סייבר, מודיעין וביטחון

כרך 2 | גיליון 2 | ספטמבר 2018

המערכה על התודעה –
מלחמת לבנון השנייה כמקרה בוחן
פנינה שוקר

קווים מנחים לניהול סיכוני סייבר
גבי סיבוני והדס קליין

אבטחה של שרשראות אספקה קריטיות:
הזדמנויות אסטרטגיות לקידום היוזמה להסמכה בין־לאומית של מוצרי סייבר
פול סטוקטון

ניהול משברי גרעין והרתעה בצל לוחמת סייבר
סטפן ג'יי סימבלה

"לוחמה כלכלית רחבה" בעידן הסייבר
שמואל אבן

כיצד מודיעין אסטרטגי לאומי ומודיעין עיסקי תחרותי יכולים לתרום אחד לשני – מבט השוואתי
אבנר ברנע

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

סייבר, מודיעין וביטחון

כרך 2 | גיליון 2 | ספטמבר 2018

תוכן

המערכה על התודעה – מלחמת לבנון השנייה כמקרה בוחן
פנינה שוקר | 3

קווים מנחים לניהול סיכוני סייבר
גבי סיבוני והדס קליין | 19

אבטחה של שרשראות אספקה קריטיות: הזדמנויות אסטרטגיות לקידום היוזמה להסמכה בין־לאומית של מוצרי סייבר
פול סטוקטון | 33

ניהול משברי גרעין והרתעה בצל לוחמת סייבר
סטפן ג'יי סימבלה | 61

"לוחמה כלכלית רחבה" בעידן הסייבר
שמואל אבן | 77

כיצד מודיעין אסטרטגי לאומי ומודיעין עיסקי תחרותי יכולים לתרום אחד לשני – מבט השוואתי
אבנר ברנע | 99

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.

עורך ראשי: אלוף (מיל.) עמוס ידלין
עורך: ד"ר גבי סיבוני
מתאמי כתב העת: הדס קליין, גל פרל פינקל

ועדה מייעצת:

סונג'וי ג'וּשי / מרכז אובזרבר למחקר, הודו
פטר ויגו ג'קובסון / הקולג' הדני המלכותי להגנה, דנמרק
רוט דיאמינט / אוניברסיטת טורקוואטו
די טלה, ארגנטינה
ג'יימס ג'. ווירץ / בית הספר הימי ללימודים מתקדמים, ארצות הברית
ריקרדו ישראל זיפר / האוניברסיטה האוטונומית של צ'ילה, צ'ילה
דניאל זירקר / אוניברסיטת וואיקאטו, ניו זילנד
ג'פרי ג'. לארסן / תאגיד יישומי מדע בינלאומי SAIC, ארצות הברית
ג'יימס לואיס / המרכז למחקר ללימודים אסטרטגיים CSIS, ארצות הברית
קובי מיכאל/ המכון למחקרי ביטחון לאומי INSS, ישראל
ג'ון נומיקוס / מרכז המחקר ללימודים אירופאים ואמריקניים, יוון
תיאו נית'לינג / אוניברסיטת המדינה החופשית, דרום אפריקה
גלן מ. סגל / סקוריטסם ויגילאתא, אירלנד
פרנק ג'. סילופו / אוניברסיטת ג'ורג' ווטינגטון, ארצות הברית
סטפן ג'. סימבלה / אוניברסיטת פן סטייט, ארצות הברית
ט. ו. פאול / אוניברסיטת מקגיל, קנדה
מריה רחל פריר / אוניברסיטת קוימברה, פורטוגל
מרים דאן קאוולטי / המכון הפדרלי השוויצרי לטכנולוגיה, ציריך, שוויץ
אפרים קארש / קינגס קולג', לונדון, בריטניה
קאי מיכאל קנקל / האוניברסיטה האפיפיורית הקתולית של ריו דה ז'נרו, ברזיל
ברונו תרטרס / קרן למחקר אסטרטגי, צרפת

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

2018 © כל הזכויות שמורות

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

המערכה על התודעה – מלחמת לבנון השנייה כמקרה בוחן

פנינה שוקר

משרתו של מאמר זה היא לבחון את האופן שבו מנהיגים מנסים לעצב את תודעת החברה מבית בזמן מלחמה. זאת, בעקבות ההנחה שהחברה לא תסכין לתמוך בכל תנאי במלחמה ממושכת ומרובת נפגעים. הכרתם של מקבלי ההחלטות בנחיצותה של תמיכה ציבורית רחבה במלחמה, מביאה אותם לשפלל את דעת הקהל מבית להכיר בצדקתה, בחשיבות משרותיה ובהישגים הרבים, כביכול, שהיא טומנת בחובה. מאמר זה ידגים כיצד הדבר בא לידי ביטוי במהלך מלחמת לבנון השנייה, עד כדי סיכון כוחות הקרקע של צה"ל בקרבות שמשרתם הייתה תודעתית גרידא, ויצביע על ההשלכות השליליות השמונות בצעדים דוגמת אלה על ניהול מלחמה ברמה האסטרטגית ועל תוצאותיה.

מילות מפתח: קרבות תודעה, דעת קהל, לגיטימציה פנימית, חוסן לאומי, קבלת החלטות

מבוא

בשנים האחרונות נוצרה הסכמה בקרב חוקרי אסטרטגיה צבאית כי השפעתם של קהלים אזרחיים על קביעת מטרות המלחמה, בחירת דרכי הלחימה, ולעיתים אף ניהול הלחימה עצמה, הולכת וגוברת.[1] תחום מרכזי הכרוך במגמה זאת, שגם בו חלו שינויים מפליגים בעידן המודרני, הוא יחס דעת הקהל למלחמות מצד אחד וההשפעה על דעת הקהל באמצעות כלי תודעה והשפעה מצד שני.

פנינה שוקר היא דוקטורנטית במחלקה למדע המדינה באוניברסיטת בר אילן וחוקרת במכון למחקרי ביטחון לאומי.

1 סטיוארט א' כהן, "היחסים המשתנים בין החברה לצבא בישראל: ההשלכות המבצעיות", בתוך: מאג'ד אלחאג' ואורי בן אליעזר (עורכים), **בשם הביטחון**, אוניברסיטת חיפה ופרדס, חיפה, 2003, עמ' 103.

מאז שנות התשעים של המאה העשרים הפכה השמירה על חיי אדם לשיקול מבצעי כבד משקל,[2] ובשנות האלפיים התעצם השיקול האנושי עד כדי פיתוח ציפייה חברתית למלחמה ללא נפגעים.[3] ההנחה העומדת בבסיסו של מאמר זה היא כי ציפייה זו, כפי שנתפסה על ידי מקבלי ההחלטות, השפיעה מאוד על דוקטרינת הלחימה של צה"ל במלחמת לבנון השנייה, ובמקביל הובילה לניהול מערכה תודעתית בלתי פוסקת מול קהלי היעד בישראל לשימור התמיכה הציבורית במלחמה. המאמר עוסק, לפיכך, בחשיבות שניתנה לעיצוב תודעת ניצחון בקרב הציבור הישראלי במהלך אותה מלחמה.

תחילה תובא סקירה תיאורטית על התופעה של רגישות החברה הדמוקרטית לנפגעים, וכפועל יוצא ממנה – על חשיבות המערכה על תודעת החברה מבית. לאחר מכן תוצג השתרשות ההיבט התודעתי בצה"ל, תוך בחינת השאלה כיצד הדבר בא לידי ביטוי במהלך מלחמת לבנון השנייה. הדבר ייעשה באמצעות דוגמאות בולטות. לבסוף יאופיינו ההשלכות השליליות העשויות לנבוע מהענקת חשיבות יתרה לממד התודעתי.

חשיבות המאבק על התודעה

אין הגדרה מוסכמת ואחידה בקרב חוקרים באשר למהותה של המלחמה על התודעה. אל"ם (מיל') מירי אייזן, לשעבר דוברת ממשלת ישראל לתקשורת הבין־לאומית, הציעה את ההגדרה הבאה: "מאבק על התודעה במלחמה הוא ניסיון כולל של מדינה, או של ישות לא מדינתית, להשפיע על קהלי יעד שונים, במטרה להשיג ניצחון בהתמודדות לאומית".[4] לטענתו של סער רווה, המושג "זירת התודעה" הוא חדש יחסית בתחום הצבא והמלחמה וקשור למספר תהליכים מרכזיים שהתחוללו מסיום מלחמת העולם השנייה ועד היום. ניתן למנות עליהם את השינוי שחל באופי העימותים בהם מעורבים צבאות בכלל וצה"ל בפרט; את המעורבות ההולכת וגוברת של המעצמות בסכסוכים אתניים או לאומיים מחוץ לגבולותיהן, ובמקביל את העלייה בחשיבותה של דעת הקהל העולמית; ואת התמורות בתחום המידע, שגרמו לכך שיצירת המידע, הבעלות עליו והפצתו מבוזרות ואינן נמצאות תחת שליטתו של גורם אחד. תהליכים אלה הפכו את הפעולות הפיזיות של הצבא למשולבות עם פעולות במישור התודעתי, שנועדו להסביר, לפרש ולהגדיר לקהלי

---

2 יגיל לוי, "הממד החברתי של הפיקוח האזרחי על הצבא: מדיניות מניעת נפגעים", בתוך: אפרים לביא (עורך), **יחסי צבא־חברה בישראל: השלכות על קבלת החלטות בנושאי ביטחון ושלום**, מכון תמי שטיינמץ למחקרי שלום, אוניברסיטת תל אביב, תל אביב, 2013, עמ' 71.

3 מאיר פינקל, "השפעת החברה על הדוקטרינה ועל התרבות של צה"ל, **מערכות**, 412, מאי 2007, עמ' 61.

4 צוטט אצל: ראובן ארליך, "תרומתו של המודיעין במלחמה על התודעה", **מרכז המידע למודיעין ולטרור ע"ש מאיר עמית**, 11 ביולי 2006.

היעד את מטרות הפעולה הצבאית, את יעדיה ואף את תוצאותיה, באופן המשקף את המדיניות והאינטרסים של יוזם הפעולה.[5]

לטענת ליאור רשף ושי שבתאי, התודעה היא ממד נוסף של המערכה הצבאית – ממד הקשור להיבטים סובייקטיביים כמו מחשבות, אמונות, תפיסות, השקפות עולם, פרשנויות וסמלים. בממד התודעה נעשה תהליך בלתי פוסק של מתן משמעויות לאירועים המתרחשים במציאות, ומכאן שזהו ממד הנתון לטפלול ולהשפעה. ממד התודעה רווי במשתנים ובשחקנים, וכדי ליצור השפעה אפקטיבית, נדרשת הלימה בין המאמצים השונים המעצבים את המציאות – במיוחד הפעלת הכוח – ובין "הסיפור" שצה"ל שואף להנחיל לקהלי היעד.[6]

בשנים שקדמו למלחמת לבנון השנייה התפתחה גם בצה"ל ההבנה כי פגיעה משמעותית ביכולתו של האויב להילחם קשורה להיבט התודעתי של הפעולה הצבאית לא פחות מאשר להיבט הפיזי.[7] צה"ל תחת הרמטכ"ל משה יעלון ראה חשיבות ונחיצות בעיצוב תודעת החברה הישראלית, כמו גם בעיצוב תודעת היריב. במסגרת זו הוקם בינואר 2005 "מרכז למבצעי תודעה" (מל"ת) שנועד לבחון את פעולות הצבא בהיבט התודעתי וליזום מבצעים שמטרתם להשפיע על תודעת האויב, בעיקר באמצעות תעמולה, לוחמה פסיכולוגית ולעיתים תרגילי הטעייה. מיקומו של המל"ת בהיררכיה הצבאית – בכפיפות ישירה לראש אגף המבצעים – מעיד על חשיבותו הרבה.[8] יחידה שנועדה למטרה דומה הייתה קיימת עוד קודם לכן, אך פעולתה הייתה מצומצמת מאוד.[9]

הרמטכ"ל דן חלוץ אימץ תפיסה דומה, לפיה כל מלחמה היא, בראש ובראשונה, קרב על התודעה.[10] הוא האמין בצורך להשפיע על תודעת האויב והקים לצורך זה מחלקה ל"עיצוב המערכה" באגף המבצעים.[11] גם היעדים של חטיבת דובר צה"ל הותאמו לתפיסה המערכתית: לא עוד עיסוק בדוברות ובהסברה, אלא "עיצוב

---

5 סער רווה, "תודעה והוויה: שני המרכיבים של השלם המבצעי", **מערכות**, 409–410, דצמבר 2006, עמ' 66–68.

6 ליאור רשף ושי שבתאי, "מאמץ התודעה בצה"ל", **מערכות**, 457, אוקטובר 2014, עמ' 35.

7 רווה, "תודעה והוויה", עמ' 71.

8 יוני שדמי וברק רביד, "היחידה שתשגע לאויבינו את המוח", **מעריב** *nrg*, 17 בדצמבר 2005.

9 Ron Schleifer, "Psyoping Hezbollah: The Israeli Psychological Warfare Campaign during the 2006 Lebanon War", *Terrorism and Political Violence*, 21 no. 2 (2009): 223.

10 Matt M. Matthews, "Hard Lessons Learned: A Comparison of the 2006 Hezbollah-Israeli War and Operation CAST LEAD: A Historical Overview", in: Scott C. Farquhar (ed.), *Back to Basics: A Study of the Second Lebanon War and Operation CAST LEAD* (Fort Leavenworth, Kansas: Combat Studies Institute Press, US Army Combined Arms Center, 2009), p. 44.

11 עמיר רפפורט, **אש על כוחותינו: כך הכשלנו את עצמנו במלחמת לבנון השנייה**, ספריית מעריב, תל אביב, 2007, עמ' 53–54; Schleifer, "Psyoping Hezbollah", p. 224.

תפיסת מציאות בשיח הציבורי". נקבע כי צה"ל צריך להפעיל בשעת מלחמה "מכלול תודעה", ממש כמו המכלולים המסורתיים במפקדות שאחראיות להפעלת האש או על תיאום הסיוע הלוגיסטי. "מכלול תודעה" הוקם אפילו בעוצבת הגליל של צה"ל, האחראית על חזית לבנון, משל היה מדובר במערך לחימה לכל דבר ועניין.

רגישות החברה הדמוקרטית לנפגעים

תופעת הרגישות לנפגעים מוגדרת כנכונות נמוכה של החברה לספוג אבידות בפעילות צבאית. קיימת הסכמה רווחת כי תופעה זו היא מאפיין חברתי ותרבותי קבוע בדמוקרטיות מערביות מאז תום המלחמה הקרה, וכי היא מצויה במגמת עלייה, עד כדי התנגדות מוחלטת לצאת לפעילות הכרוכה בנפגעים.[12] יש הטוענים כי התופעה כובלת את ידי הצבאות, בכך שהיא עשויה להניע מנהיגים לאמץ מדיניות של סלידה מאבידות, כלומר מדיניות השואפת להגביל סיכונים לכוחות הלוחמים, ולעיתים עשויה להסלים עד כדי הקרבת היעילות המבצעית ואף הימנעות ממשימות בהן צפויים נפגעים.[13]

יש חוקרים הסבורים כי רגישות החברה לאבידות תפחת ככול שהערכתה את סיכויי ההצלחה של המלחמה תהיה גבוהה יותר. כלומר, אפילו אם עצם פתיחת המלחמה נתפסת כטעות בעיני הציבור, הוא יקבל את המשך הלחימה וישלים עם אבידות נוספות, אם ייראה לו שהצד "שלו" מנצח.[14] לאור זאת, מנהיגים רואים

12 Gerhard Kummel and Nina Leonhard, "Casualties and Civil-Military Relations: The German Polity Between Learning and Indifference", *Armed Forces & Society*, 31 no. 4 (2005): 514-515; Joseph Soeters and Jan Van Der Meulen, "Considering Casualties: Risk and Loss during Peacemaking and Warmaking", *Armed Forces & Society*, 31 no. 4 (2005): 483; Joseph P. Vasquez, "Shouldering the Soldiering: Democracy, Conscription and Military Casualties", *Journal of Conflict Resolution*, 49 no. 6 (2005): 849; Yagil Levy, *Israel's Death Hierarchy: Casualty Aversion in a Militarized Democracy* (New York: New York University Press, 2012), p. 2.

13 Edward N. Luttwak, "Where Are the Great Powers? At Home with the Kids", *Foreign Affairs*, 73 no. 4 (1994): 24; Edward N. Luttwak, "A Post-Heroic Military Policy", *Foreign Affairs*, 75 no. 4 (1996): 42; Harvey Sapolsky and Jeremy Shapiro, "Casualties, Technology and America's future Wars", *Parameters*, 26 no. 2 (1996): 122; James Burk, "Public Support for Peacekeeping in Lebanon and Somalia: Assessing the Casualties Hypothesis", *Political Science Quarterly*, 114 no. 1 (1999): 54; Philip Everts, "When the Going Gets Rough: Does the Public Support the Use of Military Force?", *World Affairs*, 162 no. 3 (2000): 93.

14 Jeffrey Record, *Hollow Victory: A Contrary View of the Gulf War* (Washington: Brassey's, 1993), p. 137; Steven Kull, "Review of Eric Larson's Casualties and Consensus", *Public Opinion Quarterly*, 61 no. 4 (1997): 672; Marijke De Konink and Jan Van Der Meulen, "Risky Missions: Dutch Public Opinion on Peacekeeping in the Balkans", in: *Public Opinion and the International Use of Force*, Phillip Everts and Pierangelo Isernia eds. (London: Routledge, 2001) p. 116; Peter D. Feaver,

בעת מלחמה חשיבות רבה בהענקת תחושה לציבור כי הניצחון ממשמש ובא, בין היתר באמצעות הצגת הישגים בשדה הקרב, כמו גם טשטוש עובדות העשויות לגרום לדמורליזציה, דוגמת מחדלים, תבוסות בקרבות ואבידות כבדות.[15]

לטענת פול קורניש, דרך נוספת למניעת דמורליזציה היא דיווח כוזב על מספר ההרוגים.[16] אלא שלפי קורניש, דיווח על מספר הרוגים נמוך מהמספר האמיתי עשוי להעלות את רף הציפיות בקרב הציבור לתוצאות זהות במבצעים צבאיים עתידיים. כך, במקום להפחית את רגישות החברה לאבידות, מושגת תוצאה הפוכה.[17] בספרות המחקרית מתוארות דרכים נוספות ל"ריכוך" המידע על מספר ההרוגים: הוצאת סוגי אבידות מסוימים מתוך המספר הכולל; פיקוח על פרסום תמונות של חיילים הרוגים בכדי למנוע את התגברות הסערה הציבורית; שחרור פרטים על הרוגים בד בבד עם פרסום ידיעות על הישגים במלחמה, במטרה ליצור תחושה ציבורית שההקרבה ראויה.[18] טענתו של מאמר זה היא כי במהלך מלחמת לבנון השנייה נעשה מאמץ רב להעמיק את הלגיטימציה הפנימית ללחימה, ובכלל זה ליצור תחושת הישג מול מספר הנפגעים.

רגישות לנפגעים במהלך מלחמת לבנון השנייה

מאמרים ומחקרים רבים שנכתבו לאחר מלחמת לבנון השנייה טענו כי הססנות הדרג המדיני והדרג הצבאי מביצוע מהלך קרקעי רחב, שהיה עשוי לצמצם את מספר הרקטות שנורו על אזרחי ישראל, נבעה מרגישות מוגזמת לחיי חיילים.[19] לדברי יגיל

Christopher Gelpi and Jason Reifler, "Success Matters: Casualty Sensitivity and the War in Iraq", *International Security*, 30 no. 3 (2005): 7-8; John E. Mueller, "The Iraq Syndrome", *Foreign Affairs,* 2005, 84 no. 6 (2005): 49; Patricia L. Sullivan, "Sustaining the Fight: A Cross-Sectional Time-Series Analysis of Public Support for Ongoing Military Interventions", *Conflict Management and Peace Science*, 25 no. 2 (2008): 112; Peter D. Feaver, Christopher Gelpi and Jason Reifler, *Paying the Human Cost of War: American Public Opinion and Casualties in Military Conflicts* (Princeton: Princeton University Press, 2009), p. 1.

15 כפי שצוטט בתוך: תרצה הכטר, **מיתוסים פוליטיים – רציפות מול שינוי: התפתחותם של מיתוסים פוליטיים סביב מלחמת יום הכיפורים בקרב הציבור החילוני־יהודי: ממלחמת יום הכיפורים עד הסכם אוסלו,** חיבור לשם קבלת תואר דוקטור לפילוסופיה, אוניברסיטת בר אילן, המחלקה למדע המדינה, רמת גן, 1996, עמ' 55.

16 Paul Cornish, "Myth and Reality: US and UK Approaches to Casualty Aversion and Force Protection", *Defense Studies*, 3 no. 2 (2003): 124.

17 Cornish, "Myth and Reality"

18 Douglas L. Kriner & Francis X. Shen, *The Casualty Gap: The Causes and Consequences of American Wartime Inequalities* (New York: Oxford University Press, 2010) p. 9.

19 יצחק בן־ישראל, **מלחמת הטילים הראשונה: ישראל־חיזבאללה**, אוניברסיטת תל אביב, בית הספר לממשל ומדיניות ע"ש הרולד הרטוך, תל אביב, 2007, עמ' 20; יהודה וגמן, "ליקויים בראיית צה"ל את עצמו כאחראי לביטחון האזרחים", **עדכן אסטרטגי**, כרך 10, גיליון 2, 2007,

לוי, לנגד עיניהם של מקבלי ההחלטות ביולי 2006 עמדה רמת הלגיטימיות הנמוכה של הכנסת כוח קרקעי ללבנון שתחייב גם שילוב של אנשי מילואים.[20] הרמטכ"ל דאז, דן חלוץ, אף קבע נחרצות כי ישראל הולכת לקראת מערכה המבוססת על הפעלת אש מרחוק, בעיקר באמצעות חיל האוויר וארטילריה.[21] הוא גם החליט מפורשות להימנע מפעולה קרקעית והתנער מתוכנית המגירה "מי מרום", שיועדה לנסיבות שבהן מצאה עצמה ישראל בבוקר של 12 ביולי 2006.[22]

לאחר המלחמה טען חלוץ כי בעת שקיבל החלטות במלחמה ברור היה לו שצריך להביא בחשבון את ההורים של שנת 2006, מכיוון שהסובלנות לנפגעים

עמ' 24; אפרים ענבר, "כשלי החשיבה האסטרטגיים במלחמת לבנון השנייה", בתוך: **מלחמת לבנון השנייה ולאחריה**, אוניברסיטת בר־אילן, מרכז בגין־סאדאת למחקרים אסטרטגיים, רמת גן, 2007, עמ' 4־5; דב תמרי, "האם צה"ל יכול להשתנות בעקבות מלחמת לבנון השנייה?", **מערכות**, 415, 2007, עמ' 38; רון טירה. **המאבק על טבע המלחמה: מקלאוזביץ לסקיפיו אפריקנוס ואנואר סאדאת ועד לאויב המדינתי שהסתגל למלחמה נגד ה־RMA**, תל אביב: המכון למחקרי ביטחון לאומי, 2008, עמ' 97; משה יעלון, "הזיקה בין דרג מדיני ודרג צבאי בעריכת תמרון יבשתי", הרצאה שניתנה בכנס לטרון השני לצבא וביטחון בנושא "התמרון היבשתי במאה ה־21", לטרון, יד לשריון, 16 בספטמבר 2008; גיורא סגל, "חיוניות התמרון היבשתי בעימות א־סימטרי", **עדכן אסטרטגי**, כרך 10 גיליון 4, 2008, עמ' 24, 28־30; אמיר הרפז, "תפקידיו החדשים של התמרון היבשתי", **מערכות**, 431, 2010, עמ' 21; Uzi Rubin, *The Rocket Campaign against Israel during the 2006 Lebanon War* (Ramat-Gan: Bar-Ilan University, The Begin-Sadat Center for Strategic Studies, 2008), p. 16; Avi Kober, "The Israel Defense Forces in the Second Lebanon War: Why the Poor Performance?", *Journal of Strategic Studies*, 31 no. 1 (2008): 7; Uri Bar-Joseph, "The Hubris of Initial Victory – the IDF and the Second Lebanon War", in: *Israel and Hizbollah: An Asymmetric Conflict in Historical and Comparative Perspective*, Clive Jones and Sergio Catignani, eds. (London: Routledge, 2009), p. 153.

20 יגיל לוי, "כיצד דמוקרטיזציה מחוללת לוחמנות – מלחמת לבנון השנייה", **פוליטיקה**, 17, 2008, עמ' 122.

21 גיורא סגל, "איך מנצחים כוחות מהפכניים", **מערכות**, 415, 2007, עמ' 44; אורי בן־אליעזר, **מלחמותיה החדשות של ישראל: הסבר סוציולוגי־היסטורי**, אוניברסיטת תל אביב, תל אביב, 2012, עמ' 393־394; חיים רוזנברג, "הטכנולוגיה לא תחליף את התמרון", **מערכות**, 443, 2012, עמ' 74; Stuart Cohen, *Israel and its Army: From Cohesion to Confusion* (London: Routledge, 2008), p. 46; Efraim Inbar, *Israel's National Security: Issues and Challenges since the Yom Kippur War* (London: Routledge, 2008), p. 226.

22 גיורא סגל, "מלחמת לבנון השנייה – הזדמנות שהוחמצה", **מערכות**, 420–421, 2006, עמ' 17; מיכאל הרסגור ואהוד פוקס, **רגעים היסטוריים ורגעים היסטריים: החלטות בתנאי משבר**, דביר, אור יהודה, 2010, עמ' 326; Matt M. Matthews. *We Were Caught Unprepared: The 2006 Hezbollah-Israeli War* (Fort Leavenworth, KS: U.S. Army Combined Arms Center, Combat Studies Institute Press, 2008), p. 43; Benjamin S. Lambeth, *Air Operations in Israel's War Against Hezbollah: Learning from Lebanon and Getting it Right in Gaza* (Santa Monica, CA: RAND, 2010), p. xv.

שונה מכפי שהייתה בעבר.[23] ואכן, עם פתיחת המערכה הביא חלוץ לממשלה המלצה לפגוע בתשתיות לאומיות בלבנון, אלא שראש הממשלה התנגד לתקיפה רחבה לאור התנגדות אמריקאית.[24] למרות זאת, אושרה תקיפה של מסלולי שדה התעופה בביירות וכביש ביירות־דמשק.[25]

ועדת וינוגרד, שחקרה את מלחמת לבנון השנייה, טענה כי הפעילות הצבאית נמשכה עד סוף המלחמה תחת נהלים ואיסורים של פעילות בט"ש, תוך הטלת מגבלות על פעולת הכוחות משיקולים שהתאימו לשיקולי בט"ש, כגון שימת דגש מיוחד על הימנעות מסיכון של חיילים.[26] התייחסות לתופעה זו ניתן למצוא בספרו של דן חלוץ: "אי־הפנמת מצב המלחמה מצאה ביטוי בהנחיות הפנימיות השונות שיצאו בפיקוד הצפון, בחיל הים ובחיל האוויר, והטילו על הכוחות המבצעיים אילוצים ומגבלות בלתי מתאימים למציאות המלחמתית שאליה נכנסנו. החשש מהיפגעות חיילים חלחל עמוק..."[27]

תודעת ניצחון במלחמת לבנון השנייה

ניסיונות רבים נעשו במהלך מלחמת לבנון השנייה להביא את "תמונת הניצחון".[28] הרמטכ"ל חלוץ הצהיר כי "תכלית המהלכים היא עיצוב תודעה בדבר היחלשות חזבאללה, בין היתר באמצעות חטיפת/הריגת מחבלי הארגון ומתן תהודה פומבית לדבר".[29] לפיכך, במשך כל הלחימה הצטוו הכוחות לתעד ולצלם עדויות בשטח, כולל גופות של אנשי חזבאללה, בכדי להמחיש בדרך זו את ניצחונותיהם.[30]

לטענת קצין בכיר בצה"ל, "כל הזמן רצו שנביא תמונות של מחבלים מתים, מחבלים שמרימים ידיים, לעצב את התודעה של הציבור".[31] לשם כך הופעל נוהל

23 גל הירש, **סיפור אהבה סיפור מלחמה**, ידיעות אחרונות, ספרי חמד, תל אביב, 2009, עמ' 330.

24 ענת טל־שיר וצדוק יחזקאלי, "ממשלה באפלה", **ידיעות אחרונות – המוסף לשבת**, 18 באוגוסט 2006, עמ' 8–9; רפפורט, **אש על כוחותינו**, עמ' 22; עמוס הראל ואבי יששכרוף, **קורי עכביש: סיפורה של מלחמת לבנון השנייה**, ידיעות אחרונות, תל אביב, 2008, עמ' 165; אייל זיסר, **לבנון דם בארזים**, בני־ברק: הקיבוץ המאוחד, 2009, עמ' 306; זכי שלום, "הגדרת האויב בעימות אסימטרי: מלחמת לבנון כמשל", **עדכן אסטרטגי**, כרך 12, גיליון 3, 2009, עמ' 8־10; אמיר אשל, "בדרך לקיפאון בתמרון", **מערכות**, 434, 2010, עמ' 24; Bar-Joseph, "The Hubris of Initial Victory" ;Kober, "The Israel Defense Forces in the Second Lebanon War", p. 36.

25 רפפורט, **אש על כוחותינו**, עמ' 173.

26 ועדת וינוגרד, **מלחמת לבנון השנייה: דין וחשבון סופי**, ירושלים, ינואר 2008, עמ' 314.

27 דן חלוץ, **בגובה העיניים**, ידיעות אחרונות, ספרי חמד, תל אביב, 2010, עמ' 386.

28 הראל ויששכרוף, **קורי עכביש**, עמ' 398.

29 **שם**, עמ' 236.

30 פליקס פריש, "מחאת לוחמי צה"ל וצילומי גופות המחבלים", **מעריב**, 6 ביולי 2007, עמ' 11.

31 איתן גליקמן ונאווה צוריאל, "ואדי הבכא", **ידיעות אחרונות – 24 שעות**, 16 באוגוסט 2006, עמ' 9.

המכונה "תיעוד מבצעי", וחלק מהלוחמים צוידו על ידי דובר צה"ל בכמאתיים מצלמות סטילס ווידיאו מסוגים שונים, שחלקן הוצמדו לקסדותיהם.[32] ב"בור" בקריה בתל אביב ישב קצין בדרגת תת־אלוף, שאחד מתפקידיו היה לקבל לידיו את התיעוד המבצעי,[33] שנתפס כחיוני ביותר. על חשיבותו של תיעוד זה ניתן ללמוד מסיכום הרמטכ"ל מ־8 באוגוסט 2006, בו נאמר כי "זהו חלק תומך, מסייע ומשמעותי להצלחת המהלך המבצעי. יש להקפיד על תיעוד זה בכלל הרמות, כמו גם על הפצת תוצריו במהרה".[34] למעשה, מאמץ התיעוד המבצעי הניב תפוקה מעטה, ובסופו של דבר רוב החומרים הוויזואליים שהוצגו במהלך המלחמה הגיעו מצילומי חיל האוויר.[35]

הפיקוד והמטכ"ל לחצו על הכוחות לשבות אנשי חזבאללה:[36] "תביאו לי גופות ושבויים", חזר חלוץ ואמר לאנשי פיקוד הצפון, "אני רוצה עשרה שבויים בכל מבצע".[37] העיד על כך גם אחד ממפקדי החזית: "אמרו לנו: תביאו כמה שיותר גופות של אנשי חזבאללה ושבויים בתחתונים".[38] אלוף אייל בן ראובן, ששימש כיועץ לאלוף פיקוד הצפון אודי אדם בזמן הלחימה, מתח על כך ביקורת חריפה לאחר המלחמה, באומרו כי "צרם לי גם שפיקוד הצפון נדרש, פעם אחר פעם, להביא גוויות של מחבלים ותמונות של מחבלים. זו דרישה בלתי סבירה ממפקדים וחיילים ... הישג תודעתי מביאים דרך הכרעת האויב ולא על ידי סחיבת גוויות של מחבלים על אלונקות".[39]

במהלך המלחמה נערכו מספר פעולות צבאיות שנויות במחלוקת, שזכו לביקורת חריפה בשל סיכון הלוחמים למען השגת "תמונת הניצחון" המיוחלת. בחרתי

---

32 עמיר רפפורט, "צה"ל שידר באל־מנאר תמונות הרוגי חזבאללה", **מעריב**, 9 באוגוסט 2006, עמ' 19; יעל סלומה ולילך שובל, "בגזרת ההסברה: הלוחמים מצוידים במצלמות לתיעוד הפעילות", **במחנה**, 27 ביולי 2006, עמ' 7; נורית קנטי, "התפקוד שלנו היה מצוין", **העין השביעית**, 64, 2006, עמ' 13; מבקר המדינה, "היבטים בהיערכות גורמי ההסברה ובתפקודם במלחמת לבנון השנייה", בתוך: **דוח ביקורת שנתי 58א לשנת 2007**, משרד מבקר המדינה, ירושלים, נובמבר 2007, עמ' 483; שולמית שביט, "תמונת הניצחון", **מערכות**, 440, דצמבר 2011, עמ' 59.

33 יואב לימור ועפר שלח, **שבויים בלבנון: האמת על מלחמת לבנון השנייה**, ידיעות אחרונות, תל אביב, 2007, עמ' 270.

34 כפי שצוטט בדוח מבקר המדינה, **שם**, עמ' 468.

35 **שם**, עמ' 483; ועדת המשנה של הכנסת ליחסי חוץ והסברה, "דין וחשבון בנושא מערכת ההסברה של ישראל במלחמת לבנון השנייה", דצמבר 2007, עמ' 17.

36 אילן כפיר, **האדמה רעדה**, ספריית מעריב, תל אביב, 2006, עמ' 185.

37 לימור ושלח, **שבויים בלבנון**, עמ' 160; רפפורט, **אש על כוחותינו**, עמ' 174; הראל ויישכרוף, **קורי עכביש**, עמ' 244, 398; עמיר רפפורט, "הלילה שבו נשלפו הסכינים", **מעריב – מוסף שבת**, 29 ביוני 2007, עמ' 12.

38 רונן ברגמן, "קריסת הקונספציה 2", **ידיעות אחרונות – 7 ימים**, 18 באוגוסט 2006, עמ' 36.

39 אמירה לם, "מחדל המגירה", **ידיעות אחרונות – 7 ימים**, 9 במארס 2007, עמ' 34.

להתמקד בשלוש דוגמאות מרכזיות: הקרבות בבינת ג'בייל, מבצע "חד וחלק" והיציאה למהלך קרקעי בשלהי המלחמה.

הקרבות בבינת ג'בייל

רוב המערכה הישראלית במלחמת לבנון השנייה התנהלה מן האוויר. אף על פי כן, בשלב מסוים נצטוו כוחות קרקעיים של צה"ל להשתלט על העיירה בינת ג'בייל, שלא הייתה מטרה בעלת חשיבות אסטרטגית רבה,[40] אך נחשבה כ"בירתו של חזבאללה" – המקום שבו נשא מזכ"ל הארגון, חסן נסראללה, את נאומו המפורסם לאחר הנסיגה הישראלית מלבנון בשנת 2000, בו התייחס לישראל כחלשה יותר מקורי עכביש.[41] לטענת הראל ויששכרוף, הכוונה הייתה להביא את ראש הממשלה ואת שר הביטחון לנקודה בעיירה שבה נסראללה נשא את נאומו, כדי שהם ישאו נאום ניצחון משלהם, אלא שעד תום המלחמה הדבר לא התאפשר.[42] הוגה הרעיון למבצע בבינת ג'בייל היה מפקד זרוע היבשה, אלוף בני גנץ, שסבר כי בכך ימומש הרעיון של הישג משמעותי במקום אחד: "נאום הניצחון של נסראללה היה בבינת ג'בייל ... הייתי שוקל מהלך קרקעי מוגבל על האזור הזה, שאפשר להכיל אותו ... הייתי שם צוות עריכה שמראה את המהלך ותוצאותיו. זאת אומרת, מספר את הסיפור עד הסוף".[43]

הרמטכ"ל חלוץ תמך ברעיון של אלוף גנץ,[44] וקבע כי "המלחמות המודרניות הן מלחמות של סמלים. בינת ג'בייל היא סמל. בבינת ג'בייל נשא נסראללה את נאום קורי העכביש. יש פה סמלים שהם הגנו עליהם, ותפקידנו עכשיו להראות להם שאנחנו מכים אותם במקום הזה".[45] כך גם טען בזמן המלחמה אלוף גדי איזנקוט, ששימש אז ראש אגף המבצעים: "מה שחשוב הוא הסמל, היכולת לעשות את זה ולשבור את המיתוס".[46] השם שניתן למבצע בבינת ג'בייל – "קורי פלדה" –

---

40 Bar-Joseph, "The Hubris of Initial Victory", p. 154.

41 משה יעלון, **דרך ארוכה – קצרה**, ידיעות אחרונות, ספרי חמד, תל אביב, עמ' 208; זאב שיף, "בכיר אמ"ן הזהיר מראש את רה"מ: הרחבת הפעולה – טעות", **הארץ**, 7 בספטמבר 2006; עודד לוונהיים, "לגיטימציה לקרבנות בעת מלחמה", הרצאה שניתנה במסגרת יום עיון בנושא "מיליטריזציה ופיקוח על הצבא", האוניברסיטה הפתוחה, 13 בנובמבר 2011; עמיר רפפורט, "צה"ל וסינדרום לבנון – לקראת מלחמת לבנון השלישית?", הרצאה שניתנה במסגרת כנס בנושא "הזירה הלבנונית – שלושים שנה למלחמת לבנון", אוניברסיטת בר־אילן, מרכז בגין־סאדאת למחקרים אסטרטגיים, 30 במאי 2012.

42 הראל ויששכרוף, **קורי עכביש**, עמ' 260.

43 עמיר רפפורט, "נכנסים, הורגים, יוצאים", **מעריב – מוסף שבת**, 6 ביולי 2007, עמ' 18־19.

44 גדי היימן ועודד לוונהיים, "'שכר הולם': נקמה והמערכה הישראלית במלחמת לבנון השנייה", **פוליטיקה**, 17, 2008, עמ' 103.

45 רפפורט, **אש על כוחותינו**, עמ' 161–160.

46 רפפורט, "נכנסים, הורגים, יוצאים", עמ' 20.

כמענה לתיאוריית קורי העכביש של נסראללה, מעיד על החשיבות התודעתית הרבה שיוחסה לו.[47]

המבצע, שיצא לדרך ב־24 ביולי, אמנם נתפס כהצלחה בפיקוד הצפון, אך במטכ"ל ציפו להישגים בעלי משמעות סמלית רבה יותר, כגון לקיחת שבויים. אי לכך, ועל אף שב־25 ביולי בערב ניתנה הוראה לכוחות לנוע חזרה לישראל, התקבלה ברגע האחרון הפקודה להשאיר את חטיבת "גולני" בשטח, ובזו הפעם לכבוש את העיירה.[48] אלוף אדם, שפקפק בתבונת ההוראה, החליט על דעת עצמו לא לכבוש את העיירה מחשש למחיר הגבוה בנפגעים, אלא רק להעמיק את האחיזה בה. למרות זאת, ב־26 ביולי התנהל קרב עקוב מדם בבינת ג'בייל שבמהלכו נהרגו שמונה לוחמים.[49]

דומה כי לאור תוצאותיו של קרב בינת ג'בייל גבר הרצון להישג תודעתי, כפי שביטא זאת באותו היום שר הביטחון עמיר פרץ, לאחר שהובא לידיעתו מספר ההרוגים: "צריך לקחת נשימה עמוקה, לשנות את התמונה. אם הייתה אפשרות לשקול לסיים את המלחמה בהישגים חלקיים, היא התרחקה ... אי אפשר לצאת עכשיו עם זנב בין הרגליים, בלי כבוד".[50] לאחר הקרב מתח אלוף אייל בן ראובן ביקורת חריפה באוזני הרמטכ"ל דן חלוץ על חוסר התוחלת במשימה שניתנה לכוחות: "כיבוש בינת ג'בייל מנוגד לרעיון הפיקודי להגיע לאזורי השיגור של הקטיושות ... מתוך חמש החטיבות שיש לנו, שחקנו שלוש על כלום, עוד לפני שהמלחמה הקרקעית נגד הקטיושות התחילה".[51]

ב־27 ביולי טען סגן הרמטכ"ל, אלוף משה קפלינסקי, שאמנם "אין משמעות צבאית טקטית לכיבוש בינת ג'בייל. יש כאן משמעות אחרת ... משמעות הסמל".[52] הרמטכ"ל חלוץ קיבל את עמדתו של קפלינסקי, וב־28 ביולי שוב ניתנה פקודה לכיבוש העיירה, אך היא בוטלה למחרת, לאחר ניסיון כיבוש נוסף של גדוד הצנחנים 101.[53] ב־1 באוגוסט הונחו כוחות מאוגדה 91 לצאת למתקפה נוספת לעבר בינת ג'בייל,[54] וגם כשצה"ל כבר החל להתכונן למהלך הקרקעי הגדול שנועד להרחיק את הקטיושות, הרמטכ"ל לא ויתר על כיבוש העיירה.[55] ב־7 באוגוסט קיבלה חטיבת הצנחנים פקודה להיכנס שוב לבינת ג'בייל, להגיע עד הבניין ששימש לפני

47 היימן ולוונהיים, "'שכר הולם'", עמ' 103; הראל ויששכרוף, **קורי עכביש**, עמ' 252.
48 עמיר רפפורט, "נתקלנו, יש נפגעים", **מעריב – מוסף שבת**, 13 ביולי 2007, עמ' 16־19.
49 נחום ברנע ושמעון שיפר, "היום הארוך ביותר", **ידיעות אחרונות – המוסף לשבת**, 28 ביולי 2006, עמ' 4.
50 רפפורט, "נתקלנו, יש נפגעים", עמ' 18.
51 שם.
52 לימור ושלח, **שבויים בלבנון**, עמ' 266.
53 **שם**, עמ' 191־192.
54 ועדת וינוגרד, עמ' 368.
55 רפפורט, **אש על כוחותינו**, עמ' 259.

הנסיגה במאי 2000 כמפקדת החטיבה המערבית ברצועת הביטחון, להניף שם את דגל ישראל ולצלם אותו. מבצע זה זכה לימים לכינוי האירוני "התקפת הדגל".[56] בנוסף, תוכננה תהלוכת ניצחון ברחובות העיירה: טור של טנקים ונגמ"שים היה אמור לנוע ברחובה הראשי, ונאום ניצחון מתאים, שנועד להפריך את טענותיו של נסראללה בדבר חולשתה של החברה הישראלית, נכתב מבעוד מועד עבור מפקד הכוח הכובש, מח"ט הצנחנים חגי מרדכי. לוחמים מצוידים במצלמות וידיאו וסטילס התבקשו לתעד את הנאום ההיסטורי ואת הנפת דגל ישראל מעל מבנה מפקדת החטיבה לשעבר.

המח"ט מרדכי הסתייג מהרעיון, והייתה לו סיבה טובה לכך: כאשר הפקודה הגיעה אליו, הוא כבר היה עם כוחותיו מספר קילומטרים צפונית לבינת ג'בייל, בדרך להשתלט על שטחים שמהם שיגר חזבאללה קטיושות לעבר ישראל.[57] בשלב זה של הלחימה, גם מפקד אוגדה 91, תת־אלוף גל הירש, לא תמך בכיבוש העיירה. "אנחנו כבר נמצאים קדימה", טען בפני אלוף בן ראובן. אלא שהאחרון הסביר למפקד האוגדה שאין ברירה: המטכ"ל מעוניין בהישג תודעתי.[58]

בתחילת הקרב נראה היה שמערך חזבאללה בעיירה עומד בפני קריסה, אלא שאז נפצע באורח אנוש אחד מלוחמי סיירת הצנחנים. החל קרב הרואי לחילוצו, שבמהלכו נהרג לוחם נוסף.[59] המשימה לא נזנחה, והוטלה הפעם על גדוד 890 של הצנחנים. בסופו של דבר צולם דגל ישראל כשהוא מתנוסס על בניין סמוך למבנה שעליו תוכנן להיות מונף.[60] התצלומים הועברו לחטיבת דובר צה"ל, אך נגנזו. תוצאותיו של קרב זה רק העמיקו את התביעה לנקוט מהלך דרסטי עוד יותר שישנה את התמונה התודעתית.[61]

מבצע "חד וחלק"

במהלך המלחמה נערכו מבצעים מיוחדים בעומק שטח האויב בהיקף שצה"ל לא ידע בעבר.[62] הדבר נבע מאמונתם של מקבלי ההחלטות שפעולת קומנדו מפתיעה בעורף האויב תאפשר להם להציג הישגים תודעתיים שיחזקו את אמון הציבור

---

56 עמוס הראל, "גרסת תא"ל הירש: הביקורת מתעלמת מהישגי אוגדה 91", **הארץ**, 11 בספטמבר 2006.

57 רפפורט, **אש על כוחותינו**, עמ' 259־260.

58 הירש, **סיפור אהבה סיפור מלחמה**, עמ' 352.

59 כפיר, **האדמה רעדה**, עמ' 207.

60 הראל וישששכרוף, **קורי עכביש**, עמ' 349.

61 לימור ושלח, **שבויים בלבנון**, עמ' 208.

62 אלכס פישמן, "משימה בלתי אפשרית", **ידיעות אחרונות – המוסף לשבת**, 27 באוקטובר 2006, עמ' 10; חלוץ, **בגובה העיניים**, עמ' 467; רונן כהן, "ההבדל בין פשיטה אסטרטגית לפשיטה טקטית", *Israel Defense*, 27 בפברואר 2012.

במנהיגות המלחמה.[63] לפיכך, לצד המאמץ לפגוע בצמרת חזבאללה, לחצו ראש הממשלה אולמרט ושר הביטחון פרץ על הרמטכ"ל חלוץ להוציא לפועל מבצעים מיוחדים בסגנון מבצע אנטבה:[64] "אני צריך משהו כמו צה"ל של פעם", צוטט ראש הממשלה.[65] במקום להתמודד עם איום הקטיושות ישירות, הרצון היה להוציא אל הפועל מהלך שינפץ סמל של חזבאללה ויספק תמונת ניצחון שתשפיע על התודעה.[66]

ביום התשיעי למלחמה הוקם צוות מיוחד באגף המבצעים, בראשות תת־אלוף טל רוסו,[67] והיחידות המיוחדות – סיירת מטכ"ל, שלדג, השייטת ואחרות – נכנסו לתכנון מבצעי, לצד חיפוש אחר מטרה שתספק את האפקט התודעתי הנדרש.[68] במקביל, פוזרו בקו החזית צוותים מיוחדים בתוך האוגדות.[69] בסך הכול נערכו במהלך המלחמה 24 מבצעים מיוחדים מצפון לנהר הליטני, רובם חסויים.

מבצע "חד וחלק" מהווה את אחת הפעולות הבודדות שזכתה לפרסום נרחב.[70] תוכנית המבצע, בה יועדו להשתתף כמאתיים לוחמים מסיירת מטכ"ל ומיחידת שלדג, הייתה לפשוט על בית חולים בבעל בק שבו, לפי ההערכות, טיפל רופא איראני בחיילים הישראלים החטופים, שחטיפתם הייתה העילה למלחמה.[71]

המבצע יצא לדרך ב־1 באוגוסט, וכונה על ידי שר הביטחון פרץ "המבצע שישנה את פני ההיסטוריה".[72] לאחר ארבע שעות במעוז חזבאללה שבו הכוחות ללא נפגעים לישראל. לא הייתה זו הפעם הראשונה במלחמה שבה הכוחות המיוחדים של צה"ל הגיעו לבעל בק, אך הפעם הפעולה הייתה "רועשת" במתכוון.[73] לאחר שנודע כי הרופא המבוקש אינו שוהה במקום, המשימות שנותרו היו לתפוס כמה

---

63 כפיר, **האדמה רעדה**, עמ' 191; לימור ושלח, **שבויים בלבנון**, עמ' 260.

64 מורן וינריך, **"האומנם דור חדש של לוחמה?": מלחמת לבנון השנייה**, חיבור לשם קבלת תואר מוסמך, אוניברסיטת בר אילן, המחלקה למדעי המדינה, רמת גן, 2010, עמ' 90.

65 ברגמן, "קריסת הקונספציה 2", עמ' 34.

66 Niccolo Petrelli,"The Missing Dimension: IDF Special Operations Forces and Strategy in the Second Lebanon War", *Small Wars and Insurgencies*, 23 no. 1 2012): 67.)

67 נחום ברנע ושמעון שיפר, "מלחמה בשלוש חזיתות", **ידיעות אחרונות – המוסף לשבת**, 4 באוגוסט 2006, עמ' 3.

68 כפיר, **האדמה רעדה**, עמ' 181.

69 אלכס פישמן, "משימה בלתי אפשרית", **ידיעות אחרונות – המוסף לשבת**, 27 באוקטובר 2006, עמ' 10–11.

70 עמיר רפפורט, "מסע אלונקות ברחובות צור", **מעריב – מוסף שבת**, 20 ביולי 2007, עמ' 12; Petrelli, "*The missing Dimension*",p. 64.

71 Petrelli, Ibid.

72 עפר שלח, "מלחמה כבקשתך", **מעריב** *nrg*, 17 בינואר 2009.

73 עמית כהן, דורון נחום ופליקס פריש, "120 ק"מ בעורף חזבאללה", **מעריב**, 3 באוגוסט 2006, עמ' 4.

שיותר שבויים, לאסוף מסמכים שעשויים להיות בעלי חשיבות מודיעינית ולהרוג כעשרים אנשי חזבאללה.[74]

המבצע הוכתר בהצלחה, אך לטענת רבים, הישגיו לא הצדיקו את הסיכון שהיה כרוך בו.[75] הן קצינים במטכ"ל והן קצינים בכירים בדימוס סברו כי הסיכון היה גבוה מדי לצורך משימה שערכה היה מוטל מראש בספק.[76] לטענתם, מטרות המבצע לא הצדיקו הפעלת כוחות כה גדולים, שעלולים היו להסתבך בתקרית מרובת נפגעים ואפילו בשבויים.[77] כך גרס גם הרמטכ"ל לשעבר יעלון: "יש סוג מסוים של פעולות שהסיכון הכרוך בהן הוא מאוד גבוה, לכן אתה יוצא אליהן רק כאשר ההישג שהן אמורות להביא הוא בעל חשיבות אסטרטגית ... אני לא בטוח שהפעולה בבעל בק לא הייתה הרפתקנית".[78]

למרות ההישגים הצנועים של המבצע, פתח הצבא בקמפיין תקשורתי. תמונות שצולמו במהלך המבצע הופצו על ידי דובר צה"ל ושודרו פעמים רבות בתקשורת,[79] ומפקד המבצע בשטח, אל"ם ניצן אלון, נשלח לתדרך את העיתונאים.[80] הצמרת המדינית והצבאית ביקשה להפגין בכך הישגים שיציגו מראית עין של ניצחון ישראלי.

היציאה למהלך קרקעי רחב בשלהי המלחמה

ב־11 באוגוסט הכריע ראש הממשלה בעד יציאה למהלך קרקעי רחב עד הליטני, חרף הידיעה כי באותה שעה עשויה להתקבל במועצת הביטחון של האו"ם החלטה על הפסקת אש.[81] ההחלטה לבצע את המהלך הקרקעי הייתה תמוהה, במיוחד נוכח ההערכות בדיונים שנערכו לקראתו, בהם דובר על אפשרות של מאות הרוגים.[82] שר הביטחון הבהיר שתנאי הפסקת האש לא ישתפרו כתוצאה מהמהלך הקרקעי, אך הוא ייצור את הרושם שישראל היא שנקטה את המהלך האחרון במלחמה ושלא היא מבקשת מהקהילה הבין־לאומית הפסקת אש כחבל הצלה ממלחמה כושלת, אלא היא זאת שממנה מבקשים להפסיק את הלחימה.[83]

---

74 רפפורט, "מסע אלונקות ברחובות צור", עמ' 13.
75 רפפורט, **אש על כוחותינו**, עמ' 217.
76 לימור ושלח, **שבויים בלבנון**, עמ' 254, 258.
77 הראל ויששכרוף, **קורי עכביש**.
78 כפי שצוטט בלימור ושלח, **שבויים בלבנון**, עמ' 258.
79 כפיר, **האדמה רעדה**, עמ' 192; לימור ושלח, **שבויים בלבנון**, עמ' 255; רפפורט, **אש על כוחותינו**, עמ' 222.
80 כפיר, **האדמה רעדה**.
81 חלוץ, **בגובה העיניים**, עמ' 462; Yaakov Katz, "Wadi Saluki Battle – Microcosm of War's Mistakes", *The Jerusalem Post*, August 29, 2006.
82 רפפורט, **אש על כוחותינו**, עמ' 295.
83 לימור ושלח, **שבויים בלבנון**, עמ' 311.

הדיונים בצה"ל ובדרג המדיני סביב היציאה למהלך עסקו רבות בשאלת "בימוי הניצחון": כיצד לקבע בתודעה את התחושה כי צה"ל יצא מהמלחמה כמנצח, למרות כל מה שאירע בארבעת השבועות הקודמים.[84] היטיבו לתאר זאת הראל ויששכרוף: "כמו חזבאללה, גם ישראל מחפשת עכשיו לא רק דימוי של ניצחון, אלא 'סיפור ניצחון', תיאור מסודר של השתלשלות העניינים, שיציג לציבור את סיום המערכה כהכרעה ישראלית, המצדיקה את הדם שנשפך ואת הבתים שנהרסו".[85] ואכן, הרמטכ"ל חלוץ טען בישיבת הקבינט ב־9 באוגוסט כי "המהלך הקרקעי דרוש פעמיים: כדי להשיג את המשימה של הקטנת הרקטות, ושנית – בגלל הדימוי. צה"ל צריך ויכול לפעול על הקרקע ולנצח".[86] דוח ועדת וינוגרד מעניק ביסוס לדברים אלה, בקבעו כי "מבצע 'שינוי כיוון 11' היה אמור להיות מהלך קרקעי רחב וגדול, שישנה מן היסוד הן את המציאות בדרום לבנון והן את דימוי המבצע מבחינה צבאית".[87] בעדותו בפני ועדת וינוגרד טען ראש הממשלה אולמרט כי "אם מארון א־ראס היה נראה אחרת, אם בינת ג'בייל הייתה נראית אחרת, יכול להיות שלא היינו צריכים להגיע בסופו של דבר לנקודה שהגענו אליה".[88]

אלא שאחרים היו סבורים כי היציאה למתקפה הסופית הייתה מוטעית ביסודה וכי מלכתחילה אסור היה שתתרחש, מכיוון שמלבד הישג תדמיתי, היא לא יכלה להביא לשום הישג אסטרטגי, בייחוד לאור העיתוי שבו יצאה לפועל.[89] כך, למשל, שר התחבורה מופז טען בראיון לאחר המלחמה כי "בשישים שעות [הזמן שהוקצב למהלך] אי אפשר להספיק לעשות פעולה שתוכננה להימשך כמה שבועות ... הכניסה המסיבית של כוחות קרקע ללבנון לא הייתה כורח צבאי ומדיני, אלא פרי תסכול מהיעדר הישגים. בצבא הבינו שהישגים ניתן להציג רק בשימוש בכוחות קרקע".[90] גם לטענת אלוף (מיל') דני יתום, מי שכיהן בעבר כראש המוסד, לא היה סיכוי שהתקיפה הקרקעית תביא להישג משמעותי, ובשישים שעות גם לא היה

84 הראל ויששכרוף, **קורי עכביש**, עמ' 398.

85 אבי ישששכרוף ועמוס הראל, "עוד מעט רעידת אדמה", **הארץ**, 11 באוגוסט 2006.

86 לימור ושלח, **שבויים בלבנון**, עמ' 309.

87 ועדת וינוגרד, עמ' 387.

88 עדותו של אהוד אולמרט בפני ועדת וינוגרד, זמין ב:
http://www.vaadatwino.gov.il/pdf/%D7%AA%D7%9E%D7%9C%D7%99%D7%9C%20%D7%90%D7%95%D7%9C%D7%9E%D7%A8%D7%98.pdf.

89 יאיר אטינגר ועמוס הראל, "הקרב הצליח, אומרים בצבא, אך לא ברור מה הייתה המטרה", **הארץ**, 22 באוגוסט 2006; יוסי בן־ארי, **מלחמת לבנון השנייה בראי הפרשנות של התקשורת הכתובה בישראל**, בית ספר רוטשילד־קיסריה לתקשורת, אוניברסיטת תל אביב, תל אביב, 2007, עמ' 24; נחום ברנע, "הימים האחרונים", **ידיעות אחרונות – המוסף לשבת**, 25 בינואר 2008, עמ' 4.

90 נחום ברנע ושמעון שיפר, "ככה לא עושים מלחמה", **ידיעות אחרונות – המוסף לשבת**, 15 בספטמבר 2006, עמ' 4.

שום סיכוי להגיע לליטני.[91] עמדתו של ראש חטיבת המחקר באמ"ן, תת־אלוף יוסי ביידץ, הייתה גם היא שפעולה ברגע האחרון לא תשפיע באופן מהותי על חזבאללה. ביידץ אף הבהיר את עמדתו במכתב ששלח לאולמרט, פרץ וחלוץ.[92] קצין בכיר נוסף שהתנגד לפעולה היה מזכירו הצבאי של ראש הממשלה, אלוף גדי שמני, שאף הביע את דעתו באוזני אולמרט, לפיה לא היה טעם להיכנס לפעולה זו באותו שלב.[93] אפילו אלוף בן ראובן, שהגה את תוכנית "מי מרום"[94] ולחץ כל העת לביצועה, טען כי "האישור לתוכנית ניתן לא בזמן, כשכבר לא היה סיכוי להגיע להישג מלא".[95] הרמטכ"ל לשעבר יעלון הביע את הביקורת החריפה ביותר על המהלך, כשכינה אותו "קרב להצלת המנהיגים":[96] "המהלך הזה היה מהלך סְפִּיני ... הוא נועד להשיג את תמונת הניצחון החסרה ... שלושים ושלושה חיילים נהרגו בעבור ספין ... לא עושים דבר כזה. לא שולחים חיילים למבצע סרק אחרי שהתוצאות המדיניות כבר נקבעו".[97]

נראה כי הלחץ הציבורי לביצוע מהלך קרקעי רחב, שיביא להישגים המיוחלים, הוא שהיטה את הכף: תוצאות סקר שנערך עבור עיתון "הארץ" הצביעו על כך שרק 28 אחוזים מן הציבור הביעו תמיכה בהפסקת אש מיידית, נוכח ההישגים המוגבלים שהסתמנו בזירה המדינית. זאת ועוד, מחקר של יוסי בן־ארי מראה כי המגמה הדומיננטית בפובליציסטיקה של התקשורת הכתובה הייתה אז "לדחוף את המדינה לקרב" כדי להשיג ניצחון, או לפחות "דימוי ניצחון", במטרה להשיב את ההרתעה הישראלית שנשחקה.[98]

סיכום

ישראל השקיעה במהלך מלחמת לבנון השנייה מאמצים רבים בניסיון לעצב את תודעת הציבור ולשכנעו בהצלחות המלחמה והישגיה, ובכך להגביר את הלגיטימציה הפנימית לפעולה ולנפגעיה. עם התמשכות המלחמה, גבר הצורך

91 דני יתום, **שותף סוד,** ידיעות אחרונות, ספרי חמד, תל אביב, 2009, עמ' 431.

92 רפפורט, **אש על כוחותינו**, עמ' 321־322.

93 שיף, "בכיר אמ"ן הזהיר מראש את רה"מ: הרחבת הפעולה – טעות".

94 תוכנית מגירה שכללה תמרון קרקעי רחב בלבנון וגובשה ערב מלחמת לבנון השנייה. למרות שהייתה עדיין בשלבי גיבוש מתקדמים, התוכנית יושמה תיאורטית בתרגיל "שילוב זרועות", שתרחיש הפתיחה שלו דמה לאשר עתיד היה לקרות ביולי 2006: חטיפה ברצועת עזה המובילה לחטיפה בצפון ואחריה קטיושות והסלמה במשך כמה שבועות. תוכנית "מי מרום" לא הספיקה לעבור את כל תהליך האישורים, וכך קרה שערב המלחמה לא הייתה תוכנית התקפה מאושרת ועדכנית.

95 לם, "מחדל המגירה".

96 יעלון, **דרך ארוכה־קצרה**, עמ' 210.

97 ארי שביט, "יעלון: חיילים מתו למען ספין; המנהיגים צריכים ללכת", **הארץ**, 14 בספטמבר 2006.

98 בן־ארי, **מלחמת לבנון השנייה בראי הפרשנות של התקשורת הכתובה בישראל**, עמ' 25.

בהצגת הישגים שייתפסו בציבור כמשמעותיים. במסגרת זו הוצאו לפועל מהלכים צבאיים שמטרתם הייתה תודעתית, אלא שבמקרים רבים, מהלכים אלה לא הצליחו ליצור את תודעת הניצחון הרצויה.

הדוגמאות שנסקרו במאמר זה נועדו להמחיש את המורכבות של קבלת ההחלטות ואת המתח בין הצורך להשיג הישגים במלחמה, בהם גם הישגים תודעתיים, ובין הסיכון בביצוע פעולות אלו. ללגיטימציה הפנימית היה תפקיד חשוב בשיקולים של מקבלי ההחלטות, עד כי הלחץ הציבורי להישג משמעותי הניע את הדרג המדיני להוציא לפועל מהלך קרקעי בשלהי המלחמה, אף שתכליתו האסטרטגית הייתה מוטלת בספק לנוכח הידיעה כי הפסקת האש קרובה.

הממצאים שהובאו לעיל מצביעים על הלחצים הסותרים מצד הציבור, שבהם נתונים בעת מלחמה מנהיגיהן של מדינות דמוקרטיות: מצד אחד, הציבור רוצה בהישגים מהירים ומרשימים, ומצד שני הוא מבקש שמספר הנפגעים יהיה קטן ככול האפשר. מקבלי ההחלטות שואפים לשמור על איזון עדין בין שתי הדרישות, אך לעיתים מוכרעת הכף על פי תפיסתם את הלכי רוחו של הציבור, המודד לאורך כל תקופת הלחימה את מטרותיה והישגיה למול מספר הנפגעים.

חששה של ההנהגה הישראלית מנפגעים והצורך שלה בלגיטימציה פנימית הובילו לעיתים, באופן פרדוקסלי, לביצוע פעולות שהיו כרוכות בסיכון לוחמים. ניתן לכן לטעון כי שיקולי לגיטימציה פנימית, ובכלל זה שיקולים הנוגעים למספר הנפגעים, הרווחים בעיקר במדינות דמוקרטיות, עלולים להשפיע באופן שלילי על שיקול הדעת של מקבלי ההחלטות בעת מלחמה.

קווים מנחים לניהול סיכוני סייבר

גבי סיבוני והדס קליין

תהליך הניהול של סיכוני סייבר הוא בעל חשיבות גבוהה ביותר כדי לשפר את מידת המוגנות והמוכנות הארגונית לאירוע סייבר. תהליך זה מהווה נדבך חשוב בניהול הסיכונים התפעוליים וכן בניהול הסיכונים הכולל של הארגון. במספר מגזרים במדינת ישראל מחויבים הארגונים לקיים תהליך ניהול של סיכוני סייבר על פי הנחיות הרגולטור. משרתו של מאמר זה היא לבחון את המתודה של ניהול הסיכונים ולהציע קווים מנחים לניהול סיכונים במרחב הסייבר, תוך אפיון השלבים העיקריים בתהליך זה.

מילות מפתח: ניהול סיכונים, המשכיות עיסקית, סיכוני סייבר, מרחב הסייבר

מבוא

במאי 2017 התפרסמו ידיעות בתקשורת על גניבת פרטי לקוחות של חברת Kmart. זוהי הפעם השנייה בתוך שלוש שנים שפרטי לקוחות החברה נגנבים. מספר בנקים קטנים בארצות הברית דיווחו שקיבלו התראות מחברות כרטיסי אשראי על כמה קבוצות של כרטיסי אשראי גנובים, שלכולם היה מכנה משותף: שימוש לצורך רכישות בענקית הקמעונאות Kmart. חברת "סירס", החברת האם של Kmart, אישרה בעקבות הפרסום שחלק ממערכות התשלומים שלה נפגעו על ידי קוד עוין. לדברי החברה, לא ניתן היה לזהות את הקוד באמצעות מערכות הגילוי המוקדם, אולם לאחר זיהוי האירוע, הנוזקה הוסרה מהמערכות. החברה האם לא התייחסה לשאלה כמה מ־735 החנויות של Kmart נפגעו מהאירוע.[1]

תגובתה של חברת "סירס" היא עדות נוספת לתובנה הידועה כי יש חשיבות קריטית למניעת אירוע סייבר, אף יותר מהיכולת לזהותו ולהתאושש ממנו. במקרה

ד"ר גבי סיבוני הוא ראש תוכנית ביטחון סייבר במכון למחקרי ביטחון לאומי. הדס קליין היא חוקרת בתוכנית ביטחון סייבר במכון למחקרי ביטחון לאומי.

1 Brian Krebs, "Credit Card Breach at Kmart Stores. Again", *KrebsOnSecurity*, May 2017, https://krebsonsecurity.com/2017/05/credit-card-breach-at-kmart-stores-again.

של Kmart, הדבר היה משמעותי במיוחד: החברה הותקפה לראשונה באוקטובר 2014 וטרם התאוששה מאז; מכירותיה ירדו ב־72 אחוזים ומחיר המניה שלה ירד ב־88 אחוזים מאז אירוע הסייבר הראשון.[2]

ההתייחסות לאירועי תקיפה אלה כרצף של אירועים בודדים ולא ככשל מערכתי עלולה להיות בעייתית, במיוחד כאשר היא גוררת התייחסות חסרה לפתרון שצריך להיות מערכתי. תהליכי ניהול סיכונים בסייבר ובמערכות המחשוב התומכות באים לענות בדיוק על בעיות מערכתיות כאלו. חברת Kmart לא סיפקה נתונים מפורטים על האירוע, אולם גורמים המעורים בנושא ציינו, שאף כי יתכן שמקור הבעיה היה גורם בשרשרת האספקה או רשלנות של עובד, ניתן להניח ששורש הבעיה בשני המקרים היה זהה: ניהול סיכונים גרוע, חוסר שקיפות בין־ארגונית וקושי לזהות קשרי גומלין בין מערכות שונות.[3]

ניהול סיכונים תפעוליים ופיננסיים בארגונים הינו תורה מפותחת הממומשת כיום באופן נרחב, וארגונים רבים מיישמים גישה זאת בשנים האחרונות גם בתחום של ניהול סיכוני מערכות מחשוב וסייבר. מטרתו של מאמר זה היא לספק לעושים במלאכה קווים מנחים ומתודולוגיה לביצוע תהליך של ניהול סיכונים במרחב הסייבר. תחילה תובא סקירה תיאורטית על תחום ניהול הסיכונים והיתרונות שהוא מספק לארגונים, ובהמשך תפורט הצעה לתהליך היישום בפועל.

תיאוריה של ניהול סיכונים

ניהול סיכונים הוא מתודה שהפכה לנושא ללמידה ומחקר לאחר מלחמת העולם השנייה. מקור הידע המודרני של תחום זה הם שני ספרים שעסקו בתיאוריה של ניהול סיכונים ויצאו לאור סמוך לאמצע שנות השישים של המאה העשרים.[4] התהליך החל סביב בחינת סיכוני שוק, במטרה להגן מפני הפסדים כספיים העלולים להיגרם כתוצאה מאירועים ותאונות. בשנות השבעים של המאה העשרים התפתח הנושא בשוק הביטוח ובמערכת הפיננסית, ככלי לניהול סיכונים פיננסיים של מוסדות בנקאיים, בנקים וחברות ביטוח. ניתוח הסיכונים התפעוליים וסיכוני הנזילות הופיע בתחילת שנות התשעים של המאה.[5] מאז הפך תחום זה לפרקטיקה מקובלת במגוון ארגונים, בהם חברות עיסקיות, חברות תעופה, רשויות מדינתיות וכדומה.

2 Steven Minsky, "Kmart Cyber Breach: Another Failure in Risk Management", *LogicManager*, July 26, 2017, https://www.logicmanager.com/erm-software/2017/07/26/kmart-cyber-breach.

3 שם.

4 R. I. Mehr, B. A. Hedges, *Risk Management in the Business Enterprise* (Homewood, Illinois: R. D. Irwin, 1963); A. Williams, M. H. Heins, *Risk Management and Insurance* (New York: McGraw Hill, 1964).

5 Georges Dionne, "Risk Management: History, Definition and Critique", *Risk Management and Insurance Review*, Vol. 16, no. 2, Fall 2013.

ניהול סיכונים בעולם העיסקי מתבצע בתחומים רבים, ובהם: ניהול סיכונים תפעוליים, כלומר, הבטחה שהתשתיות התפעוליות של הארגון ימשיכו לתפקד גם במקרה של תקלות במרכיבים מהותיים; ניהול סיכונים פיננסיים, בכלל זה סיכוני אשראי, סיכוני מטבע וסיכוני שוק; ניהול סיכונים של תאימות לרגולציה, לחוק או לאתיקה.

מטרתו של תהליך ניהול הסיכונים היא להפחית את השפעתם של אירועים חריגים על הארגון. התהליך כולל את ניסוח תרחישי הסיכון העשויים לפגוע בארגון, הערכת פוטנציאל הנזק בעת התממשותו, הערכת הסבירות להתממשות התרחיש, תעדוף בקרות לטיפול בתרחישים על פי עוצמתם, שהינו שילוב בין השפעת הסיכון ובין ההסתברות להתממשותו, ולבסוף ניסוח תוכנית להפחתת הסיכון. מחזור החיים של תהליך ניהול הסיכונים יכלול בדרך כלל כמה שלבים.

שלב א': הגדרת תיאבון הסיכון הארגוני

תיאבון הסיכון הוא כמות הסיכון ברמה כללית שהארגון מוכן לקבל כדי לקיים את מטרותיו.[6] זהו ביטוי לנכונות הארגון לסבול רמות חשיפה גבוהות/נמוכות לסיכון ולחוסר ודאות, כדי להשיג את יעדיו האסטרטגיים. מקובל שתיאבון הסיכון נקבע על ידי הדירקטוריון וההנהלה.

קביעת תיאבון הסיכון היא תהליך סובייקטיבי, שנועד לאזן בין התשואות הפוטנציאליות המתלוות לנטילת הסיכון ובין ההפסד הפוטנציאלי ממנו. מסגרות תיאבון הסיכון מספקות להנהלה תמונה ברורה באשר לרצון ליטול סיכון ופרספקטיבה לאיזון בין סיכון לתמורה. תיאבון הסיכון של הארגון אינו סטטי. ההנהלה עשויה לדרוש לשנות את שיעור הסיכון שהיא מוכנה ליטול, בהתאם לנסיבות המתפתחות על ציר הזמן.

שלב ב': זיהוי תרחישי סיכון

איתור סיכונים, באמצעות עבודת מחקר הכוללת ניסוח של תרחישי סיכון על בסיס ההיסטוריה של התממשות סיכונים בארגון ומחוצה לו. תהליך זה מתבצע באמצעות סקירת התהליכים העיסקיים הקריטיים של הארגון, שמטרתה היא להבין את התהליכים המשמעותיים ביותר לתפקודו. אלה כוללים לרוב תהליכים מעולמות הייצור, התפעול והמכירות; סקירת נכסי הארגון התומכים בתהליכים אלה (כגון, כוח אדם, תשתית מחשוב, מכונות וכדומה); ניתוח החשיפה של הארגון לסיכונים שיכולים להשליך על התנהלותו, כמו ניתוח סיכונים משקיים (האטה משקית) והאופן שבו הם יכולים להשפיע על היקף המכירות בחברה, או ניתוח

6 "Principles for An Effective Risk Appetite Framework", *Financial Stability Board*, November 18, 2013.

סיכונים מגזריים, כגון השפעה של מצבה הביטחוני של מדינת ישראל על מגזר תיירות החוץ; ולבסוף, בחינת דרישות החוק והרגולציה, כמו, למשל, השפעת חוקי בטיחות, חוקי בנייה ועוד.

שלב ג': ניתוח תרחישי סיכון

סיכון מוגדר כהסתברות של התרחשות מזיקה מוגדרת, בשילוב עם התוצאה הנובעת מאותה התרחשות. סיכון הינו, לפיכך, מכפלה של שני פרמטרים: הסבירות שיתרחש תרחיש כלשהו, והשפעת הנזק הצפוי במידה והוא יתממש. התוצאה של מכפלת שני המדדים האלה קרויה הסיכון השורשי. זיהוי תרחישי הסיכון יתבסס על עבודת מחקר שתכלול ניתוח אירועים דומים בהיסטוריה של הארגון ומחוצה לו, קבלת חוות דעת ממומחים, דוחות ניהול/סקרי סיכונים קודמים, דוחות כספיים, הליכים משפטיים, נתונים על תביעות ביטוח ועוד.

עוצמת הנזק נבחנת בפרמטרים של נזק ישיר ונזק עקיף כתוצאה מתרחיש של פגיעה בארגון. נזק ישיר יכול להיגרם, למשל, כתוצאה מפגיעה ברציפות התפקודית של הארגון על רקע השבתת מערכות ואי־יכולת לייצר כמתוכנן. נזק עקיף יכול להיות, לדוגמה, פגיעה במוניטין של הארגון כתוצאה מאי־יכולת לעמוד בהתחייבויות, מתביעות משפטיות ועוד.

שלב ד': גיבוש תוכנית להפחתת הסיכון

חלק גדול ממערך הפעולות, הכלים והתהליכים בהם משתמשים ארגונים לצורך הפחתת הסיכון נקרא בקרות. מערך הבקרות בארגון כולל את כל הכלים הקיימים בתהליכי העבודה המתקיימים באותו ארגון בהקשר למושאי הסיכון. לא ניתן להפעיל ארגון באופן אפקטיבי ללא מערכת בקרות שיטתית ותקינה.

ניתן לחלק את סוגי הבקרות המופעלות בארגון למספר משפחות:

- **נקיטת פעולות לצורך מניעה** – כלומר, נקיטת צעדים למניעת הסיבה לכשל, ובכלל זה על ידי שינוי אופן הפעילות של הארגון. למשל, יתכן ותהליך ייצור מסוים נמצא מסוכן מדי, ועל כן תחליט ההנהלה להימנע ממנו.
- **נקיטת פעולות הסטה** – העברה של השפעת הכשל לגורם חיצוני, כגון קבלן משנה או חברת ביטוח.
- **בקרה מונעת** – בקרה שמטרתה למנוע מבעוד מועד התרחשותה של פעולה שאינה רצויה. לדוגמה, הגבלת הרשאות ממוחשבות בתחנות מחשב קריטיות.
- **בקרה מגלה** – בקרה שמטרתה לגלות פעולות לא רצויות שהתרחשו, כך שיתאפשר לארגון לתקן אותן לאחר מעשה. לדוגמה, הפקת דוח חריגים לניתוח וניטור פעולות חריגות.

- **בקרה מתקנת** – בקרה שמטרתה לתקן פעולות לא רצויות לאחר מעשה. לדוגמה, שחזור אוטומטי של נתונים לאחר קריסה של מערכת המחשב.
- **בקרה מפצה** – בקרה שמטרתה לתת מענה במקום שבו הבקרות הקיימות אינן חזקות מספיק.

שלב ה': ניתוח הסיכון השיורי

הסיכון השיורי הינו הסיכון שנשאר לאחר הטמעת התוכנית להפחתת הסיכון. המצב הרצוי הוא שלאחר יישום הבקרות, רמת הסיכון השיורי תהיה נמוכה יותר מרמת הסיכון השורשי של התרחיש המנותח. כמו כן נדרש שרמת הסיכון השיורי תהיה בגבולות התיאבון לסיכון שנקבע. אם הסיכון השיורי אינו קביל (גבוה מדי), יש ליישם בקרות נוספות שיורידו את הסיכון השיורי לרמה קבילה, כפי שנקבע על ידי ההנהלה בהגדרת תיאבון הסיכון.

החשיבות של ניהול סיכוני סייבר

הקצב המהיר של השינויים הטכנולוגיים, הגידול בכמות השירותים הדיגיטליים וזמינותם, ההתממשקות עם מערכות ותיקות והצורך ההולך וגדל בקווי תקשורת עם ספקים, יוצרים כר נרחב להתפתחותם של איומי סייבר ולחשיפתם של ארגונים רבים לסיכוני סייבר משמעותיים. בד בבד, חלה בעשור האחרון עלייה מתמדת במספרם של גורמי איום, בהיבטים של יכולות, זמינות, כלי תקיפה וקבוצות תקיפה. כתוצאה מכך, היה זה אך טבעי לעבור לניהול סיכוני סייבר בשיטות של ניהול סיכונים. ואף על פי כן, הדרך עדיין ארוכה עד להטמעה מלאה של מתודות אלו כדבר של שגרה.[7]

לאחר פירוט הגישה הכללית והמקורות התיאורטיים, ראוי לבחון את יתרונותיו של תהליך ניהול הסיכונים במרחב הסייבר. ניהול סיכוני סייבר הינו חלק מניהול הסיכונים התפעוליים ומניהול הסיכונים הכולל של הארגון. על פי סקר של Deloitte ישראל, שנערך בשנת 2017, יש עלייה משמעותית במספר הארגונים המנהלים סיכוני סייבר.[8] כשישים אחוזים מהחברות הגדולות בישראל אוספות ומנתחות מידע לצורך קבלת תמונה עדכנית של איומי סייבר. עוד עולה מהסקר כי יותר מחמישים אחוזים מהחברות הגדולות במשק מקיימות מסגרת לניהול סיכונים ומפעילות מדיניות הגנת סייבר תאגידית, וכי מספר דומה של חברות גדולות ערכו סקר סיכוני סייבר רוחבי בשנה שקדמה לדוח. נתונים אלה גבוהים מהממוצע בקרב כלל המשק בישראל, ועם זאת, יש עדיין מקום לשיפור רב במצב.

7 "השוק הישראלי ואיומי סייבר – תמונת מצב 2017", **דלויט ישראל**, 2017, https://www2.deloitte.com/content/dam/Deloitte/il/Documents/risk/Deloitte_Cyber_Infographic1.2.pdf

8 שם.

אימוץ גישה של ניהול סיכונים בתחום ביטחון הסייבר כולל שורה של יתרונות:

- **יתרונות פיננסים –** הטמעה מיטבית של מערך הגנות סייבר ופיתוח מדיניות אבטחת מידע נאותה מונעים הפסדים ישירים, כגון גניבת כסף, וכן הפסדים עקיפים, כגון פגיעה במוניטין, ובנוסף לכך קנסות בגין אי־עמידה בדרישות החוק והרגולציה. לדוגמה, הפרת הוראות התקנה הבין־לאומית של האיחוד האירופי להגנה על נתונים (General Data Protection Regulation) גוררת קנסות מינהליים של עד עשרים מיליון אירו, או עד ארבעה אחוזים מסך המחזור השנתי – הגבוה מבין השניים.[9] מתקפת סייבר גם עלולה להשפיע על מחיר המניה של החברה, כתוצאה מפגיעה חמורה באמון הלקוחות ו/או פגיעה במוניטין ובמותג שלה.
- **יתרונות אסטרטגיים –** התמודדות נאותה עם אתגר הסייבר באמצעות מערך הגנות אופטימלי מספקת לארגון תמונה בהירה של החשיפה לסיכוני סייבר. הדבר משפיע על מידת האמון שרוחשים בעלי העניין והמשקיעים בארגון וביכולותיו להשיג את מטרותיו.
- **יתרונות משפטיים –** שמירה על המידע שהארגון מחזיק, כמו גם שמירה על יתר הנכסים הדיגיטליים שלו, מוגדרות במדינות רבות בעולם על פי חוק כאחריות של המנהלים וחברי הדירקטוריון.
- **יתרונות תפעוליים –** אירוע סייבר עשוי להיות בעל השפעה על מגוון היבטים תפעוליים, ובהם שרשרת האספקה, תמחור הייצור, כוח אדם ועוד. לדוגמה, אירוע סייבר, שבמסגרתו נפגעו קווי התקשורת עם ספקי החברה, עשוי לגרור שיבושים משמעותיים בתהליך הייצור.
- **המשכיות עיסקית** – שכלול יכולות ההתמודדות עם אירועי סייבר ישפיע ישירות על יכולת הארגון לממש המשכיות עיסקית, או לפחות להקטין את משך הזמן עד לשובו לעבודה.

אתגר ביטחון הסייבר נתפס לעיתים כבעיה הנוגעת לאנשי מערכות מידע, שבידיהם גם מצויים הפתרונות לה, אולם ברור כיום שהבעיה נוגעת לא רק לכלים טכנולוגיים. אתגר ביטחון הסייבר הינו רחב היקף וכולל אנשים, תהליכים ארגוניים, טכנולוגיה ומדיניות ארגונית. כל אלה ועוד מהווים נדבכים חשובים ביותר בביטחון הכולל של הארגון ובאיתנותו.

ניהול סיכוני סייבר

התממשותם של סיכוני סייבר עלולה לשבש את פעילותם התקינה והמאובטחת של ארגונים ולגרום, בין היתר, למניעת שירות, לחשיפת מידע עיסקי או מידע

9 סעיף 83 לתקנה 2016/679 (EU) של הפרלמנט האירופי: Regulation (EU) 2016/679 of the European Parliament and of the European Council, April 27, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

על לקוחות, למחיקה ושיבוש נתונים ועוד. מאפיין מהותי בניהול סיכונים הוא פוטנציאל הפגיעה. פוטנציאל הפגיעה בסייבר מתבטא לא רק בנזק למידע בהקשר של משולש הסודיות, השלמות והזמינות, אלא גם בהיבטים הנוגעים לסיכונים אחרים, כגון: מוניטין, חוק ורגולציה והמשכיות עיסקית.

בשנים האחרונות הופצו מספר הוראות רגולציה בנושא ניהול סיכוני סייבר, כמו, למשל, הוראה לניהול בנקאי תקין 361 של בנק ישראל בנושא ניהול הגנת הסייבר.[10] ההוראה דורשת מהבנקים בישראל לנהל את סיכוני הסייבר שלהם כדי לצמצם את הסבירות להתממשותם. במסגרת קביעת המתודולוגיה לניהול סיכוני סייבר, נדרשים ארגונים להעריך את תרחישי הסיכון ולבחון את מערך ההגנות שלהם.

הנחיית משרד האוצר[11] קובעת כי גוף מוסדי בישראל יעריך את סיכוני הסייבר שלו באמצעות נקיטת הצעדים הבאים: זיהוי תהליכים, מערכות ונכסי מידע; מיפוי הסיכונים לתהליכים, למערכות ולנכסי המידע; מיפוי סיכונים שורשיים; מיפוי והערכת הבקרות למזעור סיכונים אלה, לרבות בחינה של מידת ההשפעה של הבקרות עליהם; ולבסוף הערכת סיכון שיורי בהתאם להשפעת הבקרות שיושמו.

כדי ליישם עקרונות אלה, מוצע לפעול לאור תרחישי סיכון הנגזרים מהתהליכים בארגון ומנכסי המידע המיועדים להגנה, ולהמשיך בהגדרת התרחישים של סיכוני הסייבר אליהם חשוף הארגון. משם מוצע לעבור להערכת הסיכון השורשי במצב של התממשות התרחיש, לניתוח בשלותו של מערך בקרות הסייבר באמצעות ניתוח רמת ההטמעה שלו, ולאחר מכן לעבור לניתוח מידת היעילות של בקרות הסייבר הזמינות בארגון. לבסוף מוצע לנתח את הסיכון השיורי ואת הפערים בהגנה, וכנגזרת מכך לתעדף את הטיפול באותם פערים על ידי גיבוש תוכנית עבודה.

הגדרת תרחישי הסיכון

ראשיתו של תהליך הגדרתם של תרחישי הסיכון היא בניתוח התהליכים העיסקיים הקריטיים של הארגון, ולצידם ניתוח המערכות והנכסים הדיגיטליים התומכים בתהליכים אלה. המשכו של התהליך הוא בניסוח תרחישי התקיפה האפשריים בסייבר. שלב זה מבוסס על איסוף וניתוח מודיעיני, ובכלל זה ניתוח מגמות תקיפה וניתוח תוקפים פוטנציאליים, כאשר התרחיש כולל פעולה של תוקף. כאשר התרחיש הינו אירוע לא מכוון במרחב הטכנולוגי, יש לנתח תרחישי תקלות. את תרחישי התקיפה שנוסחו יש למפות לתהליכים קריטיים ולמערכות התומכות בתהליכים אלה.

---

10 "הוראה 361, ניהול הגנת הסייבר", *המפקח על הבנקים, בנק ישראל*, https://www.boi.org.il/he/BankingSupervision/SupervisorsDirectives/DocLib/361.pdf.

11 "ניהול סיכוני סייבר בגופים מוסדיים", *מדינת ישראל, משרד האוצר – אגף שוק ההון, ביטוח וחיסכון*, 31 באוגוסט 2016.

ניתוח התהליכים הקריטיים וניתוח המערכות והנכסים הדיגיטליים התומכים בתהליכים אלה מתבצעים באמצעות תהליך הנקרא Business Impact (BIA) Analysis. תהליך זה הינו חלק ממערך כלים רחב המיועד לתרום להמשכיות העיסקית ולעזור לארגון להתאושש במהירות האפשרית לאחר אירוע. BIA מהווה חלק מתוכנית ההתאוששות, בכך שהוא עוזר לאמוד את הנזקים השונים שנגרמו ואת חשיבותם היחסית של חלקי הארגון השונים. מסמך BIA ארגוני חסר לעיתים התייחסות להיבטים השונים של הסייבר, כגון סודיות ושלמות המידע. אם חסרה בו התייחסות כזאת, יש לעדכנה בהיבטי הסייבר הרלוונטיים. ניתוח BIA ומסמך אסטרטגיית הגנת הסייבר הארגונית צריכים לגזור רשימה מתועדפת של הנכסים הדיגיטליים המיועדים להגנה. במסגרת זו יש להגדיר את עקרונות ההגנה ויעדיה, כפי שהם מוכתבים על ידי דירקטוריון הארגון, הרגולטורים ובעלי עניין נוספים.

כדי להתמודד עם תרחישי התקיפה האפשריים במרחב הסייבר, נדרש לבצע הערכה של מרחב סיכוני הסייבר הארגוניים באופן שמתייחס למספר נקודות, ובהן: מיהם בעלי האינטרס לתקוף את הארגון? מהם יכולותיהם והכלים העומדים לרשותם? את מי הם תקפו בעבר וכיצד? הערכה זו אמורה להישען על תהליך מקדים של איסוף מודיעיני, הכולל ניתוח מגמות תקיפה, תוקפים פוטנציאליים וניתוח יכולותיהם.

איסוף מודיעיני הממוקד בצורכי הארגון מחייב להגדיר את רכיבי המידע הרלוונטיים לאיסוף. לעיתים מקובל לכנות פעולה זו צי"ח (ציון ידיעות חשובות). הצי"ח מגדיר את מגוון מקורות המידע הרלוונטיים ואת אזורי המיקוד לאיסוף מידע. למשל, ארגון בנקאי במדינת ישראל ראוי שימקד את איסוף המודיעין באיומים על התעשייה הבנקאית מצידם של ארגוני פשיעה, איומים שמקורם באויבים, ואף איומים שמקורם בארגונים אקטיביסטיים העשויים לפעול נגד מדיניות כלכלית מסוימת או נגד "קפיטליזם גלובלי".

תוצרי איסוף המידע משמשים לשתי מטרות עיקריות. הראשונה היא עדכון מתמשך של האיומים, שישמש את הפעילות הארגונית בהערכת המצב ובתגובה מהירה וממוקדת לאיומים חדשים; השנייה היא ניסוח תרחישי הסיכון איתם עשוי להתמודד הארגון, תוך ציון פרמטרים רלוונטיים לכימות האיום, ובהם סבירות הארוע, מידת הנזק ועוד. מקורות המידע לאיסוף המודיעין יכללו: מקורות מסחריים המספקים שירותי מידע (לאור צי"ח), מקורות זמינים חינמיים, שיתופי פעולה והחלפת מידע עם גורמים רלוונטיים, דוגמת מרכזי שיתוף מגזריים, גורמי CERT ואחרים, ולבסוף – מידע שמקורו במידע שהארגון מקבל מגורמי הנחיה.

הערכת הסיכון השורשי

תהליך הערכת הסיכון השורשי מבוצע בשני שלבים: הערכת פוטנציאל הנזק בהינתן התממשות התרחיש, והערכת הסבירות להתממשותו של התרחיש. הערכת פוטנציאל הנזק צריכה להתבצע תוך היוועצות עם הגורמים העיסקיים. אלה נדרשים להעריך את רמת הנזק הכספי בכל תרחיש, תוך ניתוח הסיכונים לנכסים העיסקיים האסטרטגיים, כפי שהוגדרו על ידי הארגון, ועליהם חשוב להגן. בנוסף, נדרש להעריך את הנזק הפוטנציאלי בכל תרחיש. לצד הנזקים הישירים, נדרש להעריך גם היבטים של נזק עקיף, כגון חשיפה לתביעות, חשיפה לעיצומים, פגיעה במוניטין ופגיעה ברציפות התפקודית.

הערכת סבירות התממשותו של התרחיש מתבצעת על פי רוב באמצעות מספר מדדים. הראשון שבהם נוגע לשכיחות התממשותו מבחינה היסטורית של תרחיש דומה בארגון דומה. יחד עם זאת, השוני בין אירועים בעולם התוכן של מתקפות סייבר והעובדה שקיים מגוון רחב מאד של תרחישי תקיפה ואירועים, גורמים לכך שלא ניתן להסתמך אך ורק על מדד זה, ונדרשים כלים נוספים כדי לאמוד את הסבירות להתממשות הסיכון. ניתן, לכן, לעשות שימוש בשני מדדים נוספים: הראשון הוא מדד המתאר את ההערכה הסובייקטיבית של צוות מודיעין הסייבר באשר לסבירות התממשותו של הסיכון, וזאת על בסיס הערכת המודיעין. הערכה זו מוצגת במדרג של 1־5, כאשר 5 מציין סבירות גבוהה להתממשות. המדד השני הוא רמת החשיפה המובנית, כלומר, עד כמה קל לתקוף את הנכסים המתוארים בתרחיש. החשיפה המובנת נקבעת לפי מאפיינים שונים של הסביבה הטכנולוגית הקיימת בארגון, כמו, למשל, כמות הממשקים, מספר המשתמשים, גישה לאינטרנט, ציוד תקשורת, קישוריות בין תחנות ועוד. לכל מאפיין קיימים מספר ערכים, המדַרגים את רמת החשיפה של הסביבה הטכנולוגית לתקיפות סייבר. גם הערכות אלו מתבצעות במדרג של 1־5, כאשר 5 מציין יכולת תקיפה בקלות מרובה. לדוגמה, ככל שיש לארגון יותר נקודות גישה לאינטרנט, כך קל יותר לתקוף אותו. ארגון בעל נקודת גישה אחת לאינטרנט יקבל, אפוא, ציון 1, וארגון בעל עשרות או מאות נקודות גישה לאינטרנט יקבל ציון 5. הערכה דומה מתבצעת לכל אחד מהמאפיינים. לצורך חישוב רמת החשיפה המובנית מבוצע שקלול של ממוצע הציונים בפרמטרים השונים.

חישוב מידת הסבירות להתממשות הסיכון מתבצע באמצעות הצבת מדד הערכת חוקר המודיעין (Analyst Score) ומדד החשיפה המובנית (Risk Exposure) במשוואה שלהלן, והערכת הסבירות תתבצע באמצעות הנוסחה הבאה:[12]

12 כל הערכים במדרג שבין 1–5.

$$RL\ (Risk\ Likelihood) = \frac{RE\ (Risk\ Exposure) \times AS\ (Analyst\ Score)}{5}$$

משוואה 1

RL הינה הסבירות להתממשות הסיכון, *RE* הינו ציון החשיפה המובנית, *AS* הינו ציון הניתן על ידי חוקר המודיעין לסבירות התממשותו של הסיכון. מטרת החלוקה ב־5 היא לאפשר לדרג את הסבירות בין 1־5.
הסיכון השורשי מחושב באופן הבא:

$$IR\ (Inherent\ Risk) = \frac{RL\ (Risk\ Likelihood) \times RI\ (Risk\ Impact)}{5}$$

משוואה 2

IR הינו הסיכון השורשי (Inherent Risk), *RL* הינה סבירות הסיכון (Likelihood) ו־*RI* הינו השפעת הסיכון (Impact).[13] מטרת החלוקה ב־5 היא לאפשר לדָרג את הסבירות בין 1־5.
תהליך הניתוח של המערכות התומכות בתהליכים הקריטיים בארגון, תהליך איסוף המודיעין וניתוחו לכדי איומים, והשלמת ניתוח הסיכון, מאפשרים להעריך את סיכוני הסייבר הקריטיים לארגון. להלן דוגמה:

שם האיום	שם האיום לצורך שפה משותפת
גורם האיום	גורם האיום מתוך המידע המודיעיני שנאסף
נתיב התקיפה	נתיב מימוש התקיפה מתוך המודיעין והמידע הטכנולוגי של הארגון
מערכת קריטית מושפעת	מתוך רשימת המערכות התומכות בתהליכים הקריטיים
סבירות	הערכת הסבירות להתממשות התרחיש
נזק	הערכת פוטנציאל הנזק בהתממשות התרחיש
הסיכון השורשי	מדד הסיכון השורשי, כפי שחושב בעזרת נוסחת הסיכון השורשי

13 הגישה המוצגת במאמר זה לחישוב הסיכון השורשי הינה אחת ממספר גישות קיימות, והיא מובאת כאן לצורך הדגמה.

הערכת בשלותן של הגנות הסייבר

מקובל לסווג את הבקרות בתחום הסייבר לשלוש משפחות עיקריות:

- הראשונה – בקרות מונעות (Preventives controls), המיועדות לסייע בניטור ובפיקוח על נתונים ופעילויות, במניעת שגיאות, מחדלים או נזק מכוון. דוגמאות לבקרות מסוג זה הן הפרדת תפקידים והרשאות, בקרת כניסה, איסוף וניתוח מודיעין סייבר.
- השנייה – בקרות מגלות (Detective controls), המסייעות באיתור חריגים. דוגמאות לבקרות מסוג זה הן מערכות לגילוי אנומליות בהתנהגות משתמשים, כגון משתמש העובד בשעות לא סבירות ומבצע פעולות שאינן בשגרת עבודתו ותפקידו.
- השלישית – בקרות מתקנות (Corrective Controls), המסייעות בעיקר להחזיר את המצב לקדמותו או לסייע בהשבת השגרה (לדוגמה, תהליך גיבויים ושחזורים), ואף לשפר את ההגנה.

ראוי שמערך הבקרות הכולל יותאם לארגון על פי צרכיו. קיימים כיום מספר תקנים והנחיות המתארים מבנה כללי של מערך בקרות. דוגמאות להם ניתן למצוא בהמלצות של מכון התקנים האמריקאי (NIST) המנחה ארגונים פדרליים,[14] ושל הגוף האמריקאי הפדרלי הקובע תקנים המיועדים למגזר הבנקאות בארצות הברית (FFIEC).[15] כמו כן, ניתן להסתייע בתורת ההגנה בסייבר שנכתבה על ידי מערך הסייבר הלאומי בישראל.[16] הערכת בשלות הבקרות מתבצעת עבור כל בקרה בנפרד, באמצעות ניתוח שני מדדים: מדד רמת ההטמעה של הבקרה ומדד מידת היעילות של הבקרה.

לצורך הערכת בשלות הבקרות יש לקיים ראיונות עם גורמים טכנולוגיים בארגון ועם גורמים נוספים, כגון היחידה לניהול סיכונים (אם יש כזאת). לכל בקרה יש לנסח טבלת דירוג ייחודית לה, שבמסגרתה יש להגדיר את סולם ההערכה של רמת הטמעת הבקרה בארגון. ניתוח זה מתבצע בהתאם לפרמטרים ייחודיים לכל בקרה. פרמטרים אלה מנוסחים במדרג של 1־5, כאשר 5 מבטא הטמעה מיטבית. בטבלה שלהלן ניתנת דוגמה להמחשת העניין. הדוגמה מנתחת את בקרת המודעות של העובדים לסיכוני סייבר:

---

14 "NIST Cybersecurity Framework", https://www.nist.gov/cyberframework;

15 "Cybersecurity Assessment Tool", *Federal Financial Institutions Examination Council (FFIEC)*, https://www.ffiec.gov/%5C/cyberassessmenttool.htm.

16 "תורת ההגנה בסייבר לארגון", *מערך הסייבר הלאומי, משרד ראש הממשלה*, https://www.gov.il/he/Departments/policies/cyber_security_methodology_for_organizations.

הערכת הטמעת הבקרה	ציון
לא קיים תהליך למודעות עובדים	1
תהליך בסיסי למודעות – הדרכות, עלונים, פורטל ארגוני	2
תהליך מתקדם למודעות – בסיסי, כולל תרגילים כלליים	3
קיים תהליך ארגוני מתקדם, כולל בקרה ומדידת ביצועים	4
קיים תהליך ארגוני מתקדם, לצד תהליך חיצוני, למודעות של שותפים עיסקיים לסיכוני סייבר	5

בנוסף, יש לקבוע לכל בקרה משקל המציין את חשיבותה למערך ההגנה הכולל של הארגון. המשקל נקבע במדרג של 1־5. ככל שהבקרה משמעותית יותר למערך ההגנה, כך משקלה מוערך כגבוה יותר. עם סיום תהליך הערכת המדדים הללו, ניתן לקבוע את ציון בשלות הבקרה באמצעות שימוש במטריצה שלהלן:

$CM =$

הטמעת הבקרה CA \ חשיבות הבקרה CI	1	2	3	4	5
1	5	3	2	1	1
2	5	3	2	2	2
3	5	4	3	3	3
4	5	4	4	4	4
5	5	5	5	5	5

בשלות הבקרה (CM) הינה פונקציה של חשיבות הבקרה (CI) ורמת הטמעת הבקרה בארגון (CA), ונקבעת בהתאם לערכי המטריצה.

ציוני בשלות הבקרות ייקבעו על פי הערכים המצוינים במטריצה. באופן זה ניתן לקבוע תוכנית מתועדפת לטיפול בבקרות. ככל שציון בשלות הבקרה נמוך יותר, כך הבקרה נמצאת בעדיפות גבוהה יותר לטיפול. משמעות הדבר היא שבקרות שנמצאות בראש הרשימה יתרמו באופן המיטבי לשיפור מערך ההגנות הכולל.

ערכי המטריצה מתייחסים למצבי קיצון, באופן הבא: אין צורך להשקיע משאבים בטיפול בבקרה בעלת חשיבות 1 (נמוכה). על כן, ערך בשלות הבקרה עבור כלל הבקרות בעלות חשיבות 1 הינו 5. בנוסף, אין רלוונטיות בהשקעת משאבים בטיפול בבקרה בעלת רמת הטמעה 5 (מרבית), ועל כן, ערך בשלות הבקרה עבור כלל הבקרות בעלות רמת הטמעה 5 הינו 5.

חשוב להתייחס גם לעלויות הטיפול בבקרה. כך, למשל, טיפול בבקרה שעלות התקנתה ותחזוקתה הינה יקרה באופן שיכַלה חלק משמעותי מתקציב מערך ההגנה, אינו בהכרח אפקטיבי, גם אם ההגנה נמצאת בראש רשימת העדיפויות. במקרה כזה ניתן לבצע נרמול, באופן שישקף את העלות היחסית של הבקרות.

ניתוח הסיכון השיורי

רמת הסיכון השיורי מתארת את פוטנציאל הנזק שעלול להיגרם לארגון כתוצאה מאירוע סייבר המתרחש לאחר יישום הבקרות הקיימות. כדי שהארגון יוכל להתמודד עם סיכוני הסייבר, עליו להעריך את רמת הסיכון השיורי עבור כל תרחיש בנפרד, כפי שהיא זוהתה בשלבים מוקדמים יותר בתהליך. חישוב הסיכון השיורי מבוצע בהתאם לנוסחה הבאה:

$$RR\ (Risidual\ Risk) = IR\ (Inherent\ Risk) - w \times CS\ (Control\ Score)$$

משוואה 3

כאשר: RR הינו הסיכון השיורי (Residual Risk), IR הינו הסיכון השורשי, CS איכות הבקרות הזמינות (Controls Score), ו־w הינו מקדם לאיכות הבקרות. לעיתים מקובל לקבוע מקדם עבור חישוב הסיכון השיורי, באופן שבו איכות הבקרות הזמינות מופחתת באחוז מסוים, כדי ליהנות מדרגת ביטחון גבוהה יותר בסיכון השיורי. למשל, קובעים כי ההתייחסות לאיכות הבקרות מופחתת בשלושים אחוזים. במצב כזה נדרש להציב בנוסחה $w=0.7$.

חישוב הסיכון השיורי מחייב להגדיר את הציון הכולל של מערך הגנות הסייבר בתרחיש הנדון, וזאת באמצעות הנוסחה הבאה:

$$OCM\ (Overall\ Control\ Maturity) = \frac{\sum_{i=1}^{n} CM_i\ (Control\ Maturity)}{n}$$

משוואה 4

ציון בשלות הבקרות הכולל (OCM) הינו ממוצע n ציוני בשלות הבקרות CM_i בתרחיש הנדון. חישוב הסיכון השיורי עבור כל תרחיש מתבצע באמצעות הנוסחה הבאה:

$$RR\ (Residual\ Risk) = IR\ (Inherent\ Risk) - w \times OCM\ (Overall\ Control\ Maturity)$$

משוואה 5

RR הינו הסיכון השיורי (Residual Risk), IR הינו הסיכון השורשי, CS היא איכות הבקרות הזמינות (Controls Score), ו־w הינו מקדם לאיכות הבקרות.

כעת יכול הארגון להעריך האם הסיכון השיורי תואם את תיאבון הסיכון, כפי שהוגדר על ידי הנהלת הארגון. אם מזוהים פערים, יש לשוב לפרק תעדוף הבקרות ולנסח תוכנית עבודה לשיפור מערך ההגנות, או לחילופין, להקטין פעילות מסוכנת בסייבר.

סיכום

מטרתו של מאמר זה היא לספק קווים מנחים לניהול סיכונים במרחב הסייבר, תוך הישענות על התיאוריה הבסיסית של דיסציפלינת ניהול הסיכונים שהתפתחה מאז שנות השישים של המאה העשרים. המאמר מציג גישה אחת לתהליך המוצע. קיימות גישות נוספות, אולם רובן ככולן נשענות על הבסיס התיאורטי של תורת ניהול הסיכונים.

ניהול סיכוני סייבר הינו מרכיב קריטי במסגרת ניהול מערך הגנות הסייבר הארגוני, לצד פעולות נוספות, דוגמת מבדקי חדירות. תהליך זה מאפשר לארגון להעריך את מידת הסיכון הניצבת מולו, מגדיר באופן מתודי את בחינת אמצעי ההגנה הארגוניים, ולבסוף מאפשר לארגון להעריך האם מידת החשיפה לסיכון תואמת את המוגדר והנדרש על ידי הדירקטוריון, הנהלת הארגון ובעלי העניין השונים.

מימוש הקווים המנחים שתוארו לעיל אינו ערובה למניעת אירועים במרחב הסייבר, אולם יש בו כדי להביא להבנה עמוקה יותר של הגורמים המטפלים במערך ההגנה נגד אותם סיכוני סייבר עימם הם נדרשים להתמודד. בכך הם יכולים לסייע רבות להקטנת הסיכונים מולם ניצב הארגון במסגרת צרכיו העיסקיים. לפי הערכת מומחים, הבעיה המערכתית שהתגלתה בחברת Kmart באירועי התקיפה שתוארו לעיל, הייתה מימוש גרוע של תהליכי ניהול הסיכונים.[17] מימוש תהליך ניהול סיכונים שיטתי וסדור יכול לסייע בצמצום החשיפה לסיכונים ובהקטנת הנזק התדמיתי והכספי העלול להיגרם באירועים מסוג זה.

17 Minsky, "Kmart Cyber Breach".

אבטחה של שרשראות אספקה קריטיות: הזדמנויות אסטרטגיות לקידום היוזמה להסמכה בין־לאומית של מוצרי סייבר

פול סטוקטון

סין, רוסיה ויריבים פוטנציאליים אחרים של ארצות הברית מגבירים את מאמציהם לפגוע בשרשראות האספקה עליהן מסתמכים רשתות חשמל וענפי תשתית אחרים. כבר כיום מתקיימות יוזמות חשובות לחיזוק ניהול הסיכונים בשרשרת האספקה, אולם למרות האמצעים שננקטו, קהילת המודיעין האמריקאית סבורה שההיקף והתחכום ההולכים וגדלים של ההתקפות על שרשרת האספקה "מציבים חלקים שלמים של הממשל והכלכלה שלנו בסיכון".[1] אתגרים דומים עומדים בפני ישראל, בריטניה ושותפות ביטחוניות אחרות של ארצות הברית. אין כיום תהליך מקיף, המקודם על ידי בעלי עניין, שיבטיח לבעלי תשתיות ולמפעיליהן שמוצרי חומרה ותוכנה חיוניים לא ייחשפו לתוכנות זדוניות או לאמצעי ניצול עוינים אחרים, ולו ברמה הבסיסית ביותר. תהליך הסמכה יתרום רבות לחוסנו של מרחב הסייבר, במיוחד אם גופים ממשלתיים יוכלו לספק מידע על איומים או לתמוך ביוזמה כזאת בדרכים אחרות.

היוזמה להסמכה בין־לאומית של מוצרי סייבר (Cyber Product International Certification – CPIC), שהעלתה המועצה לביטחון תשתיות החשמל (EIS Council) תסייע במתן מענה לאתגרים אלה. היוזמה תוכל לתרום עוד יותר לחוסן התשתיות, אם היא תכלול אמצעים להסמכת מוצרים כבטוחים מפני הפרעה אלקטרומגנטית מכֻוונת (IEMI).

מילות מפתח: סייבר, איומים, שרשרת אספקה, IT, OT, אנרגיה, CPIC

ד"ר פול סטוקטון הוא מנכ"ל Sonecon ולשעבר עוזר שר ההגנה של ארצות הברית לענייני ביטחון המולדת ונושאי הביטחון ביבשת אמריקה. רוברט דנאבורג, אנליסט בכיר ב"סונקון", ערך את המחקר לצורך מאמר זה. הממצאים וההמלצות הם על דעת המחבר בלבד ואינם משקפים בהכרח את עמדות משרד ההגנה האמריקאי או כל גוף ממשלתי אחר.

1 "Supply Chain Risk Management: Intelligence.Gov Background Paper", *National Counterintelligence and Security Center*, March 2017, p. 2, https://www.dni.gov/files/NCSC/documents/products/20170317-NCSC--SCRM-Background.pdf.

היקף האיום וחומרתו

הסיכונים הנשקפים מתוכנות ומחומרות רוסיות וסיניות לחוסן התשתיות (ולביטחון הלאומי בכללותו) זכו בחודשים האחרונים לבחינה קפדנית על ידי הממשל האמריקאי.[2] חלק מהמוצרים הנמכרים על ידי חברות כמו ZTE, Huawei או Kaspersky Labs מהווים רק את "קצה הקרחון" של מאמצים עוינים לחדור לשרשראות אספקה ולהשחית אותן כדי לאפשר ליריבים פוטנציאליים לבסס נוכחות מתמשכת ברשתות בארצות הברית ואצל שותפותיה לדרך.

המסמך "מדיניות אבטחת הסייבר" של המשרד לביטחון המולדת, ממאי 2018, מזהיר כי הקישוריות ההולכת וגוברת בין ענפי התשתית והשירותים המודרניים חושפת אותם לפגיעויות חדשות ו"פותחת פתח לתוצאות הרות אסון כתוצאה מאירועי סייבר".[3] אחת הסיבות לכך היא ההסתמכות הגוברת על שרשראות אספקה שהופכות גלובליות, והמספר ההולך וגדל במהירות של מכשירים המתחברים לרשת האינטרנט. מגמות אלו עתידות להעצים את האתגרים הכרוכים בניהול סיכונים בשרשרת האספקה, וזאת מבלי להמעיט בערכם של מאמצי החדשנות השמים דגש על שיפור האבטחה והחוסן של תחומים אלה.[4] זאת ועוד, למרות המערך הנוכחי של תוכניות במגזר הציבורי והפרטי, שנועדו לצמצם ולמנוע איומים על שרשרת האספקה, "ההתפתחות של איומים מכֻוונים, מתוחכמים ומרובי פנים מאיימת לגבור על אמצעי המנע שאנו נוקטים".[5] בהתחשב בסביבת האיומים הנוכחית ובמגמות בשרשרת האספקה הגלובלית, "ניהול סיכונים בשרשרת האספקה בסייבר אינו שאלה של בחירה",[6] אלא חובה.

גורמים עוינים אמנם אינם יכולים להחדיר מרחוק פגיעויות אלקטרומגנטיות, או לנצל באותה דרך פגיעויות קיימות, כפי שהם יכולים לעשות באמצעות נשק הסייבר, ואף על פי כן, קיימים כמה סיכונים גם בדרך פעולה זאת. לדוגמה, גורמים

2 ראו, לדוגמה: Danny Lam and David Jimenez, "US' IT Supply Chain Vulnerable to Chinese, Russian Threats", *The Hill*, July 9, 2017, http://thehill.com/blogs/pundits-blog/technology/341177-us-it-supply-chain-vulnerable-to-chinese-russian-threats; Joseph Marks, "Chinese Telecoms Could Join Kaspersky on Government Wide Banned List", *Nextgov*, February 13, 2018, http://www.nextgov.com/cybersecurity/2018/02/chinese-telecoms-could-join-kaspersky-governmentwide-banned-list/145960.

3 "Cybersecurity Strategy", *Department of Homeland Security*, May 15, 2018, p. 1, https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf.

4 שם, עמ' 22־23.

5 "Supply Chain Risk Management: Intelligence.Gov Background Paper", p. 2.

6 "Best Practices in Cyber Supply Chain Risk Management", *National Institute of Standards and Technology*, n. d., p. 1, https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-SCRM-Business-Case.pdf.

עוינים יכולים להחדיר לשרשרת האספקה של התשתיות רכיבים מזויפים או רגישים במיוחד לאיומים אלקטרומגנטיים. גורמים כאלה גם יכולים לנסות לנצל פגיעויות אלקטרומגנטיות ידועות בתוך רכיבים המצויים בפריסה רחבה, ובכך להגדיל את הנזק הפוטנציאלי שייגרם ממתקפה אלקטרומגנטית.

האיומים על שרשראות אספקה עולמיות הם מרובי ממדים, ויש מספר גורמים ומגמות המעצימים אותם. התגברות האיומים על שרשראות האספקה מחייבת התמודדות איתם, אך גם מציבה מספר אתגרים בפני אלה המנסים לצמצמם.

מספר הולך וגובר של כיווני איום

גורמים עוינים ממשיכים לחפש בהתמדה אחר דרכים חדשות לפגוע, לשבש ולנצל שרשראות אספקה. ואכן, המורכבות הגלובלית הגוברת של שרשראות אלו והתעצמות האיומים מצד גורמים עוינים הכפילו את הסיכון שספקים יכניסו למערכת או לרשת, במתכוון או שלא במתכוון, חומרה, תוכנה או קושחה ששובשו.[7] יוזמות חדשות בתחום מערכות מידע (IT), כמו מחשוב בענן או "התקנים מחוברים" (IoT), תרמו גם הן להרחבת תחומי החשיפה למתקפות סייבר על שרשראות האספקה,[8] הגדילו את מספר נקודות החדירה העשויות לשמש מטרה לגורמים עוינים ויצרו אתגרים נוספים עבור בעלי התשתיות ומפעיליהן, המבקשים לאבטח את שרשראות האספקה שלהם.

גורמים עוינים תרים אחר הזדמנויות לשבש כל נקודה אפשרית בשרשראות האספקה הגלובליות התומכות בתשתיות בארצות הברית. סיכונים קיימים בכל שלב – בתכנון, בייצור, באינטגרציה, בפריסה ובתחזוקה[9] – וגורמים עוינים עלולים להחדיר פגיעויות בשרשרת האספקה עצמה, או לנצל את הפוטנציאל של פגיעויות קיימות שעדיין לא טופלו על ידי מומחי האבטחה.[10]

גם אם פגיעויות אינן קיימות בפיתוח הראשוני, גורמים עוינים יכולים להחדירן בכל שלב במחזור החיים של המערכת.[11] אפשרויות אלו כוללות עדכוני תוכנה או

7 שם, עמ' 1.

8 Jon Oltsik, "Protecting the Cyber Supply Chain", *Cipher Brief*, December 6, 2015, https://www.thecipherbrief.com/article/protecting-cyber-supply-chain.

9 "Supply Chain Risk Management: A Framework for Assessing Risk", *National Counterintelligence and Security Center*, February 2013, p. 2, https://www.dni.gov/files/NCSC/documents/products/SCRM_Framework_for_Assessing_Risk_White_Paper.pdf.

10 "Identifying and Mitigating Supply Chain Risks in the Electricity Infrastructure's Production and Distribution Networks", *Public-Private Analytic Exchange Program*, 2016, p. 4, https://www.dni.gov/files/PE/Documents/Electricity-Infrastructure-Summary.pdf.

11 "Task Force on Cyber Supply Chain", *Defense Science Board*, February 2017, p. 1, https://www.acq.osd.mil/dsb/reports/2010s/1028953.pdf.

"טלאים" שנועדו לטפל בפגיעות של מערכות מחשוב (IT) ומערכות בקרה (OT). בתרחיש כזה מחדירים למערכת קוד זדוני או קושחה ממאירה שנועדה להפעלה במועד מאוחר יותר.[12] התדירות שבה מפעילי מערכות מיישמים עדכוני תוכנה יוצרת הזדמנויות רבות לגורמים עוינים לחבל באותן מערכות, גם זמן רב לאחר שלב התכנון.

גורמים עוינים גם עלולים לחבל בחומרה שחברות תשתית מתקינות במערכת ההפעלה שלהן. לדוגמה, דוח של המועצה למדע הביטחון (Defense Science Board) ציין מספר רב של פגיעויות פוטנציאליות ברכיבי מיקרואלקטרוניקה שבשרשרת האספקה. הדוח התמקד אמנם במערכות נשק, אך רכיבי מיקרואלקטרוניקה דומים נמצאים בשכיחות גוברת בכל ענף תשתית. רכיבי מיקרואלקטרוניקה כאלה "כוללים באופן בלתי נמנע פגיעויות בלתי נראות לעין", שניתן יהיה לגלותן, אם בכלל, רק שנים לאחר שהמוצר נכנס לשירות. ההשפעות האפשריות שלהן נעות בין פגיעה בפעולת המערכת ובין כשל מלא שלה.[13]

עדכוני תוכנה מועדים במיוחד לפגיעות עוינות, שמטרתן היא להשיג גישה ארוכת טווח לרשתות המודיעין הנגדי, מתוכן יוכלו אותם גורמים עוינים לשגר בשלב מאוחר יותר מתקפות לשיבוש פעולות בתחום התשתיות. כך, למשל, מבצע Dragonfly הרוסי התמקד תחילה "בארגונים פריפריאליים, כגון ספקי צד שלישי, שהרשתות שלהם היו פחות מאובטחות", כשהוא משתמש בהם כנקודות מוצא לפגיעה בקורבנות המיועדים.[14] חברת Dragos – חברת אבטחת סייבר במערכות בקרה תעשייתיות (ICS) – שרטטה לאחרונה פרופיל של גורם מאיים ששם על הכוונת שלו רשתות ICS, בין היתר באמצעות מתקפות מסוג watering hole.[15] מתקפות אלו נועדו לגנוב מיומנויות ולהשיג גישה לרשתות ולמכונות של הקורבנות.[16]

---

12 "Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector: Recognizing Risks and Recommended Mitigation Actions", *The Public-Private Analytic Exchange Program*, 2017, p. 12.

13 "Task Force on Cyber Supply Chain", pp. 1-2.

14 "Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors", *Department of Homeland Security*, *United States Computer Emergency Readiness Team*, last updated March 16, 2018, https://www.us-cert.gov/ncas/alerts/TA18-074A.

15 תקיפת אתרים לגיטימיים הרלוונטיים למושאי התקיפה, בדרך כלל אתרים טכניים וחדשותיים בתחום המקצועי, באופן שגישה אליהם תגרום לתקיפת מערכות המשתמשים.

16 "CHRYSENE", *Dragos Inc*., May 17, 2018, https://dragos.com/blog/20180517Chrysene.html.

בעלות נסתרת וגלובליזציה של ספקים בשרשרת האספקה

שרשראות האספקה הופכות לגלובליות. ככל שהן נעשות יותר מורכבות ובין־לאומיות, כך עולה היכולת של גורמים עוינים "לחדור לשרשרת האספקה בנקודות מרובות ולבסס בהן מראש פעולות חתרניות מתמשכות ורחבות ממדים".[17]

שליטה, השפעה ואפילו בעלות של ממשלות חורשות רע או תאגידים המזוהים עם ממשלות כאלו על נקודות לאורך שרשרת אספקה גלובלית הן תופעות מטרידות במיוחד. קודים של תוכנות וקושחות מפותחים על ידי ספקים במספר רב של מדינות, ומצב זה "פותח פתח לשפע של הזדמנויות עבור אויביה של ארצות הברית, כמו רוסיה וסין, להחדיר פגיעויות לתוך מערכות שונות, באופן שיאפשר לשירותי המודיעין של אותן מדינות לנצל אותן בשלב מאוחר יותר".[18] חששות דומים קיימים גם לגבי הפוטנציאל שיש לגורמים עוינים להחדיר לשרשראות האספקה רכיבים הפגיעים במיוחד לאיומים אלקטרומגנטיים.

סין גם שולטת ברמה גלובלית ביכולת הייצור וההרכבה של כל הקשור בתחום מערכות מידע.[19] רבים ממוצרי החומרה הנמצאים ברשתות המשרתות תשתיות מכילים רכיבים המיוצרים בסין, דבר שעלול לחשוף אותם לסיכון של הדבקה וזיהום. עדות לאיום פוטנציאלי זה ניתן לראות בדאגה שהביעו לאחרונה גורמי מודיעין ומחוקקים אמריקאיים במהלך דיון שנערך בקונגרס בנוגע לחדירה הסינית לתחום הטלקום, ובמיוחד לחוזי הצטיידות פוטנציאליים עם הממשל והתעשייה האמריקאיים.[20] ארצות הברית גם אסרה על שימוש במוצרים של החברה הרוסית AO Kaspersky Lab בכל מערכות המידע הפדרליות, כשהיא מנמקת זאת בשיקולי ביטחון.[21]

ואכן, גורמים עוינים יכולים למנף את הגישה למערכות כאלו להתקפות זדוניות. יתר על כן, יריבים פוטנציאליים כבר מנסים לחתור תחת יוזמות לניהול סיכונים בשרשרת האספקה, וסביר להניח שאף יצליחו בכך בשנים הקרובות. דוגמה בולטת לכך היא חברת Huawei Technologies – חברת טכנולוגיה סינית החבֵרה במספר

---

17. "Supply Chain Risk Management: Intelligence.Gov Background Paper", p. 1.
18. Joseph Marks, "DHS to Scrutinize Government Supply Chain for Cyber Risks", *Nextgov*, February 14, 2018, http://www.nextgov.com/cybersecurity/2018/02/dhs-scrutinize-government-supply-chain-cyber-risks/145998/.
19. Lam and Jimenez, "US' IT Supply Chain Vulnerable to Chinese, Russian Threats".
20. Marks, "Chinese Telecoms Could Join Kaspersky On Government Wide Banned List".
21. "Notification of Issuance of Binding Operational Directive 17-01 and Establishment of Procedures for Responses", *Department of Homeland Security, Federal Register*, 82, no. 180, September 19, 2017, p. 43782, https://www.federalregister.gov/documents/2017/09/19/2017-19838/national-protection-and-programs-directorate-notification-of-issuance-of-binding-operational.

ארגוני אבטחת סייבר המקדמים יוזמות לניהול סיכונים בשרשרת האספקה, ובהם Open Group (עם תוכנית הסמכה המבוססת על תקן שפיתחה: Open Trusted Technology Provider – O-TTPS)[22] ו־SAFECode (שגיבשה נהלים בסיסיים לפיתוח תוכנה מאובטחת).[23] בנוסף לאיומים ישירים על שרשרת האספקה, הצפי הוא שניהול הסיכונים עצמו יהפוך גם הוא למטרה פוטנציאלית למאמצי חדירה של גורמים עוינים.

העמימות והמורכבות של שרשראות האספקה

ככל ששרשראות האספקה הופכות לבין־לאומיות, כך הן גם הופכות למורכבות יותר. תהליך הגלובליזציה מאופיין ב"רשת מורכבת של ספקים וקבלני משנה של חלקי רכיבים, שירותים וייצור, המתפרסים בכל רחבי המדינה וגם ברחבי העולם", כאשר ריבוי השכבות והרשתות של הספקים יוצר לעיתים בלבול.[24] מכון התקנים הלאומי של ארצות הברית (NIST), שהוא בעל עניין עיקרי בנושא ניהול סיכונים בשרשרת האספקה, מזהיר מפני הקושי הגובר לסנן ספקים ומוכרים. ואכן, חברות רבות מתקשות לסנן שותפים לשרשרת האספקה מעבר לשכבה הראשונה שלהם.[25] עם זאת, רבים מבעלי התשתיות ומפעיליהן תלויים ב"מערכת מורכבת של שרשראות אספקה, שיש ביניהן קישורים הדדיים ושיטת הפצה גלובלית", המשרתת מוצרים ושירותים, ובהם שכבות מרובות של מיקור חוץ וערוצי הפצה מגוונים.[26] גורמים עוינים מסוגלים לפעול באמצעות חברות קש, ארגונים ויחידים כדי להסתיר את נוכחותם, כשהם פועלים לפגוע במאמצים לחשוף אותם ולפעול נגד מהלכיהם.[27]

המספר ההולך וגדל של מוכרים וספקים חיצוניים לחברות חשמל גורם לכך ש"לעיתים מתקשים נותני השירות להבטיח את שלמות שרשרת האספקה".[28] ואמנם, קיימת אפשרות כי מוצרים שעלולים להיות מסוכנים ימצאו את דרכם לתוך מערכות תשתית ללא ידיעת הבעלים.

---

22 "Standard Open Group Membership", *The Open Group*, last updated June 5, 2018, http://reports.opengroup.org/membership_report_all.pdf.

23 "Members", *SAFECode*, https://safecode.org/members/.

24 "Supply Chain Risk Management: Intelligence.Gov Background Paper", p. 1.

25 "Best Practices in Cyber Supply Chain Risk Management: Vendor Selection and Management", p. 1.

26 "Cyber Supply Chain Risk Management".

27 שם, עמ' 2.

28 "Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector", *Mission Support Center, Idaho National Laboratory*, August 2016, p. 15, https://bit.ly/2G4OQrH.

החיבור הגובר בין מערכות מחשוב למערכות בקרה

החיבור ההולך ומתחזק בין מערכות מחשוב (IT) ובין מערכות בקרה (OT) מגביר את הסיכונים של מתקפות סייבר ואת השלכותיהן. מערכות OT, כגון מערכות שליטה, פיקוח ורכישת נתונים (SCADA), או מערכות בקרה תעשייתיות (ICS), הופכות לנפוצות בתוך מערכות התשתית. למרות שמערכות OT כאלו פעלו בעבר ברשת נפרדת ומנותקת מרשתות IT, כיום השתיים הולכות ויוצרות בהדרגה חיבור ביניהן.[29] תהליך זה גורם לפגיעויות ומגדיל את פני השטח החשופים למתקפות סייבר, אך יותר מכך מטרידה העובדה שבמקרה של פגיעה במערכות OT, במיוחד אם מדובר בפגיעה בקנה מידה גדול, עלולות להיות לכך השלכות פיזיות ישירות, ואולי אף הרות אסון, על התשתיות.

ההתקדמות בניהול סיכונים בשרשראות האספקה בתעשייה ובממשל

יוזמות חשובות לניהול סיכונים בשרשרת האספקה הולכות ומתרבות ונמצאות כיום בעיצומן. למעשה, יוזמות כאלו צומחות במהירות כה רבה, עד שאין אפשרות להציג סקירה מקיפה ועדכנית שלהן. להלן ייעשה ניסיון ראשוני להציג סקירה כזו. מדובר ברשימה שאינה ממצה את כל ההתפתחויות, ואין ספק שכמה מהיוזמות לניהול סיכונים בשרשרת האספקה הוחמצו בה, אך עם זאת, היא תכלול רבות מהיוזמות החשובות.

המאמצים לקידום ניהול סיכונים בשרשרת האספקה יכולים להתממש בדרך של קביעת תקנים, אימוץ שיטות עבודה מומלצות או נקיטת אמצעים רגולטוריים אחרים, וכולם מתמקדים באותה מטרה: "זיהוי, הערכה ומניעה של הסיכונים למוצרים ושירותים של IT/OT, הנובעים מטבען המבוזר והמקושר של שרשראות האספקה".[30] על היוזמות לניהול הסיכונים לתת מענה "למחזור החיים המלא של המערכת (לרבות תכנון, פיתוח, הפצה, פריסה, רכישה, תחזוקה והרס), שכן איומים ופגיעויות בשרשרת האספקה עלולים, במתכוון או שלא במתכוון, לחבל בכל מוצר או שירות IT/OT בכל שלב שלו".[31]

רבות מהיוזמות שיפורטו להלן עוסקות בהערכת סיכונים בשרשרת האספקה ומנסות לצמצם אותם, לעיתים עבור תחום או ענף תשתיות מסוים. תחילה ייבחנו יוזמות לניהול סיכונים בענף החשמל, ובהמשך יתוארו יוזמות לניהול סיכונים

---

29 "Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector", p. 4.

30 "Cyber Supply Chain Risk Management".

31 שם.

בשרשראות אספקה מרובות תחומים. לצידם יובא פירוט של יוזמה חדשה בתחום זה, המסתמנת כמבטיחה מאוד, אותה מובילה חברת "סימנס".

יוזמות בתחום האנרגיה

תחום האנרגיה, ובעיקר ענף החשמל, ממלאים תפקיד קריטי בהפעלת כל ענפי התשתית במשק. האיומים על תחום זה הם חמורים במיוחד ומהווים גורם מניע, הן למאמצי התעשייה והן למאמצי הממשל, להתמודדות עם ריבוי האתגרים הכרוכים בכך. למרות זאת, המאמצים להגדיר את הדרישות ואת תחומי המחקר והפיתוח לאבטחת שרשראות האספקה עבור טכנולוגיות רשת החשמל אינם מצליחים להדביק את הצרכים, למרות כל הידוע על איומים מצד גורמים עוינים ועל הסיכונים הגוברים הנובעים מהאופי הגלובלי של שרשראות האספקה.[32] יחד עם זאת, כמה יוזמות חשובות נמצאות בתכנון ועשויות להוות את הבסיס להמשך המאמצים בעתיד.

משרד האנרגיה של ארצות הברית

משרד האנרגיה האמריקאי, כגוף העוסק ספציפית בתחום האנרגיה בארצות הברית, פועל לתת מענה לפגיעויות סייבר בשרשרת האספקה בתחום זה. המדריך שהוציא המשרד, שכותרתו "הנחיות לרכש מוצרים לאבטחת סייבר עבור מערכות לאספקת אנרגיה", שגובש בשיתוף עם התעשייה, מצייד את נותני השירותים ב"אסטרטגיות והנחיות מומלצות שיסייעו לתחום האנרגיה בארצות הברית ולספקי הטכנולוגיה לבנות הגנות סייבר, תוך כדי התכנון והייצור של המוצר".[33]

משרד האנרגיה האמריקאי גם פרסם במארס 2018 את "התוכנית הרב־שנתית לאבטחת סייבר בתחום האנרגיה". בין המטרות והיעדים של התוכנית מצוינת החובה "לצמצם את הפגיעויות והסיכונים הקריטיים באבטחת סייבר של שרשרת אספקה".[34] כדי לעשות זאת, מתכנן משרד האנרגיה לנקוט את הצעדים הבאים:

- **זיהוי הפעולות שעל הממשלה הפדרלית לנקוט כדי לצמצם את הסיכונים בשרשרת האספקה**: משרד האנרגיה ישתף פעולה עם גורמים פדרליים אחרים כדי לזהות ולנקוט את הפעולות המתאימות לצמצום סיכוני אבטחת סייבר

32 "Identifying and Mitigating Supply Chain Risks", p. 2.

33 "Energy Department Releases New Guidance for Strengthening Cybersecurity of the Grid's Supply Chain", *Department of Energy*, April 28, 2014, https://www.energy.gov/articles/energy-department-releases-new-guidance-strengthening-cybersecurity-grid-s-supply-chain.

34 "Multiyear Plan for Energy Sector Cybersecurity", *Department of Energy*, March 2018, p. 6.

בשרשרת האספקה, ויסייע לבניית אמון בין בעלים ומפעילים ובין יצרני מערכות בקרה תעשייתיות (ICS) בתחום האנרגיה.

- **פיתוח מעבדת בדיקה וניתוח של מערכות אספקת אנרגיה**: לנוכח האיומים המתפתחים ופגיעויות חדשות המתגלות ומנוצלות על ידי גורמים עוינים, נדרשות יכולות לאומיות שיעריכו את סיכוניהם, יגבשו שיטות חלופיות וישתפו פעולה עם יכולות סייבר נוספות של הממשל ושל המגזר הפרטי, כדי לחלוק מידע מעשי בדרך המהירה ביותר. משרד האנרגיה ייצור בתוך מעבדות לאומיות יכולת בדיקה פיזית של הסייבר, כדי לנתח פגיעויות במערכות וברכיבים שונים, איומים מצד תוכנות זדוניות והשלכות של איומים מסוג "מתקפת אפס ימים" על תשתיות אנרגיה. כמו כן, יתמוך המשרד ביוזמות להקשיח את שרשרת האספקה. צעדים אלה יושגו על ידי פיתוח דרישות ושיתוף פעולה בין המעבדות הלאומיות ובין המגזר הפרטי.[35]

תוכנית אבטחת הסייבר של משרד האנרגיה האמריקאי לשנת 2018 גם מדגישה את חשיבות המחקר, הפיתוח והצגת כלים וטכנולוגיות לסיוע במניעת אירועי סייבר. כשמדובר ספציפית בניהול סיכונים בשרשראות האספקה, על כלים אלה לשאוף "להקטין את הסיכון הנשקף ממערכת זדונית, שעשויה להיות מוחדרת באמצעות רכיבים ומערכות העוברים בשרשרת האספקה".[36] משרד האנרגיה והגורמים השותפים לו כבר השיגו התקדמות מסוימת לקראת יעד זה. התוכנית של המשרד מציינת כי "שיתוף הפעולה המחקרי של משרד האנרגיה מקדם כלים וטכנולוגיות שיסייעו בזיהוי גורמים בלתי רצויים ובעלי פוטנציאל זדוני, שאולי הוכנסו לחומרה, לקושחה או לתוכנה של רכיבי מערכת אספקת האנרגיה דרך שרשרת האספקה". התוכנית כוללת גם "הנחיות לנוסח הדברים שבו ישתמשו רוכשים וספקים של מערכות אספקת אנרגיה, כבסיס לדיון באמצעי אבטחת הסייבר הדרושים למערכות אספקה אלו". כן מסייעת התוכנית "להבטיח את תקינות כל העדכונים והשדרוגים".[37]

האסטרטגיה של משרד האנרגיה האמריקאי קוראת ל"פיתוח קוד מאובטח והבטחת איכות התוכנה (1.2 ו־1.3): ניתן ליישם שיטות קידוד מאובטחות ובטוחות על מוצרים חדשים, אך עלותן הגבוהה, התנגשות עם מוצרים מדור קודם וחוסר ביקוש ממשיכים להיות חסמים מרכזיים בתחום זה. נדרשת השקעה משמעותית בהעלאת המודעות ובהכשרת כוח אדם. סיכוני שרשרת האספקה ממשיכים להיות סוגיה מרכזית".[38]

---

35 שם, עמ' 25.
36 שם, עמ' 34.
37 שם, שם.
38 שם, עמ' 45.

התייחסות משרד האנרגיה להוראה הנשיאותית מספר 13800 – "חיזוק אבטחת הסייבר של רשתות פדרליות ותשתיות קריטיות", שפורסמה במאי 2017, מהווה התקדמות מעודדת, אם כי עדיין לא הגיעה לשלב מימוש. דוח של משרד האנרגיה מכיר בחומרת האיומים בשרשרת האספקה על רכיבי רשת החשמל, ומדרבן את המשרד "לפתח תוכנית לבדיקות של מרכיבי הרשת על ידי מעבדות לאומיות, כדי להעריך את מצב אבטחת הסייבר של שרשרת האספקה ולבחון בסימולציות את ההשפעות של תוכנות זדוניות במרחב הסייבר על רכיבים [ברשת החשמל]".[39] לא ברור כמה התקדמות חלה בנושא זה, אם בכלל, שכן משרד האנרגיה המליץ על הדברים רק באוגוסט 2017.

משרד האנרגיה פועל, יחד עם המעבדות הלאומיות הכפופות לו, כדי לבצע גם בעצמו בדיקות של מוצרים בתחום האנרגיה החשמלית. מתחם הניסויים של תשתיות קריטיות של המעבדה הלאומית של איידהו (INL), הכולל "מתקני ניסוי" לרשת החשמל ולרכיבי סייבר אחרים, "מאפשר ניסויים מדורגים, הן פיזיים והן במרחב הסייבר, על מערכות תשתית בקנה מידה תעשייתי".[40] המשרד משתף פעולה גם עם מעבדות לאומיות אחרות במגוון רחב של פרויקטים בתחום האנרגיה הקשורים לאבטחת סייבר, ועושה זאת דרך מתקן הניסוי הלאומי של מערכות שליטה, פיקוח ורכישת נתונים (SCADA).[41] בנוסף, משתף משרד האנרגיה פעולה עם מספר מעבדות לאומיות (ובראשן INL), ועם בעלי עניין אחרים בממשל ובתעשייה, סביב תוכנית לבדיקת חוסן הסייבר של מערכות בקרה תעשייתיות (CyTRICS), הנמצאת כרגע בשלב הפיילוט. תוכנית CyTRICS משמשת את משרד האנרגיה כדי לבחון רכיבים קריטיים בשרשרת האספקה ולמנף את נתוני הבדיקה לצורך זיהוי סיכונים שיטתיים בה.

הוועדה הפדרלית לפיקוח על שוק האנרגיה והתאגיד הצפון־אמריקאי לאמינות החשמל

הוועדה הפדרלית לפיקוח על שוק האנרגיה (FERC) הניחה את היסודות לדרישות מהמגזר הפרטי בתחום ניהול הסיכונים במערכת החשמל. ביולי 2016 הורתה הוועדה לתאגיד הצפון־אמריקאי לאמינות החשמל (NERC) לפתח תקני אמינות לניהול

39 "Section 2(e): Assessment of Electricity Disruption Incident Response Capabilities", *Department of Energy*, August 9, 2017, p. 29.

40 "Securing the Electrical Grid from Cyber and Physical Threats", *Idaho National Laboratory*, https://www.inl.gov/research-programs/grid-resilience/.

41 "National SCADA Test Bed", *Department of Energy*, https://www.energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity/national-scada-test-bed.

סיכונים בשרשרת האספקה,[42] או ליתר דיוק, הפקידה בידי התאגיד את המשימה לגבש תקנים שיחייבו גופים לפתח תוכנית לניהול סיכונים, שתתמקד בארבעה יעדים: "(1) מקוריות ושלמות התוכנה; (2) גישה מרחוק של ספקים; (3) תכנון מערכות מידע; (4) ניהול סיכוני ספקים ובקרות רכש".[43] הוועדה אישרה בינואר 2018 את התקנים הבאים: תקן CIP-013-1 (אבטחת סייבר – ניהול סיכונים בשרשרת האספקה); תקן CIP-005-6 (אבטחת סייבר – פרמטרים לאבטחה אלקטרונית); תקן CIP-010-3 (אבטחת סייבר – ניהול שינויי תצורה והערכת פגיעויות).[44] להערכת הוועדה, השילוב בין תקנים אלה נותן מענה ליעדים שצוינו לעיל. כך, למשל, תקן CIP-013-1 נועד "לצמצם סיכוני סייבר לפעולה אמינה של מתקני אנרגיה מרכזיים, על ידי יישום בקרות אבטחה לניהול סיכונים בשרשרת האספקה של מערכות הסייבר במתקנים אלה".[45]

תקני האמינות של שרשרת האספקה של התאגיד לאמינות החשמל הינם חשובים ביותר לצורך מתן מענה לסיכונים בשרשרת האספקה של ענף החשמל. יתרה מכך, חברות חשמל שונות יזמו בניית יכולות עמידה מול איומי סייבר ואיומים אלקטרומגנטיים, ורבות מהן נקטו צעדים מעל ומעֵבר לדרישות של תקני האמינות ויישמו מרצונן אמצעים נוספים. באותה מידה, סביר להניח שהן ינקטו גישה דומה גם לצורך אבטחת שרשרת האספקה.

התקנים החדשים אמנם מעניקים בסיס חשוב לחיזוק שרשראות האספקה של ענף החשמל, אך הם כרוכים גם במספר מגבלות. לדוגמה, המגבלות הקיימות על הוועדה הפדרלית לפיקוח על שוק האנרגיה והתאגיד לאמינות החשמל, מתוקף סעיף 215 לחוק החשמל הפדרלי של ארצות הברית, גורמות לכך שרק גופים מסוימים בתעשיית החשמל האמריקאית נדרשים לעמוד בתקנים אלה. הוועדה הפדרלית מציינת במפורש שהתקנים אינם חלים על "ספקים, מוֹכרים או גופים אחרים שאינם כפופים לסמכות השיפוט שלה ומספקים מוצרים או שירותים לגורמים הנושאים באחריות".[46] למעשה, התקנים אינם חלים (למעט חריגה קטנה אחת) על מערכות ניטור ובקרה אלקטרוניות (EACMS), על מערכות בקרה פיזיות (PACS) ועל נכסי סייבר מוגנים (PCA) של גופים הכפופים לסמכות השיפוט של הוועדה הפדרלית

42 "FERC Directs Development of Standards for Supply Chain Cyber Controls", *Federal Energy Regulatory Commission*, July 21, 2016, https://www.ferc.gov/media/news-releases/2016/2016-3/07-21-16-E-8.asp#.WQC2DGnysuU.

43 "Supply Chain Risk Management Reliability Standards (Docket No. RM17-13-000)", *Federal Energy Regulatory Commission,* 162 FERC ¶ 61,044, January 18, 2018, p. 5.

44 שם, עמ' 1.

45 "CIP-013-1–Cyber Security–Supply Chain Risk Management", *North American Electric Reliability Corporation*, July 2017, p. 3, https://bit.ly/2A1rWyE.

46 "Supply Chain Risk Management Reliability Standards", p. 7.

ושל התאגיד לאמינות החשמל, וכן של גופים הנחשבים כ"בעלי השפעה נמוכה". הוועדה מציינת כי כתוצאה מכך, "נותר סיכון משמעותי בתחום אבטחת הסייבר, הקשור לשרשרת האספקה למערכות הסייבר של מתקני אנרגיה מרכזיים".[47]

המועצה לתיאום בענף החשמל

המועצה לתיאום בענף החשמל (Electricity Sub-sector Coordination Council – ESCC) היא חוליה קריטית המקשרת בין גורמי הממשל האחראים על ענף החשמל ובין שותפיו בתעשייה. המועצה ובכיריה ממלאים תפקיד חשוב ביוזמות לקידום חוסנו של מערך החשמל ותורמים באופן משמעותי לאבטחה הכוללת של רשת החשמל. בין יוזמות אלו של המועצה נכלל גם נושא אבטחת שרשרת האספקה. ספציפית, המועצה פועלת בשיתוף עם הממשל כדי לכנס בעלי עניין מהמגזר הציבורי והפרטי, וכן ספקי אבטחה וטכנולוגיה, "כדי לזהות ולחלוק שיטות עבודה מומלצות שיתנו מענה לאיומים על שרשרת האספקה".[48] המועצה ומשרד האנרגיה האמריקאי גם פועלים לגיבוש תוכנית מבוססת נתונים לזיהוי שיטתי של פגיעויות וסיכונים בשרשרת האספקה.

הוועדה לרגולציה גרעינית

גופים העוסקים באנרגיה גרעינית אינם כפופים לוועדה הפדרלית לפיקוח על שוק האנרגיה ולתאגיד לאמינות החשמל, אלא פועלים על פי הנחיות אבטחת סייבר משלהם. הנחיות הוועדה לרגולציה גרעינית (Nuclear Regulatory Commission – NRC) בדבר "הגנה על רשתות ומערכות מחשב ותקשורת דיגיטלית" מפרטות את דרישות אבטחת הסייבר עבור הגופים הכפופים לה,[49] אם כי דרישות אלו מחייבות רק באופן כללי את הגופים להבטיח את הגנת המערכות שלהם, ואינן כוללות הוראות ספציפיות לניהול סיכונים בשרשרת האספקה שלהם. אף על פי כן, סעיף (3)(d) בהנחיות הוועדה קובע כי על גופים אלה "להבטיח כי שינויים בנכסים ... יעברו הערכה לפני מימושם", וכי הערכה זו תוכל לטפל בפגיעויות שהוחדרו אליהם באמצעות עדכוני תוכנה וחומרה.

ההנחיות של הוועדה לרגולציה גרעינית מ־2010 מציינות במפורש את הצורך בניהול סיכונים בשרשרת האספקה, כחלק מבקרות האבטחה הניהוליות והתפעוליות. הוועדה ממליצה באותן הנחיות להגן על מתקנים מפני איומים על שרשרת האספקה

---

47 שם, עמ' 3, 8.

48 "ESCC", *Electricity Subsector Coordinating Council*, January 2018, http://www.electricitysubsector.org/ESCCInitiatives.pdf?v=1.8.

49 "§ 73.54 Protection of Digital Computer and Communication Systems and Networks", *U.S. Nuclear Regulatory Commission*, 2009, https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html.

באמצעות הקמת ערוצי הפצה מהימנים ואימות ספקים, ודורשת שמוצרים שיירכשו יכללו יכולת זיהוי של ניסיונות פריצה או חבלה (או ישאו חותם המוכיח כי קיימת בהם הגנה כזאת).[50] הוועדה לרגולציה גרעינית מתעתדת לבחון מחדש את תקנות אבטחת הסייבר שלה בשנת 2019, ולעדכנן על פי הצורך.[51]

יוזמות רב־מגזריות

המשרד לביטחון המולדת

המשרד לביטחון המולדת מרחיב את מאמציו בתחום ניהול הסיכונים בשרשרת האספקה. בינואר 2018 גיבש המשרד תוכנית משלו לניהול סיכונים בשרשרת האספקה בסייבר (C-SCRM), שנועדה לשמש כ"גורם מוביל וכנקודת התיאום המרכזית עבור כלל הממשל בנושאי ניהול הסיכונים בשרשרת האספקה בסייבר".[52] יוזמת המשרד לביטחון המולדת נושאת בחובה חזון שאפתני, המאפשר קיומה של "סביבה מבצעית ושוק לאומי וגלובלי של טכנולוגיות מידע ותקשורת, שבמסגרתם ניתן יהיה לזהות בקלות ובמהירות קיומם של חומרה, תוכנה או רכיבים מזויפים, לקויים או פגומים, אם בזדון ואם כתוצאה מרשלנות, ותתאפשר נקיטת פעולה לצמצומם או למניעתם ולהפיכתם לנדירים".[53] המשרד לביטחון המולדת מפרט את פעולותיה העיקריות של התוכנית כדלקמן:

- הקמת יכולת להערכת סיכונים בשרשרת האספקה לטובת בעלי העניין.
- הקמת יכולת לתקשורת, יידוע ושיתוף מידע בקרב בעלי העניין.
- גיבוש רשימת יצרנים וספקים מורשים באמצעות יישום תהליך אמין לאימות ואישור נוהלי אבטחה של חברות ומאפייני האבטחה של מוצרים ושירותים בתחום טכנולוגיות מידע ותקשורת.
- סיוע לבעלי עניין בפיתוח ויישום יכולות לניהול סיכונים בשרשרת האספקה.[54]

היוזמה לניהול סיכונים בשרשרת האספקה בסייבר, הכוללת את המינהל לשירותים כלליים (GSA), את משרד ההגנה, את קהילת המודיעין וכן בעלי עניין במגזר הפרטי

---

50 "Regulatory Guide 5.71: Cyber Security Programs for Nuclear Facilities", *U.S. Nuclear Regulatory Commission*, January 2010, pp. C-29–C-30, https://www.nrc.gov/docs/ML0903/ML090340159.pdf.

51 Sean Lyngaas, "Nuclear Power Plants Have a 'Blind Spot' for Hackers. Here's How to Fix That", *Motherboard*, April 27, 2018, https://motherboard.vice.com/en_us/article/mbxy33/cyberattacks-nuclear-supply-chain.

52 "Cyber Supply Chain Risk Management: Becoming a Smarter Consumer of ICT in a Connected World", *Department of Homeland Security*, June 2018, p. 15.

53 שם.

54 שם, עמ' 16.

בארצות הברית, נועדה לתרום לקבלת החלטות מושכלת בתחום הרכש הממשלתי.[55] לדברי גורם רשמי במשרד לביטחון המולדת, היוזמה "תספק למשתמשים, לקונים, ליצרנים ולמוכרים, העוסקים במוצרים טכנולוגיים, מידע מעשי על סיכונים בשרשרת האספקה ועל הדרכים לצמצומם. היא גם תזהה סיכונים לרשתות פדרליות ולבעלי עניין אחרים ברמה הלאומית או הגלובלית".[56] ג'נט מנפרה (Manfra), עוזרת השר לביטחון המולדת לענייני סייבר ותקשורת במינהלת התוכניות להגנה לאומית (NPPD), הוסיפה על כך שהיוזמה "תזהה ותצמצם איומים ופגיעויות בשרשרת האספקה" של נכסים בעלי ערך רב.[57]

היוזמה לניהול סיכונים בשרשרת האספקה בסייבר מתבססת על כלים קיימים של המשרד לביטחון המולדת, המיועדים לטיפול בסיכונים בשרשרת האספקה. לדוגמה, התוכנית לאבחון ולניטרול סיכונים כוללת אסטרטגיה שנועדה לצמצם איומי סייבר המבוססים על שרשרת האספקה. האסטרטגיה כוללת "רשימת מוצרים מאושרים", שהיא "קטלוג של מוצרים שאושרו כעומדים בדרישות הטכניות של התוכנית לאבחון ולניטרול סיכונים".[58] למשרד לביטחון המולדת יש גם תוכנית ניהול סיכונים ספציפית, שמטרתה "לספק מידע לסוכנויות השונות ולהורות על פעילויות הקשורות לדרך שבה מציעי עיסקאות מזהים, מעריכים ומנטרלים סיכונים בשרשרת האספקה, באופן שיקל על קבלת החלטות ומתן הוראות מושכלות יותר בקרב סוכנויות ממשלתיות".[59]

מכון התקנים הלאומי

מכון התקנים הלאומי (NIST) הוא מקור מרכזי להנחיות בתחום ניהול סיכונים בשרשרת האספקה. למרכז המשאבים לאבטחת מחשבים של המכון (CSRC)

---

55 Jory Heckman, "DHS, Lawmakers Doubling Down on Supply Chain Risk Management", *Federal News Radio*, February 15, 2018, https://federalnewsradio.com/cybersecurity/2018/02/dhs-lawmakers-doubling-down-on-supply-chain-risk-management/.

56 Lauren C. Williams, "DHS Developing Supply Chain Security Initiative", *FCW*, February 14, 2018, https://fcw.com/articles/2018/02/14/dhs-supply-chain-security.aspx.

57 "Statement of Jeannette Manfra, Assistant Secretary for Cybersecurity and Communications, NPPD, U.S. House of Representatives Committee on Oversight and Government Reform Subcommittee on Information Technology (2018)", *Department of Homeland Security*, p. 8.

58 "Continuous Diagnostics and Mitigation (CDM) ", *Department of Homeland Security*, last updated February 22, 2018,https://www.dhs.gov/cdm.

59 "Continuous Diagnostics and Mitigation (CDM) Approved Products List (APL) Supply Chain Risk Management (SCRM) Plan", *Government Services Agency*, August 2017, p. 1.

יש תוכנית מקיפה לניהול סיכונים בשרשרת האספקה בסייבר, המתבססת על היכרותו עם שרשרת האספקה של רשתות IT ו־OT.[60]

פרסומי מכון התקנים ב־2015 בנושא ניהול סיכונים בשרשרת האספקה מספקים הדרכה מקיפה איך לנהל סיכונים בשרשרת האספקה בסייבר. ההנחיות מספקות למשרדי הממשל ולסוכנויות פדרליות מסגרת עבודה, הניתנת לשינוי או להרחבה על פי הדרישות, המדיניות, ההנחיות ושאר המסמכים הספציפיים של כל ארגון.[61] המסמך מציג מערך של תהליכים ואמצעים להערכה וניהול של סיכונים בשרשרת האספקה, ומציע תבנית לפיתוח תוכניות לניהול סיכונים. מכון התקנים גם מספק מערך של שיטות עבודה מומלצות בנושא ניהול סיכונים, הרלוונטיות לכל ענפי התשתית במשק האמריקאי.[62] זאת ועוד, העדכונים שערך המכון בשנת 2017, במסמך שכותרתו "מסגרת עבודה לשיפור אבטחת הסייבר בתשתיות קריטיות", כללו "פרטים חדשים על ניהול סיכונים בשרשרת האספקה בסייבר".[63] עדכון נוסף, מאפריל 2018, כלל עוד שינויים בתחום "ניהול אבטחת סייבר בתוך שרשרת האספקה".[64]

בנוסף ליוזמות ולהנחיות אלו, נוהג מכון התקנים האמריקאי לכנס ראשי ממשל, מנהלים מהמגזר הפרטי ואנשי אקדמיה כדי לדון בסיכונים בשרשרת האספקה. הפורום לאבטחת התוכנה ושרשרת האספקה, הפועל בהובלה משותפת של המשרד לביטחון המולדת, המינהל לשירותים כלליים ומשרד ההגנה, מאפשר למשתתפים "לשתף את הידע והמומחיות שלהם בנוגע לסיכונים בשרשרת האספקה והתוכנה, לשיטות עבודה יעילות ולאסטרטגיות, לכלים וטכנולוגיות לניטרול סיכונים, לגישור על פערים בין אנשים, תהליכים או טכנולוגיות בתחום זה".[65]

---

60 "Cyber Supply Chain Risk Management".

61 "Supply Chain Risk Management Practices for Federal Information Systems and Organizations (SP 800-161) ", *National Institute of Standards and Technology*, April 2015, p. 2.

62 "Utility Sector Best Practices for Cyber Security Supply Chain Risk Management", *National Institute of Standards and Technology*, October 2015, https://www.nist.gov/sites/default/files/documents/itl/csd/USRP_NIST-Utility_100115.pdf.

63 "NIST Releases Update to Cybersecurity Framework", *National Institute of Standards and Technology*, January 10, 2017, https://www.nist.gov/news-events/news/2017/01/nist-releases-update-cybersecurity-framework.

64 "NIST Releases Version 1.1 of its Popular Cybersecurity Framework", *National Institute of Standards and Technology*, April 16, 2018, https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework.

65 "Software and Supply Chain Assurance Forum", *National Institute of Standards and Technology*, last updated March 29, 2018, https://csrc.nist.gov/Projects/Supply-Chain-Risk-Management/SSCA.

כלי יעיל זה לשיתוף ותיאום אכן תורם לניהול הסיכונים, אולם יכולתו מוגבלת ביותר. יהיה זה יקר מאוד ולא מעשי להניח שהמשתתפים השונים בתהליך זה יצליחו לפתח מנגנונים עצמאיים משלהם להסמכת מוצרים, או לחלוק את מסקנותיהם עם עמיתיהם וליצור את "מאגר הביקוש" המאוחד הנדרש כדי להגביר את ההיצע של המוצרים שעברו הסמכה.

משרד הניהול והתקציב

משרד הניהול והתקציב (OMB) הינו מקור מרכזי למדיניות הממשל הפדרלי בנושא אבטחת סייבר. החוק הפדרלי למודרניזציה של אבטחת מידע (FISMA) קובע כי משרד הניהול והתקציב יפקח על המדיניות והנהלים של אבטחת המידע בגופים ממשלתיים. חוזר A–130 של משרד הניהול והתקציב, שפורסם בשנת 2016 ונושא את הכותרת "ניהול מידע כמשאב אסטרטגי", מגדיר את "המדיניות הכללית לתכנון, תקצוב, פיקוח, רכישה וניהול של מידע פדרלי, כוח אדם, ציוד, כספים, משאבי IT ותשתית ושירותים תומכים" עבור הרשות המבצעת של הממשל הפדרלי.[66] המסמך גם כולל הנחיה לגופים אלה כיצד ליישם את החוק למודרניזציה של אבטחת מידע, לצורך ניהול סיכונים בשרשרת האספקה ברמה הפדרלית. ספציפית, המסמך קובע כי גופים ממשלתיים:

- "ישקלו ... סוגיות הקשורות לאבטחת שרשרת האספקה עבור כל פעילות של ניהול ותכנון משאבים, לכל אורך מחזור חיי הפיתוח של המערכת, באופן שיבטיח כי הסיכונים ינוהלו כהלכה".
- "ינתחו סיכונים (לרבות סיכונים בשרשרת האספקה) הקשורים לקבלנים פוטנציאליים ולמוצרים ולשירותים שהם מספקים".[67]

נספח למסמך A–130, ה"מגדיר דרישות סף לתוכניות לאבטחת מידע פדרלי", מחייב גופים ממשלתיים:

- "ליישם עקרונות לניהול סיכונים בשרשרת האספקה באופן שיגן מפני החדרת זיופים, מוצרים בלתי מורשים, חבלה, גניבה או הכנסה של תוכנה זדונית, וכן מפני שיטות ייצור או פיתוח לקויות, וזאת בכלל מחזור חיי הפיתוח של המוצר".
- "לפתח תוכניות לניהול סיכונים בשרשרת האספקה, כמפורט במסמך SP 800–161 של מכון התקנים הלאומי, כדי להבטיח את שלמות אבטחתן, חוסנן ואיכותן של מערכת המידע".[68]

---

66 "Circular No. A-130: Managing Information as a Strategic Resource", *Office of Management and Budget*, July 2017, p. 6, https://bit.ly/2rAjz7Q.

67 שם, עמ' 6, 11.

68 שם, עמ' 40, 42.

בהנחה שמסמך A–130 ייושם בצורה קפדנית, יהיה באפשרותו לתרום לאבטחת שרשרת האספקה שבאחריות הרשות המבצעת. עם זאת, המדיניות שנקבעה לוקה בחסר בפירוט הדרישות הספציפיות, למעֵט הפְניה להנחיות מכון התקנים הלאומי, כפי שצוינו לעיל. גם ההנחייה שכל סוכנות תגבש תוכנית משלה לניהול סיכונים אינה ישימה מבחינה כלכלית, בוודאי לא ברמה הנדרשת. יתרה מכך, למרות שהמדיניות שגובשה חלה על רוב הגופים העוסקים ספציפית בנושא (למעט על הסוכנות להגנת הסביבה, בהיותה גוף העוסק ספציפית בענף המים והשפכים), היא מוגבלת לקבוצה קטנה בלבד של גופים ממשלתיים ואינה חלה על התעשייה או על בעלי עניין אחרים.

מינהל השירותים הכלליים

מינהל השירותים הכלליים (GSA) ממלא תפקיד מפתח ברכישות שמבצעת הממשלה הפדרלית, ובהתאם לכך – באחריות על אבטחת שרשראות האספקה הפדרליות. ספציפית, המינהל "מגבש יכולת מקיפה לניהול סיכונים בשרשרת האספקה, שתבטיח כי גופים ממשלתיים ירכשו חומרה ותוכנה של מערכות מידע מיצרני ציוד מקור, ובכלל זה ממפיצים מורשים וממקורות מהימנים אחרים".[69] מינהל השירותים הכלליים גם אחראי לגיבוש תוכנית להערכת סיכונים מצד הסַפָּק, שנועדה "להעריך סיכונים מוכרים או פוטנציאליים הקשורים לספקים של מוצרים ושירותים".[70]

משרד מנָהל המודיעין הלאומי והמרכז הלאומי לריגול נגדי וביטחון

מנהל המודיעין הלאומי (DNI) גיבש מדיניות לניהול סיכונים בשרשרת האספקה עבור קהילת המודיעין האמריקאית. הנחיה 731 של קהילת המודיעין של ארצות הברית קובעת מדיניות שנועדה "להגן על שרשרת האספקה בהתייחס למחזור החיים של מוצרים, חומרים ושירותים קריטיים המשמשים את קהילת המודיעין, וזאת באמצעות זיהוי, הערכה וניטרול האיומים".[71] להנחיה זו מתלוות הנחיות ספציפיות נוספות שנועדו לקבוע את מידת הקריטיות של רכיבים, וכן פרטים הנוגעים לביצוע הערכת האיומים, ולהביא לשיפור בשיתוף המידע.

---

69 Shon Lyublanovits, "Reducing Cybersecurity Risks in Supply Chain Risk Management", *General Services Administration*, September 18, 2017, https://gsablogs.gsa.gov/technology/2017/09/18/reducing-cybersecurity-risks-in-supply-chain-risk-management/.

70 שם.

71 "Intelligence Community Directive 731 – Supply Chain Risk Management", *Office of the Director of National Intelligence*, December 2013, p. 1.

בנוסף להנחיות אלו, גם המרכז הלאומי לריגול נגדי וביטחון עוסק באיומים על ניהול סיכונים בשרשרת האספקה. נייר עמדה של המרכז משנת 2013, וחומרי רקע שלו משנת 2017, מספקים מידע תמציתי אך בעל ערך לגבי איומים בשרשרת האספקה בסייבר וניהול סיכונים.[72] המרכז הלאומי לריגול נגדי גם יזם, בשיתוף עם המשרד לביטחון המולדת, שיתוף פעולה עם התעשייה, התורם למאמצים לקדם את ניהול הסיכונים בשרשרת האספקה. התוכנית לחילופי מידע בין המגזר הפרטי למגזר הציבורי[73] זיהתה את הסיכונים בשרשרת האספקה בסייבר כסוגיה מרכזית של ענף החשמל כבר במסמך עמדה שלה משנת 2016. המסמך מציג ממצאים והמלצות מרכזיים בנושא ניהול הסיכונים עבור התעשייה והממשל גם יחד.[74] דוח מפורט יותר של התוכנית לחילופי מידע בין המגזר הפרטי והמגזר הציבורי, משנת 2017, מסתמך על אותו נייר עמדה ומספק המלצות מקיפות יותר, במיוחד לגבי איומים בתחום מערכות בקרה. הדוח הופק כדי "להדגיש סיכוני אבטחה פוטנציאליים בשרשרת האספקה של מערכות שליטה, פיקוח ובקרת נתונים בשלב ההתחלתי הנוכחי שלהן, במטרה למנוע את הצורך להכניס בעתיד תיקונים יקרים בענפי תעשייה קיימים".[75]

למרות שהדוח כולל בעיקר מידע והמלצות, ואינו מדריך מפורט לפעולה קונקרטית, בכל זאת הוא בעל חשיבות, בהדגישו את התפקיד של המרכז הלאומי לריגול נגדי וביטחון, ובמיוחד של התוכנית לחילופי מידע בין המגזר הפרטי למגזר הציבורי כשותפים מרכזיים ליוזמה להסמכה בין־לאומית של מוצרי סייבר. הדבר נכון במיוחד לאור העובדה שיישום המלצות הדוח של התוכנית לחילופי מידע בין המגזרים, לפיהן על חברות לבנות מנגנוני הסמכה משלהן וליצור את כוחות השוק הדרושים כדי להגדיל את ההיצע של תוכנות וחומרות מוסמכות, הוא בגדר שאיפה לא מעשית.

משרד ההגנה האמריקאי

גם למשרד ההגנה של ארצות הברית יש מדיניות של ניהול סיכונים בשרשרת האספקה, שמטרתה היא להבטיח מערכות ורשתות אמינות. הוראה 5200.44 של משרד ההגנה, שעודכנה בפעם האחרונה ביולי 2017, ועניינה "הגנה על פונקציות קריטיות למילוי משימות, לשם הבטחת מערכות ורשתות אמינות", קובעת כללי מדיניות שמטרתם למזער את הסיכונים הקשורים ל"פגיעויות בתכנון המערכת, או לחבלה או פגיעה בפונקציות או ברכיבים קריטיים של המערכת ... על ידי מודיעין

72 "Supply Chain Risk Management: Framework for Assessing Risk".
73 *The Public-Private Analytic Exchange Program*.
74 "Identifying and Mitigating Supply Chain Risks".
75 שם, עמ' iii.

זר, טרוריסטים או גורמים עוינים אחרים".[76] ההוראה מדגישה את החשיבות של ניהול סיכונים בשרשרת האספקה לכל אורך מחזור החיים של המוצר. זוהי מדיניות המכֻוונת ספציפית לפונקציות במשרד ההגנה, המוגדרות כקריטיות למילוי משימות, אם כי ניתן להחיל עקרונות וגישות דומים גם על המאמצים והגישה הכללית הכרוכים ביוזמה להסמכה של מוצרי סייבר.

הבית הלבן

הבית הלבן מדגיש את חשיבות האבטחה של שרשראות אספקה גלובליות בשתי יוזמות נפרדות. כדי לנהל את סיכוני שרשרת האספקה פורסמה בינואר 2012 "האסטרטגיה הלאומית לאבטחת שרשרת האספקה הגלובלית", הקוראת לפעול להרחבת ההבנה לגבי האיומים על שרשראות האספקה, הנובעים מ"ניצול המערכת על ידי המבקשים להחדיר אליה מוצרים או חומרים הגורמים נזק".[77] גם "היוזמה הלאומית המקיפה לאבטחת סייבר" של הבית הלבן מדגישה את איומי שרשרת האספקה. יוזמה זאת, שמספרה 11, נועדה "לפתח גישה מרובת מוקדים לניהול סיכונים בשרשרת האספקה העולמית", שניהול הסיכונים במסגרתה יכלול "פיתוח ויישום של כלים ומשאבים להפחתת הסיכון הטכנולוגי והתפעולי לאורך מחזור החיים של המוצרים (החל מתכנון ועד יציאה משימוש) ... ושיתוף פעולה עם התעשייה במטרה לפתח ולאמץ תקנים ושיטות עבודה מומלצות לניהול סיכונים בשרשרת האספקה".[78]

יוזמות במגזר הפרטי

אחת היוזמות במגזר הפרטי נראית מבטיחה במיוחד וראויה לתשומת לב: יוזמת "אמנת האמון" (Charter of Trust). חברת "סימנס" חברה לאחרונה ל"ועידת מינכן לביטחון" ולגורמים ממשלתיים ועיסקיים אחרים (כולל IBM ו־AES) במטרה להשיק את יוזמת האמנה, שנועדה "לפתח וליישם כללים שיבטיחו את אבטחת הסייבר בכל רחבי סביבת הרשת".[79] עיקרון מספר שבע של האמנה מציע בסיס אפשרי לדו־שיח עם חברת "סימנס" ושותפיה לאמנה. לפי עיקרון זה, "חברות, ובמידת הצורך גם ממשלות, יגבשו יכולות הסמכה עצמאיות של צדדים שלישיים

76 "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN) ", *Department of Defense*, Instruction No. 5200.44, 2017, p. 1.

77 "National Strategy for Global Supply Chain Security", *The White House*, January 2012, p. 4.

78 "The Comprehensive National Cybersecurity Initiative", *The White House*, March 2010, https://obamawhitehouse.archives.gov/node/233086.

79 "Time for Action: Building a Consensus for Cybersecurity", *Siemens*, May 17, 2018, https://www.siemens.com/innovation/en/home/pictures-of-the-future/digitalization-and-software/cybersecurity-charter-of-trust.html.

(בהתבסס על הגדרות מותאמות לעתיד, במיוחד כאשר יש סכנת חיים על הפרק), לצורך מתן פתרונות חיוניים עבור תשתיות קריטיות ו'התקנים מחוברים'".[80] יש בכך הזדמנות של היוזמה להסמכה של מוצרי סייבר לחבור למשתתפי "אמנת האמון", כדי למצוא פתרונות משותפים לניהול סיכונים בשרשרת האספקה, שימנפו את היתרונות והמשאבים של כל יוזמה בנפרד.

הסמכת מוצרים

ארגונים ויוזמות הממוקדים בנושא הסמכת מוצרים, בעיקר במגזר הפרטי, מבקשים להעריך סיכונים פוטנציאליים במוצרים, בתהליכים ובמערכות ספציפיים. יש מספר לא מבוטל של ארגונים ותוכניות הסמכה כאלה ברחבי העולם, ואנו נסקור כאן רק כמה מהם. רבים מגופי הסמכה אלה נותנים את הדעת לאבטחת הסייבר, אך רק מעטים מהם כוללים הסמכות לתקנים אלקטרומגנטיים.

מעבדות החיתום

מעבדות החיתום (Underwriters Laboratories – UL) מספקות מגוון רחב של הסמכות, החל ממוצרים, דרך מִתקנים, תהליכים או מערכות ספציפיים, ועד לדרישות ותקנים של התעשייה.[81] מעבדות החיתום, כגורם מוביל בתחומו בארצות הברית, פועלות יחד עם יצרנים, מומחי תעשייה, מעבדות בדיקה אחרות וממשלות, ותקני הבדיקה שלהן נחשבים למעשה ל"תקנים בפועל של ממשלת ארצות הברית".[82] המעבדות יכולות לשמש גם גורמי צד שלישי עצמאיים, לצורך הסמכת שרשראות אספקה ותהליכים הקשורים בהן.[83] מינהל הבריאות והבטיחות בעבודה של משרד העבודה האמריקאי מכיר במעבדות החיתום כאחת ממעבדות הבדיקה המוכרות רשמית ברמה כלל־ארצית.[84]

---

80 "Charter of Trust: For a Secure Digital World", *Charter of Trust,* February 2018, https://www.siemens.com/press/pool/de/feature/2018/corporate/2018-02-cybersecurity/charter-of-trust-e.pdf.

81 "Certification", *Underwriters Laboratories*, https://services.ul.com/categories/certification/.

82 Mike Murphy, "Inside the 122-Year-Old Company that Makes Sure our Electronics Don't Blow Up our Homes", *Quartz*, April 5, 2016, https://qz.com/643007/inside-the-122-year-old-company-that-makes-sure-our-electronics-dont-blow-up-our-homes/.

83 "Supply Chain Certification", *Underwriters Laboratories*, https://services.ul.com/service/supply-chain-certification/.

84 "Current List of NTRLs", *Occupational Safety and Health Administration*, https://www.osha.gov/dts/otpca/nrtl/nrtllist.html.

ארגון התקינה הבין־לאומי והנציבות הבין־לאומית לאלקטרוטכניקה

ארגון התקינה הבין־לאומי (ISO) והנציבות הבין־לאומית לאלקטרוטכניקה (IEC) הם שתי ישויות נפרדות המשתפות פעולה ביניהן כדי לגבש תקנים ולתת הסמכות למוצרים ולתעשייה. הוועדה הטכנית המשותפת של שני הגופים מתמקדת בפיתוח תקנים בתחום מערכות מידע.[85] תקן ISO/IEC 27036, הכולל ארבעה חלקים, מספק הנחיות שנועדות "לסייע לארגונים באבטחת המידע ומערכות המידע שלהם בהקשר של קשרים עם הספקים".[86] בנוסף לפעילות משותפת זו, הנציבות הבין־לאומית לאלקטרוטכניקה מפתחת תקינה אלקטרומגנטית, ובכלל זה תקנים עבור "מוצרים מורכבים, או כאלה הפועלים בסביבה מיוחדת".[87]

סדרת התקנים 62443 של הנציבות הבין־לאומית לאלקטרוטכניקה מציעה מודל שימושי במיוחד. תקנים אלה מתייחסים לצורך לגבש עמידות וחוסן של אבטחת הסייבר בתוך מערכות בקרה ואוטומציה תעשייתיות (IACS). תקן 1–4–62443 מתאר את הדרישות החלות על פיתוח מוצרים של מערכת הבקרה.[88] תקני ISO/IEC יכולים לסייע בקביעת הקריטריונים לתוכניות הסמכה עתידיות, אם כי יש צורך במאמצים נוספים כדי לקבוע באיזו מידה (וכיצד) יספק תקן ISO/IEC בדיקה ואימות מתמשכים של מוצרים וספקים.

חוק SAFETY (המשרד לביטחון המולדת)

המשרד לביטחון המולדת מחזיק בתוכנית להסמכת טכנולוגיות למאבק בטרור. לאחר התקפות ה־11 בספטמבר 2001 בארצות הברית, המגזר הפרטי "הסתייג מאוד מהטמעת טכנולוגיות ושירותים ביטחוניים בסביבה אזרחית, בשל סיכוני האחריות העצומים שהיו כרוכים בכך".[89] החשש של החברות היה כי הן ישאו באחריות, אם המוצר שלהן לא ימנע את המתקפה שהוא נועד למנוע, או לא ינטרל אותה. בתגובה לכך חוקק הקונגרס בשנת 2002 את חוק "התמיכה במאבק בטרור באמצעות אימוץ טכנולוגיות יעילות" (חוק SAFETY), אשר נועד "להבטיח כי איום החבות לא ירתיע יצרנים או מוכרים פוטנציאליים של טכנולוגיות נגד טרור

---

85 "ISO/IEC JTC 1 — Information Technology", *International Organization for Standardization*, https://www.iso.org/isoiec-jtc-1.html.

86 "ISO/IEC 27036-1:2014", *International Organization for Standardization*, April 2014, https://www.iso.org/standard/59648.html.

87 "EMC Product Standards", *International Electrotechnical Commission*, 2018, http://www.iec.ch/emc/emc_prod/.

88 "Overview – The 62443 Series of Standards", *ISA*, 2015, https://fr.scribd.com/document/358894928/ISA-62443-Series-Overview.

89 "Research and Development Partnerships – SAFETY Act for Liability Protection", *Department of Homeland Security*, January 14, 2014, https://bit.ly/2JPIolm.

מלפַתח ולשווק טכנולוגיות מצילות חיים".[90] חוק SAFETY מכיל מנגנון להסמכת מגוון רחב של מוצרים, שירותים וטכנולוגיות כ"טכנולוגיות מאושרות נגד טרור" (QATT), ובכך הוא מאפשר להכניס אותם לרשימת המוצרים המאושרים לצורכי הגנה על ביטחון המולדת מכוח אותו חוק.[91] המשרד לביטחון המולדת מגביל את אחריות המוכרים והמשתמשים של מוצרי הטכנולוגיות המאושרות נגד הטרור.[92] בין המוצרים הזכאים לפטור מאחריות מכוח חוק SAFETY ניתן למצוא גם טכנולוגיות לאבטחת סייבר.[93]

תוכניות בין־לאומיות להסמכת אבטחת סייבר

ישנם כמה מנגנוני הסמכה וגופים שנועדו להבטיח את אבטחת הסייבר של מוצרים. למעשה, סמכות לאבטחה שכבתית של מוצרי מערכות מידע מסחריות קיימת מזה למעלה משלושים שנה.[94] הקריטריונים שעל פיהם פועלות תוכניות הסמכה כאלו מעוגנים בתקנים, כגון "הקריטריונים השכיחים". תקינת "הקריטריונים השכיחים" גם יצרה מערכת הסמכה רחבה הכוללת תוכנית הסמכה למוצרים. המערכת כוללת הבטחת הערכה איכותית של מוצרי מערכות מידע, שיפור הזמינות של מוצרים בטוחים בעלי הסמכה, מניעת הצורך בהערכות כפולות ושיפור מתמיד של "האפקטיביות והיעילות הכלכלית של תהליך ההערכה וההסמכה".[95] עד 5 ביוני 2018 הוסמכו 2,351 מוצרים במסגרת "הקריטריונים השכיחים", ביניהם הֶתקנים ומערכות לבקרת גישה, מערכות הפעלה, התקנים ומערכות לגילוי, והֶתקנים ומערכות להגנת גבולות.[96]

בדומה ליוזמות רבות הממוקדות באבטחת סייבר (בניגוד להתמקדות בתשתיות ספציפיות), אחד החסרונות הפוטנציאליים של "הקריטריונים השכיחים" הוא ההתמקדות במערכות מידע ולא במערכות בקרה. בנוסף לכך, החברות המשתתפות ביוזמת הקריטריונים אינן כוללות את סין, רוסיה או יריבים אחרים של ארצות

---

90 "The Office of SAFETY Act Implementation", *Department of Homeland Security*, https://www.dhs.gov/science-and-technology/safety-act.

91 "Research and Development Partnerships – SAFETY Act for Liability Protection".

92 שם.

93 שם.

94 Steven B. Lipner, "SAFECode Perspective on Cybersecurity Certification", January 2018, p. 1, https://safecode.org/wp-content/uploads/2018/02/SAFECode_Perspective_on_Cybersecurity_Certification.pdf.

95 "About the Common Criteria", *Common Criteria*, https://www.commoncriteriaportal.org/ccra/index.cfm.

96 "Certified Products", *Common Criteria*, https://www.commoncriteriaportal.org/products/.

הברית במרחב הסייבר.[97] היוזמה כוללת ועדת ניהול, שבה נציגים בכירים מכל מדינה חברה, וזאת "כדי ליישם את ההסדר וכדי לספק אכוונה לכל מדינה בבואה לבצע פעילויות הערכה ואימות בתוכנית הלאומית שלה".[98]

קיים מגוון של תוכניות הסמכה נוספות במגזרים הציבורי והפרטי. כאמור, חלק מיוזמות ניהול הסיכונים בשרשרת האספקה עשוי להיפגע על ידי המדינות החברות בארגון המייסד את היוזמה. כך, למשל, ארגון Open Group מתגאה שחברים בו יותר מ־500 משתתפים בין־לאומיים, כולל נוכחות אמריקאית גדולה במיוחד, אך פריסה זאת של הארגון גם מאפשרת לכלול בתוכו יריבים פוטנציאליים. לעומתו, ארגון SAFECode הוא הרבה יותר קטן, אם כי גם בו עשויים להיות חברים יריבים פוטנציאליים של ארצות הברית.

SAFECode

SAFECode הוא ארגון הפועל במסגרת האיחוד האירופי ומתמקד באבטחת תוכנה. לתוכנית של הארגון יש חזון הדומה ליוזמה להסמכה בין־לאומית של מוצרי סייבר. SAFECode מבקש לסייע למשתמשים "לזהות מוצרים ושירותים מקוונים המספקים אבטחה יעילה, לתמרץ את הספקים להשקיע באבטחה יעילה ולהבטיח להם שיתוגמלו על השקעה זאת".[99] ראוי לציין כי SAFECode מסייע לגופים קטנים ובינוניים, הנאבקים לעמוד בתחרות עם ארגונים גדולים שמממנים תוכניות ניהול סיכונים משלהם ברחבי העולם.[100] היוזמה להסמכה בין־לאומית של מוצרי סייבר נותנת מענה לאתגר זה באמצעות ריכוז המשאבים הדרושים לאבטחת שרשראות האספקה, וכן על ידי יצירת "איתות ביקושים" חזק ועקבי למוצרים מאובטחים.

מסמכי רקע של SAFECode העוסקים בהסמכת אבטחת סייבר מספקים כמה נקודות מבט מעניינות: SAFECode מדגיש את חשיבות הסמכת המוצר כבר בשלב הפיתוח שלו, ולא לאחר יציאתו לשוק, וזאת כדי להבטיח שחברות לא ימצאו את עצמן משתמשות במוצר שיש בו פגיעויות פוטנציאליות, בשעה שהוא ממתין לקבלת ההסמכה כמוצר מאובטח.[101] יותר מכך, SAFECode מדגיש את התועלת שבמערכת הסמכה שכבתית, ומציין בהקשר זה כי "תוכניות המספקות רמות משתנות של הסמכה ימריצו מפתחים לחפש את הרמה הגבוהה ביותר של

97. "Members of the CCRA", *Common Criteria*, https://www.commoncriteriaportal.org/ccra/members/.
98. "About the Common Criteria".
99. Lipner, "SAFECode Perspective on Cybersecurity Certification", p. 2.
100. שם, עמ' 3.
101. שם, עמ' 2.

הסמכה".[102] בנוסף, SAFECode מדגיש את טביעת הרגל הבין־לאומית הבלתי נמנעת שנמצאת בשרשראות האספקה כיום, ודוחק ל"הכרה הדדית רחבה, שתביא תועלת מרבית למשתמשים ולמפתחים בכל רחבי העולם".[103]

תשתית ניהול הסיכונים של SAFECode הינה מוגבלת, שכן ההתמקדות היחידה של הארגון היא במערכות מידע (ולא במערכות בקרה). כמו כן, SAFECode מטיל את חובת הציות, הבדיקות והאימות על הארגונים עצמם, דבר שמוביל לכפילות משמעותית במשאבים ולחוסר יעילות. עם זאת, "השיטות הבסיסיות לפיתוח תוכנה מאובטחת" של SAFECode יכולות להוות מקור נוסף לתובנות עבור תוכניות הסמכה עתידיות.[104]

תוכנית ההסמכה O-TTPS

תוכנית Open Trusted Technology Provider Standard (O-TTPS) של Open Group כוללת הנחיות, המלצות, דרישות ושיטות עבודה מומלצות, שמטרתן היא "לשפר את שלמות המידע של המוצרים [מוצרי המדף המסחריים ומוצרי טכנולוגיית תקשורת] ואת אבטחת שרשראות האספקה הגלובליות שלהם".[105] הארגון מסמיך ארגונים שלדעתו עומדים בדרישות התוכנית ומסוגלים להיות "ספקי טכנולוגיה מהימנים".[106]

גם מסמכי המדיניות וההנחיות של תוכנית O-TTPS מספקים חומר בסיסי חשוב ליוזמות עתידיות בתחום אבטחת הסייבר. לדוגמה, מסמך מדיניות ההסמכה משנת 2017 כולל תרשימי זרימת עבודה מפורטים להסמכת צדדים שלישיים, עם פירוט נוסף עבור כל שלב בתהליך.[107] המסמך כולל, בנוסף לכך, גם מדיניות ספציפית הנוגעת לדרישות התאמה והסתגלות, לדרכים בהן ניתן לשמור על ההסמכה ולבצע הסמכה מחדש ולתהליך הערעור על החלטות בנושא הסמכה.

---

102 שם, שם.

103 שם.

104 "Fundamental Practices for Secure Software Development: Essential Elements of a Secure Development Lifecycle Program (Third Edition) ", *SAFECode*, March 2018, https://safecode.org/wp- content/ uploads/2018/03/SAFECode_Fundamental_Practices_for_Secure_Software_Development_March_2018.pdf.

105 "The Open Trusted Technology Provider Standard (O-TTPS) Certification Program", *The Open Group*, http://www.opengroup.org/certifications/o-ttps.

106 שם.

107 ראו: "Open Trusted Technology Provider Standard (O-TTPS) Certification Policy (Version 1.1)," *The Open Group*, January 2017, pp. 14-18, https://ottps-cert.opengroup.org/sites/ottps-cert.opengroup.org/files/doc/O-TTPS_Certification_Policy.pdf.

היוזמה להסמכה בין־לאומית למוצרי סייבר

היוזמה להסמכה בין־לאומית למוצרי סייבר (Cyber Product International Certification – CPIC) של המועצה לביטחון תשתיות החשמל (EIS) מסוגלת לתת מענה לרבים מהאתגרים שתוארו לעיל. נכון להיום, בעלים ומפעילים של תשתיות חסרים תהליך מרוכז, המוּנע על ידי בעלי עניין, שיאשר כי מוצרי חומרה ותוכנה חיוניים עמידים בפני תוכנות זדוניות או סוגי פגיעות אחרים מצד גורמים עוינים, ולו באופן מינימלי. קביעת תהליך הסמכה, כמוּצע על ידי המועצה, תתרום תרומה עצומה לחוסן הסייבר, במיוחד אם סוכנויות ממשלתיות יוכלו לספק מידע על האיומים ויתמכו בצורות נוספות ביוזמה. הסמכה בין־לאומית למוצרי סייבר גם יכולה לתרום משמעותית לחוסנן של תשתיות, בזכות הכללתם בה של אמצעים להסמכת מוצרים מפני הפרעות אלקטרומגנטיות מכוונות. להלן יפורטו הנושאים המרכזיים שיש לתת עליהם את הדעת כחלק מקידום היוזמה להסמכה בין־לאומית למוצרי סייבר.

מינוף יכולות ותוכניות קיימות לניהול סיכונים בשרשרת האספקה בארגונים

לישויות רבות במגזר הפרטי יש כבר היום הנחיות רכש המשמשות שיטות עבודה מומלצות. המידה שבה שיטות אלו מיושמות עשויה להשתנות, אך בכל מקרה הן יכולות ליצור בסיס חשוב לפיתוח היוזמה להסמכה בין־לאומית למוצרי סייבר. לא פחות חשובה מכך היא העובדה שישויות אלו כבר פיתחו תרחישים עיסקיים לחיזוק האבטחה של שרשרת האספקה שלהן, ובמקרים רבים הן גם משלמות יותר מתוך רצון לקבל מוצרים בטוחים יותר. יש ערך רב לאימוץ שיטות עבודה מומלצות כאלו.

תיאום ממורכז

מודלים פנימיים לניהול סיכונים בשרשרת האספקה דורשים שכל ארגון יפַתח ויַישם בנפרד תהליכי הסמכה משלו עבור מוצרים וספקים שמשמשים אותו. העלות הנדרשת לשם כך, במיוחד כאשר לוקחים בחשבון את המשאבים הדרושים ליישום ואימות, עשויה להיות גבוהה משמעותית לכל ארגון. אולם אימוץ יוזמת ההסמכה הבין־לאומית יאפשר לחלק עלויות אלו באופן יחסי בין כלל המשתתפים בה, ובכך לצמצם משמעותית את הכפילות במאמצים ובהשקעת משאבים. במקביל הוא יאפשר לתמרץ ולאפשר תהליכי הסמכה ואימות מקיפים הרבה יותר מאשר אלה המקובלים כיום.

הימנעות מאימוץ תקנים "מינימליסטיים"

תקנים שכוללים רק את אמצעי ניהול הסיכונים המינימליים, למרות היותם מועילים, אינם מספיקים כדי להשיג את האבטחה הנדרשת של שרשראות האספקה הגלובליות. חבר הקונגרס האמריקאי לאנגווין (Langevin) הדגיש כי "במקום לאמץ דפוס חשיבה המבוסס על ציות, המעודד את עשיית המינימום הדרוש", עלינו "לתמרץ כראוי את הארגונים לנקוט גישה מבוססת סיכונים לאבטחת הסייבר", כולל כלפי ניהול סיכונים בשרשרת האספקה.[108] באופן דומה, תוכנית AEP קוראת לממשלה ולתעשייה "לתמרץ את הפיתוח העיסקי והכלכלי בתגובה לחוסרים באבטחת שרשרת האספקה" ומתרחקת ממודל תגובתי לאבטחת סייבר לטובת מודל פרואקטיבי יותר, אשר "מכיר בקיום סיכונים מובנים ופוטנציאליים בשרשרת האספקה ומבקש לצמצמם".[109]

כדי להתמודד עם האיומים המתרבים בשרשרת האספקה, על יוזמת ההסמכה ליישם גישה לא רגולטורית, שתתמקד בהסמכה של שיטות עבודה מומלצות ולא בתקינה מינימלית וכללית. למען הסר ספק, האמצעים הרגולטוריים שנסקרו במאמר זה מספקים כולם בסיס חיוני ליכולותיו ולצורתו של חזון ההסמכה. עם זאת, היוזמה להסמכה בין־לאומית למוצרי סייבר אינה אמורה להחליף את התקנים כאמצעי לאבטחת שרשראות אספקה, אלא לספק לחברות השונות חלופות מהימנות, הטובות מסוגן, להבטחת שלמותה של שרשרת האספקה.

אי־אימוץ מודל המבוסס על תקנים יסייע ליוזמה המדוברת להימנע מליצור מבנה רגולטורי קשיח שיקשה על השגת המטרה. הדרישות של הרגולציה מתפתחות בהכרח הרבה יותר לאט מאשר האיומים שבהם הן נועדו לטפל, ונדיר שהן כוללות שיטות עבודה מומלצות. היוזמה להסמכה בין־לאומית למוצרי סייבר צריכה אמנם להיות תואמת לתוכניות ולדרישות הרגולציה, אך רצוי שהיא לא תהיה מוגבלת בגללן. הרעיון הוא שכל תהליכי ההסמכה במסגרת היוזמה יכללו סעיפים שיחייבו הערכה תקופתית ועדכונים, במטרה לתת מענה להערכות העדכניות ביותר ולאיומים המתפתחים.

בינאום היוזמה להסמכה בין־לאומית של מוצרי סייבר מתחילתה

לרוב המכריע של שרשראות האספקה בימינו יש טביעת רגל בין־לאומית. עם זאת, רוב התקנים והנחיות הרגולציה הם ספציפיים למדינה שהתקינה אותם. לדוגמה, כל היוזמות והמודלים שנסקרו במאמר זה, למעט "אמנת האמון" ותוכניות הסמכה ספציפיות לאבטחת סייבר, מתמקדים באופן בלעדי בארצות הברית (אם כי תקני

---

108. Williams, "DHS Developing Supply Chain Security Initiative".

109. "Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector", p. 2.

התאגיד הצפון־אמריקאי לאמינות החשמל חלים גם על גופים העוסקים במתקני חשמל הרשומים בקנדה ומקסיקו). עם זאת, יוזמות חדשניות בנושא ניהול סיכונים בשרשרת האספקה מתפתחות גם בבריטניה, בישראל ובמדינות נוספות, וכדאי יהיה לשלב אותן ביוזמות האמריקאיות.

בינאום היוזמה של הסמכה של מוצרי סייבר יסייע בגיבוש הבסיס הנחוץ של משתמשים במוצר ושל לקוחותיו, ולהרחבתו. ניסיונות מצד רוסיה, סין ומדינות אחרות לנצל את הפגיעויות של שרשראות האספקה נושאים אופי רב־תחומי וגלובלי. גם היוזמה להסמכת מוצרי סייבר צריכה, לפיכך, לקבל אופי דומה.

מערכת רב־שכבתית

היוזמה להסמכה בין־לאומית של מוצרי סייבר תצטרך לשקול פיתוחה של מערכת הסמכת מוצר רב־שכבתית. מבנה רב־שכבתי כזה יכלול: (1) רמה בסיסית, שתהיה גבוהה מתִקני הרגולציה הקיימים, אך לא תגיע עד כדי הרמה "הטובה בקטגוריה"; (2) רמה גבוהה, שתקבע את התקן לדרישות הגבוהות ביותר בקטגוריה. למעשה, באמצעות מינוף תמריצי השוק והגעה לאלפי לקוחות מאובטחים במגוון תחומים, יש סיכוי שרמת "ההסמכה הגבוהה" תהיה טובה אף יותר מאשר "הטוב ביותר בקטגוריה".

תפקיד הממשלה

היוזמה להסמכה של מוצרי סייבר היא בבסיסה יוזמה של התעשייה, אך השתתפות ממשלתית בה תוכל להבטיח כי היא: (1) תפיק תועלת מניסיונם של מנהיגים בכירים; (2) תהיה תואמת באופן מרבי לצרכים של בעלי העניין; (3) תיהנה מאמינות אוטומטית בעיני אותם בעלי עניין; (4) תוכל להיות משולבת ביוזמות ממשלתיות קיימות; (5) תשלב בתוכה סדרי עדיפויות ממשלתיים כדי להפחית עלויות. שילוב פקידי ממשלה של המדינות המשתתפות ביוזמה יספק יתרון נוסף – גיוון בגישות ובפרספקטיבות – אם כי עשוי גם ליצור אתגרים, לאור רמות ההשפעה שהממשלות השונות מסוגלות להפעיל על חברות הפועלות במגזר הפרטי המקומי שלהן.

מסקנות

דיווחים של קהילת המודיעין, משרד ההגנה, המשרד לביטחון המולדת וגופים אחרים בממשל האמריקאי מצביעים על התפתחות רבה של הניסיונות לנצל את שרשראות האספקה ועל המרחקים אליהם הם שולחים את זרועותיהם, באופן שמקשה יותר ויותר על זיהוים וחשיפתם. התעשייה והממשל האמריקאיים משלבים כוחות במאמץ משותף ואגרסיבי, כנדרש, כדי לנהל את הסיכונים בשרשרת האספקה בענף החשמל בפרט ובתחום האנרגיה בכלל.

היוזמה להסמכה בין־לאומית של מוצרי סייבר אינה אמורה "להמציא את הגלגל מחדש", או לשכפל מאמצים שכבר מתקיימים. במקום זאת, עליה להיבנות כך שהיא תספק תמיכה לתוכניות קיימות ותגשר על פערים הקיימים ביניהן, וזאת בדרכים ייחודיות שנובעות מהמבנה שהיא מציעה. באופן זה תתרום היוזמה באופן מרבי לחוסנן של תשתיות.

מאמר זה הציג סקירה קצרה של המאמצים הנמשכים בנושא ההתגוננות בסייבר, מתוך מטרה לסייע בדיונים עתידיים ולזהות תחומים חדשים שבהם תוכל היוזמה להסמכת מוצרי סייבר לתרום את התרומה המשמעותית ביותר. בעלים ומפעילים של תשתיות מתמקדים יותר ויותר ברכישת מוצרים נקיים מתוכנות זדוניות. יצירת תהליך של הסמכת מוצרי סייבר, שייעשה במימון ובפיקוח המגזר הפרטי, תוך תיאום עם גופים ממשלתיים, וכן רכישת מוצרים שיענו על התקנים שייקבעו, יאפשרו לבעלי תשתיות ולמפעיליהן לתרום בכך לשיפור התקנים המתהווים ולעודד את כוחות השוק, שהם חיוניים לשיפור ניהול הסיכונים בשרשראות האספקה.

ניהול משברי גרעין והרתעה בצל לוחמת סייבר

סטפן ג'יי סימבלה

לוחמת סייבר, לפני משבר גרעיני או במהלכו, עלולה לערער את יציבות ההרתעה הגרעינית – מהשפעה שולית עליה ועד השפעה קטלנית – ובכלל זה לשבש את העברת המסרים בין ממשלים בעיתות משבר ולזרוע בלבול בהערכותיהם לגבי האירוע המתגלגל. מאמר זה בוחן את התנאים לניהול מוצלח של משבר גרעיני, את נקודות התורפה האפשריות במהלכו כתוצאה מלוחמת סייבר ואת התרחישים לכשלים.

מילות מפתח: לוחמת סייבר, לוחמת מידע, הרתעה, יציבות במשבר, מלחמה גרעינית, ניהול, שליטה ובקרה, רשתות, תקשורת, שליטה בהסלמה.

מבוא

עידן המידע ויישומיו הצבאיים־טכניים עתידים, ללא ספק, לשנות את אופייה ומאפייניה של ההרתעה הגרעינית. התשובה לשאלה כיצד בדיוק יוכלו להתקיים זו לצד זו הרתעה גרעינית ולוחמת סייבר, או שהן יתחרו ביניהן כפרדיגמות מדיניות, פחות ברורה בשלב זה. אף שמִבצעי סייבר שונים באופיים ממבצעים קינטיים, יש לראות את הרכיבים השונים של לוחמת המידע "יותר ויותר כחלקים של שלם גדול, יותר מאשר כהתמחויות נפרדות התומכות, כל אחת באופן פרטני, בפעולות צבאיות קינטיות".[1] כך, לדוגמה, פאבל ק' באאב (Baev) קובע כי "הסימן

סטפן ג'יי סימבלה הוא פרופסור למדעי המדינה ב־Penn State Brandywine, ועוסק מזה שנים רבות בלימודי ביטחון בין־לאומי, בקרת נשק גרעיני ותחומים נוספים. המחבר מבקש להודות לפול דייוויס, אנדרו פוטר, לורנס קורב ושימותי תומאס על תובנותיהם בנושא מחקר זה. הם, כמובן, אינם נושאים באחריות לתכניו.

1 Martin C. Libicki, "The Convergence of Information Warfare", *Strategic Studies Quarterly* no. 1 (Spring 2017): 50, 49-65; במאמר הנוכחי השתמשתי במונחים "לוחמת מידע" ו"לוחמת סייבר" כשווי ערך, למרות שיהיו מומחים שיתעקשו כי "לוחמת סייבר" מוגבלת למתקפות דיגיטליות על מערכות מידע ורשתות בלבד, בעוד ש"לוחמת מידע" היא

המסחרי" של מדיניות החוץ הרוסית העכשווית הוא השילוב בין פעולות שיבוש, מבצעי מודיעין, מתקפות סייבר ומתקפות תעמולה, וכי מצב זה מחייב סוג חדש של הרתעה מערבית.[2]

כאשר הנשק האולטימטיבי של השמדה המונית (נשק גרעיני) והנשק המיטבי של "הכוח הרך" (לוחמת המידע) מתערבבים זה בזה בעת משבר, התוצר ההיברידי המתקבל עשוי להיות בלתי צפוי ובלתי רצוי. משברים הם אירועים חריגים מעצם הגדרתם. לפי שעה לא התרחש אף משבר בסגנון של "מלחמה קרה" בין מדינות החמושות הן בנשק המידע של המאה ה־21 והן בנשק גרעיני. בנוסף לכך, הקשר בין סייבר לגרעין הוא בעל חשיבות מיוחדת הן עבור ארצות הברית והן עבור רוסיה: שתי המעצמות מחזיקות ביותר מתשעים אחוזים מהנשק הגרעיני העולמי, ושתיהן מפתחות יכולות לוחמת סייבר מתקדמות, הגנתיות והתקפיות כאחת.[3]

הדיון בהמשך המאמר מבקש לבחון מושגים והגדרות הקשורים בניהול משברים; להצביע על תכונות ודרישות לניהול מוצלח של משברים; לפרט את האתגרים שמִבצעי מידע ולוחמת סייבר מציבים בפני יציבותו של משבר גרעיני; ולבסוף, להציג כמה תרחישים מסוכנים של הסתבכות בניהול משבר גרעיני שהמניע לו הוא מתקפת סייבר.

רחבה יותר ומתייחסת לסוגים שונים של פעולות מבצעיות, הכוללות שיטות דיגיטליות ו/או אחרות. ראו בנושא זה: P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014), pp. 67-72; John Arquilla, *Worst Enemy: The Reluctant Transformation of the American Military* (Chicago: Ivan R. Dee, 2008), ch. 6-7.

2 Pavel K. Baev, "Corruption Spoils Every Attempt to Cooperate With Russia," *Eurasia Daily Monitor*, July 17, 2017, https://jamestown.org/analyst/pavel-k-baev.

3 לדיון על דוקטרינות ויכולות הסייבר של רוסיה, ראו: Timothy L. Thomas, *Russia: Military Strategy – Impacting 21st Century Reform and Geopolitics* (Ft. Leavenworth, Kansas: Foreign Military Studies Office, 2015), pp. 253-299. לתובנות בנושא של מלחמת סייבר ומלחמה גרעינית ראו: Erik Gartzke and Jon R. Lindsay, "Thermonuclear Cyberwar", *Journal of Cybersecurity* (2017): 1-12, https://doi:10.1093/cybsec/tyw017; Andrew Futter, "The Double-Edged Word: US Nuclear Command and Control Modernization", *Bulletin of the Atomic Scientists*, June 29, 2016, http://thebulletin.org/double-edged-sword-us-nuclear-command-and-control-modernization.html; Andrew Futter, "Cyber Threats and Nuclear Weapons: New Questions for Command and Control, Security and Strategy", *RUSI Occasional Paper*, July 2016, https://rusi.org/sites/default/files/cyber_threats_and_nuclear_combined.1.pdf; Andrew Futter, "War Games Redux? Cyberthreats, U.S.-Russian Strategic Stability, and New Challenges for Nuclear Security and Arms Control", *European Security* (December 2015): 163-180.

ניהול משברים

מושגים והגדרות

ניהול משברים, ובכלל זה ניהול משברים גרעיניים, הוא מאמץ המשלב תחרות ושיתוף פעולה בין יריבים צבאיים. מעצם הגדרתו, משבר הוא תקופה של מתיחות רבה ואי־ודאות.[4] באוויר מרחפים איומים, והלחץ על קובעי המדיניות הולך וגובר. לכל צד יש מטרות שהוא רוצה להשיג וערכים או אינטרסים שהוא מבקש להגן עליהם. במהלך מצב משברי, התנהגויות כל הצדדים מתאפיינות בתלות הדדית ובתגובתיות גבוהה. אפשר לראות את התלות ההדדית בעת משבר בין שתי מדינות כמערכת, בתנאי שהמונח "מערכת" אינו נתפס כישות נפרדת לחלוטין מהמדינה או מהתנהגויותיהם של הגורמים המרכיבים אותה. הממד של המערכת פירושו סיבתיות הדדית בהתנהגויות בעת משבר, שבה "A" נובע מ־"B" ולהיפך.

אחד ההיבטים של ניהול משברים הוא השאלה המטעה בפשטותה: מה מגדיר מצב כמשבר? מתי חל המעבר הסמוי מהיכולת של הסֵדר הבין־לאומי להכיל אלימות ואיומים לעֵבר התנהגות של משבר בפועל? התמוטטות ההרתעה הכללית במערכת מגבירה את תפיסות האיום בין השחקנים השונים, אך אינה ערובה לכך שמערכת יחסים מסוימת תידרדר לאיומים מרתיעים או משכנעים. תפיסתו של פטריק מורגן (Morgan) בדבר כישלון ההרתעה "המיידי" הינה שימושית לצורך הגדרת תחילתו של משבר: מדינה אחת מזהה תופעות ספציפיות המצביעות על כוונות עוינות מצד מדינה אחרת, שתי המדינות מחליפות איומים, ועתה עליהן להחליט מה תהיה תגובותיה של האחת לאיומי השנייה.[5] הדרך המובילה למשבר מקבילה למעבר אצל תומס הובס ממצב של פוטנציאל לאלימות למצב של הנעה בפועל של חיילים והחלפת מחאות דיפלומטיות.

---

4 לדרישות הפוליטיות והמבצעיות הכרוכות בניהול משברים, ראו: Alexander L. George, "A Provisional Theory of Crisis Management", in *Avoiding War: Problems of Crisis Management*, ed. Alexander L. George (Boulder: Westview Press, 1991), pp. 22-27; לתיאור אסטרטגיות התקפיות והגנתיות לניהול משברים, ראו: Alexander L. George, "Strategies for Crisis Management", in *Avoiding War*, Ibid. pp. 377-394; Ole R. Holsti, "Crisis Decision Making", in *Behavior, Society and Nuclear War*, ed. Philip E. Tetlock et al. (New York: Oxford University Press, 1989), 1:8-84; Phil Williams, *Crisis Management* (New York: John Wiley and Sons, 1976); Alexander L. George, "The Cuban Missile Crisis: Peaceful Resolution Through Coercive Diplomacy", in *The Limits of Coercive Diplomacy,* ed. Alexander L. George and William E. Simons, 2nd ed. (Boulder: Westview Press, 1994), pp. 111-132.

5 ראו: Patrick M. Morgan, *Deterrence: A Conceptual Analysis* (Beverly Hills: Sage Publications, 1983); Richard Ned Lebow and Janice Gross Stein, *We All Lost the Cold War* (Princeton: Princeton University Press, 1994), pp. 351-355.

כל המשברים מתאפיינים, במידה מסוימת, ברמת איום גבוהה (מומנטום הסלמה מהיר, תוך סיכון משמעותי ומיידי להידרדרות למעשי איבה אינטנסיביים יותר, למרות שאף צד לא נוקט בינתיים מעשי איבה מלאים ושני הצדדים מייחסים עדיין עדיפות להרגעת ההסלמה), בלחץ זמן לקבלת החלטות, וב"ערפל משברי" המזכיר את "ערפל המלחמה" של קלאוזביץ ומקשה על המשתתפים להבין את המתרחש.

עוד לפני שהחוקרים המודרניים הגו את הדיסציפלינה של ניהול משברים, כבר דיברו ההיסטוריונים על מרכיב "הסקת המסקנות החפוזה" (rush-to-judgment) המאפיין קבלת החלטות במצבי משבר בקרב מעצמות־העל.[6] השפעת הנשק הגרעיני על קבלת ההחלטות בעת משבר אינה קלה למדידה או לתיעוד, משום שאת ההימנעות ממלחמה ניתן לייחס לסיבות רבות. נוכחות של כוחות גרעיניים משפיעה, ללא ספק, על מידת ההרס שיכולה להתרחש אם ניהול המשבר ייכשל, ולכן נשק גרעיני הוא לא פעם גורם שדווקא מרגיע הסלמה. מעבר לחשש מקטסטרופה, חוקרים מעוניינים לבחון את אופן ההשפעה שיש לנוכחותו של נשק גרעיני על תהליך קבלת ההחלטות במהלך משבר. הבעיה חמקמקה להמשגה, שכן יש גורמים סיבתיים רבים בעלי חשיבות הרלוונטיים להחלטה על מלחמה או על שלום. כאשר מחפשים אחר הסברים, מגלים שההיסטוריה מלאה במשתנים תלויים.

ניהול משברים: דרישות ותנאים

ראשית לכל, ניהול משברים מוצלח מחייב שקיפות במסרים, אם כי מסרים מעורפלים או עמומים יעילים במקרים ספציפיים, כמו באופן שבו התנהגה איראן במשבר סביב פרויקט הגרעין שלה. שקיפות כוללת איתותים ברורים ומסרים לא מעוותים. איתות מתייחס לתנאים שלפיהם על כל צד לשלוח לצד השני את הערכתו לגבי המצב. למרות ששני הצדדים לא חייבים להיות בעלי אינטרסים זהים או אפילו משלימים, מספר מספיק של איתותים שיישלחו ויתקבלו בצורה מדויקת הוא תנאי מוקדם להעברה יעילה של מטרות ויעדים בין הצדדים. אם האיתותים נשלחים בצורה לא נכונה, או שאינם מובנים, הצעדים שינקטו השולח או המקבל עלולים לגרום לתוצאות לא מכוונות, כולל הסלמה עקב מיסקלקולציה. חומרת המצב עשויה לחייב שקיפות מלאה, אם כי יש דוגמאות רבות שבהן תקשורת חלקית הספיקה. זאת ועוד, העברת המסרים אינה בהכרח מילולית; היא יכולה להיות גם קינטית, כמו הזזת כוחות, היערכות צבאית או איתותים על נחישות.

---

6 ראו לדוגמה: Richard Ned Lebow, *Between Peace and War: The Nature of International Crisis* (Baltimore: Johns Hopkins University Press, 1981); Michael Howard, *Studies in War and Peace* (New York: Viking Press, 1971), pp. 99-109; Gerhard Ritter, *The Schlieffen Plan: Critique of a Myth* (London: Oswald Wolff, 1958); D. C. B. Lieven, *Russia and the Origins of the First World War* (New York: St. Martin's Press, 1983).

שקיפות בהעברת המסרים כוללת גם תקשורת בדרגת איכות גבוהה ואמינות טכנית, הן בין היריבים והן בקרב מקבלי ההחלטות של כל צד. כל דבר שעלול להפריע מבחינה פיזית, מכנית או התנהגותית להעברת המסר עלול לעוות את דיוק התקשורת בעת משבר. פעימות אלקטרומגנטיות המשבשות מעגלי תקשורת, או הרס פיזי של רשתות תקשורת, הם דוגמאות ברורות למכשולים להשגת תקשורת מדויקת. הבדלים תרבותיים, המונעים הבנה נכונה בין מדינות, יכולים לפגוע בהרתעה שיושמה בהתאם למקובל על פי התיאוריה של כל צד. קית' ב' פיין (Payne), המתייחס לפוטנציאל של כישלון ההרתעה בעידן שלאחר המלחמה הקרה, קובע: "לצערנו, הציפיות שלנו לגבי התנהגות היריב אינן מתמלאות לעיתים קרובות, לא משום שהיריב הוא בהכרח לא רציונלי, אלא משום שאיננו מבינים את הערכים, היעדים, הנחישות והמחויבות הספציפיים שלו בהקשר של העימות, ולכן אנו מופתעים כאשר התנהגותו 'הבלתי רציונלית' שונה מהציפיות שלנו".[7]

שנית, ניהול משברים מוצלח גם מחייב להקל את לחץ הזמן המופעל על קובעי המדיניות והמפקדים, כך שהם לא ינקטו צעדים פרובוקטיביים לעבר הסלמה שלא במתכוון, רק משום שיסברו בטעות כי "הזמן נגמר". לחץ זמן הוא דבר אחד, אך צעדים בלתי מכוונים הם עניין אחר. קובעי המדיניות ואסטרטגים צבאיים מסוגלים לבנות עולמות דמיוניים של תפיסות והערכות, שבהם "שעת השין" הופכת להיות הרבה יותר מאשר סמן שימושי בתהליך קבלת ההחלטות. כחלק מהפתולוגיות האפשריות בעת קבלת החלטות במצבי משבר, יש נטייה לבלבל בין תאריך היעד ובין מטרות המדיניות עצמן: המטרה הופכת לאמצעי, והאמצעי למטרה. לדוגמה, תוכניות המלחמה של המעצמות הגדולות ביולי 1914 תרמו לנבואה שהגשימה את עצמה אצל המנהיגים בברלין, בסנט פטרסבורג ובווינה, לפיה רק באמצעות גיוס מהיר ומתקפה הם יוכלו למנוע הפסד מוחלט במלחמה. קובעי המדיניות הגיעו למסקנה כי מבנה לוחות הזמנים של הגיוס לא היה גמיש מספיק כדי להאט את המומנטום של סוף יולי ותחילת אוגוסט 1914, שהוביל להחלטה בלתי הפיכה לטובת יציאה למלחמה.

אחת התוצאות של לחץ זמן לקבלת החלטה בעת משבר, בהשוואה לדפוסים של ימי שלום, היא שהסיכוי לטעויות מסוג I (התקפה שלא זוהתה) ומסוג II (זיהוי שגוי של מתקפה) גובר. רשתות מודיעין והתרעה טקטית מורגלות להתנהגות השגרתית של צבאותיהן של מדינות אחרות ועלולות לפרש בצורה שגויה כל חריגה מהתנהגות כזאת. קפיצות בלתי צפויות ברמות ההתרעה, או דפוסי פריסה לא

7 Keith B. Payne, *Deterrence in the Second Nuclear Age* (Lexington: University Press of Kentucky, 1996), p. 57; David Jablonsky, *Strategic Rationality Is Not Enough: Hitler and the Concept of Crazy States* (Carlisle Barracks, PA: US Army War College, Strategic Studies Institute, August 8, 1991), pp. 5-8, 31-37.

אופייניים, עלולים להביא גורמים טקטיים לפרש את הסימנים המעידים בצורה לא נכונה, כפי שטען ברוס ג' בלייר (Blair): "למעשה, אחד המאפיינים הבולטים של משבר הוא העמימות שלו. מעצם הגדרתן, שיעור השגיאות מסוג I ו־II של מערכות המודיעין וההתרעה צונח במהירות. משבר מובל לא רק על ידי ערפל המשבר הידוע, האופייני להתרעות אסטרטגיות המועדות להיכשל, אלא גם על ידי ערפל הקרב, הנובע מהידרדרות מקבילה בהתרעה הטקטית".[8]

מאפיין שלישי של ניהול משברים מוצלח היא שכל צד צריך להיות מסוגל להציע לצד השני שסתום בטיחות או דרך יציאה מכובדת מהמצב הקשה שהסלים מעבר לציפיות. במקרים מסוימים אין לשני הצדדים דרך ליציאה מכובדת מהמשבר, או כזו שאינה כרוכה בהפסד. במקרים כאלה תיווצר תחרות להקטנת הסיכון. אסור שהחיפוש אחר אופציות ידחק מי מהצדדים לפינה שממנה אין דרך לסגת בכבוד. לדוגמה, במהלך משבר הטילים בקובה ב־1962, הייתה לנשיא קנדי אפשרות להציע לראש ממשלת ברית המועצות חרושצ'וב יציאה מכובדת מפריסת הטילים המוגזמת שלו. קנדי התחייב פומבית שארצות הברית תימנע מתוקפנות צבאית בעתיד נגד קובה, ובאופן פרטי הסכים להסיר ולפרק את טילי ה"יופיטר" הבליסטיים לטווח בינוני שנפרסו קודם לכן בשטחי בעלות הברית של ארצות הברית בנאט"ו.[9] לאחר כמה ימים של דיונים והבהרות לגבי האופן שבו הסובייטים תופסים את האירועים, קנדי ויועציו הקרובים הגיעו למסקנה שהשפלה פומבית של חרושצ'וב תגרום לארצות הברית להפסיד ולא להרוויח, ותפגע בתורה באינטרס של חרושצ'וב להשיג הסכם הדדי לפתרון המשבר.

מאפיין רביעי של ניהול משברים מוצלח הוא שכל צד מחזיק בתפיסה מדויקת על כוונות הצד השני ויכולותיו הצבאיות, לרבות על נקודות התורפה והפגיעויות של היריב. לדוגמה, מצג שלפיו צד אחד משדר שהוא מוכן להסלים למלחמה יכול לסיים לפעמים את המשבר בתנאים נוחים לשני הצדדים. אולם, הערכת הכוונות והיכולות של היריב הופכת לקשה במהלך משבר, משום שהכוונות והיכולות עשויות להשתנות בלהט התחרותיות והסביבה עתירת האיומים. רוברט ג'רוויס (Jervis) הזהיר בזמנו שדי היה באמונה שהמלחמה בתקופת המלחמה הקרה היא בלתי נמנעת, כדי ליצור נבואה המגשימה את עצמה, וכתב כי "האמונה של מעצמות־העל לגבי השאלה האם המלחמה ביניהן היא בלתי נמנעת, יוצרת את המציאות באותה מידה שהיא משקפת אותה. מכיוון שמכת מנע יכולה להיות הסיבה הרציונלית היחידה לפתוח במלחמה כוללת, יש חשיבות רבה לאמונות

8 Bruce G. Blair, *The Logic of Accidental Nuclear War* (Washington: Brookings Institution, 1993), p. 237.

9 Lebow and Stein, *We All Lost the Cold War*, pp. 122-123.

לגבי כוונותיו המעשיות של הצד השני, ואמונות אלו תלויות, במידה רבה, בהערכה מה הצד השני מאמין שאני עתיד לעשות".[10]

הכוונות עשויות להשתנות במהלך משבר, ככל שקובעי המדיניות הופכים אופטימיים יותר לגבי רווחים צפויים, או פסימיים יותר לגבי הפסדים פוטנציאליים. ניהול התרעות צבאיות ופריסת כוחות, או כל תנועה אחרת של כוחות צבא, עשויים לשנות את יכולות הצדדים. מצבי מוכנות והיערכות צבאית גבוהה בכל אחד מהצדדים נועדו לשדר איתות דו־צדדי: נכונות לגרוע מכול היה והצד השני יתקוף; עמדה יציבה בלתי מאיימת במצב של פסיביות מצד האויב. זהו מסר מעורב, שקשה לשדרו גם בתנאים הטובים ביותר לניהול משברים, שכן ההתנהגויות והמסרים של מדינה מסוימת יכולים להיראות כבלתי עקביים בעיני היריב.

בתנאים של לחץ זמן ואיום צבאי, גופים שונים בארגונים ביטחוניים מורכבים עשויים לקבל החלטות שיתבססו על נקודת המבט הצרה והביורוקרטית שלהם. החלטות ופעולות כאלו לא תמיד ישקפו את כוונתם של קובעי המדיניות, או שלא ייעשו בתיאום עם ההחלטות והפעולות של גורמים אחרים בממשל. הסביר זאת אלכסנדר ל' ג'ורג': "חשוב להכיר בכך שהיכולת של סמכויות פוליטיות בכירות לשלוט במהלכים ובפעולות של כוחות הצבא נעשית קשה, בשל מספרן ומורכבותן של פקודות ההיערכות הנכנסות לתוקף ברגע שפורץ משבר, וככל שהוא מתעצם. לא קל לסמכות הפוליטית הבכירה לקבל מידע מלא ומדויק על כל פקודות ההיערכות הקיימות. כתוצאה מכך, היא עלולה להיכשל בתיאום בין פקודות חשובות ובין האסטרטגיה הכוללת שלה לניהול המשבר".[11]

בשעה שקובעי המדיניות מתמודדים עם האתגר של נהלים מבצעיים רבים ומגוונים, מנהיגים פוליטיים עשויים לגלות גם חוסר רגישות לעלויות של שינויים פתאומיים בפקודות היערכות, או לא להיות מודעים לרציונל שבבסיסן של פקודות כאלו. לדוגמה, מנהיגי מדינה או ראשי ממשלה אולי לא יהיו מודעים לכך שככל שהם מאשרים רמות מוכנות גבוהות יותר, כך כללי הפתיחה באש של הכוח הצבאי הנמצא בשטח הופכים למתירנים יותר.[12] במקרים אחרים השליטה עשויה להיות הדוקה למדי. מנָהלי המשבר לומדים עד מהרה ותוך כדי התנסות לקח חשוב הקשור להבחנה בין משבר ובין מלחמה בפועל: המעבר מהאחד לשנייה הוא פחות דיכוטומי ויותר רציף, והשלב הסופי של המשבר אינו ברור מספיק, למעשה עד הצעד הגורלי לעבר מלחמה, שאין ממנו דרך חזרה. כך, לדוגמה, מנהיגי המדינות

10 Robert Jervis, *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon* (Ithaca: Cornell University Press, 1989), p. 183.

11 Alexander L. George, "The Tension Between 'Military Logic' and Requirements of Diplomacy in Crisis Management", in *Avoiding War: Problems of Crisis Management*, p. 18.

12 שם.

באירופה בשנת 1914 היו בטוחים בתחילה ביכולתם לנהל משבר שלא יתפתח למלחמה, אך ככל שהשליטה באירועים הלכה ונשמטה מידיהם, אמונה זו התחלפה באמונה פטליסטית, שהובילה לדרך ללא מוצא.

גורמים משבשים פוטנציאליים

ללוחמת מידע (או לוחמת סייבר) יש פוטנציאל לתקוף או לשבש ניהול משברים מוצלח בכל אחת מהתכונות ומהמאפיינים שהוזכרו לעיל.[13] ראשית, לוחמת סייבר יכולה לערפל את האיתותים שנשלחים מצד אחד למשנהו במהלך משבר. הדבר יכול להיעשות בכוונה או בשוגג. נניח שצד אחד שתל וירוס או תולעת ברשתות התקשורת של הצד השני.[14] הווירוס או התולעת מופעלים במהלך המשבר ומשמידים או משַנים מידע. המידע החסר או הלא תקין עלול להקשות על קורבן הסייבר לארגן התקפה צבאית. יחד עם זאת, מידע שנפגע או השתנה עלול להטעות את שני הצדדים לחשוב כי האיתות ששלחו פורש כהלכה, בשעה שלא כך היה. למשל, צד א' אולי התכוון לאותת ליריבו על "נחישות" במקום "כניעה" בסוגיה מסוימת, אולם צד ב' פירש את האיתות בטעות כמסר של "כניעה" והחליט להמשיך בתוקפנות. צד ב' ייתקל בהתנגדות בלתי צפויה, והתוצאה תהיה התפתחות מצב הרבה יותר מסוכן. יש גם אפשרות של מכת מנע בסייבר במטרה להשבית טילים גרעיניים של האויב לפני הגעתם לכן השיגור, או במהלך השיגור עצמו. ארצות הברית השתמשה ככל הנראה בטכניקות כאלו ("left-of-launch") נגד צפון קוריאה.[15] האם מהלך כזה יתקבל בעת משבר גרעיני על ידי הצד המותקף כמהלך של הפחדה והרתעה? או להיפך: האם מתקפת סייבר נגד שיגור טילים תביא למכה גרעינית ראשונה מהצד המתגונן, מתוך חשש לאבד את יכולת התגמול שלו?

לוחמת סייבר יכולה גם להרוס או לשבש את ערוצי התקשורת הנחוצים להצלחת ניהול המשבר. היא יכולה לשבש קשר תקשורתי בין קובעי המדיניות

---

13 להגדרות שימושיות ל"מתקפת סייבר" ו"לוחמת סייבר" ראו: Paul K. Davis, "Deterrence, Influence, Cyber Attack and Cyberwar", *International Law and Politics* 47 (2015): 327-355.

14 וירוס הוא תוכנית שמשכפלת את עצמה ומיועדת להרוס או לשנות את התוכן של קבצים אחרים המאוחסנים על תקליטונים או כוננים קשיחים. תולעים משחיתות את שלמות המידע במערכות תוכנה ומידע מ"בפנים החוצה", בדרכים שיוצרות נקודות תורפה שהאויב מנצל.

15 David E. Sanger and William J. Broad, "Trump Inherits a Secret Cyberwar Against North Korean Missiles," *The New York Times*, March 4, 2017, https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html?_r=0; Jesse T. Wasson and Christopher E. Bluesteen, "Taking the Archers for Granted: Emerging Threats to Nuclear Weapon Delivery Systems", Paper presented at the Annual Conference of International Studies Association, Baltimore, MD, 2017.

ובין המפקדים הצבאיים במצב של איום גבוה ולחץ זמנים קריטי. הפרעה כזו אינה חייבת להיות מתוכננת, ודי אם תהיה תוצאה של תוכנה זדונית שהושתלה קודם לכן והופעלה באופן בלתי צפוי, או שלא תחת שליטה מלאה של יוצריה. בתנאים כאלה מתעוררים שני סוגים של בעיות בלתי צפויות ביחסים בין המערכת הצבאית למערכת האזרחית: ראשית, ייתכן שמנהיגים פוליטיים יאצילו מראש סמכויות לשימוש בנשק גרעיני בתנאים מגבילים, הקובעים שרק כאשר יתקיימו תנאים מסוימים אלה (על פי הפרוטוקולים המלווים את ההאצלה מראש), המפקדים הצבאיים יהיו מורשים להשתמש בנשק הגרעיני שמצוי תחת פיקודם. תקשורת חסומה, משובשת או הרוסה עלולה לגרום לכך שהמנהיגים לא יוכלו לדעת כאשר מפקדים צבאיים יפרשו את המצב בצורה הרבה יותר נואשת ממה שהוא באמת, ולכן יסברו שיש להם היתר ליזום מהלך גרעיני. לדוגמה, תקשורת משובשת בין מטה הפיקוד הלאומי של ארצות הברית ובין הצוללות הנושאות טילים בליסטיים במהלך המלחמה הקרה, כתוצאה מהתקפה על אותן צוללות, יכולה הייתה להוביל את קציני הצוללות ואנשי הצוות שלהן להחלטה משותפת, בהיעדר הנחיות מנוגדות, לשגר טילים גרעיניים.

ביקורת שהופנתה לטיוטה מוקדמת יותר של מאמר זה זיהתה נכון את הפרדוקס שבהנחה, לפיה מנהיגים יאשרו מתקפת סייבר במהלך משבר, שאותו היו מעדיפים לסיים לפני שיתדרדר למלחמה. לכאורה, הגיוני להניח, לפחות באופן עקרוני, שמתקפת סייבר יש לשגר בשילוב עם מכה ראשונה ולא לפניה. אני מודה שיש בכך היגיון, אבל יש לכך גם צד אחר: ראשית, תקיפות סייבר במהלך משבר עשויות לשמש לא רק כאמצעי ליצירת תקלות טכניות במערכות המידע של האויב ובתהליך קבלת ההחלטות שלו, אלא גם להיות סוג של אמצעי מיקוח אסטרטגי לסיום הסכסוך מנקודת יתרון גבוהה יותר, ואפילו עם תוצאה חיובית יותר. לדוגמה, טכניקות "left-of-launch" לשיבוש הרשתות התומכות במערכות שיגור הטילים יכולות לתמוך ביכולות ההגנה מפני טילים של צד אחד, ולערער את הביטחון העצמי של הצד השני לגבי יכולתו לשגר התקפות טילים בליסטיים.

שנית, לוחמת מידע בעת משבר תגביר כמעט בוודאות את לחץ הזמן של מנהיגים פוליטיים. הלחץ יכול להיווצר מדוחק זמן אמיתי, או כתוצאה מתפיסת הזמן שקובעי המדיניות חשים שיש להם כדי לקבל החלטות. ברגע שאחד הצדדים רואה שחלקים של מערכת הפיקוד, השליטה והתקשורת שלו נפגעים בשל מידע מזויף או רעשי סייבר חיצוניים, תחושת התבהלה (פניקה) שלו מפני אובדן אפשרי של אופציות צבאיות הולכת וגוברת. כך, לדוגמה, שיבוש, ולו חלקי, של המערכת האסטרטגית לפיקוד, שליטה ותקשורת של ארצות הברית במהלך המלחמה הקרה, יכול היה למנוע ביצוע יעיל של התוכנית האסטרטגית שלה למלחמה גרעינית (SIOP). תוכנית זו הייתה תלויה באומדנים מתואמים ומתוזמנים היטב ובתחזיות

מדויקות של נזקים למטרות מסוגים שונים. שיבוש והטעיה, ולו חלקיים, של רשתות ומרכזי תקשורת היו גורמים למתקפות מיותרות על אותן מטרות, וסביר להניח שגם מביאים להתקפות בלתי מתוכננות על מתקנים צבאיים או אזרחיים ידידותיים.

השפעה משבשת אפשרית שלישית שיש ללוחמת מידע על ניהול משבר גרעיני היא הסכנה שלוחמת המידע תצמצם את החיפושים אחר חלופות זמינות מבין המעטות שיש. קובעי מדיניות המחפשים דרכי נסיגה ממשבר סבוך זקוקים לאפשרויות גמישות ולפתרון בעיות יצירתי. קורבנות של לוחמת סייבר עלולים לחוות ירידה ביכולת לפתור בעיות באופן שגרתי, ובוודאי יצירתי, לאחר שרשתות המידע מתמלאות ב"זבל". השאלות למפעילים יוצגו בצורה גרועה, והתשובות (אם יהיו בכלל זמינות) ישאפו למכנה המשותף הנמוך ביותר של תהליכי ההפעלה הסטנדרטיים שתוכננו מראש.

מערכות תגמול, התלויות בשיגור במצב של התרעה, ולא במצב של הישרדות לאחר התקפה, חשופות במיוחד לקיצורי זמנים ולחלופות מוגבלות, כפי שמציין ברוס בלייר: "גם מערכת התרעה מתוכננת היטב אינה יכולה להציל מפקדים מפני קריאה שגויה של המצב כתוצאה מאילוצי זמנים ומידע במסגרת התפיסה של 'שיגור במצב של התרעה'. תפיסה כזאת קוטעת את תהליך קבלת ההחלטות מוקדם מכדי שתאפשר הערכה חוזרת שתעלה בקנה אחד עם המציאות. תגובה מהירה היא, מעצם טיבה, בלתי יציבה, משום שהיא מקצרת את זמן הלמידה הדרוש כדי להתאים את התפיסה למציאות".[16]

הנטייה לחפש את החלופה הזמינה הראשונה שעומדת בתנאי הסף המינימליים להשגת המטרה, חזקה אצל ארגונים ביורוקרטיים לא צבאיים גם בתנאים רגילים.[17] במערכות שליטה ובקרה אזרחיות־צבאיות, הפועלות תחת הלחץ של קבלת החלטות בעת משבר גרעיני, החלופה הזמינה הראשונה יכולה להיות גם האחרונה, פשוטו כמשמעו, או כך לפחות קובעי המדיניות והיועצים הצבאיים עשויים לשכנע את עצמם. לפיכך, ההטיה לעבר פתרונות מהירים ומינימליים היא רבה. כך, למשל, במהלך משבר הטילים בקובה ב־1962, אנשי הקבוצה המייעצת לנשיא קנדי שבו והציעו, לאורך כל 13 ימי המשבר, תקיפה אווירית ופלישה לאי. אם היה פחות זמן לדיונים, או אם הנשיא לא היה מכוון את הדיונים כך שיועלו בהן חלופות שונות, ייתכן מאוד שהמכה האווירית והפלישה היו החלופה הנבחרת.[18] פול ק' דיוויס ציין בהקשר זה: "הדיונים המקובלים בנושא יציבותם של משברים מניחים כי המנהיגים שולטים ביכולות הגרעיניות שלהם. כמו תמיד, ההיסטוריה גורמת להתפכחות.

16 Blair, *The Logic of Accidental Nuclear War*, p. 252.

17 James G. March and Herbert A. Simon, *Organizations* (New York: John Wiley and Sons, 1958), pp. 140, 146.

18 Lebow and Stein, *We All Lost the Cold War*, pp. 335-336.

הנשיא קנדי החל להיות מודאג בשנת 1961 מפעולות חד־צדדיות אפשריות של מפקדים צבאיים, שיכינו מכה מקדימה נגד ברית המועצות. הוא השקיע מאמצים כדי להדק את שליטתו האישית כנשיא. ההנהגה הסובייטית, שדאגה לשרידות כוחותיה הצבאיים, פיתחה יכולת לשיגור במצב של התרעה ולתגובה אוטומטית על מתקפה. מערכות [סובייטיות] כאלו יכלו להיות מקור למלחמה בשוגג".[19]

לבסוף, מתקפת סייבר יכולה לגרום לכל צד להעביר לצד השני תמונה שגויה של הכוונות והיכולות שלו, שיש בה פוטנציאל לתוצאות הרות אסון. דוגמה נוספת ממשבר הטילים בקובה ממחישה את תופעות הלוואי האפשריות של אי־הבנה פשוטה ותקשורת לקויה בניהול משברים בארצות הברית. בשיא המתיחות של ימי המשבר, סטה מטוס ריגול אמריקאי מסוג U–2 ממסלולו ונכנס בטעות לתוך המרחב האווירי הסובייטי. מטוסי קרב אמריקאיים וסובייטיים נכנסו לפעולה, ועימות אפשרי בין חילות האוויר של שתי המדינות באזור הארקטי עמד על הפרק. חרושצ'וב סיפר אחר כך לקנדי כי ההגנה האווירית הסובייטית עלולה הייתה לפרש את טיסת ה־U–2 כמשימת סיור מוקדם לפני תקיפה, או לראות בו מפציץ, ולחייב את ברית המועצות להגיב.[20] למרבה המזל, מוסקבה בחרה לתת לארצות הברית ליהנות במקרה זה מהספק, והתירה למטוסי הקרב האמריקאיים ללוות את ה־U–2 הסורר בחזרה לאלסקה. שאלה שמעולם לא קיבלה תשובה מלאה היא מדוע לא בוטלה המשימה המתוכננת של ה־U–2 מיד עם פרוץ המשבר? ייתכן שהתשובה פשוטה וקשורה לתהליכי ביורוקרטיה, בשילוב עם חוסר תקשורת בשרשרת הפיקוד של קובעי המדיניות האמריקאים, שלא העריכו נכונה את הסיכון של משימת ריגול "רגילה" בתנאים רגישים אלה.

ההערכה של החוקר מרטין ליביצקי על היחסים בין לוחמת סייבר ובין ניהול משברים מדגישה את הדברים והדוגמאות שהובאו לעיל: "ניתן לומר בהכללה שמצב שבו אין לחץ רב להגיב במהירות ושבו נחיתות או הפסד זמניים יהיו נסבלים ויש מקום לתת לצד השני ליהנות מעט מהספק, הוא מצב שבו יש זמן לנהל את המשבר. לעומת זאת, אם אי־יכולת להגיב במהירות יביא לשחיקה במעמדה של

19 Paul K. Davis, Peter Wilson, Jeongeun Kim and Junho Park, "Deterrence and Stability for the Korean Peninsula", *Korean Journal of Defense Analysis* no. 1 (March 2016): 14.

20 Graham T. Allison, *Essence of Decision: Explaining the Cuban Missile Crisis* (Boston: Little, Brown, 1971), p. 141; Scott D. Sagan, *Moving Targets: Nuclear Strategy and National Security* (Princeton: Princeton University Press, 1989), p. 147; Lebow and Stein, *We All Lost the Cold War*, p. 342.

מדינה, לנחיתות זמנית או להפסד שהם בלתי נסבלים, ואין מחלוקת לגבי האירוע, האחראי לו וסיבותיו, אזי מדינות יכולות להגיע למסקנה כי עליהן לפעול במהירות".[21]

תרחישים וסיכונים

התוצאה של תרחיש שבו ניהול משבר גרעיני מושפע מלוחמת מידע אינה בהכרח חיובית. למרות מיטב המאמצים שהצדדים למשבר עשויים להשקיע, המחלוקת ביניהם עלולה להידרדר למכה או לתקיפה גרעינית ראשונה של אחד הצדדים ולמכת תגמול על ידי האחר. במצב כזה, פעולות סייבר של אחד הצדדים, או של שניהם, עלולות להקשות על ריסון המלחמה ועל כל ניסיון לסיים אותה לפני שתגרום הרס ואובדן חיים בקנה מידה קטסטרופלי. כפי שכבר צוין, הפרטים של כל מקרה חשובים. בלוחמה פסיכולוגית, התוקף והמותקף עשויים להציג במכוון הצלחות ככישלונות או כישלונות כהצלחות, אם הם מעוניינים בהרגעת ההסלמה, וייצוג כוזב כזה יכול לתרום לכך.

אף שאין מלחמות גרעיניות "קטנות", יש גם דעה הפוכה מכך. במהלך המלחמה הקרה התפתח הרעיון של "לחימה גרעינית מוגבלת", "לחימה גרעינית טקטית" או "חילופי שיגורים הדדיים מצומצמים", ורעיונות דומים צצו גם סביב יכולותיהן הגרעיניות של הודו ופקיסטן. בדומה למלחמות קונבנציונליות, ייתכנו גם סוגים שונים של מלחמות גרעיניות, בהתאם לסיבות ולתוצאות המיידיות שלהן.[22] האפשרויות השונות כוללות התקפה גרעינית שמקורה אינו ידוע; מקרה לא חד־משמעי ולא מוכח של שימוש בנשק גרעיני כמכה ראשונה; פיצוץ גרעיני במסגרת "ניסוי" שנועד להפחיד, אך ללא גרימת הרס מיידי; תקיפה קונבנציונלית, שלפחות בשלב הראשון פורשה בטעות כתקיפה גרעינית. כפי שציין ג'ורג' ה' קווסטר (Quester): "ארצות הברית ומעצמות אחרות פיתחו כמה ראשי נפץ קונבנציונליים גדולים ורבי עוצמה, שנועדו להרוס את הבונקרים המוקשחים שעשויים לאכסן עמדת פיקוד של האויב או מערכת נשק מסוכנת שלו. פצצות 'חודרות בונקר' כאלו מהדהדות אות קולי מסוים כאשר הן מופעלות וגורמות לאותות סיסמיים תת־קרקעיים, שממרחק עלולים להתפרש בטעות כראש נפץ גרעיני קטן".[23]

התרחיש הדומיננטי, של מלחמה גרעינית כוללת בין ארצות הברית לברית המועצות, העסיק את קובעי המדיניות של ימי המלחמה הקרה. כתוצאה מכך, חששות בנוגע לשליטה בהסלמה וסיום המלחמה נסחפו בחזון אפוקליפטי של אחרית הימים. עידן הגרעין השני, שחופף למדי לסיום המלחמה הקרה ולהתפרקותה

21 Martin C. Libicki, *Crisis and Escalation in Cyberspace* (Santa Monica: RAND Corporation, 2012), p. 145.

22 לתרחישים רלוונטיים ראו: George H. Quester, *Nuclear First Strike: Consequences of a Broken Taboo* (Baltimore: Johns Hopkins University Press, 2006), pp. 24-52.

23 שם, עמ' 27.

של ברית המועצות, מציע תפריט מורכב יותר של אפשרויות ותגובות גרעיניות.[24] מדינות סוררות, מדינות השואפות להגמוניה אזורית, או טרוריסטים, שיש להם אינטרסים לאיים בנשק גרעיני או להשתמש בו, וכן התפשטות אפשרית של נשק גרעיני למדינות שכיום אינן גרעיניות, מותחים עד קצה הדמיון את כושר ההתמודדות וההמצאה של אסטרטגים צבאיים וסופרי מדע בדיוני.

בנוסף לגורמים האפלים ביותר המעורבים באיומים גרעיניים או באיומים להנחית מכה ראשונה, קיימת אפשרות נוספת, והיא סכנת הידרדרות התלויה בתנאים הפוליטיים השוררים בין ארצות הברית לרוסיה, בין רוסיה לסין או בין סין להודו (כלומר, בין המדינות הגרעיניות של ימינו). "הממסד" הגרעיני, המכונה "מדינות ה־P–5", פועל לעיתים להרגעה, התלויה בהמשך קיומן של נסיבות פוליטיות חיוביות בפוליטיקה האזורית והגלובלית. עימותים פוליטיים, שלא ניתן להעלותם על הדעת בעשור מסוים, עשויים להתפתח למלחמות בלתי נמנעות מבחינה פוליטית בעשור אחר. מלחמת העולם הראשונה היא דוגמה מאלפת לכך. המלחמה בין רוסיה לגיאורגיה באוגוסט 2008 הייתה תזכורת נוספת לכך שסכסוכים מקומיים לאורך קווי שבר אזוריים, בין גושים או מעצמות גדולות, יכולים להתרחב לכדי עימותים קשים, כפי שקרה גם במלחמות הבלקן בשנות התשעים של המאה העשרים. במקרים כמו אלה, היתרון הצבאי החד־צדדי של רוסיה על גיאורגיה ב־2008, והעוצמה הצבאית של נאט"ו מול זו של הבוסנים ב־1995 והסרבים ב־1999, תרמו לסיום המלחמות ללא הסלמה נוספת ברמה הבין־לאומית.

הסלמה של מלחמה קונבנציונלית לכדי שימוש ראשוני בנשק גרעיני עדיין אפשרית גם בימינו, כאשר נשק גרעיני, מבצעי או טקטי, נפרס על ידי כוחות צבא לאומיים או כוחות קואליציוניים. ארצות הברית פרסה כמה מאות כלי נשק

---

24 הערכות על הרתעה לפני ואחרי המלחמה הקרה מופיעות בפרסומים הבאים: Colin S. Gray, *The Future of Strategy* (Cambridge: Polity Press, 2015), pp. 98-106; Paul Bracken, *The Second Nuclear Age: Strategy, Danger and the New Power Politics* (New York: Henry Holt – Times Books, 2012); Adam B. Lowther ed., *Deterrence: Rising Powers, Rogue Regimes and Terrorism in the Twenty-First Century* (New York: Palgrave Macmillan, 2012); Beatrice Heuser, *The Evolution of Strategy: Thinking War from Antiquity to the Present* (Cambridge: Cambridge University Press, 2010), pp. 351-383; Michael Krepon, *Better Safe than Sorry: The Ironies of Living with the Bomb* (Stanford, Calif.: Stanford University Press, 2009); Lawrence Freedman, *Deterrence* (Cambridge: Polity Press, 2004); Lawrence Freedman, *The Evolution of Nuclear Strategy*, 3rd ed. (New York: Palgrave Macmillan, 2003); Patrick M. Morgan, *Deterrence Now* (Cambridge: Cambridge University Press, 2003); Keith B. Payne, *The Fallacies of Cold War Deterrence and a New Direction* (Lexington: University Press of Kentucky, 2001); Colin S. Gray, *The Second Nuclear Age* (Boulder: Lynne Rienner, 1999); Payne, *Deterrence in the Second Nuclear Age*; Jervis, *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon*.

גרעיניים אווריים טקטיים בבסיסים של בעלות הברית שלה בנאט"ו – בלגיה, גרמניה, איטליה, הולנד וטורקיה.[25] רוסיה מחזיקה, ככל הנראה, בכמה אלפי כלי נשק גרעיניים, טקטיים או מבצעיים, כולל מספרים משמעותיים שלהם הפרוסים במערב המדינה.[26] הסכם START החדש, לאחר שיאושרר, ייצור שוויון בין ארצות הברית לרוסיה במערכות נשק גרעיניות בעלות טווח בין־יבשתי.[27]

העליונות של ארצות הברית ושל נאט"ו, מבחינה טכנולוגית ומבחינת הכוח הצבאי הקונבנציונלי מבוסס המידע, משאירה את רוסיה תלויה במידה רבה בנשק גרעיני טקטי, כפיצוי על חולשתה היחסית בכוחות לא גרעיניים. מדינות נאט"ו נשמו לרווחה כאשר הדוקטרינה הצבאית של רוסיה, שאושרה רשמית ב־2010, לא הנמיכה את סף השימוש הראשוני בנשק גרעיני בהשוואה למהדורות קודמות שלה.[28]הדוקטרינה הצבאית מ־2010 מצביעה על נכונות לעשות שימוש ראשון בנשק גרעיני במצבי חירום קיצוניים, כפי שתגדיר אותם ההנהגה הפוליטית הרוסית.[29]

למרות העליונות הברורה של הכוחות הקונבנציונליים של ארצות הברית ונאט"ו על פני אלה של רוסיה, המערב אינו משתוקק בהכרח להיפטר מהנשק הגרעיני הטקטי שנותר פרוס בשטחיהן של בעלות הברית. פאנל מומחים שכינס נאט"ו ב־2010 כדי לבחון את הדוקטרינה הצבאית של הארגון היה אמביוולנטי וזהיר בנוגע לעתיד פריסתו של הנשק הגרעיני של חברות הברית. הסוגיה של משא ומתן על פירוק נשק זה בתמורה לוויתורים מקבילים של רוסיה נותרה פתוחה לדיון נוסף. במקביל, הדוח של מומחי נאט"ו הדגיש את האווירה הנוכחית השוררת

---

25 לרקע על הנשק הגרעיני הטקטי שארצות הברית פרסה באירופה ראו: Hans M. Kristensen, *U.S. Nuclear Weapons in Europe: A Review of Post-Cold War Policy, Force Levels and War Planning* (Washington, D.C.: Natural Resources Defense Council, February 2005).

26 Pavel Podvig, "What to do about Tactical Nuclear Weapons", *Bulletin of the Atomic Scientists*, February 25, 2010, https://thebulletin.org/2010/02/what-to-do-about-tactical-nuclear-weapons/; Jacob W. Kipp, "Russia's Tactical Nuclear Weapons and Eurasian Security", *Eurasia Defense Monitor*, March 5, 2010, https://jamestown.org/program/russias-tactical-nuclear-weapons-and-eurasian-security/.

27 "Treaty between the United States of America and the Russian Federation on Measures for the Further Reduction and Limitation of Strategic Offensive Arms", *US Department of State,* Washington, D.C., April 8, 2010, http://www.state.gov/documents/organization/140035.pdf.

28 "The Military Doctrine of the Russian Federation", February 5, 2010, in *Johnson's Russia List* 2010, #35, February 19, 2010; Nikolai Sokov, "The New 2010 Russian Military Doctrine: The Nuclear Angle", *Center for Nonproliferation Studies, Monterey Institute of International Studies*, February 5, 2010, http://cns.miis.edu/stories/100205_russian_nuclear_doctrine.htm.

29 Keir Giles, "The Military Doctrine of the Russian Federation 2010", *NATO Research Review* (February 2010): 1-2, 5-6.

אצל מדינות הברית, לפיה נשק גרעיני מהווה חוליה הכרחית בשרשרת אופציות ההרתעה של מדינות אלו.[30]

קשה לתאר כיצד יתגלגלו משבר גרעיני או קבלת החלטה על שימוש ראשון בנשק גרעיני, כאשר גם נאט"ו וגם רוסיה יעשו שימוש בדיסאינפורמציה אסטרטגית ובלוחמת מידע במטרה לשבש את מערכות הפיקוד והבקרה, התקשורת וההתרעה של האויב. מבצעי סייבר משבשים נגד מערכות אויב, במצב של סף שימוש ראשון בנשק גרעיני או זמן קצר לאחר מכן, עלולים להגביר את הקושי, הרב ממילא, לעצור את הלחימה לפני התפשטות העימות על פני כל אירופה או הגעה למלחמה גרעינית אסטרטגית. הקשיים שפורטו לעיל – ניהול משברים בצל הרתעה גרעינית או בהמתנה להחלטה על שימוש ראשון בנשק גרעיני – יעמידו את לכידותן של מדינות הברית הצפון אטלנטית תחת לחץ וסכנה חסרי תקדים, שללא ספק יחמירו עוד יותר עקב מצבי אי־ודאות וערפול בזירת הקרב.

ברית נאט"ו צפויה לעמוד בפני שלושה מצבי חיכוך חדשים: ראשית, ההחלטה אם להשתמש בנשק גרעיני מתקבלת כיום אך ורק בתוך שרשרת הפיקוד האמריקאית (או זו של בריטניה/צרפת). נאט"ו לא נתנה את הדעת לאתגר של ניהול תהליך קבלת החלטות במצב של סף מלחמה על ידי 29 מדינות החברות כיום בברית, לעומת 16 בלבד בתקופת המלחמה הקרה. לא רק שמספר המדינות החברות בברית גדל מאז, גם השוני במדיניות החוץ שלהן, בסדרי העדיפויות של הביטחון הלאומי שלהן ובתפיסותיהן הצבאיות־פוליטיות מציב מכשול אדיר בפני קבלת החלטות במצבי לחץ, במיוחד קבלת החלטה לשימוש ראשון בנשק גרעיני; שנית, יהיה חיוני להשיג מודיעין מהימן לגבי כוונות רוסיה בעקבות שימוש ראשוני שלה בנשק גרעיני, או שימוש כזה על ידי נאט"ו, אלא שמודיעין כזה יהיה קשה להשגה; שלישית, שימוש ראשוני בנשק גרעיני, לראשונה מאז הטלת פצצת האטום על נגסקי, יהיה פתח למצב פסיכולוגי, פוליטי ומוסרי חדש, שבו נושאים ונותנים שיבקשו לשים קץ להסלמה, או להביא לסיום המלחמה, יצטרכו לשמור על קור רוח, לשכנע את צבאותיהם להימנע מפעולה ולהחזיר משגרים של נשק גרעיני ואת הנשק הגרעיני עצמו לאתרים מאובטחים, אך כאלה שיהיו גלויים לצדדים היריבים. את כל המהלכים האלה יהיה צורך לבצע על רקע התבהלה שתתפשט ברשתות החברתיות ובאינטרנט, שיפעלו "סביב השעון".

30 *NATO 2020: Assured Security; Dynamic Engagement, Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO* (Brussels: North Atlantic Treaty Organization, May 17, 2010), pp. 43-44.

מסקנות

השילוב האפשרי של לוחמת מידע עם המשך ההרתעה הגרעינית בתקופה שלאחר המלחמה הקרה יכול להפיק תוצרי לוואי לא מכוונים, ואלה עלולים להיות מסוכנים ליציבות העולמית. אחת המטרות של לוחמת סייבר בזמן מלחמה קונבנציונלית תהיה למנוע מכוחות האויב מודעות למתרחש בזירת הקרב, ומנגד להשיג שליטה על מודעות כזאת, כפי שארצות הברית הצליחה לעשות במידה רבה במלחמת המפרץ הראשונה ב־1991.[31] בשעת משבר, שבו נשק גרעיני זמין בידי הצד הנתון למתקפת סייבר, הפגיעה במערכות המודיעין ובמערכות השליטה והבקרה של האויב יכולה לעמוד בסתירה לרצון להגיע לשליטה על העימות ולהשיג ניצחון במחיר נסבל. בתנאים מסוימים של ניהול משבר גרעיני, פגיעה בפיקוד, בשליטה, בתקשורת, במחשבים, במודיעין וביכולת המעקב ואיסוף המידע של היריב יכולה להתברר כ"גול עצמי". כדי שמֶסר של הרתעה יפעל, גם כאשר עומד מאחוריו איום אמין בפעולת מניעה או תגמול, הוא חייב תחילה לעבור בהצלחה ובצורה משכנעת לידיו של הצד השני.[32]

31 כפי שאמר דיוויד אלברטס: "שליטה במידע תישאר עניין אקדמי בלבד, אם לא נוכל להפוך אותה לשליטה בשדה הקרב". ראו: David Alberts, "The Future of Command and Control with DBK", in *Dominant Battlespace Knowledge*, ed. Stuart E. Johnson and Martin C. Libicki (Washington: National Defense University, 1996), pp. 77-102, especially p. 80.

32 כפי שאמר קולין גריי: "מכיוון שהרתעה נובעת מיחסי גומלין, היא אינה יכולה להתקיים במצב של יכולות, התנהגות או כוונות של צד אחד בלבד. כל מי שמתייחס ל'מדיניות ההרתעה' בהא הידיעה, כנראה שפשוט אינו מבין את הנושא". ראו: Collin Gray, *Explorations in Strategy* (Westport: Greenwood Press, 1996), p. 33.

"לוחמה כלכלית רחבה" בעידן הסייבר

שמואל אבן

"לוחמה כלכלית רחבה" היא מכלול פעולות לשם פגיעה, או איום בפגיעה, במשק האויב/היריב במטרה להפעיל עליו לחצים או להחלישו, וזאת כדי להשיג את יעדיו האסטרטגיים של מפעיל הלוחמה. "לוחמה כלכלית רחבה" כוללת בתוכה: לוחמה כלכלית מקובלת (כגון סנקציות), לוחמה קינטית ולוחמת סייבר נגד כלכלת האויב.
עידן הסייבר משַנה את תחום הלוחמה הכלכלית הרחבה. בהיבט ההתקפי, יכולות סייבר מאפשרות לפגוע בכלכלת האויב בעת מלחמה ובין המלחמות. לוחמת סייבר עשויה להעצים את הפגיעה במשק האויב, וזאת בנוסף לסנקציות כלכליות ו/או התקפות קינטיות. בהיבט ההגנתי מדובר בסיכון נוסף לתפקוד המשק. תרחישי קיצון של התקפות סייבר על כלכלות של מדינות אמנם טרם התממשו, אולם למרות זאת יש להתאים כבר כיום את קצב בניית ההגנה על הסייבר המדינתי לקצב התבססותו המואצת של המשק במרחב הסייבר.

מילות מפתח: לוחמה כלכלית רחבה, כלכלה, לוחמה, סייבר, ישראל, איראן

הקדמה

מטרתו של מאמר זה היא להציג את "הלוחמה הכלכלית הרחבה" ולפרט את יישומה במרחב הסייבר. המאמר מחולק לשניים. בחלקו הראשון מוצגת "לוחמה כלכלית רחבה" כשדה משותף לכל פעולות הלוחמה שכלכלת האויב היא היעד שלהן. שדה זה מקיף לוחמה כלכלית מקובלת (כגון סנקציות), לוחמה קינטית ולוחמת סייבר נגד כלכלת האויב, והוא נוגע גם לממד ההגנתי של תחום זה. בחלקו השני מתמקד המאמר בלוחמת סייבר בתור אמצעי במסגרת "לוחמה כלכלית רחבה", תוך הבחנה בין לוחמה "רכה" ללוחמה "קשה". במאמר מובאות דוגמאות לסוגים שונים של כלי לוחמה זה.

ד"ר שמואל אבן הוא חוקר בכיר במכון למחקרי ביטחון לאומי.

רקע

אסטרטגיות לחימה בעלות מאפיינים כלכליים מוכרות עוד מהעת העתיקה. אז היה המצור אחד מכלי המלחמה הנפוצים, והשלל היה חלק מאספקה הכרחית לצבאות המתקדמים ומהתמורה למנצחים. מאז עבר הנושא התאמות, שנבעו מהשינויים במציאות הכלכלית, המדינית והצבאית בעולם. לפי אנציקלופדיה בריטניקה, "לוחמה כלכלית הינה שימוש, או האיום בשימוש, באמצעים כלכליים נגד מדינה, כדי להחליש את כלכלתה, ובכך לפגוע בכוחה המדיני והצבאי".[1] לפי מילון אוקספורד, מדובר ב"אסטרטגיה כלכלית, המבוססת על שימוש באמצעים כגון מצור, או איום בשימוש באמצעים כאלה, שמטרתה הישירה היא להחליש את הכלכלה של מדינה אחרת".[2]

הנטייה המקובלת, לפחות בעשורים האחרונים, היא לראות את הלוחמה הכלכלית ("לוחמה כלכלית מקובלת") כלוחמה המוגבלת לפעולות שאינן מבקשות להפעיל אש נגד משק האויב. כלומר, תקיפה של משק אויב בנשק קינטי כדי לפגוע בכושר הייצור שלו אינה נמנית עם ארגז הכלים של הלוחמה הכלכלית המקובלת. ברם, מצור, שהוא אמצעי צבאי שעלול להוביל לשימוש בנשק קינטי, נכלל בארגז הכלים של הלוחמה הכלכלית המקובלת. מכאן עולה ששימוש בנשק קינטי במסגרת לוחמה כלכלית מקובלת אינו חד־משמעי. הדבר מעורר שאלות גם לגבי סיווגן של התקפות סייבר רבות־עוצמה נגד יעדי המשק של האויב, שהתוצאות הצפויות מהן אינן נופלות בהכרח מעוצמתן של התקפות קינטיות. מדובר, למשל, בהתקפות סייבר רבות־עוצמה על תחנות כוח, מפעלי תעשייה ומערכות תחבורה, שלפגיעה בהם עשוי להיות אפקט קינטי (לרבות פגיעה בנפש והרס). באנלוגיה לתקיפות קינטיות, גם לתקיפות סייבר מסוג זה אין, אפוא, מקום בהגדרות המקובלות של לוחמה כלכלית.

לאור האמור לעיל, נשתמש במושג "לוחמה כלכלית רחבה" כמסגרת לכל סוגי הפעולות שמטרתן היא פגיעה, או איום בפגיעה, במשק האויב/היריב במטרה להחלישו, וזאת כדי להשיג יעדים אסטרטגיים של מפעיל הלוחמה. הבחנה בין "לוחמה כלכלית רחבה" ללוחמה כלכלית מקובלת מוצגת בלוח הבא. יצוין כי ל"לוחמה כלכלית רחבה" יש גם צד הגנתי.

---

1 George Shambaugh, "Economic Warfare", *Encyclopedia Britannica*, https://www.britannica.com/topic/economic-warfare.

2 *Oxford Dictionaries*, https://en.oxforddictionaries.com/definition/economic_war.

לוח 1: "לוחמה כלכלית רחבה" לעומת לוחמה כלכלית מקובלת

קטגוריה		פעולות אופייניות
לוחמה כלכלית (לפי הגדרה מקובלת)		סנקציות כלכליות למיניהן – הקפאת נכסים בחו"ל, איסורים בתחומי סחר והשקעות, תנאי סחר מפלים לרעה (לא משיקולים כלכליים גרידא), חרם בתחומי כלכלה שונים (Boycott), אמברגו (Embargo) ומצור (Blockade) למניעת סחר של האויב.[3]
"לוחמה כלכלית רחבה"	**לוחמה "רכה"**	סנקציות כלכליות למיניהן – הקפאת נכסים בחו"ל, חרם, איסור על סחר ואמברגו (שאינו כולל פגיעה קינטית בכלי תובלה של האויב). הרעת תנאים ביחסים הכלכליים עם היריב, למשל בתחומי הסחר וההשקעות, וזאת משיקולים אסטרטגיים־מדיניים ולא משיקולים כלכליים גרידא. לוחמת מידע ולוחמת סייבר "רכה". שימוש בכלים לא לגיטימיים לשם השגת יתרון אסטרטגי, כגון גניבת קניין רוחני בהיקף נרחב.
	לוחמה "קשה"	סגר/מצור בכוח צבאי למניעת סחר של האויב, שעלול להיות כרוך בעימות באש. התקפות קינטיות על יעדים במשק האויב התקפות סייבר רבות־עוצמה על תשתיות ומפעלים.

"לוחמה כלכלית רחבה": הגדרה, מאפיינים ומשרות

"לוחמה כלכלית רחבה" ניתנת להגדרה כמכלול פעולות לשם פגיעה, או איום בפגיעה, במשק האויב/יריב[4] במטרה להפעיל עליו לחצים או להחלישו, וזאת כדי להשיג את יעדיו האסטרטגיים של מפעיל הלוחמה.[5] בתוך מכלול זה נמצאות גם פעולות שנועדו להגן מפני מהלכים התקפיים מסוג זה מצד האויב. במילים אחרות, "לוחמה כלכלית רחבה" היא שדה משותף לכל פעולות הלוחמה שכלכלת האויב היא היעד שלהן, כגון: סנקציות, לוחמת מידע, חרם, אמברגו, סגר צבאי, לוחמה

3 *Encyclopedia Britannica.*

4 למשל, נשיא ארצות הברית, דונלד טראמפ, הגדיר את נשיא רוסיה, ולדימיר פוטין, כיריב ולא כאויב, לאחר שארצות הברית הטילה סנקציות על ארצו: "טראמפ טוען לניצחון בנאט"ו: אנגלה, תעשי משהו", *Ynet*, 12 ביולי 2018, https://www.ynet.co.il/articles/0,7340,L-5308872,00.html

5 תכלית הפעולה היא לרוב מדינית־צבאית, כגון לחץ אסטרטגי על האויב כדי שישנה את מדיניותו, או לחץ שנועד להחליש את שלטונו מבית ואת כוחו הצבאי. עם זאת, ייתכנו מצבים שבהם ללוחמה ישנה גם תכלית כלכלית־אסטרטגית, למשל, כאשר מדובר במאבק בין מדינות על נכסים כלכליים, כמו מחלוקת על מים כלכליים שבתחומם נמצאים שדות גז, או כאשר מדינה הנתונה תחת סנקציות פועלת לחלץ כספים (באמצעות התקפות סייבר). ייתכנו גם מצבים שבהם מאבקים בזירה הכלכלית (כמו מלחמות סחר) יסלימו ויתדרדרו למאבקים בעלי אופי מדיני־ביטחוני.

קינטית ולוחמת סייבר נגד משק האויב; וכן פעולות הגנתיות נגד מהלכים כאלה, למשל יכולות תגובה, היערכות מוקדמת לסנקציות, הגנה פסיבית ואקטיבית, הגנת סייבר על המשק ועוד.

לפי ההגדרה דלעיל, "לוחמה כלכלית רחבה" אינה מוגבלת לכלי הלוחמה הכלכלית המקובלת, אלא מוסיפה עליהם תקיפות קינטיות ותקיפות סייבר רבות־עוצמה נגד יעדים במשק האויב. לדוגמה, פעולות נגד מערכת החשמל של האויב עשויות לכלול: הפסקת מכירת חשמל כסנקציה מדינית; סנקציות על ייבוא חלקי חילוף לתחנות כוח; התקפת סייבר או התקפה קינטית שתביא להפסקת חשמל זמנית; התקפת סייבר רבת־עוצמה או התקפה קינטית, שתגרום לנזק בלתי הפיך לטורבינות של תחנות כוח.

"לוחמה כלכלית רחבה" עשויה לבוא בשילוב מלא או חלקי עם אמצעים אחרים, וזאת בהתאם למטרות, לאמצעים ולאסטרטגיה עליהם יוחלט. היא עשויה להיות חלק מלוחמה "רכה", כמו שילוב של סנקציות כלכליות עם התקפות סייבר על המשק במטרה להפעיל לחץ אסטרטגי כבד על האויב ללא שימוש באש. היא גם עשויה להיות חלק מלוחמה "קשה", שתכלול התקפות קינטיות והתקפות סייבר רבות־עוצמה נגד יעדים במשק האויב.

מטרותיה של "לוחמה כלכלית רחבה" הן:

- להפעיל על אויב/יריב לחצים כלכליים אסטרטגיים כדי שישנה את התנהגותו בכיוון הרצוי למפעילי הלוחמה.
- להקשות על אספקת משאבים להתעצמותו הצבאית של האויב במטרה להחליש את כוחו ("בניין כוח"); לפגוע במשאבים, בתשתיות ובנכסים כלכליים של האויב כדי לפגוע בפעילותו הצבאית ("הפעלת כוח").
- לערער את מעמדו ויציבותו של שלטון האויב, להפעיל עליו לחצים ולהביא לשינוי בסדר העדיפויות שלו ובמדיניותו (למשל, בעניין פרויקט הגרעין באיראן), לחזק את האופוזיציה נגדו ואולי אף להביא לנפילתו.
- להרתיע מפני מלחמה או לקצר את אורכה, ואף לגבות מחיר מלחמה מהאויב ולהאריך את תקופת השיקום שלו אחריה, וזאת כדי לדחות את מועד המלחמה הבאה.
- להשתמש במשאבי האויב כנגדו, או כפיצוי מצידו על פעילותו (למשל, חילוט כספי טרור לצורך מתן פיצוי לנפגעי טרור).

האמצעים והכלים של "לוחמה כלכלית רחבה"

"לוחמה כלכלית רחבה" תוצג להלן בחלוקה לשתי קטגוריות: לוחמה "רכה" – כזו שאינה עושה שימוש ישיר בכוח קינטי או בכוח ההרס של הסייבר; לוחמה

"קשה" – כזו הכרוכה בהפעלת כוח מסוגים שונים, החורגים בעוצמתם מתחום הלוחמה "הרכה".

כלי לוחמה "רכה"

מדובר בלוחמה כלכלית מצד מדינות או קבוצת מדינות, ואף ארגונים, שנועדה להפעיל לחץ כלכלי ופוליטי משמעותי על יריב/אויב, במטרה להביאו לשנות את מדיניותו ואף להחלישו, וכל זאת ללא הפעלת כוח צבאי.

פעולות עונשין

פעולות עונשין כוללות סנקציות, אמברגו וחרם על משק האויב/היריב, כמו צמצום יחסים כלכליים או השעייתם (סחר, בנקאות, תיירות, השקעות, הסכמים כלכליים למיניהם), לרבות הטלת מכסים מפלים מסיבות מדיניות; הפעלת לחצים על חברות ומדינות אחרות להפסיק את יחסיהן הכלכליים עם מדינת האויב/היריב; הרחקת מדינה סוררת ממנגנוני המשק העולמי; הקפאת כספים ונכסים של אותה מדינה בחו"ל. דוגמאות לפעולות עונשין הן הטלת הסנקציות המקיפות על איראן (לרבות הטלת חרם על ייצוא הנפט האיראני)[6] ועל צפון קוריאה[7] בשל הפרויקטים הגרעיניים שלהן; הטלת סנקציות אמריקאיות על רוסיה בגין מעורבותה בבחירות בארצות הברית באמצעות הסייבר;[8] הקפאת נכסים של עיראק בחו"ל לאחר פלישתה לכווית בשנת 1990; אמברגו הנפט של מדינות ערב על המערב ב־1974, שנועד להפעיל לחץ על הכלכלה המערבית באמצעות יצירת מחסור בנפט והאמרת מחירים; החרם של ארגון BDS על ישראל.

מעבר להשפעה הישירה של צעדי הענישה על המשק, יש להם השלכות בתחום התודעה, בכך שהם עשויים ליצור אווירה של חנק כלכלי וחוסר מוצא אצל הצד הנפגע. עם זאת, ישנן מחלוקות בין חוקרים לגבי האפקטיביות של מכשיר הסנקציות, כך שמוטב לבחון כל מקרה לגופו.[9]

---

6 כיום מוטלות הסנקציות על ידי ארצות הברית, שפרשה מהסכם הגרעין עם איראן: טל שניידר, "כל מה שצריך לדעת על הסנקציות הכלכליות שיוטלו על איראן", **גלובס**, 8 במאי 2018, https://www.globes.co.il/news/article.aspx?did=1001235164.

7 "האו"ם אישר פה אחד סנקציות חדשות נגד פיונגיאנג", **הארץ**, 12 בספטמבר 2017, https://www.haaretz.co.il/news/world/america/1.4437072.

8 רן דגוני, "בגלל התערבות בבחירות: ארה"ב מטילה סנקציות על רוסיה", **גלובס**, 15 במארס 2018, https://www.globes.co.il/news/article.aspx?did=1001228035; Missy Ryan, Ellen Nakashima and Karen DeYoung, "Obama Administration Announces Measures to Punish Russia for 2016 Election Interference", *The Washington Post*, December 29, 2016.

9 רקע תיאורטי בנושא הסנקציות ראו: ניצן פלדמן, **בצילה של מתקפת דה־לגיטימציה: רגישותה של כלכלת ישראל לסנקציות**, מזכר 154, תל אביב: המכון למחקרי ביטחון לאומי, 2016, פרק 1.

פעולות אחרות שנועדו לפגוע בכלכלת היריב באמצעים "רכים"

מדובר, בין השאר, בהתקפות סייבר לשיבוש אתרים חיוניים של הממשל והמשק של האויב/היריב; בלוחמת מידע לערעור החוסן הכלכלי של המשק שלו (למשל, הפצת מידע מטריד בעניין חולשת ערך המטבע, חולשת המערכת הבנקאית, בריחת הון, מחסור בסחורות) ובהתערבות במערכת המוניטרית של האויב/היריב (למשל, זיוף שטרות של לירות שטרלינג על ידי הנאצים במלחמת העולם השנייה); ריגול טכנולוגי ותעשייתי בין מדינות, שנועד לגניבת קניין רוחני בהיקף נרחב במטרה לשנות את המאזן האסטרטגי הכלכלי בין אותן מדינות (אף שאיסוף מידע אינו נחשב לפעולה מלחמתית). בקטגוריה של "לוחמה כלכלית רחבה" ניתן לכלול שימוש בעוצמות כלכליות להחלשת היריב לתכלית מדינית וצבאית, לרבות הטלת מכסים מפלים מסיבות מדיניות.

עניינים נוספים

פעולות רבות מתנהלות במרחב הכלכלי הגלובלי, אם במסגרת הסכמים בין מדינות ואם מחוצה להם, ואף שלעיתים צד אחד יוצא מהן נשכר וצד אחר מפסיד, אין לייחס להן משמעות של לוחמה כלכלית. הדבר נובע מההבחנה, לפיה "לוחמה כלכלית רחבה" מיועדת בעיקרה להשגת תכלית מדינית וצבאית, גם במחיר של עלויות כלכליות למפעיל הלוחמה.

פירוש הדבר הוא ש"לוחמה כלכלית רחבה" אינה אופטימלית מבחינה כלכלית גם בעיני המתכנן. זאת, לעומת מאבקים כלכליים, לרבות מלחמות סחר,[10] שבהן מצפה המתכנן להשיג יתרון כלכלי מול שותפות הסחר שלו, שחלקן הן בעלות בריתו, באמצעים המקובלים במשק העולמי. דוגמה לכך הם מכסי המגן על אלומיניום ופלדה שהטיל הממשל האמריקאי על חברות האיחוד האירופאי, קנדה ומקסיקו.

להשלמת התמונה יש להזכיר את מנופי ההשפעה הכלכליים החיוביים. זהו הצד הנגדי של "לוחמה כלכלית רחבה", אם כי מטרתם של מנופים אלה זהה לאלה של המנופים השליליים – להניע מדינות וארגונים לפעול בכיוון הרצוי למפעיל. מדובר בשימוש בתמריצים כלכליים כדי לקדם יעדים צבאיים ומדיניים, ובהם סיוע במענקים ובהלוואות נוחות, הסכמים כלכליים, תנאי סחר מועדפים, מחיקה ופריסה של חובות, העברת טכנולוגיות ועוד. שני הצדדים עשויים לצאת נשכרים משימוש במנופי השפעה כלכליים: הצד הנותן נהנה מרווח מדיני, ואילו הצד המקבל זוכה

10 המושג "מלחמת סחר" שאול משדה המלחמה, אך אינו שייך לשדה זה ואינו נמנה עם לוחמה כלכלית. מלחמת סחר היא סכסוך כלכלי המאופיין במצב שבו מדינות מעלות או יוצרות מכסי מגן, או מחסומי סחר אחרים, זו מול זו. עם זאת, מלחמות סחר עלולות להידרדר למצב של לוחמה כלכלית.

ברווח כלכלי. לדוגמה, סיוע החוץ האמריקאי לסוגיו מחזק את הלגיטימציה של ארצות הברית לבוא בדרישות אל המדינות מקבלות הסיוע.

מנופי השפעה כלכליים אלה אינם כלי לוחמה על פי הגדרתם. עם זאת, יש הרואים בהפסקת הטבות כלכליות, באיום להפסיקן או בהתניית הסיוע בהשגת תכלית מדינית של נותן הסיוע מעשה בתחום הלוחמה הכלכלית הרחבה, או על גבול הלוחמה הזאת. כך, למשל, ארצות הברית קיצצה את הסיוע לפלסטינים בשל אי־שיתוף פעולה מדיני עימה; ערב הסעודית יוצרת קשר בין הסיוע הכלכלי שהיא מעניקה לירדן ובין מילוי דרישתה לקדם את יעדיה המדיניים והביטחוניים, ובראשם בלימת ההשפעה האיראנית במזרח התיכון;[11] במלחמת המפרץ הראשונה, בשנת 1991, קיבלה מצרים מבעלות הברית שלחמו נגד עיראק סיוע במזומן בהיקף של מיליארדי דולרים, וחובותיה קוצצו ב־25 מיליארד דולר, בתמורה להשתתפותה לצידן במלחמה נגד סדאם חוסיין. גם סוריה זכתה לסיוע כלכלי בגין השתתפותה במלחמה זו.

כלי לוחמה "קשה"

סגר צבאי (blockade)

משמעותו של סגר כזה היא הפעלת כוח צבאי למניעה או להגבלת אספקה של סחורות ושירותים אל מדינת האויב וממנה לעולם, במטרה להפעיל עליה לחצים כלכליים, בעיקר לשם השגת מטרות מדיניות וצבאיות. פעילות זו עשויה להיות כרוכה לפעמים גם בהפעלת נשק קינטי.

ניתן להבחין בין סגר על מדינה סוררת, שנסמך על הסכמה וכללים בין־לאומיים, כגון סגר של הקואליציה הבין־לאומית על עיראק לאחר פלישתה לכווית בשנת 1990, ובין סגר שמנסות מדינות שונות להטיל על נתיבי הסחר של מדינות אחרות כחלק ממלחמה ביניהן. דוגמאות לסגר מהסוג השני ניתן לראות בסגר שהטילה איראן על נתיב ייצוא הנפט של עיראק במפרץ הפרסי במהלך מלחמת עיראק־איראן בשנות השמונים של המאה העשרים, באמצעות תקיפות על מכליות נפט; בחסימת נתיב השיט של ישראל במצרי טיראן על ידי מצרים במאי 1967 (שהייתה אחד הגורמים העיקריים למלחמת ששת הימים); ובשימוש שעשתה גרמניה בצוללות במלחמות העולם הראשונה והשנייה כדי להטביע אוניות סוחר של אויביה.

תקיפה של יעדי תשתית וכלכלה

מדובר בתקיפה, או באיום בתקיפה, באמצעות נשק קינטי ו/או התקפות סייבר רבות־עוצמה למטרות הרתעה של האויב או החלשתו, קיצור משך המלחמה,

11 דן ארקין, "סיוע כלכלי בתנאים של סעודיה", *IsraelDefense*, 13 ביוני 2018, http://www.israeldefense.co.il/he/node/34572.

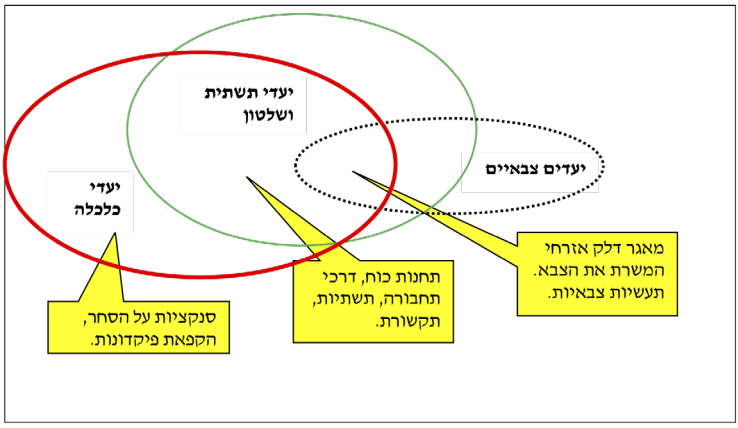
הרתעה מפני הסלמה והעלאת מחיר המלחמה. דוגמאות לכך הן: ההרתעה של ישראל כלפי חיזבאללה ולבנון באמצעות איום לפגוע בתשתיות בלבנון; פגיעה של ארצות הברית במתקני נפט עיראקיים במלחמת המפרץ הראשונה; התקפות חיל האוויר הישראלי על מטרות אסטרטגיות בעומק מצרים וסוריה במלחמת יום הכיפורים (מתקני נפט, מוסדות שלטון, בתי זיקוק ותחנות ממסר).

טרור כלכלי

טרור כלכלי הוא פגיעה של ארגוני טרור, או איומים שלהם לפגוע במטרות במשק המדינה או בתחושת הביטחון הכלכלי שלה. דוגמאות לכך הן איומיו של ארגון חיזבאללה לפגוע בתחנות כוח בישראל;[12] טרור העפיפונים מרצועת עזה בקיץ 2018, שהבעיר יבולים חקלאיים בנגב; גניבות והשחתות של ציוד חקלאי בישראל ממניעים לאומניים; פיגועי טרור במצרים שנועדו לפגוע בתיירות למדינה.[13]

ניתן להפעיל "לוחמה כלכלית רחבה" גם נגד ארגוני טרור, למשל איום על המשק של האוכלוסייה התומכת בארגונים אלה (במקרה של ארגונים סמי־מדינתיים), או פגיעה במקורות המימון ובמערכות הפיננסיות שלהם (כפי שנעשה במקרה של דאע"ש).

לוח 2: יעדי תקיפה של "לוחמה כלכלית רחבה" (דוגמאות)



12 רועי קייס, "נסראללה: אין צורך בנשק כימי, נפגע בתחנות כוח", *Ynet*, 3 בספטמבר 2012, https://www.ynet.co.il/articles/0,7340,L-4276742,00.html.

13 "מיעדי תיירות ליעדי טרור: איום ממשי למצרים", **שורטי**, המכון למחקרי ביטחון לאומי, 14 בינואר 2016, http://www.inss.org.il/he/blogs/?pauthor=55226.

הגנה נגד "לוחמה כלכלית רחבה"

ל"לוחמה כלכלית רחבה" יש גם צד הגנתי. אמצעי הגנה מדינתיים נגד לוחמה כזו כוללים:

- הרתעה – הכנת יכולת תגובה אמינה ואיום בתגובת נגד.
- הגנה פיזית אקטיבית, דוגמת "כיפת ברזל", ופסיבית, לרבות מיגון מתקנים כלכליים.
- פיזור של תשתיות ומתקנים כלכליים אסטרטגיים ברחבי המדינה והכנה של יכולות גיבוי ומערכות תשתית חלופיות, למשל בתחומי תקשורת ואנרגיה.
- הגנת סייבר על המשק (פירוט בהמשך).
- אחזקת מלאים של דלק, מזון, חלפים ועתודות מטבע חוץ בכמות גדולה מהנדרש לצרכים שוטפים.
- שימור ופיתוח יכולות ייצור עצמי של מוצרים קריטיים, כמו אנרגיה (למשל, פיתוח שדות הגז הטבעי בישראל), מזון, מלט ועוד.
- גיוון של מקורות הייבוא, ובעיקר של מוצרים חיוניים, וכן של יעדי הייצוא. מתן עדיפות לחוזים ארוכי טווח עם גורמים אמינים, שאינם מושפעים מהסכסוך הפוליטי באזור.
- הכנת תוכנית להמשכיות עיסקית במצבי חירום, לרבות בניית יכולות להתאוששות ולניהול אפקטיבי של המשק בשעת חירום, וכן תרגול והדרכה שלו לקראת מצבי חירום.

יתרונות ומגבלות השימוש ב"לוחמה כלכלית רחבה"

לשימוש ב"לוחמה כלכלית רחבה" יש, כמובן, הן יתרונות והן חסרונות. בין היתרונות ניתן למנות:

- יכולת להפעיל לוחמה כלכלית בספקטרום גדול של אמצעים ועוצמות, כמו חרם, סנקציות, סגר, התקפות סייבר והתקפות קינטיות, ובכך לנהל ולבקר את המערכה עד להשגת יעדיה.
- "לוחמה כלכלית רחבה" ניתנת להפעלה מרחוק ובלא סיכונים רבים למפעיל, למעט במקרים של תקיפות קינטיות מסוימות.
- "לוחמה כלכלית רחבה" בעת מלחמה יוצרת לחצים כלכליים על האויב להפסקת הלחימה, או משמשת לגביית מחיר כלכלי מהאויב שמטרתו היא להרחיק את המלחמה הבאה, וכל זאת תוך מזעור האבידות בנפש לאוכלוסייתו.
- ניתן לעשות שימוש ב"לוחמה כלכלית רחבה" גם במערכה שבין המלחמות (מב"ם).
- "לוחמה כלכלית רחבה", או איום להפעילה, עשויים להיות גם גורם מרתיע.

מגבלות וסיכונים הכרוכים בשימוש ב"לוחמה כלכלית רחבה" כוללים:

- מיסקלקולציה – שימוש ב"לוחמה כלכלית רחבה" עלול לגרור או להאיץ תהליכים שליליים, ואף להוביל למלחמה. למשל, בתחילת יוני 2018 הודיעה איראן על

האצה בפעילותה להעשרת אורניום, בתגובה לחידוש הסנקציות עליה מצד ארצות הברית.[14] בראייה היסטורית, הסנקציות הכלכליות שהטילו ארצות הברית ובריטניה על יפן בגין פלישתה לסין בשנת 1937 הביאו לשרשרת תוצאות לא רצויות: ברית בין יפן לגרמניה הנאצית ולאיטליה, ובהמשך – למתקפה היפנית על פרל הרבור בדצמבר 1941, שבתגובה לה הכריזה ארצות הברית מלחמה על יפן, ואילו בעלות בריתה של יפן (בהן גרמניה הנאצית) הכריזו מלחמה על ארצות הברית. השתלשלות זו הביאה, בסופו של דבר, לכניסתה של ארצות הברית למלחמת העולם השנייה.

- האוכלוסייה במדינת האויב עלולה לחוש איבה כלפי מפעיל הלוחמה, כך שהלחץ הכלכלי עשוי להביא דווקא לחיזוק התמיכה בשלטון המותקף.
- לחץ כלכלי חמור יכול ליצור פגיעה רחבה באוכלוסייה אזרחית חלשה, דבר שעלול להוביל למשבר הומניטרי ולגרור ביקורת בין־לאומית נוקבת.
- תגובת נגד – היריב עלול לפתח יכולות ולהגיב באותם כלים או בכלים אחרים. כתוצאה מכך, עלולה להתפתח מלחמה עתירת נזקים גם לתוקף.
- תיתכן פגיעה בנכסים או באינטרסים כלכליים של מדינות ידידותיות או ניטרליות לתוקף. דוגמה לכך היא פגיעה בנכס כלכלי של מדינת אויב המבוטח במדינה ידידותית, או תקיפת מחשב שזלגה ליעדים לא קרואים. מקרים כאלה עלולים להביא לתגובות נגד מפעיל הלוחמה.

"לוחמה כלכלית רחבה" בעידן הסייבר

להלן יתואר המרחב המשותף הקיים בין "לוחמה כלכלית רחבה" ובין הסייבר.[15] מהפכת המידע והטכנולוגיה העוברת על המשק והחברה נמצאת כיום בעיצומה: ענן מחשוב, ביג דאטה, מציאות רבודה, בינה מלאכותית, כלים אוטונומיים ו"האינטרנט של הדברים" הם תחומים המתפתחים ומאיצים את יחסי הגומלין בין השדה הכלכלי והחברתי ובין מרחב הסייבר, שהופך למשמעותי יותר ויותר בחייהם של פרטים, ארגונים, מדינות והמשק העולמי כולו.

כבר כיום קיימים מגזרים כלכליים, כמו מגזרי הבנקאות והפיננסים, שפעילותם העיקרית מתקיימת בעולם הווירטואלי של מרחב הסייבר, תוך שהם מצמצמים את הפעילות מחוץ למרחב זה. אמנם, השדה הכלכלי הוא ממשי, וכולל צרכנים, כוח עבודה, קרקע, חומרי גלם ואת התוצרים של תעשיות המתכת, הבנייה, המזון וכדומה, אלא שלכל אלה יש ייצוג דיגיטלי בסייבר, המתעד אותם וקושר ביניהם,

14 דניאל סלאמה וליעד אוסמו, "איראן: בחודש הבא יושלם מתקן לבניית צנטריפוגות מתקדמות", *Ynet*, 7 ביולי 2018, https://www.ynet.co.il/articles/0,7340,L-5280313,00.html.

15 ההרחבה המושגית מ"לוחמה כלכלית" ל"לוחמה כלכלית רחבה" מאפשרת לדון גם בהתקפות סייבר רבות־עוצמה, שקשה להכליל אותן בהגדרה המקובלת של "לוחמה כלכלית".

כך שלפגיעה בסייבר יש אפקט משמעותי גם מחוצה לו. תופעה חשובה נוספת היא הגלובליזציה של הסחר העולמי ושל שוקי ההון העולמיים, הנשענים על האינטרנט ועל מערכות סייבר המקושרות זו עם זו.

לוחמת סייבר היא לוחמה שבה משתמשים במרחב הסייבר כדי לפגוע ביעדים שונים של האויב, בעיקר לתכלית מדינית וצבאית. לוחמת סייבר יכולה להתלוות ללוחמה קונבנציונלית כממד לחימה נוסף, או להיות זירה בפני עצמה. היא יכולה להתממש בין המלחמות או תוך כדי מלחמה ולשאת אופי התקפי והגנתי כאחד. "לוחמה כלכלית רחבה" בסייבר משתמשת במרחב הסייבר הן כדי לתקוף יעדים כלכליים של האויב והן כדי להגן על נכסים כלכליים ותשתיות סייבר של המדינה, או על כאלה המקושרים אל מרחב הסייבר שלה (למשל, מפעלים, תחנות כוח ושדות תעופה), מפני מתקפות סייבר של האויב.

התקפת סייבר על הכלכלה

התקפת סייבר כוללת תקיפה **של** מערכות סייבר שמהוות תשתיות דיגיטליות (למשל, בסיסי נתונים ותוכנות של ארגונים), או תקיפה **דרך** הסייבר (מבלי לפגוע בו) על מערכות משובצות מחשב שפועלות מחוץ למרחב הסייבר, כמו תחנות כוח, מגדלי פיקוח, מערכות בקרת רמזורים וכדומה. המאפיין ההתקפי הייחודי ללוחמת סייבר הוא היכולת לבצע פעילות מרחוק באמצעות הסייבר ומבלי להיחשף ישירות.[16] כלומר, התוקף אינו מסתכן ויכול לנקוט מדיניות של עמימות (לרבות אי־נטילת אחריות). לעיתים, התקיפה אינה נראית על פני השטח ונדרש זמן לזהותה (למשל, בעת שיבוש בסיסי נתונים).[17]

התקפות סייבר נגד כלכלת האויב ניתנות לביצוע בדרכים שונות ויכולות להיעשות בשילוב עם סנקציות או עם התקפות קינטיות (באש), בעצימות נמוכה או גבוהה. בעת מלחמה יש לסייבר יתרון בתקיפת מוסדות פיננסיים על פני תקיפתם בדרך קינטית. לעיתים ניתן לעשות שימוש בהתקפות סייבר כתחליף להפעלת נשק קינטי.

התקפות סייבר עשויות להיות אמצעי נוסף של ארגוני טרור לשיבוש אורח החיים במדינות יעד שלהם, במיוחד נוכח העובדה שניתן להוציא אותן לפועל מכל נקודה בעולם, ולא רק באמצעות מגע קרוב. התקפות סייבר רבות־עוצמה מצד ארגוני טרור אינן נפוצות בשלב זה, אם כי יש לצפות להן כאשר לארגוני הטרור יהיו יכולות לבצע פיגועי ראווה בסייבר, כלומר התקפות סייבר עוצמתיות שתוצאותיהן ייראו לעין. התקפות בסייבר משמשות או עשויות לשמש את ארגוני

16 מה שקרוי Non-face to face business relationships or transactions

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

הטרור גם להשגת כספים למימון פעילותם. בנוסף, הסייבר משמש ארגוני טרור, כמו חיזבאללה וחמאס, לביצוע פעולות איסוף[18] ולוחמה פסיכולוגית.

מדינות שביקשו להשיג יכולת התקפית הקימו ארגוני סייבר צבאיים. כך, למשל, ביוני 2009 הוקם פיקוד הסייבר האמריקאי, ובמאי 2018 הוא קיבל מעמד של פיקוד לוחם.[19] עם הקמתו פורסם שהפעולה ההתקפית בסייבר מול האויב או היריב נועדה ליצור חמישה אפקטים (חמישה D): למנוע את יכולת הפעולה של האויב/היריב בסייבר (Deny); להחליש אותו ולפגוע במעמדו (Degrade); לשבש את פעילות המערכות שלו (Disrupt); לבצע הונאה (Deceive); להרוס (Destroy) את יכולותיו. חמשת האפקטים הללו רלוונטיים גם ל"לוחמה כלכלית רחבה" בסייבר.

הסייבר הינו פלטפורמה שבמסגרתה נעשות פעולות כלכליות רבות, ובאמצעותה ניתן להעצים לוחמה כלכלית, כמו הגברת האכיפה של סנקציות כלכליות. הסייבר גם מאפשר שליטה ובקרה במרחב הכלכלי, כגון: מניעת גישה של מדינת אויב למערכת סחר וכספים; חסימת תנועות כספים; מניעת העברת הוראות סחר; ביצוע פעילות איסוף מידע וחשיפת חברות המפרות סנקציות; הקפאת חשבונות בנקים ופיקוח עליהם; בקרה על תנועות מט"ח חוצות גבולות באמצעות דיווחים של מוסדות פיננסיים מחוץ למדינת האויב; בקרה על הסחר באמצעות אימות נתונים עם ספקים מחוץ למדינת האויב.

כלכלה, מעצם טבעה, מפגינה רגישות גבוהה למידע, וחלק ניכר מהמערכות הכלכליות מבוסס על אמון הציבור במשק ומוסדותיו, כמו הבנקים, המטבע של המדינה והמערכות הממונות על שוקי ההון. "לוחמה כלכלית רחבה" בסייבר עשויה לשמש לערעור האמון במערכות המשק, בין היתר באמצעות הפצת מידע רלוונטי. עם זאת, אין זה פשוט להגיע להישג משמעותי במלחמת מידע כזו, מאחר והסייבר מאפשר גם לנתקף להגיב במהירות ולהזים שמועות נגדו.

תקיפת יעדים של מוסדות שלטון בסייבר, למשל באמצעות חסימת הגישה אליהם מצד הקהל, עלולה לפגוע במשילות, במשק ובהכנסות המדינה. זאת, מאחר והסייבר מהווה אמצעי לקשר בין העסקים והאזרחים ובין השלטון, קשר שאינו אינפורמטיבי בלבד, אלא כזה שהופך, יותר ויותר, לקשר מעשי, כמו השימוש ההולך וגובר באתרים של הממסד השלטוני לתשלומי מיסים ואגרות.

פריצה לסייבר ואיסוף מודיעין טכנולוגי ותעשייתי בסייבר מאפשרים לרוקן ארגונים מקניינם הרוחני. מהלכים כאלה, כאשר הם נעשים בסדרי גודל ניכרים,

---

18 טל שחף, "זירת הקרב הבאה של החמאס – הסייבר", **גלובס**, 18 ביולי 2018.

19 עמי רוחקס דומבה, "פיקוד הסייבר האמריקאי מקבל מעמד של פיקוד לוחם", *IsraelDefense*, 6 במאי 2018, http://www.israeldefense.co.il/he/node/34080.

עשויים לשנות את המאזן האסטרטגי בין חברות עיסקיות גלובליות, ואף בין מדינות. ארצות הברית טוענת, למשל, כי סין מבצעת פעילות כזאת בתחומה.[20]

ניתן לנהל התקפות בסייבר בדרגת עוצמה גבוהה, שמטרתן לשבש מסחר, ייצור ופעילות פיננסית של המדינה הנתקפת, למשל על ידי שיבוש בסיסי נתונים של מערכות סחר, מחסני לוגיסטיקה, תקציבים ועוד. פעולות אלו נמצאות על גבול הלוחמה "הרכה" ויכולות להגיע אף לדרגת לוחמה גבוהה יותר (תלוי בעוצמה ובהיקף הנזק).

ניתן לבצע התקפות בסייבר בדרגת עוצמה גבוהה יותר, במסגרת לוחמה "קשה", שתכליתן היא לפגוע בתפקודן של מערכות תשתית וכלכלה (חשמל, מים, בנקאות, תחבורה, תקשורת), עד כדי שיבוש מהותי של שגרת החיים ותפקוד המשק במדינת האויב. היכולת לפגוע מרחוק בתפקודן של מערכות כלכליות, מבלי לחצות גבול טריטוריאלי ומבלי להפעיל אש, היא יתרון ייחודי לסייבר. עם זאת, פעולות התקפיות מסוימות בסייבר יכולות להיות הרות אסון למדינה הנתקפת, לרבות בחיי אדם ובנזקים לתשתיות חיוניות. במקרה זה, מעמדן דומה לזה של התקפה קינטית, ותגובת המדינה הנתקפת עלולה להיות בהתאם.

בין המדינות המשתמשות בסייבר לתקיפת יעדים כלכליים ניתן לציין את איראן. באוגוסט 2012 נערכה התקפת סייבר באמצעות הווירוס "שאמון", המיוחסת לאיראן, נגד חברת הנפט הלאומית הסעודית ערמקו. הווירוס הדביק כ־30,000 מחשבים ופגע בתפקודה של החברה.[21] בשנת 2013 דווח כי האקרים איראנים ביצעו סדרת התקפות סייבר על מטרות אמריקאיות, כמו בנקים גדולים וחברות אנרגיה הפועלות במפרץ הפרסי, אך התקפות אלו לא גרמו נזק משמעותי.[22] התקפה נוספת באמצעות הווירוס "שאמון", המיוחסת לאיראן, בוצעה בשלהי שנת 2016 על הבנק המרכזי של ערב הסעודית וגופים ממשלתיים נוספים במדינה.[23] לפי ההערכות, איראן עלולה להגיב על הסנקציות שהטיל עליה נשיא ארצות הברית טראמפ במתקפת סייבר מסיבית,[24] אלא שאז היא תסתכן בחשיפת עצמה לתגובות נגד קשות. צפון קוריאה, הנתונה גם היא תחת סנקציות, הקימה מערך

---

20 "ארה"ב מאשימה את סין בגניבת מידע עיסקי בשווי 400 מיליארד דולר", *TheMarker*, 17 בפברואר 2012, https://www.themarker.com/wallstreet/1.1644216?=.

21 עמוס הראל, "הערכות: איראן מאחורי מתקפת הסייבר על חברות נפט במפרץ הפרסי", **הארץ**, 11 בספטמבר 2012, http://www.haaretz.co.il/news/world/1.1821619.

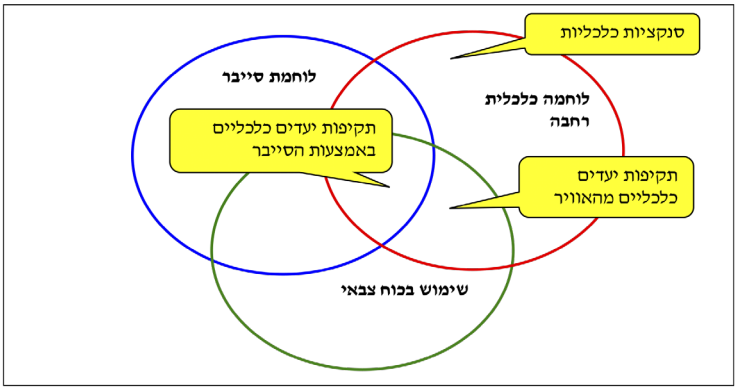
22 "דיווח: איראן מנהלת מתקפה מקוונת נגד ארה"ב", *Ynet*, 13 באוקטובר 2013, https://www.ynet.co.il/articles/0,7340,L-4291493,00.html.

23 "האקרים איראנים פרצו למחשבי הבנק המרכזי של סעודיה", *TheMarker*, 3 בדצמבר 2016, https://www.themarker.com/wallstreet/1.3140741.

24 Nicole Perlroth, "Without Nuclear Deal, U.S. Expects Resurgence in Iranian Cyberattacks", *The New York Times*, May 11, 2018, https://www.nytimes.com/2018/05/11/technology/iranian-hackers-united-states.html.

לתקיפות סייבר ומבצעת תקיפות כאלו בעיקר על דרום קוריאה ומדינות המערב.[25] הדוגמאות שהובאו לעיל מצביעות על כך שלוחמת הסייבר משמשת, בין היתר, כאמצעי תגובה של מדינות הנתונות תחת סנקציות.

לוח 3: "לוחמה כלכלית רחבה" ולוחמת הסייבר (דוגמאות)



הגנה מפני התקפות סייבר

איום הסייבר על המשק

המשק המדינתי והגלובלי תלוי במערכות מידע, בסיסי נתונים, תקשורת ואוטומטיזציה, ותלותו בסייבר הולכת וגוברת. ענפי כלכלה מסוימים, כגון תקשורת ובנקאות, מצויים כבר כיום עמוק במרחב הסייבר, ואחרים, כגון תחנות כוח, מפעלים ואמצעי תחבורה, פועלים באמצעות מערכות משובצות מחשב וסייבר.

תרחיש "יום הדין" של התקפת סייבר על המשק כולל מצב שבו בנקים ייסגרו; המסחר בבורסה ייפסק; התפקוד של תחנות כוח, מערכות מים, מפעלים ומערכות תחבורה ישובש מאוד; בשדות תעופה תיעצר תנועת המטוסים; מפעלים ומשרדים יסגרו את שעריהם; סחר החוץ ייבלם. כתוצאה מכך, אזרחים יתקשו לבצע פעולות בסיסיות, כמו משיכת כספים, קבלת שכר באמצעות הבנקים, תדלוק, רכישה במרכולים, תנועה ממקום למקום, מציאת תעסוקה ותקשורת עם מוסדות השלטון. השלטון, מצידו, יתקשה לנהל את המשק ולגבות מיסים, והפעילות במשק כולו תיעצר. למעשה, אין צורך בפגיעה כה רחבה כדי לעצור את התהליכים במשק, ודי לפגוע באחדות מהחוליות הרגישות בו. יחד עם זאת, עד היום לא נרשם אירוע

25 David E. Sanger, David D. Kirkpatrick and Nicole Perlroth, "The World Once Laughed at North Korean Cyberpower. No More", *The New York Times*, October 15, 2017, https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html.

מדינתי בסדר גודל של "יום הדין". בין הסיבות האפשריות לכך: מגבלות יכולתם של שחקני סייבר רבים, על רקע מנגנוני הגנה שהוקמו במדינות שונות (יש הבדל גדול בין פגיעת סייבר ביעד כזה או אחר לבין פגיעה מערכתית במשק); זהירות מצד מעצמות סייבר בחשיפה מוקדמת של נשקי סייבר; חשש מתגובות נגד, ואף החשש מפני הצתת מרוץ חימוש בסייבר ומלחמת סייבר גלובלית.[26]

להשלמת התמונה יש לציין שאירועי הסייבר הדרמטיים ביותר בשנים האחרונות, הנוגעים לביטחון הלאומי, היו בתחום המשילות במדינות דמוקרטיות. כך, ארצות הברית טוענת שרוסיה ביצעה מתקפת סייבר שנועדה להשפיע על תוצאות הבחירות לנשיאות בה בשנת 2016, דבר שנתפס כאיום ממשי על הדמוקרטיה האמריקאית. ניסיון להתערב בבחירות לנשיאות אירע גם בצרפת בשנת 2017, ובשיטה דומה – באמצעות הפצת מידע רגיש ברשתות חברתיות נגד המועמד, מידע שהושג, בין השאר, באמצעות פריצות למחשבים הקשורים אליו.[27] לעומת זאת, הסייבר אִפשר לנשיא טורקיה, ארדואן, לסכל ניסיון הפיכה צבאית נגדו ביולי 2016: ארדואן עלה לשידור טלוויזיה באמצעות אפליקציה סלולרית וקרא לתומכיו להפר את העוצר שהטיל הצבא ולצאת לרחובות.

קבוצה חשובה במשק, הזוכה לעדיפות מצד המדינה בהגנה בסייבר, הן "תשתיות מדינה קריטיות" (תמ"ק). קבוצה זו כוללת בישראל את תשתיות החשמל, המים, הגז הטבעי, הרכבות, רשות שדות התעופה, בתי הזיקוק, שרשרת ייצור החשמל והולכתו, משרדים ממשלתיים ובתי חולים. מדובר ב־26 תשתיות קריטיות, שאותן מנחה מערך הסייבר הלאומי באופן ישיר.[28]

המגזר הפיננסי (בנקים, חברות אשראי, מערכת הסליקה, שוק ההון, ביטוח, קרנות פנסיה) הוא אחת החוליות הרגישות במיוחד להתקפות סייבר, שכן הוא קריטי לתיווך פעולות כלכליות וחברתיות. בשונה ממגזר התשתיות הכבדות, מגזר הפיננסים חשוף לתקיפות סייבר יותר מאשר לתקיפות קינטיות. המערכת הפיננסית הינה מבוססת סייבר, רגישה לאמון הציבור וקריטית לתפקודן של מדינות.

דוגמה להתקפת סייבר על המערכת הפיננסית היא גניבה של 81 מיליון דולר מהבנק המרכזי של בנגלדש בפברואר 2016, במסגרת מתקפה שבה הצליחו האקרים (יתכן מצפון קוריאה) להעביר לפיליפינים כסף מחשבונות של הבנק המרכזי

---

26 גדי עברון ובועז דולב, "משחקי מלחמה: למה ארה"ב לא עורכת מתקפת סייבר על צפון קוריאה", *Ynet*, 19 בספטמבר 2017, https://www.ynet.co.il/articles/0,7340,L-5017828,00.html.

27 דודי סימן טוב, גבי סיבוני, גבריאל אראל, "איומים קיברנטיים על תהליכים דמוקרטיים", **סייבר, מודיעין וביטחון**, כרך 1, גיליון 3, דצמבר 2017.

28 דן ארקין, "ערוכים היטב לאיומים", *IsraelDefense*, 24 במאי 2018, http://www.israeldefense.co.il/he/node/34321.

של בנגלדש בבנק הפדרלי של ניו יורק.[29] אירוע דומה של גניבת כסף אירע בבנק וייטנאמי בתחילת 2016, שבמסגרתו נעשתה חדירה של האקרים למערכת "סוויפט", הנחשבת למערכת התשלומים הבין־בנקאית המאובטחת ביותר בעולם.[30] דוגמאות אלה מציגות יכולות שאותן ניתן להפעיל במידה גדולה יותר במסגרת "לוחמה כלכלית רחבה".

חברות אחרות במשק הרגישות למתקפות סייבר הן: חברות העוסקות בתשתיות, חברות ביטחוניות, חברות תקשורת, חברות סחר באינטרנט וארגונים העושים שימוש במידע רגיש (משרדי עורכי דין, מאגרים של קניין רוחני, של סודות מסחריים, של סודות רפואיים וכדומה). בשנים האחרונות גוברת המודעות לכך ששרשרת האספקה של ארגונים (גופים המספקים לאותם ארגונים תוצרי ביניים ושירותים) מהווה ציר כניסה למתקפות סייבר רבות עליהם. המשמעות היא שיש להגן לא רק על יעדים חיוניים במשק, אלא גם על המעטפת שלהם.

האיום עלול להגיע גם מקרב עובדי החברות, לרבות עובדים בתעשיות הביטחוניות העוסקות בסייבר. דוגמה לכך היא פרשה ביטחונית חמורה שנחשפה ביולי 2018, כאשר עובד בחברת הסייבר ההתקפי NSO נעצר בחשד שגנב נשק סייבר של החברה (תוכנת "פגאסוס") וניסה למכור אותו ברשת האפלה (Dark Web) תמורת חמישים מיליון דולר. ניסיונו של העובד סוכל לאחר ש"הקונה הפוטנציאלי" פנה לחברה. האירוע מצביע על הצורך שהמדינה תפקח על הנעשה גם בחברות העוסקות בתחום הסייבר.[31]

עיקר הנזק הכלכלי שנגרם עד היום למשק בתחום הסייבר אינו נובע מ"לוחמה כלכלית רחבה" של מדינות וארגונים פוליטיים, אלא מפשיעה, שמניעיה הם בעיקר כלכליים. עם זאת, יש להניח שכל מה שמגזר הפשיעה יודע לעשות בתחום הסייבר יודעות או יידעו לעשות גם מדינות, שיכולותיהן מאפשרות להן לעשות אף יותר מכך, אם וכאשר הן יחליטו להפעיל לוחמת סייבר מסיבית. המחשה ליכולת מדינתית עוצמתית כזו ניתנה בחשיפתן בשנת 2010 של התקפות סייבר (באמצעות תולעת "סטוקסנט"), שהרסו צנטריפוגות איראניות להעשרת אורניום.[32] התקפות אלו הבהירו לעולם שהאיום הנשקף מהתקפות סייבר כולל גם פגיעות פיזיות במפעלי

---

29 "מבצע לזרוס: כך צפון קוריאה גונבת כספים מבנקים במערב באמצעות מתקפות סייבר", *Nana10*, 5 באפריל 2017, http://media.nana10.co.il/Article/?ArticleID=1240370.

30 "מתקפת סייבר על הבנקאות הגלובלית: האקרים שוב פרצו למערכת התשלומים המאובטחת בעולם", *TheMarker*, 13 במאי 2016, https://www.themarker.com/wallstreet/1.2942637.

31 אלה לוי־וינריב, טל שחף, "הותר לפרסום: NSO ופרשת הסייבר מהחמורות בתולדות ישראל", **גלובס**, 5 ביולי 2018, https://www.globes.co.il/news/article.aspx?did=1001244618.

32 "תיק איראן נפתח: מלחמת הסייבר", **ערוץ 2**, **תוכנית עובדה**, 2 בנובמבר 2012, https://www.mako.co.il/tv-ilana_dayan/specials/Article-a996bba5fccba31006.htm.

תעשייה, בתשתיות ובתחום התחבורה, המצוידים כולם במערכות שליטה ובקרה ממוחשבות, ואינו מוגבל לפגיעות בבסיסי נתונים בתוך מרחב הסייבר בלבד.

המענה לאיום

פגיעה קשה במרחב הסייבר המדינתי עשויה להיחשב לבעיה של ביטחון לאומי. הגנת סייבר בהקשרה הכלכלי היא מכלול פעולות, בתוך מרחב הסייבר ומחוצה לו, שתכליתן להגן על המשק המדינתי, הן במרחב הסייבר והן במרחבים אחרים, מפני תקיפות העושות שימוש בסייבר. את הגנת הסייבר יש להפעיל מול מדינות, ארגונים אויבים, ארגוני פשע, אנשי זדון וגם לצורך התאוששות מתקלות.

ההבדל העיקרי בין לוחמה כלכלית של מדינות הנעשית בסייבר ובין פעולות פשיעה במרחב זה הוא בכך, שהמניע של פושעי הסייבר הוא לרוב כלכלי־פלילי (גניבת כספים, גניבת סודות מסחריים וקניין רוחני, מעילות והונאות, סחיטה, גביית כופר).[33] עם זאת, יש מקרים בהם מדינות מתייחסות לפעילות של פשיעה בהיקף נרחב בסייבר, ואף לפעילות כלכלית חריגה של גופים שפועלים למטרות רווח, כאיום הנוגע לביטחון הלאומי שלהן.[34]

להבדיל מתחומים אחרים, כמו ההגנה על הגבולות והגנה על העורף מפני טילים, שעליהם ממונה הצבא, ההגנה על נכסי המשק בסייבר, הן בישראל והן ברחבי העולם, מבוססת בעיקרה על שירותי אבטחה, תוצרים ואסטרטגיות של המגזר הפרטי[35] ועל משאביו של מגזר זה. קיימת תעשייה ענפה של חברות המפתחות, מייצרות ומשווקות מערכות הגנה בסייבר ותומכות בהן.

הגורם העיקרי להתפתחותה של תעשיית אבטחת הסייבר במשק המקומי והעולמי בעשורים האחרונים אינו הממסד, אלא הצורך של המגזר הפרטי להתגונן מפני חדירות של פורצים, שמניעיהם מגוונים: גניבת כספים, גניבת קניין רוחני וסודות מסחריים וטכנולוגיים ותקיפות סייבר ממניעים אידיאולוגיים או פסיכולוגיים (כמו אגו, ונדליזם וכדומה). תפקידם העיקרי של גורמי הביטחון הממשלתיים בהגנת

---

33 Alan Blinder and Nicole Perlroth, "Atlanta Hobbled by Major Cyberattack that Mayor Calls 'a Hostage Situation'", *The New York Times*, March 28, 2018, https://www.seattletimes.com/nation-world/atlanta-hobbled-by-major-cyberattack-that-mayor-calls-a-hostage-situation/.

34 לדוגמה, בתחילת 2010, בעיצומו של המשבר הכלכלי באירופה, סומנו ספקולנטים כ"טרוריסטים כלכליים". שר האוצר של גרמניה אמר אז שגרמניה עשויה לשקול להורות לסוכנויות הביון שלה להתחיל לנהל מעקב אחר התארגנויות של משקיעים ספקולנטים כדי להגן על האירו. בעיתון הספרדי **אל פאיס** נכתב כי השירות החשאי של ספרד פתח בחקירה של "התקפות" מצד ספקולנטים על המדינה.

35 גבי סיבוני, הדס קליין, "פיתוח יכולות ארגוניות לניהול משברי סייבר", **סייבר, מודיעין וביטחון**, כרך 2, גיליון 1, אפריל 2018, http://www.inss.org.il/he/publication/developing-organizational-capabilities-to-manage-cyber-crises/?offset=1&posts=2&type=715

המשק הוא הנחיה של גופים בולטים בעלי חשיבות לאומית ופיקוח עליהם. המדינה עוסקת בעיקר בהגנה על מוסדותיה ובהנחייה של ארגונים בקטגוריה של "תשתיות מדינה קריטיות". כלל המשק והציבור נהנים, לכל היותר, מהיכולת לפנות למוקד החירום הלאומי (CERT) ומהכתוב במדריך למתגונן בסייבר.

קצב השינוי של טכנולוגיית הסייבר הוא מהיר, כך שקשה לחזות כיצד היא תיראה בעוד מספר שנים. משום כך, קשה להכין תוכנית רב־שנתית בתחום הגנת הסייבר.[36] להשתנות המהירה ישנן גם עלויות גדולות של פחת טכנולוגי: אמצעים שיותקנו היום לא יהיו בהכרח רלוונטיים תוך מספר שנים, ויש לעדכן בהתמדה גרסאות של תוכנות, דבר שמגביר את התלות בספקי המחשוב.

העובדה שברוב מתקפות הסייבר קשה לזהות את התוקף (הנוקט אמצעי הסתרה וחמקנות), וכן ריבוי התוקפים, מחייבים את הארגונים והחברות במשק לאמץ אסטרטגיית הגנה רחבה בסייבר, שאינה מכוונת דווקא לתוקף מסוים, אלא להגנה מפני תקיפות מסוגים שונים, מכיוונים שונים וברמות קושי גוברות – הכל בשל ההתפתחויות הטכנולוגיות המהירות בתחום זה. בתחילה התפתחו מערכות הגנה היקפיות, ששמו את עיקר הדגש על הגנה מפני חדירה מרחוק ועל הסרת הווירוס שחדר, אך בעשור האחרון נפוצות בחברות גם מערכות שתכליתן לבלום או להתריע על פעילות לא מורשית, ואף עוינת, מצד אדם שחדר פיזית לארגון (חדירה ממגע קרוב), ובכלל זה עובד או ספק של אותו ארגון. כיום ממלאים תפקיד חשוב במערך ההגנה בסייבר גם מערכות ההגנה הפיזיות, קב"טים ומערך מיון כוח האדם ביחידת משאבי אנוש של הארגונים.

במהלך השנים הפכה ההגנה על התשתיות ועל המגזר הפיננסי מפני התקפות סייבר לדרישה רגולטורית מצד המדינה. במסגרת זו גם הוקמו גופים העוסקים בהגנה על הסייבר ברמה הלאומית: בישראל הוקמה כבר בשנת 2002 הרשות הממלכתית לאבטחת מידע, הפועלת במסגרת השב"כ; בשנת 2011 הוקם מטה הסייבר הלאומי; בשנת 2015 הוקמה הרשות הלאומית להגנת הסייבר;[37] בסוף 2017 הוחלט על הקמת מערך הסייבר הלאומי במשרד ראש הממשלה, כגוף שיאחד את מטה הסייבר הלאומי עם הרשות הלאומית להגנת הסייבר.[38] למרות כל הצעדים הללו, עדיין רבה הדרך להשגת הגנה מלאה על מרחב הסייבר הלאומי. כחזון לעתיד, ניתן לצפות מהמדינה שתיטול על עצמה אחריות מעשית רבה יותר להגנת מרחב הסייבר המדינתי עבור כלל המשק והאוכלוסייה. כשם שהמדינה מספקת מים

36 יצחק בן ישראל, "כי מציון ייצא סייבר", **הארץ**, **תוצרת ישראל – מוסף מיוחד ליום העצמאות**, אפריל 2018.

37 עמי רוחקס דומבה, "רשות הסייבר תחליף את השב"כ בפיקוח על אבטחת מידע בבנקים", *IsraelDefense*, 9 במאי 2016.

38 אתר מערך הסייבר הלאומי, https://www.gov.il/he/Departments/about/newabout.

צלולים וזרם חשמל יציב הן לעסקים והן לבתי המגורים, כך ראוי שהיא תדאג ליציבותה של תקשורת המחשבים ולהיותה נקייה מנוזקות.

לאור האמור לעיל, קיימת חשיבות רבה לשילוב בין המגזר הממשלתי למגזר הפרטי בתחום הגנת הסייבר. על המדינה לשלב את המגזר הפרטי בפעילות להגנת הסייבר הלאומי, הן כצרכן עיקרי והן כמשתתף במערך ההגנה.[39] דוגמה לכך ניתן למצוא בהקמתו, בינואר 2017, של מרכז בנקאי להגנת הסייבר בישראל, שהוא פרי יוזמה משותפת של הרשות הלאומית להגנת הסייבר, משרד האוצר, הפיקוח על הבנקים, התאגידים הבנקאיים וחברות כרטיסי האשראי.[40] לישראל יתרון בתחום זה, מאחר שיש בה מספר מועט יחסית של בנקים, פיקוח ממשלתי הדוק ויכולות סייבר גבוהות. עם זאת, מיעוט בנקים עלול להיות גם חיסרון, בהיבט של פיזור הסיכונים.

העובדה שמרחב הסייבר נטול גבולות טריטוריאליים מחייבת שיתופי פעולה בין־לאומיים לצורך הגנת הסייבר הלאומי. ואכן, בפסגת נאט"ו ביולי 2018 הסכימו מנהיגי המדינות החברות על הגברת המוכנות של מדינותיהם גם מול התקפות סייבר.[41] בהקשר הישראלי, יש לציין את דבריו של ראש השב"כ, נדב ארגמן, כי "מדינת ישראל נמצאת היום עם מעצמות הסייבר המובילות בעולם, בתוך זה מערכת הביטחון וקהילת המודיעין הישראלית. אנחנו כמובן משתפים פעולה עם שירותי מודיעין ומערכות ביטחון מרחבי העולם. לנו כארגון יש יכולת סייבר, גם הגנה וגם התקפה, די משמעותית. אנחנו כמובן משתפים פעולה עם כלל מערכת הביטחון הישראלית ולא עושים כלום לבד. אנחנו עם יכולת רחבה מאוד".[42]

דוגמה לשיתוף פעולה בין־לאומי בתחום הכספים הוא ארגון Financial Action Task Force (FATF),[43] שהוקם בשנת 1989 במטרה לפתח ולקדם מדיניות למלחמה בהלבנת הון ובמימון טרור ונשק להשמדה המונית. אלה תחומים שעל אף שונותם, עוסקים כולם בכסף שיש כוונה להסתיר את מקורו או את ייעודו, ואמצעי הטיפול בהם דומים. אחד הסיכונים שעליהם הצביע הארגון בעידן הסייבר הוא היכולת לבצע עסקאות לא חוקיות, או לעשות שימוש בכספים לא כשרים בסייבר, ללא חשיפה ישירה של המבַצע (פנים אל פנים). הארגון גם פרסם רשימה של קריטריונים, על פיהם

---

39 שמואל אבן, "אסטרטגיה לשילוב המגזר הפרטי בהגנת הסייבר הלאומי בישראל", **צבא ואסטרטגיה**, כרך 7, גיליון 2, אוגוסט 2015, http://www.inss.org.il/he/publication/?pauthor=50089&load_offset=30.

40 "מרכז סייבר בנקאי הוקם והחל לפעול בינואר", *READ IT NOW*, 20 במארס 2017, https://www.readitnow.co.il/news.

41 "נאט"ו שרדה את טראמפ, בינתיים", **הארץ**, 15 ביולי 2018.

42 איתי בלומנטל, "ראש השב"כ: סיכלנו השנה מתקפות סייבר מכל העולם", *Ynet*, 30 בינואר 2018, https://www.ynet.co.il/articles/0,7340,L-5078254,00.html.

43 http://www.fatf-gafi.org/home.

ייבָדקו מדינות שאינן חברות במסגרתו, ואם יוחלט שאינן עומדות בקריטריונים, הן עלולות להיכנס ל"רשימה שחורה", שתאפשר להטיל עליהן סנקציות כבדות.

הסיכון של העברת כספים לא כשרים גבר בשנים האחרונות, עם התפתחות השימוש במטבעות וירטואליים כגון ביטקוין, אטריום ודומיהם, שמאפשרים עסקאות מחוץ למערכת הפיננסית המדינתית והגלובלית הממוסדת. התפתחות של אמצעי תשלום ומערכות פיננסיות הנמצאים מחוץ לתחום שליטתן של מדינות עלולה להוביל להשלכות מרחיקות לכת, כמו מימון פעילות טרור, גיוס הון מצד ארגוני טרור וארגונים חתרניים, עקיפת סנקציות, תשלומים חשאיים עבור חומרים וטכנולוגיות רגישים ואסורים (נב"ק, טק"ק, יכולות סייבר), ערעור מערכות פיננסיות ממוסדות, פגיעה בגביית מיסים, פשעי סייבר וכופר, הלבנת הון, תשלומי שוחד ופגיעה בכספי ציבור. מדינות שונות נוקטות גישות שונות כלפי מטבעות אלה, אך המערכת הבין־לאומית טרם קיבלה החלטה משותפת לגביהם. ראשי המערכת הפיננסית במערב אינם רואים במטבעות הווירטואליים איום קרוב, נוכח הממדים המוגבלים של התופעה ביחס לשוק ההון העולמי. אם תופעת המטבעות הדיגיטליים תתפשט, יהיה צורך בנקיטת צעדי חקיקה ואכיפה ברמה המדינתית ובהסכמות בין־לאומיות, ואלה עשויים להיות חלק משמעותי מהפתרון לבעיה.[44]

הצורך בשיתוף פעולה גלובלי להגנת הסייבר הינו ברור. ארגון התקשורת הבין־לאומי (International Telecommunication Union – ITU) פועל לקדם הסכמה גלובלית סביב הגנת מרחב הסייבר. היו גם יזומות לגיבוש אמנה בין־לאומית בתחום הגנת הסייבר, בדומה לאמנות בתחום הגבלת תפוצת הנשק הכימי והביולוגי, אך ההערכות הן שהסיכויים לכך נמוכים כיום, משום שהדבר מחייב מנגנון פיקוח ואימות אמין, דבר שקשה ליישמו בתחום הסייבר.[45] גם נראה שארצות הברית חוששת שאמנה כזאת תגביל את יכולותיה ולא תתרום משמעותית להגנתה, מה שמפחית עוד יותר את הסיכוי להשגת הסכמה סביב אמנה אפקטיבית בתחום זה.

סיכום

חלקו הראשון של המאמר הציג את "הלוחמה הכלכלית הרחבה", שהיא סוג של לוחמה שהיקפה רחב יותר מהלוחמה הכלכלית על פי הגדרתה המקובלת. בחלקו השני של המאמר נדונה הלוחמה בסייבר כחלק מ"הלוחמה הכלכלית הרחבה". תחום "הלוחמה הכלכלית הרחבה" מאפשר לדון באופן מערכתי במגוון פעולות נגד כלכלת האויב, תוך שימוש בשורה של כלים – כלכליים, דיפלומטיים, תודעתיים, קינטיים

44 שמואל אבן, "מטבעות האינטרנט והביטחון הלאומי", **מבט על**, 28 בדצמבר 2017.

45 קמרון בראון ודוד פרידמן, "אמנה בינלאומית להתמודדות עם לוחמת סייבר? לקחים מהאמנות בתחום הנשק הכימי והביולוגי", בתוך: אמילי לנדאו וענת קורץ (עורכות), **בקרת נשק וביטחון לאומי: אופקים חדשים**, מזכר 136, תל אביב: המכון למחקרי ביטחון לאומי, מאי 2014.

וסייבר. מטרתן של פעולות אלו היא להפעיל לחץ על הכלכלה של האויב במטרה להרתיעו או להחלישו, בעיקר לשם השגת יעדים מדיניים וצבאיים. ניהול "לוחמה כלכלית רחבה" בעידן הסייבר מותנה בפיתוח יכולות התקפיות והגנתיות כאחד. היכולת ההתקפית חיונית גם לצורכי הגנה – לשם הרתעה ולתגובות נגד – ואילו יכולות ההגנה בסייבר הכרחיות גם למצבי התקפה, כדי לעמוד בפני התקפות נגד.

עידן הסייבר משַנה את תחום "הלוחמה הכלכלית הרחבה". מבחינה התקפית הוא מאפשר לפגוע בכלכלת האויב בעת מלחמה ובין המלחמות, הן באמצעות לוחמת סייבר "רכה" והן באמצעות תקיפות סייבר רבות־עוצמה, שעשויות להיות עדיפוֹת על פני תקיפות קינטיות, המלוות במקרים רבים בפגיעות בנפש. מבחינה הגנתית, התלות הגוברת של מדינות בסייבר מעצימה את איומי הסייבר על המשקים הכלכליים, ועל כן מחייבת מאמצים מרובים והשקעות כבדות להגנה על המשק, לצד שיתופי פעולה בתוך המשק, בין המשק הפרטי לממשלה ובין מדינות במערכת הגלובלית.

תרחישי קיצון של התקפות סייבר על כלכלות של מדינות אמנם טרם התממשו, אולם הדבר אינו מונע את הצורך להתאים בכל מקרה את קצב בניית ההגנה על הסייבר המדינתי לקצב התבססותו המואצת של המשק במרחב הסייבר.

כיצד מודיעין אסטרטגי לאומי ומודיעין עיסקי תחרותי יכולים לתרום אחד לשני – מבט השוואתי

אבנר ברנע

מודיעין אסטרטגי לאומי ומודיעין עיסקי תחרותי (competitive intelligence) נראים כשתי דיסציפלינות שונות,[1] והמחקר מתמקד בהם כשני תחומים נפרדים, ללא כל ניסיון ליישם לקחים והסברים רלוונטיים מתחום אחד למשנהו. עם זאת, מבט מעמיק על שני תחומים אלה מגלה כי יש להם הרבה מן המשותף. מכיוון שמתודולוגיית המודיעין במישור הממשלתי והעיסקי כאחד הגיעה ל"תקרת זכוכית", הפערים בין הציפיות ובין הביצועים בשני התחומים יוצרים צורך לזהות את הניתן לעשות כדי לשפר מצב זה בשני התחומים. אחת האופציות שעלו מההשוואה בין הביצועים המודיעיניים בשני התחומים היא האפשרות ליישם את הניסיון שהצטבר בתחום העיסקי כדי לשפר את התחום הלאומי, ולהיפך. הן הדיסציפלינה המודיעינית של המודיעין האסטרטגי ברמה הממשלתית והן המודיעין התחרותי הם שיטה מקובלת התומכת בקבלת החלטות. השימוש בגישה המודיעינית הוא דרך חשובה לסיוע למנהלים בכירים בשני התחומים כיצד להימנע משעויות במהלך תהליך קבלת ההחלטות על צעדיהם הבאים.

מילות מפתח: מודיעין לאומי, מודיעין אסטרטגי, מודיעין תחרותי, מודיעין שיווקי, קבלת החלטות

ד"ר אבנר ברנע הוא עמית מחקר במרכז לחקר הביטחון הלאומי, אוניברסיטה חיפה.

1 לפי SCIP (Strategic and Competitive Intelligence Professionals), מודיעין תחרותי הוא התהליך של איסוף וניתוח מידע באופן חוקי ואתי על מתחרים ועל גורמים אחרים המשפיעים על הענפים בהם הם פועלים, במטרה לסייע לארגון לקבל החלטות טובות יותר ולהגשים את מטרותיו. ראו: http://www.scip.org/.

מבוא

מודיעין אסטרטגי לאומי ומודיעין תחרותי נראים כשתי דיסציפלינות בלתי קשורות זו לזו. אולם, בשנים האחרונות מראה המחקר האקדמי על המודיעין הלאומי מצד אחד, ועל המודיעין התחרותי והשיווקי מצד שני, כי ניתן לערוך ניתוח השוואתי בין שני התחומים (ממשל ועסקים) ולחשוף יחסי גומלין אפשריים המתקיימים ביניהם. נושאים מעניינים במיוחד בהקשר זה הם ההשוואה בין הכשלים המודיעיניים בשני התחומים והאופן בו ניתן למונעם, והשאלה היא האם כל אחד מן התחומים יכול להיעזר בניסיון שנצבר בתחום האחר לצורך שיפור ביצועים.

הפתעות מודיעיניות בעלות משמעות הרת גורל נפוצות בתחום הביטחוני ובתחום העיסקי כאחד. ההתקוממות העממית בשנת 2011 נגד הממשלות והשליטים במצרים, בתוניסיה, בתימן ובסוריה, שזכתה לכינוי "האביב הערבי", ובכלל זה המהפכות שהובילו לנפילתו של משטר מובארק במצרים ולמלחמת האזרחים הטראגית והאכזרית בסוריה, ממחישה את ההשלכות מרחיקות הלכת של ההפתעה האסטרטגית בזירה הלאומית, שבפניה עמדו ישראל, ארצות הברית ומדינות מערביות אחרות. בזירה העיסקית ספגה חברת "נוקיה" – "המובילה העולמית בתחום התקשורת" – הפתעה עיסקית בדמות הופעתו של ה"אייפון" של "אפל" (2007), אשר הביא לחיסול הטלפונים הניידים של "נוקיה". כך קרה גם לחברת "קודאק" שלא נערכה למהפכה הדיגיטלית בצילום. אך טבעי הוא שאלה המתכננים מהלך אסטרטגי עושים כל שביכולתם כדי לגרום להפתעה, ואילו אלה האמונים על סיכול צעדיו האסטרטגיים של האויב עושים כמיטב יכולתם למנוע אותה.[2]

במשך שנים רבות נחשבו היכולות המודיעיניות לחלק מכישוריה הבסיסיים של המדינה, מעצם העובדה שמקבלי ההחלטות זקוקים למודיעין איכותי עליו יוכלו להסתמך. הגדרה הולמת של מודיעין היא "פעילות של מדינה, שמטרתה היא להבין או להשפיע על מדינות זרות".[3] מייקל הרמן מתייחס למודיעין ככלי חשאי וקובע כי מודיעין חשאי הוא מידע הנאסף באמצעים מיוחדים, המתחיל במקום שבו התקשורת והמקורות הגלויים חדלים לפעול.[4]

מאז מלחמת העולם השנייה מודעים מקבלי החלטות ברמה הממשלתית לעובדה כי מודיעין מהווה, לעיתים קרובות, כלי חשוב ואף קריטי בתהליך קבלת ההחלטות ברמה הלאומית. המחקר הנרחב על המודיעין ברמה הלאומית החל לפני

---

2 Avner Barnea, "Failures in National and Business Intelligence: a Comparative Study", PhD diss., University of Haifa, School of Social Sciences, 2015.

3 Michael Warner, "Wanted: A Definition of 'Intelligence'", *Studies in Intelligence* 46, no. 3 (2002):15-22.

4 Michael Herman, "Intelligence and policy: A comment", *Intelligence and National Security* 6 no. 1 (1991): 229-239.

כחמישים שנה, וכיום הוא מוכר כחלק בלתי נפרד מלימודי היחסים הבין־לאומיים ומדע המדינה.[5] המודיעין התחרותי והשיווקי נוצר והתמסד רק בשנות השמונים של המאה הקודמת, וביתר שאת מאז המחצית השנייה של שנות התשעים. הוא הושפע, במידה רבה, מחֶקר הניסיון הרלוונטי שנרכש בתחום המודיעין הלאומי, בשילוב עם תשומות מיוחדות מן המגזר העיסקי.[6] ספרו פורץ הדרך של מייקל פורטר *Competitive Strategy* (**אסטרטגיה תחרותית**) – אחת היצירות המשפיעות ביותר בתחום האסטרטגיה העיסקית – היה אחד הגורמים שהניעו את התפתחותו של המודיעין העיסקי.[7] בעוד שמהפכת המידע הפכה למשמעותית בעסקים בסוף שנות התשעים, השינויים הדינמיים בסביבה התחרותית הגלובלית חוללו תמורה בתחרות וקידמו את המחקר ההשוואתי והאקדמי בנושא המודיעין התחרותי והשיווקי.[8]

מערכות להתרעה מוקדמת זוכות למידה רבה של הכרה הן בתחום המודיעין ברמה הלאומית והן בתחום המודיעין העיסקי. בחינה מעשית של אופן יישומן של מערכות אלו בכול אחד מן התחומים מגלה כי האתגרים בשניהם דומים למדי, ולעיתים קרובות תלויים בפרשנות של המידע המודיעיני ובממשק עם מקבלי ההחלטות.[9]

---

5 Abram Shulsky and Gary Schmitt, *Silent Warfare, Understanding the World of Intelligence* (Washington, DC: Potomac, 2002); Uri Bar-Joseph and Rose McDermott, *Intelligence Success and Failure: The Human Factor* (Oxford: Oxford University Press, 2017); Karin Yarhi-Milo, *Knowing the Adversary: Leaders, Intelligence and Assessment of Intentions in International Relations* (New Haven: Princeton University Press, 2014).

6 Alf H. Walle, *Qualitative Research in Intelligence Marketing: the New Strategic Convergence* (Westport, CT: Quorum Books, 2001).

7 Michael Porter, *Competitive Strategy: Techniques for Analyzing Industries and Competitors* (New York: Free Press, 1980).

8 John Prescott, "The Evolution of Competitive Intelligence, Designing a Process for Action", *APMP* (Spring 1999); Qui Tianjiao, "Scanning for Competitive Intelligence: The Managerial Perspective", *European Journal of Marketing* 42, no. 7/8 (2008): 814-835; Richard G. Vedder and Stephen S. Guynes, "A Study of Competitive Intelligence Practices in Organizations", *Journal of Computer Information Systems* 41, no. 2 (2000): 36-39; Paul Dishman and Jonathan Calof, "Competitive Intelligence: A Multiphasic Precedent to Market Strategy", *European Journal of Marketing* 42, no. 7/8 (2008): 766-786; Sheila Wright and Jonathan Calof, "The Quest for Competitive, Business and Marketing Intelligence: A Country Comparison of Current Practices", *European Journal of Marketing* 40, no. 5/6 (2006): 453-465..

9 Jami Miscik, "Intelligence and the Presidency, How to Get it Right", *Foreign Affairs* (May/June 2017); Ben Gilad, *Early Warning: Using Competitive Intelligence to Anticipate Market Shifts, Control Risk and Create Powerful Strategies* (New York: Amacom, 2004); Cynthia M. Grabo, *Anticipating Surprise: Analysis for Strategic Warning* (University Press of America, 2004).

קווי דמיון בין שתי הדיסציפלינות המודיעיניות

ההנחה הבסיסית עליה נשען מאמר זה היא שבשני התחומים, הלאומי והעיסקי כאחד, המודיעין הנאסף על ידי יריבים או מתחרים על השינויים המתחוללים בסביבה החיצונית מסייע בתהליך קבלת ההחלטות. עם זאת, בשני התחומים קיים צורך בשיפור. מטרה זו ניתנת להשגה באמצעות מחקרים חוצי־ארגון, במיוחד משום שמקבלי ההחלטות המקבלים את המידע ומעבדים אותו נוטים לטעות, וטעויות אלו נחקרות ביעילות רבה יותר בארגונים עיסקיים מאשר בגופים מודיעיניים.[10]

מאמר זה יבחן מה יכולים תחומים אלה ללמוד האחד מהשני, וזאת על בסיס סקירת הספרות הקיימת בנושאי מידע תחרותי ומודיעין ממשלתי (אסטרטגי) כאחד. המאמר מבקש להראות כי לימוד הדדי ישפר את איכות המודיעין, יסייע בהבנה טובה יותר של מצבים סבוכים ויתרום בכך לתהליכי קבלת ההחלטות. המאמר עשוי להועיל במיוחד במניעת הפתעות אסטרטגיות, וכן בשיפור הבנתם של מצבים מורכבים.

שתי הדיסציפלינות – המודיעין הלאומי והמודיעין התחרותי – מבוססות על "מעגל המודיעין".[11] מעגל זה הוא תהליך שיטתי בן חמישה שלבים, המבטיח כי הפעילויות המודיעיניות מבוצעות תחת בלמים ואיזונים:

- **הגדרה של נושאי עניין מודיעיניים**: מה אנו יודעים על נושא מסוים ומה עלינו לגלות עוד?
- **איסוף**: איסוף מידע ממספר מקורות.
- **ארגון**: נטילת כל המידע הרלוונטי שנאסף, מיונו וארגונו (כך שיהיה זמין לאיחזור ולטיפול נוסף).
- **ניתוח**: בחינת כל פריטי המידע הרלוונטיים שנאספו וקביעת האופן בו הם משתלבים זה בזה, פירושם ומשמעותם.

10 Andrew P. Sage, "Human Judgment and Decision Rules", in *Concise Encyclopedia of Information Processing in Systems and Organizations*, ed. Andrew P. Sage (New York: Pergamon Press, 1990), pp. 227-229; Daniel Kahneman and Amos Tversky, "Choices, Values and Frames", *American Psychologist* 39 (1984): 341-350; Lowell W. Busenitz and Jay B. Barney, "Differences between Entrepreneurs and Managers in Large Organizations: Biases and Heuristics in Strategic Decision-Making", *Journal of Business Venturing* 12, no. 1 (January 1997): 9-30.

11 Judith Johnston and Rob Johnston, "Testing the Intelligence Cycle Through Systems Modeling and Simulation", in *Analytic Culture in the US Intelligence Community*, ed. Rob Johnston, (Washington DC: CIA, Center for the Study of Intelligence, 2005), https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/analytic-culture-in-the-u-s-intelligence-community/chapter_4_systems_model.htm; Thomas Smith, *Encyclopedia of the Central Intelligence Agency* (New York: Infobase Publishing, 2003), pp. 137-138; David Omand, *Securing the State* (C. Hurst & Co Publishers, 2010), pp. 113-137.

- **עיבוד והפצה**: העברת התוצר הסופי למקבלי ההחלטות. מכיוון שמעגל המודיעין הוא מעגל סגור, הוא דורש משוב ממקבלי ההחלטות וצי"ח עדכני.

ניתוח הספרות המחקרית מראה כי קיים דמיון בהסברים לכשלים מודיעיניים אסטרטגיים, הן בתחום הלאומי והן בתחום העיסקי, וזאת בחמישה תחומים עיקריים:

- **יכולת איסוף**: בדרך כלל לא קיים מחסור במידע.
- **סביבת מידע רועשת**: קיימים קשיים בקבלת המידע ובסיווגו, עוד לפני שלב ההערכה, כתוצאה מכמויות גדולות של מידע, חלקו בלתי ברור ולעיתים סותר.
- **כשלים של הגורם האנושי**: הספרות מתמקדת בכשלים של מנתח המודיעין (האנליסט) בזיהוי הפתעה מרוכזת ולא בכשלים בזיהוי היעד המודיעיני (בהפתעה מפוזרת המודיעין טועה בזיהוי יעד המודיעין שמולו, וכך הצד שכנגד מצליח להפתיע).[12] תשומת לב פחותה יותר ניתנת בספרות לפיתוח יכולת אנליטית לצורך מניעת הפתעה מפוזרת כתוצאה מהיעדר מודעות לסוג הפתעה זה.
- **קשיים ארגוניים ושיתוף פעולה לוקה בחסר**: כשלים הנגזרים ממורכבותם המבנית של ארגונים, ותחרות בין־ארגונית ופנים־ארגונית, הפוגעים בשיתוף הפעולה ובשיתוף במידע המודיעיני
- **יחסי גומלין בין המודיעין ומקבלי ההחלטות**: הבעייתיות בתחום זה עלולה לגרום להערכות מוטות וגם למנוע את העברתן, וזאת כדי למנוע קונפליקט בין המדיניות הרצויה למקבלי ההחלטות ובין ההערכות המודיעיניות.[13]

המודיעין התחרותי אימץ את הדיסציפלינה של המודיעין הלאומי ומשתמש בה לצרכיו, תוך הכנסת השינויים הדרושים. אי־הקצאת משאבים למילוי צורכי המודיעין התחרותי של תאגידים גורם להגבלת היקפו, ועל כן יש ביכולתו של מודיעין זה להתמודד עם מספר קטן בלבד של סוגיות מפתח מודיעיניות, וכתוצאה מכך לעבד פחות מידע. עם זאת, כבר מתחילתו התמקד המודיעין התחרותי לא רק במעקב אחר איומים מצד מתחרים, או בניטור של התפתחויות טכנולוגיות משמעותיות (כגון המדיה הדיגיטלית שהחליפה את ה־DVD וה־CD; מדפסת הלייזר שהחליפה את מדפסת הדיו; הצילום הדיגיטלי שהחליף את הפילם הכימי; הפלסטיק שהחליף את המתכות והזכוכית, וכן הלאה), אלא גם בחקר מגמות בשוק, תוך שימת דגש על הבנת רצונותיו של הלקוח, וזאת לצורך קבלת החלטות

12 על פי ההגדרות שהוצעו על ידי אבנר ברנע בעבודת הדוקטורט שלו, "הפתעה מפוזרת" היא התפתחות מפתיעה הנגרמת בשל קושי בזיהוי היעד המודיעיני הניצב בצד השני. את סוג ההפתעה האחר ניתן לכנות "הפתעה מרוכזת" ומוכוונת, שכן היא תוצאה של מאמצים מוכוונים (ומוצלחים) של אחד השחקנים למנוע מיריבו להעריך נכונה את כוונותיו ויכולותיו האמיתיות באמצעות הסתרה והונאה, במטרה לזכות ביתרון חד־צדדי.

13 Barnea, "Failures in National and Business Intelligence"

היוצרות יתרון תחרותי.[14] מודיעין תחרותי ומודיעין שיווקי משלימים למעשה זה את זה: מודיעין תחרותי עוקב, בדרך כלל, במבט נרחב אחרי הסביבה החיצונית העשויה להשפיע על תאגידים, תוך שיגור מבט מעמיק יותר לעבר העתיד,[15] בעוד שמודיעין שיווקי מתמקד במצב הקיים בשווקים.[16]

הקִבלה אחת הראויה לציון בין מודיעין לאומי למודיעין תחרותי היא הניסיון המתמשך לאפשר למקבלי ההחלטות להשיג את המרב מן המודיעין המוצג בפניהם. מעקב אחר שינויים תכופים בתחום העיסקי ובתחום ביטחון המדינה אינו פשוט, משום שקשה להעריך את משמעותם של אותות ורעשים ולצפות את העתיד, וכתוצאה מכך להפחית את אי־הוודאות.[17] נקודת דמיון נוספת היא שבשני התחומים, המודיעין הינו פרואקטיבי ושואף להשיג מידע העשוי להתריע על שינויים המתרחשים בסביבה החיצונית ומשמעותם.[18] זאת ועוד, המודיעין בשני התחומים, המוצג לעיתים קרובות בפני מקבלי ההחלטות, עשוי לשמש גם כזרז לפעולות נוספות וליוזמות חדשות, שמטרתן היא להשיג יתרונות.[19]

מודיעין תחרותי ומודיעין לאומי עוסקים, בדרך כלל, בעת ובעונה אחת בתחום הטקטי והאסטרטגי, וזאת כדי לתת מענה לדרישות ולצרכים שונים של צרכני המודיעין. עם זאת, מקבלי החלטות בכירים נוטים לנהות, בראש ובראשונה, אחר מודיעין אסטרטגי.[20] במודיעין תחרותי, מקבלי ההחלטות פועלים, לעיתים קרובות, בצמוד ליחידות העוסקות בניתוח אסטרטגי ולאנשי שיווק, ואילו במודיעין הלאומי־אסטרטגי, יחידות אלו פועלות בצמוד, ולעיתים קרובות ישירות, עם

---

14 Jan Herring, "Key Intelligence Topics: A Process to Identify and Define Intelligence Needs", *Competitive Intelligence Review* 10, no. 2 (1999): 4-14.

15 Bernard J. Jaworski, Deborah J. Macinnis and Ajayk Kohli, "Generating Competitive Intelligence in Organizations", *Journal of Market-Focused Management* 5 (2002): 279-307.

16 Dishman and Calof, "Competitive Intelligence"; Avner Barnea, "Competitive Intelligence in the Defense Industry: A Perspective from Israel – A Case Study Analysis", *Journal of Intelligence Studies in Business* 4, no. 2 (2014): 91-111.

17 Farshad Rafii and Paul J. Kampas, "How to Identify Your Enemies Before They Destroy You", *Harvard Business Review* (November 2002).

18 Prescott, "The Evolution of Competitive Intelligence".

19 Anders Johansson, Daniel Roos and Volker Kirchgeorg, "The Art of Systematic Surveillance", *Arthur, D. Little*, March 2013, http://www.adlittle.cn/sites/default/files/viewpoints/ADL_Intelligence_management_2012.pdf.

20 Jan Herring, "Senior Management Must Champion Business Intelligence Program", *Journal of Business Strategy* (September–October, 1990): 48-52; Douglas Bernhardt, "Strategic Intelligence for Executives", *Wits Business School Journal* 3, no. 22 (2010).

מקבלי ההחלטות הבכירים,[21] בניסיון להשפיע עליהם ולהשיג הכרה בתשומות המסופקות על ידם.[22]

מקומו של המודיעין במגזר העיסקי

בשנים האחרונות יש הכרה גוברת והולכת בקרב המגזר העיסקי כי מודיעין תחרותי הוא אחת מיכולות הליבה הדרושות לתהליך קבלת ההחלטות,[23] בדומה ליכולות אחרות, כמו שיווק, מכירות, מחקר ופיתוח, תפעול ומשאבי אנוש. נחיצותו של מודיעין תחרותי לא הייתה ברורה כלל עד אמצע שנות התשעים של המאה העשרים, ומנהלים הגיעו בעבר למעמדם בעולם העסקים באמצעות הסתמכות על מידע בלתי מאורגן, "תחושות בטן" וניסיון אישי.[24]

גם היום, המודיעין התחרותי עדיין לא התבסס לחלוטין ואינו תופס את המקום הראוי לו בחשיבתם של מקבלי ההחלטות. במשך שנים רבות התמקדו מומחי המודיעין התחרותי בעיקר בטקטיקה: בפעולות המיידיות של מתחרים ושחקנים אחרים, בגילוי כוונותיהם לטווח הקצר ובזיהוי שינויים בסביבה העיסקית. בשנים האחרונות ניתן, עם זאת, לראות התגברות ההכרה ביתרון המודיעין התחרותי בתחום האסטרטגי,[25] וזאת בזכות הסיוע שהוא נותן בזיהוי המתרחש בסביבת התחרות, ולפיכך גם בהערכתו, בהכרת היריבים שהחברה נלחמת בהם,[26] ובתרומה לתכנון ולהיערכות לשנים הבאות.[27] קלאוס סוילן הראה, עם זאת, כי על אף חשיבותם של המודיעין התחרותי והמודיעין השיווקי, כאשר חברה נאבקת בסביבת התחרות, הבעיה עלולה להימצא דווקא בתיפקוד ההנהלה הבכירה עצמה, ומצב זה עלול להשפיע גם על המודיעין,[28] בכך שתשומותיו לא יקבלו את הקשב הנדרש.

---

21 Klaus S. Søilen, "A Place for Intelligence Studies as a Scientific Discipline", *Journal of Intelligence Studies in Business* 5, no. 3 (2015): 35-46.

22 Stephen Marrin, "Why Strategic Intelligence Analysis has Limited Influence on American Foreign Policy", *Intelligence and National Security* 32, no. 6 (2017), http://dx.doi.org/10.1080/02684527.2016.1275139.

23 Robert Grant, *Contemporary Strategy Analysis* (Wiley-Blackwell, 2005).

24 Michael D. Watkins and Max H. Bazerman, "Predictable Surprises: The Disaster You Should Have Seen Coming", *Harvard Business Review* (April 1, 2003).

25 Craig Fleisher, Sheila Wright and Helen T. Allard, "The Role of Insight Teams in Integrating Diverse Marketing Information Management Techniques", *European Journal of Marketing* 42, no. 7/8 (2008): 836-851.

26 Yuval Atsmon, "To Develop a Winning Strategy, Know Who You Are Fighting", *McKinsey & Company*, June 27, 2017, http://bit.ly/2IB2kZN.

27 John Prescott and Stephen Miller, *Proven Strategies in Competitive Intelligence: Lessons from the Trenches* (New York: Wiley & Sons, 2001).

28 Klaus S. Søilen, "Why Care about Competitive Intelligence and Market Intelligence? The Case of Ericsson and the Swedish Cellulose Company", *Journal of Intelligence*

אלו אתגרים ניצבים בפני המודיעין?

במודיעין לאומי, וכן במודיעין בעסקים, מצליחים מאמצי האיסוף להשיג בדרך כלל מידע מספיק ומשמעותי דיו, שהינו בעל ערך ושימושי להערכת איומים והזדמנויות ומשמעותם. בשונה ממודיעין לאומי, המשיג מידע סודי באמצעות שימוש במשאבים גדולים וייחודיים, אלה העוסקים במודיעין תחרותי מקפידים מאוד לפעול על פי החוק, ותרומתו של מודיעין זה להצלחה העיסקית זוכה להערכה רבה.[29] פעילותו של המודיעין התחרותי מבוססת בעיקר על איסוף מידע פומבי (הידוע כמודיעין ממקורות גלויים, או Open Source Intelligence - OSINT) בהיקף מצומצם, אולם עדיין כזה שיש ביכולתו להשיג תוצאות באיכות גבוהה באמצעות יצירת תמונת מודיעין עדכנית על הדינמיקה של הסביבה החיצונית.[30] ועם זאת, מודיעין תחרותי מתפתח ככול שצורכי העסק משתנים, ולא כאשר השיטה או הטכנולוגיה המסייעים באיסוף ובניתוח המידע מתפתחים.[31]

ההעדפה בעסקים היא ליצור יחידה ארגונית אחת שתהיה אחראית על המודיעין והאסטרטגיה, אך בה בעת להקים צוותים חוצי־ארגון לצורך סיוע בניתוח המידע.[32] אולם, מה שחשוב באמת, אף יותר מאשר סוג הנתונים וכמותם, הוא יצירת תרבות תאגידית של קבלת החלטות המבוססת על מידע. לדברי או'קונל ופריק, פירושו של דבר הוא גם לעודד כל אחת ואחד בארגון להשתמש בנתונים באופן אפקטיבי יותר.[33]

Studies in Business 7, no. 2 (2017): 27-39, https://ojs.hh.se/index.php/JISIB/article/view.

29 Cynthia A. Bulley, Kofi F. Baku and Michael M. Allan, "Competitive Intelligence Information: A Key Business Success Factor", *Journal of Management and Sustainability* 4, no. 2 (2014).

30 Leonard M. Fuld, *The Secret Language of Competitive Intelligence* (New York: Crown Business, 2007).

31 John McGonagle and Michael Misner-Elias, "The Changing Landscape of Competitive Intelligence: Two Critical Issues Investigated",*Salus Journal* 4, no. 1 (2016); Troy Mouton, "Organizational Culture's Contributions to Security Failures", MA thesis (Louisiana State University, 2002), http://digitalcommons.lsu.edu/cgi/viewcontent.cgi?article=2120&context=gradschool_theses; Ming-Jer Chen and Mary Summers Whittle, "Competitor Acumen: The Heart of Competitor Analysis", Darden Case No. UVA-S-0293, https://ssrn.com/abstract=2975253; Nanette J. Bulger, "The Evolving Role of Intelligence: Migrating from Traditional Competitive Intelligence to Integrated Intelligence", *International Journal of Intelligence, Security and Public Affairs* 18, no. 1 (2016): 57-84.

32 Gary L. Neilson, Karla L. Martin and Elizabeth Powers, "The Secrets to Successful Strategy Execution", *Harvard Business Review* (June 2008).

33 Andrew O'Connell and Walter Frick, "You have got the information, but what does it mean? Welcome to 'From Data to action'", *Harvard Business Review* (November 19, 2013).

ענפי המודיעין התחרותי והשיווקי היו החלוצים בפיתוח יכולות משמעותיות למעקב אחר רשתות חברתיות ושימוש בתובנות המתקבלות מהן, ככלי תומך בקבלת החלטות.[34] השילוב בין מידע המתקבל מרשתות חברתיות בזמן אמת ובין מודיעין שיווקי ותחרותי מספק תמונה מפורטת ומקיפה שאף אחד משני תחומים אלה אינו מסוגל לספק לבדו. שימוש ב־"big data" מגבירים יכולות אלו. לאחרונה הציגה חברת הייעוץ העיסקי המובילה מק'קינזי כיצד עולם העסקים פיתח כלים אנליטיים מתקדמים להשגת מידע עיסקי נרחב המופק מרשתות חברתיות, לצד זה המופק ממקורות "קונבנציונליים",[35] בדגש על התרומה שלו לקבלת החלטות.

מודיעין לאומי מעניק משקל מוגבר גם ל־OSINT, המתגלה כמקור חשוב ואיכותי שלא ניתן להתעלם ממנו. אם בעבר ניתן היה לטעון כי מודיעין אסטרטגי ברמה הלאומית מסתמך, בראש ובראשונה, על מידע סודי, המצב כיום משתנה במהירות. OSINT הפך למשמעותי ביותר, שכן אנו חיים בעידן של שקיפות הולכת וגוברת במידע.[36] הרשתות החברתיות הפכו בשנים האחרונות למקור משמעותי למודיעין הלאומי,[37] בעוד שבתחום המודיעין התחרותי והשיווקי, הן משמשות כמקור מידע איכותי כבר למעלה מעשר שנים.[38]

עם התפתחותם המהירה של האינטרנט, מהפכת המידע, ולאחרונה הגידול העצום של הרשתות החברתיות, הופך עולם העסקים לשקוף הרבה יותר מבעבר. הקשיים בהשגת מידע מתמעטים בהדרגה, אולם הבעיה העיקרית הינה עדיין הטיפול בכמויות העצומות של המידע. האתגר הגדול ביותר במסגרת זו הוא התפתחות היכולות האנליטיות שבעזרתן ניתן יהיה להפיק תועלת מהמידע המתקבל. שלב חדש נרשם עם התפתחותו של המודיעין התחרותי החברתי, שביצועיו הטובים

34 Fleisher, Wright and Allard, "The Role of Insight Teams in Integrating Diverse Marketing Information Management Techniques"; Topi Laakso, *Handbook of Social Media Intelligence (*M-Brain, 2016), https://www.mbrain.com/ebook/getting_intelligence_out_of_social_media.

35 Martin Harrysson, Estelle Métayer and Hugo Sarrazin, "How 'social Intelligence' Can Guide Decisions", *McKinsey Quarterly* (November 2012).

36 Sean P. Larkin, "The Age of Transparency", *Foreign Affairs* 95, no. 3 (May/June 2016): 136-146; Nicholas Ballasy, "Brennan: CIA Must Rely on Social Media in the Middle East", *PJ Media* (May 20, 2015), http://pjmedia.com/blog/brennan-cia-must-rely-on-social-media-in-the-middle-east/.

37 Eyal Pascovich, "Intelligence Assessment Regarding Social Developments: The Israeli Experience", *International Journal of Intelligence and CounterIntelligence* 26, no. 1 (2013): 84-114; Kristan J. Wheaton and Melonie Richey, "The Potential of Social Networks in Intelligence", *E-International Relations* (January 9, 2014), http://www.e-ir.info/2014/01/09/the-potential-of-social-network-analysis-in-intelligence/.

38 Lars Degerstedt, "Social Competitive Intelligence: Socio-Technical Themes and Values for the Networking Organization", *Journal of Intelligence Studies in Business* 5, no. 3 (2015): 5-34.

ביותר הם בארגון המשקיע בתמיכה בתהליך האנליטי[39] באמצעות הרשת הפנימית של המומחים בארגון.

קהילת המודיעין האמריקאית מעניקה בהדרגה עדיפות הולכת וגדלה ל־OSINT. מאז "האביב הערבי" מכירים גופי המודיעין של ארצות הברית בצורך להבין מגמות, העדפות ותפיסות בקרב קהלים נרחבים – תחום שבו עולם העסקים כבר צבר ניסיון רב באמצעות מחקר ומודיעין שיווקי העוקב אחר קהלי צרכנים ענקיים. קהילות מודיעין מערביות אחרות, וביניהן גם קהילת המודיעין הישראלית,[40] נעות בכיוונים דומים ומפיקות אותו סוג של לקחים מן "האביב הערבי".[41]

אחד האמצעים המשמעותיים ביותר לאיסוף איכותי של מידע בתחום העיסקי הם עובדי הארגון עצמם. מכיוון שרבים מהם מקיימים, כחלק מתפקידם, קשרים נרחבים עם גורמים מחוץ לחברה בה הם עובדים, הם נחשפים למידע חשוב העשוי לסייע בהשגת יתרון איכותי לחברתם. לשם כך נדרשים אנשי המקצוע בתחום המודיעין התחרותי לבנות לעיתים קרובות רשתות פנימיות של יחסים בלתי רשמיים עם עובדים רלוונטיים, לעדכן אותם בסוגיות מפתח מודיעיניות ולקבל מהם מידע המגיע לידיעתם. יש לציין כי חברות עיסקיות מקפידות שפעילותן העיסקית תהיה חוקית ובהתאם לקודים אתיים. בשנים האחרונות, עם התפתחותם המהירה של ה־OSINT ובמיוחד של הרשתות החברתיות, מתקשרות חברות רבות עם עובדיהן באמצעות מערכות חברתיות פנימיות ויישומים נוספים, לצורך שיתוף מידע תחרותי שימושי.[42] מתברר כי תאגידים משתוקקים להימצא בעמדה כמו זו שתיאר מנכ"ל סיסקו, ג'ון צ'יימברס: "אנחנו מבינים את השוק, את המתחרים שלנו, וחשוב מכל – כיצד המתחרים חושבים ... יש לי מושג טוב למדי לגבי הצעדים הבאים שלנו."[43]

כשלים מודיעיניים במישור הלאומי והעיסקי

אחת ההגדרות של כשל מודיעיני מקורה ב־CIA: "הפתעה ארגונית מערכתית, הנובעת מהנחות שגויות או חסרות, מהנחות שהתעלמו מהן או מהנחות לא

---

39 שם.

40 Pascovich, "Intelligence Assessment Regarding Social Developments".

41 CIA, "INTellingence: Open Source Intelligence", *CIA: News and Information,* 2010, https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source-intelligence.html.

42 Maral Mayeh, Rens Scheepers and Michael Valos, "Understanding the Role of Social Media Monitoring in Generating External Intelligence", *Twenty-third Australasian Conference on Information Systems,* Geelong, December 3-5, 2012.

43 John Swartz, "Cisco's Chambers: 2 days with man on a mission at CES", *USA Today*, January 9, 2013, http://www.usatoday.com/story/tech/2013/01/09/cisco-ibm-oracle-hp/1791255/.

ראויות." לפי הגדרה אחרת, כשל מודיעיני הוא "הפתעה ארגונית הנובעת ממידע שגוי, מחוסר מידע, מהתעלמות או מהנחות בלתי מאימות."[44] לעיתים קרובות מדובר בגילוי מאוחר של איום משמעותי המעניק יתרון מהותי לצד היוזם, שכתוצאה ממנו נגרם נזק משמעותי לצד השני.[45] בחינה של הכשלים והסיבות להתרחשותם מובילה למסקנה כי במקרים רבים הם היו ניתנים למניעה.[46] הסיבות לכשלים הן, בדרך כלל, לא חוסר מידע, אלא דווקא הגורם האנושי, כלומר, חוסר הבנה של משמעויות המידע הזמין והערכת חסר של איומים חדשים ובלתי מוכרים.[47] התוצאה היא הצגה שגויה של משמעות האיום, כשלים ארגוניים וקשיים בהחלתה של "התרבות המודיעינית."[48] לעיתים תכופות מדי זו גם תוצאה של חדירת שיקולים פוליטיים להערכות המודיעיניות,[49] כפי שניתן לראות ב"דוח על ההערכות המודיעיניות של קהילת המודיעין של ארצות הברית טרם המלחמה בעיראק" משנת 2004.[50] כאשר ראשי מדינות מתעלמים מהתרעות מודיעיניות, הדבר נחשב ככשל מודיעיני.[51]

אחד החוקרים הישראלים הדגולים בתחום האסטרטגיה הצבאית והביטחונית, יהושפט הרכבי, הדגיש כי היעדר הבחנה של מהות האיומים הוא תוצאה של כשלים קוגניטיביים, הגורמים לקשיים ביצירת תמונת המציאות.[52] לאחר כשלים אסטרטגיים ברמה הלאומית, מבצעות ממשלות בדרך כלל בחינה מעמיקה של הסיבות לאותם כשלים במטרה להימנע מהם בעתיד, וכן חושפות את תוצאות

44 Rob Johnston, *Analytic Culture in the US Intelligence Community: An Ethnographic Study* (Central Intelligence Agency, 2005), https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/analytic-culture-in-the-u-s-intelligence-community/chapter_1.htm.

45 Bar-Joseph and McDermott, *Intelligence Success and Failure: The Human Factor*, pp. 13-17.

46 Paul R. Pillar, "Presidents Make Decisions Based on Intelligence", *Foreign Policy*, Jan/Feb 2012.

47 Bar-Joseph and McDermott, *Intelligence Success and Failure: The Human Factor*, pp. 13-17.

48 Philip Davies, "Intelligence Culture and Intelligence Failure in Britain and the United States", *Cambridge Review of International Affairs* 17, no. 3 (October 2004): 495-520; Mouton, "Organizational Culture's Contributions to Security Failures".

49 Zeev Maoz, "Intelligence Failures: An Analytical Framework", paper presented at the annual meeting of the American Political Science Association, Philadelphia, PA, August 31, 2006, http://www.allacademic.com/meta/p151465_index.html.

50 Russ Travers, "The Coming Intelligence Failure: A Blueprint For Survival", *Studies in Intelligence* no. 1, 1997, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/97unclass/failure.html

51 Mark A. Jensen, "Intelligence Failures: What Are They Really and What Do We Do about Them? *Intelligence and National Security* 27, no. 2 (2012): 261-282.

52 יהושפט הרכבי, **יסודות בסכסוך ישראל־ערב**, משרד הביטחון־ההוצאה לאור, תל אביב, 1971.

הבחינה בפני הציבור (כמו, למשל, דוח הוועדה לחקר פיגועי 9 בספטמבר 2001 בארצות הברית, משנת 2004).

המחקר מצביע על כך שבמרבית מתקפות הפתע שהתרחשו מאז שנת 1939 טענו קהילות המודיעין, קודם למתקפה, כי אין סיכון שהיא תתרחש. זו הסיבה שמקבלי ההחלטות הפנו לאחר מכן אצבע מאשימה כלפי אנשי המודיעין על כך שלא חזו את המתקפה ולא התריעו מפניה.[53] הציפיות שהגידול בכמות המשאבים והאמצעים המוקצים למודיעין בשנים האחרונות יביא לשיפור איכות המודיעין לא התממשו, ולא נרשם שיפור משמעותי ביכולותיהן של קהילות המודיעין של ארצות הברית, בריטניה וישראל בתחום האסטרטגי, בעוד שהסיבות לכשלים נותרו בעינן.[54]

ניתן להגדיר כשל מודיעיני בתחום העיסקי כהפתעה משמעותית שנגרמה עקב הערכה שגויה של הסביבה התחרותית.[55] למרבה הצער, תהליכים השוואתיים ולקחים שנלמדו מכשלים עיסקיים אינם נפוצים דיים.[56] עם זאת, בשנים האחרונות מחלחלת ההכרה כי חלק מהסיבות לכשלים עיסקיים קשור להיעדר תהליכים מודיעיניים, לקשיים של מנהלים בזיהוי שינויים בסביבה העיסקית, למידע מוטה שהוגש להם, לרצון להגיש מידע מודיעיני מרגיע, או למקבלי החלטות שהתעלמו מהמידע שהוצג בפניהם. זה בדיוק מה שקרה לחברת "נורטל" – אחת מחברות הטלקומוניקציה המובילות בעולם – כאשר ההנהלה הבכירה שלה התעלמה מסימני אזהרה מוקדמים בדבר שינויים גדולים בסביבה התחרותית, שסופקו לה על ידי יחידת המודיעין התחרותי שלה.[57] כשל זה היה אחד מגורמי המפתח שהובילו לקריסת החברה.[58]

---

53 Bar-Joseph and McDermott, *Intelligence Success and Failure: The Human Factor*, pp. 17-19.

54 Richard Betts, "Fixing Intelligence", *Foreign Affairs* 81(2002): 43-59.

55 Natalia Tsitoura and Derek Stephens, "Development and Evaluation of a Framework to Explain Causes of Competitive Intelligence Failures", *Information Research* 17, no. 2, June 2012.

56 Avner Barnea, "Lack of Peripheral Vision – How Starbucks Failed in Israel?" *African Journal of Marketing Management* 3, no. 4 (April 2011): 78-88.

57 Paul Schoemaker, George Day and Scott Snyder, "Integrating Organizational Networks, Weak Signals, Strategic Radars and Scenario Planning", *Technological Forecasting & Social Change* 80 (2012): 815-824.

58 Jonathan Calof, Laurent Mirabeau and Greg Richards, "Towards an Environmental Awareness Model Integrating Formal and Informal Mechanisms – Lessons Learned from the Demise of Nortel", *Journal of Intelligence Studies in Business* 5, no. 1 (2015): 57-69.

גודלם של תאגידים מביא ליצירתם של כיסי מודיעין איכותי המשרתים בודדים או קבוצות קטנות, אך לעיתים מונעים את היכולת לגבש תמונה מודיעינית מלאה.[59] התוצאה הינה, לעיתים קרובות, אי־הנגשתו של מידע חשוב למקבלי ההחלטות, לרוב כתוצאה מהיעדר מודעות מודיעינית, או מנטייה לשימור עוצמה בידי בודדים או קבוצות קטנות על ידי אי־שיתוף מידע.

המגזר העיסקי נע בהדרגה לעבר שיתוף פנימי של מידע והגיע למסקנה כי שיתוף מידע (sharing of information), בייחוד על המתרחש בסביבה החיצונית, הוא אחד האמצעים לחיזוק התחרות העיסקית.[60] ההנחה היא כי מידע איכותי כבר קיים בתוך הארגון וכי יש לתעל אותו בדרך הנכונה כדי שיוכל לסייע בקבלת החלטות. במודיעין לאומי, שיתוף מידע הוא אחד הלקחים החשובים ביותר שנלמדו מוועדת החקירה שחקרה את פיגועי הטרור בארצות הברית ב־11 בספטמבר 2001. הוועדה מצאה כי שיתוף המידע במודיעין הלאומי נתקל בקשיים ובהתנגדות מבפנים, עקב סודיות ומידור חסרי פרופורציה, שנבעו מקוצר ראות ומקיבעון מחשבתי. לדעת ועדת החקירה, זו הייתה אחת הסיבות העיקריות שגרמו לכשל המודיעיני שלא אִפשר למנוע את פיגועי ספטמבר 2001.[61] אותה בעיה באה לידי ביטוי גם בכשל המודיעיני למנוע את פיגוע הטרור במרוץ המרתון בבוסטון באפריל 2013.[62]

בעקבות פיגועי ספטמבר 2001 והכישלון בהערכה סביב תוכנית הנשק להשמדה המונית של עיראק ב־2003 – שני כשלים מודיעיניים הממחישים שני סוגים שונים לחלוטין של שגיאות[63] – נערכו חקירות רשמיות לקביעת הסיבות שגרמו להם. במסגרת חקירות אלו לא ניתן כל משקל לתשומות הפוטנציאליות של מודלים אנליטיים בהם נעשה שימוש במגזר העיסקי. כל ההמלצות היו להמשיך ולנהוג

---

59 Kurt April and Julian Bessa, "A Critique of the Strategic Competitive Intelligence Process within a Global Energy Multinational", *Problems and Perspectives in Management* 4, no. 2, 2006, https://businessperspectives.org/journals/problems-and-perspectives-in-management/issue-10/a-critique-of-the-strategic-competitive-intelligence-process-within-a-global-energy-multinational.

60 Christopher G. Myers, "Is Your Company Encouraging Employees to Share What They Know?" *Harvard Business Review*, November 6, 2015; Clayton Christensen, "Knowledge Sharing: Moving Away from the Obsession with Best Practices", *Journal of Knowledge Management* 11, no. 1 (2007): 36-47.

61 "The 9/11 Commission Report", 2004, http://www.911commission.gov/report/911Report.pdf.

62 Mark Giuliano, "How the FBI is Evolving to Meet Threats in a Changing Environment", *From the Boston Marathon to the Islamic State, Stein Counterterrorism Lectures*, ed. Matthew Levitt, Counterterrorism Lecture 6, Policy Focus 139 (Washington DC: The Washington Institute for Near East Policy, 2014), pp. 9-16.

63 Richard Betts, "Two Faces of Intelligence Failure: September 11 and Iraq's missing WMD", *Political Science Quarterly* 122, no. 4 (2007): 585-606.

באותו אופן, במסגרת הפרקטיקות המודיעיניות המקובלות במישור הלאומי. גם שנים קודם לכן, בעקבות פגמים בהערכה, ששיאם היה הכישלון במתן התרעה מוקדמת על נפילת חומת ברלין (1989) והתמוטטותה של ברית המועצות מאוחר יותר, הגיעה קהילת המודיעין של ארצות הברית למסקנות דומות, כלומר שעליה לבצע רק שינויים קלים, ואלה לא שיפרו בפועל את איכות הניתוח וההערכה המודיעיניים. לא נשקלה אז ברצינות האפשרות לבצע מחקר "מחוץ לקופסה", שיתבסס על הפרקטיקות המחקריות שכבר היו ידועות ושימשו את קהילת העסקים והאקדמיה.

מחקר אקדמי של כשלים עיסקיים אינו מדגיש לעיתים קרובות את הכשלים המודיעיניים, אלא מתמקד בגורמים אחרים, כגון מוצרים בלתי מתאימים, תמחור בלתי הולם, תגובה איטית לתחרות, צעדים אסטרטגיים שגויים וטעויות ניהול של מנהלים בכירים.[64] במקרים רבים, בייחוד בתאגידים גדולים בהם מחיר הכישלון הוא גבוה, ניתן לתקן אותו בתוך זמן סביר, ועל כן הוא פחות מדאיג בהשוואה להשלכות דומות של כשלים מודיעיניים במישור הלאומי. ייתכן כי כמה מן האיומים החמורים ביותר על חברות אף אינם נתפסים ככאלה שיכולים לסכן את שרידותן.[65] פתרונות מקובלים לכשלים עיסקיים, כגון החלפת ההנהלה הבכירה ושינויים ארגוניים, מתעלמים בדרך כלל מהבעיה של היעדר מודיעין או של תשומת לב לקויה אליו מצידם של מקבלי ההחלטות. הכישלונות העיסקיים של "ליווי'ס"[66] ו"נוקיה"[67] מהווים דוגמאות מאלפות לכך, ויש עוד דוגמאות רבות.

ברחבי העולם, ולעיתים גם בישראל, נוצר הרושם כי הולך וגדל מספרם של דירקטורים (חברי מועצות מנהלים) המבינים כי מודיעין איכותי המגיע בזמן הנכון הינו קריטי להצלחה עיסקית. כתוצאה מכך, אותם דירקטורים מיישמים את דיסציפלינת המודיעין התחרותי והשיווקי בארגוניהם ומבקשים מהמנהלים הבכירים לעדכן אותם באופן שוטף גם בנושאים אלה.

---

64 Kevin Coyene and John Horn, "Predicting you Competitor's Reactions", *Harvard Business Review*, April 2009.

65 Michael Stahl and David Grigsby, *Strategic Management for Decision Making* (New York: KWS Kent Publishing, 1992).

66 Mathew Olson, Derek van Bever and Seth Verry, "When Growth Stalls", *Harvard Business Review*, March 2008.

67 James Surowiecki, "Where Nokia Went Wrong?", *The New Yorker*, September 13, 2013, http://www.newyorker.com/online/blogs/currency/2013/09/where-nokia-went-wrong.html?printable=true&currentPage=all.

מה יכול המודיעין הלאומי ללמוד מהמודיעין התחרותי והשיווקי

לאורך שנים ארוכות הכירה החשיבה העיסקית הקונבנציונלית בעובדה כי לימודי המודיעין התחרותי והשיווקי נובעים מן הניסיון של המודיעין במישור הלאומי,[68] וזאת במספר תחומים:

- יישום "מעגל המודיעין" בתהליך המודיעין העיסקי.
- יישום המתודולוגיה המודיעינית של החברה סביב סוגיות מודיעיניות עיקריות.
- יצירת אינטראקציה הדוקה בין יחידות המודיעין ובין מקבלי ההחלטות, תוך שימוש במדדים מודיעיניים לצורך אזהרה על איומים בסביבה תחרותית, כגון אובדן נתח שוק, קשיים מול לקוחות גדולים, עניין פוחת במתחרים מצד ההנהלה הבכירה, התעלמות ממתחרים חדשים, עיכובים בתגובה לשינויים וחוסר מידע על המתחרים.

האתגר היה ליישם דיסציפלינה חוצה ארגון חדשה, אלא שהדבר נתקל לעיתים קרובות בהתנגדויות עיקשות ובאי־נכונות לשינוי.[69] אתגר זה ניצב במוקדו של מאמר שעסק ביישום מודיעין תחרותי בארגונים, אשר פורסם על ידי סוכנות הייעוץ של ארתור ד' ליטל תחת השם "The Art of Systematic Surveillance" ("אומנות המעקב השיטתי"). המאמר הצביע על הצורך של חברות לפתח בתוכן לא רק יחידות מודיעין, אלא גם תרבות מודיעינית, כדי להגדיל את סיכוייהן להיות תחרותיות ולשרוד בעולם היפר תחרותי.[70]

קהילת המודיעין האמריקאית סברה בשוגג כי אין ביכולתה ללמוד מהניסיון שנצבר בתחום המודיעין העיסקי, וזאת חרף העובדה כי ועדות המודיעין של הקונגרס האמריקאי ומספר מומחים בקהילת המודיעין של ארצות הברית ניסו לשכנע כי גישה זו היא שגויה. התברר כי גופי המודיעין הלאומיים נהגו קודם לכן לבחון ארגונים יריבים על בסיס מידע חסוי והתעלמו לרוב ממידע גלוי עליהם (OSINT).[71] כתוצאה מכך, הם הזניחו את הניתוח של קהלים גדולים, למשל לצורך זיהוי מוקדם של תסיסה אזרחית או מגמות משתנות בקרב דעת הקהל, אשר היה בהן כדי לאיים על משטרים קיימים.

במקביל, רכש עולם העסקים ניסיון נרחב ומוצלח בשימוש במחקרי שוק ובאיסוף מידע פומבי (גלוי) לצורך זיהוי העדפותיהם של צרכנים וניתוח צעדיהם

---

68 Thomas Kelley, *Marketing Intelligence: The Management of Marketing Information* (London: Staples Press, 1968).

69 Søilen, "Why Care about Competitive Intelligence and Market Intelligence?".

70 Johansson, Roos and Kirchgeorg, "The Art of Systematic Surveillance".

71 David Steele, "The Open Source Program: Missing in Action", *International Journal of Intelligence and CounterIntelligence* 21 no. 3 (2008): 609-619.

של מתחרים. דייוויד שֶד (Shedd), סגן מנהל סוכנות הביון של משרד ההגנה האמריקאי, התייחס לכישלונה של קהילת המודיעין בחיזוי אירועי "האביב הערבי": "האנליסטים לא הבחינו בסימנים שעשויים היו להצביע בפנינו, להראות לנו, כי יש חוסר שביעות רצון הולך וגדל ... בקרב הציבור הכללי. טעינו בכך".[72] אירועים אלה הובילו את סוכנויות המודיעין של ארצות הברית לבחון ניסיונות רלוונטיים שנעשו בתחום העיסקי, תוך ניתוח עמדותיהם של קהלים נרחבים (מיקור המונים – crowd sourcing), וזאת בשילוב עם האקדמיה וחברות גלובליות רבות, ביניהן "אינטל", "יולט פאקארד" (HP), "דל", "גוגל", "אלי לילי", "פרוקטר אנד גמבל", "ג'נרל אלקטריק" ועוד.

תחום נוסף המאפשר למודיעין האמריקאי ללמוד מן הניסיון שנצבר בעולם העסקים הוא חיזוי שווקים,[73] הידוע בשם "שוקי חיזוי" (prediction markets). הניסיון העיסקי הנרחב מאפשר לנו להעריך את הכיוונים והמגמות בשווקים ולקבל התרעות מוקדמות לגבי שינויים משמעותיים אפשריים בהם.[74] קהילות המודיעין בארצות הברית, בבריטניה ובישראל בוחנות בעת האחרונה את הניסיון שנרכש על ידי המגזר העיסקי במדידת ביצועים, וספציפית – במדידת ערך המידע.[75]

---

72 Ken Dilanian, "U.S. Intelligence Official Acknowledges Missed Arab Spring Signs", *Los Angeles Times*, July 19, 2012, http://latimesblogs.latimes.com/world_now/2012/07/.us-intelligence-official-acknowledges-missed-signs-ahead-of-arab-spring-.html
קהילת המודיעין האמריקאית גם לא הבחינה בסימנים המעידים שהצביעו על ההתקוממות הממשמשת ובאה של האוכלוסייה באיראן נגד משטר השאה ב־1979. ראו: Douglas MacEachin and Janne E. Nolan, "Iran: Intelligence Failure or Policy Stalemate?" in *Discourse, Dissent and Strategic Surprise Formulating U.S. Security Policy in an Age of Uncertainty*, eds. Douglas MacEachin and Janne E. Nolan (Washington DC: Institute for the Study of Diplomacy, Georgetown University, 2006).

73 Richard Betts, "Analysis, War and Decision: Why Intelligence Failures Are Inevitable?", *Strategic Intelligence: Windows into a Secret World, an Anthology*, eds. Loch Johnson and James Wirtz (Los Angeles: Roxbury Publishing, 2004), pp. 97-99.

74 Poung Fei Yeh, "Using Prediction Markets to Enhance US Intelligence Capabilities", *Studies in Intelligence* 50, no. 4 (2006).

75 Boyd Hendriks and Ian Wooler, "Establishing the Return on Investment for Information and Knowledge Services", *Business Information Review* 23, no. 1 (2006): 13-25; John Hollister Hedley, "Learning from Intelligence Failures", *International Journal of Intelligence and CounterIntelligence* 18, no. 3 (Fall 2005): 435-450;
אסף גלעד, מאיר אורבך, "8200 פינת עמק הסיליקון: היחידה הגדולה בצה"ל לומדת לעבוד כמו סטארט־אפ", **כלכליסט**, 1 ביולי 2012, http://www.calcalist.co.il/internet/articles/0,7340,L-3575727,00.html;David Moore, Lisa Krizan and Elizabeth Moore, "Evaluating Intelligence: A Competency-Based Model", *International Journal of Intelligence and CounterIntelligence* 18, no. 2, (Summer 2005): 204-220.

האינטראקציות בין המודיעין הלאומי למודיעין התחרותי: מקרה בוחן[76]

תאגידים גדולים מתקשים, לעיתים קרובות, לחזות אירועים ואיומים עתידיים בזירה התחרותית, למרות שקיימים כלים טובים במיוחד לשיפור יכולת החיזוי העיסקית, כגון "מודל ארבע הפינות" של פורטר[77] ומודלים שהוכיחו את עצמם, כמו זה של ג'ק וולץ', המנכ"ל לשעבר של "ג'נרל אלקטריק".[78] כשלים אלה יכולים לגרום לקשיים בלתי צפויים, העלולים להביא לקריסתו של תאגיד, ובמקרים קיצוניים אף לפשיטת רגל. למרות זאת, כשלים עיסקיים כאלה אינם בגדר אירועים חריגים, והם מתרחשים פעם אחר פעם. למעשה, אחד מתחומי אחריותם של מנהלי מודיעין תחרותי הוא להציג בפני מקבלי ההחלטות ומועצות המנהלים תחזיות לגבי עתיד הענף הרלוונטי.

חברת "צים" בע"מ הייתה תאגיד ישראלי גדול בתחום הספנות, שנמנה על עשר החברות הגדולות ביותר בתחום התובלה הימית במכולות.[79] ב־2009 הציגה "צים" מצגת בפני מחזיקי אגרות החוב שלה, כהכנה לדיון על פריסה אפשרית של חובותיה. המצגת, שכללה גרפים, הציגה את העלייה החזויה בנפח התובלה הימית מול ההשקעות בבניית ספינות חדשות הצפויות בשנים הקרובות. אין סודות בעסקי ייצור הספינות, ומספר הספינות הנבנות ותאריכי האספקה שלהן הם מידע פומבי. היה ברור כי קצב הבנייה של ספינות גדול יותר מקצב הגידול החזוי בנפח המטען. לפי המצגת של "צים", הקיבולת של התעבורה הימית הייתה אמורה לגדול פי שלושה וחצי – מ־4.9 מיליון TEU (יחידת מידה מקובלת עבור מכולות) בשנת 2000 ל־17.9 TEU בשנת 2013. הסחר העולמי לא היה צפוי לגדול בשיעור דומה באותן 13 שנים, ועל כן התוצאה הייתה יצירת קיבולת עודפת של מכולות ימיות. יתרה מזאת, מאז סוף 2008 הורע המצב עקב הירידה בביקוש, אשר החמירה באופן דרמטי את בעיית קיבולת היתר בתובלה הימית. גם ללא הירידה בביקוש לקיבולת זאת, עדיין הייתה קיבולת יתר, כתוצאה מבניית כמות עודפת של ספינות. השאלה היא, אפוא, זאת: אם היה ביכולתה של "צים" לחזות את הקיבולת העודפת בתובלה הימית, מדוע היא נכנסה לתוכנית אסטרטגית שכללה רכישה של ספינות ענק ושקיעה בחוב אדיר, שעלולה הייתה לסכן את עצם קיומה?

---

76 דורון צור, "צים הפסידה 186 מיליון דולר וגררה את החברה לישראל להפסד של 157 מיליון דולר", **דה מרקר**, 23 באוגוסט 2009, http://www.themarker.com/tmc/article.jhtml?ElementId=nl20090827_78683

77 Porter, *Competitive Strategy*.

78 Jack Welch, *Winning* (New York: Harpers Business, 2005).

79 המקרה של "צים" מוצג כאן בקצרה, אך היבטי הכשל המודיעיני שבו זוכים לתשומת לב מיוחדת.

הדוח השנתי של "צים" משנת 2004, אשר פורסם על ידי החברה האם שלה, "החברה לישראל" בע"מ, כָּלל את התחזיות הבאות, אשר התבססו על דוחות מודיעיניים: "הנהלת 'צים' ציינה כי שיעור הגידול של ההיצע צפוי להיות גבוה מן הגידול בביקוש להובלת מכולות, בהתחשב בעלייה בהזמנות חדשות לספינות הנמצאות בבנייה. לצמיחה שכזו עשויה הייתה להיות השפעה משמעותית על התוצאות העיסקיות של חברות ספנות מובילות". מצב זה, של היצע רב מדי של קיבולת תובלה, היה ברור, אפוא, כבר ב־2004, וההערכה שפורסמה על ידי "החברה לישראל" מוכיחה כי ההנהלה הבכירה נחשפה אליה. במצב זה השאלה נותרת בעינה: מדוע החליטה ההנהלה הבכירה של "צים" להיכנס לתוכנית הכרוכה בהשקעה מסיבית בשנים 2006 ו־2007 ולהזמין ספינות חדשות?

אם מנתח מודיעין תחרותי מזהה קיבולת עודפת צפויה בתוך שנתיים או שלוש שנים, הדבר ההגיוני ביותר לעשותו הוא לייעץ להנהלה הבכירה להחליף את העלויות הקבועות בעלויות משתנות ולצמצם את החוב, קרי, לא היה כדאי לרכוש ספינות וציוד או לחתום על הסכמי חכירה ארוכי טווח, ועדיף היה למכור ספינות, לקצר הסכמי חכירה לטווח ארוך ולהתמקד בחוזים לטווח קצר. כך הייתה יכולה החברה לצמצם בקלות את הוצאותיה בעיתות שפל ולהחזיר ספינות שתאריכי החכירה שלהן חלפו.

הבעיה היא שבמציאות לא תמיד פועלים כך: ראשית, טקטיקה כזו הייתה פוגעת ברווחיות לטווח הקצר, במחיר של הגדלת העלויות השוטפות לצורך גמישות עתידית והקטנת הסיכון; שנית, איש אינו רוצה להיות זה המקטין ענף הנמצא בצמיחה. לכן, הנהלות נוטות לעשות כל מה שהאחרים עושים, כלומר להתרחב כאשר גם אחרים עושים זאת. במקרה של "צים", היה זה שילוב בין חולשה אנושית ונטייה קוגניטיבית גם יחד, מעין אמירה: "אנו מעדיפים לשגות ביחד עם כולם מאשר להיות צודקים לבדנו". בסופו של דבר, החריגה מקיבולת הייצור השוטפת היוותה נטל כבד על כתפיה של "צים" במשך מספר שנים לאחר 2009, עד שהובילה אותה מאוחר יותר לפשיטת רגל.

הלקח שניתן להפיק מהמקרה של "צים" הוא שאנשים הפועלים בעולם העסקים צריכים להיות מסוגלים להתנתק מ"חשיבה קבוצתית"[80]. קל לומר זאת, אך קשה יותר לבצע את הדבר.

מהם הלקחים שנלמדו מהאירוע ב"צים" מבחינת המודיעין התחרותי? האם ניתן היה להימנע מן המצב הכספי הקטסטרופלי אליו הגיעה החברה ב־2009 באמצעות שימוש בניתוח מודיעין תחרותי? התשובה הברורה לכך היא חיובית: מודיעין תחרותי עוסק, בין השאר, בזיהוי המגמות הגדולות שיעצבו מחדש את הסביבה העיסקית ואת הגורמים המשבשים ענף עיסקי מסוים. ניתן להכין תחזיות

80 א' ג'ניס, ל' מאן, **תהליך קבלת החלטות**, מערכות, תל אביב, 1980.

עבור ענפי תעשייה שונים, לרבות ענף הספנות, בעיקר משום שהמידע פתוח ונגיש. ניתוח כזה יכול לסייע בזיהוי המגמות שתהיה להן ההשפעה הגדולה ביותר, וכן הבעיות שעלולות להיגרם כתוצאה מהן, ובנוסף לכך את התרחישים העתידיים האפשריים.

טבלה 1: שימוש בכלים מודיעיניים לשיפור תהליך קבלת ההחלטות

תחומי פעילות	כלים המיובאים מן המודיעין העיסקי־תחרותי	כלים המיובאים מן המודיעין הלאומי
ניתוח	SWOT	סימנים מעידים מוקדמים
איסוף	OSINT	מערכת צרכים ייחודית של הארגון
ניהול אי־ודאויות	חיזוי	ניתוח הזדמנויות

כלים מודיעיניים מתחומי המודיעין הלאומי האסטרטגי והמודיעין העיסקי היו יכולים לסייע למקבלי ההחלטות ול"צים". ניתן להעריך כי השימוש בחיזוי ובניתוח SWOT ו־OSINT (כמפורט בטבלה 1) לא היה מספיק כדי להפעיל השפעה חזקה על מקבלי ההחלטות, שכאמור, התעלמו מהניתוח שהוצג בפניהם והביאו מאוחר יותר לפשיטת הרגל של "צים". החברה יכולה הייתה לשפר את ביצועיה המודיעיניים באמצעות שימוש בכלים מדיסציפלינת המודיעין הלאומי, כגון סימנים מעידים מוקדמים. בדרך זו יכולה הייתה "צים" לדעת יותר על האיומים הנובעים מהשינויים הגלובליים בסחר הבין־לאומי, להכיר את מערכת הצרכים הייחודית לשיפור ההתמקדות במה שהיה חשוב באמת ל"צים" באותו שלב ולנתח הזדמנויות בדרך שעשויה הייתה לזהות הזדמנויות חיצוניות ונקודות תורפה, אותן ניתן היה לנצל לקידום אסטרטגיה זהירה יותר.[81] בחינה פנימית לא תספק לעולם את מלוא התשובות. לפיכך נראה כי רק מאמצים תכליתיים בתחום המודיעין האסטרטגי יכולים היו לספק למקבלי ההחלטות ב"צים" את האמת הבלתי נוחה על הצפוי לחברה, אם תתעלם מגורמי השינוי בזירה התחרותית.

מסקנות

כשלים מודיעיניים, ובכלל זה אי־חיזוי "האביב הערבי", גרמו לגופי המודיעין האמריקאיים, הבריטיים והישראליים לבחון את הניסיון שנרכש בניתוח עיסקי של קהלים גדולים, חיזוי, טכניקות של ניתוח הזדמנויות וניסיונות למדוד את ערכו של המידע – תחומים המוכרים היטב בעולם העסקים. נראה כי ארגוני מודיעין לאומיים מבינים בהדרגה את הצורך לחקור וללמוד מדיסציפלינות אחרות, לרבות

81 Karen Rothwell, "Opportunity Analysis in an Intelligence Context", *Competitive Intelligence Magazine* 15, no. 1 (January/March 2012).

בתחום העיסקי, כדי לבחון כיצד יש באפשרותם לחזק את יכולותיהם, וכן את הצורך בפתיחות כלפי המגזר העיסקי וביישום יכולות חדשות, שלאחר ביצוע ההתאמות הנדרשות בהן, יוכלו לסייע בהתמודדות עם האתגרים הניצבים בפניהם. דוגמה מצוינת היא האופן בו ה־FBI "המציא עצמו מחדש" לאחר אירועי ספטמבר 2001 והפך מסוכנות לאכיפת חוק לארגון ביטחון לאומי. הדבר נבע ממחקר שנערך על ידי שלושה חוקרים בעלי שם מאוניברסיטת הרווארד, בראשותו של יאן ריבקין, שעשו שימוש ביכולות אקדמיות בתחומי התכנון הארגוני והזהות הארגונית.[82]

אנשים העוסקים בדיסציפלינות של מודיעין תחרותי ושיווקי שואפים ללא הרף להגיע לרמה המקצועית הגבוהה ביותר, כך שתהיה מוכרת על ידי המנהלים בארגון, בדומה לקורה במודיעין הלאומי, אותו הם רואים כמודל האמיתי לניהול מידע ומודיעין. השימוש בדיסציפלינה המודיעינית מאפשר ליצור התרעה מוקדמת, אף לפני התפרצותו של אירוע כלכלי גדול כמו המשבר הפיננסי ב־2008,[83] אשר שינה את פני הכלכלה העולמית. הדבר נכון גם לגבי תאגידים חזקים, שלא הצליחו להבחין בשינויים שבוצעו על ידי מתחריהם ובתנודות אסטרטגיות בשווקים, מה שהותיר אותם ללא סיכוי לשרוד.

דיסציפלינת המודיעין הינה מערכת המסייעת לקבלת החלטות הן במודיעין האסטרטגי ברמה הממשלתית והן במודיעין התחרותי. השימוש בגישה אובייקטיבית מהווה דרך חשובה לסייע למנהלים בכירים בשני התחומים להימנע מטעויות בתהליך קבלת ההחלטות הקשורות לצעדיהם הבאים: הוא מוביל להערכה כוללת וזהירה יותר של חלופות ומשמעויות, ובכך מאפשר להתגבר על רבות מן הבעיות הקשורות בעמדות מוטות בשלבי עיבוד המידע, בנטיות מוקדמות, בדינמיקה הקבוצתית ובקבלת החלטות אינדיבידואלית. בנוסף, ניתוח עיסקי טומן בחובו את היתרון שבהצגה שיטתית של כלל המידע בפני מקבלי ההחלטות.

---

82 Ranjay Gulati, Ryan Raffaeli and Jan Rivkin, "Does 'What We Do' Make Us 'Who We Are'? Organizational Design and Identity Change at the Federal Bureau of Investigation," *Harvard Business School*, Working Paper 16-084, January 12, 2016.

83 Timothy Walton, "The 2007-2008 Financial Crisis as a Way to Better Understand Intelligence Failure", paper presented in ISA conference, April 2012; Avner Barnea, "Financial Crisis as an Intelligence Failure", *Competitive Intelligence Magazine* 14, no. 2 (April/June 2011).

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
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
אוניברסיטת תל אביב TEL AVIV UNIVERSITY

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