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.