להבין את איום הסייבר בעזרת האנלוגיה של "טרור בליסטי"

דוד שטרנברג

"אנו לא מבינים ולא מפנימים עד כמה אנו חשופים [לאיומים בעולם הסייבר] ... בעיני, הדבר דומה לטילים ... הייתי שם כשהחלו לשגר טילים בשנות השמונים. הם היו אז כלי נשק קטנים ולא מדויקים ולא נראו כאיום רציני. אבל כיום, כמעט שלושים שנה מאוחר יותר, עשויה להיות לטילים יכולת לפגוע אפילו בצלחת שעל גג בניין המטכ"ל. הדבר נכון גם לגבי תחום הסייבר. בעודנו עסוקים בהגנה על סודות הליבה, על מערכות ההגנה ועל התשתית הלאומית שלנו, אנו עשויים למצוא את עצמנו סופגים נזק רב במגזר האזרחי."

תא"ל איתי ברון[1]

איומי סייבר הם תופעה חדשה, מתפתחת ומורכבת. אחת הדרכים המרכזיות לסייע למקבלי ההחלטות להתמודד עם הקושי שהיא יוצרת היא על ידי שימוש באנלוגיות כתבניות פסיכולוגיות מפשטות. אנלוגיה שימושית כזו היא הטרור, ובמיוחד "טרור בליסטי", כפי שהוא נחווה במקרה הישראלי. כאשר נשענים על אנלוגיה זאת, ניתן להפיק ממנה שלוש תובנות: הראשונה היא כי יש מקום לשוב ולבחון הנחות יסוד מרכזיות על עתיד ביטחון הסייבר; השנייה היא האפשרות לאמץ מהמאבק בטרור אסטרטגיה היברידית לעולם הסייבר, הבנויה משישה רכיבים – הגנה, מעקב, הרתעה, הכרעה, מניעה ודיפלומטיה; השלישית, שנגזרת מאותה אנלוגיה, נוגעת להתארגנות אל מול האתגר ומדגישה את הצורך ליצור גם בעולם הסייבר תצורות מבצעיות גמישות חדשות, לצד רשת גופי שיתוף פעולה בין־לאומיים (ובעתיד אפשר שילוב בין השניים).

מילות מפתח: איום סייבר, טרור, בליסטיקה, אנלוגיה, מטאפורה, ישראל

1 Yoav Limor, "'Attacks in the Golan Heights are a Matter of Time'", *Israel Hayom*, January 16, 2005, http://www.israelhayom.com/site/newsletter_articlr.php?id=22837.

דוד שטרנברג הוא בוגר בית הספר על שם קנדי באוניברסיטת הרווארד. מאמר זה הוא גרסה מקוצרת של מחקר שנכתב במסגרת זו.

להבין תופעה חדשה בעזרת אנלוגיות ומטאפורות[2]

מחקר היחסים הבין־לאומיים מתייחס בהרחבה לשימוש באנלוגיות ככלי לקבלת החלטות.[3] הספרות בנושא זה מתבססת על חקירה של אירועים היסטוריים, המשמשים להפקת לקחים אותם ניתן ליישם על נושאים עכשוויים. יחד עם זאת, אנלוגיות ומטאפורות ניתן לאמץ וליישם לא רק על אירועים היסטוריים, אלא גם על רעיונות, נושאים, אנשים, מנגנונים ומצבים.

השימוש באנלוגיות ומטאפורות תורם היבטים פסיכולוגיים חשובים לקבלת החלטות. אנלוגיות ומטאפורות משמשות כמבני ידע לצורך עיבוד המידע והבנתו, וכן לשם השלמת נתונים חסרים.[4] תיאוריות בלשניות ופילוסופיות מדגישות את תפקידן של האנלוגיות והמטאפורות גם כאמצעי המשמש יחידים וקבוצות להבנת תופעות מורכבות ובלתי מוחשיות, ובסופו של דבר לגזור מכך פעילויות.[5]

ועדיין, ישנן סכנות בשימוש באנלוגיות ומטאפורות. האנלוגיה כמנגנון פסיכולוגי יכולה להוביל את מקבל ההחלטות לצורות עיבוד חשיבתיות פשוטות ונגישות יחסית, אך לאו דווקא נכונות. כמו כן, היא יוצרת הטיית "מסגור" שיש בה כדי להשפיע על הגישה והאופן שבהם מקבלי החלטות יתפסו את הבעיה.[6]

מדוע הנושא רלוונטי לסייבר?

זירת הסייבר היא עולם מורכב המתפתח במהירות. זוהי זירה קשה להבנה ולהמשגה בשל אופייה עתיר הטכנולוגיה, ההשפעה הרבה שיש לה על חיי היומיום, ריבוי הרכיבים המקושרים ביניהם, הדיסציפלינות השונות שמעורבות בה וקצב ההתפתחות המהיר שלה. פער דורות בין מקבלי ההחלטות, שפעמים רבות הם "חסרי אוריינות טכנולוגית", לבין אנשי המקצוע המומחים, רק מחריף מתחים אלה. אנלוגיות ומטאפורות יכולות לפשט את המכשול האינהרנטי הקיים בין שני הצדדים ולסייע בהכוונת אלה שהם בעלי ידע כללי.

---

2 אנלוגיות מוגדרות במאמר זה כהשוואה בין שתי ישויות שונות המבוססות על היבטים דומים, בעוד שמטאפורות הן השלכה של מאפיינים מישות אחת על השנייה. לצורך המחשה, " איטי כמו צב" היא אנלוגיה ואילו "שאגת האדם" היא מטאפורה.

3 Yuen Foong Khong, *Analogies at War: Korea, Munich, Dien Bien Phu and the Vietnam Decisions of 1965* (Princeton: Princeton University Press, 1992); Sean Lawson, "Putting the 'War' in Cyberwar: Metaphor, Analogy and Cybersecurity Discourse in the United States", *First Monday* 17, no. 7 (2012), http://firstmonday.org/ojs/index.php/fm/article/view/3848/3270#p2.

4 Khong, *Analogies at War.*

5 George Lakoff and Mark Johnson, *Metaphors We Live By* (Chicago: University of Chicago, 1980).

6 Daniel Kahneman and Amos Tversky, "Prospect Theory: An Analysis of Decision under Risk," *Econometrica*, 47, no. 2 (1979): 263-291.

כאשר בוחנים את שיח הסייבר העכשווי בארצות הברית, קשה שלא להתרשם מריבוי האנלוגיות המשמשות בתחום זה. ככול הנראה, יש בכך ביטוי לאתגר שהנושא טומן בחובו ולצמא להיאחז בעוגנים מוכרים בסוגיה קשה לתפיסה מבחינה אינטלקטואלית. האנלוגיות מגוונות בסוגן ובהיקפן, אולם הן מציעות פתרונות חלקיים בלבד. חלקן מציגות אירועים, ואחרות – קטגוריות של לוחמה, סוגי נשק או תהליכים היסטוריים.[7] רשימה קצרה שלהן כוללת את אירועי פרל הרבור ו־11 בספטמבר 2001, הוריקן קתרינה, "המלחמה הקרה", "דוקטרינת מונרו", "פרויקט מנהטן", דיני הים, "מלחמת בזק" (בליצקריג), "יוזמת ההגנה האסטרטגית", פרוץ מלחמת העולם הראשונה, בלקניזציה, עוצמה אווירית, לוחמה כלכלית, לוחמה ביולוגית, מערכת החיסון, הרתעה גרעינית באמצעות "הרס הדדי מובטח" (MAD), מלחמת צוללות, תופעת הפיראטיות, "מלחמות חדשנות", "התקוממות", וכן הלאה.[8]

יש הטוענים כי החלת המשגה צבאית על מרחב הסייבר אינה יעילה, שכן היא מחזקת את רעיון ה"איום" וזורעת תבהלה קבוצתית הפוגעת ביכולת לפתור בעיות באופן קולקטיבי. מטאפורות ידועות בשדה הסייבר, דוגמת "מרחב הסייבר" (cyberspace) או "ביולוגיה", לוקות גם הן בחסר. כך, הגדרות צרות כגון "מרחב הסייבר" מחמיצות את טבעו של עולם הסייבר, המשולב במרחב האמיתי, ואת הדינמיקה הבלתי ליניארית שלו. זאת ועוד, מטאפורות ביולוגיות, המתייחסות למתודולוגיות הקשורות לבריאות הציבור, למגיפות, למערכת החיסון ולרעיונות של "הסתגלות" או "הוליסטיות", מתעלמות מהמקור של הבעיה: מרחב הסייבר הוא יצירה אנושית, המשרתת רציונל חברתי־פוליטי ומתקיימת ברמה הסמנטית.[9]

הכתיבה בנושא זה בישראל פחות מפותחת מאשר בארצות הברית. עם זאת, כאשר בוחנים את השיח הציבורי בישראל, יש שימוש ברור באנלוגיות. לדוגמה, ישנם חוקרי אקדמיה המשתמשים במטאפורות מהעולם הביולוגי ("קוד מוטציה") או באנלוגיות מההיסטוריה של המלחמות, כגון התייחסות למתקפות סייבר כאנלוגיה להכנסת כטמ"מים (כלי טיס מופעלים מרחוק) לשדה הקרב.[10] חלק מהחוקרים מתייחסים לעליית הזירה האווירית כדי לתאר את תחום הסייבר

---

7 Emily O. Goldman and John Arquilla, eds., *Cyber Analogies* (Monterey: Naval Postgraduate School, 2014).

8 Robert Axelrod, "A Repertory of Cyber Analogies", in *Cyber Analogies*, eds. Emily O. Goldman and John Arquilla.

9 David J. Betz and Tim Stevens, "Analogical Reasoning and Cyber Security", *Security Dialogue* 44, no. 2 (2013): 147-164.
לניתוח מעמיק של אנלוגיית בריאות הציבור, ראו לדוגמה: Brent Rowe, Michael Halpern and Tony Lentz, "Is a Public Health Framework the Cure for Cyber Security?", *Crosstalk* (Nov/Dec 2012): 30-38.

10 Gabi Siboni, ed., *Cyberspace and National Security: Selected Articles* (Tel Aviv: Institute for National Security Studies, 2013).

החדש,[11] ואילו אחרים מעדיפים אנלוגיה של "ונדליזם" במקום מלחמה.[12] גורמים רשמיים בממשלת ישראל המבקשים להסביר את הנושא לציבור משתמשים גם הם באנלוגיות, למשל מעולם הבריאות או מתחום הבטיחות בדרכים.[13]

האנלוגיה של "טרור בליסטי"

מאמר זה עושה שימוש במונח "טרור בליסטי" כדי לתאר את הטקטיקות של המתקפות שמבצעים ארגוני טרור, ובכלל זה ירי ארטילרי של פצצות מרגמה, של רקטות קצרות טווח וארוכות טווח, של רקטות מונחות ושל טילים (כולל, למשל, טילי קרקע־קרקע, ים־יבשה, נגד טנקים, טילי שיוט, טילי כתף), וכן כטמ"מים. כאמור לעיל, נעשה שימוש בקשת רחבה של אנלוגיות כדי להבין את האתגר שמציב עולם הסייבר, ומאמר זה בוחן האם האנלוגיה של הטרור מתאימה לתיאור מתקפות סייבר. כדי להימנע מהשוואות כלליות, מתמקד המאמר במיוחד במקרה של אתגר "הטרור הבליסטי" שארגוני הטרור העמידו בפני ישראל במהלך שני העשורים האחרונים.

נוישטט ומאי הציעו בעבודתם הידועה *Thinking in Time* כי שימוש באנלוגיות ייעשה על ידי הבחנה ברורה בין הדומה ובין השונה,[14] שכן בדרך זו מקבלי ההחלטות יהיו מודעים לנקודות החוזק והחולשה של אותן אנלוגיות. מאמר זה יעשה שימוש בפרקטיקה פשוטה ואינטואיטיבית זו כדי להשוות בין ירי טילים מצד ארגוני טרור על ישראל לאיום הסייבר, תוך הצבעה על קווי הדמיון והשוני ביניהם, ובסייגים הרלוונטיים.

החלת האנלוגיה של טרור בליסטי על איומי סייבר – קווי הדמיון

מאפייני הנשק

המאפיינים של סוגי הנשק הבליסטי הם הסיבה המרכזית לכך שארגוני הטרור אימצו את הטרור הבליסטי כטקטיקה מובילה. מדובר בנשק פשוט ולא יקר: הוא בעל יכולת חדירה עמוקה לשטח האויב, וניתן להפעילו במקביל ובמרווחי זמן

11 Shmuel Even and Dayid Siman-Ṭov, *Cyber Warfare: Concepts and Strategic Trends* (Tel Aviv: Institute for National Security Studies, 2012).

12 Jonathan Silber, "Cyber Vandalism – Not Warfare", *Ynet*, January 26, 2012, http://www.ynetnews.com/articles/0,7340,L-4181069,00.html.

13 Hadas Geifman, "Dr. Eviatar Matania: 'Cyber Security is Likened to Hand Washing to Maintain Health – Important, But Not Enough'", *People and Computers*, June 26, 2012, http://www.pc.co.il/it-news/89919/ 4, (in Hebrew).

14 Richard E. Neustadt and Ernest R. May, *Thinking in Time: The Uses of History for Decision Makers* (New York: Free Press, 1986).

קצרים (נדרשות דקות ספורות מרגע ההחלטה ועד הירי בפועל). זאת ועוד, קשה להתגונן מפני סוג זה של נשק, וקשה לאתרו בשל החתימה המזערית שלו ופריסתו הרחבה. במובן זה, לנשק הסייבר יש תכונות דומות: הוא מופעל במקביל ופעולתו מיידית, לרוב הוא קל לבנייה ולשימוש, אינו יקר (בעיקר מחייב ניצול חולשות ומודיעין) ויכול בקלות לחדור דרך "נקודות עיוורות ורכות" של היריב, במיוחד בתחום האזרחי והפרטי, אולם גם במטרות צבאיות.

היבטים של ייחוס מתקפות סייבר

מרחב הסייבר מעורר קושי מרכזי במה שנוגע לייחוסו לגורם כלשהו (בעיקר בזמן אמיתי). זאת, עקב הטשטוש בין זהויות אמת ובין כתובת ה־IP הניתנת לזיהוי.[15] מצב זה מחליש את הבסיס לפעולת תגמול והרתעה, שכן תגובה שגויה עשויה להיות בלתי מדויקת ולהוביל להסתבכות, למבוכה ולנזקים שונים.

כאשר מחילים את אנלוגיית הטרור הבליסטי ברמת רזולוציה של אירוע ירי ספציפי (ולא מערכה רצופה), מופיעות שתי בעיות ייחוס דומות: הראשונה נוגעת למצב של תקרית ירי בודדת המתרחשת בין סבבים של עימות בקנה מידה גדול. במקרה זה הדילמה היא האם היריב העיקרי הוא שאחראי לירי או שמדובר בצד שלישי. זוהי בעיה מודיעינית מרכזית הקשורה לשאלה של עוצמת ההרתעה; הבעיה השנייה היא במקרה של אירוע ירי מסוים המתרחש במהלך עימות אינטנסיבי. כאן השאלה היא האם ניתן לזהות ולהפליל אתר מסוים כאחראי לשיגור. שאלה זו חשובה עקב אופי הסביבה האזרחית שבתוכה פועל ארגון הטרור. המספר הגבוה של שיגורים, האחסון והירי הנעשים מאתרים אזרחיים וממתקנים הומניטריים, הפעולה המבוזרת מבחינת פיקוד ושליטה, והתכונות של ניידות והסוואה, כל אלה תורמים לקושי בזיהוי. אין מדובר בזיהויו של אחראי־העל, אלא באדם או במקום ספציפיים הנושאים באחריות, שנגדם יש לפעול. הצורך בתגובה הולמת למקרה הספציפי מכתיבה את הצורך בייחוס ברור.

15 כמו בכול התחומים הטכנולוגיים, גם סוגיה זו משתנה במהירות. יש הטוענים כי בעיית הייחוס אינה רק טכנולוגית, אלא משתנה בהתאם לסדר הגודל של המטרה (הייחוס למטרות בעלות ערך גבוה לרוב אינו שגוי), וכן כי ייחוס הוא "אמנות": תהליך רב היבטים שמשלב הוכחות טכנולוגיות עם חשיבה מבצעית ואסטרטגית. כמו בחיים האמיתיים, התהליך אינו בינארי (נפתר/לא נפתר) ואינו מבוסס ראיות בלבד. בסייבר, כמו בתחומים אחרים, ייחוס מתבסס לא רק על ראיות פורנזיות, אלא גם על טווח רחב של מקורות מודיעין. יחד עם זאת, ייחוס בסייבר יכול לסטות מאנלוגיית הטרור הבליסטי מבחינת זמן, משאבים ותחכום היריב. עוד בנושא הייחוס ראו: Jon R. Lindsay, "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack", *Journal of Cybersecurity* 1 no. 1 (2015): 53-67; Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks", *Journal of Strategic Studies* 38 no. 1-2 (2015): 4-37.

תפקידם של גורמים לא מדינתיים ושל מדינות חסות

בלוחמת סייבר קיימת הבחנה בין פעולות סייבר שמבצעות מדינות או ממשלות לבין כאלו שמוצאות לפועל על ידי גורמים לא מדינתיים. יחד עם זאת, גורמים לא מדינתיים משמשים לעתים כזרוע או כהסוואה של מערכת לאומית, כך שהמדינה תוכל להכחיש מעורבות או להימנע מחציית הקו המהווה עילה למלחמה. תופעה דומה קיימת בשדה הטרור הבליסטי. הן מדינות (איראן לדוגמה) והן גורמים לא מדינתיים (למשל חזבאללה) השתמשו בעבר בארגונים קטנים כאמצעי עקיף לפעולה נגד ישראל.[16] בשני המקרים, גורמים לא מדינתיים עשויים לרכוש יכולות משמעותיות בדומה למדינות, או להסוות עצמם כמדינות. כפי שהוסבר לעיל, פירוש הדבר הוא סבירות גבוהה יותר לתקריות שמטרתן לעורר עימות, וסיבוך נוסף ביכולת לשלוט במצב ולמנוע הסלמה.

ערבוב של תשתיות אזרחיות וצבאיות

ייחוס שגוי עלול לגרום לטעות בזיהוי התוקף. הדוגמה הקלאסית בתחום הסייבר היא מתקפת בוט־נט שעושה שימוש בתשתית שנתפסה והוכנה מראש במטרה לשגר ממנה את המתקפה. ההשלכה המרכזית של התקפה על מחשב שנקלע להשתלטות "תמימה" היא יצירת נזק משני. כאשר תשתיות צבאיות ואזרחיות מעורבבות זו בזו, הדבר יוצר בעיה מהותית. מצב דומה שורר כאשר מתקיים ירי רקטות מצד ארגוני טרור הפועלים משכונות אזרחיות. הצד השני אך הדומה בין מתקפות סייבר ובין הטרור הבליסטי הוא המטרה המשותפת של שניהם – הסבת נזק לתשתיות אזרחיות קריטיות, ובדרך זו שיבוש השגרה האזרחית. הן רקטות מונחות שנורות על תחנת כוח והן נטרול תחנת כוח באמצעות מתקפת סייבר נועדו לעורר אימה באוכלוסייה ולזרוע חוסר ודאות, יותר מאשר לפגוע במאמץ המלחמתי הכללי.

מרכיבים של דינמיקת הסלמה

סכנת ההסלמה גדולה יותר במתקפות סייבר, משום שאלו אינן מחייבות תנועה של כוחות ואמל"ח, הן זולות, קלות למימוש ומיידיות, ובמקרים מסוימים ברגע ששוגרו הן יודעות להתפשט במרחב.[17] כמה ממרכיבים אלה נכונים גם לטרור בליסטי: כאשר מנהלים מתקפה ומתקפת נגד יש מעט מאוד זמן לקבלת החלטות. בדומה לכך, טעויות במתקפת נגד או גרימת נזק משני גבוה, דבר שהוא אופייני למלחמת טילים, יכולות להתרחש גם בעקבות שיגור מתקפת סייבר כלפי יעדים

16 Eyal Zisser, "The Return of Hezbollah", *Middle East Quarterly* (Fall 2002): 3-11.

17 מת'יו ס' כהן, צ'אק ד' פריליך, גבי סיבוני, "ארבעה עקרונות ועוד אחד: מודל חדש להגנת סייבר" (ראו מאמר בגיליון זה).

בעלי רגישות אזרחית. מהלך כזה עלול לעורר הסלמה מהירה, עקב פעולת תגמול ותגובת נקמה נגדית לפעולת התגמול. המאפיין של חתימה נמוכה שהוזכר לעיל מוסיף לערפל הקרב ולקושי להגיע לייחוס נכון.

ניתן לטעון שהשוני בקנה המידה ובקצב בין שני המקרים של טרור בליסטי ושל מתקפת סייבר הוא זה היוצר את ההבדל המהותי ביניהם: במקרה של הסייבר אין קווים אדומים ברורים או תפיסה ברורה האם יש מתקפה שהיא "חשובה יותר" או "אגרסיבית יותר" מהאחרת, כך שהשליטה על רמת ההסלמה הופכת לקשה ביותר. בניגוד לכך, בהקשר הבליסטי ניתן ליישם אמות מידה ברורות יחסית. אפשר גם לומר שבמקרה של מתקפה בליסטית ישראל יכולה להמתין עם תגובתה יום או יומיים, ולא להיגרר להסלמה הנובעת מדינמיקה של "הגנה אקטיבית". עם זאת, דומה שלמרות הקצב השונה בין מתקפות בליסטיות למתקפות סייבר, אותו עיקרון נשמר בשתיהן: אתגרים קבועים ניצבים בפני פעולות תגמול על מתקפות בליסטיות, ובאותה מידה תקריות סייבר אינן מסתיימות בהכרח בהסלמה מהירה.

גיוון הנשק

מאגר נשק הסייבר מתפרס על פני רצף הנמדד לפי מידת תחכומו. בקצה האחד נמצאות נוזקות (malware) נפוצות, שמרבית מערכות האבטחה יודעות לנטרל בזכות חתימתן המוכרת. בצד השני של הרצף נמצאים האמצעים המשוכללים יותר, היודעים לנצל חולשות ברגע התגלותן ("מתקפת אפס ימים"), לדלג בין רשתות, להסוות עצמם ולפגוע בתשתית חיונית ספציפית. בעולם הטילים קיים רצף אחר אך דומה: בקצה האחד שלו נמצאים טילים לטווח קצר או פצצות מרגמה (למרות שהניסיון מלמד שגם הם מסוכנים וקטלניים), ואילו בצד השני מצויים כלים ארוכי טווח מדויקים, כטמ"מים התקפיים, טילי שיוט וטילי חוף־ים, היודעים לתמרן בצורה שונה ומבטאים את ההתקדמות בכול הנוגע לטווחים, לדיוק ולקטלניות, וכך מחייבים חשיבה אסטרטגית ומבצעית שונה.

בעיית הרב־קושביות

למרות שכוחות חיצוניים, דוגמת איראן, רוסיה או קוריאה הצפונית, תרמו להפצת טכנולוגיות הטילים, נראה שהלחץ שהפעילה ישראל על נתיבי האספקה הביא לשינוי בתהליך זה. הלחץ הישראלי האיץ את הפיתוח של מחרטות וסדנאות הנשענות על יכולות מקומיות לייצור נשק – כפי שניתן לראות בשנים האחרונות ברצועת עזה. ההתרחבות של התעשייה המבוזרת, הנתמכת על ידי העברת ידע יותר מאשר על ידי העברת חומרים וציוד, מתפתחת לכדי איום מגוון ורב־מוקדי, בעיקר בצורה של מערכות טילים לטווחים קצרים שאינן זקוקות למוקדי אספקה.

במקביל, עולם הסייבר חולק את אותו מבנה של ריבוי שחקנים המנהלים בעצמם את המחקר והפיתוח, או לפחות את הייצור והשכלול של מערכת הנשק.

תהליך הלמידה

אחד מקווי הדמיון המרכזיים בין מתקפות סייבר ומתקפות בליסטיות הוא דינמיקת הלמידה. שלא כמו אנלוגיות מהעולם הביולוגי, מדובר בהתמודדות עם יריבים תבוניים שהאתגר שלהם הוא העברת טכנולוגיות ("טכנולוגיה טרנספורמטיבית"),[18] וזאת בשל הקושי להבין אותה מבחינה אסטרטגית. בשני המצבים, החיכוך המבצעי המתמשך מקדם את ההבנה, את אוצר המילים ואת התפיסות. בהקשר זה ניתן לציין כי אפילו התנסויות ייחודיות, דוגמת השימוש בווירוס "סטקסנט" (מתקפה על תשתית), ב"להבה" או ב־"Heartbleed", הן "טרנספורמטיביות" ומהוות חלק מרצף של למידה.

גם הטרור הבליסטי נגד ישראל רשם התקדמות שהתבססה על למידה ממשברים (כגון מלחמת לבנון השנייה), אם כי במונחים מעשיים מדובר בתהליך למידה שהיה ממושך יותר. בהקשר זה יש לציין כי המונח המשמש בעגה הצבאית להגדרת התפתחויות בשדה הטרור הוא "תחרות למידה".[19] גם במקרה הבליסטי יש מתח מובנה בלימוד והמשגת התופעה בין השקפותיהם של אנשי האקדמיה ובין האנשים בשטח,[20] בדיוק כפי שקורה במרחב הסייבר.[21]

החלת אנלוגיית הטרור הבליסטי על איומי הסייבר – קווי השוני

כחלק מההיצמדות למסגרת של נוישטט ומאי, ומתוך מודעות לכשלים קודמים, חשוב גם לעמוד על ההבדלים המרכזיים בין טרור בליסטי ובין איומי סייבר. להלן פירוט ההבדלים.

חוקי הפיזיקה מול חוקי הסייבר

כאמור, כאשר בוחנים את המאפיינים המשותפים לשני סוגי הנשק – טרור בליסטי ומתקפות סייבר – כדאי לזכור גם את ההבדלים ביניהם. מן העבר האחד ישנם טילים בעלי מאפיינים הנענים לחוקים פיזיקליים מוכרים וצפויים; מן העבר השני

18 Joseph S. Nye Jr., "Nuclear Lessons for Cyber Security", *Strategic Studies Quarterly* (Winter 2011): 19-38.

19 Brian A. Jackson, "Organizational Learning and Terrorist Groups", RAND Working Paper (2004): 27.

20 יוסי בידץ ודימה אדמסקי, "התפתחות הגישה הישראלית להרתעה – דיון ביקורתי בהיבטיה התאורטיים והפרקטיים", **עשתונות**, גיליון 8, אוקטובר 2014.

21 Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft", *International Security* 38, no. 2 (2013): 7-40.

נמצאות מתקפות סייבר, שהן נשק בעל פוטנציאל לטווח אינסופי ויכולת לשהות במערכת במשך שנים מבלי להתגלות, וכן לרכוש מאפיינים בלתי צפויים וחדשים (למשל, כאשר היריב מגלה לפתע פגיעות מהותית שלא הייתה ידועה בעבר).

דבר דומה ניתן לטעון לא רק על סוג הנשק אלא גם על הסביבה. ירי טילים, כמו גם שרשרת האספקה שלהם ופריסת המשגרים, מתנהלים בתוך מרחבים פיזיים ותחת תנאים מסוימים. הצדדים הלוחמים משתמשים בתנאים אלה כדי לאשר הישגים של היריב או להתכחש להם. לדוגמה, קיים קשר הגיוני בין טווח הטילים לבין אתרי השיגור. כדי לטוֵוח מטרות רגישות, ארגוני הטרור חייבים לקרב את הנשק לעמדות חדשות. רק הגדלת טווח הטילים משנה משוואה זאת. זה היה ההיגיון מאחורי החלטה 1701 של מועצת הביטחון של האו"ם בתום מלחמת לבנון השנייה.[22]

בניגוד לטרור הבליסטי, למרחב הסייבר יש יכולת לעבור עיצוב מחדש. דוגמה אחת לאפשרות כזו היא הוויכוח המתמשך בנוגע לשינוי הארכיטקטורה של האינטרנט ושאלת המשילות באינטרנט. הוויכוח על עקרון ה"קצה לקצה" ממחיש באופן מעשי את היכולת הפוטנציאלית להגדיר מחדש את שדה הקרב של הסייבר.

ממדי האתגר

טרור בליסטי הוא מאבק המוגבל על ידי טווח וריבונות. ישראל מתמודדת עם מספר אזורים וגורמים, בעיקר לבנון, רצועת עזה, חצי האי סיני, סוריה ואיראן. לאזורים ולגורמים אלה יש שורה של מאפיינים, כגון טופוגרפיה, גבולות, דרכים ונמלים, וכן התפלגות אתנו־דמוגרפית. גם האויבים, או לפחות האויב המרכזי, ידועים. לכן, במובן מסוים מדובר במערכת בעלת גבולות, היררכיות, קישורים ומתחים, אותה ניתן לחקור וללמוד לאורך זמן. פני השטח, היכולות והכוונות נלמדים על סמך עימותי עבר ואיסוף מודיעיני.

לעומת זאת, למתקפות סייבר יש טווח בלתי מוגבל. התוקפים יכולים להימצא במיקומים מרוחקים, להשתייך למספר גורמים, להיות בעלי סדרי גודל שונים, זהות ישנה או חדשה (כולל זהות היברידית במקרה של שיתופי פעולה), ומונעים מאינטרסים שונים. אלה יוצרים הבדל כבר מלכתחילה בכול הנוגע לשאלת הייחוס, כפי שנדונה לעיל. במקרה של טרור בליסטי, מספר האפשרויות צר יותר ושאלת הייחוס נבחנת ברזולוציה שונה.[23]

---

22 ההחלטה (מ־11 באוגוסט 2006) קבעה כי לא תורשה נוכחות של כוחות חמושים (במשתמע, חזבאללה) מדרום לנהר הליטאני, למעט יוניפי"ל וצבא לבנון. הרעיון היה למנוע פריסה של טילים קצרי טווח באזור זה.

23 כאשר שוקלים את ההשתייכויות, הגדלים, הזהויות והאינטרסים השונים של ארגוני הטרור על רקע האנלוגיה הכללית של טרור, ההבדלים מוגבלים יותר.

הֶקשר העימות

תופעת הטרור הבליסטי נחוותה בעיקר במהלך עימותים גדולים (כגון בלבנון) או בסבבים חוזרים של לחימה (כמו מול רצועת עזה ובחצי האי סיני). כחריג מכך ניתן להביא את ירי הטילים המתמשך ("טפטופים") נגד היישובים בדרום ישראל (כמו שדרות) מאז שנת 2002 ועד 2014 (ואף מעבר לכך בעצימות נמוכה יותר), כדפוס פעילות מתמשך ולא כאירוע חד־פעמי. איומי הסייבר נתפסים גם הם דרך פריזמה של משבר או אירוע מרכזי. יחד עם זאת, הם רבים יותר במספרם ובתדירותם, ומטבעם אינם בעלי דפוס של שיא ושפל. התוצאה היא שהדינמיקה של הטרור הבליסטי רגישה מאוד להקשר של העימות הספציפי, בניגוד לאיומי הסייבר. במילים אחרות, במקרה של הסייבר לא קיים "זמן שלום" לעומת "זמן מלחמה", משום שפעילות הסייבר מתקיימת באופן קבוע ובדרגות שונות של הטרדה.

הגנת "החוליה החלשה" ומתקפה "מדורגת"

מרחב הסייבר מתאפיין בכך שהוא מתקשה להגן על החוליה החלשה ביותר. גם אם ההגנה חזקה ומשוכללת במרבית הרמות, מספיקה פירצה לא מזוהה אחת כדי לאפשר את קריסת המערכת כולה. כמובן שאפשר לפתח ארכיטקטורות שנלחמות בשבריריות זו באמצעות הכנסת גורמים אנושיים או אנלוגיים לשידור, פישוטם או פירוקם.[24] עם זאת, אלה אינם משקפים את המגמות העכשוויות, שמאופיינות בתלות הדדית מוגברת ובשילוביות. תכונה ייחודית זו מובילה גם לטקטיקות מתקפה שונות, כגון מתקפה "מדורגת" (cascade-based), המנצלת תהליך של "למידה באמצעות חיכוך" כדי לגלות את נקודות התורפה.

בטרור בליסטי המצב שונה: מערכות ההגנה פועלות לפי פרמטרים סטטיסטיים וניהול סיכונים, בעוד שמאגר הטילים נבנה על תכנון ארוך טווח ועל הזדמנויות. עם זאת, יריבים עשויים לנסות לאתר במהלך עימותים נקודות "רכות" ביכולות ההגנה או ההתקפה של הצד השני. גילוי של נקודת תורפה ספציפית, גם אם אינה חלק בלתי נפרד מתפקוד כלל המערכת (כמו בסייבר), עלול להביא לשינויים דרמטיים במצב האסטרטגי. לדוגמה, ירי של כמה טילים מרצועת עזה לעבר שדה התעופה הבין־לאומי של ישראל במהלך מבצע "צוק איתן" גרם לרשויות בארצות הברית להוציא צו שאסר באופן זמני על נחיתות של מטוסים אמריקאיים בנמל התעופה בן־גוריון. חברות תעופה זרות הזדרזו ללכת בעקבות ארצות הברית. לעצירת הטיסות בפועל הייתה, למשך פרק זמן קצר, השפעה אסטרטגית[25]

24 Richard Danzig, *Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies* (Washington DC: Center for a New American Security, 2014).

25 דבר דומה ניתן לטעון לגבי תקרית אפשרית של פגיעה המונית בגן ילדים או פגיעה באתר סמלי כלשהו, באופן שעשוי לשנות לחלוטין את הדינמיקה של העימות המזוין.

תפוצת נשק

השוואה בין תהליך תפוצת הנשק של טרור בליסטי ושל לוחמת סייבר מדגישה שתי סוגיות: הראשונה היא העברת ידע פיזי לעומת העברת ידע אלקטרוני. נשק הסייבר אינו מאופיין בחומר או במטען מסוימים, אלא בנוי מביטים (bits), בתים (bytes) ונוסחאות לוגיות. הקטלניות או היעילות של נשק זה מקושרות ישירות לתכונות אחרות שהוא נושא, בעיקר המיקוד המודיעיני (כלומר, הכרת נקודות הכניסה לרשת או למערכת), נקודות התורפה שהוא מנצל, היכולת להתגבר על מערכות אבטחה והחתימה הנמוכה. לאור זאת, אפשר לייצר כלי נשק כאלה כמעט בכול הנסיבות. לעומת זאת, טילים, למרות שגם עבורם נדרש ידע מסוים (כמו כיצד לייצר מנוע טיל מתפקד או מערכת הנחיה לטווח מסוים), עדיין מחייבים העברה פיזית של חלקים וחומרים דרך גבולות או נמלים.

הבעיה השנייה היא הדרך הייחודית של תפוצת הנשק: נשק הסייבר יכול לשמש פעם אחת בלבד והופך לחסר תועלת ברגע שהוא משאיר חתימה ומזוהה.[26] תפוצתו נובעת לעתים מתהליך של למידה ואימוץ שימוש אחר מאשר השימוש המקורי שלו. לדוגמה, ברגע שקוד כמו "סטקסנט" או "להבה" מופץ בעולם, הוא הופך אוטומטית לבסיס לבניית גרסאות חדשות של אותה טכנולוגיה, ותפוצת הנשק מתבצעת למעשה באמצעות תהליכי הנדסה לאחור. בניגוד לתכונות ייחודיות אלו, טרור בליסטי נשען רבות, לפחות עד לאחרונה, על הפצת טילים ורקטות באמצעות ספקים שונים, בעיקר איראן.

תפקיד המגזר הפרטי־אזרחי בתחום הסייבר

בניגוד לנשק בליסטי, נשק סייבר הוא "כְּפול־שימוש" (דואלי), הן מבחינת אופיו (טכנולוגיות רלוונטיות) והן מבחינת התפיסה. חברות פרטיות ומגזרים אזרחיים ממלאים תפקיד חשוב הן במתקפות סייבר והן באבטחת סייבר: הם אינם רק מטרות למתקפה, אלא גם גורמים התורמים להגנה, להערכת האיום ואף לתקיפה. בנוסף לכך, לנשק הסייבר יש השפעה כלכלית גדולה לא רק כתוצאה מההרס הפיזי (כפי שקורה במתקפות טילים), אלא גם כתוצאה של מגוון פעולות אחרות, כמו גניבה של פיתוחים טכנולוגיים.

לסיכום, טרור בליסטי חולק קווי דמיון רבים עם אתגר הסייבר, אולם במקביל ישנם גם הבדלים משמעותיים ביניהם. ניתוח קווי הדמיון והשוני מעלה תמונה מורכבת. יחד עם זאת, דומה שיש בסיס טוב להשוואה בין השניים. כנקודת מוצא, חשוב לא להתייחס להבדלים בקצב, בקנה המידה ובטווח, שכן סביר להניח שאלה לא יהיו בני השוואה גם בכול אנלוגיה אחרת. במקום זאת, מוצע להסתכל על מודל הטרור הבליסטי דרך משקפיים של דינמיקות, תהליכי למידה, התפתחות

26 Siboni, ed., *Cyberspace and National Security: Selected Articles*.

איומים ויחסים. כאשר משקללים את כל אלה, קווי הדמיון בין הטרור הבליסטי לאתגר הסייבר מתחזקים במידה ניכרת.

הרחבת אנלוגיית הטרור

החלה של האנלוגיה הספציפית של "טרור בליסטי" על מתקפות סייבר מאפשרת לטעון שגם "טרור" באופן כללי יכול להיות אנלוגיה למתקפות סייבר. המאמר הנוכחי לא עוסק בביסוס טענה זו, אולם דומה שכאשר בוחנים את הדילמות המשותפות העומדות בפני מקבלי החלטות העוסקים הן במתקפות טרור והן במתקפות סייבר, יש בסיס לטענה זו.[27] המדובר, בין היתר, בדילמות הבאות:

- **בעיית ההגדרה**: אין הסכמה לגבי הגדרה אוניברסלית לתופעת הטרור, כמו גם לאיומי הסייבר.
- **אתגרים מודיעיניים**: בשני המקרים המודיעין חיוני לזיהוי, לתגמול, להפללה ולקביעת מטרות, אולם נאלץ להיאבק עם שורה של מתחים רב־ממדיים, חוצי גבולות וחוצי גופים.
- **שאלת ההרתעה**: שאלה זו מתעוררת כחלק מהתמודדות עם ארגונים חשאיים, מבוזרים, לא היררכיים ובעלי נכסים מוגבלים.
- **משקלן של טקטיקות התקפיות**: המאבק בטרור יצר מערך של טקטיקות התקפיות, המכוונות לפגוע הן ביכולת והן במוטיבציה של ארגוני הטרור. מרחב הסייבר מעלה גם הוא שאלות בנוגע לצורך, לעיתוי ולקריטריונים של מתקפות יזומות.
- **סוגיות חקיקה**: שאלות הנוגעות לקיומה של חקיקה ראשית ייחודית,[28] למידת האחידות וההתאמה של החקיקה הבין־לאומית,[29] להגדרה של מתקפה וליישום חוקים העוסקים בסיוע (תמיכה, הכשרה ומימון) לארגוני טרור קיימות גם כשדנים במתקפות סייבר.
- **הממד הציבורי והממד התקשורתי**: בשני המקרים – של טרור ושל סייבר – הכיסוי בתקשורת ההמונים מעצים את הפעולות או מנצל אותן להעברת מסרים לקהלי יעד. מצב זה מעלה שורה של דילמות בנוגע למדיניות המידע, למדיניות החינוך, לצֶנזור התקשורת ולסוגיות של אתיקה.

---

27 Boaz Ganor, *The Counter-Terrorism Puzzle: A Guide for Decision Makers* (New Brunswick NJ: Transaction, 2007).

28 זהו עיקרון המשתקף במקרה האמריקאי, דוגמת "חוק הפטריוט". החקיקה הישראלית נגד טרור לא בנויה על מקור חקיקה ראשי שעוסק ישירות בנושא, אלא נשענת על חקיקת חירום. תקנות החירום מעניקות לממשלה גמישות וכוח רבים לפעול נגד טרור, אולם הן גם נתקלות בביקורת רבה ונתונות לוויכוח.

29 Jack Goldsmith, "Cybersecurity Treaties: A Skeptical View", in *Future Challenges in National Security and Law*, ed. Peter Berkowitz (Stanford: Hoover Institution, Stanford University, 2011).

- **הצורך החיוני בשיתוף פעולה בין־לאומי**: הארכיטקטורה הדומה של הבעיה בשני התחומים – רשת בין־לאומית שמעורבים בה נותני חסות מדינתיים, ישויות הפועלות בתוך מדינות המעניקות חסות והגנה, ארגוני "שליח" (proxy) או ארגוני חזית – יצרה את הצורך במסד של נורמות וחוקים בין־לאומיים משותפים, וכן במסגרות עבודה מבצעיות ובשיתוף מודיעיני.

תובנות מרכזיות

אימוץ האנלוגיה של טרור בליסטי מאפשר לגזור ממנה שלוש תובנות מרכזיות: הראשונה נוגעת להנחות היסוד של עתיד אבטחת הסייבר; השנייה מתייחסת למרכיבים של המאבק באיום; השלישית עוסקת ברמה הארגונית ובצורך לגבש תצורות מבצעיות גמישות חדשות, וכן גופי שיתוף פעולה בין־לאומיים.

נוישטט ומאי הציגו את השאלה "האם אנלוגיה מסוימת ממשיכה להתאים גם כאשר בוחנים מצב חדש?". בחינה מחודשת של חיבורם *Thinking in Time* מאפשרת לקבוע כי אין די בכך שאנלוגיה תהיה "מתאימה", אלא שעליה גם ללמד אותנו דבר מה בנוגע להנחות היסוד ולאי־הבהירות שנלוות לתיאור הסוגיה האסטרטגית.

ניתוחם של מורן וסוּלק[30] מאפשר להשתמש באנלוגיית הטרור הבליסטי כדי לחקור ולבחון חמש הנחות, או שאלות יסוד, לגבי אבטחת הסייבר. ההנחות הן:

- "למדינות יש יכולת לשמור על עליונות במרחב האינטרנט". כאשר בוחנים את אנלוגיית הטרור הבליסטי במקרה הישראלי, אין ספק שישראל שומרת על עליונות במרחב האווירי שלה לפחות מאז שנות השמונים של המאה העשרים. למרות זאת, הטרור הבליסטי, שנתפס תחילה כלא מתוחכם, הפך עד מהרה לגורם אסטרטגי היוצר איזון חלקי עם עליונות ישראלית זו, או למצער מאתגר אותה.
- "מדינות לאום הן איום חמור יותר מאשר גורמים לא מדינתיים". בעולם הבליסטי, הנחה זו תלויה כמובן בסוגיית ההתחמשות (קונבנציונלית או לא קונבנציונלית). נכון להיום, מדובר בעיקר בהבחנה בין יכולות של מדינה ובין יכולות של גורם לא מדינתי. עם זאת, כשמוציאים את הנשק הלא קונבנציונלי מהתמונה, ומניחים כי הן כוח הירי והן הדיוק, הקטלניות והטווח (המכסה את כלל שטח ישראל) של אלה הנמנים על מחנה הקיצונים (איראן, סוריה, חזבאללה וחמאס) הפכו למרכיבים בני השוואה, אזי דומה שגם גורמים לא מדינתיים מחזיקים ברשותם כוח משמעותי. לכן, כמו בהנחה הראשונה, גם הנחה זו צריכה לעבור עדכון.

30 David Sulek and Ned Moran, "What Analogies Can Tell Us about the Future of Cybersecurity", *The Virtual Battlefield: Perspectives on Cyber Warfare* no. 3 (2009): 118-131.

- "עד כמה חמור האיום?". סוגיה זו עוררה ויכוח גדול בזירה האקדמית והציבורית הדנה בסייבר. הספקנים (ויימן, ליביצקי, גרצקה, מנקן, ריד ואחרים)[31] רואים הגזמה באיום הסייבר ומפקפקים ביכולת שלו לגרום נזק רציני וקבוע למדינות, כזה שיגרור עלויות צבאיות ונזק פוליטי. המחנה השני (קאר, קלארק, קלו ואחרים), המשקף את הלך הרוח בקרב אנשי המקצוע, גורס שהאיום שמציבות מתקפות הסייבר הוא אמיתי, מִתחזק ומהיר יותר מאשר אמצעי ההגנה מפניו ותורות ההתגוננות שפותחו נגדו.[32] לדעתם, מתקפות סייבר התגלו כמשמעותיות בתחום הצבאי (כגון בעימותים עם רוסיה באסטוניה ובגיאורגיה) והמחישו היטב את הפוטנציאל לקריסה מאסיבית של תשתיות (כמו במקרה של "סטקסנט"). לעומת זאת, במקרה של טרור בליסטי, למרות שהוא מביא לאובדן רכוש וחיי אדם ולמרות הפוטנציאל שלו לגרום אבדות גדולות הרבה יותר, אי אפשר שלא לתהות האם לא מדובר בפגיעה מוגבלת בהרבה ביחס לציפיות ולהשקעה בהתגוננות, והאם תהליך קבלת ההחלטות התבסס על הנחת "הגרוע מכול".[33] בהתאם לכך, היו שקראו לשים את הדגש במאבק בטרור הבליסטי על פתרונות התקפיים במקום על התגוננות.[34] עם זאת, ובמבט לאחור, מרבית השיח רואה בהחלטה של ישראל להשקיע במערכת הגנה רב־שכבתית הצלחה מוכחת. האנלוגיה הישראלית מחזקת אפוא את ההערכה שמרחב הסייבר מהווה איום ממשי ההולך וגדל.
- "האם הדור הבא של הטכנולוגיות והיישומים האינטרנטיים יהיה בטוח יותר?". שאלה זו עוסקת ברמות הפגיעות של תשתיות מתפתחות, וזאת בשונה מעולם הבליסטיקה. עם זאת, ניתן לטעון שהשילוב בין נשק וטקטיקות ובין המציאות הפוליטית־כלכלית המתפתחת עשוי להציג דור חדש לחלוטין של איומים. כדי להמחיש זאת בהקשר של הטרור הבליסטי, ניתן לציין כמה נושאים המעוררים חשש: הסכנה לאסדות הגז ליד אשקלון (השולטות בשמונים אחוזים מאספקת האנרגיה של ישראל) ולהובלה הימית בנמל אשדוד (המכסה שישים אחוזים מהייבוא למדינה) – שני אתרים הפגיעים לטילי חוף־ים, לכטמ"מים או לטילי שיוט; מסילת הרכבת לשדרות, החשופה לטילים נגד טנקים; הסכנה לפעילות האווירית האזרחית בעתיד (נמל התעופה בן־גוריון ושדה התעופה העתידי בתמנע).

---

31 ראו לדוגמה: Martin C. Libicki, "Cyberattacks Are a Nuisance, Not Terrorism", *Rand Blog*, February 20, 2015, http://www.rand.org/blog/2015/02/cyberattacks-are-a-nuisance-not-terrorism.html.

32 כהן, פריליך, סיבוני, "ארבעה עקרונות ועוד אחד: מודל חדש להגנת סייבר".

33 יצחק רביד, "על הנחת החמור ביותר", **מערכות** 351 (1997), עמ' 2–12.

34 Avi Kober, "Iron Dome: Has the Euphoria Been Justified?", *BESA Center Perspectives Paper* no. 199, February 25, 2013, http://besacenter.org/perspectives-papers/iron-dome-has-the-euphoria-been-justified/.

- "האם יש מספיק רצון פוליטי לשיתוף פעולה דיפלומטי בין־לאומי?". כאמור, היכולת לקבוע מסגרות משפטיות נורמטיביות נראית חלשה. מקרה הטרור הבליסטי ממחיש זאת דרך כישלון יישומה של החלטת מועצת הביטחון 1701. דומה שגם אימוץ מהלכים הדרגתיים וחלקיים נכשל. חלוקת האיום למקטעים שונים, כפי שנעשה במאמצים הדיפלומטיים שהושקעו בסוגיית הטילים הזעירים קרקע־אוויר (טזק"א – MANPADS), במזכר ההבנות הבילטרלי בין ישראל לארצות הברית בנושא מניעת הברחות נשק לחמאס (מינואר 2009), בהחלטה 1747 של מועצת הביטחון של האו"ם (ממארס 2007) האוסרת על יצוא והעברה של נשק מאיראן, או בהסכמי הפסקת אש, התגלתה כהישג זמני, לא מספק או בלתי ניתן לאכיפה. זאת, עקב אינטרסים ועדיפויות מנוגדים (סין ורוסיה בולמות פעילות במועצת הביטחון של האו"ם), אזורים שאין בהם שליטה ריבונית (לוב, לבנון, סיני) ומדינות סוררות. הלקח האפשרי שניתן להפיק מניסיון הטרור הבליסטי הוא שיש להשקיע הון פוליטי, בעיקר בשיתופי פעולה המתבססים על תפיסות זהות, וכן בפעולות חד־צדדיות למניעה ולהרתעה.

מאסטרטגיית "ארבעת ה־D" לאסטרטגיית "ששת ה־D"

"האסטרטגיה הלאומית למאבק בטרור", עליה הכריזה ממשלת ארצות הברית בפברואר 2003, כללה "ארבעה D" להתמודדות עם אתגר הביטחון הגדול של המילניום החדש. ארבעת היסודות היו Defeat – הבסה של ארגוני הטרור; Deny – מניעת חסות, תמיכה ומקלט מטרוריסטים; Diminish – צמצום התנאים המעודדים טרור, משמשים קרקע פורייה לרעיונות ומובילים אנשים לאמץ טרור; Defend – התגוננות מפני מתקפות טרור.

כהן, פריליך וסיבוני מציעים ארבעה D שונים, ובוחנים את התאמתם לסוגיית איומי הסייבר.[35] הם משאירים את יסודות ההבסה וההתגוננות, אך מדגישים שני עקרונות אחרים: גילוי (Detection) והרתעה (Deterrence). במובן מסוים, ארבעת ה־D האלה הם חלק מהעקרונות של פרדיגמת הביטחון של ישראל. הניסיון בפועל של ישראל מול הטרור הבליסטי התאפיין בעקרונות הבאים: אִפחוּת (mitigation) – פגיעה במשגרים ובמתקנים; מניעה – עצירת אספקת נשק; התגוננות – מערכת הגנה רב־שכבתית; הרתעה מפני ביצוע פעולות בעתיד; דיפלומטיה – הבנות והסכמות.

כאשר בוחנים את שלוש אסטרטגיות המאבק – האסטרטגיה הלאומית למאבק בטרור של ארצות הברית, ארבעת ה־D של כהן, פריליך וסיבוני, והאמצעים שנוקטת ישראל נגד טרור בליסטי – ברור למדי שיש ביניהן חפיפה וכי הן חולקות עקרונות דומים. לדוגמה, היעד של "הבסה" (defeat) בשתי המסגרות של ארבעת ה־D, מקביל ליעד "אפחות" (mitigation) באסטרטגיה של ישראל נגד הטרור הבליסטי,

35 כהן, פריליך, סיבוני, "ארבעה עקרונות ועוד אחד: מודל חדש להגנת סייבר".

במובן זה שמדובר בגישה התקפית שמטרתה פגיעה ביכולות האויב ובמורל שלו. דבר דומה ניתן לומר על היעד "מניעה" (prevention) באסטרטגיה הישראלית נגד הטרור הבליסטי, שדומה לרעיון ה"מניעה" (Deny) בארבעת ה־D של ארצות הברית, קרי פגיעה בחימוש ובתמיכה הלוגיסטית. דוגמה נוספת היא המרכיב "גילוי" (Detection) שמציעים כהן, פריליך וסיבוני, המגולם בתוך המרכיבים של "התגוננות", "מניעה" ו"אפחות" באסטרטגיה של ישראל, שכן שלושתם לא יבואו לידי מימוש ללא "גילוי" האיום תחילה.

כהן, פריליך וסיבוני מדגימים היטב ובפירוט כיצד מרכיבים אלה משתקפים גם בתחום הסייבר. יתר על כן, ארבעת ה־D אותם הם מחילים על מתקפות סייבר, יכולים להיות מוחלים גם על אנלוגיית הטרור הבליסטי. לעומת זאת, אסטרטגיית המאבק בטרור הבליסטי כוללת שני מרכיבים בלבד הישימים לניתוח עולם הסייבר – "דיפלומטיה" ו"שלילה" (או "מניעה"). בדרך זו מתקבלת אסטרטגיה של "שישה D" ללחימה במתקפות סייבר (Defeat, Deny, Diminish, Defend, Diplomacy, Detection).

באשר למרכיב "דיפלומטיה", התייחסתי לעיל לקושי לבסס פתרונות משפטיים נורמטיביים במרחב הסייבר. עם זאת, ראוי לבחון אפשרויות ליצירת פתרונות נורמטיביים כלליים במרחב זה אצל מדינות החולקות תפיסות דומות, ובהמשך הזמן לעודד מדינות אחרות לאמץ נורמות אלו (בדומה למודל "קבוצת ספקיות הגרעין" שגובש לצורך בקרת ייצוא). שיתוף פעולה רב־צדדי בין מדינות החולקות תפיסות דומות נראה ככלי פעולה סביר ואף חיוני במציאות המשפטית המורכבת של ימינו. שיתוף פעולה כזה יכלול לא רק שיתוף בתחום המבצעי (כגון אכיפה) והמודיעיני (שיתוף מידע), אלא גם מחקר ופיתוח טכנולוגיים משותפים, וכך ישפר את יכולות הגילוי והניטור. שיתוף הפעולה הישראלי־אמריקאי בפיתוח מערכות הגנה אווירית, והצעת פתרונות אלה לשותפים נוספים, יכולים גם הם לשמש כמודל לתחום הסייבר.

באשר ל"שלילה" (המקבילה ל"מניעה"), ניתן להניח שהמרכיבים של סיוע, תמיכה ומימון היריב חלשים יותר בעולם של איומי הסייבר יחסית לזירת הטרור הבליסטי, וכי לאור זאת הם פחות פגיעים. במילים אחרות, כאשר שרשרת האספקה קצרה וצרה יותר והמערכת הסביבתית כולה פחות גלויה לעין, היריב פחות חשוף להתערבות. עם זאת, מרכיבים אחרים המצויים בידי היריב, כגון ידע, מודיעין ויכולת הסוואה, הם בעלי משמעות וניתנים לגילוי וחשיפה. דוגמה לכך בתחום הטרור הבליסטי היא תפיסתם או סיכולם של משלוחי נשק מאיראן לארגוני טרור פלסטיניים בשנים 2001, 2009 ו־2014.

סוגיה מרכזית הנמצאת על הפרק, בנוסף להכרת האסטרטגיות השונות, היא סדר העדיפויות של כל אחת מאסטרטגיות אלו. בדוגמה של הטרור הבליסטי,

ברור כי האמצעי הבולט ביותר הוא השילוב של "מניעה" ו"הגנה". פגיעה ישירה במאגרי המשגרים והטילים, השפעה באמצעות הדרך הדיפלומטית ויצירת הרתעה לא השיגו את אותן תוצאות כמו צעדי המניעה שהובילו לתפיסה ולסיכול העברות נשק בקנה מידה גדול (כמובן, לצד אמצעי ההגנה של "כיפת ברזל").

אם לשפוט את הדברים על פי כהן, פרייליך וסיבוני, נראה כי לא כך המצב בתחום הסייבר, שבו לכול האסטרטגיות שנוסו יש מגבלות משמעותיות, ודומה שאין אסטרטגיה אחת דומיננטית. אמנם, האסטרטגיות של "הגנה" ו"גילוי" מפותחות יותר מאחרות, וישראל אף מדגישה את יכולותיה בתחומים אלה,[36] אך המספר הגדול של מתקפות סייבר (יותר ממיליון במבצע "עופרת יצוקה" בלבד) יוצר אתגר גדול.[37] במילים אחרות, בניגוד לניסיון שהצטבר בלחימה בטרור הבליסטי, המסקנה המרכזית שעולה מעולם הסייבר היא שנדרשת אסטרטגיה היברידית במקום אסטרטגיה מובילה אחת.

ההיבט הארגוני

השאלה כיצד לארגן פעולת נגד בסייבר מתבססת בהכרח על המורכבות והדינמיקה של האיום. הניסיון שהצטבר ממבצעי המאבק בטרור מצביע על החשיבות שיש להקמתם ולשילובם של הגופים הנכונים במאמץ הלאומי.[38] בהקשר זה, יש לטפל תחילה בהקמתו של ארגון אסטרטגי חדש ברמה הלאומית, שיתמודד עם האתגר. כאשר בוחנים את אנלוגיית הטרור, נראה כי חקר מקרים קודמים, כגון הלמידה הארגונית בעידן שלאחר 11 בספטמבר 2001 והקמת "המרכז הלאומי למאבק בטרור" (NCTC), לצד פרקטיקות צבאיות שנעשה בהן שימוש במרחב הסייבר, עשויים לסייע בהקמת ארגונים לאומיים חדשים לצורך מאבק זה. עיקרון דומה שהביא להקמתו של ארגון חדש להתמודדות עם בעיית הסייבר ניתן למצוא, לדוגמה, ב־2009, כאשר הצבא האמריקאי הקים פיקוד משנה לסייבר.[39] גם צה"ל החל לאחרונה לבחון מהלך דומה.[40] בפברואר 2015 החליטה ממשלת ישראל לפעול

36 Yonah Jeremy Bob, "Rule of Law: Obama, Israel and Cyber Warfare", *Jerusalem Post*, March 22, 2013, http://www.jpost.com/Features/Front-Lines/The-cyber-partys-over-307367.

37 David Shamah, "Hackers Threaten 'Israhell' Cyber-Attack over Gaza", *Times of Israel*, July 9, 2014, http://www.timesofisrael.com/hackers-threaten-israhell-cyber-attack-over-gaza.

38 Bruce Hoffman and Jennifer Taw, *A Strategic Framework for Countering Terrorism and Insurgency* (Santa Monica: RAND Corporation, 1992).

39 היו כאלה, לרבות אדמירל (מיל') ג'יימס סטברידיס (המפקד העליון של נאט"ו לשעבר), שקראו להקמת זרוע סייבר חדשה בכוחות הביטחון.

40 "Election Results and the Defense Establishment", *Israel Defense*, March 19, 2015, http://www.israeldefense.co.il/en/content/election-results-and-defense-establishment.

להאחדת כוחות ואמצעים על ידי הקמת רשות סייבר לאומית. גוף זה אמור לקבל לידיו אחריות מבצעית ולהצטרף למטה הסייבר הלאומי שכבר קיים.

מבט מקרוב על הרמה הארגונית מצביע על כמה סוגיות: בזירת הטרור, לא ברור אם "המרכז הלאומי למאבק בטרור" מבַצע את המצופה ממנו, וגם הקשרים בינו לבין שאר גופי המודיעין הלאומיים בארצות הברית, כגון ה־CIA, אינם ברורים דיים.[41] גם בזירת הסייבר יש חוסר בהירות בכול מה שנוגע לפעילות מול קהילת המודיעין, אף מעבר לחוסר הבהירות הקיים בזירת הטרור. המודיעין אינו רק גורם מסייע למתקפה אלא, כפי שמוכיח הטרור הבליסטי, משולב בצד ההתקפי ובצד ההגנתי גם יחד, בשל העובדה שהגבולות בין איסוף מודיעין (ניצול הסייבר) ובין המבצעים הינם כיום מעורפלים.[42]

הניסיון הישראלי מחדד את הדילמה, משום שמערכת הביטחון של ישראל קטנה יותר בממדיה מזו של ארצות הברית ונשלטת על ידי שלושה גופים חזקים. גופים אלה לא רק נהנים מעוצמה פוליטית,[43] אלא גם יצרו אפשרות ליחסי עבודה סימביוטיים בעת הצורך ולחלוקת עבודה הכוללת רוטציה בפיקוד בהתאם להקשר.[44] כאשר מסתכלים על זירת הטרור הבליסטי, ניתן להיווכח בלקח שהפיק צה"ל, המוצא את ביטויו בקבלת אחריות מלאה על המאבק בזירה זו.[45] אין זה מפתיע שמתחים סביב שאלת הסמכויות בתחום הסייבר צצים ועולים כבר כיום.[46]

---

41 Richard A. Best, *The National Counterterrorism Center (NCTC) Responsibilities and Potential Congressional Concerns* (Washington DC, Congressional Research Service, 2011).

42 דוגמה לכך ניתן לראות בארצות הברית, שם קהילות המודיעין והמבצעים תלויות מאוד האחת בשנייה, עובדה המומחשת, בין השאר, בכך שפיקוד הסייבר וה־NSA חולקים אותו מפקד. הסיבה לסימביוזה זו נובעת מהבעיה להגדיר גבולות ברורים בין המבצעים, איסוף המידע המודיעיני והמידע הסיכולי, ובין יוזמות ותגובות התקפיות, הגנתיות ושל הגנה פעילה.

43 שניים מהם כפופים ישירות לראש הממשלה, וכך מצמצמים את הסמכות של כל גוף מקביל אחר.

44 ישראל אכן הקימה גוף מתמחה לתיאום בתחום הטרור – "המטה ללוחמה בטרור", שהוקם ב־1996, בזמן גל פיגועי ההתאבדות. אולם גוף זה אינו כולל יכולות מודיעין, מבצעים ותכנון בפועל, שנותרו בלעדית בידי זרועות הביטחון הקיימות, ובראשן שירות הביטחון הכללי (שב"כ). למידע נוסף על המבנה והמשמעות של קהילת המודיעין בישראל ראו: שמואל אבן ועמוס גרניט, **קהילת המודיעין הישראלית – לאן?** (תל אביב: המכון למחקרי ביטחון לאומי, 2009); Yosef Kuperwasser, *Lessons from Israel's Intelligence Reforms*, Analysis Paper, no. 14 (Washington DC: Brookings Institute, 2007).

45 צה"ל פיתח זרוע משולבת חזקה מול הרשויות האזרחיות בדמות פיקוד העורף, לתיאום סוגיות של הגנה אזרחית. ניסיון להפעיל גוף מקביל במסגרת משרד ממשלתי חדש, "המשרד להגנת העורף", כשל עקב מאבקים פוליטיים פנימיים בממשלה.

46 לדוגמה, מאבק שהתעורר בין השב"כ ובין מטה הסייבר הלאומי סביב שאלת האחריות להגנה על רשתות ציבוריות ואזרחיות קריטיות.

השאלה שעומדת על הפרק בסופו של דבר היא מדוע לא להפוך את ארגוני המודיעין הקיימים לכאלה שיוכלו להתמודד עם אתגר הסייבר, במקום להקים ארגונים חדשים.[47] אחת הדרכים לעשות זאת היא באמצעות התארגנות חדשה ברמה המבצעית. במילים אחרות, הדגש צריך להיות מושם לא על הסוגיה של אחדות הפיקוד, אלא על פלטפורמות שמאפשרות פעילות גמישה. בהמשך לקו מחשבה זה, ההגדרה של "כוחות מיוחדים" בהקשר של איומי טרור יכולה להיות מיושמת גם בעולם הסייבר. אחת האפשרויות יכולה להתבסס על אנלוגיית הטרור הבליסטי, שהביאה את צה"ל להקים "מרכזי אש" משולבים.[48] מבנה ארגוני זה פותח כדי לרכז את כל הכלים הדרושים לגילוי משגרי הטילים, והוא משלב יכולות שונות שנועדו להשיג גמישות וזריזות ברמה הטקטית.[49]

פלטפורמות משותפות כאלו אינן צריכות להיות מוגבלות לרמה המקומית בלבד, אלא ניתן להרחיבן לרמה הבין־לאומית. בדומה למאבק בטרור, גם אסטרטגיה לשיתוף פעולה בין־לאומי בסייבר אינה נעדרת בעיות הקשורות לאינטרסים, חוקים ושיקולים פוליטיים. עם זאת, ממשלת ישראל מכירה בחשיבות פיתוחו של תחום זה. כך, למשל, ישראל ושותפים בין־לאומיים השקיעו מאמצים במחקר ובפיתוח,[50] והתחזק שיתוף הפעולה הבין־לאומי בין גופי CERT באמצעות שימוש בכלים מיוחדים לשיתוף מידע, ללמידה משותפת ולמבצעים.[51] עם זאת, יש עדיין מקום לשפר ולהרחיב משמעותית מגמה זאת.

גורמים בכירים לשעבר במערכת הביטחון של ישראל רמזו כי שיתוף הפעולה בין ישראל לארצות הברית בתחום הסייבר אינו מיטבי, וכי יש צורך ליצור "מנגנון משותף לשילוב יכולות טכנולוגיות ומודיעיניות". אותם גורמים ציינו כי "שותפות מבצעית בין ישראל לארצות הברית קיימת כבר עשרות שנים, אבל יש רמות שונות

47 אביאם סלע, "הקמת רשות הסייבר הלאומית – טעות", *Israel Defense*, 17 בפברואר 2015, http://www.israeldefense.co.il/he/content/.

48 "Employing any OrBat on the Ground or in the Air", *Israel Defense*, June 2, 2015, http://www.israeldefense.co.il/en/content/employing-any-orbat-ground-or-air.

49 זאת, בשונה מ"צוות החירום לאירועי מחשב" (CERT), המתמקד בענפי התשתית המרכזיים ומגיב למתקפות מחשבים ברמה הלאומית. פורמט קרוב יותר לרעיון של "כוחות מיוחדים" הם "צוותי ההתערבות" שהקים אגף התקשוב/ C4I של צה"ל. ראו: "Ready for any Scenario: Military or Civil", *Israel Defense*, February 24, 2014, http://www.israeldefense.co.il/en/content/ready-any-scenario-military-or-civil.

50 "Israel's New National Cyber Operations Center", *Israel Defense*, November 13, 2014, http://www.israeldefense.co.il/en/content/israel%E2%80%99s-new-national-cyber-operations-center.

51 "IAI: Cyber R&D Center in Singapore", *Israel Defense*, February 13, 2014, http://www.israeldefense.co.il/en/content/iai-cyber-rd-center-singapore.

של שיתוף פעולה בתחומים השונים", וכי "המודל הטוב ביותר הוא שיתוף הפעולה בתחום הגנת הטילים, שהוליד את פיתוח ה'חץ', 'כיפת ברזל' ו'שרביט קסמים'".[52]

אחד המודלים האפשריים לפעול על פיו הוא שיתוף הפעולה הבין־לאומי בתחום הפיננסים המתקיים כחלק מהמאבק בהלבנת הון ובמימון הטרור. זאת, באמצעות רשת של ארגונים בין־לאומיים, דוגמת ארגון Financial Action Task Force (FATF)[53] ברמה הגלובלית, וארגון Financial Crimes Enforcement Network (FinCEN) ברמה הלאומית.[54] אנלוגיה זו היא נושא ראוי למחקר עתידי.

עקב המאפיינים המיוחדים של בעיית ביטחון הסייבר, לא יהיה זה מרחיק לכת לקבוע כי שתי ההמלצות האחרונות של פיתוח שיתופי פעולה בין־לאומיים וטקטיים עשויות בשלב מסוים להתכנס יחדיו: המורכבות, קנה המידה והשונות של האתגרים עשויים להביא לכך ששיתוף הפעולה העתידי יתפתח ויהפוך מתחום שעניינו חילופי מידע בלבד לפעולות משולבות ומשותפות, ואולי אף יכלול הקמת "כוחות משימה משותפים" או חילופי נציגים בפיקודים מבצעיים וביחידות, שיפעלו כקציני שיתוף פעולה.

סיכום

אנלוגיות הן כלי עזר חיוני להתמודדות עם אתגרים חדשים. האיומים במרחב הסייבר הם עצומי ממדים, אינטנסיביים מבחינה טכנולוגית ומתפתחים במהירות, ומטבעם הם זקוקים לאנלוגיות ומטאפורות. הטרור הינו תופעה הדומה לאיומי הסייבר מבחינת קנה המידה, הצורה וההשפעה ההרסנית שלו על שגרת החיים, והוא גם זירה שבה מדינות שונות צברו ניסיון רב ומומחיות.

מאמר זה ביקש לערוך השוואה בין איום הסייבר ובין איום הטרור, באופן פחות אינטואיטיבי ויותר אנליטי. בהתאם לכך חודדה רזולוציית ההשוואה מ"טרור" בכלל ל"טרור בליסטי", והוגבלה להקשר הישראלי. המסקנה שהתקבלה היא שניתן ללמוד רבות מהאנלוגיה, וזאת מבלי להתעלם מהבעיות שבה, כגון שאלות של מהירות, היקף וחוסר האפשרות לחזות את האירועים.

---

52 רן דגוני, "ידלין: בלוחמת סייבר, מדינה צריכה לתקוף, לא רק להתגונן", **גלובס**, 29 באפריל 2015, http://www.globes.co.il/news/article.aspx?did=1001031543.

53 FATF הוא ארגון בין־ממשלתי שהוקם בשנת 1989 ביוזמת מדינות ה־G7 כדי לגבש מדיניות למאבק בהלבנת הון. בשנת 2001 התרחב ייעודו גם לתחום המאבק במימון הטרור. הארגון מנטר את התקדמותן של מדינות ביישום המלצותיו באמצעות שימוש בסקירות של עמיתים (הערכות הדדיות) בין המדינות החברות. מזכירות FATF שוכנת במטה ארגון ה־OECD בפריז. לפרטים נוספים ראו: www.fatf-gafi.org/.

54 FinCEN הוא גוף השייך למשרד האוצר האמריקאי, ותפקידו הוא לאסוף ולנתח מידע בנוגע לעסקאות פיננסיות, במטרה להיאבק בהלבנת הון מקומית ובין־לאומית, במימון טרור ובפשעים פיננסיים אחרים. למידע נוסף ראו: www.fincen.gov/.

המאמר ניתח שלוש הצעות מרכזיות: הראשונה – בחינה מחדש של הנחות יסוד הנוגעות לעתיד אבטחת הסייבר; השנייה – האפשרות לאמץ את מסגרת "ששת ה־D" מהמאבק בטרור לעולם הסייבר; השלישית, ברמה הארגונית – הצורך בתצורות מבצעיות גמישות חדשות ובגופי שיתוף פעולה בין־לאומיים (ובעתיד שילוב בין השניים).

המסגרת המוצעת במאמר משאירה מקום למחקר נוסף של הסוגיות, כאשר החשובות שבהן אמורות להתייחס לעצם יישום ההצעות שלעיל. לדוגמה, כיצד ניתן לתרגם רעיונות כמו "מניעה" לטקטיקות של לחימה באיום הסייבר, או האם גוף ביטחוני יטפל במאמצים הלאומיים לאבטחת הסייבר טוב יותר מאשר גוף אזרחי? התייחסות מרכזית נוספת אמורה להתמקד בשאלות: כיצד להרכיב יחידות וכוחות חדשים, מה יהיו המרכיבים של יחידות אלו וכיצד יוקצו תחומי האחריות והמשאבים ביניהם? שאלות אלו ממחישות את הנקודה המרכזית של המאמר, והיא שהאנלוגיה בין איומי הסייבר ובין איומי הטרור צריכה לשמש לא רק לקביעת מדיניות מסוימת, אלא גם כדי לפתוח את הדלת לשיח עשיר ורלוונטי שישפיע על תפיסות ויעלה רעיונות חדשים לפעולה.

לבסוף, השאלה שהוצגה על ידי הקצין הישראלי הבכיר שצוטט בפתח המאמר עדיין נותרת בעינה. במבט לאחור, קל לראות כיצד התפתח האיום הבליסטי, על שיטותיו, מרכיביו והדינמיקה שלו. החשיבה המבצעית סביב איום הסייבר נמצאת רק בראשיתה, במיוחד בכול מה שנוגע לאיום מצד גורמים לא מדינתיים. לכן, קשה לדמיין את אופיו המדויק של איום זה, והשאלות לגבי הצורות שילבש וכיצד למנוע את התפתחותו הן סוגיות מפתח להמשך עיסוק בעתיד.