סייבר, מודיעין וביטחון

כרך 3 | גיליון 2 | אוקטובר 2019

מרוץ החימוש בחלל: מגמות עולמיות ואינטרסים מדינתיים
זאב שפירא וגיל ברעם

יכולת מגזרית לניהול סיכוני סייבר בשרשרת האספקה
גבי סיבוני, הדס קליין וזיו סולומון

טכנולוגיה ומודיעין: מגמות בהשתנות התהליך המודיעיני בצה"ל בתקופה שלאחר מהפכת המידע
יסמין פודמזו

מבצעי השפעה בסייבר ברשת האפלה (Dark Web)
לב טופור ופנינה שוקר

שינוי חברתי באמצעות הנגשה ממוחשבת של כללים משפטיים
עו"ד מיכל תג'ר, מיכאל בר־סיני, מור וילוז'ני

השימוש בטכנולוגיות ביומטריות – היבטים נורמטיביים ומשפטיים
לימור עציוני

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

סייבר, מודיעין וביטחון

כרך 3 | גיליון 2 | אוקטובר 2019

תוכן

מרוץ החימוש בחלל: מגמות עולמיות ואינטרסים מדינתיים
זאב שפירא וגיל ברעם | 3

יכולת מגזרית לניהול סיכוני סייבר בשרשרת האספקה
גבי סיבוני, הדס קליין וזיו סולומון | 21

טכנולוגיה ומודיעין: מגמות בהשתנות התהליך המודיעיני בצה״ל בתקופה שלאחר מהפכת המידע
יסמין פודמזו | 35

מבצעי השפעה בסייבר ברשת האפלה (Dark Web)
לב טופור ופנינה שוקר | 53

שינוי חברתי באמצעות הנגשה ממוחשבת של כללים משפטיים
עו״ד מיכל תג׳ר, מיכאל בר־סיני, מור וילוז׳ני | 69

השימוש בטכנולוגיות ביומטריות – היבטים נורמטיביים ומשפטיים
לימור עציוני | 85

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: פרופ' גבי סיבוני
מתאמי כתב העת: גל ספיר וגל פרל פינקל

ועדה מייעצת:

סונג'וי ג'ושי / 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 / סקוריטשס ויגילאתא, אירלנד
פרנק ג'. סילופו / אוניברסיטת ג'ורג' וושינגטון, 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: אלינור, 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

2019 © כל הזכויות שמורות

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

מרוץ החימוש בחלל: מגמות עולמיות ואינטרסים מדינתיים

זאב שפירא וגיל ברעם

בשנים האחרונות הפך החלל לזירת פעילות בעלת השפעה רבה על הביטחון, הצבא, הכלכלה והשגרה היומיומית של מדינות רבות, המושכת אליה בעלי עניין רבים. כתוצאה מכך, חלה עלייה בעיסוק העולמי בפיתוח אמצעי לחימה כנגד זירת החלל – תהליך המכוּנה "מרוץ חימוש החלל". מטרת המאמר היא להציג את התפיסות השונות הקיימות כיום בנושא חימוש החלל ואת פעילותן של המדינות הראשיות והמשניות בזירה זו, ולהציע חלוקה חדשה שלהן בהתאם למעמדן הטכנולוגי. במאמר נדונים קווי הדמיון והשוני בין דפוסי הפעולה של המדינות הפעילות בחלל בכל הנוגע לחימוש החלל, וזאת במטרה לסייע בהבנת מפת האינטרסים הלאומיים והבין־לאומיים בחלל בעת הנוכחית.

מילות מפתח: חימוש החלל, מעצמות חלל, ביטחון לאומי

מבוא

יותר מעשור לאחר שהקהילה הבין־לאומית ביקרה את סין וארצות הברית על ניסויים פומביים בטילים נגד לוויינים,[1] ובכך הביאה לצמצומם של ניסויים מסוג זה, ניתן לזהות חזרה של מדינות לפעילות בעלת מאפיינים התקפיים בחלל: רוסיה ביצעה תמרונים חשודים בקרבת לוויינים של מדינות אחרות; סין שיגרה מערכות חלל סודיות בעלות שימוש כפול; ארצות הברית פועלת להקמת חיל חלל עצמאי

זאב שפירא הוא יועץ למשלחת ישראל באו"ם וחוקר חלל, סייבר וביטחון לאומי. גיל ברעם היא מנהלת המחקר בסדנת יובל נאמן למדע, טכנולוגיה וביטחון, אוניברסיטת תל אביב.

1 Jim Wolf, “U.S. Shot Raises Tensions and Worries over Satellites”, *Reuters*, February 22, 2008, https://www.reuters.com/article/us-satellite-intercept-vulnerability/u-s-shot-raises-tensions-and-worries-over-satellites-idUSN2144210520080222; “US, other Countries Condemn China ASAT Test”, *Spacetoday*, January 19, 2007, http://www.spacetoday.net/Summary/3637.

נפרד. במארס 2019 ערכה הודו ניסוי פומבי ראשון בנשק נגד לוויינים. הניסוי של הודו – מדינה ללא היסטוריה של פעילות חלל התקפית – ממחיש את הדילמה של מדינות רבות הפועלות בחלל: האם לפעול בצורה תקיפה ועצמאית בזירה זו כדי להגן על האינטרסים שלהן, או לשים את מבטחן בפורומים בין־לאומיים כדי לנסות ולהגביל את תהליך חימוש החלל?

חימוש החלל מציב שני איומים עיקריים: הראשון הוא איום ביטחוני – פעולות חד־צדדיות של מדינות לחימוש החלל מגבירות את אי־הוודאות במערכת הבין־לאומית. לדוגמה, לאחרונה הזהירו חוקרי חלל כי הקמת חיל החלל על ידי ארצות הברית מעלה את הסיכון לסכסוכים ולהחרפת המתח בינה ובין יריבותיה;[2] השני הוא איום סביבתי – ניסויים שבוצעו בנשק נגד לוויינים הובילו ליצירת פסולת חלל רבה, שהקשתה על הפעילות במרחב הקרוב לכדור הארץ. אם תהליך חימוש החלל יואץ, עלולה זירת החלל להפוך למסוכנת ולבלתי נגישה לשחקנים השונים.[3]

התפתחותו המואצת של שוק החלל המסחרי הרחיבה אמנם את מעגל בעלי העניין בשמירה על החלל כמרחב ניטרלי, אך גם הגבירה את הסיכונים האפשריים אם הוא יהפוך לזירת לוחמה. שווי תעשיית החלל העולמית מוערך כיום בכ־340 מיליארד דולר, וצפוי לשלש את שוויו תוך כעשרים שנה.[4] חלק מצמיחה זו הוא המשך הגידול בהשקעה בחברות חלל.[5] במקביל, המתיחות הפוליטית הגוברת בעשור האחרון בין ארצות הברית, רוסיה וסין, בשילוב טכנולוגיות חלל מסחריות וטכנולוגיות חדשות כחלק מתעשיית ה־Newspace – בהן סייבר ובינה מלאכותית – העצימו את החשש מפני התפתחותו של מרוץ לחימוש החלל.

כיום קיימת הבחנה בין שני תהליכים המתרחשים בחלל: **מיליטריזציה של החלל** (Militarization of Space) – כלומר, שימוש בטכנולוגיה מבוססת חלל (לווייני תקשורת, חישה מרחוק וניווט) לתמיכה בפעולות צבאיות; **חימוש החלל** (Weaponization of Space) – הכנסת נשק למרחב החלל, כמו נשק נגד לוויינים, לוויינים בעלי יכולות פגיעה בלוויינים אחרים ונשק הפועל מהחלל לכיוון כדור

2 Laura Grego, “There Are Much Better Options than a Space Force”, *Union of Concerned Scientists*, February 19, 2019, https://www.ucsusa.org/press/2019/there-are-much-better-options-space-force-0.

3 “Trump’s Proposed Space Force could Worsen Earth’s Orbital Debris Problem”, *The Washington Post*, August 10, 2018, https://www.washingtonpost.com/world/2018/08/10/trumps-proposed-space-force-could-worsen-earths-orbital-debris-problem/.

4 Jeff Foust, “A Trillion-Dollar Space Industry will Require New Markets”, *Spacenews*, July 5, 2018, https://spacenews.com/a-trillion-dollar-space-industry-will-require-new-markets./

5 Caleb Henry, “Space Startup Investments Continued to Rise in 2018”, *Spacenews*, February 4, 2019, https://spacenews.com/space-startup-investments-continued-to-rise-in-2018.

הארץ. מקובל כיום לראות את המיליטריזציה שעבר החלל כעובדה מוגמרת; לעומת זאת, התפיסה הרווחת היא כי החלל טרם הפך למרחב חמוש, ועל כן מדובר בתהליך הפיך.[6]

בשנים האחרונות חלה עליית מדרגה בחימוש החלל על ידי המעצמות: בכירים בממשל ובצבא האמריקאי הביעו חשש מפני השימוש ההתקפי של סין ורוסיה בחלל,[7] דבר שהוביל לרפורמות נרחבות בארצות הברית בתחום החלל הביטחוני ולהקמת "חיל חלל" עצמאי בהוראת הנשיא טראמפ.[8] מהלכים אמריקאיים אלה הובילו לעליית המתח עם סין ורוסיה.[9]

במקביל, גברו בשנים האחרונות היוזמות בזירה הבין־לאומית למציאת פתרונות דיפלומטיים לשאלת חימוש החלל, ביניהן הצעה רוסית־סינית להגבלת הכנסת נשק לחלל (שהוצעה כבר ב־2008) והצעת האיחוד האירופי מ־2014 לכתיבת קוד להתנהלות בחלל.[10] לצד זאת, החלו יוזמות לא ממשלתיות לחיזוק השקיפות בנוגע לחוקי לוחמת חלל ולבחינת התאמת החוק הבין־לאומי לשימושים צבאיים בחלל: יוזמת MILAMOS,[11] שהושקה בשנת 2016 באוניברסיטת מקגיל שבקנדה, במסגרתה פועלים מומחים ממדינות שונות לגיבוש מדריך המגדיר את התאמתו של החוק הבין־לאומי לשימושים צבאיים בחלל בזמני שלום; ויוזמת ה־Woomera Manual, שהושקה בשנת 2018 באוניברסיטת אדלייד שבאוסטרליה, בשיתוף

6 להרחבה על ההבדלים ולסקירה על אי־הוודאות והקונצנזוס לגבי המונח "חימוש החלל" ראו: Columba Peoples, "The Securitization of Outer Space: Challenges for Arms Control", *Contemporary Security Policy* 32.1 (2011): 2-5.

7 Sandra Erwin, "DNI Coats: Enemies are Developing Advanced Technology, Space Weapons", *Spacenews*, April 4, 2018, http://spacenews.com/dni-coats-enemies-are-developing-advanced-technology-space-weapons-we-have-to-up-our-game; Colin Clark, "CSAF Predicts War in Space 'In a Matter of Years'", *Breaking Defense*, February 26, 2018, https://breakingdefense.com/2018/02/csaf-predicts-war-in-space-in-a-matter-of-years.

8 Mike Wall, "Trump Signs Directive to Create Military Space Force", *Space*, February 21, 2019, https://www.space.com/president-trump-space-force-directive.html.

9 Joel Gehrke, "China Warns Trump about Dangers of New Space Force", *Washington Examiner*, June 19, 2018, https://www.washingtonexaminer.com/policy/defense-national-security/china-warns-trump-about-dangers-of-new-space-force; "Russia Warns against Trump's 'Alarming' Plans for US Space Force", *Military*, June 20, 2018, https://www.military.com/daily-news/2018/06/20/russia-warns-against-trumps-alarming-plans-us-space-domination.html

10 David C. DeFrieze, "Defining and Regulating the Weaponization of Space", *Joint Force Quarterly* 74.1 (2014).

11 MILAMOS – Manual on International Law Applicable to Military Uses of Outer Space.

אוניברסיטאות נוספות, במטרה לבחון את התאמת דיני החוק הבין־לאומי הקיים לקיום מבצעים בחלל.[12]

בזירה המקצועית והאקדמית הופיעו בשנים האחרונות פרסומים רבים על פעילותן הצבאית של מדינות בחלל, ועימם גם ספרות רבה הנוגעת לחימוש החלל. על אף התגברות השיח בנושא, מרבית הספרות המחקרית עוסקת במעצמות החלל (ארצות הברית, סין ורוסיה), דבר שעלול להגביל את היקף הדיון בנושא חימוש החלל ולהציג תפיסה חלקית של התהליכים המתרחשים בזירה זו.

במאמר זה אנו ממחישים את המורכבות הקיימת כיום בתפיסות השונות לחימוש החלל ומציעים חלוקה של המדינות בהתאם ליכולותיהן הטכנולוגיות בזירת החלל, וזאת כדי להבין את מצבה העדכני של הפעילות באותה זירה. אנו מציעים לחלק את המדינות הפעילות בחלל לפי מעמדן הטכנולוגי: (1) שלוש המעצמות הגדולות הפועלות בחלל – ארצות הברית, רוסיה וסין; (2) מעצמות ביניים בחלל – האיחוד האירופי, הודו ויפן; (3) שחקניות מתפתחות בזירה. חלוקה זו מצביעה על מנעד רחב יותר של אינטרסים ותפיסות חימוש חלל שונות בין המדינות, בשונה מהתפיסה הרווחת של חימוש החלל. בחלק הראשון של המאמר אנו מציגים את התפיסות הקיימות כיום בספרות העוסקת בחימוש החלל ודנים באתגרים שהיא מציבה להבנת תהליכי החימוש הנוכחיים שמקיימות המדינות השונות; בחלקו השני אנו מציעים חלוקה שונה – על פי עוצמתן הטכנולוגית של המדינות – ודנים בתהליכים הביטחוניים, הלאומיים והדיפלומטים שמבצעת כל אחת מהמדינות בנושא; לבסוף אנו עוסקים בקצרה בישראל, וכן דנים במסקנות העולות מהחלוקה החדשה שהצענו ובהשלכותיה על הבנת פעילותן של המדינות בחלל כיום.

תפיסות חימוש החלל

בספרות חימוש החלל קיימים שני מחנות עיקריים – מתנגדי חימוש החלל והתומכים בו. אולם, בשנים האחרונות התפתח שיח מורכב יותר בנושא, המציע מנעד רחב של תפיסות עולם ודרכי פעולה. קארל מולר (Karl Mueller) מבחין בין שש תפיסות שונות לתהליך חימוש החלל, הכוללות שלושה גורמים המתנגדים לחימוש (Idealists, Internationalists, Nationalists) ושלושה גורמים המצדדים בו (Space Racers, Space Controllers, Space Hegemonists). מדובר בגישות המייצגות שלבים שונים בספקטרום של חימוש החלל, כאשר "האידיאליסטים" נמצאים בקצה

12 לקריאה נוספת על היוזמות הללו באתרים הרשמיים ראו: https://www.mcgill.ca/milamos
https://law.adelaide.edu.au/woomera

האחד ו"הגמוני החלל" נמצאים בצד הנגדי.[13] מולר מגביל את ניתוחו לתפיסות האמריקאיות בלבד ואינו מספק דוגמאות מעשיות לתפיסות אלו.

פיטר הייס (Peter Hays) מציע חלוקה לארבע תפיסות – שתיים בעד חימוש החלל (Space Hawks, Inevitable Weaponizers) ושתיים נגד חימוש החלל (Space Doves, Militarization Realists) ומתמקד גם כן בזווית האמריקאית.[14] חלוקות נוספות הקיימות בספרות משקפות נטייה דומה,[15] וניתן לראות מהן כי על אף שישנן וריאציות שונות לחלוקה, המכנה המשותף להן הוא הצגת שני מחנות בלבד – המתנגדים והתומכים – תוך התמקדות גבוהה בפעילותה של ארצות הברית ובמדיניותה בתחום זה.

גם בקרב חוקרים המייצגים את המחנות השונים בגישתם לחימוש החלל ניתן לזהות את ארצות הברית כמוקד המחקר.[16] חוקרים המצדדים בחימוש החלל, אם מטעמי הגנה על נכסי חלל חיוניים[17] ואם מטעמי שאיפה לנצח במרוץ להשגת נשק מבצעי בחלל,[18] נוטים לתאר באופן נרחב יותר את פעילותן של סין ורוסיה, אך גם אז לרוב מנקודת מבט אמריקאית. ההתמקדות בארצות הברית מובנת, שכֵּן היא מעצמת החלל הגדולה ביותר, המפרסמת מסמכי מדיניות מפורטים ופועלת בשקיפות רבה יחסית.[19] עם זאת, להתמקדות זאת יש שתי מגבלות: האחת, תפיסות חימוש חלל נבחנות בהתאם לפעילות האמריקאית, ובכך הן נמדדות בהתאם לשאלה "בעד או נגד", ללא העמקה במנעד הרחב יותר של אפשרויות; השנייה, דחיקתן של שאר המדינות במערכת לשולי השיח בנושא חימוש החלל גורמת לכך שתמונת המציאות הינה חלקית בלבד, דבר המגביל את היכולת לנתח תפיסות חלופיות לחימוש החלל.

13 Karl P. Mueller, "Totem and Taboo: Depolarizing the Space Weaponization Debate", *Astropolitics* 1.1 (2003): 5-12.

14 Peter L. Hays, *United States Military Space: Into the Twenty-First Century* (DIANE Publishing, 2002), pp. 96-100.

15 Sterling Michael Pavelec, "The Inevitability of the Weaponization of Space: Technological Constructivism versus Determinism", *Astropolitics* 10.1 (2012): 2-3; Mike Moore, *Twilight War: The Folly of US Space Dominance* (Oakland, CA: The Independent Institute, 2008), p. 16.

16 Bruce M. DeBlois, "Space Sanctuary. A Viable National Strategy", *Airpower Journal* (Winter 1998); James Clay Moltz, "Preventing Conflict in Space: Cooperative Engagement as a Possible US Strategy", *Astropolitics* 4.2 (2006).

17 Alan Steinberg, "Weapons in Space: The Need to Protect Space Assets", *Astropolitics* 10.3 (2012): 6-7.

18 Pavelec, "The Inevitability of the Weaponization of Space", pp. 5-6.

19 Rebecca Johnson, "Security without Weapons in Space: Challenges and Options", *Disarmament Forum* 1 (2003): 2-3; Todd Harrison, Kaitlyn Johnson and Thomas G. Roberts, *Space Threat Assessment 2018* (Center for Strategic and International Studies, April, 2019): Introduction.

בחלק הבא אנו מציעים חלוקה חדשה של תפיסות חימוש החלל, המושפעת ממידת בשלותן הטכנולוגית של המדינות השונות. חלוקה זו תאפשר לזהות דפוסי פעולה דומים בתהליכי חימוש החלל בין מדינות המצויות באותו מעמד טכנולוגי, ובכך לספק נקודת מבט שונה מזו של התפיסות המסורתיות לחימוש החלל.

חשיבות המעמד הטכנולוגי

כאמור, החלוקה המוצעת במאמר זה היא לשלוש קבוצות: מעצמות החלל (Space Superpowers); מעצמות ביניים (Medium Space Powers); מדינות מתפתחות בחלל (Emerging Space Powers).[20] ארצות הברית, רוסיה וסין מהוות את שלוש מעצמות החלל, והן בעלות יכולות פיתוח, שיגור ושליטה עצמאיות בלוויינים לכלל המסלולים בחלל ובעלות תוכנית חלל מאוישת; מעצמות הביניים הנבחנות במאמר זה הן האיחוד האירופי, הודו ויפן, שביכולתן לפתח, לשגר ולשלוט בלוויינים מתקדמים באופן עצמאי, אך אינן בעלות תוכנית חלל מאוישת (הודו מתכננת לבצע שיגור מאויש בשנת 2022);[21] מדינות חלל מתפתחות הן אותן המדינות שאינן בעלות היכולות הנ"ל, או שנמצאות בשלבי פיתוח ראשוניים שלהן. על אף המספר הגדול של מדינות הנמצא בקבוצה זו, במאמר נבחנות רק שלוש מתוכן – פקיסטן, ברזיל ואוסטרליה – שמהן תגובש הערכה של האינטרסים השונים הקיימים בקבוצה זו.

מעצמות החלל

ארצות הברית

ארצות הברית היא השחקנית הפעילה ביותר בחלל כיום. כתוצאה מהדומיננטיות שלה, הפכה ארצות הברית לתלויה במערכות מבוססות חלל לביטחונה הלאומי, ואלו הסבו לה יתרונות משמעותיים על פני יריבותיה. יתרונות אלה באו לידי ביטוי במלחמת המפרץ, בסכסוך בבלקן, בפלישה לעיראק ועוד.

במהלך המלחמה הקרה התמקדה ארצות הברית בסיכול האיום הסובייטי בחלל, ואף פיתחה בשנות השמונים של המאה העשרים יוזמות מתקדמות, כגון תוכנית Strategic Defense Initiative (שכוּנתה גם Star Wars) להגנה מפני טילים בליסטיים בין־יבשתיים. עם שקיעתה של ברית המועצות והתפרקותה, הלכו יוזמות אלו ודעכו.[22] בתחילת המאה ה־21 עלתה שוב לדיון שאלת ביטחון החלל,[23]

20 לצורך יצירת החלוקה נעזרנו בהגדרת "מעצמת ביניים" של: John J. Klein, "Space Strategy Considerations for Medium Space Powers", *Astropolitics* 10.2 (2012): 3.

21 יש המזהים מדינות נוספות בקבוצה זו, כגון ישראל, צפון קוריאה ואיראן.

22 Brian Weeden and Victoria Samson, eds., *Global Counterspace Capabilities: An Open Source Assessment* (Secure World Foundation, April, 2019), pp. 3.1, 3.16.

23 מזכיר ההגנה האמריקאי דאז, דונלד רמספלד, אף הזהיר מפני "פרל הרבור בחלל".

אך מגבלות כלכליות ופוליטיות מנעו פיתוח אסטרטגיה מקיפה בנושא זה.[24] עם זאת, ארצות הברית המשיכה להחזיק בעמדה התקפית בחלל, שבאה לידי ביטוי בפרסום מסמכי מדיניות הקוראים לחיזוק השליטה בו[25] ובנסיגה מאמנת ABM ‏(Anti-Ballistic Missiles) בשנת 2002.[26] בעשור האחרון גברה המתיחות ביחסים בין ארצות הברית ובין סין ורוסיה, שבאה לידי ביטוי, בין השאר, בשינויים במדיניות וברטוריקה לגבי לוחמת החלל ובהנחיית הנשיא טראמפ בשנת 2018 להקים חיל חלל עצמאי.[27]

מבחינה דיפלומטית, ארצות הברית מתנגדת בעקביות להצעות להגבלת הנשק בחלל החיצון (PPWT),[28] בשל דאגתה מפני עמימות ההגדרות וחוסר אמון בכוונותיהן של רוסיה וסין.[29] היוזמה האירופית לכתיבת קוד להתנהלות בחלל, שהינו בלתי מחייב, קיבלה תמיכה מסויגת מארצות הברית בזמן כהונתו של הנשיא אובמה,[30] אך נראה כי זו נחלשה מאז כניסתו של הנשיא טראמפ לתפקיד.[31]

לארצות הברית יכולות נרחבות לפגוע, לנטרל ולמנוע מיריבותיה את יכולותיהן בזירת החלל. כבר בשנת 1985 ערכה ארצות הברית ניסוי מוצלח בהשמדת לוויין באמצעות טיל המשוגר מהאוויר (ASM–135), שתוכנן להוות משקל נגד לנשק נגד לוויינים שפיתחה ברית המועצות. ארצות הברית אינה מפתחת כיום תוכנית ייעודית לנשק בנסיקה ישירה (Direct Ascent) נגד לוויינים, אולם הידע אותו צברה, בשילוב יכולתה המוכחת לפגוע בלוויינים, משקפים יכולת מבצעית ממשית

24 Weeden and Samson, *Global Counterspace Capabilities*, p. 3.1.

25 Johnson, "Security without Weapons in Space", pp. 2-3.

26 אמנת ABM הגבילה את ארצות הברית ורוסיה בפיתוח מערכות נגד טילים בליסטיים, שיכלו לשמש גם נגד לוויינים.

27 Weeden and Samson, *Global Counterspace Capabilities*, p. 3.18.

28 "Treaty on Prevention of the Placement of Weapons in Outer Space and of the Threat or Use of Force Against Outer Space Objects" – הצעה שממשיכות להעלות סין ורוסיה באו"ם מאז שנת 2008. ההצעה ממשיכה לספוג ביקורת על עמימותה בכל הנוגע להגדרות של נשק חלל.

29 Stephanie Nebehay, "U.S. Warns on Russia's New Space Weapons", *Reuters*, August 14, 2018, https://www.reuters.com/article/us-russia-usa-space/u-s-warns-on-russias-new-space-weapons-idUSKBN1KZ0T1; Jeff Foust, "U.S. Dismisses Space Weapons Treaty Proposal As 'Fundamentally Flawed', *Spacenews*, September 11, 2014, https://spacenews.com/41842us-dismisses-space-weapons-treaty-proposal-as-fundamentally-flawed/.

30 Marcus Weisgerber, "U.S. Wants Changes to EU Space Code of Conduct", *Spacenews*, January 12, 2012, https://spacenews.com/18667us-wants-changes-to-eu-space-code-of-conduct/.

31 John Yoo, "Military Use of Space is Coming, Trump can Help America Prepare", *The Hill*, December 28, 2017, https://thehill.com/opinion/national-security/366663-military-use-of-space-is-coming-trump-can-help-america-prepare.

להשמדת לוויני אויב. לאור היכולות הטכניות הנוכחיות של האמצעים נגד טילים בליסטיים בין־יבשתיים (ICBM) שברשותה, ההשערה היא כי יכולות אלו מוגבלות כיום למסלול נמוך (Low Earth Orbit – LEO),[32] אך ייתכן כי הטווח שלהן יוגדל בעתיד והן יוכלו לפגוע במסלולים גבוהים יותר בחלל.

בתחום כלי הנשק נגד לוויינים במסלול (Co-Orbital), ארצות הברית מפתחת אמצעים שנועדו לצרכים שונים שאינם התקפיים, כגון שירות ובדיקת לוויינים, ואף ביצעה ניסויים לאורך השנים במבצעי "תמרון וקרבה" (Rendezvous and Proximity Operations – RPO). ארצות הברית אמנם לא הכריזה על תוכנית לשימוש באמצעים אלה למטרות התקפיות, אך ההערכה היא שהיא מסוגלת לנצל את הידע שצברה כדי לפתח יכולות כאלו בתוך זמן קצר.[33] בידי ארצות הברית קיימת מערכת בשם Counter Communications System (CCS), שיכולותיה אמנם חשאיות, אך ההערכה היא שהיא מסוגלת לשבש אותות של מערכות לווייניות בעת הצורך. בנוסף לכך, ארצות הברית פיתחה במרוצת השנים מספר תוכניות בתחום של נשק באנרגיה גבוהה, שחלקן הן בעלות יכולת פוטנציאלית לפגוע בנכסי חלל.[34]

רוסיה

בתקופת המלחמה הקרה פיתחה ברית המועצות מגוון יכולות נגד נכסי החלל של יריבתה ארצות הברית. לאחר סיום המלחמה הקרה והתפרקותה של ברית המועצות איבדה תעשיית החלל הרוסית את מרבית תקציבה, ותוכניות צבאיות רבות שלה נגנזו.[35] בעשור האחרון נראה כי רוסיה החלה במאמצים לבצע תהליכי מודרניזציה במערכות החלל הצבאיות והאזרחיות שלה בניסיון לשחזר את מעמדה וכדי לא לפגר אחרי סין וארצות הברית. תחת הנשיא פוטין פועלת רוסיה באופן תקיף יותר לבסס את מעמדה האזורי והבין־לאומי, ובמסגרת זו היא סימנה את החלל כזירה משמעותית בכל מאבק עתידי.

מאז שנת 2004 פועלת רוסיה במישור הדיפלומטי ביחד עם סין לקידום הגבלת החימוש בחלל, ואף העלתה באו"ם הצעות, כגון ההצעה לאי־הכנסה ראשונה של נשק לחלל.[36] עם זאת, על פי טענת הממשל האמריקאי, המאמצים הדיפלומטיים הרוסיים אינם עולים בקנה אחד עם פעולותיה ההתקפיות של רוסיה בזירת החלל, המעידות, לדעת ארצות הברית, על כוונותיה האמיתיות.[37]

32 LEO – מסלול בגובה של עד 2,000 ק"מ סביב כדור הארץ.
33 Weeden and Samson, *Global Counterspace Capabilities*, pp. 3.1-3.6.
34 *Ibid*, pp. 3.9-3.15.
35 Harrison et al., *Space Threat Assessment 2018*, pp. 17-18.
36 "No First Placement of Weapons in Outer Space"
37 Harrison et al., *Space Threat Assessment 2018*, p. 19.

רוסיה מחזיקה באמצעים רבים לפגיעה במערכות לוויינים, המבוססים בחלקם על תוכניות מתקופת המלחמה הקרה ובחלקם הם פיתוחים חדשים. בתחום הנשק בנסיקה ישירה, רוסיה מחזיקה במספר תוכניות נגד לוויינים להפעלה מהקרקע ומהאוויר, המבוססות על מערכות כמו A–235 ו־Kontakt, שפותחו עוד בשנות השבעים והשמונים של המאה שעברה. במקביל, היא מפתחת כיום את המערכת נגד טילים בליסטיים S–500, שיש לה יכולת משוערת גם נגד לוויינים. על אף שרוסיה לא ביצעה יירוט ממשי של לוויין, כפי שעשו ארצות הברית וסין, ניתן להסיק כי הניסיון הטכני שצברה במלחמה הקרה נתן לה יכולת לפרוס נשק נגד לוויינים תוך מספר שנים, וזאת למרות מגבלותיה הטכניות.

בשנות השישים פיתחה רוסיה מערכת ליירוט לוויינים במסלול נמוך, שהוכרזה כמבצעית ב־1973. היא גם שאפה לפתח מערכת מתקדמת יותר בשם Naryad, לפגיעה בלוויינים גם במסלול גיאוסטציונרי (GEO-Geostationary orbit),[38] אך הניסויים במערכת זו נפסקו ב־1991. בעשור האחרון מפתחת רוסיה יכולות "תמרון וקרבה" באמצעות לוויינים חשאיים, בהם היא משתמשת כדי לתמרן באופן מחשיד בסמוך ללוויינים זרים – פעולה היכולה לשמש בעתיד גם לפגיעה פיזית בהם או לשיבושם.[39] רוסיה משקיעה גם בכלי נשק נוספים נגד לוויינים, כגון אמצעים לשיבוש אותות לוויינים, כולל לווייני ניווט, לווייני תקשורת ואף לווייני תצפית. בנוסף, רוסיה מחזיקה בידע טכני רב שמקורו בפיתוחי נשק לייזר בתקופת המלחמה הקרה, ואף שִׁחזרה תוכנית להצבת לייזר על גבי מערכת מוטסת (Aircraft-borne laser) לפגיעה בלווייני תצפית, אך לא ברור אם זו הגיעה לבשלות מבצעית.[40]

סין

בתקופת המלחמה הקרה נמצאה תוכנית החלל של סין בעדיפות נמוכה, וסין נותרה שחקנית משנית בזירה זו. עם זאת, בעשורים האחרונים השקיעה סין מאמצים ניכרים בפיתוח יכולותיה בחלל והפכה לשחקנית משמעותית המחזיקה בתוכניות אזרחיות וצבאיות מתקדמות, כמו תוכנית חקר חלל ומערכת ניווט עצמאית. תוכניות אלו הובילו אותה להתמודד עם ארצות הברית על השפעה אזורית וגלובלית.

במסגרת היריבות הגוברת עם ארצות הברית בעשור האחרון, פיתחה סין אסטרטגיה המבוססת, בין השאר, על מניעת יכולות אמריקאיות בחלל. בנוסף, סין החלה לפעול בצורה תקיפה יותר בזירת החלל: פרסום מסמכי מדיניות הקוראים

38 GEO – מסלול בגובה של כ־35,000 ק"מ מעל כדור הארץ. משמש לרוב עבור לווייני תקשורת.

39 Weeden and Samson, *Global Counterspace Capabilities*, pp. 2.1-2.14.

40 *Ibid*, pp. 2.15-2.22.

לדומיננטיות בחלל ופיתוח נשקי חלל מתקדמים. לא ידוע על שימוש שסין עושה כיום ביכולותיה בחלל לצורך פעילותה הצבאית, וייתכן כי יכולות אלו נבנות בעיקר לצורכי הרתעה.[41]

בזירה הדיפלומטית, סין שותפה למאמציה של רוסיה לקדם חקיקה בין־לאומית להגבלת חימוש החלל. למרות זאת, סירובה של סין לתמוך ביוזמות כגון קוד להתנהלות בחלל, בעודה מעודדת חקיקה שאין לה מנגנוני אכיפה ואינה מונעת ניסויים בנשק נגד לוויינים, מעידה, לדעת ארצות הברית, על ניסיונה להגביל אך ורק את הפעילות האמריקאית בחלל, מבלי לפגוע בהמשך פיתוח תוכניותיה שלה, ותוך הצגת עצמה כתומכת לכאורה ביוזמות שלום.[42]

בעשורים האחרונים פיתחה סין מספר יכולות בתחום הנשק בנסיקה ישירה לפגיעה בלוויינים – חלקן ייעודיות וחלקן כיכולת ליירוט טילים. סין אמנם החלה בפיתוח כלי נשק אלה כבר בשנות השישים של המאה העשרים, אך רק הניסויים בשני העשורים האחרונים, ובעיקר יירוט הלוויין שביצעה בשנת 2007, העידו על התקדמותה בתחום זה. ניתן להסיק כי סין מסוגלת כיום להשיג יכולת מבצעית לפגוע בלוויינים במסלול נמוך בעזרת מערכת קרקעית ניידת.

בעשור האחרון החלה סין לבצע פעילות "תמרון וקרבה" רבה, דבר המעלה חשש מפני פיתוח יכולות סיניות התקפיות נגד לוויינים במסלול. בין פעילויות אלו בולט שיגורו של לוויין ניסוי לניקוי פסולת Aolong-1 בשנת 2016, שגרם לחשש מפני שימוש אפשרי בו לצורך פגיעה בלוויינים. בדומה לחששות הקיימים מפני רוסיה, החשש מפני סין הוא כי בעת הצורך היא תוכל להשתמש ביכולות של לווייניה גם כדי לפגוע פיזית בלוויינים זרים.[43]

סין מפתחת אמצעים נוספים לפגיעה בלוויינים, כגון פיתוח יכולות לשיבושם, והיא גם בעלת יכולת משוערת לשבש הן אותות תקשורת והן אותות של לווייני ניווט. בנוסף, נראה כי ישנה התעניינות סינית בפיתוח אמצעי לייזר נגד חלל, ואף נטען כי בשנים 2005 ו־2006 נעשו ניסיונות סיניים לעוור לוויינים בצורה זו.[44]

לסיכום, לשלוש מעצמות החלל יש יכולות חלל נרחבות, הן בתחום האזרחי והן בתחום הצבאי, המאפשרות מניעה ופגיעה ביכולות החלל של יריבותיהן בעת

41 *Ibid*, p. 1.1.

42 הנושא מוצג בהרחבה בדוח של ועדת המסחר והביטחון האמריקאית־סינית: "China's Position on a Code of Conduct in Space", *U.S.-China Economic and Security Review Commission*, September 2017, https://www.uscc.gov/sites/default/files/Research/USCC_China%27s%20Position%20on%20a%20Code%20of%20Conduct%20in%20Space.pdf.

43 Weeden and Samson, *Global Counterspace Capabilities*, pp. 1.1-1.4.

44 *Ibid*, pp. 1.15-1.18.

סכסוך. אף שנראה כי ארצות הברית מחזיקה בתפיסה התקיפה ביותר בחלל מתוך כוונה להשיג דומיננטיות ולשמור על חופש פעולה, רוסיה וסין רואות גם הן את החלל כזירה משמעותית שבה ייקבעו תוצאות המלחמה הבאה. על כן, גם הן שמות דגש על פיתוח יכולות נגד חלל ומניעת הישגים מיריבותיהן.

בזירה הדיפלומטית פועלות רוסיה וסין באופן שונה מארצות הברית, למרות ששלושתן מחזיקות בגישה התקפית לפעילות בחלל. בעוד שארצות הברית ממשיכה לסכל הצעות חוק בין־לאומיות מחייבות להגבלת חימוש החלל ומעדיפה הצעות רכות יותר, כגון קוד התנהלות בחלל, עושות רוסיה וסין מאמצים לקידום יוזמות מחייבות להגבלת חימוש החלל. למעשה, שלוש המעצמות עושות שימוש בדיפלומטיה בעיקר כדי להגביל את יריבותיהן, בעוד שהן עצמן פועלות להעצים את יכולותיהן במטרה להשיג עליונות במרוץ החימוש בחלל.

שלוש המעצמות פועלות בהתאם לתפיסה התקפית, שנועדה אם כדי להגן על נכסי החלל שלהן ומעמדן הבין־לאומי ואם כדי לא להימצא בחיסרון אסטרטגי. אמנם, ניתן לעמוד על מספר הבדלים ביניהן – ארצות הברית שואפת להגמוניה בחלל, סין שואפת להשיג שוויון, ורוסיה רוצה לצמצם את חולשתה היחסית – אך המכנה המשותף לשלושתן הוא הימצאותן בצד התומך בחימוש החלל (Pro-Weaponization).

מעצמות הביניים

אירופה

גרמניה, בריטניה, צרפת ואיטליה מחזיקות בתשתית חלל צבאית נרחבת, הכוללת לוויני תצפית ומערכות נוספות. עם זאת, לא ידוע על קיומה של תוכנית לחימוש החלל של אף אחת ממדינות אלו, של מדינות אחרות באיחוד האירופי או של האיחוד עצמו כגוף. למעשה, רק באסטרטגיה העדכנית של הנציבות האירופית, שפורסמה בשנת 2016, הושם דגש על מרכיב ההגנה בחלל, הכולל שיפור בתחום המודעות למצב בחלל ובחינת איומים עליו, כגון מזג האוויר בחלל ומתקפות סייבר.[45] סוכנות החלל האירופית מפתחת מספר יוזמות לניקוי פסולת חלל ולחקר החלל, שעל אף שמטרתן היא אזרחית, הוערך כי הן טומנות בחובן את האפשרות הטכנית לפגוע בנכסי חלל במידת הצורך.[46]

---

45 “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Space Strategy for Europe”, *The European Commission*, October 26, 2016, pp. 8-10, https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/COM-2016-705-F1-EN-MAIN.PDF.

46 Harrison et al., *Space Threat Assessment 2018*, pp. 36-37.

בזירה הבין־לאומית, האיחוד האירופי התנגד להצעות סין ורוסיה להגבלת חימוש החלל, מתוך תפיסה שהן אינן ברורות ומקיפות מספיק.[47] עם זאת, מאז שנת 2008 מוביל האיחוד את היוזמה לכתיבת קוד להתנהלות בחלל במטרה לשבור את הקיפאון בדיון בנושא חימוש החלל.[48] פעולות האיחוד האירופי נועדו להגביל את חימוש זירת החלל, אך גם מהוות ניסיון להתברג כשחקן מרכזי הקובע את סדר היום הנורמטיבי בזירה זאת,[49] כחלק מתפיסה רחבה יותר של חשיבות ההגנה על נכסי החלל.[50]

הודו

הודו החלה בפיתוח תוכנית חלל בשנות השישים של המאה העשרים, אך עד לשנות התשעים לא רשמה הישגים משמעותיים ובנתה תשתית בסיסית בלבד. על אף שמטרת תוכנית החלל ההודית הייתה לשפר את מעמדה הכלכלי של הודו באמצעות חדשנות טכנולוגית, היא הושפעה רבות מהתחזקותה הצבאית של סין. לאור זאת, שימושים צבאיים ראשוניים בחלל נבחנו על ידי הודו כבר בשנות השמונים, עם פיתוח מערכת הטילים IGMDP,[51] שעל בסיסה פותחו גם מערכות הגנה מפני טילים בליסטיים בשנות התשעים.[52]

יריבותה של הודו עם סין ופקיסטן המשיכה להשפיע על תוכנית החלל הצבאית שלה והובילה אותה לפיתוח יכולותיה בתחום ההגנה מפני טילים ולחיזוק קשריה עם ארצות הברית, כולל בחילופי טכנולוגיה. על אף שהודו רמזה מספר פעמים על פיתוח יכולות ליירוט לוויינים, לא התקיימה בה תוכנית פומבית לפיתוח כלי נשק אלה, עד שבמארס 2019 היא ביצעה ניסוי מוצלח בטיל נגד לוויינים והשמידה לוויין שלה. הדבר העלה חשש כי הודו מתכוונת להמשיך לפתח נשקי חלל כדי לא להישאר מחוץ להסכם עתידי להגבלת חימוש החלל.[53]

---

47 Statements on behalf of the EU, “EU Explanation of Vote – United Nations 1st Committee: No First Placement of Weapons in Outer Space”, *European Delegation to the UN Website*, November 2, 2018, https://eeas.europa.eu/delegations/un-new-york/53334/eu-explanation-vote-%E2%80%93-united-nations-1st-committee-no-first-placement-weapons-outer-space_en.

48 Peoples, “The Securitization of Outer Space”, pp. 11-14.

49 Max M. Mutschler and Christophe Venet, “The European Union as an Emerging Actor in Space Security?”, *Space Policy* 28.2 (2012): 4-6.

50 Phillip A. Slann, “Anticipating Uncertainty: The Security of European Critical Outer Space Infrastructures”, *Space Policy* 35 (2016): 8.

51 “Integrated Guided Missile Development Programme.

52 Zulfiqar Khan and Ahmad Khan, “Chinese Capabilities as a Global Space Power”, *Astropolitics* 13.2-3 (2015): 12-13.

53 Dorin Elin Urrutia, “India’s Anti-Satellite Missile Test is a Big Deal. Here’s Why”, *Space*, March 30, 2019, https://www.space.com/india-anti-satellite-test-significance.html.

בזירה הדיפלומטית, הודו ממשיכה לתמוך במאמצים גלובליים ואזוריים לשימוש בחלל למטרות שלום ולקדם נורמות לבטיחות ולקיימות בחלל. כחלק ממאמציה, הודו הציעה לשגר לוויין עבור הארגון הדרום אסייתי לשיתוף פעולה אזורי (SAARC),[54] ואף שיגרה בשנת 2017 לוויין תקשורת לסיוע למדינות האזור.[55] הודו גם תומכת ביוזמות של סין ורוסיה להגבלת חימוש החלל, ולאחרונה אף חזרה על תמיכה זו בעקבות הניסוי שביצעה בנשק נגד לוויינים.[56] כמו כן, הודו תומכת בניסוח קוד להתנהלות בחלל, אך נותרה מסויגת לגבי מספר סעיפים בו, וגם נוכח העובדה שלא הייתה שותפה מלאה בגיבושו.[57]

יפן

הפעילות היפנית בחלל התמקדה מתחילתה במרכיב האזרחי ולא בפיתוח תשתיות צבאיות וביטחוניות. עם זאת, לחצים גוברים בעשור האחרון מצד ארצות הברית וחשש גובר מפני שכנותיה, הובילו את יפן לאמץ גישה פעילה יותר להגנת החלל ולארגן מחדש את תשתיות החלל הצבאיות שלה כדי להגביר את עצמאותה בזירה זאת.[58] כחלק ממאמצים אלה, שיגרה יפן בשנים האחרונות לווייני תקשורת ותצפית, הקימה מטה חדש למעקב אחרי איומים בחלל,[59] ואף אישרה בסוף שנת 2017 את תקציב ההגנה הגדול ביותר שלה (כ־46 מיליארד דולר).[60]

ליפן אין כיום תוכנית לפיתוח נשק חלל, אך היא מחזיקה ביכולת פוטנציאלית לפגיעה בלוויינים באמצעות המערכת האמריקאית ליירוט טילים Aegis הפרוסה

---

54 ארגון "South Asian Association for Regional Cooperation" כולל את אפגניסטן, בנגלדש, בהוטאן, הודו, האיים המלדיביים, נפאל, פקיסטן וסרי לנקה.

55 "India Launches 'Invaluable' South Asia Satellite", *BBC*, May 5, 2017, https://www.bbc.com/news/world-asia-india-39814455.

56 Sachin Parashar, "Not Entering into Outer Space Arms Race, India Tells P-5 Countries", *The Times of India*, March 28, 2019, https://timesofindia.indiatimes.com/india/not-entering-into-outer-space-arms-race-india-tells-p-5/articleshow/68604921.cms.

57 Rajeswari Pillai Rajagopalan, "The Space Code of Conduct Debate: A View from Delhi", *Strategic Studies Quarterly* 6.1 (2012): 7-12.

58 Paul Kallender and Christopher W. Hughes, "Hiding in Plain Sight? Japan's Militarization of Space and Challenges to the Yoshida Doctrine", *Asian Security* (2018): 8-9.

59 Shinichi Fujiwara, "Japan to Set Up Space Command Center to Track Debris, Threats", *Asahi Shimbun*, November 20, 2018, http://www.asahi.com/ajw/articles/AJ201811200034.html.

60 Mari Yamaguchi, "Japan Cabinet Approves Record 46B$ Defense Budget", *Defense News*, December 27, 2017, https://www.defensenews.com/global/asia-pacific/2017/12/27/japan-cabinet-approves-record-46b-defense-budget/.

בשטחה, ויכולת עתידית של מערכות "תמרון וקרבה" אותן היא מפתחת.[61] יתרה מכך, התקדמותה הצבאית של יפן בחלל בשנים האחרונות מעידה על זניחה מסוימת של הנורמות ההגנתיות המסורתיות שלה ומעבָר לאסטרטגיה בעלת מאפיינים התקפיים יותר.[62]

בזירה הדיפלומטית, יפן תומכת הן בהצעות שהעלו רוסיה וסין להגבלת חימוש החלל והן ביוזמה האירופית לפתח נורמות וקוד להתנהלות בחלל.[63] עם זאת, נראה כי הברית האסטרטגית של יפן עם ארצות הברית ממשיכה לזכות בחשיבות עליונה מבחינתה; לפני שארצות הברית החלה לתמוך ביוזמת קוד ההתנהלות של האיחוד האירופי, נמנעה יפן מלהביע את עמדתה כדי לא להגביל את ארצות הברית.[64]

לסיכום, מעצמות הביניים מחזיקות בתשתיות חלל אזרחיות נרחבות, ביניהן לוויינים רבים לשימוש כפול, שנועדו לתמוך במידת הצורך בפעילותן הצבאית. אולם, נראה כי עד עתה פעלו מדינות אלו בריסון מסוים, לא פיתחו אמצעים לפעולה התקפית בחלל, ואף המשיכו לתמוך ביוזמות בין־לאומיות למניעת חימוש החלל. למרות זאת ולאור ההתקדמות הטכנולוגית הרבה של מדינות אלו בשנים האחרונות והשקעת התקציבים הניכרת שלהן בתחום זה, יש להניח כי יהיה ביכולתן לפתח נשקי חלל מבצעיים תוך זמן קצר מקבלת החלטה בנושא. יוצאת דופן כאמור היא הודו, שכבר ביצעה ניסוי כזה.

בניגוד למעצמות החלל, ששואפות להשיג עליונות באמצעות אסטרטגיה צבאית התקפית ותמיכה מוגבלת ביוזמות בין־לאומיות, מעצמות הביניים מנסות להגביל את תפוצת נשק החלל באמצעות יוזמות בין־לאומיות וביסוס תשתיות הגנתיות בחלל, כגון אמצעי תצפית ומערכות יירוט. מעצמות הביניים אמנם מעוניינות בהגבלת תפוצת נשק החלל, אך נדמה כי קיימת שונות במניעיהן בשאלה זו.

האיחוד האירופי – יוזם הקוד להתנהלות בחלל – מבקש למקם עצמו כשחקן ראשי במניעת תפוצת נשק חלל ולחזק בכך את מעמדו הבין־לאומי; הודו, השואפת לבסס את מעמדה האסטרטגי האזורי, אותתה מצד אחד על יכולותיה ההתקפיות בחלל, ומצד שני ממשיכה לתמוך ביוזמות בין־לאומיות נגד חימוש החלל ובשיתופי

---

61 Laura Grego, “A History of Anti-Satellite Programs”, *Union of Concerned Scientists* (January 2012): 10-12.

62 Kallender and Hughes, “Hiding in Plain Sight”, pp. 17-18.

63 “Japan’s Disarmament and Non-Proliferation Policy (5th Edition)”, *Ministry of Foreign Affairs of Japan*, March 2011, pp. 26-27, https://www.mofa.go.jp/policy/un/disarmament/policy/pamph0812/1-3.pdf.

64 Kazuto Suzuki, “Japan, Space Security and the Code of Conduct”, in *Decoding the International Code of Conduct for Outer Space Activities*, ed. Ajey Lele (New Delhi: Institute for Defence Studies & Analyses: Pentagon Security International, 2012), pp. 94-96.

פעולה אזוריים; נדמה כי יפן פועלת מתוך המניעים הצרים ביותר, בהם שמירה על ביטחונה הלאומי באמצעות חיזוק יכולותיה בחלל ובריתה עם ארצות הברית, והמשך שיתוף הפעולה עם הקהילה הבין־לאומית לגבי הגבלות חימוש החלל.

בעוד שמעצמות החלל מחזיקות בתפיסת החימוש ההתקפית ביותר, המדינות מהדרג השני שהוצגו לעיל פועלות במספר מישורים המייצגים גישות שונות, ולעיתים אף מנוגדות, לחימוש החלל. נראה כי הימצאותן של מדינות אלו ב"אמצע" ההירככיה הטכנולוגית בחלל[65] מובילה גם למעין "תפיסת אמצע" שלהן בשאלת חימוש החלל: מצד אחד, הן פועלות במישור הדיפלומטי להגביל את החימוש בחלל ואינן מקדמות תוכניות חלל התקפיות (בסייג של הניסוי ההודי בנשק נגד לוויינים), ומצד שני, הן אינן מתחייבות באופן מלא לכל היוזמות הבין־לאומיות וממשיכות לפתח אמצעי חלל מתקדמים שעלולים לשמש בעת הצורך ללחימה.

המדינות המתפתחות בחלל

הקבוצה השלישית כוללת את המדינות המתפתחות בחלל (Emerging Space Powers) – אלו שאינן בעלות יכולות פיתוח, שיגור ושליטה עצמאיות בלוויינים. קבוצה זו כוללת בפועל את כל המדינות שלא נכללו בשתי הקבוצות הקודמות, ובה נמצאות הן מדינות בעלות תשתיות בסיסיות וסוכנויות חלל, כמו פקיסטן, ברזיל ואוסטרליה, והן מדינות ללא תשתיות חלל בסיסיות, כגון רוב מדינות אפריקה. מפאת היקף הקבוצה לא ייסקרו כל השחקנים הנמצאים בה, אך יידונו המאפיינים המשותפים להם וייחודם.

מבחינה צבאית, חלק מהמדינות המתפתחות הן בעלות מערכות חלל לצרכים ביטחוניים או לשימוש כפול, כמו לווייני תקשורת ותצפית, אך בשל חוסר בשלותן הטכנולוגית הן נאלצות להסתייע בשחקניות מתקדמות יותר בחלל כדי לשגר מערכות אלו, ולעיתים גם לפתח אותן ולתפעלן. על כן, ניתן להעריך כי אין למדינות אלו יכולות צבאיות מתקדמות יותר בחלל.

המדינות המתפתחות פועלות באופן משמעותי יותר בזירה הדיפלומטית, אם על ידי הבעת תמיכה כמעט מוחלטת ביוזמות של סין ורוסיה להגבלת חימוש החלל, ואם על ידי נוכחות ולקיחת חלק פעיל ביוזמות בין־לאומיות, כגון קוד ההתנהלות בחלל.[66] על אף התמיכה הברורה של המדינות המתפתחות בהגבלת תפוצתו של נשק החלל, ניתן לזהות הבדלים באינטרסים העומדים מאחורי תמיכתן זאת.

65 Klein, "Space Strategy Considerations for Medium Space Powers", p. 3.

66 למשל, בשנת 2017 לא הצביעה אף מדינה מתפתחת נגד הצעת "Further practical measures for the prevention of an arms race in outer space", ורק שתיים (אוקראינה וגיאורגיה) הצביעו נגד הצעת "No first placement of weapons in outer space":

פקיסטן, כמדינת חלל מתפתחת המצויה בסכסוך רב־שנים עם הודו, היא בעלת יכולות החלל המתקדמות יותר. פקיסטן הביעה תמיכה ביוזמות בין־לאומיות שונות בתחום החלל, אך הצהירה שאינה מוכנה לשאת בהשלכות של אמנות נגד תפוצת נשק או של סנקציות שעלולות להגביל את מאמציה בחלל.[67]

ברזיל, הנמצאת באזור בעל מתח גיאו־פוליטי נמוך יותר, תמכה ואף השתתפה בהצעתן של סין ורוסיה להגבלת נשק ("No First Placement of Weapons in Outer Space"),[68] אך הביעה חוסר שביעות רצון מתהליך ניסוח הקוד להתנהלות בחלל ומחֵלק מסעיפיו.[69] בכך היא מיצבה את עצמה כפעילה וכתומכת בקידום אמצעים חזקים יותר להגבלת נשק חלל.

אוסטרליה, הנמצאת בברית אסטרטגית עם ארצות הברית ומסתמכת על יכולותיה בחלל,[70] תומכת ביצירת קוד להתנהלות בחלל, בין היתר במטרה להפחית את הסכנה לסביבת החלל ואת פסולת החלל.[71]

כפי שנראה, על אף תמיכתן באמצעים דיפלומטיים להגבלת נשק חלל, המדינות המתפתחות פועלות מתוך מניעים שונים הנובעים ממאפייניהן הייחודיים, כגון מצב גיאו־פוליטי, שאיפות טכנולוגיות או תפיסות ביטחון שונות. למרות שלא ניתן לקבוע כי אין ברצונן למנוע מרוץ חימוש בחלל גם ממניעים אידיאליסטיים, ניתן ללמוד כי גם במקרה של קבוצה זו יש צורך במיפוי האינטרסים השונים, שאינם מתיישבים עם התפיסה המוגבלת יחסית של "בעד או נגד" חימוש החלל.

באופן דומה לזה של הקבוצות הקודמות, יש הלימה בין מיקומן של המדינות המתפתחות בהיררכיה הטכנולוגית ובין פעילותן בחלל. מכיוון שהמדינות המתפתחות מחזיקות ביכולות החלל הבסיסיות ביותר, הן תומכות בצורה הברורה

"First Committee Submits Six Drafts to General Assembly, One Calling for Immediate Start of Negotiations on Treaty Preventing Outer Space Arms Race", *United Nations Website*, October 30, 2017, https://www.un.org/press/en/2017/gadis3591.doc.htm.

67 Urooj Tarar, "Pakistan Opposes the Weaponization of the Final Frontier, Outer Space", *Daily Pakistan*, October 19, 2017, https://en.dailypakistan.com.pk/pakistan/pakistan-opposes-the-weaponization-of-the-final-frontier-the-outer-space./

68 "UN Adopts Russian 'No First Placement of Weapons in Outer Space' Resolution", *Russia Beyond*, December 8, 2015, https://www.rbth.com/news/2015/12/08/un-adopts-russian-no-first-placement-of-weapons-in-outer-space-resolution_548679.

69 Zahid Imroz, "Space Code of Conduct: Need to Re-analyse", in *Decoding the International Code of Conduct for Outer Space Activities*, p. 134.

70 Connie Agius, "Australia's Reliance on US Space Capabilities could Put Security at Risk, Defense Expert Says", *ABCnews*, February 23, 2018, https://www.abc.net.au/news/2018-02-23/australias-reliance-on-us-in-space-a-national-security-risk/9474122.

71 Dylan Welch, "Australia Joins Race to Defend Space", *The Sydney Morning Herald*, January 19, 2012, https://www.smh.com.au/technology/australia-joins-race-to-defend-space-20120118-1q6k2.html.

ביותר ביוזמות להגבלת נשק החלל. זאת, אם מתוך סירוב לשאת בעול של סנקציות עתידיות (כפי שהתבטאה פקיסטן) ואם כדי לשמור על ביטחון זירת החלל, אליה הן שואפות להצטרף בעשורים הקרובים (כפי שמאותתות ברזיל ואוסטרליה).

ישראל

לישראל יכולות חלל מתקדמות וכיום היא מסוגלת לפתח, לשגר ולהפעיל לוויינים מתקדמים באופן עצמאי (כפי שהדבר בא לידי ביטוי בסדרת לווייני "אופק"). לפיכך, ניתן למקם אותה בקבוצת מעצמות הביניים. עם זאת, אין לישראל אסטרטגיית חלל לאומית רשמית, והיא נאלצת להיסמך על מדינות אחרות כדי לשגר לוויינים למסלול גיאוסטציונרי. בתחום נשקי חלל, אין לישראל תוכנית מוצהרת לפיתוח אמצעים נגד לוויינים, אך היא מחזיקה ביכולת הטכנית להשמיד לוויינים באמצעות מערכת יירוט הטילים "חץ 3".[72] בתחום הדיפלומטי, ישראל מצביעה באופן קבוע יחד עם ארצות הברית נגד היוזמות של סין ורוסיה להגבלת חימוש החלל.

ישראל פועלת באופן התואם את מיקומה ההירכי בין המדינות הפועלות בחלל: היא אינה פועלת באופן תקיף בזירת החלל; עם זאת, היא ממשיכה להתנגד ליוזמות להגבלת חימוש החלל, כחלק מהברית האסטרטגית עם ארצות הברית, ונוטה לתמוך בשימור יחסי הכוחות הקיימים בחלל.

סיכום

למרות התגברות השיח בנושא חימוש החלל בשנים האחרונות, הדיון האקדמי בתפיסות הנוגעות לחימוש החלל נותר מוגבל ומתמקד בחלוקה פשטנית יחסית בין מתנגדי החימוש לבין תומכיו. לצורך בחינה מחדש של תפיסות אלו, הוצגה במאמר זה חלוקה חדשה של המדינות המעורבות לפי מעמדן הטכנולוגי בחלל. חלוקה זאת מאפשרת לזהות אינטרסים ותפיסות שונות, שאינן עולות בקנה אחד עם החלוקה הקיימת בספרות האקדמית.

מעצמות החלל, המצויות בצמרת ההירכיה הטכנולוגית, מבטאות בפעילותן את תפיסות חימוש החלל ההתקפיות ביותר, וזאת מתוך שאיפה להשיג עליונות (ארצות הברית וסין), או שוויון אסטרטגי (רוסיה); מעצמות הביניים מבטאות אינטרסים שונים, הנעים בין רצון להוביל שיח ביטחוני ונורמטיבי חדש (האיחוד האירופי), לביסוס עוצמה אזורית (הודו), או לשמירה על הביטחון הלאומי באמצעות חיזוק הברית עם ארצות הברית (יפן); קבוצת המדינות המתפתחות מציגה גם היא תפיסות שונות: על אף שהחברות בה תומכות בהגבלת חימוש החלל, מניעיהן לא מתיישבים באופן ברור עם התפיסה האידיאליסטית של מתנגדי החימוש, כפי שבאה לידי ביטוי בספרות המחקר.

72 Harrison et al., *Space Threat Assessment 2018*, p. 38.

מניתוח פעילותן של מדינות שנמצאות פריפריאלית לשיח השולט, נראה כי קיים אצלן מנעד רחב של אינטרסים ותפיסות בשאלת חימוש החלל, המאתגר גם הוא את הספרות הקיימת בנושא זה. על אף השוני בתפיסת חימוש החלל של כל מדינה ומדינה, ניתן לזהות התאמה בין מיקומה על ציר ההישגים הטכנולוגיים ובין מידת נחישותה בסוגיית חימוש החלל.

יכולת מגזרית לניהול סיכוני סייבר בשרשרת האספקה

גבי סיבוני, הדס קליין וזיו סולומון

מאמר זה מציג את סיכוני הסייבר שמקורם בשרשרת האספקה ואת אתגרי ההתמודדות עם סיכונים אלה. המאמר בוחן מספר מתודולוגיות ותקינות בעולם לניהול סיכוני הסייבר בשרשרת האספקה ומציע מודל לניהול מגזרי מרוכז של האתגר באופן שייעל את תהליך בדיקת הספקים והסמכתם. המודל המוצע נמצא כדאי הן מבחינת השקעת המשאבים ואיגומם והן מבחינת העלאת רמת הביטחון הכוללת של המגזרים השונים, וכנגזרת מכך – העלאת רמת המוגנוּת של הסייבר במשק הישראלי כולו.

מילות מפתח: איום הסייבר, ניהול סיכוני סייבר, שרשרת אספקה, מרחב הסייבר

מבוא

בחודש יולי 2018 זיהה צוות מחקר של חברת "מיקרוסופט" מתקפה[1] על חברת תוכנה, שמטרתה הייתה להטמיע קוד זדוני במוצר תוכנה לגיטימי, ובדרך זו להגיע לאלפי לקוחות אחרים. במקרה זה, תוקפים אנונימיים הצליחו להשתלט על תשתית משותפת של חברת תוכנה המספקת עורך מסמכי PDF ושל חברה המספקת לה את חבילת ההתקנה (Installer), באופן שבו ה־Installer יתקין, בנוסף לעורך ה־PDF, גם קוד זדוני. חקירת המקרה העלתה כי בית התוכנה המספק את עורך ה־PDF כלל לא הותקף; המוצר שלו הוחלף באמצעות התערבות בתהליך

פרופ׳ גבי סיבוני הינו ראש תוכנית ביטחון סייבר במכון למחקרי ביטחון לאומי. הדס קליין היא חוקרת סייבר במכון למחקרי ביטחון לאומי. זיו סולומון הוא יועץ בתחום ביטחון סייבר.

המאמר מתבסס על עבודת מחקר שנכתבה על ידי גבי סיבוני, זיו סולומון והדס קליין, **ניהול סיכוני שרשרת אספקה במגזר הפיננסי: צמצום איומים בשרשרת האספקה**, המכון למחקרי ביטחון לאומי, דצמבר 2018.

1 "Attack Inception: Compromised supply chain within a supply chain poses new risks", *Microsoft Defender Research Team*, July 2018, https://bit.ly/2UcVsGB.

הנמצא בבית התוכנה השני – זה המספק את חבילת ההתקנה. דוגמה זו מהווה הוכחה למשאבים הגדולים אותם משקיעים תוקפים כדי להגיע ליעדם דרך שרשרת האספקה.

"שרשרת אספקה" תוגדר כאן כ"מערכת של גורמים המעורבים באספקה של מוצר או שירות, בכלל אלה: נותני שירותים, ספקי תוכנה ומערכות מידע, ספקי חומרה וכדומה". בעידן הגלובלי הנוכחי, המתאפיין במורכבות טכנולוגית של מוצרים ושירותים, תוך הסתייעות במגוון ספקים רחב לכל מוצר או שירות, קיים צורך להבטיח את הגנת הסייבר אצל ספקים של כל ארגון באשר הוא. הדוגמה שהובאה לעיל הינה אחת מני רבות בהן תוקף ניצל פרצות אבטחה אצל ספקים של ארגון במטרה לחדור לרשת המחשוב הארגונית של הארגון שאותו הוא ביקש לתקוף.

התמודדות מיטבית עם אתגרי הסייבר בשרשרת האספקה מחייבת התייחסות קונקרטית לצורכי הארגון והמגזר אליו הוא משתייך, כמו גם התייחסות לארגונים שמזוהים כישראליים מתוקף היותם חשופים לתקיפות על רקע אנטי ישראלי. ארגונים רבים בישראל כפופים להנחיות של רגולטורים, כגון הפיקוח על הבנקים, הפיקוח על חברות הביטוח, משרד הבריאות בהיותו הרגולטור של ארגוני הבריאות השונים בישראל, ועוד. הגנת ארגונים אלה מחייבת מגוון מרכיבים הגנתיים, בהם שכבת הגנה טכנולוגית ונוהלי עבודה, כולל התייחסות לאיומי הסייבר בשרשרת האספקה. ככל שהארגונים יצליחו לזהות את האיומים ולנקוט את האמצעים הנדרשים למיגורם בשלב מוקדם יותר, כך תגדל רמת ההגנה הכוללת שלהם.

מאמר זה מתאר את אתגר ההתמודדות עם סיכוני הסייבר בשרשרת האספקה ומספק המלצות כלליות להתמודדות, תוך התייחסות לתקינה רלוונטית בעולם, לרגולציה בישראל, לניתוח מפת האיומים הרלוונטיים בהקשרי שרשרת האספקה, למתודולוגיות קיימות, למודלים לניהול ספקים בשרשרת האספקה ולגישות אפשריות. המאמר מביא דוגמאות מהמשק הישראלי, שיש להן קשר אפשרי לנושא.

רקע תיאורטי

בתעשייה ובספרות המקצועית קיימים מספר מודלים ומתודולוגיות לניהול סיכונים בשרשרת האספקה. בספר *Purchasing and Supply Chain Management* מתוארות שלוש קטגוריות של ספקים:[2] ספקים אסטרטגיים בעלי חשיבות גבוהה מאוד לחברה הרוכשת, שיֵש קושי רב במציאת תחליף להם; ספקים מועדפים בעלי חשיבות לחברה הרוכשת, אולם ניתן להחליפם תוך השקעת מאמץ מסוים; ספקים בני החלפה, קרי ספקים שניתן להחליפם בתוך זמן קצר. בנוסף לחלוקה המוצעת

2 W.C. Benton, *Purchasing and Supply Management* (Irwin Professional Publishing, 2nd edition, 2009), Ch. 8.

לסוגי ספקים, תובא להלן סקירה של מספר מודלים של ניהול שרשרת אספקה בגופים רלוונטיים לענייננו.

המתודולוגיה הנהוגה בחברת Deutsche Telekom לניהול שרשרת האספקה עבור יותר מ־30,000 הספקים שלה ביותר משמונים מדינות היא מתודולוגיה בת ארבעה שלבים.[3] מטרתה היא למזער את הסיכונים ולעודד את ספקי החברה לשפר את שיטות העבודה שלהם. בשלב הראשון נשאלים כל הספקים הפוטנציאליים עם נפח הזמנה שנתי של יותר מ־100,000 אירו על נושאים כגון זכויות אדם, שחיתות, הגנת הסביבה ובריאות תעסוקתית. כל הספקים מחויבים בבחינה חוזרת לאחר שלוש שנים. ככל שהיחסים העיסקיים נמשכים, החברה מבקשת מהספקים הרלוונטיים מבחינה אסטרטגית ו/או אלה הנמצאים בסיכון גבוה להעביר מידע נרחב על שיטות העבודה שלהם באמצעות מערכות המידע.

בשלב השני מתבצעת הערכה של ההצהרות הללו על בסיס מידע רקע נוסף ומחקר ממוקד. עבור ספקים בעלי סיכון גבוה יותר נדרש מידע נוסף, וכן נערכות ביקורות באתרים שלהם. יעילות הביקורת גוברת, ונמנעת יתירות ביקורות, על ידי שיתוף פעולה עם 13 חברות נוספות, המבצעות את התהליך ב־Joint Audit Cooperation (JAC).

בשלב השלישי מְסווגים הספקים ומוערכים בהתבסס על המידע המתקבל מהם ועל תוצאות הביקורת. לפי Deutsche Telekom, החברה מקיימת שיתוף פעולה הדוק עם הספקים שלה כדי לטפל בבעיות חריפות שזוהו.

בשלב הרביעי מבוצעת תוכנית פיתוח ונערכות סדנאות לספקים. במקרים של התעלמות משמעותית של ספק מדרישות החברה, מתחיל תהליך הסלמה – תהליך שבמסגרתו מערבים גורמים גבוהים יותר בקרב הספק ולעיתים ננקטות סנקציות חריפות יותר, וזאת בכדי לזרז את הטיפול ואת תהליך סגירת הפערים בהתאם לנוהלי Deutsche Telekom.

מסמך של Information Technology Infrastructure Library (ITIL) מציג מודל דו־ממדי לסיווג ספקים[4] – Risk and Impact מול Value and Importance. ככל שהערך של הממדים בקרב ספק מסוים הינו גבוה יותר, כך הספק משמעותי יותר. מודל זה מסווג את הספקים לארבעה סוגים:

- ספקי סחורה רגילה: ספקים המספקים מוצרים ושירותים בעלי ערך נמוך ו / או זמינים (למשל ספקי מחסניות נייר או מדפסת).
- ספקים תפעוליים: ספקים של מוצרים או שירותים תפעוליים. קשרים אלה ינוהלו בדרך כלל על ידי ניהול תפעולי זוטר והם יהיו כרוכים בביקורות בתדירות נמוכה

3 “Corporate Responsibility Report”, *Deutsche Telekom*, 2017.

4 “ITIL Service Management”, Version 3, Ch. 4.7.5.2, https://www.hci-itil.com/ITIL_v3/books/2_service_design/service_design_ch1.html.

אך קבועה של אנשי קשר (למשל, ספק שירותי אירוח אינטרנטי, המספק שטח אירוח לאתר אינטרנט בעל השפעה נמוכה).

- ספקים טקטיים: ספקים שיש עימם פעילות מסחרית משמעותית ואינטראקציה עיסקית. קשרים אלה ינוהלו בדרך כלל על ידי הנהלת הביניים והם יהיו כרוכים בביקורות וסקירות ביצועים קבועות ובתוכניות שיפור מתמשכות (למשל, ספק תחזוקת חומרה המספק פתרון של כשלי חומרת שרתים).
- ספקים אסטרטגיים: ספקים איתם משותף מידע אסטרטגי סודי. קשרים אלה יהיו בדרך כלל באחריות הרמה הניהולית הבכירה וכרוכים בביקורות שוטפות ותכופות (למשל, ספק שירות רשת, המספק שירות רשתות עולמי ותמיכה בהם).

מתודולוגיה המציגה מודל פירמידלי פשוט יותר לסיווג ספקים נמצאת בשימוש על ידי חברת United Utilities[5] – חברה לאספקת מים בצפון־מערב אנגליה, המספקת כ־1,700 מיליון ליטר מים מדי יום. מודל זה מחלק את הספקים לארבעה סוגים: שותף, אסטרטגי, מועדף ומאושר. ככל שהתלות של החברה בספק מורכבת יותר ועלות ערך הסחורה/השירותים גבוהים יותר, כך הספק מוגדר כמשמעותי יותר. המודל מאפשר להגדיר את דרישות החברה מהספק כנגד מדדי ביצוע של לקוחות, רגולציה/משפט, קיימות, יעילות, בטיחות וכדומה.

מתודולוגיה נוספת לסיווג ספקים מופיעה במודל של Amway – Europe Supplier Information Portal.[6] על פי מתודולוגיה זו, סוג היחסים שמתפתח בין ספק ללקוח תלוי בחשיבות האסטרטגית של המוצרים או השירותים המסופקים, ובכישורים, ביכולות ובביצועים של הספק. כל ספק נמדד על פי קריטריונים ומסווג בהתאם, על פי המודל. הדבר מבטיח שכל ספק יקיים פעילויות ממוקדות שתוכננו במיוחד כדי לפתח, לשפר או לייעל ביצועים תפעוליים. הקריטריונים שעל פיהם נמדד כל ספק כוללים מדדי ביצוע (הזמנה, מלאי, אספקה, שירות ובקרת איכות), מוצר/שירות (חדשנות, פיתוח, יתרון שיווקי, ערך כלכלי) ופיננסים (תלות, חלופות, סיכונים פיננסיים ותמחור). הערכת הקריטריונים הללו והתוצאות הנובעות ממנה מובילות לגיבוש תוכניות ספציפיות עם הספק כדי להשיג את רמות הביצועים התפעוליים הנדרשים לצרכים העיסקיים.

בישראל מתקיימות מספר פעילויות לשיפור ההתמודדות עם סיכוני סייבר בשרשרת האספקה. אחת מהן היא פעילות מערך הסייבר הלאומי לפיתוח מתודה להגנה על שרשרת האספקה. מתודה זו כוללת שאלון לספקים, שיטת ביקורת ובקרה והנגשתה באמצעות פורטל. הכוונה היא שהשימוש במתודה ובפורטל יתפתח

---

5 “Suppliers”, *United Utilities,* https://www.unitedutilities.com/corporate/about-us/governance/suppliers.

6 “Supplier Segmentation”, *Europe Supplier Information Portal*, http://supplier.amway.com/europeanportal/suppliersegmentation/SitePages/Home.aspx.

באמצעות כוחות השוק ולא יוטל כחובה על הספקים. לצד זאת מתקיימת פעילות במשרד האוצר – על ידי היחידה להסדרת סייבר ורציפות בשרשרת האספקה הפיננסית,[7] שייעודה הוא להבטיח את חוסן המערכת הפיננסית בפני סיכוני סייבר ורציפות בשרשרת האספקה, לשמור על יציבות המערכת ולעמוד ביעדי השירות לציבור ולממשלה. נכון למועד כתיבת המאמר, פעילות היחידה מול הספקים של המערכת הפיננסית הינה וולונטרית וללא עלות. הפעילות מול הספקים כוללת סקירת פעילותם, מיפוי והערכת סיכונים, מיפוי בקרות קיימות, הערכת הבקרות וגיבוש תוכנית להפחתת הסיכון. יצוין כי פעילות זו מול ספקי המערכת הפיננסית הינה חדשה יחסית, ונמצאת בשלבים מוקדמים שלה.

בנוסף לכך קיימות במספר תחומים במשק הישראלי גישות בעלות קשר אפשרי לנושא של מאמר זה, כמו קטגוריזציה המבוצעת ברמה הלאומית לספקים מענף משקי אחר (סיווג קבלני בניין) ותהליך תשתיתי המבוצע/מונחה ממקום אחד (היחידה הממלכתית לקביעת התאמה ביטחונית בשירות הביטחון הכללי) עבור מועסקים בגופים רבים. זאת ועוד, מערך הסייבר במשרד ראש הממשלה הקים בשלהי 2018 מערכת מידע לאומית,[8] שבאמצעותה יוכל כל ארגון במשק לבדוק את רמת ההגנה שלו בסייבר ואת כשירותו בתחומי אבטחת מידע והגנת הסייבר, ולפי הנתונים שיאסוף – לקבל המלצות כיצד להיערך, לשנות ולשפר. המודול הראשון במערכת, ששמה יוב"ל (יעדים ובקרות לארגון), נועד לטיפול בשרשרת האספקה למשק. המערכת מבוססת על תורת ההגנה לארגונים במשק הישראלי, אותה פרסם מערך הסייבר הלאומי. האתגר שעמד לנגד אנשי המערך בבואם לאפיין את המערכת היה הצורך לגבש מתודולוגיה להגנה על שרשרת האספקה במשק. מטרת היוזמה הייתה העלאת רמת האבטחה במשק הישראלי, לצד התייעלות כלכלית. בעזרת המערכת נבנה מערך אחיד ומסודר של שאלות ובקרות, כאשר המטרה היא ליצור אמון בין ארגונים ובין ספקים במשק.

תקן בין־לאומי נפוץ בתחום אבטחת המידע הינו ISO 27001[9] (שם התקן הישראלי שאומץ הינו "ת"י ISO 27001"). תקן זה עוסק במיסוד מערכת לניהול אבטחת מידע ארגונית ובתהליך השוטף הכרוך בהקמת המערכת ובשיפורה השיטתי. פרק 15 בתקן עוסק בקשרי ספקים. הבקרות בהקשר זה מפורטות בתקן ISO 27002.[10] על פי תקן זה, הארגון נדרש להגדיר מדיניות עבור הספקים,

---

7 "היחידה להסדרת סייבר ורציפות בשרשרת האספקה הפיננסית", *משרד האוצר*, http://mof.gov.il/Units/CyberEmergenciesSafetyDraft/Pages/CyberSeriesUnit.aspx.

8 "מערך הסייבר הקים מערכת להגנה על שרשרת האספקה במשק", **אנשים ומחשבים**, ינואר 2019, https://www.pc.co.il/news/282242/.

9 “Information Technology – Security Techniques – Information Security, Management Systems – Requirements”, *ISO/IEC 27001*, 2013.

10 “Code of practice for information security controls”, *ISO/IEC 27002*, 2013.

שתהיה מוסכמת עליהם וממוסמכת. בנוסף, המדיניות צריכה להתמקד בתהליכים הרלוונטיים המתרחשים הן באתרי הארגון והן באתרי הספק, ובכלל זה: זיהוי סוגי הספקים שהארגון התיר להם גישה למידע; הגדרת מחזור חיים לניהול קשרי ספקים; הגדרת סוגי המידע המותר לגישה לפי סוגי הספקים; תהליכי ניטור ובקרה על הגישה; הגדרת דרישות האבטחה המינימליות לפי סוגי המידע וסוגי הגישה למידע כדי שיהוו בסיס להסכמים המבוצעים מול כל ספק רלוונטי; הגדרת אופן הטיפול באירועי אבטחה ובתקלות הקשורות לספק; הגדרת האחריות של כל צד; העלאת מודעוּת ותרגול עובדים. כמו כן, נדרש להגדיר בהסכם כתוב את דרישות האבטחה לכל ספק שיש לו יכולת לגשת/לעבד/לאחסן/ליצור תקשורת, או לספק מידע או רכיבי טכנולוגיות מידע עבור הארגון. בנוסף, ההסכמים עם הספק צריכים לכלול דרישות אבטחה הנובעות מסיכונים הנוצרים משרשרת האספקה של מוצרים או שירותים. התקן גם מדגיש את הצורך לנהל, לנטר ולהכניס שינויים בכל הקשור לקשרי ספקים ולשרשרת האספקה.

תקן רלוונטי נוסף הינו NIST 800-161[11] – גם הוא תקן מקיף ומפורט, שמטרתו היא לספק מדריך לסוכנויות הפדרליות בארצות הברית בהיבטי זיהוי, הערכה, בחירה והטמעה של תהליכי ניהול סיכונים ובקרות על ניהול סיכוני שרשרת האספקה של טכנולוגיות המידע. התהליכים והבקרות המפורסמים בתקן זה ניתנים לשינוי או להרחבה בגין דרישות רגולטוריות, מדיניות ארגונית, הנחיות וכדומה. התקן מציין כי על הארגונים לפתח אסטרטגיות להפחתת סיכוני שרשרת האספקה של טכנולוגיות המידע, המותאמות ספציפית אליהם והמושפעות ממשימות/צרכים עיסקיים, איומים וסביבות תפעוליות. התקן מדגיש את מורכבות שרשרת האספקה של טכנולוגיית המידע ואת העובדה שלספקים יש ספקים נוספים, ולכן יש קושי לארגון לראות, להבין ולבקר את המצב, קושי שגובר ככל שהספק אינו ספק ישיר שלו. התקן גם מציין כי הטיפול בסיכוני שרשרת האספקה בטכנולוגיית המידע צריך להיות מוטמע בתוך תהליכי ניהול הסיכונים הכלל־ארגוני הרחב. הבקרות המפורטות בתקן מתייחסות לנושאים הבאים: בקרת גישה; מוכנות ותרגול; חיווי ואחריות; הרשאות; ניהול תצורה; המשכיות; זיהוי ואימות; תגובה לאירועים; תחזוקה; הגנה על המדיה; אבטחה פיזית; תכנון; ניהול יישומים; מהימנות עובדים; בקרת שינויים; הערכת סיכונים; רכישת מערכות ושירותים; הגנה על מערכות ותקשורת; שלמות מערכות ומידע.

תקן General Data Protection Regulation (GDPR),[12] שנקבע על ידי הפרלמנט האירופי, מועצת האיחוד האירופי והנציבות האירופית, חל על מדינות האיחוד

11 “Supply Chain Risk Management Practices for Federal Information Systems and Organizations”, *NIST Special Publication 800-161*, April 2015.

12 “GDPR – General Data Protection Regulation”, *The European Parliament*, 2016.

האירופי בכל הנוגע לאיסוף, שמירה והעברה של נתונים אישיים של אנשים פרטיים, וקובע כללים אחידים לשמירה על הפרטיות. התקן התקבל ב־27 באפריל 2016 והוא בר אכיפה החל מ־28 במאי 2018. הוא מחליף את הדירקטיבה האירופית בנוגע להגנה על נתונים (הנחיה EC/95/46) שנקבעה בשנת 1995. התקן חל על כל הארגונים המעבדים נתונים של נושאי מידע בטריטוריה של האיחוד האירופי, גם אם אינם פועלים בטריטוריה של האיחוד. התקן מטיל איסורים ומגבלות על העברת מידע אל מחוץ לשטח האיחוד האירופי בשל החשש להפרות שעלולות להתרחש באזורים בעולם שבהם הפרטיות אינה מוגנת כראוי. אחד העקרונות של התקן הוא אחריותיות (Accountability). במקרים של ארגונים המשתמשים בספקים כמיקור חוץ לעיבוד נתונים אישיים (לדוגמה, הפקת תלושי שכר), עליהם לוודא כי נעשו טיפול אבטחתי נאות והבטחת תאימות לדרישות לאורך כל שרשרת האספקה שלהם, לרבות אצל ספקיהם.

הוראת בנק ישראל־הפיקוח על הבנקים[13] דורשת מהתאגיד הבנקאי לקבוע את הפעולות הנחוצות כדי לוודא שהגורמים החיצוניים נוקטים את האמצעים הנדרשים להפחתת חשיפתו של התאגיד הבנקאי לסיכוני סייבר. ההוראה גם עוסקת באחריות התאגיד הבנקאי לקיום תצורת עבודה מאובטחת מול הספקים החיצוניים, ואת חובותיו לניהול סיכוני סייבר הולמים בפעילותם של ספקים אלה "בחצרותיהם, בחצרי התאגיד הבנקאי" ובממשקים שלהם עם התאגיד. ההוראה מתייחסת לצורך במיפוי וזיהוי "ספקים מהותיים",[14] במתן אפשרות בידי התאגיד הבנקאי לדרוש מהספק לעמוד בהנחיות האבטחה ובשמירת יכולת אכיפה ובקרה של התאגיד הבנקאי מול הספק.

משרד האוצר־אגף שוק ההון, ביטוח וחיסכון פרסם חוזר[15] החל על גופים המנהלים כספים של הציבור, כגון כספי פנסיה וקרנות נאמנות, לרבות חברות ביטוח ובתי השקעות. סעיף ה' בחוזר מתייחס לנושא מיקור חוץ, מפרט את דרישות הגנת הסייבר בהסכמי מיקור חוץ ודורש שהגוף יגדיר נוהל שיפרט את דרישות הגנת הסייבר מול סיכוני מיקור חוץ וביחס לאבטחת שרשרת האספקה. בנוסף לכך, נדרש שייאסר על נותן השירות להעביר לצד שלישי מידע שקיבל במסגרת ההתקשרות, או להשתמש במידע שאליו הוא נחשף אגב ביצוע ההתקשרות לכל מטרה אחרת שלא קשורה לביצוע ההתקשרות. עוד נקבע בחוזר שכאשר קיים

---

13 "ניהול סיכוני סייבר בשרשרת האספקה", *בנק ישראל*, 2018.

14 ההוראה מגדירה את "הספקים המהותיים" כגורמי חוץ הנכללים בשרשרת האספקה של התאגיד הבנקאי (דוגמת חברות התומכות במתן שירותי מסחר בשוק ההון), שהם מהותיים לפעילותו ו/או חושפים אותו לסיכוני סייבר ואבטחת מידע פוטנציאליים גבוהים, שבהתממשותם ניתן לתקוף את התאגיד הבנקאי או לפגוע בפעילותו. הכוונה היא לגורמי חוץ הנותנים שירותים לתאגיד בתחומים הקשורים לטכנולוגיית המידע בלבד.

15 "ניהול סיכוני סייבר בגופים מוסדיים", *משרד האוצר*, אוגוסט 2016.

צורך בהעברת נתונים, יבוצע תהליך של גישה מבוקרת לנתונים פרטניים ולא שכפול של כלל בסיס הנתונים.

תקנות הגנת הפרטיות (אבטחת מידע) של הרשות להגנת הפרטיות (לשעבר רמו"ט), שנכנסו לתוקף במאי 2018,[16] מתבססות על ההנחה שמתן גישה לגורם חיצוני יוצר סיכונים מיוחדים, ולכן מצריך בחינת סיכוני אבטחת המידע האפשריים הכרוכים בהתקשרות עימו. התקנות קובעות שיש לבחון, לפני ביצוע ההתקשרות, סיכוני אבטחת מידע הכרוכים בה, ואם הם גבוהים מדי בהתחשב ברגישות המידע – יש להימנע ממיקור החוץ לחלוטין. כמו כן קובעות התקנות שיֵש להגדיר מהו המידע שהגורם החיצוני רשאי לעבד ולאלו מטרות; לאלו מערכות הוא רשאי לגשת; מהו סוג העיבוד שאותו הוא רשאי לבצע; מהו משך ההתקשרות; מה יהיה אופן השבת המידע לידי הבעלים בסיום ההתקשרות; אופן יישום ההוראות של תקנות אבטחת המידע; חובת הגורם החיצוני להחתים את בעלי ההרשאות שלו על התחייבות לשמור על סודיות המידע.

כפי שעולה מהנאמר לעיל, קיים מגוון רחב של תקינות ורגולציות ברחבי העולם המיועדות לניהול סיכונים כלליים בשרשרת האספקה, דבר שמלמד כי קיימת מודעות גלובלית לנושא זה. במסגרת זו קיימת מוּדעות גם לאיומי הסייבר שמקורם בשרשרת האספקה. איומים אלה מציבים מספר אתגרים המחייבים התייחסות ייחודית.

איומי סייבר וסיכוני שרשרת האספקה

על פי ה־CERT הבריטי, ניתן להבחין בארבעה סוגי איומים על שרשרת האספקה, המבוססים על אירועי אמת:[17] האיום הראשון הינו תקיפת המערכת דרך ספק צד שלישי. באירוע האמת הספציפי התוקף תקף תוכנת מערכת בקרה תעשייתית (Industrial Control System – ICT) המותקנת בארגון באמצעות ספק תוכנה צד שלישי; האיום השני הינו תקיפת אתרי אינטרנט עיסקיים באמצעות עיצוב ובניית אתרים. באירוע האמת הספציפי התוקף תקף אתרי אינטרנט פיננסיים באמצעות סקריפטים שהועברו מחברות דיגיטציה ועיצוב; האיום השלישי הינו תקיפת חברות צד שלישי העוסקות באחסון נתוני חברות. הכוונה הינה למצב שבו חברות רבות מאחסנות את המידע שלהן, לעיתים אף מידע רגיש, אצל חברות צד שלישי, המהוות גם הן יעד לתקיפה ישירה; האיום הרביעי הינו תקיפת Watering hole. הכוונה היא לשתילת קוד עוין באתרים הנמצאים בשימוש נרחב על ידי מושאי

16 "תקנות הגנת הפרטיות (אבטחת מידע) – תקנה 15 – מיקור חוץ", *כנסת ישראל*, מאי 2017.

17 "Cyber-security Risks in the Supply Chain", *Cert UK*, 2015.

התקיפה, כך שהגישה אל אותם אתרים תגרום לתקיפת מערכות המשתמשים שהם מושאי התקיפה.

דוגמאות לאיומים בהקשר האמור מופיעות גם בתקן ISO 27036-1:[18] גישה פיזית של ספק לאתרי הלקוח; גישה למידע או למערכות מידע של הלקוח על ידי עובדי הספק באתרי הלקוח; גישה מרחוק של הספק למידע או למערכות מידע של הלקוח; עיבוד מידע של הלקוח על ידי הספק מחוץ לאתרי הלקוח; הפעלת יישומים של הלקוח על תשתיות הספק; אירוח (Hosting) של ציוד הלקוח באתרי הספק ואחסון נתוני הלקוח (לרבות גיבוי) אצל הספק.

בדוח של חברת מודיעין סייבר, הסוקר תקיפות סייבר משמעותיות שאירעו בשנים 2016–2018 בעולם ובישראל,[19] מצוין כי ארגונים במגזר הפיננסי (בנקים) הינם מטרה מרכזית לתוקפים מיומנים (הן גורמי פשיעה והן תוקפים מדינתיים), וכי מערכות ליבה בנקאיות, כמו Swift ומערכות ATM, הפכו בשנים האחרונות ליעד מועדף לתוקפי סייבר. כמו כן מצוין בדוח כי בעשור האחרון בנו חברות וארגונים מערכי הגנה קדמיים מול שדרת האינטרנט והשקיעו פחות בהגנה על הקישורים שלהם מול ספקים. כך הפכה תקיפת סייבר שמקורה באחת מהחוליות בשרשרת האספקה לשיטה יעילה להשגת אחיזה וחדירה לארגונים אסטרטגיים: התוקפים מנצלים את היכולת הקלה יחסית לחדור לחברות ולארגונים קטנים בעלי מערך הגנת סייבר מוחלש, כדי לחדור דרכם לארגוני יעד בעלי חשיבות קריטית. תוקפים גם מנצלים את העובדה שלחֵלק מספקי המשנה של ארגונים קריטיים יש גישה ישירה או קלה יותר אל הארגון, כדי לבצע חדירה דרכם. התקיפה באמצעות שרשרת האספקה הופכת למתוחכמת יותר, וכוללת שימוש בעדכוני תוכנה לגיטימיים כדי להפיץ נוזקה. מכיוון שארגונים אינם מסוגלים להתמודד עם בדיקה של עדכוני תוכנה, חלה עלייה משמעותית ברמת הסיכון של פגיעה במערכות הליבה של ארגונים ומדינות.

על פי הדוח של חברת מודיעין הסייבר, ניתן להפיק שלוש תובנות עיקריות מהמצב הקיים בכל הנוגע להיבטי ההתמודדות הארגונית עם האיומים:

- **בניית מודל הגנה חדש** – המודל המסורתי, שעיקרו יישום אמצעי אבטחה מוגברים ב"גבולות" הארגון החיצוניים, תוך השארת ליבת הארגון בלתי מוגנת, אינו מתאים יותר. תפיסה זו הביאה בשנים האחרונות לטיפול חסר באבטחת המערכות הפנים־ארגוניות. המצב הנוכחי הוא שארגונים רבים משקיעים מאמצים רבים בהקשחת מעטפת ההגנה שלהם, אך האבטחה הפנים־ארגונית אינה זוכה

18 "Information Technology – Security Techniques – Information Security for Supplier Relationships", *ISO 27036*.

19 "דו"ח אירועי סייבר 2016–2018 – ניצול שרשרת אספקה SWIFT", *CLEARSKY*, מארס 2018.

לתקצוב והשקעה מספקים. חוסר האיזון בהשקעה מביא לכך שכאשר תוקף מצליח לחדור לתוך הארגון, ביכולתו להתפשט בתוכו ולפעול בו בקלות רבה.

- **הקשחה ועיבוי מנגנוני ההגנה בין הארגונים ובין ספקי המשנה שלהם** – קיים קושי רב בהגנה על הקשר בין ארגונים וחברות ובין ספקי משנה המספקים להם שירותים ומידע, קל וחומר כשעוסקים בהגנה על מידע מפני חברות המספקות שירותי מחשוב מבוססי ענן. חלק מספקי המידע במגזר הבנקאי הם גופים בין־לאומיים (לדוגמה, חברת "בלומברג" וחברת "רויטרס"). ברי כי היכולת להשפיע על מערכי הגנת המידע שלהם היא פחותה יחסית. יכולת ההשפעה והשליטה של בנקים ורגולטורים על מערך האבטחה של ספקים בישראל היא גבוהה יותר, אך מחייבת קביעת סטנדרטים ומערכי הגנה ברורים למערכי אבטחת המידע הנדרשים מספקי משנה המתחברים באופן ישיר למערכות הליבה הבנקאיות. במקביל, יש לחזק את מערכי ההגנה ולהקטין ככל האפשר חשיפה לספקי משנה במערכות הפנימיות של הבנקים ושל הגופים הפיננסיים.
- **פריסת מערך הגנה אחורי הדומה במאפייניו למערך ההגנה הקדמי** – מומלץ לבנות מערך ניטור והגנה מול ספקי המשנה, הזהה במאפייניו למערך ההגנה הקדמי של החברה, כולל הקמת מרחב DMZ, מערך הזדהות חזק הכולל הזדהות כפולה, מערך סינון מידע, מערך "ארגזי חול" לבחינת תוצאות של התקנת עדכוני תוכנה, ומערך ניטור הכולל שמירת הנתונים לפרק זמן ארוך וניטור רציף של הַקשר מול ספקי המשנה. מערך הגנה זה אמור להיפרס גם מול החברות הבנות של החברה. העבודה מול החברות הבנות, שלהן מערכי הגנה נפרדים ומערכות תוכנה נפרדות, מסכנת את החברה בדיוק כמו עבודה מול ספק משנה.

מסמך של מערך הסייבר הלאומי בנושא "סיכונים במיקור חוץ ושרשרת אספקה"[20] מפרט את הסיכונים הבאים כסיכונים ייחודיים לשרשרת האספקה: הכנסה של תוכנה או חומרה הנגועה בנוזקה; ביצוע פעולה זדונית על ידי גורם תחזוקה; ביצוע פעולה זדונית באמצעות ערוץ התחזוקה מרחוק. המסמך מציע אמצעים למזעור הסיכון, בכללם: שילוב הסיכון בניהול הסיכונים הארגוני; פיקוח על גורמי התחזוקה – למשל, באמצעות ניטור פעולתם ברשת, ליווי צמוד שלהם בעת שהותם בארגון, הצמדת תג זיהוי לגורם הנכנס, ניטור ערוץ התחזוקה מרחוק וניתוקו בזמנים שאין בו צורך; הסתרת יעד הקצה הספציפי במסגרת רכש עבור ארגונים גדולים – למשל, כאשר רוכשים עבור ארגון גדול מאוד, שרק חלקים ממנו הינם רגישים, ניתן לא לציין בהזמנה למי בדיוק בארגון מיועד הרכש.

מסמך של *SANS Institute* מתייחס להיערכות הנדרשת בארגון נוכח סיכוני הסייבר הנוצרים משרשרת האספקה.[21] המסמך מציע לארגונים לבנות תוכנית

20 "סיכונים במיקור חוץ ושרשרת אספקה", *מערך הסייבר הלאומי*, 18 במאי 2017.
21 "Combatting Cyber Risks in the Supply Chain", *SANS*, 2015.

לניהול ספקים, המבוססת על ארבעה מרכיבים: זיהוי והגדרת הספקים החשובים; הגדרה מדויקת של ההסכמים עבור כל ספק; קביעת הנחיות ובקרות ויישומן; אינטגרציה ארגונית. כמו כן מציע המסמך לארגונים לפעול על פי Best Practices (בהיבטי אנשים, תהליכים וטכנולוגיה) כדי להקטין את חשיפתם לסיכוני שרשרת האספקה. לבסוף מסכם המסמך את המרכיבים העיקריים של התוכנית לאבטחת שרשרת האספקה על פי מרכיבים בסיסיים ומקיפים, בחתך של כל אחד משלושת המרכיבים, כמפורט בטבלה הבאה:

המרכיב	בסיסי	מקיף
אנשים	בדיקות רקע	דרישות אבטחה המופיעות בחוזים
תהליכים	סקרים בסיסיים וסקרי בקרות וסיכונים אצל הספקים	יישום תוכנית מלאה לניהול ספקים
טכנולוגיה	סגמנטציה ברשתות וניטור	Code Review ובדיקת פגיעויות אצל גורמי צד שלישי, ניטור מעמיק, ניתוח איומי אבטחה והתבססות על מודיעין

האיומים על הארגון באמצעות תקיפת שרשרת האספקה שלו יכולים להתבצע באמצעות ערוצי תקיפה מגוונים מאוד, כגון: חדירה למערכות של ספק בעל רמת הגנה נמוכה יחסית (אך בעל גישה למערכות הארגון), ודרכו ביצוע חדירה למערכות הארגון, שימוש בעדכוני תוכנה לגיטימיים להפצת נוזקה וכדומה. אין המדובר באיומים תיאורטיים לארגונים, אלא באיומים המתבססים על מספר רב של אירועים שאירעו בפועל בארץ ובעולם, שמהותם פגיעה בארגונים תוך ניצול שרשרת האספקה שלהם. מורכבות האיום, המגוון הרחב של התרחישים האפשריים והתעצמות התוקפים מחייבים את הארגונים לנקוט צעדים הגנתיים משמעותיים כדי להתמודד עם האתגר ולצמצם את הסיכונים.

לסיכום, הסקירה שהובאה לעיל מלמדת כי קיימת התייחסות רבה לנושא איומי הסייבר בשרשרת האספקה. אולם התייחסות זו אינה יעילה, שכן כל גוף נדרש לקיים את ההנחיות וההמלצות בעצמו ובאופן מבוזר, ובנוסף לכך, כל ספק נדרש לענות על דרישות לקוחותיו בנפרד ולהשקיע משאבים רבים ביישום הדרישות השונות, שמִטֶבע הדברים אינן אחידות.

המודל המוצע

אחד המרכיבים הקריטיים בניהול סיכוני שרשרת האספקה הוא היכולת לסקור את סיכוני הסייבר בקֶרב הספקים ולבנות תוכנית עבודה שתאפשר לסגור פערים באמצעות בקרות מתאימות. ככלל, מאמר זה מבקש להתמקד בגיבוש תהליך רוחבי מגזרי שיאפשר לספקים לקבל הסמכה מגוף בוחן מרכזי. המאמר מתבסס על ההנחה שארגונים המשתייכים לאותו מגזר עיסקי חולקים חלק ניכר מספקיהם (ספקים

משותפים). כך, לדוגמה, מרבית הבנקים בישראל נעזרים באותו ספק הדפסות, אלא שהמצב כיום הוא שכל בנק מבצע סקר עבור אותו ספק הדפסות בנפרד.

המודל המוצע הוא שתהליכי ההסמכה ימומנו על ידי כלל הארגונים הנעזרים בספק, ובכך יתאפשר איגום משאבים והשקעת משאבים גדולים יותר באופן יחסי בכל תהליך ההסמכה. ההסמכה תבוצע על פי מדרגים שונים ועל פי מאפייני הספק ודרישות הארגונים החברים במגזר. באופן זה, הארגונים יישענו על עבודת הגוף הבוחן, ולספקים ייחסכו ביקורות חוזרות ונשנות בכל פעם על ידי גוף אחר. המודל המוצע יכול להוות בסיס בלבד; במידת הצורך, הארגונים השונים יוכלו להעמיק את הדרישות מספקיהם המהותיים בשרשרת האספקה, לדוגמה: הצבת דרישות מחמירות ואף דרישות להתקנה של מערכות ניטור נוספות אצל הספק.

את פעילות סקירת הסיכונים, הנדרשת לביצוע מול הספקים בהיבטי ההתמודדות עם סיכוני הסייבר בשרשרת האספקה, ניתן לבצע באמצעות שתי חלופות תפעוליות עיקריות:

- **ניהול עצמי על ידי כל ארגון במגזר**. זהו למעשה המצב הנוהג כיום, בו כל ארגון פועל באופן עצמאי מול ספקים בשרשרת האספקה שלו. כל ארגון גם קובע את מערכת הדרישות שלו מכל ספק או קבוצת ספקים.
- **ניהול מגזרי מרכזי (עבור כלל/רוב הארגונים במגזר)**. לשם מימוש הדבר, יהיה צורך לבחון הקמת גוף מגזרי מרכזי שיהיה בבעלות משותפת של הגופים הפעילים במגזר. מטרתו של גוף זה תהיה, רובה ככולה, טיפול וניהול סקרי סייבר ומעקב ביצוע בקרב ספקי המגזר. גוף זה יהיה אחראי לנהל את הסוקרים (בין אם בביצוע סקרים באופן ישיר על ידי סוקרים העובדים בגוף ובין אם באמצעות סוקרים חיצוניים), להכתיב את מערכת הדרישות מהסקרים, לנטר ולעקוב אחר יישום תוכניות לתיקון הפערים שיעלו מהסקרים, ולעדכן את מתודולוגיות הבדיקה ואת הכלים שבשימוש על פי צורכי השעה והתפתחות התחום. בנוסף לכך יצטרך הגוף לדון בשאלת הבקרה על ספקים מחו״ל – כיצד ליישם את הבדיקות ואת תהליכי הבקרה גם עליהם. דוגמה לגוף כזה ניתן לראות בחברת מס״ב/שב״א, שהוקמה על ידי הבנקים הגדולים בישראל ומספקת שירותים לכלל המגזר הבנקאי.

מערכת הדרישות תוכל להתבסס על תקינה מקובלת או על הצעת מערך הסייבר הלאומי בישראל לסיווג ספקים. בחינת שתי החלופות נוגעת למספר היבטים עיקריים נוספים:

- **שיפור ביטחון הסייבר המגזרי** – ההיבט הראשון בניתוח נוגע לשאלה: איזו חלופה תגדיל את רמת ביטחון הסייבר והיציבות של המגזר הספציפי? לאור הניתוח שערכנו, התשובה לשאלה זו ברורה. לניהול מרכזי של סקירת ספקים יש יתרונות במגוון היבטים: הקמת גוף מקצועי מתמחה תאפשר לו לפַתח ידע באופן שיטתי ולשפר ולשכלל את יכולותיו עבור כלל המגזר; סקירת ספקים

אחודה תאפשר קביעה של ספי ביטחון סייבר נדרש עבור כלל המגזר, תוך נרמול הדרישות מספקים בשרשרת האספקה, ובכך תסייע משמעותית ליציבות המגזר בהקשר של שרשרת האספקה; הגדלת עוצמת הדרישות של הארגונים במגזר מהספקים תיצור יכולת טובה יותר לכפות מימוש בקרות משופרות, מאחר ודרישות אלו יהיו תוצר של גוף מרכזי; הקטנה משמעותית של העומס על הספקים, המתמודדים כיום עם סקירה ודרישות נפרדות של ארגונים שונים במגזר; ולבסוף, יכולת איגום המשאבים תאפשר הגדלה משמעותית באיכות ובעומק הסקירה, וכתוצאה מכך – ברמת ניהול סיכוני הספקים.

- **ההיבט הכלכלי** – רכיב נוסף אותו ראוי לבחון נוגע להיבטים הכלכליים, להם משמעות לכל מגזר בנפרד. בחינת היבט זה מראה שהקמת יכולת סקירה מרוכזת תוכל להוזיל את עלות המאמץ בכל גוף, ולעומת זאת תגדיל את האפקטיביות של הסקירה לאור ההתמקצעות של הגוף הסוקר במגזר האמור.
- **הגבלים עיסקיים** – היבט נוסף המחייב בחינה נוגע לשאלת ההגבלים העיסקיים. בהקשר זה יש לבחון באיזו מידה פעולה משותפת של הארגונים במגזר למול ספקים בשרשרת האספקה תיצור חריגה מתקנות ההגבלים העיסקיים. בניתוח שערכנו התברר שהקמת גוף סוקר מרכזי אינה מהווה פגיעה בתקנות ההגבלים העיסקיים, וזאת לאור ההבנה שתקנות אלו אמורות לחול על היבטים של תחרות עיסקית, ואילו הקמה של גוף סקירה מרכזי אינה נוגעת במרכיב זה וכל עניינה הוא שיפור רמת הביטחון והיציבות של המגזר הספציפי. בנוסף, בתהליך הסקירה ניתן יהיה לוודא שמידע רגיש של הארגונים אינו משותף לגורמים אחרים – דבר המתרחש כבר כיום, למשל במרכז הסייבר הפיננסי בבאר שבע, כמו גם בארגונים של המערכת הפיננסית בעולם, דוגמת FFIEC ואחרים. ברור שבתהליך הקמתו של הגוף המרכזי נדרש יהיה להסדיר את מגוון המגבלות שיחולו על תהליך הסקירה. להבנתנו, ניתן יהיה ליצור הסְדרה באופן שייתן מענה לדרישות הרגולטורים השונים.
- **פתיחה של ספקים חדשים** – כבר כיום מתמודדים ארגונים שונים עם תהליכים ארוכים הכרוכים בפתיחה של ספקים חדשים במערכת. תהליכים אלה נמשכים חודשים ארוכים מאוד. הפעלה של גוף מרכזי תוכל לאפשר קיצור התהליך ואף ליצור מצב שבו גופים יוכלו לבקש סקירה והסמכה מראש.

מכלל הנאמר לעיל ניתן לראות שהקמת גוף מרכזי תשפר מהותית את רמת ביטחון הסייבר המגזרי ותאפשר פיתוח ידע מתמיד. זאת ועוד, ניהול מרכזי יחזק את השפעתו ועוצמתו של הגוף הסוקר כלפי הספקים (שכן הוא ייצג את כל/רוב הגופים במגזר ולא רק ארגון מסוים), יאפשר התמקצעות טובה של הצוות (גוף מתמחה ברמה המגזרית), יקטין תקורות (תקורות ניהול, תקורות פיזיות וכדומה) עבור כל ארגון ויביא לחיסכון משמעותי של המשאבים הנדרשים בסקירת גורמים

בשרשרת האספקה. יודגש כי האחריות למתקפת סייבר כתוצאה מכשל בשרשרת האספקה תיוותר גם אז בידי הגוף המפעיל את הספק, שכן מטרת המודל המוצע הינה אך ורק לייעל ולשפר את התהליך ואת העלויות הנלוות אליו.

סיכום והמלצות

מכיוון שמבחינה כלכלית ישנה כדאיות מובהקת לנהל סקירות מרכזיות של סיכוני סייבר בשרשרת האספקה, מומלץ שניהול הפעילות יהיה מרכזי. כך גם תגדל השפעתה של הפעילות מול הספקים, מכיוון שהגוף הסוקר ייצג עבורם את דרישות כלל הארגונים החברים במגזר ולא רק דרישות של גוף מסוים. יודגש כי ארגון מסוים יוכל להוסיף דרישות ספציפיות מספק מסוים, במידת הצורך. מוצע כי מנגנון התמחור בין הארגונים החברים במגזר, לצורך הקמתו ותפעולו של הגוף המרכזי, יבוצע באופן דיפרנציאלי, שיבטא את היקף הפעילות של כל ארגון במיזם.

המודל המוצע טומן בחובו גם סיכונים, אותם יהיה צורך לבחון באופן מקיף ולנהל בהתאמה. סיכונים אלה כוללים, בין היתר, פגיעה אפשרית בשוק החברות המספקות סקרי סייבר (ייתכן שחברות יחליטו להפסיק לספק שירותים אלה, שכן יידרשו פחות חברות לאחר בחירת "הגוף הבוחן" בכל מגזר), דבר שיפחית את התחרות בענף; כאשר כל תהליך הסקירה מבוצע על ידי גוף אחד, קיים סיכון שלא כל הליקויים יתגלו. זאת, לעומת מצב שבו קיימים סוקרים שונים, המהווים "עין" נוספת ומגלים לעיתים ליקויים שאינם מתגלים על ידי סוקר מרכזי אחד; סיכון נוסף נוגע לאבטחת רמת המוגנוּת של הגוף המנהל ולחדירה של גורם עוין לגוף הבוחן, חדירה שעלולה במקרה זה לסכן את כל המגזר; לבסוף, קיים סיכון של ניגוד אינטרסים, קרי, במצב שהחברה הבודקת היא גם מתקנת הליקויים. סיכון זה רלוונטי כמובן רק למקרה שבו הגוף המרכזי שיוקם יבחר להפעיל ספקים חיצוניים לביצוע הסקרים מטעמו.

באשר לישראל, מומלץ שמערך הסייבר הלאומי יקיים תהליך עומק של בחינת המודל המוצע. ראוי שראשית התהליך תהיה במיפוי המגזרים הרלוונטיים למודל (קרי, מגזרים שלגביהם מתקיימת ההנחה כי חלק משמעותי מספקיהם הם ספקים משותפים). לאחר מכן כדאי לקיים תהליך של בחינת כדאיות, בדומה למגזר הפיננסי, כפי שהוצג במאמר זה. בשלב הבא אנו ממליצים להגדיר עבור כל מגזר את מערכת הדרישות הרלוונטיות מהספקים השונים ואת תהליכי סקירת הסיכונים.

טכנולוגיה ומודיעין:
מגמות בהשתנות התהליך המודיעיני בצה"ל בתקופה שלאחר מהפכת המידע

יסמין פודמזו

מאמר זה עוסק בשינויים שחלו בעבודת המודיעין בצה"ל בתקופה שלאחר מהפכת המידע של שנות התשעים של המאה העשרים, תוך ניסיון לענות על השאלה: כיצד פיתוחים טכנולוגיים בעולם המודיעין בתקופה שלאחר מהפכה זו הביאו לשיפור התהליך המודיעיני, ובתוכו לשיפור ההתמודדות עם הפתעות מודיעיניות? במאמר מתוארת השפעת הפיתוחים הטכנולוגיים בתקופה שלאחר מהפכת המידע (שני העשורים הראשונים של המאה ה־21) על כל אחד מהשלבים ב"מעגל המודיעין" הקלאסי – איסוף, עיבוד, מחקר והפצה. כמו כן, מבוצע ניתוח השוואתי של התהליכים טרום מהפכת המידע ולאחריה, תוך התבססות על מקורות גלויים. המסקנות העיקריות העולות מן הניתוח הן כי בעקבות השינוי הטכנולוגי מתחוללות שלוש מגמות מרכזיות: אופן עשיית המודיעין הקלאסי משתנה; מתקיים שיפור בהנגשת המודיעין לגורמים המבצעיים; מרחב ההפתעה הולך ומצטמצם.

מילות מפתח: "מעגל המודיעין", טכנולוגיה, מהפכת המידע, נגישות איסופית, שילוביות

מבוא

מהפכת המידע, שתחילתה בעשור האחרון של המאה העשרים, מסתמנת כמהפכה המשמעותית ביותר מאז המהפכה התעשייתית של המאה ה־19, שכמוה השפיעה באופן נרחב על הכלכלה, הפוליטיקה והטכנולוגיה. מאפיינה המרכזי של מהפכת המידע הוא היצף של מידע, נגישות נרחבת אליו וקישוריות מהירה שמאפשרת העברת מידע באופן גלובלי בקבועי זמן קצרים ביותר. כל זאת, על ידי תהליך

יסמין פודמזו היא סטודנטית לתואר שני בתוכנית ללימודי ביטחון באוניברסיטת תל אביב.

אבולוציוני של שינוי וחדשנות, בעיקר בתחום הטכנולוגי. בתקופת מהפכת המידע הבשילו טכנולוגיות מידע (Information Technologies – IT), שהיוו את הבסיס לפיתוחים טכנולוגיים שנוצרו בשנות האלפיים. קשה למתוח קו בין סיום תקופת מהפכת המידע ובין התקופה שבאה אחריה, המהווה עליית מדרגה נוספת בתחום הטכנולוגיה והמידע. מאמר זה יתמקד בשני העשורים הראשונים של המאה ה־21, אשר יוגדרו לצורך זה כ"תקופה שלאחר מהפכת המידע של שנות התשעים".[1]

היום, בתקופה של היצף המידע ומציאות של זירות דינמיות ומשתנות, ניצבים אתגרים חדשים ומורכבים מתמיד בפני עבודת המודיעין הנעשית בגופי המודיעין השונים בארץ ובעולם. חדשנות בתחום הטכנולוגי וניהול חכם ומחושב של המידע הרב והזמין הם קריטיים לבניית תמונת המודיעין הטובה ביותר ומשפיעים, בסופו של דבר, על יכולת ההתמודדות עם האויבים השונים ועל יכולת ההתרעה בנוגע לאירועים חריגים.

תפקידו הקלאסי של המודיעין הוא, בראש ובראשונה, בירור המציאות הקיימת מֵעבר לקווי האויב. לפיכך, ישנה חשיבות רבה למודיעין איכותי ומדויק כדי להתמודד עם שלל סוגי ההפתעות האפשריות בשגרה ובחירום. כיום, התפיסה הרווחת היא כי מודיעין איכותי מהווה מקור כוח בשדה הקרב (לפני ובזמן מלחמה), שלא ניתן לוותר עליו; הוא מתאפשר, בין היתר, הודות לטכנולוגיה המודרנית, היוצרת יכולות מתקדמות של איסוף ועיבוד מידע באופן המאפשר ללמוד את האויב ולצמצם את אי־הוודאות לגביו. עליונות של צד מסוים מושגת, במידה רבה, הודות למודיעין איכותי ומדויק על הנעשה בצד השני. מודיעין מקל על השליטה בשטח ומאפשר למנוע מראש פעולות של האויב. ככל שהמודיעין מדויק יותר, כך הוא מאפשר פעולה ממוקדת יותר נגד האויב, תוך צמצום הפגיעה בבלתי מעורבים. המודיעין משמש גם את מקבלי ההחלטות בדרג המדיני והצבאי ומאפשר שליטה טובה יותר על האירועים טרם התרחשותם ובמהלכם. עם זאת, יש לזכור כי תהליך המודיעין חשוף תמיד לכשלים פוטנציאליים, ובמיוחד כשלים קוגניטיביים, שהינם חלק בלתי נפרד מתהליך החשיבה וקבלת ההחלטות בתנאי אי־ודאות.

מהפכת המידע של שנות התשעים והפיתוחים הטכנולוגיים בעולם המודיעין בתקופה שאחריה יצרו שיפור משמעותי ביכולות של גופי המודיעין השונים לספק מענה לשאלות המחקריות ולבנות תמונה מהימנה ומיטבית של האויב. אחד האתגרים הניצבים בפני המחקר המודיעיני היום הוא מיצוי המידע ופיתוח כלים

1 מקובל לייחס את מהפכת המידע לתקופה של סוף שנות התשעים של המאה העשרים ותחילת שנות האלפיים, כאשר טכנולוגיות שנוצרו אז משפיעות על תהליכים המתרחשים בעולם עד היום. עם זאת, יש הטוענים כי כיום אנו נמצאים כבר בתקופה אחרת, ייתכן אף במהפכה הבאה, המאופיינת בשימוש מוגבר בסייבר ובכלים בלתי מאוישים בשדה הקרב. אפשר שבפרספקטיבה היסטורית העשור הנוכחי יהיה רק שלב במהפכה שתמשיך ללוות אותנו בשנים הבאות.

טכנולוגיים להתמודדות עימו. השפעת המהפכה ניכרת גם בצד השני: האויב אינו שוקט על שמריו ועסוק באופן תמידי באיסוף מודיעין על הצד הראשון ובפיתוח אמצעי הלחימה של המחר. יתרה מכך, האויב לומד את היכולות של מי שעומד מולו ומשנה את אופן התנהלותו בהתאם לכך, כדי להקשות על הצד הראשון באיסוף המודיעין עליו.

מאמר זה מבקש לענות על השאלה: כיצד פיתוחים טכנולוגיים בעולם המודיעין בתקופה שלאחר מהפכת המידע של שנות התשעים הביאו לשיפור התהליך המודיעיני, ובתוכו לשיפור ההתמודדות עם הפתעות מודיעיניות? השאלה תיבחן תוך התבוננות בשינויים שחלו על רקע המהפכה, ובעיקר לאחריה, וכן באבני היסוד המהוות את הבסיס לעבודה המודיעינית: איסוף, עיבוד, מחקר והפצה. בנוסף לכך יתמקד המאמר בשינויים שחלו בצה"ל בתחום המודיעין בשני העשורים האחרונים.

ההתייחסות לכל אחת מאבני היסוד תכלול דוגמאות להשפעת הפיתוחים הטכנולוגיים בתקופה שלאחר מהפכת המידע של שנות התשעים על עבודת המודיעין ועל היכולת של גופי המודיעין לבנות תמונה מלאה ומהימנה, המאפשרת מתן התרעה וזיהוי הפתעות אפשריות. המאמר ינתח מספר מקרי בוחן ויעלה את הטענה כי קיימת השפעה חיובית של הפיתוחים הטכנולוגיים על אופן עבודת המודיעין. לצד זאת יובהר כי עידן היצף המידע מציב אתגרים ב"הפרדת המוץ מהתבן" ומצריך לעיתים התאמות ושינויים ארגוניים כדי לתת את המענה המודיעיני המלא. זאת ועוד, ההתמודדות עם אויב לומד, הממשיך להשתפר באופן תמידי, דורשת גם היא התאמות נכונות.

על העשייה המודיעינית בעידן שלאחר מהפכת המידע

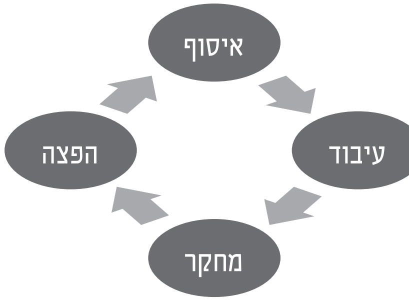
היכולות הטכנולוגיות בתחום המידע נמצאות במגמת צמיחה והתעצמות בתקופה שלאחר מהפכת המידע (מראשית שנות האלפיים ועד היום). היצף המידע, הנגישות והקישוריות המהירה והגלובלית יוצרים אתגרים חדשים. במסגרת זו ניתן לעמוד על שתי מגמות מרכזיות הכרוכות זו בזו: האחת מתייחסת לשינוי שחל באופן שבו נעשה שימוש בטכנולוגיה שמייצרת מידע, ובעקבות זאת – לגידול המעריכי (אקספוננציאלי) בכמות המידע הזמין; המגמה השנייה מתייחסת להתפתחויות הטכנולוגיות בתחום ניתוח המידע, שנוצרו מתוך הצורך לנתח ולעבד כמויות גדולות של מידע בקבועי זמן קצרים.[2]

אחת ההתפתחויות המשמעותיות והמשפיעות בתחום עיבוד המידע מכונה מהפכת נתוני העתק (Big Data). עולם נתוני העתק נוצר מתוך חיבור של מספר

2 סא"ל צ', "נגזרות מודיעיניות של עולם הביג דאטה", בתוך: יוסי קופרווסר ודודי סימן טוב (עורכים), **מודיעין הלכה ומעשה: ביג דאטה ומודיעין**, המרכז למורשת המודיעין, רמת השרון 2018, עמ' 24–32.

התפתחויות טכנולוגיות שהתרחשו במקביל: ראשית, שיפור ביכולת האיסוף של כמויות מידע גדולות על ידי מגוון רחב של חיישנים, ובעקבות זאת הגדלת נפחי אחסון הנתונים במטרה לאגור את כל החומר שנאסף; שנית, גידול עצום בכמות המידע בעולם, הנובע משימוש הולך וגובר בטכנולוגיות המשאירות חתימה דיגיטלית; שלישית, שיפור ביכולות החישוב, המאפשרות התמודדות עם כמויות מידע גדולות וניתוחן במהירות ואף במקביל.[3]

על פי תפיסת המודיעין הישנה, ישנם מספר שלבי יסוד בתהליך המודיעיני, המכונה "מעגל המודיעין": איסוף המידע, עיבוד החומר, מחקר והפצת התוצר המודיעיני המעובד לצרכנים. השלבים חוזרים על עצמם באופן מעגלי ומוכוונים על ידי הצי"ח (ציון ידיעות חשובות), או במילים אחרות – על ידי שאלות המחקר שנדרש לתת עליהן מענה. התהליך מתחיל בשליחת שאלות הצי"ח על ידי גורמי המחקר לגורמי האיסוף, וממשיך בגורמי האיסוף שעושים את עבודתם כדי להביא את המידע הדרוש. בשלב הבא החומר הגולמי עובר תהליך של עיבוד, ולבסוף הוא מופץ לצרכנים, וחוזר חלילה.



בהסתכלות על השפעת מהפכת המידע על "מעגל המודיעין" הקלאסי ניתן לראות שינויים בכל אחת מאבני היסוד של המודיעין: המגמה הבולטת בתחום **איסוף המודיעין** היא הגידול והשיפור ביכולות הסייבר, המהווה את ממד הלוחמה החדש ביותר. בעידן הדיגיטלי ניתן להמיר סוגי מידע רבים לביטים, שמתחברים לרשתות מידע שונות. בעולם כזה, שבו הכול מחובר ונמצא ברשת, משתנות הנחות יסוד של העבודה המודיעינית בתחום המידע והידע. כמות המידע הזמין היום לאנשי המודיעין יוצרת אתגר חדש בתחום מיצוי המידע: סינון המידע הרלוונטי למענה על שאלות המחקר. זאת ועוד, בעידן הדיגיטלי יש לאנשי המודיעין נגישות

3 מ' – סגן מנהל בית הספר למודיעין של שירות הביטחון הכללי, "מלאכים בשמי ברלין – שאלות מודיעיניות חדשות בעולם רווי נתונים", בתוך: קופרווסר וסימן טוב (עורכים), **מודיעין הלכה ומעשה: ביג דאטה ומודיעין**, עמ' 55–60.

איסופית פוטנציאלית, כמעט אין־סופית, למידע, והם נדרשים למיומנויות חדשות ב"כרייתו".

ארגוני המודיעין מוצפים היום במידע, הן מחיישנים שונים הפרוסים במרחבי העניין והן מנגישות למאגרי מידע בממד הסייבר המתמלאים ומתחדשים ללא הפסקה. במקומות שבהם הנגישות למידע מורכבת בשל מעטפות אבטחה והצפנות, תפקיד גורמי האיסוף הוא לפתח כלי סייבר שינצלו את פרצות האבטחה והחולשות בצד השני.

האתגר המרכזי הוא בהתמודדות עם אחסון נפחי מידע גדולים הנובעים מהגידול המעריכי בכמות המידע – דבר הכרוך בעלויות לא מבוטלות. כתוצאה מכך הוחלט באמ"ן, למשל, להפסיק הכנסה של חומרים מודיעיניים מסוימים למאגרים, על אף המשאבים והסיכון שהושקעו בהשגתם, ולהגביל את משך זמן שמירתם לתקופות מסוימות בלבד. שיטה זו מציבה אתגרים בפני החוקרים, משום שהיכולת שלהם לשאול שאלות מודיעיניות שמתבססות על תהליכי למידה לאורך זמן מצטמצמת מאוד.[4]

תחום איסוף ההולך ומתפתח בעשורים האחרונים, בנוסף לסייבר, הוא תחום הלוויינות. יכולות הלוויינות מאפשרות הבאת תצלומים מכל רחבי העולם באמצעות מערכות אופטיות מתקדמות, ובכך הן מסייעות במחקר המודיעיני על אתרי עניין מרוחקים. פיתוחים טכנולוגיים בתחום הצילום והאופטיקה מביאים לתוצרים איכותיים וברזולוציות גבוהות ומשרתים את גורמי הפענוח בניתוח השטח.

בתחום האיסוף החזותי מבוסס הלוויינים, מהפכת המידע אפשרה את המעבר מהעידן האנלוגי לעידן הדיגיטלי. העידן האנלוגי אופיין במחסור בחומרי גלם (הדמאות)[5] ובתהליך עיבוד ידני ארוך, בעוד שהעידן הדיגיטלי (החל משנות התשעים של המאה העשרים) הביא לקפיצת מדרגה מבחינת כמות חומרי הגלם ואיכותם. כיום יש שפע של צילומי לוויין ברזולוציות שהולכות ומשתפרות, באורכי גל שונים (מולטי־ספקטרליים ומכ"מיים) ובספיקת שטח גדולה.[6] לוויינים מולטי־ספקטרליים, למשל, מסייעים במתן מענה לצי"חים מודיעיניים מורכבים, כאשר הם מסייעים למחקר על אויב המנסה לשמור על חתימה נמוכה, וגם על מרחבים מורכבים, מרובי צמחיה או עירוניים. לדוגמה, צילום באורכי גל שונים מאפשר להצביע על מצבור מתכות הנמצא תחת מעטה של צמחיה ולאתר אתרי שיגור

4 סא"ל צ', "נגזרות מודיעיניות של עולם הביג דאטה", בתוך: קופרווסר וסימן טוב (עורכים), **מודיעין הלכה ומעשה: ביג דאטה ומודיעין**, עמ' 27–28.

5 הדמאה הינה ייצוג ויזואלי של תמונה, המתקבל באמצעות שיטות, כלים וסוגי מדידות שונים שאינם בהכרח אופטיים, כלומר אינם בהכרח מבוססים על אור נראה.

6 סא"ל א', "מודיעין גיאוגרפי – ממפת הנייר ל'גיאו־רשת'", בתוך: שמואל אבן ודוד סימן טוב (עורכים), **אתגרי קהילת המודיעין בישראל**, המכון למחקרי ביטחון לאומי, תל אביב 2017, עמ' 99.

מוסתרים בסביבה מיוערת. סוג נוסף של לוויינים, שנעשה בהם שימוש במודיעין, הוא לוויני מכ"ם (Synthetic Aperture Radar – SAR), המתבססים על שידור מבוקר של קרינה אלקטרו־מגנטית. יתרונם המרכזי של מכ"מים אלה הוא היכולת להפיק תמונות של שטח נתון בכל שעה, בכל תנאֵי ראות ובכל תנאי מזג אוויר.[7]

בשנים האחרונות הולך החלל ומתמלא בלוויינים, ומספרם היום גבוה כמעט פי 2.5 משהָיה לפני שני עשורים.[8] כלל המידע הנאסף מהלוויינים מגיע אל סוכנויות האיסוף בהתאם לצי"ח, ובעזרת אפליקציות גיאוגרפיות הוא מונגש ישירות לחוקרי המודיעין, שיכולים להסתייע בחומר בעצמם וללא תיווך של גופי הפענוח המקצועיים. מדובר ברובד נוסף, המדגיש את הצורך בשילוביות בין גופי המודיעין (שתידון בהמשך).

נדבך נוסף באיסוף החזותי נוגע לשימוש ההולך וגובר בכלי טיס בלתי מאוישים לצורכי איסוף מודיעין. בעשור האחרון ישנה מגמת עלייה בשימוש מסיבי בכטב"מים מסוגים שונים לסיוע לדרגי השטח במשימותיהם. הדבר בא לידי ביטוי בהפעלת כטב"מים המצוידים בחיישנים איכותיים, שמסוגלים לשהות באוויר שעות ארוכות ולסייע בחיבור תמונת המצב בשטח בזמן אמת, הן לאנשי המודיעין העוסקים בהפללת מטרות והן לגורמי הפעלת הכוח לצורך "סגירת מעגל" על מטרות בזמן הקצר ביותר. בנוסף, גובר השימוש בכטב"מים קטנים וברחפנים לצורך ביצוע משימות איסוף טקטיות וסיוע לכוחות בשטח במהלך לחימה. הנגישות לטכנולוגיות מתקדמות, המשולבת עם מחירי ייצור נמוכים, מאפשרת ייצור נרחב של כלי טיס בלתי מאוישים מסוגים שונים, כולל רחפנים מסחריים. בעקבות כך, השימוש בכלים אלה הופך לזמין עבור מדינות רבות בעולם, ואף עבור גורמים צבאיים שאינם מדינתיים.[9]

בהיבט **העיבוד והמחקר** המודיעיני, הסייבר יצר במובן מסוים מרחב מודיעיני משותף, שבו גורמי האיסוף, כמו גם גורמי המחקר, חולקים מיומנויות עבודה משותפות. פיתוחים טכנולוגיים באמ"ן בשנים האחרונות יצרו את "שולחן העבודה החדש של הקמ"ן", הכולל אפליקציות שנועדו ליצור מרחב עבודה רשתי בקהילת המודיעין. דוגמה לכך היא מערכת "טרייסבוק", אליה מועלות תמציות גולמיות של ידיעות מודיעיניות על ידי אנשי האיסוף העוסקים בעיבוד המידע, בטרם אלו

7 עמי רוחקס דומבה, "לראות הכל, מכל מקום, בכל זמן", *IsraelDefense*, 29 בנובמבר 2014, https://www.israeldefense.co.il/he/content/לראות־הכל־מכל־מקום־בכל־זמן.

8 הרצי הלוי, "'אמ"ן 2048 – עליונות מודיעינית בעידן הדיגיטלי", **מערכות**, גיליון 477, 2018, עמ' 28–29.

9 לירן ענתבי, "העין הפקוחה בשמים – יתרונות ואתגרים בשימוש בכטב"מים לאיסוף מודיעין", בתוך: אבן וסימן טוב (עורכים), **אתגרי קהילת המודיעין בישראל**, עמ' 113–120.

הופקו באופן מלא על פי תו התקן של יחידה 8200 (יחידת האיסוף המרכזית של אגף המודיעין בצה"ל).[10]

פיתוחים טכנולוגיים נוספים, שנוצרו מתוך הצורך להתמודד עם נתוני העתק, כוללים בין השאר טכנולוגיות לזיהוי אוטומטי של תמונה או להמרת דיבור לטקסט (Speech to Text – STT), וישנה אף מגמה של תחילת שימוש בהם בגופי המודיעין. כיום קיימות במגזר האזרחי טכנולוגיות המסוגלות להמיר קבצי שמע לקבצי טקסט על פי מודלים של הבנת שפה טבעית. חברות כמו "גוגל", IBM ואפילו "ורביט" (Verbit) הישראלית פיתחו מנועי תמלול, המאפשרים לחסוך שעות עבודה רבות של העברת שיחות מוקלטות אל הכתב.[11] שימוש בטכנולוגיות המרת דיבור לטקסט על ידי גופי המודיעין עשוי להביא למהפכה מבחינת נפח השמע המתורגם בזמן נתון ולייצר מנגנוני התרעה על פי שאילתות שהוגדרו מראש בהתאם לצי"ח הרלוונטי.

פיתוחים נוספים של שיטות עיבוד מידע ניתן לראות בעולם המודיעין החזותי, שבו המעבר מהעידן האנלוגי לעידן הדיגיטלי הביא לקיצור זמני ההפקה של המודיעין, לפיתוח יכולות היתוך מידע בין דיסציפלינות מודיעיניות שונות ולפיתוח אפליקציות להצגה ויזואלית של שכבות מידע גיאוגרפיות. יכולות אלו אפשרו, למשל, שילוב של מידע מהדמאה אופטית עם מידע מהדמאת מכ"ם ושכבות מידע של תשתיות בשטח. כל אלה שיפרו באופן ניכר את יכולות סגירת המעגל מִשלב האיסוף לשלב התקיפה בזמן אמת ואת תהליכי ייצור המטרות בכלל.[12]

התקדמות נוספת בעיבוד המידע החזותי באה לידי ביטוי בתחומי הראייה הממוחשבת ולמידת המכונה (Machine learning), המאפשרות לזהות עצמים, לגלות שינויים בשטח ולאתר תבניות של תופעות באופן ממוחשב. שימוש באלגוריתמים להשוואת תמונות וזיהוי אוטומטי של שינויים בתשתית ובתכסית, המופעלים על כמויות גדולות של הדמאות, עשויים לחסוך לגופי המודיעין שעות פענוח רבות ולסייע בניתוח כמויות גדולות של חומר בזמן הקצר ביותר. ייתכן כי אלגוריתמים כאלה יוכלו בעתיד לשמש ככלי להתרעה על אירועים מודיעיניים חזותיים.

התפתחויות ביכולות הטכנולוגיות חלו בתחום **הפצת** המודיעין, והן משפרות באופן ניכר את הנגשת המודיעין לדרגי השטח. אחד הלקחים ממלחמת לבנון השנייה (2006) היה שתוצרים מודיעיניים שיועדו לשימוש כוחות השדה לא הגיעו ליעדיהם, בין השאר בשל מידור[13] גבוה מדי של המידע. התפתחויות טכנולוגיות

---

10 אור גליק, "החומות לא נשברו – הסיפור של טרייסבוק", **בין הקטבים**, גיליון 18, 2018, עמ' 164־165.

11 אהוד מקסימוב, "אוצר מילים: האם נמצא הפתרון האולטימטיבי לתמלול?", **מקור ראשון**, 19 באוגוסט 2018, https://www.makorrishon.co.il/magazine/70017/.

12 סא"ל א', "מודיעין גיאוגרפי – ממפת הנייר ל'גיאו־רשת'", בתוך: אבן וסימן טוב (עורכים), **אתגרי קהילת המודיעין בישראל**, עמ' 98–99.

13 מידור הינו מניעת חשיפה של גורמים מסוימים למידע מטעמי אבטחת מידע.

מאז שנות התשעים הביאו לשיפור משמעותי ביכולת הנגשת המודיעין לכוחות הלוחמים בשטח, על ידי שיתוף פעולה בין אמ"ן ובין זרוע היבשה.

שינוי נוסף הנוגע להפצת המודיעין הוא התפתחותה בשנים האחרונות של תפיסת הלוחמ"ם – לוחמה מבוססת מודיעין – בצה"ל. במרכזה של תפיסה זו עומד הצורך לספק מודיעין רלוונטי לגורמי השטח כדי ליצור יכולת תמרון אפקטיבי ויעיל יותר. תהליך הנגשת המודיעין ללוחמים בשדה הקרב כָּלל פיתוח מערכות של חיישנים לאיסוף מודיעין בזמן אמת ודרש התאמה של רמות סיווג המידע כדי להקל על הפצתו. התפיסה התפתחה מתוך הבנה כי האויב השתנה וכי צה"ל נדרש להתמודד עם ארגוני טרור תת־מדינתיים, השונים משמעותית בפעולתם מצבאות מדינתיים. בעקבות כך החל פיתוח של מערכות שליטה ובקרה דיגיטליות, שנכנסו בהמשך לשימוש בצה"ל, כמו למשל פרויקט צי"ד (צבא יבשה דיגיטלי) בזרוע היבשה. בנוסף לכך, הוקמו ענפי לוחמת רשת, שנועדו לממש את החזון של הלחימה הרשתית והתאמתו ליכולות ולאתגרים החדשים.[14]

פרויקט צי"ד יצא לדרך בתחילת שנות האלפיים ובמסגרתו פיתחה חברת "אלביט" מערכות שליטה ובקרה לכל צבא היבשה.[15] המערכות שפותחו מחברות את גורמי איסוף המודיעין אל דרגי הפיקוד ואל אמצעי האש והתקיפה על בסיס רשת של סיבים ותקשורת אלחוטית מוצפנת. הפרויקט כולל, בין השאר, מערכות וידאו, מערכות לניהול שדה הקרב על מפות ממוחשבות, ותמונת מודיעין מקיפה ורלוונטית, שבזכות המערכת מגיעה לגורמי השטח בזמן שיא. למערכת תצורות נייחות וניידות, ואחד היתרונות שלה הוא חסינותה לחסימות, כך שכאשר קיימת חסימה, כלל המידע שמאוחסן על המערכת באותה עת נשמר.

דוגמה לפיתוח טכנולוגי המאפשר את הנגשת המודיעין לכוחות הלוחמים ניתן לראות במערכת של מִשקפי מציאות רבודה, שפותחה ביחידה 9900[16] ומספקת ללוחם מידע גיאוגרפי על תוואי השטח ופעילות האויב.[17] המערכת מבוססת על מוצר מדף של חברת Oculus, המייצרת מסכות עבור גיימרים, שנעשו בה התאמות לצורכי צה"ל. הרעיון המרכזי שעומד בבסיס המערכת הוא שילוב מרב המידע הקיים מכלל גופי האיסוף והנגשתו ללוחמים. באמצעות משקפי המציאות הרבודה ניתן לסמן את המטרות, להעביר מידע בזמן אמת על שיגורים רקטיים ולהסתכל "פנימה" לתוך מבנים. האתגר המרכזי שהמערכת מנסה לתת לו מענה

---

14 גבי סיבוני ושגיא בן־יעקב, "לוחמת יבשה מוכוונת מודיעין", בתוך: אבן וסימן טוב (עורכים), **אתגרי קהילת המודיעין בישראל**, עמ' 78.

15 פריסת המערכת ברוב עוצבות היבשה בצה"ל הסתיימה בשנת 2014.

16 יחידה 9900 היא יחידה באגף המודיעין העוסקת במודיעין חזותי.

17 ענבל אורפז, "מהאנשים שהביאו לכם את 8200: הכירו את 9900 – האחות הקטנה והשאפתנית", *The Marker*, 31 במארס 2015, https://www.themarker.com/technation/1.2603595.

הוא עודף מידע. התוצר הסופי שמשתקף במערכת הוא תוצר מעובד, הרלוונטי לביצוע משימה מסוימת, בין אם באימון ובין אם במשימה מבצעית.

על אף התמקדותו של מאמר זה בשינויים שחלו בכל אחד משלבי "מעגל המודיעין" בזירה הישראלית, לא ניתן להתעלם מתהליכים דומים המתרחשים בזירה הבין־לאומית. ישראל וצה"ל הם מקרה בוחן בודד בתוך תהליך רחב בהרבה של השפעת הטכנולוגיה על תהליכים מודיעיניים, הנותן את אותותיו מאז תחילת המאה ה־21 במדינות ובצבאות אחרים בעולם, דוגמת ארצות הברית, בריטניה, סין ועוד. הספר *Technology and the Intelligence Community*, למשל, עורך ניתוח של השפעת הפיתוחים הטכנולוגיים על שלבי המודיעין השונים, כפי שהם באים לידי ביטוי בקהילת המודיעין האמריקאית.[18]

שאלה נוספת העולה על הפרק עוסקת במקור לאותם פיתוחים טכנולוגיים שנעשה בהם שימוש בסביבה הצבאית ומשפיעים על התהליך המודיעיני. בהסתכלות רחבה יותר על סוגיה זו ניתן לראות כי בהרבה מקרים מקורם של הפיתוחים הטכנולוגיים הוא בסביבה האזרחית, המובילה מבחינת התחדשות טכנולוגית ומספקת השראה לסביבה הצבאית בהטמעת הטכנולוגיות בתוכה. דוגמאות לכך הם השימוש בכלים המבוססים על מנוע החיפוש של חברת "גוגל" לצורך שליפת מידע ממאגרי יחידה 8200; פיתוח אפליקציות לשימוש חוקרי המודיעין, המבוססות על אתרים אזרחיים (דוגמת "טרייסבוק" שהוצגה לעיל); שימוש בפיתוחים טכנולוגיים של חברות אזרחיות לצורכי הצבא (דוגמת מִשקפי המציאות הרבודה של חברת Oculus). הטכנולוגיות המתקדמות המוטמעות בצבא מביאות לקפיצת מדרגה משמעותית בתמיכה שהן מספקות, בסופו של דבר, לגורמי המודיעין, כמו גם לדרגי השטח.[19]

תחילתה של פרדיגמה חדשה בעבודת המודיעין

התקופה שלאחר מהפכת המידע יצרה את היסוד לפיתוח פרדיגמה חדשה בעבודת המודיעין, אשר נבעה, בין השאר, מהשימוש המוגבר בכלי סייבר.[20] בשנים האחרונות חלו שינויים בתפקידים הקלאסיים של גורמי האיסוף והמחקר, שנבעו מכניסת טכנולוגיות חדשות, שמצידן הביאו לטשטוש ההבדל בין השניים. המצב החדש

18 Margaret E. Kosal, ed., *Technology and the Intelligence Community: Challenges and Advances for the 21st Century* (Springer, 2018).

19 Florin-Eduard Grosaru, "The Revolution in Military Affairs in Information Age and its Impact on Defense Resources Management Performance", Conference Proceedings of eLearning and Software for Education (eLSE) no. 1 (Bucharest, April 2015), pp. 445-452.

20 דודי סימן טוב ונעם אלון, "הסייבר מחייב ומאפשר מהפכה בענייני מודיעין", **סייבר, מודיעין וביטחון**, כרך 2, גיליון 1, אפריל 2018, עמ' 67–68.

ערער את "מעגל המודיעין" הקלאסי והעלה את הצורך בצורה חדשה של התמודדות עם המציאות. הדבר עולה בקנה אחד עם התיאוריה שהציגו בשנות התשעים אנדרו מרשל וריצ'רד הנדלי, שעסקו במהפכות בעניינים צבאיים וטענו כי אין בטכנולוגיות לבדן כדי להביא למהפכה, אלא יש צורך גם בהתאמות ובשינויים ארגוניים כדי שזו תתקיים.[21]

המושג "שילוביות" מתאר תהליכי שינוי ארגוני שמתרחשים בגופי המודיעין, הנוצרים מתוך שיתופי פעולה בין מסגרות מובחנות. כך נלקחים היתרונות של כל מסגרת ארגונית ומותכים לכדי יחידה ארגונית חדשה, העולה ביכולותיה על כל אחת מהמסגרות הנפרדות.[22] סוגיה הכרוכה בכך היא העובדה שכל ארגון חייב לרכוש ולפתח את הידע לעצמו, אך בפועל הרבה ממנו נמצא בתווך שבין הארגונים. הדבר מחייב גישור, האמור להיעשות באמצעות קשרים ושיתופי פעולה, אלא ששיתופי הפעולה לא תמיד מתקיימים, בין השאר מתוך רצון של הארגון לשמור לעצמו על הייחודיות והיוקרה שלו.

פיגועי 11 בספטמבר 2001 בארצות הברית יכולים להוות דוגמה לכך. המסקנה המרכזית מתחקיר ועדת החקירה של האירועים הייתה שלא היה מחסור במידע שיכול היה להביא לסיכול המתקפה; הבעיה הייתה בכך שאף אחד מגופי המודיעין בארצות הברית לא החזיק בתמונה המלאה, ואוסף פריטי המידע שבאמצעותם ניתן היה לבנות את תמונת המודיעין המלאה ולהתריע באופן ממוקד על כוונות ארגון הטרור "אל־קאעידה" היה מפוזר בין גופי מודיעין שונים. אותם גופים לא שיתפו ביניהם את המידע בשל חוסר שיתוף פעולה ארוך שנים ומידור שלא לצורך.

המובילה בתחום השילוביות כיום היא ארצות הברית, שהרעיון המכונה "Jointness" התפתח בה עוד בסוף שנות השבעים של המאה העשרים. רעיון זה מתייחס לפעולות ולמבצעים שבהם השתתפו יותר משתי זרועות צבאיות. אירועי 11 בספטמבר 2001 הביאו להקמתה בארצות הברית של הפונקציה "מנהל המודיעין הלאומי" (Director of National Intelligence – DNI), שהיוותה מעֵין מסגרת לניהול קהילת המודיעין האמריקאית. ל־DNI ניתנו סמכויות לגיבוש מדיניות המודיעין של ארצות הברית, להמליץ על מינויי בכירים בקהילת המודיעין האמריקאית ולהקים צוותים משותפים לשירותי המודיעין במדינה. הרעיון הבסיסי

21 Richard O. Hundley, *Past Revolution Future Transformation* (Washington D.C: RAND, 1999), pp. 1-17; Andrew W. Marshall, "Some Thoughts on Military Revolutions", Memorandum for the Record, OSD Office of Net Assessment, July 27, 1993.

22 קובי מיכאל, דודי סימן טוב ואורן יואלי, "התפתחות תפיסת השילוביות בארגוני מודיעין", בתוך: יוסי קופרווסר ודודי סימן טוב (עורכים), **מודיעין הלכה ומעשה: השילוביות במודיעין**, המרכז למורשת המודיעין, רמת השרון 2016, עמ' 6.

שמאחורי ה־DNI היה להגביר את השילוביות ולקדם שיתופי פעולה וסנכרון בין גופי המודיעין השונים כדי למנוע אירועים דומים לפיגועי 11 בספטמבר.[23]

מבט לעתיד על טכנולוגיות מתקדמות

כיום הולך ומתפתח עולם ה־Internet of Things (IOT), שבו מתאפשרת תקשורת מתקדמת בין אובייקטים שמשולבים בהם רכיבי אלקטרוניקה, תוכנה, חיישנים ומצלמות. ה־IOT מתאר עולם שבו אובייקטים יומיומיים מצוידים במחשבים זעירים, המסוגלים לנטר את סביבתם, להציג מידע ולבצע פעולות במידה מסוימת של עצמאות. התקשורת בין האובייקטים יוצרת הזדמנויות לאיסוף מידע דרך גישה לרשתות אליהן מחוברים האובייקטים.[24]

נראה כי בשנים הבאות תלך ותתעצם הקישוריות ותצמח יכולת הניטור והנגישות למידע בעולם, באופן שבו ניתן יהיה לדעת כמעט בכל רגע נתון מה קורה בכל נקודת עניין. בעקבות זאת, תחום ה־IOT יעשה קפיצת מדרגה משמעותית וידרוש שינוי בשיטות הניתוח, העיבוד והאחסון של המידע. מציאות כזו תשרת את גופי המודיעין ותיצור הזדמנויות איסופיות חסרות תקדים על ידי פיתוח הנגישויות המתאימות. הנגשת המידע מְרכיבי ה־IOT גם תיצור דיסציפלינה מודיעינית חדשה ותאפשר לחוקרי המודיעין לקבל מידע שישלים את תמונת המודיעין שהתקבלה מדיסציפלינות המודיעין האחרות.

איסוף בעולם ה־IOT יוכל לספק, למשל, מידע אינטימי על יעדים אנושיים מסוימים באמצעות חיבור לרשתות המקושרות ליעד, לדוגמה, באמצעות שעון או טלפון חכם שהוא נושא עימו. באופן זה אפשר יהיה ללמוד על שגרת הפעילות של אותו אדם ולהשתמש, במידת הצורך, במידע זה ככלי מפליל ומסייע במבצעי סיכול. ניתן להתחבר גם למכשירים, כמו טלוויזיות חכמות היכולות לקלוט ולשדר את מה שנעשה בקרבתן, וזאת כדי להאזין למה שקורה בחדר שלא הייתה אליו נגישות קודם לכן. בנוסף, ניתן יהיה להשיג מידע חזותי על יעדים מרוחקים ברחבי העולם לא רק באמצעות הדמאות לוויין איכותיות, אלא גם, למשל, על ידי חיבור באמצעות הסייבר למצלמות אבטחה באתר מסוים.

ניתוח השינויים

לאור הנאמר לעיל, ניכר כי העשייה המודיעינית לאחר מהפכת המידע משַנה את פניה. מכאן עולה השאלה האם עידן היצף המידע מסייע בהתמודדות של גופי

23 קובי מיכאל, דודי סימן טוב ואורן יואלי, "שילוביות בארגוני מודיעין – משמעויות תיאורטיות במבחן המעשה", **סייבר, מודיעין וביטחון**, כרך 1, גיליון 1, ינואר 2017, עמ' 5–28.

24 טל שטיינהרץ, "Internet of Things – הגנה בסייבר בעולם ה'אינטרנט של הדברים'", *IsraelDefense*, 23 במאי 2015, https://www.israeldefense.co.il/he/content/internet-things–הגנה־בסייבר־בעולם־ה־'אינטרנט־של־הדברים.

המודיעין עם הפתעות מודיעיניות אפשריות, או שמא דווקא מקשה על "ברירת המוץ מן התבן" ועל זיהוי פריטי המידע הרומזים להפתעה הבאה? במלחמת יום הכיפורים, למשל, נתפס צה"ל לא מוכן אל מול השימוש המצרי בטילי נ"ט ונ"מ מתקדמים. הייתה זו הפתעה טכנולוגית שעלתה לצה"ל באבדות בנפש ובאובדן תשתיות ואמצעים. אחד הטילים שהמצרים עשו בהם שימוש אז היה ה"סאגר" הסובייטי. למרות המידע שהיה ידוע על טיל זה באותה עת, נשמרו הדברים באמ"ן ברמת סיווג גבוהה ולא הגיעו לגופי בניין הכוח ולכוחות בשטח. כלומר, תיאורטית האיום היה מוכר, אך לא נעשו מאמצים מתאימים להיערכות מולו, לא ברמת המודיעין והכוחות הלוחמים ולא ברמת בניין הכוח – לפיתוח יכולת התמודדות איתו.[25]

במבצע "צוק איתן" בשנת 2014 נאלץ צה"ל להתמודד עם איום המנהרות ההתקפיות של חמאס, שהתפרש בקרב הציבור והצבא כהפתעה אסטרטגית מבחינת השימוש הנרחב והיעיל שעשה בהן האויב. על אף ההיכרות עם האיום, ההבנה בדבר חלקו המרכזי באסטרטגיה הצבאית החדשה של חמאס לא חלחלה מספיק לדרג מקבלי ההחלטות ולא נעשו מאמצים לתכנון ההתמודדות איתו ברמת בניין הכוח, תוכניות הלחימה ותוכניות לסיכול המנהרות. בחלק הדן בהתמודדות של גופי המודיעין עם איום המנהרות בדוח מבקר המדינה על "צוק איתן" מוצגות מספר נקודות שבהן המודיעין לקה בטיפול בנושא המנהרות:

- **שיתוף הפעולה המודיעיני בין אמ"ן ובין שב"כ בנושא המנהרות וחלוקת האחריות המודיעינית בין הארגונים על המתרחש ברצועת עזה.** מאז יציאת צה"ל והשב"כ מהרצועה בשנת 2005 ועד 2015 לא הוגדרה הרצועה כ"מדינת יעד" שנדרש לחקור ולא נבחנה חלוקת האחריות המודיעינית בין הגופים, כך שהשב"כ היה אחראי על האיסוף והסיכול ברצועה ולצידו פעלו אמ"ן, פיקוד הדרום ואוגדת עזה.
- **שילוב צי"ח המנהרות בצי"ח המודיעיני הלאומי, בצי"ח של אמ"ן ובצי"ח של השב"כ.** רק בשנת 2009 שולב איום המנהרות בצי"ח הלאומי וגם אז לא נחשב כנושא בפני עצמו שיש להקדיש לו תשומת לב מודיעינית ייחודית. כתוצאה מכך לא חל שינוי בהתייחסות אליו בשנים שלאחר מכן.
- **המאמץ האיסופי של גופי המודיעין מול איום המנהרות.** לא התקיים מאמץ מודיעיני משותף של כלל הגופים והמערכים באמ"ן, ואפילו השב"כ, שהשקיע מאמצים רבים ברצועה בין השנים 2008 ל־2012, הגביר את מאמצי האיסוף בצי"ח המנהרות רק בשנת 2013.
- **המחקר המודיעיני של איום המנהרות ברצועת עזה.** בשנת 2012 קבע ראש אמ"ן דאז כי פד"ם ואוגדת עזה יעסקו במחקר המודיעיני על איום המנהרות

25 אפי מלצר (עורך), **טכנולוגיה צבאית: אמצעי לחימה ומודיעין**, רעות: אפי מלצר בע"מ – מחקר צבאי, עיתונאות והוצאה לאור, 2012, עמ' 86־87.

ולא חטיבת המחקר באמ"ן. כך קרה שגוף המחקר המרכזי של צה"ל הסתפק רק בשיקוף התמונה מהפיקוד והאוגדה ולא עסק באופן עצמאי בעניין.

- **איכות המודיעין על המנהרות שסופק לכוחות בשטח.** נמצאו פערים משמעותיים במודיעין שהועבר לכוחות בשטח ביחס למנהרות ברצועה, מה שהקשה מאוד על הכוחות באיתור, נטרול והשמדה של כלל המנהרות ההתקפיות והגביל את היכולת לסכל התקפות שנעשו מהן בשטח הארץ.[26]

מִשּׁוּרת הליקויים דלעיל ניתן ללמוד כי היו פערים מודיעיניים משמעותיים סביב המנהרות ההתקפיות של חמאס בתקופה שלפני מבצע "צוק איתן", שהשפיעו על התמודדות צה"ל עם האיום במהלך המבצע עצמו. אחד הפערים היה העובדה כי בשנים שלאחר מלחמת לבנון השנייה, הצי"ח המודיעיני הלאומי התמקד בעיקר בגזרה הצפונית, ולשם הופנו רוב המשאבים. סוגיית המנהרות ברצועת עזה נותרה בעדיפות נמוכה יותר בצי"ח, מה שהשפיע על העבודה המודיעינית בנושא זה ועל הידע שהיה קיים בעת היציאה למבצע "צוק איתן". אחד הלקחים מתחקור הפתעת המנהרות ב"צוק איתן" היה כי יש להשקיע יותר בפעולות איסוף ומחקר מודיעיני סביב איום המנהרות בגזרה הצפונית. בדוח מבקר המדינה על "צוק איתן" נכתב, בנוגע להתמודדות המודיעינית עם איום המנהרות בגזרת פצ"ן, כי "במהלך השנים שמאז מלחמת לבנון השנייה ועד בסמוך למבצע 'צוק איתן' נעשו פעולות איסוף ומחקר רבות על ארגון חיזבאללה, אך רק באופן חלקי על תשתית המנהרות בלבנון".[27]

סוגיית המנהרות ברצועת עזה שמה את תחום תת־הקרקע במוקד והעלתה אותו לרמת עדיפות גבוהה יותר בצי"ח המודיעיני הלאומי. ההבנה כי גם ארגון חיזבאללה עוסק, ככל הנראה, בבניית מנהרות החודרות לשטח ישראל כחלק מתוכניות ההתקפה שלו למלחמה הבאה, הביאה להשקעת מאמצים איסופיים גדולים שנועדו להביא מודיעין על המנהרות. במסגרת זו הוקם צוות מיוחד, בו שולבו גורמי מודיעין וטכנולוגיה, שמטרתו הייתה להשיג מודיעין איכותי, מדויק ומוסמך, שיסייע בתכנון פעולה לאיתור ולסיכול המנהרות בשטח.[28] חלק מהמידע הגיע מעולם הסייבר וסייע לגורמי ההנדסה באיתור ובנטרול המנהרות במבצע "מגן צפוני", בו אותרו ונוטרלו שש מנהרות חיזבאללה שחצו לתוך שטח ישראל.

ההפתעה של טילי ה"סאגר" במלחמת יום הכיפורים ממחישה את המציאות המודיעינית טרום מהפכת המידע, שאופיינה בעבודה על פי "מעגל המודיעין"

---

26 "מבצע 'צוק איתן': תהליכי קבלת החלטות בקבינט בנוגע לרצועת עזה לפני מבצע 'צוק איתן' ובתחילתו; ההתמודדות עם איום המנהרות, דוח ביקורת מיוחד", משרד מבקר *המדינה*, 2017, חלק ב' עמ' 13־19.

27 שם, עמ' 19.

28 "פיתוח המענה השלם לאיום: מאחורי הקלעים של מבצע 'מגן צפוני'", *אתר צה"ל*, 6 בדצמבר 2018, https://www.idf.il/אתרים/פיקוד־הצפון/מאחורי־הקלעים־של־מבצע־מגן־צפוני/.

הקלאסי, בגופי מחקר ואיסוף מובחנים וביכולות מוגבלות להפצת המודיעין לשטח. ניכר כי יכולות ההתרעה בזמן אמת על איום הטילים היו מוגבלות באותה עת וכי לא היו קיימים אז אמצעים מתקדמים להעברת המודיעין לשטח. בהיעדר עבודת הכנה מוקדמת ארוכה וממוקדת לא הייתה דרך להכנת הכוחות לאיום הקיים ולאופן ההתמודדות איתו. בתקופה שלאחר מהפכת המידע השתפרה הנגישות של גורמי המודיעין למידע והתקצרו קבועי הזמן מהשגת המודיעין הגולמי ועד עיבודו. השיפור בא לידי ביטוי גם ביכולת המענה לשאלות מודיעיניות מורכבות, שבעבר הותירו מקום רק להערכות החוקרים. הדוגמה של ההתמודדות עם איום המנהרות החודרות בגבול הצפון ממחישה כיצד מיקוד נכון, תעדוף הצי"ח ושימוש ביכולות האיסופיות הקיימות מאפשרים להגיע למודיעין איכותי ומדויק, שמצידו מאפשר ביצוע מִבצעי סיכול להסרת האיום המתהווה.

דוגמה נוספת לאירוע שבו מודיעין איכותי סיפק התרעה ומנע הפתעה מצה"ל ומדינת ישראל הוא אירוע חדירת המל"ט האיראני ב־2018: בבוקר שבת, 10 בפברואר 2018, יירט צה"ל באמצעות מסוק קרב מל"ט איראני ששוגר ממרחב תדמור בעומק סוריה וחדר לשטח ישראל, תוך הפרת הריבונות הישראלית. המל"ט זוהה במערכות ההגנה האווירית בשלב מוקדם והיה במעקב עד לרגע הפלתו. בהמשך הותקף קרון השליטה של המל"ט במרחב ממנו שוגר.[29] ניתן להניח כי אירוע מסוג זה תוכנן בצד השני לאורך זמן וכי לישראל היה מידע מקדים על כוונות האויב לביצוע הפעולה. תקיפה כירורגית ומדויקת של קרון השליטה לא הייתה מתאפשרת ללא מודיעין בזמן אמת על מיקומו המדויק, דבר שהתאפשר הודות ליכולות איסוף מתקדמות שהופעלו לפני האירוע ובמהלכו.

מהפכת המידע והתקופה שאחריה לא פתרו לחלוטין את חוסר הוודאות בסוגיות מודיעיניות שונות, אך האפשרויות העומדות היום בפני חוקרי המודיעין להשגת המידע החסר רבות יותר. כמו בעבר, החוקר נדרש לשאול את השאלות הנכונות שיובילו אותו אל פתרון הפערים המודיעיניים בסוגיות שבתחום אחריותו, אך כפי שניתן לראות בטבלה 1, השפעת מהפכת המידע ניכרת בכל אחד משלבי התהליך המודיעיני. מהפכה זו גם דורשת תהליכי לימוד והסתגלות של גורמי המודיעין ליכולות הקיימות.

בעידן שבו אמצעי האיסוף יכולים לתת מענה כמעט לכל סוגיה מודיעינית, נדרש לבחור את הצי"חים המודיעיניים שבהם יושקעו משאבי האיסוף והעיבוד, ומכאן החשיבות של תעדוף הצי"ח. בעבר, כשהאיסוף היה מוגבל יותר, צי"חים מסוימים פשוט לא קיבלו מענה; היום, צוואר הבקבוק עובר למשאבי העיבוד

29 יואב זיתון ואחרים, "צה"ל יירט מל"ט איראני שחדר לישראל; תקיפה בסוריה; F-16 התרסק בשטח ישראל", *Ynet*, 10 בפברואר 2018, https://www.ynet.co.il/articles/0,7340,L-5102924,00.html.

שנדרשים להתמודדות עם כמויות אדירות של מידע שנאסף. ללא תעדוף הצי"ח, היכולת לתת מענה לכל סוגיה מודיעינית היא כמעט בלתי אפשרית בשל שיקולי עלויות, כוח אדם וזמן.

טבלה 1: השוואה בין השלבים בתהליך המחקר המודיעיני לפני מהפכת המידע ואחריה

	טרום מהפכת המידע	לאחר מהפכת המידע
איסוף	התבססות על סיגינט וויזינט[30] קלאסי.	סייבר כממד חדש. נתוני עתק (Big Data). ריבוי פלטפורמות וחיישנים.
עיבוד	תהליכי עיבוד מבוצעים על ידי גורמי המקצוע – כוח אדם והכשרתו. אמצעים ידניים וכלים אנלוגיים.	פיתוח כלים טכנולוגיים אוטומטיים להתמודדות עם נתוני עתק. פיתוחים טכנולוגיים המאפשרים היתוך מידע בין דיסציפלינות מודיעיניות שונות.
מחקר	הבחנה ברורה בין גורמי המחקר לגורמי האיסוף. החוקר "מחכה" לקבלת החומר המודיעיני המעובד.	פיתוח כלים ואפליקציות המנגישות גם את חומרי המודיעין הגולמיים לחוקר. שילוביות בין גורמי האיסוף לגורמי המחקר. "טכנולוגים" כאנשי מקצוע מודיעיניים חדשים.
הפצה	העברת המודיעין לשטח באופן חלקי. מידור כמכשלה.	פיתוחים טכנולוגיים המנגישים את המודיעין בזמן אמת ללוחמים בשטח.

כפי שהוצג קודם לכן, הטשטוש הקיים כיום בין גורמי המחקר ובין גורמי האיסוף מביא לשינויים ארגוניים שמטרתם לתת מענה לצרכים המודיעיניים. בעידן שבו הסייבר תופס נפח משמעותי מעבודת המודיעין נוצרת סביבה חדשה, בה כלל הגורמים נדרשים לעבודה משותפת וחולקים ידע משותף ומיומנויות משותפות, כגון יכולות חיפוש ב"בריכות" המידע, איתור המידע הרלוונטי ועיבודו. גורמי האיסוף אינם עוסקים רק באיסוף המידע, כמו בעבר, ותפקידם משתנה לזה של "טכנולוגים". בתוך כך, גורמי האיסוף נדרשים להבנה בסיסית בנושאי המחקר של החוקר העובד עימם, ועבודתם צריכה לבוא לידי ביטוי ביצירת הכלים הטכנולוגיים שיסייעו לאותו חוקר לשאול את השאלות המודיעיניות הנכונות ובמציאת המענה

30 סיגינט (Signal Intelligence) הינו מודיעין אותות, כלומר, מודיעין המבוסס על איסוף מידע המועבר באמצעות שידור של אותות אלקטרוניים; ויזינט (Visual Intelligence) הינו מודיעין חזותי, כלומר, מודיעין המתקבל ממקורות חזותיים שונים.

להן. החוקר, מצידו, נדרש להבנה בסיסית ולהיכרות עם טכנולוגיות המידע ועם יכולות מיצוי המידע, להבנה בסיסית ברשתות ועוד. באמ"ן, למשל, מתקיימת כיום חשיבה על "בסיסי אמ"ן החדשים", שיתנו מענה למסגרות עבודה משותפות אלו. ארגון גורמי המודיעין באופן משותף יהווה הזדמנות לייעול תהליכי העבודה ולניצול יתרונותיו של כל גוף כדי לשפר את התוצרים המודיעיניים ולקצר את משך זמן הפצתם.

קצב השתנות הסביבה בעידן המידע הולך וגובר ומביא להתחדשות ולשינויים גם אצל האויב. בנוסף לכך, ישראל ניצבת בפני אתגר מיוחד, מכיוון שעליה להתמודד לא רק עם אתגרים מבחוץ, אלא גם עם איומים מבית, כמו פיגועי טרור או אינתיפאדת הסכינים ב־2016.

אלוף הרצי הלוי, לשעבר ראש אמ"ן, טוען במאמרו "אמ"ן 2048: עליונות מודיעינית בעידן הדיגיטלי" כי המעצב העיקרי של העשורים הבאים הוא טשטוש הגבול בין הממד הפיזי לממד הדיגיטלי. לדבריו, מי שישיג עליונות במידע ובידע בעידן הדיגיטלי, יהיה זה שישלוט בתהליכים המרכזיים.[31] מה היא אותה "עליונות מודיעינית"? הכוונה היא ליכולת להביא את המידע המודיעיני החסֵר ולהפוך אותו לידע על האויב, באופן שיאפשר השפעה עליו בזמן רלוונטי.

המלחמות בעידן מהפכת המידע ואחריה ידרשו מודיעין אחר כדי להכריען, ומקור אותו מודיעין יהיה, במידה רבה, בממד הסייבר. במצב זה, כל מידע שזמין לצד אחד יכול תיאורטית להיות זמין גם לאויב. בנוסף, כלי הלוחמה בסייבר ניתנים ללימוד ומצויים לא רק בידי גופי מודיעין מדינתיים, אלא מגיעים גם לידיהם של ארגוני טרור ומפַגעים בודדים. יכולות הסייבר הולכות והופכות לפופולריות וזמינות, מה שמאפשר את פיתוחן גם בצד השני. כפי שטוען ראש אמ"ן לשעבר, "יתרונות המהפכה הדיגיטלית זמינים גם לאויבינו, ואין סיבה להניח שהם ישקטו על שמריהם"[32]. בעידן המידע, כאשר הכול פתוח וזמין, גם האויב מסוגל לפתח יכולות לימוד, הוא דינמי יותר מאשר בעבר ומסוגל לפיכך להפתיע ביכולותיו.

בדומה לתופעת ה־O-RMA ("המהפכה בצד השני"),[33] שמתארת את התגובות וההתפתחויות בצד השני אל מול המהפכות בעניינים צבאיים, ניתן להסתכל על מהפכת המידע והתקופה שאחריה ולטעון כי גם היריב חי במציאות טכנולוגית גלובלית ונהנה מיתרונותיה של אותה מהפכה: היריב לומד ומתפתח, מכיר ביתרונותיו של הצד שכנגד ומנסה להשתפר ולפגוע בנקודות התורפה שלו. עובדה זו מציבה

31 הלוי, "אמ"ן 2048: עליונות מודיעינית בעידן הדיגיטלי", עמ' 26–27.
32 שם, עמ' 28.
33 איתי ברון וכרמית ולנסי, "המהפכה בעניינים צבאיים של הציר הרדיקלי", **מערכות**, גיליון 432, 2010, עמ' 4–17.

אתגר בפני ארגוני המודיעין, משום שהנגישות למידע של כלל השחקנים עשויה לשחוק את היתרונות היחסיים המסורתיים שהיו נחלתם של ארגוני המודיעין בעבר.[34]

סיכום ומסקנות

ניתן להצביע על שלוש מגמות מרכזיות בהן באה לידי ביטוי השפעת הטכנולוגיה על עבודת גופי המודיעין בתקופה שלאחר מהפכת המידע. המגמה הראשונה היא שלאחר מהפכת המידע והפיתוחים הטכנולוגיים בתחום המודיעין שבאו בעקבותיה, הולכת ומתחדדת ההבנה ש**אופן עשיית המודיעין הקלאסי משתנה** וכי נדרשות התאמות לשיטות החדשות, גם ברמה הארגונית. השילוביות בין גופי המחקר והאיסוף, כמו גם השינויים בכישורים הנדרשים מגורמי המחקר והאיסוף, יוצרים תהליכי עבודה חדשים במציאות המודיעינית, השונה מזו שהייתה בעבר.

המגמה השנייה היא **השיפור בהנגשת המודיעין לגורמים המבצעיים** על ידי פיתוחים טכנולוגיים המאפשרים העברת מידע מודיעיני בצורה בטוחה מבחינת אבטחת המידע, וזאת בהיקפים גדולים, בעיתוי המתאים ובאופן רבוד בסוגי מידע שונים. הנגשת המודיעין לשטח בעידן שלאחר מהפכת המידע מתבצעת באופן המשרת טוב יותר את צורכי הגורמים המבצעיים ומקל עליהם בהתמודדות עם אירועים בלתי מתוכננים בזמן אמת. איכות התוצר המודיעיני וחיבורו לגורמי השטח משפיעים באופן ישיר על יכולת ההתמודדות עם הפתעות מודיעיניות. מגמה שלישית, שראוי לשקול אותה, היא השפעת הפיתוחים הטכנולוגיים בשימוש המודיעין על **צמצום מרחב ההפתעה**. ניתן לראות כי עידן המידע הביא לשיפור משמעותי ביכולת המענה לשאלות המחקר המודיעיניות באמצעות טכנולוגיות שנכנסו לשירות המודיעין בכל אחד משלבי התהליך המודיעיני. אנו נמצאים היום בתקופה שבה כמעט ואין מידע שאינו זמין – הכול פתוח, נגיש ומקושר, מידת חוסר הוודאות הולכת ומצטמצמת והאתגר הופך להיות פיתוח מיומנויות שיאפשרו להשיג את המידע הנחוץ. לעומת התקופה שלפני מהפכת המידע, היום גדלים פי כמה הסיכויים להשגת מידע בשל היצף המידע וריבוי הנגישויות האפשריות אליו. עם זאת, ועל אף המאמצים הנעשים היום בהנגשת מרב המידע לדרגי השטח, עדיין ייתכנו קשיים, הנובעים ממידור מרכיבי מידע מסוימים. עניין זה דורש חשיבה, בעיקר על היכולת להתגבר על המידור, באופן שלא יפגע בהיערכות ובמוכנות דרגי השטח לכל מצב שיידרשו אליו.

השפעותיה של מהפכת המידע מהוות נדבך חשוב ומשמעותי בעבודת גופי המודיעין: השפעות אלו ניכרות בכל אחת מאבני היסוד של עבודת המודיעין, כפי שתואר במאמר זה, והפיתוחים הטכנולוגיים, שהם תוצאה ישירה שלהן, משפיעים

34 ד"פ, "התפיסה כמצפן לבניין כוח מודיעיני טכנולוגי", בתוך: קופרווסר וסימן טוב (עורכים), **מודיעין הלכה ומעשה: ביג דאטה ומודיעין**, עמ' 137.

באופן יומיומי על יכולתם של גורמי המודיעין להביא את המודיעין המדויק במקום ובזמן הנכון כדי להתריע על ההפתעה הבאה ולמנוע אותה. חשוב לציין, בהקשר זה, כי הטכנולוגיה אמנם שיפרה באופן מהותי את תהליכי המודיעין, אך הצד השני ממשיך גם הוא ללמוד ולהשתפר, ולכן נדרשות התאמות מצידנו כדי לשמור על עליונותנו הטכנולוגית.

בהסתכלות קדימה, נשאלת השאלה היכן נהיה בעוד עשור, שני עשורים או אף יותר? ברור, בנקודת הזמן הנוכחית, כי כמות המידע הזמין ברשת תמשיך לגדול בקצב מעריכי וכי מגמה זו תמשיך להשפיע על עבודת המודיעין, תאתגר את גורמי האיסוף, העיבוד והמחקר המודיעיני ותחייב אותם לפתח פתרונות יצירתיים שיתנו מענה לשאלות הצי"ח. שאלות מעניינות נוספות הן מה יהיה מקומו של החוקר המודיעיני בעשיית המודיעין וכמה זמן יושקע, למשל, בפיתוח כלי סייבר לטובת האיסוף והמחקר, לעומת הזמן שיושקע במחקר עצמו, כדי לאפשר מתן התרעה? כמה תהליכים יהפכו להיות אוטומטיים ומה יהיה מקומו של החוקר במניעת ההפתעה הבאה? שאלות אלו ראויות למחקרי המשך.

חשיבותה של הטכנולוגיה בתהליך המודיעיני תמשיך להעמיק ולהתפתח, ויותר פעולות המבוצעות כיום על ידי בני אדם יעברו תהליכי אוטומציה ויוחלפו באלגוריתמים ממוחשבים. הדבר יסייע בהתמודדות עם כמויות החומר הגולמי הנקלט על ידי גופי האיסוף – בין אם יהיה זה מידע שמקורו ויזינט ובין אם מקורו יהיה סיגינט – ויקצר את קבועי הזמן הנדרשים היום לעיבוד המידע והפצתו לצרכנים. האם יכולת ההתרעה מפני ההפתעה הבאה תישאר בידי החוקר האנושי, או שתוחלף בעתיד באלגוריתמים ממוחשבים? שאלה זו ונוספות לה ימשיכו להעסיק את אנשי המודיעין, ומה שנראה כמו מדע בדיוני היום, ייתכן ויהפוך למציאות בשנים הקרובות. על כן, ראוי לעסוק בנושא זה ולהיערך לקראתו.

מבצעי השפעה בסייבר ברשת האפלה (Dark Web)

לב טופור ופנינה שוקר

בשנים האחרונות חלה עלייה משמעותית בהיקפה ובעוצמתה של מלחמת המידע בין המעצמות והכוחות השונים בזירה הבין־לאומית, ומבצעי השפעה הפכו לכלי לגיטימי בידי שחקנים פוליטיים תועלתניים ומעצמות גלובליות כאחד. העיסוק העיקרי בהקשר זה הוא במִבצעי השפעה ברשתות החברתיות, והספרות המקצועית אינה מתייחסת באותה מידה למִבצעי השפעה הנעשים ברשת האפלה; עיקר העיסוק המחקרי במבצעים כאלה כיום הוא בהקשר של עשייה פלילית. הרשת האפלה פותחה על ידי הצי האמריקאי לצורכי מודיעין, ולאחר מכן קודמה על ידי המערב ככלי ציבורי להגנה על פרטיות ואנונימיות. כיום היא משמשת כר פורה להדלפות מכוונות של מדינות שאינן רוצות לפרסם מידע מסוים בכלי התקשורת המסורתיים. הדלפות אלו נתפסות כאותנטיות, מה שמוביל לעיתים את אמצעי התקשורת וארגוני מודיעין לבלוע את הפיתיון ולבחון את הדברים לעומקם, ובמקרים אחדים אפילו לשנות דפוסי פעולה. מטרתו של מאמר זה היא להציג את האופן שבו נעשה שימוש ברשת האפלה לטובת מבצעי השפעה, בעיקר באמצעות הדלפה מכוונת של מידע.

מילות מפתח: רשת אפלה, מבצעי השפעה, תעמולה, לוחמת מידע, דיסאינפורמציה

מבוא

בינואר 2019 דלפו לרשת האפלה עשרות אלפי מסמכים ותכתובות דואר אלקטרוני של בכירי ממשל רוסיים, אנשי דת מהכנסייה האורתודוכסית הרוסית ואוליגרכים רוסיים. המידע הודלף, ככל הנראה, בעקבות פריצה ופעילות מכוונת של האקרים אקטיביסטים ("האקטיביסטים"), שהצהירו כי פעולות אלו נבעו לא ממטרה

לב טופור הוא יועץ אסטרטגי בכיר וחוקר גזענות וסייבר. פנינה שוקר היא חוקרת (מלגאית ניובאואר) במכון למחקרי ביטחון לאומי.

אידיאולוגית, אלא מהרצון להבטיח את חופש המידע: "אין לנו כל מטרה מלבד להבטיח כי המידע יהיה נגיש לטובת מי שזקוק לו יותר מכל – העם".[1] אירוע זה מלמד על השימוש שנעשה ברשת האפלה לעקיפת מגבלות שמשטרים טוטליטאריים מטילים על חופש הביטוי. אלא שבנוסף לכך, בשנים האחרונות ניכר ששחקנים רבים במערכת הבין־לאומית עושים שימוש בהדלפות מכוונות, בחלקן כוזבות, כדי ליצור השפעה פוליטית. כך מתחדד פעם נוספת המתח המובנה ברשתות האינטרנט בין הגנה על הפרטיות ובין צורכי הביטחון הלאומי.

באופן מסורתי, הרשת האפלה מהווה כר נרחב לפעילות פלילית, כמו גם להדלפות ולסחר במידע. בשנים האחרונות חלה עלייה משמעותית בהיקפה ובעוצמתה של מלחמת המידע בין השחקנים השונים בזירה הבין־לאומית באמצעות הרשת האפלה, כאשר כל צד משתמש בהדלפות מכוונות ובדיסאינפורמציה כדי לטפלל את תודעת הצד השני. זאת, בין אם מדובר בהדלפה שמטרתה היא צבאית גרידא, ובין אם מדובר בהדלפה שמטרתה היא השפעה חברתית־אזרחית או אפילו עיסקית. לדוגמה, מדינות שאינן מעוניינות לפרסם דברים מסוימים בצורה רגילה בתקשורת המסורתית מדליפות מידע ברשת האפלה, תוך ניסיון לשוות למידע מראית עין של אותנטיות. בנוסף לכך, כלי התקשורת עצמם הקימו פלטפורמות שמטרתן לספק יכולת תקשורת מוצפנת שנועדה לעודד הדלפות. כאלו הן פלטפורמות דוגמת WikiLeaks ו־Secure Drop, עליהן יבוא פירוט בהמשך המאמר. כמו כן, ברשת האפלה מוצעות למכירה נוזקות, רוגלות, תולעים ועוד אין ספור תוכנות וקבצים זדוניים, וכן כלי הצפנת תקשורת וסייבר אחרים (למשל, מדריכי הצפנת PGP והצפנות אחרות קלות לשימוש).

מטרתו של מאמר זה היא להציג את האופן שבו שחקנים בזירה הבין־לאומית עושים שימוש ברשת האפלה כדי להפיץ תעמולה ודיסאינפורמציה נגד יריבים, וכיצד פעולות אלו עשויות להיתרגם למבצעי השפעה רחבי היקף. המאמר בנוי משלושה חלקים: החלק הראשון כולל סקירה תיאורטית העוסקת במניפולציה של מידע בכלל ובמבצעי השפעה בפרט, תוך הבאת מספר דוגמאות למבצעי השפעה מרכזיים בשנים האחרונות; החלק השני עוסק ברשת האפלה, מאפייניה ושימושיה העיקריים; בחלק השלישי, המשלב את שני החלקים הראשונים, מוצגים האופן שבו נעשה שימוש ברשת האפלה כדי להוציא לפועל מבצעי השפעה, ולצד זאת היקפה של התופעה.

---

1 Stephan Jajecznyk, "The Dark Side of the Kremlin: Hacked Russian Documents Explained", *Al Jazeera*, February 25, 2019.

מהם מבצעי השפעה?

מִבצע השפעה הוא יישום מתואם, משולב ומסונכרן של יכולות דיפלומטיות, אינפורמטיביות, צבאיות וכלכליות, כמו גם יכולות לאומיות אחרות, וזאת בעיתות שלום, בזמני משבר, במצבי עימות ובמצבים שלאחר עימות. המטרה של מבצע ההשפעה היא להשפיע על התנהגויות או החלטות של קהלי יעד זרים, כך שיאמצו עמדות ההולמות את האינטרסים של יוזמי המבצע.[2]

מבצעי השפעה על התודעה הם דפוס פעולה מוכר, אשר נועד לשרת מגוון תכליות מדיניות, ביטחוניות, כלכליות וחברתיות. מבצעי השפעה על התודעה ברמה המדינית נועדו להשיג את יעדיהם באמצעות, בין היתר, פגיעה בביטחון האישי והכלכלי, ערעור האמון והתמיכה של הציבור במוסדות המדינה ופגיעה בלכידות החברתית. האמצעים להשגת תכליות אלו כוללים התערבות פעילה במערכות ובתהליכים, או הפעלת מנופים שונים כדי להניע לפעולה או להניא מפעולה, השגת מידע ושימוש בו ליצירת מסרים, הפצה של מסרים ויצירת תהודה להשגת אפקט מרבי. הערוצים להעברת המסרים הם המדיה המסורתית, ולצידה המדיה החדשה, דהיינו האינטרנט והרשתות החברתיות המתנהלות על גביו. מובילי דעה משמשים לעיתים כ"סוכנים לא מודעים" לחיזוק אמינותם של המסרים ולהגברת תפוצתם.[3]

בשנים האחרונות גוברים ניסיונות של גורמים זרים (מדינות וגורמים לא מדינתיים) להתערב במערכות בחירות של מדינות יריבות באמצעות כלים דיגיטליים. פעילות זו נעשית בחלקה באמצעות תקיפות סייבר על מערכות המחשוב התומכות את תהליך הבחירות באותן מדינות (מסדי נתונים, תוכנות למיניהן ומערכות תקשורת) במטרה לשבש את הנתונים, לגנוב אותם כדי לעשות בהם שימוש, או לפגוע ביכולת הפעולה של מערכות אלו. לצד פעילות זו, נעשים מאמצים רחבי היקף להטיית השיח באותן מדינות, שמטרתם היא להשפיע על תודעת הבוחרים.

הסוג השלישי של מבצעי תודעה מהווה סינתזה של השניים הראשונים: מבצעי השפעה על התודעה באמצעות שימוש בסייבר. המטרות של ניסיונות אלה עשויות להיות מגוונות: החל מניסיון לערער את אמון הציבור בתהליך הדמוקרטי וכלה בניסיון להשפיע על התמיכה במפלגות ובמועמדים שונים. חלק מהניסיונות

---

2 Eric V. Larson, Richard E. Darilek, Daniel Gibran, Brian Nichiporuk, Amy Richardson, Lowell H. Schwartz, Cathryn Quantic Thurston, *Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities* (California: RAND Corporation, 2009), p. 2.

3 רון שלייפר, "הלוחמה הפסיכולוגית בעופרת יצוקה", **מערכות**, 432, אוגוסט 2010, עמ' 19–20.

אף נועד להניא אנשים מלהשתתף בבחירות, וזאת על בסיס זהותם או מעמדם הסוציו־אקונומי.[4]

השחקנים העיקריים המוציאים לפועל ניסיונות מהסוגים שנמנו לעיל הם משטרים אוטוריטריים, דוגמת רוסיה, סין ואיראן. גם משטרים דמוקרטיים־ליברליים, דוגמת ארצות הברית, בריטניה ואף ישראל, מנסים להשפיע בדרכים כאלו בזירה הבין־לאומית. למשל, לרוסיה יש מסורת ארוכה של פעולה בתחום מבצעֵי ההשפעה והיא מחזיקה במשנה סדורה וביכולות מבצעיות לשם כך.[5] על שיטות הפעולה הרוסיות בתחום מבצעי ההשפעה ניתן למנות הפצת ידיעות כוזבות ברשתות החברתיות על ידי פרופילים מזויפים; רכישת פרופילים אותנטיים במטרה להפיץ פרסומות פוליטיות שתומכות במועמדים פרו־רוסיים במערכות בחירות ברחבי העולם וכדי לפרסם ידיעות כוזבות או מידע מפליל על יריבי מוסקבה; שימוש נרחב בתקשורת הממוסדת הרוסית הנמצאת בבעלות הקרמלין במטרה להפיץ מידע כוזב ומניפולטיבי.[6] כך, במחצית השנה האחרונה בלבד הוצאו לפועל מבצעי השפעה רוסיים סביב מערכות בחירות רבות ברחבי העולם, בכללן הבחירות הכלליות בספרד, הבחירות לפרלמנט האירופי, הבחירות האחרונות בניגריה, אינדונזיה, דרום אפריקה ועוד.[7]

גם סין עושה שימוש ענֵף בתעמולה ובמבצעי השפעה, הן בכדי לעצב את תדמיתה של המפלגה הקומוניסטית הסינית והן בכדי לערער את יציבותן של יריבותיה.[8] לאחרונה הולכים ורבים הדיווחים על מאמציה של סין להתערב בבחירות במדינות רבות, דוגמת סרי לנקה, מלזיה ואוסטרליה.[9] בנוסף לכך, ערב בחירות אמצע הכהונה בארצות הברית הודיע הממשל האמריקאי כי סין, יחד עם איראן

4 Chris Tenove, Joran Buffie, Spencer McKay and David Moscrop, *Digital Threats to Democratic Elections: How Foreign Actors Use Digital Techniques to Undermine Democracy* (The University of British Columbia: Center for the Study of Democratic Institutions, 2018), p. 26.

5 דימה אדמסקי, "אומנות אופרטיבית קיברנטית: מבט מזווית לימודי האסטרטגיה ומפרספקטיבה השוואתית", **עשתונות** 11, מרכז המחקר, המכללה לביטחון לאומי, 2015, פרק ב': "הגישה הרוסית לאומנות המערכה הקיברנטית", עמ' 28–48.

6 Alina Polyakova, "Want to Know What's Next in Russian Election Interference? Pay Attention to Ukraine's Elections", *Brookings*, March 28, 2019; Michael Schwirtz and Sheera Frenkel, "In Ukraine, Russia Tests a New Facebook Tactic in Election Tampering", *The New York Times*, March 29, 2019.

7 פנינה שוקר, "התערבות זרה בבחירות בעולם: מאפיינים, מגמות ולקחים לישראל", **מבט על**, מס' 1173, 10 ביוני 2019.

8 Erica Pandey, "How China Became a Global Power of Espionage", *AXIOS*, March 23, 2018.

9 Prashanth Parameswaran. "China's Influence Operations in Asia: Minding the Open Door Challenge", *The Diplomat*, May 14, 2019.

ורוסיה, מנסות לערער את ההליך הדמוקרטי באמצעות קמפיין תעמולתי מקוון, שכולל הפצת דיסאינפורמציה ברשתות החברתיות במטרה להעמיק את השסעים האידיאולוגיים בארצות הברית וללבות ויכוחים פנימיים בסוגיות שעל סדר היום המקומי.[10] במסגרת יריבותה עם ארצות הברית, סין מנסה גם לקדם את השפעתה בסינגפור: לאחרונה פורסם כי המפלגה הקומוניסטית הסינית פונה אל סינגפורים ממוצא סיני, בעיקר באמצעות אפליקציית Wechat הסינית, לצורך השפעה על הפוליטיקה והחברה בסינגפור.[11] במקביל דווח כי נחשף מאמץ השפעה סיני בהיקף חסר תקדים על גבי פלטפורמות "פייסבוק", "טוויטר" ו"יוטיוב" – שלושתן אסורות בשימוש בסין עצמה – כדי להנמיך את גובה הלהבות במחאות הסוערות בהונג קונג נגד מעורבותה של סין בנעשה במקום.[12]

גם איראן אינה טומנת ידה בצלחת; באוגוסט 2018 מחקו "טוויטר" ו"פייסבוק" מאות חשבונות החשודים כמקושרים למבצע דיסאינפורמציה איראני.[13] התוכן שהועלה בחשבונות אלה נועד להבליט נושאים ונרטיבים ההולמים את מדיניות החוץ האיראנית ולקדם נושאים אנטי־סעודיים, אנטי־ישראליים ופרו־פלסטיניים, וכן לעורר תמיכה בנושאים מסוימים במדיניות ארצות הברית המשרתים את האינטרסים האיראניים, כמו הסכם הגרעין בין איראן ובין המעצמות מ־2015.[14] בשלהי אוקטובר 2018 גם נחשפה רשת עמודי "פייסבוק" שמקורה באיראן, שנועדה להשפיע על דעת הקהל בארצות הברית ובבריטניה.[15] כמו כן, לאחרונה הולכים ורבים הדיווחים על תקיפות סייבר ומבצעי השפעה איראניים נגד ישראל. בסוף ינואר 2019 הצהיר ראש הממשלה נתניהו בכנס Cyber Tech כי איראן מנסה להשפיע על הבחירות בישראל דרך חשבונות מזויפים ברשת, וכי היא מבצעת מתקפות סייבר נגד ישראל "על בסיס יומי".[16] בניגוד למאמצי ההשפעה הרוסיים

10 Abigail Grace, "China's Influence Operations Are Pinpointing America's Weaknesses", *Foreign Policy*, October 4, 2018.

11 Muhammad Faizal Bin Abdul Rahman, "Foreign Influence in Singapore: Old Threats in New Forms", *The Diplomat,* July 23, 2019.

12 Raymond Zhong, Steven Lee Myers and Jin Wu, "How China Unleashed Twitter Trolls to Discredit Hong Kong's Protesters", *The New York Times,* September 18, 2019.

13 Craig Timberg, Elizabeth Dwoskin, Tony Romm, Ellen Nakashima, "Sprawling Iranian Influence Operation Globalizes Tech's War on Disinformation", *The Washington Post*, August 21, 2018.

14 Adriane M. Tabatabai, "A Brief History of Iranian Fake News: How Disinformation Campaigns Shaped the Islamic Republic", *Foreign Affairs*, August 24, 2018.

15 "פייסבוק נלחמת בפייק ניוז מאיראן: 'חיסלנו רשת תעמולה – מיליון משתמשים נחשפו'", **דה מרקר**, 27 באוקטובר 2010.

16 סתו נמר, "נתניהו: איראן מתקיפה את ישראל בסייבר על בסיס יומי", **מעריב**, 29 בינואר 2019.

המוּפָּרים המגלים רמת תחכום גבוהה יחסית, המאמצים האיראניים והמאמצים הסיניים ניחנו ברמת ביצוע ירודה למדי, וניתן להתחקות אחריהם בקלות יחסית.

מערכות בחירות שנערכו ברחבי העולם במחצית השנה האחרונה התקיימו בצל החשש ממבצעי השפעה. ואכן, ברבות מהן זוהו מאמצי השפעה, בעיקר רוסיים. מניתוח מאמצים אלה עולה כי פעולות נגד, שננקטו על ידי ענקיות המדיה והמדינות עצמן, הביאו להפחתת ניסיונות ההשפעה הזרה באמצעות בוטים שנעשו ברשתות החברתיות. לעומת זאת, ניתן לזהות כיום פעילות גוברת מצד סוכני השפעה אנושיים. זאת ועוד, מאמצי ההשפעה בתקשורת הממוסדת שבים למלא תפקיד משמעותי, וכמוהם גם מאמצי השפעה באפליקציות להעברת מסרים מיידיים, דוגמת "ווטסאפ" ו"טלגרם", להן מיוחסת רמת מהימנות גדולה יותר: המידע מועבר בפלטפורמות סגורות אלו בתוך קבוצות מצומצמות יחסית של חברים ומשפחה, מה שמעניק למסרים מראית עין של מהימנות. יתרה מזאת, טכנולוגיית ההצפנה מקצה לקצה, המאפיינת פלטפורמות אלו, אינה מאפשרת אפילו למנהליהן גישה למסרים שנשלחים בהן, אלא אם כן משתמש מדווח על תוכן מסוים כבעייתי. מאפיינים אלה מקשים על ניטור מידע כוזב והסרתו.[17]

הרשת האפלה: מאפיינים ושימושים

בשנים האחרונות הפכה הרשת האפלה לאחד הנושאים המדוברים ביותר בקרב העוסקים בביטחון סייבר.[18] כדי להבין כיצד נוצרה והתפתחה הרשת האפלה ומהם מאפייניה הייחודיים, יש להתחיל בסקירה קצרה של מאפייני הרשת הרגילה: רשת האינטרנט הרגילה (Surface Web) נוצרה מפרויקט תקשורת של משרד ההגנה של ארצות הברית בשנות השישים של המאה העשרים, הידוע בשם Advanced Research Project Agency Network – ARPANET. ב־1983 שונה הפרויקט מרשת סגורה (Network Control Protocol – NCP) לפרויקט פתוח, הידוע כיום בשם "פרוטוקול שליטה" או "פרוטוקול אינטרנט" /Transmission Control Protocol (Internet Protocol – TCP/IP).[19] פתיחת הרשת הביאה להרחבה מסיבית של רשת האינטרנט – ממספר חיבורים בודדים לכדי מיליונים כיום – ולחלוקה מעמדית של רשתות – רשת ארצית (National, Class A), רשת אזורית (Regional, Class B) ורשת מקומית (Local, Class C) – והניחה את התשתית לרשת האינטרנט

17 שוקר, "התערבות זרה בבחירות בעולם: מאפיינים, מגמות ולקחים לישראל".
18 Mihnea Mirea, Victoria Wang and Jeyong Jung, "The Not So Dark Side of The Darknet: A Qualitative Study", *Security Journal* 32 no. 2 (2019): 102-118.
19 George Hurlburt, "Shining Light on the Dark Web", *IEEE Computer* 50, no. 4 (2017): 100-105.

הציבורית המוכרת לנו כיום. רשת האינטרנט של ימינו היא רשת המחברת מספר מחשבים/מכונות דרך צמתים (Nodes) או נקודות גישה.[20]

פרויקט ARPANET נסגר רשמית ב־1989 והותיר אחריו את תחומי הרשת הציבוריים: כתובות מאגרי מידע (דפי אינטרנט) ופרוטוקולי רשת נגישים, דפדפנים לכלל הציבור ושפת רשת נגישה (למשל שפת HTML). לצורך הפיכת האינטרנט לנגיש לכלל הציבור, הוקם ארגון ICANN (Internet Corporation for Assigned Names and Numbers), אשר סיפק כתובות ומספרי רשת וצירף שמות לכתובות IP. הארגון החל למפתח כמעט כל שירות ומידע ציבורי והזמין חברות טכנולוגיות רבות לבנות מאגרי מידע נגישים לציבור, דוגמת Google, Bing, AOL, Yandex.ru ועוד.[21] התוצאה הייתה שחברות ענק וממשלות יכלו לעצב את רשימות החיפושים כראות עיניהן, ובדרך זאת לשלוט במידע הנגיש לציבור ולמנוע ממנו צריכת מידע שלא רצוי להן. כך נוצרה למעשה הרשת העמוקה.[22]

הרשת העמוקה היא כל סוג של מידע שאינו ממופה על ידי מנועי חיפוש והגישה אליו מוגבלת, אך נעשית באמצעות דפדפנים (תשתיות) רגילים; למשל, דפי אינטרנט דינמיים, דפי אינטרנט ללא קישורים, דפי אינטרנט שאינם מבוססים על Hyper Text Markup Language (HTML) ומאגרי מידע מוגבלים אחרים. גורמי ביטחון רבים מקיימים גם רשתות פרטיות (למשל, מקומיות) וכן רשתות עמוקות, כמו למשל רשת צבאית או רשת משטרתית, שהציבור הרחב לא יכול לגשת אליהן. יחד עם זאת, הרשת העמוקה מורכבת גם ממידע פרטי, דוגמת מאגרים פיננסיים, מאגרי מידע ביומטרי, רפואי וכדומה. לדוגמה, כאשר משתמש נכנס לחשבון הבנק שלו, הוא נכנס לרשת העמוקה, אך כאשר הוא נמצא בדף הבית של הבנק שלו, הוא נמצא ברשת הרגילה.[23]

הרשת האפלה (Darknet/Dark web) מהווה חלק מהרשת העמוקה, ולמעשה היא השכבה החבויה ביותר בה.[24] ניתן לגלוש אליה רק באמצעות דפדפן מיוחד או הגדרת פרוטוקולי רשת מיוחדים, כך שהפעולות הנעשות בה הן ברוב המקרים

20 Mitch Waldrop, *DARPA and the Internet Revolution: 50 Years of Bridging the Gap* (Defense Advanced Research Projects Agency, 2018).

21 Vincenzo Ciancaglini, Marco Balduzzi, Robert McArdle, and Martin Rösler, “The Deep Web”, *Trend Micro*, 2015.

22 Lucas D. Introna and Hellen Nissenbaum, “Shaping the Web: Why the Politics Search Engines Matters”, *The Information Society* 16, no. 3 (2000):169-185; Eszter Hargittai, “The Social, Political, Economic and Cultural Dimensions of Search Engines: An introduction”, *Journal of Computer-Mediated Communication* 12, no. 3 (2007): 769-777.

23 Hurlburt, “Shining Light on the Dark Web”, pp. 100-105.

24 Gabriel Weimann, “Going Darker: The Challenge of Dark Net Terrorism”, *Wilson Center*, April 27, 2018.

אנונימיות לחלוטין. המאפיינים הייחודיים של הרשת האפלה, לעומת הרשת העמוקה, הם הפרוטוקולים (הכללים) המיוחדים והתשתית המיוחדת הנדרשים לצורך שימוש וגלישה בה. התשתית המיוחדת מגיעה לעיתים בצורת דפדפנים המתוכנתים לגשת לפרוטוקולים שונים, כגון כתובות Onion, Riffle, Freenet או i2p ועוד, או בתור הגדרות רשת מסוימות הידועות רק לצדדים המשתמשים ברשת.[25] ארגונים ופרטים, למשל כוחות צבא, מודיעין ומשטרה, ואף ארגונים עיסקיים ופרטים בודדים, יכולים להקים רשתות אפלות, שהפרוטוקולים והדפדפנים שלהן יהיו מיוחדים וידועים רק למקימיהן.[26]

הרשת האפלה הנפוצה ביותר היא The Onion Route (TOR), אשר פותחה על ידי מעבדות הצי האמריקאי במטרה לאפשר תקשורת פרטית ואנונימית בקרב אנשי מודיעין ונחשפה בשנת 2002. רשת זו מורכבת מעשרות אלפי אתרי אינטרנט שאליהם ניתן לגשת רק באמצעות דפדפן TOR. אתרים אלה מכונים אתרי "בצל" על שם סיומת ה־onion המאפיינת אותם ודימוי הבצל, המשמש כמטאפורה לשכבות הרבות המקשות על הגישה למקור. אתרי הבצל אינם מקוטלגים, ואין מנוע חיפוש מרכזי היכול לסייע בצורה מַספקת במציאתם. רשת TOR פועלת באופן שהתקשורת בין שתי נקודות (למשל, המחשב של המשתמש והאתר אליו הוא גולש) אינה מועברת בצורה ישירה, אלא דרך מספר תחנות ביניים (כתובות IP). כל תחנה מקבלת אמצעי ייחודי לפענוח, יודעת רק מהי התחנה הבאה בשרשרת ואינה יודעת מהי התחנה הסופית או מהו המקור. הסיבה לכך היא שחלק נכבד מהשרתים מוצפן, כך שספק האינטרנט יכול לגלות ברוב המקרים את הצומת הראשון אליו מגיע המשתמש, אך לא את הצמתים הבאים.[27] גם השרת המקבל את הקריאה לא יכול לאתר את הצמתים, אלא רק את הצומת שממנו הוא מקבל את הקריאה למידע/אינטראקציה. למעשה, גם צומת זה מוחלף מדי מספר דקות. בדרך זו, כל הצמתים הנמצאים באמצע הדרך מוגנים ברוב המקרים מפני מעקב פרטי או ממשלתי.[28]

הבעיה העיקרית ברשת TOR טמונה בייחודה: היא מאפשרת אבטחה ואנונימיות, אך היא אינה סמויה עבור ספקי רשת מקומיים. אלה אמנם אינם יכולים לגלות

25 Dakota S. Rudesill, James Caverlee and Daniel Sui, *The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box*, Ohio State Public Law Working Paper No. 314 (Ohio State University, Woodrow Wilson International Center for Scholars, 2015).

26 Ibid; Lev Topor, "Deep and Dark Webs – Liberty or Abuse", *International Journal of Cyber Warfare and Terrorism* 9, no. 2 (2019): 1-14.

27 רועי גולדשמידט, "שימוש בתשתיות תקשורת אנונימיות על גבי הרשת למטרות פשיעה", *מרכז המחקר והמידע של הכנסת*, ינואר 2012.

28 Eric Jardine, *The Dark Web Dilemma: Tor, Anonymity and Online Policing* (London: Global Commission on Internet Governance and Chatham House, 2015).

את המידע והיעדים של משתמשי הרשת, כמו למשל של פעילי מודיעין מערביים במדינות העוינות למערב, אך שימוש בדרך השלילה פתר בעיה זו, לפחות חלקית: ספקי רשת מקומיים יכולים לגלות שמתוך מספר משתמשים מסוים בשכונת מגורים, למשל, משתמש או מספר משתמשים בודדים היו בעלי תעבורת רשת יוצאת דופן. בדרך זו, כל מה שהממשל יכול היה לראות היה תעבורת רשת רגילה, וכל מה שהוא לא יכול היה לראות היה גלישה פרטית ואנונימית.[29]

פרט לתעבורת הרשת המיוחדת המאפיינת את הרשת האפלה, שכאמור עושה מסלול מבלבל וקשה לאיתור במספר צמתים, פלטפורמת TOR, המגיעה בצורת דפדפן נוח לשימוש, יכולה למנוע מאתרים לדלות מידע על משתמשים. הפרטיות היא דבר מקודש ברשת TOR, ואף אתר אינו יכול לדלות מתוכה מידע לגבי מיקום, סוגי חומרה, סוגי תוכנה ודפוסי פעילות. ניתן גם לבטל בדפדפן של TOR את השימוש ב־JavaScript, HTML 5, Media, Images, Icons, Symbols ועוד. כך יוצרת הרשת האפלה פרדוקס מעניין: מצד אחד, היא מקדשת את הפרטיות והאנונימיות, ומצד שני, דווקא יתרונות אלה הופכים לחסרונות כאשר נעשה בהם שימוש על ידי ארגוני פשיעה וטרור וגורמים עוינים, שכן הם מאפשרים להם לסחור במידע בחתימה נמוכה.[30]

בנוסף לנאמר לעיל, הרשת האפלה מהווה מעין שוק לביצוע פעולות לא חוקיות המאפשר, בין היתר, סחר בכלי סייבר. כך, למשל, אם חברה מסוימת מעוניינת לגרום נזק לחברה מתחרה, יש באפשרותה להיכנס לרשת האפלה, לקנות מתקפת כופר, נוזקה או רוגלה ולהפעיל רשת בוטים או כל כלי אחר. ברוב המקרים, הקונה והמוכר מבצעים העברה בביטקוין, מה שמאפשר את שמירת האנונימיות. רשתות אפלות משמשות אפילו כזירות למסחר בנשק ובסמים ולהפצת תכנים פורנוגרפיים,[31] ומהוות כר נוח לפעילות של ארגוני טרור: במשך כעשור, חלק ניכר מהתקשורת בין מנהיגי "אל־קאעידה" ברחבי העולם התנהל על גבי הרשת האפלה.[32] מן העבר השני, ברשת פועלים גופים שייעודם סיכול טרור, כמו למשל ארגוני ביטחון פנים ומודיעין.[33] לפי נתוני חברת Webhose, כחמישים אחוזים מהפעילות ברשת האפלה היא פלילית, שמשמעותם הנוספת היא שמחצית מהפעילות הינה חוקית ולגיטימית.

לאחרונה ניכרת עלייה בשימוש ברשת האפלה ככלי להתארגנות ומידע עבור פעילים במשטרים טוטליטאריים. ברשת האפלה יש גם אתרי מראה (Mirror)

29. Topor, “Deep and Dark Webs – Liberty or Abuse”.
30. Ibid.
31. Nyshka Chandran, “From Drugs to Killers: Exploring the Deep Web”, *CNBC,* June 23, 2015; Cara McGoogan, “Dark Web Browser Tor is overwhelmingly Used for Crime, Says Study”, *The Telegraph,* February 2, 2016.
32. Weimann, “Going Darker”.
33. Topor, “Deep and Dark Webs – Liberty or Abuse”.

לאתרים מוכרים, כמו אתרי חדשות מערביים ומידע, כדי שאנשים החיים במשטרים טוטליטאריים יוכלו להגיע אליהם. כך, למשל, הכתובת facebookcorewwwi.onion מובילה ל"גרסת הבצל" של הרשת החברתית עבור משתמשים במדינות שבהן רשת "פייסבוק" חסומה. באופן דומה, הכתובת nytimes3xbfgragh.onion מובילה ל"גרסת הבצל" של "ניו יורק טיימס". בנובמבר 2018 העלה מהנדס לשעבר בחברת "פייסבוק" "גרסת בצל" ל"ויקיפדיה" – גרסת מראה ברשת האפלה לאנציקלופדיה החופשית, שחסומה לחלוטין או באופן חלקי במדינות שונות.[34] בעוד משטרים טוטליטאריים מתמודדים עם בעיית האנונימיות באמצעות מעצרים וחקירות, הממשל האמריקאי בחר להציף את העולם ברשת TOR, תוך קריאה לקידום חופש הביטוי וזכויות אדם, אנונימיות, תקשורת חופשית ופתוחה והתנגדות למשטרים טוטליטאריים.

שימושים פוטנציאליים ברשת האפלה למִבצעי השפעה

בעבר, כאשר מעצמה רצתה להשפיע על שחקן אחר בזירה העולמית – מדינה, ארגון טרור או אדם מסוים – היא עשתה שימוש בעוצמה צבאית או כלכלית. העידן הקיברנטי הוסיף ממד חדש למושג "עוצמה", בשלבו יכולות קיברנטיות מתקדמות וקלות לתפעול, שיש בהן כדי להפוך את יחסי הכוחות על פניהם ולעיתים אף להוות "שוברות שוויון". לדוגמה, מדינה יכולה לפתח פרויקט צבאי סודי, שעשוי לרדת לטמיון אם פושעי סייבר ומדליפים אחרים יחשפו אותו ברשת.[35] כך, למשל, ביולי 2018 נחשף כי האקר אמריקאי ניסה למכור ברשת האפלה תוכניות רגישות של מל"ט צבאי בשם MQ-9;[36] חברה מתחום התעשייה הצבאית פנתה במהלך השליש השני של שנת 2019 לאחד מכותבי מאמר זה וביקשה לאתר הדלפות עליה ברשת האפלה משום שחששה מפני הדלפת תוכניות רגישות שלה על ידי מספר עובדים מתוכה.

להלן יוצגו מספר פלטפורמות ברשת האפלה העשויות לשמש למבצעי השפעה: 1. פלטפורמות הדלפה; 2. פלטפורמות פסיביות שייעודן אחסון מידע; 3. פלטפורמות סחר. אלו כוללת הצעות למכירת מידע, כלי סייבר התקפיים ובוטים, ואף הצעות ל"מעורבות" מזויפת ברשתות החברתיות.

34 אמיתי זיו, "הצד האפל של האינטרנט: סמים, נשק, מתקפות סייבר ומתנגדי המשטר", **דה מרקר**, 18 ביולי 2018.

35 Joseph S. Nye. “Soft Power and American Foreign Policy”, *Political Science Quarterly* 119 no. 2 (2004): 255-270; Ernest J. Wilson, “Hard Power, Soft Power, Smart Power”, *The Annals of the American Academy of Political and Social Science* 616 no. 1 (2008): 110-124.

36 זיו, "הצד האפל של האינטרנט: סמים, נשק, מתקפות סייבר ומתנגדי המשטר".

פלטפורמות הדלפה

בעידן בו ניתן לגנוב יותר מֶטֶרה־בייט אחד של מידע בשבריר שנייה באמצעות החסן נייד ולהדליף באופן אנונימי בזמן אמת מידע מישיבות ממשלתיות, ביטחוניות ועיסקיות, אין זה מפתיע שתדירותן של ההדלפות גברה.[37] הדלפות משמשות פעמים רבות את אלה המתנגדים לפעולות שנויות במחלוקת, בעיקר בנושאים הקשורים לצבא ולביטחון. יחד עם זאת, לא מעט פעמים הממשל המקומי הוא זה שמפעיל מדליפים, הן באמצעות הפעלה ישירה והן באמצעות הפעלה משוטה: כפי שארגוני ביטחון ושיטור מפעילים סוכנים הפועלים ברשת האפלה (והרגילה) או מתחזים לקטינים כדי ללכוד פדופילים, כך ארגוני מודיעין בכל העולם מפעילים פלטפורמות הדלפה, מפיצים מעין "קולות קוראים" להדלפות ומציעים תשלום עבורן. יתרה מכך, ממשלות רבות אף פונות לספקים חיצוניים, כגון חברות מודיעין עיסקי או חברות היי־טק, כדי לנטר, לנתח ולהפעיל גורמים מסוימים ברשת האפלה.[38] חשוב לציין בהקשר זה שפרויקט הרשת האפלה עלול להיות מלכודת דבש גדולה.[39]

דוגמה מובהקת נוספת לפלטפורמת הדלפה היא אתר העיתונות החופשית "ויקיליקס", שהוקם ב־2006 והספיק מאז לעורר מספר מהומות תקשורתיות לאחר שהדליף מאות אלפי מסמכים, ידיעות וחומרים נוספים על פעילות אמריקאית שנויה במחלוקת. האתר נמצא ברשת האינטרנט הרגילה, אך ממליץ לכל הגולשים בו, המעוניינים לשתף ולהדליף מידע, להשתמש ברשת האפלה. המעוניינים בכך מופנים לרשת האפלה, ממלאים את פרטי הידיעה ונדרשים לתאר אותה בצורה המפורטת ביותר, ובנוסף לכך להעלות קבצים, כגון תמונות או מסמכים, אשר יוכיחו את אמיתותה, וזאת למרות שאין כל חובה מצד האתר לעשות כן.[40]

פלטפורמת הדלפה עיתונאית נוספת היא מערכת Secure Drop, אשר פותחה וקודמה על ידי הארגון Freedom of the Press Foundation. המערכת מספקת שירותי תקשורת והעברת נתונים בצורה מוצפנת ואנונימית. סינדיקטי עיתונות כגון: "Associated Press", "The Guardian", "The New York Times", "Al Jazeera", וכן גורמים רבים אחרים, משתמשים במערכת זו כדי לחלוק ולקבל מידע רגיש.

ממשלות יכולות לעשות שימוש בשתי הפלטפורמות שהוזכרו לעיל כדי להדליף מידע שפרסומו בתקשורת המסורתית הגלויה עשוי להיות בעייתי מבחינתן. דוגמה מובהקת לכך הוא המידע בדבר הימצאותו של נשק גרעיני ברשות מדינת ישראל:

37 Scott Shane, “The Age of Big Leaks”, *The New York Times*, February 2, 2019.

38 Chris Bing, “How the FBI Relies on Dark Web Intel Firms as Frontline Investigators”, *Cyber Scoop*, April 13, 2017.

39 Topor, “Deep and Dark Webs – Liberty or Abuse”.

40 David Leigh, Luke Harding and Charles Arthur, *Wikileaks: Inside Julian Assange’s War on Secrecy* (New York: Public Affairs, 2011).

ישראל אינה חתומה על האמנה הבין־לאומית למניעת הפצת נשק גרעיני (NPT), ועל כן פרסום גלוי בדבר הימצאותו של נשק כזה ברשותה עשוי להיות בעייתי מבחינת החוק הבין־לאומי. יחד עם זאת, פרסום יזום של ידיעות על נשק אסטרטגי בצורה אנונימית דווקא, יכול לחזק את מעמדה הגיאו־פוליטי של ישראל ולהוות איתות למדינות עוינות. כך, למשל, ניתן למצוא בעמוד ייעודי מפורסם באתר The Hidden Wiki מידע על תוכנית הגרעין הישראלית, הכולל, בין היתר, את ציר הזמן של התוכנית ואת הדוקטרינה, המדיניות והשיטות ליישומה. מידע נוסף על הגרעין הישראלי, וכן על הגרעין ההודי ופרויקטים אחרים השנויים במחלוקת, נמצא בפורומים נוספים ברשת האפלה.

פלטפורמות פסיביות שייעודן אחסון מידע

מדובר באתרי אחסון או בפורומים שבהם דנים בנושא מסוים וחולקים מידע לגביו. למשל, באתר DOXBIN ברשת האפלה ניתן להעלות מידע וקבצים שהמדליפים מעוניינים לשמור לשעת הצורך או להדליף לכל. דוגמה לכך הוא מידע שהודלף ב־30 במאי 2019 על שלושים עובדי הבולשת הפדרלית של ארצות הברית (FBI), הכולל את כתובותיהם האישיות ודרכי התקשרות אליהם, כולל מספרי טלפון וכתובות דואר אלקטרוני, פירוט על בני משפחותיהם ועוד.

פלטפורמה נוספת לאחסון מידע עליו ניתן לדון גם עם אחרים הם פורומים, כגון פורום בשם IntelExchange, בו חולקים ידיעות (חלקן הקטן מודלף), או פורום בשם The Stock Insider, בו משתמשים שעברו אשרור חולקים מידע על מסחר בבורסות השונות ומדליפים ספקולציות. דרך נוספת לשימוש באתרי אחסון מידע אופיינית לא רק למדליפים זדוניים, אלא גם לגופים ממשלתיים או לאנשי מודיעין, המעוניינים להעביר מידע בצורה אנונימית. אלה "מדביקים" באתרי האחסון קבצים אותם הם רוצים לחלוק עם אחרים, עושים זאת תחת כינוי מטעה ושולחים מסר בתקשורת המסורתית (למשל, בהודעת טקסט) עם אותו כינוי ספציפי.

פלטפורמת סחר

אתרים אנונימיים שלמים מציעים למכור או לקנות מידע מסווג. חברות עיסקיות בעלות אמצעים מעלות פעמים רבות בקשות לקנות הדלפות הנוגעות לפרויקטים של חברות אחרות, ויש מקרים שבהם עיתונאים או אנשי ביון מבקשים לסחור במידע. כך, למשל, באתר SellFile מציעים לסחור במידע ובשירותים באמצעות תשלום במטבע הביטקוין. כשמדובר במִבצעי השפעה, ניתן לרכוש ברשת האפלה מאגרי בוחרים שלמים, הכוללים פרטי התקשרות, כמו גם נטיות פוליטיות. מידע כזה יכול לשמש כדי לסמן מצביעים פוטנציאליים ברשתות החברתיות.

לא רק מידע נסחר בפלטפורמות אלו. לאחרונה פורסם מחקר, לפיו הרשת האפלה הופכת למקור העיקרי למכירה ולמשלוח של נוזקות המותאמות אישית לפריצות

לארגונים ולמגזרי תעשייה ספציפיים.[41] נוזקות אלו עשויות להיות מופעלות גם במסגרת תקיפות סייבר שמטרתן היא שיבוש מערכות בחירות. בכירים בשירותי המודיעין של ארצות הברית מעריכים שקיים סיכוי גבוה כי האקרים ינסו להטות, ואף להשמיד, את מאגרי רישום הבוחרים לקראת בחירות 2020 לנשיאות ארצות הברית באמצעות וירוס כופר (Ransomware). מתקפות סייבר מסוג זה בדרך כלל נועלות מחשבים הנגועים בווירוס עד אשר התשלום, שלרוב מתבצע באמצעות מטבע הקריפטו, נשלח להאקרים. דוגמה לכך היא מתקפת הסייבר העולמית NotPetya שהוצאה לפועל ביוני 2017 ויוחסה לרוסיה. במתקפה זו נעשה שימוש בווירוס כופר לצורך מיסוך טכניקת מחיקת נתונים, מה שהפך את מחשבי הקורבנות לבלתי שמישים לחלוטין. איום זה מדאיג במיוחד לנוכח השפעתו הפוטנציאלית על תוצאות ההצבעה. מתקפה מסוג זה, שלא זוהתה לפני הבחירות, עשויה לחבל ברשימות הבוחרים, ליצור בלבול ועיכובים עצומים, לגרום לשלילת זכות הצבעה, ואף לפגוע משמעותית בתקפותן של תוצאות הבחירות.[42]

כלי נשק דיגיטליים, כמו התוכנות הזדוניות לפריצה EternalBlue ו־WannaCry, שעקבותיהן מוליכות לצפון קוריאה ואשר גרמו בשנת 2018 נזק שנאמד בכמעט ארבעה מיליארד דולר למערכות מחשבים עיסקיים וממשלתיים במספר מדינות, זמינים אף הם ברשת האפלה בעלות נמוכה יחסית. כלים אלה עשויים לשמש גורמים עוינים למבצעי השפעה בסייבר.[43]

מלבד נוזקות וכלי פריצה, לאחרונה ניכר כי פלטפורמות מדיה חברתית עם מספר רב של חשבונות נטושים מהוות מטרה מרכזית ונוחה להאקרים בשל פגיעויות האבטחה הרבות בהן. רשתות בוטים ב"טוויטר", "פייסבוק" ו"אינסטגרם", שמטרתן להפיץ דיסאינפורמציה ולהגדיל את מידת ה"מעורבות", דהיינו Like ו־Share, כדי ליצור מצג שווא של עניין ציבורי סביב תכנים מסוימים, מוצעות למכירה ברשת האפלה תמורת סכומים זעומים. באופן דומה מוצעות למכירה חבילות נפרדות של "ריטוויטים", "לייקים" וצפיות ב"יוטיוב".[44]

לשלוש הפלטפורמות שנסקרו יש שלושה שימושים נפוצים: העצמת המדינה המדליפה; פגיעה במדינה שעליה מדליפים; קידום זכויות האדם במדינה שעליה מדליפים. כך, למשל, באתר РосПравосудие ברשת האפלה פורסמו כחמישים

---

41 יוסי הטוני, "מהם כלי הפריצה הפופולריים שמוצעים למכירה בדארקנט?", **אנשים ומחשבים**, 11 ביוני 2019.

42 Christopher Bing, “Exclusive: U.S. Officials Fear Ransomware Attack against 2020 Election”, *Reuters,* 26 August 2019.

43 Ibid.

44 Dan Patterson, “The Dark Web is Where Hackers Buy the Tools to Subvert Elections”, *CBS News,* September 26, 2018; “Influence for Sale: Bot Shopping on the Darknet”, *DFRLab*, June 19, 2017.

מיליון מסמכים העוסקים במערכת המשפט הרוסית, שכללו מידע אישי על שופטים, עורכי דין, אנשי פרקליטות ועוד. האתר עצמו מציין כי מפעיליו רוצים להדליף פרטי מידע כדי לגרום לאי־נוחות וללחץ על אלה אשר משתמשים בחוק בצורה מניפולטיבית לטובת הממשל, וחשוב מכך – לרעת אלה העומדים בפני משפט לא הוגן שתוצאותיו כבר נכתבו מראש. לפי שעה לא ברור מי עומד מאחורי אתר זה – אלה המנסים לערער את מעמדה של רוסיה מבפנים ומבחוץ, או אזרחים רוסים המבינים את החשיבות של מערכת משפט תקינה.[45]

להלן מספר דוגמאות לשימושים שכבר נעשו ברשת האפלה בהקשר של השפעה על בחירות: ב־2016 נפרצו השרתים של הוועדה הפדרלית לבחירות בארצות הברית (U.S. Election Assistance Commission), ואישורי כניסה גנובים של עובדיה התגלו ברשת האפלה;[46] באותה שנה השקיעו האקרים רוסיים כ־95,000 דולר במטבע הקריפטו כדי להקים אתרים וחשבונות מדיה חברתית מזויפים ברשת האפלה במטרה להשתמש בהם למִבצעי השפעה;[47] בראשית 2017 חשף משרד המשפטים האמריקאי כי במסגרת מבצעי ההשפעה הרוסיים בבחירות 2016 לנשיאות ארצות הברית, הצליחו האקרים רוסיים להשיג גישה ליותר מחצי מיליארד חשבונות מייל באתר האינטרנט "יאהו". ההאקרים גם הצליחו לחדור לחשבונותיהם של 6,500 משתמשים, וביניהם יעדים שסומנו מראש על ידי הממשל הרוסי, כמו עיתונאים וחברי אופוזיציה. גישה לחשבונות נוספים נמכרה לכל המרבה במחיר ברשת האפלה, ככל הנראה כדי להגדיל את הרווח מהפריצה;[48] ב־2017 גם הוצעו למכירה ברשת האפלה כארבעים מיליון רשומות של אזרחים אמריקאים תמורת ארבעה דולר בלבד. הסכום הנמוך שנדרש תמורת המידע מחזק את הסברה שלא הייתה מטרת רווח מאחורי המכירה, אלא מטרה אידיאולוגית. זאת ועוד, על רקע בחירות אמצע הכהונה בארצות הברית בשלהי 2018, נחשף מאגר מידע של עשרות מיליוני בוחרים אמריקאים שהוצע למכירה ברשת האפלה. המאגר הציע, מלבד פרטיהם האישיים של הבוחרים, גם מידע על השקפותיו הפוליטיות של כל אחד מהם, ובכלל זה האם הוא תומך במועמד רפובליקני או דמוקרטי.[49]

מאגרי מידע אלה יכולים לשמש הן להגברת היעילות בסימון קהלי יעד פוטנציאליים כמטרות והן להגברת תדירותן של מתקפות דיוג. מדובר בהקשר זה

45 Topor, “Deep and Dark Webs – Liberty or Abuse”.
46 Menn Joseph, “U.S. Election Agancy Breached by Hackers after November Vote”, *Reuters*, December 16, 2016.
47 Topor, “Deep and Dark Webs – Liberty or Abuse”.
48 אילן גלר, "פשוט וגאוני: ככה האקרים רוסים פרצו למיליוני חשבונות דואר בלי סיסמה", **וואלה**, 19 במארס 2017.
49 רפאלה גויכמן, "פרטיהם של 62 מיליון בוחרים אמריקאים מוצעים למכירה בדארקנט", **דה מרקר**, 6 בנובמבר 2018.

בהתחזות לספקיות שירות, כמו בנק, מערכת הפעלה או מוסד ממשלתי, במטרה לקבל פרטים אישיים מהמשתמשים, ובאמצעותם להוציא לפועל מבצעי השפעה.[50]

על רקע הבחירות בישראל ב־2019 הוצעו למכירה ברשת האפלה כלי סייבר התקפיים שפותחו על ידי האקרים, ככל הנראה ממוצא אוקראיני, שנועדו להתגבר על ההגבלות שהטילה "ווטסאפ" על מספר אנשי הקשר אליהם ניתן להעביר מסרים בעת ובעונה אחת. כלי הסייבר שהוצעו ברשת מקנים למי שרוכש אותם יכולת להשתלט מרחוק על כל קבוצות ה"ווטסאפ" בישראל ולשתול בתוכן סרטונים או מסרונים כרצונו. מעבר לכך, החברים בקבוצת הצ'ט לא יקבלו את הסרטון ממספר לא מוכר, אלא מאחד החברים האחרים בצ'ט, מה שיגביר את רמת המהימנות של הסרטון.[51] לטענת בן כספית, לאחרונה רכשו גורמים ישראליים במאות אלפי דולרים את האופציה לשיגור 15 מיליון הודעות "ווטסאפ" בתוך 48 שעות. האפשרות של "פייסבוק" לחסום יכולת זאת הינה מוגבלת, אם כי ברשת האפלה יש האקרים המוכרים יכולת הגנת נגד, שתוקפת את הסרטונים הללו עם הופעתם, יוצרת ביקוש מלאכותי עצום וגורמת לקריסת המערכת.[52]

סיכום

מטרתו של מאמר זה היא להסב את תשומת הלב לרשת האפלה כערוץ נוסף להוצאתן לפועל של מתקפות סייבר ומבצעי השפעה בסייבר, ולהסביר כיצד השחקנים השונים מממשים זאת. חשיבותה של הרשת האפלה כפלטפורמה לניסיונות השפעה על מערכות בחירות הולכת וגוברת בחודשים האחרונים, בד בבד עם הִתרבות הניסיונות להתערבות זרה במערכות בחירות ברחבי העולם, בעיקר מצד רוסיה. כפועל יוצא מתופעה זו חלה עלייה במאמצי ההתגוננות של ענקיות המדיה והמדינות עצמן נגד שיטות הפעולה המוכרות בתחום זה. על רקע זה ניכרות ירידה בשימוש בבוטים ברשתות החברתיות לצורך מבצעי השפעה ועלייה בפעילות באפליקציות להעברת מסרים מיידיים. עלייה בפעילות חלה גם ברשת האפלה, המאפשרת פרטיות ואנונימיות במידה גבוהה יותר מאשר ברשת הרגילה, ומשום כך מהווה אתגר להתמודדות עם מבצעי השפעה. מעבר להיותו אתגר טכנולוגי, מדובר גם במקרה זה בהתנגשות בין הצורך להגן על השיח הציבורי ובין עקרון השמירה על חופש הביטוי, אותו חותרת, בין היתר, לקדם הרשת האפלה.

בהמשך המאמר נסקרו שלוש פלטפורמות הדלפה עיקריות ברשת האפלה: פלטפורמות הקוראות למדליפים להדליף מידע, כגון WikiLeaks או Secure Drop;

50 Patterson, "The Dark Web is Where Hackers Buy the Tools to Subvert Elections".

51 בן כספית, "האיום על הבחירות הגורליות האלו נמצא בעולם התחתון של האינטרנט", **מעריב**, 9 בספטמבר 2019.

52 שם.

פלטפורמות פסיביות, כגון DOXBIN, IntelExchange או The Stock Insider, המשמשות לאחסון מידע מודלף; פלטפורמות סחר, דוגמת SellFile, בה מוצע מידע למכירה ומתקבלות בקשות למידע לפי הזמנה. בנוסף לכך, ברשת האפלה זמינים לרכישה נוזקות, רוגלות, רשתות בוטים וכלי סייבר והצפנת תקשורת, באמצעותם ניתן להוציא לפועל את מבצעי ההשפעה בצורה קלה ואנונימית.

כלים אלה, כמו גם שלוש הפלטפורמות המוזכרות לעיל, עשויים לשמש מדינות וארגונים כדי להוציא לפועל מבצעי השפעה במרחב הקיברנטי, כפי שהודגם במאמר. אמנם, מהימנותו של המידע הזורם ברשת האפלה שנויה במחלוקת, אך נראה שפעמים רבות אין הדבר רלוונטי עבור גורמים החותרים להוציא לפועל מבצעי השפעה, שעצם ההדלפה משמשת את מטרתם המרכזית – זריעת ספק וערעור הַסדר הקיים. לנוכח עלותן הנמוכה יחסית של היכולות המוצעות למכירה ברשת האפלה והקושי להתחקות אחר המקורות המדליפים בה, ניתן לצפות בשנים הקרובות לעלייה בהיצע ובביקוש של אמצעים ברשת זו לצורך הוצאתם לפועל של מִבצעי השפעה.

סוגיה מעניינת נוספת העולה מן העיסוק בנושא היא נוכחותם של משטרים דמוקרטיים ברשת האפלה והשימוש שהם עושים בה: מצד אחד, הצורך להתמודד עם חתרנותם של ארגוני טרור ומשטרים טוטליטאריים, כמו גם עם פשיעה, יוצר מצב שבו אין מנוס ממעורבות ברשת האפלה, בבחינת "דע את האויב"; מצד שני, עצם השימוש שעושים משטרים דמוקרטיים ברשת האפלה ובאנונימיות שלה מעורר לכאורה בעייתיות; אמנם, משטרים דמוקרטיים אינם פטורים ממשחק קשוח בזירה הבין־לאומית, אך הדרך בה הם עושים זאת היא בעלת חשיבות, במיוחד כאשר משטרים אלה מתיימרים להיות "ערכיים" יותר מהמשטרים הטוטליטאריים. יש להניח שהמשטר הדמוקרטי שהשיק רשת אפלה גם עושה את השימוש הנרחב ביותר בה, כפי שרמז בכיר בממשל האמריקאי.[53]

שאלה ערכית חשובה נוספת העולה מהמאמר היא: האם משטרים דמוקרטיים עושים שימוש ברשת האפלה לא רק נגד יריבים בזירה הבין־לאומית, אלא גם נגד יריבים מבית? חברי פרלמנט רבים ברחבי העולם, כמו גם חברי כנסת בישראל, מדליפים מידע מישיבות, ואלה הנתפסים עשויים לעמוד לדין. לעומת זאת, הדלפה ברשת האפלה יכולה לאפשר גם אנונימיות גדולה יותר וגם לזרוע כאוס במערכת הפוליטית.

53 לאחד מכותבי המאמר במהלך כנס בוושינגטון בספטמבר 2019.

שינוי חברתי באמצעות הנגשה ממוחשבת של כללים משפטיים

עו״ד מיכל תג׳ר, מיכאל בר־סיני, מור וילוז׳ני

המאמר מציג מערכת הנגשת זכויות בעזרה עצמית באמצעות ראיון אינטרנטי. הראיון מבוסס על מודל פורמלי של כללי המשפט הרלוונטיים ואינו דורש מעורבות של נציג שירות, אלא רק של המשתמש הרוצה להבין מהן זכויותיו. בנוסף לכך, המאמר מציג מתודולוגיה לבניית מודלים וראיונות להקשרים חברתיים דומים ומתאר בנייה של מודל לזכויות עובדים בסיום העסקה על פי הדין הישראלי. בנוסף לביצוע ראיונות, מודלים אלה מאפשרים לערוך עיבודים ממוחשבים נוספים של החוק, כגון יצירת שרטוטים וביצוע שאילתות. מערכות מסוג זה יכולות למלא תפקיד מרכזי בהעצמת אוכלוסיות חלשות, מכיוון שהן מאפשרות להנגיש זכויות בצורה ידידותית המותאמת למקרה של המרואיין, במקום להעמיס עליו מידע רב שקשה להתמצא בו. המערכת המוצגת במאמר זה — PolicyModels — ניתנת לשימוש בהקשרים נוספים, כגון מידול דרישות פרטיות במסדי נתונים.

מילות מפתח: שיתוף מידע, כלי תוכנה, מודלים חישוביים, הגנת מידע, דיני עבודה, זכויות עובדים

הקדמה

בכל יום צובאים עשרות עובדים על המשרדים העמוסים של ״קו לעובד״. עובדים אלה באים מרקעים שונים, מארצות שונות, ודוברים שפות שונות. קבלת הקהל מאורגנת כך, שבכל יום מגיעות אוכלוסיית עובדים אחרת וקבוצת מתנדבים אחרת. כך, למשל, לימי קבלת קהל של מבקשי מקלט מגיעים מתנדבים דוברי טיגרינית

עו״ד מיכל תג׳ר עוסקת משנת 2003 בעריכת דין בנושאי עבודה והגירה במסגרת ארגונים לשינוי חברתי ללא מטרות רווח. מיכאל בר־סיני הגיש עבודה לתואר דוקטור בהנדסת תוכנה לאוניברסיטת בן־גוריון בנגב, משמש כעמית במכון למחקר סוציולוגי כמותי באוניברסיטת הרווארד (IQSS), והקים את CodeWorth.io. מור וילוז׳ני היא מהנדסת תוכנה בכירה ב־CodeWorth.io. העבודה המתוארת כאן מומנה בחלקה על ידי רשות החדשנות, דרך מסלול ״חדשנות במגזר הציבורי״.

וערבית, ולימי קבלת קהל של מהגרי עבודה בחקלאות מגיעים מתורגמנים לתאית. בצוות העובדים הישראלים נמצאים גם דוברי אמהרית ורוסית. העובדים מבקשים מידע, סיוע ועצה, ולעיתים קרובות גם סיוע משפטי להבנת זכויותיהם ומימושן. במרכז החדר יש דוכן ובו דפי מידע על חוקי עבודה, ביטוח לאומי, ביטוח רפואי, אשרות למבקשי מקלט, מידע לעובדי סיעוד, וגם מידע הנוגע להטרדה מינית. מכיוון שהפונים מתקשים למצוא את הדף המתאים לבעיה שלהם, הם נאלצים להמתין בתור הארוך והמתארך.

אדם שזכויותיו נפגעו צריך לעבור מספר שלבים עד הבשלת השלב של התביעה המשפטית. השלבים מכונים Naming, Blaming, Claiming:[1] השלב הראשון הוא הענקת שם לפגיעה, כלומר היכולת להעניק לה הגדרה משפטית; השלב השני הוא שלב הטלת האשמה, שעיקרו ההבנה מיהו הגורם האחראי לפגיעה בזכויות וההתייצבות מולו; השלב השלישי הוא שלב הפנייה לערכאות, שבו הטענות והתובנות מתורגמות לשפה משפטית. פרק הזמן שתהליך זה נמשך הוא ארוך במיוחד אצל נפגעים השייכים לאוכלוסיות המוחלשות.[2] הניסיון המצטבר מעיד כי ככל ששני השלבים הראשונים בתהליך מתרחשים בצמידות לאירוע, כך גדלים הסיכויים לאיין את הפגיעה ולהשיב את המצב לקדמותו (כמו, למשל, בפיטורים לא חוקיים), או להגיש תביעה ללא חשש להתיישנות העבירה.

חיפשנו דרך קלה וישירה שתאפשר לעובד גישה עצמאית אל המידע הנדרש, כך שיוכל לעבור בכוחות עצמו את שלבי ה־naming וה־blaming. פתרון אפשרי מצאנו בכלי המכונה PolicyModels. כלי זה מאפשר יצירת מודל פורמלי של כללים משפטיים ועיבוד ממוחשב שלו בדרכים שונות. המונח "מודל פורמלי" לקוח מתחום הנדסת התוכנה ומתייחס לתיאור מוגדר היטב של מערכת כלשהי באמצעים מתמטיים (כגון, תורת הקבוצות או תורת הגרפים). יישומי ניווט (כגון Waze) הם דוגמה לכלי תוכנה המבוסס על מודל – במקרה זה מודל פורמלי של הסביבה הבנויה. כך, משתמשים יכולים לקבל הדרכה להגיע ליעד ספציפי, או מידע על כל תחנות הדלק במרחק שלושה קילומטרים ממיקומם הנוכחי.

מודל של כללים משפטיים במערכת PolicyModels, אותו נכנה כאן "מודל מדיניות", מורכב משני חלקים עיקריים:

- **מרחב מדיניות**: מתאר את כל המצבים שבהם אזרח יכול להימצא בהקשר המשפטי אותו מתאר המודל.

1 William Felstiner, Richard Abel & Austin Sarat, "The Emergence and Transformation of Disputes: Naming, Blaming, Claiming", *Law & Society Review* 15, no. 3 (1980): 631.

2 יובל אלבשן, "נגישות האוכלוסיות המוחלשות בישראל למשפט", **עלי משפט** ג׳, תשס"ד, עמ׳ 501־503.

- **גרף החלטה**: גרף המדריך את המשתמש במרחב המדיניות בעזרת שאלות והוראות למחשב.

ניסיון היומיום ב״קו לעובד״ מלמד כי אנשים, בפרט כאלה הנמנים על אוכלוסיות מודרות, אינם יודעים לכנות בשמות משפטיים את שאירע להם. לכן, כשעסקנו בזכויות הנובעות מהעסקה שנגמרה, לא קראנו למודל הזכויות ״פיטורים״, ״התפטרות״ או ״התפטרות בנסיבות פיטורים״, אלא התחלנו מהמצב של ״נפסקה העבודה״. ממצב זה, שכל אדם יודע להעיד עליו, מתחיל שרשור של שאלות, המנוסחות בשפה פשוטה ומיועדות לתרגום לכל השפות. משאלות אלו נגזרות מסקנות משפטיות והמלצות לפעולה במישורים שונים, ובעקבותיהן נקבעים גורמים שאליהם כדאי לפנות כדי לטפל בסיטואציה. למשל, להפסקת עבודה יש השלכות בכל מישורי החיים. השלכות אלו נגזרות ממעמדו של האדם במדינת ישראל: אין דין הפסקת עבודה של מהגר עבודה במסלול של כבילה למעסיק[3] כדין הפסקת עבודה לעובדת ישראלית בהריון. הראשון חייב לטפל במהירות בסוגיות הנוגעות לאשרת השהייה שלו כדי לעבור למעסיק אחר; השנייה תצטרך לפנות לממונה על חוק עבודת נשים במשרד העבודה והרווחה, ועליה לדעת שפיטוריה אינם תקפים, אלא אם הממונה נתן היתר למעסיק לעשות זאת.

ניסינו להעריך את כל ההשלכות המשפטיות שיכולות להיות לסיטואציה מסוימת, תוך שימת דגש מיוחד על אוכלוסיות מוחלשות שיתקשו לאסוף את המידע בעצמן ושיחסי הכוחות בעניינן בלתי שוויוניים באופן קיצוני, ולתת להן מענה נגיש, מהיר, עצמאי ומותאם אישית. התאמה זו מהווה שיפור משמעותי ביחס לאתרי הנגשת זכויות קיימים (דוגמת האתר **כל זכות**),[4] המבוססים על תיאור טקסטואלי של הזכויות. תיאור כזה אמנם מפַשט את המונחים המשפטיים, אך המשתמש עדיין נדרש לקרוא טקסט רב, בין השאר על זכויות או מצבים משפטיים שאינם רלוונטיים למקרה הפרטי שלו. בנוסף, תרגום אתרים מסוג זה דורש מאמץ רב, מה עוד וטבע העבודה של ״קו לעובד״ דורש תרגומים למספר גדול יחסית של שפות.

3 הסדר הכבילה למעסיק יוסד על סמכותו של שר הפנים, על פי סעיף 6 לחוק הכניסה לישראל. סעיף זה מקנה לשר הפנים סמכות ״לקבוע תנאים למתן אשרה או רישיון ישיבה ולהארכה או החלפה של רישיון ישיבה ...״, וכן סמכות ״לקבוע באשרה או ברישיון ישיבה תנאים שקיומם יהיה תנאי לתוקפם של האשרה או של רישיון הישיבה״. חוק עובדים זרים, תשנ״א–1991, ס״ח 1349 (להלן: **חוק עובדים זרים**) מורה כי ״לא יקבל אדם עובד זר לעבודה, אלא אם כן הממונה או עובד משרד הפנים מטעמו התיר בכתב את העסקתו של העובד הזר אצל אותו מעסיק, ובהתאם לתנאי ההיתר״ (סעיף 1יג(א)). לתיאור הסדר זה – ״נוהל מעבר ממעסיק למעסיק״ – שנקבע בשנת 2002, ראו: בג״ץ 4542/02, **קו לעובד נ׳ ממשלת ישראל**, פ״ד סא(1) 346, פסקאות 7, 9־11 לפסק דינו של השופט לוי (2006) (להלן: עניין **הסדר הכבילה**).

4 **כל זכות**, https://www.kolzchut.org.il.

המאמר שלהלן מאורגן באופן הבא: פרק "מטרות" מפרט את יעדי פרויקט מידול זכויות בסיום העסקה (עליו מתבסס מאמר זה); פרק "מעבר משדה משפטי לשדה ממוחשב" מפרט את האתגרים ביצירת תיאור פורמלי של כללים משפטיים ומציע מענה לאתגרים אלה; פרק "מערכת PolicyModels" מספק תיאור כללי של מערכת התוכנה בה השתמשנו ליצירת המודל המשפטי ולביצוע ראיונות; פרק "שיטה לבניית מודלי מדיניות" מציע מתודולוגיה כללית לבניית מודלים להנגשת זכויות.

מטרות

הפרויקט מיועד לפעול בשדה של זכויות עובדים, וכוונתו היא לתת לכלי הממוחשב תפקיד ממשי באיזון אי־השוויון האינהרנטי הקיים בין עובדים ובין מעסיקים.[5] הושטת סיוע לעובדים בעלי כוח מיקוח מוגבל בשוק העבודה היא "הבסיס המוסרי והנרטיב המכונן" של משפט העבודה,[6] ובלשון בית הדין הארצי לעבודה: "משפט העבודה הוא משפט של 'אי שוויון', שמטרתו לפצות [על] חולשתם של העובדים מול המעבידים".[7]

על מצע מסורתי זה של דיני העבודה מתרחשים תהליכים הפוכים. תופעת הגלובליזציה ותמורות בכלכלה ובחברה הישראלית יצרו במהלך העשור האחרון שינויים משמעותיים בשוק העבודה בישראל. תאגידים רב־לאומיים משפיעים ביתר שאת על הכלכלה המקומית; ארגונים רבים עוברים תהליכי שינוי; הדרישה ליעילות כלכלית מתחזקת, ובד בבד ערכים כמו העבודה המאורגנת והסולידריות החברתית נדחקים הצידה; ניודם של עובדים ומפעלים היה לדבר שבשגרה; המדינה מקדמת הליכים של הפרטת שירותים ציבוריים בשם היעילות הכלכלית; האינדיבידואליזם מתחזק והתחרות החופשית הופכת לזכות יסוד חוקתית;[8] עובדים לא ישראלים

5 Judy Fudge, “Labour as a ‘Fictive Commodity’: Radically Reconceptualizing Labour Law”, in *The Idea of Labour Law*, eds. Guy Davidov and Brian Langille (Oxford University Press 2011), pp.120, 124; Paul Davies and Mark Freedland, *Kahn-Freund’s Labour and the Law* (3rd ed. London: Stevens & Sons, 1983), p.18: “The main object of labour law has always been, and we venture to say will always be, to be a countervailing force to counteract the inequality of bargaining power, which is inherent and must be inherent in the employment relationship. Most of what we call protective legislation… must be seen in this context. It is an attempt to infuse law into a relation of command and subordination”.

6 Brian Langille, “Labour Law’s Theory of Justice”, in *The Idea of Labour Law*, p. 101, footnote 83, p. 105. עם זאת, הרעיון המרכזי המוצג במאמר זה הוא כי יש לנסח תכלית חדשה לדיני העבודה במקום התכלית המסורתית.

7 דיון בית דין לעבודה (ארצי) שם/35–2, **קוזלוביץ נ' "אורדן" בע"מ**, פד"ע י"ב (1), 1981, עמ' 200.

8 ראו בין היתר: ר' בן ישראל, "זכות היתר (הפררוגטיבה) הניהולית של המעביד", **עיוני משפט** כ"ה, תשס"ו; ר' בן ישראל, "צדק חברתי בעידן בתר העבודה", בתוך: מ' מאוטנר (עורך),

משתתפים בשוק העבודה במכסות הולכות וגדלות, משפיעים על נורמות ההעסקה בענפים רבים ומושפעים בעצמם ממדיניות הגירה, שבתורה משפיעה באופן עמוק על זכויותיהם בעבודה ועל כוח המיקוח שלהם.[9]

מצד שני, נגישות הציבור למידע הולכת וגוברת, והרשתות החברתיות משמשות כיום מקור מידע עיקרי.[10] ב"קו לעובד" הלכה והתגברה ההכרה בחשיבותו של כלי זה דווקא עבור אוכלוסיות מבודדות עם מחסומי שפה, ולפיכך העמותה שמאחורי "קו לעובד" מפעילה מספר עמודי "פייסבוק" ייעודיים לקהילות שונות של עובדים ובשפות שונות. לדוגמה, בדף ה"פייסבוק" שמוקדש למהגרות עבודה בענף הסיעוד חברות למעלה מ־40,000 עובדות (שני שליש ממספר מהגרות העבודה בענף זה בישראל), וכל פוסט זוכה למאות שיתופים, תגובות ושאלות. נראה כי ככל שהאוכלוסייה מבודדת יותר, עולים החשיבות של הנגשת המידע וכוחה של הטכנולוגיה ליצור קהילה, ולו וירטואלית, שמקלה על הבידוד החברתי ומהווה כתובת נגישה למידע ולייעוץ. בהקשר זה יש לציין כי מחקרים מצביעים על שימוש מוגבר של נשים במדיה חברתית ומציינים את תפקידו של שימוש זה ביחסי הכוחות המגדריים.[11] עם זאת, כמות המידע הזמין מקשה על העובדים למצוא בעצמם את המידע הרלוונטי להם, ועמיתיהם לקהילה הווירטואלית לרוב אינם מקצועיים מספיק כדי לעזור להם בכך.

נתייחס בקצרה אל תיאוריית "עושר המדיה",[12] – נקודת מבט המאפשרת לבחון את אמצעי התקשורת השונים על פי יכולתם לשאת מידע. הנחת היסוד היא שככל

צדק חלוקתי בישראל, הוצאת רמות, 2000; א' גרוס, "כיצד הייתה 'התחרות החופשית' לזכות חוקתית", **עיוני משפט** כ"ג, תש"ס.

9 גיא מונדלק, "עובדים או זרים בישראל? חוזה התשתית והדפיציט הדמוקרטי", **עיוני משפט** כ"ז(2), 2003, עמ' 423.

10 מכון המחקר Pew השווה בין השימוש שנעשה ברשתות החברתיות בארצות הברית בשנת 2005 לזה של שנת 2011. מהמחקר עולה כי במהלך שש השנים הללו חלה עלייה רבה במספר המשתמשים ברשתות חברתיות. בשנת 2005, רק שמונה אחוזים מאוכלוסיית הגולשים דיווחו על שימוש ברשת חברתית; נכון לשנת 2011, שני שליש (65 אחוזים) מאוכלוסיית הגולשים הבוגרת משתמשים באתרים של רשתות חברתיות – יותר מפי שניים מנתוני שנת 2008, שבה דיווחו 29 אחוזים כי הם משתמשים ברשת חברתית.

11 מכון המחקר Pew מוצא במחקריו באופן עקבי דפוס, שלפיו נשים משתמשות ברשתות חברתיות יותר מאשר גברים באותן מדינות.

12 John Carlson and Robert Zmud, "Channel Expansion Theory and the Experiential Nature of Media Richness Perceptions", *Academy of Management Journal*, 42, no. 2 (2017): 153-170; Vivian Sheer and Ling Chen, "Improving Media Richness Theory: A Study of Interaction Goals, Message Valence and Task Complexity in Manager-Subordinate Communication", *Management Communication Quarterly* 11, no. 1 (2004): 76-93; Richard Daft and Robert Lengel, "Information Richness: A New Approach to Managerial Behavior and Organizational Design", *Research in Organizational Behavior*, vol. 6 (1984): 191-233.

שהמידע עמום יותר, יש לבחור באמצעי תקשורת עשיר יותר, כאשר האמצעי העשיר ביותר הוא תקשורת פנים־אל־פנים. אולם, "פרדוקס העושר" גורס שאמצעי תקשורת "עשיר" עלול להעביר מידע רב מדי (שבחלקו לא רלוונטי), להסיח את הדעת מהמסר העיקרי ולהפריע בהבנת המצב. פרדוקס זה עשוי להסביר גם את השימוש הדל בדפי המידע העמוסים במשרדי "קו לעובד". ברוב המקרים, העובד הנמצא במצוקה אינו פנוי למצוא את "המחט בערמת השחת".

האם מצבו של העובד הוא באמת כה עמום עד שנדרשת פגישה אישית שלו עם מתנדב של "קו לעובד"? המידול שאנו מציעים כאן טוען שאפשר גם אחרת. בהחלטות צרכניות, האינטרנט משפיע על הצרכנים יותר מכל;[13] מטרתנו בפרויקט זה היא למקסם את יכולת ההשפעה של האינטרנט לצורך רווחת העובד הנמצא במצוקה.

המעבר משדה משפטי למודל ממוחשב

משפט וטכנולוגיה הם חלק מ"תרבות".[14] בדומה לספרות ולמשפט, "אלה שתי תופעות תרבותיות שונות שקיים ביניהן קשר מורכב, ולמרות השוני – הן צריכות זו לזו ומשלימות זו את זו".[15] תקצר היריעה מלדון בהבדל בין כללים משפטיים ובין מודל טכנולוגי. סוד גלוי הוא שהשדה המשפטי אינו ערוך להבניה חד־משמעית. לא במקרה, הכרעות משפטיות נכתבות על פני עשרות ומאות עמודים. השדה המשפטי מורכב מחקיקה ראשית, מתקנות (חקיקת משנה), מהלכות משפטיות שנקבעו בבתי המשפט, ואפילו מנהלים של משרדי ממשלה. פרשנות משפטית לעניינו של אדם תחייב לברור נתונים מתוך אירועי חייו, לתת להם כותרת משפטית, ולבסוף לפנות לפרשנות.

גם הטכנולוגיה טומנת בחובה בחירות פרשניות שעלולות להיות מוטות:[16] למשל, הנחות סמויות לגבי יכולות של משתמשים עלולות ליצור מצב שבו יימנע

---

13 Brian Solis, "Report: The Rise of Digital Influence and How to Measure It," *BrianSolis*, March 21, 2012, https://www.briansolis.com/2012/03/report-the-rise-of-digital-influence/.

14 ראו דיון מקיף במשפט כתרבות אצל: מנחם מאוטנר, "המשפט כתרבות, לקראת פרדיגמה מחקרית חדשה", בתוך: מנחם מאוטנר, אבי שגיא, רונן שמיר (עורכים), **רב־תרבותיות במדינה דמוקרטית ויהודית**, הוצאת רמות, 1998, עמ׳ 545־587, וכן: מנחם מאוטנר, "המשפט הסמוי מהעין", **אלפיים**, 16 (תשנ"ח), עמ׳ 45־72.

15 שולמית אלמוג, **משפט וספרות בעידן הדיגיטלי**, הוצאות נבו, 2007, עמ׳ 5.

16 Kate Crawford and Tarleton Gillespie, "What is a Flag for? Social Media Reporting Tools and the Vocabulary of Complaint", *New Media & Society* 18, no. 3 (2016): 410-428; Sandra Petronio, Jess Alberts, Michael Hecht and Jerry Buley, eds., *Contemporary Perspectives on Interpersonal Communication* (Madison, Brown & Benchmark, 1992), pp. 318-358; Janet Bavelas, "Some Problems with Linking Goals to Discourse", in

מאנשים מסוימים להשתמש במערכת. דוגמה להנחה כזאת היא עיצוב שלא מביא בחשבון עיוורי צבעים. במקרים שבהם מתכנני המערכת מניחים לטכנולוגיה לבצע החלטות בעצמה, למשל על ידי שימוש בטכניקות של אינטליגנציה מלאכותית או למידה ממוחשבת, עלולה להיווצר אפליה אלגוריתמית של ממש. במקרים כאלה, מערכת ממוחשבת עלולה להפגין אפילו התנהגות גזענית[17] או מיזוגנית.[18]

כדי להשיב על השאלה מהן הזכויות והחובות הנובעות ממצב אישי מסוים (למשל, הפסקת עבודה של מהגר עבודה לאחר התקף לב), צריכה להיות מוכנות לוותר על אבחנה מתבקשת בין מה שנקבע בחוק, ומצוי לפיכך בדרגה הגבוהה ביותר, לבין מה שקובעים נוהלי משרד הפנים, שמעולם לא עברו ביקורת שיפוטית. הדין במודל ממוחשב אינו יכול להיות מרובד כפי שהוא בפסקי דין, בעתירות ובכתבי תביעה. עבודה על מידול ממוחשב דורשת מוכנות לפשט את השדה המשפטי, להנגישו ולוותר על ההיררכיות בתוכו; הוא חייב לעבור התאמה לכלי הממוחשב ולמגבלותיו, תוך הבנה שמגבלות אלו, ברוח אותו ״פרדוקס העושר״ שהוזכר לעיל, הן גם יתרונותיו.

מערכת PolicyModels – הכרה, תיאור, תכונות

כדי ליצור מודלים פורמליים לכללים משפטיים (״מודלי מדיניות״), השתמשנו במערכת PolicyModels,[19] המאפשרת לבנות תיאור פורמלי של כללים משפטיים בתחום מסוים, ולחשב כיצד הם מתייחסים למקרה ספציפי. המערכת פותחה במקור כדי לאפשר לחוקרים לטפל במסדי נתונים רגישים, מבלי להפר חוקים המתייחסים לפרטיות ומבלי שיידרשו למומחיות בתחומי הפרטיות או הטכנולוגיות

Understanding Face-to-Face Interaction: Issues in Linking Goals and Discourse, ed. K. Tracy (Hillsdale, NJ: Lawrence Erlbaum, 1984), pp. 119-130.

17 Latanya Sweeney, “Discrimination in Online Ad Delivery”, *ACM Queue – Storage* Vol. 11, no. 3 (April 2, 2013); Julia Angwin, Jeff Larson, Surya Mattu and Lauren Kirchner, “Machine Bias”, *ProPublica*, May 23, 2016, https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

18 Amit Datta, Michael Carl Tschantz, Anupam Datta, “Automated Experiments on Ad Privacy Settings: A Tale of Opacity, Choice and Discrimination”, *Proceedings on Privacy Enhancing Technologies*, 2015, pp. 92-112.

19 Michael Bar-Sinai, Latanya Sweeney and Merce Crosas, “DataTags, DataHandling Policy Spaces and the Tags Language”, *IEEE Security and Privacy Workshops*, San Jose, CA, 2016, pp. 1-8.

הרלוונטיות.[20] מאוחר יותר נעשה שימוש במערכת זו כדי למדל את פרק דמי האבטלה בחוק הביטוח הלאומי בישראל.[21]

בהינתן מודל מדיניות, מערכת PolicyModels יכולה להציג בעזרתו ראיון אינטראקטיבי, המיישם אותו על מקרה ספציפי. בנוסף לכך, המערכת יכולה לצייר תרשימי זרימה ומבנה של המודל, וכן לזהות את כל המקרים שבהם תנאי כלשהו מתקיים (למשל, כל המקרים שבהם עובד יכול לתבוע את המעסיק). מבנה המערכת מאפשר לבצע ניתוחים נוספים לפי הצורך.

המערכת עצמה מורכבת מליבה וממספר כלים. ליבת המערכת היא רכיב של תוכנה ("ספריה") המאפשרת לתוכנות מחשב שבהן היא כלולה לעבוד עם מודלי מדיניות. סביב ליבה זו פותחו שתי תוכנות: האחת משמשת לפיתוח המודלים, והשנייה היא אתר אינטרנט המאפשר לבצע ראיונות על בסיס המודלים.

הקוד במערכת PolicyModels משוחרר ברישיון קוד פתוח ידידותי לתעשייה (Apache v2.0). רישיון זה מאפשר לכל גורם לקרוא את קוד המקור של המערכת ולפתח על בסיסה מערכות נוספות, כולל מערכות מסחריות, מבלי לשלם על כך. רישיונות מסוג זה מונעים "נעילה" לספק תוכנה מסוים ("vendor lock-in"), וכך שומרים על כוח המיקוח אצל הגופים המשתמשים במערכת, המסוגלים להחליף את ספקי התוכנה לפי שיקוליהם. בנוסף לכך, רישיונות אלה מאפשרים כתיבת תוכנות על ידי מתנדבים ומעודדים יצירה של קהילות משתמשים ומפתחים.

להלן נציג את מבנה המודלים של PolicyModels, וכן את הכלים הקיימים לפיתוחם והנגשתם של מודלים אלה.

מודל מדיניות

כאמור, מודל מדיניות מורכב משני חלקים: מרחב מדיניות וגרף החלטה. **מרחב מדיניות (Policy Space)** מתאר את כל המצבים האפשריים של אדם בהקשר המשפטי שעל פיו נבנה המודל. תיאור זה בנוי בצורת מרחב רב־ממדי, בו כל נקודה מתארת סיטואציה אפשרית אחת תחת החוק. כל ממד במרחב מתאר היבט משפטי יחיד, וכל קואורדינטה בממד נתון מתארת מצב אפשרי של היבט זה. לדוגמה, הקואורדינטות עבור ממד "קבוצת גיל" יכולות להיות "לפני גיל העבודה", "בגיל העבודה", "גיל פנסיה וולונטרית" ו"גיל פנסיה" (בסדר הזה). ממדי המרחב הם סודרים (ordinal), כלומר, יש סדר בין הקואורדינטות, אולם אין משמעות

20 Latanya Sweeney, Merce Crosas, Michael Bar-Sinai, “Sharing Sensitive Data with Confidence: The Datatags System”, *Technology Science*, October 16, 2015, http://techscience.org/a/2015101601

21 Michael Bar-Sinai and Rotem Medzini, “Public Policy Modeling using the DataTags Toolset”, *The Network for European Social Policy Analysis*, 2017, http://mbarsinai.com/files/inii/ESPAnet17-Final.pdf.

למרחקים ביניהן.[22] סדר זה מאפשר לנסח באופן פורמלי כללים, כמו ״מגיל העבודה ואילך, עובד זכאי ל־X״.

ככל שמספר הממדים גדל, כך גדל גם הדיוק האפשרי בתיאור סיטואציה משפטית נתונה. יחד עם זאת גדל גם מספר השאלות עליהן נדרשים משתמשי השאלון לענות. לכן, מרחב מדיניות יעיל יכיל מספיק ממדים כדי לתאר את כל ההיבטים הרלוונטיים של הסיטואציה, אולם לא מעבר לכך. לדוגמה, במרחב המדיניות של מודל זכויות בסיום העסקה יש טעם לפרֵט האם העובד סובל מנכות, אולם אין טעם לפרט מהי נכות זו. זאת, מכיוון שפרטי הנכות לא משנים את זכויות העובד כאשר העסקתו מסתיימת.

מרחב מדיניות טיפוסי מכיל מספר רב של ממדים: מודל הזכויות בסיום העסקה, המתואר בהמשך, מכיל 62 ממדים; מודל דמי האבטלה לפי חוק הביטוח הלאומי מכיל 13 ממדים; ואילו מודל חוקי הפרטיות, הנוגעים למסדי נתונים מדעיים, כולל 58 ממדים.[23] לבני אדם הרגילים לעולם תלת־ממדי קשה לעבוד באופן אינטואיטיבי עם כמות גדולה כל כך של ממדים. על רקע זה פיתחנו מספר תצוגות שמאפשרות להנגיש מרחבי מדיניות מרובי ממדים. בנוסף לכך, שפת תיאור מרחבי המדיניות של PolicyModels כוללת אמצעים שנועדו לקבץ את הממדים באופן היררכי; למשל, ממדים הנוגעים לזכויות בקבוצה אחת וממדים הנוגעים לתיאור המצב בקבוצה אחרת. היררכיה זו עוזרת לבוני המודל לארגן את המרחב לצורך עבודתם, אולם אינה משפיעה על המרחב באופן מהותי, מכיוון שבעת ביצוע החישובים המערכת מתעלמת מהקבוצות ומתייחסת רק לממדים עצמם.[24]

גרף החלטה (Decision Graph**)** הוא חלקו השני של מודל המדיניות. גם כאן, המונח ״גרף״ לקוח ממדעי המחשב, והוא מתאר מבנה מתמטי המורכב ממקומות (״צמתים״) וממעברים אפשריים בין מקומות אלה (״קשתות״). ניתן לעבור בין שני צמתים רק אם הם מחוברים בקשת. נהוג לתאר גרף באופן ויזואלי, על ידי קבוצת עיגולים המחוברים בחיצים. העיגולים מתארים את צומתי הגרף, והחיצים מתארים את הקשתות. החישוב במערכת PolicyModels מתחיל מצומת מיוחד בגרף ההחלטה, ומשם הוא מתקדם לאורך הקשתות של גרף זה. כאשר המחשב מגיע לצומת חדש, הוא מבצע פעולה התלויה בסוג הצומת. פעולה זו יכולה להיות, לדוגמה, עדכון המיקום במרחב המדיניות, הצגת שאלה למשתמש או הרצה של חלק אחר בגרף.

22 בזאת שונים הממדים המדוברים מממדים בדידים (דיסקרטיים) המשתמשים במספרים שלמים (בהם יש סדר ויש משמעות למרחק) וממממדים רציפים המשתמשים במספרים ממשיים.

23 חשוב לציין כי מודל זה עדיין לא עבר תיקוף.

24 לפירוט האלגוריתם שמאפשר למערכת להתעלם מהקבוצות, ראו: Bar-Sinai et al., “DataTags, Data Handling Policy Spaces and the Tags Language”.

גרפי ההחלטה של PolicyModels מאפשרים למצוא את המיקום של אדם מסוים במרחב המדיניות של המודל. הם יוצרים סינרגיה בין המחשב ובין האדם, כאשר המחשב מטפל בחלקים המוגדרים היטב (למשל, שמירת המיקומים במרחב המדיניות ובגרף ההחלטה), ואילו האדם מטפל בחלקים הדורשים ידע על פרטי המקרה או בתשובות לשאלות ״רכות״, כגון ״האם סיום התעסוקה נובע מהפרה משמעותית של זכויות העובד״? חלוקת אחריות זו בין האדם ובין המחשב מאפשרת למערכת PolicyModels להתגבר על האתגר המובנה של טיפול ממוחשב במקרים משפטיים מורכבים, מכיוון שאינה נסמכת על שיפוט ממוחשב בשאלות ״רכות״, שהן אנושיות במהותן.

חשוב לציין כי תשובות המרואיין אינן משַנות את מיקום המקרה במרחב באופן ישיר. שינויים כאלה מתבצעים על ידי המחשב כאשר הוא מגיע לצמתים המורים לו לשנות את המיקום. תשובות האדם יכולות לנווט את המחשב לצמתים כאלה בגרף ההחלטה. הפרדה זו בין תשובות האדם ובין שינוי המיקום במרחב המדיניות מאפשרת לבוני הגרף לשאול את האדם שאלות בשפה שהוא מבין, אך לנהל את המצב במונחים פורמליים. בנוסף לכך, היא מאפשרת לשאול את האדם מספר שאלות מנחות לפני שינוי מיקומו של המקרה במרחב. במובן זה, תהליך החישוב המשותף דומה לשיחה של בעל רכב עם מכונאי במוסך: המכונאי שואל שאלות שבעל הרכב מבין; למשל, האם שומעים דפיקות מהמנוע במהירויות גבוהות. בהתאם לתשובות מסמן המכונאי לעצמו האם לבדוק את המצתים, את אטם ראש המנוע או את שרשרת התזמון – מונחים סתומים למדי עבור בעל הרכב הממוצע.

התהליך המיוצג על ידי גרף החלטה נתון אינו בהכרח התהליך היחיד. למשל, סדר וסוג השאלות המתאימות למומחה בדיני תעסוקה יהיו שונים מסדר השאלות המתאימות להדיוט בתחום זה. גרפי החלטה שונים יכולים לעבוד על אותו מרחב מדיניות. מבחינת המערכת וההגדרות הפורמליות, הגורם החשוב הוא תוצאת הראיון – אותה קואורדינטה במרחב המדיניות המתארת את המקרה, שאליה מגיעים בסוף הראיון. תהליך ההגעה לקואורדינטה זו אינו חשוב לתהליכים בהמשך, כמו למשל ההמלצות שיוצגו למרואיין.

גרף ההחלטה יכול להיות גדול למדי; הגרסה הנוכחית של הגרף במודל הזכויות בסיום העסקה כוללת 216 צמתים. כדי לאפשר עבודה יעילה עם כמות צמתים כזו, שפת תיאור הגרף מאפשרת ארגון של הצמתים לפי נושאים, חלוקה של הגרף למספר תתי־גרפים, וכן חלוקה של תיאור הגרף עצמו למספר קבצים.

טקסטים ותרגום

מודל המדיניות, כפי שהוצג עד כה, מכיל בעיקר מבני נתונים – מרחב המדיניות וגרף ההחלטה. מבנים אלה מכילים מידע רב, אולם כוללים מעט מאוד טקסט

שמיועד לבני אדם. טקסט זה נשמר באופן נפרד במה שמכונה ״חבילות תרגום״ (“localization packages”).

״חבילת תרגום״ כוללת טקסט ארוך לכל שאלה, שמות והסברים לכל ערך ולכל ממד במרחב המדיניות, ותרגום של המֶטָא־דאטה של המודל (כותרת, טקסט הסבר וכדומה). הטקסטים לשאלות יכולים לכלול קישורים לאתרים חיצוניים, טבלאות והדגשות. הערכים במרחב המדיניות מייצגים מושגים שלא תמיד מובנים לאנשים שאינם מכירים את התחום הממודל, כגון ״חֵלֶף הודעה מוקדמת״[25] או ״גמר חשבון״. לכן, ההסברים לכל ערך וממד כוללים שלוש רמות: שם הממד; הסבר קצר המופיע בבועית מעל תצוגת הערך כאשר המשתמש מעביר את הסמן מעליה; הסבר מפורט שיכול לכלול מספר פסקאות, קישורים וטבלאות.

מודל מדיניות יחיד יכול להכיל מספר רב של ״חבילות תרגום״. בדרך זו ניתן להנגיש מודל יחיד לדוברי שפות שונות. בדומה לתרגום תוכנות, כתיבת ״חבילת תרגום״ חדשה דורשת מעט ידע טכני, כך שמתרגמים לא נדרשים לעבור הכשרה ארוכה כדי לבצע תרגום זה.

פרטיות משתמשים

במהלך הראיון מוסר המשתמש פרטים אישיים למערכת. לפיכך, ראוי לגעת בנושא שמירת הפרטיות של המשתמשים. עקרונות התכנון לפרטיות,[26] שהנחו אותנו בכתיבת מערכת זו, קובעים כי יש לשמור מידע על משתמשים רק אם הוא נדרש לצורך הפקת תועלת עבורם. לכן, למשל, משתמשים לא נדרשים להזדהות בפני המערכת בטרם הראיון, ושמם הפרטי, שם משפחתם או מספר האשרה שלהם אינם משפיעים על הזכויות להן הם זכאים על פי חוק. ברירת המחדל של המערכת היא לא לשמור את מהלך הראיון ותוצאותיו. מנהלי המערכת יכולים לבקש לשמור סטטיסטיקות לשימוש עבור מודלים מסוימים, למשל, כדי להבין אילו שאלות מסבכות את המשתמשים. סטטיסטיקות אלו מאפשרות אמנם לשחזר מהלך מלא של ראיון, אולם לא מקשרות אותו לאדם ספציפי, אלא משתמשות במזהה אקראי שנוצר בשָׁרַת.

אימות מודל מדיניות

במהלך הראיון עוברים המחשב והמרואיין על גרף ההחלטה ביחד, כאשר בכל שאלה המרואיין בוחר תשובה אחת המתאימה ביותר למקרה הנבדק. אפשרות

25 מצב בו המעסיק מוותר על עבודת העובד למשך תקופת ההודעה המוקדמת, וכתחליף משלם עבור תקופה זו שכר מלא.

26 Ann Cavoukian, “Privacy by Design [Leading Edge]”, *IEEE Technology and Society Magazine* 31, no. 4 (2012).

נוספת היא לבחור את כל התשובות עבור כל שאלה. בשיטה זו, המחשב עובר על גרף ההחלטה לבדו, ללא עזרת המרואיין, וכאשר הוא נתקל בצומת עם שאלה, הוא בוחר תשובה אחת. משם הוא ממשיך לשאלה הבאה ובוחר את התשובה לה, ושוב ממשיך ובוחר, עד שהראיון מסתיים. כך ניתן לבדוק את התוצאות של כל הראיונות האפשריים במודל.

שיטה זו, הלקוחה מתחום אימות תוכנה (formal verification), מאפשרת לשאול שאילתות רוחב על המודל. לדוגמה, ניתן לשאול באילו מקרים אישה בגיל העבודה תהיה זכאית לדמי אבטלה באופן מיידי? התשובות לשאלה זו מאפשרות לוודא כי המודל מתאים לחוק. אם המודל מתאר את החוק נאמנה, התשובות לשאלה זו מאפשרות למצוא מקרים אותם החוק אינו מכסה.

מגבלות המודל

המגבלה העיקרית של שיטת מידול המדיניות ב־PolicyModels היא הדרישה כי ממדי המרחב יהיו סודרים ובעלי מספר קואורדינטות סופי. לכן, לא ניתן לשאול שאלות פתוחות; התשובות חייבות לבוא מקבוצה סגורה. לדוגמה, לא ניתן לשאול את המרואיין לגילו (תשובה מספרית), אלא רק לאיזו קבוצת גיל הוא שייך (בחירה מִתוך רשימה מוגבלת). באופן דומה, לא ניתן לקבל מהמרואיין תאריכים.

ניתן להרחיב את המודל כך שיוכל להכיל ממדים מספריים, ואנו מתכננים לחקור כיוון זה בהמשך. עם זאת, כבר עכשיו ניתן להתגבר על המגבלה המתוארת לעיל בשתי שיטות: הראשונה – חלוקת תחום מספרי לטווחים שהחוק הממודל מבדיל ביניהם. למשל, במקום לשאול את המרואיין על גיל מספרי, ניתן לשאול אותו האם הוא בגיל העבודה או הפנסיה; השיטה השנייה היא להפנות את המרואיין בסיום הראיון למחשבון זכויות שנכתב במיוחד עבור התחום הממודל. מחשבון זה יקבל את תוצאות הראיון וישתמש בהן כדי לבקש מהמרואיין את המספרים הרלוונטיים ולבצע את חישוב הזכויות הסופי. שיטה זו מאפשרת, לדוגמה, לחשב במדויק את פיצויי הפיטורין המגיעים לעובד.

שיטה לבניית מודלי מדיניות

בחלק זה של המאמר אנו מציעים שיטה לבנייה של מודלי מדיניות, המבוססת על ניסיוננו ביצירת מספר מודלים כאלה. מודלי מדיניות דומים מאוד לתוכנות קטנות, ולכן התהליך המוצע מבוסס על מתודולוגיות של פיתוח תוכנה. אין אנו טוענים כי זוהי השיטה היחידה לבנות מודלים אלה, ואפילו לא השיטה הטובה ביותר (בהנחה שיש כזו). כוונתנו היא להציע שיטה מספיק טובה כדי לאפשר לאחרים להתחיל לכתוב מודלים וכדי להתניע דיון בנושא. תחילה נעמוד על האתגרים הניצבים בפני

צוותים המבקשים לכתוב מודלי מדיניות; לאחר מכן נבחן את הכלים הקיימים; לבסוף נציע מתודולוגיה.

מודלי מדיניות הינם יצורי כלאיים משפטיים־טכנולוגיים. בנייה של מודל מדיניות לתחום משפטי מסוים דורשת מומחיות בשני תחומים – התחום המשפטי עצמו ומערכת PolicyModels – ומציבה אתגר של שילוב פורה ביניהם. לכן, צוות בניית מודל יהיה מורכב לרוב משני מומחים שיגיעו מרקעים שונים ולא יכירו את התחום המשלים. חשוב לציין כי רמת ההתמחות הנדרשת בכל תחום הינה שונה: מומחיות משפטית דורשת הכרה עמוקה של תחום המשפט, לצד התעדכנות שוטפת בו (למשל, הכרה של פסקי דין מהתקופה האחרונה). לעומת זאת, אדם עם הכשרה בסיסית בתכנות יכול להשתמש ב־PolicyModels לאחר לימוד קצר יחסית: סטודנטים למדעי המחשב הצליחו להשתמש במערכת לאחר שקראו את מסמכי ההדרכה. לכן, להערכתנו, מתכנת עם ניסיון מועט יוכל לבנות מודלים לאחר יום אחד של לימוד עצמי. מובן שיעילות המתכנת תגדל ככל שיצבור ניסיון.

הבדלים "תרבותיים" בין מתכנתים ובין משפטנים הם אתגר נוסף עליו יש לגשר, במיוחד בתחילת תהליך העבודה: מתכנתים רבים מתקשים להתמודד עם תחומים עמומים, כמו התחום המשפטי, שיש בהם מגוון דעות סותרות; משפטנים, מצידם, צריכים להתרגל לחשיבה על סיטואציות חוקיות באמצעים פורמליים, כמו מרחב המדיניות וגרפי החלטה.

מערכת PolicyModels מציעה מספר כלים העוזרים לטפל באתגרים אלה. ראשית, ניתן ליצור באופן אוטומטי שרטוטים של מרחב המדיניות ושל גרף ההחלטה. שרטוטים אלה ידידותיים יותר, או למְצער מאיימים פחות, מאשר הקוד הטקסטואלי של המודל; שנית, המערכת האינטרנטית שמבצעת את הראיונות מאפשרת לאסוף הערות לפני פרסום המודל, וזאת בעזרת קישורים פרטיים ומערכת הערות פנימית; שלישית, שפת המידול עצמה תומכת באפשרות לסמן חלקים מסוימים כ"דורשים השלמה" (TODO). המערכת מסוגלת להפיק דוח המפרט חלקים אלה, וכן מזהה באופן אוטומטי חלקים במרחב המדיניות שגרף ההחלטה לא עושה בהם שימוש.

בנוסף לכלים אלה, צוות פיתוח מודל יכול להשתמש בכלים קיימים לפיתוח תוכנה, כגון מערכות ניהול גרסאות ומשימות. מערכות אלו מאפשרות לשמור גרסאות של המודל בזמנים שונים, לבחון אפשרויות שונות על בסיס מודל קיים, לקשר בין משימות ובין העדכונים למודל ולדון בעדכונים למודל טרם קבלתם. האפשרות להתבסס על מערכות אלו נובעת מהעובדה שמערכת PolicyModels מתבססת על קוד טקסטואלי פתוח, ולא על מבנה קבצים ייחודי וסגור. דוגמה

למערכת פופולרית כזו היא GitHub[27] – מערכת ששימשה אותנו בעת פיתוח מודל זכויות בעת סיום העסקה.

מתודולוגיית פיתוח המודלים שאנו מציעים מבוססת על תהליך פיתוח תוכנה איטֶרָטִיבִי.[28] בתהליך זה המודל מפותח במספר מחזורים ("אִיטֶרָציות"), כאשר בסיומו של כל מחזור נוצר מודל עובד, אותו ניתן להציג למומחים ולמשתמשים. עם כל מחזור שעובר, המודל "מכסה" את החוק באופן נאמן יותר.

להלן מוצגים שלבי פיתוח מודל: מחזור פיתוח ("איטרציה") כולל חזרה על שלבים 2–4. **שלב 1** הוא שלב הכנה ראשוני. לפני תחילת העבודה כדאי לעשות מפגש מרוכז, שבו אנשי המידול יציגו את היכולות והמגבלות של PolicyModels, והמשפטנים יסקרו את הדין בתחום המדובר. דוגמה לכך הוא המפגש שערכנו לפני פיתוח מודל הזכויות בסיום העסקה, שנמשך ארבע שעות וכלל מומחים משפטיים מ"קו לעובד" ואת צוות הנדסת התוכנה של הפרויקט. במפגש זה הצגנו סקירה של החוקים הרלוונטיים ושל מערכת PolicyModels, וכן בחרנו תחומים מתאימים למידול.

שלב 2 הוא שלב הפיתוח. במסגרת זו:

- בוחרים תת־תחום מהתחום הממודל למידול באיטֶרָציה הנוכחית ומתכננים לאיזו רמת פירוט ייבנה המודל. לדוגמה, בשלבים הראשונים ימודלו תחומים רחבים ברמת פירוט נמוכה; בשלבים מתקדמים יותר ימודלו תחומים צרים לעומק. הדוח המפרט אילו חלקים עדיין לא הושלמו יכול לשמש כלי עזר לבחירת תת־תחום לאיטרציה נתונה.
- סוקרים את הידע המשפטי הרלוונטי לתחום: חוקים, תקנות, פרשנויות וכדומה. לפי סקירה זו בונים גרסה ראשונית של מרחב המדיניות. אזורים שאינם מפורטים עד הסוף יש לסמן ב־TODO, כך שהם יופיעו בדוחות כדורשים פירוט.
- כותבים את גרף ההחלטות. גם כאן יש לסמן ב־TODO חלקים שאינם מפורטים עד הסוף. שרטוטים אוטומטיים של עץ ההחלטה שימושיים מאוד בשלב זה כדי לוודא שסדר השאלות בראיון משקף נאמנה את כוונת המפתחים. כתיבה זו תכלול, בדרך כלל, גם שינויים במרחב המדיניות, ולעיתים גם שינויים בחלקים אחרים בעץ.
- כותבים טקסטים מפורטים לשאלות החדשות, לממדים ולערכים.

שלב 3 הוא שלב הבדיקות, שבמסגרתו:

- מעלים את הגרסה החדשה לשרת ומגדירים אותה כ"פרטית", כך שרק משתמשים מורשים יכולים לראותה. בודקים את הגרסה על מספר מקרים. אוספים משוב

27 "Built for Developers," *GitHub*, July 2019, https://github.com.
28 Craig Larman and Victor Basili, "Iterative and Incremental Development: A Brief History", *IEEE Computer* 36, no. 6 (2003): 47-56.

ממומחים בתחום, וזאת על ידי הצגה של הראיון או על ידי שליחת קישור ורישום הערות במערכת.

- מעדכנים את המודל לפי המשוב.

שלב 4 הוא שלב שחרור גרסה: מעלים את המודל לשרת ומגדירים אותה פומבית כדי לאפשר לכלל הגולשים להשתמש בה.

מניסיוננו בפיתוח מודל זכויות בסיום העסקה ומודל זכויות אבטלה בחוק הביטוח הלאומי למדנו כי סדרת פגישות שבועיות של מומחה משפטי בתחום ושל מתכנת PolicyModels היא דרך יעילה יחסית לבנות מודל. משך כל פגישה כזאת נע בין שעתיים לשלוש שעות, ולעיתים אף יותר – תלוי בזמן שעומד לרשות אנשי הצוות ולסיבולת שלהם.

סיכום

אחת המטרות של פיתוח המודל שתואר במאמר זה הייתה לבחון את יכולתו לפשט מידע משפטי ולהנגיש אותו לאוכלוסיות מוחלשות. ההנחה הייתה שרצף של שאלות פשוטות יוכל להביא לאבחון המצב המשפטי הייחודי למשתמש. לשאלון כזה יש יתרון, במיוחד עבור אוכלוסיות שאינן מורגלות בקריאת טקסטים ארוכים ובסינון מידע, ולכן הן נרתעות מאתרי הנגשת זכויות מבוססי טקסט (דוגמת "כל זכות" הנזכר לעיל).

מצאנו כי ניתן לבנות מודל כזה, וכי על אף שהוא מציג תמונה מרודדת של המצב המשפטי, העובדה שתמונה זו מותאמת אישית למשתמש הופכת אותה לשימושית. יחד עם זאת, יש למידול כזה חיסרון, הנעוץ בפישוט יתר של התמונה המשפטית ובחוסר היכולת להיכנס לניואנסים פרשניים הנפוצים מאוד בשדה המשפטי. על כן, יש לבחור תחום או תת־תחום שקיימת לגביו הסכמה משפטית סבירה (מחלוקות בין משפטנים נוטות להיות נפוצות יותר מאשר בין מהנדסים; זהו הבדל תרבותי שמהנדסים מופתעים ממנו, אבל גם צריכים להתרגל אליו). בנוסף, מידול שדות משפטיים, המחייבים שימוש בשאלות פתוחות, יהיה קשה יותר, ויכול אף לדרוש עיבוד נוסף של התוצאות על ידי מערכת ייעודית או על ידי מומחה אנושי.

אין ספק שהמעבר מהמשפט לתבנית של חד־משמעיות והפשטה, הנדרשת בכלי הממוחשב, הוא מעבר מורכב שאינו מתאים לכל שדות המשפט. יש צורך לבחור סיטואציה ממוקדת, שהמסקנות המשפטיות ממנה פשוטות יחסית, ולזכור כי ב"שורה התחתונה" מדובר בכלי עזר ולא במענה חד־משמעי. כך, במקרים שבהם השאלון שלנו העיד על פגיעות חמורות, כגון ניצול או תקיפות מיניות, מיהרנו להפנות לגורמי הסיוע הנכונים. ראוי להדגיש כי עצם זיהוי העבֵרה ואיתור הגוף הנכון שאליו יש לפנות הם חלק מהפתרון.

הדרישה להתמקד ולבחור מענה אחד נכון מסייעת, לעיתים קרובות, לעובדים נסערים, הנמצאים במצבים של בלבול ועומס, להתמקד. היא גם מגדירה עבורם ועבור המסייעים להם מהי הזכות הנפגעת. כל משפטן שהתנדב, או עבד בארגוני סיוע לאוכלוסיות מוחלשות, יודע שהמשימה הקריטית היא, במקרים רבים, להבין, מתוך בליל החוויות, התחושות והנרטיבים, מהי הנקודה המשפטית שדורשת טיפול ומאפשרת אותו. מידול החוק בשיטה המוצעת כאן עשוי, אפוא, להועיל לעובדים ולמתנדבים כאחד.

השימוש בטכנולוגיות ביומטריות – היבטים נורמטיביים ומשפטיים

לימור עציוני

התפתחות הטכנולוגיה לזיהוי מגוון מאפיינים (פיזיים ונפשיים) והשימוש בטכנולוגיות ביומטריות הגיעו לרמת בשלות ותפוצה כזו, המחייבת בחינה והתייחסות משפטית ונורמטיבית מפורשת לכלל היבטיהם. הריצה חסרת המעצורים קדימה של חברות הטכנולוגיה בישראל ובעולם גורמת לכך שהיבטים אלה נותרים מאחור. מאמר זה בוחן את התפתחות השימוש בטכנולוגיות ביומטריות ואת ההיבטים האתיים והמשפטיים הנגזרים ממנו. לישראל יש עניין רב בפיתוח הכלכלי הנגזר מיישומים ביומטריים, ולכן מציע המאמר להוביל מהלך בין־לאומי שמטרתו יצירת דיון ערכי ומשפטי בשאלות החשובות העולות מתפוצת הטכנולוגיה הביומטרית. בדרך זו תוכל מדינת ישראל להמשיך ולהשפיע על נורמות שיתפתחו בעתיד בתחום זה.

מילות מפתח: ביומטריה, זיהוי פנים, פרטיות, מאגרי מידע

מבוא

בדצמבר 2018 פרסם העיתון הבריטי ״גארדיאן״ כתבה על שימוש באמצעים ביומטריים בהופעתה של הזמרת טיילור סוויפט, לרבות שימוש במצלמות נסתרות לזיהוי פנים במטרה להצליב את תמונות הקהל עם מאגר של תמונות מטרידנים (Stalkers) של הזמרת – מעריצים כפייתיים העלולים להוות בעיה ביטחונית למושא הערצתם. אין להקל ראש באתגרים הביטחוניים היוצרים מטרידנים אלה: לזמרת מספר מטרידנים מוכרים, שנגדם אף הוצאו צווי הרחקה, ואחד מהם אף

ד״ר לימור עציוני היא דקאנית בית הספר למשפטים במרכז האקדמי שערי מדע ומשפט וחוקרת בכירה בתוכנית לבישחון סייבר במכון למחקרי בישחון לאומי.

איים עליה באונס וברצח. הבעיה היא שהשימוש במצלמות הנסתרות נעשה מבלי שהקהל ידע על קיומן ותפקידן.[1]

היו כמובן אירועים שקדמו להצבת המצלמות הנסתרות בהופעתה של טיילור סוויפט: באפריל 2019 פורסם שנער אמריקאי תובע את חברת "אפל" בעקבות מעצר שווא שלו שנגרם על ידי החברה, אשר הפעילה תוכנת זיהוי פנים בחנויותיה תוך פגיעה קשה בפרטיות הקונים.[2] האירוע החל אחרי ששוטרים עצרו את הצעיר בניו יורק בעקבות תלונה שהגישה חברת "אפל". הצעיר נעצר מכיוון שאדם אחר השתמש בתעודת הזהות שלו, שלא נשאה תמונה, ובפרטים נוספים שגנב מתוכה, כדי לבצע גניבות בחנויות החברה בניו ג'רזי, דלאוור ומנהטן. בעקבות הגניבות עשתה החברה שימוש בפרטי זהותו שהיו ידועים לה, כדי לאתר את תמונתו ולהשוות אותה עם מערכות זיהוי הפנים המותקנות בחנויותיה. הזיהוי הביא להגשת תלונה נגדו במשטרה. לשוטרים התברר כי העצור הינו קורבן לתרמית וכי אינו הגנב האמיתי. בתביעתו של הנער נגד החברה הועלתה הטענה שהקישור שעשתה "אפל" בין פרטים שנגנבו ובין זהותו האמיתית, כולל תמונת פנים שלו שהוזנה למערכות האבטחה של החנויות, פוגע בזכויות יסוד שלו מבלי שלחברה יש סמכות לכך. בעקבות הגשת התביעה התעורר ויכוח בין מומחי משפט בשאלה האם יש לתביעה בסיס איתן והאם חברת "אפל" עברה על החוק. היו אף מי שטענו שמדובר במימוש חזונו של ג'ורג' אורוול, כאשר חברת טכנולוגיה מסוגלת להפוך ל"אח הגדול" ולעקוב אחרי כל אדם.

טכנולוגיות ביומטריות לזיהוי פנים התפתחו מאוד בשנים האחרונות ומשמשות ארגוני ביטחון במגוון יישומים ביטחוניים, ביניהם זיהוי מפַגעים במקומות הומי אדם (תחנות רכבת, שדות תעופה וכדומה) על ידי השוואה למאגר נתונים ביומטריים קיים. טכנולוגיה זו משמשת גם לצורכי הכנסה יעילה ומהירה של קהל למתחמים גדולים.

מאמר זה בוחן את הדילמות האתיות והמשפטיות הנובעות מהתקדמות השימוש בטכנולוגיות ביומטריות במגוון יישומים, תוך בחינת ההיבטים השונים של המסגרת החוקית הקיימת. כבר עתה ברור כי התפתחות הטכנולוגיה הגיעה לרמת בשלות ותפוצה כזו, המחייבת בחינה והתייחסות משפטית ונורמטיבית מפורשת לכלל ההיבטים של השימוש בטכנולוגיות ביומטריות ובמאגרי מידע ביומטריים.

---

1 Laura Snapes, "Taylor Swift Used Facial Recognition Software to Detect Stalkers at LA Concert", *The Guardian*, December 13, 2018.

2 Bob Van Voris, "Apple Face-Recognition Blamed by N.Y. Teen for False Arrest", *Bloomberg*, April 23, 2019.

רקע תיאורטי

התקדמות טכנולוגיית הזיהוי הביומטרי הובילה וממשיכה להוביל מגוון יישומים רחב במרחב הפרטי, כמו גם במרחב הציבורי. מקומות עבודה רבים הם הראשונים לאמץ יישומים ביומטריים. אולם, למרות שטכנולוגיות ביומטריות מאפשרות למעסיקים לחסוך במשאבים ואף להגביר את האבטחה במקום העבודה, עובדים מהססים לעיתים קרובות לאפשר שימוש בנתונים אלה. זאת, משום שאיסוף ואחסון של נתונים ביומטריים של עובדים מעלים חששות לגבי שימוש נאות במידע האישי המצטבר.

דארל קרפנטר ועמיתיו[3] בחנו מספר היבטים של השימוש בטכנולוגיות ביומטריות בהקשר של פרטיות, וזאת בשלושה ממדים: הראשון נוגע לשאלה כיצד האחריות לפרטיות נתפסת על ידי העובדים; השני נוגע לתפיסת הפגיעות שהמערכות הביומטריות יוצרות; השלישי מתייחס לתפיסת חוסר האמון כלפי הארגון. במסגרת מחקרם הם בחנו את ההתפתחויות ביחסם של העובדים בארגון שהתקין מערכות ביומטריות. התוצאות הצביעו על כך ששיתוף עובדים בניסוח כללי השימוש במערכות אלו מילא תפקיד משמעותי בכל הקשור להקטנת החשש בנוגע לפגיעה בפרטיות, וזאת בכל שלושת הממדים.

מחקר אחר בחן היבטים הנוגעים לשימוש ביישומים ביומטריים במגזר הבריאות. החוקרים בחנו היבטים של שימוש בנתוני גנום בהקשר למחלות סרטן ומחלות נדירות, אשר התלוו לו שימושים משניים שעלולים היו לקבל תפוצה רחבה ביותר.[4] המחקר בחן עד כמה ניתן לקבל הסכמות לשימוש במידע ביומטרי פרטי (בהקשר זה, מידע הנוגע למיפוי הגנום האישי), והראה שמטופלים עשויים לבחור לאחסן חלק מהמידע שלהם, כגון מידע גנטי, באופן מקוון ולאפשר לאנשי מקצוע בתחום הבריאות לגשת אליו. המחקר נגע בצורך לוודא שבתהליך האחסון והשימוש של המידע הרגיש, כל מי שייגש אליו תאומת זהותו בצורה נכונה, וזאת כדי להגן על פרטיות המטופלים. המחקר הראה כי לאימות כזה יש שני תפקידים: מניעת התחזות, והוכחה של כוונת השימוש במידע – המהווים צעד חיוני להבטיח שמחקר רפואי וחילופי מידע בנושאי בריאות מתבצעים לשם מטרה ראויה מבחינה אתית.

---

3 Darrell Carpenter, Alexander McLeod, Chelsea Hicks and Michele Maasberg, "Privacy and Biometrics: An Empirical Examination of Employee Concerns", *Information Systems Frontiers*, Vol. 20, No. 1 (February 2018).

4 Atsushi Kogetsu, Soichi Ogishima and Kazuto Kato, "Authentication of Patients and Participants in Health Information Exchange and Consent for Medical Research: A Key Step for Privacy Protection, Respect for Autonomy and Trustworthiness", *Front Genet*, Vol. 9 (June 1, 2018).

אנטון אלתרמן בוחן היבטים אתיים בזיהוי ביומטרי.[5] טענתו היא שבזיהוי ביומטרי קיים אינטרס פרטי לצד אינטרס ציבורי, וכי שני אלה נדרשים לצורך האיזון; כך מתקיים מעין סחר חליפין בין הפרטי לציבורי בשימוש בטכנולוגיה ביומטרית לצורכי זיהוי. מסקנתו העיקרית היא שהזכות הכללית לפרטיות כוללת גם את הזכות לשלוט במידע שנאסף ובשימוש במרכיבים הביומטריים, וכי זכות זו חייבת להיות זכות גוברת. המשמעות מבחינתו היא שיש לנהוג בזהירות יתר ולשקול היטב את ההחלטה לאפשר גישה למידע ביומטרי אישי לגורמים אחרים. לדעתו, יש לשקול את הדברים לאור מספר היבטים: הפיכת מידע ביומטרי לזמין לאור אפשרות אובדן השליטה על המידע; אבטחת המידע; הסיכונים של שימוש לרעה במידע.

השימוש הגובר והולך בזיהוי ביומטרי מחייב את הפרט לבחון עד כמה הוא מוכן שנתוניו האישיים יועברו לגורמים אחרים בכדי לקבל שירות מהיר וטוב יותר. השאלה הנשאלת בהקשר זה היא עד כמה יש לַפרט יכולת לשלוט בשימוש שנעשה במידע הביומטרי עליו. אלתרמן מציע שכל מי שיתבקש לספק מידע ביומטרי יהיה בעל יכולת להבין את התוצאות ואת ההשפעה של העברתו, אל מול שיפור השירות הצפוי כתוצאה מזיהוי ביומטרי מהיר, וגם מודע לסיכונים הפוטנציאליים הכרוכים בכך.

בישראל הוקמה בשנת 2011 יחידה לפיתוח תחום היישומים הביומטריים במשרד ראש הממשלה. זאת בהמשך לחוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע התש"ע– 2009, הקובע כי ראש הממשלה ימנה "ממונה על יישומים ביומטריים". היחידה עברה בהמשך לאחריות מערך הסייבר הלאומי.[6] בישראל גם הוקם מאגר נתונים ביומטרי לאומי. המאגר הביומטרי הלאומי הוקם במטרה למנוע התחזות וגניבת זהויות. באתר האינטרנט של רשות המאגר הביומטרי הלאומי נכתב: "כיום, במצב הנוכחי, ואפילו במצב של תיעוד ביומטרי חכם אך ללא מאגר ביומטרי, יכול עדיין אדם להתחזות ולהנפיק בו־זמנית מספר תעודות בזהויות שונות. זאת, מפני שבהיעדר מאגר נתונים ביומטרי, לרשות האוכלוסין אין דרך לוודא שמבקש התעודה אינו מתחזה".[7] יש לזכור, בהקשר זה, כי צריך להבחין בין מערכת ביומטרית המאפשרת זיהוי המשווה נתונים של אדם למאגר רחב והמנסה לאתר את זהותו מתוך המאגר הזה (לדוגמה, זיהוי עבריין לפי טביעות אצבע, צילומים או נתוני DNA) ובין מערכת המאפשרת אימות זיהוי,

5 Anton Alterman, "'A Piece of Yourself': Ethical Issues in Biometric Identification", *Ethics and Information Technology*, Vol. 5 (2003).

6 אתר מערך הסייבר הלאומי, על היחידה להזדהות וליישומים ביומטריים, פורסם במאי 2018: https://www.gov.il/he/departments/news/bio_aboutbiometric.

7 אתר רשות המאגר הביומטרי הלאומי: https://www.gov.il/he/departments/general/target_goals.

תוך בחינת פרטים ביומטריים של אדם שנדגמו בעבר (לדוגמה, המעבר במסלול הדרכון הביומטרי בשדה התעופה).

ויכוח ער מתנהל סביב מכלול ההיבטים הנוגעים לשימוש ביישומים ביומטריים, ועוד יותר – באשר לעצם הקמתו של המאגר הביומטרי הלאומי. עומר טנא מראה במאמרו[8] עד כמה חוק המאגר הביומטרי בישראל יוצר סיכונים לפגיעה בזכות לפרטיות, כשזו לא נעשית לתכלית ראויה ההולמת את ערכיה של מדינת ישראל. לטענתו, מערכות ביומטריות מעוררות בעיות אתיות כתוצאה מאופן השימוש במידע, כאשר זה משלב אותו במערכות נוספות, כמו מצלמות אבטחה ומעקב. בדרך זו, המטרות הביטחוניות והאבטחתיות של המאגר עלולות לפגוע באופן לא מידתי בערכי יסוד, כמו פרטיות והזכות לאוטונומיה של אדם על גופו. התפתחות הטכנולוגיה נוגסת בזכות לפרטיות באופן קבוע ומתמשך: חברות הטכנולוגיה אוספות מידע רב על משתמשים ברשת האינטרנט דרך מנועי החיפוש, נתוני הגלישה, נתוני המיקום, קשרים ברשתות חברתיות ועוד. בצורה זו מתקיים זיהוי באמצעות מידע ביומטרי שאינו ניתן להכחשה. לטענתו של טנא, אף שלמערכות ביומטריות עשויה להיות השפעה חיובית על הזכות לפרטיות, לאור העובדה שהן מאפשרות זיהוי ואיתור תוך שימוש במידע מינימלי, עלולה להיות לשימוש זה גם השלכה שלילית על הזכות לפרטיות, כאשר זהותו של אדם תצומצם "לאוסף של נתונים ביומטריים".

ברשות לניהול המאגר הביומטרי בישראל הוחלט לאמץ קוד אתי.[9] בקוד נקבע שהרשות נושאת באחריות המעשית לעיבוד הנתונים הביומטריים, שמירתם, אבטחתם והנגשתם לשימוש על פי דין. כמו כן, הרשות מתחייבת לשמור על הפרטיות של בעלי הנתונים הביומטריים שבידיה ולמנוע כל שימוש בנתונים הביומטריים שלא על פי דין. עוד נקבע בקוד האתי שהרשות ועובדיה מבצעים כל פעילות במסגרת הפרויקט הביומטרי הלאומי בהתאם לתפיסה של שירות לטובת הכלל, שמירה על כבוד האדם ושמירה על זכויות האזרח בהתאם לעקרונות המשטר הדמוקרטי. קביעה נוספת של הקוד נוגעת לדרישה שהרשות תפעל על יסוד נתונים ביומטריים מינימליים, כאשר הדבר נדרש לעיצוב תעודות זהות ודרכונים אמינים, להגנה על הזהות האישית ולסיכול כל ניסיון לעשות שימוש מזויף בתעודות זהות ובדרכונים.

---

8 עומר טנא, "חוק המאגר הביומטרי: סיכונים והזדמנויות", **המשפט**, יז (2) תשע"ג–2013.

9 "הרשות לניהול המאגר הביומטרי – הקוד האתי", *מדינת ישראל, משרד הפנים, הרשות לניהול המאגר הביומטרי*, 2015. להרחבה על היבטים אתיים של זיהוי ביומטרי ראו: Annemarie Sprokkereef, Paul De Hert, "Ethical Practice in the Use of Biometric Identifiers within the EU", *Science and Policy*, 3(2007): 177-201; Emilio Mordini, Carlo Petrini, "Ethical and Social Implications of Biometric Identification Technology", *Annali dell'Istituto superiore di sanita*, 43 (2017): 5-11.

ישראל אינה לבדה בתחום זה; מדינות נוספות הקימו מאגרים ביומטריים: באפריל 2019 קיבל הפרלמנט האירופי החלטה להקים מאגר ביומטרי, העשוי להפוך למאגר הגדול בעולם.[10] מטרתו היא לאפשר בקרה ושליטה טובות יותר בגבולות מדינות האיחוד האירופי. המאגר הביומטרי האירופי, הידוע בשם Common Identity Repository (CIR), מיועד לאחסן כ־350 מיליון זהויות ולכלול פרטים רבים, בכללם: שמות, תאריכי לידה, מספרי דרכון ופרטי זיהוי אחרים, לצד פרטים ביומטריים כגון טביעות אצבעות וסריקות פנים. נתונים אלה יהיו זמינים לרשויות הגבול וגורמי האכיפה במדינות האיחוד. אף שהפרלמנט האירופי והמועצה האירופית הבטיחו "אמצעי הגנה נאותים" כדי להגן על זכותם של האנשים לפרטיות ולהסדיר גישה של גורמי האכיפה לנתונים, לא ברור עדיין על אילו אמצעי הגנה מדובר.

תקנות הפרטיות שאומצו באיחוד האירופי (GDPR) העמידו אתגר גם בפני הגורמים באיחוד העוסקים בביומטריה. ראול סנצ'ס־רֶיו ועמיתיו בחנו את השאלה כיצד ניתן לאמץ את הרגולציה האירופית בכל הקשור לשמירה של נתונים ביומטריים.[11] בעבודתם הם מתארים את האתגר וממליצים על סדרה של צעדים שנועדו להגן על רכישת מידע ביומטרי ושימוש בו. מדובר בהליך המבוסס על 11 שלבים, ביניהם: קביעת רמת הגנה לפי רגישות הנתונים; בנייה של סביבות עבודה מבודלות במטרה למזער את הסיכוי לגישה לא מורשית ואת הסיכויים להתקפה ישירה על הרשת; הקפדה על עבודה עם יישומים מקומיים במקום יישומים המבוססים על האינטרנט; מחיקה או הסרה של הנתונים לאחר גמר המחקר עליהם.

התפתחות השימוש ביישומים ביומטריים והיבטים משפטיים אתיים

קצב התפתחות השימוש ביישומים ביומטריים הינו גבוה מאוד. מאמר שפורסם בעיתון "ניו יורק טיימס" תיאר את הקלות שבה ניתן להקים מערכת לזיהוי פנים של אנשים במרחב הציבורי.[12] לפי המאמר, המחשבה שתנועה במרחב הציבורי מאפשרת שמירה על פרטיות הינה שגויה. כך, למשל, זיהוי הפנים המופעל ברשת המצלמות הקיימת ברוב הערים מהווה איום על הפרטיות. המאמר גם מראה את הקלות שבה ניתן לעקוב אחרי אנשים ללא ידיעתם: במהלך תשע שעות נאספו

---

10 Catalin Cimpanu, "EU Votes to Create Gigantic Biometrics Database", *zdnet*, April 22, 2019.

11 Raul Sanchez-Reillo, Ines Ortega-Fernandez, Wendy Ponce-Hernandez, Helga C. Quiros-Sandoval, "How to Implement EU Data Protection Regulation for R&D in Biometrics", *Computer Standards & Interfaces*, Vol. 61 (January 2019).

12 Sahil Chinoy, "We Built an 'Unbelievable' (but Legal) Facial Recognition Machine", *The New York Times*, April 16, 2019.

תמונות של אנשים באחד הגנים בעיר ניו יורק. התמונות הורצו דרך שירות זיהוי הפנים של חברת "אמזון", ומתוכן זיהתה המערכת פנים של 2,750 אנשים.

השימוש בטכנולוגיות זיהוי פנים הואץ עם שילוב הטכנולוגיה במצלמות CCTV רגילות המותקנות בקרנות רחוב, בחנויות ובבתי עסק. שימוש זה יוצר עולם שבו אזרחים מנוטרים באופן אינטנסיבי וקבוע.[13] בריטניה מובילה בהטמעת טכנולוגיה זו. במהלך עשרות השנים האחרונות הותקנו בבריטניה מיליוני מצלמות רחוב. התפתחות מערכות זיהוי ביומטריות מאפשרת כיום שימוש במצלמות אלו לזיהוי אנשים ולהקמת מערכות מעקב בעלויות זניחות. בפועל, אין מגבלה חוקית על פעולות אלו, והשימוש בטכנולוגיות זיהוי פנים נעשה כמעט ללא פיקוח. כך, אין כל מסגרת משפטית המסדירה את השימוש במצלמות המבוססות על טכנולוגיה של זיהוי פנים ואין כל מנגנון פיקוח על התקנת הטכנולוגיה והשימוש בה. כתוצאה מכך, לא נבחנת המידתיות של השימוש בכלים אלה, ואין איזון בין ערכי החירות והפרטיות ובין ערכי הביטחון.

השימוש שנעשה בבריטניה במצלמות CCTV נתקל בביקורת גוברת על היעדר כל דיון ציבורי סביב הטכנולוגיה המתפתחת או היעדר בסיס משפטי להפעלתה. בהקשר זה מועלות שאלות כבדות משקל, כמו החדירה לפרטיות האזרחים וההידרדרות לתופעות של "האח הגדול".[14] בדוח שפורסם בבריטניה במאי 2018[15] נטען שהשימוש בטכנולוגיה זו מהווה איום חסר תקדים על פרטיותם וחירותם של אזרחים ועלול אף לערער את הזכויות הבסיסיות שלהם במקומות ציבוריים. בדוח נטען כי משטרת המטרופולין בבריטניה סובלת מדיוק ירוד של שני אחוזים בלבד במערכת הזיהוי האוטומטי אותה היא מפעילה, וכי שיעור התרעות השווא מגיע ל־91 אחוזים, כלומר, אדם תמים מזוהה לעיתים קרובות כאדם מנוטר. האו"ם הצטרף לביקורת זו כשפרסם דוח שביקר את השימוש בזיהוי פנים במהלך הפגנה בדרום ויילס. בדוח, שנכתב על ידי ג'וזף קנטאצ'י, שמונה על ידי ארגון זכויות האדם של האו"ם לבחון את הנושא, נטען שההפגנה הייתה שקטה והשימוש בטכנולוגיה היה לא מידתי לאור רמת האיום שהיא הציבה על הביטחון הציבורי.[16]

---

13 להרחבה על פגיעה בפרטיות ומיגור פשיעה באמצעות מצלמות CCTV ראו: Andrei Costin, "Security of CCTV and Video Surveillance Systems: Threats, Vulnerabilities, Attacks and Mitigations", TrustED, 16 Proceedings of the 6th International Workshop on Trustworthy Embedded Devices, 2016, pp. 45-54.

14 Michael Friedewald, Ronald J. Pohoryles, eds., *Privacy and Security in the Digital Age: Privacy in the Age of Super-Technologies* (Routledge, 2016).

15 "Face Off – The Lawless Growth of Facial Recognition in UK Policing", *Big Brother Watch*, May 2018.

16 Chris Burt, "UN Privacy Rapporteur Criticizes Accuracy and Proportionality of Wales Police Use of Facial Recognition", *Biometric*, July 3, 2018.

ניסיונות להתמודד עם נושא זה בישראל הובילו להקמת יחידה ליישומים ביומטריים במשרד ראש הממשלה, ובהמשך לחקיקת חוק המאגר הביומטרי שאושר במארס 2017.[17] אחת ממטרות החוק היא להתמודד עם הבעיות החמורות הקיימות בישראל בכל הנוגע למסמכי זיהוי, דוגמת דרכונים ותעודות זהות. החוק שם לו למטרה לקבוע הסדרים שיאפשרו אימות זהות וזיהוי של תושבי ישראל, תוך שימוש באמצעים ביומטריים ובנתונים ביומטריים שיופקו מהם. נתונים אלה ייכללו במסמכי הזיהוי ובמאגר ביומטרי מרכזי, באופן שיקשה מאוד על זיוף התיעוד, ניפוק תיעוד כפול לאותו אדם ושימוש בזהות גנובה. אחת הטענות נגד החוק הייתה שאיסוף נתונים ביומטריים אינו מסייע במיגור תופעת הזיוף, וכי לכל היותר נתונים אלה יוכלו לסייע בשלב אימות זהותו של בעל התעודה. עוד נטען כי ניתן היה להסתפק ביצירה של תעודות אותן יהיה קשה לזייף.[18]

באשר לשימוש במצלמות במרחב הציבורי בישראל, עוד בשנת 2012 פרסמה הרשות להגנת הפרטיות מסמך הדן בשימוש במצלמות במרחב הציבורי ובמידע הנאגר בהן.[19] זאת, מתוך הבנת הפוטנציאל הבעייתי של הדבר, הנובע מהתרחבות השימוש במערכות במעגל סגור למגוון צרכים, ובהם: מניעת עבירות, הכְוונת תנועה ואיסוף מידע חזותי אחר. התפתחות נוספת בנושא זה נרשמה בישראל בעקבות יישום התוכנית "עיר ללא אלימות" ולנוכח היוזמה המשטרתית לצייד שוטרים במצלמות לבישות. בהמשך למסמך ההנחיה הראשוני, ולאור התפתחות הטכנולוגיה והאתגרים שהיא מציבה, פרסמה הרשות להגנת הפרטיות בשנת 2017 טיוטה מעודכנת של ההנחיה כדי לקבל עליה את הערות הציבור.[20] מטרת ההנחיה הייתה להבהיר את עמדת רשם מאגרי המידע ביחס לתחולת הוראות חוק הגנת הפרטיות התשמ"א–1981 על שימוש במצלמות מעקב במרחב הציבורי, במיוחד במקרים שבהם הצילומים הנקלטים בהן נאגרים במאגרי מידע.

טיוטת ההנחיה החדשה כוללת התייחסות למגוון היבטים, בהם: דרישה שהשימוש במצלמות במרחב הציבורי יעמוד בתבחינים של תכלית ראויה ומידתיות ולאחר בחינת חלופות פוגעניות פחות; דרישה שלפני התקנת המערכות ייבחן היקף חשיפת הציבור להן וייעשה הדרוש כדי למזער חשיפה זו ככל האפשר; איסור שימוש במצלמות ובמידע הנקלט בהן למטרות אחרות זולת התכלית שלשמה הותקנו, בתנאי שהתועלת מהשימוש במצלמות תגבר על הפגיעה בפרטיות שתיגרם בעטיין.

---

17 לדיון מעמיק ביתרונות ובחסרונות של המאגר הביומטרי ראו: קרין נהון, "קול פרטי: הפוליטיקה של המאגר הביומטרי", **משפט, חברה ותרבות**, ב 9, 2019, עמ' 271.

18 טנא, "חוק המאגר הביומטרי".

19 "הנחיית רשם מאגרי מידע מס' 4/2012 – שימוש במצלמות אבטחה ומעקב ובמאגרי התמונות הנקלטות בהן", *משרד המשפטים, הרשות להגנת הפרטיות*, 21 באוקטובר 2012.

20 "שימוש במצלמות מעקב ובמאגרי הצילומים הנקלטים בהן", *משרד המשפטים, הרשות להגנת הפרטיות*, 11 בספטמבר 2017.

עוד נקבע בהנחיה שהתקנת מצלמות באזורי קטינים תחייב הסכמה מפורשת של ההורים. ההנחיה גם מחילה מגבלות באשר למיקום המצלמות ומספרן. כך נדרש בה למקם את המצלמות רק במרחב הרלוונטי ולמנוע צילום ואגירת נתונים ממרחבים שאינם במסגרת התכלית האמורה.

בנוסף, חוק הגנת הפרטיות מקנה למצולמים זכות לעיין בהקלטות הנוגעות אליהם. החוק ותקנות הגנת הפרטיות (אבטחת מידע) התשע"ז–2017 מחייבים לאבטח את המידע הנקלט ונאגר במערכות המצלמות. ההנחיה מ־2017 מתייחסת במפורט להיבטי זיהוי ביומטרי והשוואה עם מאגרי מידע, אולם נעדרת התייחסות מפורשת למגבלות של טכנולוגיה זו ולהשפעתן על חירות האזרח ופרטיותו.

מהנדסים ומומחי אלגוריתמיקה נשענים לעיתים נדירות על מחקרים חברתיים. תופעה דומה מתרחשת גם בכיוון ההפוך. כך נתפסים יישומים ביומטריים כ"קופסה שחורה" ומסתורית וכמחזיקים מידע חד־ערכי על אנשים ונהלים, תהליכי אימות זהות, השוואה והתאמה. השילוב של חישובים מתמטיים עם נתונים ביולוגיים מעניק לכאורה לגיטימציה טכנית ומדעית־אובייקטיבית לתחום היישומים הביומטריים. יש לזכור בהקשר זה שטכנולוגיות ביומטריות מעורבות יותר ויותר בקבלת החלטות אוטומטית, ללא התערבות אנושית. כתוצאה מכך, גדֵלה הדילמה האתית באשר למיון חברתי העלול ליצור אפליה הנשענת על מאפיינים ביולוגיים חיצוניים.

סיכום

התפתחות הטכנולוגיה הגיעה לרמת בשלות ותפוצה כזו, המחייבת בחינה והתייחסות משפטית ונורמטיבית מפורשת לכל היבטי השימוש בה, ובכלל זה בטכנולוגיות ביומטריות לזיהוי מגוון מאפיינים (פיזיים ונפשיים). הריצה חסרת המעצורים קדימה, בה נמצאות חברות הטכנולוגיה בישראל ובעולם, גורמת להיבטים אלה להיוותר מאחור. לישראל עניין רב בפיתוח הכלכלי הנגזר מיישומים ביומטריים, ולכן טוב יהיה אם הגורמים הממשלתיים הרלוונטיים (משרד המשפטים, הרשות להגנת הפרטיות) יובילו מהלך בין־לאומי שמטרתו פיתוח דיון ערכי ומשפטי בשאלות החשובות העולות לאור תפוצת הטכנולוגיה בכלל והטכנולוגיה הביומטרית בפרט. בדרך זו תוכל מדינת ישראל להמשיך ולהשפיע על נורמות שיתפתחו בעתיד בתחום זה.

בעבר, הטכנולוגיה הביומטרית הייתה תחומה לצורכי ביטחון ואכיפה, אולם המצב כיום שונה. השימוש ביישומים ביומטריים גובר הן במגזר האזרחי והן במגזר המסחרי. התפוצה הנרחבת של יישומים ביומטריים מקנה חשיבות ממעלה ראשונה לטיפול בבעיות האתיות הטמונות בפיתוח טכנולוגיה בעלת תפוצה רחבה ופריסתה. מוטלת עלינו חובה לחקור ולפתח את הידע בדבר ההשלכות האתיות והמשפטיות של מצב זה על ארגונים אזרחיים ועיסקיים. נושא מפתח אותו יש לבחון במסגרת זו הוא שאלת הפרטיות.

למרות התפשטות הטכנולוגיה הביומטרית, יש מחקר אמפירי מועט על ביומטריה יישומית ואתיקה במגזר האזרחי והעיסקי. תהליך פיתוח הידע מחייב, לפיכך, תשומת לב גם לבחינת פוטנציאל הפגיעה והנזק העלולים להיגרם תוך כדי מעקב ביומטרי.

אין לראות בתחום הביומטריה פיתוח טכנולוגי גרידא. יש להעמיק בבחינת ההשלכות המשפטיות והאתיות שלו, כדי לגבש מסגרת חוקית ורגולטורית משוכללת שתוכל להתמודד עם מגוון האתגרים הצפוי בעתיד מכיוון זה.

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 פרופ׳ 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

גל ספיר galps@inss.org.il | **גל פרל פינקל** galp@inss.org.il
מתאמי כתב העת **סייבר, מודיעין וביטחון**

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