סייבר, מודיעין וביטחון

כרך 1 | גיליון 3 | דצמבר 2017

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
TEL AVIV UNIVERSITY אוניברסיטת תל אביב

סייבר, מודיעין וביטחון

כרך 1 | גיליון 3 | דצמבר 2017

תוכן

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
אוניברסיטת תל אביב
TEL AVIV UNIVERSITY

סייבר, מודיעין וביטחון

כתב העת **סייבר, מודיעין וביטחון** מיועד להעשיר, להפרות ולהעמיק את השיח הציבורי באשר לנושאים רלוונטיים.

המאמרים המופיעים בכתב עת זה, הרואה אור שלוש פעמים בשנה, נכתבים על ידי חוקרי המרכז ואורחיו והדעות המובעות בהם הן של המחברים לבדם.

כתב העת **סייבר, מודיעין וביטחון** רואה אור במסגרת תוכנית המחקר 'ביטחון סייבר', המתנהלת במכון למחקרי ביטחון לאומי.

עיצוב גרפי: מיכל סמו־קובץ ויעל ביבר, המשרד לעיצוב גרפי, אוניברסיטת תל־אביב
דפוס: אליניר, פתח־תקווה

כתובת:
המכון למחקרי ביטחון לאומי, רח' חיים לבנון 40, ת"ד 39950, תל־אביב 6997556.
טל' 03-6400400, פקס' 03-7447590, דוא"ל: info@inss.org.il

המאמרים המתפרסמים בכתב העת סייבר, מודיעין וביטחון
מוצגים באתר המכון: www.inss.org.il

ISSN 2519-6685 (מקוון) • ISSN 2519-6677 (מודפס)

ביטחון סייבר וריגול כלכלי: המקרה של ההשקעות הסיניות במזרח התיכון

שרון מגן

הנושא המרכזי של מאמר זה הוא השימוש בטכנולוגיות מתפתחות למטרות ריגול בסייבר. רבים עסקו עד היום בסיכוני הסייבר הקשורים לתחום הביטחוני, אך איומים על הביטחון הלאומי כתוצאה מריגול כלכלי בסייבר לא נדונו עד כה באותו היקף. מצב זה מטריד למדי: ככול שמרחב הסייבר מנוצל יותר ויותר למטרות ריגול, יש הכרח להעמיק ולבחון את אפשרויות ניצולו הספציפיות למטרות אלו בזירה הבין־לאומית. תהליך הגלובליזציה הכלכלית הפך את הזירה הבין־לאומית לזירה של קשרי גומלין ותלות הדדית אינטנסיביים ביותר, ומאפיין זה מגביר את חשיפתה של הכלכלה העולמית לפגיעות בתחום ביטחון הסייבר.

מילות מפתח: ריגול בסייבר, ריגול כלכלי, גלובליזציה, ביטחון לאומי.

מבוא

במוקד מאמר זה נמצאים השימוש שנעשה לאחרונה בטכנולוגיות מתפתחות לביצוע התקפות סייבר או ריגול סייבר, כמו גם האיום שמהלכים אלה מהווים לביטחון הלאומי של מדינות בתחום פעילותן הכלכלית. על אף שרבים בחנו כבר את סיכוני הסייבר הקשורים ישירות לתחום הביטחון, איומים על הביטחון הלאומי כתוצאה מהתקפות סייבר או מצעדי ריגול מבוססי סייבר בתחום הכלכלי טרם טופלו באותו היקף, ומצב זה מעורר תמיהה.

ככול שהשימוש במרחב הסייבר למטרות ריגול הופך לנפוץ בתחומים שונים, יש הכרח להמשיך ולבחון את הפוטנציאל לניצולו גם לצורך פעולות ריגול בזירה הכלכלית הבין־לאומית. תהליך הגלובליזציה יצר קשרי גומלין ותלות הדדית רחבי היקף בכלכלה העולמית, ומאפיין זה הפך אותה לחשופה יותר ויותר להפרות

שרון מגן היא בעלת תואר שני בלימודי ביטחון משעם אוניברסיטת תל אביב, והשלימה תקופת התמחות במכון למחקרי ביטחון לאומי בנושא יחסי סין־ישראל ו"מועצת שיתוף הפעולה של מדינות המפרץ" (GCC).

אפשריות של ביטחון הסייבר. הפרה אפשרית מעין זו תהיה בעלת השלכות רחבות על האינטרסים של הביטחון הלאומי של מדינות. היעדר מחקר עדכני על השימוש באמצעי סייבר לניהול ריגול כלכלי ועל השלכותיו, הביא אותי לבחון נושא זה, כפי שיפורט במאמר הנוכחי.

חשיבותה ההולכת וגוברת של התופעה, שבה ישויות זרות עושות שימוש באמצעי סייבר לביצוע ריגול כלכלי כדי להשיג יעדים אסטרטגיים, היוותה את התמריץ העיקרי שלי לעריכת המחקר שהביא לכתיבת מאמר זה. הסיכון הגובר והולך לביטחון הלאומי בעקבות ריגול הסייבר הכלכלי, בשילוב עם התחזקותה הכלכלית והמדינית של סין, נותנים משנה תוקף לחשיבות העיסוק בנושא זה. קיימת סבירות גבוהה שסין, כמדינה השואפת להפוך לגורם מכריע ("משנה כללי משחק") בזירה העולמית, עוסקת באופן נרחב ובהיקף משמעותי יותר ממדינות אחרות בריגול כלכלי בסייבר, וזאת מתוך מטרה להשיג את יעדיה בתחומים אחרים, ובהם הביטחוני והמדיני. יש להעמיק וללמוד את הנושא, גם כדי לקבוע האם הריגול הכלכלי של סין מהווה איום ממשי, וגם כדי לבחון אם יש לקחת איום זה בחשבון כאשר שוקלים תהליך של אינטגרציה כלכלית עם גורמים סיניים.

ממשלות זרות יכולות, הן באמצעות חברות פרטיות והן על ידי חברות ממשלתיות, להגדיר כלכלות מסוימות, או לחילופין תאגידים זרים, כראויים לביצוע השקעה. אותן ממשלות מסוגלות להשיג, באמצעות ההשקעה, טכנולוגיות חדשות, שבמקרה אחר לא היו מסוגלות להשיג לעצמן – צעד שעשוי להטות את הכף לטובתן. אפשרות כזאת מחזקת את התפיסה לפיה הריגול הכלכלי בסייבר הוא איום משמעותי על הביטחון הלאומי.

ארצות הברית מאשימה בכך בעיקר את סין, שכן חברות סיניות, שמרביתן נמצאות בבעלות ממשלתית, מעוררות את חשדה שהן משתמשות בסייבר ובאינטגרציה הכלכלית כפלטפורמה לניהול ריגול כלכלי. עם זאת, יש הטוענים כי סין אינה המדינה היחידה המבצעת ריגול כלכלי בסייבר, ולכן אין להתייחס אליה בצורה שעושה זאת ארצות הברית. למעשה, כל המדינות עוסקות בריגול כלכלי בהיקף כזה או אחר. מאמר זה יבחן את הסיבה לכך שארצות הברית מובילה את הטענה לפיה סין מנהלת ריגול כלכלי בוטה בסייבר, על אף שכאמור, פעילות ריגול כזאת ננקטת כנראה גם על ידי מדינות נוספות.

המתודולוגיה שבחרתי כדי לבחון הנחה תיאורטית זו מבוססת על הערכת הגישה אותה נוקטות מדינות אחרות מלבד ארצות הברית כלפי הטענות בדבר כוונות הריגול הכלכלי בסייבר של סין. אם מדינות אחרות טוענות גם הן כי סין היא המקור העיקרי לריגול סייבר כלכלי (על אף הקביעה שמדינות נוספות נוקטות סוג זה של ריגול), יהיה זה חיוני להבהיר את הסיבות העומדות מאחורי סוג התנהלות זה. כדי להעריך את גישותיהן של מדינות אחרות כלפי הריגול הכלכלי

הסיני באמצעות הסייבר, יהיה זה אפקטיבי להתמקד במדינות לא מערביות, כגון מדינות המזרח התיכון, העשויות לתרום לתיאור מאוזן יותר של היחס אל כוונות הריגול הכלכלי של סין.

מאמר זה בוחן את גישותיהן של מדינות נבחרות במזרח התיכון כלפי מעורבותה המסיבית של סין בסחר העולמי וכלפי אפשרויות הריגול הכלכלי שלה בסייבר, וזאת, כאמור, כאמצעי להערכת אמיתותה של הטענה האמריקאית. ספציפית, המאמר בוחן את המקרים של איחוד האמירויות הערביות ושל טורקיה. הרציונל העומד מאחורי בחירת שתי מדינות אלו הוא שהנושא האסטרטגי העיקרי הקושר את סין למזרח התיכון הוא ביטחונה הכלכלי, שכן היא מייבאת יותר ממחצית מכמויות הנפט והגז הטבעי שלהן היא זקוקה ממדינות באזור זה של העולם.

איחוד האמירויות הערביות מהווה את הכלכלה השלישית בגודלה במזרח התיכון אחרי ערב הסעודית ואיראן, ומשמש לסין מקור לנפט ולגז טבעי, אם כי לא ספק עיקרי. מאחר שלא ניתן לאפיין את איחוד האמירויות הערביות כמדינה החיונית לאינטרסים הכלכליים הסיניים, היא יכולה לשמש מקרה בוחן משמעותי לטענה האמריקאית. גישת איחוד האמירויות כלפי כוונות הריגול הכלכליות של סין באמצעות הסייבר לא תהיה, לפיכך, מוטה לטובת בייג'ין.

בניגוד למצב השורר בקרב מרבית השחקנים האחרים באזור, נפט וגז אינם ממלאים תפקיד חשוב ביחסיה של טורקיה עם סין, מה שהופך גם את אנקרה לבחירה ראויה ללימוד האינטרסים והיחסים של סין במזרח התיכון. לפיכך, בחינת התגובות האפשריות של טורקיה לריגול הסיני הכלכלי בסייבר עשויה לתרום גם היא לחקר הנושא.

התפיסה שלפיה סין תוכל לזכות בגישה לאינטרסים כלכליים חיוניים במדינה מארחת באמצעות ריגול כלכלי בסייבר, ולממש בכך את האינטרסים שלה תוך התעלמות מן האינטרסים של אותה מדינה, אמורה הייתה לגרום לאיחוד האמירויות הערביות ולטורקיה לנקוט צעדים נגד עסקאות כלכליות עם סין, ובהם השעיית השקעות סיניות או אף הפסקתן. כדי להעריך את גישתן של שתי מדינות אלו לריגול כלכלי אפשרי בסייבר מצידה של סין, יבחן המאמר הגבלות ממשלתיות על עסקאות כלכליות ועל קידום פרויקטים במימון סיני בשתי המדינות הללו. מגמה עקבית של הצבת מכשולים על ידי הממשלים המקומיים בפני מימוש פרויקטים במימון סיני, תאפשר לי לטעון כי הדבר נובע מכך שאותם ממשלים חשים כי קיים איום מוחשי על הביטחון הלאומי שלהם באמצעות ריגול כלכלי בסייבר המתאפשר על ידי אינטגרציה כלכלית.

מאמר זה מדגיש, אפוא, את הכורח ללמוד לעומק את סוגיית האינטגרציה הגלובלית בסייבר ואת הסיכונים הכרוכים בריגול כלכלי באמצעותו. אינטגרציה

זו עשויה אמנם להיות הזדמנות לצמיחה, אך מדינות חייבות לקחת בחשבון גם את הסיכון הכרוך בחשיפת הכלכלה שלהן לריגול באמצעות הסייבר.

ריגול כלכלי באמצעות הסייבר

מרי אלן סטנלי גורסת כי ההתקדמות הטכנולוגית והאינטגרציה הכלכלית שינו באופן מרחיק לכת את תפיסת הביטחון הלאומי בתחום המודיעין, וזאת בעקבות פעילות ריגול כלכלי רחבת היקף בסייבר.[1] בהקשר דומה, מתיו קרוסטון טוען כי פעילות כלכלית בין־לאומית טיפוסית עשויה ליצור מערכת איסוף מודיעין באמצעות הסייבר, המתוכננת למעשה להעצים יכולות צבאית.[2] סוביק סאהה מצידו מדגיש באופן ספציפי את נקודת המבט האמריקאית, העוסקת במעורבותה של סין בריגול כלכלי ובאיום שפעילות זו מהווה על הביטחון הלאומי.[3] מגנוס יורטדל מדגיש כי מרחב הסייבר מהווה מרכיב מכריע באסטרטגיה של סין שנועדה לקדם את מעמדה במערכת הבין־לאומית, וכי אחד מאמצעי המפתח שלה להשגת יתרון אסטרטגי הוא ניהול ריגול כלכלי.[4]

לעומתם, אבראהים ארדוגן טוען כי פעילות הריגול הכלכלי בסייבר היא תעשייה משתלמת עד מאוד שבה נוטלות חלק כל המדינות,[5] ולכן לא ניתן ליחסה למדינה ספציפית. זאת ועוד, כשמדובר בארצות הברית, דנקן קלארק טוען כי אפילו בעלות בריתה, כמו ישראל, מנהלות נגדה פעילות ריגול כלכלית מזה שנים. על פי קלארק, גופי מודיעין ישראליים ממשיכים להשתמש ברשתות קיימות כדי לאסוף מודיעין כלכלי, לרבות על ידי חדירה למחשבים,[6] דבר שמפריך את הטיעון שריגול הסייבר הכלכלי נגד ארצות הברית מובל על ידי מי שהם יריביה. הטיעון שלפיו מדינות רבות, ובכללן בעלות בריתה של ארצות הברית, עוסקות גם הן בריגול כלכלי בסייבר נגדה, יש בו כדי להחליש את חומרת הצעדים אותם נוקטת סין, ובנוסף

1 Mary Ellen Stanley, "From China with Love: Espionage in the Age of Foreign Investment", *Brooklyn Journal of International Law* 40, no. 3 (2015): 1033–1079.

2 Matthew Crosston, "Soft Spying: Leveraging Globalization as Proxy Military Rivalry", *International Journal of Intelligence and Counterintelligence* 28, no. 1 (2015): 105–122.

3 Souvik Saha, "CFIUS Now Made in China: Dueling National Security Review Frameworks as a Countermeasure to Economic Espionage in the Age of Globalization", *Northwestern Journal of International Law and Business* 33, no. 1 (2012): 199–235.

4 Magnus Hjortdal, "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence", *Journal of Strategic Security* 4, no. 2 (2011): 1–24.

5 İbrahim Erdoğan, "Economic Espionage as a New Form of War in the Post-Cold War Period", *USAK Yearbook of International Politics and Law* no. 2 (2009): 265–282.

6 Duncan Clarke, "Israel's Economic Espionage in the United States", *Journal of Palestine Studies* 27, no. 4 (1998): 20–35.

לכך את טענתה של קהילת המודיעין האמריקאית שסין היא זו הנמצאת בחזית פעילות הריגול הכלכלי בסייבר בארצות הברית.

לדברי ג'ון יו, סוכנויות המודיעין והביטחון הלאומי האמריקאיות אינן מציגות תמיד תמונה מדויקת של האיומים הקיימים על הביטחון הלאומי.[7] במילים אחרות, ארצות הברית עשויה להשתמש בטיעונים כוזבים כדי להגן על ביטחונה הלאומי, תוך הקרבה של ממד היושרה. גם רוברט בז'סקי מעלה ספק באשר לאמינות ההצהרות של גופי הביטחון והמודיעין האמריקאיים. על פי בז'סקי, יש בסיס לטענה שהזרוע המבצעת בארצות הברית עלולה להשפיע על הערכות המודיעין כך שיתמכו בעמדה המועדפת עליה. לדבריו, לסוכנות הביון המרכזית (CIA), למשל, יש היסטוריה ארוכה של הטיה פוליטית של המודיעין. ואכן, בכנס שהתקיים באוניברסיטת הרווארד בשנת 2001 טען פאנל של מומחים, שדן בהיסטוריה של סוכנות הביון המרכזית, כי כאשר היא נדרשת לחלוק אמיתות בלתי נעימות עם הזרוע המבצעת, היא אינה ממלאת את תפקידה בנאמנות.[8]

נוכח כל הנאמר לעיל, ולמרות שפעילות הריגול הכלכלי בסייבר אכן עלולה להוות איום על הביטחון הלאומי של ארצות הברית, האשמתה הפורמלית של סין כגורם הראשי המנהל פעילות ריגול כזאת עלולה להתברר כמוטה. ייתכן אמנם שסין נוקטת צעדי ריגול כלכלי תוך שימוש בכלי סייבר, אך לא ניתן לאשר בשלב זה את הטענה כי היא המובילה תחום זה יותר מכול מדינה אחרת.

תלות הדדית מתגברת

התפתחויות טכנולוגיות במהלך העשורים האחרונים שינו באופן מרחיק לכת את האופן שבו מדינות תופסות את המושג ביטחון לאומי. ריגול קונבנציונלי, שניתן לזהות מאחוריו ישות מוחשית, התמזג זה מכבר עם תחום הסייבר, מה שהפך את האיום המודיעיני למעורפל מבעבר וחשף תחומים חדשים לאיסוף מידע מזיק, כגון השוק הגלובלי.[9] תופעת האינטגרציה הפיננסית מובילה כיום את העולם לעֵבר כלכלה גלובלית אחת.[10] המציאות הנוכחית של טכנולוגיה מודרנית, בשילוב עם אינטגרציה כלכלית כלל־עולמית, שינתה את פניה של פעילות הריגול ויצרה מצב

7 John Yoo, "The Legality of the National Security Agency's Bulk Data Surveillance Programs", *Harvard Journal of Law and Public Policy* 37, no. 3 (2014): 901–930.

8 Robert Bejesky, "Politicization of Intelligence", *Southern University Law Review*, no. 40 (2013): 243-292.

9 Stanley, "From China with Love: Espionage in the Age of Foreign Investment".

10 Lucyna Kornecki and Dawna Rhoades, "How FDI Facilitates the Globalization Process and Stimulates Economic Growth in CEE", *Journal of International Business Research* 6, no. 1 (2007): 113–126.

שבו הביטחון הלאומי עלול להיפגע גם על ידי שימוש באמצעי סייבר בשווקים הגלובליים.

ככול שהגלובליזציה הכלכלית מאפשרת ריגול באמצעות הסייבר – הבסיס ליחסי התלות ההדדית המאפיינים את השווקים הבין־לאומיים – גובר הצורך במציאת איזון בין עושרה של מדינה ובין השמירה על הביטחון הלאומי שלה. השיטות המרכזיות שבאמצעותן עשויה האינטגרציה הכלכלית הבין־לאומית לאפשר פעילות ריגול כלכלי בסייבר הן פעילותן העסקית של ישויות בבעלות מדינה זרה המנהלות עסקים במדינה מארחת, או כאשר ישות זרה רוכשת פעילות עסקית מקומית במדינה מסוימת.[11] אפשר לטעון כי סוג זה של פעילות מהווה לא רק ביטוי למדיניות כלכלית, כי אם גם תוכנית מתוכננת היטב לאיסוף מודיעין, המיועדת לפעול כצורה נוספת של תחרות, לצד היריבות הצבאית הקיימת בין הצדדים.[12] אף שלא ניתן לקבוע כי ריגול בסייבר מהווה את התמריץ העיקרי העומד מאחורי השאיפה לאינטגרציה כלכלית, אינטגרציה זו מאפשרת מעצם קיומה לנהל פעילות ריגול בסייבר. יתר על כן, מדינות עלולות לנצל לרעה את האינטגרציה הכלכלית כדי לנקוט פעולות של ריגול כלכלי בסייבר, גם כדי להגדיל את עוצמתן הצבאית.

רבים טוענים כי סין היא המובילה בתחום הריגול הכלכלי בסייבר.[13] לפי טענה זו, סין שואפת לרתום את אפשרויות הריגול הנפתחות בזכות השוק הכלכלי הגלובלי כדי לבסס עליונות אזורית וכלל־עולמית. בין הטוענים כך בולטת במיוחד ארצות הברית, התופסת את כוונתה של סין לנקוט פעולות ריגול כלכלי בסייבר כסיכון מבשר רעות לביטחון הלאומי שלה, שכן הצלחתה של סין לנהל ריגול כלכלי יעיל עלולה להיות מתורגמת לעלייה חדה בעוצמתה בהשוואה לזו של ארצות הברית. מדיניות ההשקעות הסינית הנוכחית בכלכלות כגון זו של ארצות הברית מבוססת על מיזוגים ורכישות, המאפשרים זליגה בלתי רצויה של קניין רוחני ושל סודות מסחריים לחברות סיניות באמצעות רשתות הסייבר.[14]

מדיניות ההשקעות הסינית הינה בעייתית במיוחד כאשר תאגידים סיניים רב־לאומיים, שרובם נמצאים בבעלות ממשלתית, מנסים לרכוש חברות אמריקאיות בעלות משמעות אסטרטגית, או כאלו שתחום עיסוקן הוא תשתיות או נכסים

11 Stanley, "From China with Love: Espionage in the Age of Foreign Investment".

12 Crosston, "Soft Spying: Leveraging Globalization as Proxy Military Rivalry".

13 Stuart Malawer, "Confronting Chinese Economic Cyber Espionage with WTO Litigation", *New York Law Journal*, December 23, 2014.

14 "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace", *The Office of the National Counterintelligence Executive*, April 14, 2016, https://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf; Saha, "CFIUS Now Made in China: Dueling National Security Review Frameworks as a Countermeasure".

חיוניים. על פי הערכות אחרונות של קהילת המודיעין האמריקאית, סין מקדמת בנחישות רבה את מדיניותה הבין־לאומית, ועל רקע זה היא עוסקת גם בריגול כלכלי בסייבר בהיקף נרחב.[15] יתר על כן, על פי דוחות של הפנטגון, סין צפויה להמשיך לאסוף באופן אגרסיבי מידע טכנולוגי אמריקאי באמצעות ריגול בסייבר.[16]

הטענה שסין מהווה את המקור העיקרי לפעילות הריגול הכלכלי בסייבר עשויה לשרת שיקולים פוליטיים מסוימים של המדיניות האמריקאית, יותר מאשר לשקף את המצב האמיתי. אמנם, ג'יימס קומי, לשעבר מנהל ה־FBI, הצהיר כבר במאי 2014 כי ממשלת סין פעלה בבוטות כדי להשיג באמצעות ריגול בסייבר יתרון כלכלי עבור חברות בבעלותה, אך רוברט גייטס, מי שכיהן אז כמזכיר ההגנה האמריקאי, ציין לעומתו כי באותה העת נקטו לא פחות מ־15 מדינות שונות צעדי ריגול כלכלי שנועדו להשיג סודות מסחריים אמריקאיים וכן טכנולוגיה אמריקאית,[17] והסיט בהצהרתו זו את ההתמקדות בסין כשחקן המוביל בסוג זה של פעילות. לצד כל זאת יש להוסיף כי בעבר נטען שגם הסוכנות לביטחון לאומי של ארצות הברית (NSA) ביצעה פעילות ריגול כלכלי בסייבר – נגד צרפת.[18]

בנסיבות אלו, השאלה המתעוררת היא מדוע רוב גופי הביטחון והמודיעין האמריקאיים הרשמיים מובילים את הטענה שסין מהווה כיום את הגורם העיקרי בפעילות הריגול הכלכלי בסייבר ברחבי העולם, וזאת למרות שגורמים אחרים טוענים כי גם מדינות נוספות נקטו צעדי ריגול כלכלי כאלה, ובכללן ארצות הברית עצמה. נראה כי גופים מובילים בתחומי הביטחון והמודיעין בארצות הברית מפיצים את הטענה שסין מובילה את פעילות הריגול הכלכלי בסייבר ברמה הכלל־עולמית כדי לתמוך בצרכיה הפוליטיים של ארצם, וכן במדיניותה כלפי סין, שמעמדה המתחזק בזירה האזורית והעולמית מאיים על מעמדה הגלובלי של ארצות הברית ועל עוצמתה האסטרטגית. במילים אחרות, עלייתה של סין מהווה איום מדיני על ארצות הברית, ועובדה זו היא שהובילה לפעילות האמריקאית נגד האינטרסים הכלכליים של סין.

שאלה אחרת היא האם קיימות מדינות נוספות הטוענות כי סין נמצאת בחזית פעילות הריגול הכלכלי בסייבר. אם אכן מדינות נוספות מצטרפות לטענה

15 Saha, "CFIUS Now Made in China: Dueling National Security Review Frameworks as a Countermeasure".

16 Geoff Dyer, "China in 'Economic Espionage'", *Financial Times*, May 9, 2012.

17 Zachary Keck, "Robert Gates: Most Countries Conduct Economic Espionage", *The Diplomat*, December 17, 2015, http://thediplomat.com/2014/05/robert-gates-most-countries-conduct-economic-espionage/.

18 "WikiLeaks Reveals NSA's Economic Espionage against France", *Progressive Digital Media Technology News*, June 30, 2015, http://search.proquest.com/docview/1692699265?accountid=14765.

האמריקאית, השאלה היא מהן הסיבות לכך? ואם מדינות אחרות טוענות כי סין היא המובילה העולמית בפעילות ריגול כלכלי בסייבר למרות שקיימות מדינות רבות נוספות הפועלות באותו אופן, נשאלת השאלה מדוע הן מעלות טענה זו? ההנחה שלי היא כי הדבר נובע משיקולי ביטחון הקשורים למעמדה העולה של סין ולאיום הביטחוני שהיא מהווה באמצעות צמיחתה הכלכלית. תשובה כזאת תסייע לאשר את ההנחה שצמיחתה של סין מהווה איום דה־פקטו על האינטרסים האסטרטגיים של ארצות הברית.

אפשר לטעון כי מרבית ארגוני הביטחון והמודיעין האמריקאיים אינם מציגים הערכה מדויקת של התופעה הכלל־עולמית של ריגול כלכלי בסייבר, שכן קיימים שחקנים נוספים העוסקים בכך בזירה הגלובלית, ולא ניתן להצביע על מדינה אחת כגורם המוביל בתחום זה. עם זאת, אני טוענת כי **הגישה הפורמלית** של רוב ארגוני המודיעין האמריקאיים כלפי סין בכול הנוגע לפעילות הריגול הכלכלי בסייבר עשויה להיות מכוונת לשרת את האסטרטגיה־רבתי של ארצות הברית מול סין, מתוך אמונה כי צמיחתה עלולה לפגוע באינטרסים אסטרטגיים אמריקאיים.

ההשערה שארצות הברית דחפה ליצירת הרושם שסין מובילה את פעילות הריגול הכלכלי מבוסס הסייבר בזירה העולמית מנימוקים פוליטיים ומשיקולים של מדיניות חוץ וביטחון, עשויה לסייע בהבהרת הפער הקיים בין הטענה של הממסד הביטחוני האמריקאי ובין טענתם של גורמים אחרים בכול הנוגע לפעילותה זו של סין. רבים טוענים כי צמיחתה הכלכלית המואצת של סין, בשילוב עם חיזוק יכולותיה הצבאיות, העמידו אותה בנתיב התנגשות מול ארצות הברית.[19] כקריאת תגר נגד צמיחתה זאת של סין, מציגה אותה ארצות הברית כמדינה הרוחשת כבוד מזערי לקניין רוחני, לעקרון הריבונות ולנושאים קריטיים נוספים הניצבים ביסוד הסחר הבין־לאומי. סחר זה מהווה את לחם חוקה של סין, ומזין את צמיחתה ואת יכולתה להגדיל את עוצמתה הצבאית. אם יעלה בידי ארצות הברית לגרום נזק ליכולתה של סין לנהל סחר בין־לאומי על ידי טענתה שסין מקדמת פעילות ריגול כלכלי בסייבר, היא תוכל לפגוע גם ביכולותיה של בייג'ין בתחום הביטחוני.

כדי להבין טוב יותר את הסיבות שבגללן ארצות הברית טוענת שסין מובילה את פעילות הריגול הכלכלי בסייבר, ולהעריך את מידת האמינות של טענות אלו, נבחן כעת מה הקשר בין איחוד האמירויות הערביות וטורקיה למעורבותה המסיבית של סין בפעילות הסחר הבין־לאומי ולריגול הכלכלי הבוטה שלה באמצעות סייבר.

19 Saha, "CFIUS Now Made in China: Dueling National Security Review Frameworks as a Countermeasure".

איחוד האמירויות הערביות

איחוד האמירויות הערביות הוא פדרציה של שבע אמירויות, המהוות יחד את הכלכלה השלישית בגודלה במזרח התיכון, אחרי ערב הסעודית ואיראן. מדינת איחוד האמירויות נמצאת במקום השביעי בעולם מבחינת עתודות מוכחות של נפט ושל גז. בשנת 2010 ייבאה סין מאיחוד האמירויות הערביות 64,500 טון של גז טבעי נוזלי בשווי של יותר מ־23 מיליון דולר. בנוסף, תאגיד הנדסת הנפט והבנייה הסיני (CPECC) סייע בבניית פרויקט צינור הנפט הגולמי של אבו דאבי, המאפשר להוביל 1.5 מיליון חביות נפט גולמי ליממה מנקודת האיסוף בחבשן שבאבו דאבי למסופי הייצוא בפוג'יירה. הנפט המובל בצינור זה עוקף את מצרי הורמוז הצרים, שאיראן איימה לא אחת לחסום אם תותקף צבאית.

יש לציין כי פרויקט צינור הנפט של אבו דאבי, שנאמד ב־3.3 מיליארד דולר, ספג עיכובים רבים ביוזמת איחוד האמירויות הערביות.[20] באורח רשמי הוצהר כי האיחוד נאלץ לעכב את הקמת הצינור בגלל בעיות בנייה,[21] אך מקורות המקורבים לפרויקט טענו כי הסיבות לעיכוב היו אחרות. מתברר כי חברת הנפט של אבו דאבי (ADCO) לא הייתה מעורבת בתהליך הראשוני של הזמנת הצינורות, אף שהתאגיד הסיני כבר היה מוכן לעשות זאת. מצב זה מעורר תמיהה, שכן ניתן היה לצפות ש־ADCO היא זו שתאשר את תכנון מערכת הצינורות כדי שתעמוד בתקנים שלה עוד לפני תחילת ייצורה בפועל.[22]

העובדה שהסינים החלו בתכנון הצנרת ללא השתתפותו של תאגיד ADCO – החברה הממשלתית מטעם איחוד האמירויות הערביות שהייתה אחראית על הפרויקט – וללא מעורבותו, מצביעה על אפשרות שלסינים היו כוונות זדוניות בבניית הצינורות: מערכת הצינורות שתוכננה כללה תוכנת בקרה מתוחכמת במיוחד, שאפשר לפרוץ אליה ואף להשתלט עליה עוד טרם הרכבתה. בהקשר זה מעניין לציין כי תומס ס' ריד, השר לענייני חיל האוויר האמריקאי בזמן כהונתו של הנשיא רייגן, כתב בשנת 2004 כי ארצות הברית הצליחה לשתול תוכנת סוס טרויאני בתוך ציוד מחשוב אשר שימש לבקרה על צינור הגז הטרנס־סיבירי, שברית המועצות רכשה מספקים קנדיים.[23]

---

20 Manochehr Dorraj and James English, "The Dragon Nests: China's Energy Engagement of the Middle East", *China Report* 49, no. 1 (2013): 43–67.

21 "UAE Delays Project to Bypass the Strait of Hormuz", *Al Bawaba*, January 9, 2012, http://www.albawaba.com/business/uae-delays-project-bypass-strait-hormuz-408210.

22 "UAE Delays Oil Pipeline to Bypass Hormuz to June", *Oil & Gas News*, January 16, 2012, http://search.proquest.com/docview/916274658?accountid=14765.

23 John Markoff, "Old Trick Threatens the Newest Weapons", *New York Times*, October 26, 2009, http://www.nytimes.com/2009/10/27/science/27trojan.html?_r=2&ref=science&pagewanted=all.

יהיה זה סביר להניח שהסינים התחילו בתכנון מערכת הצינורות שהוזמנה על ידי איחוד האמירויות הערביות מבלי לערב את ADCO מכיוון שאכן היה להם מה להסתיר, למשל התקנה של אמצעי ריגול מבוססי סייבר. אם אכן כך היה, לא מדובר באירוע בודד. בשנת 2013 טען מייקל היידן, לשעבר ראש ה־CIA, כי ענקית הטלקום הסינית Huawei ריגלה לטובת סין,[24] דבר שמחזק את הטיעון שלפיו סין אכן משתמשת בעסקאות מסחריות לביצוע ריגול בסייבר. העיכובים הרבים שנגרמו לפרויקט צינור הנפט הגולמי של אבו דאבי, שנבעו מהרחקתו של תאגיד ADCO מתהליך התכנון של מערכת הצינורות, יכולים להיות מוסברים, אפוא, בכך שהתאגיד הסיני CPECC עסק בפעילות בלתי חוקית במהלך ייצור הצינורות, כלומר בהשתלת אמצעים לריגול סייבר. למרות זאת, איחוד האמירויות הערביות הסתפק במקרה זה בדחיית מימוש הפרויקט ובחר שלא לבטלו לחלוטין.

טורקיה

על אף שיותר ממחצית הייבוא של נפט וגז טבעי לסין מקורו במדינות המזרח התיכון, מצב שמעמיק את תלותה של בייג'ין באזור זה של העולם, נפט וגז אינם ממלאים תפקיד מרכזי ביחסיה של סין עם טורקיה. טורקיה מהווה, עם זאת, כוח עולה באזור ולא חוותה מהומות דוגמת אלו שנרשמו בעולם הערבי בשנים האחרונות, ולפיכך היא מהווה את אחד השותפים המרכזיים של סין במזרח התיכון, הן בתחום הכלכלי והן במישור המדיני.[25] על עמדת ממשלת טורקיה בנושא הריגול הכלכלי של סין באמצעות סייבר ניתן ללמוד מהעובדה שבנובמבר 2015 ביטלה אנקרה מכרז בשווי של 3.4 מיליארד דולר לרכישת מערכת הגנה מפני טילים ארוכי טווח, שבו זכתה בשנת 2013 חברה בבעלות ממשלתית סינית.[26]

טורקיה החלה לנהל בשנת 2013 משא ומתן עם תאגיד היבוא־יצוא הסיני למיכון מדויק (CPMIEC) במטרה להשלים את החוזה בן מיליארדי הדולרים לרכישת הטילים, למרות שגם הקונסורציום הצרפתי־איטלקי Eurosam והחברה האמריקאית Raytheon הגישו הצעות למכרז. העדפתה של ממשלת טורקיה לנהל שיחות דווקא עם התאגיד הסיני גרמה לדאגה עמוקה סביב מידת התאימות של המערכות הסיניות של תאגיד CPMIEC למערכות ההגנה של נאט"ו – ארגון

24 "Huawei Spies for China, says Former NSA and CIA Chief Michael Hayden", *Business Insider*, July 19, 2013, http://www.businessinsider.com/huawei-spies-for-china-says-michael-hayden-2013-7.

25 Altay Atli, "A View from Ankara: Turkey's Relations with China in a Changing Middle East", *Mediterranean Quarterly* 26, no. 1 (2015): 117–136.

26 "Turkey Says 'Yes' to China's Trade Initiative, 'No' to its Missiles", *South China Morning Post*, November 15, 2015, http://www.scmp.com/news/china/diplomacy-defence/article/1879097/turkey-says-yes-chinas-trade-initiative-no-its-missiles.

הביטחון שבו חברה טורקיה. בסופו של דבר ביטלה טורקיה את העסקה עם סין, ובהצהרה רשמית שפורסמה על ידי משרדו של ראש הממשלה דאז, אהמט דבוטאולו, הודיעה כי עשתה זאת, בראש ובראשונה, מאחר שהחליטה לפתח פרויקט טילים משל עצמה.[27]

למרות הטענה הטורקית הרשמית שהסיבה העיקרית לביטול העסקה בת מיליארדי הדולרים עם סין הייתה ההחלטה לפתח בעצמה מערכת הגנה מפני טילים ארוכי טווח, ייתכן שדאגות אמיתיות של ממשלת טורקיה מפני ריגול כלכלי סיני היו אלו שהובילו לביטול העסקה. כפי שצוין לעיל, טורקיה קבעה כבר בשלב מוקדם תהליך מקיף לבחירתה של חברה זרה שתוביל את הפרויקט האמור. אילו הייתה מעוניינת לפתח מערכת הגנה בכוחות עצמה, סביר להניח שהייתה עושה כך מלכתחילה ונמנעת מניהול הליך שלם לבחירת חברה זרה שתנהל את הפרויקט בעבורה. במילים אחרות, אפשר לטעון כי לאחר שטורקיה החליטה לבחור בתאגיד CPMIEC להמשך יישום הפרויקט, ממשלתה החלה לחשוש מפני חשיפתן האפשרית של מערכות רגישות של נאט"ו בפני הסינים. אמנם, העסקה לא הייתה כרוכה במפורש בחשיפה ישירה של מערכות קריטיות ומסווגות, אך השתתפות גורמים סיניים בעסקה הייתה עשויה לאפשר להם גישה למערכות שבאמצעותן יכלו לאסוף מידע שעלול היה להזיק לנאט"ו. עסקאות מן הסוג הזה, שבהן חברות זרות זוכות בגישה למערכות ממוחשבות ובחשיפה אליהן, עלולות לאפשר חדירה של ישויות זרות באמצעות פלטפורמות סייבר. איסוף מידע מזיק באמצעות עסקאות מסחריות תמימות לכאורה הוא מסוכן במיוחד כאשר מעורבות בדבר תשתיות קריטיות של המדינה המארחת.

לכאורה ניתן לקבל את הטיעון של ממשלת טורקיה כי מניעים אחרים גרמו לה לבטל את שיתוף הפעולה עם החברה הסינית הנמצאת בבעלות ממשלתית, כמו זה שהוצג בתגובה הרשמית לפיה טורקיה החליטה לפתח בכוחות עצמה מערכת הגנה מפני טילים; אלא שטיעון זה הינו בעייתי, שכן, כאמור, טורקיה כבר החלה בתהליך ארוך של בחירת קבלן ממדינה זרה. לפיכך, אפשר לטעון כי המניע המהותי האמיתי מאחורי החלטתה של טורקיה לבטל את העסקה עם סין היה האיום הפוטנציאלי של ריגול כלכלי סיני בסייבר, לאחר שהממשלה הטורקית הגיעה למסקנה שהדבר מהווה סכנה ממשית לביטחון הלאומי.

נראה, אפוא, שלמרות שאיחוד האמירויות הערביות וטורקיה אינן חולקות עם ארצות הברית את דאגתה העמוקה מפני האיום הכרוך בפעילות הריגול הכלכלי הסיני בסייבר, הן מבינות כי קיימת אפשרות של איום פוטנציאלי כזה, והבנה זו

27 "Turkey Cancels $3.4 Bln Missile Deal with China", *French Chamber of Commerce and Industry in China*, November 15, 2015, http://www.ccifc.org/fr/single-news/n/turkey-cancels-34-bln-missile-deal-with-china/.

משתקפת בביטול העסקאות עם חברות סיניות או בעיכובן. אף אחת משתי מדינות אלו לא טענה (בשונה מן הטענה האמריקאית) כי סין עושה שימוש באמצעי סייבר כדי לבצע ריגול כלכלי, אולם התנהלותן אל מול אפשרות של השקעות סיניות מהותיות בתחומן מצביעה על כך שהן מבינות שהתנהלותה הכלכלית של סין שונה מזו של מדינות אחרות וכי היא מהווה איום גובר של ריגול כלכלי בסייבר.

איחוד האמירויות הערביות וטורקיה אינן מעורבות ב"משחק המעצמות" הגדולות כמו ארצות הברית, ועל כן אין להן לא התמריץ להוקיע את התנהלותה הכלכלית של סין ולא אמצעי ההגנה כדי לעשות כן. הרמה המסוימת של התנגדות ממשלותיהן לביצוע עסקאות רחבות היקף עם תאגידים סיניים באה לידי ביטוי בעיקר בנקיטת שיטות "רכות" ולא בולטות, כגון השעיית פרויקטים. עם זאת, עצם ההשעיה של פרויקטים וביטול עסקאות מסחריות עם חברות סיניות יוצרים בסיס איתן לטענה כי עסקאות עם חברות סיניות אינן זוכות לטיפול זהה לזה שלו זוכות עסקאות הנחתמות עם חברות ממדינות אחרות. דבר זה מצביע, ללא ספק, על כך שעסקאות כאלו נתפסות באותן מדינות כמהוות איום פוטנציאלי.

למרות האמור לעיל, העובדה שהצעדים שנקטו ממשלות איחוד האמירויות הערביות וטורקיה נגד סין בתחום הכלכלי היו על פי רוב דיסקרטיים מאוד, מעוררת ספקות שהם ננקטו נוכח כוונות ממשיות של סין לבצע ריגול כלכלי. אפילו כאשר שתי ממשלות אלו הודיעו בפומבי על כוונתן להשעות את ההתקדמות בפרויקטים שמומנו על ידי סין או אף לבטל אותם, הן לא ציינו כי הדבר נבע מהתנהלות שהייתה ראויה לגינוי ושבסיסה היה ריגול כלכלי בסייבר.

בכול מקרה, ההתייחסות השונה לשאלת ההתנהלות הכלכלית של סין, יחסית לזו המוענקת לעסקאות כלכליות שמקורן במדינות אחרות, עשויה לחזק את הטענה האמריקאית כי התנהלות סינית זאת אינה תמימה. יתר על כן, אילו ממשלות טורקיה ואיחוד האמירויות הערביות היו סבורות כי סין פעלה בתום לב, הן לא היו מודיעות בפומבי על השעיית הפרויקטים רחבי ההיקף במימון סיני או על ביטולם.

הזכרתי לעיל את גישתו של קרוסטון, הקובע כי פעילות כלכלית בין־לאומית מסוימת עשויה להיות למעשה דרך לאיסוף מודיעין המיועד לחזק את עוצמתה הצבאית של המדינה האוספת. בנוסף לכך, התייחסתי לדברי סאחה, לפיו הערכות עדכניות של קהילת המודיעין האמריקאית טוענות כי המדיניות הבין־לאומית של סין משקפת נחישות רבה, וכי במסגרתה נוקטת סין פעילות של ריגול כלכלי משמעותי בסייבר. ואכן, התמקדות פעילותה העסקית של סין במגזרי התשתיות, האנרגיה והטלקומוניקציה – כולם מגזרים חיוניים מן ההיבט של הביטחון הלאומי – עשויה להצביע על כוונת הסינים להשתמש באמצעי הסייבר כדי לאסוף מידע לטובת מטרותיהם האסטרטגיות. ההשעיה של פרויקטים חשובים במימון סיני

וביטולם, על פניהם מנימוקים טכניים, מצביעה על כך שהמדינות שנסקרו במאמר זה מעריכות כי העמקת המעורבות הכלכלית הסינית בתחומן הינה איום עליהן.

סיכום

נוכח כל הנאמר לעיל, ניתן להבין כיצד התלות ההדדית הגלובלית בתחום הסייבר, יחד עם האינטגרציה הכלכלית בזירה העולמית, משפיעות על תפיסת הביטחון הלאומי של מדינות. גם כאשר נטען כי פעילות כלכלית בין־לאומית טיפוסית היא בעלת אופי כלכלי בלבד, זו עלולה להוות בסיס לאיסוף מודיעין באמצעות סייבר, שאמור לסייע בהעצמת כוחה של המדינה האוספת. ההתנהלות הכלכלית הבין־לאומית יכולה ליצור הזדמנויות למדינות המשקיעות במדינות אחרות לאסוף מודיעין כלכלי עליהן באמצעות הסייבר, דבר שמעמיד בסכנה את ביטחונה הלאומי של המדינה המקבלת את ההשקעות.

הטענה האמריקאית, שלפיה סין עומדת כיום בראש פעילות הריגול הכלכלי בסייבר ברחבי העולם באמצעות תהליך של אינטגרציה כלכלית, נתמכה גם על ידי מדינות אחרות, וזאת בנוסף לצעדים שנקטו טורקיה ואיחוד האמירויות הערביות ביחס לניהול עסקאות עם סין. כאמור לעיל, למרות שהתגובה של שתי מדינות אלו לפעילות הסינית לא הייתה חדה וישירה כמו זו של הממשל האמריקאי, ניכרת ממנה שאיפתן להגביל את היקף ההשקעות הסיניות בהן, או לפחות לנטר אותן.

מאמר זה ביקש להשיב על השאלה מדוע רשויות המודיעין האמריקאיות טוענות כי סין עומדת כיום בחזית השימוש בריגול כלכלי בסייבר, גם כאשר מקורות אחרים טוענים כי מדינות נוספות נוקטות גם הן ריגול כלכלי. נוכח הצעדים של איחוד האמירויות הערביות וטורקיה כלפי סין, אפשר להניח כי טענת ארצות הברית, הנובעת מראייתה את ההשקעות הסיניות כאיום על הביטחון הלאומי, מקובלת גם על מדינות נוספות. כפי שראינו במקרים של טורקיה ושל איחוד האמירויות הערביות, ההשעיה של פרויקטים סיניים או ביטולם מצביעה על כך שעסקאות מסחריות עם חברות סיניות אכן נתפסות על ידי מדינות אלו, ולא רק על ידי ארצות הברית, כמקור לסיכון. זאת, למרות שניתן לומר כי בשאלות של אינטגרציה כלכלית וריגול כלכלי בסייבר סין אינה שונה מכול מדינה אחרת.

מאמר זה תורם להמשך ההתמקדות בלימוד יחסי הגומלין והתלות ההדדית בתחום הסייבר, במקביל להעמקת הידע לגבי האינטגרציה הכלכלית הגלובלית והסיכון של פעילות ריגול הכרוכה בה. השוק העולמי מתאפיין יותר ויותר ביחסי גומלין ובתלות הדדית באמצעי הסייבר, ולפיכך על מדינות לקחת בחשבון את הסיכון הכרוך בחשיפתן לסיכוני ביטחון לאומי כתוצאה מתופעת האינטגרציה הכלכלית הכלל־עולמית, העלולה להתברר כמכשיר לריגול כלכלי. ארצות הברית אינה מגזימה כאשר היא מתארת את כוונות הריגול הכלכלי של סין בסייבר;

כמעצמת־על, היא נהנית מן הזכות הנתונה למדינות מעטות בלבד להצהיר ברבים על עמדתה בנושא זה. העובדה שסין משתמשת באינטגרציה הכלכלית לפעילות ריגול ולחיזוק עוצמתה הצבאית והאסטרטגית מחייבת, אפוא, להתייחס לניהול העסקים איתה באופן שונה מן האופן שבו יש להתייחס לפעילות עסקית עם מדינות אחרות.

אני מציעה לבחון את התגובה של גורמים רבי־עוצמה אחרים, כגון האיחוד האירופי ורוסיה, לצעדי הריגול הכלכלי הסיני בסייבר, שכן, כאמור, התפיסה הרואה בסין גורם מוביל כלל־עולמי בתחום זה נפוצה גם במדינות שמעֵבר לארצות הברית. במקרה של רוסיה, ייתכן שהממשל הרוסי לא יתמוך בפומבי בטענה על ריגול כלכלי סיני, וזאת כדי לחזק את עמדתה של סין אל מול ארצות הברית. לעומת זאת, רוסיה עשויה להחליט לנקוט צעדים לא פומביים וחשאיים כדי להגן על עצמה מפני איום הריגול הכלכלי בסייבר מצידה של סין. צעדים כאלה לא יפגעו ביחסיה של רוסיה עם סין מצד אחד, ולא יהוו תמיכה בסדר היום האמריקאי מצד שני.

אם מעצמות נוספות על ארצות הברית אכן תופסות את פעילות הריגול הכלכלי מבוסס הסייבר של סין כאיום מרכזי על ביטחונן הלאומי, יהיה זה חיוני לנסות לקבוע איך הדבר עשוי להשפיע על הפוליטיקה העולמית ועל הסחר הבין־לאומי. חלק מן המעצמות משתמשות כיום באמצעים מתוחכמים כמשקל נגד לפעילות הריגול הכלכלי של סין, ויהיה עליהן לפעול במשותף לבלימתה. כדי להביא להפסקת פעילות הריגול בסייבר של סין, ייתכן שהמעצמות יידרשו להקים מערך ניטור סייבר בין־לאומי בתחום הכלכלי, שמטרתו תהיה לצמצם את פעילות הריגול הכלכלי הגלובלי בסייבר.

המענה הבריטי לאיומים במרחב הסייבר

דניאל כהן

איום הסייבר נמצא כיום במקום גבוה בין הגורמים המהווים סיכון לאינטרסים ולביטחון הלאומי של מדינות. איום זה בא לידי ביטוי בשנים האחרונות בסדרה של מתקפות סייבר על מוסדות פוליטיים, מפלגות, ארגונים, מוסדות פיננסיים ותשתיות לאומיות קריטיות בכול רחבי העולם. בעתיד הקרוב צפויים סיכונים נוספים הנובעים מאיום הסייבר, במיוחד על המגזר האזרחי, שמקורם ב"אינטרנט של הדברים". סיכונים אלה הם תוצאה של העלייה במספר המכשירים המחוברים, שרובם אינם מאובטחים על ידי היצרנים או המשתמשים, וכן של העלייה במספר התקפות מניעת שירות, בשילוב סחיטה ודרישות כופר, על מערכות ציבוריות ופרטיות.

מאמר זה מתמקד בנעשה בתחום ביטחון הסייבר בבריטניה. הפערים המובנים בין מאפייני המגזר הפרטי הבריטי, הגמיש והדינמי, ובין צורכי מערכת הביטחון החשאית, הביורוקרטית והאיטית משבעה, הֻקשו על שיתופי פעולה בין תעשיית הסייבר בבריטניה ובין המערכת הביטחונית שם ועל שיתוף ידע חוצה מגזרים כנדרש היום. כמענה למצב זה, יושמו בשנים האחרונות בבריטניה תהליכים אסטרטגיים ממשלתיים לתמיכה בנושאי חדשנות וטכנולוגיה, בדגש על תעשייה עתירת ידע וביטחון סייבר. משרתם של תהליכים אלה הייתה להתמודד עם הדינמיות המשתנה של איומי הסייבר, תוך ניסיון לבניית גשר בין סוכנויות הביון והמודיעין הבריטיות ובין השוק הפרטי, כולל בנושאי הגנה, מחקר ופיתוח.

מילות מפתח: ביטחון סייבר, בריטניה, מחקר ופיתוח, הגנת סייבר, GCHQ, NCSC, הרתעה, שיתוף פעולה בין־לאומי.

דניאל כהן הינו חוקר בסדנת יובל נאמן למדע, טכנולוגיה וביטחון ובמרכז למחקר סייבר בינתחומי ע"ש בלווטניק, אוניברסיטת תל אביב.

מבוא

לבריטניה היסטוריה ארוכה של שימוש במדע ובטכנולוגיה לצורכי ביטחון לאומי, וממשלותיה שמרו לאורך השנים על אסטרטגיה ומדיניות ארוכות טווח לתמיכה בנושאי חדשנות, טכנולוגיה ותעשייה עתירת ידע. צוותי סיגינט שפעלו מטעם משרד המלחמה הבריטי עסקו מאז מלחמת העולם הראשונה ביירוט תשדורות של הגרמנים, תוך שיתוף ידע עם צוותים מקבילים מצרפת. פיצוח קודים ואיסוף מודיעין התרחבו מאוד בבריטניה במלחמת העולם השנייה, ובשנת 1945 שירתו בשירות מודיעין הסיגינט הבריטי בבלצ'לי פארק כ־10,000 עובדים.[1]

"מטה התקשורת הלאומי" הבריטי (Government Communications Headquarters – GCHQ) הוקם בזמן המלחמה הקרה, ומאז הוא הגוף האחראי על סיגינט וטכנולוגיה, סייבר ומשימות נוספות בתחום הביטחון הלאומי בבריטניה. במקביל הוא משמש כגוף המנחה את ארגוני הממשל וארגוני תשתיות קריטיות בנושאי אבטחת מערכות מידע. לצד מחלקות אופרטיביות שונות, פועלת ב־GCHQ מחלקת מחקר מתקדמת העוסקת במגוון נושאים, כמו ארכיטקטורת רשת, אבטחה, בלשנות, בינה מלאכותית, מכונות אוטונומית ועוד.

ה־GCHQ עמד בשנת 2013 במוקד דיון ציבורי, עם פרסום דוח הממונה על המודיעין מטעם ממשלת בריטניה ובו המלצות לרפורמות, לחוקים חדשים ולתהליכים הנדרשים כדי להסדיר את אפשרויות המעקב והציתות על ידי המודיעין והמשטרה הבריטיים. הדוח הדגיש את הצורך ביצירת גשר בין סוכנויות הביון הבריטיות ובין השוק הפרטי בנושאי הגנה, שיתוף ידע ומו"פ.[2]

כחלק מהשינוי המבני שנועד להקים יכולת לאומית להגנת סייבר במגזר האזרחי, הודיעה ממשלת בריטניה בנובמבר 2015 על הקמת "מרכז ביטחון הסייבר הלאומי" (National Cyber Security Centre – NCSC). המרכז יהיה כפוף ל־GCHQ, אך יישא באחריות מדינתית להגנת הסייבר לכלל החברה הבריטית ויהווה כתובת אחודה לייעוץ ולתמיכה לטובת המערכת הכלכלית, תוך שיתוף פעולה ישיר עם האקדמיה וגורמים בין־לאומיים. כוונת הממשלה הבריטית הייתה לאפשר למערכת הביטחונית העוסקת בהתמודדות עם איומי הסייבר להפוך לנגישה יותר ולבעלת יכולת לשתף פעולה עם המגזר הפרטי לטובת שיתוף ידע ומשאבים.[3]

---

1 ראו אתר Government Communications Headquarters (GCHQ), https://www.gchq-careers.co.uk/about-gchq.html.

2 Mark Waller, "Report of the Intelligence Services Commissioner for 2013", *Intelligence Services Commissioner*, June 26, 2014, http://intelligencecommissioner.com/docs/40707_HC304IntelligenceServicesCommissioner_Accessible.pdf.

3 "Progress and Research in Cybersecurity: Supporting a Resilient and Trustworthy System for the UK", *The Royal Society*, July 2016, p. 37, https://royalsociety.org/topics-policy/projects/cybersecurity-research/.

מימון ממשלתי בריטי למחקר ופיתוח טכנולוגי

בשלושת העשורים האחרונים הפחית הממשל הבריטי את השקעותיו במחקר ופיתוח. בשנת 2012, לדוגמה, היו ההשקעות במו"פ כ־1.72 אחוזים מהתל"ג הבריטי, לעומת כשני אחוזים מהתל"ג בסוף שנות השמונים של המאה העשרים. נתון זה גם נמוך מהממוצע במדינות האיחוד האירופי, שעמד בשנת 2012 על 2.06 אחוזים.[4] בשנת 2014 קבעה הממשלה הבריטית יעד של עלייה בהשקעה המדינתית במו"פ, לרמה של שלושה אחוזים מהתל"ג עד שנת 2020.[5]

מרבית ההשקעות בטכנולוגיה ובחדשנות בבריטניה מוקצות כיום לעידוד המגזר הפרטי ולא הציבורי. התקצוב הממשלתי למדע ולמחקר עומד על כ־4.6 מיליארד ליש"ט בשנה, ואינו כולל הקצאות ישירות למגזר הביטחוני (שבו חל קיצוץ בתקציב מאז שנת 2010). בין השנים 2010–2014 צמחו התעשיות הדיגיטליות בבריטניה בכ־32 אחוזים – מהר יותר מאשר המשק הבריטי – וההעסקה בתעשיות אלו גדלה ב־2.8 אחוזים – מהר יותר משאר מגזרי המשק. בשנת 2015 היו 86 אחוזים ממשקי הבית במדינה מחוברים לאינטרנט ו־76 אחוזים ערכו קניות באמצעותו. כ־56 אחוזים מאוכלוסיית הבוגרים אזרחי בריטניה השתמשו בשנת 2016 בבנק דיגיטלי. תעשיית הדיגיטל בבריטניה מהווה היום כשבעה אחוזים מהכלכלה הבריטית, ומעסיקה חמישה אחוזים מכוח העבודה.[6] למרות התגברות השימוש במרחב הדיגיטלי, המשק הבריטי סובל מעלייה באחוזי האבטלה של בעלי מקצועות טכנולוגיים, ולעומת זאת קיים מחסור באנשי מקצוע בתחום הסייבר.[7] פער זה זוהה על ידי הממשלה, ומטרתה כיום היא להעמיק את שיתוף הפעולה בין GCHQ ובין התעשייה הבריטית ולתרום לצמיחת שוק הסייבר. שוויו של שוק זה מוערך כיום בכ־22 מיליארד ליש"ט, אך רק שני מיליארד ליש"ט הם הכנסות מייצוא מוצרי סייבר.[8]

4 Charlie Edwards and Calum Jeffray, "The Future of Research and Development in the UK's Security and Intelligence Sector", *Occasional Paper*, *Royal United Services Institute*, March 2015, https://rusi.org/publication/occasional-papers/future-research-and-development-uk%E2%80%99s-security-and-intelligence-sector.

5 "Research and Development Funding for Science and Technology in the UK", *National Audit Office*, *Memorandum for the House of Commons Science and Technology Committee*, June 2013, p. 7.

6 "Internet Access – Households and Individuals: 2015", *Office for National Statistics*, http://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2015-08-06.

7 "Jammin' in the Capital", *The Economist*, June 21, 2014, http://www.economist.com/news/britain/21604591-londons-creative-talents-have-unleashed-wave-innovative-technology-firms-jammin.

8 שם.

הצורך ביצירת מערכת סביבתית יעילה, בה יפעלו במשולב הממשלה, מערכת הביטחון, האקדמיה, תעשיות וחברות הזנק במטרה לענות על צורכי הביטחון הגוברים בשל עליית האיומים במרחב הסייבר, הביא את ממשלת בריטניה לגבש בשנת 2011 אסטרטגיה לאומית לביטחון סייבר לשנים 2011–2016. במסגרת זו החליטה הממשלה על השקעה של 860 מיליון ליש"ט בפיתוח תוכנית ביטחון סייבר לאומית.

יישום האסטרטגיה החדשה בא לידי ביטוי בשלב הראשון בהקמת גופי הגנה בסייבר, כגון ה־CERT הלאומי, פלטפורמות לשיתוף ידע, עידוד מחקרי סייבר באקדמיה וחלוקת אחריות בין הגופים השונים האמונים על ביטחון סייבר. למרות מספר הצלחות, אסטרטגיה זו לא הצליחה להתגבר על הפערים המבניים הקיימים בין המגזר הפרטי הגמיש והדינמי ובין צורכי מערכת הביטחון החשאית, הביורוקרטית והאיטית מטבעה. חוסר השקיפות המערכתי גם הקשה על ייעול שיתופי הפעולה בין התעשייה ובין המערכת הביטחונית בבריטניה ועל שיתוף ידע חוצה מגזרים. רוב תקציב הסייבר הלאומי הבריטי הושקע בשנים אלו בפיתוח יכולות הגנת סייבר מדינתיות, כולל הפניית תקציבים לגופי אכיפת החוק הנלחמים בפשע מאורגן. תקציבים נמוכים באופן יחסי הופנו למגזר הפרטי, לאקדמיה ולמערכת החינוך.[9]

עדכון אסטרטגיית הסייבר הלאומית של בריטניה

"אסטרטגיית הביטחון הלאומי" (NSS) הבריטית, שפורסמה בשנת 2015, הגדירה את איום הסייבר כאיום ראשון במעלה וכסיכון ברמה עליונה לאינטרסים של בריטניה.[10] שנה לאחר מכן פורסמה אסטרטגיית הסייבר הלאומית של בריטניה לשנים 2016–2021. במסגרת זו הוגדר ביטחון הסייבר כ"הגנה על מערכות מידע (תוכנה, חומרה ותשתיות נלוות), המידע שנמצא על מערכות אלו והשירותים שהמערכות מספקות, מפני חדירה של גורמים לא מורשים, נזק או שימוש לא נכון, כולל נזק שנעשה בכוונה תחילה על ידי מפעיל מערכת, או לא בכוונה כתוצאה מאי־עמידה בתקנות אבטחה".[11]

9 כשלושה רבעים מתקציב הסייבר הלאומי לשנים 2011–2016, בגובה של 650 מיליון ליש"ט, הופנו ל־GCHQ ולסוכנויות ביטחון נוספות. ראו: "The UK Cyber Security Strategy: Landscape Review", *National Audit Office*, February 12, 2013, p. 16, https://www.nao.org.uk/wp-content/uploads/2013/03/Cyber-security-Full-report.pdf.

10 "National Security Strategy and Strategic Defence and Security Review 2015", November 23, 2015, https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015.

11 Cabinet Office, National security and intelligence, HM Treasury, and The Rt. Hon. Philip Hammond MP, "HM Government, National Cyber Security Strategy 2016-2021", p. 15.

אסטרטגיית הסייבר הלאומית זיהתה את האיומים העיקריים הבאים על מרחב הסייבר הבריטי:[12]

- **פשיעת סייבר**: פשעים מבוססי סייבר המתבצעים באמצעות השימוש בטכנולוגיית מידע ותקשורת (ICT), כאשר גם התוקף וגם הקורבן משתמשים בכלי ICT; פיתוח נוזקות לביצוע הונאות פיננסיות, פריצה, גניבה, שיבוש או מחיקת מידע; פשעים "מסורתיים" בהם נעזרים הפושעים במחשבים, ברשתות מחשבים או בכול סוג אחר של ICT (כגון גניבת מידע או הונאה); פשיעת סייבר מאורגנת על ידי ארגוני פשיעה, בדגש על ארגונים דוברי רוסית שמקורם במזרח אירופה.
- **מדינות וקבוצות בחסות מדינתית**: ניסיונות חוזרים ונשנים של גורמים להסתנן לרשתות מידע בריטיות במטרה להשיג יתרונות אסטרטגיים, פוליטיים, טכנולוגיים, מדיניים ומסחריים. האיומים העיקריים בהקשר זה הם כלפי גורמי ממשל, ביטחון, כלכלה, אנרגיה ותקשורת. רק למספר מדינות מצומצם יש יכולת להוות איום רציני על בריטניה, אך מדינות רבות נוספות נמצאות בתהליכי פיתוח (או רכישה) של כלי סייבר שיוכלו להוות איום עליה בעתיד הלא רחוק. בנוסף לקמפיינים של ריגול, קיים איום של נשק סייבר התקפי גם נגד תשתיות קריטיות.
- **טרור**: קבוצות טרור מנהלות פעילות במרחב הסייבר נגד מטרות בריטיות, למרות שהיכולות הטכניות שלהן הן נמוכות בשלב זה. אף על פי כן, גם תקיפה באמצעות כלים פשוטים היא בעלת פוטנציאל לנזק גדול. עיקר האיום מגיע מתקיפות להשחתת אתרים, הדלפת פרטים אישיים וכדומה. מטרת ארגוני הטרור היא השגת חשיפה ציבורית והרתעת הקורבנות. הצפי הוא לעלייה בתדירותן של תקיפות מסוג מניעת שירות והשחתת אתרים, ולצד זאת התגברות האיום של הפעלת אנשים מבפנים (Insider Threat).
- **האקטיביזם**: מדובר בקבוצות של האקטיביסטים, שתקיפותיהן העיקריות הן מסוג מניעת שירות והשחתת אתרים. אלו הן קבוצות מבוזרות, המכַוונות את תקיפותיהן לנושאים ממוקדים ובוחרות את קורבנותיהן בקפידה.
- **Script Kiddies**: מדובר לרוב ביחידים בעלי יכולות סייבר מוגבלות שמשתמשים בכלי תקיפה שפותחו על ידי אחרים. הם אינם בעלי פוטנציאל להוות איום רחב על הכלכלה והחברה, אך בעלי פוטנציאל לגרום לנזק משמעותי ליחיד או לארגון.

האסטרטגיה שפורסמה ב־2015 לא השיגה את היעד של הבטחת נכסיה הדיגיטליים של בריטניה. מצב זה הביא את ממשלת בריטניה לתובנה כי נדרשת השקעת משאבים רבים יותר כדי לעמוד מול הדינמיות המשתנה של האיומים, והוביל לניסוח החזון לשנת 2021, הנשען על תפיסה אסטרטגית לאומית לביטחון סייבר.

12 שם, עמ' 18.

תפיסה זו כוללת ארבעה מרכיבים עיקריים: הגנה, הרתעה, פיתוח ופעילות בין־לאומית, כמפורט להלן:[13]

- **הגנה**: התבססות על המשאבים הקיימים בבריטניה להגנה מפני איומי סייבר במטרה ליצור יכולת תגובה אפקטיבית לאירועים ולהבטיח את תקינות הרשתות ומערכות המידע. נקודת המוצא היא שיש להגיע ליעד שבו אזרחים, עסקים והשירות הציבורי יהיו בעלי ידע ויכולת להגן על עצמם מפני תקיפות סייבר. לצורך זה תמקד הממשלה את משאביה, ביחד עם אלה של התעשייה, לפיתוח וליישום הגנת סייבר אקטיבית שתצמצם עד למינימום את תקיפות הסייבר בשגרה, ובהן תקיפות דיוג, פילטור כתובות IP זדוניות וחסימה אקטיבית של פעילות זדונית.[14] היכולת המדינתית נגד צורות תקיפה בסיסיות אלו תשפר את יכולת ההתגוננות הבריטית מול רוב איומי הסייבר הידועים.
- **הרתעה**: ביצור מרחב הסייבר הבריטי מפני כל צורות של תוקפנות, תוך זיהוי ניסיונות תקיפה, הבנתם, חקירתם ושיבושם. בנוסף לכך, רדיפת התוקפים והעמדתם לדין, גם על ידי פעילות התקפית במרחב הסייבר. בריטניה תפעל להעברת מסרים ברורים לאויביה על התוצאות הצפויות של כל איום או ניסיון לפגוע באינטרסים שלה או של בעלות בריתה במרחב הסייבר.
- **פיתוח**: תמיכה בחדשנות ובצמיחה של תעשיית הסייבר הבריטית. מדובר, בין היתר, במחקר ופיתוח מדעיים; בהשקעה במשאבים אנושיים במגזר הציבורי והפרטי; בהשקעה בהכשרת חוקרים ומומחים לאיומי הסייבר העתידיים; בהשקעה במחקר בראייה ארוכת טווח במטרה לעודד פיתוח הון אנושי של אנשי אקדמיה בתחום הסייבר.
- **פעילות בין־לאומית**: העמקת שיתופי הפעולה הקיימים עם השותפים הבין־לאומיים הקרובים לבריטניה ויצירת שיתופי פעולה חדשים לבניית יכולות שיסייעו לאבטחת נכסי הממלכה ברחבי העולם. שיתופי פעולה אלה יושגו באמצעות הסכמים בילטרליים ומולטילטרליים ויכללו, בין השאר, את האיחוד האירופי, נאט"ו והאו"ם.

דוח משותף של "סוכנות הפשיעה הלאומית" (NCA) ושל "מרכז ביטחון הסייבר הלאומי" (NCSC), שפורסם במארס 2017, מדגיש את הצורך בשיתוף פעולה בין התעשייה, הממשלה וגורמי אכיפת החוק בבריטניה לנוכח התגברות איום הסייבר והשינויים המהירים המתרחשים בתחום זה. הדוח מתמקד בתהליך שבו גורמי

13 שם, עמ' 15.

14 על פי נתוני הממשלה, מאז יוני 2016 נבלמו בסה"כ 54,456 מתקפות סייבר מסוג דיוג והחדרת וירוסים לאתרים. כ־36 אחוזים ממתקפות אלו מקורן בכתובות IP בריטיות. מתוך שאר המתקפות, 64 אחוזים כוונו ספציפית נגד אתרי ממשלה ויועדו להשגת פרטים אישים של אזרחים מתוך מאגרי מידע ממשלתיים.

פשע לומדים את הדרכים בהן שחקנים מדינתיים תוקפים ארגונים כגון מוסדות פיננסיים; בסיכון הנובע מ"האינטרנט של הדברים" לאור העלייה בשיעור המכשירים המחוברים, שרובם אינם מאובטחים על ידי היצרנים או המשתמשים; וכן בעלייה במספר התקפות מניעת שירות בשילוב עם סחיטות ודרישות כופר.[15]

יישום האסטרטגיה הבריטית הלאומית במרחב הסייבר

כדי להשיג את היעדים שהוגדרו באסטרטגיית הסייבר הלאומית לשנים 2016–2021, החליטה ממשלת בריטניה בשנת 2016 על השקעת 1.9 מיליארד ליש"ט בביטחון סייבר. החלטה זו באה בעקבות סדרת מתקפות סייבר אסטרטגיות על מוסדות פוליטיים, מפלגות וגופים פרלמנטריים, וכן איסוף מידע על תשתיות בריטיות לאומיות. כצעד ראשון בשיפור ביטחון הסייבר התבצע שינוי ארגוני במערך הסייבר הבריטי והוחלט על הקמת "מרכז ביטחון הסייבר הלאומי" (National Cyber Security Centre – NCSC),[16] שקיבל את אחריות הביצוע האופרטיבי המדינתי על כל תחום ההגנה של ביטחון הסייבר בבריטניה. אחריות זו כוללת, בין השאר, שיתוף ידע, התמודדות עם נקודות תורפה והובלה מקצועית של נושא הסייבר ברמה הלאומית. מכיוון שלמערכת הביטחון הבריטית יש יכולת חזקה להגן על מערכותיה הפנימיות והיא נדרשת לפעילות אופרטיבית גמישה ועצמאית, הוחלט כי "מרכז ביטחון הסייבר הלאומי" ישתף פעולה עם "מרכז מִבצעֵי ביטחון הסייבר" (Cyber Security Operations Centre) של הצבא הבריטי, תוך יצירת פלטפורמה בין־ארגונית שתאפשר לצבא לקחת חלק בהגנה מול אירועי סייבר בעלי פוטנציאל לפגיעה אסטרטגית ברמה הלאומית.

"מרכז ביטחון הסייבר הלאומי" הושק רשמית באוקטובר 2016 כחלק ממטה ה־GCHQ. החזון שמאחורי הקמתו היה ליצור גוף מטה שיתכלל את ניהול אירועי תקיפות סייבר בחירום, יספק הנחיה בשגרה ובחירום וישמש כמוקד ידע לקהילת הסייבר הבריטית, וכן יהווה גוף מקשר בין הממשלה לתעשייה. המרכז איגם בתוכו גופי ביטחון סייבר קיימים, ובהם "המרכז להערכת סיכוני סייבר" (Centre for Cyber Assessment), ה־CERT הלאומי, וכן את הזרוע של GCHQ שעסקה באבטחת מידע (CESG). בנוסף לכך, המרכז החדש קיבל את האחריות על כל נושאי הסייבר שהיו לפני כן תחת אחריותו של "המרכז לאבטחת תשתיות לאומיות" (Centre for the Protection of National Infrastructure).

15 "The Cyber Threats to UK Businesses, 2016/2017 Report", *NCSC & NCA*, March 14, 2017 http://www.nationalcrimeagency.gov.uk/publications/785-the-cyber-threat-to-uk-business/file.

16 "The Launch of the National Cyber Security Centre", *National Cyber Security Centre*, February 13, 2017, https://www.ncsc.gov.uk/news/launch-national-cyber-security-centre.

תפיסת ההגנה

תפיסת ההגנה הבריטית בתחום הסייבר מבוססת על הצורך לגבש מענה מדינתי לחיזוק ההגנה ברמה הלאומית, לצד הנחיית התעשייה לגיבוש צעדים לאבטחת תשתיות קריטיות לאומיות במגזרים חיוניים, כמו אנרגיה ותחבורה. תפיסת ההגנה הבריטית אמורה להתממש באמצעות שיתוף פעולה עם התעשייה,[17] כולל מיקור חוץ, במטרה להשתמש בטכניקות הגנה אוטונומיות להפחתת השפעתן של תקיפות סייבר המבוצעות על ידי האקרים, ועצירת וירוסים ודואר זבל לפני שהם מגיעים לקורבנות התקיפה. אחד המדדים להצלחה שהוגדרו על ידי הממשלה בהקשר זה הינו משך הזמן שבו אתר זדוני המפיץ נוזקות נשאר פעיל. הסטטיסטיקה בבריטניה הצביעה בעבר על משך זמן של כחודש, לעומת כיומיים בלבד כיום. מדד נוסף הוא מספר אתרי מתקפות דיוג הרשומים בבריטניה אשר מוּרדים מהרשת לאחר כשעה (בעבר משך הזמן להורדתם היה כ־24 שעות).

תפיסת ההגנה הבריטית קובעת עוד כי חלק גדול מהשקעות הממשלה בביטחון סייבר יוקצה לחיזוק יכולות הסייבר של סוכנויות אכיפת החוק וליצירת מענה הגנתי שיגדיל משמעותית את מחיר פשעי הסייבר, וכן לגיבוש שותפויות בין־לאומיות ולבניית יכולות סייבר התקפיות כתגובה לתקיפות מדינתיות נגד בריטניה. כחלק מההתעצמות בתחומים אלה, גויסו יותר מחמישים חוקרי סייבר ומומחים טכנולוגיים ליחידה הלאומית להתמודדות עם פשיעת סייבר ותוקצבו עשרות מיליוני ליש"ט ללחימה בפשעי סייבר.

הגנת סייבר אקטיבית

כדי ליישם את צעדי הביטחון הנדרשים ברמה הלאומית, גובשה תפיסה הנקראת "הגנת סייבר אקטיבית" (Active Cyber Defence – ACD).[18] בהקשר המסחרי, המושג ACD מתייחס בדרך כלל לניתוח סיכוני ביטחון סייבר, לפיתוח הבנה של איומים ברשת וליישום צעדים פרו־אקטיביים הנדרשים כמענה הגנתי לכך. באסטרטגיית הסייבר הלאומית הבריטית, הממשלה בחרה ליישם את התפיסה המסחרית בהקשר רחב יותר: להביא לידי ביטוי את יכולותיה הייחודיות כדי להשפיע על הצעדים שיינקטו נגד מגוון האיומים בסייבר. לפי תפיסה זאת, "הרשת" מייצגת את כל מרחב הסייבר הבריטי ברמת המקרו. כדי לעמוד ביעד ולצמצם את איומי הסייבר נגד בריטניה, כולל מצד קבוצות פשע מאורגנות וישויות מדינתיות

17 דוגמה לשיתוף פעולה עם התעשייה היא עידוד של ה־CERT הלאומי ליצירתם של אשכולות (Clusters) לשיתוף והעמקת ידע בנושאי הגנת סייבר, הפזורים ברחבי בריטניה ופועלים בצורה התנדבותית, עצמאית ולא פורמלית. ראו רשימת האשכולות: https://www.ukcybersecurityforum.com/cyber-security-clusters.

18 "National Cyber Security Strategy 2016-2021", p. 33.

בעלות כוונות זדון, יורחבו סמכויותיהם ויכולותיהם של GCHQ, משרד ההגנה ו"סוכנות הפשיעה הלאומית".

הצלחתה של תפיסת "הגנת הסייבר האקטיבית" תימדד על פי התוצאות הבאות:[19]

- הקמת מערך הגנה רחב שיקשה על ניסיונות לתקיפות דיוג, SMS וזיופים (Spoofing) כחלק מקמפיינים של הנדסה חברתית.
- חסימת נוזקות זדוניות.
- הבטחת התנועה באינטרנט ותקשורת נגד ניסיונות Rerouting.
- הגברת יכולות ה־GCHQ, "סוכנות הפשיעה הלאומית" והצבא הבריטי לתת מענה הגנתי יעיל מפני תקיפות סייבר אסטרטגיות.

שיתוף ידע

אחת התובנות המרכזיות של אסטרטגיית הסייבר הבריטית היא שרוב התקיפות נעשות בכלי תקיפה בסיסיים שהיערכות נכונה של ארגונים יכולה למנוע אותן. לשם כך יצר GCHQ פלטפורמה לשיתוף ידע וכתב מדריך למשתמש בשם *Cyber Essentials*, שהינו שימושי בעיקר להגנה על עסקים קטנים ובינוניים.[20] "מרכז ביטחון הסייבר הלאומי", מצידו, כתב מדריך למשתמש בנושאי הערכת סיכוני סייבר, בשם "עשרה צעדים לביטחון סייבר".[21] למהלכים אלה יש גם משמעויות רגולטוריות הנוגעות לגיבוש הַתֶּקן על פיו נדרשים ארגונים בבריטניה להיערך מבחינת איומי סייבר.[22]

גורם נוסף בתחום ביטחון הסייבר בבריטניה הוא "המשרד לביטחון סייבר ואבטחת מידע" (Office of Cyber Security and Information Assurance – OCSIA). מדובר בגוף הפועל ברמה הממשלתית ותפקידו לתמוך במשרדי הקבינט וב"מועצה לביטחון לאומי" במכלול היבטי הסייבר, להעניק הכוונה אסטרטגית ולתאם את תוכניות ביטחון הסייבר ברמה הממשלתית.[23] "המשרד לביטחון סייבר ואבטחת מידע" עובד בשיתוף פעולה עם משרדי ממשלה וסוכנויות ממשלתיות, כגון משרד ביטחון הפנים, משרד ההגנה, משרד החוץ, משרד התקשורת ו־GCHQ.

---

19 שם, עמ' 35.

20 "Cyber Essentials", *HM Government*, http://www.cyberaware.gov.uk/cyberessentials/

21 "10 Steps to Cyber Security", *NCSC*, April 10, 2016, https://www.ncsc.gov.uk/guidance/10-steps-cyber-security.

22 "Minister for Digital and Culture Matt Hancock's speech at the Cyber Security Institute of Directors Conference in London", March 27, 2017, https://www.gov.uk/government/speeches/matt-hancocks-cyber-security-speech-at-the-institute-of-directors-conference.

23 ראו אתר OCSIA: https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance.

"המשרד לביטחון סייבר ואבטחת מידע" גם אמון על הקצאת משאבים ותכלול בין משרדי הממשלה בתחום הסייבר, וכן עוסק בהיבטים של מדיניות סייבר בממשק מול המגזר הפרטי. בהמשך מתוכנן לקום גוף בשם Emerging Technology and Innovation Analysis Cell (ETIAC). גוף זה אמור לזהות התפתחויות, איומים והזדמנויות טכנולוגיות לטובת הביטחון הלאומי וגופי הסייבר הממשלתיים.[24]

גוף נוסף בעל אחריות מדינתית בנושאים הקשורים לפשעי סייבר הינו "יחידת פשעי הסייבר הלאומית" (The National Cyber Crime Unit – NCCU).[25] היחידה, הכפופה ל"סוכנות הפשיעה הלאומית", החלה בפעילות אופרטיבית בשנת 2013. היא מובילה את תחום התגובה המדינתית לפשעי סייבר, כולל תמיכה בשותפיה במערכת הביטחונית, וכן את תיאום התגובה המדינתית לרוב פשעי הסייבר החמורים במדינה. היחידה פועלת בשיתוף פעולה עם יחידות פשעי סייבר מחוזיות (Regional Organized Crime Units – ROCUs), יחידת פשעי הסייבר של משטרת המטרופולין (של לונדון) (Metropolitan Police Cyber Crime Unit – MPCCU), גורמי תעשייה, גופי ממשל ויחידות אכיפת חוק בין־לאומיות.

בבריטניה פועלת החל משנת 2013 פלטפורמת שיתוף הידע Cyber-Security Information Sharing Partnership. פלטפורמה זו כוללת יותר מאלפיים ארגונים ציבוריים וחברות פרטיות. לחברות ולארגונים הבריטיים ישנה גם נגישות ליוזמת X-Force Initiative של חברת IBM, המסַפקת יותר מ־700 טרה בייט של מידע על איומי סייבר.[26]

מחקר ופיתוח

עידוד המו"פ בא לידי ביטוי בהחלטה להקים מרכזי חדשנות סייבר שיגבשו פתרונות סייבר מתקדמים ויהוו תשתית להקמת חברות סייבר חדשות, וכן בהשקת קרן למימון חדשנות בסייבר, בתמיכה בחברות הזנק ובמחקרים אקדמיים בשיתוף התעשייה. בסך הכול הוקצו במסגרת אסטרטגיית הסייבר של 2016 כ־165 מיליון ליש"ט לתמיכה בחדשנות בנושאי הגנה וביטחון סייבר.[27]

בנוסף לאלה מקימה בריטניה "מוסד למחקר ביטחון סייבר" (Cyber Security Research Institute), שיאגד את האוניברסיטאות המובילות במדינה לפעילות לחיזוק אבטחת מכשירים חכמים. "מרכז ביטחון הסייבר הלאומי" ו־GCHQ, מצידם, תומכים בחדשנות ובמחקר בנושאי סייבר לגילאי בית ספר. אחת התוכניות אותה

24 יש לציין כי כיום פועל צוות ייעוץ לחשיבה אסטרטגית בקבינט בשם Secretary's Advisory Group on Horizon Scanning (CSAG).

25 ראו פרטי הסוכנות: http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit

26 "Progress and Research in Cybersecurity", p. 42.

27 שם, עמ' 10.

ממנן GCHQ היא תוכנית Cyber First, במסגרתה לוקחים חלק כ־2500 תלמידי בית ספר בגילאי 11–17 בקורסי סייבר חינמיים.[28] בין השאר כוללת התוכנית תחרות סייבר לבנות בגילאי 13–15.[29]

כ־250 סטודנטים הלומדים מקצועות רלוונטיים במסגרות אקדמיות מקבלים בכל שנה מלגות בשווי 4,000 ליש"ט לשנה, כאשר הכוונה היא להגיע למספר של אלף סטודנטים בשנת 2020. "מרכז ביטחון הסייבר הלאומי" ו־GCHQ משתפים פעולה עם כעשרים אוניברסיטאות מובילות ברחבי בריטניה בהעברת עשרים קורסים לתלמידי תואר שני, בהם ממשיכים הסטודנטים לשנה נוספת של לימודים אינטגרטיביים מתקדמים בפורנזיקה דיגיטלית, מדעי המחשב וסייבר. "מרכז ביטחון הסייבר הלאומי" גם יצא במספר יוזמות מחקריות הכוללות, בין השאר, תוכנית להקמת 13 מרכזים אקדמיים למחקר מצוינות בסייבר ומתן מלגות לשלושים תלמידי תואר שלישי שנבחרים מתוך מרכזי המצוינות. "מרכז ביטחון הסייבר הלאומי" גם הקים את "מרכז חדשנות הסייבר הממשלתי" (Cyber Security Innovation Centre) המשמש כחממה לחברות הזנק.

GCHQ פרסם ב־2017 קול קורא למימון מיזמים ומחקרים והקים תוכנית האצה לחברות הזנק בתחום הסייבר.[30] תוכנית האצה זו כוללת בשלב הראשון שבע חברות הזנק הזוכות לתמיכה מתאגידים כגון "טלפוניקה" ו"סיסקו". הכוונה של GCHQ היא למצוא חברות הזנק, דוגמת Cyber Owl, שפיתחה מערכת התרעה מוקדמת המספקת מודיעין בזמן אמת; Status Today, שפיתחה פלטפורמת בינה מלאכותית כדי להבין התנהגות אנושית במקום העבודה ולמנוע מתקפות מתוך הארגון; ו־Elemendar, שהיא פלטפורמת בינה מלאכותית לניתוח דוחות סיכונים.

יוזמה המתמקדת בשיתוף פעולה ממשלתי עם התעשייה במימון מחקרי סייבר באקדמיה היא תוכנית Cyber Invest. ממשלת בריטניה הכריזה על התוכנית בשנת 2015, כחלק משיתוף פעולה בינה ובין התעשייה המקומית במטרה ליישם מחקרי סייבר במישור המסחרי. תוכנית זאת היא חלק מ־165 מיליון ליש"ט שהוקדשו להגנה וחדשנות בסייבר במטרה לסייע לחברות הזנק להגיע להישגים מסחריים,

28 "Applications open for GCHQ's Cyber Summer Schools", *GCHQ,* May 20, 2016, https://www.gchq.gov.uk/press-release/applications-open-gchqs-cyber-summer-schools.

29 "National Challenge will Develop Schoolgirls' Cyber Security Skills", *GCHQ*, January 18, 2017, https://www.gchq.gov.uk/press-release/national-challenge-will-develop-schoolgirls-cyber-security-skills.

30 "The first-ever GCHQ-backed accelerator programme for cyber security start-ups concludes today, with all parties involved hailing it as a huge success", *Wayra*, March 30, 2017, https://wayra.co.uk/first-cyber-security-start-ups-graduate-from-unique-gchq-cyber-accelerator-programme/

וכן לסייע ליוזמות לא מסחריות בתחום הסייבר.[31] בשנה שלאחר ההכרזה על התוכנית התחייבו 18 חברות להשקיע 6.5 מיליון ליש"ט במהלך חמש השנים הבאות בתחום זה.

גוף מחקרי נוסף בתחום ביטחון הסייבר הוקם בשנת 2013 – "מכון המחקר למדעי ביטחון הסייבר" (The Research Institute in Science of Cyber Security).[32] ייעודו הוא פיתוח מדעי ויצירת סטנדרטים ושיטות פעולה לטובת מקבלי ההחלטות בתחום הסייבר. המכון ממומן על ידי ה־GCHQ ו"המועצה למחקר בהנדסה ופיזיקה" (The Engineering and Physical Sciences Research Council).

פעילות בין־לאומית

בריטניה מימנה בשנת 2016 תוכניות לחיזוק החוסן הלאומי בתחום הסייבר ולתמיכה ב־35 פרויקטים בכשבעים מדינות בעולם, בעלות של 3.5 מיליון ליש"ט. אחת המדינות איתן מקיימת בריטניה תוכניות מחקר משותפות בתחום הסייבר היא סינגפור. תוכנית מו"פ משותפת לשתי המדינות בנושאי ביטחון סייבר הושקה ב־2015, והיא כוללת מימון למחקרים בתחום זה.[33] מאז השקת התוכנית נערכו במסגרתה שש תוכניות מחקר משותפות בעלות מוערכת של 2.4 מיליון ליש"ט.[34]

בריטניה חתומה על הסכמי שיתוף פעולה בתחום הסייבר עם מדינות רבות ברחבי העולם ומקיימת שיתופי פעולה אסטרטגיים בתחום זה עם ארצות הברית, אוסטרליה, ניו זילנד וקנדה.[35] שיתוף הפעולה הבין־לאומי של בריטניה בתחום פשיעת הסייבר נמצא באחריות "סוכנות הפשיעה הלאומית", המקיימת קשרים עם "אינטרפול", "יורופול" וסוכנויות נוספות.[36] ממשלות בריטניה גם מקדמות בשנים האחרונות דיאלוגים אסטרטגיים עם מדינות שונות בתחום הסייבר. כך, ב־2016 גיבשה בריטניה מסמך הבנות עם סין להעמקת קשרי שתי המדינות בתחום הסייבר, כולל בניית מכניזם לשיתוף מידע מודיעיני, שיתוף פעולה במצבי חירום

31 "Progress and Research in Cybersecurity", p. 60.

32 ראו אתר התוכנית: http://www.riscs.org.uk.

33 ראו אתר התוכנית: https://www.nrf.gov.sg/funding-grants/international-grant-calls/joint-singapore-uk-research-in-cyber-security.

34 Ankit Panda, Conrad Prince, "On the United Kingdom's Cyber Strategy and Asia", *The Diplomat*, October 15, 2016, http://thediplomat.com/2016/10/conrad-prince-on-the-united-kingdoms-cyber-strategy-and-asia/.

35 "What is the Five Eyes Intelligence Alliance?", *France 24*, March 17, 2017, http://www.france24.com/en/20170317-what-five-eyes-intelligence-alliance.

36 "International Cooperation", *The National Crime Agency*, http://www.nationalcrimeagency.gov.uk/about-us/working-in-partnership/international-cooperation.

ועוד.[37] באותה שנה גם יצאו ממשלות בריטניה והודו בהצהרה משותפת על שיתוף פעולה אסטרטגי ביניהן, כולל בתחום הסייבר.[38]

פערים ביישום האסטרטגיה הבריטית

למרות הגדלה משמעותית של התקציב הבריטי להגנת מרחב הסייבר לשנים 2016–2021, וכן הארגון מחדש ואיגום הסמכויות של זרועות הגנת הסייבר בבריטניה, אתגרים ופערים רבים מַקשים עדיין על הטמעתה ויישומה האפקטיבי של אסטרטגיית הסייבר הבריטית: ראשית, המדיניות של השפעה פעילה על תהליכי פיתוחה של חדשנות טכנולוגית לטובת הגנת הסייבר, אותה נקטה ממשלת בריטניה, דורשת יצירת איזונים בין המרכיבים הביטחוניים, הטכנולוגיים, הכלכליים והחברתיים. למרות זאת, נראה כי המרכיב הביטחוני הוא דומיננטי ביחס למרכיבים האחרים ומשמש ציר מרכזי שדרכו פועלת הממשלה ליצור תנאים שיאפשרו התפתחות ידע וסביבה טכנולוגית חדשנית. מהזווית ההגנתית־ביטחונית, ובמיוחד לאור המבנה ההיסטורי של מערכת הביטחון והאכיפה הבריטית, טבעי הוא שריכוז יכולת הגנתית ברמה גבוהה ייעשה באמצעות זרועות ה־GCHQ; אך ציר זה מהווה חיסרון בכול הנוגע לממשקים המתקיימים מחוץ למערכת הביטחון הבריטית, שיכולים לסייע בהפריה הדדית בין המערכת הביטחונית ובין המערכת האזרחית, כגון פיתוח ידע אקדמי, הכשרת אנשי מקצוע איכותיים, קשרי גומלין בין התעשייה לאקדמיה, פיתוח עסקי וחדשנות טכנולוגית. הדומיננטיות של GCHQ גם מקשה על בריטניה בכול הקשור לשיתוף פעולה עם חברות טכנולוגיה גלובליות. כלומר, בחירתם של מעצבי התפיסה האסטרטגית הבריטית להתבסס על המשאבים הקיימים בבריטניה להגנה מפני איומי סייבר יוצרת כשל מובנה המציב אתגרים בפני יישום המענה הרצוי. כשל זה בא לידי ביטוי, בין השאר, בהיעדר עידוד משמעותי לחברות טכנולוגיה גלובליות לקדם פיתוח, מחקר ועשייה עסקית משמעותית בבריטניה.

שנית, יש המצביעים על דמיון בין המבנה והמדיניות של מערך הסייבר הבריטי לאלה של מדינת ישראל. השוואה זו לא עומדת במבחן התוצאה בכול הקשור לקשיים של המודל הבריטי לאפשר מערכת סביבתית יעילה של ביטחון, תעשייה, חינוך ואקדמיה. כך, למשל, ישראל שומרת על רמת תחרותיות גבוהה בשוק הסייבר העולמי, בין השאר כתוצאה מכך שבוגרי יחידות טכנולוגיות במערכת

37 "China-UK High Level Security Dialogue: Communique, Policy Paper", *Cabinet Office*, June 13, 2016, https://www.gov.uk/government/publications/china-uk-high-level-security-dialogue-official-statement/china-uk-high-level-security-dialogue-communique.

38 "Joint Statement between the Governments of the UK and India, Press Release", *Prime Minister Office*, November 7, 2016, https://www.gov.uk/government/news/joint-statement-between-the-governments-of-the-uk-and-india.

הביטחון שלה הקימו חברות מצליחות המספקות מוצרים ביטחוניים דואליים המיועדים לשימוש ביטחוני ואזרחי כאחד, ו/או טכנולוגיות ביטחוניות שניתן למצוא להן יישומים אזרחיים. יתרונה היחסי של מערכת הביטחון הישראלית הוא בכך שהיא לא בהכרח ממציאה את הטכנולוגיה, אלא מבצעת התאמות של פיתוחים אזרחיים הקיימים בשוק הפרטי בהתאם לצרכיה. לעומת זאת, המצב בבריטניה נראה שונה, ובמקרים רבים אף הפוך: המערכת הביטחונית הבריטית תורמת את חלקה לפיתוח טכנולוגי, שרק חלקו עובר לאחר מכן לשוק האזרחי. כתוצאה מכך, המנגנון הממשלתי הבריטי מצמצם את יכולת תעשיית הסייבר המקומית לשמור על יתרון יחסי במציאות של תחרות גלובלית וגם מול איומים מתהווים. מצב זה יישמר כל עוד ממשלת בריטניה תמשיך להשקיע את מרבית תקציב הגנת הסייבר בסוכנויות האמונות על כך. יש להניח כי בתקציב הממשלתי להגנת סייבר המיועד לסוכנויות הביטחון והמודיעין הבריטיות, כגון GCHQ, משאבים רבים מופנים גם כיום להתקפה ולא להגנה, ויותר משאבים מופנים להגנת תשתיות קריטיות ולא להגנת תשתיות אחרות. כמענה לפער זה, על בריטניה לשקול את ניתוקו המלא או החלקי של "מרכז ביטחון הסייבר הלאומי" מ־GCHQ ולהפוך אותו לגוף בעל מאפיינים אזרחיים יותר שיַקלו על הנגשתו למגזר הפרטי. בריטניה גם נדרשת למצות באופן נכון יותר מידע ופתרונות טכנולוגיים המועברים מהמגזר הביטחוני הבריטי לתעשייה האזרחית וחוזר חלילה. דרך נכונה ליישם זאת היא, בין השאר, גישה הוליסטית שתחלק את המשאבים בצורה מאוזנת יותר בין ביטחון ובין השקעות בחינוך, באקדמיה ובמגזר הפרטי.

שלישית, יציאת בריטניה מהאיחוד האירופי צפויה להיות בעלת השלכות על ביטחון הסייבר הלאומי שלה. העזיבה תביא, ככול הנראה, ליציאה של בריטניה מארגונים באיחוד האירופי בהם היא חברה כיום, כגון "מרכז פשיעת הסייבר האירופי" (European Cybercrime Centre), ובכך היא לא תהיה עוד שותפה למאמצי מניעת פשיעת סייבר באיחוד. טרם ברור מה תהיה המדיניות הבריטית לגבי נושאים רגולטוריים משותפים למדינות האיחוד האירופי, כגון "רגולציית אבטחת המידע" (General Data Protection Regulation – GDPR), ועד כמה היא תשתנה בעקבות עזיבת בריטניה את האיחוד.[39] אתגר שאיתו תיאלץ בריטניה להתמודד ביתר שאת בעקבות עזיבת האיחוד האירופי הינו גיוס כוח אדם איכותי למקצועות הסייבר. ביטחון סייבר התווסף בנובמבר 2015 לרשימת המקצועות בהם ישנו מחסור בבריטניה, דבר שאִפשר לאזרחים מחוץ לאיחוד האירופי להגיש בקשה לאשרת עבודה שם. עזיבת בריטניה את האיחוד עלולה להביא למצב הפוך,

39 החלטה במסגרת GDPR, שצפויה להיכנס לתוקף באיחוד האירופי במהלך 2018, היא דרישה מחברות הרשומות באיחוד להודיע לממשלותיהן על תקיפות סייבר נגדן בתוך 72 שעות. ראו גם אתר אבטחת המידע האירופי: http://www.eugdpr.org /

בו בעלי מקצוע בריטיים בתחום הסייבר יבחרו לעבוד במדינות אחרות (בהן רמת ההכנסה ואפשרות המוביליות יהיו גבוהות יותר לאחר ה"ברקזיט"). כמו כן, בריטניה תיאלץ למצוא דרכים תקציביות לממן מחקר אקדמי בתחומים טכנולוגיים, שכיום ממומן חלקית מתקציבי האיחוד האירופי. מענה לכך בטווח הקצר הינו הסטת משאבים שיועדו למחקר ופיתוח ולמימון קרנות של האיחוד האירופי לטובת פתיחת קרנות ייעודיות למחקרים אקדמיים במרכזי הידע הבריטיים. לעומת זאת, עזיבת האיחוד האירופי לא צפויה לפגוע בשותפויות הסייבר האסטרטגיות של בריטניה עם מדינות ה־"Five Eyes" (אוסטרליה, קנדה, ניו זילנד, בריטניה וארצות הברית).[40]

סיכום

בריטניה קיבלה החלטה אסטרטגית ארוכת טווח בנושא ביטחון הסייבר הלאומי, שכוללת חיזוק החוסן הלאומי במרחב הסייבר בכלל ובמרחב הדיגיטלי בפרט. זאת, באמצעות השקעות ממשלתיות המכוונות ליצירת הון אנושי, החל מרמת בתי הספר, כולל הקמת מרכזי מצוינות למחקרי סייבר ותוכניות האצה בסייבר לחברות הזנק. חלק מהמשאבים מוקדשים לארגון מחדש של מערך הסייבר ההגנתי ולגיוס מומחי סייבר לרשויות אכיפת החוק וסוכנויות הביון של בריטניה. גולת הכותרת של האסטרטגיה הבריטית היא הקמת "מרכז ביטחון הסייבר הלאומי", האמון על בניית גשר בין הממשלה והתעשייה ועל הנחייה וניהול של מצבי חירום, כולל נגד תקיפות סייבר המכוונות לתשתיות לאומיות קריטיות.

לצד בניית יכולות הרתעה התקפיות, פועלת בריטניה בטווח הקצר לצמצום תקיפות סייבר "בסיסיות", המהוות את רוב המתקפות עליה. לצד זאת, בריטניה גיבשה חזון, לפיו נושאים כמו מערכות אוטונומיות, "האינטרנט של הדברים" וטלפונים חכמים, שיהוו את מרבית האיומים בטווח הבינוני, זוכים כבר היום למענה. זאת, על ידי הקמת תשתית מחקרית אקדמית ומסחרית שתנסה להתמודד עם האתגרים והאיומים לאורך זמן.

אסטרטגיית ביטחון הסייבר הלאומית של בריטניה לשנים 2016–2021, המתוקצבת בכ־1.9 מיליארד ליש"ט, הציבה במוקד את יישום התפיסה של הסתמכות עצמית על המשאבים הטכנולוגיים והאנושיים לצורך הגנה, וכן את יצירתם של מנגנוני הרתעה ושיתופי פעולה בין־לאומיים. נראה כי בניגוד לעבר, בו GCHQ וארגוני הביטחון הבריטיים הסתמכו על מערכותיהם שלהם בכול מה שנוגע לתחומי המו"פ הביטחוניים, התפיסה הבריטית הנוכחית מעודדת ביזור יכולות ומחקר, ואף כוללת אסטרטגיה חדשה, בה GCHQ פתוח יותר מבעבר לשיתופי

40 "The Implications of Brexit on UK Cyber Policy", *Council on Foreign Affairs*, June 28, 2016, https://www.cfr.org/blog/implications-brexit-uk-cyber-policy.

פעולה עם גופים אזרחיים וציבוריים כדי לקדם חדשנות טכנולוגית, פיתוח הון אנושי וצמיחת שוק הסייבר הבריטי האזרחי.

למרות כל המאמצים שנעשו עד כה, אתגרים ופערים רבים ממשיכים להקשות על הטמעת אסטרטגיית הסייבר הבריטית. בין שאר האתגרים – ריכוזיות היתר של מבנה הגנת הסייבר הבריטי בראשות GCHQ ועזיבתה הצפויה של בריטניה את האיחוד האירופי. מענה אפשרי לאתגרים אלה הינו חלוקת משאבים מאוזנת יותר בין השקעה בביטחון סייבר ובין השקעות בחינוך, באקדמיה ובמגזר הפרטי.

מערכה בסייבר או סייבר במערכה

אבנר שמחוני

תחום הסייבר הופך לזירת פעולה יותר ויותר לגיטימית, אגב הרגלת המערכת הבין־לאומית לשימושים השונים הנעשים בזירה זו למגוון צרכים. ישראל רואה בתחום זה מרכיב חיוני במארג הביטחון הלאומי, המצריך השקעה ושיפוח.
בראייה היסטורית, ניתן לקבוע כי הצלחה של מערכות ביטחוניות ומודיעיניות נבעה משילוב מושכל של התחומים החדשים אל תוך המארג הקיים – באמצעים, בשיטות ובתפיסות – אגב ביצוע השינויים וההתאמות הנדרשים.
על רקע התבססותו המהירה של תחום הסייבר בתודעה ובמערכות השונות, יש לשמור על פרספקטיבה כוללת, שבה הסייבר הוא מרכיב חשוב ומתרחב, אבל לא מובחן או עומד בפני עצמו. דברים אלה מקבלים משנה תוקף בכול הנוגע לתהליכי הערכת המצב וקבלת ההחלטות ולסוגיית הפעלת הכוח לנוכח מגוון האיומים והזירות.

מילות מפתח: הערכת מצב, תהליך קבלת החלטות, סייבר במערכה, הפעלת הכוח, מולטי־דיסציפלינריות, מהפכות טכנולוגיות.

מבוא

אנו מצויים בעיצומה של מגמה כלל־עולמית שבה ממד הסייבר הופך לגורם מרכזי בכול תחומי החיים. מרכזיות זו יוצרת תלות של מדינות מפותחות וכלכלות מתקדמות בסייבר כתווך חיוני, החל מההתנהלות ברמת הפרט, דרך המערכות הכלכליות והתנהלות המדינה מול אזרחיה, וכלה בהשפעה על מהלכים גלובליים. לצד זאת ניכרות מעורבות והשפעה של הסייבר בהיבטים ביטחוניים וצבאיים, הגוברות ככול שמערכות רבות יותר משובצות במרכיבי תקשורת ומחשוב.

בין אירועי הסייבר הבולטים שדווחו בשנת 2016 ניתן למנות:

- תקיפות נגד תשתיות חיוניות באירופה, לרבות מערכות חשמל.

* מוסמך התוכנית ללימודי ביטחון באוניברסיטת תל אביב. חוקר בתחומי הביטחון והאסטרטגיה. המחבר מבקש להודות לתא"ל (מיל') מאיר פינקל, מפקד מרכז דדו, על הערותיו המועילות.

- תקיפת שרתי המפלגה הדמוקרטית בארצות הברית.
- תקיפות נגד יעדים בווייטנאם.
- תרגיל הסייבר הבין־לאומי Locked Shields בהשתתפות חברות נאט"ו ומדינות נוספות.
- פריצה למערכת מסחר אלקטרונית בהודו וגניבת פרטיהם של כעשרה מיליון לקוחות.
- תקיפת ה־DDOS הנרחבת נגד ספקית השירות האינטרנטי האמריקאית, חברת DYN, ושיבוש הפעילות באתרים רבים ומרכזיים למשך זמן מה.
- פריצה וגניבה של עשרות מיליוני דולרים מהבנק המרכזי בבנגלדש באמצעות מנגנון ה־SWIFT (פעולה אוחרת אפקטיבית הביאה לצמצום ניכר בסכום שנגנב באירוע זה).[1]

תחום הסייבר הופך לזירת פעולה יותר ויותר לגיטימית, תוך הרגלַת המערכת הבין־לאומית לשימושים השונים הנעשים בזירה זו למגוון צרכים. לצד גורמים מדינתיים או נתמכי מדינות, פועלים בתחום זה, בעוצמה פחותה, גם האקרים בודדים וארגונים "פרטיים", המנצלים את בעיית הייחוס (Attribution) במרחב הסייבר. כיום מוכרות בעולם למעלה מחצי מיליארד נוזקות מסוגים שונים הפועלות במרחב זה.

בשונה מתחומי עוצמה מסורתיים, תאגידי האינטרנט והסחר הענקיים, ברובם אמריקאיים (דוגמת Apple, Amazon, Twitter, Microsoft, Facebook, Google), משמשים גם הם שחקני מפתח בזירה, כאשר בעקבותיהם דולקות חברות סיניות (דוגמת Huawei, Alibaba ואחרות). תאגידי ענק אלה משמשים הרבה מעבר ל"פלטפורמות" ניטרליות והפכו למעין "שומרי הסף" ומעצבי התודעה החדשים: הם המנגישים והקובעים מה יוגש לציבור ומתי, בעוד שמדינות וגורמים בין־לאומיים נעדרים כמעט לחלוטין סמכות רגולציה לגביהם. יש לצרף לכך את חברות האבטחה וההגנה בסייבר, אשר ביחד עם תאגידי האינטרנט יוצרות סביבה ייחודית לתחום הסייבר. מהפכת ה־Big Data (נתוני העתק) והחיבוריות הגבוהה

1 מאיר אורבך, "חדשנות ההאקרים מתפתחת כמו הסייבר", **כלכליסט**, 24 בינואר 2017; "נגיד הבנק המרכזי של בנגלדש התפטר לאחר ש־81 מיליון דולר נגנבו מחשבון הבנק ע"י האקרים", **גלובס**, 15 במארס 2016; Jim Finkle, "Bangladesh Bank Hackers Compromised SWIFT Software, Warning Issued", *Reuters*, April 25, 2016; Eric Lipton, David E. Sanger and Scott Shanedec, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.", *The New York Times*, December 13, 2016; Kyle York, "Dyn Statement on 10/21/2016 DDoS Attack", *Company News*, October 22, 2016, http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/; "Cyber-Terrorists Attack Flight Info Screens at Vietnam's 2 Major Airports", *VnExpress*, July 29, 2016, http://e.vnexpress.net/news/news/cyber-terrorists-attack-flight-info-screens-at-vietnam-s-2-major-airports-3444504.html; "Locked Shields 2016", *NATO Cooperative Cyber Defence Centre of Excellence*, April 18, 2016.

כתוצאה מהמימוש הגובר של התקני "האינטרנט של הדברים" העמיקו עוד יותר את המודעות והחשיפה לתחום הסייבר, ואיתן את ההיערכות וההשקעה של השחקנים השונים בתחום זה, ולמעשה בכלל הדיסציפלינות.

במקביל לכך מתנהלת פעילות דיפלומטית באו"ם, בנאט"ו ובמוסדות אחרים (לרבות במישור הבילטרלי, כמו בהסכם אי־התקיפה המוגבל בין סין לארצות הברית מ־2016) לצורך גיבוש נורמות ולהתמודדות בין־לאומית מתואמת ויעילה יותר נגד האיומים המשותפים. כך, הרשויות בארצות הברית ובמספר מדינות אחרות גיבשו דרישות בתחום הרגולציה הפנימית ביחס לאתגרי הסייבר,[2] וכן באשר לחיזוק יכולת הבנקים להתמודד עם מתקפות סייבר. במוקדן של דרישות אלו ניצבת (בשלב זה) הוכחת יכולת גיבוי והתאוששות של המוסדות הפיננסיים ממתקפת סייבר חמורה. ואכן, מוסדות אלה מסתמנים כיום כמובילים במגזר הפרטי־אזרחי בהשקעה בהגנת סייבר.

על פי סקר של פירמת רואי החשבון פאהן קנה, הנזק הכלכלי השנתי מאירועי סייבר בעולם נאמד במאות מיליארדי דולר.[3] עוד מוערך, כי תקיפות הסייבר הגיעו למקום השני בפשיעה הכלכלית העולמית וכי הן פוגעות בכ־35 אחוזים מהחברות. מקרים של תקיפות מסוג Ransomware ("כופרה") עלו בשנה האחרונה בכאלף אחוזים ברחבי העולם, ומספר התקיפות מסוג זה צפוי להמשיך ולגדול.[4]

יעדי תקיפות הסייבר הם מגוונים: גופי ביטחון, גורמים ממשלתיים ופוליטיים, מגזרי התעשייה והפיננסים (גניבת מידע עסקי וגניבת כסף), מאגרי מידע, פשיעה נגד אזרחים ואף תקיפת תשתיות חיוניות.[5] קשה לכמת את הנזק שנגרם בהיבט הביטחוני־צבאי הישיר כתוצאה מתקיפות הסייבר, אך ברור כי גם בהיבט זה תוחלת הנזק גבוהה מאוד, וכתוצאה מכך ממסדי הביטחון בכול העולם משקיעים משאבים רבים להגנת מערכותיהם. ראש ה־CIA לשעבר, דיוויד פטראוס, ציין בעניין זה: "ההאקרים נהיים יותר ויותר יצירתיים ומרושעים [...] החדשנות בתחום הפריצות מתפתחת כמו תעשיית הסייבר עצמה".[6]

---

2 טלי ציפורי, "רגולציה מסביב לעולם: התמודדות הממשלות עם אתגרי הסייבר", **גלובס**, 5 באפריל 2016.

3 עידן רבי, "הנזק השנתי מהתקפות סייבר בעולם – כ־315 מיליארד $", **גלובס**, 23 באוקטובר 2015.

4 אביב לוי, "פשיעת הסייבר טיפסה למקום השני בפשיעה הכלכלית בעולם", **גלובס**, 8 בנובמבר 2016.

5 Vindi Goel, "Yahoo Says 1 Billion User Accounts Were Hacked", *The New York Times*, December 14, 2016.

6 אורבך, "חדשנות ההאקרים מתפתחת כמו הסייבר".

מאמר זה מבקש לברר היכן ניצבת ישראל ביחס למגמות הללו, ובאופן ספציפי – כיצד ראוי שהפעלתנות הישראלית בתחום הסייבר תשולב בתוך ההקשר הרחב של הביטחון הלאומי וההתמודדות המערכתית עם איומים בזירות שונות.

המצב בישראל

ישראל רואה בתחום הסייבר מרכיב חיוני במארג הביטחון הלאומי שלה. ככזה הוא מצריך המשך השקעה וטיפוח כדי לשמור על מעמדה המוביל בתחום הסייבר מחד גיסא, ולהתמודד עם האיום הגובר במסגרתו מצד יריבים ואויבים מאידך גיסא. ביטוי לכך ניתן כבר בראשית העשור הנוכחי בוועדת "המיזם הקיברנטי הלאומי" בראשות פרופ' יצחק בן ישראל, שמונתה על ידי ראש הממשלה. ועדה זו התוותה את העקרונות לבניית מערכת סביבתית (eco-system) ישראלית שתאפשר התמודדות מיטבית עם אתגרי עידן הסייבר. החזון והמטרה שהוגדרו במסגרת זו היו: "לשמר את מעמדה של ישראל בעולם כמרכז לפיתוח טכנולוגיות מידע ולהקנות לה יכולות מהשורה הראשונה במרחב הסייבר, כדי להבטיח את חוסנה הכלכלי והלאומי כחברה פתוחה, דמוקרטית ומבוססת ידע".[7]

כמדינות וארגונים אחרים, ישראל היא יעד לתקיפות רבות מסוגים שונים ועל בסיס יומיומי. התקיפות הן לא רק לצורכי גניבת מידע וכסף, אלא גם למטרות שיבוש או גרימת נזק למערכי ייצור, ניהול ובקרה. מספר התקיפות וניסיונות התקיפה עשוי להגיע להיקפים של רבבות מדי יום. בסקר שנערך לאחרונה בין 150 ארגונים עלה כי רבע מהארגונים בישראל סבלו בשלוש השנים האחרונות מתקיפת סייבר כלשהי (על ידי גורמי פשיעה, האקטיביסטים או גורמי טרור), אשר השפיעה על התנהלותם השוטפת.[8] להערכת המכון למחקרי ביטחון לאומי, נזקי פשיעת הסייבר בישראל מתקרבים לעשרה מיליארד דולר בשנה, מתוכם כמה מיליארדי דולרים נזקים מגניבת מידע מסחרי.[9] אירועים מדיניים, ביטחוניים או רגישים אחרים משמשים בדרך כלל כקטליזטור להגברת התקיפות או למימוש יכולות לטנטיות בתחום הסייבר.

---

7 יצחק בן ישראל, "המיזם הקיברנטי הלאומי", *משרד המדע והטכנולוגיה*, מאי 2011. יצוין בהקשר זה כי כבר ב־2002 הכירה ישראל (מבעוד מועד, בין היתר בהמלצתו ובמעורבותו של המל"ל) באספקט מסוים של איום הסייבר על התשתיות החיוניות והקימה גוף ייעודי להתמודדות עם איומים אלה. ראו: יוסי מלמן, "המועצה לביטחון לאומי תרוויח מהבחירות", **הארץ**, 13 בדצמבר 2000.

8 עמי רוחקס דומבה, "חצי מהמשיבים בסקר 'מצב הגנת הסייבר בישראל': לא מוכנים למתקפת סייבר", **Israel Defense**, 29 במאי 2016.

9 רבי, "הנזק השנתי מהתקפות סייבר בעולם".

ההובלה הישראלית בתחום הסייבר מתבטאת בהתוויית מדיניות ואסטרטגיה,[10] בפעולה של גורמים אופרטיביים, בהרחבה של מערך שיתוף הפעולה עם גורמים במערכת הבין־לאומית, בפיתוח טכנולוגי של מוצרי סייבר ביטחוניים ואזרחיים ברמה הגבוהה ביותר בעולם,[11] בידע ותשתית אקדמיים רחבים (כיום פועלים בישראל חמישה מכוני מחקר אוניברסיטאיים בתחום הסייבר) ובהכשרת הון אנושי מיומן בדיסציפלינות המדעיות הקשורות בעולם הסייבר ובמימושו. בישראל פועלות כ־400 חברות סייבר בתחומים שונים,[12] אשר ייצאו בשנת 2015 מוצרים ושירותים בסכומים של מיליארדי דולרים, המהווים קרוב לעשרה אחוזים מכלל שוק הסייבר העולמי. במקביל מקצה ישראל, וכן מושכת מבחוץ, מימון רב למחקר ופיתוח בתחום הסייבר, המצוי בעשור האחרון במגמה עקבית של עלייה. ישראל מרכזת כיום ישראל כ־15 אחוזים מסך ההשקעות במחקר ופיתוח בתחום הסייבר בעולם[13] (נתונים אלה משתנים מדי שנה בשנים האחרונות, עם הגידול בשוק הסייבר העולמי, אם כי ישראל שומרת על מעמד הבכורה שלה הן במונחים מוחלטים והן בערכים יחסיים). התבססות תעשיית הסייבר בישראל מציבה אותה במקום השני בעולם בתחום זה (בערכים מוחלטים) לאחר ארצות הברית.[14]

מערכת הביטחון, המרחב האזרחי והשוק הפרטי בישראל מקיימים ביניהם קשרי גומלין הדדיים בתחום הכשרת כוח אדם ופיתוח יכולות בסייבר: תלמידים רוכשים השכלה טכנולוגית ומדעית עוד לפני גיוסם לצה"ל; המערך הטכנולוגי בצה"ל ובמערכת הביטחון מכשיר ומאמן כוח אדם רב בחזית הטכנולוגיה; כוח האדם שמשתחרר ממערכת הביטחון ממשיך את קידום תחום הסייבר בשוק הפרטי ובתעשיות הביטחוניות; האקדמיה פועלת כל העת לפיתוח הידע התיאורטי

---

10 ראו לדוגמה: רמי אפרתי וליאור יפה, "כך בונים הגנה קיברנטית לאומית", **Israel Defense**, 11 באוגוסט 2012; "מדיניות אסדרת מקצועות הגנת הסייבר במדינת ישראל", *מטה הסייבר הלאומי*, 31 בדצמבר 2015. פעילות בתחום זה מתקיימת גם במרחב האקדמי־מחקרי. ראו לדוגמה: גבי סיבוני ועופר אסף, **קווים מנחים לאסטרטגיה לאומית במרחב הסייבר**, מזכר 149, תל אביב: המכון למחקרי ביטחון לאומי, 2015; Ashton Carter, "Preface by Secretary of Defense", in "The DoD Cyber Strategy", *DoD*, 2015.

11 ראש הממשלה בנימין נתניהו, "ישראל – מעצמת סייבר עולמית", **גלובס**, 3 באפריל 2016. חשוב להזכיר בהקשר זה גם את המגמה של הנבטת טכנולוגיות ויישומים מתקדמים בתוך המערכות הצבאיות (מתוך צרכים מבצעיים), אשר עוברים עם הבשלתם להמשך פיתוח והתבססות בשוק האזרחי־מסחרי. כך היה, לדוגמה, עם המחשבים ומכשירי הסלולר.

12 "The Israeli Cyber Security Map", *IVC Research Center*, January 2017.

13 מאיר אורבך, "15% מההשקעה העולמית בסייבר – בישראל", **כלכליסט**, 26 בינואר 2017.

14 אמיתי זיו, "מעצמת סייבר: המכירות של חברות ישראליות – 10% מהעסקות בעולם", **The Marker**, 25 במאי 2015.

והיישומי. ההשקעה של המדינה, באמצעות זרועותיה השונות, ניכרת ברוב החוליות שנמנו לעיל, בין במישרין ובין בעקיפין.

תחום הסייבר הולך וצובר בשנים האחרונות מעמד מרכזי במדינה, על רקע החזון והמטרה שהוגדרו במיזם הקיברנטי הלאומי, מדיניות ראש הממשלה, החלטות הממשלה והחלטות צה"ל. בינואר 2016 אמר ראש הממשלה בהופעה פומבית כי "הסייבר מייצר הזדמנויות כלכליות נרחבות. אנחנו רוצים להפוך לאחת מחמש המעצמות בתחום הסייבר [...] להוביל את התחום. יש שלושה תחומים עיקריים בסייבר: הלאומי, האזרחי והצבאי [... הדבר הראשון הוא ש]צריך לחסן ארגונים ואזרחים. כל חברה וכל אדם צריכים להיות מוגנים. הדבר השני הוא הגנה. [הדבר] השלישי זה אירועים גדולים שמחייבים תגובה נגד התקיפה והתוקף".[15] לאחרונה התבטא ראש הממשלה שוב בפומבי בנושא זה וציין כי

> הסייבר קשור לכול תעשייה היום [...] האינטרנט של הדברים ייצור כל כך [הרבה] קישורים, שנצטרך הרבה פתרונות להתמודד עם ההגנה בסייבר [...] הסייבר הוא גם זירה חדשה בשדה הקרב [...] בלחיצת כפתור אחת, האקר בודד יכול להוריד מדינה על הברכיים. כמעט כל התשתיות והמידע של המדינה חשופים להתקפות במרחב הסייבר [...] לפני כמה שנים הצבתי יעד שישראל תהפוך למובילה בסייבר. השגנו זאת. פתחנו גם מרכז מחקר בבאר שבע. ישראל מרכזת כחמישית מההשקעות בעולם בתחום הסייבר. זה מכפיל של מאתיים ביחס לאוכלוסייה [...] אנחנו מפתחים את ההון האנושי של ישראל דרך תוכניות הכשרה בצבא ובאקדמיה.[16]

באשר לאיום הגובר בסייבר ציין ראש הממשלה: "ארגוני טרור משתמשים באותם כלים [בהם] אנו משתמשים – נגדנו [...] איראן בונה בשנים האחרונות תשתית טרור במזרח התיכון. האינטרנט של הדברים יכול לשמש ארגוני טרור אלו למטרות מסוכנות. אם לא נעבוד יחד ונשתף פעולה, העתיד יכול להיות מאיים מאוד. בהקשר זה, ישראל, ארצות הברית ומדינות נוספות צריכות לשתף פעולה ברמה ממשלתית ובקרב התעשיות".[17]

תובנות והחלטות אלו מתבטאות בהקצאת משאבים, בהקמתם של ארגונים ובשינויים בארגונים קיימים, בקשב הפיקודי והניהולי ובשילוב הסייבר בתורה, בתוכניות בניין הכוח ובהפעלתו. בין הצעדים שננקטו בשנים האחרונות בהקשר זה

---

15 רפאל קאהאן, "נתניהו בנאום בסייברטק: 'אנחנו רוצים להוביל את תחום הסייבר בעולם'", **כלכליסט**, 26 בינואר 2016.

16 עמי רוחקס דומבה, "דברי ראש הממשלה בכנס סייברטק 2017", **Israel Defense**, 31 בינואר 2017.

17 שם.

ניתן למנות את הקמת מטה הסייבר הלאומי,[18] הרשות הלאומית להגנה בסייבר,[19] מערך הסייבר בצה"ל וגופיו,[20] הקצאה גוברת של משאבים לאומיים, פיתוח תפיסות, גיבוש רגולציה ומימוש נהלים,[21] הרחבת שיתופי פעולה ועוד. גם ביתר גופי הביטחון והמודיעין של ישראל תופס תחום הסייבר מעמד בכיר יותר ויותר כחלק ממילוי המשימות של כל אחד מארגונים אלה.[22] מצב דומה קיים גם בגופים במערכת האזרחית בישראל, ובכללם משרדי ממשלה, רשויות סטטוטוריות, גופים עסקיים ותאגידים ציבוריים.

הסייבר כמרכיב במכלול

ההבנה שהסייבר עתיד להימצא "כמעט בכול", תוך מחיקת גבולות מסורתיים בין האזרחי לביטחוני, הפרטי לקולקטיבי, הלאומי לבין־לאומי, המוחשי לווירטואלי, יוצרת אתגר למערכות המדינה המבקשות לשמר רמת תפקוד גבוהה, ולכן דורשת היערכות מיוחדת. בהקשר זה יש לציין לחיוב את מערך הסייבר הלאומי המתרחב בשנים האחרונות, שמטרתו היא לסייע במימוש חזון הסייבר הלאומי וליצור מערכת סביבתית שתתמוך בהמשך השגשוג וההובלה של ישראל בתחום זה.

עם זאת, ההשפעה העמוקה של הסייבר ניכרת גם בתחומים נוספים הנוגעים לעולמות הביטחון, המודיעין והצבא, בדגש על סוגיות הפעלת הכוח וניהול המערכה. הסתכלות בפרספקטיבה היסטורית רחבה דיה תעלה עוד מספר מהפכות טכנולוגיות, תשתיתיות ותפיסתיות שהיו בעלות אפקט עמוק וממושך והשפיעו על פניו של שדה הקרב ועל עולם המודיעין והביטחון הלאומי בכלל. כך בתחומי האמל"ח, התקשורת, התעבורה, עיבוד הנתונים, אמצעי האיסוף ועוד. ההשפעה העמוקה של הסייבר על התפיסות והפרקטיקות שנהגו עד להופעתו במלוא עוצמתו, אינה שונה במהותה מזו של הופעת חומר הנפץ, הטלגרף, הרכבת, מנוע הבעירה הפנימית או המטוס.

---

18 החלטת ממשלה 3611 מיום 7 באוגוסט 2011: "קידום היכולת הלאומית במרחב הקיברנטי".

19 החלטת ממשלה 2444 מיום 15 בפברואר 2015: "קידום ההיערכות הלאומית להגנה בסייבר".

20 גבי סיבוני ומאיר אלרן, "משמעויותיה של הקמת זרוע הסייבר בצה"ל", **מבט על**, גיליון 719, 7 ביולי 2015; יוסי מלמן, "חור ברשת: החלטת הרמטכ"ל לא להקים זרוע סייבר בצה"ל היא טעות", **מעריב־סופהשבוע**, 7 בינואר 2017; יוסי הטוני, "הדחייה בהקמת זרוע הסייבר – צעד מוצדק", **אנשים ומחשבים**, 1 בינואר 2017.

21 החלטת ממשלה 2443 מיום 15 בפברואר 2015: "קידום אסדרה לאומית והובלה ממשלתית בהגנה בסייבר".

22 איתמר אייכנר, "חשיפה: יחידת הסייבר של השב"כ מבפנים", **YNET**, 18 בינואר 2017; אלירן רובין, "כך פספסתם הזדמנות להיות האקרים במוסד", **The Marker**, 15 במאי 2016; יוסי יהושוע וראובן וייס, "גיקים באפלה", **ידיעות אחרונות**, המוסף לשבת, 10 בפברואר 2017.

בהסתכלות לאחור, לבטח מתחילת המאה העשרים, ניתן לקבוע כי הצלחה של צבאות ומערכות מודיעיניות נבעה בדרך כלל משילוב מושכל של התחומים החדשים אל תוך המארג הקיים, הן באמצעים, הן בשיטות והן בתפיסות, אגב ביצוע השינויים וההתאמות הנדרשים. כך בשימוש ברכבות בשינוע גייסות וציוד בין חזיתות ואליהן; בשילוב הטנקים בקרבות האש והתנועה ביבשה; ברתימת מהפכת המחשוב לאיסוף המודיעיני; או בבניית יכולת הפצצה בעומק באמצעות כוח אווירי. בה בשעה, חלק מהכישלונות הביטחוניים היו תוצאה (גם אם לא בלעדית) של נהייה חזקה מדי או הישענות בלתי מבוקרת על "החדש והמבטיח" (אוונגרד) – ע"ע המפקדים שמאחורי "מסכי הפלזמה". בכך אין כדי לרמוז להלך רוח ריאקציוני או שמרני המבקש להתנער מהקִדמה וההתפתחויות הבלתי נמנעות, אלא לכוונה למקם את השינוי או המהפכה בתוך הֶקשר רחב.

בנקודה זו אני מבקש לטעון כי דווקא על רקע התבססותו המבורכת של הסייבר במערכות השונות בשנים האחרונות (ועוד זרועו נטויה), חובה עלינו, כלקח היסטורי, לשמור על פרספקטיבה רחבה בכול אחד מתחומי הביטחון והמודיעין, ולזכור כי הסייבר הוא כלי ותווך נוספים, גם אם רבי היקף ומשמעות, המצטרפים אל המכלול הקיים והמתפתח תמידית. עם כל החשיבות והמאפיינים הייחודיים של הסייבר, ובראשם ההשפעה הרוחבית והעמוקה שלו על מערכות רבות בהתבסס על הקישוריות (inter-connectivity) הרבה, אל לנו לראותו כשדה מובחן ונפרד, באופן שיבוא לידי ביטוי בתהליכי המטה, בניין הכוח והפעלתו.

הסייבר מתאפיין בהיותו תחום מולטי־דיסציפלינרי ולא חד־ממדי; הוא אינו "עוד טכנולוגיה", אלא תופעה בעלת ממדים סוציולוגיים, משפטיים, כלכליים ועוד.[23] הרב־גוניות של הסייבר מחזקת את הצורך לשלבו בתוך המרקם המערכתי הכולל ורב־הפנים ולא לבודד אותו.

סוגיית ההרתעה בסייבר משקפת גם היא את הצורך בהסתכלות מערכתית כוללת. בעיית הייחוס (אף כי יש להניח שעוצמתה תפחת בחלוף הזמן ועם השכלול בכלי ההגנה) יוצרת קושי בזיהוי מושא ההרתעה ובהתאמת כלי ההרתעה להישג הנדרש.[24] התשובה המתבקשת לבעיה זו היא שההרתעה בסייבר אינה חייבת להישאר בתחומי הסייבר ("תגובה מְסוגה"), אלא יכולה וצריכה לשלב גם אלמנטים כלכליים, נורמות בין־לאומיות ועוד. פרופ' ניי טוען[25] שהרתעה אפקטיבית בסייבר לא יכולה להיות גנרית, אלא מצריכה התאמה פרטנית ביחס לאיום ספציפי. תובנה

23 Isaac Ben Israel, "Cyber: Not What You Thought!", *CyberTech 2017*, January 2017, pp. 7-8.

24 Joseph Nye, "Can Cyber Warfare Be Deterred?", *Project Syndicate*, December 10, 2015.

25 שם.

זו משתלבת היטב בצורך לקיים הערכת מצב כוללת, אשר תאפשר שימוש במגוון כלי מדיניות מדיסציפלינות שונות.

יש הרואים בסייבר מרכיב עוצמה בעל פוטנציאל כה רב (בין אם בתוך תחום הסייבר או, כאמור, מחוצה לו), עד כי ניתן להשתמש בו לצורך הקרנת העוצמה הלאומית כלפי חוץ, באופן אנלוגי להקרנת עוצמה לאומית (לרוב מעצמתית) באמצעות כוח ימי השולט בימים, במְצרים, בסחר ימי, בזירת הקרב הימי ועוד.[26] ייתכן שאנלוגיה זו מתאימה יותר לראשית ימי הסייבר, בהם טכנולוגיה מתקדמת בתחום זה נראתה כנחלת מעצמות־העל בלבד; עתה היא נראית מעט מרחיקת לכת, לאור הפרוליפרציה המואצת של טכנולוגיות סייבר הגנתיות ואחרות. יחד עם זאת, יש באנלוגיה זו כדי להציף שוב את הפוטנציאל הרב הטמון בסייבר, החורג הרבה מעבר לתחומו הצר, באופן המחייב הסתכלות גלובלית ובין־תחומית.

באשר לתהליכי קבלת ההחלטות, המטה הכללי ברמה הצבאית והמטה לביטחון לאומי ברמה הלאומית הם הגופים האמונים על ההסתכלות הכוללת – ראיית השלם – ושקלול כלל התשומות להערכת מצב אינטגרטיבית, כבסיס לקבלת החלטות על בניין הכוח והפעלתו. הסייבר מהווה את אחת התשומות בלבד, תהיה חשיבותה ככול שתהיה, אך לא התשומה היחידה. כך ניתן גם לפרש את אמירתו של ראש הממשלה על "אירועים גדולים שמחייבים תגובה נגד התקיפה והתוקף".[27] לא נכון לקיים "הערכת מצב סייבר" שלא כמרכיב/תשומה בהערכת המצב הכוללת, כשם שלא נכון לקיים "מל"ל סייבר" מחוץ לגוף־העל המתכלל האמון על הערכת המצב הלאומית – המל"ל.[28] כשם שלא יעלה על הדעת לקיים "מל"ל חיל אוויר" או "מטכ"ל שריון", לצד גורמי ההנהגה והפיקוד העליונים, כך יש להיזהר מנטייה לניהול "מערכה לאומית בסייבר" כמערכה בפני עצמה, ויש לראות בה תמיד חלק מהמערכה הרחבה של צה"ל או של כל גוף אחר, כל אחד בהתאם למשימותיו וסמכויותיו, וכולם יחד כחלקים משלימים בתצרף הביטחון הלאומי.

נכון ומקובל להקים גופי מטה נושאיים, הן בצה"ל והן מחוצה לו, אך אלה אמורים להיות כפופים לתהליך הערכת המצב וקבלת ההחלטות במטכ"ל ובקבינט, הניזונים משלל מקורות, על פי כללי עבודת המטה המוגדרים בפקודות המטכ"ל, בחוק המל"ל ובנהלים נוספים. מצב שבו גוף נושאי האמון על תחום מסוים – חשוב

---

26 Joseph Nye, *Cyber Power* (Cambridge, MA: Belfer Center for Science and International Affairs, 2010), p. 4.

27 קאהאן, "נתניהו בנאום בסייברטק: 'אנחנו רוצים להוביל את תחום הסייבר בעולם'".

28 ראו חוק המטה לביטחון לאומי התשס"ח־2008, בו נקבע כי "המטה לביטחון לאומי ישמש גוף המטה לראש הממשלה ולממשלה בענייני החוץ והביטחון של מדינת ישראל" (סעיף 1 ב'), ויכין בין היתר "הערכה שנתית ורב־שנתית של המצב המדיני־ביטחוני" (סעיף 2 א' 6).

ככול שיהיה – משמש בעת ובעונה אחת גם כמתַכלל־על, משקף סתירה פנימית ומעלה את הסיכון להטיה ולשיבוש בהליכי עבודת המטה וקבלת ההחלטות.

מטה ההסברה הלאומי, שהוקם אחרי מלחמת לבנון השנייה ב־2006 לנוכח הבנת חשיבותו של הפן הציבורי־תקשורתי במערכה, ממוקם במשרד ראש הממשלה, אך אין לו כל יומרה להחליף את מי מגופי הביצוע בתחום ההסברה והדוברות (משרד החוץ, דובר צה"ל וכדומה); המטה ללוט"ר הוקם בשנות התשעים של המאה הקודמת במשרד ראש הממשלה, ובהמשך הוכפף למל"ל, ומטרתו היא לתאם ולשפר את התיאום הבין־ארגוני בתחום הלוחמה בטרור אל מול האיום הגובר, אך לא לשמש כמחליף של מי מגופי הביטחון והמודיעין. תוצרי העבודה ומיקומם הביורוקרטי של שני הגופים הללו משקפים את ההבנה כי קיים צורך לחזק את עבודת המטה ולהגביר את הקשב לתחומים אלה ברמה הלאומית. עם זאת, אין הם מהווים גופים אוטונומיים או "סמכות אחרונה" בתחומם, אלא מספקים תשומה חשובה לתהליך האינטגרציה וקבלת ההחלטות המסתיים ומוכרע בדרג המדיני, על כלל תהליכי המטה הגנריים המשרתים אותו.

גם בקרב גופי הביטחון יש להקפיד על הכנסת "תשומת הסייבר" למערבל של תהליך הערכת המצב הכולל, לצד נתונים ותשומות אחרים – "מסורתיים" וחדשים ככול שיצוצו – לצורך ביצוע הערכת מצב שלמה. אם אכן "הסייבר הוא זירה חדשה בשדה הקרב"[29], כפי שאמר ראש הממשלה, הרי שיש לנהל את "קרב הסייבר" כעוד אחד מהקרבות המרכיבים יחדיו את המערכה, ולא כמערכה בפני עצמה. ראש ה־CIA לשעבר, דיוויד פטראוס, התבטא לאחרונה בהקשר זה: "תקיפות הסייבר הביאו כבר להטלת סנקציות, וברור מאליו שאנחנו נכנסים לעולם שהתגובות בו יהיו תלויות בחומרת הפגיעה. אני מאמין שפגיעה משמעותית במערכות חשמל לזמן ארוך תגרור תגובה משמעותית. התגובה יכולה להיות בסייבר, בצעדים דיפלומטיים, בסנקציות או אפילו תגובה חמורה יותר".[30] הסייבר משתלב, משפיע ומושפע מהתחומים הנוספים. במצב זה של זיקות גומלין והשפעות הדדיות, בידוד הסייבר יהווה כשל מתודולוגי.

מיקום הסייבר בהקשר הנכון מתחייב גם מהבחינה הארגונית. מאחר שאנו מצויים בשלב מוקדם יחסית של מהפכת הסייבר והשתלבותו בכול תחומי החיים ובמערכות הביטחוניות, איננו יכולים לדעת היום אל נכון מה תהייה הצורה האופטימלית לארגן את תחום הסייבר במערכות השונות בעתיד. באופן טבעי, כל ארגון עובר שינויים במשך הזמן, ומבנים ארגוניים מעוצבים ונזנחים בהתאם לניסיון המצטבר. ואכן, בשנים האחרונות הגופים השונים קובעים ומעדכנים את היערכותם תוך כדי תנועה, בתהליך חיובי ומתבקש של למידה, הסתגלות והתאמה.

29 קאהאן, "נתניהו בנאום בסייברטק: 'אנחנו רוצים להוביל את תחום הסייבר בעולם'".
30 אורבך, "חדשנות ההאקרים מתפתחת כמו הסייבר".

לנוכח הקושי האובייקטיבי והסובייקטיבי גם יחד לחזות את האופן שבו יתקבע חלקו היחסי של הסייבר במכלול, חובה לשמור על גמישות ועל ראייה מכלילה. ההתנסות המעשית, הפקת הלקחים ותהליכי הלמידה, בד בבד עם דוגמאות מהעבר ותובנות היסטוריות, יובילו אותנו, כמקֻוה, לנקודה האופטימלית. נוכל לתרום לכך מבחינה תהליכית וארגונית אם נבטיח איזון ראוי וחשיפה להשפעות גומלין בין המרכיבים השונים, אשר יוכלו לתרום בתורם גם לעיצוב המהותי של תחום הסייבר עצמו.

סיכום

הסייבר חולל וימשיך לחולל תמורה עמוקה בתחומי הביטחון, הצבא והמודיעין. כל זאת, כחלק מהתפשטותו במערכות חיינו ומהמהפכה החברתית והכלכלית האדירה שהוא מביא עמו, שיש האומרים כי היא דומה למהפכות החקלאות, הדפוס והתעשייה ששינו את פני האנושות. הסייבר הוא גורם המערער מערכות מסורתיות, והוא משתלב במגמות עכשוויות הקוראות תגר על הסדר הליברלי־דמוקרטי הקיים שהתבסס לאחר מלחמת העולם השנייה. הסייבר גם משנה את חלוקת הכוח ואת מקורות הסמכות, כפי שהכרנו אותם עד היום, לרבות מושגים של ריבונות, טריטוריה, מונופול על אמצעי האלימות ושינוי ביכולת להפעיל כוח. כפי שכבר הוכח, ובהתאם להערכות הרווחות, הסייבר נושא בחובו פוטנציאל אדיר, לטוב ולרע, ועל כן יצריך השקעת משאבים גדולה, ניהוג וניהול בכול גופי המדינה, ברמה הלאומית ובזירה הבין־לאומית. מכאן שהתנופה בפיתוח ובהשקעה בסייבר על כל היבטיו מחויבת המציאות, וטוב שבישראל, על כל גופיה הביטחוניים והאזרחיים, עולה המוּדעות לתחום זה.

עם זאת, דווקא על רקע התבססותו המהירה של תחום הסייבר בתודעה ובמערכות השונות, חובה עלינו לשמור על פרספקטיבה כוללת, שבה הסייבר הוא מרכיב חשוב ומתרחב, אבל לא מובחן או עומד בפני עצמו. דברים אלה מקבלים משנה תוקף בכול הנוגע לסוגיית הפעלת הכוח לנוכח איומים וזירות שונות. בראייה לאומית ומערכתית, התבוננות צרה מדי עלולה להביא לכשלים בהערכת המצב, לעיוותים ארגוניים, ובסופו של דבר אף לטעויות בקבלת ההחלטות. המערכה לעולם תהייה תוצר של תשומות מתחומים שונים, היוצרים יחד אפקט סינרגטי מנצח. הטיה לתחום מסוים, חשוב ככול שיהיה, מגדילה את הסיכוי לכשלים קוגניטיביים ולהחלטות שגויות.

כשם שהמלחמה מורכבת מסדרה של מאמצים וקרבות במקומות שונים ומסוגים שונים – ים, יבשה, אוויר, חלל, אזורים גיאוגרפיים שונים, מהלכים מדיניים, היבטים כלכליים, שיקולים טכנולוגיים ולוגיסטיים ועוד – שרק השפעתם המצטברת מביאה לתוצאה הסופית, כך גם עולם הסייבר משתלב במערכה הכוללת בתחום

המדיני־ביטחוני. אל לנו לנסות לקיים "מערכה בסייבר" כתחום מובחן המנוהל בפני עצמו, אלא לפעול להכללתו המושכלת, במלוא כובד משקלו, של "הסייבר במערכה", על כל פניה.

לאחרונה נוכחנו כי התקיפה על שרתי המפלגה הדמוקרטית בארצות הברית במהלך מערכת הבחירות לנשיאות בסתיו 2016 גררה תגובה (לפחות בחלקה) במישור הדיפלומטי והציבורי. המסקנה היא שהקינטי, הקיברנטי, מאמץ התודעה והתקשורת, התמרון, הדיפלומטיה, העוצמה הכלכלית והלוגיסטיקה – כל אלה ואחרים חוברים יחד ליצירת השלם. בהתאם לכך, עלינו להתייחס לכול אחד מחלקיו.

"המאמץ החסר" – שילוב הממד "הרך" במעשה הצבאי בישראל

דודי סימן טוב ודוד שטרנברג

מאמר זה בוחן מהו הרעיון של "לוחמה רכה" וכיצד ניתן ונכון לשלבו במסגרת מאמצי המערכה של צה"ל. בתוך כך, הוא מונה את החסמים הארגוניים, התפיסתיים והתרבותיים הניצבים בפני מהלך כזה ואת השינויים הנדרשים בעקרונות הפעולה של צה"ל: מיסוד קווי המאמץ "הרכים"; שינוי תפיסת הזמן של הפעולה הצבאית; מעבר ממבנה של מערכות סגורות למערכות פתוחות ומקושרות עם הסביבה האזרחית; בניית מנגנון מודיעין ומבצעים תומך. במונחים מעשיים, הדרך לקידום "הלוחמה הרכה" בצה"ל דורשת התמקדות בארבעה יתרונות יחסיים: חדשנות טכנולוגית; מערכת היחסים עם ארצות הברית; ניצול יתרונות הקוטן במערכת הביטחון; הישענות על רכישת ידע אזרחי דרך מערך המילואים, או יצירת מנגנונים אחרים לזרימת ידע ויכולות "רכות" למערכת הביטחונית.

מילות מפתח: לוחמה רכה, השפעה, תודעה, אסטרטגיית צה"ל, לוחמה משפטית, לוחמה כלכלית, לוחמה פסיכולוגית.

מבוא

בספרו **התועלת שבכוח** קבע הגנרל הבריטי רופרט סמית' כי השינוי בשדה המערכה הנוכחי הפך את המלחמה "בין אנשים" למלחמה "בתוך אנשים".[1] כוונתו הייתה שבעולם המודרני, בו יש חשיבות הולכת וגוברת לתקשורת, לדעת קהל ולשיקולים גלובליים, מושגים כמו "הכרעה" ו"ניצחון" תלויים בתפיסה ובהכרה של קהלים

1 רופרט סמית', **התועלת שבכוח – אמנות המלחמה בעולם המודרני**, מערכות, תל אביב, 2013.

דודי סימן טוב הוא חוקר במכון למחקרי ביטחון לאומי. דוד שטרנברג הוא בוגר התוכנית למדיניות ציבורית באוניברסיטת הרווארד.

רלוונטיים שאינם בהכרח חלק ישיר מהמערכה הצבאית. זאת, בניגוד למלחמות הקלאסיות שבהן המנצח היה זה שהכריע בשדה הקרב.

ברקע לשינוי זה ניצבות שתי מגמות־על המאפיינות את הסביבה הגלובלית המודרנית: הראשונה היא מהפכת המידע, המביאה לעלייה בקצב שינוי המידע, זמינותו ודפוסי צריכתו, ויותר מכך – גורמת לכך שהוא חוצה גבולות וריבונות. במסגרת זו, החיבוריות התודעתית והרשתיות הטכנולוגית מעצימות את יכולת הפרט, ובה בשעה מגבירות את הפגיעות המערכתית של מדינות ושל חברות. המגמה השנייה כוללת את התמורות שחלו בשדה המדיני־דיפלומטי: בשני העשורים האחרונים אנו עדים לגידול במשקלם של ארגונים לא ממשלתיים, לעלייה במשקלה של דעת הקהל בקבלת החלטות ביטחוניות, בהיווצרות ערכאות בין־לאומיות, בהסתעפות דיני הלחימה, ובשיח ער על זכויות האדם כקריטריון מרכזי לבחינת הלגיטימיות והחוקיות של הפעלת כוח צבאי.

שתי המשמעויות המרכזיות של תמורות אלו הן: קושי של המדינות לשלוט במידע ולעצב את הנרטיב והלגיטימציה של הפעולה, והחלשת האפקטיביות של אסטרטגיות עוצמה קטלניות במטרה להשיג יעדים אסטרטגיים. יצוין, כי הפעלת עוצמה קטלנית גבתה במקרים רבים מחירים מדיניים מצבאות מדינתיים, עד שרבים העדיפו לא לעשות בה שימוש.

על רקע זה, ולצד הרצון לפתח כלי השפעה שאינם צבאיים אלא רעיוניים, תרבותיים וכלכליים, עלתה במערב הגישה של "עוצמה רכה", כבסיס למדיניות הביטחון והחוץ של מעצמות ומדינות רבות. המושג "עוצמה רכה" (Soft Power) מתייחס ליכולת לשכנע אחרים לפעול כרצונך מבלי להפעיל כוח פיזי, והתבסס על שימוש במשאבים ויכולות שאינם קטלניים, כגון: משאבים כלכליים, משפטיים, דיפלומטיים, תרבותיים ואידיאולוגיים.[2]

הבעיה של "העוצמה הרכה" היא הצורך שלה להתמודד גם עם השתנות האויב וגם עם השתנות סביבת הלחימה. בעימותים של העת הנוכחית נוצר חוסר איזון בין צבאות מדינתיים מסורתיים ובין שחקנים חדשים עִמם הם צריכים להתמודד. בעוד שהראשונים מאופיינים בקשיחות ביורוקרטית, תפיסתית ומשאבית, האחרונים מגלמים מרכיבים של גמישות, חדשנות ויכולת הסתגלות המאפשרות ניצול מיטבי של השדה האסטרטגי החדש. עם זאת, הדיכוטומיה בין השניים אינה גזרת גורל, ובמספר צבאות מדינתיים ניכרת חתירה לסַגל תפיסה ויכולת פעולה בתחום של הפעלת כלים לא קטלניים, שלצורך מאמר זה נכנה אותם כלים "רכים".

מאמר זה בוחן מהו הרעיון של "לוחמה רכה" וכיצד ניתן ונכון לשלבו במסגרת מאמצי המערכה הצבאיים. הפרק הראשון במאמר הוא תיאורטי ובוחן את מקור המושג ואת מרכיביו וכן מביא מספר דוגמאות לגורמים שאימצו את ההיגיון "הרך"

2 Joseph Nye, "Soft Power", *Foreign Policy*, no. 80 (1990), pp. 153-171.

כחלק מרכזי באסטרטגיית הפעולה שלהם. הפרק השני מציג את זווית הראייה הישראלית בכול הקשור לצורך לאמץ את ההיגיון של מבצעי השפעה. הפרק השלישי מנתח את האתגרים והחסמים העומדים בפני הטמעת ההיגיון "הרך" בתפיסת ההפעלה של צה"ל. הפרק האחרון מציג את עקרונות המענה לאתגרים אלה ומביא המלצות לכיווני פעולה עתידיים.

יצוין כי המאמצים "הרכים" אינם נחלת הצבא לבדו וכי גופים ממשלתיים אחרים בישראל נדרשים לעשות בהם שימוש כחלק מתפיסת הביטחון ומדיניות החוץ של ישראל, בין השאר כדי להקל על פעולתו של צה"ל. מאמר זה לא יעסוק במכלול המאמץ הלאומי, הגם שהצבא נדרש לפתח יחסי גומלין הדוקים בכדי למצות את הפוטנציאל המשותף של המגזר הביטחוני, הממשלתי והפרטי לקידום האינטרסים של ישראל.

רקע תיאורטי

שורשי הפעולה "הרכה" מעוגנים בתוך מאגר היסטורי מוכר של תפיסות וכלים מדיניים ואסטרטגיים. ואולם, הניסיון לפתח כלים "רכים" קונה משנה חשיבות בשל השינוי העמוק באופי העימותים ואתגרים חדשים שנוצרו לצבאות בעידן המודרני. כך, למשל, קשה לתקוף ארגוני טרור וגרילה המסתתרים בתוך אוכלוסייה אזרחית, גם בשל הקושי המודיעיני והמבצעי לאתרם ולפגוע בהם, אך בעיקר בשל החשש מפגיעה באזרחים בלתי מעורבים, שעלולה להביא ל"ניצחון פירוס". דוגמה אחרת היא הצורך בהתמודדות עם התעצמות ארגוני טרור וארגונים סמי־צבאיים. מדובר במהלכים המתבצעים בשגרה, וכרוכים לעיתים קרובות בהפעלת לחץ מדיני או כלכלי. דוגמה נוספת עולה מעולם הסייבר המתפתח, שם הלוחמה אינה מכוונת בהכרח לרובד התשתית הפיזיקלית (מערכות הנשק של האויב), אלא גם לאפקטים ברובד של "המרחב הסמנטי", הכוללים הונאה, בלבול, שיתוק, מבוכה וכיוצא באלה. כדי להשפיע על מרחב סמנטי זה יש צורך בכלי תכנון ופעולה חדשים.[3]

מקורות המחשבה הצבאית בנושא "הלוחמה הרכה" נטועים היטב בעשייה הביטחונית־צבאית מזה מספר רב של עשורים. כך, למשל, לארצות הברית יש היסטוריה נכבדה של מבצעי חתרנות ופעולות ללוחמה פסיכולוגית וכלכלית. ברמה האסטרטגית, פרדיגמת "הכוח הרך" של ארצות הברית, הקיימת מאז שנות השבעים של המאה העשרים, מצאה את גלגולה גם לדוקטרינות מודרניות, כגון "העוצמה החכמה" של ממשל אובמה, שהובילה להפעלת סנקציות פיננסיות אפקטיביות על איראן ועל רוסיה.

---

3 M.C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007).

לאור זאת הקימה ארצות הברית פיקוד ייעודי לסייבר ויצרה דיסציפלינה וארגון תומך למבצעי מידע.[4] היכולת לשפוט את יעילותה של פעילות זו הינה מוגבלת לפי שעה, אולם בכול מקרה היא משולבת במאמצים הצבאיים המרכזיים של ארצות הברית. יתר על כן, נראה כי חשיבותם של מאמצים אלה צפויה אף לגבור, נוכח ההערכה כי מקומה של "הלוחמה הרכה" עתיד לגדול בשנים הקרובות.[5]

המושג "עוצמה רכה" (Soft Power), כפי שהוגדר בראשית הדרך, מתייחס כאמור ליכולת לשכנע אחרים לפעול כרצונך מבלי להפעיל נגדם כוח פיזי. הכוונה המקורית שעמדה בבסיס המושג הייתה הנחלת רעיונות ותפיסות דמוקרטיות וליברליות באמצעות כלים תרבותיים וכלכליים (ברוח "תיאוריית קשתות הזהב" של תומס פרידמן, שטען כי הגלובליזציה מונעת אלימות בין מדינות).[6] כוונה מקורית זו משתקפת עד היום בחשש של יריבי ארצות הברית במזרח מפני מה שהם רואים כאיום המרכזי ליציבותם. כך, למשל, רוסיה, סין ואיראן חוששות מיכולותיה הכלכליות, התקשורתיות והתרבותיות של וושינגטון "לתדלק" כוחות פנימיים ולהביא ל"מהפכות קטיפה".

מחקר שנערך לאחרונה על ידי מכון RAND עבור הצבא האמריקאי גורס כי החלוקה הדיכוטומית המסורתית בין "רך" ל"קשה" דורשת עידון וחידוד. המחקר מציע המשגה של תווך ביניים בין הפעלת כוחות צבאיים ובין השפעת כוחות "רכים" בלבד, המבוססת על דיפלומטיה חיובית ובעלת ראייה ארוכת טווח. מרחב חדש זה מכונה במחקר Power to Coerce (P2C), והוא כולל שלל צעדים, כגון סנקציות כלכליות, סיוע צבאי לכוחות אופוזיציה, לוחמה קיברנטית התקפית, לוחמה פסיכולוגית ועוד.[7]

לצד ארצות הברית, התפיסות "הרכות" דומיננטיות בהוויה התרבותית־פילוסופית ובדוקטרינות הצבאיות של מדינות נוספות, ובהן רוסיה וסין. במקרה הרוסי, הביטוי לכך בשנים האחרונות הוא בהפעלה מופגנת של "לוחמה היברידית", כפי שהיא מכונה במערב, במספר זירות, כגון בפלישה לחצי האי קרים, בסכסוך הרחב יותר עם אוקראינה ובהתערבות הצבאית הרוסית בסוריה. שיטת פעולה רוסית זו נדונה רבות בחוגים ביטחוניים ואקדמיים, והמאפיין הבולט בה הוא שילוב של הפעלת כוח צבאי עם חתרנות פוליטית, כפייה כלכלית וקמפיינים תודעתיים. במסגרת זו בולטות פעולות סייבר התקפיות (למשל, בגיאורגיה, באסטוניה, באוקראינה, ולאחרונה ייתכן גם בארצות הברית), שימוש בכוחות שאינם מזוהים עם המדינה

4 "Information Operations", *Joint Publication*, 3-13, 2016.

5 *The DCDC Global Strategic Trends Programme 2007-2036*, http://www.cuttingthroughthematrix.com/articles/strat_trends_23jan07.pdf.

6 תומס פרידמן, **הלקסוס ועץ הזית**, הד ארצי, אור יהודה, 2000.

7 David Gompert and Hans Binnendijk, *The Power to Coerce* (RAND Corporation, 2016).

(למשל, בהסתננות כוחות לפעולות גרילה באוקראינה), מתקפות דיסאינפורמציה ותעמולה נרחבות (למשל, בגיאורגיה ובאוקראינה) ועוד.

המחשה של קווי פעולה אלה ניכרת במהלכי הלחימה הרוסית בסוריה. מהלכים אלה כוללים פעולות מתמשכות ובהן: זריעת בלבול לגבי יעדי המעורבות (למשל, בהצהרה על לחימה נגד טרור או בהכרזות על "נסיגה" ו"תום הלחימה", תוך קניית מראית עין של לגיטימציה בין־לאומית); קיום ערוצי הידברות עם ארצות הברית והפסקות אש הומניטריות; הפעלת כוחות לא סדירים (באמצעות איראן וחזבאללה); העצמה של דימוי הכוח בסדרת פעולות מתוקשרות, ובהן שיגורים ממפציצים ושיגורים של טילי שיוט משטח רוסיה, תמרוני שיט ימיים, פריסת מערכות הגנה אווירית ארוכות טווח ויצירת מצגי דיסאינפורמציה לגבי הישגים.

למרות שקיים ויכוח האם אכן מדובר במודל רוסי חדש,[8] אין להתעלם מהמסד התרבותי־צבאי התומך באפשרות זאת, ובכלל זה תפיסות כגון "השליטה הרפלקסיבית", הרואה מקום מרכזי בפעולה הצבאית ליצירת מהלכים פרובוקטיביים המכוונים להפיק תגובות מתוכננות מצד היריב ותיעולו למרחבים אותם מבקש המתכנן האסטרטגי להשיג.[9] ביטויים מפורשים לדוקטרינה הרוסית ניתן למצוא במאמר משנת 2013 של רמטכ"ל צבא רוסיה, גרסימוב,[10] כשברקע לו ניתן לראות תהליכים מסבירים אפשריים, ובהם פנייה של הרוסים לעשות שימוש בשיטות המחפות על חולשותיהם בתחום הקונבנציונלי ועל אורך הנשימה המוגבל שלהם במשאבים. בנוסף לכך, רוסיה למדה בעשור האחרון היטב את משמעות הפעלתה של "עוצמה רכה" על ידי המערב, וכן רכשה ניסיון בעימותים שלה־עצמה, למשל באסטוניה. כל אלה מחזקים את הרושם כי מדובר בשינוי תפיסתי ומעשי רחב בדוקטרינת הלחימה הרוסית.

שילוב של הפעלת כוח "רך" ניתן לראות גם בתפיסת "שלוש הלוחמות" הסינית. תפיסה זו גורסת את הצורך בהפעלה משולבת של שלושה סוגי לוחמה – יחסי ציבור, לוחמה פסיכולוגית ולוחמה משפטית – לשם השגת מטרות אסטרטגיות. מדריך רשמי בנושא זה פורסם על ידי המטכ"ל הסיני עוד ב־2005, וסימני הטמעתה של התפיסה בולטים מאוד בכתבים צבאיים סיניים מרכזיים מהשנים האחרונות. ניתן ללמוד מכתבים אלה כי "שלוש הלוחמות" נועדו הן לפעולה בשגרה והן לפעולה בעת מלחמה, וכוללות שורת תכליות, בהן: שליטה בדעת הקהל, פגיעה בנחישות היריב ובתקשורת האסטרטגית שלו, יצירת סכסוך בקרב האויב והטלת

8 Michael Kofman and Matthew Rojansky, "A Closer Look at Russia's 'Hybrid War'", *Kennan Cable Wilson Center*, no.7, April 2015.

9 דימה אדמסקי, "אומנות אופרטיבית קיברנטית: מבט מזווית לימודי האסטרטגיה ומפרספקטיבה השוואית", **עשתונות**, מס' 11, המכללה לביטחון לאומי, אוגוסט 2015.

10 מקס פישר, "חוקי המלחמה החדשים של רוסיה", **הארץ** (תרגום מ"ניו יורק טיימס"), 28 ביולי 2016, http://www.haaretz.co.il/news/world/europe/.premium-1.3020671

מגבלות משפטיות עליו. עדות לקו פעולה זה ניתן לראות בצורה ברורה בפרשת הסכסוך עם הפיליפינים בים סין הדרומי, שם הפעילו הסינים מערכת של כלים דיפלומטיים, משפטיים ותודעתיים במאבקם על הלגיטימציה לשליטה בנכסים טריטוריאליים המצויים בסכסוך.[11]

גם צבאות באזור המזרח התיכון מיישמים תפיסה זו. רמז לכך ניתן לראות בהצהרת איראן מ־2013 על הקמת מפקדות ל"מלחמה רכה", שיתכן והביאה לשינוי מבנה במטה הכללי של צבא איראן, וזאת מתוך הכרה כי העולם הווירטואלי הוא "כלי הנשק החשוב, המורכב והנוח ביותר של האויב".[12] ההיערכות האיראנית ללוחמה "רכה", לפחות כפי שהיא עולה מהודעה זאת, הינה הגנתית, כתגובה לעוצמה המערבית, אך היא מלמדת על היערכות ארגונית צבאית בתחום חדש זה, שייתכן וכוללת גם נגזרות התקפיות.

ראינו, אפוא, כי השינויים הגוברים בסביבה האסטרטגית בשנים האחרונות הביאו להופעתה של הגדרה חדשה למושג "עוצמה רכה" בשיח האסטרטגי והאופרטיבי, שהינה אמנם המשך למצבים מוכרים, אך בעוצמה, גיוון ותחכום חדשים. אלה שמים את הדגש על "מהפכת המידע" והסייבר, על יעדים כלכליים ועל הפעלת מִבצעי מידע. לפי הגישה החדשה, מאמץ מוצלח של "לוחמה רכה" משלב אמצעים גלויים וחשאיים וממנף עליונות מודיעינית והיכרות עמוקה עם היריב כדי למקד מאמצי משנה בתחום התודעה ודעת הקהל ולשבש ולהשפיע על קבלת החלטות, וכול זאת לצד מהלכים צבאיים קינטיים מסורתיים.

הזווית הישראלית

ההיסטוריה הצבאית הישראלית רוויה בצלקות מניסיונות להשפיע באופן "רך" – למשל, אלה שנסובו סביב מבצע "שלום הגליל" ב־1982 ומערכת היחסים המורכבת עם הפלגים הנוצריים בלבנון. ההכרזות של ראשי צה"ל בתחילת האינתיפאדה השנייה, לפיה ניצחון הוא בבחינת "צריבת התודעה" של הפלסטינים כי הם מפסידים במערכה, וכן המהלכים שאמורים היו ליצור אפקט תודעתי במלחמת לבנון השנייה (כמו הנפת הדגל בבינת ג'בייל), יצרו ספקנות בצה"ל כלפי צעדים "רכים" ותודעתיים.

למרות זאת, התבוננות על העשור האחרון מראה כי ישראל וצה"ל חוו סדרה של התנסויות משמעותיות, המעלות את הצורך ברתימת יכולות "רכות" למעשה הצבאי. בין התנסויות אלו היו אירועים שהמחישו את המחיר הנגזר מהזנחת הממד

---

11 Elsa Kania, "The PLA's Latest Strategic Thinking on the Three Warfares", *Jamestown Foundation China Brief*, 16, no. 13, August 22, 2016.

12 תרגום הידיעה באתר של טל פבל, 26 באוקטובר 2013: "איראן מקימה מפקדות אזוריות ל'מלחמה רכה'", http://middleeasternet.com/

"הרך", לעומת השימוש הענֵף שעושה בו היריב. דוגמאות לכך הם משט הספינה "מרמרה" לרצועת עזה ודו"ח גולדסטון, ומנגד אירועים המלמדים על ההזדמנות הטמונה בכלים "רכים", כגון מבצעי דיפלומטיה מוצלחים שנעשו כלפי אירן.

ישראל מתמודדת עם סדרת אתגרים ייחודיים, המעלים את הצורך בכלי פעולה "רכים". ראשית, צה"ל הוא בין הצבאות המערביים היחידים שהתנסה בהפעלת תמרון משמעותי ואש בסביבה אורבנית מורכבת. זאת, מול אויבים אסימטריים שהסתתרו בקרב האוכלוסייה ואיימו באש על העורף ועל תשתיות אסטרטגיות בישראל. צה"ל נאלץ להתמודד עם אוכלוסייה גדולה של בלתי מעורבים ועם אתגרים שביקשו לקזז מהיתרונות האסטרטגיים שלו, כגון לחימה בתווך התת־קרקעי. המשמעות של כל אלה היא קושי מהותי להציג הכרעה ברורה במונחים קינטיים, במיוחד כאשר נזק אגבי הנגרם שלא במתכוון מנוצל על ידי היריב וממונף להגברת הלחץ על חופש הפעולה המבצעי והמדיני של ישראל ולקיזוז הישגיה.

שנית, ההיקף הרחב של הזירות הגיאוגרפיות ואופי האתגרים עמם ישראל נאלצת להתמודד מביאים לכך שחסרים לה משאבים מספיקים כדי לתמוך במערכות צבאיות נרחבות ובזירות שונות. כלים "רכים" יכולים לסייע במקרה כזה על ידי העצמת הישגים פיזיים, מהלכי הונאה (לטובת כילוי משאבי היריב או יצירת הפתעה שתקל על מימוש התוכנית האופרטיבית), שליטה במרחב ההסלמה ויצירת חלופות מבצעיות אטרקטיביות.

שלישית, מכיוון שישראל מתמודדת גם עם סיכונים מתהווים וגם עם סיכונים המרוחקים מגבולותיה, החלופות "הרכות" עשויות לתת מענה לסוגיות של מניעה ועיצוב. מדובר, למשל, בצמצום הפצה ופיתוח של אמצעי לחימה בטרם יגיעו לשדה הקרב, וזאת באמצעים מדיניים וכלכליים, או לחילופין, בעיצוב של תנאי מערכה, כגון יחס של אוכלוסייה באזורים מסוימים כלפי ישראל.

כפי שהוצג קודם לכן, המֻשגת העוצמה "הרכה" שאובה מניסיון, תנאים ויכולות של עולם מעצמתי, כמו הפעלת סנקציות, תזוזת כוחות צבא במטרה לאותת על כוונות, או שימוש מסיבי בכלי תקשורת. אולם, למרות השונות בין נקודת המבט של מעצמה לזו של מדינה, דומה שגם מדינות כמו ישראל יכולות לאמץ מודל היברידי העושה שימוש בכלים ממוקדים יותר ומותאמים למידותיה, כגון כלי לוחמה תקשורתית, פיננסית או קיברנטית, שתכליתם העצמת המרכיב הצבאי ויצירת תנאים מיטביים למימושו.

בשיח הצבאי קנתה לה זה מכבר ההכרה בחשיבותו של מרחב פעולה זה. מסמך **אסטרטגיית צה"ל** משנת 2015 קובע כי פעולת האויב "בממדים שאינם צבאיים־קינטיים [...] מתוך מרחבי אוכלוסייה, או במרחב התת־קרקעי והתקשורתי", מאפשרת לו לראות את עצמו "מצליח לקזז בכך מהישגי ישראל במערכה". המסמך

גורס כי הפתרון לבעיה זו טמון "בגישה רב־ממדית, תוך כדי מערכה ובין מערכות, הכוללת מתקפות סייבר ומאמץ תודעתי ומשפטי".[13]

גם השיח האקדמי בישראל מעלה את הטענה לפיה אין די במאמצים צבאיים מסורתיים וכי על ישראל לפתח גישה רב־תחומית ולשלב באסטרטגיה האזורית שלה מרכיבים מדיניים, תקשורתיים, כלכליים, משפטיים, סייבר, סיוע הומניטרי לבעלי ברית ועוד.[14] יש בכך המשך ישיר להבחנות של "פורום הרצליה" משנת 2010, שקרא להציב את איום "המלחמה הרכה" בסדר עדיפות גבוה ולהיערך אליה באמצעות הקמת גופים ממלכתיים שזו תהיה משימתם העיקרית. אמנם, המסמך של הפורום האמור דן בהיבטים הגנתיים בלבד שעל ישראל לאמץ מול "הלוחמה הרכה" (המדינית או המשפטית) שמופעלת נגדה, אולם דומה כי כיום ראוי לבחון גם אימוץ של הגיונות התקפיים לצד אלה ההגנתיים.[15]

אתגרי "הלוחמה הרכה" בתפיסת ההפעלה של צה"ל ובתוכניותיו המבצעיות

אין די בהבנה אסטרטגית כדי להביא לשינוי אופרטיבי בעשייה הצה"לית. שינוי כזה מחייב בירור ופיתוח בקרב אלה הנוגעים בעומק המעשה הצבאי ותרגום העקרונות ה"רכים" לפרקטיקות מבצעיות, הן ארגונית והן מקצועית. מספר חסמים משמעותיים ניצבים בפני שילוב של היגיון וכלים "רכים" בחשיבה הצה"לית בכלל ובתוכניות האופרטיביות במיוחד.

קבוצת החסמים הראשונה נוגעת לעניינים תפיסתיים־ארגוניים. בראש אלה עומד התפר בין פעולות של "לוחמה רכה" ובין המאמץ המבצעי. המפקד המבצעי, שבדרך כלל חסר ניסיון בתחומים שאינם קשורים בהפעלת כוחות צבאיים, מתקשה לשזור את הגיונות "הלוחמה הרכה" בתכנוניו המבצעיים, במיוחד כאשר במרבית המקרים, הגדרת ההישג הנדרש והקריטריונים להערכת ההצלחה במאמץ "רך" אינם חדים וברורים. מכאן נוצר עיוות בראיית חשיבותה של "הלוחמה הרכה" במנגנון קבלת ההחלטות. זאת ועוד, פעולה בעלת אופי קינטי (למשל, סיכול ממוקד או הרס מנהרה) תיחשב לרוב משמעותית ואטרקטיבית יותר מאשר פעולה "רכה", שקשה יותר להעריך את האפקט שלה. משמעות הדברים היא שבמרבית המקרים, הנכונות הבסיסית של מפקדים להקדיש קשב לפעולה "רכה", להקצות לה משאבי

13 **אסטרטגיית צה"ל**, *לשכת הרמטכ"ל, אתר צה"ל*, 2015, עמ' 12.

14 אודי דקל ועומר עינב, "הצורך בעדכון תפיסת הביטחון הלאומית – אסטרטגיית השפעה רב־תחומית", **מבט על**, 13 באוגוסט 2015.

15 שמואל בר, שמואל בכר ורחל מכטיגר, **המלחמה הרכה נגד ישראל – מניעים ומנופים להתמודדות עם הבעיה**, נייר עבודה לקראת פורום הרצליה, 2010, http://www.herzliyaconference.org/_Uploads/3036HateHeb.pdf.

איסוף, להסתכן בחשיפת מידע רגיש, להשקיע שעות אדם או להעדיף את הסיכון שבה על פני חלופה קינטית, תהיה נמוכה.

יתר על כן, מכיוון שחלק גדול מהתחומים "הרכים" הוא נחלתם של מומחים דיסציפלינריים, נוצרת הטיה ארגונית נוספת. הדובר, הפרקליט הצבאי, גורם קשרי החוץ, הקמ"ן או גורמי הלוחמה הפסיכולוגית מהווים לרוב "קופסה שחורה" הנספחת לחשיבה האופרטיבית אותה מוביל המפקד. כל עוד מדובר באוסף דיסציפלינות הנתפס כנבדל מהמקצוע הצבאי, ברירת המחדל היא להטיל את התכנון "הרך" על גורמי המקצוע כמאמץ צדדי. זאת ועוד, גופי הפעולה המקצועיים העוסקים ב"לוחמה רכה" פחות נכונים לוותר על המונופול המקצועי שלהם ולייצר שלם ארגוני שגורע, לכאורה, ממעמדם. לבסוף, על העניין התפיסתי־ארגוני מעיב גם היעדרו בצבאות של "בית גידול" טבעי לאנשי תוכן בעולמות "הרכים". מִשְׁפָּך, המחשבה, הניסיון ודרך הפעולה, ההולכים ומשתכללים בסביבה האזרחית, גדֵלים באופן מבודד, חלש ואנכרוניסטי בחממה הצבאית.

קבוצת החסמים השנייה, והמשמעותית יותר, נוגעת לתרבות הצבאית־ישראלית ולאתוס הצה"לי.[16] תרבות זו מעריכה, בראש ובראשונה, פעולה על פני דיבור, תוצאות והישגים מוחשיים על פני תהליכים, ומכאן שאופק הזמן שלה הוא לרוב קצר. עדות לכך ניתן למצוא בדיאלקטיקה הבעייתית אותה צה"ל מנהל מזה עשור ויותר עם בית המדרש של החשיבה המערכתית סביב קיומו או אי־קיומו של "אינטלקטואליזם" במערכת הצבאית וסביב חשיבותו.[17] מכאן, אך טבעי הוא שהַתרבות הצבאית הבסיסית מסויגת מכול השקעה ברכיבים גלויים, בתעמולה, במעשים ציבוריים או במבצעים שקשה יותר להעריך את תרומתם ואת הצלחתם. נראה שבתרבות האסטרטגית הישראלית, קידום מהלך עמוק ומקיף, שאינו רק פעולה של יחידות ייעודיות או השקעה במאמצים מרוכזים, אלא מאמץ כולל ומשולב, דורש תחושת משבר עמוקה, שאינה קיימת כיום.

כיווני חשיבה עתידיים לצה"ל

השינויים הנדרשים בעקרונות ההפעלה של צה"ל צריכים להתקיים בשלושה ממדים. השינוי הראשון צריך להתרחש במרחבי הפעולה של הצבא. כאן מתחייב פיתוח אפיקי פעולה "רכים" חדשים, כחלק מהיכולת הצבאית הבסיסית. השינוי השני נדרש בממד הזמן של הפעולה הצבאית. ממד זה לא צריך להיות מחולק יותר ל"מלחמה" ול"התכוננות למלחמה", אלא לבוא לפני המערכה ולהימשך

16 דימה אדמסקי, **תרבות אסטרטגית וחדשנות צבאית**, מערכות, תל אביב, 2010, עמ' 184.

17 דודי קמחי, "המהפכה האינטלקטואלית בצה"ל", **מערכות**, גיליון 464, דצמבר 2015, עמ' 14–25.

גם אחריה. השינוי השלישי נדרש להיעשות במבנה המערכת הצבאית – ממבנה פעולה שנע ממערכות סגורות, היררכיות והומוגניות, למערכות פתוחות ורשתיות, המתקשרות עם הסביבה האזרחית.

ההתקדמות בכיוון הרצוי והנדרש עוברת דרך בניית תפיסת הפעלה שתתמקד בארבעה יתרונות יחסיים של צה"ל ומדינת ישראל: חדשנות טכנולוגית; הישענות על מערכת היחסים המיוחדת עם ארצות הברית; ניצול יתרונות לקוטן של מערכת הביטחון, קהילת המודיעין והמערכת הממשלתית; הישענות על רכישת ידע אזרחי – דרך מערך המילואים ודרך פיתוח שיטות התקשרות גמישות לגופים רלוונטיים עם המגזר האזרחי.

מרחבי הפעולה – מהקינטי ל"רך"

הפעילות התודעתית, הדיפלומטית, הכלכלית והמשפטית בזירה "הרכה" כוללת באופן טבעי מעגל רחב של שותפים במישור הלאומי והבין־לאומי. במקרה הישראלי, קהילה זו מונה משרדי ממשלה שונים, כמו גם את קהילת המודיעין, מערכי הסברה וגורמים פרטיים. גופים אלה הם בעלי הידע המקצועי, הניסיון ורשת הַקשרים הנדרשים להניע פעולות. הם גם פועלים במרחבים בין־לאומיים מול גופים מדינתיים, ארגונים בין־לאומיים, החברה האזרחית, מוסדות ומנגנוני תקשורת וכלכלה ועוד. אל מול אלה עולה השאלה מה תפקידו הייחודי של צה"ל בהקשר של פיתוח ידע וכלים אופרטיביים "רכים".

לצה"ל שתי עוצמות מרכזיות מעבר להיבטים צבאיים־ביטחוניים:

- הוא יכול להיות מקור מרכזי לנתונים, למידע ולידע הנחוצים לקיום כל מערכה "רכה". הדבר נובע ראשית מהיותו יעד מרכזי של היריב (למשל, לקעקוע הלגיטימציה, חופש הפעולה שלו ודימויו בישראל ובעולם), ושנית – מהיותו מחולל ראשי של אירועים בכל זירות הלחימה.
- הוא מחזיק זרועות ביצוע חזקות ורלוונטיות רבות – מודיעיניות, קשרי חוץ צבאיים, תקשורתיות, משפטיות ועוד. מנגנונים אלה עשויים להיות מסד לפעולה בקנה מידה לאומי.

יחד עם זאת יצוין כי דווקא בתחומי הפעולה ה"רכים" ישנה הובלה של גופים אזרחיים – ממשלתיים ופרטיים – וצה"ל נדרש להתחבר אליהם בדרכים שונות ויצירתיות. לפיכך, על צה"ל ליצור יכולות חדשות או להגביר יכולות קיימות כדי לקדם את אפשרויותיו בממד "הרך", וזאת בתחומים הבאים:

- **לוחמה תודעתית־תקשורתית־פסיכולוגית** – סוג לוחמה זה מנצל את המישור התקשורתי הפומבי, החשאי והבין־לאומי להעברת מסרים שנועדו להשפיע על קהלי יעד נרחבים מובחנים, ובהם ציבורים של האויב, הזירה האזורית, הזירה הבין־לאומית והזירה הפנימית. זאת, לשם קידום מגוון רחב של תכליות, ובכללן

הרתעה, החלשה, הונאה, התססה ועוד. לוחמה כזאת יכולה להיות ממוקדת באדם מסוים, בארגון, בקבוצות חברתיות, בציבורים ובקהילות.

- **לוחמה מדינית־משפטית** – זו מושתתת על המערכת הדיפלומטית הבין־לאומית וגיוסה באמצעות מסגרות של שיתוף פעולה דיפלומטי, צבאי וחוקי, במישורים הבין־לאומי, הפומבי והחשאי. לוחמה משפטית יכולה להיות בממד הגנתי, במטרה להתמודד עם תביעות משפטיות נגד ישראל, אולם עליה להיות גם בעלת פוטנציאל למאמץ התקפי, שיתבע משפטית גורמים הפועלים נגד ישראל או ישדל מוסדות בין־לאומיים לפעול נגדם.[18]
- **לוחמה כלכלית** – לוחמה מסוג זה מושתתת על פגיעה במשאביו ובנכסיו של האויב במטרה להחליש הן את בניין כוחו, הן את יכולת הפעולה שלו והן את נכונותו להמשיך ולפעול. בהקשר זה מוכרות היטב בשנים האחרונות בארץ ובעולם פעולות מגוונות שנעשו אל מול מדינות סוררות (איראן, סוריה, צפון קוריאה ועוד), כמו גם אל מול ארגוני טרור שונים ובראשם המדינה האסלאמית.
- **לוחמת סייבר** – לוחמה זו מאופיינת על ידי ניצול התווך הקיברנטי להישגים שונים: קינטיים, תודעתיים, איסופיים ועוד. המרחב הקיברנטי מזַמן בחובו הזדמנויות "רכות" למימוש "לוחמה רכה" ויכול להיות משולב בממדים אחרים, כמו תקשורת או כלכלה, או להופיע בנפרד (לצורך הדיון, נוציא את תחום התקיפה הקיברנטית על אמל"ח או תשתיות אל מחוץ לגבולותיו של מאמר זה).

זמן הפעולה – ממאמץ עָצים למאמץ מתמשך

עניין שני הדורש שינוי הינו תפיסת הזמן. העשייה הצבאית צריכה לעבור מחלוקה לשני מצבי היסוד הקלאסיים – "מלחמה" ו"התכוננות למלחמה" – למבט רחב ומורכב יותר של ממד הזמן, הכולל את:[19]

- **המאמץ המתמשך** כולל את הפעולות המתקיימות בשגרה, שמטרתן היא מניעת העימות. מאמץ זה מכוון לתכליות כגון הרתעה, עיכוב תהליכי הסלמה, יצירת השפעה ומינופה, העצמת נכסיות או שינוי מציאות בעייתית.
- **המאמץ המעצב** פועל גם הוא בזמן שגרה, ותכליתו היא לצפות את פני העימותים העתידיים, ליצור את התנאים המיטביים לניצחון בהם ולעצב את שדה המערכה העתידי. דוגמה לכך היא קידום הבנות בין־לאומיות לאפשרות של הפעלת חימוש מסוים או של תצורת לחימה, החיוניים למאמצי התמרון הצה"ליים.

---

18 נועם נוימן, "לוחמת משפט – איומים והזדמנויות", **מערכות**, גיליון 449, יוני 2013, עמ' 22.

19 גור ליש, "עיקרי תפיסת הביטחון של המל"ל", **עשתונות**, מס' 10, המכללה לביטחון לאומי, יולי 2015, עמ' 41.

- **המאמץ המקדים** חותר למַקסם את התנאים לניצחון במערכה כפי שהם מופיעים בתוכנית האופרטיבית הקיימת. כך, למשל, ניתן לכלול במאמץ המקדים היבטי הונאה אופרטיבית, הנבנים לאורך זמן ומחלישים את תפיסת האויב לגבי יכולת או כוונת פעולה מסוימת של צה"ל.
- **המאמץ המלווה והאוחר** כולל את הפעולות המלוות את המערכה ואת תוצאותיה. משעה שהמערכה נכנסת לפעולה, התוכניות המבצעיות משתנות. תגובת האויב יוצרת מציאות חדשה הדורשת תכנון חוזר, מגלה עובדות חדשות ויוצרת תוצאות שלא נצפו מראש. לפיכך, נדרשת יכולת תגובה גם בהיבטים "רכים". דוגמאות לתגובות כאלו הן השפעה על תודעת האויב לגבי הישגיו, סיוע "רך" לעיצוב מנגנוני סיום יעילים, וריכוך השפעות שליליות על חופש הפעולה העתידי של צה"ל. גם לאחר המלחמה עולות לדיון סוגיות מדיניות ומשפטיות, שעליהן נדרשת "הלוחמה הרכה" להגיב או ליזום.

מבנה המערכת ויחסה לסביבה: ממערכת סגורה לפתוחה

ההתארגנות הנדרשת לצורך הפעלת מאמצים "רכים" במעשה הצבאי מאתגרת את צה"ל, שנבנה בעבר לפעילות קטלנית, בעוד שהמאמצים "הרכים" שעשה תוחמו לפעולה התקשורתית של דובר צה"ל, שהדגש העיקרי בעשייתו היה מול הציבור הישראלי. כאמור, צה"ל אינו מהווה בית גידול טבעי למאמצים "רכים", משום שהאנשים שחונכו לפעול בשדות אלה, ופועלים בהם, אינם קציני צבא טיפוסיים. לפיכך, המסקנה המתבקשת היא שמבנה הפעולה בממדים "הרכים" צריך להיות פתוח ושטוח – כזה שאינו פועל בין קצות הפירמידות הביורוקרטיות, אלא מתקיים כמרחב משותף.

משמעות הדברים היא שכדי ליצור מאמצים "רכים" משמעותיים, צה"ל זקוק למודל פעולה אחר. מודל כזה יצטרך ליצור רשת פעולה יומיומית בשלושה מעגלים: במעגל הצבאי, בו נדרשת יכולת לשלב בין מפקדות הכוח הרלוונטיות וגורמי הביצוע; אל מול רשויות המדינה, על ידי תיאום, סנכרון ורתימה של שותפים מרכזיים במשרדי הממשלה וברשויות האחרות; קידום שיתוף פעולה, דיאלוג ויכולת הפעלת שותפים, כגון מכוני מחקר, מלכ"רים, ספקי שירותים, מדינות מפתח, גורמי או"ם, ארגונים אזרחיים וארגונים לא ממשלתיים.[20] רשת זו אמורה לספק לצבא ולשותפיו שני "גשרים" מהותיים: הראשון, יכולת לפעפע ידע רלוונטי מהזירה הביטחונית לטובת ייזום, תכנון וקידום פעילויות חשיפה והשפעה באמצעות פלטפורמות גלויות; השני, כזה שמאפשר הבנה של הזירה האזרחית, על ההזדמנויות והסיכונים הגלומים בה והיכולות המקצועיות והניסיון שרכשו העוסקים בה, לשם עיצוב פעולה צבאית מיטבית.

20 **אתגר הדה־לגיטימציה של ישראל – יצירת חומת אש מדינית**, מכון ראות, ינואר 2010.

עקרונות לעיצוב תפיסת "הלוחמה הרכה" בצה"ל

ניתן לאפיין ארבעה יתרונות מרכזיים שיש לישראל, אותם נכון למנף כחלק מקידום תפיסת "הלוחמה הרכה" בצה"ל:

- **יכולות טכנולוגיות גבוהות**, במיוחד בעולם מערכות המידע, המדיה החדשה והרשתות החברתיות. דווקא בעולם כזה, על מורכבותו, משקלה הסגולי של ישראל והחדשנות הטבעית שלה יכולים לאפשר לה לפתח קווי מאמץ חדשים שיתמכו בפעולותיה הצבאיות. בעניין זה ניתן ליצור הקבלה בין המובילות העולמית שקנו להן יחידות צבא ישראליות, כגון 8200, בתחומי איסוף המודיעין, ובין יכולת עתידית לגבש מענה הולם בעולם ההשפעה (בלשונו של צבי האוזר, מזכיר הממשלה לשעבר: "יחידה 8300").[21] יתרה מכך, המדיום המתעצם של הרשתות החברתיות יוצר אפשרויות ודרכי השפעה שלא היו קיימות בעבר, ומכאן – פוטנציאל רב לפעולות בממדים "רכים".
- **מערכת היחסים המיוחדת עם ארצות הברית** – זו עשויה לאפשר לישראל יכולת השפעה עקיפה על המערכה ועל הסביבה הבין־לאומית דרך שיתופי פעולה בתחום "הלוחמה הרכה" וחיבור יכולות משלימות.
- **היתרון לקוטן** – יתרון מרכזי של המערכת הביטחונית הישראלית הוא ביכולתה ליצור אינטגרציות קלות ומהירות בין סוכנויות לאומיות שונות. אמנם, גם בישראל קיימים מתחים תרבותיים־פוליטיים וטכניים בין הארגונים, המקשים על כך, אך דומה שמשקלו הדומיננטי של צה"ל, יחד עם הזריזות והגמישות היחסיות שלו, יכולים לאפשר לישראל פריון גבוה יותר בתחום "הלוחמה הרכה" מאשר למקבילותיה. כך, למשל, חיבור ארגוני (ולאו דווקא יצירת גוף אחד) ויצירת תפיסת הפעלה משותפת בין כלל הגופים העוסקים בנושא זה בצה"ל או בקהילת המודיעין הישראלית יכולים להוות "מכפיל כוח" לקידום מעשי של "הלוחמה הרכה".
- **אינטגרציה עם העולם האזרחי** – מרבית מומחי התוכן האזרחיים נגישים לצבא דרך מערך המילואים. לפיכך, מיצוי היחסים עם הסביבה האזרחית בישראל נותן סיכוי גבוה יותר ליצירת חיבוריות מוצלחת של ידע מקצועי אזרחי עם ידע צבאי. החיבור בין המגזר הביטחוני ובין המגזר האזרחי־הפרטי יבטיח מיצוי טוב יותר של הידע האזרחי בעשייה הצבאית ויביא להפריה של הידע הצבאי ברעיונות, בכלים ובשיטות פעולה המפותחים במגזר האזרחי והממשלתי.

פעולה מערכתית אפקטיבית בכלים "רכים" מחייבת שני תנאי יסוד:

- **תפיסה מבצעית** – על המאמץ "הרך" להיות מחובר לרעיון המבצעי. מאמץ כזה לא יכול להצטרף בשלב מאוחר יותר, מאחר והוא נגזר לרוב מהיבטים אסטרטגיים

21 צבי האוזר, "יחידה 8300", **YNET**, 5 באפריל 2016.

הקשורים לנרטיב של המעשה הצבאי, למנגנוני הסיום שלו, למשאבים הלאומיים ולהבנת כוונות ויכולות האויב.

- **מודיעין תומך ומאפשר** – מימוש מאמצים "רכים" דורש פיתוח מודיעין תומך מסוג חדש, הבונה הבנה מערכתית על יעדים ונושאים חדשים: חברתיים, תרבותיים, כלכליים, תקשורתיים, ארגוניים ואישיים. הוא גם דורש הקצאה של חלק מהיכולות האופרטיביות של אמ"ן לטובתו (כגון איסוף מיוחד וקשרי חוץ חשאיים). בנוסף לכך, קיים צורך לפתח גישה ומנגנונים שיאפשרו פרסום מהיר ושימוש אופרטיבי במידע ובידע מודיעיניים. זאת, נוכח הנטייה הטבעית של ארגוני מודיעין, הפועלים בחשאיות ושומרים על מקורותיהם, לא לפרסמם.

סיכום

מאמר זה בחן את הרעיון של "לוחמה רכה" מנקודת מבט תיאורטית, צבאית ואסטרטגית, וכיצד הוא בא לידי ביטוי בעשייה האסטרטגית והאופרטיבית של מעצמות מרכזיות בעידן המידע והסייבר. במסגרת זו נבחנו הזווית הישראלית והאתגרים הייחודיים עמם מתמודד צה"ל, וכן הדרכים שבהן ניתן ונכון לשלב את המאמצים "הרכים" במסגרת מאמצי המערכה שלו.

בתוך כך נבחנו החסמים הארגוניים, התפיסתיים והתרבותיים העומדים בפני אימוץ גישה "רכה" באסטרטגיה של צה"ל ובתפיסת ההפעלה שלו, והוצגו השינויים העיקריים הנדרשים בעקרונות הפעולה הצבאיים במטרה להגביר את משקלו של הממד "הרך" בין שאר ממדי הפעולה של צה"ל. במסגרת זו שם המאמר דגש על מיסוד שיטות וכלים "רכים" שיופעלו לצד המאמצים הקטלניים, ובראשם לוחמה פסיכולוגית־תודעתית, לוחמה כלכלית ולוחמה משפטית; על שינוי תפיסת הזמן של הפעולה הצבאית; על מעבר ממבנה של מערכות סגורות למערכות פתוחות ומקושרות עם הסביבה האזרחית; ועל בניית מנגנון מודיעין ומבצעים תומך. במונחים מעשיים, הדרך לקידום הממד "הרך" בעשייה הצה"לית דורשת התמקדות בארבעה יתרונות יחסיים של צה"ל ומדינת ישראל: חדשנות טכנולוגית, מערכת היחסים עם ארצות הברית, ניצול יתרונות הקוטן במערכת הביטחון, והישענות על רכישת ידע אזרחי דרך מערך המילואים, או יצירת מנגנונים אחרים לזרימת ידע ויכולות "רכות".

איומים קיברנטיים על תהליכים דמוקרטיים

דודי סימן טוב, גבי סיבוני, גבריאל אראל

המעורבות המיוחסת לרוסיה בבחירות לנשיאות בארצות הברית ובצרפת מעלה שאלות באשר לצורך וליכולת של מדינות דמוקרטיות להגן על תהליך הבחירות שלהן. מאמר זה מצביע על החשיבות שיש לייחס לבחירות במדינה דמוקרטית כתשתית וכתהליך קריטיים ומציג את האיומים עליהן הנובעים מהתפתחויות קיברנטיות ותרבותיות. המאמר מציף את התובנה לפיה השימוש הנרחב ברשתות חברתיות ובערוצי תקשורת ישירים מאפשר לגורמים זרים להשפיע בצורה משמעותית על ההליך הדמוקרטי, וזאת לא על ידי השבתה של מערכות ההצבעה אלא באמצעות השפעה זרה על השיח הפוליטי. הדבר מהווה אתגר חדש למדינות דמוקרטיות, המחייב התארגנות וחשיבה חדשות.

מילות מפתח: בחירות, סייבר, הגנת סייבר, תשתית קריטית, רשתות חברתיות, חתרנות מדינית.

מבוא

ערכי היסוד של מדינות דמוקרטיות הם חירות, שוויון, השתתפות וזכויות אזרח. אחד המאפיינים המרכזיים של המדינה הדמוקרטית הינו קיומן של בחירות כלליות, חופשיות, חוזרות ונשנות במרווחי זמן הנקבעים בחוק. בחירות הן שיאו של ההליך הדמוקרטי ומהוות מרכיב מרכזי בבניית אמון הציבור במדינה ואמון האזרחים במוסדותיה.

בשנים האחרונות אנו עדים לניסיונות התערבות חיצונית ולפגיעה בהליכי הבחירות במדינות דמוקרטיות רבות בעולם באמצעות תקיפות קיברנטיות. את האיומים הקיברנטיים על הליך הבחירות במדינות דמוקרטיות ניתן לסווג לאיומים שמטרתם לשבש את ההליך עצמו באמצעות כלים טכנולוגיים שנועדו לפגוע

דודי סימן טוב הינו חוקר במכון למחקרי ביטחון לאומי. ד"ר גבי סיבוני הינו חוקר בכיר במכון למחקרי ביטחון לאומי ועומד בראש תוכנית ביטחון הסייבר שם. גבריאל אראל היא עוזרת מחקר במכון למחקרי ביטחון לאומי. המחברים מבקשים להודות לאל"ם ג' על תרומתו למאמר זה.

במערכות מידע ובמערכות הסיקור וההצבעה, ולאיומים מהותיים על המוסדות הדמוקרטיים בכללותם באמצעות פגיעה בשמם הטוב ובאמון הציבור בהם. בעוד שהאיום הראשון מוכר ומדינות נערכות היטב מולו, האיום השני, המופשט יותר, הינו חדש ומחייב חשיבה הולמת.

דו"ח של קהילת המודיעין האמריקאית, שהוגש לנשיא ארצות הברית בינואר 2017, מעריך כי רוסיה ניהלה קמפיין נרחב לערעור סיכוייה של המועמדת לנשיאות הילרי קלינטון ולקידום המועמד דונלד טראמפ, ועשתה זאת הן על ידי תקיפות סייבר חשאיות והן באמצעות מאמצי השפעה גלויים. להערכת קהילת המודיעין של ארצות הברית, גורמי סייבר של רוסיה פרצו למחשבי המפלגה הדמוקרטית האמריקאית כבר ביולי 2015 ועשו שימוש במידע שנאסף במסגרת פריצה זו.[1] מקרה זה מצטרף לדיווחים נוספים על חשד לחדירות קיברנטיות של רוסיה לגופי ממשל גם באירופה ולשיבוש מערכות בחירות שם.[2] רוסיה נחשדה בניסיון כושל להתערבות בבחירות לנשיאות בצרפת, שמטרתה הייתה לשבש את בחירתו של עמנואל מקרון, וזאת באמצעות פרסום ברשת של מידע שנגנב ממטה הבחירות שלו (שייתכן וחלקו היה מזויף).[3]

מקרה אחר של התערבות במערכות בחירות זרות הוא חשיפה של גורמים שעמדו מאחורי הטיית הבחירות במספר מדינות בדרום אמריקה. אנדֶרֶס סֶפּוּלְוֶדָה, שעמד לדבריו בראש צוות האקרים שפעלו בעשור האחרון במטרה להטות תוצאות בחירות במספר מדינות בדרום אמריקה, כמו למשל במקסיקו, סיפר כי צוות ההאקרים שלו התקין תוכנות ריגול במחשבים של יריבים, גנב אסטרטגיות של מערכות בחירות ותמרן את המדיה החברתית במטרה ליצור אווירה של התלהבות או של בוז ולגלוג.[4]

השוני בין שני המקרים שתוארו לעיל הינו ברור: מאחורי המקרה הראשון עומדת כנראה מעצמה, שניסתה להשפיע על תוצאות הבחירות לנשיאות בארצות הברית ובצרפת. במקרה השני עומדים גורמים פרטיים, שגויסו למהלך על ידי יריבים פוליטיים.

---

1 "Background to Assessing Russian Activities and Intentions in Recent US Elections: The Analytic Process and Cyber Incident Attribution", *Intelligence Community Assessment, ODNI*, January 6, 2017.

2 "לא רק ארה"ב: רוסיה מתערבת גם בבחירות באירופה", **YNET**, 10 בדצמבר 2016.

3 Eric Auchard and Felix Bate, "French Candidate Macron Claims Massive Hack as Emails Leaked", *Reuters*, May 6, 2017.

4 Jordan Robertson, Michael Riley, Andrew Willis, "How to Hack an Election", *Bloomberg*, March 31, 2016, https://www.bloomberg.com/features/2016-how-to-hack-an-election.

מאמר זה מתמקד באיום של התערבות מהסוג הראשון, אותו אנו מגדירים "חתרנות מדינית קיברנטית אסטרטגית". המאמר עוסק בנקודות התורפה של תהליך הבחירות במדינה דמוקרטית, המאפשרות התערבות זרה, ועושה זאת באמצעות ניתוח מרכיבי התהליך וחולשותיהם מול אפשרות של פגיעה קיברנטית. כמו כן מציג המאמר את הבחירות כתהליך קריטי ששיבוש שלו עלול לערער את היציבות הדמוקרטית ואת אמון הציבור במוסדות הדמוקרטיים ככלל.

בין תשתיות קריטיות לתהליכים קיברנטיים חיוניים

בראייה האמריקאית, תשתיות קריטיות הינן מערכות חיוניות, המהוות את הבסיס של החברה האמריקאית ותומכות בביטחונה, בכלכלתה ובמערכות הבריאות שלה. הגדרה זו מתייחסת ל־16 קטגוריות של מערכות וסוכנויות, שהממשל האמריקאי אחראי להבטיח את ביטחונן הפיזי והקיברנטי. קטגוריות אלו הן: התעשייה הכימית, הכוללת תעשיות רוקחות, כימיקלים לחקלאות וכימיקלים מיוחדים; תשתיות מסחר; תקשורת; תעשיות ייצור, כגון תעשיית המתכת; אנרגיה; סכרים; תעשיות ביטחוניות לייצור ותחזוקה של אמצעי לחימה ומערכות צבאיות; שירותי חירום; תשתיות פיננסיות; מגזר המזון והחקלאות; תשתיות ממשל; מערכות בריאות; מערכות מידע; תשתיות גרעיניות; תשתיות תחבורה; תשתיות מים.[5]

בישראל, תשתית חיונית להגנה קיברנטית היא תשתית ציבורית, בין אם היא נמצאת בבעלות ממשלתית ובין אם היא בבעלות פרטית, וההגנה עליה מחייבת הגנה פיזית, אבטחת מידע ואבטחת מערכות המחשוב שלה.[6] תשתית מוגדרת כקריטית כאשר פגיעה בה עלולה להוביל לנזק כלכלי־חברתי שיש לו פוטנציאל לערעור היציבות הכלכלית, החברתית או הביטחונית של המדינה. תשתיות קריטיות מורכבות לרוב משלושה מאפיינים עיקריים: משקלן הסמלי; התלות התפקודית של המדינה בהן, שכתוצאה ממנה כל פגיעה בהן עלולה להוביל לנזק מתמשך ולפגיעה בחיי אדם או לנזק כלכלי משמעותי; קשרי הגומלין עם תשתיות אחרות.[7] אל התשתיות הקריטיות המסורתיות (מערכות החשמל, התקשורת, הרכבות, צנרת הולכת המים והדלק, התעופה וכדומה) התווספו בשנים האחרונות תשתיות נוספות, כגון ספקיות אינטרנט וחלק מהמגזר הפיננסי. ההחלטה אם להגדיר תשתית כקריטית היא של ועדה בראשות ראש מטה הסייבר הלאומי וכרוכה בשינויי חקיקה. תשתית קריטית חייבת לעמוד ברגולציה לאומית להגנה בסייבר.

---

5 ההגדרה נלקחה מתוך אתר המשרד להגנת המולדת של ארצות הברית: https://www.dhs.gov/critical-infrastructure-sectors.

6 רועי גולדשמידט, "המרחב הקיברנטי וההגנה על תשתיות קריטיות", *הכנסת, מרכז המחקר והמידע*, 2013.

7 ליאור טבנסקי, "הגנה על תשתיות קריטיות מפני איום קיברנטי", **צבא ואסטרטגיה**, כרך 3 גיליון 2, נובמבר 2011.

הרגולציה נעשית באמצעות הנחיית גופי התשתית הקריטית על ידי ה"רשות לאבטחת מידע" (רא"ם) בשב"כ. חלק נרחב מסמכות ההנחיה של רא"ם נמצא בתהליך מעבָר ל"רשות הלאומית להגנת סייבר". שירותים ציבוריים אחרים, כגון חינוך, בריאות ומשפט, וגם מערכת הבחירות בישראל, אינם מוגדרים כתשתיות קריטיות המחויבות בהכוונה והנחיה של הגופים המוסמכים. יחד עם זאת, ועדת הבחירות המרכזית בישראל מקבלת הנחיה מרשות הסייבר הלאומית.

בארצות הברית נשמעו באחרונה קריאות לעדכון ההגדרה של תשתיות קריטיות ודרישות לכלול בתוכה גופים ותהליכים נוספים הפגיעים לתקיפות קיברנטיות, כגון מערכות בחירות וגופי מחקר ואקדמיה. קריאות אלו מתבססות על העלייה החדה בשימוש באינטרנט ובמערכות ממוחשבות בכלל המגזרים (ציבורי, עסקי, ממשלתי, פרטי, תשתיות ואקדמיה), המחייבת הגדרה מחדש של התשתיות. זאת, לאור הרגישות של מערכות מורכבות המבוססות על תשתיות תקשורת ומחשוב, ובכלל זה מערכות בחירות.[8]

תהליך בחירות דמוקרטי – איומים קיברנטיים מרכזיים

בחירות דמוקרטיות הן תהליך המורכב משחקנים וגורמים שונים המקיימים ביניהם קשרי גומלין. הפעילות והשימוש של מרכיבי ההליך הדמוקרטי בתשתיות, ובתוכן של המרחב הקיברנטי, הולכים ומתרחבים. תהליך הבחירות מורכב מארבעה שלבים המתקיימים בסדר כרונולוגי, כמפורט בתרשים שלהלן. האיומים הקיברנטיים המשמעותיים בתהליך זה, מפניהם נדרשות מדינות להתגונן, הינם תקיפה קיברנטית של תשתיות, איסוף מידע על מועמדים ומפלגות וניסיונות השפעה על התודעה.

חולשות סייבר בתהליך הבחירות

שיבוש, שינוי וזיוף מאגרי מידע

משרדי הממשלה האחראים על רישום ושמירת הפרטים האישיים של אזרחי המדינה ושל החברות עוברים בעשורים האחרונים תהליכים מתקדמים של דיגיטציה וייעול באמצעות הטמעה של מערכות ממוחשבות לרישום וניהול רשומות. מערכות אלו פגיעות מאוד למתקפות קיברנטיות, כפי שהוכח במדינות ג'ורג'יה, אילינוי ואריזונה בארצות הברית.[9] בשלוש מדינות אלו התגלו חדירות קיברנטיות למאגרי הרשומות, אשר עלולות היו להביא לגניבה או לחשיפת פרטיהם של כ־21 מיליון

8 Kate O'Keeffe and Byron Tau, "U.S. Considers Classifying Election System as 'Critical Infrastructure'," *Wall Street Journal,* August 3, 2016.

9 Dan Goodin, "US E-Voting Machines are (still) Woefully Antiquated and Subject to Fraud," *arsTechnica*, November 7, 2016.

אזרחים אמריקאים. לגניבת זהות, הדלפת פרטים ו/או שינוי שלהם יכולה להיות השלכה על ההליך הדמוקרטי כולו.

חשיפה של מבצע לשיבוש נתוני אזרחים או לפגיעה במקומות ההצבעה שלהם (למשל, הודעה מזויפת על מיקום הצבעה ואף אפשרות לפסילת קולות) עלולה לפגוע באמון הציבור במערכת הבחירות. דוגמה לכך ניתן לראות בבחירות הכלליות בקנדה בשנת 2011, בהן נעשו "מתיחות" על אזרחים, שבמסגרתן הודיעו להם טלפונית על מיקום שגוי של קלפי, כנראה במטרה לפגוע במוטיבציה של מצביעים לממש את זכות ההצבעה שלהם.[10]

בישראל, פרטי הבוחרים אינם נשמרים במאגרי המדינה וועדת הבחירות בלבד, אלא מועברים לכול מפלגה המתמודדת בבחירות. מצב זה יוצר נקודת תורפה באבטחת המידע על הבוחרים, אם כי עד היום טרם נחשפו ניסיונות לשיבושו

10 מתוך סיכום מנהלים של סמינר שנערך בקנדה לבחינה השוואתית של מערכות בחירות מרכזיות, http://www.elections.ca/content.aspx?section=res&dir=rec/tech/comp&document=p4&lang=e#ftn10.

בישראל. הדבר מעורר את הסוגיה כיצד ניתן להבטיח שימוש הולם במאגר הבוחרים ולפקח עליו בצורה אמינה.

שיבוש מערכות הצבעה ביום הבחירות

הצבעה בבחירות מחייבת אימות פרטים אישיים, כוללת הצבעה ידנית או ממוחשבת, ספירת קולות בקלפי והעברת הנתונים למערכת המרכזית. שיבוש של אחד מהתהליכים הללו יביא לפגיעה משמעותית בתהליך כולו. המערכות האלקטרוניות המסייעות לניהול יום הבחירות כוללות שירותים שונים: ניהול הרישום לקלפי ומימוש זכות הבחירה; יכולת בחירה אלקטרונית בקלפי (באמצעות מסך מגע או כרטיס אישי); יכולת בחירה אלקטרונית מרחוק על בסיס גישה לאינטרנט בלבד; סיוע לספירת הקולות. להרחבת השימוש במערכות הצבעה אלקטרוניות יש השלכות חיוביות ושליליות: מצד אחד, הטמעה של מערכת אלקטרונית תגדיל את השתתפות האזרחים בבחירות (יכולה לאפשר להם להצביע מהבית או ממכשירים ניידים); מצד שני, הסיכון לחדירה למערכת כזו ולשיבושה הינו גבוה ומחייב השקעת משאבים לאבטחה ותחזוקה שלה.[11]

מחקר שערך המכון לחקר ביטחון סייבר בארצות הברית, החוקר טכנולוגיות סייבר עבור תשתיות קריטיות, העלה כי מערכת ההצבעה הישירה, וכן מערכת הסריקה (Op Scan) הסורקת את כרטיסי ההצבעה והמערכות המבצעות את שקלול הנתונים ומאגרי המידע הממוחשבים, אינן מספקות הצפנה מקצה לקצה ומענה אבטחתי מתאים. כמו כן נמצא כי בקלפיות רבות בארצות הברית מופעלות מערכות אלו באמצעות מחשבים, שאינם מוגנים וניתנים לפריצה בקלות. עוד נקבע במחקר כי יריבים בעלי יכולות מתאימות יוכלו למצוא דרך לפגוע במערכות מקומיות ומפלגתיות בעלות רמת אבטחה נמוכה יותר ממערכות הבחירות הכלליות במדינה, וזאת על ידי החדרת נוזקות למחשבים, השבתת המערכות, גניבת מידע, חשיפתו או שיבושו.[12]

שיבוש ספירת הקולות

אופן ספירת הקולות בתום יום הבחירות משתנה ממדינה למדינה בהתאם לשיטת ההצבעה. בישראל, שיטת ההצבעה במערכות בחירות ארציות הינה ידנית, באמצעות פתקים הנספרים באופן ידני בקלפיות ומוזנים למערכת אלקטרונית המחשבת את שיעורי ההצבעה האזוריים לכדי חישוב ארצי סופי. סמינר שהתקיים בקנדה

11 Goodin, "US E-Voting Machines are (still) Woefully Antiquated and Subject to Fraud,"

12 James Scott and Drew Spaniel, "The Painfully Vulnerable Election System and Rampant Security Theater", *ICIT Blog, Institute for Critical Infrastructure Technology*, October 24, 2016.

בשנת 2014, לבחינה השוואתית של מערכות בחירות מרכזיות בין בריטניה, קנדה, ארצות הברית, אוסטרליה, ניו זילנד והודו, הגיע למסקנה כי כלל הגופים המעורבים בתהליכי בחירות יידרשו בעתיד להתמודד עם אתגרים הנובעים מהתפתחות של מערכות מבוססות רשת ועם השלכותיהם על מערכות הבחירות, ובכלל זה אבטחה של תהליכי הצבעה מקוונים או מרחוק, וכן אבטחה של מאגרי נתונים ומערכות של ספירת קולות.[13]

פרסומים רבים בארצות הברית מצביעים על האפשרויות שבאמצעותן ניתן להשפיע על מערכות לספירת קולות ולזייף את הכרטיסים המפעילים את מערכות הבחירה הישירה האלקטרונית. כך, למשל, בחלקים מארצות הברית נכנסה לשימוש מערכת הצבעה ישירה אלקטרונית המבוססת על זיהוי באמצעות כרטיס אישי והצבעה על בסיס מסך מגע. מערכת זו שומרת את הנתונים ומאפשרת להדפיס פלט בסוף יום הבחירות, הכולל את חלוקת הקולות באותו קלפי. מתברר כי ניתן לזייף הצבעות באמצעות שימוש בכרטיס מזויף המאפשר שינוי של הנתונים במסך, מחיקת קולות ואף מחיקת מועמדים.[14] זאת ועוד, למרות הזיהוי באמצעות כרטיס, ניתן לחדור מרחוק למערכות אלו ולשבש את ספירת הקולות ואפילו את הפילוח שלהם. בחירה אלקטרונית, המבוססת על מחשבים נגישים לאינטרנט, קלה עוד יותר להתערבות חיצונית, להונאה ולפגיעה בתהליך הבחירות הכללי.[15]

פגיעה באמון הציבור באמצעות השפעה על תכנים בשיח הציבורי

כאמור, לצד תהליך הבחירות קיימים גורמים נוספים המהווים בסיס לאמון הציבור במדינה ובמוסדותיה. אחד החוקרים הצביע על שורת מאפיינים המהווים את המרכיבים המשמעותיים ביותר באמון הציבור בממסדים הפוליטיים במדינה דמוקרטית: תקשורת עצמאית, דעת קהל אקטיבית, מערכת משפטית עצמאית, רמת מחייה הוגנת (שירותי בריאות, דיור, חינוך ותעסוקה) ובחירות חופשיות. פגיעה ברכיבים אלה עלולה להשפיע באופן משמעותי על תחושת הביטחון האישי של האזרח במדינתו ועל אמון הציבור בממסדי המדינה ובשירות הציבורי בכלל.[16]

---

13 מתוך סיכום מנהלים של הסמינר: http://www.elections.ca/content.aspx?section=res&dir=rec/tech/comp&document=p4&lang=e#ftn10.

14 Goodin, "US E-Voting Machines are (still) Woefully Antiquated and Subject to Fraud".

15 Dimitris A. Gritzalis, *Secure Electronic Voting* (Springer Science & Business Media, 2012).

16 מתוך הרצאת פרופ' מרקו מאייר בכנס "סייבר, פוליטיקה ובחירות", סדנת יובל נאמן למדע, טכנולוגיה וביטחון, אוניברסיטת תל אביב, 17 בינואר 2017.

הופעתם בשנים האחרונות של מרחבי שיח ותקשורת חדשים (בדגש על המדיה החברתית) הביאה להתפתחות שיח פוליטי וציבורי נרחב הפונה לקהל מגוון יותר מאשר בתקשורת המסורתית ומאפשר קשר ישיר ובלתי אמצעי עם האזרחים והבוחרים. שינוי זה הביא להגברת השימוש באינטרנט כמרחב לגיוס פעילים ותמיכה, להעברת מסרים ולניהול מסעי בחירות. האינטרנט כבר אינו נחלתם של גורמי השיווק והפרסום בלבד. ניתן לזהות פעילות ענפה של מועמדים לבחירות במערכות תקשורת שונות, ואף ניסיונות השפעה של מדינות עוינות על דעת הקהל המתגבשת ברשתות החברתיות ובמרחבי הרשת.[17]

הגנה על תהליכים דמוקרטיים מחייבת אפוא להוסיף לאיומים הישירים שהוגדרו לעיל איומים במרחב התודעתי, שעלולים להשפיע באופן קריטי על ההליך הדמוקרטי, וכתוצאה מכך על אמון הציבור בו. בהקשר זה מתעוררת דילמה הנוגעת לצורך ליצור הבחנה בין מהלכים לגיטימיים במאבק פוליטי ובין התערבות בלתי לגיטימית של גורמים זרים. ההגנה מפני איומים כאלה אינה נוגעת להיבטי הסייבר הישירים (הגנת תחנות קצה, שרתים, רשתות וכדומה), אלא להגנה מפני התערבות בתוכן המסרים בשיח הפוליטי. השאלה העומדת לדיון נוגעת לגבולות התקשורת החופשית: האם היא כוללת את אזרחי המדינה ומנהיגיה בלבד, או גם גורמים חיצוניים (דוגמת מדינות זרות וארגוני טרור), שהתערבותם אינה לגיטימית ונועדה לשבש את ההליך הדמוקרטי. במילים אחרות, ניתן אולי להשלים עם מניפולציות, שקרים ושמועות כחלק לגיטימי במאבק הפוליטי בתוך המדינה, אולם לא ניתן לקבל התערבות זרה העלולה לערער את ביטחון האזרחים במוסדות המדינה ולהביא לערעור היציבות בה.

מבנה הרשתות החברתיות מאפשר לתוכן להפוך ל"ויראלי" באמצעות שיתוף רחב, המגביר את החשיפה והפרסום של תוכן מסוים על בסיס התנועה והתגובות שהוא מייצר. לכן, מספיק שכמה מאות משתמשים (אמיתיים או מדומים) ייצרו תוכן שיפנה לקהל יעד ספציפי, כדי שהמסר יהפוך ל"ויראלי" ויעורר שיח ציבורי, אליו יצטרפו גורמי התקשורת המסורתיים. כל הנאמר לעיל מצביע על כך שיש מקום לבחון כיצד ניתן למנוע מניפולציות של גורמים חיצוניים על התהליכים הדמוקרטיים במדינה – בחירות כלליות, תהליכים פנים־מפלגתיים, תהליכים משפטיים וכדומה.

כאמור, בשנים האחרונות נחשפו מספר ניסיונות המיוחסים לרוסיה להשפיע על השיח הפוליטי במדינות המערב. יש הגורסים כי ניסיונות ההשפעה וההתערבות במערכות הבחירות במדינות אחרות מבטאים כוונה של רוסיה לערער את האמון של אזרחי המערב בהליך הדמוקרטי בכלל ובמערכות הבחירות בפרט, תוך יצירת

17 אזי לב־און וארז כהן, **מקושרים: פוליטיקה וטכנולוגיה בישראל**, האגודה הישראלית למדע המדינה, ירושלים, 2011.

תחושה של היעדר יכולת של המערכת להגן על פרטיות אזרחיה ולשמור על הליך דמוקרטי נקי.[18] דומה שבשנים האחרונות רוסיה אכן עושה את המרב מבחינתה כדי להשפיע על דעת הקהל במדינות שיש לה אינטרסים בהן, כגון אוקראינה והרפובליקות הבלטיות, וכן גרמניה, הולנד וצרפת, המסמלות את הגורמים המשמעותיים ביותר באיחוד האירופי. דוגמאות לכך הן: חדירה קיברנטית לבונדסטאג בגרמניה בשנת 2015 בניסיון לאסוף מודיעין שיפגע במפלגת השלטון, והניסיון להתערבות במשאל העם שהתקיים בהולנד באפריל 2016, שנערך בעקבות דרישה לבטל את הסכם הסחר של האיחוד האירופי עם אוקראינה משנת 2014. סקר שבחן את עמדות המצביעים נגד ההסכם העלה כי מרבית הנימוקים שהם נתנו היו נימוקי כזב, שלא היו מבוססים על עובדות, וככול הנראה מקורם היה בתעמולה רוסית.[19] בנוסף לנאמר לעיל, נרשמו ניסיון רוסי להשפיע על ה"ברקזיט" של בריטניה מהאיחוד האירופי, ניסיון להשפיע על מערכת הבחירות בארצות הברית לטובתו של דונלד טראמפ, וניסיון שכשל להשפיע על הבחירות בצרפת מספר חודשים מאוחר יותר.

הדוגמאות שהובאו לעיל מלמדות על העלייה בפרסום מידע פוליטי או אסטרטגי באמצעות רשתות חברתיות או באמצעות אתרים שמתמחים בחשיפה (דוגמת "וויקיליקס") במטרה להשפיע על דעת הקהל ועל השיח הציבורי. גורמים המעוניינים להשפיע על השיח ועל תוצאות הבחירות יכולים לעשות זאת באמצעות חשיפה של מידע, אמיתי או מזויף, בעיתוי מתאים. חשיפה כזו מיועדת ליצור ספק בדבר כשרותו של המועמד ומאפשרת הפצת שמועות שיפגעו במועמדותו. הדוגמאות הללו גם מראות כיצד ניתן להשפיע על בחירות באמצעות הפצה של ידיעות כוזבות, פרסום סקרים שקריים, יצירת הד תקשורתי סביב דיווח כזב שיש לו השלכה על מדיניות חוץ, והדלפת מידע אישי ומביך על מועמדים. כל אלה יכולים להשפיע על תהליכים דמוקרטיים ועל יחסים בין מדינות.

ההבנה כי קיימת עלייה בשימוש באסטרטגיה זו מחייבת דיון מקיף בהרחבת ההתגוננות במדינה דמוקרטית נגד איום זה.[20] יתר על כן, גם אם תהיה הגנה מלאה על ההיבטים הטכנולוגיים של תהליך הבחירות, עדיין ניתן יהיה להשפיע על ההליך הדמוקרטי כולו. זהו אחד האתגרים המרכזיים העומדים בפני הגנה על כל מערכת בחירות: לא די בהגנה על תשתיות ומערכות טכנולוגיות; נדרש גם מענה הגנתי

18 Keir Giles, "Russia's 'New' Tools for Confronting the West", *Chatham House, Russia and EuroAsia Programme*, March 2016.

19 Anne Appelbaum, "The Dutch just Showed the World how Russia Influences Western European Elections", *The Washington Post*, April 8, 2016.

20 מתוך שימוע של ראש המרכז לסייבר והגנת המולדת בפני ועדת הקונגרס האמריקאי להגנת המולדת ותת־הוועדה לסייבר, הגנת תשתיות וטכנולוגיות ביטחון, 25 בפברואר 2016, http://docs.house.gov/meetings/HM/HM08/20160225/104505/HHRG-114-HM08-Wstate-CilluffoF-20160225.pdf

על השיח כולו מפני זיהום אנטי דמוקרטי חיצוני. אם בעבר הדגש היה על מניעת השבתה של מערכות התקשורת והמחשבים, בעידן של האיום החדש התוקף דווקא מעוניין שמערכות אלו יפעלו כדי שיוכל להזרים בהן את מסריו המניפולטיביים.

גורמים מאיימים על תהליך הבחירות הדמוקרטי

האיום הקיברנטי על מערכות בחירות יכול לבוא לידי ביטוי בהתערבות של מעצמות או של מדינות זרות, בפשיעה בין־לאומית או בפעילות טרור. ההבחנה בין סוגי האיום נעשית על פי זהות התוקף, המוטיבציה שלו לתקיפה, מורכבות ותחכום התקיפה והמשאבים שעמדו לרשותו כדי לבצעה. בבחינת אופן ההגנה על הליך הבחירות או על תשתית קריטית אחרת, ניהול הסיכונים צריך לכלול ניתוח של השחקנים בעלי המוטיבציה והיכולת לפגוע בתהליך הבחירות הדמוקרטי.[21] מאמר שפורסם בארצות הברית, אשר ניתח את הרגישות של תהליך הבחירות לאור ניסיונות ההתערבות הרוסיים, בחן, בין היתר, מיהם השחקנים השונים העלולים להוציא לפועל תקיפה קיברנטית נגד מרכיבי מערכת הבחירות בארצות הברית ומנה ביניהם מדינות עוינות, יריבים פנימיים ומפגעים בודדים (האקרים), כמו גם גורמים הפועלים ממניעים אידיאולוגיים, כגון קהילות "אנונימוס" או "וויקיליקס", או ארגונים ממומנים בעלי אידיאולוגיה פוליטית הפועלים להשפיע על הבחירות באמצעות קמפיינים מסיביים ברשתות ובקרב צעירים.[22]

המניעים של מדינות יריבות להתערב במערכות בחירות של מדינות אחרות משתנים בהתאם ליעד התקיפה. מניע מרכזי יכול להיות הרצון לערער את תחושת הביטחון האישי ואת אמון הציבור בהליך הדמוקרטי כולו. ההבנה כי דעת הקהל משפיעה על אופן קביעת המדיניות מניעה מדינות יריבות להתסיס אזרחים נגד המסגרת הדמוקרטית, ובעיקר נגד הממשל והפוליטיקה הפנים־מדינתית. מניע נוסף להתערבות במערכת בחירות במדינה זרה הוא הרצון להשפיע על תוצאות הבחירות. לכן, הגורמים המתערבים ישקיעו את משאביהם במספר ערוצים: השפעה על דעת הקהל באמצעות תעמולה, כמו למשל באמצעות שתילת "טרולים" הפועלים במרחב הרשת נגד הממסד, ולעיתים נגד קהילת האינטרנט, הפצה של תגובות שליליות ומשלהבות נגד מידע מסוים, חדירה לאתרים, הפצה של ספאם ועוד, ערעור דעת הקהל ואמונו במערכת והדלפת מידע רגיש על המועמדים היריבים. לאותם גורמים המתערבים במערכת הבחירות עשוי להיות גם מניע של ריגול ואיסוף מודיעין, כולל גניבת מידע רגיש על המועמדים או על מטה הבחירות שלהם, כפי שנעשה בקיץ 2016 בהדלפת דואר אלקטרוני מוועידת המפלגה הדמוקרטית בארצות הברית.

21 גולדשמידט, "המרחב הקיברנטי וההגנה על תשתיות קריטיות".

22 Scott, Spaniel, "The Painfully Vulnerable Election System and Rampant Security Theater".

סיכום

מאמר זה הציג את האיומים על מערכות בחירות אל מול התפתחויות קיברנטיות ותרבותיות והצביע על החשיבות של ראיית מערכות בחירות כתשתיות וכתהליכים קריטיים. המסקנה היא כי נדרשת הגנה כוללת על תהליך הבחירות, משום שהשפעה חיצונית עליו עלולה לערער מהיסוד את אמון הציבור בממסד הפוליטי במדינתו ובערכי הדמוקרטיה בכלל. גורמים בכירים במערך הסייבר הלאומי של ישראל מגלים הבנה לחשיבות ההגנה על מערכות המחשבים של ועדת הבחירות המרכזית ועל מאגר הבוחרים, ומסכימים כי ייתכן ונדרש גם שינוי חקיקה שיגדיר מערכות אלו כתשתיות קריטיות. יחד עם זאת, דומה שלא קיימת הבנה מספקת באשר להגנה הנדרשת על השיח הפוליטי מפני זיהומים חיצוניים.

מערכת בחירות הינה "בטן רכה" במדינה דמוקרטית, ותקיפתה עלולה להשפיע הן על המדינה והן על המועמדים. על מדינות המערב לשקול להרחיב את ההתייחסות ואופני המענה לאיומים על הליכים דמוקרטיים, כמו הגנה על השיח התקשורתי מפני זיהום והגנה על מפלגות, וזאת לצד הגנה על ועדות הבחירות ועל מנגנוני ההצבעה. הגנה על פלח אחד בלבד מהמערכת הכוללת לא תספיק. הניסיונות להשפיע על בחירות באמצעות חשיפה ופרסום של מידע שנאגר במערכות מחשב של מפלגות או מועמדים, שחלקם הצליח ככול הנראה, מחייבים להגביר את ההגנה על מערכות אלו. אותם ניסיונות גם מעוררים את השאלה בדבר אחריותה של המדינה להכוונת ההגנה הקיברנטית על מוסדות פוליטיים.

מאמר זה לא דן במענים לאיומים המוצבים בפני מערכת הבחירות במדינה דמוקרטית, וזאת מתוך כוונה לאפשר, בשלב ראשון, יצירת שיח על איומים אלה, בדגש על האיומים החדשים על השיח הפוליטי במדינה דמוקרטית. הפניית הזרקור אל איומים חיצוניים מדגישה את תפקידה של המערכת הביטחונית במדינה לבלום איומים של חתרנות מדינית. הדבר גם מחייב אותה להגדיר את האיומים ולתחם אותם באופן שלא יפגע בחופש הביטוי מצד אחד, אך ישמור על השיח הפוליטי מפני התערבות לא לגיטימית מצד שני.

הייחוד שבהגנה על תהליך הבחירות או על שאר ההליכים הדמוקרטיים, כמו שלטון החוק וחופש הביטוי, הוא שאין מדובר בשמירה על תפעול התשתית בלבד, אלא בהגנה על אמון הציבור במערכת – הישג חמקמק בהרבה, שניתן לערער עליו בדרכים שונות ומגוונות. המאמר הציג לפיכך את הצורך בהגנה על מערכת המחשבים המתפעלים את מערכת הבחירות – צורך שקיימת לגביו הסכמה רחבה – ולצידו גם את הצורך בהגנה על השיח הפוליטי מפני זיהום חיצוני, שתכליתו לערער את אמון הציבור במערכת הדמוקרטית כולה – צורך שעדיין לא קיימת הכרה רחבה בו, בין השאר משום שהוא מאתגר עקרונות דמוקרטיים, כמו שמירה על חופש הדיבור (במדיה החברתית ובאמצעי התקשורת).

יתרון שאינו רק טכנולוגי – השינוי הארגוני בארצות הברית בתחום הלוחמה במרחב הסייבר

עמית שיניאק

מרוץ החימוש בתחום הסייבר הוא חלק מהמציאות הביטחונית המדינתית בימינו. מאמר זה מעלה את הטענה כי מאפייניו הייחודיים של ממד הסייבר והירידה ברמת התחכום הטכנולוגי הנדרשת למימוש יכולות תקיפה והגנה בו, גורמים לכך שהשגת יתרון ביטחוני בממד זה מחייבת קידום ופיתוח יצירתיים בתחום ארגון הכוח וגיבוש תורת לחימה צבאית המשלבת בין הפעילות הביטחונית במרחב הסייבר הווירטואלי ובין מרחבים פיזיים. טענת המאמר מתבססת על סקירה מקיפה של החקיקה, התוכניות וההחלטות סביב תהליך בניין הכוח, הארגון ותורת הלחימה של מבצעי סייבר בארצות הברית, מראשית שנות השמונים של המאה העשרים ועד שנת 2012. המאמר מדגיש את השינויים והעלייה בהיקף האיומים במרחב הסייבר, את השינויים בתפיסת האיום ואת המעבר מגישה טכנית לגישה הרואה באינטרנט מרחב לחימה בעל מאפיינים ייחודיים. מסקנותיו של המאמר רלוונטיות לאנשי מקצוע ומקבלי החלטות כאחד ומכוונות להביא לארגון ופיתוח תורת לחימה בצבאות ובארגוני ביטחון אזרחיים כצעד הכרחי בדרך ליצירת יתרון אסטרטגי במרחב לחימה זה. למרות שהמאמר מתמקד בארצות הברית ובפרק זמן מוגבל בלבד, משרתו היא להפנות זרקור לתחום הארגון כזירה רלוונטית ומשמעותית להשגת יתרון מדיני בתחום ביטחון הסייבר, וזאת מול המצב השורר כיום, בו קיימת התמקדות יתר בקרב חוקרים ומקבלי החלטות בפיתוח טכנולוגי ככלי המרכזי להשגת יתרון בתחום זה.

מילות מפתח: מרחב הסייבר, ביטחון סייבר, בניין כוח, ארגון, תורת לחימה, ארצות הברית, יתרון אסטרטגי, דומיננטיות.

ד"ר עמית שיניאק הוא עמית מחקר פוסט־דוקטורנט בתוכנית ללימודי מדע, טכנולוגיה וחברה (STS) בבית הספר קנדי לממשל באוניברסיטת הרווארד.

מבוא

המאבק הבין־מדינתי בתחום הסייבר הוא עובדה ידועה זה מכבר ונושא שכיח למחקרים בתחום הביטחון והיחסים הבין־לאומיים.[1] מרוץ החימוש ובניין הכוח הצבאי בתחום הסייבר מוצאים את ביטוים בעלייה המשמעותית בהקצאת משאבים לאומיים ליצירת ביטחון במרחב זה.[2] לאור פעילות אינטנסיבית זו, ראוי לשאול מה היא הדרך להשיג יתרון מדינתי במרוץ החימוש הקיים בתחום הסייבר?

במאמר זה אטען כי החזית במרוץ החימוש הקיברנטי נמצאת לא רק בפיתוח טכנולוגי של כלי פעולה חדשים ומתקדמים יותר ובהשגת ניסיון מבצעי במרחב הסייבר, אלא גם, ובמיוחד, בהתקדמות בארגון כוחות הביטחון ויחידות הצבא הפועלים במרחב זה ובתיאום בין הדרגים המדיני והצבאי. זאת, באופן שיבטא שינוי בתפיסת האיום של מרחב הסייבר על מדינות ובדרך הפעולה הצבאית הנדרשת כדי להתמודד איתו. במילים אחרות, למרות שאנו חיים בתקופה שבה ניתן לפתח יכולות לוחמת סייבר בקלות יחסית, ורמת התחכום הנדרשת מהתוקף נמצאת בירידה, המאבק בין מדינות באמצעות מרחב הסייבר מחייב חשיבה שונה: השקעה בתהליכי ארגון ובניין כוח עשויה להיות הגורם המבדיל בין מדינות בעלות דומיננטיות בתחום הסייבר ובין שחקנים בין־לאומיים אחרים, ולכן, כדי להשיג יתרון מדיני במרחב הסייבר היא עדיפה על השקעה בפיתוח טכנולוגי.[3]

המאמר אינו מציג מחקר השוואתי,[4] אך הדוגמה האמריקאית שתפורט בהרחבה בהמשך הינה משמעותית, משום שהיא מעידה על שינוי תפיסתי וארגוני, במסגרתו

---

1 ראו כמה דוגמאות ידועות לכך: Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Washington: CCSA Publication, 2013); Martin Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND Corporation, 2007); Martin Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge: Cambridge University Press, 2009); Ben Buchanan, *The Cybersecurity Dilemma: Hacking Trust and Fears between Nations* (New York: Oxford University Press, 2016); P. W. Singer and Allen Friedman, *Cybersecurity and Cyberwar: What everyone Needs to Know* (Oxford: Oxford University Press, 2014); Harris Shane, *@War: The Rise of the Military-Internet Complex* (New York: Mariner Books, an Eamon Dolan Book, 2015).

2 ניתן לראות זאת בנתונים של חברות ביטוח בין־לאומיות, למשל:
"Risk Nexus: Overcome by Cyber Risks? Economic Benefits and Costs of Alternate Cyber Future", *Atlantic Council and Zurich Insurance Group Report*, September 10, 2015, Figure 13, http://publications.atlanticcouncil.org/cyberrisks//.

3 המונח "ארגון ובניין הכוח" מכוון לתהליך התכנון, השינוי והסדרת האחריות בין גופים שונים על תחום לחימה מסוים, וזאת לצורך שליטה, בקרה, פיתוח כוח אדם, אמצעי לחימה ודוקטרינה ייעודיים.

4 להשוואה בין ארצות הברית, ישראל וסין ראו: עמית שיניאק, **המרחב המקוון כאזור גבול: תהליך יצירת הריבונות ויכולת האכיפה במרחב המקוון בישראל, ארה"ב וסין**, הוצאת המחבר, ירושלים, 2015.

אימצה ארצות הברית גישה הרואה בסייבר "מרחב סייבר" ("Cyberspace"), או באופן מדויק יותר "מרחב לחימה".[5] זהו הבסיס לתפיסה הצבאית בארצות הברית היום, שממנו נובע ארגון הכוח האמריקאי בתחום הסייבר, המתבסס על גישה הרואה, כאמור, בסייבר מרחב לחימה. מרחב לחימה זה מצריך פעולה מדינית וצבאית משולבת, בדומה לפעולה הנדרשת לשימור הביטחון הטריטוריאלי והאינטרסים של המדינה במרחבים הפיזיים – באוויר, בים וביבשה.[6]

טענה זו תיבחן במאמר באמצעות ניתוח התפתחות התפיסה הביטחונית, ובמיוחד ארגון ובניין הכוח בתחום הסייבר בארצות הברית, כפי שהדבר מתבטא במסמכים רשמיים גלויים. זאת, בחלוקה לשלוש תקופות: בין השנים 1983–1998, שבהן חל תהליך של הפנמת הסיכונים הפוטנציאליים הגלומים בסייבר לאינטרסים מדיניים והחל תהליך ארגון ביחידות המודיעין האמריקאיות בניסיון לאבטח את המידע הקיים במערכות התקשורת החשאיות מתָווכות המחשב; בין השנים 1998–2008, במהלכן הופנמו במסד הביטחוני האמריקאי המשמעויות של קיומן התקין של מערכות תקשורת מתָווכת מחשב והשלכותיהן על תפקודם הסדיר של תשתיות בסיס ומשאבי יסוד הנדרשים לקיומה של מדינה מודרנית (כגון: מים ומזון, אנרגיה ותחבורה); בין השנים 2008–2012, בהן התרחש מהפך בתפיסת מרחב הסייבר, שבמסגרתו אומצה גישה הרואה במאמץ הצבאי במרחב זה מאמץ מקביל ומשיק לממדים הנוספים (ים, אוויר, יבשה).

הסקירה שתוצג במאמר זה מראה כי ההיגיון המנחה את בניין הכוח לפעולה במרחב הסייבר בקרב מדינות ומעצמות כמו ארצות הברית עבר תמורות לאורך שלושים השנים האחרונות, וזאת לאור העלייה באיום הסייבר ובהשפעתו על מגוון של אינטרסים מדינתיים. תמורות אלו תומכות בטענת המאמר כי ארצות הברית, כמעצמה בתחום הסייבר, היא גורם מוביל בתחום זה גם משום שהיא ארגנה מחדש את כוח הסייבר הצבאי שלה על בסיס אותו היגיון שהנחה אותה בארגון כוחותיה הצבאיים במרחבי הים, האוויר והיבשה. אין בכוונת המאמר לנתח את המחלוקות באשר ליתרונות ולחסרונות של מאפייני ארגון הכוח בתחום הסייבר בתוך הצבא,[7] או ליישב ביניהן. כוונתו היא להדגיש את החשיבות שבקידומו של ארגון הכוח במרחב הסייבר ושל תפיסת הפעלתו, וכן את חשיבות הצורך להתארגן סביב

5 גישה זו באה לידי ביטוי גם בשינוי בהגדרת המונחים המקצועיים המתייחסים אל הסייבר היום כסביבה/ממד/מרחב.

6 יש לציין כי כמה מחקרים העוסקים בשימוש בשפה, במטאפורות, בדימויים ובמודלים מתחומי ביטחון וטכנולוגיות אחרים, במיוחד נשק גרעיני, גם מתייחסים לחשיבות השינוי התפיסתי בתחום ביטחון הסייבר, אך אינם מדגישים את השינוי הארגוני המוסדי עליו מרחיב מאמר זה.

7 למשל, בשאלה האם יש לשלב את גורמי ההגנה, ההתקפה ואיסוף המודיעין באותו גוף, האם לשמר את הדומיננטיות של גורמי המודיעין או הטכנולוגיה, וכדומה.

הרעיון שהסייבר הוא מרחב לחימה מקביל למרחבי לחימה פיזיים. זאת, לעומת התפיסה הרווחת היום בקרב אלה החוקרים את תחום הביטחון בסייבר, הממקדת את תשומת הלב של מקבלי ההחלטות והחוקרים בפיתוח הטכנולוגי ובניסיון המבצעי ככלים המרכזיים וכמוקדי השקעה עיקריים להשגת יתרון בתחום זה.[8]

ניתן להרחיב ולטעון כי תפיסה זו של מרחב הסייבר היא המבדילה בין פעולה צבאית של מדינות מובילות בתחום ביטחון הסייבר (כגון ארצות הברית) ובין ישויות פוליטיות ושחקנים מדינתיים, על־מדינתיים ותת־מדינתיים אחרים. הראשונות מפעילות מאמץ צבאי סדור ומתואם הנשען על תוכניות ופקודות רשמיות שמטרתן להגשים תכלית טקטית ו/או אסטרטגית מסוימת במרחב הסייבר (בדומה לפעולות בים, באוויר וביבשה). האחרונות פועלות במרחב הסייבר בצורה שאינה סדורה, אלא בעלת דפוס רשתי ו"טפילי", הדומה יותר לפעולות טרור או ללחימת גרילה, כגון חבלה, שיבוש, הפחדה והשפעה על התודעה, שנעשות באמצעות תקשורת ממוחשבת.

1983–1998: תפיסת אבטחת המידע

בתקופה שבין שנת 1983, בה הופרדה מערכת המחשבים הצבאית האמריקאית (Milnet) מרשת המחשבים האזרחית, ובין השינוי במאפייני האיום ב־1998 התחולל שינוי משמעותי בתפיסת האיום בתחום אבטחת המידע מתָווך המחשב (ICT), ובהתאם לכך בארגון ובבניין הכוח הביטחוני האמריקאי באותו תחום. עיקרו של השינוי נבע מגישה אמביוולנטית יותר כלפי היתרונות והחסרונות שבתקשורת מתָווכת מחשב. הדבר התבטא במעבר מפעולות מדינתיות שיועדו בעיקרן לשפר ולייעל את זרימת המידע לצורך קידום פעילות אזרחית מחקרית וכלכלית, לפעולות שמטרתן ליצור בקרה, שליטה וחסמים כדי להגן על מידע מדיני רגיש (ביטחוני ואזרחי) שנתפס כמאוים בשל אותה זרימת מידע.

המשמעויות המעשיות של בניין הכוח של ארצות הברית במרחב הסייבר באותה העת התבטאו בעיקר בפעולות להגנת ואבטחת מידע רגיש, באופן שניתן לתאר אותו כיישום או הרחבה של תפיסת ההגנה על המידע, כפי שהייתה קיימת אז בקרב צבאות וארגוני ביון, על מאגרי המידע הממוחשבים שהפכו עם השנים לאמצעי עיקרי לשימור וניהול מידע זה. לפיכך, הפעולות העיקריות שננקטו ביחס לרשתות המחשבים של ארגוני המודיעין והצבא כוונו לשיפור היכולת לשלוט במידע חשאי ומסווג (יצירת רשת תקשורת מחשבים נפרדת וסגורה לצבא היא דוגמה ברורה לכך), ולראשונה גם להשגת מידע חשאי ובעל ערך במסגרת לוחמת

8 ראו, למשל, את הנטייה לניתוח טכנולוגי בכתבי העת *The Cybersecurity Journal, The Journal of Cyber Policy* ודומיהם, המדגישים את הפיתוח הטכנולוגי והניסיון המבצעי ככלים מרכזיים להערכת הביטחון בסייבר ולקידומו.

מודיעין ומידע ולגיבוש הסמכות המדינית המשפטית הנדרשת לשם כך. בתקופה זו הוקמו מוסדות ויחידות ייעודיות, שונו הגדרות האחריות של גופי ממשל וביטחון קיימים והחלה ראשיתה של חקיקה האוסרת על כניסה לא מאושרת למאגרי מידע ממוחשבים רגישים ומאפשרת ענישה ואכיפה. שינויים אלה לא הובילו, עם זאת, לשינוי משמעותי בחשיבה הצבאית.

עצם יצירתה של הפרדה פיזית ומוסדית בין תקשורת מתֻווכת מחשב צבאית ואזרחית הייתה בעלת משמעות רבה ליצירת יכולת שליטה וביטחון במידע הממוחשב. הפרדה זו נוצרה בעקבות שורת פעולות, שעיקרן הפרדת מערכת התקשורת הצבאית ממערכת התקשורת האזרחית בשנת 1983; יצירת מערכת סיווג המאפשרת רק לבעלי תפקידים רלוונטיים לפעול בה;[9] וחקיקה מ־1984 שאסרה על כניסה ללא רשות של אזרחים למערכות מחשב פדרליות שהוגדרו כ"מערכות מחשב מוגנות"[10]("Protected Computers") והרחיבה את סמכות השירות החשאי האמריקאי להגן עליהן.[11]

פרסומים על פרשיות ריגול ופשיעה באמצעות פריצה למערכות מחשב, למשל פרשיית "ביצת הקוקייה"[12]("The Cucko's Egg") ומעצר כנופיית "414" בשנת 1983, הובילו לחקיקה נוספת בשם "Computer Security Act of 1987",[13] שחייבה פיתוח קריטריונים ותקנים לאבטחת מידע ממוחשב ברשויות הפדרליות האמריקאיות,[14] הכשרת כוח אדם ייעודי ומתן הדרכה לעובדים עם מערכות מחשב בדבר הסכנות הפוטנציאליות.[15] בנוסף לכך נקבע באותו חוק כי המערכת הביורוקרטית האזרחית תהיה כפופה בתחום זה לפיקוח והנחייה של סוכנות מודיעין האותות (NSA).[16] הכפפה זו, שהיא אחד מעיקרי השינוי המוסדי שנוצר אז ונאכף עד היום, קיבלה משנה תוקף בהוראה הנשיאותית NSD42 משנת 1990, המנחה לחזק את אבטחת מערכות התקשורת הלאומיות ולבדל אותן ממערכות תקשורת ציבוריות אחרות.[17] הוראה זו מציבה את ראש ה־NSA כסמכות פיקוח בכירה על כלל משרדי הממשלה,

9 תמר אשורי, **מהטלגרף עד המחשב: היסטוריה של אמצעי התקשורת**, רסלינג, תל אביב, 2011, עמ' 138.

10 "18 U.S. Code § 1030: Fraud and related activity in connection with computers", *U.S. Congress*, 1986, §a2C.

11 שם, סעיף D.

12 Clifford Stoll, *The Cuckoo's Egg: Tracking a Spy through a Maze of Computer Espionage* (New York: Doubleday Pocket Books, 1989).

13 "Computer Security Act of 1987", *U.S. Congress*, 1987.

14 שם, סעיף 1.

15 שם.

16 שם, סעיף 5.

17 "National Security Directive No. 42: National Policy for the Security of National Security Telecommunications and Information Systems", *U.S. White House*, 1990, §2.

וזאת באמצעות ועדה בראשות שר ההגנה של ארצות הברית שקמה במסגרת "המועצה לביטחון לאומי".[18]

בשנת 1988, לאור ההד הציבורי שנוצר עקב פעולתו ההרסנית של אחד הווירוסים הראשונים – "תולעת מוריס" ("Morris Worm") – שפגע בכעשרה אחוזים מכלל המחשבים שהיו מחוברים לאינטרנט באותה עת,[19] הוקם ביוזמת המכון להנדסת תוכנה (IES) באוניברסיטת קרנגי מלון, ותחת אחריותו, מרכז הניטור והתגובה הראשון להתמודדות ומזעור נזקים מתקיפות באמצעות מחשבים ("Computer Emergency Response Team" – CERT). למרות שהיוזמה להקמת המרכז הייתה אקדמית, פעל הממשל האמריקאי להחיל ולקבע את פעולותיו כנהוג ביחסי הממשל עם האקדמיה – באמצעות חוזה שקבע כי משרד ההגנה של ארצות הברית יממן את פעולתו, אך גם יגדיר את מסגרת פעולותיו.[20] המרכז שהוקם היווה מאוחר יותר את המודל למסגרות פיקוח וניטור איומים במרחב הסייבר בארצות הברית ובמדינות רבות נוספות.

בתקופה זו רווחה התפיסה הרואה באינטרנט כלי להעצמת יכולת במרחב הפיזי ולאו דווקא מרחב חדש להתנהלות בין מדינות. הדבר עולה מהתפיסה הביטחונית ומהדוקטרינה הצבאית האמריקאית המנוסחות בחזון המטות המשולבים של צבא ארצות הברית שפורסם ב־1996 במטרה לחזות את הדרישות לשדה הקרב העתידי עד שנת 2010. למרות העובדה שהמשמעות של יכולות ממוחשבות כבר הייתה ברורה באותה עת,[21] האינטרנט שהומשג אז לראשונה במסגרת הצבאית כ"רשת המחברת רשתות" ("Network of Networks"), נתפס בעיקר כתשתית בסיסית המאפשרת את היכולת להפעיל אמצעי לחימה מתקדמים המבוססים על רשת נתונים (Information Grid).[22]

זו הייתה הדוקטרינה שהובילה להקמתה, בשנת 1995, של יחידה ייעודית בחיל האוויר האמריקאי ללחימה הגנתית והתקפית באמצעות תקשורת מתָווכת מחשב, שנקראה The 609th Information Warfare Squadron.[23] לחימה באמצעות

18 שם, סעיפים 4–6.

19 Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, p. 26.

20 "U.S. Department of Homeland Security Announces Partnership with Carnegie Mellon's CERT Coordination Center", *SEI Press Release*, September 15, 2003, http://www.sei.cmu.edu/newsitems/uscert.cfm

21 כך, למשל, ההגנה על תשתיות ממוחשבות זכתה להתייחסות במסמך, אך צוינה ככלי שמטרתו העיקרית היא לאפשר עליונות בלוחמת מידע (IW).

22 "Joint Vision 2010", *U.S. Office of the Joint Chiefs of Staff*, 1996, p. 16.

23 היחידה פעלה מ־1995 עד 1999. אז היא הוכפפה לארגון הצבאי החדש בתחום הלחימה בסייבר. להיסטוריה הרשמית של היחידה ראו פרסום של חיל האוויר האמריקאי: "609th IWS: A Brief History, October 1995-June 1999", *U.S. Department of the Air Force*, 1999.

מחשבים עדיין נתפסה אז בקרב הפיקוד העליון האמריקאי כאמצעי לחימה נוסף ולא כמרחב לחימה עצמאי שמתקיימים בו מאמצי הגנה והתקפה,[24] הדורש לכן את ארגון הכוח הצבאי מחדש.[25] גישה זו, שראתה במרחב הסייבר רק אמצעי פרקטי ללחימה (ולא מרחב לחימה חדש), מוצאת ביטוי במזכר רשמי שפרסמו מפקד חיל האוויר ושרת האווירייה האמריקאית בשנת 1997, בו נקבע כי "לוחמת מידע היא אמצעי ולא מטרה, בדיוק כשם שלוחמה אווירית היא אמצעי ולא מטרה בפני עצמה".[26] התפיסה העולה מציטוט זה מעידה על חשיבה צבאית שאינה מזהה את חשיבות המושגים "מרחב" ("Space") או "ממד" ("Dimension") כבסיס לקביעת מדיניות ביטחון בכלל (לא רק באוויר ולא רק בסייבר). ייתכן שגם היום יש בקרב אלה המפעילים אמצעי לחימה במרחב האווירי (וכן הימי והיבשתי) הרואים פעולות בסייבר כאקט תומך בלבד. גישת כותבי המזכר באותה העת הייתה כי איום הסייבר מכוון למידע בלבד והם התקשו לחזות את היקף העיסוק הצבאי בו היום.

1998–2008: תפיסת התשתיות

בתקופה זו חל שינוי משמעותי בתפיסת האיום הנובע מרשתות מחשבים, הן ברמת הדחיפות והן בסיכון שאיום זה מציב לריבונות המדינה וליכולת תפקודה תחת מתקפה. הסיבה לכך הייתה השינוי במאפיינים הטכניים של פריצות למערכות מחשב, שהפכו למורכבות יותר ויותר, בעוד שרמת התחכום והידע הטכני שנדרשה מהפורץ ירדה משמעותית מאז אמצע שנות התשעים של המאה העשרים.[27]

מספר אירועי פריצה למערכות המחשב של הפנטגון בשלהי שנות התשעים, הן במסגרת תרגיל ER97 והן בפרשיית הריגול "Solar Sunrise", נתפסו כ"קריאת השכמה" למערכת הביטחון האמריקאית. הם גם הבהירו כי אין במערכת הצבאית והביטחונית של ארצות הברית גורם אחד המוגדר כאחראי על פעולות נגד איומים מעין אלה.[28] בעקבות זאת התקבלה לראשונה החלטה, בנובמבר 1998, להקים כוח משימה ייעודי –JTF) "Joint Task Force for Computer Network Defense"

24 ראוי לציין שלמול תפיסה זו של הפיקוד הצבאי העליון רווחה בקרב דרגי העבודה שהקימו את טייסת 609 ההבנה שהם חלוצי הלחימה במרחב חדש. הם אף השוו את עצמם לטייסת הראשונה שפיתחה את תורת הלחימה באוויר ב־1913: שם, עמ' 1.

25 Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, p. 31.

26 "Information warfare is a means, not an end, in precisely the same manner that air warfare is a mean, not an end": "Cornerstones of Information Warfare", *U.S Department of the Air Force*, 1997, http://www.c4i.org/cornerstones.html.

27 "Securing the Nation's Critical Cyber Infrastructure", *U.S. Department of Homeland Security*, 2010, p. 3. תשומת לב לגרף בעמוד 3, המצביע על נקודת האיזון בין הדרישות לידע של התוקף ובין רמת התחכום של התקיפה בשנת 1990. בשנת 1995 כבר ניתן היה לרכוש כלי תקיפה מתוחכמים מן המוכן.

28 Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, p. 36.

(CND – שהוכפף ל"סוכנות ההגנה למערכות מידע" (Defense Information Systems Agency" – DISA), ומאוחר יותר לפיקוד החלל האמריקאי. כוח המשימה פעל בסנכרון עם ה־NSA ויועד ללחימה במרחב הסייבר ולהתמודדות התקפית (לא פסיבית) עם תקיפות מצד מדינות זרות לצורך אבטחת רשתות מחשב.[29] הכוח, שפורק בשנת 2010, היה גורם משמעותי בקידום המוכנות של ארצות הברית להגנה על מרחב הסייבר, במיוחד בזכות כוח האדם המגוון והרלוונטי שרוכז לצורך הקמת גופים שיוכלו להתמודד עם מבצעי מחשב התקפיים: מומחי מחשבים, אנשי צבא ממגוון זרועות, אנשי מודיעין ואנשי ביטחון. מאוחר יותר אף נשלחו אנשי צבא ללימודים מתקדמים בתחום המחשבים ויצרו שילוב אידיאלי מבחינת הכשרתם המקצועית.[30]

בשנת 2004 קיבל כוח המשימה אחריות על כלל מבצעי ההגנה וההתקפה בתחום הסייבר, ועבר מעיסוק ישיר בתחומים אלה להיות גוף מטה צבאי סדור שאינו פועל בעצמו להגן או לתקוף, אלא מסנכרן ומנחה את כל המפקדות האופרטיביות והיחידות הטקטיות האחראיות על פעולות ביטחוניות במרחב הסייבר בזרועות ובחילות השונים.[31] הגוף החדש – JTF-CNO –הוביל הן לשינוי ביורוקרטי־ארגוני והן לשינוי ביכולת ההתגוננות המעשית של מערכת הביטחון האמריקאית: מבחינה ארגונית, שינוי זה היווה את הפתח להקמתו בהמשך של פיקוד הסייבר; מבחינה מעשית, כוח המשימה, שגובש במקור לצורך התמודדות עם אתגרים ביטחוניים, הפך למשמעותי גם בגיבוש יכולת התמודדות עם סוגיות משיקות, שלא היו חלק מייעודו המקורי אך סיכנו את המוכנות המבצעית ואת הריבונות האמריקאית במרחב הסייבר. מדובר, בין היתר, בווירוסים עצמאיים שתרמו לתחושת האיום בשל ההשלכות האפשריות של פגיעתם בתקשורת מתֻווכת מחשב.

תחושת איום חדשה זו הובילה להגדרת הצורך בהערכת מצב לאומית מתמשכת לאיתור הבעיות הביטחוניות בתקשורת מתֻווכת מחשב, וזאת ככלי לגיבוש מדיניות, לתכנון ולהתמודדות עם בעיות אלו. נקודת התורפה המרכזית שהתגלתה בהערכת המצב הייתה שתשתיות קריטיות ומשאבי היסוד האזרחיים של המדינה, שאינם חסויים ולא חלה עליהם חובת פיקוח והסתרת מידע, פתוחים לפגיעה אפשרית באמצעות תקשורת המחשבים שעליה הם נסמכים. אחד המהלכים להתמודדות עם מִפגע זה היה חקיקתו בשנת 2002 של חוק "Critical Infrastructure Information Act". החוק הגדיר את המונח "מידע תשתיתי קריטי/חיוני" כחלק מתוכנית

29 שם, עמ' 38–40.
30 שם, עמ' 38–39.
31 שם, עמ' 57.

להתמודדות עם פגיעה בתשתית רגישה זו,[32] והרחיב את הגדרת המונח "מערכות מוגנות", כך שתכלול גם מערכות ציבוריות אזרחיות.[33]

בשנת 2003 קיבלו הנשיא בוש הבן והשר להגנת המולדת של ארצות הברית החלטה (Homeland Security Presidential Directive No. 7 – HSPD7) שתיקפה את הצורך בפעילות ביטחונית שאינה צבאית להגנה על תשתיות אזרחיות. הגופים שהוקמו במסגרת זו תחת המשרד להגנת המולדת קיבלו אחריות לניטור, תכנון, הנחייה, הגנה וקביעת עדיפויות במרחב הסייבר (ללא כוחות מבצעיים; אלה נותרו בידי הצבא וסוכנויות המודיעין). כמו כן הואצלו סמכויות למשרדי הממשלה השונים כדי שיקיימו סקר מקיף שיכלול הערכה וסקירה של כלל התשתיות והאינטרסים שבתחום אחריותם, וזאת במטרה לאתר אפשרויות לתקיפת תשתיות על ידי ארגוני טרור באמצעים ממוחשבים.[34] ההחלטה אף יצרה הקבלה בין פגיעה במערכות המחשב של תשתיות מסוימות לבין הפעלת נשק להשמדה המונית.[35] להקבלה זאת הייתה משמעות מבחינה דוקטרינרית, משום שהשתמע ממנה שיש להיערך למניעת איומים ממרחב הסייבר באופן דומה ובהשקעה דומה להיערכות של ארצות הברית אל מול איומים בנשק בלתי קונבנציונלי ואיומים של מתקפות טילים בליסטיים. הקבלה זו גם הובילה את תורת הלחימה בסייבר לשימוש נרחב בדימויים מעידן המלחמה הקרה, כמו "הרתעה" ו"הגנה אקטיבית" – דימויים הרווחים בתחום לוחמת הסייבר עד היום.[36]

התוכנית המדינית שתוכננה לאור סקר המִפגעים פורסמה על ידי ממשל בוש הבן בשנת 2003 וכללה מרכיבים שהצביעו על שינוי תודעתי וארגוני משמעותי הן לגבי הממשל הפדרלי והן לגבי המגזר הפרטי:[37] הקמת צוות תגובה ביטחוני לתקיפות סייבר על בסיס CERT אקדמי; תוכנית להפחתת הסיכון הביטחוני ונקודות הכשל הלאומיות אל מול איומי סייבר; תוכנית לאומית להכשרה וליצירת מודעות בהקשרי ביטחון סייבר; שיפור אבטחת מרחב הסייבר הממשלתי; שיתוף פעולה

---

32 ראו ההגדרה המלאה בחוק: "Critical infrastructure information means information not customarily in the public domain and related to the security of critical infrastructure or protected systems": "Public Law 107-296: Homeland Security Act of 2002 – Critical Infrastructure Information Act", *U.S. Congress*, 2002, Sec. 211/3.

33 שם, פרק 211/6.

34 "Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization and Protection", *U.S. Department of Homeland Security*, 2003, §12

35 שם, סעיף 13.

36 על העיסוק בסוגיית ההרתעה בסייבר ראו, למשל: Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace", *International Security*, 41, no. 3 (2016-2017), pp. 44-71.

37 "The National Strategy to Secure Cyberspace", *U.S. White House*, 2003, p. X.

בין־לאומי לצורך שיפור הביטחון הלאומי בסייבר; הקמת שני מוסדות לשיפור הפיקוח על רמת האבטחה של התשתיות הממוחשבות הפיננסיות.[38]

האסטרטגיה הלאומית לאבטחת מרחב הסייבר כללה מרכיב נוסף, שנבע מההבנה שהעלייה הגבוהה במספר בסייבר גורמת לרגישות מדינית נוספת כתוצאה מהיכולת לפגוע במדינות באמצעות פגיעה באינטרסים הכלכליים שלהן – דבר שהופך את המגזר הפרטי לשותף הכרחי ליצירת ביטחון ולשימור הריבונות. גישה זו קיבלה משנה תוקף בהחלטה הנשיאותית EO 13286 משנת 2003, שהובילה לשינוי ארגוני נוסף: מינוי גורמים רשמיים לגישור בין המגזר הביטחוני ובין המגזר הפרטי, על בסיס ארגונים אזרחיים, כגון "המועצה המייעצת לתשתיות לאומיות" (National Infrastructure Advisory Council" – NIAC), ו"המרכז לשיתוף וניתוח מידע" ("Information Sharing and Analysis Center" – ISAC).[39] למרות חשיבותו של המגזר הפרטי, קוצר היריעה של מאמר זה, המתמקד בשינוי בארגון הכוח הצבאי וזרועות הביטחון, לא מאפשר להרחיב על השינוי הארגוני שנוצר לצורך הרחבת שיתוף הפעולה בין המגזר הביטחוני ובין המגזר הפרטי בארצות הברית, שיתוף פעולה המהווה כיום גורם מרכזי בניטור האיומים במרחב הסייבר שם.

חוק נוסף, משנת 2004, נועד ליצור רפורמה בכלל שירותי המודיעין האמריקאיים ולהתאים אותם לאיומים העכשוויים.[40] החוק כלל לראשונה התייחסות גלויה לאפשרות שארצות הברית תעשה שימוש פסיבי ואקטיבי בתקשורת מתווכת מחשב כדי לשפר את ההגנה על עצמה. החוק גם מזכיר שני סוגי פעולות שונות במרחב הסייבר: פעולה התקפית נגד עסקאות ממוחשבות המתבצעות באמצעים אלקטרוניים, שנועדו למימון פשיעה וטרור חוצי גבולות; פעולת מודיעין לאיסוף מידע הקיים במרחב הסייבר לצורך מניעת כניסתם לארצות הברית של אנשים המשתייכים לארגוני טרור ופשיעה.[41]

בשנת 2006 פורסמה "התוכנית להגנה על תשתיות לאומיות" (National Infrastructure Protection Plan" – NIPP)[42] שיישמה את תהליכי הארגון שצוינו לעיל וקבעה את המשרד להגנת המולדת כגוף המתאם וקובע המדיניות להגנה על תשתיות לאומיות ומשאבים חיוניים, ובכלל זה מתאם בין הגורמים המדיניים

38 Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, p. 56.

39 "Executive Order No. 13286: Critical Infrastructure Protection in the Information Age", *The White House*, 2003.

40 "Public-Law 108-458: Intelligence Reform and Terrorism Prevention Act of 2004", *U.S. Congress*, 2004.

41 שם, פרק 6302, סעיף b1.

42 המסמך מחייב הערכת מצב עיתית, שנוסח מעודכן שלה יפורסם כל כמה שנים. מאמר זה מסתמך על גרסה מאוחרת יותר של המסמך משנת 2009: "National Infrastructure Protection Plan", *U.S. Department of Homeland Security*, 2009.

האזרחיים לגורמים הצבאיים והמודיעיניים. בתוכנית הוגדר לראשונה מרחב הסייבר כתשתית לאומית חיונית שיש להגן עליה, ולא רק ככלי תיווך שבאמצעותו תתבצע הפגיעה בתשתיות.[43]

המעבר מהחלטות מדיניות לארגון מחדש של הכוח הצבאי התרחש בשנת 2006 בעקבות המסמך "אסטרטגיה צבאית לאומית למבצעי סייבר" (National Military Strategy for Cyberspace Operations"), שנועד להגדיר את הידע הצבאי הנדרש לצורך שילובו של הצבא האמריקאי במאמצים להגן על מרחב הסייבר. המסמך הגדיר את ההקשר האסטרטגי, את הרגישויות ואת קווי המִתאר לגיבוש תוכניות פעולה ודוקטרינה ייחודית לפעילות צבאית סדורה במרחב הסייבר,[44] אך לא קבע את הקמתו של גוף פיקודי כללי ייעודי לנושא זה.

2012–2008: התפיסה המרחבית

תקופה זו מהווה את שיאו של השינוי המוסדי בארגון הפעלת הכוח האמריקאי בממד הסייבר. שינוי זה מתאפיין בשני עקרונות הנובעים מהגישה הרואה בסייבר מרחב בעל חשיבות צבאית: ארגון הכוח הצבאי על בסיס תפיסה מרחבית (Cyberspace); ממד הסייבר כמקור מידע ואינטראקציה חברתית ופוליטית, הדורש ניטור ופיקוח לצורך שימור הביטחון המדיני והאינטרסים הלאומיים.

את ניצני ההתייחסות של הממשל האמריקאי לאינטרנט כאל מרחב בעל מאפיינים ומורכבות ספציפיים, הדורשים התאמה ביורוקרטית ייחודית, ניתן לאתר במסמכים שליוו את הבחירות לנשיאות בשנת 2008 (אובמה מול מקיין). תשומת הלב הציבורית הפכה את המדיניות הנוגעת למרחב הסייבר, ובמיוחד את הממד הביטחוני שלה, לאחת הסוגיות המרכזיות של אותה תקופה. בעקבותיה פרסם "המרכז ללימודים אסטרטגיים ובין־לאומיים" (Center for Strategic and International Studies" – CSIS) דוח של מומחים בתחום ביטחון הסייבר שיועד לנשיא ה־44 של ארצות הברית.[45] הדוח קרא להגברת המעורבות של הממשל הפדרלי במרחב הסייבר ויצא נגד הגישה המסתמכת על הסדרה פנימית שלו בהובלת המגזר הפרטי. בין המלצות הדוח הייתה גם קריאה ליצירת מאזן הרתעה מול יריבים בתחום הסייבר.

43 שם, סעיף 3.2.5.

44 "The National Military Strategy for Cyberspace Operations", *U.S. Office of the Joint Chiefs of Staff*, 2006, p. 1.

45 "CSIS Commission on Cybersecurity for the 44th Presidency: Securing Cyberspace", *Center for Strategic and International Studies*, 2008.

בשנת 2009, עם תחילת כהונתו, פרסם ממשל אובמה מדיניות חדשה בתחום הסייבר תחת הכותרת "Comprehensive National Cyber Initiative" (CNCI).[46] מטרותיה המוצהרות של התוכנית היו להניע מהלך בין־סוכנותי נרחב במטרה לשפר את תחושת הביטחון במרחב הסייבר בקרב אזרחי ארצות הברית.[47] במסגרת זו הצהירה התוכנית על שינוי ארגוני באופן ניהול ההתמודדות עם האיומים בסייבר, תוך חלוקה לשני מאמצים מרכזיים: שיפור הריכוזיות באופן שיעלה את רמת השליטה והבקרה המדינית בממד הסייבר; תכנון אסטרטגי וניהול שותפויות עם גורמים בין־לאומיים בתחום זה. שיפור הריכוזיות בא לידי ביטוי בפיתוח טכני של מערכות שליטה ובקרה על רשתות המידע והמחשוב הפדרליות.[48] התכנון האסטרטגי בא לידי ביטוי בהקמת מוסדות לפיתוח ורכש לטווח ארוך שימנעו, בין השאר, חדירה של רכיבי חומרת מחשב נגועים, ובקביעת יעדים לחינוך של עובדי הממשל למודעות להגנה מפני איומי סייבר.[49] שותפויות בין־לאומיות כוננו עם גורמים שונים בזירה הגלובלית (מדינות, חברות וארגונים) במטרה ליצור יכולת הרתעה בתחום הסייבר.[50]

הצורך בתכנון אסטרטגי קבוע וסדור, מרמת מוסד הנשיאות ומטה, מצא ביטוי בשורת מסמכים שנכתבו בתחילת כהונתו של ממשל אובמה, ובכלל זה במסמך יסוד שפורסם תחת הכותרת "Cyberspace Policy Review". המסמך המליץ על כינון משרד לביטחון בסייבר (The Cybersecurity Office) כחלק מצוות היועצים של הנשיא ובשילוב עם "המועצה לביטחון לאומי".[51] ההמלצה יושמה בחוק משנת 2009 "United States Information and Communications Enhancement – Act"[52] – שגם קבע כי בראש המשרד לביטחון בסייבר יעמוד יועץ הנשיא לביטחון

---

46 התוכנית הייתה למעשה יישום של החלטה NSPD54 של הנשיא בוש, אותה אימץ הנשיא אובמה. נכללו בה חלק מההמלצות של דוח CSIS. ראו: "Comprehensive National Cybersecurity Initiative", *U.S. White House*, 2009, http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.

47 מכיוון שהתוכנית הייתה יישום של החלטה NSPD54, שהייתה חשאית בעיקרה והתמקדה על פי הפרסומים גם במהלכים ביטחוניים התקפיים ומודיעיניים, ניתן להניח שהיו לה גם מטרות לא גלויות.

48 "Comprehensive National Cybersecurity Initiative", pp. 2-3.

49 שם, עמ' 4–7.

50 שם, עמ' 5.

51 "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure", *U.S. White House*, 2009, p. 7.

52 הרקע לחוק היה שימוע שנערך בסנאט בשנת 2008 על יכולות ההגנה על תשתיות ה־IT הפדרליות והביקורת שנמתחה על חוק FISMA מ־2002, שבבסיסה עמדה הטענה שהמדדים שהוא מציב לבדיקה עמומים וכי לא ברור לכול סוכנות מה היקף המידע עליו היא אמורה לפקח: "Information and Communications Enhancement Act of 2009 (S.921/ ICE Act)", *U.S Congress*, Sec. 2/4, 5.

קיברנטי, שישמש כחלק מצוות היועצים המצומצם שלו.[53] חשיבות הקמתו של המשרד לביטחון בסייבר הייתה בשיפור התיאום ויכולת המימוש של מדיניות ביטחונית כוללת מרמת הנשיא (המפקד העליון של כוחות הצבא האמריקאי), דרך סוכנויות הביטחון השונות ועד ליחידות הצבא, ובמיוחד ביכולת לגבש מדדים לפיקוח שיתבססו על פיתוח סטנדרטים לאבטחה במרחב הסייבר בכלל, ובמערכות מידע לאומיות בפרט.[54]

תוצאה משמעותית נוספת של המהלך ליצירת ריכוזיות בתחום הסייבר הייתה שיפור היכולת לגבש מדיניות להפעלת כוח לגיטימית בסייבר. זאת, כפועל יוצא של מדיניות תגובה סדורה שבראשה עומד הנשיא, על בסיס דוח של "המועצה המדעית הלאומית של ארצות הברית" ("U.S. National Science Council"),[55] שניתח את המשמעויות המשפטיות והאתיות של התקפות סייבר והמליץ כי התקפות כאלו ייחשבו כ"שימוש בכוח", דהיינו פעולה המצדיקה מענה מלחמתי (בממד הפיזי).[56]

הביטוי המשמעותי ביותר לשינוי הארגוני־תפיסתי שחל בארצות הברית ביחס לצורך להתמודד עם האינטרנט כמרחב הוא בשינוי בארגון הכוח הצבאי ובדוקטרינה להפעלתו. השינוי הארגוני הבולט בכוח הצבאי האמריקאי, המבטא את התאמתו להכרה בקיומו של מרחב סייבר, הוא ההקמה הרשמית של "פיקוד הסייבר של ארצות הברית" (CYBERCOM). ההחלטה על הקמת הפיקוד התקבלה בשנת 2009, והוא הוכרז כמבצעי שנה אחר כך והוכפף תחת "הפיקוד האסטרטגי של צבא ארצות הברית" (STRATCOM).[57] הפיקוד החדש הוגדר כ"תת־פיקוד אחוד" (Sub-Unified/Subordinated Command), כלומר גוף צבאי המוקם בהוראת הנשיא, כפיקוד המופקד על משימה מרחבית מוגדרת הדורשת התמחות מקומית, ופועל תחת פיקוד מרחבי של הצבא האמריקאי.[58]

יחידות ללוחמה באמצעות מחשבים ורשתות תקשורת ממוחשבות כבר היו קיימות בארצות הברית מאז שנות התשעים של המאה הקודמת (ראו ההתייחסות לעיל ליחידה 609), אך הקמת תת־פיקוד מרחבי לצורך זה ביטאה שינוי תפיסתי בעל משמעויות סמליות וארגוניות עמוקות. מבחינה ארגונית, למרות שעדיין

53 שם, פרק 3552.

54 שם, פרק 3556.

55 הדוח המקיף נכתב על ידי ועדה ייעודית לנושא, שהוקמה על ידי "המועצה המדעית הלאומית של ארצות הברית", והוא מנתח היבטים רבים נוספים הקשורים לתקיפות מקוונות, בתחום המשפט הפלילי והאזרחי.

56 "Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities", *U.S. National Science Council*, 2009, pp. 33-34.

57 "U.S. Cyber Command Fact Sheet", *U.S. Department of Defense*, 2010.

58 תתי־פיקוד מרחביים נוספים בצבא האמריקאי הוקמו לניהול הביטחון באלסקה, לסיוע לקוריאה הדרומית וללחימה באפגניסטן: "Joint Publication 1", *U.S. Office of the Joint Chiefs of Staff*, 2009, p. V-9.

לא הוקם פיקוד מרחבי מלא או זרוע/חיל למבצעים בתחום הסייבר,[59] הפיקוד הצבאי החדש הוא היום הגורם המנחה והמסנכרן את כלל המבצעים הצבאיים של ארצות הברית במרחב הסייבר, וכפופות אליו מבחינה מקצועית מפקדות ללוחמה מקוונת בזרועות ובחילות השונים (ים, אוויר, יבשה, נחתים). בנוסף לכך, "פיקוד הסייבר של ארצות הברית" אחראי לאיתור ופיתוח כוח האדם ואמצעי הלחימה ולגיבוש הדוקטרינה בתחום הסייבר. להקמת הפיקוד ניתן הד תקשורתי ובין־לאומי נרחב, והוא הפך לסמל מבחינת האופן הברור והגלוי שבו המחישה ארצות הברית למדינות אחרות את השלב המתקדם בו היא נמצאת במיליטריזציה של מרחב הסייבר. מעמדה זה של ארצות הברית כמעצמה צבאית מובילה (ואולי אף יחידה) בתחום הלחימה בסייבר הביא לשינויים ארגוניים דומים בקרב צבאות של מדינות נוספות ברחבי העולם (כמו, למשל, הקמת פיקוד הסייבר הסיני בשנת 2010).[60]

את השינוי הארגוני, ששיאו היה הקמת "פיקוד הסייבר של ארצות הברית", ליווה וייתכן שאף הוביל שינוי בדוקטרינה הצבאית, שפורסם במסמכים רשמיים של המטות המשולבים של ארצות הברית. אמנם, ההכרה במרחב הסייבר כמרחב שבו מתבצעת לחימה במקביל ובנוסף למרחבי הלחימה הקיימים החלה עוד בשנת 2006, אך נראה כי הידע שנצבר לא הבשיל לכדי דוקטרינה סדורה עד לפרסום עיקרי הדוקטרינה החדשה בשנת 2012,[61] שמטרתה הייתה מתן הנחייה אחודה לצבא האמריקאי כיצד לבצע מבצעי לחימה הגנתיים והתקפיים במרחב הסייבר.[62]

רמת הבשלות הגבוהה בפיתוח אמצעים, בהכשרת כוח אדם ובניסוח תורת לחימה ייחודית למרחב הסייבר, אליה הגיע הממסד הביטחוני האמריקאי מאז הקמת הפיקוד, נחשפה בהוראה הנשיאותית מספר 20 של הנשיא אובמה משנת 2012, העוסקת בפעילות התקפית בתחום הסייבר, לרבות "הגנה אקטיבית".[63] המסמך, המסווג "סודי", פורסם בעיתון הבריטי *The Guardian* כחלק ממצגות ומסמכים

---

59 הפיקודים בצבא האמריקאי נחלקים לפיקודים מרחביים האחראים להפעלת הכוח באזורים שונים בעולם (למשל, פיקוד המרכז, CENTCOM, המופקד על המזרח התיכון), ולפיקודים פונקציונליים־ייעודיים האחראים על בניין כוח, הכשרה והקצאת כוחות (למשל, פיקוד הכוחות המיוחדים, SOCOM). תחת סוג שני זה של פיקודים גם ניתן למנות את החילות ה"קלאסיים", כגון אוויר, ים ויבשה.

60 Tania Branigan, "Chinese Army to Target Cyber War Threat", *The Guardian*, July 22, 2010.

61 "Joint Publication 3-13 Information Operation", *U.S. Office of the Joint Chiefs of Staff*, 2012.

62 "Compendium of Key Joint Doctrine Publications", *U.S. Office of the Joint Chiefs of Staff*, 2014.

63 "Presidential Policy Directive 20: U.S. Cyber Operations Policy", *U.S. White House*, 2012.

סודיים שחשף והדליף אדוארד סנאודן,[64] והוא מהווה עדות משמעותית לשינוי המוסדי שעברה מערכת הביטחון האמריקאית ביחסה לתקשורת מתֻווכת מחשב, עד לראייתה כמרחב פעילות. ההוראה הנשיאותית כוללת הגדרות מפורטות של סוגי תקיפות ומהלכי הגנה בסייבר, ובהם: הגנת רשתות פסיבית; פעילות סייבר התקפית; מבצעי השפעה בסייבר; איסוף מודיעין מתוך או באמצעות מרחב הסייבר; לוחמת סייבר לצורך הגנה; פעולות הגנה לא פולשניות; פעולות סייבר לחירום ועוד.[65] ההוראה מתייחסת לכך שכבר קיימות יכולות התקפיות מוכחות של ארצות הברית, אותן היא מפעילה כחלק מיישום זכותה להגנה עצמית, וזאת לאחר תהליך קפדני של אישורים.[66]

שינוי תפיסתי וארגוני נוסף שהחל בתקופה זו, מעֵבר לתפיסת הסייבר כמרחב מקביל למרחבים פיזיים, היה תחילתה של התייחסות אל מרחב הסייבר גם כאל זירה חברתית־ציבורית מרכזית, המגלמת בתוכה פוטנציאל שלילי וחיובי ודורשת ניטור והגנה. להגדרת מרחב הסייבר כתשתית העומדת בפני עצמה, שאינה רק מרחב המתווך בין אינטרסים במרחב הפיזי, נוספה בשנת 2010 הגדרה חדשה, כחלק מתוכנית המדיניות של המשרד לביטחון המולדת, שנקראה "Securing the Nation's Critical Cyber Infrastructure". תוכנית זו התייחסה אל מרחב הסייבר כזירה חברתית פוליטית וכלכלית העומדת בפני עצמה, שבתוכה נכללים מדינות, גורמי פשיעה, ארגוני טרור ויחידים.[67]

העיסוק הביטחוני באינטראקציה החברתית במרחב הסייבר השפיע גם על עדכון הדוקטרינה של צבא ארצות הברית שעסקה בהוצאה לפועל של מבצעי תודעה (Information Operations). במסמך דוקטרינרי גלוי משנת 2012 נאמר כי הסייבר הוא מרחב חיוני לקיומם של מבצעי תודעה, כחלק ממאמץ צבאי מתמשך,[68] וכי הוא נתפס כאחד הערוצים להשפעה על "סביבת המידע". זאת, הן ביכולת לעשות בו או דרכו שימוש כדי לשבש ולמנוע מסרים, והן ביכולת להחדיר מסרים או לבצע הונאה, תוך שימוש במדיה חברתית.[69] הפיכתו של מרחב הסייבר לחלק

64 אדוארד סנאודן הוא עובד לשעבר של סוכנויות המודיעין האמריקאיות CIA ו־NSA, שהתמחה במודיעין מקוון. סנאודן הדליף בשנת 2012 כמות גדולה של מסמכים לגורמי תקשורת מובילים בעולם. המסמכים חשפו את עומק האיסוף המודיעיני והפעולות האקטיביות שנוקטות ארצות הברית ובעלות בריתה (קהילת המודיעין המשותפת לבריטניה, קנדה, ניו זילנד ואוסטרליה) במרחב הסייבר.

65 "Presidential Policy Directive 20: U.S. Cyber Operations Policy", pp. 2-4.

66 שם, עמ' 4–11.

67 "Securing the Nation's Critical Cyber Infrastructure" *U.S. Department of Homeland Security*, 2010, pp. 7-10.

68 "Joint Publication 3-13: Information Operations", *U.S. Office of the Joint Chiefs of Staff*, 2012, p. III.

69 שם, עמ' II–9.

מתחומי הפעולה של הצבא האמריקאי מתברר גם מאופן ההתייחסות אליו במצגות רשמיות של הפיקודים המרחביים של צבא ארצות הברית, שם הוא מוצג כחלק בסיסי מתפיסת הפעולה האופרטיבית.[70]

לצד זאת, ארצות הברית מכירה בכך שמבחינה ארגונית, היכולת לפעול במרחב הסייבר הציבורי־אזרחי אינה בלעדית לה, ולכן עליה לשתף פעולה עם גורמים תת־מדינתיים ועל־מדינתיים, ובעיקר עם חברות ייעוץ ותוכנה מקומיות ובין־לאומיות, המהוות שותף ומקור מידע לצורך שיפור האבטחה במרחב הסייבר, כפי שעולה גם מהמלצות של ועדות ודוחות רשמיים שונים בארצות הברית.[71] כך, למשל, מהמלצות אלו עולה כי למרות התמורות הארגוניות שהובילו להכשרת כוח אדם צבאי וממשלתי ייעודי לתחום הסייבר, עדיין נותרו תחומים שבהם ישנו יתרון לגורמים חיצוניים שאינם צבאיים, וכי אין לארצות הברית יכולת לגשר על פער זה בתקופה הקרובה, ולפיכך עליה להסתמך על היתרון היחסי של גורמים חיצוניים אלה. מדובר במיוחד בתחומים כגון זיהוי פורֶנזי, שניכר כי עדיין לא נמצא להם פתרון בדרג המדינתי.[72]

בניין הכוח בסייבר כביטוי לשינוי תפיסתי ארגוני

בפברואר 2016 פרסם הנשיא אובמה מאמר דעה בעיתון *Wall Street Journal*, בו טען כי יש להגדיל את ההשקעה התקציבית של ארצות הברית בפיתוח טכנולוגיות להגנה בסייבר, בדגש על תשתיות של מערכות מידע ממשלתיות.[73] פרסום המאמר הקדים במעט את החלטת הממשל האמריקאי להגדיל את ההוצאות על פיתוח טכנולוגיות אלו ב־19 מיליארד דולר.[74] התפיסה המוצגת במאמר של אובמה מייצגת גישה הפוכה לתהליך שתואר במאמר זה, והיא רווחת עדיין בקרב רבים ממקבלי ההחלטות בארצות הברית, וככול הנראה גם במדינות נוספות. במוקדה נמצאת ההנחה כי הגברַת הפיתוח הטכנולוגי והשקעת משאבים נוספים בו הן

70 למשל, במצגת קונצפטואלית לא מסווגת שהוכנה עבור גנרל מולטון, ראש מרכז התכנון והמבצעים של הפיקוד האירופי של צבא ארצות הברית, להצגה במכללה לקצינים של צבא היבשה: "The Operational Art of Fighting In and Through Cyberspace (Unclassified PP presentation)", *U.S. European Command*, Slide 12.

71 "CSIS Commission on Cybersecurity for the 44th Presidency: Human Capital Crisis in Cybersecurity", *Center for Strategic and International Studies*, 2010, p. VIII.

72 למשל, פעילות וירוס נחשפה על ידי חברות מסחריות המתמחות בכך, כגון מעבדות קספרסקי ואחרות.

73 Barak Obama, "Protecting U.S. Innovation from Cyberthreat", *Wall Street Journal*, February 9, 2016, http://www.wsj.com/articles/protecting-u-s-innovation-from-cyberthreats-1455012003.

74 Tobias Naegele, "7 Keys to President Obama's 19 Billion Cybersecurity Plan", *GOVTECH Works*, February 16, 2016, https://www.govtechworks.com/7-keys-to-obama-19-billion-cybersecurity-plan/#gs.iMSThHM.

המזוֹר לקשיים הגוברים של ארצות הברית לספק ביטחון במרחב הסייבר ולהגן על תשתיות לאומיות ומשאבים חיוניים. למרות שמאמר הדעה של אובמה מתייחס לכך שהגישה הארגונית המרחבית יושמה על ידי בכירי מערכת הביטחון והצבא האמריקאיים, נראה כי גם היום אין זו התפיסה הרווחת בקרב כלל מקבלי ההחלטות בארצות הברית.

הדיון שלהלן יעסוק בחלופה להשקעה עיקרית בפיתוח הטכנולוגי, לעומת החלופה להשקעה גם בפיתוח ארגוני, ויעמוד על המשמעויות האפשריות של שתי החלופות. אף שאין מדובר בסקירה השוואתית, יש בדיון זה ערך להבנת עמדתן של מדינות אחרות החותרות להשגת יתרון ביטחוני במרחב הסייבר ונוקטות גם הן מדיניות של העדפת הפיתוח הטכנולוגי על פני פיתוח הארגון והתפיסה.

כפי שצוין, מחקרים בתחום לימודי הביטחון והיחסים הבין־לאומיים שנעשו בשנים האחרונות עסקו רבות בהתפתחות צורת הלחימה בסייבר, באסטרטגיה המדינתית הרצויה במרחב זה ובאמצעי הלחימה למימושה.[75] לכן, יש לחזור ולשאול מהי החשיבות של התמקדות בשינוי הארגוני והתפיסתי בעת הזאת לעומת ההתמקדות בפיתוח טכנולוגי, ובאופן ספציפי: מהי דרך ההתארגנות המיטבית להשגת יתרון ביטחוני במרחב הסייבר ומהי התרומה שבתיאור תהליך זה להבנה ולשיפור היכולת של מדינות להעניק ביטחון לאזרחיהן אל מול האיומים הגלומים בממד הסייבר?

בפתח המאמר צוין כי בעת הזו יש להתמקד בארגון הכוחות הפועלים להחיל ביטחון במרחב הסייבר ולבנות את תפיסת ההפעלה שלהם על בסיס הגישה הצבאית האמריקאית, הרואה בסייבר מרחב לחימה מקביל למרחבים הפיזיים. הצורך בהתמקדות זו נעוץ בשני גורמים משלימים: התעצמות האיומים הנובעים ממרחב הסייבר והשינויים שחלו בהם; המאפיינים הטכנולוגיים הייחודיים של אמצעי הלחימה במרחב הסייבר.

באשר לגורם הראשון – השינוי בתפיסת האיום – הדוגמאות מתוך שלוש התקופות שתוארו לעיל ממחישות את השינוי הארגוני שחל בממסד הביטחוני האמריקאי כביטוי להפנמה גוברת של עומקו ומהותו של האיום הגלום במרחב הסייבר על מדיניות הביטחון בכלל ועל יכולת הפעלת הכוח הצבאי בפרט. מקור השינוי הוא במעבר מתפיסת מרחב הסייבר כמערכת להעברת מידע אל תפיסתו כמרכיב מהותי בחיים המודרניים: מאיום על מידע מדינתי רגיש וחשאי מטבעו (מידע

---

75 ראו, למשל, הדיון על יכולת ההתגוננות מול מתקפות סייבר, תוך ניצול תקשורת מחשב המשמשת מכשירים ("האינטרנט של הדברים"): Bruce Schneier, "Security and the Internet of Things", *Schneier on Security*, 2016, https://www.schneier.com/blog/archives/2017/02/security_and_th.html; וכן הדיון על יכולת ההרתעה בסייבר: Nye, "Deterrence and Dissuasion in Cyberspace", pp. 44-71.

מדיני רשמי, מודיעין, ידע טכנולוגי וכדומה) מצד מדינות אחרות או פרטים, שניתן להגדירו כחלק מ"אבטחת מידע", לאיום על התשתיות הבסיסיות ומשאבי היסוד של המדינה המודרנית הנשענים על תשתיות מידע ממוחשב, שניתן להגדירו כחלק מהגנה על תשתיות ואתרים אסטרטגיים ("הגנה אזרחית"), וממנו לאיום מרחבי ("מרחב הסייבר") המשיק ומשפיע על חלק גדול מהפעולות האזרחיות והצבאיות של מדינות במרחבים הפיזיים, שניתן להגדירו כאיום על ריבונות המדינה וקיומה ועל האינטראקציה הבין־אישית – כלכלית, פוליטית וחברתית – קרי, על ביטחון החברה והציבור. השימוש האנושי המגוון במרחב הסייבר, המהווה חלק משמעותי בהתקשרות חברתית, כלכלית ופוליטית, אינו מאפשר עוד להתמקד בהגנה על תשתיות מדינתיות באמצעות פיתוח טכנולוגי בלבד (כפי שמשתמע מהצהרתו של הנשיא אובמה). לעומת זאת, תפיסה הרואה במרחב הסייבר מרחב פיזי מאפשרת הגדרת יעדים ומטרות לפעולה שמכילים את מגוון האינטראקציות הללו.

הגורם השני הוא, כאמור, הייחודיות הטכנולוגית של אמצעי הלחימה במרחב הסייבר, הנובעת ממהירות ההתפתחויות הטכנולוגיות בתחום זה ומזמינותם של אמצעי הלחימה בשוק הפרטי. הצורך לעדכן חומרה ותוכנה בקצב מהיר במערכת המחשב הביתית גורם תסכול לרבים, לא כל שכן כשמדובר בביטחון המדינתי בתחום הסייבר: התפתחות אמצעי הלחימה והריגול הממוחשבים, הניתנים לרכישה בקלות יחסית במגזר הפרטי, יחד עם פשטות הפעלתם,[76] פוגעות ביכולת של מדינות להשיג יתרון טכנולוגי באמצעות פיתוח אמצעי לחימה חדשים. מערכות הפיתוח המדינתיות מתקשות להתמודד עם קצב הפיתוח והזמינות של אמצעים דומים בשוק הפרטי, ולכן פיתוח בלבד אינו יכול להיות הדרך היחידה או אף העיקרית להשגת יתרון בתחום זה. מאפיין ייחודי זה הוא שמוביל למסקנה שיכולת השליטה וההגנה על ביטחון מרחב הסייבר לא יכולה להתבסס רק על שכלול טכנולוגי של אמצעי לחימה, אלא חייבת לכלול גם את ארגון הכוח ופיתוח תפיסה ודוקטרינה להפעלתו, באופן שישלב אותן עם הפעולות הצבאיות הנוספות של המדינה להגברת הביטחון ולשימור הריבונות. גישה זו דומה להתארגנות ליצירת ביטחון במרחבים פיזיים, כגון ארגון הכוח האווירי להגנה על המרחב האווירי. ההקבלה המוצגת במאמר זה בין המרחב הווירטואלי ובין המרחב הפיזי – בין תחום הנתפס כחדש ומהפכני לבין צורת הפעולה "הישנה והשמרנית" – היא חלק מהפתרון הנדרש.

מהסקירה לעיל עולה כי הגישה הארגונית המרחבית היא למעשה הגישה אותה מיישמת הביורוקרטיה הביטחונית (במיוחד הצבאית) האמריקאית. הביטוי המעשי לה הוא כינון ממסד ביטחוני ייעודי רחב ואיתן במרחב הסייבר, הכולל כוח אדם ייעודי רב הפועל באופן הירכי – מרמת משרד היועץ במטה הנשיא, דרך יחידות

76 סוגיה זו כבר זכתה להכרה על ידי הממשל האמריקאי. ראו, למשל: "Securing the Nation's Critical Cyber Infrastructure", p. 3, Figure 1.

צבאיות וכלה במערך פיקוד צבאי ושליטה לאומי (US-CERT), תוך תיאום עם יחידות שיטור וחטיבות במשרד להגנת המולדת ועם גופים סמי־ממשליים המגשרים בין האוכלוסייה האזרחית (NIAC, NCSC), כולל המגזר העסקי והאקדמיה (ISAC), ובין הממשל. צעדים אלה מעידים על הפנמת חשיבותו של מרחב הסייבר לצורך הגנה והשפעה על ציבורים שונים. הפנמה זו הובילה, כאמור, גם לשינוי במאפייני הפעלת הכוח בסייבר – מפעולות להשגת מידע רגיש שיאפשר יכולת פיתוח, פעולה או הרתעה באמצעות "כוח קשה" קינטי או אחר, לאיום ב"כוח רך", המשפיע על תודעת היריב, על הלגיטימציה לחופש הפעולה הצבאי והביטחוני שלו, ואף על הפעולות המתקיימות בתוך מרחב הסייבר, כגון העברת מידע ממוחשב, תקשורת ופעולות כלכליות ממוחשבות.

ייתכן כי השינוי הארגוני המרחבי הוא גם אחת הסיבות להירכיה ביחסי הכוחות בין מדינות שונות הפועלות במרחב הסייבר. זאת, משום ששינוי זה הוא אחד המאפיינים הייחודיים של מעצמות כמו ארצות הברית, המהוות כוח בין־לאומי ביטחוני מוביל גם במרחב הסייבר ומסוגלות להקצות את המשאבים לארגון הפעולה הצבאית על בסיס עיקרון מרחבי. שינוי זה הוא פעולה יקרה, הדורשת משאבי כוח אדם, חשיבה וארגון שהם ייחודיים למדינות מפותחות המורגלות בהוצאה ביטחונית גבוהה. במילים אחרות, פעולות אסימטריות במרחב הסייבר, כגון טרור, חבלה, גניבת מידע, לוחמה פסיכולוגית ותקשורת מוטת "Fake News", יכולות להתבצע על ידי מדינות חלשות וארגונים שאינם מדינות. לעומת זאת, היכולת לארגן את הפעולות במרחב הסייבר כפעולות צבאיות סדורות, על בסיס הגישה הארגונית המרחבית המאפיינת את הפעולות הצבאיות במרחבים הפיזיים, היא נחלתן של מעצמות עולמיות ואזוריות ועוד מספר מדינות בעלות צבאות מודרניים עתירי טכנולוגיה. השאלה האם אנו עדים לתחרות ארגונית בין הסגנון המערבי של ארגון הכוח בסייבר באמצעות כינון מוסדות צבאיים וביטחוניים מדינתיים רשמיים, שארצות הברית היא המובילה אותו, ובין תפיסות ארגון "היברידיות", קרי מימוש פעולות סייבר התקפיות באמצעות שילוב וסנכרון מוסדות ביטחון מדינתיים וגורמים אקדמיים, המגזר הפרטי וגורמי פשיעה, אותן מובילות מדינות כגון סין ורוסיה, דורשת מחקר נוסף שחשיבותו עולה כיום, כפי שמתברר ממאמר זה.

לאור יישום השינוי בארגון הסייבר ככוח צבאי, ראוי לשאול האם ניתן לבחון אותו באותם הכלים בהם אנו מודדים את בניין הכוח הצבאי במרחב הפיזי ולהשוותו אליו? התשובה לכך אינה חד־משמעית. מצד אחד, מבחינת חישובים של עלות לעומת תועלת, ברור שלא ניתן להשוות בין העלות של פלטפורמה אווירית חדשה, הן מבחינה כספית והן מבחינת משאבי הפיתוח וההשקעה המקצועית, ובין פיתוח כלי הפעולה בסייבר; מצד שני, בשני המקרים בניין הכוח טומן בחובו צורך לפתח את היכולת להפעיל את אמצעי הלחימה בשילוב ובהלימה לאמצעי

לחימה קיימים המיועדים ללחימה במרחב אחר, וזאת באמצעות נהלים, דוקטרינה וכלים טכנולוגיים המאפשרים פיקוד ושליטה משופרים. ניתן אף לערוך השוואה היסטורית בין הדברים – בין התפתחות מערכי לחימה צבאיים במרחבי האוויר והים ובין התפתחות מערכי הלחימה במרחב הסייבר בעקבות התפתחויות טכנולוגיות. השוואה כזאת מדגישה, כאמור, את חשיבות ארגון הכוח והתפיסה המרחבית בתחום הסייבר כדרך לבסס יתרון ביטחוני בין המדינות הפועלות במרחב זה.[77]

סיכום ומסקנות

השינוי הארגוני במרחב הסייבר בארצות הברית הוביל לתוצאות בשלושה תחומים: שינוי במנעד הפעולות בסייבר; שינוי במאפייניהן של פעולות אלו; שינוי בתפיסת הפעילות במרחב הסייבר והשלכותיה על תפיסת הביטחון הלאומית של ארצות הברית והאסטרטגיה רבתי שלה.

התפתחות מנעד הפעולות הביטחוניות של ארצות הברית במרחב הסייבר, ממצב מצומצם ומוגבל שהפעילות בו נועדה בעיקר לאבטח את מרחב הסייבר הלאומי (מוסדות ואינטרסים ברורים) ולהגן עליו, למצב שבו הסייבר ערוך לפעולה התקפית, הגנתית ומודיעינית כאחת, נובעת מהשינוי הארגוני. זה הוביל להקמת יחידות, סוכנויות וארגונים בעלי אחריות מוגדרת ומכניזם לאומי לתיאום הפעילות במרחב הסייבר. למרות התפתחות זו, השינוי הארגוני אינו זוכה להכרה מספקת (לא במחקר ולא במסגרות המקצועיות), והחלטות תקציביות משמעותיות, כגון זו של ממשל אובמה, מבטאות גישה לפיה הבסיס ליצירת ביטחון ויתרון במרחב הסייבר הוא קידום השקעות בפיתוח טכנולוגי גרידא. גישה זו סותרת את ההתפתחות המשמעותית בארגון מרחב הסייבר כפי שתוארה במאמר זה ומסכנת את המשכה. היא נובעת גם מגישה ביורוקרטית הנוטה להעריך מדיניות באמצעות מדדים כמותניים (עלות לעומת תועלת), תוך התעלמות מהיבטים איכותניים, כגון יצירת תפיסה, ארגון ודוקטרינה, שהם חלק ממרכיבי האיכות המעניקים יתרון למדינות בהפעלת אמצעי לחימה בכול מרחב, ובכלל זה במרחב הסייבר.

המסקנה הסופית של המאמר היא כי במסגרת תכנון האסטרטגיה הביטחונית היום, כדאי להתייחס גם למאפיינים ולהבדלים ביכולת לארגן את הפעולה הביטחונית במרחב הסייבר בין מדינות, בדגש על מעצמות אזוריות והכוחות הביטחוניים המובילים בעולם. תהליך הארגון וביסוס תפיסת הפעולה המרחבית, המאפיין את המדיניות הצבאית האמריקאית היום, הוא חלק מיצירה וביסוס של נורמות

77 שאלה זו החלה לקבל תשומת לב של חוקרים בשנים האחרונות. ראו, למשל: עמית שיניאק, "התהוות המדינה במרחב הספר המקוון: השוואה תיאורטית והיסטורית", **בין הקטבים**, מרכז דדו לחשיבה צבאית בין־תחומית, דצמבר 2014, עמ' 13–44; Florian Egloff, "Cybersecurity and the Age of Privateering: A Historical Analogy", *Cyber Studies Programme*, Working Paper Series No. 1, University of Oxford, March 2015.

התנהלות, ואף הסכמים בין מדינות, סביב כללי המשחק במרחב הסייבר. אלה נמצאים במוקד השיח הבין־לאומי סביב מרחב הסייבר כיום, וראוי שיילמדו, ייחקרו ויהוו חלק מהערכת העלות והתועלת בפיתוח יכולות בתחום זה. הגישה הנדרשת כיום, עליה ממליץ המאמר, היא גישה ארגונית המתבססת על השוואה מסוימת בין התנהלות של מדינות במרחב הסייבר ובין התנהלותן במרחבים פיזיים. גישה זאת מאפשרת פיתוח יכולות שליטה רב־ממדיות לניהול "קרב משולב" מסונכרן ומתואם בין מרחבי הלחימה השונים – הפיזיים והטכנולוגיים – ויצירת יתרון ביטחוני במרחב הסייבר.

הארכיטקטורה הפגיעה של מערכות אוויריות בלתי מאוישות: מיפוי והתמודדות עם איומים במתקפות סייבר

גבריאל בוליאן גוביי ולירן ענתבי

כלי טיס בלתי מאוישים (כטב"מים), המכונים לעיתים קרובות בשם מל"טים (מטוסים ללא טייס), הפכו לכלי חיוני ודומיננטי בשימושם של כוחות צבא מתקדמים, בייחוד כאלה המעורבים בלוחמה אסימטרית. במקרים אלה הם משמשים בעיקר למשימות איסוף מודיעין, מעקב והכרת שטח האויב וכן לצורך מבצעים שונים המחייבים תקיפות מדויקות. ככול שגוברת ההסתמכות על מערכות בלתי מאוישות לשימושים צבאיים, כך גם עולה פגיעות הכוחות למתקפות סייבר, שהן תוצאה של התלות ההולכת וגוברת במערכות מבוססות מחשב.

מאמר זה ממפה את הסוגים השונים של מתקפות סייבר נגד מערכות אוויריות בלתי מאוישות, מעריך את הסיכויים להתרחשותן, ומציע מספר הצעות למדיניות מומלצת לאלה המשתמשים במערכות אלו.

מילות מפתח: מתקפות סייבר, אבטחת סייבר, טכנולוגיה צבאית, כלי טיס בלתי מאוישים (כטב"מים).

מבוא

התפקיד אותו ממלאים כלי טיס בלתי מאוישים (כטב"מים) בלוחמה בת זמננו התרחב מאז כניסתם לראשונה לשימוש מבצעי משמעותי בתחילת שנות השבעים

גבריאל בוליאן גוביי הוא סטודנט לתואר ראשון במשפט אזרחי בפקולטה למשפטים, אוניברסיטת מק'גיל. הוא בעל תואר שני בביטחון ודיפלומטיה מאוניברסיטת תל אביב ותואר שני במדע המדינה מאוניברסיטת אוטווה. ד"ר לירן ענתבי היא עמיתת מחקר במכון למחקרי ביטחון לאומי, מרצה באקדמיה וחברה ב־IPRAW (הפאנל הבין־לאומי לרגולציה של נשק אוטונומי). המחברים מבקשים להודות למר ניב דוד על הערותיו המועילות לטיוטה המוקדמת של מאמר זה.

של המאה העשרים.[1] כלים אלה, שהמשתמש העיקרי בהם הוא צבא ארצות הברית, מכוונים על ידי דניאל ביימן כ"נשק המועדף" על וושינגטון.[2] אופיים הבלתי מאויש, המאפשר הפעלת כוח ללא צורך במשלוח חיילים מעבר לקווי האויב וסיכון חייהם, הגביר את כוח המשיכה שלהם בעיניהם של שחקנים אחרים.[3] ואולם, המאפיין המאפשר את הפעלתם ממרחק מהווה חרב פיפיות פוטנציאלית, שכן הוא מותיר את הטכנולוגיה פגיעה לאיומי סייבר. חרף העובדה כי כטב"מים מתאפיינים ברמת מחשוב גבוהה ביותר ונהנים מן היתרון שבהיעדר נוכחותם של מפעילים אנושיים בתא הטייס, מאפיין זה הוא גם שמאפשר להאקרים לנצל את מערכות הכטב"מים.

מאמר זה מבקש להסב את תשומת הלב לפגיעויות אלו של כטב"מים. קיימת סבירות גבוהה כי אלה העושים שימוש בכטב"מים ויהיו מודעים לפגיעויות המערכת יהיו ערוכים טוב יותר למנוע מתקפות סייבר פוטנציאליות ולהתגונן מפניהן. המאמר נפתח בבחינה של המרכיבים השונים הכרוכים בהפעלה נרחבת של כטב"מים. ניתוח המערכת יאפשר לנו להבין את פגיעותם של כטב"מים למתקפות סייבר פוטנציאליות. האקרים שואפים לזכות בגישה למערכת עצמה, אך עושים זאת באמצעות שימוש במרכיב אחד שלה לפחות כנקודת כניסה לתוכה. בהמשך מפרט המאמר מתקפות סייבר נגד מערכות כטב"ם שהתרחשו בעבר, ודן בכאלו שהן סבירות מבחינה טכנולוגית. מתקפות סייבר מסוימות עשויות להתבצע על ידי האקרים בודדים, אך מתקפות מתוחכמות דורשות יכולות מתקדמות יותר וניתנות לביצוע אך ורק על ידי שחקנים המחזיקים במשאבים רבים יותר, כגון ארגוני טרור, תאגידים מסחריים או אפילו מדינות. יחד עם זאת, כפי שיפורט במאמר, אפילו מתקפות הסייבר הפשוטות ביותר עלולות להוות סיכון לגורמים המפעילים כטב"מים. המאמר מסתיים בהמלצות למדיניות המיועדת לסייע בהתמודדות עם האיומים הנובעים ממתקפות סייבר כאלו.

שאלות המחקר ומבנה המאמר

הספרות בנושא כלי טיס בלתי מאוישים, אשר קיבלה תנופה בחמש השנים האחרונות, חוקרת מספר שאלות חשובות הקשורות ספציפית לשימוש בכטב"מים לצורך חיסולים ממוקדים.[4] חלק ניכר מספרות זו ניסה לקבוע האם תקיפות כטב"מים

1 Ty McCormick, "Lethal Autonomy", *Foreign Policy*, January 24, 2014, pp.18-19.

2 Daniel L. Byman, "Why Drones Work: The Case for Washington's Weapon of Choice", *Brookings Institution,* June 17, 2013, https://www.brookings.edu/articles/why-drones-work-the-case-for-washingtons-weapon-of-choice./

3 Sarah Kreps, *Drones: What Everyone Needs to Know* (Oxford: Oxford University Press, 2016), p. 60.

4 למעשה, כטב"מים (המכונים לעיתים קרובות בשם מל"טים) נשלטים על ידי מפעיל אנושי מרחוק. מכאן שההגדרה הנכונה יותר שלהם תהיה "כלי טיס הנשלטים (או מאוישים)

המיועדות לחסל ארגוני טרור הינן אפקטיביות מבחינה אסטרטגית.[5] מחקר נוסף בחן האם דרכי השימוש בכטב"מים עומדות בסטנדרטים של החוק והאתיקה הבין־לאומיים, וזאת בניסיון להבין את ההשלכות של השימושים השונים בטכנולוגיה זאת.[6]

אף על פי כן, מעולם לא הוצגה על ידי מומחים סקירה מקיפה של המגבלות הטבועות בארכיטקטורה הטכנית של כטב"מים, למעט ההתייחסות השטחית לעובדה שכטב"מים רגישים למתקפות סייבר.[7] מטרתו העיקרית של מאמר זה היא, לפיכך, למלא חלל זה, ובכך לתרום לפתיחת דו־שיח בין הספרות האקדמית העוסקת בכטב"מים ובין המחקרים העדכניים בתחום לימודי הביטחון הצומח במהירות, קרי תחום אבטחת הסייבר.

המאמר מתחלק לשלושה חלקים. החלק הראשון מסביר את אופן פעולתם של כטב"מים ושל המערכת הגדולה יותר שהם מהווים חלק אינטגרלי ממנה. דיון זה הינו שלב נדרש בטיפול בשאלת המחקר העיקרית של מאמר זה, המוצגת בחלק השני, והיא: מהן הפגיעויות הנובעות מאופן פעולתם של כטב"מים? לאחר זיהוי פגיעויות אלו, החלק השלישי של המאמר מתמודד עם שאלה חשובה נוספת: כיצד ניתן להתמודד עם האיומים הנובעים מאותן פגיעויות? מטרתו הרחבה של המאמר, במסגרת זיהוי פגיעויות הסייבר, היא להבין כיצד הארכיטקטורה של טכנולוגיית הכטב"מים הופכת אותם לפגיעים למתקפות סייבר שונות. כל זאת,

---

מרחוק", כפי שהגדיר לאחרונה חיל האוויר הישראלי. עם זאת, בהתחשב בעובדה כי מונח זה אינו נפוץ בספרות, נעשה במאמר זה שימוש במונח המוכר יותר – כטב"ם.

5 Stephanie Carvin, "The Trouble with Targeted Killing", *Security Studies* 21 (2012); Matt Frankel, "The ABCs of HVT: Key Lessons from High Value Targeting Campaigns Against Insurgents and Terrorists", *Studies in Conflict and Terrorism* 34 (2011); Jenna Jordan, "Attacking the Leader, Missing the Mark: Why Terrorist Groups Survive Decapitation Strikes", *International Security* 38, no. 4 (2014); Avery Plaw, "Terminating Terror: The Legality, Ethics and Effectiveness of Targeting Terrorists", *Theoria: A Journal of Social and Political Theory* 114 (2007); Bryan C. Price, "Targeting Top Terrorists: How Leadership Decapitation Contributes to Counterterrorism", *International Security* 36, no. 4 (2012).

6 Grégoire Chamayou, *Théorie du drone* (Paris: La Fabrique éditions, 2013); John Kaag and Sarah Kreps, *Drone Warfare* (Cambridge: Polity, 2014).

7 Kaag and Kreps, *Drone Warfare*, pp. 44-45; Kreps, *Drones*, p. 39; Peter W. Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century* (New York: Penguin, 2009), p. 253; Peter W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2014), pp. 314-315; Robert O. Work and Shawn Brimley, *20YY: Preparing for War in the Robotic Age* (Washington, DC: Center for a New American Security, 2014), p. 23, https://s3.amazonaws.com/files.cnas.org/documents/CNAS_20YY_WorkBrimley.pdf.

במטרה להציע המלצות למדיניות, אשר יסייעו לצמצם את הסיכונים הכרוכים בשימוש בכטב"מים.

מאמר זה מתייחס לכטב"מים המסווגים על ידי צבא ארצות הברית כ"קבוצה 4" ו"קבוצה 5".[8] שתי קבוצות אלו כוללות כטב"מים שמשקלם הוא מעל 1,320 פאונד (כ־600 ק"ג) ומסוגלים לטוס בגובה של עד 18,000 רגל (כטב"מים בקבוצה 4) ומעל 18,000 רגל (כטב"מים בקבוצה 5). כטב"מים דוגמת Predator, Reaper ו־Global Hawk, הנמצאים כיום בשימוש צבא ארצות הברית, משתייכים לשתי קטגוריות אלו, ועל כן מאמר זה מתמקד בהם. כטב"מים קטנים יותר, שלצורך הפעלתם נדרש "קשר עין" ועל כן הינם בעלי ארכיטקטורה השונה מזו של קבוצות 4 ו־5, לא יידונו במאמר זה. אין פירוש הדבר שכטב"מים מקבוצות 1 עד 3 אינם פגיעים לפריצות. בניגוד לכטב"מים מקבוצות 4 ו־5, המשמשים ליעדים אסטרטגיים, כטב"מים מקבוצות 1 עד 3 משמשים לרוב במשימות טקטיות, כמו למשל ה־Raven. מכאן שסביר להניח כי הקדשת משאבים להגנה על כטב"מים מקבוצות 1 עד 3 מפני מגוון רחב של מתקפות סייבר תהיה בלתי אפקטיבית במונחי עלות, מכיוון שפעולה זו עלולה לפגוע באפקטיביות של אותם כלים, הנובעת מעובדת היותם קלי משקל, ניידים, זולים יחסית ולא מתוחכמים במיוחד. במילים אחרות, הבחירה ב־Raven היא בחירה מודעת להשתמש בכטב"ם המיועד להעניק יתרונות טקטיים מסוימים, מתוך ידיעה שאלה עלולים להצטמצם עקב הוספת מנגנון אבטחה מורכב.

יתרה מזאת, מאמר זה מתמקד באופן בלעדי בכטב"מים מקבוצות 4 ו־5 מכיוון שבניגוד לדגמים מקבוצות 1 עד 3, הם מתאפיינים ברמת מחשוב גבוהה וכוללים תתי־מערכות רבות, ההופכות אותם לפגיעים במיוחד למתקפות סייבר. כטב"מים המסווגים כקבוצות 4 ו־5 טומנים בחובם גם סיכונים רבים יותר בהתחשב בעובדה כי ניתן לציידם בטילים ולהשתמש בהם לביצוע סיכולים ממוקדים, וזאת בניגוד לכטב"מים מקבוצות 1 עד 3. כמו כן, פלטפורמות נשק מתוחכמות יותר דורשות תשומת לב מיוחדת, מכיוון שהפגיעויות שלהן כרוכות בסיכון כספי וביטחוני גבוה יותר בהשוואה לסיכון הכרוך במערכות מתקדמות פחות, דוגמת כטב"מים מקבוצות 1 עד 3. הוספת מנגנון אבטחה לכטב"מים מקבוצות 4 ו־5 תבוא באופן בלתי נמנע על חשבון הפחתת האפקטיביות שלהם (כגון במקרה של לוויינים, בו הצפנת קישור הנתונים של לוויין במטרה לאבטח את השידור של מידע רגיש מאלצת בהכרח את המפעיל להקדיש זמן רב יותר לפענוח המידע). עם זאת, עלויות אלו פחותות יחסית ליתרונות אותם הן מעניקות לאבטחה הכוללת של המערכת.

הופעתם של הכטב"מים הביאה עמה יתרונות חשובים במסגרת האינטראקטיביות הטכנולוגית של המלחמה. יתרון ברור אחד הוא הוצאתם הפיזית של חיילים משדה

8 "'Eyes of the Army': U.S. Army Roadmap for Unmanned Aircraft Systems 2010-2035", *United States Army*, 2010, p. 12.

הקרב. כמו כן, מורכבותם הטכנולוגית של הכטב"מים נסמכת על רשתות מחשבים, המכונות לעיתים קרובות בשם "מערכות אווירית בלתי מאוישות",[9] שייצורן הוא משימה טכנית מסובכת.[10] כטב"מים הם מערכות טכנולוגיות מתוחכמות יחסית, אשר בנייתן והפעלתן דורשות משאבים וידע ניכרים. יתרה מכך, הפלטפורמה המוטסת שלהם, הטסה בגובה רב יחסית, הופכת את תקיפתם באמצעים קינטיים למסובכת יותר, ומכאן שנדרשות יכולות מתקדמות יותר כדי להפילם. מסיבות אלו סביר להניח כי שחקנים המעוניינים לתקוף כטב"מים יחפשו חלופות בעולם הסייבר. מתקפות סייבר מהוות תחליף הגיוני למתקפות קינטיות, מכיוון שהארכיטקטורה של כטב"מים, כלומר הסתמכותם על מערכות ממוחשבות, הופכת אותם לפגיעים מטבעם להאקרים המבקשים לנצל את מגבלותיה של הטכנולוגיה. לכן, חשוב שגורמים העושים שימוש בכטב"מים יבינו כיצד ניתן לנצל את הטכנולוגיה שלהם, כדי שיוכלו להתמודד עם האיומים הנובעים ממנה. אינטראקציות אלו בין מפעילי כטב"מים ובין האקרים ראויות לתשומת לב מיוחדת הן במסגרות הביטחוניות והן בחוגים האקדמיים. זוהי המשימה הניצבת בפני מאמר זה.

שלושה מרכיבים מרכזיים של מערכות כטב"ם: כיצד כטב"מים פועלים?

כטב"מים הינם חלק ממערכת סבוכה המורכבת ממספר רכיבים משולבים הקשורים ביניהם, הנדרשים כולם כדי שהכטב"ם יוכל לבצע את משימות איסוף המודיעין, המעקב והכרת שטח האויב, או אפילו איתור מטרות ופגיעה בהן. אף על פי שמערכת זו מכילה מספר חלקים, מתמקד המאמר באופן בלעדי בשלושת המרכיבים העיקריים הבאים: (1) הבסיס הצבאי או מרכז הפיקוד והשליטה ממנו שולט המפעיל על הכטב"ם; (2) הלוויין המקשר בין הכטב"ם ובין מרכז הפיקוד והשליטה; (3) הכטב"ם – משמע כלי הטיס עצמו.[11] מרכיבים אלה מתבססים על מפת הדרכים של חיל האוויר של ארצות הברית, הרואה ב־Predators וב־Reapers יותר מאשר כלי טיס בלבד, ובעצם "מערכות" שלמות.

---

9 Kaag and Kreps, *Drone Warfare*, pp. 49-50.

10 Kreps, *Drones*, p. 63.

11 להמחשה ויזואלית של שלושת חלקי המערכת ראו איור 1; להמחשות גרפיות שימושיות אחרות של מערכת זו ראו: "MQ-9 Reaper", *United States Air Force Eye in the Sky*, directed by Gavin Hood (Toronto: Entertainment One, 2015); Derek Gregory, "From a View to a Kill: Drones and Late Modern War", *Theory, Culture and Society* 28, no. 7-8 (2011): 197; Ian G. R. Shaw, "The Rise of the Predator Empire: Tracing the History of U.S. Drones", *Understanding Empire*, 2014, https://understandingempire.wordpress.com/2-0-a-brief-history-of-u-s-drones/.

בסיס קרקעי נוסף, המכונה תחנת שיגור והתאוששות, חיוני אף הוא כדי שהכטב"ם יוכל להמריא לפני ביצוע המשימות ולנחות אחריהן. תחנות אלו, העשויות להיות גם נושאות מטוסים המשמשות לתדלוק ולאחסון כטב"מים כאשר אינם בשימוש, מהוות חלק מן המערכת. עם זאת, הן אינן נדונות כאן, משום שהסבירות שהן יהיו מטרה למתקפות סייבר נמוכה בהשוואה לסבירותן של מתקפות קינטיות עליהן. יתרה מזאת, כל אחד מן החלקים של מערכת כטב"ם מכיל טכנולוגיות דומות העלולות להיות חשופות למתקפות סייבר. לדוגמה, מרכז הפיקוד והשליטה מצויד במספר טכנולוגיות תקשורת המאפשרות תקשורת עם הכטב"ם, אשר כל אחת מהן עלולה לשמש מטרה נפרדת להאקרים. כפי שיידון בקצרה במאמר, גם טילים או מטען ייעודי הנמצאים על כטב"מים עלולים להוות מטרה למתקפות סייבר. אף על פי כן, אין ביכולתו של מאמר זה לדון בכול הדרכים הרבות מספור בהן ניתן לפרוץ למגוון החלקים העצום של המערכת. על כן, די אם נתעכב על שלושת המרכיבים שנזכרו לעיל במערכות הכטב"מים כדי לאפשר לקורא לזהות את נקודות החדירה העיקריות לתוך כטב"ם במקרה של מתקפת סייבר.

מרכיב 1: מרכז הפיקוד והשליטה

המרכיב הראשון של המערכת – מרכז הפיקוד והשליטה – הוא האתר הקרקעי ממנו הטייסים והמפעילים שולטים ומפקחים על המערכת מרחוק. אף על פי שמרכז פיקוד ושליטה הממוקם בארצות הברית למשל עשוי להפחית את החשיפה של הצוות לפגיעה פיזית, סביר להניח כי הוא ישמש מטרה למתקפות סייבר. מרכזי הפיקוד והשליטה מצוידים במגוון מחשבים וטכנולוגיות והינם חיוניים לצורך תפעול הכטב"מים, אך הם גם פגיעים לחדירות סייבר חיצוניות ופנימיות.

מרכיב 2: הלוויין

בניגוד לכטב"מים קטנים יותר, התלויים באות רדיו לצורך תמרונם ונשארים בדרך כלל בקו הראייה של המפעיל, הכטב"מים המסווגים על ידי צבא ארצות הברית כקבוצות 4 ו־5 תלויים בלווייניים, שהם המרכיב השני של המערכת. לווייניים אלה פועלים כמתווכים בין הכטב"מים עצמם לבין המפעילים. הם מאפשרים שידור מכלי הטיס של תמונות ונתונים הנקלטים באמצעות המצלמות והחיישנים המותקנים על הכטב"מים אל מרכז הפיקוד והשליטה, ובאופן דומה בכיוון הפוך – שידור של פקודות מן הבסיס בחזרה לכטב"מים. הלוויין ממלא חלק מכריע במערכת, משום שהוא מספק לכטב"ם ולמפעיל את המיקום המדויק שלו ומאפשר לכטב"ם לאתר את מטרתו. כמו כן, כפי שמציין איאן שואו, השימוש בלווייניים לצורך קישור בין כטב"מים לבין מפעיליהם הוא שמאפשר להגדיל באופן משמעותי את המרחק בין

שני חלקים אלה של המערכת.[12] שואו מסביר כי לפני השימוש בלווויינים, כטב"מים היו מצוידים בקישור נתונים בעל טווח קצר לצורך פיקוד ושליטה, שלא אִפשר להפעיל כטב"ם במזרח התיכון מבסיס הנמצא בארצות הברית, כפי שניתן לעשות כיום עם Predators, Reapers ו־Global Hawk.

הלוויין ממלא, אפוא, שתי פונקציות מפתח עבור הכטב"ם: הוא מהווה חלק בלתי נפרד ממערכת ה־GPS שלו, והוא משמש כערוץ התקשורת העיקרי לצורך כל תעבורת הנתונים בין כלי הטיס ובין המפעילים האנושיים. מכיוון שהלוויין משמש להעברת מידע חיוני, חיבור הנתונים העובר דרכו מהווה מטרה אסטרטגית עבור כל האקר המעוניין להפריע ולשבש את פעילותם של כטב"מים (אפשרויות אלו יידונו בפירוט רב יותר בהמשך).

מרכיב 3: כלי הטיס (כטב"ם)

המרכיב השלישי של המערכת הוא הכטב"ם – כלי הטיס עצמו. כפי שצוין קודם לכן, אחד התמריצים העיקריים לשימוש בכטב"מים הוא ההגנה על טייסים מפני פגיעה פיזית בעת פעולה בזירות לחימה שונות. מסיבה זו ניתן להפעיל כטב"מים באזורים הנמצאים אלפי קילומטרים מן המקום בו נמצאים המפעילים. ברם, העובדה שהמפעילים אינם נמצאים בתא הטייס מאלצת אותם לסמוך על הנתונים המתקבלים מן הכטב"ם. לכן, כטב"מים מצוידים גם במצלמות צמצם וגם במצלמות אינפרה אדום, המאפשרות למפעילים לכוון אותם ולעקוב אחר תוואי השטח שמתחתם גם בתנאי מזג אוויר קשים.[13] במילים אחרות, מצלמות הכטב"ם משמשות כעיניו של המפעיל, מלקטות מידע ומעבירות אותו באמצעות תמונות המופיעות על מסכי המחשב של המפעילים, המסתמכים על ההזנה האופטית הרציפה בשידור חי המופיעה בפניהם לצורך תמרון הכטב"ם. הרזולוציה הגבוהה של המצלמות המותקנות על הכטב"מים והעובדה שהתמונות מוזרמות באופן חי יוצרות מצב של פגיעות פוטנציאלית וניצול לרעה. לדוגמה, מערכות Gorgon Stare ו־ARGUS כוללות בהתאמה 12 ו־29 מצלמות ברזולוציה גבוהה, הניתנות להתקנה על כטב"מים לצורך שדרוג המצלמות הפחות מתוחכמות שלהם.[14] מכיוון שהכמות העצומה של התמונות המצולמות על ידי Gorgon Stare ו־ARGUS עלולה להציף את המפעיל האחראי על המעקב אחריהן, ייתכן שאותו מפעיל לא יוכל לדעת האם הכטב"ם הפך למטרה להאקר. מצב זה מדגיש עוד יותר את פגיעותה של המערכת.

---

12 Shaw, "The Rise of the Predator Empire".

13 שם.

14 Noah Shachtman, "Air Force to Unleash 'Gorgon Stare' on Squirting Insurgents", *Wired*, February 19, 2009, https://www.wired.com/2009/02/gorgon-/stare.

מיפוי מתקפות הסייבר הסבירות ביותר על מערכות כטב"ם

מכיוון שכטב"מים הם מכונות מורכבות מבחינה טכנולוגית, ייתכן שהדרך הקלה ביותר העומדת בפני יריב המעוניין לתקוף כטב"מים אינה להתחרות עימם, אלא דווקא לנצל את החולשה של הארכיטקטורה שלהם. יתרה מכך, ארצות הברית משתמשת בעשורים האחרונים בכטב"מים בראש ובראשונה נגד שחקנים לא מדינתיים דוגמת טרוריסטים, ובעיקר במצבים של "עליונות אווירית". בהתחשב ביתרון תחרותי זה, השחקנים השואפים לתקוף כטב"מים יגלו כי תקיפה באמצעים קינטיים הינה קשה יותר מאשר אם היו בידיהם כלי נשק מתוחכמים יותר. מכאן שחלופה סבירה עבור שחקנים לא מדינתיים היא לנצל את הארכיטקטורה של הכטב"מים, דבר אותו ניתן לעשות גם באמצעות משאבים מוגבלים ביותר (בטבלה 1 מפורטים הסוגים השונים של מתקפות סייבר העלולות להיות מכוונות נגד מערכות אוויריות בלתי מאוישות).

השתלטות מלאה על כטב"ם (כפי שהיו עושים שודדי ים לו היו מצליחים לעלות על ספינה) מחייבת מתקפת סייבר הדורשת מידה רבה של תחכום. לעומת זאת, קבלת מידה מסוימת של "גישה" לכטב"מים היא משימה לא מורכבת באופן יחסי, בהתחשב בעובדה שהיא מבוססת על הרכיבים הממוחשבים של המערכת. הרכיב הפגיע ביותר של המערכת האווירית הבלתי מאוישת הוא קשר הלוויין בין המטוסים ובין מרכז הפיקוד והשליטה עימו הם עומדים בקשר. למעשה, האקרים מסוגלים להתחבר למערכות קישור הנתונים והתקשורת של המטוסים ולנצלן כדי לגנוב מידע מודיעיני רב ערך. לדוגמה, צבא ארצות הברית תיעד מספר מקרים שבהם האקרים הצליחו להשיג גישה לסרטי הווידאו של כטב"מים מסוג Predator.[15]

15 Siobhan Gorman, Yoshi J. Dreazen and August Cole, "Insurgents Hack U.S. Drones: $26 Software Is Used to Breach Key Weapons in Iraq; Iranian Backing Suspected", *Wall Street Journal*, December 17, 2009, http://www.wsj.com/articles/SB126102247889095011.

טבלה 1: מתקפות סייבר המכוונות נגד מערכות כטב"ם והיכולות הנדרשות לצורך ביצוען[16]

סוג מתקפת הסייבר	רכיב מותקף; סוג הכטב"ם	שחקנים בעלי יכולת מינימלית נדרשת[16]	דוגמאות היסטוריות	דרכי התגוננות אפשריות
גישה לסרטי הווידאו	קישור נתוני לוויין; מל"ט סיור ותקיפה	בודדים	האקרים נגד Predators. ארצות הברית ובריטניה נגד ישראל	הצפנת קישור נתונים
גישה לסרטי הווידאו ומתקפות DoS (מניעת שירות)	קישור נתוני לוויין; מל"ט סיור ותקיפה	בודדים או ארגוני טרור	לא פורסמו עד כה	הצפנת קישור נתונים
גישה לסרטי הווידאו והחלפת סרטון בסרטון חלופי	קישור נתוני לוויין; מל"ט סיור ותקיפה	תאגידים	לא פורסמו עד כה	הצפנת קישור נתונים
שיבוש GPS (spoofing)	קישור נתוני לוויין; מל"ט סיור ותקיפה	מדינות	לכאורה, איראן נגד RQ-170 Sentinel	קריפטוגרפיה, זיהוי עיוות אות, ו/או חישת כיוון הגעה (direction-of-arrival)
פריצה למחשבים השולטים על חיבור הווידיאו	מרכז הפיקוד והשליטה	מדינות	וירוס מסוג Key logger בבסיס חיל האוויר Creech	"פער אווירי" (Airgap) סביב מרכז הפיקוד והשליטה; שימוש מוגבל בכוננים נשלפים; שימוש מוגבל בטכנולוגיות חיצוניות (לדוגמה, טלפונים חכמים או מחשבים ניידים פרטיים בקרבת או בתוך מרכז הפיקוד והשליטה)

16 קטגוריה זו כוללת ארבעה סוגי שחקנים. בסדר עולה, המבוסס על המשאבים הזמינים העומדים לרשותם לצורך ביצוע מתקפות סייבר. שחקנים אלה הם: אנשים בודדים; ארגוני טרור; תאגידים; מדינות. על הקורא לשים לב כי קטגוריה זו מהווה סף מינימום משוער. כלומר, מתקפת סייבר הניתנת לביצוע על ידי אדם בודד תוכל להתבצע גם על ידי ארגוני טרור, תאגידים ומדינות, שכן לרשות האחרונים עומדים משאבים רבים יותר בהשוואה לאנשים בודדים. יחד עם זאת, מתקפת סייבר הניתנת לביצוע על ידי מדינה ככול הנראה לא תוכל להתבצע על ידי בודדים, ארגוני טרור ותאגידים, אשר המשאבים העומדים לרשותם מעטים יותר.

פיטר סינגר ואלן פרידמן מסבירים כי ההאקרים לא נזקקו במקרים אלה ליותר מאשר למחשב נייד ול־"Skygrabber" – תוכנה שפותחה ברוסיה, שמחירה 29.95 דולר, אותה ניתן להשיג בקלות באינטרנט.[17] Skygrabber אפשרה להאקרים ליירט ולנצל תשדורות לוויין בלתי מוצפנות בין כטב"מים ובין מרכזי פיקוד ושליטה ולהשיג שעות של צילומי וידאו אותם הם שיתפו עם עמיתיהם.[18] העובדה שעלות הפריצה לקישורי נתונים של כטב"מים היא כה נמוכה, בעוד שעלות אבטחתם מגיעה למיליונים, מביאה את סינגר ופרידמן לשאול: "[האם] עולם אבטחת הסייבר מקנה עדיפות לחלש או לחזק?"[19]

מתקפת סייבר מסוג זה היא אחת מן ההתקפות הפשוטות אך המדאיגות ביותר את המשתמשים הצבאיים. היכולת לראות מה האויב עושה עשויה לספק להאקר מודיעין קריטי. לדוגמה, הגישה לסרטי וידאו של כטב"ם מאפשרת להאקר ללמוד על יכולות איסוף המודיעין של המשתמש, כולל אופיין וזהותן של מטרות, שיטות ורוטינות של איסוף מודיעין, מעקב והכרת שטח האויב. אמנם, היכולת לראות מה האויב (או הידיד) עושה אינה מאפשרת לקבוע אלו תהליכי חשיבה מתקיימים ומהי האסטרטגיה מאחורי מה שנראה לעין; עם זאת, היא מסייעת ללא ספק לצפות את הצעד האפשרי הבא של המשתמש ומאפשרת להאקר להימצא צעד אחד לפניו, ובכך היא עשויה להעניק לו יתרון מכריע בשדה הקרב.

דוגמה נוספת ומתוחכמת יותר לגישה חשאית למצלמות של כטב"ם תוארה על ידי האתר *The Intercept*. לדברי קורה קורייר והנריק מולטקה, מספר כטב"מים ישראליים, חלקם מדגמי "הרמס" ו"מחץ", נפרצו על ידי סוכנויות המודיעין של ארצות הברית ובריטניה.[20] לפי טענת השניים, הסוכנות לביטחון לאומי של ארצות הברית (NSA) וגוף התקשורת של בריטניה (GCHQ) הקימו בסיס בקפריסין לצורך יירוט האותות של כטב"מים ישראליים ואספו בהצלחה צילומי וידאו, בהם השתמשו כדי לעקוב אחר פעילותה של ישראל ברצועת עזה ובגדה המערבית. קורייר ומולטקה מוסיפים כי תוכנית סודית משותפת זו, אשר כונתה בשם "האנרכיסט", אפשרה לאמריקאים ולבריטים לעקוב אחר נתיבי הטיסה של כטב"מים ישראליים, דבר המצביע על כך שארצות הברית ובריטניה מסוגלות, קרוב לוודאי, גם לזהות את מיקומן של תחנת השיגור וההתאוששות של מרכז הפיקוד והשליטה הישראלי.

17 Singer and Friedman, *Cybersecurity and Cyberwar*, pp. 260-261.

18 Gorman et al., "Insurgents Hack U.S. Drones".

19 Singer and Friedman, *Cybersecurity and Cyberwar*, p. 260.

20 Cora Currier and Henrik Moltke, "Spies in the Sky: Israeli Drone Feeds Hacked by British and American Intelligence", *The Intercept*, January 29, 2016, https://theintercept.com/2016/01/28/israeli-drone-feeds-hacked-by-british-and-american-intelligence./

העובדה שארגונים או מדינות מסוגלים להתחבר למצלמה של כטב"ם ולראות את הדברים שהכטב"ם עצמו רואה אכן מהווה נקודת תורפה, כפי שהוסבר לעיל. עם זאת, השלכות התופעה עלולות להיות חמורות הרבה יותר אם ההאקר יצליח להתחבר לא רק למצלמה, אלא גם ללוח הבקרה של הכטב"ם. לדוגמה, די בהתקפת מניעת שירות (DoS) כדי לגרום למפעיל לאבד קשר עין עם המטרה למשך פרק זמן כזה שיאפשר למטרה להימלט. התקפת מניעת שירות כזו עלולה, בהתאם למועד התרחשותה (לדוגמה, ממש לפני ההמראה או הנחיתה של הכטב"ם), להביא גם להתרסקותו של הכטב"ם, מכיוון שמפעיל "עיוור" לא יהיה מסוגל להתחמק ממכשולים בקרבת הכלי. לארגונים לא מדינתיים עשוי להיות תמריץ חזק לבצע התקפה כזאת בשעה שהם מנסים לחמוק מכטב"ם המרחף מעליהם. ככול שמתקפת ה־DoS ארוכה יותר, יהיה לאותם גורמים זמן רב יותר לעזוב את האזור שמעליו אורב הכטב"ם.

מתקפת סייבר המכוונת לפגוע בקישור נתונים עלולה להשחית את סרטי הווידאו ולהסיט את המפעילים מנתיב הטיסה. תרחיש כזה תואר בסרטים רבים, בהם אדם בודד או ארגון פורצים למערכת מחשב ולמצלמות מעקב המחוברות למערכת כלשהי ומקרינים צילומים שונים (לעיתים מדובר בצילומים חוזרים ונשנים של אותו אתר עצמו) בהם לא מתרחש שום דבר חריג, כך שהאנשים העוקבים אחר המצלמות לא יידעו כי הם מולכים שולל. ניתן למתוח קו מחבר בין כטב"מים ובין תסריט קולנועי טיפוסי כזה, מכיוון שמצלמות של כטב"מים הן האמצעי העיקרי המאפשר למפעיל לראות מה מתרחש. לכן, אם האקר יצליח לפרוץ למצלמה של כטב"ם (כפי שממחישה הדוגמה של Skygrabber) ולשלוח סרטון וידאו שיראה כאילו הכטב"ם מרחף מעל למדבר, ייתכן שהמפעיל לא יוכל להבין כי למעשה הוא אינו רואה את מה שהכטב"ם רואה בפועל. הכוונה שגויה עלולה, בסופו של דבר, לסכן את הצלחת המשימות ואף מעבר לכך.

קישורי נתונים לוויניים הופכים את הארכיטקטורה של מערכת הכטב"ם לפגיעה מסיבה חשובה נוספת, וזאת משום שקישורים הם הערוץ המשמש להעברת נתוני GPS מן הכטב"ם למרכז הפיקוד והשליטה. במתקפות מסוג spoofing, הדומות לתסריט הקולנועי שהוזכר לעיל, יכול ההאקר לפרוץ לתשדורת ה־GPS, להנחות את הכטב"ם בנתיב שגוי ולגרום למפעיל להאמין כי הכטב"ם נמצא במקום שונה מזה שבו הוא נמצא בפועל. דוגמה בולטת למתקפת סייבר מסוג זה התרחשה ב־2011, כאשר איראן ביצעה לכאורה spoofing של מערכת ה־GPS של כטב"ם חמקן מדגם RQ–170 Sentinel. איראן טענה אז כי פרצה למערכת ה־GPS של אחד

מן הכטב"מים האמריקאיים, גרמה לו לכבות את הטייס האוטומטי שלו ושלחה לו קואורדינטות GPS שונות, אשר הובילו אותו בסופו של דבר לנחות באיראן.[21]

מומחים רבים העלו ספקות באשר ליכולתה של איראן לבצע פריצה מסוג זה.[22] יחד עם זאת, ריצ'רד לנגלי, מומחה ל־GPS, טוען כי "מבחינה תיאורטית קיימת אפשרות להשתלט על מל"ט באמצעות שיבוש קוד ה־P(Y), ובכך לגרום למַקלט ה־GPS להשתמש בקוד ה־C/A הבלתי מוצפן כדי לאתר בקלות רבה יותר את ההכוונה המגיעה מלווייני ניווט".[23] קוד ה־C/A הוא האות המשמש את כל מערכות ה־GPS לצורך שידור מידע ללווייינים. קודים אלה אינם מוצפנים, ולכן קלים יותר לפענוח. הקוד "המדויק" (קוד P) הוא גרסה עוצמתית ומדויקת יותר של קוד C/A וממלא את אותו התפקיד. ה־Y נוסף לאחר ה־P כדי לציין כי הקוד המדויק מוצפן, משום שאות מוצפן מאובטח יותר מקוד בלתי מאובטח.

אין ודאות כי ההאקר יצליח לפענח את נתוני ה־GPS המשודרים באמצעות קוד P(Y), וזאת בשל ההצפנה. אף על פי כן, יש באפשרותו לשנות את האות שלו ולאלצו לעבור לקוד C/A, שכאמור אינו מוצפן. לאחר המעבר לקוד C/A ניתן יהיה ליירט את נתוני ה־GPS הבלתי מוצפנים, כפי שקרה במתקפה שהתבססה על Skygrabber. מכאן, שגם אם איראן לא הצליחה לפרוץ ל־RQ-170 Sentinel בשנת 2011, האפשרות ששחקנים אחרים יוכלו לעשות זאת שרירה וקיימת, בתנאי שברשותם ידע טכנולוגי מספיק לשם כך. בהתחשב ברמת התחכום הנדרשת, סביר להניח כי היכולת לבצע מתקפות spoofing שמורה לקומץ שחקנים מדינתיים בלבד.[24]

"קריפטוגרפיה", "גילוי עיוות אות" ו"חישת כיוון הגעה" הם שלושת מנגנוני ההגנה המסוגלים להתמודד עם מתקפות spoofing נגד מערכות GPS.[25] פסיאקי והאמפריז מסתמכים על נתונים, אליהם הגיעו באמצעות גילוי מתקפות spoofing נגד מערכת ה־GPS של כלי שיט גדול, כדי לציין כי ייתכן שלא יהיה די במנגנוני הגנה מורכבים כאלה לצורך הגנה מפני מתקפות מסוג זה, אם השימוש בכול אחד ממנגנונים אלה ייעשה בנפרד. לעומת זאת, הפעלתם במשותף מגבירה את הסבירות להתגוננות מוצלחת.[26] אף על פי כן, ייתכן כי חלק מן המנגנונים אינם

21 Adam Rawnsley, "Iran's Alleged Drone Hack: Tough, but Possible", *Wired*, December 16, 2011, https://www.wired.com/2011/12/iran-drone-hack-gps/.

22 David Axe, "Nah, Iran Probably Didn't Hack CIA's Stealth Drone", *Wired*, April 24, 2012, https://www.wired.com/2012/04/iran-drone-hack/; Rawnsley, "Iran's Alleged Drone Hack".

23 Rawnsley, "Iran's Alleged Drone Hack".

24 Mark L. Psiaki and Todd E. Humphreys, "Protecting GPS from Spoofers is Critical to the Future of Navigation", *IEEE Spectrum*, July 29, 2016, http://spectrum.ieee.org/telecom/security/protecting-gps-from-spoofers-is-critical-to-the-future-of-navigation.

25 שם.

26 שם.

מתאימים ל־RQ–170 Sentinel או לכטב"מים חמקנים אחרים. זאת, משום שהוספת מערכות הגנה לכטב"ם עלולה לפגוע ב"חמקנות" שלו, אלא אם המערכת מצוידת באותה טכנולוגיית חמקן של כלי הטיס עצמו. אם מערכת ההגנה אינה חמקנית, היא עלולה להתגלות על ידי מערכות המכ"ם של האויב, ובכך להוציא את העוקץ ממטרתו העיקרית של הכלי.

בהתחשב בעובדה שה־RQ-170 Sentinel הוא אחד מן הכטב"מים הסודיים והמתקדמים ביותר מבחינה טכנולוגית המצויים בידי ארצות הברית, האפשרויות התיאורטיות שהובאו לעיל מדגישות עוד יותר את פגיעותה של ארכיטקטורת הכטב"מים האמריקאיים.[27] כפי שצוין, בניגוד ל־Sentinel, הכטב"מים מסוג Predator ו־Reaper עדיין אינם עושים שימוש בקישורי נתונים מוצפנים, ולכן מערכות ה־GPS שלהם רגישות עוד יותר למתקפות spoofing.

מעֵבר לערך האסטרטגי הטמון ביכולת ההאקרים לראות באמצעות מתקפות spoofing את מה שהאויב רואה, יש להם תמריץ לבצע מתקפות כאלו כאשר כטב"ם מרחף מעל אזור שהינו בעל חשיבות עבורם־הם. התמריץ הופך לחזק אף יותר במקרה של כטב"ם תקיפה, במיוחד אם ההאקר סבור כי הימנעותו מפעולה תאפשר לכטב"ם לפגוע במקום המחבוא של חמושים, עליהם מנסה ההאקר להגן. במקרה זה ייתכן כי לא יהיה די במתקפת DoS בלבד, משום שבניגוד ללוחמים חמושים המסוגלים לנסות להימלט מפני כטב"ם הרודף אחריהם, תשתית פיזית, כגון מקום מחבוא או מחנה אימונים, אינה ניתנת להעתקה בקלות ובמהירות, אם בכלל.

לא רק הנתונים המקשרים בין כטב"מים לבין מרכזי הפיקוד והשליטה הם רכיבים פגיעים בארכיטקטורה של מערכות הכטב"ם, אלא גם מרכזי הפיקוד והשליטה עצמם. אלה רגישים למתקפות סייבר מעצם העובדה שהם פועלים באמצעות מערכות מחשב בלבד. רשתות אלו מוגנות באמצעות "כיסי אוויר" (air gaps), אך הדבר לא מנע את הדבקתן בנוזקות, כפי שהוכח מחדירה של וירוס מסוג key logger למערכות המחשב הצבאיות בבסיס חיל האוויר Creech ב־2011.[28] רשת פרטית נחשבת למוגנת באמצעות "כיס אוויר" כאשר היא מנותקת מן הרשתות הציבוריות הסובבות אותה. הדבר נעשה כדי להבטיח שהרשת תהיה מאובטחת ושלא ניתן יהיה להגיע אליה באמצעות אחת מן הרשתות הציבוריות הפועלות בקרבה אליה. במילים אחרות, "כיס האוויר" מבודד את הרשת הפרטית (כלומר, הרשת בה נעשה שימוש במרכז הפיקוד והשליטה), כך שההאקר יוכל לפרוץ לרשת

27 אף על פי שבאתר האינטרנט של חיל האוויר של ארצות הברית מופיע ב־2009 דף נתונים של ה־RQ-170 Sentinel, לא פורסמו במסגרתו נתונים טכניים כלשהם על יכולותיו של כלי הטיס ומאפייניו העיקריים, וזאת בניגוד ל־MQ-1B Predator ול־MQ-9 Reaper.

28 Noah Shachtman, "Exclusive: Computer Virus Hits U.S. Drone Fleet", *Wired*, October 11, 2011, https://www.wired.com/2011/10/virus-hits-drone-fleet/.

רק באמצעות גישה פיזית למחשבים המחוברים אליה, דבר שמצמצם את הסיכוי לפגיעה בה. מכיוון שלא פורסם כל מידע פומבי על הווירוס הספציפי שתקף את בסיס חיל האוויר Creech, קשה לקבוע במדויק כיצד הוא פגע ברשת המחשבים שם, אולם הסברה היא כי הווירוס הגיע לרשת באמצעות כוננים נשלפים שהוכנסו על ידי מפעילי הכטב"מים עצמם, ומאז לא נעשה בהם שימוש בצבא ארצות הברית.[29]

אירוע זה ממחיש את פגיעותו של הגורם האנושי.[30] פירוש הדבר הוא כי אף שהמפעילים אינם נוכחים באופן פיזי בשדה הקרב, נותר בעינו הסיכון לניצולם על ידי האקרים לצורך השגת גישה בלתי מורשית למערכת. לסיכון זה עלול להיות מגוון רחב של השלכות מבצעיות: הדבקה פשוטה של הרשת באמצעות וירוס עלולה להביא להפצת מידע מסווג שנאסף על ידי כטב"מים לגורמים עוינים; מתקפת נוזקה מתוחכמת יותר מסוגלת לשלוח פקודות לא מוסמכות לכטב"ם, ובה בעת לשדר לצגים של המפעילים כי הכול פועל כשורה, באופן דומה לפעולתה של "תולעת סטקסנט" שפגעה במתקני העשרת האורניום של איראן ב־2009.[31] אף שמתקפות אלו אינן מורכבות במיוחד מבחינה קיברנטית, הן עדיין מתוחכמות למדי, משום שהן דורשות גישה פיזית למרכז הפיקוד והשליטה, דבר העשוי להתברר כמהלך מסורבל ומורכב בהתחשב ברמת האבטחה הפיזית הגבוהה סביב אתרים אלה.

אף כי מתקפות המכוונות נגד מרכזי פיקוד ושליטה הינן קשות ביותר לביצוע, כפי שהוסבר לעיל, יש להאקרים תמריצים משמעותיים לממש אותן, וזאת בהתחשב בערך האסטרטגי הטמון במתקפות מוצלחות כאלו. לדוגמה, השתלת נוזקה בעלת רמת תחכום גבוהה מאפשרת להאקר ליצור אפקט קינטי על כטב"ם תקיפה באמצעות מתן פקודה לשגר את הטילים שלו על מטרות לא נכונות. יתרה מכך, הנוזקה עלולה לגרום לטילים של הכטב"ם, הכוללים מחשבים קטנים החשופים אף הם למתקפות סייבר, לצאת מכלל פעולה או אף להתפוצץ בעודם על הכטב"ם, ובכך להרוס את כלי הטיס. העובדה שארגוני טרור חסרים לעיתים קרובות את היכולת לבצע התקפות אוויר־קרקע יוצרת להם תמריץ נוסף לבצע מתקפות סייבר, שכן אלו עשויות לאפשר להם להשיג מידה מסוימת של שליטה על המטען הייעודי של

29 שם.

30 מתקפות המתבססות על הגורם האנושי עשויות להיראות על פניהן כמתוחכמות פחות, שכן הן אינן כרוכות בידע טכנולוגי מתקדם. למרות זאת, אין להמעיט בנזק הפוטנציאלי שהן עלולות להסב. כך, תולעת הכופר WannaCry, אשר זכתה למידה רבה של הד בתקשורת כאשר הגיעה ב־12 במאי 2017 ל"עשרות אלפי" מחשבים בלא פחות מ־74 מדינות", ניצלה למעשה פגיעות במערכת ההפעלה "חלונות" של "מייקרוסופט", עבורה כבר היה קיים עדכון אבטחה מאז 14 במארס 2017, אלא שהאנשים שהמחשבים שלהם נדבקו פשוט לא טרחו להתקינו.

31 Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon", *Wired*, November 3, 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet./

הכטב"מים ולהשתמש בו כאילו היה שלהם. האפשרויות של מתקפות סייבר כאלו הן אינסופיות ולא ניתן לעסוק בהן כאן באופן מקיף. עם זאת, עצם ההיתכנות להתרחשותן אמורה להספיק כדי להתריע בפני הקורא (והכוחות העושים שימוש בכטב"מים) מפני איומים פוטנציאליים אלה.

בלי קשר לסוג המתקפה אותה ההאקרים מנסים להוציא לפועל, יש להם תמריץ ליצור נוזקות שיישארו סמויות במשך זמן רב, וזאת כדי שניתן יהיה לנצל את המערכת במשך פרק זמן ארוך ככל הניתן. גורם במשרד ההגנה של ארצות הברית ניסח זאת באופן הבא: "עבור יריב מתוחכם, יש יתרון בכך שהרשת שלכם תמשיך לפעול. הוא יכול לגלות מה אתם יודעים, הוא יכול לגרום לבלבול, לעכב את זמני התגובה שלכם ולעצב את פעולותיכם".[32] ומכיוון שכטב"מים זכו למעמד כה חשוב בצבא ארצות הברית, הפריצה לתוכם הופכת לבעלת ערך רב, ייתכן אף יותר מאשר הפלתם. במילים אחרות, ככול שכלי הנשק רב־עוצמה ואפקטיבי יותר, כך הוא יהפוך ליעד נחשק יותר עבור שחקנים שמטרתם היא לזכות ביתרונות מבצעיים.

סיכום והמלצות

כטב"מים נמצאים כיום בלב המאבק בטרור שמנהלות כמה מן המדינות המובילות בעולם, ביניהן ארצות הברית, ישראל ובריטניה. לפי שרה קרפס, המתייחסת להערכה של מכון ראנד משנת 2014, סין, הודו, איראן, רוסיה, טייוואן, טורקיה ואיחוד האמירויות הערביות מפתחות כיום כטב"מים משלהן.[33] לדבריה, "העולם הופך למוצף במל"טים, והסימנים מצביעים על כך שהם לא יישארו בהיקפם הנוכחי, אלא מספרם ילך ויגדל".[34] על כן, הנושא הופך לחשוב ולרלוונטי ביותר עבור כל המדינות המפעילות אותם במשימות צבאיות.

הפיכתן של מערכות כטב"ם לחלק בלתי נפרד מן הצבאות הסדירים הביאה לכך שאיום הסייבר הנשקף למערכות אלו הפך לתכוף יותר וממומש על ידי מגוון של יריבים. ואולם, כפי שהוסבר לעיל, לא כל היריבים מסוגלים להוציא לפועל את כל סוגי מתקפות הסייבר נגד כטב"מים. חלק חשוב בהתמודדות עם האיומים מתחיל ביצירת מודעות לקיומם – שהיא מטרתו של מאמר זה. אלא שאין די במודעות בלבד לקיומן של נקודות תורפה, וחובה לנקוט פעולות נוספות כדי לצמצם את הנזק הפוטנציאלי העלול להיגרם למשתמשים בכטב"מים כתוצאה ממתקפות סייבר.

---

32 צוטט ב: Nathan Hodge and Noah Shachtman, "Insurgents Intercept Drone Video in King-Size Security Breach (Updated, with Video)", *Wired*, December 17, 2009, https://www.wired.com/2009/12/insurgents-intercept-drone-video-in-king-sized-security-breach./

33 Kreps, *Drones*, p. 60.

34 **שם**, עמ' 160.

רצוי להתייחס לשלוש ההמלצות שלהלן כאל צעדים קריטיים שיש לנקוט כדי לטפל בפגיעויות של כטב"מים למתקפות סייבר ולחזק את מערכות ההגנה שלהם:

- השלב הראשון הוא **הערכת הפגיעות** של המערכות על ידי המדינות המשתמשות. על הערכה זו להתבסס הן על הארכיטקטורה של המערכת, הכוללת את מרכז הפיקוד והשליטה, הלוויין וכלי הטיס, והן על מודיעין בנוגע ליכולותיהם של היריבים או של גורמים אחרים שיש להם עניין לפרוץ למערכת.
- על הגורמים המשתמשים בכטב"ם ליצור פתרונות טכנולוגיים לגיבוי, אשר יתריעו או **יציינו כי בוצעה גישה למערכת** על ידי שחקן בלתי מורשה, ועל כן היא נמצאת בסכנה. בהיעדרה של מערכת התרעה כזו, לא יהיה ביכולתו של המפעיל לגלות כי מתקפת סייבר התרחשה או נמצאת בעיצומה, והסבירות כי יוכל להתגונן מפניה תפחת.
- יש להשקיע מאמצים רבים יותר ב**הצפנת קישורי נתונים המשמשים לשידור מידע** מחלק אחד של המערכת למשנהו. על המפעיל לתכנן גם שיטות התגוננות אחרות, בייחוד עבור מערכות חמושות, אף אם אלו פרוסות בזירות בהן ההערכה לקיומו של איום נמוכה יותר, שכן גם מתקפות הסייבר הפחות מתוחכמות עלולות לגרום נזק למערכת.

אין ספק כי המלצות אלו מוסיפות לעלותה של המערכת, הן מבחינה כספית והן במונחים של האפקטיביות היחסית שלה. לדוגמה, הצפנה של קישורי נתונים אמנם הופכת אותם למאובטחים יותר, אך מאריכה באופן בלתי נמנע את תהליך הפענוח. בכל מקרה, סביר להניח שהנזק הפוטנציאלי העלול להיגרם עקב מתקפת סייבר מוצלחת על מערכת כטב"ם גובר על העלויות. מודעות היא המפתח, והערכה מציאותית של פגיעויות המערכת, אשר אינה ממעיטה מן הנזק הפוטנציאלי של מתקפת סייבר בודדת המבוצעת על ידי אדם יחיד, ארגון טרור או אפילו מדינה, היא הצעד ההכרחי הראשון לקראת יצירתם של אמצעי הגנה יעילים עבור הכטב"מים.

סייבר, מודיעין וביטחון
קול קורא להגשת מאמרים לכתב העת

כתב העת **סייבר, מודיעין וביטחון** הינו כתב עת **שפיט** היוצא לאור שלוש פעמים בשנה בעברית ובאנגלית. עורך כתב העת הינו ד"ר גבי סיבוני, העומד בראש תוכנית צבא ואסטרטגיה ותוכנית ביטחון בסייבר במכון למחקרי ביטחון לאומי.
פנייה זו הינה קול קורא להגשת מאמרים ומחקרים שיפורסמו במסגרת כתב העת, על פי שיקולי המערכת.

ייבחנו מאמרים הנוגעים לתחומים הבאים:

- מדיניות גלובלית ואסטרטגיה בסייבר
- רגולציה במרחב הקיברנטי
- אבטחת החוסן הלאומי בסייבר
- לוחמת סייבר והגנה על תשתיות חיוניות
- בניין הכוח הקיברנטי על מרכיביו: המשאב האנושי, אמצעי לחימה, תורה, ארגון, הכשרה ופיקוד
- היבטים אתיים, מוסריים ומשפטיים במרחב הקיברנטי
- טכנולוגיה במרחב הקיברנטי
- הרתעה במרחב הקיברנטי
- ניתוח איומים וסיכונים במרחב הקיברנטי
- ניתוח תקריות ומשמעויות במרחב הקיברנטי
- חשיבה צבאית ואסטרטגית, הפעלת הכוח הצבאי במרחב הסייבר ומבצעי תודעה
- מודיעין, שיתוף מידע, ושותפות ציבורית־פרטית (PPP)
- שיטות מחקר, פעולה והליכים (TTPs)

ניתן לעיין במאמרים בתחומים קרובים שנכתבו בגיליונות כתב העת **צבא ואסטרטגיה**, באתר האינטרנט של המכון: http://www.inss.org.il

ייבחנו מאמרים בהיקף של עד 5,000 מילים בעברית (עד 6,000 מילים באנגלית) כולל הערות שוליים ומראי מקום. המאמרים יכללו תקציר בהיקף של 100–120 מילים ורשימת מילות מפתח בהיקף של עד עשר מילים.

להגשת מאמרים ולפרטים נוספים ניתן לפנות לח"מ.

בברכה
הדס קליין, מתאמת כתב העת **סייבר, מודיעין וביטחון**
hadask@inss.org.il

המכון למחקרי ביטחון לאומי – תוכנית ביטחון סייבר
רח' חיים לבנון 40, ת"ד 39950, רמת אביב, תל אביב 61398 | טל': 03-6400400 | פקס: 03-7447588