב מוצרים שונים בתוך אותה מערכת, ועד לאמון בין מערכות שונות בארגונים שונים, כמו למשל מסחר באינטרנט. גופי תקינה, כגון Trusted Computing Group (TCG),[9] עוסקים במגוון היבטים של הנושא, אך שיתוף מידע סייבר הוא אתגר שהמודלים הקיימים לא סיפקו לו מענה שלם, ומכאן גם הצורך בחשיבה ותקינה נפרדות לנושא זה.

ניתן לזהות שלוש ארכיטקטורות עקרוניות לבניית תשתית שיתוף המידע,[10] שיש לבחור באחת מהן בשלב ייזום השיתוף. הארכיטקטורה הראשונה היא תפיסה של מרכז וקצוות (Hub and Spoke), המבוססת על אתר מרכזי המקבל את המידע מארגוני הקצה ומפיץ אותו לאחר היתוכו כשהוא מותאם לצרכנים השונים.[11] המרכז משמש כמסלקה המגֵנה על הפרטיות ועל הקניין הרוחני של כל ארגון, והיכולת לנתח בו כמות גדולה של מידע בצורה יעילה, מתאפשרת בין היתר בזכות ההתפתחות הטכנולוגית המואצת בתחום ה־Big Data. זו מאפשרת עיבוד וניתוח כמויות מידע גדולות ומהווה אבן יסוד בבניית יכולת להיתוך מידע ממקורות שונים. חסרונות המודל הם בעיקרם תוצר של התפיסה הריכוזית שלו: אתגרי גודל, תלות באתר המרכזי למבצעיות המערך, שיהוי בעיבוד המידע והפצתו ועוד.

הארכיטקטורה השנייה היא של פרסום לכל (Post to All), בה מתבצעת הפצה ישירה בין הארגונים. ארכיטקטורה זו מחייבת בהכרח תשתית ניתוח בארגונים, מכיוון שההפצה היא של מידע גולמי ולא של מידע לאחר היתוך. הארכיטקטורה השלישית משלבת בין שתי הקודמות, תוך ניצול היתרונות היחסיים בכל אחת מהן, אך במחיר מימוש מסובך ויקר יחסית.

מימוש השיתוף צריך להתבצע מבחינה טכנולוגית תוך שמירה על נכסי הארגון ופרטיותו, וזאת בשתי רמות: הראשונה היא שליטה על תוכן המידע המועבר (Information Control), המתבצעת בארגון עצמו כחלק מהגדרות האובייקטים אותם משתפים, וצריכה להיות מתוקננת בתסדיר (פורמט) מוסכם. חלק מהגדרות אלו נועדו להלבין את מקורות המידע כפי שקורה בעולם המודיעין, כך שלא ייחשפו פרטים שאינם הכרחיים אל מחוץ לארגון. הרמה השנייה היא הגבלת גישה למידע, הכוללת שליטה על מערך ההפצה שלו, לאן הוא מועבר ומי רואה אותו, וצריכה להתבסס על פרוטוקול שיתוף מתוקנן.

בחירה עקרונית נוספת שיש לבצע היא בין מודל שיתוף אוטומטי למודל שיתוף ידני. משמעות השיתוף הידני היא שגורם מורשה בארגון, בעל נגישות למערכת השיתופית, יזין ויקבל מידע אליה וממנה וישלוט בגישה למידע. למודל הידני חיסרון בולט – הגורם האנושי, המהווה חסם וצוואר בקבוק, בעיקר כאשר הארגון נמצא תחת מתקפה. חסרונות נוספים הם הקושי לשמור על עדכניות המידע לאורך זמן וחשיפתו לטעויות אנוש.

שיתוף אוטומטי מחייב להחליט תחילה על תסדיר אחיד ומנורמל של מידע, על מערכת חיישנים בארגון שתאסוף ותחלק אותו, על מערכת קבלת התרעות מקומית, ועל מימוש בקרות קפדני שנועד למנוע זליגת מידע שלא היה צריך להישלח. דרך זו מאפשרת להתגבר על המגבלות הקיימות בשיתוף הידני. יחד עם זאת, היא מחייבת התמודדות עם תרחישי התקפה אליהם חשוף מערך השיתוף האוטומטי, כמו הרעלת בסיס הנתונים השיתופי במידע כוזב (Database Poisoning).[12]

קיימות מספר פעילויות תקינה בסוגיה זו, אשר המתקדמת שבהן, שגם אומצה על ידי משרד ההגנה של ארצות הברית, כוללת תסדיר שיתוף מידע סייבר בשם Structured Threat Information eXpression (STIX™).[13] תסדיר זה מגדיר מבנה רשומה, ובה מידע הנוגע למשתמש ו/או תעבורה הנשלחת באופן יזום מהארגון אל ישות חיצונית או מישות חיצונית אל הארגון, כשהיא מכילה מגוון פרטים מובנים על אירוע אבטחה. תקינה נוספת הרלוונטית למיכון השיתוף קרויה Trusted Automated eXchange of Indicator Information (TAXII™),[14] והיא כוללת מבנה מסרים ופרוטוקולי רשת התומכים בהעברת מסרים מסוג STIX בין הישויות השונות. ישנם מספר פרוטוקולים משיקים נוספים, תחת ארכיטקטורת מעטפת הקרויה Cyber Observable Expression (CyBOX),[15] הנתמכים על ידי משרד ההגנה האמריקאי כחלק מהמאמץ למיכון השיתוף.

נראה כי מרבית המודלים התיאורטיים המוצעים באקדמיה,[16] או המודלים השימושיים המוצעים על ידי מכוני מחקר שונים,[17] מבוססים על מימוש אוטומטי, אֵמון וארכיטקטורת שיתוף של מרכז וקצוות. מאמצי התקינה שהוזכרו לעיל תואמים את רוח המודלים האקדמיים והשימושיים, כך שנראה כי יש קונצנזוס מבחינה טכנולוגית סביב הדרך הנכונה לבניית מערך כזה. ואכן, גופים משמעותיים כמו משרד ההגנה האמריקאי פועלים לקידום המיזמים על פי מתווה זה.[18] יחד עם זאת, הדרך למימוש שיתופי מידע אפקטיביים עדיין ארוכה, עקב ריבוי האתגרים הטכנולוגיים, העסקיים, התפעוליים, המשפטיים, ויש שיאמרו אף המוסריים, העומדים בפני מיזם השיתוף.

תועלות וסיכונים בשיתוף מידע

כדאיות השיתוף משתנה בהתאם למפת האינטרסים של הגופים המעורבים השונים. במקרה של ארגונים עסקיים, השיתוף מאפשר הגדלת רמת האבטחה וקיצור זמן התגובה להתקפה או לחיסון מפני התקפה עתידית אפשרית. זאת, באמצעות קבלת התראה מראש מהישות המרכזית ועזרה בזיהוי, ניתוח והתמודדות עם מתקפות. ניסוי שערך צוות חוקרים מדרום קוריאה מצא סימוכין להערכה זו.[19] השיתוף גם מאפשר את הקטנת הוצאות האבטחה של הארגון, וזאת

כתוצאה ממיקור חוץ, חלקי לפחות, של הניתוח והתגובה לצד שלישי. כמו כן, הארגון עשוי ליהנות מהקלות של הרגולטור כתוצאה מהגדלת השקיפות ועמידה בחובת הדיווח ובתנאים נוספים.

במקרה של מגזר יצרני הפתרונות והשירותים, מדובר בפלח שוק חדש, מוטה טכנולוגיה ובעל פוטנציאל גידול, היכול לבדל את עצמו באמצעות יצירת יתרונות תחרותיים בני קיימא. אחד השירותים העיקריים שמגזר זה יכול להציע הוא זיהוי דפוסי תקיפה אפשריים והפצת חיסונים והתראות לארגונים, וזאת על בסיס היתוך מידע של התקפות ומתקיפים שנאסף מהארגונים עצמם.

במרחב המדינתי, כדאי לגופי הרגולציה, הממשל והביון לעודד את מגמת השיתוף, מכיוון שבכך הם מגדילים את השקיפות של הארגונים, מקבלים תמונת מצב רחבה על זמינות השירותים ואמינות המידע, מבצעים אנליזות על פני רשתות וארגונים שונים לזיהוי דפוסי תקיפה שהתממשו או עלולים להתממש, ומאפשרים יכולת תגובה מהירה, תוך הפצת מידע לארגונים אחרים במטרה לחסן אותם. ניתן להניח כי לגוף הגנה מדינתי שזהו תחום עיסוקו יש יכולת גבוהה יותר מאשר לגופים פרטיים, לבנות כשירות טכנולוגית גבוהה של אנשיו ולשמור עליה, וכן את הרצון לשתף ארגונים אחרים במשאבים האנושיים והטכנולוגיים שברשותו. השיתוף הוא אינטרס לאומי מובהק, המאפשר לממשל להילחם את מלחמת הסייבר הלאומית ולהכות בפשיעה הקיברנטית באופן יעיל יותר, וכן ליצור שליטה בזמינותן של תשתיות לאומיות, ציבוריות ופרטיות קריטיות. דוגמה למימוש רגולציה בעלת תפיסה דומה, אך בתחום אחר, ניתן למצוא בהנחיות המשרד להגנת הסביבה בישראל בעניין פליטת מזהמים מתעשייה, המחייבות מפעלים בניטור ובדיווח רציפים ומקוונים של נתוני איכות האוויר בארובות ובמקורות מזהמים אחרים.[20]

על אף היתרונות שפורטו לעיל, ישנם מספר סיכונים הקשורים ישירות לשיתוף מידע סייבר בין ארגונים. ניתוח הסיכונים הללו צריך להתבצע במסגרת אסטרטגיית ניהול הסיכונים הארגונית, ולכלול את הסבירות של כל סיכון, את ההשפעה שלו, את הבקרות הנדרשות לשליטה בו ואת הדרכים לצמצם אותו. לדוגמה, הדרך להפחתת הסיכון לחשיפה משפטית לתביעות בגין גילוי מידע פרטי או עסקי, היא באמצעות חוקים ותקנות המעניקים הגנה משפטית של הממשל או הרגולטור. דוגמה נוספת היא הסיכון לאובדן נכסי מידע ארגוניים כתוצאה משיתוף לא מבוקר. הדרך להקטין סיכון זה היא באמצעות שימוש בתבנית שיתוף מובנית ומתוקננת שאינה כוללת מידע רגיש, וכן בבלמים נוספים, כמו הנחייה, רגולציה או חקיקה, שיחייבו את הארגון להסיר מידע פרטי או עסקי מהמידע שנועד לשיתוף לפני שליחתו.

הזדמנויות עסקיות

התפתחות איום הסייבר ושינוי תפיסת השיתוף של ארגונים מהווים הזדמנות עסקית ליצרני פתרונות טכנולוגיים, לגופי אינטגרציה ולספקי שירותים, שיכולים למנף את בסיס המוצרים, הידע והשירותים שלהם כדי ליצור ערכים מוספים סביב אתגר השיתוף.

אחת הדוגמאות להזדמנות כזאת נוגעת לאתגרים שמעמידות טכנולוגיות התקפה חדשניות, כמו התקפה מתוחכמת ועקבית (Advanced Persistent Threat – APT),[21] או ניצול פרצות אבטחה שאינן ידועות או שלא סופק להן עדיין פתרון. שתי הטכנולוגיות ההתקפיות הללו מורידות מיעילותם של מנגנוני ההגנה המסורתיים,[22] אך ניתן לפצות על כך, במידה מסוימת, באמצעות שירות אבטחה שיתופי בין־ארגוני. שיתוף כזה מאפשר זיהוי אנומליה בענן והשוואה של אירועים ארגוניים לא רק אל מול בסיס ההתנהגות באותו ארגון, אלא גם אל מול ארגונים דומים אחרים, ובכך הוא מחדד את מנגנון הזיהוי ומקטין את הסיכון שתעבורה תקינה תזוהה בטעות כחריגה. בנוסף לכך, לאחר זיהוי התקפה או תוקף בארגון מסוים, ניתן להפיץ את מרכיבי הזיהוי או את החיסון ליתר הארגונים, ובכך למנוע התקפה דומה אצלם.

מספר יצרני מערכות אבטחה מספקים פתרון לשיתוף מידע סייבר המבוסס על תשתית איסוף מידע מבוזרת, וזאת באמצעות מערך מבחנים (Probes) המשמשים לעיתים גם כ"מלכודות דבש" למתקיפים. אלה מותקנים בארגונים ואצל לקוחות קצה או בצמתים מרכזיים באינטרנט השייכים ליצרן. תשתית זו אוספת מידע בזמן אמת על התקפות ותוקפים, בחתכים של מיקום גיאוגרפי וסוג ההתקפה, ומפיצה אותו כשירות לארגונים החברים בשיתוף. המערכת מהווה בסיס נתונים מבוסס שיתוף בענן על תוקפים ו/או התקפות, ולעיתים אף כוללת רכיב של סינון וחסימה המתבסס על המידע המתעדכן באופן דינמי.

במקרה של ספקיות שירותי תקשורת ואחסון על גבי תשתית ענן, השיתוף מהווה הזדמנות להקטין את שיעור העזיבה של לקוחותיהן, וזאת באמצעות מתן עוד רובד אבטחה כערך מוסף.[23] הפתרון באמצעות ענן המשותף לכל הארגונים המתארחים מאפשר לספק השירותים, לאחר שזיהה התקפה בארגון אחד ועצר אותה, לטייב את מדיניות האבטחה עבור יתר הארגונים במטרה למנוע את הישנותה.

הזדמנות עסקית נוספת הקשורה ישירות למיזמי שיתוף היא בניית פתרון לאיסוף, ניתוח והפצה של מידע סייבר ברמה לאומית או מגזרית. למספר חברות אינטגרציה בעולם יש פתרון כולל ליצירת תמונת מצב, ניתוח אירועים, הפצת חיסונים, סימולטור אימונים ורכיבים נוספים, כמקובל במערכות צבאיות וציבוריות גדולות. כמו כן, יש יצרניות של פתרונות בצורת האזנה וניתוח מעמיק של התעבורה

(Deep Packet Inspection), המאפשרים לספקיות שירותי התקשורת לשתף מידע באופן סלקטיבי עם רשויות החוק, כדי שאלו יוכלו להאזין לרשתות הטלפוניה והאינטרנט ולדלות מתוכן איומים. חלק מהחברות הללו אף מספקות את רכיב הפתרון שאחראי לניתוח המידע, המבוסס על לוגיקה חכמה וכולל אנליזה לכמות עצומה של מידע הנאסף ממקומות שונים, חקר אנומליות וקורלציות בין אירועים.

ניתן להניח כי גל החדשנות הטכנולוגית בעולם של פתרונות ההגנה יימשך, מתוך צורך להתאים את מערכי ההגנה לאיומי הסייבר הקיימים והמתהווים. בנוסף ניתן להניח כי רעיון השיתוף, התופס מקום גדל והולך במדיניות ההגנה של ארגוני מפתח, ימשיך להוות הזדמנות עסקית לגורמים המסחריים הפועלים בתחום זה.

היבטי רגולציה ופרטיות

ישנם תחומים בהם הרגולטור ו/או החוק מחייבים כבר היום שיתוף מידע הנוגע לסיכוני סייבר ולאירועי סייבר, ונראה כי מגמה זאת הולכת ומתעצמת. זאת, נוכח הצורך של ממשלות להקים מערך הגנה לאומי ללחימה בפשיעה הקיברנטית, וכן ליצור שקיפות של אירועי סייבר בחברות ציבוריות או במגזרי שוק אסטרטגיים, כגון תקשורת, פיננסים ובריאות. כמו כן, רגולציות שונות, כגון בזל III ו־ISO-27032, מעודדות את שיתוף המידע בין הארגונים לרשויות, הן באמצעות הנחייה והן באמצעות הצעת תועלות והקלות כלכליות לארגונים המשתפים פעולה בנושא זה. מאמר המנתח את שקלול התמורות בין השקעות באבטחת מידע בגופים פיננסיים ובין שיתוף מידע סייבר,[24] מגיע למסקנה כי כדאיות השיתוף בין ארגונים גוברת ככל שיש תלות הדדית ביניהם, וכי ככל שהשיתוף בין גופים אלה גדל, כך קטנה ההשקעה שהם צריכים להשקיע באבטחת מידע. בשווקים מגזריים רבים (פיננסים וטלקומוניקציה למשל), הקישור בין הארגונים חיוני לתפקודם השוטף, ופגיעה בארגון אחד עלולה לפגוע בקלות גם בתפקודו של ארגון אחר. דוגמה לכך ניתן לראות בביצוע העברה פיננסית בין בנקים או בשיחת טלפון העוברת בין רשתות השייכות למפעילים שונים.

ארגונים דומים חולקים גם אתגרים משותפים, ולעיתים כאלה הייחודיים להם. לדוגמה, לארגוני הבריאות אתגר ייחודי של התמודדות עם התקפות סייבר על ציוד רפואי. שיתוף בין ארגונים אלה באיסוף מודיעין או בנוהלי הקשחה של ציוד כזה, יחסוך השקעות שכל אחד מהארגונים היה צריך לבצע בנפרד.

מספר מדינות חשפו את כוונתן להקים מערכי סייבר לאיסוף מידע, הכולל שילוב של גופים ממשלתיים וגופים פרטיים/ציבוריים בעלי חשיבות לאומית.[25] מהות המהלך היא יצירה של תמונת מצב סייבר כוללת, יכולת למתן מענה בכוח אדם איכותי במקרה של מתקפה, וכמובן הפצה מיידית של חיסון או מידע על מתקפה לכל הארגונים הכפופים. כאמור, הבסיס הטכנולוגי ליצירת מערך כזה

עשוי לחייב חקיקה ומצריך שיתוף מידע סייבר בין הארגונים, הקמת מרכז המשמש להיתוך המידע ויישום מנגנוני שמירה על נכסים ארגוניים ועל פרטיות.

ממשלת בריטניה הקימה מיזם שיתוף בשם Cyber Security Information Sharing Partnership (CISP), כחלק מתוכנית לאומית להתמודדות עם אתגרי הסייבר.[26] המיזם כולל כבר כיום יותר מ־250 ארגוני מפתח, וכן את רשויות החוק, ומטרתו היא להגדיל את היכולת להתמודד עם טרור ופשיעה קיברנטיים. בארצות הברית פועלים מתחילת שנות האלפיים מיזמים לשיתוף מגזרי בתחומים שונים, כגון בריאות, פיננסים ועוד, הנקראים Information Sharing and Analysis Centers (ISAC). רוב המיזמים הללו פועלים בבעלות ובמימון הארגונים החברים בהם, אך לאחרונה הם זוכים לגב טכנולוגי ואף מימוני של משרד ההגנה של ארצות הברית, המכיר באינטרס של הממשל להיות מעורב בנושא. דוגמאות למעורבות כזו הן מתן גישה למרכז התגובה הממשלתי להתקפות סייבר (US-CERT)[27] והקמת מיזם אב שמטרתו לאחד את המידע הבין־מגזרי בארצות הברית למארג אחיד.[28]

גם בישראל הוקם זה מכבר גוף ביטחוני בשם הרשות הממלכתית לאבטחת מידע, המופקד על הנחיה מקצועית של הגופים האזרחיים שתחת אחריותו בתחום אבטחת תשתיות מחשב חיוניות מפני איומי טרור וחבלה, אבטחת מידע מסווג והתגוננות מפני איומי ריגול וחשיפת מידע. כמו כן, פועל בישראל מטה הסייבר הלאומי, שבין יתר תפקידיו פועל לגבש יוזמות להקמת מרכזי שיתוף מגזריים בתחומים שונים, כמו אנרגיה, פיננסים ובריאות, ולהקמת מרכז לאומי לתגובה לאירועי סייבר.

ברור כי לחימה בפשיעה או בטרור קיברנטיים, שמטבעם חוצים גבולות גיאוגרפיים ופוליטיים, ניתנת לביצוע רק באמצעות שיתופי פעולה טכנולוגיים ומשפטיים בין מדינות. מיזם אחד כזה הוא תוכנית לשיתוף פעולה מחקרי בתחום הסייבר שניזומה על ידי נאט"ו והאיחוד האירופי.[29] מיזם נוסף הוא תשתית שיתוף המוקמת בנאט"ו, ומתאפיינת באוטומציה של המידע על בסיס STIX, מתוך מטרה לאפשר שיתוף בין ארגונים שונים במדינות החברות בברית.[30] בהיבט המשפטי, נוסחה ונחתמה אמנת בודפשט שנועדה לתאם בין מערכות החקיקה של המדינות החברות באיחוד האירופי, לשפר את שיטות החקירה המשולבת ולהגביר את שיתוף הפעולה בהתמודדות עם פשעי מחשב.

מאמר הסוקר שיתוף פעולה בין־לאומי בהגנה על תשתיות קריטיות מפני התקפות סייבר[31] מאשש את הסברה כי סיכויי ההצלחה של מיזם שיתוף המידע גוברים גם במישור הבין־לאומי, אם הישויות החברות הן בעלות אינטרסים ותפיסות תרבותיות ופוליטיות דומות. שיתוף מידע בין גופים שונים מהווה מטבעו אתגר בהיבט השמירה על סודיות, מכיוון שהוא מחייב הגדרה של גבולות השיתוף ובקרות שיוכלו להבחין בין מידע פרטי או פנים ארגוני ובין מידע שניתן לשתף בו.

במהלך השנים זוכות ממשלות לשיתוף פעולה שקט, הנאכף לעיתים בחקיקה, מצד ספקי שירותים, תשתיות ואפליקציה, וזאת הן לצורכי ביטחון לאומי והן לצורכי לחימה בפשיעה. התופעה הולכת ונחשפת בתקופה האחרונה, במיוחד לאחר שה"גארדיאן" הבריטי פרסם, על בסיס הדלפה של אדוארד סנודן, כי ה־NSA האמריקאי מאזין לתעבורה של חברות אמריקאיות מובילות, במסגרת תוכנית בשם PRISM.[32] בנוסף חשף העיתון כי גוף המודיעין הבריטי המקביל ל־NSA מנטר את תעבורת האינטרנט על גבי תשתיות הסיבים האופטיים בממלכה,[33] וכי סוכנות הביון הפנימית בבריטניה, MI5, מתכוונת לפרוס אמצעים טכנולוגיים המאפשרים ביצוע סינון למילות מפתח ולמידע נקודתי בכל תעבורת המידע במדינה.[34]

חשיפת המידע על תוכניות ההאזנה של ארצות הברית העלתה לכותרות שם את נושא ההגנה על הפרטיות וגבולות הכוח של הממשל בהתנהלותו מול האזרח, וכן את האפשרות להטלת סנקציות משפטיות על הגורמים המשתפים מידע. עד כה דחה בית המשפט העליון בארצות הברית תביעות נגד ענקיות הטלקום המקומיות ואשרר את חוקיות העברת המידע האינטרנטי ושיחות טלפון לרשויות הביון והחוק.[35] עם זאת, האפשרות לתביעה נגד ארגון המשתף מידע מהווה חסם לשיתוף, ואותו מעוניין הממשל להסיר.

החל מסוף שנת 2011 מקודמת בארצות הברית חקיקה העוסקת בשיתוף מידע בתחום הסייבר,[36] שמטרתה לאפשר לחברות פרטיות וציבוריות לשתף מידע בזמן אמת עם הממשל ועם ארגוני ביון ואכיפת החוק, אם יבחרו בכך וכחלק ממלחמת הסייבר, וזאת מבלי להסתכן בתביעות משפטיות על הפרת סודיות או פרטיות. הצעת החוק עברה בבית הנבחרים, הועברה לסנאט ומשם להתאמות בוועדה לענייני מודיעין,[37] והיא נמצאת עדיין בתהליך החקיקה. המתנגדים לחוק טוענים כי הוא מפר את התיקון הרביעי לחוקה,[38] הקובע תנאי סף לחיפוש ולקבלת מידע פרטי על אזרח, כמו למשל צו שופט וסיבה מוצדקת לחיפוש. לדבריהם, החקיקה תאפשר לרשויות הביון לקבל מידע פרטי או עסקי מספקיות תשתית ותוכן ללא הבלמים המופיעים בתיקון לחוקה. גם ברשתות החברתיות ובמרחבי האינטרנט בארצות הברית קיימות התארגנויות העוסקות בבעייתיות של החוק המוצע[39] ומנסות לגייס את הציבור להתנגד לו ולמנוע את אישורו הסופי.

המתח בין התומכים בחקיקה לשיתוף מידע סייבר ובין המתנגדים לה אינו ייחודי רק לתחום זה, אלא נוגע לכל נושא הפרטיות בממשק שבין המדינה לאזרחיה ולמידת המעורבות של "האח הגדול" בחייהם. דוגמאות לעימות דומה הן מיזם המאגר הביומטרי של ממשלת ישראל הנתקל בביקורת רבה, ומיזם העיר החכמה של בריטניה, הכולל רישות העיר במצלמות ותוכנות לזיהוי פנים.

תובנות לסיכום

המגמות בהתפתחות איום הסייבר העכשווי כוללות שימוש במתודולוגיית תקיפה מכוונת מטרה ולא רק אקראית, דילוג על פני גבולות גיאוגרפיים ומשפטיים, ניצול פרצות אבטחה שאינן ידועות ושימוש בפיסות קוד מודולרי עוין במרחב הקיברנטי. הצד התוקף מתַחזק קהילה משגשגת, בעלת מבנה, סדר פנימי ומערכת פיננסית תומכת, המאפשרים שיתוף קל ומהיר של מידע התקפי. נראה כי מימוש מודלים של קהילה גם בצד ההגנתי, ומעבר מפרדיגמת הארגון המבודד למיזם של שיתוף מידע, יובילו לתוצאות טובות יותר גם בתחום המגננה מפני התקפות סייבר. בראייה רחבה יותר, אחד המשאבים המשמעותיים ביותר המתהווים במאה ה־21 הוא חוכמת ההמונים והקהילה (The wisdom of crowds). ניתן לראות דוגמאות לכוחה של חשיבה משותפת בתחומים רבים, ותחום הסייבר אינו יוצא דופן בהיבט זה.

המעבר למודלים של שיתוף נתמך על ידי אחדות אינטרסים של מרבית כוחות השוק המעורבים, ובהם גופי הרגולציה, הממשל, רשויות החוק והביון, יצרני הפתרונות והשירותים, ואף הארגונים עצמם. כדאיות השיתוף עם גורמי חוץ היא, בין היתר, תוצר של חוסר היכולת של הארגון הבודד להילחם את מלחמת הסייבר לבדו. היא תורמת לא רק לחיזוק משמעותי של מערך האבטחה והשרידות שלו, אלא גם להצלחתו העסקית, עקב חיסכון בהשקעות, תעדוף על ידי הרגולטור ועוד.

ארכיטקטורות הפתרון והתקנים המתפתחים יאפשרו ליצור בעתיד מעטפת טכנולוגית לקישור בין ארגונים, תוך שמירה על נכסי הארגון. הם גם יתמכו בקישור בין מימושים נפרדים של שיתוף, שיוכלו להתחבר אחד לשני לכדי מארג הירכי של מידע, כמו למשל שיתוף בתוך שוק מגזרי שיתממשק לשיתוף ברמה הלאומית.

חלק מהצלחת כל תהליך של תקינה תלוי בכוחות השוק התומכים בו. במקרה זה נראה כי גורמי הממשל בארצות הברית, ובראשם משרד ההגנה, מקדמים את התהליך בנחישות. עם זאת, לא נראים עדיין מימושי שיתוף מידע אפקטיביים בקנה מידה גדול, וזאת עקב ריבוי אתגרים שאינם בהכרח טכנולוגיים, ולעיתים גם גישה שמרנית של מקבלי ההחלטות בארגונים.

עם הבשלת התחום, אנו צפויים לראות תחילה שיתופים בין גופים דומים באותו המגזר, ובהמשך – מימוש שיתופי מידע בקנה מידה גדול יותר. אחדות אינטרסים, תרבות ארגונית דומה ויחסי תלות בין ארגונים מגדילים את סיכויי ההצלחה של המיזם ומפחיתים מהסיכונים שבו.

שניים מהחסמים הבולטים לשיתוף הם החשש של ארגונים מפני קישור מערכות שעלול לחשוף מידע פנים ארגוני רגיש לגופים מתחרים, והחשש מפני קבלת מידע סייבר לא תקין עקב הרעלת בסיס הנתונים המשותף, דבר העלול לגרום לפגיעה בשירות. ניתן להקטין את הסיכון בשני החסמים באופן משמעותי

באמצעים טכנולוגיים ובתקינת תהליכים ופרוטוקולים שימומשו בישות השיתוף המרכזית.

האתגר הגדול יותר ניצב בפני ארגונים שהמהות העסקית שלהם נוגעת לנושא הסייבר, כמו יצרני פתרונות אבטחה, מוצרי ושירותי תוכנה או גופי הפרויקטים והאינטגרציה הגדולים בתחום זה. השאלה היא האם ניתן לגבש מודל עבודה כדאי בין יצרנים אלה, כך שישתפו ביניהם מידע סייבר, וזאת למרות שנושא האבטחה והסייבר הוא חלק מהתחום בו הם מתחרים. מודל כזה יצטרך לכלול בהכרח שילוב יסודות הן של תחרות והן של שיתוף פעולה (Coopetition), באופן שיספק יתרונות לכל אחד משותפי המיזם לאורך זמן.

הוויכוח בין התומכים ובין המתנגדים לשיתוף מידע ולפעילות החקיקה המאפשרת אותו עדיין נמשך. לאור זאת, ולאור כל היבטי הנושא שנדונו במאמר, השאלה שצריכה להישאל היא האם ישנה פרדיגמה אחרת בעולם טכנולוגיות המידע שתאפשר את ההתמודדות עם אתגרי הסייבר הנוכחיים והעתידיים ללא צורך בשיתוף, או שאין ברירה אלא לשלב כוחות במאבק ולאמץ בהקדם תקינה אחידה לתשתית שיתופית. בכל מקרה, תשתית כזו תצטרך לשמור ככל שניתן על האיזון בין זכויות הפרט ובין יכולת המדינה להגן על תשתיותיה, נכסיה ואזרחיה.

הערות

1 Zero Day Attack הוא ניצול של פרצת אבטחה ברכיב המותקף, שאינה ידועה ליצרן הרכיב או לכל גוף אחר מלבד הגורם המתקיף עצמו, או שידועה ליצרן ועדיין לא הופץ עבורה טלאי תוכנה (Patch).

2 אחד המחקרים שנערכו בשנה האחרונה בנושא זה על ידי מכון RAND מספק ניתוח של האופן בו "השווקים השחורים" של עולם הסייבר בנויים ומתפקדים, סוקר מגמות היסטוריות ומספק תחזיות לעתיד. חוקרי המכון ערכו ראיונות עומק עם מומחים המעורבים באופן רשמי או אחר בשווקים אלה, בהם אנשי אקדמיה, חוקרי אבטחה, עיתונאים, ספקי אבטחה וגורמי אכיפת החוק. הדו"ח מגיע למסקנה כי "השווקים השחורים" בסייבר מהווים ענף כלכלי של מיליארדי דולרים, עם תשתית איתנה ומבנה חברתי וארגוני ברור. ראו:
L. Ablon, M.C. Libicki, A.A. Golay, *Markets for Cybercrime Tools and Stolen Data*, RAND Corporation, 2014, http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf.

3 הגישה הדוגלת במידור מידע סייבר מתוארת במקורות רבים כחלק מהיערכות הארגון מול אירוע אבטחתי. דוגמה לכך הוא מודל ההיערכות המוצע של SANS, מתוך קורס העוסק בנושא. ראו: SANS, SEC504: Hacker Techniques, Exploits & Incident Handling, 2014.

4 L.A. Gordon, M.P. Loeb and W. Lucyshyn, "Sharing Information on Computer Systems Security: An Economic Analysis", *Journal of Accounting & Public Policy*, Vol. 22, No. 6, November-December 2003, pp. 461-485.

5 באזל III היא רגולציה בתחום הפיננסים, הכוללת עקרון שקיפות מול הרגולטור המחייב

ארגונים פיננסיים לשתף סיכונים תפעוליים ואירועי סייבר. לפרטים נוספים ראו:
Basel III: A Global Regulatory Framework for more Resilient Banks and Banking Systems, http://www.bis.org/publ/bcbs189.pdf.

6 הוראת ניהול בנקאי תקין 206 של בנק ישראל מ־9 ביולי 2012, דנה בין היתר בקשר שבין רמת הסיכון התפעולי להלימות ההון של הבנק. ראו: http://www.bankisrael.gov.il/he/BankingSupervision/LettersAndCircularsSupervisorOfBanks/HozSup/h2341.pdf

7 תקינה הכוללת הנחיות הגנה בסייבר, וביניהן דרישה לשיתוף מידע בין ארגונים. ראו:
Information Technology – Security Techniques – ISO/IEC 27032:2012 Guidelines for Cybersecurity, July 16, 2012, http://www.iso.org/iso/catalogue_detail?csnumber=44375.

8 שלושת יסודות ה־CIA מהווים את עקרונות הבסיס הקלאסיים של אבטחת המידע: סודיות (Confidentiality) – שמירה על תוכן המידע מפני קריאה של גורם לא מורשה; אמינות ושלמות (Integrity) – שמירה על המידע כך שלא ישונה על ידי גורם לא מורשה; וזמינות (Availability) – שמירה על זמינות המידע והמערכות.

9 אתר ארגון TCG ראו: http://www.trustedcomputinggroup.org/

10 *Cyber Information-sharing Models: An Overview*, MITRE, October 2012, http://www.mitre.org/sites/default/files/pdf/cyber_info_sharing.pdf.

11 לפי ויקיפדיה, היתוך מידע הוא תהליך שמטרתו לקשר בין נתונים (Data), מידע (Information) וידע, (Knowledge) לחברם ולהצליבם ולמצוא קורלציה ביניהם, וזאת לצורך שיפור היכולת להעריך נתוני מיקום וזיהוי של ישויות עליהן מבצעים איסוף, וכן לצורך יצירת תמונת מצב והערכת איומים ורמת החשיבות שלהם. בנוסף, מתבצעת הערכה של איכות התוצרים ונוצרות דרישות ממקורות המידע, כחלק בלתי נפרד מתהליך היתוך המידע ובמטרה לשפר את תוצריו.

12 הרעלת בסיס הנתונים במידע כוזב עלולה להוביל ארגון הנחשף אליה לחסימת הפעילות שלו, פנימית או מול גופים אחרים (Denial Of Service). יתרונו של מערך שיתוף אוטומטי הוא גם חסרונו הגדול, והוא חשוף יותר ממערך שיתוף ידני להרעלה כזו, מכיוון שאינו כולל בקרה אנושית בזמן אמת.

13 S. Barnum, *Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™)*, February 2014, http://stix.mitre.org/about/documents/STIX_Whitepaper_v1.1.pdf.

14 M. Davidson, C. Schmidt, *TAXII Overview*, version 1.1, January 2014, http://taxii.mitre.org/specifications/version1.1/TAXII_Overview.pdf.

15 *CybOX – Cyber Observable eXpression – A Structured Language for Cyber Observables*, 2014, http://cybox.mitre.org/.

16 דוגמה לארכיטקטורת שיתוף עקרונית המתייחסת לנושא האמון במסגרת מחקר אקדמי היא ארכיטקטורה בשם PEI שהוצעה על ידי Krishnan ואחרים, וכוללת שלוש שכבות הכרחיות: שכבת המדיניות (Policy), המפרטת את מטרות השיתוף והגדרות האובייקטים, שכבת האכיפה (Enforcement), הכוללת את ארכיטקטורת הפתרון העקרונית, ולבסוף שכבת המימוש (Implementation), הכוללת ירידה לרמה הטכנולוגית של פרטי השיתוף. ראו:
R. Krishnan, R. Sandhu, K. Ranganathan, *PEI Models towards Scalable, Usable and High-Assurance Information Sharing*, **ACM**, New York, NY, USA, 2007, pp. 145-150.

17 מכון המחקר MITRE, הפועל במימון פדרלי, מפרט את אבני הדרך וההחלטות שצריכות להתקבל כחלק מתהליך בניית השיתוף. בין היתר נדרשות החלטות לגבי ארכיטקטורת השיתוף, מודל האמון בין הגופים, מיכון השיתוף, תפעול וחברות במיזם. ראו:

B. Bakis, *Cyber Partnership Blueprint: An Outline*, MITRE, October 2013, http://www.mitre.org/sites/default/files/publications/Bakis_Partnership_Blueprint_Outline_0.pdf;
מכון המחקר האמריקאי Bipartisan Policy Center פרסם מודל, בו גוף מרכזי משמש כמסלקה (Clearance Center) למידע המשותף לגופי התשתיות הקריטיות בארצות הברית. ראו:
Cyber Security Task Force: Public-Private Information Sharing, Bipartisan Policy Center (BPC), July 2012, http://bipartisanpolicy.org/sites/default/files/Public-Private%20Information%20Sharing.pdf.

18 המגזין Federal Blue Print מתאר את התקנים הטכנולוגיים למימוש שיתוף, אותם מקדם משרד ההגנה האמריקאי. ראו:
A. Merchant-Dest, *How the Department of Defense and the Department of Homeland Security are Taking Steps toward Information Sharing*, Federal Blue Print March 2014, http://federalblueprint.com/latest-news/department-defense-department-homeland-security-taking-steps-toward-information-sharing/.

19 צוות החוקרים מדרום קוריאה מוכיח, באמצעות ניסוי שערך, כי שיתוף המידע בין גופים שונים (Zones) מקצר את זמן התגובה להתקפה ומגדיל את רמת האבטחה. ראו:
B. Chang, D. Kim, H. Kim, J. Na, T. Chung, *Active Security Management Based on Secure Zone Cooperation*, Future Generation Computer System, 2004, 20(2), p. 283.

20 המשרד לאיכות הסביבה, **נהלים והנחיות לעניין פליטת מזהמים מתעשייה**, http://www.sviva.gov.il/subjectsEnv/SvivaAir/Industry/Pages/Regulations.aspx.

21 APT הוא מערך כלי התקפה בעולם הסייבר המכוון כלפי יעד ספציפי ומופעל על ידי האקרים מקצועיים, ולפיכך ניתן לפיתוח ולתפעול באופן שיקשה מאד על זיהויו בכלי הגנה סטנדרטיים.

22 שתי הטכנולוגיות ההתקפיות הללו מורידות מיעילות מנגנוני הגנה מסורתיים, שעיקרם זיהוי תבניות התקפה ברורות. הן מחייבות התייחסות מבוססת ניסיון כדי לזהות את האיום, ומעבר מפיתוח מוצרי אבטחה מבוססי חתימה (Signature Based) למוצרים מבוססי אנומליה בהתנהגות (Behavior Based Anomaly). שניים מהאתגרים העיקריים במוצרים מבוססי אנומליה הם הצורך ליצור בסיס התנהגותי ארגוני שמתעד את ההתנהגות הנורמלית של הארגון ומערכות המחשוב שלו במטרה לזהות חריגה מהתנהגות זו, והסכנה של הפרעה לתנועה לגיטימית עקב טעות בזיהוי.

23 נקרא גם שירות אבטחה מנוהל על ידי ספק השירותים (Managed Security Service Provider – MSSP).

24 K. Hausken, "Information Sharing among Firms and Cyber Attacks", *Journal of Accounting and Public Policy*, Vol. 26, No, 6, 2007, pp. 639-688.

25 דוגמה לאסטרטגיה של מדינה בהקמת מערך סייבר לאומי ניתן למצוא במסמך של ממשלת פינלנד הכולל, בין השאר, חזון ועקרונות לבניית מערך סייבר לאומי חוצה ארגונים ושורה של המלצות קונקרטיות לצעדים בכיוון זה. ראו:
Finland Cyber Security Strategy, Secretariat of the Security Committee, 2013, http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf.

26 תוכנית לאומית של ממשלת בריטניה להתמודדות עם איומי הסייבר:
The National Cyber Security Strategy, Our Forward Plans – December 2013, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/265386/The_National_Cyber_Security_Strategy_Our_Forward_Plans_December_2013.pdf

27 אתר מרכז התגובה האמריקאי להתקפות סייבר:

US-CERT – United States Computer Emergency Readiness Team, http://www.us-cert.gov

28 אתר מיזם השיתוף הבין־מגזרי בארצות הברית:
National Council of ISACs, http://www.isaccouncil.org/memberisacs.html

29 *The Multinational Cyber Defense Capability Development (MNCD2) Program*, http://mncd2.ncia.nato.int/Pages/default.aspx

30 *The Cyber Security Data Exchange and Collaboration Infrastructure (CDXI)*; L. Dandurand, *Cyber Security Information Exchange*, http://www.rsaconference.com/writable/presentations/file_upload/sect-t08-cyber-security-information-exchange.pdf

31 L. Tabanski, "International Cooperation in Critical Infrastructure Protection against Cyber Threats", *Atlantic Voices*, Vol. 2, No. 9, September 2012, http://sectech.tau.ac.il/node/114

32 המדובר בפעילות מעקב אלקטרונית של ה־NSA, שהושקה בשנת 2007, לאיסוף מידע לצורכי מודיעין, בין היתר מספקיות תשתית, תוכנה ותוכן, כמו Google, Yahoo, Microsoft, Apple, Skype, AOL. הפעילות נחשפה בהדלפה של אדוארד סנודן ל"גארדיאן" בשנת 2013.

33 E. MacAskill, J. Borger, N. Hopkins, N. Davies, J. Ball, "How does GCHQ's Internet Surveillance Work?", *The Guardian*, June 21, 2013, http://www.theguardian.com/uk/2013/jun/21/how-does-gchq-internet-surveillance-work

34 טכנולוגיית הניטור המאפשרת סינון מילות מפתח מתעבורת האינטרנט נקראת Deep Packet Inspection.

35 בית המשפט העליון בארצות הברית דחה תביעה נגד ענקיות הטלקום AT&T, Verizon ו־Sprint, ואשרר את החוקיות של העברת מידע מדוא"ל ומשיחות ל־NSA;
B. Kendall, "High Court lets Telecom Firms Wiretap Immunity Stand", *Wall Street Journal*, October 9, 2012, http://online.wsj.com/news/articles/SB10000872396390444024204578046312896501562

36 *Cyber Intelligence Sharing and Protection Act of 2013*, The Permanent Select Committee on Intelligence, 2013, http://intelligence.house.gov/bill/cyber-intelligence-sharing-and-protection-act-2013

37 *Cybersecurity Information Sharing Act of 2014*. עדכון שוטף על מצב החקיקה ניתן למצוא בספריית הקונגרס: http://thomas.loc.gov/home/thomas.php

38 Fourth Amendment: "The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized".

39 שניים מהגופים הפעילים בנושא זה הם הארגון להגנה על זכויות בעידן הדיגיטלי Electronic Frontier Foundation (EFF) וארגון בשם Fight for the Future – שניהם מריצים מערכה בשם CISPA Is Back להחתמת אזרחים על עצומה נגד החקיקה. ראו: http://www.cispaisback.org/; https://www.eff.org/cyberspying

התפתחויות בלוחמת הסייבר של איראן 2013–2014

גבי סיבוני וסמי קרוננפלד

במהלך 2013 הפכה איראן לאחד השחקנים המרכזיים בזירת לוחמת הסייבר הבין־לאומית. ההתפתחות הזו הנה תוצאה של הבשלת תהליכי בניין כוח הן בהקשרי הגנה והן באלה ההתקפיים מחד ושחרור הרסן לביצוע מתקפות בעולם מצד מקבלי ההחלטות באיראן מאידך. הפעילות האיראנית מראה קפיצת מדרגה בכל הקשור ביכולות הטכנולוגיות והמבצעיות שלה. המאמר בוחן את ההתקדמות והפעילות של מערך הגנת הסייבר האיראני ואת השימוש ביכולות אלו גם לריסון המתנגדים מבית ובוחן גם את היכולות ההתקפיות בעיקר דרך בחינת מתקפות סייבר המיוחסות לגורמים איראניים ולשליחים ובעלי ברית של איראן.

מילות מפתח: סייבר, איראן, בטחון סייבר, הגנת סייבר, בידול רשתות.

מבוא

גורם בכיר בחברת אבטחת הסייבר CrowdStrike דֵרג בתחילת 2013, בראיון למכון המחקר האמריקאי Atlantic Council את איראן ב"מעגל השלישי" (Third Tier) בכל הקשור ליכולותיה לפעול במרחב הסייבר, והעריך כי יכולות לוחמת הסייבר שלה נחותות משמעותית מיכולותיהן של מדינות "המעגל הראשון", כגון ארצות הברית, רוסיה ובריטניה, ושל מדינות "המעגל השני", דוגמת סין. תפיסה זו משקפת גם את הערכותיהם של מומחי מודיעין ואנשי ממשל מערביים רבים.

איראן נתפסת כמי שביכולתה להטריד את מערכי האבטחה המערביים ולפגוע במטרות "רכות", אך חסרה את הידע והאמצעים להוציא אל הפועל מתקפות סייבר

ד"ר גבי סיבוני הינו ראש התכניות ביטחון סייבר וצבא ואסטרטגיה במכון למחקרי ביטחון לאומי

סמי קרוננפלד הוא בוגר תואר מוסמך בחוג ליחסים בינלאומיים באוניברסיטה העברית בירושלים ולשעבר מתמחה בתכנית ביטחון סייבר במכון למחקרי ביטחון לאומי

מאמר זה ראה אור לראשונה ב**צבא ואסטרטגיה**, כרך 6, גיליון 2, אוגוסט 2014, עמ' 83-102.

אסטרטגיות.[1] עם זאת, במהלך 2013 הפכה איראן לאחד השחקנים המרכזיים בזירת לוחמת הסייבר הבין־לאומית. נראה כי התפתחות זו היא תוצאה של שילוב בין שחרור מדוד של הרסן מצד מקבלי ההחלטות האיראניים בכל הקשור לפעילות התקפית במרחב הסייבר, ובין קפיצת מדרגה איכותית של מערך לוחמת הסייבר האיראני, אשר הפתיע מומחים מערביים רבים בהיקפי פעילותו, בתחכומו המקצועי ובבחירה השאפתנית של מטרותיו.

אירועים דוגמת מתקפת ה־Stuxnet שפגעה קשות במערך הצנטריפוגות של איראן, והמחאה הנרחבת שליוותה את הבחירות שם בשנת 2009 – מחאה שלרשתות החברתיות ולמרחב האינטרנט היה חלק גדול בארגונה ובהסלמתה – מיצבו את זירת הסייבר כזירה מרכזית בחשיבותה בעיני המשטר האיראני. הניסיון של איראן באירועים אלה ובמתקפות סייבר אחרות שספגה הובילו אותה להקים מערך סייבר נרחב, הכולל מסגרות מבצעיות בעלות מִדרג פיקודי ומקצועי, המתמחות במגוון תחומים. איראן השקיעה יותר ממיליארד דולר בפיתוחים טכנולוגיים, בהקמת תשתיות ובאימון כוח אדם הגנתי והתקפי.[2] אסטרטגיית הסייבר האיראנית נקבעת ומפוקחת על ידי הדרגים הגבוהים ביותר, ביניהם הנשיא, מפקד משמרות המהפכה ושרים בכירים, המכהנים ב"מועצה העליונה למרחב הסייבר" – הגוף הבכיר המתכלל את פעילות הסייבר של המדינה.[3]

מאמר זה מבקש להציג תמונה עדכנית של הפעילות האיראנית במרחב הסייבר. המאמר מחולק לשני חלקים: החלק הראשון בוחן את ההתקדמות והפעילות של מערך הגנת הסייבר האיראני ואת השימוש ביכולות אלו גם לריסון המתנגדים מבית; החלק השני בוחן את הממד ההתקפי, בעיקר דרך בחינת מתקפות סייבר המיוחסות לגורמים איראניים ולשליחים ובעלי ברית של איראן. תובנות מסכמות ניתנות בסוף המאמר.

תפיסת ההגנה

תפיסת ההגנה האיראנית במרחב הסייבר משולבת עם הפעילות האיראנית לנטרול איומי פנים מצד מתנגדי המשטר. לאור זאת, איראן שואפת לייצר הגנה רב־שכבתית, המשלבת בין טכנולוגיות אבטחה, ניטור ופיקוח ובין מנגנוני אכיפה פיזית הרודפים באופן אגרסיבי אחר פעילי רשת הפועלים נגד המשטר במרחב הסייבר. איראן פועלת לשם כך בשלושה צירים מרכזיים: ראשית, יצירת מעטפת הגנה נגד תקיפות סייבר על תשתיות חיוניות ומידע רגיש, כמו מתקפת Stuxnet שפגעה בתוכנית העשרת האורניום האיראנית; שנית, נטרול פעילות הסייבר של גורמי אופוזיציה ומתנגדי משטר, עבורם מהווה מרחב הסייבר פלטפורמה מרכזית לתקשורת, הפצת מידע וארגון פעולות נגד המשטר; שלישית, הרחקה של תכנים

ורעיונות מערביים ופוגעניים ממרחב הסייבר הפנים־מדינתי – רעיונות העשויים לתרום להתפתחותה של "מהפכה רכה" שתפגע ביציבות המשטר.

היעדים והעקרונות האופרטיביים של מערך הגנת הסייבר האיראני מוכתבים על ידי "המועצה העליונה למרחב הסייבר" ומוצאים אל הפועל על ידי גופי ממשל מרכזיים, כמו "ארגון ההגנה הפסיבית" (The Passive Defensive Organization) המשתייך לצבא, "המועצה לתרבות מהפכנית" הכפופה למנהיג העליון, וכן המשטרה האיראנית ומשרד התקשורת.[4] חלק מהתשתיות הטכנולוגיות והארגוניות אותן הקימה איראן הבשילו במהלך השנה האחרונה לכדי גופים מבצעיים המחזקים משמעותית את פעילות ההגנה האיראנית במרחב הסייבר.

פרויקט בידול הרשתות – מתנתקים מהעולם

תוכנית בידול הרשתות הינה אחת מאסטרטגיות ההגנה המרכזיות של המשטר האיראני במרחב הסייבר. הפרויקט החל לקרום עור וגידים כבר ב־2009, כאשר היעד של איראן הוא העברת כלל פעילות הסייבר במדינה לרשת תקשורת פנים־מדינתית המנותקת מה־World Wide Web ומכונה "חלאל" (Halal Internet). הרשת האיראנית תוכננה לפעול ברוח הנורמות המוסלמיות־שיעיות אותן מעודד הממשל ולהעניק לו שליטה ופיקוח מלאים על התכנים, המידע והמשתמשים בה. בעיני המשטר, הקמת רשת אינטרא־נט והפרדת מרחב הסייבר האיראני מהמרחב הגלובלי הן צעד מרכזי בחיזוק ההגנה מפני מתקפות סייבר וריגול, בעצירת החדירה של רעיונות מערביים אנטי־משטריים ובנטרול האופוזיציה הפנימית.[5]

עדויות ראשונות להפעלתה של הרשת האיראנית התגלו באוקטובר 2012, כאשר חוקרי סייבר אמריקאיים, בשיתוף עם מקורות פנים איראניים, הצביעו על כך שספקיות האינטרנט האיראניות החלו להקצות שתי כתובות IP לכל מחשב המחובר לרשת האינטרנט – כתובת רשת רגילה לצד כתובת רשת פנים־איראנית אליה ניתן לגשת רק מתוך המדינה. החוקרים העריכו כי הרשת הפנים איראנית מסוגלת לנהל כ־17 מיליון כתובות IP, וכי יותר מ־10,000 מחשבים ביתיים, מסחריים וממשלתיים התחברו אליה במהלך 2012. במהלך 2013 החלה רשת "חלאל" לצבור תכנים (מצונזרים ומפוקחים כמובן), תוך מתן דגש רב לפיתוח גרסאות מקומיות של שירותי רשת פופולריים, כגון דואר אלקטרוני, רשתות חברתיות, תקשורות וידאו ואודיו, אתרי מפות ואתרי וידאו.[6]

ביולי 2013 חנך המשטר האיראני שירות דואר אלקטרוני, post.ir@, אשר כלל האזרחים חויבו להירשם אליו ואשר תוכנן להוות את צינור הקשר המרכזי בין האזרח לבין זרועות הממשל השונות. השירות, שיש לו תמיכה בפרסית, אנגלית, צרפתית וערבית, מסוגל לספק כתובות דואר אלקטרוני לכמאה מיליון משתמשים, כאשר לכל משתמש מוקצית תיבת דואר בת חמישים מגה־בייט, אותה ניתן להרחיב

עד לשני ג׳יגה־בייט. פתיחת תיבת הדואר מחייבת את האזרח לתת את שמו וכתובתו, ונראה כי התכתובות המועברות בו אינן מוצפנות – תנאים המאפשרים למשטר לקיים פיקוח הדוק על המשתמשים ועל התכתובות.[7] בדצמבר 2012 השיקה רשות השידור הממלכתית של איראן אתר דמוי ״Youtube״ תחת השם Mehr, המציג תכנים מפוקחים ומאפשר לגולשים להעלות תכנים משלהם, תחת כללי צנזורה קפדניים.[8] הרשויות האיראניות גם אסרו על שימוש בתוכנות אבטחת מידע זרות ופיתחו מערכת אנטי־וירוס מקומית, המכונה Padvish. על פי מקורות באיראן, מערכת זו יכולה להגן גם על רשתות ולמנוע חדירה של תוכנות זדוניות.[9]

כדי להגדיל את מספר המשתמשים ברשת ״חלאל״ ובשירותי הרשת האיראניים, ליווה המשטר את הפעלתה בהרחבת השימוש באמצעים טכנולוגיים ובחקיקה, המגבילים את אפשרויות האזרח האיראני להתחבר לרשת האינטרנט הגלובלית: הרשויות האיראניות חסמו את השימוש בתוכנות voice over IP, כמו Skype ו־Google Talk. כמו כן, נחסמו לשימוש רבות מרשתות ה־VPN, TOR ותוכנות עוקפות סינון, המהוות כלים מרכזיים בעקיפת הפיקוח והצנזורה הממשלתיים על מרחב הסייבר.[10] בנוסף לכך, רשויות הסייבר האיראניות החלו להאט באופן מכוון אתרי אינטרנט ושירותי רשת חיצוניים (בעיקר שירותים של חברת Google, שהם פופולריים מאד באיראן), לעיתים עד כדי שישה אחוזים מהמהירות הרגילה. כמו כן, הרשויות מבצעות חסימות אקראיות של אתרים ושרותים (Migrating blocks) ומגבילות מאד את תעבורת הרשת המוצפנת. פעולות אלו מערימות קשיים טכניים, חוקיים ופסיכולוגיים על האזרח האיראני המבקש לגלוש ברשת האינטרנט הגלובלית, ולמעשה דוחפות אותו להשתמש ברשת ״חלאל״ המפוקחת והמצונזרת.[11]

פיתוח טכנולוגיות הגנה ופיקוח

כהשלמה למאמצי בידול הרשתות, איראן משקיעה רבות גם בפיתוח טכנולוגיות ואמצעי הגנת סייבר מתוצרת מקומית, וזאת כדי להקטין את תלותה במוצרים זרים העשויים להיות ״סוסים טרויאניים״. בדצמבר 2013, בטקס מתוקשר בו נכחו בכירים בממסד הביטחוני האיראני, ביניהם שר ההגנה הגנרל Hossein Dehqan ומפקד מערך ההגנה האזרחית בריגדיר־גנרל Gholam Reza Jalali, נחשפו 12 פיתוחים טכנולוגיים פרי התעשייה האיראנית, ביניהם טלפון סלולרי מאובטח האמור לספק למשתמשים קו תקשורת חסין לציטוטים. בנוסף הוצגו בכנס מערכת הפעלה מאובטחת למחשבים שאמורה לבטל את התלות האיראנית במערכות ההפעלה האמריקאיות; מכשיר GPS; מערכת תקשורת אופטית; תוכנות ומערכות נגד תוכניות זדוניות ו־Firewall; מערכת לזיהוי מתקפות סייבר; ומכשור למרכזי אבטחת מידע.[12] בנוסף לכך, סוכנות הידיעות האיראנית ISNA דיווחה כי איראן

הכניסה לשימוש מערכת הגנת סייבר כלל־ארצית העונה לשם Shahpad. על פי ראש הפרויקט, Mohammad Naderi, המערכת מאפשרת היתוך מידע ממגוון תחנות קצה וחיישנים ומייצרת תמונת מצב קיברנטית מדינתית כוללת. בעת התקפה Shahpad מיידעת באופן מידי את מרכזי אבטחת המידע במדינה, ומאפשרת להם להגיב במהירות ולפעול לבלימת המתקפה.[13]

איראן אינה מסתמכת אך ורק על פיתוח מקומי לחיזוק יכולת אבטחת הסייבר שלה. בספטמבר 2012 היא חתמה על הסכם לשיתוף פעולה טכנולוגי נרחב עם קוריאה הצפונית, הכולל גם שיתוף פעולה בתחום טכנולוגיות המידע. על פי מומחים, קיימת סבירות גבוהה כי שתי המדינות, אשר ספגו בעבר מתקפות סייבר ורואות בזירה זו מוקד אסטרטגי חשוב, ישלבו כוחות במסגרת הסכם זה לפיתוח טכנולוגיות אבטחת מידע, ניטור ואף התקפה.[14]

איראן גם משתפת פעולה עם סין בתחום הסייבר, ובעבר רכשה מחברת ZTE Corp. הסינית מערכת מעקב המאפשרת ניטור של שמע, הודעות טקסט וגלישת אינטרנט.[15] שיתופי הפעולה עם מדינות אלו ומדינות נוספות, דוגמת רוסיה, מסייעים רבות לחיזוק מערך הגנת הסייבר האיראני וליכולתה של איראן לעקוב אחר האינטרנט ואחר אזרחיה.

חיזוק מערכי ההגנה

מעֵבר להיבטים הטכנולוגיים, שמה איראן דגש מיוחד על חיזוק היכולת של גופי המדינה השונים להתמודד עם מתקפות סייבר ולבלום אותן. מערך הסייבר האיראני ביצע מספר תרגילי הגנת סייבר מקיפים, במהלכם אומנו יחידות אזרחיות וצבאיות. בנוסף, נערך תרגיל לוחמת סייבר כחלק מתרגיל ימי של משמרות המהפכה במצרֵי הורמוז במהלך דצמבר 2012. במסגרת התרגיל שוגרה מתקפת סייבר נגד רשת המחשבים של הצי, במטרה לשלוף מידע ולהחדיר תוכנות זדוניות. מפקדי התרגיל הכריזו כי המתקפה התגלתה ונחסמה על ידי מערכי הגנת הסייבר של הצי.[16]

בפברואר 2013 דיווחה סוכנות הידיעות האיראנית Fars, המקורבת למשטר, על תרגיל מקיף של כוחות היבשה של משמרות המהפכה, במהלכו תורגלו ונבחנו מערכות הגנת הסייבר של הארגון.[17] תרגיל נוסף נערך באוקטובר 2013, כחלק מתרגיל הגנה כולל של "ארגון ההגנה הפסיבית". במסגרת תרגיל זה אומנו ונבדקו מערכי הגנת הסייבר של גופי ממשל מרכזיים, ביניהם מתקני הגרעין, רשת רכבות המטרו של טהראן, רשות השידור האיראנית, נמלים, הבנק המרכזי וספקי תקשורת סלולריים. על פי מפַקד "ארגון ההגנה הפסיבית", נמצאו ונסגרו פרצות אבטחה רבות במערכי הגנת הסייבר של הארגונים ובעקבות התרגיל הוחלט על הקמת מרכז הגנת סייבר במתקן הגרעיני בנתאנז.[18]

ריסון מתנגדי המשטר

את המהלכים הטכנולוגיים שמבצעת איראן במטרה להגן על מרחב הסייבר שלה היא משלימה בפעילות אכיפה פיזית אגרסיבית נגד מתנגדי המשטר במדינה, העושים במרחב הסייבר שימוש חתרני נרחב. שחקן מרכזי במאמצי המשטר האיראני לשלוט במרחב הסייבר היא משטרת הסייבר, FATA, שהוקמה בתחילת 2011 תחת פיקוד המשטרה האיראנית. במהלך השנה האחרונה הפכה FATA לאגרסיבית יותר במאמציה לאכוף את מגבלות הצנזורה ולמנוע פעילות חתרנית במרחב הסייבר. אנשי היחידה פועלים לאיתור ולכידה של בלוגרים, עיתונאי רשת ופעילי אופוזיציה, המפיצים רעיונות ודעות שאינם עולים בקנה אחד עם עמדות המשטר.

האגרסיביות הרבה המאפיינת את פעילותה של משטרת הסייבר האיראנית נגד מתנגדי המשטר זכתה לתהודה עולמית בנובמבר 2012, בעקבות דיווחים על מותו של הבלוגר האיראני Sattar Beheshti בבית כלא בקרבת טהראן. בהשתי, שנעצר על ידי FATA יום לאחר שפרסם בלוג בו מתח ביקורת חריפה על מערכת המשפט האיראנית (אותה כינה "בית המטבחיים" של ח'מנהאי), מת כתוצאה ממסכת עינויים והכאות קשה מצד אנשי משטרת הסייבר.[19] הפרסום על מותו הביא לגל ביקורות בתוך איראן ומחוץ לה. כתוצאה מכך, הטיל האיחוד האירופי סנקציות על FATA ועל גורמים אחרים שהיו מעורבים במוות, ביניהם שופטים והאחראי על הצנזורה באיראן.[20] הלחץ הבין־לאומי אמנם הוביל לפיטוריו של מפקד משטרת הסייבר בעיר טהראן,[21] אך על פי ארגוני זכויות אדם בין־לאומיים FATA ממשיכה באסטרטגיית המעצרים הנרחבת שלה ופועלת באגרסיביות לאיתור ולענישה של אירנים היוצאים נגד המשטר ברשתות החברתיות ובבלוגים.[22] משטרת הסייבר האיראנית אף הידקה בחודשים האחרונים את הפיקוח על מוסדות הקפה־אינטרנט הפופולריים באיראן וסגרה עשרות מהם עקב אי־עמידה בחוקי הרישום וההגבלה המחמירים של המדינה.[23]

הפיקוח והאכיפה של המשטר הפכו לאינטנסיביים ונרחבים במיוחד בחודשים שהובילו לבחירות לנשיאות ב־14 ביוני 2013. יומיים לפני הבחירות פרסמה "גוגל" כי אנשיה איתרו ובלמו מתקפת "דיוג" (phishing) ששוגרה על ידי גורמים בתוך איראן וכוּוונה נגד עשרות אלפי חשבונות דואר אלקטרוני של אזרחים איראניים. המתקפה כללה שליחה של דואר אלקטרוני שהוסווה כדואר תחזוקה של מערכת Gmail וביקש את הגולש להזין את שם המשתמש וסיסמת הדואר האלקטרוני שלו. המידע המוזן הועבר ישירות לתוקפים ואִפשר להם גישה חופשית לתיבות הדואר האלקטרוני של המשתמש.[24] ניתוח המתקפה העלה חשד כי מדובר באותם תוקפים איראניים אשר תקפו את שרתי החברה ההולנדית DigiNotar ב־2011.[25] אמנם, מטרות התקיפה לא הובהרו, אך נראה כי קיים קשר הדוק בינה לבין

מערכת הבחירות וכי התוקפים רצו לאפשר לשלטונות האיראניים לאסוף מידע על פעולותיהם ודעותיהם של אזרחים איראניים ולפעול נגד גורמים "בעיתיים".[26] בנוסף, בשבועות שהובילו לבחירות התקיימה מתקפת סייבר נרחבת נגד אתרי אופוזיציה ותקשורת איראניים. קבוצת האקרים העונה לשם "The Unknown Cyber Jihad" וטוענת כי היא קשורה לארגון חזבאללה, פרצה למספר אתרי אופוזיציה איראניים והחליפה את תוכנם בהודעה נגד מתנגדי המשטר. כמו כן, אתרי אופוזיציה מרכזיים, כגון אתר התנועה הקומוניסטית באיראן, אתר התנועה הירוקה ואתרי זכויות אדם, נחסמו למשך שעות רבות על ידי המשטר, ועשרות פעילי רשת ועיתונאים נעצרו ונכלאו על ידי כוחות הביטחון האיראניים.[27]

הפעילות האיראנית נגד האופוזיציה ומתנגדי המשטר השתכללה והתפתחה מאז האירועים שליוו את בחירתו מחדש של אחמדינג'אד ב־2009. בעוד שבאותה שנה האופוזיציה השתמשה בקלות יחסית במרחב הסייבר לארגון הפגנות, להפצת רעיונות ולהעברת מידע על המתרחש באיראן החוצה (בעיקר על ידי שימוש ברשתות VPN), בבחירות 2013 מערך הסייבר האיראני היה ערוך ומוכן מבחינה טכנולוגית ואופרטיבית כדי לשלוט בשיח שהתקיים במרחב האינטרנט הפנימי ולנטר פעילות חתרנית ויציאת מידע מתוך איראן.

נראה, כי נכון להיום, מערך הגנת הסייבר האיראני נדרש עדיין לעבור כברת דרך כדי שיוכל להתמודד באופן אפקטיבי ועקבי עם מתקפות סייבר ברמת תחכום גבוהה, דוגמת Stuxnet ו־Flame, ולמנוע כל חדירה של תכנים או רעיונות חיצוניים. יש המתארים מערך זה כלא יותר מאשר גרסה מאולתרת ומאורגנת פחות של "חומת" הסייבר הסינית.[28] עם זאת, קפיצת המדרגה הטכנולוגית והארגונית שביצעה איראן בשנה האחרונה מעידה כי יש לה עקומת למידה חדה וכי היא עשויה לגבש מערך הגנה יעיל ומקיף מוקדם מהצפוי.

הממד ההתקפי – חיפוש אחר מתקפות "איכות"

הרפובליקה האסלאמית של איראן רואה בלוחמת הסייבר פלטפורמה יעילה המאפשרת לפגוע ביריבות בעלות עליונות צבאית ברורה, ובד בבד לשמור על מרווח הכחשה שימנע הוקעה בין־לאומית או אף סנקציות ומתקפות נגד. תפיסה זו הביאה את איראן להשתמש בלוחמת הסייבר ככלי מרכזי לתקיפת מטרות מערביות בתגובה לסנקציות וכאמצעי להרתעת הסלמה בפעילותן של מדינות המערב נגד איראן. היקפן, יעדיהן והצלחתן היחסית של מתקפות סייבר שהתרחשו בשנה האחרונה ושויכו לגורמים איראניים מעידים על התעצמות היכולות העומדות לרשותה של איראן. אנשי מודיעין וממשל בישראל ובארצות הברית אף הביעו דאגה מקצב ההתפתחות הגבוהה של יכולות לוחמת הסייבר האיראניות.[29]

גורמים מערביים משייכים את ההתקדמות בתוכנית לוחמת הסייבר של איראן להצלחתה לשלב בין היכולות, הידע וכוח האדם המוכשר הצומח בפקולטות האיראניות למדעי המחשב[30] ובין הניסיון והיכולות הגבוהות של קהילת ההאקרים האיראנית, שרבים מחבריה מזדהים עם המשטר ועם מטרותיו. קהילת ההאקרים האיראנית היא אחת הקהילות הדומיננטיות והפעילות בעולם, ועדויות מצביעות על קשרים בין קבוצות שונות שלה לבין משמרות המהפכה. השימוש בהאקרים, אשר קשריהם לממסד האיראני לוטים בערפל, מעניק לאיראן מרחב עמימות ויכולת להכחיש את מעורבותה בפעילות סייבר זדונית ובלתי חוקית כאשר העקבות מובילים אליה.

אחת מקבוצות ההאקרים האיראניות המובילות היא Ashiyane Digital Security Team, הנתפסת כבעלת קשרים למשמרות המהפכה וחבריה מונעים על ידי תפיסות אידיאולוגיות התומכות במשטר האיראני ובמהפכה.[31] Ashiyane דורגה על ידי האתר Zone-H, המתמחה בניתוח פעילות של האקרים במרחב הסייבר, במקום השני בעולם במספר אתרי האינטרנט שחבריה הצליחו לפרוץ ולהשחית, לרוב על ידי החלפת התוכן בצלמית של הקבוצה או בתעמולה פרו איראנית. נכון לתחילת נובמבר 2013, מיוחסות לקבוצה יותר מ־6,000 פריצות.[32] בין האתרים שנפרצו על ידי חברי Ashiyane נמצאים 26 אתרי ממשל ברזילאיים, ובכללם האתר של המשטרה הצבאית, וכן אתרי ממשל באנגליה ובפקיסטן.[33] על פי אתר האינטרנט Zone-H, מלבד Ashiyane, שבע קבוצות האקרים איראניות נוספת נמצאות בין ארבעים קבוצות ההאקרים הפעילות בעולם בכל הקשור להשחתת אתרים (defacement website). מתקפות השחתה אמנם נחשבות לקלות יחסית, אך הן מעידות על יכולות טכניות גבוהות ובמקרים רבים הן מהוות שלב ראשוני בהתפתחותן של קבוצת ההאקרים איראניות לכיוון מתקפות מתוחכמות והרסניות יותר. דוגמה להתפתחות כזו היא Ajax Security Team, קבוצת האקרים איראנית, שהחלה לפעול ב־2010 והתמקדה במתקפות השחתת אתרים. דוח של קבוצת FireEye המנתח לעומק את פעילותה מצביע על טרנספורמציה מסוכנת. ראשית חברי הקבוצה, שבתחילה פעלו בעיקר במטרה להוכיח את כישוריהם (הם אף תקפו אתר ממשלתי איראני), עברו תהליך פוליטיזציה והחלו למקד את מתקפותיהם בחברות אמריקאיות ובמתנגדי משטר בתוך איראן. במקביל לכך, חלה גם הסלמה בדפוסי התקיפה של הקבוצה, אשר זנחה את מתקפות השחתת האתרים ועברה לריגול קיברנטי, הכולל איסוף מידע בקנה רחב כנגד מתנגדי משטר, תוך שימוש בתוכנות Malware מתקדמות ובטכניקות דיוג. תפקידו של המשטר בתהליך אבולוציה זה וקשריו עם קבוצת Ajax אינם ברורים, אך אין ספק כי פעילות הקבוצה עולה בקנה אחד עם ניסיונות המשטר לשלוט במרחב האינטרנט הפנימי ורדיפתו אחר מתנגדים.[34]

גורם נוסף שתורם להתקדמות המהירה בתוכנית לוחמת הסייבר האיראנית הם הקשרים המתהדקים של מערך הסייבר האיראני עם פושעי סייבר, האקרים ומומחי אבטחת מידע, בעיקר רוסים, המוכנים "להשכיר" את יכולותיהם בכסף. גורמים אמריקאיים רואים קשרים אלה כמרכיב מרכזי בקפיצת המדרגה האיראנית, וחבר הקונגרס מייק רוג'רס, ראש ועדת המודיעין, אף ציין כי בגל תקיפות סייבר נגד אתרי בנקים אמריקאיים, אשר יוחס לגורמים איראניים, ניתן היה לאתר סימנים למעורבות של גורמים רוסיים.[35] לצד כוח האדם ה"מיובא", ביכולתה של איראן גם לרכוש "נשק" סייבר מתוחכם וחזק המוצע בשוק השחור לכל המוכן לשלם את המחיר הנדרש. נשק סייבר זה מאפשר לאיראנים להעצים במהירות את יכולותיהם ומסוכנותם.[36]

ההתקדמות ביכולות לוחמת הסייבר האיראניות משתקפת בסדרה של מתקפות שהתרחשו במהלך המחצית השנייה של 2012 וב־2013, אשר עשו שימוש בטכניקות מתוחכמות יותר, תקפו יעדים איכותיים יותר והתרחשו בהיקפים משמעותיים יותר מאשר תקיפות מוקדמות יותר שיוחסו לאיראן. מתקפה אחת שיוחסה לגורמים איראניים החלה בספטמבר 2012 ונמשכה גם לתוך 2013, כללה תקיפה רחבת היקף של אתרי האינטרנט של בנקים ומוסדות פיננסיים מרכזיים בארצות הברית. המתקפה תוארה על ידי מומחה לאבטחת מידע כ"חסרת תקדים בהיקפה ובמידת יעילותה". ייחודיותה ואיכותה נעוצות בשיטת הפעולה אותה נקטו התוקפים: במקום לתקוף דרך פרצות במחשבים בודדים, הם ניתבו את מתקפותיהם דרך רשתות המחשוב של מרכזי מידע. מרכזי מידע אלה, המופעלים על ידי חברות כגון "גוגל" ו"אמָזון", מורכבים מרשתות מחשבים ענקיות המחברות בין מאות, ולעיתים אלפי שרתים ומחשבים, ומספקות שירותי "ענן" למספר רב של חברות ועסקים ברחבי העולם. התוקפים הצליחו להשתלט על חלק מ"ענני" מחשוב אלה ולהשתמש בעוצמת המִחשוב האדירה שלהם כפלטפורמה למתקפות על אתרי בנקים וחברות פיננסיות בארצות הברית. מומחי אבטחה תיארו מהלך זה כ"מקבילה הקיברנטית של הפיכת גוּר של צ'יוואווה לגודזילה יורקת אש".[37]

קבוצת האקרים המכנה עצמה "לוחמי הסייבר של עז א־דין אל־קסאם" קיבלה אחריות על התקפת מניעת שירות נגד אתרי האינטרנט של בנקים אמריקאיים מרכזיים, ביניהם Citigroup, Bank of America ו־HSBC. חברי הקבוצה ניצלו את פלטפורמת המחשוב של מרכזי המידע וניתבו נפחים עצומים של תעבורת רשת לאתרי הבנקים, מה שהביא לקריסתם ומנע את גישת הלקוחות לחשבונותיהם. בנוסף לשימוש בתעבורת רשת, השתמשו התוקפים בטכניקה המכונה Encrypted DDoS. שיטה זו מנצלת את מנגנוני הצפנת המידע של הבנקים עצמם – מנגנונים שפעולתם צורכת משאבי מערכת רבים. התוקפים הציפו את אתרי הבנקים

בפעולות הדורשות הצפנה, ובכך גרמו להאטה ולפגיעה משמעותית בפעילותם. עם זאת, במהלך המתקפות לא נפרצו חשבונות בנק ולא נגנבו כספי לקוחות.[38]

מומחי אבטחת מידע מציינים שהיכולות הגבוהות הנדרשות לביצוע מתקפה בהיקף נרחב כל כך ובתחכום רב כל כך מצביעות על מעורבותה של מדינה. לתקיפה נגד תשתיותיה הפיננסיות של מדינה, במיוחד של מעצמה כלכלית כמו ארצות הברית, משמעויות חמורות והיא עשויה להביא לנזקים כלכליים כבדים עקב הפגיעה בשגרת הפעילות הפיננסית של חברות מסחריות ובתי אב רבים.

למרות היעדר הוכחות פיזיות והכחשה איראנית, בכירים בממשל ובשירותי המודיעין של ארצות הברית משוכנעים כי איראן היא העומדת מאחורי המתקפות, כתגובה לסנקציות הבין־לאומיות עליה ולמתקפות הסייבר שפגעו בתשתיותיה ונתפסות בעיניה כמעשה ידיהן של ארצות הברית וישראל. מזכיר ההגנה האמריקאי דאז, ליאון פאנטה, התייחס למתקפות נגד הבנקים ואמר כי מדובר ב"הסלמה משמעותית", מבלי שהזכיר את שמה של איראן.[39]

גל תקיפות נוסף המיוחס לגורמים איראניים התמקד בחברות תשתית ואנרגיה אמריקאיות והחל לתפוס תאוצה בחודשים הראשונים של 2013, עד אשר הסוכנות האמריקאית להגנת המולדת החליטה בחודש מאי להוציא באופן חריג אזהרה לחברות האנרגיה והתשתיות בדבר עליית מדרגה באיום הסייבר על רשתות המחשוב שלהן. האזהרה ציינה כי אין מדובר במתקפות שגרתיות של גניבת מידע, ריגול תעשייתי ופגיעה במערכות מנהליות, אלא במתקפות המבקשות להשתלט על מערכי הבקרה שלהן ולפגוע בפעילותן הפיזית או באמצעי הבטיחות של תשתיות קריטיות, דוגמת מערכות הולכת גז ונפט ומערכות חשמל. הממשל האמריקאי אמנם לא הצהיר באופן רשמי כי הממסד האיראני הוא העומד מאחורי גל המתקפות, אך מומחים ואנשי ממשל ציינו כי ישנן עדויות המצביעות על מוצאן בשטחה של איראן וכי הוצאתן אל הפועל מחייבת תמיכה כלשהי מצד הגורמים השולטים במרחב הסייבר האיראני.[40] התחזקות עתידית של הסנקציות נגד שוק האנרגיה האיראני,[41] עשויה להוביל את איראן למהלך אסטרטגי נגד שוק האנרגיה הבין־לאומי, הן כצעד הרתעתי והן כדי להגביר את הדרישה לנפט שלה.

מומחים מתארים את המתקפות על רשתות המחשוב של חברות האנרגיה האמריקאיות כמהלך נרחב של איסוף מידע, לימוד ובחינה, אשר נועד לייצר תשתיות ידע וניסיון לטובת מתקפה עתידית על מערכות בקרה המפעילות ומווסתות את פעילותן של תשתיות קריטיות. פגיעה במערכות אלו עשויה להביא לנזק משמעותי ואף לאובדן חיים בקנה מידה נרחב. ואכן, במהלך המתקפות הצליחו התוקפים לעקוף חלק ממערכות האבטחה ולאסוף מידע על המבנה שלהן, יכולותיהן ופרצות האבטחה הקיימות בהן.[42] בכיר בחברת אבטחת המידע Mandiant אמר כי לפחות במקרה אחד הצליחו חוקריו לשייך את המתקפה

לקבוצת האקרים איראנית, אשר קשריה עם המשטר אינם ברורים. לדבריו, מטרת התוקפים, אשר נעו בתוך מערכות המחשוב האמריקאיות ולמדו את מערכי הגילוי והאבטחה שלהן, היא לצבור ניסיון בפעילות ברשתות "חיות" ולתור אחר נקודות חולשה.[43] בכירים אמריקאיים ציינו כי ההתקפות על חברות האנרגיה וההצלחות היחסיות של הפורצים מעידות כי יכולות הסייבר ההתקפיות העומדות לרשותה של איראן משתפרות ומתפתחות במהירות.[44] היה ואיראן תשיג יכולות תקיפה אפקטיביות נגד מערכות בקרה של תשתיות חיוניות, הדבר עשוי להוות איום אסטרטגי על יריבותיה.

תקיפה משמעותית נוספת שיוחסה לאיראן אירעה בספטמבר 2013, כאשר גורמים רשמיים בארצות הברית דיווחו על פריצה לרשת מחשבים לא מסווגת של הצי האמריקאי. הגורמים ציינו כי המתקפה נעשתה על ידי קבוצת האקרים הפועלים בשירות הממשל האיראני או בהסכמתו ותמיכתו. הרשת שנפגעה היא הרשת הפנימית של הצי האמריקאי, אשר אמנם אינה מסווגת, אך משמשת בין השאר להתכתבויות והתקשרויות וכוללת מידע רגיש, כגון כתובות דואר אלקטרוני של ראשי הצי ושל בכירי ממשל. גורמים בממשל דיווחו כי התוקפים הצליחו לחדור למערכת הניהול של הרשת, אך לטענתם לא נגנב מידע בעל ערך משמעותי ולא נפרצו תיבות דוא"ל. מדאיגה במיוחד הייתה העובדה שהפורצים הצליחו להמשיך ולפעול ברשת המחשבים של הצי גם אחרי שגורמי הביטחון האמריקאיים דיווחו על סילוקם מהרשת. התחכום האיראני שהתגלה בתקיפה זו מהווה סימן נוסף להתפתחות ולהתקדמות ביכולות הפריצה האיראניות ועל נכונותה של איראן לפעול גם נגד יעדי סייבר צבאיים.[45]

מלבד שרשרת המתקפות נגד מוסדות אמריקאיים, גורמים המזוהים עם איראן קיבלו על עצמם בשנה האחרונה אחריות גם למתקפות סייבר נגד מוסדות ישראליים. ביוני 2013 הצהיר ראש הממשלה בנימין נתניהו כי חלה עלייה משמעותית בתקיפות הסייבר האיראניות על תשתיות מחשוב חשובות בישראל.[46] במהלך דצמבר 2013 וינואר 2014 טענה קבוצת האקרים אסלאמית, המכנה עצמה The Islamic Cyber Resistance Group (ICRG) כי ביצעה מספר מתקפות סייבר איכותיות נגד גורמים בישראל ובמזרח התיכון כנקמה על חיסולו של בכיר חזבאללה חסן לקיס. הקבוצה, הזוכה לסיקור נרחב מצד סוכנות הידיעות האיראנית Fars, טוענת כי הצליחה לחדור למערכות השליטה של רשות התעופה האזרחית של ישראל ולשהות במערכת במשך חודשים מבלי להתגלות. אנשי הקבוצה טוענים כי הצליחו לגנוב מידע רגיש ואף יכלו להשתלט על מערכות הניווט והתקשורת של הרשות ולגרום לאסון אווירי באם היו בוחרים לעשות כך.[47] אנשי ICRG גם הצהירו כי הצליחו לחדור לשרתי המחשוב של צה"ל ולגנוב מידע סודי, כגון תיקים אישיים של חיילי צה"ל, רשימות של בעלי תפקידים, סיסמאות,

כתובות מגורים ודואר אלקטרוני וקודים צבאיים. פרט למתקפות על ישראל, הצהיר ארגון ICRG כי הצליח לפרוץ למאגר מידע של הצבא הסעודי ולמחשבים של חברות הנמצאות בבעלות משפחת בן־לאדן.[48] עם זאת, גורמים בישראל קבעו כי המתקפות בהן התפארה הקבוצה לא התרחשו מעולם וכי מדובר בלא יותר מאשר תעמולה ולוחמה פסיכולוגית מצד איראן.

ברקע המאבקים הללו עומדת תעלומת מותו של איש משמרות המהפכה מוג'תבא אחמדי שנמצא מת בתחילת אוקטובר 2013. דיווחים במערב קובעים כי מדובר בבכיר ששימש כמפקד מטה לוחמת הסייבר של משמרות המהפכה. בתחילה יוחס מותו לישראל, אך משמרות המהפכה הכחישו זאת נחרצות וקבעו כי היה תוצאה של "תאונה מוזרה".[49] למרות הערפול הרב סביב האירוע, לא ניתן לפסול את ההשערה כי למותו של אחמדי היו השלכות על פעילות הארגון בזירת הסייבר.

מערך שליחים ללוחמת סייבר

לצד חיזוק מערך הסייבר המדינתי ושיתוף הפעולה עם קהילת ההאקרים באיראן, מתעצמים הניסיונות האיראניים להרחיב ולחזק את יכולות לוחמת הסייבר בהן מחזיקות בעלות בריתה. נראה כי איראן מבקשת לייצר מערך יעיל של שליחים הפועלים עבורה במרחב הסייבר. אחד ממרכזי הכובד של פעילות איראנית זו הוא הזירה הסורית, שלה משמעות אסטרטגית עבור איראן. עם תחילת העימותים בין משטר אסד לבין כוחות המורדים, החלו האיראנים לממן, לצייד ולאמן את כוחות הביטחון הסוריים באמצעי ניטור ושליטה על מרחב הסייבר ששימש כפלטפורמה מרכזית למורדים לארגון הפעילות נגד המשטר. יועצים ומומחים איראניים אימנו וחיזקו את משטרת הסייבר הסורית וסייעו לה לעקוב אחר רשתות המחשבים והסלולר במדינה ולפגוע ביכולתם של המורדים להעביר מסרים ומידע הן בתוך המדינה והן אל מחוץ לה.[50]

שחקן מרכזי בהקשר זה הוא "צבא סוריה האלקטרוני" (Syrian Electronic Army – SEA). קבוצה זו של האקרים תומכי אסד החלה לפעול ב־2011, ובמהלך השנה הראשונה לפעילותה ביצעה בעיקר מתקפות "ונדליזם" חובבניות יחסית נגד אתרים בעלי רמת אבטחה נמוכה, שתקיפתם אינה דורשת יכולת טכנית גבוהה: מתקפות spam, הצפת מערכות הטוקבק של פורומים ואתרי חדשות שונים וכדומה.[51] במהלך 2012 החל SEA להוציא אל הפועל פעילויות מורכבות יותר נגד אתרים בעלי רמת אבטחה המחייבת ידע טכני ויכולות גבוהות יחסית. מומחי סייבר ואנשי ממשל מערביים מיחסים קפיצת מדרגה זו למעורבותם והדרכתם של מומחי לוחמת סייבר איראניים, אשר מאמנים ומציידים את פעילי הארגון. מייקל היידן, שעמד בעבר בראש ה־CIA וה־NSA, אף קבע כי קבוצת ההאקרים הסורית הינה שליח איראני לכל דבר ועניין.[52]

התפתחותו של SEA באה לידי ביטוי בשנה האחרונה בגל מתקפות נגד אתרים של גורמי תקשורת וארגוני זכויות אדם, אותם הוא תופס כעוינים למשטר אסד. בין השאר, תקפו חברי SEA אתרי חדשות מובילים ביניהם "ניו יורק טיימס", BBC, "אל־ג'זירה", "וושינגטון פוסט" ו־The Huffington Post. כמו כן תקף הארגון את אתר Human Rights Watch המספק מידע על מספר האזרחים שנפגעו בקרבות בסוריה. חברי הארגון אף הצליחו להסב נזק משמעותי כאשר השתלטו על חשבון ה"טוויטר" של סוכנות הידיעות AP ופרסמו ידיעה כוזבת בדבר מתקפה כביכול על הבית הלבן ופגיעה בנשיא אובמה. הידיעה יצרה פאניקה מיידית בוול סטריט והביאה לצניחת מניות ולנזק שהוערך ב־136 מיליארד דולר. באפריל 2013 קיבל SEA על עצמו אחריות להפלת שרתי הרשת החברתית "טוויטר" ולהפניית הגולשים באתר הגיוס של חיל המארינס לאתר תעמולה נגד המורדים.[53]

לאחרונה נראה כי SEA עשה קפיצת מדרגה נוספת ביכולותיו ומתחיל להפעיל טכניקות וכלי תקיפה מתוחכמים יותר, כגון דיוג, תוכנות זדוניות ו"סוסים טרויאניים". כלים אלה אפשרו לארגון להוציא אל הפועל התקפות איכותיות נגד שרתים של חברות תקשורת אינטרנט, כגון אינדקס הטלפונים הגדול בעולם TrueCaller, שירות ההודעות והווידיאו Tango, ואפליקציית התקשורת Viber. במהלך מתקפות אלו הצליחו התוקפים לגנוב כמויות עצומות של מידע, כגון פרטי אנשים וכתובות מייל, אשר ייתכן מאד שהועברו לידי המודיעין הסורי ושימשו לפעילות נגד מתנגדי המשטר ולריגול.[54] סוכנות הידיעות האיראנית Fars אף דווחה כי הארגון תקף את מערכת המים של העיר חיפה,[55] אולם התמונות שצורפו לידיעה הראו ש־SEA חדר אך ורק למערכת בקרת ההשקיה של אחד מיישובי הצפון בישראל.[56] עם זאת, התקיפה והחדירה למערכת הבקרה של תשתית ישראלית מצביעות על ניסיון של SEA להתרחב גם לשיטות ומטרות מתקדמת יותר של לוחמת סייבר.

יכולות מתקדמות אלו, אשר מומחים רבים רואים אותן כתוצר של אימון, הכוונה וסיוע איראניים, הפכו את SEA לגורם משמעותי במרחב הסייבר, ואת לוחמת הסייבר בכלל למרכיב משמעותי באסטרטגיית ההרתעה הסורית. כשסוריה ביקשה למנוע תקיפה אמריקאית, בתגובה לשימוש של כוחות אסד בנשק כימי, שלחו אנשי SEA הודעה לסוכנות "רויטרס" כי במקרה של תקיפה אמריקאית בסוריה, הארגון יסלים את מתקפותיו ויפעל נגד מטרות משמעותיות יותר. ריצ'רד קלארק, יועץ הבית הלבן לשעבר לנושאי אבטחת סייבר ולוחמה בטרור, העריך כי במקרה של מתקפה אמריקאית על סוריה, כל תגובה של גורמים סוריים במרחב הסייבר תתבצע בסיוע גורמים איראניים.[57]

בנוסף לתמיכה ביכולות הסייבר של משטר אסד, ממשיכה איראן את תמיכתה המסורתית במערך הסייבר של בעל בריתה וחסותה הקרוב, חזבאללה, שהפך

לשחקן פעיל בתקיפת ישראל.[58] דו"ח של מרכז מאיר עמית מצביע על מעורבות ותמיכה עמוקות של איראן במערך אתרי האינטרנט של חזבאללה. מערך זה מהווה פלטפורמה לתעמולה ולאינדוקטרינציה של רעיונות המהפכה האסלאמית וכולל תעמולה פרו־איראנית, פולחן אישיות של המנהיג העליון ח'מנהאי ושל מנהיג חזבאללה חסן נסראללה, ותעמולה אנטי־ישראלית ואנטישמית. התוכן באתרים אלה נקבע בשיתוף עם איראן ובכפוף לאסטרטגיית התעמולה האיראנית וחלק מהם אף מופעלים מתוך שטחה של איראן על ידי מקורבים לשלטון.[59]

תובנות מסכמות

יכולות לוחמת הסייבר של איראן מתקדמות באופן עקבי וכבר היום היא מהווה גורם משמעותי שאין לזלזל בכוונותיו. ניתן להעריך שההחלטה האיראנית לפעול באופן נרחב במרחב הסייבר נובעת משני מניעים עיקריים: הראשון נוגע לעובדה שאיראן ספגה מתקפות סייבר חמורות. כמי שחוותה על בשרה את העוצמה והיכולות של תקיפה בתווך הקיברנטי, היא מכירה בחשיבות ההקמה של יכולות הגנה, לצד בנייה והפעלה של יכולות תקיפה. המניע השני של איראן נוגע להתפתחות הטכנולוגית העולמית, וכנגזר מכך האיראנית, המאפשרת להרחיב את תמהיל הפעולה גם למרחב הקיברנטי ולא רק לזה הפיזי. התפתחות זו משתלבת בצורה מיטבית עם תפיסת האסטרטגיה האסימטרית של איראן.

ניתוח מתקפות הסייבר המיוחסות לאיראן ושלוחותיה מצביע על מגוון רחב של מטרות, יעדים ושיטות פעולה. אחת המסקנות העולות ממאמר זה היא, שבתקופה האחרונה הבשילו יכולות הסייבר של איראן הן במרחב ההגנתי והן במרחב ההתקפי. על אף שנדמה שיכולות אלו עדיין נחותות ביחס ליכולות הסייבר של מעצמות טכנולוגיות מובילות, נראה שהאיראנים מגשרים על הפערים במהירות וביעילות.

אחת המגמות המסוכנות ביותר בפעילות הסייבר ההתקפית של איראן היא פעולה נגד מערכות הליבה המבצעיות של ארגונים ומדינות. מערכות אלו, השולטות בתהליכי ייצור, אספקה ושירותים חיוניים ומבקרות אותם, עלולות להיות מטרה לתקיפה איראנית. פעולות הגישוש, הסריקה והלמידה שהתגלו במערכות המחשוב של חברות אנרגיה אמריקאיות ויוחסו לגורמים איראניים, ניתנות רק לפרשנות אחת: איראן מנסה ליצור יכולת ונגישות לתשתיות קריטיות. נגישות כזאת עלולה לא להתגלות כלל, ותוכל להיות מופעלת בעתיד לצרכים התקפיים לפי החלטה איראנית. מתקפה מוצלחת על מערכות בקרה של מתקני אנרגיה, גז ומים עשויה לגרום לנזק משמעותי. ניתן לכאורה לקבל, במסגרת כללי המשחק, פעולות של ריגול וגניבת מידע במרחב הסייבר, אך לא ניתן ואין להסכים

כלל להשלמה עם ניסיונות חדירה למערכות בקרה של מתקני תשתית אזרחיים. ניסיונות כאלה מחייבים תגובה חריפה.

נדמה שההבנה שאיראן מהווה איום משמעותי על יריבותיה במרחב הסייבר כבר מניעה שיתוף פעולה הדוק בין מדינות המאוימות על ידי יכולות אלו. אולם אין להסתפק אך ורק בשדרוג המודיעין והעמקת יכולות ההגנה; אלה לעולם לא יספיקו מול יריב נחוש ובעל יכולות מבצעיות, מודיעיניות וטכנולוגיות. מרחב הסייבר מאפשר מִנעד רחב של פעולות להעברת מסרים באמצעותו, מתחת לסף של מלחמה פיזית. פעולות אלו ידרשו להדגים את הנזק שייגרם לאיראן אם תמשיך לפעול ללא ריסון נגד מטרות רגישות. לאחרונה פורסמו פרטים על מבצע לתקיפת סייבר רחבת היקף בסוריה שהוכן על ידי ה־NSA באביב 2011, סמוך לפרוץ מלחמת האזרחים במדינה.[60] אם דיווח זה נכון, הרי שהכנת מהלומה קיברנטית נגד איראן, לצד הדגמה מעת לעת של יכולות איכותיות, יוכלו לסייע לרסן את פעולתה במרחב התשתיות הקריטיות.

עד שתימצא נוסחת הפלא הטכנולוגית לזהות ברמה גבוהה של ודאות הניתנת להוכחה משפטית את מקור התוקפים במרחב הסייבר, ניתן במקרים לא מעטים להסתפק גם בעדויות נסיבתיות באשר למקור התקיפה, ולפעול מול מקור זה בחריפות במרחב הסייבר, מתחת לסף מלחמה פיזית.

מעל כל אלה, העמקת שיתוף הפעולה בין המדינות הדמוקרטיות היא אבן יסוד בהתמודדות עם איראן ושלוחותיה. שיפור הקשר המבצעי, המודיעיני והטכנולוגי הינו חיוני. כך גם שיפור שיתוף הידע באשר לשיטות וכלים בהם עושים איראן ושלוחיה שימוש. בנוסף לכך, ישראל עשויה למצוא בעלי ברית נגד מלחמת הסייבר האיראנית גם בקרב המשטרים הסוניים באזור המפרץ, ובראשם הממלכה הסעודית, המאוימים באופן קבוע ואף נפגעו בעבר בידי גורמים איראניים. תחום הגנת הסייבר, שישראל היא שחקן מוביל בו, עשוי לשמש כבסיס ליצירת דו־שיח אסטרטגי פורה בסוגיות אזוריות נרחבות יותר, כגון האיום האיראני במובנו הכולל, המשבר בסוריה והסוגיה הפלסטינית.

התנהלותו התוקפנית של מערך הסייבר האיראני מבליטה את אופיו הטוטליטרי של המשטר באיראן. הפיקוח ההדוק והחודרני, הפוגע בחופש הביטוי והדיבור של אזרחי איראן, לצד האלימות והאגרסיביות המאפיינות את פעילותם של גופים כמו משטרת הסייבר, מהווים תמונת מראה לתדמית אותה מבקש לקדם משטר רוחאני במטרה לסדוק את משטר הסנקציות הבין־לאומי על איראן. ישראל ומדינות נוספות יכולות להשתמש בפעילותה של איראן במרחב הסייבר כפלטפורמה הסברתית המבליטה את אופייה הטוטליטרי והתוקפני של הרפובליקה האסלאמית.

מציאות זו, של ההתפתחות המהירה ביכולת לוחמת הסייבר של איראן ושל שלוחיה ובעלי בריתה, מחייבת את ישראל, כמו גם מדינות מערביות אחרות, לפעול

באופן נחרץ ושיטתי לשימור עליונותן האיכותית והמבצעית במרחב הסייבר. חשיבותו של מרחב זה לתפיסת הביטחון הישראלית, והדחיפות שביצירת "כיפת ברזל" דיגיטלית, הודגשו היטב בדבריו של רמטכ"ל צה"ל, רב־אלוף בני גנץ: "ישראל חייבת להיות ברמה המעצמתית בסייבר... אין לחכות עם הסיפור הזה".[61]

הערות

1 Barbara Slavin and Jason Healey, *Iran: How a Third Tier Cyber Power Can Still Threaten the United States*, The Atlantic Council, 2013, http://www.atlanticcouncil.org/images/publications/iran_third_tier_cyber_power.pdf.

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

3 Gabi Siboni and Sami Kronenfeld, "Iran and Cyberspace Warfare", *Military and Strategic Affairs*, Vol. 4, No. 3 (Dec. 2012), pp. 77-99.

4 שם.

5 Majid Rafizadeh, "Iran's 'Halal' Version of the Internet", *Al-Arabiya News*, July 12, 2013, http://english.alarabiya.net/view-renderer?mgnlUuid=cb92c5e3-f973-45ce-8d46-12b8fb4dfe17.

6 Sara Reardon, "First Evidence for Iran's Parallel Halal Internet", *New Scientist*, October 10, 2012, http://www.newscientist.com/article/mg21628865.700-first-evidence-for-irans-parallel-halal-internet.html#.UnZubT4UHVI

7 Saeed Kamali Dehghan, "Iran Launches 'National Email Service'", *The Guardian*, July 9, 2013, http://www.theguardian.com/world/2013/jul/09/iran-launches-national-email-service

8 "Iran launches own 'YouTube' website", *AFP*, December 9, 2012, http://en-maktoob.news.yahoo.com/iran-launches-own-youtube-website-121634740.html

9 Trend F. Karimov, "Iran Introduces Domestically-made Antivirus Padvish", *Trend News Agency*, June 30, 2013, http://en.trend.az/capital/it/2166121.html /

10 חסימה זו התבצעה בין השאר באמצעות הפצה מתוכננת של תוכנות זדוניות שהוסוו כתוכנות עוקפות סינון, דבר שאִפשר למשטר להתחקות אחר רשתות בלתי חוקיות.

11 Urt Hopkins, "Why Iranians might Actually Use the Censored "Halal Internet", *The Daily Dot*, April 25, 2013, http://www.dailydot.com/society/iran-halal-private-internet-blocked-censorship; Small Media, *Iranian Internet Infrastructure and Policy Report*, February-March 2013, http://smallmedia.org.uk/InfoFlowReportMARCH.pdf.

12 "Iran Unveils 12 Cyber Products", *Fars News*, December 14, 2013, http://english.farsnews.com/newstext.aspx?nn=13920923001322.

13 "Iran Launches Home-made Defense Shield", *ISNA*, December 9, 2013, http://isna.ir/en/news/92091812343/Iran-launches-home-made-defense-shield /

14 Alastair Stevenson, "Iran and North Korea Sign Technology Treaty to Combat Hostile Malware", *V3*, September 3, 2012, http://www.v3.co.uk/v3-uk/news/2202493/iran-and-north-korea-sign-technology-treaty-to-combat-hostile-malware#.

15 Steve Stecklow, "Chinese Firm Helps Iran Spy on Citizens", *Reuters*, March 22, 2012, http://graphics.thomsonreuters.com/12/03/IranChina.pdf.

16 "Iran for the First Time Stages Cyber Warfare Drill", *Al-Arabiya*, December 31, 2012, http://www.alarabiya.net/articles/2012/12/31/257960.html.

17 "Drones, Cyber-Defense Feature in Iran Guards Drill", *The Jerusalem Post*, February 23, 2013, http://www.jpost.com/Iranian-Threat/News/Drones-cyber-defense-feature-in-Iran-Guards-drill.

18 "Iran Holds Defense Exercises", *Trend*, October 22, 2013, http://en.trend.az/news/politics/2203465.html; "Iran Carries Out Drills to Detect Cyber Vulnerabilities", *Tasnim News Agency*, October 22, 2013, http://www.tasnimnews.com/english/Home/Single/172473.

19 "Iranian Blogger who Told Supreme Leader Khamenei 'Your Judicial System... is nothing but a Slaughterhouse' Tortured to Death in Prison", *MEMRI*, November 19, 2012, http://www.memri.org/report/en/0/0/0/0/0/0/6819.htm.

20 European Parliament Resolution of November 22, 2012 on the Human Rights Situation in Iran, Particularly Mass Executions and the Recent Death of the Blogger Sattar Beheshti, *The European Parliament*, November 22, 2012, http://www.europarl.europa.eu/document/activities/cont/201301/20130109ATT58696/20130109ATT58696EN.pdf.

21 Thomas Erdbrink, "Head of Tehran's Cybercrimes Unit is Fired over Death of Blogger", *The New York Times*, December 1, 2012, http://www.nytimes.com/2012/12/02/world/middleeast/after-death-of-sattar-beheshti-iranian-blogger-head-of-tehrans-cybercrimes-unit-is-fired.html.

22 "Intelligence Ministry Admits Arresting News Providers, Blames Foreign Media", *Reporters Without Borders*, February 20, 2013, http://en.rsf.org/iran-intelligence-ministry-admits-20-02-2013,44099.html; "Iran: Two Arrested for 'Insulting Regime Officials' on their Facebook Page", *National Council of Resistance of Iran*, July 10, 2013, http://www.ncr-iran.org/en/news/human-rights/14138-iran-two-arrested-for-insulting-regime-officials-on-their-facebook-pa.

23 "Tehran Closes Dozens of Internet Cafes", *Mohabat News*, July 27, 2013, http://www.mohabatnews.com/index.php?option=com_content&view=article&id=7222:tehran-closes-dozens-of-internet-cafes&catid=35:inside-iran&Itemid=278.

24 Eric Grosse, "Iranian Phishing on the Rise as Elections Approach", *Google Blog*, June 12, 2013, http://googleonlinesecurity.blogspot.co.il/2013/06/iranian-phishing-on-rise-as-elections.html.

25 Siboni and Kronenfeld, "Iran and Cyberspace Warfare", 2012.

26 Betsy Isaacson, "Iran's Pre-Election Phishing Scheme Detected, Disrupted by Google", *The Huffington Post*, June 13, 2013, http://www.huffingtonpost.com/2013/06/13/iran-phishing-google_n_3435811.html.

27 "Iranian Authorities Target Internet, Media before Elections", *CPJ*, June 13, 2013, http://www.cpj.org/2013/06/iranian-authorities-target-internet-media-before-e.php; Helle Dale, "Iran Clamps down on Dissidents before Election", *The Foundry*, June 12, 2013, http://blog.heritage.org/2013/06/12/iran-clamps-down-on-dissidents-before-election.

28 Neal Ungerleider, "Iran's 'Halal Internet' is really a 'Filternet'", *Fast Company*,

2013, http://www.fastcompany.com/3009714/irans-halal-internet-is-really-a-filternet.

29 Thom Shanker & David E. Sanger, "U.S. Helps Allies Trying to Battle Iranian Hackers", *New York Times*, June 8, 2013, http://www.nytimes.com/2013/06/09/world/middleeast/us-helps-allies-trying-to-battle-iranian-hackers.html?nl=todayspheadlines&emc=edit_th_20130609&_r=4&pagewanted=all&

30 Siboni and Kronenfeld, "Iran and Cyberspace Warfare".

31 Frank J. Cilluffo, *The Iranian Cyber Threat to the United States*, *A Statement before the U.S. 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. 5.

32 http://www.zone-h.org/stats/notifierspecial.

33 "Brazilian Military Police & 26 Govt Websites Hacked by Ashiyane Digital Security Team", *Hackread*, January 28, 2013, http://hackread.com/brazilian-military-police-26-govt-websites-hacked-by-ashiyane-digital-security-team.

34 Nart Villeneuve, Ned Moran, Thoufique Haq and Mike Scott, "Operation Saffron Rose", Fire-eye, 2014.

35 Julian E. Barnes and Siobhan Gorman, "U.S. Says Iran Hacked Navy Computers ", *The Wall Street Journal*, September 27, 2013, http://online.wsj.com/news/articles/SB10001424052702304526204579101602356751772; Adam Kredo, Mike Rogers, "China, Iran and Russia Launching Cyber Attacks Against U.S.", *The Washington Free Beacon*, July 22, 2013, http://freebeacon.com/mike-rogers-china-iran-and-russia-launching-cyber-attacks-against-u-s.

36 Shanker and Sanger, "U.S. Helps Allies Trying to Battle Iranian Hackers".

37 Nicole Perlroth and Quentin Hardy, "Bank Hacking Was the Work of Iranians, Officials Say", *The New York Times*, January 8, 2013, http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html?pagewanted=1&_r=1&ref=iran&&version=meter+at+6&region=FixedCenter&pgtype=Article&priority=true&module=RegiWall-Regi&action=click.

38 שם.

39 Julian E. Barnes and Siobhan Gorman, "Iran Blamed for Cyberattacks ", *The Wall Street Journal*, September 27, 2013, http://news.walla.co.il/?w=/15/2569449.
"איראן שיגרה מתקפת סייבר עוצמתית על בנקים בארה"ב", **וואלה**, 9 בינואר 2013, http://news.walla.co.il/?w=//2605254.

40 Ellen Nakashima, "U.S. Warns Industry of Heightened Risk of Cyber Attack", *The Washington Post*, May 10, 2013, http://www.washingtonpost.com/world/national-security/us-warns-industry-of-heightened-risk-of-cyberattack/2013/05/09/39a04852-b8df-11e2-aa9e-a02b765ff0ea_story.html;
ראו בנוסף ניתוח על היכולות הנדרשות לצורך ביצוע מתקפת סייבר ברמה גבוהה: גבי סיבוני, דניאל כהן ואביב רוטברט, "איום ארגוני הטרור במרחב הסייבר", **צבא ואסטרטגיה**, כרך 5, גיליון 3, המכון למחקרי ביטחון לאומי, דצמבר 2013, http://d26e8pvoto2x3r.cloudfront.net/uploadImages/systemFiles/pdf;
Nicole Perlroth & David E. Sanger, "New Computer Attacks Traced to Iran, Officials Say", *The New York Times*, May 24, 2013, http://www.nytimes.com/2013/05/25/world/middleeast/new-computer-attacks-come-

from-iran-officials-say.html?_r=1&.

41 לעת כתיבת מאמר זה מתנהל משא ומתן בין איראן למעצמות בנושא הגרעין. אין לשלול את האפשרות שעיצומי האנרגיה יחוזקו במידה ושיחות אלה יעלו על שרטון.

42 Siobhan Gorman & Danny Yadron, "Iran Hacks Energy Firms, U.S. Says", *The Wall Street Journal*, May 23, 2013, http://online.wsj.com/news/articles/SB10001424127887323336104578501601108021968.

43 Chris Strohm, "Iran-Based Hackers Traced to Cyber Attack on U.S. Company", *Bloomberg News*, May 14, 2013, http://www.businessweek.com/news/2013-05-14/iran-based-hackers-traced-to-cyber-attack-on-company-inside-u-dot-s-dot.

44 Shanker and Sanger, "U.S. Helps Allies Trying to Battle Iranian Hackers".

45 Barnes and Gorman, "U.S. Says Iran Hacked Navy Computers".

46 Gili Cohen, "Netanyahu Confirms: U.S. is Working with Israel on Cyber Defense, Iranian Attacks Increasing", *Ha'aretz*, June 9, 2013, http://www.haaretz.com/news/diplomacy-defense/.premium-1.528728.

47 "Israel's Aviation Agency Under Muslim Hackers' Control for Months", *Fars News*, January 8, 2013, http://english.farsnews.com/newstext.aspx?nn=13921018001457.

48 "Saudi Army, Al-Qaeda Company, Israeli Army Hacked in Revenge for Assassination of Hezbollah Leader", *Fars News*, December 16, 2013, http://english.farsnews.com/newstext.aspx?nn=13920925001699.

49 Damien McElroy and Ahmad Vahdat, "Iranian Cyber Warfare Commander Shot Dead in Suspected Assassination", *The Telegraph*, October 2, 2013, http://www.telegraph.co.uk/news/worldnews/middleeast/iran/10350285/Iranian-cyber-warfare-commander-shot-dead-in-suspected-assassination.html; Lisa Daftari, "Internal Plot, not Israel, Eyed in Latest Hit on Iranian Scientist", *Fox News*, October 8, 2013, http://www.foxnews.com/world/2013/10/08/internal-intrigue-not-israel-eyed-in-latest-hit-on-iranian-scientist.

50 Simon Tisdall, "Iran Helping Syrian Regime Crack down on Protesters, say Diplomats", *The Guardian*, May 9, 2011, http://www.theguardian.com/world/2011/may/08/iran-helping-syrian-regime-protesters; Lisa Daftari, "Iranian General Admits 'Fighting every Aspect of a War' in Defending Syria's Assad", *Fox News*, August 28, 2012, http://www.foxnews.com/world/2012/08/28/iranian-general-admits-fighting-every-aspect-war-in-defending-syria-assad; Geneive Abdo, "How Iran Keeps Assad in Power in Syria", *Foreign Affairs*, August 25, 2011, http://www.foreignaffairs.com/articles/68230/geneive-abdo/how-iran-keeps-assad-in-power-in-syria.

51 Ronald Deibert, "Waging the Cyber War in Syria", *National Post*, May 21, 2013, http://fullcomment.nationalpost.com/2013/05/21/ronald-deibert-waging-the-cyber-war-in-syria.

52 Joseph Menn, "Syria, Aided by Iran, could Strike back at U.S. in Cyberspace", *Reuters*, August 29, 2013, www.reuters.com/article/2013/08/29/us-syria-crisis-cyberspace-analysis-idUSBRE97S04Z20130829.

53 Sarah Hurtubise, "Syrian Hacker Army could be Advancing with Iranian Help", *The Daily Caller*, April 9, 2013, http://dailycaller.com/2013/09/04/syrian-hacker-army-could-be-advancing-with-iranian-help; Andrea Peterson, "The Post Just Got Hacked

by the Syrian Electronic Army. Here's Who they Are", *The Washington Post*, August 15, 2013, http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/15/the-post-just-got-hacked-by-the-syrian-electronic-army-heres-who-they-are.

54 Kenneth Geers and Ayed Alqartah, "Syrian Electronic Army Hacks Major Communications Websites", *FireEye*, July 30, 2013, http://www.fireeye.com/blog/technical/cyber-exploits/2013/07/syrian-electronic-army-hacks-major-communications-websites.html.

55 "Syrian Electronic Army Reveals Documents of Haifa Hack", *Fars News Agency*, June 15, 2013, http://english2.farsnews.com/newstext.php?nn=9203180050.

56 Elad Salomons, "Did the Syrian Electronic Army Attack Haifa's Water Supply SCADA System?", *Water Simulation*, June 5, 2013, http://www.water-simulation.com/wsp/2013/06/05/did-the-syrian-electronic-army-attack-haifas-water-supply-scada-system.

57 Menn, "Syria, Aided by Iran, could Strike back at U.S. in Cyberspace".

58 Olivia Goldhill and Reuters, "Benjamin Netanyahu: Iranian Cyber Attacks on Israel 'Non-Stop'", *The Telegraph*, June 10, 2013, http://www.telegraph.co.uk/technology/10110381/Benjamin-Netanyahu-Iranian-cyber-attacks-on-Israel-non-stop.html.

59 *Terrorism in Cyberspace: Hezbollah's Internet Network***,** The Meir Amit Intelligence and Terrorism Information Center, 2013, http://www.terrorism-info.org.il/en/article/20488.

60 David E. Sanger, "Syria War Stirs New U.S. Debate on Cyberattacks", *The New York Times*, February 24, 2014, http://www.nytimes.com/2014/02/25/world/middleeast/obama-worried-about-effects-of-waging-cyberwar-in-syria.html?hp&_r=2.

61 Amos Harel & Gili Cohen, "2014: Iran out, Global Jihad in", *Ha'aretz*, February 1, 2014, http://d26e8pvoto2x3r.cloudfront.net/uploadimages/systemfiles/iran%20out,%20global%20jihad%20in.pdf.

האם נשק סייבר משפיע על כלים צבאיים?

אמיליו אייזלו

מתקפות סייבר נתפסות בכתיבה הצבאית והאקדמית, לרוב, כנשק אסטרטגי אסימטרי וככלי שיש לו פוטנציאל ליצירת שוויון במערכה בין מדינות חזקות למדינות חלשות יותר. עם זאת, אין עדויות רבות לכך שמתקפות סייבר הן אופציה צבאית ממשית בעימות בין מדינות. במקומות שבהם התנהלו מבצעים צבאיים של ממש (כמו אפגניסטן, גיאורגיה, עיראק או ישראל ורצועת עזה), יש מעט מאוד עדויות לצבא המבַצע מתקפות סייבר נגד מטרה צבאית או אזרחית. זוהי עובדה מעניינת, לאור ההנחה שחלק מהמדינות שהיו מעורבות בעימות צבאי או במשימות לשמירת השלום באזורים עוינים מחזיקות ברמה מסוימת של יכולת סייבר התקפית. מאמר זה מבקש להציג טיעון נגדי לרעיון שכלי סייבר הם נשק צבאי אינסטרומנטלי בלוחמה של העידן המודרני. המאמר ייטען כי נשק סייבר הוא אופציה אפקטיבית בזמנים של מתיחות בין מדינות יותר מאשר בעימות צבאי, ואמצעי יעיל לאיתות מסרים יותר מאשר ככלי להשגת יתרון צבאי.

מילות מפתח: התקפת סייבר, נשקי סייבר, לוחמת מידע, סין, רוסיה, ארצות הברית.

מבוא

מתקפות סייבר נתפסות בכתיבה הצבאית והאקדמית, לרוב, כנשק אסטרטגי אסימטרי וככלי שיש לו פוטנציאל ליצירת שוויון במערכה בין מדינות חזקות למדינות חלשות יותר. עם זאת, אין עדויות רבות לכך שמתקפות סייבר הן

אמיליו אייזלו (Emilio Iasiello) צבר מעל 12 שנות ניסיון כחוקר מודיעין סייבר אסטרטגי. הוא מייעץ לארגוני מודיעין צבאיים ואזרחיים של ממשלת ארצות הברית, כמו גם לחברות במגזר הפרטי המספקות מודיעין סייבר.

מאמר זה ראה אור לראשונה ב**צבא ואסטרטגיה**, כרך 7, גיליון 1, מארס 2015, עמ׳ 21-37.

אופציה צבאית ממשית בעימות בין מדינות. במקומות שבהם התנהלו מבצעים צבאיים של ממש (כמו אפגניסטן, גיאורגיה, עיראק או ישראל ורצועת עזה), יש מעט מאוד עדויות לצבא המבַצע מתקפות סייבר נגד מטרה צבאית או אזרחית. זוהי עובדה מעניינת, לאור ההנחה שחלק מהמדינות שהיו מעורבות בעימות צבאי או במשימות לשמירת השלום באזורים עוינים מחזיקות ברמה מסוימת של יכולת סייבר התקפית. דוגמאות מובהקות יותר מראות כי מתקפות סייבר יעילות יותר במסגרת פעילות לא צבאית, וזאת כנשק סודי המאפשר לשתק מערכות ללא סימנים מוקדמים, וככזה שיש ביכולתו להסתיר את הזהות האמיתית של מי שעומד מאחוריו – באמצעות שימוש ב"ארגוני שליח" (proxy) והישענות על יכולת הכחשה סבירה (plausible deniability).

מאמר זה מבקש להציג טיעון נגדי לרעיון שכלי סייבר הם נשק צבאי אינסטרומנטלי בלוחמה של העידן המודרני. במקום זאת אטען במאמר שנשק סייבר הוא אופציה אפקטיבית בזמנים של מתיחות בין מדינות יותר מאשר בעימות צבאי, ואמצעי יעיל לאיתות מסרים יותר מאשר ככלי להשגת יתרון צבאי. במצבים של עימות בין מדינות, סביר יותר להניח שנטרול המטרות החשובות של היריב ייעשה באמצעות נשק קונבנציונלי, המאפשר לכמת ביתר קלות את מידת הנזק בקרב. השאלה היא, לפיכך, האם נשק סייבר הוא כלי צבאי אפקטיבי?

מינוח

אין קונצנזוס בין־לאומי סביב הגדרת המונחים "מתקפת סייבר" (cyber attack) ו"נשק סייבר" (cyber weapon). עם זאת, קיימת הסכמה כי מונחים אלה פירושם שיגור נוזקה (malware) מתוך כוונה למנוע, לשבש, לפגוע, להרוס או לבצע מניפולציה במערכות מידע או במידע השמור בהן. לצורך המאמר הנוכחי אומצו ההגדרות שלהלן:

- **מתקפת סייבר**: "פעולות המתבצעות באמצעות רשתות מחשב ומיועדות למנוע גישה אל מערכת מידע, רשת מידע או נתונים שנמצאים בהן, לפגוע בהן, ולשבש או להרוס אותן".
- **נשק סייבר**: "קוד מחשב שמשַמש, או מיועד לשמש, לאיום או לגרימת נזק פיזי, תפקודי או מנטלי למבנים, מערכות או יצורים חיים".[1] דוגמאות לכך כוללות מתקפות של מניעת שירות מבוזרת (DDoS), או החדרת נוזקה המיועדת להרוס מערכות מידע או את המידע השמור בהן.

סייבר כנשק אסימטרי

הכתיבה הצבאית על לוחמת סייבר – נושא משנה בתוך נושא העל של "לוחמת מידע" – נוטה לראות בתשתיות קריטיות יעדים מרכזיים לפעולה צבאית במהלך

עימות, שכן תשתיות כאלו נתפסות כמאפשרות את היכולת הצבאית של המדינה. המשרד לביטחון המולדת של ארצות הברית מגדיר תשתית קריטית באופן הבא: "הנכסים, המערכות והרשתות, בין אם פיזיים או וירטואליים, שהם כה חיוניים לארצות הברית, עד שלהשבתה או להרס שלהם יהיה אפקט הרסני על הביטחון, ביטחון הכלכלה הלאומית, בריאות ובטיחות הציבור או כל שילוב של אלה".[2]

מתקפות סייבר בסביבת מידע הן זירה חשובה להקרנת כוח, במיוחד נגד מטרות רכות כמו מערכות תקשורת, נמלים, שדות תעופה, אזורי היערכות, אוכלוסייה אזרחית, תשתית קריטית ומרכזים כלכליים. בהקשר זה, נשק סייבר הוא התגלמות אידיאלית של אסטרטגיה אסימטרית: ככל שתשתית המידע של מעצמה נהנית מתחכום טכני רב יותר, כך היא פגיעה יותר למתקפות סייבר.

הכתיבה על לוחמת מידע במדינות השונות

העיקרון הבסיסי של אסטרטגיה אסימטרית הוא להפוך את מה שנתפס כעוצמתו של האויב לנקודת התורפה שלו. קרוב לוודאי שאין עוד תחום הממחיש זאת כמו תחום הסייבר, שבו מורכבות התוכנה והחומרה מגבירה את האפקטיביות הצבאית והחברתית מצד אחד, אך מהווה נקודת תורפה שניתן לנצלה לרעה מצד שני.

תיאורטיקנים אקדמאיים וצבאיים עוסקים במלחמת מידע מזה שנים רבות. האזכור המוקדם ביותר ללוחמת מידע בארצות הברית היה של ד"ר טום רונה (Rona) – בשנות השבעים של המאה העשרים.[3] האימוץ הצבאי הראשון של המונח היה ב־1992, כאשר משרד ההגנה של ארצות הברית פרסם הגדרה רשמית של לוחמת מידע במסמך המדיניות המסווג שלו – TS3600.1.[4] במהלך השנים עדכן הצבא האמריקאי את ההגדרה, אולם המונח "לוחמת מידע" הפך לחלק מהלקסיקון שלו, גם אם לא היו עדיין אסטרטגיות רשמיות שהכתיבו כיצד ליישמו בעת מלחמה.

ארצות הברית לא הייתה היחידה במשימה של פיתוח חשיבה מתקדמת על טבעה של לוחמת המידע ובשאלה כיצד ניתן למנף אותה להשגת השפעה מרבית. תיאורטיקנים צבאיים של סין ורוסיה כתבו גם הם בהרחבה בנושא זה. כתיבתם הראשונית דמתה ברובה לדברים שפורסמו עוד קודם לכן, ואף על פי כן היו בה רעיונות חדשים לגבי האופן שבו לוחמת מידע יכולה לשמש בזמן מלחמה. חרף ניואנסים תרבותיים, שררה הסכמה לגבי הפוטנציאל של לוחמת מידע לשמש כנשק המגשר על הפער בין החזק לחלש ומספק לצד החלש אמצעים לתקוף את החזק, מבלי להסתכן בעימות חזיתי של כוח מול כוח. המונח "אסימטריות" מדגיש היטב מצב זה, כפי שניסחו זאת ברין וגלצר: "[הדבר] מזכיר במקצת את אמנות המלחמה היפנית של הג'יו ג'יטסו, המבוססת על הרעיון שניתן לגייס את כוחו ועוצמתו של היריב ככלי נגדו, במקום לתקוף אותו ישירות עם הכוח הקיים".[5]

שלא כמו נשק גרעיני, המחייב משאבים ניכרים ויכולת ייצור וניהול, מלחמת מידע והכלים הדרושים לה נגישים בקלות להמונים.

הכתיבה הסינית על לוחמת מידע

הכתיבה המוקדמת ביותר בנושא לוחמת מידע בסין הייתה, ככל הנראה, בספר "לוחמת מידע", שיצא לאור ב־1985 ופורסם מאוחר יותר כמאמר ב־*Liberation Army Daily*.[6] עם זאת, רק במבצע "סופה במדבר" בעיראק ב־1991 הזדמן לתיאורטיקנים סיניים לראות כיצד צבא עושה שימוש בטכנולוגיה מתקדמת כדי להביס את האויב. ב־1995 כתב רמטכ"ל צבא סין, וואנג פּוּ פֶנג, את "האתגר של לוחמת המידע", שבו כָּלל אזכורים רבים ללוחמת המידע של ארצות הברית במבצע נגד עיראק.[7] כותב סיני אחר ראה מערכה זו של ארצות הברית בעיראק כ"טרנספורמציה גדולה", שבה המידע שינה, יחד עם הפיקוד והשליטה, את פני שדה הקרב.[8] מאז ראו חוקרים סיניים ברעיון של "שליטה במידע" את המפתח להשגת ניצחון במלחמות העתיד.

שני מקורות סיניים העוסקים בדוקטרינות צבאיות – "מדע האסטרטגיה" ו"מדע המערכה הצבאית" – מכירים בלוחמת המידע ככלי צבאי חשוב להתגברות על יתרונות של יריב חזק יותר בתחומי הטכנולוגיה והמידע. אסטרטגים צבאיים רבי השפעה מבתי ספר ואקדמיות צבאיים מובילים בסין הציעו לצבא הסיני ליישם מתקפות סייבר או מתקפות של נשק מדויק נגד מטרות תשתית קריטיות, כמו נמלים ושדות תעופה. ואמנם, רבים מהמקורות שנוטים לגישה סמכותנית בחשיבה הצבאית בסין תומכים בסוג זה של פעולה. מחבר המחקר "מדע המערכה הצבאית" טוען כי לוחמת מידע אמורה לשמש:

> ... בזמן ובאזור שהם קריטיים לפעולת המערכה הכוללת, כדי לחסום את היכולת של האויב להשיג, לשלוט ולעשות שימוש במידע, במטרה להשפיע על היכולות של האויב לתצפת, לקבל החלטות או לפקד ולשלוט בחייליו, וכן להפחית ואף להרוס אותן. כל זאת, במקביל לשמירת יכולת הפיקוד והשליטה שלנו, כדי להחזיק בעליונות בתחום המידע ולהשיג עליונות מערכתית ואסטרטגית, וכך ליצור תנאים לניצחון מוחלט בקרב.

תיאוריית "הלוחמה האלקטרונית המשולבת ברשת" (Integrated Network Electronic Warfare – INEW) של סין כוללת מתקפה על רשת מחשבים בעתות מלחמה או שלום, וכן לוחמה אלקטרונית המתנהלת תחת סמכות אחת. המשימה היא לשבש את היכולת של היריב לעבד מידע ולהשתמש בו. האסטרטגיה הסינית מאופיינת ביישום משולב של כלים אינטרנטיים ונשק ללוחמה אלקטרונית נגד מערכות מידע של היריב, וזאת כבר בשלבים הראשונים של העימות.[9] על פי אותה אסטרטגיה, עוצמתן של מתקפות כאלו טמונה ביכולתן להפתיע את האויב.

בטקסט מעורר מחלוקת שחיברו שני קולונלים (לשעבר) בצבא סין, הם שמו את הדגש על הפוטנציאל שיש למתקפות סייבר לפגוע במוסדות פיננסיים של מעצמות זרות,[10] במיוחד כאופציה של מכה ראשונה. על פי ג'יימס מָלְבנון (Mulvenon), מומחה ידוע ללוחמת מידע סינית, "הכתיבה הצבאית הסינית נוטה ברובה להחזיק בדעה כי לוחמת מידע היא כלי לא קונבנציונלי, ולא מכפיל כוח בשדה הקרב [...] שיאפשר לסין להילחם ולזכות במלחמת מידע ללא צורך בפעולה צבאית".[11]

מלחמת מידע היא זירת קרב רחבה, ומרחב הסייבר הוא רק חלק אחד בעולם המידע הגדול יותר. מרחב המידע מתייחס ל"ספֵרת הפעילות הקשורה לעיצוב, יצירה, המרה, העברה, שימוש או אחסון של מידע, אשר יש לה השפעה על התודעה של היחיד והחברה, על תשתית המידע ועל המידע עצמו".[12] על פי השקפתה של סין, התפקיד העיקרי של מרחב המידע הוא "לאפשר לאנשים להשיג ולעבד נתונים [...], מישור חדש לתקשר עם אנשים ועם פעילויות. זהו המרחב המשלב בין כל רשתות התקשורת, מסדי הנתונים והמידע בעולם, היוצר סביבת פעולה".[13] מכאן עולה שסין רואה במרחב המידע טווח איום רחב יותר, המשתרע מעֵבר לעולם הדיגיטלי המוגבל לאינטרנט.

הכתיבה הרוסית על לוחמת מידע

בדומה לסין, גם רוסיה מתייחסת ל"מרחב המידע" כאל מונח הוליסטי. ב־2010 עדכנה ממשלת רוסיה את הדוקטרינה הצבאית שלה, לאחר שהמונח "לוחמת סייבר" בלט בהיעדרו ממנה (בדומה לסינים, גם הרוסים עושים שימוש במונח "מידע" ומעדיפים אותו על פני המונח הפופולרי יותר "סייבר"). עם זאת, היו בדוקטרינה הרוסית מספר אזכורים ל"לוחמת מידע", שעל פי הגדרתם כוללים מתקפות יזומות על מערכות מידע (כלומר, מחשבים) ו/או על המידע השמור בהן. חשוב מכך, הדוקטרינה הרוסית הכירה בכך שמרחב המידע הוא תחום קריטי המחייב הגנה צבאית מפני איומים חיצוניים. עובדה זו מחזקת את הנאמר ב"דוקטרינת ביטחון המידע 2000" של רוסיה, כי הגנה מפני מידע חיצוני מזיק וקידום ערכים פטריוטיים הם יעדים של הביטחון הלאומי.[14] יעדים נוספים מופיעים ב"דוקטרינה הצבאית 2010" של רוסיה וכוללים[15]: "[...] פיתוח מטרות ומשאבים ללוחמת מידע [...] יצירת מודלים חדשים של כלי נשק מדויקים ופיתוח תמיכה מבוססת מידע עבורם [...] יישום מקדים של אמצעים ללוחמת מידע, במטרה להשיג יעדים מדיניים מבלי להשתמש בכוחות צבאיים".

תיאוריית לוחמת המידע של רוסיה מעוגנת ברעיון לפיו היא חייבת "להגיב במלחמה למלחמת המידע שנפתחה נגדה",[16] ומכסה טווח רחב של פעולות, בין היתר מדיניות, כלכליות, תרבותיות וצבאיות. כותבים רוסיים רואים בלוחמת מידע מלחמה המשפיעה על תודעת ההמון, בהיותה חלק מהיריבויות בין המערכות

הלאומיות האזרחיות השונות שמדינות אימצו. אלו הופכות לרלוונטיות כאשר אמצעים מיוחדים מאפשרים להפוך מקורות מידע ל"נשק מידע".[17] גם רוסיה מגדירה "מרחב מידע" כ"מרחב הפעילות הקשורה לגיבוש, יצירה, המרה, העברה, שימוש או אחסון של מידע, אשר יש לה השפעה על התודעה של היחיד והחברה, על תשתית המידע ועל המידע עצמו".[18] לאור זאת, מה שמדאיג את רוסיה במרחב המידע הן ההשפעות הטכניות (כגון הרס פיזי של מערכת מידע) והפסיכולוגיות (דוגמת השפעה ומניפולציה על אוכלוסייה) על המרחב.

הפרשנות הרחבה של מרחב המידע מביאה את רוסיה לראות ב"נשק המידע" (information weapons) מקור לדאגה. על פי הגדרתה, נשק מידע יכול לשמש בתחומים שמעֵבר לסייבר, לרבות בתחום ההכרה האנושית,[19] ולכלול אזורים גיאוגרפיים שבהם מתגוררים דוברי רוסית או אנשים ממוצא רוסי.[20] אין ספק שרוסיה רואה בהצלחות של "מהפכות הצבע" במרכז ובמזרח אירופה ושל "האביב הערבי" דוגמאות לאובדן השליטה החברתית והשליטה במידע.

הכתיבה האמריקאית על לוחמת מידע

לשיטתה של ארצות הברית, מרחב הסייבר כולל את הרשתות והמערכות שמרכיבות את הארכיטקטורה שלו, אך לא את סביבת המידע כולה כפי שגורסות ההגדרות של סין ורוסיה. מחקרים אסטרטגיים ומבצעיים רבים נכתבו בארצות הברית, שבהם הכותבים הביעו דעתם כיצד על הצבא האמריקאי לפעול ב"מבצעי מידע" (Information Operations) בתחום הסייבר, שבהם פעולות סייבר (או "לוחמת סייבר") הן רק אופציה אחת מתוך כמה אופציות. המסמך "האסטרטגיה לפעולה במרחב הסייבר" שפרסם משרד ההגנה של ארצות הברית ב־2011, וכן הפרסום בנושא "מבצעי מידע" (JP 3–13) מטעם המטות המשולבים של צבא ארצות הברית במהדורת 2012, מציגים את החשיבה האמריקאית העדכנית בנושא מרחב הסייבר כזירת קרב. הקמת מטה הסייבר האמריקאי (CYBERCOM) עולה בקנה אחד עם שאיפתה של ארצות הברית לאפשר לה יד חופשית לפעול בתחום הסייבר, במקביל למניעת יכולות דומות מיריבותיה. על פי מסמך האסטרטגיה של משרד ההגנה האמריקאי, מטה CYBERCOM משקף את היעדים הבאים: "[...] להבטיח פיתוח יכולות משולבות באמצעות עבודה צמודה עם מפקדות, שירותים וסוכנויות לענייני לוחמה ועם קהילת הרכש, במטרה לפתח וליישם במהירות יכולות חדשניות במקומות שהן דרושות במיוחד".[21]

המסמך של המטות המשולבים (JP 3–13) מספק מידע לגבי פריסת יכולות הסייבר האמריקאיות ומציג דוקטרינה והנחיות של המטות המשולבים לפעילויות של צבא ארצות הברית במבצעים משותפים. על פי המסמך: "[...] מִבצעי מידע (לרבות פעולות ברשתות מחשב) מיועדים להשפיע על, לשבש את, או להשתלט

על, יכולת קבלת ההחלטות של יריבים קיימים ופוטנציאליים, במקביל להגנה על היכולת שלנו".[22]

שורש ההבדל בין הכתיבה של סין ורוסיה לזו של ארצות הברית מצוי בפרשנות ההוליסטית של מרחב האיום אצל הראשונות לעומת פרשנות צרה יותר שלו אצל האחרונה. רוסיה וסין מעדיפות לשלב את ההיבט האנושי עם ההיבט הטכנולוגי, בעוד שארצות הברית מתמקדת בהיבט הטכנולוגי בלבד. ארצות הברית רואה את המערכה הגדולה של מִבצעי מידע כמורכבת מכמה יכולות צבאיות הנפרדות זו מזו, אם כי כאלו שעשויות להיות קשורות זו לזו. לעומתה, רוסיה וסין מציגות תפיסה לפיה קיימים קשרים הדדיים הדוקים יותר, שבהם אין הבחנה ברורה בין הפעילויות שבוצעו והתוצאות שהושגו. לאור זאת, מתקפת סייבר יכולה להיות, על פי ההשקפה האמריקאית, החדרת נוזקה לתשתית קריטית, ועל פי ההשקפה הרוסית/סינית – מידע עוין המשוגר על ידי גורמים יריבים ומכָוון נגד הממשלה או הציבור שעליו היא שולטת.

אירועי מתקפת סייבר

כמה ממתקפות הסייבר שזכו לפרסום חושפות את ההתפתחות של נשק הסייבר מכוח משבש לכוח הרסני. אין בכך כדי לומר שכל מתקפות הסייבר בעתיד יכללו הרס של מערכות מידע, אלא שיש תקדימים לכך שהרס נתפס כבר בעבר כאופציה מועדפת במקרים מסוימים שבהם הצדדים היריבים שרויים במבוי סתום דיפלומטי. במקרים שיפורטו להלן היה חשד לקיומה של יד מכוונת מדינתית, או לחסות של מדינה, אך הדבר לא הוכח מעולם. דבר זה מלמד שאם ממשלות עומדות מאחורי ניהול מתקפות סייבר, הן מעדיפות להשתמש בהן כנשק הפתעה בזמנים של מתיחות דיפלומטית, תוך שמירה על יכולת הכחשה סבירה ועל מינימום של עימות חזיתי, אם בכלל.

וירוס "וַויפֶּר", קוריאה הדרומית, 2013

במארס 2013 מחקה הנוזקה "וַויפר" (wiper) נתונים ממערכות מחשב של שלושה בנקים בקוריאה הדרומית ושל חברות הביטוח שלהם, וכן של שלושה גופי שידור. מרבית המתקפות התרחשו ב־20 במארס, אך העדויות מלמדות שבחלק מהמקרים המערכות נדבקו עוד קודם לכן בווירוסים, ואלה כָוונו להפעלה בתאריך המיועד.[23] הווירוס "וויפר" מחק את רשומת האתחול הראשית במחשבים השולטים ברשתות התקשורת של גופים אלה, וכן השבית את תוכנת האנטי־וירוס של חברה דרום קוריאנית ידועה.[24] לפי ההערכות, המתקפה פגעה ב־48,000 מחשבים.[25]

היה זה האירוע הרביעי בסדרה של מתקפות הקשורות לווירוס "וויפר" שזכו לפרסום. המתקפה הראשונה התרחשה באפריל 2012 נגד מתקן אירָאני באי חארג'.

השנייה הייתה בחברה הסעודית "עראמקו" והשלישית הייתה בחברה הקטרית "ראסגָז". מתקפות אלו היו איתות לכך שגורמים לא מדינתיים מוכנים לעבור לפעולות הרסניות יותר בעתות של מתחים פוליטיים. כמו באירוע ב"עראמקו", גם במקרה של קוריאה הדרומית נטל את האחריות ארגון לא מוכר בשם WHOIS,[26] למרות שהיו מי שהטילו ספק באמינות הודעתו עקב היעדר מידע על עברו או עדות ליכולתו לבצע מתקפה ברמה כזו.

גורמים רשמיים בקוריאה הדרומית מאמינים שיחידות המודיעין הצבאי של קוריאה הצפונית הן שאחראיות למתקפה, תוך שהן פועלות מכתובות IP סיניות.[27] על רקע המתיחות המתמשכת בין קוריאה הצפונית לקוריאה הדרומית, אירע לא פעם, לפחות מאז 2009, שהרטוריקה המדינית והדיפלומטית בין הצדדים גלשה לעולם הסייבר, כאשר רשתות "סוכני תוכנה" (botnet) כיוונו מתקפות למניעת שירות מבוזרת (DDoS) נגד אתרי אינטרנט של ארצות הברית וקוריאה הדרומית.[28] קוריאה הצפונית אף הגבירה את איומיה על קוריאה הדרומית וארצות הברית במהלך התרגיל הצבאי השנתי המשותף של השתיים, Key Resolve, שנערך ב־11 עד 21 במארס 2013 (זמן קצר לאחר שבפברואר 2013 ערכה קוריאה הצפונית ניסוי במתקן הגרעין שלה).[29] אם קוריאה הצפונית אכן עומדת מאחורי מתקפות אלו, הרי שיש בכך סטייה מהשיטה שנהגה בה עד אז – בדרך כלל פעילות נמרצת למניעת שירות, אך למעשה כזאת שלא גרמה נזק של ממש. חשוב מכך, התקרית של מרץ 2013 אותתה לממשלת קוריאה הדרומית שקוריאה הצפונית מסוגלת לבצע מתקפות סייבר הרסניות כאשר היא מעריכה שהייתה הפרה של ה"נורמות" שהתבססו בין שתי הקוריאות.

וירוס "וייפר", "עראמקו", 2012

באוגוסט 2012 גרם וירוס שכונה "שאמוּן" למחיקת נתונים ב־75 אחוזים מכלל מחשביה של חברת "ערמאקו" – חברת הנפט הלאומית של ערב הסעודית ומי שנחשבת לחברת הנפט בעלת הערך הגבוה בעולם.[30] הנוזקה נועדה להשיג שתי מטרות: להחליף את הנתונים בכוננים הקשיחים בתמונה של דגל אמריקאי העולה באש ולהעביר רשימה של כתובות נגועות למחשב שנמצא בתוך הרשת של החברה; למחוק את הזיכרון במחשבים הנגועים.[31] הווירוס הרס את הכוננים הקשיחים של 30,000 מחשבים.[32]

חשיבות האירוע נעוצה בכך שמדובר בנוזקה שהוטמעה מתוך כוונה להרוס כוננים רבים ככל האפשר במחשבים של חברה הקשורה לתשתית קריטית. התחכום של הנוזקה נתון לוויכוח. שר ההגנה של ארצות הברית דאז, ליאון פָּנֶטָה, התייחס לווירוס "שאמון" כאל כלי מתוחכם מאוד,[33] ולעומתו סברו חוקרי אבטחה ממעבדת קָסְפֶּרסקי ששגיאות הקידוד בקוד היו אינדיקציה לעבודה חובבנית ושלווירוס

היה פוטנציאל להיות הרסני אפילו יותר.[34] הווירוס "שאמון" הופעל נגד חברת "עראמקו" יום לפני אחד המועדים הקדושים ביותר בשנה המוסלמית.[35] ניתן לשער שהתוקפים ביקשו להגביר את הצלחתם המבצעית כשהעריכו, ובצדק, שבמועד זה ניטור המחשבים יהיה מצומצם יותר, דבר שייתן זמן נוסף לווירוס להתפשט. ואכן, המתקפה השפיעה על ייצור הנפט ועל ההתנהלות העסקית של החברה, עקב איבוד חלק מנתוני הקידוח והתפוקה.[36] על פי אחד המקורות, נדרשו עשרה ימים להחליף את הכוננים הנגועים.[37]

ארגון לא מוכר בשם "חרב הצדק" קיבל על עצמו את האחריות למתקפה על מחשבי "עראמקו", בטענה שזו תגובה למדיניות הסעודית במזרח התיכון.[38] למרות זאת, רבים, וביניהם גורמים אנונימיים בממשל האמריקאי, חשדו שמדובר במעורבות איראנית.[39] אם איראן אכן עמדה מאחורי המתקפה, פירוש הדבר שהיא מעדיפה לתקוף את ערב הסעודית בחשאי באמצעות "שליח", כדי לשמור על יכולת הכחשה סבירה, במיוחד לאור העובדה שהמתקפה כוונה ישירות נגד יצרנית נפט גלובלית מרכזית ונגד תשתית קריטית.

אין כיום קונצנזוס בין־לאומי סביב השאלה מה מהווה "קו אדום" בתחום הסייבר, ואף על פי כן ניתן להניח שפעולת הרס מכוונת נגד ארגון בעל ממדים גלובליים תיחשב לצעד תוקפני (act of force) על פי דיני המלחמה במשפט ההומניטרי הבין־לאומי, המסדירים פעולות איבה חמושות בין מדינות לאום. בהקשר זה, ניתן לפרש את הפגיעה המכוונת בחברת "עראמקו" – סמל לשלטון הסעודי – כאיתות איראני לערב הסעודית על חוסר שביעות רצונה של טהראן מכך ש"עראמקו" נהנית מהסנקציות שהטיל האו"ם על איראן, וכן ממה שנראה כשיתוף פעולה סעודי־אמריקאי נגד שאיפותיה הגרעיניות של איראן.

מתקפת "סטוקסנֶט" על הצנטריפוגות האיראניות, 2010

ההערכה היא שווירוס "סטוקסנט" (Stuxnet) קשור קשר הדוק לשלוש נוזקות דומות, ואולי אף מתוחכמות ממנו, המוכרות בשמות Duqu, Flame ו־Gauss. שלוש נוזקות אלו קשורות בעיקר לריגול סייבר, ולפיכך המאמר הנוכחי אינו עוסק בהן.

ב־2010 הודתה איראן כי נשק סייבר, שחוקר בחברת "מיקרוסופט" הדביק לו את הכינוי "סטוקסנט", גרם נזק לצנטריפוגות הגז במתקן שלה להעשרת אורניום. "סטוקסנט" תואר כיישום מורכב ו"מתוחכם במיוחד", שכל תכליתו הייתה לחבל בצנטריפוגות להעשרת אורניום של איראן שנשלטו על ידי "משנה מהירות" (high frequency converter drivers) במתקן להעשרת האורניום בנָתָנְז.[40] כאלף צנטריפוגות נפגעו מהנוזקה, שגרמה להן לצאת מכלל שליטה, ובסופו של דבר היה צורך להחליפן.[41] למרות ש"סטוקסנט" התגלה ב־2010, ההערכה היא שהווירוס חדר לרשת כבר ב־2009,[42] דבר המלמד על יכולת גישה חשאית למטרה.

תקרית "סטוקסנט" הייתה בעלת משמעות רבה, משום שלראשונה נוצר ויושם נשק סייבר במטרה לפגוע, לשבש ולהרוס מערכת מידע מסוימת. חשוב מכך, התחכום של הנוזקה, כמו גם חדירתה החשאית לרשת של מערכת בקרה תעשייתית – למרות שזו הותקנה עם הפרדה פיזית (air gap) מהאינטרנט ופעלה בסביבה מאובטחת – הצביעו באופן ישיר על מעורבות וחסות של מדינה. אף ארגון לא קיבל על עצמו אחריות לאירוע.

איראן הבהירה בכמה הזדמנויות שבכוונתה ליישם את זכותה הריבונית לפתח את תוכנית הגרעין שלה למטרות שלום.[43] דברים אלה עוררו אי־נחת רבה בארצות הברית, כמו גם במדינות מערביות ומזרח־תיכוניות אחרות, וכן ברוסיה ובסין הידידותיות לאיראן.[44] אמנם, אף ממשלה לא קשרה עצמה באופן רשמי ל"סטוקסנט", אך הסברה המקובלת היא שמדובר בפרי שיתוף פעולה בין ארצות הברית לישראל.[45] השימוש המוצלח ב"סטוקסנט" מנע את הצורך בתקיפה צבאית קונבנציונלית על מתקני העשרת האורניום של איראן – מהלך שעלול היה לגרום לפעולת תגמול איראנית מסלימה. אם ארצות הברית אכן עומדת מאחורי "סטוקסנט", ניתן לפרש את הדבר כאיתות לאיראן כי וושינגטון נותרה מחויבת לעמדתה שלא להתיר לאיראן להעשיר אורניום למטרות צבאיות, וכן כהוכחה ליכולתה של ארצות הברית לחדור למתקן רגיש ומאובטח היטב שיש בו נשק להשמדה המונית.[46]

מתקפות מניעת שירות מבוזרת (DDoS), גיאורגיה, 2008

באוגוסט 2008 פלש כוח רוסי לגיאורגיה בעקבות החלטת ממשלתה לפתוח במתקפת פתע נגד כוחות הבדלנים בדרום אוסֶטיה.[47] קודם לפלישה הרוסית שוגרו מתקפות סייבר רוסיות נגד אתרי אינטרנט של ממשלת גיאורגיה.[48] מתקפות דיגיטליות אלו, שנמשכו לאורך רובו של חודש אוגוסט, כללו בעיקר השחתה של אתרי אינטרנט (בראש ובראשונה אתרי אינטרנט ממשלתיים) ומתקפות מניעת שירות שכוונו לאתרי תקשורת, מוסדות פיננסיים, אתר של קהילת האקרים בגיאורגיה ואתרים של ממשלת גיאורגיה.[49]

מתקפות סייבר אלו בלטו מסיבה מרכזית אחת: הן התרחשו במקביל לפלישה הצבאית של רוסיה לגיאורגיה. מתקפות הסייבר של 2008 על גיאורגיה היו דומות במובנים רבים למתקפות סייבר שהיו עליה בשנת 2007, מתקפות שכללו השחתת אתרים ומניעת שירות ביעדים של המגזר הפרטי והציבורי במדינה. הייחודיות של מתקפות הסייבר על גיאורגיה הייתה בתיאום ובעוצמה שלהן, וזאת בניגוד למתקפות על אסטוניה, בהן התיאום היה מדורג.[50] אם אותם גורמים עומדים מאחורי אותן מתקפות, הרי שהם שינו את מתודולוגיית המתקפה שלהם כדי להשיג יעילות מרבית.

כמו באסטוניה, גם המתקפות בגיאורגיה יוחסו להאקרים לאומניים רוסיים, וממשלת רוסיה נחשדה כמי שממממנת אותם.[51] אם אכן מוסקבה עמדה גם הפעם מאחורי המתקפות, ניתן לראות בכך ביטוי להפקת לקחים שעשתה בכל הנוגע לפגיעה מכוונת במדינה זרה באמצעות נשק הסייבר. המטרה המרכזית של מתקפת הסייבר באסטוניה הייתה התשתית, ואילו בגיאורגיה היו אלה ארגוני תקשורת וחדשות שהפכו לקורבנות הראשיים שלה. באמצעות המתקפה על גופים אלה, ביקשו התוקפים לשלוט במרחב המידע של גיאורגיה ולמנוע שידור של גילויי תמיכה בהתנגדות לרוסיה. היה זה ביטוי לתפיסה הרוסית של לוחמת מידע, המוצגת גם על ידי תיאורטיקנים רוסיים מובילים בתחום לוחמת המידע, דוגמת איגור פנארין (Panarin).[52]

המאמצים של אלה שקיוו לשלוט במידע בגיאורגיה כשלו בסופו של דבר, ורבים סבורים שגיאורגיה ניצחה במלחמת המידע הזאת.[53] אף על פי כן, התקרית ממחישה כי אפילו במהלך עימות חזיתי בין כוחות, רוסיה מעדיפה לשמור על יכולת הכחשה סבירה בנוגע למעורבותה במתקפות סייבר. לכאורה, ניתן היה להניח שברגע שרוסיה יזמה מתקפה פיזית על גיאורגיה היא לא תראה עוד צורך להסוות את מבצעי הסייבר שלה, במיוחד אם הם לא נועדו להרוס מערכות מידע או נתונים, ועל אחת כמה וכמה כשמדובר במדינה בעלת יכולות סייבר ברמה דומה לזו של ארצות הברית.[54] למעשה, נראה שמתקפות מניעת השירות על גיאורגיה נועדו לאותת לשכנותיה של רוסיה ולמדינות ברית המועצות לשעבר כי עליהן לצַפות לפגיעה דומה בהן, אם ממשלותיהן ייכנסו למצבי מתיחות דיפלומטית עם הפדרציה הרוסית.

עימות צבאי בפועל

לא כל מקרי העימות החזיתי של צבא מול צבא כללו מתקפות סייבר, בין אם כמרכיב מרכזי ובין אם כמרכיב משני. הדבר ראוי לציון לאור העובדה שכמה מהמדינות המעורבות בעימותים כאלה מחזיקות ביכולות הדרושות ללוחמת סייבר, וידוע שהדוקטרינות הרשמיות שלהן כוללות התייחסות לשאלה כיצד מתקפות סייבר עשויות וצריכות להתבצע בתרחישי עימות. ניתן אמנם לייחס את אי־הפעלתן של מתקפות סייבר אסטרטגיות להיעדר מטרות אסטרטגיות למתקפות כאלו, אולם העדויות מלמדות שההימנעות ממתקפות סייבר נבעה בעיקר מהקושי להשיג בדרך זו יתרון אסטרטגי. מצב זה גורם להטלת ספק ביעילותן של מתקפות סייבר כנשק בעל יכולת להשיג תוצאות הדומות לאלו שמשיג נשק קונבנציונלי.

משבר ישראל־חמאס, 2014

ביולי 2014 שיגרה ישראל טיל שפגע בתחנת החשמל היחידה של עזה, ובכך עצרה את אספקת החשמל לאזור. על פי דיווחי העיתונות, מהלך זה היה צפוי להחמיר בעיות של מים וביוב שהיו קיימות עוד קודם לכן.[55] קשה להניח שהשימוש שעשתה ישראל בנשק קונבנציונלי במקרה זה נבע מחוסר היכולת שלה לפגוע באותו מתקן באמצעי סייבר; הדבר סותר את המוניטין שלה כמעצמת סייבר מובילה ואת היותה חשודה במעורבות בכמה מאירועי סייבר מפורסמים, כמו מתקפת הסייבר של 2012 על תחנת כוח איראנית ומתקנים איראניים נוספים,[56] מתקפת ה"סטוקסנט" של 2010 נגד הצנטריפוגות במתקני העשרת האורניום של איראן,[57] או מתקפות הסייבר של 2007 נגד מערכות ההגנה האווירית של סוריה.[58] ניתן להניח שכאשר מדובר במטרה אסטרטגית, כמו השבתת יעד אסטרטגי מרכזי, השימוש בנשק קונבנציונלי הופך לאופציה המועדפת על ישראל, וזאת בשל היותה דרך פעולה אמינה יותר מאחרות להשגת היעדים המידיים.

משבר רוסיה־אוקראינה, 2014

במהלך המשבר בין רוסיה לאוקראינה ב־2014 דיווחה חברת הטלקומוניקציה האוקראינית Ukrtelecom כי חמושים פשטו ב־28 בפברואר אותה שנה על המתקנים שלה בחצי האי קרים, חיבלו בכבלי הסיבים האופטיים והשביתו את פעולת מערכות האינטרנט והטלפון המקומיות.[59] לאור מומחיותה של רוסיה בפעולות סייבר,[60] כמו גם העובדה שחלק גדול מהטלקומוניקציה האוקראינית נבנתה כאשר אוקראינה עוד הייתה חלק מהגוש הסובייטי, ניתן לשער שמתקפת סייבר הייתה דרך הפעולה המתבקשת במקרה זה, במיוחד בשל יכולתה להישען על היכרות קרובה עם המטרה מצד אחד, במקביל ליכולת ליהנות מהיתרונות של פעולה אנונימית מצד שני. היסטוריית הפעילות של האקרים לאומניים רוסיים (כגון בשנת 2007 באסטוניה ובשנת 2008 בגיאורגיה) מגבירה גם היא את הסבירות לנקיטת פעולה כזאת גם באוקראינה, או לפחות להעדפתה. למרות זאת, אין עדות ישירה למתקפות סייבר רוסיות נגד אוקראינה. יתרה מכך, למרות שדיווחים גלויים דיברו על "התכתשויות סייבר" בין גורמים פרו־בדלניים לגורמים פרו־אוקראיניים, לא נרשמה מאז יוני 2014 כל עדות לפעילות משמעותית שפגעה בתשתית קריטית אוקראינית או ביעדי פיקוד ובקרה של אוקראינה.

מלחמת האזרחים בסוריה, 2013

על פי מאמר שהתפרסם ב"ניו יורק טיימס" ב־2014, משרד ההגנה והסוכנות לביטחון לאומי של ארצות הברית פיתחו, בעקבות ההתקוממות הפנימית נגד ממשלת סוריה, תוכנית לחימה שכללה מתקפת סייבר מתוחכמת על מערכות

הפיקוד של צבא סוריה ושל הנשיא בשאר אל־אסד.[61] על פי המאמר, הנשיא אובמה דחה את התוכנית (וכן אופציות תקיפה קונבנציונלית אחרות), הן בשל ערכה האסטרטגי המוגבל והן בשל העובדה שהיכולות של נשק סייבר במהלך עימות צבאי לא נבחנו עדיין.[62] ואכן, ממשל אובמה טרם הכריע בשאלה האם נשק הסייבר הוא כלי צבאי יעיל, או שיש לשמור אותו לפעולות חשאיות בלבד.[63]

מלחמת האזרחים בלוב, 2011

ארצות הברית שקלה שימוש בנשק סייבר נגד לוב ב־2011. על פי דיווח ממקורות גלויים, המטרה הייתה לפרוץ את "חומות האש" של רשתות המחשב הממשלתיות של לוב, כדי לנתק תקשורת צבאית ולמנוע מגלאי התרעה מוקדמת לאסוף מידע ולהעבירו לסוללות טילים שהיו מכוונות נגד מטוסי נאט"ו.[64] עם זאת, ברגע שצבא ארצות הברית החליט לעבור לשימוש בכוח, הוא גם עבר להסתמך על נשק קונבנציונלי לביצוע המשימה. מאז התעורר ויכוח באשר לסיבה שמאחורי התנהלות זו (שתי סברות פופולריות היו שארצות הברית לא רצתה להפגין את יכולות הסייבר שלה ושהיא לא רצתה להיות הראשונה להשתמש בנשק סייבר למטרה זו),[65] אך ייתכן שהשאלה הרלוונטית יותר מבחינתה של ארצות הברית הייתה האם מתקפות סייבר יכולות להשיג אותה רמה של יעילות צבאית כמו מתקפות של טילים קונבנציונליים.

מסקנות וסיכום

אין חולק על כך שממשלות זרות מפתחות יכולות סייבר, בין אם כדי לחזק את מערכות איסוף המודיעין שלהן ובין אם ככלי של עוצמה מדינית. הכתיבה האקדמית והצבאית בשלוש מדינות מובילות מעידה על תמיכה בשימוש בנשק סייבר במצבי עימות, במיוחד נגד תשתיות קריטיות. ההיסטוריה עשירה באירועים שבהם הותקפו תשתיות קריטיות של האויב בעתות מלחמה משיקולים של יתרון אסטרטגי וטקטי גם יחד. סביר היה להניח שנשק מבוסס מחשב ימונף באופן דומה.

עם זאת, מרבית פעילויות הסייבר שידוע שבוצעו נגד מטרות מדיניות התרחשו במהלך תקופות של מתיחות דיפלומטית ובוצעו בעיקר על ידי גורמים לא מדינתיים, שההשערה הלא מוכחת היא כי פעלו בשליחותה של מדינה. מתקפות סייבר היו יעילות ביותר כנשק של מכה ראשונה, שנהנה מיתרון ההפתעה והאנונימיות, וזאת בשל הקושי לייחס את הפעולה ליוזם כלשהו. לעומת זאת, עימותים שבהם היה מעורב כוח צבאי (שבהם הצורך להסוות את הגורם העומד מאחוריו הוא פחות רלוונטי) עשו רק במקרים ספורים שימוש במתקפות סייבר להשגת המטרה הצבאית – בין אם כמרכיב תומך ובין אם לצורך הטעיה. במרבית

המקרים, תקיפות פיזיות היו דרך הפעולה הנבחרת, אולי משום שהן היוו חלופה אמינה ויעילה יותר.

דומה שבעתיד הנראה לעין, נשק הסייבר יתאים לפעילות חשאית ולשליחת מסרים מדיניים יותר מאשר להכרעה במלחמה ולשינוי כללי המשחק. אין בכך כדי לומר שהמצב לא ישתנה בעתיד הרחוק, אולם לשם כך יהיה על מדינות להתנסות בהפעלה ממשית של נשק הסייבר במהלך עימותים, לחוות את הבעיות שיתעוררו במהלך השימוש בו ולהפיק לקחים כדי לשפר את יעילותו. עד כה הדבר לא נעשה, כך שהשאלה "האם לנשק סייבר יש תפקיד בעימות?" נותרה על כנה. לנוכח הנטייה של צבאות לכלול טכנולוגיה בפעולותיהם, התשובה לשאלה זו היא "כן, יש תפקיד לנשק הסייבר", אלא שבשלב זה נראה שלא מדובר בתפקיד מרכזי.

הערות

1 Thomas Rid and Peter McBurney, "Cyber Weapons," *Rusi Journal*, February/March 2012, https://www.rusi.org/downloads/assets/201202_Rid_and_McBurney.pdf

2 *What is Critical Infrastructure?*, Department of Homeland Security, November 1, 2013, http://www.dhs.gov/what-critical-infrastructure

3 Daniel T. Kuehl, "Information Operations, Information Warfare and Computer Network Attack: Their Relationship to National Security in the Information Age," *International Law Studies*, 76 (2002).

4 DoD Directive TS3600.1," *IT Law Wiki*," http://itlaw.wikia.com/wiki/DOD_Directive_TS3600.1

5 Michael Breen and Joshua A. Geltzer, "Asymmetric Strategies as Strategies of the Strong," *Parameters*, Spring 2001, http://strategicstudiesinstitute.army.mil/pubs/parameters/Articles/2011spring/Breen- Geltzer.pdf

6 Shen Weiguang, "Focus of Contemporary World Military Revolution – Introduction to Information Warfare," *Jiefangjun Bao*, November 7, 1995, p. 6.

7 Major General Wang PuFeng, *The Challenge of Information Warfare*, 1995, http://fas.org/irp/world/china/docs/iw_mg_wang.htm

8 Liu Yichang, ed., *Gaojishu zhanzheng lun* (On High-Tech War) (Beijing: Military Sciences Publishing House, 1993), p. 272.

9 Deepak Sharma, "Integrated Network Electronic Warfare: China's New Concept on Information Warfare, "*Journal of Defence Studies*, 4, No. 2 (April 2010).

10 Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, 1999), p. 168.

11 James C. Mulvenon, "The PLA and Information Warfare," in *The People's Liberation Army in the Information Age*, eds. James C. Mulvenon and Richard H. Yang (Washington D.C.: RAND, 1999), pp. 175-186.

12 Keir Giles and William Hagestad, "Divided by a Common Language: Cyber Definitions in Chinese, Russian and English," 2013 5th International Conference on Cyber Conflict (NATO: CCD COE Publications).

13 Ibid.

14 *Information Security Doctrine of the Russian Federation (2000)*, http://www.mid.ru/

bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument

15 *Russian Military Doctrine (2010)*, http://carnegieendowment.org/files/2010russia_military_doctrine.pdf

16 Jolanta Darczewska, "The Anatomy of Russian Information Warfare," *Point of View*, 42, May 2014, http://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf

17 Ibid.

18 Giles and Hagestad, "Divided by a Common Language".

19 Ibid.

20 Darczewska, "The Anatomy of Russian Information Warfare".

21 *Department of Defense's Strategy for Operating in Cyberspace – July 2011*, Department of Defense, http://www.defense.gov/news/d20110714cyber.pdf.

22 *Joint Publications 3-13 Information Operations*, Department of Defense, http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.

23 Matthew J. Schwartz, "North Korea Behind Bank Malware, South Korea Says," *Dark Reading*, April 10, 2013, http://www.darkreading.com/attacks-and-breaches/north-korea-behind-bank-malware-south-korea-says/d/d-id/1109474?

24 Michael Mimoso, "Theories Abound on Wiper Malware Attack against South Korea," *ThreatPost*, March 21, 2013, http://threatpost.com/theories-abound-wiper-malware-attack-against-south-korea-032113/77654

25 Schwartz, "North Korea Behind Bank Malware".

26 Wiper Malware Analysis Attacking Korean Financial Sector," *Dell Secure Works*," March 21 2013, http://www.secureworks.com/cyber-threat-intelligence/threats/wiper-malware-analysis-attacking-korean-financial-sector/

27 Sean Gallagher, "North Korean Military Blamed for Wiper Cyber Attacks against South Korea," *ArsTechnica*, April 10, 2013, http://arstechnica.com/security/2013/04/north-korean-military-blamed-for-wiper-cyber-attacks/

28 Choe Sang-Hun and John Markoff, "Cyber Attacks Jam Government and Commercial Websites in U.S. and South Korea," *The New York Times*, July 8, 2009, http://www.nytimes.com/2009/07/09/technology/09cyber.html

29 Comprehensive Nuclear Test Ban Treaty Organization, "On the CBTO's Detection in North Korea," February 12, 2013, http://www.ctbto.org/press-centre/press-releases/2013/on-the-ctbtos-detection-in-north-korea/

30 Nicole Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," *The New York Times*, October 23, 2012, http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all

31 Ibid.

32 Kelly Jackson Higgins, "The Long Shadow of Saudi Aramco," *Dark Reading*, October 14, 2013, http://www.darkreading.com/attacks-breaches/the-long-shadow-of-saudi-aramco/d/d-id/1140664?

33 Phil Stewart, "Shamoon Virus Most Destructive Yet for Private Sector, Panetta Says," *Reuters*, October 11, 2012, http://www.reuters.com/article/2012/10/12/us-usa-cyber-pentagon-shimoon-idUSBRE89B04Y20121012

34 Fahmida Y. Rashid, "Coding Errors in Shamoon Malware Suggest it may be the Work

of Amateurs," *Security Week*, September 12, 2012, http://www.securityweek.com/coding-errors-shamoon-malware-suggest-it-may-be-work-amateurs

35 Paul Roberts, "Whoddunnit? Conflicting Accounts on ARAMCO Hack Underscores Difficulty of Attribution," *Naked Security*, October 30, 2012, http://nakedsecurity.sophos.com/2012/10/30/whodunnit-aramco-hack/

36 John Roberts, "Cyber Threats to Energy Security as Experienced by Saudi Arabia," *Platts*, November 27, 2012, http://blogs.platts.com/2012/11/27/virus_threats/#comments

37 Roberts, "Whoddunnit?"

38 Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back".

39 Siobhan Gorman and Julian E. Barnes, "Iran Blamed for Cyber Attacks," *The Wall Street Journal*, October 12, 2012, http://online.wsj.com/news/articles/SB10000872396390444657804578052931555576700

40 Matthew Schwartz, "Stuxnet Launched by United States and Israel," *Information Week*, June 1, 2012, http://www.reuters.com/article/2011/12/02/us-cyberattack-iran-idUSTRE7B10AV20111202

41 Ellen Nakashima, Greg Miller and Julie Tate, "U.S. Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say," *The Washington Post*, June 19, 2012, http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html

42 "Stuxnet Effect: Iran still Reeling," *Industrial Safety and Security Source*, August 3, 2011, http://www.isssource.com/stuxnet-affect-iran-still-reeling/

43 "Timeline of Iran's Controversial Nuclear Program," *CNN*, March 19, 2012, http://www.cnn.com/2012/03/06/world/meast/iran-timeline/

44 Max Fisher, "Nine Questions about Iran's Nuclear Program you were Afraid to Ask," *The Washington Post*, May 19, 2013, http://www.washingtonpost.com/blogs/worldviews/wp/2013/11/25/9-questions-about-irans-nuclear-program-you-were-too-embarrassed-to-ask/

45 David E. Sanger, "Obama Order Sped up Wave of Cyberattacks against Iran," *The New York Times,* June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0

46 Emilio Iasiello, "Cyber Attack: A Dull Tool to Sharpen Foreign Policy", 2013 5th International Conference of Cyber Conflict, 2013, http://www.ccdcoe.org/publications/2013proceedings/d3r1s3_Iasiello.pdf

47 Council of Europe Parliamentary Assembly Resolution (2008), *The Consequences of War between Georgia and the Russian Federation*, http://assembly.coe.int/ASP/Doc/XrefViewHTML.asp?FileID=12031&Language=en

48 Eneken Tikk, Kadri Kaska, and Liis Vihul, "International Cyber Incidents: Legal Considerations," *Cooperative Cyber Defence Centre of Excellence*, 2010, http://www.ccdcoe.org/publications/books/legalconsiderations.pdf

49 Ibid.

50 Ibid.

51 Ibid.

52 Darczewska, "The Anatomy of Russian Information Warfare."

53 Clifford J. Levy, "Russia Prevailed on the Ground but Not in The Media," *The New York Times*, August 21, 2008, http://www.nytimes.com/2008/08/22/world/europe/22moscow.html?_r=0

54 Keir Giles, "Information Troops – A Russian Cyber Command?" 2011 3rd International Conference on Cyber Conflict (CCD COE Publications: 2011), http://www.ccdcoe.org/publications/2011proceedings/InformationTroopsARussianCyberCommand-Giles.pdf

55 Alan Greenblatt, "Israeli Bombing Ruins Gaza's Only Power Plant," *NPR*, July 29, 2014, http://www.npr.org/blogs/thetwo-way/2014/07/29/336386340/israeli-bombing-destroys-gazas-only-power-plant

56 Rick Gladstone, "Iran Blames U.S. and Israel for Spree of Cyber Attacks," *Sydney Morning Herald*, December 27, 2012, http://www.smh.com.au/it-pro/security-it/iran-blames-us-and-israel-for-spree-of-cyber-attacks-20121226-2bwa1.html

57 Ellen Nakashima and John Warrick, "Stuxnet was Work of US and Israel, Experts Say," *The Washington Post*, June 2, 2012, http://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html

58 John Leyden, "Israel Suspected of Hacking Syrian Air Defenses," *The Register*, October 4, 2007, http://www.theregister.co.uk/2007/10/04/radar_hack_raid/

59 P. Polityuk, and J. Finkle, "Ukraine says Communications Hit, MPs Phones Blocked." *Reuters*, March 4, 2010, http://www.reuters.com/article/2014/03/04/us-ukraine-crisis-cybersecurity-idUSBREA231R220140304

60 D. Smith, *Russia Cyberoperations* (Washington, D.C.: Potomac Institute Cyber Center, 2010), http://www.potomacinstitute.org/attachments/article/1273/Russian%20Cyber%20Operations.pdf

61 David E. Sanger, "Syria Stirs new U.S. Debate on Cyberattacks," *The New York Times*, February 25, 2014, http://www.nytimes.com/2014/02/25/world/middleeast/obama-worried-about-effects-of-waging-cyberwar-in-syria.html

62 Ibid.

63 Ibid.

64 Eric Schmitt and Thom Shanker, "U.S. Debated Cyberwarfare in Attack Plan on Libya," *The New York Times*, October 17, 2011, http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html

65 Jack Goldsmith, "Quick Thoughts on the USG's Refusal to Use Cyberattacks in Libya," *Lawfare Blog*, October 18, 2011, http://www.lawfareblog.com/2011/10/quick-thoughts-on-the-aborted-u-s-cyberattacks-on-libya/

השפעת התפתחות טכנולוגיית הלוחמה הקיברנטית על שינויים בבניין הכוח בישראל

גיל ברעם

בעשור האחרון חלו ההתפתחויות מהירות בתחומי המחשוב וטכנולוגיות המידע, שהובילו לשינויים מרחיקי לכת כמעט בכל תחומי החיים, ביניהם גם בתחום הצבאי־ביטחוני. בתחום זה התרחשו שינויים רבים במאפייני הלחימה ובבניין הכוח של צבאות, בין היתר בשל התפתחויות שחלו בדפוסי המחשבה האסטרטגית ובגיבוש הדוקטרינות הצבאיות שהותאמו למציאות המשתנה. ניסיונות שנעשו לבחון את השלכות המעבר לעידן המידע על העיסוק הביטחוני הובילו בשנות התשעים של המאה ה־20 להתפתחותו של רעיון "המהפכה בעניינים צבאיים". הרעיון נולד בעקבות ההמצאות הטכנולוגיות החדישות, שהובילו לעליית מדרגה בזמינות המודיעין ובאיכותו, בקצב זרימת המידע וביכולות הדיוק של כלי הנשק. בשנים הבאות, ובייחוד עם הכניסה למאה ה־21, התפתחו טכנולוגיות מתקדמות בתחום הלוחמה הקיברנטית, שהובילו לשינוי איכותי במאפייני שדה הקרב ובדפוסי פעילותם של הצבאות המודרניים.

הטכנולוגיה הקיברנטית המשמשת לצורכי לחימה משפיעה על דפוסי הלחימה כך שמדינה המחזיקה בה נהנית מעליונות בשדה הקרב, ממודיעין איכותי ומקיף, מיכולת תקיפה מדויקת ומהירה, מיכולות הגנה על תשתיות קריטיות, מיכולות שליטה ובקרה גבוהות ועוד. יכולות אלה תורמות לעוצמתה של המדינה ומחזקות את ביטחונה הלאומי. טכנולוגיית הלוחמה הקיברנטית טומנת בחובה פוטנציאל ליתרונות עצומים, לצד סיכונים חדשים ובלתי־מוכרים. לאור חדשנותו הרבה של תחום זה, הבנת טיבו והשלכותיו עודם מצויים בראשית הדרך.

בשנים האחרונות הגבירו מדינות רבות, ובראשן ארצות־הברית וישראל, את קצב פעילותן בזירה הקיברנטית. פעילות זו מהווה עבורן מקור עוצמה, אך

גיל ברעם היא תלמידה לתואר שני בתוכנית ללימודי ביטחון באוניברסיטת תל אביב, עמיתת מחקר בסדנת יובל נאמן למדע טכנולוגיה וביטחון.

מאמר זה ראה אור לראשונה ב**צבא ואסטרטגיה**, כרך 5, גיליון 1, מאי 2013, עמ' 19–36.

גם חושפת את "הבטן הרכה". זאת משום שהתשתיות החיוניות לתפקודה של כל מדינה הפכו תלויות במחשבים. אופן ההתמודדות הרצוי עם האיום הנשקף כתוצאה מהתפתחות טכנולוגיית הלוחמה הקיברנטית הוא תחום עיסוק מרכזי שעמו מתמודדת מדינת ישראל בשנים האחרונות.[1]

האינטרס הלאומי של ישראל מתרכז בשמירה על ביטחונה מפני אלה המעוניינים לפגוע בה ומערערים על עצם קיומה. אינטרס זה, וכן מיקומה הגיאו־פוליטי של ישראל, מחייבים אותה ליצור עליונות בתחום הקיברנטי כחלק בלתי־נפרד מיכולתה להגן על עצמה מפני פגיעות קונוונציונליות וקיברנטיות, וכיכולת התקפית הרתעתית בזירת המזרח התיכון ומעבר לו.

ישראל נחשבת למובילה בעולם מבחינת יכולת התמודדותה עם תקיפות קיברנטיות: בדו"ח מקיף שבחן את מידת מוכנותן של 23 מדינות בתחום הקיברנטי קיבלה ישראל את הציון הגבוה ביותר – ארבעה כוכבים וחצי מתוך חמישה. מהדו"ח עלה כי ישראל נתונה בכל דקה תחת כאלף מתקפות קיברנטיות. נתון זה הרשים במיוחד את מחברי הדו"ח, ששיבחו את מערכות ההגנה הישראליות וציינו שישראל ערוכה היטב להתמודדות עם מתקפה קיברנטית נגדה.[2]

פיתוח יכולות הפעולה של ישראל בזירת הלוחמה הקיברנטית הוא מרכיב מרכזי בשמירה על חוסנה הלאומי. הכלכלה, התעשייה, הביטחון, החינוך והשמירה על קיומה כחברה דמוקרטית, פתוחה ומבוססת ידע תלויים, ברובם, ביכולתה להגן על רשתות המחשבים החיוניות שלה מפני פגיעה שעלולה להוביל לשיבוש אורח החיים התקין במדינה. ההישענות הגוברת על מערכות מחשב בארץ ובעולם הביאה עמה אתגרים חדשים, המצריכים מענה מיידי ברמה הלאומית.[3]

מטרת המאמר היא להציג את מקומה של טכנולוגיית הלוחמה הקיברנטית בתפיסת הביטחון הישראלית, ולבחון את ההיערכות שבוצעה בישראל במטרה להתמודד עם האיום הקיברנטי באמצעות בחינת שלושה תחומים מרכזיים: גיבוש אסטרטגיה סדורה להתמודדות עם האיום הנשקף כתוצאה מהתפתחות טכנולוגיית הלוחמה הקיברנטית; הקצאת משאבים ותקציבים; יצירת שינויים בבניין הכוח. ההנחה היא כי באמצעות בחינת הפרסומים הממשלתיים אפשר יהיה ללמוד על מידת חשיבות הנושא עבור מקבלי ההחלטות, ומכאן על המשאבים המוקצים להתמודדות איתו. כל זאת, מתוך כוונה להציג את המצב בישראל ולנסות להצביע על הפערים הקיימים בתחום.

המאמר מתבסס על ספרות עדכנית בנושא ועל מידע פומבי בלתי־מסווג הכולל קטעי עיתונות, הצהרות לתקשורת, מסמכי ממשל וראיונות עם אישים מרכזיים בתחום. יש לציין כי בישראל קטן מספרם של הפרסומים הרשמיים על אודות דרכי ההתמודדות עם האיום הקיברנטי, ובפרט ביחס ליכולותיה ההתקפיות בתחום.

על כן, סביר להניח שלאור אופייה הביטחוני של ישראל, מידע רב על פעולות המבוצעות בנושא ותקציבים המוקצים לתחום נותר חסוי.

ביצוע המחקר לווה במספר קשיים: כיוון שמדובר בתחום מחקר חדש יחסית, עדיין לא קיים מספיק ידע היסטורי בנושא השפעתה של התפתחות טכנולוגיית הלוחמה הקיברנטית על יצירת שינויים באסטרטגיות הקיימות ועל בניין הכוח. עם זאת, כיוון שמדובר בתחום בעל חשיבות רבה רצוי להתחיל להתעמק בו חרף פערי הידע הקיימים.

חשוב לציין כי המחקר מתמקד בתחום הלוחמה הקיברנטית, המורכב מהיערכותה של המדינה בתחומי ההגנה וההתקפה, ואינו עוסק בתחום השימוש במחשבים לצרכי תקשורת או ניהול לחימה. משום שהמחשבים משמשים כיום לביצוע פעולות רבות בתחומי התקשורת והלחימה, מדובר בתחום נרחב מאוד, החורג מהיקפו של מאמר זה.

מקומה של טכנולוגיית הלוחמה הקיברנטית בתפיסת הביטחון הישראלית

השינויים הרבים שחלו בתחום טכנולוגיות הלוחמה הקיברנטיות מאתגרים את התפיסות הביטחוניות הקיימות, ומחייבים בחינה מחודשת של מושגי היסוד. נוצר מצב שבו יש חשיבות ראשונה במעלה להגנה על התשתיות החיוניות של המדינה בתחומי האנרגיה, המים, המחשוב, התקשורת, התחבורה והכלכלה – הן במגזר האזרחי והן במגזר הביטחוני. על כן, יש לערוך את ההתאמות הנדרשות בתפיסת הביטחון על מנת שתוכל לספק מענה לאיומים החדשים.[4]

באפריל 2006 הוגשה לשר הביטחון דאז, עמיר פרץ, הצעה לתפיסת ביטחון מעודכנת. ההצעה הוכנה על ידי ועדה בראשות דן מרידור, שבין חבריה היו ראש המועצה לביטחון לאומי, ראש השב"כ, הממונה על הביטחון במערכת הביטחון ונוספים. מדו"ח הוועדה עלה שישראל נמצאת בעידן של שינויים אסטרטגיים גדולים ומהירים, ביניהם שינויים טכנולוגיים מרחיקי לכת.[5] בין היתר, המליצה הוועדה להוסיף את ההגנה כרכיב נוסף לשלושת הרכיבים המסורתיים (הרתעה, התרעה והכרעה),[6] ובפרט המליצה על הצטיידות בכלי־טיס בלתי־מאוישים ועל יצירת הגנה על מערכות המחשב הלאומיות מפני חדירת גורמים עוינים.[7]

בעקבות דיוני הוועדה עלתה האפשרות לצרף מונח יסוד רביעי ל"משולש הביטחון", והוא "התגוננות" או "הגנה".[8] ישראל אכן השקיעה חלק ניכר מתקציבה וממאמצי הביטחון שלה בהתגוננות פסיבית. רעיון ה"הגנה" הורחב, ונכללו בו, נוסף לכלי ההתגוננות הפסיביים, גם כלים התקפיים נקודתיים שמטרתם לסכל ירי תלול־מסלול או פיגועי טרור שמתחת לרף ההסלמה הרחבה.[9]

בתחום הלוחמה הקיברנטית קיימת חשיבות עליונה להגנה, כיוון שבאמצעות הגנה יעילה אפשר לוודא שמערכותיה החיוניות של המדינה ימשיכו לתפקד. נוסף על כך, יכולות קיברנטיות מתקדמות מאפשרות למדינה הגנה יעילה על התשתיות הקריטיות שלה וכך מספקות מענה לצורך בהגנה אקטיבית, כפי שהוצג בדו"ח ועדת מרידור.

במשך זמן רב נהוג היה לכנות את תחום ההגנה על מערכות ממוחשבות "אבטחת מידע", לפי התפיסה שהדבר המרכזי שעליו יש להגן הוא מידע רגיש (מידע מסווג או עסקי). עם השנים התפתחה גישה זו והקיפה איומים נוספים מלבד פגיעה במידע – מניעת שירות, השבתת תהליכים חיוניים מבוססי מחשב ועוד. ברמה הלאומית התרחב מושג ההגנה על מערכות ממוחשבות, ואפשר לכנותו "הגנה קיברנטית".[10] מאז פרסום הדו"ח חלה עלייה ניכרת בשימוש בטכנולוגיה קיברנטית לצורכי לחימה שונים בשדה הקרב. על כן, ראוי לבחון את מקומה של טכנולוגיית הלוחמה הקיברנטית בתהליכי עדכון תפיסת הביטחון של ישראל.

במבט היסטורי על מלחמות ישראל אפשר לראות שחשיבות הטכנולוגיה עלתה ממלחמה למלחמה, והשתכללה עם השנים. בין ישראל לבין מדינות ערב קיימים הבדלים בסיסיים, וכן קיימת א־סימטריה כמותית ברורה. אם שוקלים את הפערים הכמותיים הגדולים, בולט יתרונה היחסי של ישראל בהסטת המלחמה למישור הטכנולוגי: לישראל קל יותר להתמודד עם העולם הערבי בקרבות אוויר מתוחכמים או בביצוע פעולות קיברנטיות (על פי פרסומים זרים) מאשר בזריקת אבנים או בהתמודדות של חייל מול חייל. ככל ששדה הקרב רווי בטכנולוגיות מתקדמות, הולכים ומצטמצמים הפערים הכמותיים, וגדל ערכן של איכויות מערכות הנשק ושל כוח האדם. בצה"ל היטיבו לזהות את הפוטנציאל הרב הטמון במחשבים, וכבר משנות התשעים החל השימוש בלוחמת מחשבים (computer warfare) על סוגיה השונים.[11]

ההתמודדות עם האיום הנשקף כתוצאה מהתפתחות טכנולוגיית הלחימה הקיברנטית הולמת את תפיסת הביטחון הישראלית: מדובר בתחום המופעל ביכולות "כחול־לבן", שמסתמך על כושר הפיתוח וההמצאה "היהודי", בשילוב טכנולוגיות עולמיות. התחום מוכר היטב לישראלים הצעירים במדינה, שהוגדרה לאחרונה כ"מדינת סטארט־אפ"[12] ומתבסס על העיקרון של חשיבות האיכות על פני הכמות.

אפשר לראות ש"שלוש הרגליים" המקוריות של תפיסת הביטחון הישראלית המסורתית רלוונטיות עבור ההתמודדות עם האיום הקיברנטי:

1. הרתעה – יכולות קיברנטיות מתקדמות יאפשרו לישראל ליצור הרתעה מול אויביה. כדוגמה אפשר לראות את אירוע וירוס "סטקסנט" המיוחס לארצות־הברית ולישראל, שנתפס כעליית מדרגה בכל הנוגע ליכולות התקיפה

הקיברנטיות של מדינות ולעוצמת השפעתן, זכה לתהודה רחבת־היקף בתקשורת העולמית ותרם לחיזוק ההרתעה הישראלית.[13]

2. התרעה – היכולות הקיברנטיות מאפשרות לישראל לאסוף מידע רב על אויביה ובמקביל, למנוע מהם גישה למאגרי המידע שלה. כך תוכל המדינה להתריע באופן יעיל על כוונותיהם נגדה.
3. הכרעה – ישראל היא מהמדינות המובילות בעולם מבחינת יכולותיה הקיברנטיות. יכולות אלה מאפשרות לה להשיג יתרון בקרב, באמצעות שימוש בכלים קיברנטיים מתקדמים, ולהכריעו לטובתה. חשוב לציין כי מושג ההכרעה בתחום הקיברנטי, כמו למושג ההרתעה, הם מושגים חמקמקים שמשמעותם בהקשר הקיברנטי טרם מוצתה עד תום. עם זאת, כיום ברור כי עליונות קיברנטית בשילוב עם יכולות קינטיות מתקדמות עשויה להוביל להכרעת קרבות.

מקום המדינה ועד היום מושתתת תפיסת הביטחון על עקרון חשיבות האיכות על פני הכמות. טכנולוגיית הלחימה הקיברנטית עונה על עיקרון זה: באמצעות כלים קיברנטיים, שאינם דורשים הפעלת כוח פיזי רב אלא הכשרת כוח אדם מיומן, מתאפשרות פעולות המסייעות להגברת יכולת ההרתעה של ישראל ומקנות לה יוקרה רבה בזירה הבינלאומית.

לסיכום, נראה שאפשר לשלב את יכולות הלחימה הקיברנטית בתפיסת הביטחון הישראלית באופן פשוט יחסית, אם אכן זו תעודכן בקרוב. זאת משום שיכולות אלה עונות על שלושת העקרונות הבסיסיים שעליהם בנויה תפיסת הביטחון. כמו כן, פיתוח יכולות לחימה קיברנטיות עצמאיות וכלי לוחמה קיברנטיים מממשים בבירור את עקרון האיכות על פני הכמות: כל שנדרש הוא כוח אדם מיומן ברמה גבוהה לפיתוח מערכות המאפשרות ביצוע פעולות ביעדים רחוקים, מבלי לסכן חיי אדם ומבלי להזדקק למשאבים רבים.

גיבוש אסטרטגיה סדורה לתחום הקיברנטי

האיום הקיברנטי הוא פועל יוצא של תפקידן הקריטי של מערכות המחשב בתשתיות הלאומיות ובחיי היום־יום. מרחב וירטואלי זה נוצר מהתפתחות מבוזרת של מערכות ומגזרים שונים, כחלק מהתפתחות כלכלית וטכנולוגית מואצת, ללא הקשרים ביטחוניים מובהקים. כשעלה בשנים האחרונות הצורך לעסוק בהיבטים הביטחוניים של התחום הקיברנטי, נשאלה השאלה – מיהו "בעל הבית" והאחראי לביטחון בו?[14]

אבטחת מידע והגנה על תשתיות ממוחשבות אינם נושאים חדשים בישראל. ישראל הייתה מהמדינות הראשונות בעולם שהכירו בחשיבות ההגנה על מערכות ממוחשבות חיוניות. כבר בשנת 1996 קיבלה הממשלה החלטות באשר לדרך

ההתגוננות הרצויה מפני איומים קיברנטיים.[15] בשנת 1997 הוקם פרויקט תהיל"ה (תשתית הממשלה לעידן האינטרנט), שמטרתו להגן על חיבור משרדי הממשלה לאינטרנט ולספק שירותי גלישה מאובטחים למשרדי הממשלה.[16] בהמשך, בשנת 1998 חוקק "החוק להסדרת הביטחון בגופים ציבוריים", שעסק בהגדרת מערכות ממוחשבות חיוניות ובאבטחתן.[17]

ההחלטה על הקמת הרשות הממלכתית לאבטחת מידע

בישראל אין פרסום מוסדר של המדיניות הציבורית בתחום ההתמודדות עם האיום הקיברנטי, ומרבית המידע הקיים נסמך על פרסומים בתקשורת ומחקרים אקדמיים. עם זאת, מספר החלטות רשמיות שפורסמו שופכות אור על המצב: בפברואר 2002 התקבלה בוועדת השרים לענייני ביטחון לאומי ההחלטה בנושא "אחריות להגנה על מערכות ממוחשבות במדינת ישראל" (החלטה ב/84), שעיצבה את מתווה ההגנה על התשתיות הממוחשבות הקריטיות במדינה. ההחלטה משמשת בסיס להפעלת המענה הישראלי לאיום הקיברנטי על תשתיות מחשב לאומיות חיוניות. בהחלטה נקבעה הקמתם של שני גופים ייעודיים: האחד – ועדת היגוי עליונה שתבחן באופן שוטף את זהות הגופים הציבוריים והפרטיים החיוניים לתפקודה של מדינת ישראל; השני – יחידה ממלכתית להגנה על המערכות הממוחשבות.

ואכן, בהמשך להחלטת ועדת השרים הוקמה כבר באותה שנה ועדת היגוי בראשות ראש המועצה לביטחון לאומי, שמטרתה הייתה לגבש מכלול צעדים להגנה על מערכות המחשב החיוניות של המדינה. בוועדה נקבעו עקרונות תפיסת ההגנה, איומי הייחוס והגופים שיחויבו בצעדי הגנה.[18] כמו כן, היא פעלה כצוות היגוי המנחה את היחידה הממלכתית לאבטחת תשתיות ממוחשבות בשירות הביטחון הכללי (שב"כ).

באותה השנה הוקמה "הרשות הממלכתית לאבטחת מידע", הפועלת במסגרת חוק השב"כ. הרשות מנחה את הגופים שהוגדרו כחיוניים בנושאי ביטחון המחשוב והגנה על הרשתות, ומפקחת על ביצוע הנחיות אבטחת המידע והגנתו. כמו כן, היא מוסמכת לנקוט סנקציות נגד גופים המפרים את הנחיותיה. יש לציין כי גופי הביטחון השונים פועלים להגנה על תשתיותיהם הקריטיות באופן עצמאי, ללא הנחיה רשמית של הרשות לאבטחת מידע.[19]

ההחלטה על הקמת המטה הקיברנטי הלאומי

בנובמבר 2010 הטיל ראש הממשלה על יושב ראש המועצה הלאומית למחקר ולפיתוח, אלוף במיל' פרופסור יצחק בן ישראל, להציג תוכנית עבודה למיזם לאומי להתמודדות עם האיום הקיברנטי.[20] בין המלצותיו של צוות המיזם היו: המלצה 1 א' – הקמת מטה קיברנטי לאומי להגנה, שייעודו קידום הגנת המרחב

הקיברנטי בישראל. המלצה 1 ב' – הרחבת סמכויות שב"כ כגוף הביצוע לטיפול במרחב האזרחי.[21]

המסמך המרכזי בנושא הוא החלטת הממשלה מיום ה־7 באוגוסט 2011 בנושא "קידום היכולת הלאומית במרחב הקיברנטי".[22] החלטה זו היא תולדה של פעילות צוות המיזם. בהחלטה נקבעה הקמת המטה הקיברנטי הלאומי, ונקבע כי מטרתו היא "קידום היכולת הלאומית במרחב הקיברנטי ושיפור ההתמודדות עם האתגרים הנוכחיים והעתידיים במרחב הקיברנטי". אחד מתפקידיו של ראש המטה הוא "להמליץ לראש הממשלה ולממשלה על מדיניות קיברנטית לאומית, להנחות את הגורמים הרלבנטיים אודות המדיניות עליה הוחלט... ליישם את המדיניות ולבקר את יישומה".[23] ההחלטה על הקמת המטה, שפורסמה בפומבי, הייתה התקדמות משמעותית באופן טיפולה של הממשלה בנושא האיום הקיברנטי, והיוותה נקודת מפנה בתחום.

בעוד גופי הממשל, זרועות הצבא וגופי מערכת הביטחון מוגנים על פי חוק, מרבית המגזר העסקי והאזרחים מהשורה נותרו ללא הגנה מספקת בתחום. המגזר העסקי אינו נתון לפיקוח רשמי ואינו כפוף לגוף לאומי כלשהו, האחראי לבדוק את יכולות ההתמודדות עם פגיעה במערכות המחשב החיוניות שלו בשעת חירום. זוהי נקודת תורפה משמעותית של ישראל, שכלכלתה תלויה בכושר הייצור והייצוא של המגזר העסקי והתעשייתי.[24]

מקבלי ההחלטות בישראל צופים שבמלחמה הבאה ייעשה שימוש באמצעי לוחמה קיברנטיים, ואף על פי כן, אין כיום גוף רשמי בישראל שאחראי ישירות על הגנת המגזר העסקי. נכון הוא שרשות לאומית אינה יכולה להחליף את המנהלים האחראיים על עסקיהם, אך מאחר שחלק מהארגונים הפרטיים במשק מספקים שירותים החיוניים להמשך החיים התקינים בעורף, יש מקום להתערבות ממשלתית בהנחיות, בתקנות ובבקרה.[25]

עם הקמת המטה הקיברנטי הלאומי אמר ד"ר אביתר מתניה, ראש המטה, כי לתפיסתו קיימים חמישה היבטים שבהם על המדינה להתערב בהקשר הקיברנטי:

1. יצירת נקודת מבט כלל־מערכתית ברמה הלאומית: ההגנה הקיברנטית מחייבת בחינה רב־מערכתית, מאחר שקיימת תלות הדוקה בין המערכות הציבוריות למערכות הפרטיות והעסקיות.
2. "איגום" משאבים, פעולות ומידע: משמעות האיגום היא איחוד משאבים ממקורות שונים לגוף מתַכלל אחד, במטרה להתמודד בצורה טובה יותר עם האיומים הנשקפים לישראל.
3. יצירת שיתוף פעולה בינלאומי: על ישראל להוביל את נושא שיתוף הפעולה באופן יזום, וליצור שיתופי פעולה עם בעלות־ברית ברחבי העולם.

4. יצירת הסדרה לתחום הקיברנטי: ביצוע הסדרה תקינה, רישוי והסמכה, וכינון שיטה שבה ארגונים ופרטים יהיו מסוגלים להגן על עצמם על פי סטנדרטים מוגדרים וברורים.[26]
5. קידום תהליכים על ידי המדינה: כפי שפעלה המדינה בשנות השישים לקידום תחום התעופה בארץ, באמצעות הקמת הפקולטה לאווירונאוטיקה בטכניון, כך היא צריכה לספק כלים ומנופים על מנת לתמרץ פיתוחים אקדמיים ותעשייתיים בתחום הקיברנטי.[27]

לדברי מתניה, מטרת המטה הקיברנטי הלאומי היא תכנון כלל העשייה בתחום ההגנה הקיברנטית: חיזוק האבטחה בארגונים באמצעות יצירת הסדרה חוצת ענפים המותאמת למאגרי המידע, וכן הסדרה ענפית לכל תחום ותחום. נדבך נוסף הוא בניית תוכניות לאומיות, שיתוף פעולה ושיתוף המידע, במיוחד בקשר שבין המערכת הביטחונית והמערכת האזרחית.[28]

מהות פעילות המטה נוגעת להסדרה, לתִכלול ולקידום הפעילות הכלל־ממשלתית בתחום הקיברנטי בראייה רחבה, אזרחית וביטחונית כאחד. המטה פועל ברוח החלטת הממשלה, יחד עם הגופים הרלוונטיים, לגיבוש מדיניות הגנה ובניית תפיסת הגנה לאומית, וליצירת שיתופי פעולה בין כלל הגופים הפועלים בתחום. זאת לצד גיבוש תוכניות כוללות ובניית מנגנונים לטיפוח ההון האנושי בתחום הקיברנטי; פיתוח תשתיות טכנולוגיות ומחקריות באקדמיה ובתעשייה; קידום שיתופי פעולה בין המגזר הפרטי־עסקי, המגזר הממשלתי, התעשייה, האקדמיה ומערכת הביטחון; קידום המודעות הציבורית לאיום הקיברנטי ועוד.[29]

מהאמור לעיל אפשר לראות שישראל היטיבה לזהות את האיום הנשקף לתשתיותיה הלאומיות, ופעלה להקמת מערך הגנה ברמה הלאומית. שתי נקודות ציון מרכזיות הן: הקמת הרשות הממלכתית לאבטחת מידע (רא"מ) בשנת 2002; החלטת הממשלה מאוגוסט 2011 על "קידום היכולת הלאומית במרחב הקיברנטי" והקמת המטה הקיברנטי הלאומי. עם זאת, הממשל הישראלי טרם הפיץ לציבור אסטרטגיה מוסדרת ואחידה בנושא.

ישראל היא מהמדינות המובילות בעולם ביכולותיה הקיברנטיות, אולם, כנהוג בישראל, אין לכך ביטוי הולם בכל הנוגע לקביעת אסטרטגיה סדורה ולפרסום ברור של דרך הפעולה הרשמית בתחום. נראה כי בישראל טרם גובשה אסטרטגיה בתחום,[30] וכי עיקר המידע מגיע מהצהרות לעיתונות ומכתבות בתקשורת, ולא ממידע ממשלתי רשמי. אמנם קיימת החלטת ממשלה רשמית בנושא, אולם טרם פורסמה אסטרטגיה סדורה.

הקצאת תקציבים

בחלק זה ייבחנו התקציבים והמשאבים שהוקצו להתמודדות עם האיום הנשקף כתוצאה מהתפתחות טכנולוגיית הלוחמה הקיברנטית, מתוך הנחה שבחינת התקציבים תאפשר להקיש על מידת חשיבותו של הנושא עבור מקבלי ההחלטות בישראל.

המועצה הלאומית למחקר ופיתוח (המולמו"פ) יזמה בשנת 2007 ומימנה מחקר בנושא "מדדים למדע, לטכנולוגיה ולחדשנות בישראל", בשיתוף הלשכה המרכזית לסטטיסטיקה. מטרת המחקר הייתה לבחון את התקציבים המוקצים לנושאי מדע וטכנולוגיה בישראל. מהמחקר עלה שבעשור האחרון הוצאו בישראל מדֵי שנה כ־30 מיליארד ש"ח למחקר ופיתוח (מו"פ) אזרחי. בחינת האחוז מהתוצר הלאומי הגולמי המושקע במחקר ופיתוח הראתה שישראל מדורגת במקום הראשון בעולם – 4.3% בשנת 2009, לעומת 1.8% בממוצע במדינות הארגון לשיתוף פעולה כלכלי ולפיתוח (OECD). מרבית המימון בישראל, כ־79%, מגיע מהמגזר העסקי. הממשלה מממנת באופן ישיר כ־5 מיליארד ש"ח מהמו"פ האזרחי, נוסף על הכספים המוקצים למימון המו"פ בתחום הביטחוני.[31]

מהנתונים אפשר ללמוד שמדינת ישראל והמגזר העסקי שלה משקיעים סכומים לא־מבוטלים במחקר ופיתוח בתחום הטכנולוגי. לכך אפשר לצרף את התקציבים השונים שחולקו בשנה האחרונה למחקר ופיתוח בנושאים יישומיים ותיאורטיים בתחום הקיברנטי.[32] מצירוף הנתונים ניתן להניח שהתחום הקיברנטי מקבל תקצוב למטרות מחקר ופיתוח, מתוך הכרה בחשיבותו הגוברת לביטחון המדינה. התקצוב המדויק אינו מתפרסם ברבים.

אחת ההוצאות העיקריות בהצעת תקציב המדינה לשנים 2011–2012 יועדה ל"אשכול הביטחון והסדר הציבורי". מתוך הוצאה זו מוקצים כספים לגופי מערכת הביטחון השונים, האחראים על הטיפול בתחום הקיברנטי. סך התקציב שהופנה למימון האשכול עמד על סכום כולל של 61.8 מיליארד ש"ח בשנת 2011, וסכום כולל של 63.4 מיליארד ש"ח בשנת 2012. מתוך הסכומים האמורים, ההוצאות שהופנו לפעילות משרד הביטחון היו הגבוהות ביותר, ושיעורן עמד על כ־18% מסך ההוצאה התקציבית.[33] ניתן להניח שמשרד הביטחון משקיע סכומים לא־מבוטלים גם בפיתוח תחום הלוחמה הקיברנטית בגופים המצויים באחריותו.

המלצה נוספת של צוות המיזם הקיברנטי הייתה לייסד תוכנית מו"פ לאומית לבניית יכולות קיברנטיות, בשיתוף עם מערכת הביטחון, עם האקדמיה ועם התעשייה. התוכנית כללה המלצות להכוונת המשאבים הלאומיים הקיימים והוספת משאבים במידת הצורך. כל זאת במטרה להציב את ישראל בחמישייה המובילה של מדינות העולם מבחינת יכולותיה הקיברנטיות עד שנת 2015.[34] בהקשר זה חשוב לציין כי לא מדובר בהכרח רק בפיתוח יכולות צבאיות־ביטחוניות,

אולם סביר להניח כי לפחות חלק מהתקציב יוקצה לפיתוח ביטחוני בתחום הקיברנטי.

תקציב המטה הקיברנטי

בהחלטת הממשלה מאוגוסט 2011 שבה הוחלט על הקמת המטה הקיברנטי הלאומי, הוחלט להקצות למטה תקציב שיועבר למשרד ראש הממשלה ממקורות משרד האוצר.[35] התקציב המלא שהוקצה לפעולות המטה אינו מפורט בהחלטה, מלבד סכום קטן (כ־4.5 מיליון ש"ח) שהוקצה עבור "הקמת ותפעול המטה" לשנת 2011.

תקציב המטה הקיברנטי כיום הוא 2.5 מיליארד ש"ח לחמש השנים הבאות, כ־500 מיליון ש"ח בשנה. 100 מיליון מתוכם יוקצו כסכום ייעודי מתקציב המדינה עבור המטה הקיברנטי, ו־400 מיליון יינתנו לאחר תהליך "איגום" כספים ממקורות שונים.[36] לדבריו של רס"ן טל, ראש תחום בכיר במטה הקיברנטי, ראש הממשלה רואה בתחום הקיברנטי נושא בעל חשיבות עליונה ופועל רבות לקידומו. קיימת נכונות לפיתוח התחום והתקציבים ניתנים בהתאם. חשיבות האיום הקיברנטי צוברת תאוצה, ואף נבנתה תוכנית ארוכת־טווח שתבטיח את תקציביו.[37]

בישיבת ועדת הכספים מחודש מאי 2012 הוקצו באופן מפורש תקציבים להמשך קידום פעילותו של המטה, מעבר לסכומים שכבר הוקצו.[38] בקשת המטה, כפי שהובאה לאישור הוועדה, כללה כ־12 מיליון ש"ח למימון שני נושאים מרכזיים: הראשון – תקציב תפעול המטה, שכלל תשלום משכורות לעובדי המטה ויצירת תשתיות ממוחשבות ותשתיות אבטחה פיזיות עבור גופים מסווגים הנדרשים לתשתיות מסוג זה. השני – תחילת מימוש תקציב פעילותו השוטפת של המטה.[39]

מתוך הכרה בחשיבות הקשר בין האקדמיה, התעשייה והמטה הקיברנטי הוקצו על ידי המטה, בשיתוף משרד המדע, כ־50 מיליון ש"ח לשלוש שנים עבור מלגות ומחקרים בתחומי עיסוק שונים של תחום העיסוק הקיברנטי, במטרה למצב את ישראל כמובילה בעולם בתחום.[40] נוסף לכך, הכריזו המדען הראשי והמטה הקיברנטי על הקצאת 80 מיליון ש"ח עבור תוכנית קידמ"ה,[41] שמטרתה פיתוח המו"פ והיזמות בנושא ה־Cyber Security.[42] גם במקרה זה, סביר להניח שחלק מהמלגות יוקצו לתחומים הנוגעים ללוחמה הקיברנטית.

לנוכח מיעוט הפרסומים העוסקים בנושא התקציב, קשה לאמוד מהי ההשקעה הממשלתית המדויקת בהתמודדות עם האיום הקיברנטי בישראל. עם זאת, מהנתונים שהוצגו לעיל אפשר לראות שהאיום הנשקף כתוצאה מהתפתחות טכנולוגיית הלוחמה הקיברנטית לא נעלם מעיניהם של מקבלי ההחלטות במדינה, וכי הנושא זוכה למשאבים לא־מבוטלים.

החל משנת 2011 החלו להתפרסם בפומבי הקצאות תקציבים לתחום הקיברנטי. ניתן להניח במידה רבה של ודאות, שלאור העובדה שהטיפול בתחום הקיברנטי הובל בעשור האחרון על ידי מערכת הביטחון במעטה סודיות, תקציבים שונים שהוקצו לתחום זה אינם מפורסמים בגלוי. עם זאת, לאחר קבלת ההחלטה הרשמית על הקמת המטה הקיברנטי הלאומי באוגוסט 2011, החל להתפרסם בגלוי מידע על התקציבים המופנים להתעצמות ולנושאי מחקר ופיתוח בתחום.

שינויים בבניין הכוח

טכנולוגיית הלוחמה הקיברנטית יצרה שינוי במערכות הנשק של זירת הלחימה המודרנית, והפכה אותן למדויקות וליעילות יותר. בעקבות השינויים הרבים שחלו בסביבתה החיצונית של ישראל, גברו אתגרי הביטחון שמולם היא ניצבת, וגדלה מידת חשיבותו של המודיעין בתפיסת הביטחון הישראלית. כיום ניצבת ישראל בחזית הטכנולוגיה ומתמודדת עם האיומים הנשקפים לה, בסיוע כלים טכנולוגיים קיברנטיים המשולבים בכל זירות הלחימה.[43]

להתפתחויות מסוג זה הייתה השפעה לא־מבוטלת על עקרונות המלחמה ועל שינויים שחלו במבנה צבאות, ובכלל זה במבנה צה"ל. בבואו לבחון את מקומה של הטכנולוגיה לאורך מלחמות ישראל, טען פרופ' בן ישראל כי ככל ששדה הקרב מתקדם יותר מבחינה טכנולוגית, כך הגמישות והיכולת לאלתר ולשנות (changeability) תופסות חלק גדול יותר בלחימה המודרנית. למשל, מלחמת יום־הכיפורים הדגימה היטב שלא די לבנות מערכות לוחמה אלקטרונית נגד האיומים המוכרים של האויב, אלא יש צורך לבנותן כך שיוכלו להתמודד עם השינויים שיעשה האויב בפרמטרים האלקטרוניים של מערכותיו תוך כדי הלחימה.[44]

להלן ייבחנו השינויים המרכזיים שחלו בגופים הממשלתיים ובגופי מערכת הביטחון בישראל, לאור ההכרה הגוברת בסיכונים הנשקפים מהתפתחות האיום הקיברנטי ומכניסתה של הטכנולוגיה הקיברנטית לשדה הקרב.

המטה הקיברנטי הלאומי

באוגוסט 2011 הכריז ראש הממשלה על הקמת "המטה הקיברנטי הלאומי", שייעודו העיקרי הוא הרחבת יכולות ההגנה על מערכות התשתית החיוניות למדינה מפני התקפות טרור קיברנטי, העלולות להיגרם הן על ידי מדינות זרות והן על ידי גורמי טרור.[45] המטה, הפועל כשנה וחצי ומצוי בשלבי צמיחה, מורכב כיום מארבעה אגפים: האגף הביטחוני; האגף האזרחי; אגף המודיעין והערכת מצב; האגף לארגון ולמדיניות. נוסף לכך הוקם חדר מצב בירושלים, הפעיל 24 שעות ביממה שבעה ימים בשבוע, ומצוי בקשר רציף עם הגופים הביטחוניים העוסקים בתחום. חדר המצב מאפשר ראייה כוללת של סך האיומים ואפשרויות ההתמודדות,

כך שבשעת ביצוע תקיפה קיברנטית על גוף אחד, אפשר יהיה לדעת בזמן אמת על אילו גופים נוספים יש להגן.

שלושת הנושאים המרכזיים שעליהם אמון המטה הקיברנטי הם:

הראשון – גיבוש תפיסת ההגנה הרשמית של ישראל, זאת באמצעות שיתוף פעולה בין כלל הגופים האמונים על תחום ההגנה. נוסחה תפיסה הפועלת בשתי רמות: רמת האבטחה הכללית במשק ורמת האבטחה המדינתית.

השני – פיתוח התשתית וקידום המובילות הלאומית של ישראל בתחום הקיברנטי. בין היתר, באמצעות הרחבת ההון האנושי וקידום נושא המלגות למחקרים בתחום הקיברנטי.

השלישי – הובלת תהליכים לאומיים בתחום הקיברנטי, כמו יצירת הסדרה בשוק האבטחה; יצירת תשתית אבטחה מדינתית באמצעות חקיקה וביצוע תרגילי חירום; חיזוק קשרי החוץ עם מדינות שונות בעולם ועוד.[46]

ההחלטה על הקמת המטה הייתה צעד חשוב בהתמודדותה של ישראל עם האתגר הקיברנטי, אולם יש להבטיח כי המטה יפעל על פי אסטרטגיה לאומית שתגובש בהקדם. לנוכח פיגורה של ישראל בקביעת אסטרטגיה פומבית סדורה, יש חשיבות רבה לכך שהמטה יקבל סמכויות רחבות־היקף. רק כך אפשר יהיה להתחיל לצמצם את הפער שנוצר ברמה הלאומית בניהול האסטרטגי המקיף של כלל הגופים האזרחיים והצבאיים הפועלים בתחום הקיברנטי.[47]

הרשות הממלכתית לאבטחת מידע

הגוף הוותיק ביותר העוסק בנושא אבטחת המידע על היבטיו השונים הוא "הרשות הממלכתית לאבטחת מידע" בשב"כ. רשות זו צמחה מתוך יחידה שטיפלה במשך עשרות שנים בתחום אבטחת המידע הקלאסית, עד שקיבלה בשנת 2002 את האחריות על הנחיית כל גופי התשתיות הלאומיות האזרחיים להתגוננות מפני מתקפות סייבר אפשריות.

השב"כ קיבל סמכות על פי חוק להנחות גופים כגון חברת חשמל, מקורות, רכבת ישראל וחברות הגז. תחומי ההנחיה כוללים הוראות כמו כיצד למנוע השתלטות עוינת מרחוק, שעלולה לגרום פגיעה קשה במערכות קריטיות בלחיצת מקש, וכדומה. בשנים האחרונות התרחבה רשימת הגופים המונחים על ידי הרשות, מתוך הכרה לאומית באיום הקיברנטי הגובר.[48]

צפריר כץ, שכיהן עד לאחרונה כראש אגף הטכנולוגיה בשב"כ, העניק הצצה נדירה אל הנעשה בתחום הטכנולוגי בשב"כ ואמר כי כ־20% מאנשי השירות הם אנשים טכנולוגיים. השירות שינה את פניו לעומת שנות השמונים של המאה הקודמת, אז לא היה מוטה לכיוון הטכנולוגיה. היה צורך לפתח צורות העסקה

למספר שנים עבור אנשים צעירים. לתפיסתו, מדובר במהפכה הנמשכת לאורך כל העשור האחרון.[49]

צה"ל

בשנת 2009 הגדיר הרמטכ"ל דאז, רב־אלוף גבי אשכנזי, את המרחב הקיברנטי "כמרחב לחימה אסטרטגי ואופרטיבי עבור מדינת ישראל". בהמשך לכך הוקם "מטה הסייבר הצה"לי", שנועד לשמש מטה מטכ"לי לתיאום ולהכוונה של פעולות הצבא בתחום הקיברנטי. המטה הוקם ביחידה 8200 באגף המודיעין של צה"ל.[50]

בחיל התקשוב הוקמה מחלקת הגנה בסייבר, שפעילותה מסווגת ברובה. המחלקה מאפשרת לקיים פעילויות מבצעיות ביבשה, באוויר ובים, בעידן שבו הצבא נשען יותר מתמיד על טכנולוגיית מחשבים. המחלקה פועלת בשיתוף פעולה עם מרבית היחידות המובחרות של צה"ל, בעודה מפעילה אמצעים טכנולוגיים מתקדמים מגוונים על מנת לנטרל את התקיפות הקיברנטיות של האויב.[51]

במטרה להגן על מערכות המחשוב של צה"ל, פיתח חיל התקשוב תוכנית הכשרה המכונה "מסלול הגנת הסייבר". במאי 2012 הסתיים המחזור הראשון של קורס "מגן בסייבר" של החיל. לאחר מספר חודשי לימוד אינטנסיביים הוכשרו החיילים לבצע פעולות הגנה במרחב הממוחשב, על רקע המציאות הטכנולוגית המתפתחת.[52]

משרד הביטחון

בינואר 2012 פורסם כי משרד הביטחון עומד להקים מנהלת מיוחדת ללוחמה קיברנטית, שתרכז את כלל פעולות גופי הביטחון והתעשיות הביטחוניות העוסקים בפיתוח מערכות מתקדמות בתחום. במהלך שנת 2012 הוקמו מטות מיוחדים לעיסוק בלוחמה קיברנטית בתעשיות הביטחוניות המרכזיות, דוגמת אלביט מערכות, רפא"ל והתעשייה האווירית; גם התעשייה הצבאית שוקלת להיכנס לתחום[53]. טרם הוחלט מי יעמוד בראש המִנהלת החדשה, ואולם לדברי גורמים ביטחוניים, עצם ההחלטה להקים מנהלת חדשה "תיקח את העיסוק בתחום למקום חדש".[54]

הרשות למשפט וטכנולוגיה

בספטמבר 2006 הוקמה הרשות למשפט ולטכנולוגיה (רמו"ט) במשרד המשפטים. תפקידה הוא להגן על המידע האישי בישראל. יעדי רמו"ט הם חיזוק ההגנה על מידע אישי; הסדרת השימוש בחתימות אלקטרוניות ופיקוח עליו; הגברת האכיפה על עבירות פגיעה בפרטיות, בכלל זה עבירות המבוצעות במרחב הקיברנטי.[55] רמו"ט משמשת גם מרכז ידע בממשלה לחקיקה ולפרויקטים בעלי היבטים

טכנולוגיים, כגון ממשל זמין.[56] בימים אלה מטפלת הרשות בחקירת פרטי האירוע שבו פורסם באינטרנט מידע אישי רב, לרבות נתונים של כרטיסי אשראי, על ידי מי שהזדהו כהאקרים סעודיים.[57]

"ממשל זמין" – e-gov.il (תהיל"ה)

מערך "ממשל זמין" הוקם באגף החשב הכללי במשרד האוצר בשנת 1997 כיחידת תהיל"ה. מטרת פעילותו היא לאפשר לאזרחים לבצע מגוון פעולות רחב מול משרדי הממשלה ורשויות המדינה באמצעות האינטרנט, במקביל לשמירה על אבטחת המידע המועבר ועל פרטיות המשתמש. המערך מפעיל משאבים רבים לשמירת הפרטיות, החל בצוות מומחי אבטחת מידע וכלה בשימוש בטכנולוגיות אבטחה מהמובילות בעולם.[58]

סיכום

ישראל היטיבה לזהות את מאפייניו של האיום הנשקף כתוצאה מהתפתחות טכנולוגיית הלוחמה הקיברנטית, החלה לפעול ליצירת השינויים הנדרשים ונראה כי קיימת זיקה הדוקה בין אופן הטיפול באיום הקיברנטי לבין ביטחונה הלאומי של המדינה. אופן הטיפול מתרכז בשלושה נושאים: **הראשון** – ארגונים ביטחוניים, צה"ל, קהילת המודיעין והתעשייה הביטחונית, שבמצב הקיים פועלים להגן על מערכותיהם באופן עצמאי, ואינם מונחים על ידי השב"כ. **השני** – התשתיות הלאומיות הקריטיות שאפשר לתקוף אותן תקיפה קיברנטית, ומונחות על ידי הרשות לאבטחת מידע. **השלישי** – המגזר הפרטי, שבו פועלות חברות אזרחיות החשופות למתקפות קיברנטיות. שכבה זו מטופלת בחלקה על ידי רמו"ט, ובחלקה הגדול אינה מטופלת כלל.[59]

המלחמה הקיברנטית מתחוללת במלוא עוזה, וישראל היא שחקנית ראשית בה.[60] ניתן לבחון את העובדות היבשות ולהתרשם: הוקם מטה קיברנטי לאומי במשרד ראש הממשלה; מענקים בגובה מיליוני שקלים יוענקו בכל אחת מהשנים הבאות למחקרים ולפעילויות חינוך בתחום הקיברנטי; בצבא חולקה האחריות בתחום הקיברנטי בין אגף המודיעין (התקפה) ואגף התקשוב (הגנה); והרשות הממלכתית לאבטחת מידע צפויה להרחיב את פעילותה.[61] נראה שהטיפול בתחום הקיברנטי צובר תאוצה במספר היבטים מרכזיים: החל להתפרסם בגלוי מידע על אודות העיסוק הממשלתי באיום הקיברנטי, הוקצו תקציבים ייעודיים למחקרים בתחום ונעשה ניסיון לתקצב את פעילות המטה הקיברנטי הלאומי באופן שוטף. במקביל, גופים שונים הוקמו ו/או התפתחו מאוד במטרה להתמודד באופן מיטבי עם האיום הקיברנטי הגובר.

השינויים הטכנולוגיים המהירים שהתרחשו בשנים האחרונות השפיעו על סדר העדיפויות של מקבלי ההחלטות במדינה בדרכים שונות, ביניהן פרסום החלטות ממשלה רשמיות והקמת גופים ייעודיים להתמודדות עם האיום הקיברנטי. אף שבמבט ראשון נראה שישראל מתקדמת מאוד בדרך התמודדותה עם האיום הקיברנטי הגובר, עדיין יש מקום לנקיטת פעולות נוספות המגדירות בצורה ברורה יותר מהי המדיניות הרצויה לטיפול כולל בנושא.

הערות

1 דברי פרופ' יצחק בן ישראל ונוספים, מתוך: פרוטוקול מס' 95 – ישיבת וועדת המדע והטכנולוגיה: "לוחמה קיברנטית – הערכות מדינת ישראל למתקפות על רשתות מחשבים ותקשורת". יום שני, ב' תמוז תשע"א, (4 ביולי 2011), שעה 11:00. http://www.knesset.gov.il/protocols/data/html/mada/2011-07-04.html

2 לפי דו"ח של צוות חשיבה בינלאומי בנושא ביטחון – SDA (Security & Defense. Agenda) שנעשה בשיתוף חברת אבטחת המידע מקא'פי (McAfee) שהתפרסם בפברואר 2012: Cyber-security: The vexed question of global rules. An Independent report on cyber-preparedness around the world. With the support of *McAfee*. SDA, Belgium. בדו"ח זה קיבלה ארצות־הברית ציון של ארבעה כוכבים. http://www.mcafee.com/hk/resources/reports/rp-sda-cyber-security.pdf
ראו גם: אהוד קינן, "דו"ח: ישראל מוכנה יותר מארה"ב למתקפה מקוונת". YNET, 31 בינואר, 2012. http://www.ynet.co.il/articles/0,7340,L-4183126,00.html

3 נייר מטה לדיון הוועדה העליונה למדע וטכנולוגיה בנושא: **המיזם הקיברנטי הלאומי.** הצעה להקמת תוכנית לאומית לבניית יכולות קיברנטיות בשילוב היבטי מו"פ, כלכלה, אקדמיה, תעשייה וצורכי הביטחון הלאומי. תל אביב, נובמבר 2012, עמ' 18.

4 שמואל אבן ודוד סימן טוב, **לוחמה במרחב הקיברנטי: מושגים, מגמות ומשמעויות לישראל**, המכון למחקרי ביטחון לאומי, מזכר 109, (תל אביב: המכון למחקרי ביטחון לאומי, 2011).

5 זאב שיף, "דו"ח ועדת מרידור: חשש שמדינות מזרח־תיכוניות יצטיידו בגרעין בעקבות איראן", **הארץ**, 24 באפריל, 2006. http://www.haaretz.co.il/misc/1.1100503

6 שי שבתאי, "תפיסת הביטחון של ישראל – עדכון מונחי יסוד", **עדכן אסטרטגי**, כרך 13, גיליון 2, (אוגוסט 2010), עמ' 8–10.

7 אמיר בוחבוט, "משנים את תפיסת הביטחון", **NRG מעריב**, 24 באפריל, 2006. http:// www.nrg.co.il/online/1/ART1/076/915.html

8 ההצעה לא אושרה באופן רשמי בממשלה, בשל חילוקי דעות בין קברניטים. עם זאת, מרכיב ההגנה הפך לחלק מתפיסת הביטחון של ישראל באופן בלתי־רשמי.

9 "תפיסת הביטחון של ישראל – עדכון מונחי יסוד". עמ' 8–10.

10 רמי אפרתי וליאור יפה, "כך בונים הגנה קיברנטית לאומית", **Israel Defense**, 11 באוגוסט, 2012. http://www.israeldefense.co.il/?CategoryID=512&ArticleID=2960

11 יצחק בן ישראל . "לקחים טכנולוגיים", **מערכות**, גיליון מספר 332, (1993). עמ' 13.

12 עמוס ידלין, "הממד החדש של הלחימה – סייבר". **מבט מל"מ**, (ינואר 2010). עמ' 4. http://www.intelligence.org.il/KotarPort.aspx#http://malam.barebone.kotar.co.il/KotarApp/Viewer.aspx?nBookID=94837032&sSelectedTab=tdBookInfo%231.undefined.3.fitwidth

13 סוכנות הידיעות "רויטרס", "סטוקסנט שפגע באיראן – רק אחד מ־5 וירוסים", YNET, 29 בנובמבר, 2011. http://www.ynet.co.il/articles/0,7340,L-4168852,00.html

14 "כך בונים הגנה קיברנטית לאומית".

15 ליאור טבנסקי, "הגנה על תשתיות קריטיות מפני איום קיברנטי", **צבא ואסטרטגיה**, כרך 3, גיליון 2, (נובמבר 2011). , ע' 72.
החלטות לדוגמה: החלטת ממשלה 1886 בק/9 מ־20 במרס 1997: הקמת ועדת היגוי לנושאי מחשוב בכל משרד ממשלתי; החלטת ממשלה 3582 בק/77 מ־16 במרס 1998: אחריות לנושא אבטחת מידע במשרדי הממשלה; החוק להסדרת הביטחון בגופים הציבוריים 1998.

16 לפירוט נוסף על תהיל"ה ראו פרק אחרון במאמר זה העוסק בנושא בניין הכוח.

17 "כך בונים הגנה קיברנטית לאומית".

18 "הגנה על מערכות משובצות מחשב".
http://www.nsc.gov.il/NSCWeb/Templates/CounterTerrorismActivities.aspx.

19 "הגנה על תשתיות קריטיות מפני איום קיברנטי", עמ' 72–73.

20 בנובמבר 2010 הנחה ראש הממשלה על הקמת צוות מיוחד, שיעסוק בגיבוש תוכנית לאומית להצבת ישראל בין חמש המדינות המובילות בתחום הקיברנטי. העבודה בנושא, שכותנתה "המיזם הקיברנטי הלאומי", הובלה על ידי הוועדה העליונה למדע וטכנולוגיה, בראשות פרופ' בן ישראל. הצוות כלל נציגים מהגופים המרכזיים העוסקים בתחום הקיברנטי בישראל והורכב ממספר תת־צוותים שבחנו את המרכיבים החיוניים להתמודדותה של ישראל עם האיום הקיברנטי, וניתחו את התועלות הלאומיות בהיבטי הכלכלה, האקדמיה והביטחון הלאומי.

21 "המיזם הקיברנטי הלאומי", בתוך: **המועצה הלאומית למחקר ולפיתוח, דו"ח לשנים 2010–2011**. עמ' 10–17.
http://knesset.gov.il/committees/heb/material/data/mada2012-10-15.pdf

22 ההחלטה התקבלה בעקבות עבודת מטה מקיפה שבוצעה על ידי צוות לאומי בראשות יו"ר המועצה הלאומית למחקר ופיתוח , פרופסור יצחק בן ישראל.

23 "קידום היכולת הלאומית במרחב הקיברנטי". החלטת ממשלה מספר 3611 מיום 7 באוגוסט 2011.
http://www.pmo.gov.il/Secretary/GovDecisions/2011/Pages/des3611.aspx

24 "כך בונים הגנה קיברנטית לאומית".

25 יהודה קונפורטס, "דרושה: "כיפת ברזל" לסייבר שתגן על העורף", **אנשים ומחשבים**, 1 בפברואר 2012. http://www.pc.co.il/?p=79406

26 יוסי הטוני, "ד"ר אביתר מתניה: המרחב הקיברנטי מחייב התייחסות עסקית ולאומית־מדינתית; המסע לא קל", מתוך כנס CyberSec שהתקיים בפברואר 2012. **אנשים ומחשבים**, 12 בפברואר 2012. http://www.pc.co.il/?p=80025

27 שם.

28 דברי ד"ר אביתר מתניה, **כנס הסייבר הבינלאומי השני**, אוניברסיטת תל אביב, ב־9 ביוני 2012.

29 "כך בונים הגנה קיברנטית לאומית".

30 פרט לפרסום החלטת הממשלה על אודות הקמת המטה הקיברנטי הלאומי.

31 "מדיניות מו"פ לאומית כמערכת כלים שלובים", מסמך מסכם. מדברי פרופ' יצחק בן ישראל, כנס הרצלייה השנתי 2011. http://www.herzliyaconference.org/_Uploads/dbsAttachedFiles/OriSlonim2.pdf

32 "קול קורא למלגות בתחום: הגנת הסייבר ומחשוב מתקדם".
http://exactsci-info.tau.ac.il/exact_sciences/site/temp/cybersco.pdf

33 **תקציב המדינה – הצעה לשנות הכספים, 2011–2012 עיקרי התקציב ותוכנית תקציב רב־שנתית**. ירושלים, 2010. http://www.mof.gov.il/BudgetSite/StateBudget/Budget2011_2012/Lists/20112012/Attachments/1/Budget2011_2012.pdf

34 נייר מטה לדיון הוועדה העליונה למדע וטכנולוגיה בנושא: **המיזם הקיברנטי הלאומי.** הצעה להקמת תוכנית לאומית לבניית יכולות קיברנטיות בשילוב היבטי מו"פ, כלכלה, אקדמיה, תעשייה וצורכי הביטחון הלאומי. תל אביב, נובמבר 2012. ע' 20

35 "קידום היכולת הלאומית במרחב הקיברנטי", החלטת ממשלה מספר 3611, מיום 7 באוגוסט 2011.
http://www.pm.gov.il/PMO/Secretarial/Decisions/2011/08/des3611.htm

36 מתוך ראיון עם פרופ' יצחק בן ישראל בנושא המיזם הקיברנטי. התקיים בתאריך 5 באוגוסט 2012, באוניברסיטת תל אביב.

37 מתוך ראיון עם רס"ן טל, ראש תחום בכיר במטה הקיברנטי. התקיים בתאריך 23 באוגוסט 2012, במטה הקיברנטי, רמת אביב. תוכנית התקצוב המוזכרת טרם פורסמה בפומבי.

38 שם.

39 **שינויים בתקציב לשנת 2012**, פרוטוקול מס' 1069, ישיבת ועדת הכספים. יום שני, א' באייר התשע"ב (1 במאי 2012), שעה 12:30. www.knesset.gov.il/protocols/data/rtf/ksafim/2012-05-01-02.rtf

40 "התקציב ותוכניות העבודה של מטה הסייבר הלאומי אושרו על ידי ראש הממשלה נתניהו". 6 ביוני 2012. http://www.pmo.gov.il/MediaCenter/Spokesman/Pages/spokecyber060612.aspx

41 ב־13 נובמבר 2012 הודיע ראש מטה הסייבר הלאומי על השקת תוכנית קידמ"ה – קידום מו"פ הגנת הסייבר. התוכנית היא פרי שיתוף פעולה בין המטה לבין המדען הראשי במשרד התמ"ת, שמטרתו לקדם את המו"פ והיזמות בתחום ה־Cyber-Security במטרה לשמר את הפוטנציאל התחרותי של התעשייה הישראלית בתחום זה בשוק העולמי, ואף להעצימו.

42 חוזר המדען הראשי: "תוכנית קידמ"ה (קידום מו"פ הגנת הסייבר) לקידום יכולות התעשייה הישראלית בתחום הגנת הסייבר". 21 בנובמבר 2012.
http://www.moital.gov.il/NR/rdonlyres/89646959-5455-4A5A-99FD-C4B07D07E8E5/0/syber122012_3.pdf
ראו גם: "שמונים מליון ש"ח לקידום הסייבר", **IsraelDefenseTech**, 30 בדצמבר 2012, http://www.israeldefense.co.il/?CategoryID=760&ArticleID=3796

43 שמואל אבן ועמוס גרנית, "**קהילת המודיעין הישראלית – לאן? ניתוח, מגמות והמלצות**". מזכר מספר 97, תל אביב: המכון למחקרי ביטחון לאומי. מרס 2009. עמ' 64.

44 "יצחק בן ישראל, "לקחים טכנולוגיים", **מערכות**, גיליון מספר 332, (1993). עמ' 10.

45 כפי שפורט בהרחבה בפרק העוסק בקביעת האסטרטגיה.

46 מתוך ראיון עם רס"ן טל, ראש תחום בכיר במטה הקיברנטי. התקיים בתאריך 23 באוגוסט 2012 במטה הקיברנטי, רמת אביב.

47 מתוך דברי ראש הממשלה, מר בנימין נתניהו, **כנס הסייבר הבינלאומי הראשון**, אוניברסיטת תל אביב, 9 ביוני 2011.

48 עמיר רפפורט, "מתקפת סייבר על תשתיות לאומיות". **Israel Defense**, 8 בדצמבר 2011. http://www.israeldefense.co.il/?CategoryID=536&ArticleID=1421

49 עמיר רפפורט, "להגיב מהר כדי להיות רלוונטי", **Israel Defense**, 3 באפריל 2012, http://www.israeldefense.co.il/?CategoryID=512&ArticleID=2153

50 אמיר אורן, "זירת הלחימה החדשה של צה"ל נמצאת ברשתות המחשבים", **הארץ**, 1

בינואר 2010. http://www.haaretz.co.il/misc/1.1182490

51 "מקצועות המחשב מסלול מגן בסייבר", אתר חיל הקשר והתקשוב. http://www.tikshuv.idf.il/site/General.aspx?catId=60698&docId=76101

52 הדס דובדבני, "הסתיים קורס הסייבר הראשון בצה"ל. המטרה: שלושה מחזורים בשנה". אתר צה"ל. 3 במאי 2012. http://www.mako.co.il/pzm-soldiers/Article-595ec4bc4611731006.htm&sCh=3d385dd2dd5d4110&pid=1093150966

53 "חשיפה: מנהלת סייבר חדשה", **Israel Defense**, 12 בינואר 2012. http://www.israeldefense.co.il/?CategoryID=512&ArticleID=1657 – לא נמצאו פרסומים נוספים לגבי המִנהלת במשרד הביטחון, סביר להניח שמטעמי סיווג. ראו גם: "מתקפת סייבר על תשתיות לאומיות".

54 עמיר רפפורט, "חשיפה: תרגיל הגנת סייבר לאומי", **Israel Defense**, 19 בינואר, 2012. http://www.israeldefense.co.il/?CategoryID=512&ArticleID=1706

55 מתוך ראיון עם עו"ד יורם הכהן, ראש הרשות למשפט ולטכנולוגיה דאז, התקיים ב־5 בספטמבר 2012 בקריית הממשלה, תל אביב.

56 אתר הרשות למשפט, טכנולוגיה ומידע (רמו"ט) http://www.justice.gov.il/MOJHeb/ILITA/

57 הודעה לעיתונות בשם הרשות למשפט טכנולוגיה ומידע, משרד המשפטים, לשכת הדובר. http://www.justice.gov.il/NR/rdonlyres/4C39E414-E501-48C2-9C53-8EB533FD8B7D/32913/dover5.pdf

58 "אודות מערך ממשל זמין", http://e.gov.il/AboutUs/Pages/AboutUs.aspx

59 יוסי הטוני, "אל"מ (מיל') ד"ר גבי סיבוני: "יש שכבה שלמה של ארגונים שלא מוגנים מפני מתקפות סייבר", מתוך: כנס CyberSec 2012 המכון למחקרי ביטחון לאומי, ב־12 בפברואר 2012. **אנשים ומחשבים**, 15 בפברואר 2012. http://www.pc.co.il/?p=80466

60 אירועי ה־"סטקסנט", ה־"פליים" ונוספים, אשר על פי פרסומים זרים בוצעו על ידי ישראל.

61 "מתקפת סייבר על מתקני תשתית לאומית".

נשק סייבר ויציבות בינלאומית: איומים חדשים על היציבות מחייבים סוגים חדשים של דוקטרינות אבטחה[1]

גיא פיליפ גולדשטיין

מאמר זה בוחן את הסיכונים האסטרטגים של נשק סייבר ואת הנחיצות לפתח דוקטרינות ייחודיות להגנת סייבר, כדי לצמצם ככול האפשר את הסיכון להסלמת משבר עד לכדי יציאתו מכלל שליטה. כיום, לוחמת אינטרנט ממוחשבת, היא אחת מתוך כמה זירות צבאיות שצפויות לצמוח, הן בארצות הברית והן במדינות נאט"ו. המאמר הנוכחי מציע רעיונות ומסגרות עבודה מהספרות ה"קלאסית", העוסקים באסטרטגיה, במטרה לעצב תפישה מוסדרת יותר של הסיכונים הטמונים בנשק הסייבר ליציבות הבינלאומית, ובעקבות זאת, לזהות את סוגיות הליבה בהגנת סייבר, שישמשו נקודת משען לדוקטרינות עתידיות.

מילות מפתח: לוחמת סייבר, הרתעה, דוקטרינת הגנת סייבר, נשק סייבר, ארצות הברית, נאט"ו, אסטרטגיה, הערכת סיכונים

כבר בתחילת 2013, הפך מרחב הסייבר למוקד בעל חשיבות אסטרטגית. מפקדת הסייבר של ארצות־הברית היא מפקדה מאוחדת אחת, הכפופה לפיקוד האסטרטגי האמריקאי מאז 2009. כמו במבצעים אסטרטגיים או מיוחדים אחרים, גם כאן מחייבות החלטות מרכזיות קבלת אישור ישירות מנשיא ארצות־הברית. ההשפעות של נשק סייבר עשויות להיות כה נרחבות, עד ש"יש להתיר את השימוש בו רק בעקבות פקודה ישירה של העומד בראש כוחות הביטחון (המפקד העליון)".[2] לעומת זאת, מבחינת הפנטגון, חבלה ממוחשבת שמקורה במדינה אחרת יכולה להוות עילה למלחמה – כפי שהוצהר בצורה רשמית למחצה במגזין 'וול סטריט' ביוני 2011. האיום של מתקפות סייבר הוצב בראש רשימת סיכוני הביטחון הלאומי,

גיא פיליפ גולדשטיין הוא סופר; מחבר רב המכר **בבל שעת אפס**.

מאמר זה ראה אור לראשונה ב**צבא ואסטרטגיה**, כרך 5, גיליון 2, ספטמבר 2013, עמ' 103-119.

כחלק מהערכת האיומים הכלל־עולמיים של קהילת המודיעין לשנת 2013.[3] כיום, לוחמת רשת ממוחשבת היא אחת מתוך כמה זירות צבאיות שצפויות לגדול, הן בארצות־הברית והן במדינות נאט"ו.[4]

למרות כל זאת, לא פורסמה בנושא כל דוקטרינת שימוש ברורה כגון דוקטרינת ההרתעה הגרעינית. ראשית, דומה שכללים רבים נותרו חשאיים, ואך ורק במסגרת הדרג הגבוה ביותר של הבכירים. כמו כן, התחום עצמו אינו מוגדר בצורה ברורה: הוא יכול להיות תחום של לוחמה[5] או לאו דווקא, למעשה.[6] האם מרחב הסייבר קריטי רק משום שהוא תורם לביטחון הצבאי,[7] או שהוא חיוני בזכות עצמו, בשל ערכם העולה של הנתונים המאוחסנים ומוגנים בו? לבסוף, לפיתוח דוקטרינה נדרשים זמן ותקדימים היסטוריים. למרות שתפיסות של הרתעה גרעינית החלו לצמוח ב־1946 בעקבות עבודות של ברודי,[8] הדוקטרינה של 'השמדה הדדית מובטחת' (Mutually Assured Destruction) לא עמדה למעשה במקום מרכזי לפני סוף שנות החמישים.[9] בברית־המועצות, "גרף הלמידה" של האסטרטגיה הגרעינית היה אף מתקדם פחות.[10] השדה של מחקרי הסייבר עדיין צעיר יחסית, ונשק הסייבר עצמו מתפתח ללא הרף, ברמה ובהיקף.

אולם, מדוע היעדר דוקטרינה מציב בעיה חמורה? ללא מסגרת ניהול ראויה או דוקטרינה של יחסים בינלאומיים – הכנסתה לשימוש של כל טכנולוגיה הרסנית שטרם נבדקה מהווה פוטנציאל להשלכות בלתי־צפויות. הדבר נכון במיוחד בעסקי המלחמה. ללא מסגרת של דוקטרינה, הסתמכות בלעדית על פתרונות טכנולוגיים אינה ערבות לשימור הסטטוס קוו. יציבות במהלך 'המלחמה הקרה' לא הובטחה על ידי טכניקות הגנה כמו מערכות יעילות של טילים אנטי־בליסטיים. לא רק שמדובר בפתרונות טכנולוגיים חמקמקים – הם גם היו בלתי־רצויים לצורך שימור מאזן האימה העומד במרכז דוקטרינת ההשמדה ההדדית המובטחת (MAD). שתי המסקנות הובילו לחתימה על ההסכם להגבלת טילים אנטי־בליסטיים (TreatyABM) ב־1972.[11]

אין בכך כדי לבטל את הנחיצות של התפתחויות טכנולוגיות מסוימות – כמו למשל שיגור טילים בליסטיים מצוללות (SLBM) שמבטיחים יכולת מכה שנייה של השורדים, אולם אלה חייבות להתלוות לדוקטרינה סדורה שתחזק אותן ותמנע סתירות. הדבר נכון במיוחד למרחב הסייבר, שטבעו והסיכונים שבו מצביעים כי הגיע הזמן למאמץ מעין זה. ראשית, הנושא אמנם אינו מפותח דיו עדיין, אולם אין מדובר עוד בשלב הראשוני. אנו נמצאים יותר מ־15 שנה לאחר התרגיל האמריקאי Eligible Receiver בשנת 1997, שעורר בדרג הפדרלי את החשש הממשי הראשון בנוגע ללוחמת סייבר,[12] ומאחורינו כבר למעלה מחמש שנים שעומדות בסימן כמה וכמה תקריות סייבר ביחסים הבינלאומיים, החל מלוחמת הגרילה־סייבר בין רוסיה לאסטוניה ב־2007[13] ועד המתקפות הזרות נגד חברת ארמקו בערב־הסעודית,

שמקורן אולי באיראן.[14] אנו מגיעים לנקודה שבה יש לנו מספיק דוגמאות לניסוח ההנחות הראשונות בסוגיות ובדוקטרינות. שנית, ניתן לגשת לנושא מהזווית הקלאסית של מסגרות פוליטיות ומשפטיות. למרות שחייבת להינתן תשומת הלב לייחודיות התחום, אין צורך בגישת "לוח חלק". דוגמה עדכנית לכך היא Tallinn Manual – מחקר שבחן את ישימות החוק הבינלאומי בלוחמת סייבר, והצליח להחיל תקדימים משפטיים על מצבי לוחמת סייבר.[15] בהמשך לדוגמה זו, המאמר הנוכחי יבקש להחיל מסגרות מספרות האסטרטגיה ה"קלאסית", כדי להציע הערכה מוסדרת יותר של הסיכונים הטמונים בנשק הסייבר ליציבות הבינלאומית, ובעקבות זאת – לזהות את סוגיות הליבה בהגנת סייבר שיחייבו מענה באמצעות דוקטרינות עתידיות.

טיבו של מרחב הסייבר והסיכונים הנוכחיים בו

מהו מרחב הסייבר? השאלה נדונה בהרחבה, לרוב תוך התמקדות במרכיבים הטכנולוגיים (כגון ספקטרום אלקטרומגנטי, טכנולוגיות של מידע ותקשורת).[16] להלן מובאת הצעה למבט משלים שיהיה שימושי למאמר הנוכחי. מרחב הסייבר הוא השם העכשווי לכל מערכות המידע המבוססות על נתונים דיגיטליים. רדיו אלקטרומגנטי אנלוגי אינו חלק ממרחב הסייבר. הוא אינו יודע כיצד "לדבר דיגיטלית". מחשב דנ"א, לעומת זאת, שעובד עם נתונים דיגיטליים, מהווה חלק ממנו. קלטת אלקטרומגנטית שניתן להפעילה במכשיר הקלטה אנלוגי אך היא מקודדת בנתונים דיגיטליים – גם היא חלק ממרחב הסייבר. מידע דיגיטלי הוא השפה שבני־האדם יצרו כדי לדבר עם מכונות. מקורה במהפכה התעשייתית – במכונת האריגה של ז'קרד (Jacquard loom (1801), כאשר המורכבות הגוברת של מכונות חדשות עוררה צורך ביצירת שפה כזאת, וראשיתה בכרטיסי ניקוב. לאחר מכן נדרשו כמעט מאתיים שנה להתפשטות השפה בין המכונות, בייחוד לאור המצאות כמו מכונת החישוב של טיורינג ופרוטוקול האינטרנט. הסייבר מורכב משלושה רכיבים בסיסיים: חומרה (כולל ציוד טלקומוניקציה), תוכנה (כולל פרוטוקולים להעברת נתונים), ו"חוֹשבה" ("brainware") – החלק האנושי. בני־אדם הם חלק מהעברת הנתונים ומהווים נקודות יירוט פגיעות מאוד.[17] בני־אדם הם גם כותבי הקוד: חלק מהנשק המסוכן ביותר במרחב הסייבר כיום הוא המוחות המרושתים של האקרים מוכשרים. מבחינת תפקוד, ניתן לחלק את מרחב הסייבר לשניים: התמיכה הפיזית שמשפיעה באופן חומרי על התקשורת והחישוב, והתחום הסמנטי שמתרגם פעולות מהתמיכה הפיזית לנתונים, לפקודות ולמשמעות, ושולט בתמיכה הפיזית שלו עצמו.

תיאור פשוט זה של מרחב הסייבר מסייע להבין מדוע יש כיום דחיפות להגדיר את התנאים להגנת סייבר, ומהן נקודות התורפה הקריטיות ביותר במרחב הסייבר.

ראשית, החלוקה לנתונים דיגיטליים לעומת אנלוגיים מסייעת להבין מדוע הפכה לוחמת סייבר לנושא אסטרטגי רק לקראת סוף שנות האלפיים. המחשוב מלווה אותנו כבר למעלה מ־65 שנים, מאז תום מלחמת העולם השנייה. עם זאת, בשנת 1986 היוו נתונים דיגיטליים רק 0.6% מכלל הנתונים לאחסון, לתקשורת ולשידור, ו־24% בלבד בשנת 2000, אך שיעורם הגיע ל־93% ב־2007. בנקודה זו, יכולות המידע האנלוגי ה"ישן" הפכו לבלתי־חשובות.[18] כפי שניסח זאת מרק אנדריסן כעבור ארבע שנים: "התוכנה אכלה את העולם".[19] דבר זה יכול להסביר את התפוצה והפיזור של תקריות מתקפת סייבר במהלך הזמן: עד המחצית השנייה של שנות האלפיים העברנו לפורמט דיגיטלי את אחת מהמערכות הקריטיות ביותר שיש לכל מוסד או אורגניזם – את מערכת המידע שלו.

שנית, תיאור זה מדגיש את הממד הסמנטי. ממד זה משקף את מרכז הכובד האמיתי של מערכות מידע מרושתות. היעד של ARPAnet, הרשת שהולידה את האינטרנט, היה "להדגיש עמידות ויכולת הישרדות, לרבות היכולת לעמוד באובדן של חלקים גדולים מרשתות הבסיס".[20] רשתות מיתוג מנות (Packet switching) תוכננו כך שיעמדו בבלאי של חומרה. במרחב הסייבר, הנזק החמור ביותר מתרחש כאשר הנתונים נפגעים ומשמעותם מתעוותת, כפי שניתן היה לראות, למשל, ב"מבצע בוסתן"[21] או בסטקסנט. בשני המקרים, ההשפעה המרבית הושגה בעקבות הפעלת מניפולציה על אנשי שליטה ובקרה, באמצעות פגיעה במערכות פיקוד ובקרה. כמו כן, השחתת בקרים תעשייתיים שקובעים את קצב המנועים בצנטריפוגות $p-1$ השיגה חבלה ממשית יותר.[22]

מאפיינים של מתקפות סייבר

ביוון העתיקה, פירוש המילה 'לוגוס' היה המילה שנאמרה, המשפט, המשמעות הישירה של התיאור וגם הרעיונות העמוקים שהוא ביטא.[23] הייתה זו הגדרה מבלבלת אך עשירה. היא גם הובילה להאקרים הראשונים: הסופיסטים (המורים הנודדים). הסופיסטים תמרנו את המילים ואת התחביר כדי לעוות את המשמעות. מה שאנו מכנים כיום 'מרחב סייבר' הוא הלוגוס הדיגיטלי החדש שלנו. השפה שלנו מתוכננת לדבר עם מכונות, החל מהתמיכה הפיזית שלה דרך התרגום הסמנטי המיידי לפקודות המכוונות למכונות או לאנשים, ועד "ההזיה המוסכמת"[24] (consensual hallucination) של גיבסון. בלוגוס הדיגיטלי, הסופיסטים המודרניים פועלים כמו שוליית הקוסם של פול דיקא (Paul Dukas): אחד שולח את הקוד, וסביבת המכונות – שהיא מעשה ידי אדם – משתנה. מכונות נבנות כך שיאמינו לפקודות ולטיעונים שגויים. כך הן משנות את העולם הפיזי. איכות המתקפה תלויה בראש ובראשונה בכישרונו של הקוסם.

נשק סייבר פוגעני עושה שימוש בפרצות שנוצרו בעת ייצור המכשור[25] או הקוד או על ידי האדם המפעיל אותו, בין אם באופן טבעי ובין אם בכוונה תחילה, ואז מנצל זאת לפעולה נוספת. כדי להעריך ביתר דיוק את ההשפעות על העולם הפיזי, לוחמי סייבר בונים מודלים של חלקים מהעולם הפיזי, ואז בודקים את המתקפה עליהם[26]. נשק סייבר יכול גם להסתיר את חתימתו ומקורו.[27] מבחינת מידע, מאפיינים אלה מעניקים יתרון אסימטרי לתוקף ברגע שמתגלה ליקוי (או פִּרצה): רק התוקף יודע על הפִּרצה, ורק הוא יודע איזו מדינה תוקפת. אסימטריה זו במידע מעניקה יתרון ברור לתוקף. עם זאת, כיוון שמרחב הסייבר מתעדכן בהתמדה על ידי שדרוגי תוכנה והסביבה הפיזית של הסייבר משתנה בהתאם, יכולת הניצול לרעה מוגבלת וארעית: חיפוש או ייצור של פרצות מחייב מאמץ מתמיד.

השפעות של מתקפות הן מיידיות, ומתרחשות ברגע שהמחשבים מקבלים את המסר – הקוד תוקף ב"שעת האפס". טווח ההשפעות רחב ביותר, בשל השימוש הנרחב שהוסבר לעיל במכונות הדוברות את השפה הדיגיטלית: מריגול (חדירה למחשבים שמאחסנים מידע) וחבלה כלכלית (חדירה ו/או השחתה של מחשבים המאחסנים מידע בעל ערך פיננסי או כתובות IP), ועד חבלה פיזית (מתקפות נגד מחשבים ששולטים ומפקחים על סוגים שונים של תהליכים בתעשייה האזרחית או במערכות נשק טקטי או אסטרטגי). כיוון ש"התוכנה אכלה את העולם" וממשיכה לעשות זאת, אין גבול למה שאפשר לתקוף. להשפעות יש גם מרכיב פסיכולוגי. חובה להחליף ציוד שניזוק במתקפה קינטית. ציוד שנפגע ממתקפת סייבר עשוי להיות עדיין שמיש, אבל הספקות בדבר היכולות שלו יישארו לעד.

חוסר יציבות גאו־פוליטית כתוצאה מנשק סייבר – (I) מגמה התקפית ומהירות

המאפיינים הפוטנציאליים שהוזכרו לעיל במונחים של מגמה התקפית, מהירות ופוטנציאל להשפעות רחבות־היקף יוצרים סביבת טכנולוגיה צבאית שנוטה להפר את הסטטוס קוו. בניתוחו המקורי לתיאוריית התקפה־הגנה טוען רוברט ג'רוויס שתנאי דילמת האבטחה נשענים על שני "משתנים מכריעים": "האם ניתן להבחין בין מדיניות ונשק הגנתיים לבין התקפיים, והאם יש יתרון לאחד מהם – להגנה או להתקפה".[28] שילוב בין שני המשתנים האלה יוצר ארבעה עולמות אפשריים, וג'רוויס מציין שבעולם שבו "לא ניתן להבחין בין עמדה התקפית להגנתית" וכאשר "להתקפה יש יתרון", קשה ביותר למעצמות עולמיות לשמר את הסטטוס קוו. במקרה כזה, האמונות חזקות בדיוק כמו טכנולוגיה. מלחמת העולם הראשונה הייתה תוצאה של עולם כזה, שהוגדר "בעל סכנה כפולה". מעצמות־העל דאז למעשה הוּלכו שולל: הטכנולוגיות של מכונות הירייה ומסילות הרכבת נתנו יתרון

להגנה.[29] אולם עקב הניצחונות המהירים בקרבות של ביסמרק בעשורים שלפני כן, מעצמות־העל האמינו שטכנולוגיות צבאיות עדיין מעניקות יתרון להתקפה.[30]

ההקבלה לסביבה הצבאית שמעוצבת ונשלטת על ידי נשק סייבר היא ברורה. ראשית, קיימת אמונה מוסכמת שנשק סייבר מעניק יתרון למתקיף.[31] יתרון זה עשוי להיות טמון באסימטריה שבין המתקיף למתגונן בכל הנוגע למידע: תחילה, מעצם טבעה של הבעיה, הצד המתגונן מתעלם מקיום הפְרצה כל עוד אינה מוחשית. כמו כן, כאשר קיומה של הפְרצה בא לידי ביטוי זה עלול להיות מאוחר מדי. טיעון זה מצריך חידוד ואולי בחינה נוספת – אולם אינו קשור לענייננו. העובדה שיתרון זה יכול להיות מוגבל וזמני במציאות היא שולית מבחינת ישימות המודל שמציג ג'רוויס. כמו אירופה שלאחר ניצחונותיו של ביסמרק, מה שחשוב הוא האמונה שבאה לידי ביטוי בקונצנזוס הכללי. נקודה שנייה – נשק סייבר אינו ניתן לניטור. בקושי ניתן להבחין בין יכולת הגנה להתקפה. דוקטרינות של שימוש כפול, לרבות שימוש להתקפה והגנה גם יחד הופיעו בסין, אך גם במדינות מערביות מובילות.[32] יכולות הליבה כוללות נכסים שלפחות ממרחק ניתן לפרשם כמיועדים לשימוש התקפי או הגנתי – כמו תשתית IT או כותבי קוד. נכון להיום, בתחום נשק הסייבר, אין מקבילה למה שכונה בשיחות Salt II "ההבדלים הגלויים", כלומר, הסימנים ששימשו לזיהוי מטוסי תקיפה שנושאים טילי שיוט ארוכי־טווח.[33] קשה מאוד להבדיל בין פיתוח יכולת הגנה לפיתוח יכולת התקפה, שכן הגנה מקורה בעיקר בתרגולים של צוותי אבטחת מידע (Red-Team).[34]

הסיכונים של "סכנה כפולה" יכולים להחמיר גם עקב מתקפה מהירה שמשמשת מכת פתיחה. מתקפת פתע כזו שבאה "משום מקום" תהיה כה יעילה, עד שתמנע כל תגובה מהצד המותקף. בניתוח ראשוני של משחקי הרתעה הדדית הראה זאגארה שככל שהמשחק קצר יותר מבחינת מספר המהלכים, כך עולה הסבירות שהוא יפר את הסטטוס קוו.[35] התמריץ להכות ראשון משותף לכוחות שחולקים רמה דומה של פיתוח טכנולוגי. במקרה כזה, התפיסה שמדובר בסיכוני התקפה שווים תוביל למה ששלינג מכנה "חשש הדדי ממתקפת פתע".[36] כפי ששלינג מנסח זאת בספרו Arms and Influence:

> "[...]טכנולוגיה צבאית ששמה דגש על מהירות בזמן משבר שמה דגש על המלחמה עצמה.[...]אם הנשק יכול להיות מופעל מיידית בלחיצת כפתור או במתן "אור ירוק", ויכול להגיע ליעד כמעט ללא התרעה ולהסב הרס מוחלט, תוצאת המשבר תלויה בפשטות בשאלה, מי הראשון שימצא כי המתח בלתי־נסבל[...]"[37]

ניתן לראות ששורות אלה נכתבו כמה שנים לפני הקמתה של ARPAnet. הן מהדהדות בכתובים הראשונים של קציני חיל האוויר האמריקאי על המלחמה

בעידן המידע, כאשר ציינו כי "שימוש בכוח מקדים עשוי להפוך לתנאי מוקדם להצלחה".[38]

הדינמיקה המובילה לעימות מחריפה גם בשל ההשקעה הטכנולוגית המתמשכת במחקר ופיתוח של נשק סייבר. המניע להשקעה נוספת ניזון מהתרחבות מרחב הסייבר ליותר ויותר תחומי חיים אזרחיים וצבאיים, ומהצורך להגן על עולמות חדשים אלה במרחב הסייבר. היות שקשה להבחין בין יכולות מחקר ופיתוח של הגנה לאלה של התקפה, מטבע הדברים נוצר מרוץ חימוש. קצב ההמרה הפנימי של תהליכים לא־מקוונים בסייבר לתהליכים מקוונים אינו תמיד בשליטת הצבא: בהבדל ממהפכות אחרות בתחום הצבא שהונעו מתוך תחרות ממשית, הדחף לדיגיטליזציה של הצבא האמריקאי נמשך בקצב מהיר גם לאחר התפוררות ברית־המועצות.[39] ייתכן שניתן לראות בכך את התגלמות הדינמיקה האוטונומית של נתונים דיגיטליים ושל תוכנה שממשיכה "לאכול" את הצבא. במקרה כזה, גם האבולוציה האיכותנית של הטכנולוגיה עצמה יכולה לשבש את יציבות הסטטוס קוו. כפי שציין קיסינג'ר, מדינות יריבות עלולות לחיות בחשש כי "[...] הסכנה להישרדותן טמונה בפריצת דרך טכנולוגית של היריב".[40] ג'וינט וקורבט ציינו כי קצב השינויים יוצר "אי־ודאות מהותית בנוגע לטכנולוגיות מתקדמות": "[...] טכנולוגיה אינה יכולה לספק את התנאים המספיקים להשגת הרתעה יציבה".[41] ואכן, כדוגמה אזורית מביא הורוויץ את מרוץ חימוש הסייבר במזרח־אסיה כמגביר את אי־היציבות.[42] לבסוף, מעבר לזרועותיו המתארכות של הסייבר, היריבות הפנימית הדינמית והתסיסה המתמדת של תעשיית ה־IT מייצרים שדרוג מתמשך במרחב הסייבר עצמו. אולם שיפורים חיוביים אלה מהווים גם מקור לשינויים חדשים בשדה המשחק הצבאי, כמו למשל בהיבט של פרצות חדשות. די בגורם זה, שאינו תלוי ביריבות צבאית או פוליטית, כדי להאיץ באופן מכני את מרוץ החימוש.

חוסר יציבות גאו־פוליטית כתוצאה מנשק סייבר – (II) ייחוס וסף

בנוסף לתפיסת הסייבר כסביבה במגמה התקפית "נוטה לחיפזון" ותחום המשתנה בהתמדה מבחינה טכנולוגית, מרחב הסייבר מאופיין גם ביכולת לשקול מתקפה גם ללא (1) ייחוס ברור ו־(2) זיהוי ברור של הסף שחצייתו מסוכנת בעקבות המכה הראשונה. גורמים אלה תורמים לערעור נוסף של היציבות.

כפי שכבר צוין לעיל, היעדר חתימה – סוגיית הייחוס – מעניק יתרון לתוקף. אם הותקף, הצד המתגונן אינו יודע במי לנקום. יתרה מכך, הדבר פוגע בהגנה שלו שכן הוא אינו יכול להנחית מכת נגד שתוכל לפגוע ביכולות התוקף, או להרתיע אותו. ללא זיהוי ברור של התוקף, המותקף יתקשה גם להניע קשרים דיפלומטיים

כדי לארגן לחץ נגדי. אם ינקוט פעולת תגמול או הגנה נגד המדינות הלא־נכונות, הוא עלול להגביר את הבידוד שלו עצמו, ואף להביא להסלמה בזירה הבינלאומית. ייחוס אינו סוגיה של מה בכך. במשחקי מלחמה, זוהי אחת השאלות הראשונות ששואל השחקן שעומד בראש מערך ההגנה: "מי עשה את זה"?[43]

כדי לצבור רווח דיפלומטי, הייחוס צריך להגיע לרמה גבוהה של ודאות, ומבחינה טכנית קשה להשיג זאת בזמן מוגבל.[44] תוקפים פוטנציאליים יכולים לנקוט מדיניות של "הכחשה אמינה" (plausible deniability), שתנטרל את הקהילה הבינלאומית ותצמצם את טווח התמרון של המותקף. ניתן להסיק את הייחוס מההקשר הבינלאומי.[45] עם זאת, הדבר אינו שקול ליצירת "אקדח מעשן" באופן שאינו ניתן לסתירה, הדרוש כדי לשלב תמיכה דיפלומטית עם תמיכה צבאית חיצונית, בייחוד לנוכח הכשלים המודיעיניים שהובילו לפלישה לעיראק ב־2003. בנוסף, אפילו ההקשר הבינלאומי עלול להיות עמום. מאז ה־BrainVirus ב־1986, שהדביק דיסקטים דיגיטליים בכל העולם טרום עידן האינטרנט,[46] מרבית ההידבקויות בתוכנות זדוניות היו כלל־עולמיות בטבען. כל המכונות שמדברות בשפה הדיגיטלית רגישות להידבקויות דיגיטליות. למרות שעל סטקסנט נאמר שכוון ספציפית למתקני העשרת הגרעין באיראן, הוא נמצא גם בהודו, בסין, ברוסיה ובארצות־הברית.[47] דבר זה מקל עוד יותר על התוקף לאמץ את עמדת ההכחשה האמינה – גם הוא קורבן.

אי־הכרה בסף ברור מערערת מאוד את היציבות. בעבודתו הקלאסית על מלחמות "Arms and Influence" מציין שלינג את חשיבות הצבת סף בניסוח "סגנון המלחמה"[48] (idiom of war). שלינג מדגיש שעל מנת שהספים יבנו בצורה יעילה את הדיאלוג באווירה האלימה של המלחמה, עליהם להיות "פשוטים, ניתנים לזיהוי ובולטים".[49] לדוגמה, חצייה של נהר או הר, או תנועת כוחות צבא.

השאלה הופכת קריטית, שכן החישוב שמבצע כל שחקן תלוי ב"עקומת האמינות"[50] של כל משתתף – כלומר, בסיכונים שכל מדינה קיבלה על עצמה בעימות, בין אם מרצונה החופשי או מתוך אילוץ שכפה עליה היריב. סיכונים אלה תחומים באותם גבולות שהוזכרו לעיל. הם ממוקמים בתוך מערך היררכי, המארגן בצורה אמינה את שיטת הפעולה המקובלת על הממשלה. ההנחה שיש מידתיות שקשורה למערך ההיררכי היא המפתח לאמינות זו. הנחה זו מאפשרת את השליטה בדיאלוג האלים. אם חלה טעות בהבנת עקומת האמינות של היריב, נוצרת תפיסה של "חוסר איזון בפתרון",[51] שעלולה להכניס את העימות לסחרור.

לדוגמה, מדיניות הנקמה המסיבית לפי מסמך NSC-162/2 הוגדרה על ידי ויליאם קאופמן כחסרת אמינות, משום שיהיה זה 'לא על פי מנהגה של ארצות־הברית' לבצע אותה.[52] מנגד, כפי שזיהו זאגארה וקילגור בעבודתם על 'תיאוריית ההרתעה המושלמת', אמינות ההרתעה הגרעינית טמונה במתן העדפה לנקמה

על פני נסיגה.[53] העדפה זו נשענת על קיומו של איום סביר (במיוחד מכה שנייה של השורדים), אך גם על חישוב מושכל של נקמה: העדפה מושכלת כזו מייצרת אמינות. לדוגמה, אם הפגיעה היא במקום קדוש במדינה, במיוחד במרכזי האוכלוסייה שלה, ואם מדינה זו יכולה להגיב במכת נגד ועדיין לגרום נזק משמעותי לתוקף, אזי קיימת סבירות גבוהה שתעשה כך. הסיכון הגבוה משנה את חישוב התגמול. במצב כזה, המדינה תוכל לנייד משאבים פנימיים ביתר קלות, הודות ללכידות וקונצנזוס לאומי. האפשרות של תגובה חריפה יותר הופכת אמינה. ואכן בתחילת עידן הגרעין, לידל הארט ציין כי "קורבנות של תוקפנות מונעים מדחף בלתי־נשלט להגיב במכת נגד ללא קשר להשלכות [...]", ולכן "התוקף יהסס להפעיל פצצות אטום" בשל הסבירות לנקמה.[54]

כאן טמון קושי נוסף בהקשר של מתקפות סייבר: הן אינן מציעות אפיון פשוט, ניתן לזיהוי ובולט של הסף הנחצה. האם קשיים מסוימים בבנקאות מקוונת יובילו לפניקה פיננסית ולאסון כלכלי? ואם כן, בכמה שעות, ימים או שבועות מדובר? אם בעיר הבירה של המדינה המותקפת יש הפסקת חשמל, כמה אנשים עתידים למות תוך יום אחד? כאשר הייתה הפסקת חשמל בחוף המזרחי של ארצות־הברית במשך יותר מ־52 שעות ב־2003, ההשפעות היו מזעריות למדי, אם כי לא ניתן להתעלם מהן.[55] הפגיעה לאורך זמן אינה מתפתחת בהכרח בקו ישר. הקשיים נובעים גם מהיעדר תקדימים לשימוש בנשק המתפתח בהתמדה. עצם הפלישה ללא הרשאה של חיל אוויר זר למרחב האווירי של מדינה אחרת מהווה הפרה של הריבונות, אולם מה לגבי מתקפות סייבר שפוגעות שוב ושוב בשרתים שמשמשים חברות במדינה, אך ממוקמים מחוץ לגבולותיה? לבסוף, הפגיעות עשויות להיגרם מפעולות לא־ישירות או פסיכולוגיות. לדוגמה, בעצם החדרת ספקות באשר לשימוש הבטוח ביכולות צבאיות או אזרחיות, נשק סייבר יכול לעורר שיתוק גם אם לא חולל זאת ישירות. האם דומה הדבר לשיתוק שהוא תוצאה של פגיעה ישירה?

אפשר לנתח את ההשלכות על יציבות מתוך (1) היעדר ייחוס ו־(2) היעדר סף ברור באמצעות תיאוריית 'ההרתעה המושלמת'.[56] תיאוריה זו מניחה שעל מנת שאיום יהיה מרתיע, הוא חייב להציג מסוגלות: השימוש בו חייב ליצור פגיעה כואבת משמעותית לצד המאוים, כלומר, הצד המאוים יעדיף שלא לספוג אותה. האיום חייב גם להיות אמין: הצד המאיים חייב להיתפס כמי שמעדיף לממש את האיום על פני נסיגה. עם זאת, ללא חתימה, איום ההרתעה אינו כשיר עוד: הצד המאוים אינו יודע במי לנקום. התוקף החסוי אינו מאוים. גם הצד המתגונן אינו אמין אם הוא מאיים לפגוע "בהכול ובכולם" בתגובה למתקפות ממקור לא ידוע. באותה מידה, אם מזוהה ייחוס אולם קשה לאמוד את הפגיעה ולא ניתן להצביע על הסף שנחצה, אזי הנקמה לא תהיה "מידתית", אלא קשה מדיי או קלה מדיי.

ברמת המאקרו יש הסכמה גם בספרות העוסקת באסטרטגיה, כי אסימטריה או פערים במידע הזמין לכל אחד מהצדדים (מי תוקף? מה מותקף?) יובילו לעימות. כניסה לסחרור נחשבת כנובעת משגיאות בהערכה, או כפי שמנסחים זאת זאגארה וקילגור: "[...] אי־ודאות אסטרטגית ותגובה בלתי־צפויה, כאשר שתיהן יכולות להיות בעיקר תוצאה של טעויות שמקורן בכשל מודיעיני, בלבול בירוקרטי, חישוב שגוי או כל ליקוי אחר, בין אם בחשיבה ובין אם באיסוף המידע".[57] הסיכונים של כניסה לסחרור יגברו אם המדינות יגיבו במתקפות שמטרתן ליצור מידע כוזב במערכת של היריב. ניתן לראות גם במלחמה תהליך שנועד לפתור בעיית מידע: מה עוצמת המכה שמדינה יכולה להנחית על היריב?[58] התשובה לשאלה זו תאפשר יצירת סדר היררכי של המדינות. היררכיה זו תשמש מערכת מיקוח מסודרת ומובנת לכול. דבר זה מסביר כיצד הסיכוי למלחמה גובר כאשר שתי המדינות היריבות מחזיקות בעוצמה דומה, בהשוואה למצב פחות שוויוני (שאז תוצאת העימות ברורה).[59] עם זאת, שיטת הפעולה של לוחמת סייבר היא יצירת בלבול בנתונים. אופן פעולה זה מאיים לפגוע במידע אסטרטגי, ולחולל אי־ודאות וסיכונים שיערערו את הסטטוס קוו.

היעדר המחשה אמיתית ובקנה־מידה גדול של מתקפות סייבר הוא אחד הגורמים שהגביל עד כה את סיכון הסחרור. היכולת לפגוע בסוג כזה של נשק אינה ברורה כמו במקרה של נשק קינטי או גרעיני. עם זאת, היכולת של תולעת סטקסנט וההפנמה המתמשכת ש"התוכנה אוכלת את העולם" גם יחד הובילו לאחרונה מעצמות עולמיות להיות חשופות יותר לסיכונים מסוג הנשק החדש. התפיסות אכן משתנות בעקבות שינויים בשטח ושינויים בהכרזות הפומביות. המסגרות הפסיכולוגיות המעורבות במשחק, על פי ג'רוויס ועל פי תיאוריית 'ההרתעה המושלמת', הופכות רלוונטיות לסביבה גאו־פוליטית שנתונה להשפעה מתגברת של נשק סייבר.

סיכום – הצורך בדוקטרינות של "בקרת הסלמה" בהגנת סייבר

אין סיבה להאמין שה"דיפלומטיה של האלימות"[60] – כפי שמנסח שלינג את התעוררות תופעת הלוחמה – עתידה להיעלם במקביל להיטמעות הציוויליזציה שלנו במרחב הסייבר. בזמן בועת האינטרנט של שנות התשעים הראה מייקל פורטר כיצד "הכלכלה החדשה" של האינטרנט עשויה להדגיש סוגים מסוימים של יתרונות עלות על פני אחרים בחיפוש אחר בידול תחרותי[61]; אולם אין זה אומר שהכללים הישנים של האסטרטגיה ייעלמו. להיפך, המנצחים יהיו אלה שיצליחו "לראות באינטרנט השלמה לדרכים המסורתיות של התחרות ולא חלופה להן".[62] באופן דומה, "הכוח להכאיב" מגולם במלואו בסייבר – אבל אינו מחליף את כללי

האסטרטגיה. כפי שמציג זאת ג'ון שלדון, ניתן לבחון את עוצמת הסייבר דרך הממדים הקלאסיים של האסטרטגיה, כפי שהציגו מייקל הוארד וקולין ס. גריי.[63]

טכנולוגיות חדשות אינן מבטלות את סיכוני הסחרור בלוחמה. בקצרה, הדבר תלוי בהשפעות של כל טכנולוגיה על הגורמים הבלתי־משתנים המעוררים לוחמה כוללת: התפיסה שיכולות צבאיות אסטרטגיות נוטות לטובת התוקף, האפשרות שיכולות הצבא המתגונן ישמשו גם הן לתקיפה, מצב כניסה מהירה לפעולה שיקצר את משך ה"משחק" הצבאי, קצב מהיר של שינוי טכנולוגי שיש לו פוטנציאל להפר מחדש את האיזון בין כוחות הצבא (או זו לפחות התפיסה). עוצמתם של גורמים אלה היא שתשפיע על יכולת האיום והאמינות של כל שחקן, וכך תשנה את ההרתעה שבבסיס היחסים בין השחקנים. בסופו של דבר, ניתן לסכם את שאלת מאזן האימה כבעיית מידע: האם זיהיתי במדויק את היכולות האמיתיות של האויב – ושל עצמי? האם האויב יכול להבין את כוונותיי? היכן עוברים הקווים האדומים שלי – והאם אני מבין היכן עוברים הקווים האדומים שלו?

בשל כל השיקולים הללו, ובייחוד עקב היכולת להשחית נתונים ומידע אסטרטגי, נשק סייבר מגביר את הסיכון לכך ששגיאות מידע יסלימו מצב משבר לכדי מלחמה כוללת. הדיון שלעיל על (1) היעדר ייחוס ו־(2) היעדר סף ברור מסייע להסביר מדוע סיכון זה מתממש בצורה כה ברורה בנשק סייבר. יתרה מכך, הפתרון לשתי הסוגיות הופך דוחק אפילו יותר בשל טבעו של המשחק, שמתקצר בעקבות טכנולוגיה שעובדת במהירות האור ונתפסת כמגמה התקפית. כל אלה רק מדגישים עד כמה חיוני הצורך בדוקטרינה שתנהל את משבר המידע. לכן, דוקטרינה ליציבות הסייבר לא תתבסס אך ורק על היכולות לפעולת תגמול – כמו לדוגמה היכולת למכה שנייה מוכחת של השורדים, שנמצאת בלב ההרתעה הגרעינית, אלא, באותה מידה של חשיבות, היא תתבסס על היכולות להשיג בהירות ברמה האסטרטגית. אם לא ניתן לבסס את האמת לגבי הערכת הנזק והייחוס, אזי הצד המתגונן נמצא בסיכון לאחד מהשניים – להודות בתבוסה (אבל בפני מי?) או להיכנס לפעולת תגמול כשהוא "מגשש באפלה", תוך סיכון גבוה לסחרור העימות. לעומת זאת, אם מושגת ידיעת אמת ברורה, לפחות ב"חוֹשבה" של מקבלי ההחלטות האסטרטגיות ואולי אף בכל שאר מערכות התוכנה והחומרה של הצד המתגונן, אזי הצד המתגונן יוכל לפחות לעשות שימוש בכל שאר האופציות המסורתיות שברשותו, מאיומים דיפלומטיים ועד אסטרטגיים, על מנת לאלץ בצורה משכנעת את התוקף לסגת. ההקבלה ליעדי חיפוש האמת בקרב שירותי המודיעין אינה אמורה להפתיע. אם בסייבר, כמו במודיעין, "האמת משחררת",[64] הרי זה בין היתר משום ששניהם פועלים בתחומים אינפורמטיביים – האחד מבוסס על פורמט דיגיטלי והשני מבוסס על "חשאיות".[65]

קווי מתאר כאלה לדוקטרינות להגנת סייבר עשויים להיות דומים לאלה של פעולות הבהרה כגון חקירות משטרה או ריגול נגדי, אם כי בהובלת דרג אסטרטגי – כמו ראש מדינה. חקירות אלה ייתמכו ביכולות טכניות ניכרות ויפעלו לפי מתודולוגיות חדשניות לחיפוש האמת, החל מבדיקה דדוקטיבית לייחוס ועד סימולציית מערכות להערכת קווים אדומים. כמו כן, יהיה בהן מרכיב דיפלומטי משמעותי שימנף כמה מעגלים של שיתופי פעולה הדוקים. לא ניתן להגיע לאמת באמצעות מרכז אחד בלבד. מדובר בתהליך חברתי המבוסס על שיתוף בנתונים התומכים במסקנות ובשקילה זהירה של האילוצים הקיימים על פי ההקשר המודיעיני, או בהתבססות על היכולת לשכפל ניסויים.[66] מבחינה זו, דוקטרינות הגנה צבאיות למרחב הסייבר מקבילות במידה מסוימת לדרך שנקטו לאחרונה הנהלות תאגידים, משיווק[67] עד משאבי אנוש:[68] כזו שמאמצת גישה של פיקוח ומדע לפתרון בעיות. זוהי הדרך הבטוחה ביותר להגיע למקום הטוב ביותר בממלכת המידע: לאמת.

הערות

1 מאמר זה בוחן את הסיכונים האסטרטגים של נשק סייבר ואת הנחיצות לפתח דוקטרינות ייחודיות להגנת סייבר, כדי לקזז את הסיכון של הסלמת משבר עד כדי יציאה מכלל שליטה. פירוט דוקטרינות אלה הוא מעבר להיקף הדיון של המאמר הנוכחי. במאמר שייצא בקרוב אבחן כמה מהפתרונות לבעיות היציבות שיוצגו כאן.

2 David E. Sanger and Thom Shanker , "Broad Powers Seen for Obama in Cyberstrikes", *New York Times*, February 3, 2012.

3 Luis Martinez, Intel Heads Now Fear Cyber Attack More Than Terror, *ABCNews*, March 13, 2013, http://abcnews.go.com/Blotter/intel-heads-now-fear-cyber-attack-terror/story?id=18719593

4 Despite austerity cuts, the UK's cybersecurity budget has been expected to grow by some £650m ($1.07bn) over the 2012-2015 period. In James Blitz,"Country profile: UK defences are boosted to fight e-crime", *Financial Times*, June 2, 2011.

5 Keith B. Alexander, "Warfighting in Cyberspace", *Joint Forces Quarterly*, 46, 3rd quarter (2007): pp. 58-61.

6 Martin C. Libicki, "Cyberspace is not a warfighting domain", *I/S: A Journal of Law and Policy for the Information Society*, 8, no. 2, (2012): pp. 325-340.

7 שם.

8 Bernard Brodie, "The development of nuclear strategy", *International Security*, 2, No.4, (1978): pp. 65-83.

9 Lawrence Freedman, *The Evolution of Nuclear Strategy, Third Edition*, (New York: Palgrave Macmillan, 2003), pp.234-236.

10 שם, עמ' 243–244.

11 ראו לדוגמה: Lawrence Freedman (2003), p. 338

12 ראו ריאיון עם ג'ון האמר, לשעבר סגן שר ההגנה בין השנים 1997 ל־1999, בתוך: Michael Kirk, "Cyberwar!", *PBS*, April 24, 2003. http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/hamre.html

13 "Estonia hit by 'Moscow cyber war", *BBC News*, May 17, 2007, http://news.bbc.co.uk/2/hi/europe/6665145.stm.

14 Nicole Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back", *New York Times*, October 23, 2012.

15 Michael N. Schmitt, Gen. ed.,*Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, 2013).

16 Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem", in *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz (Washington D.C.: National Defense University Press,2009), pp.26-28.

17 שגיאות אנוש בתצורת האבטחה זוהו כ"אחראיות ל-80% מהפגיעויות של חיל האוויר" James A. Lewis ed., *Securing Cyberspace for the 44th Presidency,* Center for Strategic and International Studies, 2008, p. 55. צמיחתה של ההנדסה החברתית ומתקפות 'פישינג' הדגישו את חשיבות "הגורם האנושי" באבטחת סייבר. קווין מנדיה מציין: "בעוד הדורות הקודמים של המתקפות כיוונו לטכנולוגיה כמו רשתות ושרתים וניצלו פגיעויות בתוכנה, כיום התוקפים התפתחו והם מכוונים לחולשות ולליקויים אנושיים" בתוך: Kevin Mandia, "Cyber threats and ongoing efforts to protect the Nation*"*, *Permanent Select committee on Intelligence, US House of Representatives*, October 4, 2011.

18 Martin Hilbert, Priscila Lopez, "The World's Technological Capacity to Store, communicate and compute information", *Science,* 332, no. 6025 (2011):60-65.

19 Marc Andreessen, "Why Software is Eating the World", *The Wall Street Journal*, August 20, 2011.

20 Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, Stephen Wolff, *A Brief History of the Internet* (The Internet Society, 2012). ,http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet

21 David A. Fulghum, "Why Syria's Air Defenses Failed to Detect Israelis", *Aviation Week & Space Technology*, October 3,2007.

David A. Fulghum, "Israel used electronic attack in air strike against Syrian : וכן mystery target", *Aviation Week & Space Technology*, October 8, 2007.

22 Nicolas Falliere, Liam O Murchu, Eric Chien, *W32. Stuxnet Dossier*, (Symantec, 2010).

23 Barbara Cassin, CNRS, "Logos et Polis: La force du Discours", in Catherine Golliau ed., *La Sagesse Grecque* (Paris : Le Point Référence, 2011), p.41-43

24 William Gibson, *Neuromancer* (New York: Ace Science Fiction, 1984)

25 See for example the issue of kill switch in chips in Sally Adlee, "the hunt for the kill switch", *IEEE Spectrum*, May 1st, 2008.

26 For example, according to David Sanger (New York Times), when Israel and the US developed a "bug" to derail nuclear enrichment operations at Natanz plant in Iran, research teams "[…]began building replicas of Iran's P-1 centrifuges[…]" since "the bug needed to be tested". See David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran", *New York Times*, June 1, 2012. In particular, the Dimona complex in Israel may serve as a testing ground for cyber-attacks of centrifuges- see William J. Broad, John Markoff & David E. Sanger, "Israeli Test on Worm Called

Crucial in Iran Nuclear Delay", *New York Times*, January 15, 2011.

27 The issue of cyber-attacks attribution is a major difficulty explored in fiction (see for example, Guy-philippe Goldstein, *Babel Minute Zero* (Paris: Denoel,2007) and illustrated in real life episodes such as the cyber-attacks against Estonia in 2007 - see Mikko Hypponen,"9thof May", *F-Secure Weblog*, February 15, 2010, http://www.f-secure.com/weblog/archives/archive-052007.html

28 Robert Jervis, "The Security Dilemma", *World Politics*, 1978, pp. 187.

29 לדיון מפורט ראו: Charles L. Glaser and Chaim Kaufmann, "What is the Offense-Defense Balance and Can We Measure it?", *International Security*, Vol. 22, No. 4 (Spring, 1998), pp. 44-82.

30 Jervis (1978), p. 190.

31 ב־2009 הציג גרגורי ג'יי. רטריי את הנושא של "דומיננטיות המתקפה" במרחב הסייבר: ראו Gregory J. Rattray, "an environmental approach to understanding cyberpower" in F. Kramer, S. Starr, L. Wentz, "*Cyberpower and National Security*", National Defense University, Potomac Books, 2009. שלוש שנים לאחר מכן, דיוויד טי. פרנקרוג מהמשרד להערכת נושאי רשת/משרד ההגנה, ציין כי "ההנחה הנוכחית היא כי בסייבר לתוקף יש את היתרון המוחלט" David T. Fahrenkrug, "Countering the Offensive Advantage in Cyberspace: an Integrated Defensive Strategy", 2012 4th International Conference on Cyber Conflict, NATO CCD COE Publications, Tallinn.

32 תוכניות פיתוח צבאי חדשות שהושקו ב־2012 הן עבור DARPA והן עבור חיל האוויר האמריקאי מצביעות על עניין ברור בנשק התקפי, בתוך: Tom Gjelten, "First Strike: US Cyber Warriors Seize the Offensive", *World Affairs*, January-February 2013. בנוסף, במרס 2013, "[...]גנרל קית' אלכסנדר, שעומד בראש הסוכנות האמריקנית לביטחון לאומי ומפקדת הסייבר, העיד בפני המחוקק שהצבא הקים לפחות 13 יחידות שיהיו להן יכולות התקפיות בסייבר". "Obama Calls China Cyber Attacks 'State Sponsored'", News Wires, March 13, 2013). בצרפת, הפרויקט "Livre Blanc" לשנת 2013 ציין את הצורך ב־"Lutte Informatique Offensive" (LIO או "לוחמת סייבר התקפית" (בתוך Vincent Lamigeon, "Livre Blanc de la Defense: Les 5 nouvelles priorités imposes à l'armée francaise", Challenges, April 29, 2013).

33 ראו: Thomas K. Longstreth and Richard A. Scribner, "*Verifications of Limits on Air Launched Cruise Missiles*", in Frank von Hippel and Roald Z. Sagdeev, eds., *Reversing the Arms Race: How to Achieve and Verify Deep Reductions in the Nuclear Arsenals* (New York: Gordon and Breach, 1990), pp. 185

34 לסקירה אמריקאית קצרה ביותר, ראו: Zachary Fryer-Biggs, "Building Better Cyber Red Teams", *Defense News*, June 14, 2012.

35 Frank C. Zagare, "The *Dynamics of deterrence*", University of Chicago Press, 1987 – see discussion on rules relaxation and lengthening the game, pp. 48-56.

36 Thomas C. Schelling, "The Strategy of Conflict", Harvard University Press, 1960, Chap. IX, "The Reciprocal fear of surprise attack".

37 Thomas C. Schelling, "*Arms and Influence*", Yale University Press, 1966, pp. 225.

38 ראו: David S. Fadok, Major, USAF, "John Boyd and John Warden: Air Power's Quest for Strategic Paralysis", School of Advanced Air Power Studies, 1995, pp. 49. שנה קודם לכן כבר ציין ג'ון וורדן כי "לכידה וניצול של סַפֶּרת הנתונים עתידה להיות המאמץ החשוב ביותר ברוב המלחמות העתידיות". כיבוש 'סַפֶּרת הנתונים' (datasphere) מוגדר כעדיפות להצלחה צבאית, ראו: Col. John A. Warden III, USAF, "Air Theory for the Twenty-first Century", Chap. 4, in Challenge and Response:

Anticipating U.S. Military Security Concerns, ed. Karl P. Magyar, Maxwell AFB, Ala., Air University Press, August 1994.

39 ראו: Keith L. Shimko, "The *Iraq Wars and America's Military Revolution*", Cambridge University Press, p. 129.

40 Henry Kissinger, 'Arms control, inspection and surprise attack', *Foreign Affairs*, xxxviii:3 (April 1961), pp. 370.

41 Carey B. Joynt, Percy E. Corbett, "Theory and Reality in World Politics", Macmillan Press, London, 1978, pp. 92-93.

42 Michael Horowitz, "Information Age Weaponry and the Future Shape of Security in East Asia", *Global Asia*, Vol. 6, Summer 2011.

43 בנושא בכירי ממשל אמריקאיים שמתלבטים בפומבי בסוגיית הייחוס, ראו: John Markoff, David E. Sanger, Thom Shanker, "In Digital Combat, U.S. Finds no easy deterrent", *New York Times*, January 26, 2010; David E. Sanger, Elisabeth Bumiller, "Pentagon to consider cyberattacks acts of war", *New York Times*, May 31, 2011.

44 דוגמה עדכנית – לאחר שדרום־קוריאה התמודדה עם קריסה בו־זמנית של רשתות מחשבים בכמה מהמשדרים והבנקים מרכזיים ב־20 במרס 2013, היא טענה תחילה שמתקפות הסייבר הגיעו מסין Warwick Ashford, "South Korea says cyber attack came from IP address in China", *Computer Weekly*, March 21, 2013. למחרת הודתה דרום־קוריאה בטעות Warwick Ashford, "South Korea admits mistake in linking cyber attacks to China", *Computer Weekly*, March 22, 2013. שלושה שבועות לאחר מכן, האשימה דרום־קוריאה את צפון־קוריאה Warwick Ashford, "South Korea accuses North Korea of launching cyber attacks", *Computer Weekly*, April 11, 2013.

45 לתזה שממזערת את "בעיית הייחוס" באמצעות ניתוח ההקשר הבינלאומי, ראו: Richard L. Kugler, *Deterrence of Cyber Attacks*, Chapter 13, in F. Kramer, S. Starr, L. Wentz, *Cyberpower and National Security*, National Defense University, Potomac Books, 2009.

46 Rupert Goodwins, "Ten Computer viruses that changed the world", *ZDNet*, August 3, 2011.

47 Nicolas Falliere, Liam O Murchu, Eric Chien, W32. Stuxnet Dossier, Symantec, November 2010, pp. 6; Chinese infections in "Stuxnet 'cyber superweapon' moves to China", AFP, September 30, 2010.

48 Thomas C. Schelling, "Arms and Influence", Yale University Press, 1966, pp. 135: "שלבים סופיים בהתפתחות מלחמה או שינוי בהשתתפות. אלה קווי גבול או מקומות עצירה מוסכמים. יש להם אופי חוקי והם תלויים בתקדימים או בהשוואה למקרים דומים. יש להם תכונות שמאפשרות לזהות אותם, והם שרירותיים בחלקם. [...]אנו לא מייצרים אותם או ממציאים אותם, רק מכירים בהם. [...] נראה שכל סוג של עימות מרוסן זקוק לריסון ייחודי ששני הצדדים יכירו בו – נקודות עצירה בולטות, מוסכמות ותקדימים לציון מה נמצא בגבולות ומה מחוץ להם, דרכים להבחין מתי מדובר ביוזמה חדשה ומתי בפעילות שגרתית".

49 Thomas C. Schelling, "*Arms and Influence*", Yale University Press, 1966, pp. 137.

50 ראו: Carey B. Joynt, Percey E. Corbett, *Theory and reality in world politics*, University of Pittsburgh Press (Pittsburgh), 1978, pp. 94-95.

51 ראו: Frank C. Zagare, D.Marc Kilgour, *Perfect Deterrence*, Cambridge studies in international relations, 2000, pp. 301.

52 ראו: Freedman, 2003, p. 96 - citing William Kaufman, Military Policy and National Security, Princeton University Press, 1956, pp. 21, 24-25.

53 Zagare, Marc Kilgour, 2000, chapter 3.

54 ראו: Freedman, 2003 p. 40 citing B. M. Liddell Hart, *The Revolution in Warfare*, London: Faber and Faber, 1946 pp. 85-6.

55 במהלך הפסקת החשמל הגדולה בעיר ניו־יורק חלה עלייה גדולה במקרי התקפי הלב ובעיות נשימה, וכן נרשמו קריאות נוספות לשירותי רפואת החירום (Gary Kalkut, MD, MPH, Effects of the August 2003 blackout on the New York City healthcare delivery system: a lesson for disaster preparedness, Critical Care Medicine, January 2005, Volume 33, Issue 1, pp. S96-S101). לפי דיווחים מהעיתונות שצוטטו בוויקיפדיה, נמנו 11 קורבנות לא־ישירים.
http://en.wikipedia.org/wiki/Northeast_Blackout_of_2003;
עם זאת, מחקר נוסף מציין כי "דווח על מספר מינימלי של מקרי תחלואה ומוות שניתן לייחס לאירוע (בתוך: Kile J, Skowronski S, Miller MD, Reissman SG, Balaban V, Klomp RW,Reissman DB, Mainzer HM, Dannenberg AL: "Impact of 2003 Power Outages on Public Health and Emergency Response", *Pre-hospital and Disaster Medicine* 2005, 20(2), pp. 93-97.) ההערכות של סך העלויות בארצות־הברית נעו בין 4 ל־10 מיליארד דולר, או כמעט 0.1% מהתמ"ג האמריקאי, ראו: U.S.-Canada Power System Outage Task Force, August 14th Blackout: Causes and Recommendations, 2004, p.1

56 Frank C. Zagare, D.Marc Kilgour, *Perfect Deterrence*, Cambridge studies in international relations, 2000.

57 Frank C. Zagare, D.Marc Kilgour, *Perfect Deterrence*, Cambridge studies in international relations, 2000, pp. 302.

58 במילים אחרות, אם מדינות היו יודעות את התוצאה של מלחמה אפשרית, וכל אחת מהן הייתה מחזיקה במידע מושלם על היכולות וההחלטות של השנייה, סביר שהן היו נמנעות ממלחמה. ראו: Fearon, James D. 1995. Rationalist Explanations for War. *International Organization* 49 (Summer), pp. 379-414. and Dan Reiter, "Exploring the bargaining model of war", *Perspectives on politics,* Vol. 1, No. 1, March 2003.

59 Stephen L. Quackenbush, "General Deterrence and International Conflict: Testing Perfect Deterrence Theory", *International Interactions*, Vol. 36, pp. 60-85, 2010.

60 Schelling, 1966, Chap 1.

61 Michael Porter, "Strategy and the Internet", *Harvard Business Review*, March 2001.

62 שם.

63 John B. Sheldon, "The Dimensions of Strategy for Conceptualizing Cyberpower: Laying the Foundations for Sensible Cyber Security Policy and Doctrine", Presented to the panel on 'Comparative Cyber Security Strategies: Theory and Practice' International Studies Association Conference, San Diego, 2012.

64 מתוך Gospel according to St.John, נחקק במקור על חזית בניין ה־CIA – ראו: https://www.cia.gov/news-information/featured-story-archive/ohb-50th-anniversary.html

65 Dr. Michael Warner, "Wanted: a definition of intelligence", *Studies in Intelligence*, Volume 46, No. 3, 2002, pp. 20-21.

66 שיתוף נתונים הוא דרישת בסיס בכל הגשת מאמר לכתב־עת עם ביקורת עמיתים (ראו לדוגמה את ההמלצות עבור המגזין Nature בקישור http://www.nature.com/authors/policies/availability.html); אין ספק שבנושאי מודיעין, שיתוף חייב לאזן את הרווח עם הסיכונים מהחשיפה – או כפי שראש המודיעין הלאומי ג'יימס ר. קלאפר מכנה

זאת, הצורך למצוא את "הנקודה הרכה" בין שיתוף להגנה על מידע. ראו: Remarks and Q & A by Director of National Intelligence, Mr. James Clapper, 2010 Geospatial Intelligence Symposium, New Orleans, Louisiana, November 2, 2010, quoted in Richard A. Bets Jr., *Intelligence Information: Need-to-Know vs. Need-to-Share*, Congressional Research Services, June 6, 2011.

67 ראו את ההשפעה של A/B Testing בהנהלת חברות הסטארט־אפ של עמק הסיליקון ועד גוגל, בתוך:
Brian Christian, "The A/B Test: Inside the Technology That's Changing the Rules of Business", *Wired*, April 25, 2012.

68 ראו: Steve Lohr, "Big Data, Trying to Build Better Workers",*New-York Times*, April 20, 2013.

הגנת סייבר באמצעות אסטרטגיות של "צמצום מידע אסימטרי"[1]

גיא פיליפ גולדשטיין

"אם אתה יודע את האויב ויודע את עצמך, אל לך לחשוש גם לא ממאה קרבות. אם אתה יודע את עצמך אך לא את אויבך, אזי כל ניצחון שלך יִלָווה בתבוסה. אם אינך יודע לא את האויב ולא את עצמך, תובס בכל קרב".
סאן צו, אמנות המלחמה[2]

מאמר זה מתמודד עם שתי בעיות מרכזיות בהגנת סייבר: סוגיית ייחוס התקיפה (מי התוקף) וסוגיית סף ההחלטה (האם הפגיעה מצדיקה מלחמה כוללת). המאמר פותח בתרחיש של משחק מלחמה, ומציע מסגרת אנליטית המבוססת על "מדריך טאלין" לשרטוט מקרים של מלחמה ואזורי משבר. בהמשך מציע המאמר דרכים להתמודד עם משברי סייבר, וזאת באמצעות שתי אסטרטגיות של "צמצום מידע אסימטרי": טיפול בסוגיית הסף בעזרת הבנה טובה יותר של ההשפעות הגלויות והמדומות על מדינות מרושתות הפועלות כמערכת המתגוננות מפני מתקפות סייבר, תוך התבססות על הרעיון של קולונל ג'ון וורדן; טיפול בבעיית הייחוס, המחייב מצוינות בשיטות הליבון וההבהרה, וכן חקירה כופה הזוכה בתמיכה בין־לאומית – בהשראת מושג הכפייה (compellence) של תומאס שלינג. השליטה הגוברת של העולם הדיגיטלי בחברות המודרניות עשויה להפוך אסטרטגיות אלו לחלק מאבני היסוד של דוקטרינה חדשה להשגת יציבות צבאית ופוליטית במאה ה־21.

מילות מפתח: נשק הסייבר; הגנת הסייבר; הרתעה; דוקטרינה; אכיפה; מדריך טאלין

גיא פיליפ גולדשטיין הוא סופר; מחבר רב המכר **בבל שעת אפס**, הוצאת שוקן, 2010.

מאמר זה ראה אור לראשונה ב**צבא ואסטרטגיה**, כרך 5, גיליון 3, דצמבר 2013, עמ' 111–134.

מבוא – תרחיש אזורי

השעה 09:00 במדינה X. הכספומטים בבירת המדינה הפסיקו לעבוד. חלק מהלקוחות המקוונים של שלושה מהבנקים הגדולים במדינה לא מצליחים ליצור גישה לחשבונות הבנק שלהם. בחלק מהמקרים, נתוני החשבונות המקוונים נמחקו. טלפונים סלולריים כמעט שלא מתַפקדים. דומה שמדובר במתקפה מסוג חדש, שההשפעות שלה דומות למתקפות הסייבר של שנת 2007 באסטוניה, אולם מבחינה טכנית, הפעם הן לא נראות כמתקפות מפוזרות למניעת שירות: לא זוהתה כמות גדולה של כתובות IP המכבידות על השרתים. אין פתרונות מיידיים לתיקון התקלה ולא ברור כמה זמן היא תימשך. החרדה ברחובות מדינת X גואה במהירות. האם ניתן יהיה לשחזר את הנתונים? האם זהו גל ראשון המבשר על מתקפות נוספות?

מדינת X אינה לבדה. שבוע לאחר מכן, חברת אבטחת תוכנה ידועה ממדינה B זיהתה תוכנה זדונית חדשה: GlobalWorm. למרות שאופן פעולתה אינו ידוע ברגע הגילוי, נראה ש־GlobalWorm הדביקה מערכות רבות במדינות שונות. בהודעת התרעה שמוציאה חברת אבטחת התוכנה, היא מקשרת את המתקפה נגד מדינה X ל־GlobalWorm. מדינות נוספות שנפגעו מ־GlobalWorm חוֹוֹת קשיים, וביניהן מדינות ידידות של מדינה X וגם אויבות שלה, אולם מדינה X חווה את ההשפעות החמורות ביותר.

מי אחראי למתקפות על מדינה X באמצעות GlobalWorm? מהו סוג האיום ש־GlobalWorm מציב בפני מדינה X? כיצד עליה להגיב? התשובה לשאלה השלישית תלויה בשתי השאלות הראשונות.

כאילו המצב לא סבוך דיו, מתברר שלחברת אבטחת התוכנה, שבידיה המידע הרב ביותר על GlobalWorm, יש קשרים הדוקים עם המערכת הצבאית של מדינה B, שאינה ידידה קרובה של מדינה X. כאשר המועצה לביטחון לאומי של מדינה X מתכנסת, השאלות מתלהטות: האם זו מכה נוספת מכיוונה של מדינה Y – האויב המוצהר של מדינה X? האין זה נכון שמדינה Y הגדילה את השקעותיה בנשק סייבר? או שמא המתקפה מגיעה ממדינה Z, שקשריה עם מדינה X התערערו בצורה דרמטית במהלך חמש השנים האחרונות?

ראש מדינת X מנסח את שלוש השאלות המרכזיות שעומדות על הפרק:

1. האם תוכלו להוכיח לי שמדינה Y ומדינה Z לא קשורות לעניין?
2. כמה זמן עומד לרשותי לפני שיהיה עליי להגיב?
3. כיצד אוכל להגיב אם איני יודע את התשובות לשאלה הראשונה והשנייה ?

ראש המודיעין של מדינה X מאשר כי בשלב זה אין אינדיקציה ברורה שמדינה Y או מדינה Z עומדות מאחורי המתקפות, למרות שלא ניתן לשלול זאת. במקביל, הוא לא שולל את האפשרות שמדובר במניפולציה של מדינה B.

המתקפות אמנם זעזעו את אוכלוסיית המדינה, אולם לא הסלימו במהלך שמונה השעות האחרונות. לא ניתן לומר כיצד האיום עתיד להתפתח – אם הוא בכלל ימשיך להתפתח. מה שברור הוא שחלה פגיעה בעוצמתה של מדינה X. ללא נקיטת צעדים כלשהם לבירור הנושא, לשיקום העוצמה ולתגמול על הפגיעה, מעמדה של מדינה X כמעצמת סייבר יאותגר, דבר שאין להקל בו ראש. הסברה המקובלת בעידן הנוכחי היא שפעולות מלחמתיות גדולות יתחילו במרחב הסייבר, כך שהשליטה במרחב זה היא מבחן לעוצמה הצבאית הכוללת.

שר החוץ של מדינה X מקבל את רשות הדיבור. לדבריו, למדינה A, אחת מהידידות הקרובות ביותר של מדינה X בזירה הבין־לאומית, אין אינדיקציה ברורה על מקור ההדבקה ב־GlobalWorm. עם זאת, מכיוון שמדינה A רואה בכך בעיה עולמית, היא לא תתיר למדינה X להגיב ללא הוכחה ודאית מיהו התוקף. מעבר לכך, מדינה A טוענת שהתגובה צריכה להיות מתואמת היטב, למקרה שהיא תביא לעוד פעולות תגמול בסייבר, שכן גם מדינה X וגם מדינה A אינן יודעות כיצד GlobalWorm עובד. המצב שונה מתרחישים שבהם מדינה X היא הצד התוקף. מדינה X אינה שולטת בנתונים וגם לא בסביבה, ומהלך שגוי שלה עלול להתגלות כמסוכן עבורה, ואולי אף עבור שאר המדינות. ניתן לדמיין אינספור מניפולציות, והלא ידוע רב על הידוע.

מצב זה של בלבול אסטרטגי הוא אולי מה שהתוקף כיוון אליו כשתכנן את המתקפה. מדינה X עדיין אינה יודעת על מה ועם מי מתנהל השיג והשיח. ההצעה הברורה היחידה מגיעה ממדינה B: באמצעות חברת אבטחת התוכנה שלה, היא מציעה מומחיות ייחודית ב־GlobalWorm. מן הסתם יהיה לכך מחיר. בנוסף, מדינה A ומדינה B הן מדינות מתחרות בזירה הבין־לאומית. מדינה A עשויה להתנגד לכך שמדינה B תגיש סיוע למדינה X. היחסים בין מדינה A למדינה X עלולים אז להיפגע.

בתרחיש שתואר לעיל לא ניתן להסתמך על תגובה בכלים קונבנציונאליים או אסטרטגיים. למעשה, מדינה X ניצבת בפני שיתוק אסטרטגי. תיאוריית ההרתעה המושלמת קובעת כי האסטרטגיה האופטימלית היא "תגובה בעוצמה זהה" (response in kind)[3]. אסטרטגיה כזו תוכיח שהצד המותקף מחזיק באיום אמין לגמול על התקפה עליו. במקרה המדובר, יהיה בכך איתות שמדינה X אינה מחפשת בהכרח להסלים את המצב. פול הות' (Huth) תיאר מצב זה כסגנון משא ומתן "קשוח אך גמיש".[4] תגובה הנמנעת מהסלמה חריפה, ובמקום זאת מציגה עמדה קשוחה, מאפשרת לרמוז על אופציות מבלי ליישם אותן: זוהי העֶמדה המועדפת ביותר על פוליטיקאים, כמו גם על אנשי המערכת הפיננסית. זהו מצב אופטימלי גם כשמדובר בתהליכי החלטה בתחום הסייבר. אולם במצב הנוכחי שבו נתונה מדינה X, "תגובה בעוצמה זהה" אינה אפשרית. ראשית, ישנו מכשול

מרכזי: מדינה X אינה יודעת כלפי מי להגיב ונתקלת למעשה בבעיית הייחוס.[5] אבל גם אם הייתה יודעת בוודאות מי התוקף, אזי עומד בפניה מכשול גדול נוסף: היא לא בהכרח יודעת כיצד להגיב.

הבה נניח לרגע שמדינה X הוכיחה שמדינה Y היא הצד התוקף. מכיוון שנפרצו כספומטים של בנקים, חשבונות בנק מקוונים וכמה רשתות סלולריות, מדינה X מבקשת להגיב בעוצמה זהה. הבה נניח עוד שמדינה Y לא הקשיחה מראש את אבטחת הסייבר סביב מה שהיא יודעת שיהיו יעדי התגובה של מדינה X. נותר עדיין ספק גדול באשר לשאלה האם מדינה X תהיה מסוגלת לגרום לפגיעה במדינה Y לפחות באותה רמה כמו זו שהיא עצמה ספגה. אם היא תנסה לגרום נזק דומה אך תיכשל בכך, אמינות האיום שלה תיפָגע עוד יותר; אם היא תגרום לנזק גדול מדי, היא עלולה לעורר השלכות לא צפויות ולהכניס את העימות לסחרור. במצב הנוכחי של היכולות הטכניות, קשה לחזות במדויק את ההשפעות של נשק הסייבר, וקושי זה גובר עוד כאשר מדובר בשימוש מאולתר בנשק זה במטרה להשיג תגמול מהיר.

מדינה X ניצבת בפני בעיה נוספת: סוגיית הסף.[6] אין לה פתרון בדרך של תגובה בעוצמה זהה, כלומר אין לה יכולת לאיים בצורה אמינה בתגמול. דוקטרינה הדוגלת ב"תגמול מאסיבי" בסייבר עשויה להיות נתונה לאותה ביקורת כמו זו של וויל קאופמן על החלטה NSC-162/2 של נשיא ארצות הברית אייזנהאואר משנת 1954,[7] בתוספת אזהרה שהמונח "מאסיבי" קשה להגדרה, אלא אם מדובר בפגיעה מאסיבית וודאית באזרחים. מנגד, היעדר תגמול פוגע בבירור בעקרון ה"תגובה בעוצמה זהה", ועשוי להזמין תקיפה נוספת.

בשלב זה אין אופציות תגמול טובות למדינה X. אם המתקפות הגיעו לסף נזק מסוים ומדינה X תחוש מאוימת ממצבה הגיאופוליטי המשתנה, היא עשויה לרצות לרמוז לשכנותיה שיהיו השלכות למתקפה עליה. היא גם עשויה לנסות להוציא לפועל "תגובה בעוצמה זהה" שאינה מושלמת, בכך שתשים את הדגש על האיום האמין והקביל ביותר שיש לה – איום שאינו בתחום הסייבר אלא בתחום הקינטי, כמו הפגנת כוח אווירית או קרקעית. אם הייחוס לא יהיה ודאי, יהיו לכך השלכות דיפלומטיות נגדיות שיחזרו כמו בומרנג במקרה שמתקפות הסייבר יימשכו, וסופן שיעלו את הסיכון לפגיעה באמינותה של מדינה X (לאור העובדה שחשפה את היכולות הקונבנציונאליות שלה). מצד שני, אם מתקפות הסייבר לא גבו מחיר גבוה מדי, ומקורן נותר מעורפל, אזי ייתכן שמדינה X תרצה להפיג את המתח ולהפחית את הסיכון, ואז תוכל לייחס את הקשיים שנוצרו לבעיות טכניות או לגורמים שאינם מדינתיים. מדינה X תוכל אז להסכים לקבל סיוע ממדינה B דרך חברת אבטחת התוכנה שלה. כמובן שיהיה לכך מחיר, כפי שכבר צוין קודם לכן.

אסטרטגיה ראשונה של "צמצום מידע אסימטרי": הבהרת שאלת הסף בעזרת תהליך ומסגרת להערכת מתקפות סייבר

מסגרת ההערכה

למדינה X יכולה להיות דרך פעולה טובה יותר. כדי לתכנן את התגובה הטובה ביותר, עליה להבין אילו סוגי מתקפות עומדים בפניה. במיוחד עליה לפתור שתי בעיות שכבר הוזכרו: ייחוס וסף. הייחוס חייב להיות מקושר בצורה ישירה יותר לסוגיית "ההכחשה הסבירה" (plausible deniability), שכן מה שמוטל בכף הן ההשלכות הפוליטיות והדיפלומטיות של היעדר ייחוס. הגדרת הסף היא בעיה מורכבת אפילו יותר: ישנו קושי מובנה בהגדרה של "סף פשוט וניתן לזיהוי" במתקפות סייבר.[8] פעולות המתקרבות אל הסף ניתן לחלק לשתיים: כאלו שיש להן השפעה ישירה על המדינה (כמו שיבוש של ענף תעשייה ואובדן חיים), והכנות צבאיות (כמו תזוזת צבא ופעולות איסוף מידע) הקודמות לפעולות אלו שיש להן השפעה ישירה.

האם הצבת מלכודות לוגיות ברשת האלקטרונית של היריב מהווה פעולת מלחמה? האם יש מקבילה בלוחמת סייבר לתזוזת צבאות וריכוזם על הגבול? לשאלות אלו אין מענה פשוט, במיוחד משום שהן מתייחסות לנושאים כמו סוגיית הסף לפעולת תגמול על פי "עקומת האמינות"[9].

"מדריך טאלין" הוא נקודת מוצא לתשובות לשאלות אלו, אולם נכון להיום אינו מציע מענה מוסמך להן.[10] מבחינה כללית והיסטורית, אלו הן סוגיות המצויות בליבת ההתנהלות האסטרטגית של מדינות, שנענות כל אחת לגופה מתוך ראיית המציאות, אולם מבלי שגובש להן מענה רשמי ומקיף. אסטרטגיית הסייבר מחייבת מאמץ נוסף להמשגת התשובה. למרות שיהיה בכך משום חריגה ממסגרתו של מאמר זה, ניתן לציין בו כמה מראי דרך ראשוניים.

נקודת המוצא, המוזכרת בספרות העוסקת בלימודי לוחמת הסייבר וכן ב"מדריך טאלין", היא ההשפעה הישירה.[11] זוהי גישה שצבאות רבים בעולם יכולים להבין, החל מחיל האוויר של ארצות הברית, שהוא עדיין חסיד של מבצעים מבוססי־תוצאה המקשרים בין פעולות, תוצאות ויעדים.[12] כפי שמודגש ב"מדריך טאלין", לגישה כזאת יש גם תקדימים משפטיים, במיוחד סביב המונח "היקף ותוצאות".[13] יחד עם זאת, נותרת בעינה השאלה אילו תוצאות פירושן חציית קו אדום מבחינת הצד המתגונן? קל יותר להתחיל מִמה שנתפס כקביל או כנסבל, ולאחר מכן להבהיר מה לא יהיה קביל לעולם ויגרור תגובה צבאית אוטומטית, כאשר בין שני אלה שוכן השטח האפור של המשברים.

לדוגמה, ריגול הוא בגדר הנסבל (אם כי לא רשמית). הוא נהנה מסובלנות בין־לאומית, מכיוון שהוא "שלוחה של משטרים המקיימים פיקוח", דבר שמאפשר

שיתוף פעולה פונקציונלי.[14] דומה שחלק מסובלנות זו התפשט גם לכמה מ"יישומי הסייבר" של הריגול.[15]

מה שלא יהיה קביל לחלוטין ואף יצית תגובה צבאית אוטומטית, הוא מספר גבוה של קורבנות בקרב אוכלוסייה שאינה לוחמת. מקרה כזה יתורגם ככלל להפרה של דיני העימות החמוש בנוגע ל־*jus ad bellum* (צדקת המלחמה), כפי שנוסחו באמנת ז'נבה משנת 1949 ואושררו ב"מדריך טאלין".[16] מה שלא יהיה קביל לחלוטין מבחינה אסטרטגית, וייחשב כמלחמה, גם הוא ברור ממבט ראשון: הרס חלקי או מלא של מקומות מקלט (sanctuary). הדבר מתייחס גם לכל ניסיון משמעותי לפגוע בצורה הרסנית במוסדות המגנים על מקומות אלה. מכיוון שהמדינה מחזיקה במונופול על הפעלת אלימות בקנה מידה רחב,[17] פירוש הדבר הוא להגן הן על היכולת לממש אלימות בהיקף גדול והן על מרכז קבלת ההחלטות המפקח על השימוש באלימות. במונחים מעשיים, הגנה על מקום מקלט פירושו, בראש ובראשונה, הגנה על חיי האזרחים. מלחמה הופכת לבלתי נמנעת כאשר אומה סופגת אבידות כבדות.

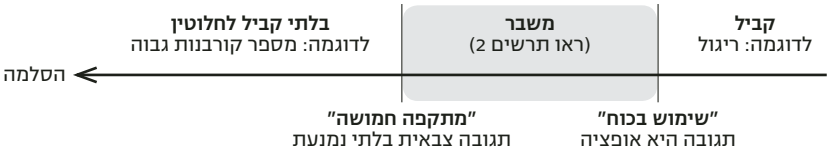
כשמדובר בהפעלת אלימות בקנה מידה גדול, ישנן כמה סוגי יכולות ומערכות שאין לפגוע בהן: בראש ובראשונה יכולת המכה השנייה של המדינה, אולם גם מערכות אחרות שכל תפקוד כושל שלהן עשוי לפגוע באופן משמעותי ביכולת להגן על מקומות המקלט. באלו נכללים מערכות התקשורת ברשת והחיישנים הספציפיים הדרושים להפעלת מערכות אלו, וכן מערכות תקשורת פנים־ממשלתיות החיוניות לראש המדינה ולצוותו לצורך פיקוד ושליטה ולשם תקשורת בין ראשי מדינות. תנאים אלה זכו להסכמת שתי המעצמות הגדולות במהלך המלחמה הקרה. ההסכם לאמצעים שיש לנקוט בעת תאונות (Accident Measures Agreement) וההסכם למודרניזציה של "הקו החם" (Hotline Modernization Agreement) משנת 1971 הגנו על תקשורת לוויינית החיונית להעברת מסרים בין ארצות הברית לברית המועצות בעתות משבר, כמו גם על מתקני התקשורת למערכות התרעה נגד טילים.[18]

ניסיונות לפעול נגד כוחות חירום ונגד אמצעים רפואיים שנועדו להגביל את מספר האבידות מהווים גם הם קו אדום. סוגיה זו זכתה להסכמתם של דיפלומטים רוסיים ואמריקאיים ב־2011 ונכללה גם ב"מדריך טאלין", וזאת במטרה להחיל את החוקים הקיימים של דיני העימות החמוש על ההתנהלות בתחום הסייבר.[19] המדובר באמצעים ובמערכות תקשורת לפיקוד ושליטה של כוחות חירום ורפואה, וכן לתקשורת עם ראש המדינה. חשוב לציין עוד שהגנה על מערכות התקשורת פירושה גם הגנה על נתונים מפני השחתה: אם לא ניתן להגן על הנתונים, המשמעות המעשית היא חבלה במערכות התקשורת המשמשות להעברת הוראות.

כאשר מדובר בהגנה כלכלית על מקום המקלט, יש לשאול את השאלה: באיזה שלב הופך הנזק הכלכלי לחמור כל כך, עד שמלחמה היא בלתי נמנעת? לפי ספרות מדע המדינה, קשיים כלכליים יכולים להביא לשינוי פוליטי: מיתון יכול להוביל להחלפת מפלגת השלטון במדינות דמוקרטיות,[20] ותקופות שפל יכולות להביא לשינוי משטר דרך עליית תנועות קיצוניות, כפי שאירע בתקופה שבין שתי מלחמות העולם.[21] אם תסיסה כלכלית כזו מקורה בחבלת סייבר, היא מהווה "פעולה כופה" שנועדה להרוס את שלמותה של המדינה.[22] תוצאה "פוליטית" זו עשויה להצטרף להגבלת משאבים שתוטל על צבאה של אותה מדינה כתוצאה מהקשיים הכלכליים. צמצום משמעותי במוכנות הצבאית הוא נקודת סף בפני עצמה. תרחישים אחרים עשויים להיות מניפולציה ישירה על מנגנוני הפיקוח הפוליטיים של המדינה (למשל, השחתה של מערכות הצבעה אלקטרוניות וסחיטה אלקטרונית המונית של נבחרי ציבור). אם רוב פוליטי יכול ליפול בעקבות חבלת סייבר, דינה של חבלה כזו הוא כדין ניסיון משמעותי לפגיעה בשלמות המדינה, ולכן כדין חציית קו אדום. אלו הן פעולות הפוגעות בצורה כה חמורה, עד שניתן לסווגן בקלות כ"בלתי קבילות לחלוטין". מתקפות שגורמות לתוצאות כאלו נחשבות ב"מדריך טאלין" ל"מתקפות חמושות".[23] בנקודת סף זאת, תגובה צבאית היא ודאית.

אם זהות התוקף ידועה, זהו חלק מ"שפת האלימות" המקובלת בין מדינות, וניתן להחיל עליה את כלליה של "שפה" זו. המדינות ייכנסו אז למשחק הסלמה – מתגובה קונבנציונלית ועד תגמול בעל פוטנציאל אסטרטגי. נשק הסייבר יהפוך אז לנשק נלווה לשאר מערכות הנשק,[24] אף שמדינות יכולות להגיב בעוצמה זהה עם נשק שאינו סייבר. הדבר יוסיף ממד של הבהרה ודגש לשיח זה. (ראו תרשים 1)

תרשים 1: מסגרת לקבלת החלטות בעלת סובלנות להשפעות



אם התוצאות ניתנות לזיהוי ומשפיעות על נכסים או על אוכלוסייה אזרחית, ואם זהות התוקף ידועה, אזי ניתן להגדיר את הפעולה כטרור. האקרים המאפשרים מתקפות כאלו, ללא ייחוס לאומי הניתן לזיהוי, פועלים כ"לוחמים בלתי חוקיים"[25] או כ"לוחמים חסרי זכויות".[26] הם אזרחים המעורבים ישירות בעימות חמוש, תוך הפרה של דיני המלחמה. מכיוון שלא ניתן לקשר אותם למדינה המחויבת לאמנת ז'נבה, ברגע שהמתקפה שלהם גורמת לנזק "בלתי קביל לחלוטין", הם מאיימים למעשה על כל המטרות האזרחיות. התגובה למתקפת טרור כזו חייבת להוביל

למאסר ההאקרים, או לכל הפחות להענשת המדינה המארחת אותם. זאת, בהתאם לתקדים המשפטי שנקבע בעקבות המתקפה על אפגניסטן לאחר אירועי 11 בספטמבר 2001, ובמיוחד לאור החלטות 1368 ו־1372 של מועצת הביטחון של האו"ם מ־2001.[27] כמו במקרה של טרור גרעיני הנעדר ייחוס, גם כאן, איסוף מודיעין הוא המפתח לפעולת תגמול.[28]

בין ה"קביל" ל"בלתי קביל לחלוטין" משתרע שטח אפור של משברים. הנזק במקרים הנכללים בשטח זה ברור דיו כדי שאותם מקרים יוגדרו כ"שימוש בכוח", אך עוצמתו אינה חמורה מספיק כדי להגדיר אותו בוודאות כ"מתקפה חמושה".[29] כפי שמציין בית המשפט הבין־לאומי לצדק, המצוטט ב"מדריך טאלין": "[...] לא כל שימוש בכוח עולה לדרגת מתקפה חמושה".[30] המשבר יכול להישאר נסתר מעיני הציבור – אופציית ברירת מחדל שנועדה למנוע התערבות ידיים רבות מדי בעולם חסר החוקים של מרחב הסייבר – אם כי הוא יהיה עדיין אמיתי. לאי־הוודאות במקרה זה יש סיבות רבות. התוצאות של מקרה "בלתי קביל לחלוטין" אולי טרם התממשו, אולם ניתן להתייחס אליהן כאל ודאיות: אם הבעיות בבנקאות המקוונת מתפשטות ונמשכות מספר שבועות, האם הדבר לא יוביל לפאניקה פיננסית? האם ההתאוששות תהיה פשוטה? כך גם לגבי מקרה של פריצת רֶשת החשמל, אף שביום השני לאירוע יהיה עדיין קשה לומר דברים ברורים.

לא רק שקשה להעריך את התוצאות הישירות, אלא שגם קשה להעריך מה המשמעות של פעולות צבאיות של האויב במרחב הסייבר, קרי של "תזוזת צבאות וירטואלית". זוהי נקודה קריטית, מכיוון שעל פי כללי המלחמה, כפי שנוסחו לראשונה על ידי סאן צו, ההפתעה היא המפתח לניצחון:[31] הלוחם הטוב יותר הוא זה שאינו יוצר דפוסים קבועים או תקדימים, ושצעדיו קשים לניבוי.

חובה להתמודד עם מצב זה של "שטח אפור" ולמפות אותו. ניתן להיעזר לצורך זה בקטגוריות ההסלמה שתיאר הרמן קאהן בספרו *On Escalation*.[32] מהי עוצמת המתקפה, מבחינת הסבירות שהיא תגיע לדרגה של "בלתי קבילה לחלוטין"? כמה מרכיבים שונים של המדינה כמערכת מותקפים? מהם ההתפתחות והקצב של המתקפה, במיוחד לאור העובדה שהאצה חדה בהם עלולה להיות סימן לפעולות צבאיות פיזיות העומדות על הפרק? הסיווג שמציע הרמן קאהן מאפשר לעשות הבחנה פשוטה בין:

1. מה שאינו קביל, אולם מבטא ריסון עצמי בהסלמה: המתקפה מוגבלת בעוצמתה ולא ניתן להגדירה כמאיימת על מי שאינם לוחמים. היא מוגבלת בהיקפה בכך שרק סוג אחד של מטרות מותקף; היא מוגבלת בממד הזמן שלה בכך שהתרחשה רק פעם אחת או פעמים ספורות בלבד, או שיש לה "תאריך תפוגה". מתקפות כאלו ניתן לסווג כמתקפות "מוגבלות".

2. מה שאינו קביל וניתן להגדירו כבעל פוטנציאל להסלמה: העוצמה או ההיקף של המתקפה נראים כנטולי ריסון עצמי ועלולים להסלים, או שיש חזרה והאצה שלהם לאורך זמן, ללא תאריך סיום ברור. מתקפות כאלו ניתן לסווג כמתקפות "מסלימות".

לדוגמה, אם GlobalWorm היה מכוון במודע לשנות את התפקוד של תוכנה או של ציוד ספציפיים בלבד, או אם התוכנה או הציוד שנפגעו מ־GlobalWorm היו רק לשימוש צבאי או לשימוש כפול, ולא הייתה זליגה למערכות נשק אחרות או לתשתית אזרחית, או אם השינוי שחל לא הוביל לנזק נלווה משמעותי בקרב כוח אדם אזרחי או בחיי אזרחים, או אם ל־GlobalWorm היה תאריך תפוגה ידוע (לדוגמה, כתוצאה מאישורים דיגיטליים שהגנו עליו ואשר נועדו לפוג במועד מסוים), אזי מתקפת GlobalWorm נגד מדינה X הייתה מוגדרת כמתקפה "מוגבלת". אולם נראה שאין זה כך במקרה של מדינה X: תוצאות המתקפה עליה אינן מוגבלות לציוד מסוים אלא הולכות ומסלימות, וכמו כן קשה לזהות מה יהיו ההשלכות המשניות שלה, למשל של היעדר פעילות בנקאית מקוונת במשך 48 שעות.

כדי לפשט את העניין, ניתן לצרף יחדיו תוצאות "מזוהות"[33] (שניתן לזהותן ולהבין היטב את כל ההשלכות המיידיות שלהן) אך "מסלימות", עם תוצאות שהן "קשות לזיהוי" (שלא ניתן להבין באופן מלא מה יהיו כל ההשלכות המיידיות שלהן). שני סוגי התוצאות מציגים סיכון גבוה להפתעה, לשיפוט שגוי ולהסלמה, כמפורט בתרשים 2.

תרשים 2 – מסגרת החלטות ל"משברים"

		אפיון התוצאות	
		מזוהות ומוגבלות	קשות לזיהוי / מזוהות ומסלימות
אפיון הזהות	ידוע	מִבצעים מיוחדים/ מכה מוגבלת. יריית אזהרה.	מתקפות נגד מערכות נשק טקטי. מתקפות בעצימות נמוכה נגד אזרחים.
	לא ידוע	מבצעים חשאיים. פעולת ריגול (שלא נחשפה).	מתקפת חבלה. טרור בעצימות נמוכה. פעולת איסוף מידע.

תהליך ההערכה

הקטגוריה של תוצאות "קשות לזיהוי" הינה בעייתית במיוחד. קשה להשיג דרגה מספיקה של חיזוי לתוצאות אלו: לא מדובר בנזקים "סבירים לחיזוי", אם להשתמש בביטוי שמופיע ב"מדריך טאלין";[34] לא די בהסתמכות על צפייה בתוצאות, מקיפה ככל שתהיה, תוך התמקדות במודיעין, או בניתוח צורת הפעולה של התוכנה הזדונית בסביבת התוכנה שלה; גם לא ניתן להגיע, בעזרת צעדים חיוניים אך בלתי מספקים אלה, להערכת ההשלכות על "מדינה הנתפסת כמערכת" – אם להשתמש במונחים של קולונל ג'ון וורדן.[35] הערכה כזו היא תוצאה של בניית מודלים, הדמיה וניתוח מערכות, כולל רכיבים חברתיים וכלכליים. המטרה של ניתוח כזה היא להעריך את הנזק הפוליטי הצפוי למדינה המותקפת. בהקשר הגנתי, הצעד הבא יוביל באופן טבעי לניתוח, באמצעות תהליך של הִנדוס לאחור, של "מבצעים מבוססי תוצאה". המטרה היא לא להשיג את הדיוק הדרוש לשימוש התקפי ב"מבצעים מבוססי תוצאה", שהיה קשה למדי להשגה עד היום, עם כלי התוכנה הנוכחיים;[36] המטרה היא להטמיע, כחלק מהשימוש ההגנתי, צורה של לוחמת סייבר שנקודת הסף שלה מוכרת מבחינה בין־לאומית ושתקשר את פעולות הסייבר עם יעדים רצויים ועם תוצאות ישירות. הדבר גם ישמש למתַן תוקף חוקי לכל סוגי התגובות, לרבות פעולות קינטיות או דיפלומטיות. או אז, הקטגוריה של "פשוט, בולט וניתן לזיהוי" תהפוך לקטגוריה של "מדויק ביותר".

כדי שאפשר יהיה לתת אמון בצורת לוחמה זו, חיוני שמעצמות הסייבר המובילות יצהירו עליה. השתתפות מדינות נוספות בגיבושה, על פי אותו הגיון מרכזי משותף, תבטיח שהיא גם תוכר על ידי גורמים רבים, ובאופן כזה גם תהפוך לשיטה הבולטת והמקובלת. כדי להיות גם אמינה, יהיה עליה לשקף את ההשפעה האמיתית שיש לה על עקומת האמינות של המדינה. לשם כך, יהיה צורך לפעול על פי המתווה של קולונל ג'ון וורדן ולפתח מסלול של מחקר והדמיות, שמטרתו להבין את מהותה של "המדינה המרושתת כמערכת". במסגרת זו ניתן יהיה לבחון ב"טווחי סייבר" וירטואליים לא רק את האינטרנט, אלא גם רכיבי משנה של המדינה.

ארגונים ומערכות תשתית שונים לוקחים כיום חלק בהפצת "נתוני ענק" (big data) – החל מפרויקטים של נתונים פתוחים במגזרים ציבוריים, דרך ממשקיAPI בתהליכים פנימיים של תאגידים ותעשיות,[37] וכלה בשימוש חברתי ופוליטי, כפי שהוא מתבטא ברשתות חברתיות. כל אלה מסייעים בפיתוח מודל בסיסי משופר ומדויק יותר של "המדינה המרושתת כמערכת". מודלים דינמיים אלה של מידע יכולים להיבדק אז מול הדמיות של מקרי אלימות. במקרה זה, הדייקנות פחות חשובה מאשר הערכות אמינות ומוסכמות. התפתחות זאת תהיה כרוכה במאמץ מתמשך, שכן מרחב הסייבר מתפתח ללא הרף.

הבנה של נקודת הסף אינה פותרת את הבעיה המרכזית השנייה בתחום המידע, והיא שאלת הייחוס. בעיה זו מחייבת מאמץ ייחודי המעֵרֵב מודיעין, כפייה ודיפלומטיה.

אסטרטגיה שנייה של "צמצום מידע אסימטרי": הבהרת שאלת הייחוס בעזרת "כפייה משותפת"

מכיוון שמרחב הסייבר נשען על שלושה יסודות – חומרה, תוכנה,[38] ו"תודעת רשת" (brainware) – על המודיעין לחקור ולפתח השערות לגבי כל אחד משלושת היסודות האלה. מערך הייחוס צריך להיות מורכב מאוסף של סימנים אופייניים שונים, כמו דפוסי תעבורת IP, סגנונות קידוד ושיטות פעולה. יש לכלול גם מודיעין אנושי "קלאסי" על ההאקרים עצמם ועל נותני החסות הפוליטיים שלהם. פעולות חקירה אלו צריכות להשתמש בשיטות העבודה הטובות ביותר בתחום ליבון הנתונים, תוך שימת דגש על שיטות דדוקטיביות המיושמות במודיעין, כפי שמציע יצחק בן־ישראל.[39] לפי אחת המתודולוגיות של עבודת המודיעין,[40] השערות ייחוס יכולות להיות מוצגות בקבוצות שונות (כגון, "השערה 1: מדינה Y היא התוקפת"; "השערה 2: מדינה Z היא התוקפת"). לאחר מכן ניתן להעמיד נתונים אמפיריים המפריכים כל השערה בכל קבוצה. צבירת נתונים מול השערת הייחוס תהיה השלב הראשון בניסיון לענות על השאלה איזו מדינה היא החשודה העיקרית בתקיפה.[41] הדבר יחייב לזהות מראש את המודלים הרבים של ההכנות הדרושות לפתיחה במתקפת סייבר מאסיבית על ידי מדינה כלשהי ולעשות הדמיה שלהם. מודלים אלה יכללו, כמובן, גם מאמצים נוספים להסתרה ולהקשחת ההגנה. במצב אידיאלי ניתן יהיה לערוך בשלב זה מבחני דדוקציה A/B, בצורה של ניסויים מבוקרים ב"נאשמים" אפשריים, כדי לאשר או להפריך השערות ייחוס. לדוגמה, ניתן לעשות שימוש באחת מהאסטרטגיות ששימשו את הדמות הבדיונית ג'ורג' סמיילי: הדמיה של השפעות בלתי צפויות של תוכנה זדונית עשויה לחשוף את מקורה האמיתי, וזאת בשל חוסר נוחות ומבוכה פתאומיים שהיא גורמת.[42] איתור חוסר נוחות כזה יכול לסייע לקביעת הייחוס.

חתירה אל האמת היא קריטית ליצירת הגנה וחיונית לשכנוע בעלות ברית שאין כוונה לתמרן אותן. אם מדינות אלו ישוכנעו בכנות הדברים, הן יוכלו להיות "עדי אופי" בפני דעת הקהל העולמית ולספק קונצנזוס דיפלומטי רחב יותר לאופציות התגמול. חתירה אל האמת גם תבטיח שהדרג הפוליטי של המדינה המתגוננת לא יטעה טעות חמורה בייחוס המתקפה, ושלממשלתה יהיה ביטחון מלא בהחלטותיה. בשלב זה תימצא הממשלה במקום נוח יותר לבחון אמצעים לא פומביים ולא מענישים, אם אלה הם אכן האמצעים הנדרשים. כמו בכל עבודת

ריגול נגדי, ייתכן שטוב יותר לשמור לזמן מה את האויב באשליה שתחבולותיו טרם נחשפו.

במרחב הסייבר, כמו בכל תחום מידע אחר דוגמת המודיעין ה"מסורתי",[43] אמת היא כוח. האמצעים והשיטות לביסוס אמת שלכאורה אינה ניתנת להפרכה הם המפתח לכוח, ולכן המפתח להשפעה. יבוא יום שזירת הדיפלומטיה בסייבר תִדמה לזירת האינטרנט האזרחי הרגיל, שבו כמה ממנועי החיפוש הגדולים ביותר או ספקי תוכן (כמו ויקיפדיה) מתחרים על מקומם כבעלי הרלוונטיות הגבוהה ביותר. היכולת להפריד ולבודד את האות הנכון היא התכונה החשובה ביותר של כל מערכת מידע.

מן הסתם, קשה לשתף מספר רב של מדינות בנתונים ובטכניקות של קביעת הייחוס שצוינו לעיל, כפי שמקובל לרוב בשיתוף פעולה מודיעיני. בעולם ההופך בהדרגה לרב־קוטבי, אם לא תימצא דרך לטפל בהבהרת סוגיית הייחוס או לנהל אותה במשותף, הדבר עשוי להוביל לשיתוק יכולת ההגנה או לחילופין לירידה באמינות ההרתעה. ייתכן שניתן למצוא שיטה כזו באמצעות מבחן דדוקטיבי רחב היקף ופומבי, במיוחד לאור העובדה שדדוקציה היא שיטה מעולה להבהרת האמת בניתוחים מודיעיניים.[44]

ריצ'רד קלארק ורוברט נֶייק מדגישים בספרם *Cyberwar* את "עקרון ה־רֶסָנִיסְט": נטל החקירה צריך להיות מועבר מהחוקרים אל המדינה שממנה שוגרה המתקפה.[45] אם המדינה החשודה תסרב לשתף פעולה, היא תיחשב לאחראית. במקרה כזה, גוף בין־לאומי, שקלארק ונייק מכנים "צוות בין־לאומי לציות וזיהוי פלילי בסייבר", יהיה רשאי להציע סנקציות סייבר, החל מהשבתת ספקי שירותי אינטרנט מסוימים ועד חסימת אותה מדינה בפני מרחב הסייבר.[46] הישענות על גישה זו והרחבתה מאפשרות לטפל באופן ממשי בכמה מקרים של לוחמת סייבר, שהם בעלי פוטנציאל להיות חמורים במיוחד, ולשקם מחדש את הרתעת הסייבר. בנוסף לקביעת עצם הייחוס באמצעות "עקרון הארסניסט", גישה כזו יכולה לייחס מעשית את המתקפה לתוקף מסוים. במונחים דיפלומטיים, היא יכולה למנוע מהתוקף את השימוש ב"הכחשה סבירה". ביסוס הייחוס הוא חקירה מודיעינית לא פחות משהוא תהליך דיפלומטי, שבֵּן יש לפעול לשכנע בו מדינות נוספות.

אמינותה של האמת מושגת טוב יותר כאשר משקיפים (או בוחנים) חיצוניים מאשרים את השערת הייחוס. תהליך חברתי זה קיים מאז "כלל שני העדים" במשפטי בגידה בימי אנגליה האליזבתנית,[47] דרך הכלל של הופר בנוגע ל"עדות בו־זמנית",[48] ועד לשיטות הסטטיסטיקה המודרניות, שבהן עולה הביטחון בתחזיות ככל שגדֵל מספר התצפיות. מבחן ברמה הציבורית מחייב שמדינות ותושביהן יהפכו לתצפיתנים.

תהליך דיפלומטי יבטיח תיאום טוב יותר, ולכן יחזק את מצור הסייבר שיש להטיל כדי ללחוץ על מדינות חשודות. חוזק המצור חיוני כדי שהאיום יהיה אמין. אם ניתן יהיה להתגבר עליו, כפי שמעצמות המערב הצליחו לעשות במהלך משבר ברלין ב־1948 כנגד המצור שהטילה ברית המועצות על העיר, אזי המדינה המאיימת תיכשל במאמציה[49]. אם לא ניתן יהיה להתגבר על המצור, אזי המדינה המאוימת תיאלץ לבחור בין הסלמה ובין נסיגה, וכאשר הסיכון לעצמה יהיה גבוה מדי, יש סיכוי סביר שהיא תבחר לסגת, כפי שברית המועצות עשתה במהלך משבר הטילים בקובה ב־1962. בנוסף לכך, קידום תהליך הייחוס – תחילה עם ידידות קרובות ולאחר מכן עם קבוצה גדולה יותר של מדינות – יוביל ליצירת רצון טוב, להתקרבות וליתר הבנה כלפי המדינה המתגוננת. מצב זה נותן למדינה המתגוננת שוליים פוליטיים לתמרון, אם תבקש לפעול להטלת סנקציות דיפלומטיות, כלכליות או צבאיות נוספות מעבר למרחב הסייבר ולמצור הסייבר. הדבר יתרום לאמינות נוספת לְמה שביסודה היא אסטרטגיה כופה, או כפי שתיאר זאת שֶלינג: "איום המיועד להניע את האויב לפעולה כלשהי".[50] מדינות חשודות ייאלצו לשתף פעולה, אחרת הן ימשיכו לסבול לא רק ממצור הסייבר, אלא גם מבידוד. מדינות שיהיו מעוניינות להוכיח את רצונן הטוב יעדיפו לשתף פעולה ולו כביכול, ואולי אפילו יחלקו את המודיעין שלהן הנוגע לסוגיית הייחוס, כמחווה נוספת של רצון טוב. מדינות שלא ישתפו פעולה יַחשפו בכך את כוונותיהן האמיתיות.

קל יותר לכפות שיתוף פעולה אם המדינות המעורבות לא צריכות להתבזות. ניתן להשתמש באבטחת סייבר במודל לבריאות הציבור של רָטְרֵי והִילֵי ובמטאפורה של צוותי החקירה של ארגון הבריאות העולמי (WHO) הפועלים בעת מגפות:[51] ממשלות אינן חייבות להיות מואשמות ישירות, שכן הן אינן האחראיות למגפה; במקרה שלנו האשמה מוסטת אל עבר התוכנה הזדונית או אל עבר ההאקרים הזדוניים שמאחוריה. ניתן לנצל את העובדה של היעדר ייחוס ברור של המתקפה למדינה מסוימת, כדי לאפשר לקואליציה של המדינות המתגוננות לבקש את שיתוף הפעולה של המדינות החשודות. כשם שאזורים שלמים מוכנסים להסגר בעת מגפות, כך יכולה להתבצע גם חסימת הסייבר. במצב זה, המחיר של אי־שיתוף פעולה יוטל על הצד התוקף, ומחיר זה יעלה ככל שמדינות אחרות ישתפו פעולה והמדינה התוקפת תידחק לבידוד הולך וגובר. מנגד, מחיר שיתוף הפעולה מצד המדינה התוקפת יהיה נמוך יותר, שכן הוא לא יהיה כרוך באובדן כבוד, גם אם הוא יכלול עדיין איום ממשי – עצם המחיר שהתוקפן אמור לשלם על ביצוע הפעולה: חשיפה ונטרול של יכולות התקיפה שלו (שרתים, קודים, האקרים) כאשר יחליט לבסוף לשתף פעולה. שיתוף פעולה מתמשך מצד המדינה התוקפת, והמודיעין הנוסף שיתלווה אליו, יסייעו לשמר מצב זה.

מדינות שהתחמקו משיתוף פעולה ייאלצו לחזור ולשתף פעולה, וההשקעה שלהן ביכולות ההתחמקות תרד לטמיון. עם זאת, שיתוף הפעולה שלהן לא יהיה כרוך בהכרח בנזק לעצמן בדעת הקהל – דבר ההופך את "החזרה לשיתוף פעולה" לאפשרות סבירה, ולפיכך לבעלת פוטנציאל להשגת יציבות. במצב כזה, המשימה הקשה של ייחוס פומבי ורשמי של המתקפה לגורם ספציפי – דבר המחייב רמת ודאות גבוהה מאד – הופכת למיותרת.

אסטרטגיות ותנאים לכפייה משותפת

כדי שאסטרטגיה זו תצליח, עליה למנף את המאמצים להגיע לייחוס המתקפה. איכות המודיעין היא קריטית למימושה של גישת כפייה זו. ראשי המדינות נמצאים בלב העימות האסטרטגי. דרך התנהלותם ואופן העברת המסרים המאיימים ישפיעו על אמינות פעולת התגמול שלהם. ראש המדינה המתגוננת, בסיוע קואליציה של מדינות ידידותיות, כמוהו כחוקר משטרה המטיח בפני החשודים: "תנו לנו גישה למידע, שתפו עמנו פעולה, או שנשאיר אתכם במעצר". מדובר במיקוח, בדיוק כפי שנעשה בעבודת המשטרה.[52] ככל שהמודיעין טוב יותר, כך תכנון החקירה והתהליך יהיו יעילים יותר: "המידע עשוי להיות מקור הכוח החשוב ביותר" בחקירות.[53] כשנעשה בו שימוש בתהליך החקירה, הוא ממחיש את ההתמצאות הרבה של החוקר. בכך הוא מבסס את אמינותו ואת העובדה שלא ניתן להוליך אותו שולל, והנחקר יהסס למסור לו מידע שגוי. במקביל, החוקר מוכיח שהוא יכול להיות בן־שיח בעל ידע. עסקת שיתוף פעולה תהיה, במקרה זה, עסקה יציבה.

במקרה שלנו, "החוקר" יכול ליזום מבחנים כדי לבדוק באמצעותם את תגובת המדינות החשודות. מבחנים כאלה יכולים לעשות הדמיה של תוצאות בלתי צפויות למדינה המתגוננת. המדינה המתגוננת, מצדה, יכולה לזרוע ספק במדינה התוקפת באמצעות מניפולציה נגדית, המשדרת למדינה התוקפת מסר, לפיו נשק הסייבר אינו כלי אמין ועלול לגרום להסלמה לא רצויה לתוקף.

המדינה המתגוננת יכולה לזכות ביתר קלות באהדה ובתמיכה חיצוניות ככל שהתוכנה הזדונית פוגעת באינטרסים פנימיים חיוניים שלה. הסולידריות שיפגינו כלפיה מדינות אחרות תעמיק ככל שמקורה של התוכנה הזדונית לא יהיה מזוהה, כך שכל מדינה עלולה להפוך ליעד למתקפה שלה. התהליך הדיפלומטי שילווה את הכפייה יסייע בהפניית המתקפה של התוקף כלפי עצמו, כפי שקורה בג'ודו. ככל שמתקפת הסייבר חמורה יותר, כך תתחזק הסולידריות בין המדינה המתגוננת ובין ידידותיה ויתהדק מצור הסייבר על המדינות החשודות. באופן כזה, היוזמה תעבור לידיו של המתגונן, והוא אף יוכל לשלוט בקצב ההסלמה.

אסטרטגיית כפייה זו לפתרון בעיית הייחוס היא בת־ביצוע, שכן מאחורי כל מתקפה מתוחכמת חייבת לעמוד מדינת לאום, ומאחורי כל מתקפה של גורמים

לא מדינתיים עומדת בהכרח מדינה מפותחת. לארגוני טרור הממוקמים ב"מדינות כושלות" אין כרגע יכולת טכנית ליזום מתקפות סייבר מתוחכמות ואסטרטגיות. לדוגמה, "סטקסנט" היה קוד שנכתב על ידי מהנדסי IT מוכשרים ביותר. הוא עשה שימוש באישורים דיגיטליים שנגנבו משתי חברות טיוואניות חוקיות,[54] ונבדק על מודל סייבר מלא, שכָּלל הדמיות של צנטריפוגות P-1.[55] כל אלה מחייבים מימון רב לגיוס ולשימור המומחים, גישה ממשית למאגר מומחים רב־תחומיים (במיוחד אם יש צורך במודלים של סייבר), וכן השקעה קבועה בהכשרה ובפיתוח, שכֵּן מרחב הסייבר משתדרג ללא הפסקה. אין גם לשכוח בהקשר זה את הצורך בשירותים חשאיים שיחדרו לתוכנות חסויות או ישיגו גישה אליהן. מדובר ביכולות שנכון להיום אינן מצויות באזורים לא מפותחים של העולם.

כאמור, מאחורי כל ארגון אד־הוק הפותח במתקפת סייבר מתוחכמת ניצבת מדינת חסות מפותחת ומתקדמת. מדינות מתקדמות תלויות יותר מתמיד במרחב הסייבר לצורך גישה לנתונים, פיתוחם ועיבודם. חלק גדול מהתקשורת העסקית ועיבוד הנתונים עובר ל"ענן", כלומר לשרתים הממוקמים לרוב במדינות זרות. לאור זאת, ההשפעה המשתקת שיש לחסימת הסייבר עשויה להיות חריפה במיוחד במדינות מפותחות.

אסטרטגיית הכפייה המשותפת תפעל אם בעלות בריתה של המדינה המתגוננת ייאלצו או יומרצו גם הן לפעול. יש ליצור תיאום מתמשך, הסכמה על נורמות ושיתוף תהליכים כתנאים מוקדמים לכך, עוד לפני פרוץ המשבר. רמות שיתוף הפעולה יהיו פועל יוצא של מעגלי הקִרבה בין המדינות משתפות הפעולה – מהידידות הקרובות ביותר ועד לרחוקות ביותר – כך שמרחב הסייבר ישקף את מערכת היחסים והסכמי שיתוף הפעולה הקיימים ביניהן זה מכבר.[56] בנוסף, כדי להוסיף אמינות לתהליך, ניתן להגביר את שיתוף הפעולה בתוך המעגלים ובין מעגלים סמוכים. התוויית הכיוון הצפוי חשובה כדי לגבש שיתוף פעולה בין־לאומי. חשובים עוד יותר הם הקשרים בין הצדדים, שצריכים לקבל תרגום מעשי בשטח. לדוגמה, מדינות ידידותיות יכולות לעשות שימוש בתוכנות הנמצאות בשימוש אצל מדינות ידידותיות אחרות. שימוש משותף באותה תוכנה או באותם תקנים יגביר את הסיכון של המדינה התוקפת להיתקל בתוצאות בלתי צפויות. שימוש כזה גם מעביר מסר חזק שהתקפה על מדינה מסוימת כמוה כהתקפה על כל ידידותיה. שימוש משותף באותה תוכנה במרחב הסייבר עשוי למלא תפקיד דומה לזה שמילא הכוח הצבאי האמריקאי בברלין במהלך המלחמה הקרה[57]: הוא ייצור מעורבות אוטומטית ולא יותיר ספק בכך שתהליך הכפייה מופעל במשותף בידי קואליציה של מדינות ידידות.

על המדינות המתגוננות לייצר יכולות סייבר עודפות כדי שיוכלו לספוג את המכה הראשונה. יכולות מִחשוב ותקשורת עודפות יפחיתו באופן זמני צווארי

בקבוק. ניתן לנטרל באופן חלקי מניפולציה סמנטית בעזרת שמירה של נתונים חיוניים במאגר נתונים "לכתיבה בלבד", וזאת כדי לאפשר שחזור "ערכי אמת" לפני מתקפה.

אמצעי הגנה הם לרוב בלתי מספיקים. כל עוד לא מתמודדים עם נחישותו של האויב ללמוד טכניקות מתקפה חדשות, הוא ימשיך ללמוד ולאמץ כאלו, כשהוא מחקה את דינמיקת האבולוציה של "המַלכּדה האדומה" הקיימת בטבע.[58] ללא התמודדות כזו לא ניתן להשיג הרתעה. כדי להשיגה יש להתמודד ישירות עם רצון התוקף ללמוד שיטות תקיפה חדשות מבלי לחלוק אותן עם אחרים; כמו כן, יש לקבוע מחיר לאויב על שאיפותיו אלו. בכל מקרה, חיוני שתימצא בידי המותקף יכולת לספוג את המכה הראשונה. מודלים להרתעה קונבנציונלית יוצאים מתוך הנחה שחולשה של המותקף מזמינה מתקפות עליו.[59] במצב של חולשה, מכה ראשונה עלולה להיות כה קשה, עד שלמדינה המותקפת לא יהיה זמן לתגובה ראויה ולגיבוש קואליציה של ידידות.

המצב האידיאלי הוא שתהליך הייחוס ייקבע בעזרת צוות מפקחים בין־לאומי. דבר זה יבטיח את שמירת "הצל הארוך של העתיד":[60] במצב כזה, האמת תצא לאור, סוגיית הייחוס תובהר סופית והתוקף לא יוכל לברוח מאחריות.

לסיכום, ברגע שנקבע הייחוס וניתן לזהות ולהעריך את תוצאות התקיפה במסגרת עקומת האמינות של המדינה המתגוננת, האסימטריה פוסקת לפעול לטובת הצד התוקף. "שפת הפעולה הצבאית" שבה לפעול לטובת הצד המתגונן, שיכול אז לאיים בצורה אמינה בתגמול. לאחר זיהוי ראוי של תוצאות ההתקפה, המתגונן יכול ליזום תגובה הולמת אפילו בעזרת אמצעים שאינם סייבר – דיפלומטיים, כלכליים, קינטיים או אסטרטגיים. יכולת זו מעניקה משקל רב יותר לצד המתגונן, וכל האופציות הופכות אז לזמינות עבורו. איומים בתגובה שאינה בתחום הסייבר יכולים להיות עדיפים, אם יתברר שתגובה כזו היא בלתי פגיעה למתקפות סייבר. יכולת העמידה שלה תהפוך אותה אז לבת מימוש. חריגה מתגובה באמצעות סייבר בלבד מהווה איתות של הצד המתגונן כי ביכולתו לעבור למתקפות שיש להן תוצאות חומריות ממשיות. התוקף ייאלץ אז לבחור בין נסיגה להסלמה, וייקלע למצב קשה, במיוחד כאשר יעמוד מול כפייה רבתי. כאמור, כפי שהיה בעת משבר הטילים בקובה, במצב כזה התוקפן המבקש לחרוג מהסטטוס קוו יעדיף לסגת מאשר להסלים את המצב.

סיכום: לקראת דוקטרינה צבאית ומדינית חדשה לעידן הדיגיטלי

הצורך ליצור שוויון בתוצאות השימוש בנשק הסייבר ובנשק שאינו סייבר, והצורך להחליף את אמצעי התגמול מאמצעי סייבר לכאלה שאינם סייבר, מצביעים

על החשיבות הרבה שיש להגדרה מחודשת של הפעולות הנעשות במסגרת לוחמת הסייבר, יחסית לשאר מערכות הנשק. בהמשך לדברי אדוארד לוטוואק,[61] אסטרטגיית סייבר המתבססת על כוח אחד (one force) עשויה להיות בלתי יעילה, בדומה למה שלוטוואק מכנה בביטול "לא־אסטרטגיה", דהיינו, אסטרטגיה המבוססת על כוח אחד בלבד וטוענת לאוטונומיה אסטרטגית, כמו "אסטרטגיה ימית", "אסטרטגיה אווירית" ו"אסטרטגיה גרעינית".

מרכזי הכובד של אסטרטגיות הלחימה התפתחו תמיד בד בבד עם השינויים הטכנולוגיים באמצעי הלחימה. כך, מרכזי הכובד במלחמה הקרה היו שונים מאלה של מלחמת הבזק של גוּדֶריאן, או של וָאוּבָּאן ומבצרי הענק שלו; האסטרטג ג'וליאן קוֹרְבֶט קבע ששליטה ימית ניתן להשיג לא על ידי כיבוש שטחים ימיים – שאינם אפשריים בהחזקה – אלא על ידי הבטחת יכולת המעבר בימים.[62] ככל שהעימותים עוברים לעולם הדיגיטלי או אל ה"לוגוס" הדיגיטלי,[63] עתידים להתפתח מרכזי כובד חדשים.

ככל שהקריטיות של המרחב הסמנטי גבוהה יותר מאשר הבסיס הפיזי, פוחתת חשיבותם היחסית של קווי התקשורת המסורתיים: האינטרנט נבנה כדי שאפשר יהיה לשגר מידע גם בהיעדר תשתית פיזית. החשוב מכל הוא לוודא את נתוני האמת – מיהם התוקפים? מה הם תוקפים? – לדעת למי לייחס את המתקפה ולהכיר ולזהות את תוצאותיה. אלה הם מרכַזי כובד קוגניטיביים. במונחים אסטרטגיים, זוהי עליונותו של הידע: להפעיל פיקוח ולגונן על המדינה ועל מערכות המשנה שלה מפני מניפולציות במידע. במילים אחרות, האמת היא הגורם החשוב ביותר בעולם המידע.

חשיבות עולם המידע הדיגיטלי יחסית לשאר המרכיבים של "האומה המרושתת הפועלת כמערכת" עשויה לשנות עדיפויות אסטרטגיות. שינויים נוספים בתעשייה עשויים לשנות עוד את סדר העדיפויות החדש. ככל שהתוכנה ממשיכה "לאכול את העולם",[64] וחשיבותם של נתונים ושל יישומים מבוססי־נתונים עולה, כך שמירה על ה"לוגוס" הדיגיטלי עשויה להפוך לחשובה לא פחות מאשר שמירה על הנכסים הפיזיים. בחלק מהתחומים החיוניים זוהי המציאות כבר כיום: עושר נמדד ועובר ידיים באמצעות ביטים אלקטרוניים המייצגים ערכים כספיים. בעוד שעל פי הגדרתו של לוטוואק, לוחמת סייבר נחשבת ללא־אסטרטגיה, יש אפשרות – קטנה ורחוקה ככל שתהיה – שהאסטרטגיה של ה"לוגוס" הדיגיטלי תהפוך לאוטונומית, כלומר תייצג הן את המטרה והן את האמצעים. מערכות מידע, החל מהדנ"א ועד לשפה המדוברת, חיוניות לניהול כל אורגניזם, כך שעליונותו של ה"לוגוס" הדיגיטלי אינה אמורה להפתיע איש.

תהליך זה מסמן שינוי עמוק בתפקיד המדינה המגֵנה על האומה. המדינה חייבת לשמור על המונופול שיש לה להפעיל אלימות בקנה מידה גדול, אלימות

אותה ניתן להגדיר כהגנה על נכסים פיזיים מפני השחתה באמצעות כוח קינטי. יהיה עליה גם להגן על מהימנות הנתונים שמשמשים את המערכות האסטרטגיות האזרחיות והצבאיות, וברמה גבוהה יותר – לשמר את מהימנותו של המידע האסטרטגי עצמו, וזאת כדי לאפשר המשך המודעות למצב של "אומה הפועלת כמערכת". המדינה תהיה אז קו ההגנה האחרון של האמת.

כל האפשרויות האלו נידונו להתממש בשל התגברות יכולות המחשוב והאחסון של טכנולוגיות המידע. לשם דוגמה, כוח המחשוב של מחשבי העל המובילים עתיד להתחזק פי עשר בשלישית פלופס לפחות במהלך עשר השנים הבאות.[65] לאור העלייה בסדרי הגודל של עוצמת המחשוב, אין לשלול גם שינויים גדולים ביכולת ההדמיה והלמידה של המחשבים.[66] אפשר שהמגבלות הקיימות כיום בניתוחי "מבצעים מבוססי תוצאות" ו"מדינה הפועלת כמערכת" הן זמניות, כמו הקשיים שהיו בזמנם בתחום הבינה המלאכותית: הבינה המלאכותית הוגדרה במשך עשורים כשדה מחקר בעייתי,[67] אך כיום היא נחשבת לתחום מבטיח.[68] לאור זאת, היכולות המתפתחות של ניתוח והדמיה של "מבצעים מבוססי תוצאות" עשויות לגרום לשינויים גם בשיקולים של מעצמות גדולות.

עלייה ביכולת ההדמיה פירושה שיפור יכולת החיזוי: בדרך זו מתאפשר מבט ארוך טווח וצפוי יותר על המתרחש. ככל שהמידע על היכולת ה"אמיתית" של כל צד מדויק יותר, כך פוחת הסיכון למלחמה. גם זֶנָארה[69] וגם אקסלרוד[70] מראים, כל אחד בנפרד, שככל שתהליך זה הולך ומתפתח, כך גובר הסיכוי לגיבוש אסטרטגיות שיתופיות (או אסטרטגיות של סטטוס קוו).[71] שימוש מוצלח באסטרטגיית כפייה משותפת יביא גם הוא בטווח הארוך להעדפת הסטטוס קוו: אם אין תועלת במעבר מצד לצד והכפייה המשותפת צפויה להביא להגברת שיתוף הפעולה, אזי אין טעם בתשלום הכרוך במעבר כזה, והדבר מעלה אוטומטית את ערכה היחסי של אופציית הסטטוס קוו (כלומר המשך שיתוף הפעולה). כפי שמניחה תיאוריית "ההרתעה המושלמת", העלייה בערכה של אופציית הסטטוס קוו יחסית לכל אסטרטגיה אחרת של מעבר מצד לצד, היא אחד הגורמים החשובים ביותר להשגת יציבות.[72]

על רקע דברים אלה ניתן להוסיף, כי הגישות העוסקות בהדמיות של "מדינה הפועלת כמערכת" ושל "כפייה משותפת" מצביעות על כך שכניסתה המואצת של הציביליזציה האנושית למעמקי ה"לוגוס" הדיגיטלי עשויה להפוך לגורם נוסף שיביא לשלום וליציבות. אסטרטגיות אלו של "צמצום מידע אסימטרי" יכולות לשמש כאבני בניין מרכזיות למסגרת דוקטרינרית חדשה לקבוצות חברתיות בעידן ה"לוגוס" הדיגיטלי. מסגרת דוקטרינרית זאת תמשיך לקדם שלום ויציבות, תוך שילוב הדוקטרינות העכשוויות של הרתעה קונבנציונלית והרתעה גרעינית. היא גם תכיר ביתרון של מערכות המידע הדיגיטליות בנושאים אזרחיים וצבאיים, ולבסוף תוביל להגדרה מדויקת יותר של מושג העימות.

הדוקטרינה של "השמדה הדדית מובטחת" הפכה את המלחמות בין מתחרים לעמיתים בזירה הבין־לאומית לתרגיל עקר ב"משחק־סכום־שלילי", וזאת במידה רבה בשל היכולות להנחית מכה שנייה. דוקטרינה של שיתוף פעולה דיגיטלי כפוי, המלווה בביטול כל יתרון אסימטרי בתחום המידע שיש למדינה הקוראת תגר, עשויה לסייע בבלימת הסלמתם של משברים בין־לאומיים ב"ציביליזציה הדיגיטלית" של המאה ה־21.

הערות

1 ניתן לראות מאמר זה כהשלמה לסוגיות אי־היציבות במרחב הסייבר שפורטו במאמר: Guy-Philippe Goldstein, "Cyber Weapons and International Stability", *Military and Strategic Affairs*, Vol. 5, No. 2, 2013, pp. 121-139.

2 Sun Tzu, *The Art of War*, (transl. Lionel Giles), 1910, Ch. 3, http://www.gutenberg.org/cache/epub/132/pg132.html

3 Frank C. Zagare, D. Marc Kilgour, *Perfect Deterrence*, Cambridge: Cambridge Studies in International Relations, 2000, pp. 296-301.

4 Paul K. Huth, *Extended Deterrence and the Prevention of War*, New Haven: Yale University Press, 1988, cited in: Zagare, Kilgour, *Perfect Deterrence*, pp. 296-301.

5 לפירוט נוסף של הסוגיה ראו לדוגמה: Goldstein, "Cyber Weapons and International Stability".

6 שם.

7 William W. Kaufmann, *The Requirements of Deterrence*, Princeton: Center of International Studies, Princeton University Press, 1954; Fred Kaplan, *The Wizards of Armageddon*, Stanford: Stanford University Press, 1983, pp. 193-200.

8 ראו דיון בנושא זה אצל: Goldstein, "Cyber Weapons and International Stability". גולדשטיין מפנה להגדרות של תומס שלינג ל"קו אדום":
Thomas C. Schelling, *Arms and Influence*, Yale University Press, 1966, p. 137.

9 ראו דיון אצל גולדשטיין, שם, המפנה לרעיון של "עקומת האמינות" בתוך:
Carey B. Joynt, Percey E. Corbett, *Theory and Reality in World Politics*, Pittsburgh: University of Pittsburgh Press, 1978, pp. 94-95.

10 Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, New York: Cambridge University Press, 2013, p. 88: "The international Group of Experts achieved no consensus as to whether non-destructive but severe cyber operations satisfy the intensity criterion"; Ibid. pp. 82-83, comments #14 and #15.

11 דוגמה לדיון על לוחמת סייבר בהקשר של "לוחמה מבוססת השפעה" ראו:
Amit Sharma, "Cyber Wars: A Paradigm Shift from Means to Ends", in: Christian Czosseck and Kenneth Geers (eds.), *The Virtual Battlefield: Perspective on Cyber Warfare*, Amsterdam: IOS Press, 2009.
"מדריך טאלין" מציין בצורה מפורשת עוד יותר כי "פעולת סייבר מהווה שימוש בכוח כאשר ניתן להשוות את ההיקף וההשפעה שלה לפעולה שאינה סייבר שעושה שימוש בכוח" (כלל מספר 11); ולאחר מכן: "מתקפת סייבר היא פעולת סייבר, בין אם לצרכי הגנה או התקפה, שיש סיכוי סביר שתגרום לפגיעה או למוות לאנשים, או לנזק או להרס של אובייקטים" (כלל מספר 30). הדיון מדגיש בהקשר זה כי: "אין לראות

'פעולות אלימות' כמוגבלות לפעולות של כוח קינטי. הדבר מוסדר היטב בדיני העימות החמוש. בהקשר זה יש לציין שמתקפות כימיות, ביולוגיות או רדיולוגיות חסרות בדרך כלל השפעה קינטית על המטרה, אולם יש הסכמה כוללת שהן מהוות מתקפות על פי החוק". מה שחשוב הוא ההשפעה הישירה על אוכלוסייה אזרחית או על רכוש, ואין זה משַנה באיזו דרך – קינטית או אחרת.

12 Col. Paul M. Carpenter and Col. William F. Andrews, "Effects-Based Operations – Combat proven", *Joint Force Quarterly* 52, 1st Quarter (2009), pp. 78-81.

13 קבוצת המומחים הבין־לאומיים של "מדריך טאלין" מציינת את הרעיון של "היקף ותוצאה", שהוצג בפסק הדין של בית הדין הבין־לאומי לצדק בעניין ניקרגואה: "Nicaragua judgement: Military and Paramilitary Activities in and against Nicaragua (Nicar. V. US), 1986 I.C.J.14 (27 June); Schmitt, *Tallinn Manual*, p. 45.

14 Christopher D. Baker, "Tolerance of International Espionage: A Functional Approach", *American University International Law Review*, Vol. 19, Issue 5 (2003), pp. 1091-1113.

15 "The lack of an international prohibition of espionage leaves decision makers with the usually acceptable liability of merely violating the target nation's domestic espionage law": Thomas C. Wingfield, "Legal Aspects of Offensive Information Operations in Space", *USAF Academy Journal of Legal Studies*, 121, 1999, p. 140; Martin C. Libicki, *Cyberdeterrence and Cyberwar*, Santa Monica: Rand Corporation, 2009, pp. 23-24.
הדיון על כלל 10 ("איסור על איום או שימוש בכוח") ב"מדריך טאלין" (מהדורת 2013) מציין: "[...] לא כל התערבות ב[מערכות] סייבר מפרה אוטומטית את החוק הבין־לאומי האוסר על התערבות [...] כפי שציין בית הדין בניקרגואה, 'התערבות' מנוגדת לחוק כאשר היא עושה שימוש בשיטות של כפייה. יוצא מכך שריגול סייבר וניצול של סייבר, הנעדרים מרכיב של כפייה, אינם מפרים כשלעצמם את עקרון אי־ההתערבות".

16 Schmitt (ed.), *Tallinn Manual*, Part I, Section 2: Self-Defence, and Rule 32, "Prohibition on attacking civilians".

17 Charles Tilly, "War Making and State Making as Organized Crime", in: Peter Evans, Dietrich Rueschemeyer and Theda Skocpol (eds.), *Bringing the State Back*, Cambridge: Cambridge University Press, 1985; Antonio Giustozzi, *The Art of Coercion: Armed Force in the Context of State Building*, CSRC Seminar, 2008.

18 Agreement on Measures to Reduce the Risk of Outbreak of Nuclear War Between the United States of America and the Union of Soviet Socialist Republics, http://www.state.gov/t/isn/4692.htm; Agreement Between the United States of America and the Union of Soviet Socialist Republics on Measures to Improve the USA-USSR Direct Communications Link, http://www.state.gov/t/isn/4787.htm, Cited in: Laura Grego, *A History of Anti-Satellite Programs*, UCS Global Security Programs, 2012.

19 Karl Frederick Rauscher, Andrey Korotkov, "Russia-US Bilateral on Critical Infrastructure Protection", in: *Working toward Rules for Governing Cyber Conflict*, East-West Institute, 2011; Schmitt, (ed.), *Tallinn Manual*, "3/The law of armed conflict generally" (in particular "Rule 20"), "4/Conduct of hostilities" (in particular "Rule 29 – Civilians" and Section 3: "Attacks against persons").

20 Michael S. Lewis-Beck, Mary Stegmaier, "Economic Determinants of Electoral Outcomes", *Annual Review of Political Science*, Vol. 3 (2000), pp. 183-219.

21 Alan de Bromhead, Barry Eichengreen and Kevin Hjortshøj O'Rourke, *Right Wing Political Extremism in the Great Depression*, Discussion Papers in Economic and Social History, Number 95, University of Oxford, 2012.

22 "מדריך טאלין" מגדיר כלא חוקית פעולת סייבר המנסה לפגוע בעצמאות הפוליטית של מדינה כלשהי (כלל 10).

23 "מדריך טאלין", כלל 11, עמ' 51.

24 Martin C. Libicki, "Cyberspace is not a Warfighting Domain", *I/S: A Journal of Law and Policy for the Information Society*, 8, no. 2 (2012), p. 330.

25 ראו "מקרה קווירין" מ־1942, העוסק במחבלים גרמניים, עם דגש מיוחד על מחבלים שלא ענדו סמלים לאומיים: "[...] מרגל שחוצה את הגבול בזמן מלחמה בצורה חשאית וללא מדים, מתוך כוונה לאסוף מידע צבאי ולהעבירו לאויב, או לוחם של האויב החוצה את הגבול באופן חשאי וללא מדים, במטרה לפגוע בחיים או ברכוש, הם דוגמאות ללוחמים שבאופן כללי אינם זכאים למעמד של אסירי מלחמה, אלא של מי שהפרו את דיני המלחמה, והם יועמדו למשפט וייענשו בבתי דין צבאיים". U.S. Supreme Court, EX PARTE QUIRIN, 317 U.S. 1 (1942). יש לציין שלוחמים בלתי חוקיים זכאים בכל זאת "ליחס הומאני, ובמקרה של משפט לא תימָנע מהם הזכות למשפט סדיר והוגן על פי האמנה הנוכחית": Geneva Convention Relative to the Protection of Civilian Persons in Time of War, August 12, 1949 (GCIV).

26 על "לוחמים חסרי זכויות" ראו "מדריך טאלין" 2013, עמ' 100, הערה 17.

27 Ben Smith, Arabella Torp, "The Legal Basis for the Invasion of Afghanistan", *House of Commons, International Affairs and Defence Section*, February 26, 2010, pp. 4-5.

28 Ashton B. Carter, Michael M. May, William J. Perry, *The Day After – Action in the 24 Hours following a Nuclear Blast in an American City*, Report based on Workshop, The Preventive Defense Project, Harvard and Stanford Universities, 2007, in particular: "6. Retaliation and Deterrence", pp.15-17.

29 כלל 11 ב"מדריך טאלין", 2013.

30 כלל 13, הערה 5 ב"מדריך טאלין" 2013, עמ' 55, המצטט את פסק דין ניקרגואה, פסקה 191.

31 "All warfare is based on deception", Sun Tzu, *The Art of War*, p. 66.

32 Herman Kahn, *On Escalation*, London: Pall Mall Press Ltd., 1965.

33 לזיהוי התוצאה יש לצרף ניתוח טכני של התוכנה הזדונית עצמה. דבר זה עשוי לארוך זמן רב. לדוגמה, הווירוס "סטקסנט" זוהה על ידי וירוס "בלוקדה" ביוני 2010, אך נותח לעומק רק בנובמבר 2010. ראו: Nicolas Falliere, Liam O. Murchu, Eric Chien, *W32.Stuxnet Dossier*, Symantec, 2010. מכאן הדרישה לחילופי התרעות מידע עדכניות, שיזרמו מכל מרכזי הפעילות האזרחיים והצבאיים לנקודת איסוף אחת בתחום הסייבר, שתהיה מסוגלת לפרש תקריות סייבר וליצור תמונה שלמה לשימושם של מוסדות הביטחון של המדינה.

34 ראו כלל 30, הערה 5, ב"מדריך טאלין" 2013, עמ' 106.

35 John A. Warden III, "The Enemy as a System", *Airpower Journal*, Vol. 9, Issue 1, 1995.

36 General James N. Mattis, USMC, "USJFCOM Commander's Guidance for Effects Based Operations", *Joint Force Quarterly,* No. 51, 2008; Paul M. Carpenter, William F. Andrews, "Effects-Based Operations Combat Proven", *Joint Force Quarterly*, No. 52, 2009: (ביקורת של קציני חיל האוויר האמריקאי על USJFCOM).

37 Robin Vasan, "Business Process API-ification: the LEGO promise fulfilled",

GigaOm, October 6, 2012, http://gigaom.com/2012/10/06/business-process-api-ification-the-lego-promise-fulfilled/; Mark Boyd, "Getting C-Level Buy-In: Demonstrating the Business Value of APIs", *ProgrammableWeb*, September 11, 2013, http://blog.programmableweb.com/2013/09/11/getting-c-level-buy-in-demonstrating-the-business-value-of-apis/

38 לדיון במרכיבים המרכזיים של מרחב הסייבר ראו: Goldstein, "Cyber Weapons and International Stability".

39 Isaac Ben-Israel, *Philosophie du renseignement*, Paris : Editions de l'Eclat, 2004.

40 שם.

41 דוגמה זו שואבת השראה ישירה מניתוח מלחמת יום הכיפורים, כפי שהובא ב: Ben-Israel, *Philosophie du renseignement*.

42 כדי לגלות את הזהות של "ג'רלד", החפרפרת שעבדה עבור ברית המועצות, שולח סמיילי הודעה לראש ה"סירקוס", המאלצת את "ג'רלד" לבקש פגישת חירום עם איש הקשר הסובייטי שלו בדירת מבטחים, שמיקומה היה ידוע זה מכבר לסמיילי. זה המבחן שאִפשר לסמיילי לפרוץ לדירת המבטחים ולזהות את "ג'רלד": John Le Carré, *Tinker Tailor Soldier Spy*, London: Hodder & Stoughton, 1974.

43 לדיון המשווה בין העולם "הדיגיטלי" המגדיר את מרחב הסייבר לבין עולם "המידע החסוי" שמגדיר את תחום המודיעין המסורתי ראו: Goldstein "Cyber Weapons and International Stability".

44 Ben-Israel, *Philosophie du renseignement*.

45 Richard Clarke and Robert K. Knake, *Cyberwar*, New York City: HarperCollins Publishers, 2010, pp. 249-254.

46 שם.

47 L. M. Hill, "The Two-Witness Rule in English Treason Trials: Some Comments on the Emergence of Procedural Law", *American Journal of Legal History*, 12, 1968, pp. 95-111.

48 Glenn Shafer, "the Combination of Evidence", *International Journal of Intelligent Systems*, Vol. I, 1986, pp. 155-179.

49 ראו ניתוח על פי תיאוריית המשחקים של משבר ברלין ב־1948 בתוך: Frank C. Zagare, *The Dynamics of Deterrence*, Chicago: University of Chicago Press, 1987, pp. 11-28.

50 Thomas C. Schelling, *the Strategy of Conflict*, Cambridge: Harvard University Press, 1963, p. 69.

51 Greg Rattray, Chris Evans, Jason Healey, "American Security in the Cyber Commons", in: Abraham M. Denmark and James Mulvenon (eds.), *The Future of American Power in a Multipolar World*, Washington D.C.: Center for a New American Security, 2010, pp. 151-172.

52 Daniel L. Shapiro, "Negotiation Theory and Practice: Exploring Ideas to Aid Information Eduction", in: Robert A. Fein, Paul Lehner, Bryan Vossekuil (eds.), *Educing Information*, Washington D.C.: Intelligence Science Board, National Defense Intelligence College Press, 2006, pp. 267-280.

53 M. P. Rowe, "Negotiation Theory and Educing Information: Practical Concepts and Tools", in: Fein, Lehner, Vossekuil (eds.), *Educing Information*, p. 295.

54 וירוס "סטקסנט" עשה שימוש באישורים דיגיטליים של החברות הטיוואניות Realtek ו־JMicron, שעברו מניפולציה. ראו: Falliere, Murchu, Chien, *W32. Stuxnet Dossier*.

55 David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks against Iran", *The*

New York Times, June 1, 2012.

56 ניתן להתחיל, למשל, במדינות החברות ב"תוכנית לשיתוף פעולה טכני" (5 eyes" nations"), שיש להן היסטוריה של שיתוף פעולה צמוד בסוגיות קריטיות (למשל, בפעולות סייבר משותפות או בסוגיות לשיתוף מודיעיני), כמו המדינות המשתתפות בברית נגד אל־קאעדה. ראו:
Dana Priest, "Help from France Key in Covert Operations", *The Washington Post*, July 3, 2005.

57 Schelling, *Arms and Influence*, p. 47.

58 לניסוח ראשוני של הביולוגיה האבולוציונית ראו:
Leigh Van Valen, "A New Evolutionary Law", *Evolutionary Theory* 1 (1973), pp. 1-30; Rattray et al., *The Future of American Power in a Multipolar World*, Section "Adaptation and Counter-Adaptation", p. 154; Kevin Mandia, "Cyber Threats and ongoing Efforts to Protect the Nation", Permanent Select Committee on Intelligence, US House of Representatives, October 4, 2011.

59 Edward Rhodes, "Conventional Deterrence", *Comparative Strategy*, 19: 3 (2000), pp. 221-253, in particular pp. 222-223.

60 Robert Axelrod, *the Evolution of Cooperation*, New York City: Basic Books, 1984. ראו עמ' 13 להסבר על "צל העתיד" ועמ' 124 על "הגדלת צל העתיד" לקידום שיתוף פעולה.

61 Edward N. Luttwak, *Strategy – The Logic of War and Peace*, revised and enlarged edition, Cambridge: The Belknap Press of Harvard University Press, 2001, Chapter 11, "Nonstrategies", pp. 168-184.

62 Julian S. Corbett, *Some Principles of Maritime Strategy*, London: Longmans, Green & Co., 1911, p. 90: "Command of the Sea, therefore, means nothing but the control of maritime communications, whether for commercial or military purposes".

63 לדיון על "לוגוס" דיגיטלי ראו: Goldstein "Cyber Weapons and International Stability".

64 Marc Andreessen, "Why Software is Eating the World", *The Wall Street Journal*, August 20, 2011.

65 FLOPS – Floating Point Operations Per Second – יחידת מידה לעוצמתם של מחשבים. מחשב העל המהיר ביותר ב־2010 היה Cray Jaguar, שמהירותו הייתה 1.8 10^15 פלופס: top500.org, November 2009-2010. ביצועים מעבר לאקסא־פלופ אחד או 10^18 פלופס צפויים להיות מושגים עד שנת 2020: Agam Shah, "SGI, Intel Plan to Speed Supercomputers 500 Times by 2018", *Computerworld*, June 20, 2011.

66 יכולות של זטא־פלופ (10^21) עשויות לאפשר יצירת מודלים לחיזוי מדויק של מזג האוויר לתקופה של שבועיים מראש. ראו בעניין זה:
Erik P. DeBenedictis, "Reversible Logic for Supercomputing" *Proceedings of the 2nd Conference on Computing Frontiers*, Sandia National Laboratories, 2005, pp. 391-402.

67 חוקרים דיברו על "חורף של בינה מלאכותית" במהלך שתי תקופות לפחות: בין 1974 ל־1980 ובין 1987 ל־1993. ראו:
Jim Howe, "Artificial Intelligence at Edinburgh University: a Perspective", 1994; Stuart J. Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach*, (2nd ed.), Upper Saddle River, New Jersey: Prentice Hall, 2003, p. 24.

68 באמצע העשור הראשון של שנות האלפיים השתנתה הגישה כלפי הבינה המלאכותית והתחילו לדבר על "אביב" בתחום זה. ראו לדוגמה:

John Markoff, "Behind Artificial Intelligence, a Squadron of Bright Real People", *The New York Times*, October 14, 2005.

69 Zagare, *The Dynamics of Deterrence*, pp. 48-56.

70 Axelrod, *The Evolution of Cooperation*, p. 13 (דיון על "צל העתיד").

71 Goldstein, "Cyber Weapons and International Stability".

72 Zagare, Kilgour, *Perfect Deterrence*, pp. 293-296.

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: המשגה 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