סייבר, מודיעין וביטחון

כרך 2 | גיליון 1 | אפריל 2018

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

סייבר, מודיעין וביטחון

כרך 2 | גיליון 1 | אפריל 2018

תוכן

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

סייבר, מודיעין וביטחון

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

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

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

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

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

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

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

כאשר פחות הוא יותר: קוגניציה ותוצאת הכפייה בסייבר

מיגל אלברשו גומס

העלייה במספר מקרי האינטראקציות ההתקפיות בסייבר בין מדינות ממשיכה לעורר עניין במה שנוגע לפוטנציאל הכפייתי של מִבצעי הסייבר. הדוגלים בגישה מהפכנית זאת מתעקשים על כך שהיא מהווה שינוי במאזן היחסים בין מדינות. עם זאת, עדויות המבוססות על מקרים שאירעו בעבר מאתגרות גישה זו, שכן הן מוכיחות שמהלכי הכפייה בסייבר מובילים לעיתים קרובות דווקא להתנגדות מתמשכת ולא לציות. אף על פי כן, וללא קשר לתוצאות, לא ניתן לבטל בקלות את פוטנציאל הכפייה שקיים במרחב הסייבר. מאמר זה טוען כי ניתן להסביר את התוצאה של מבצעי כפייה בסייבר על ידי שימוש באסטרטגיה האוריסטית של קבלת החלטות יותר מאשר בגישות הנורמטיביות, כגון האסטרטגיה של מידת "התועלת הצפויה".

מילות מפתח: האוריסטיקה קוגניטיבית, תועלת צפויה, כפייה, מרחב סייבר

מבוא

ב־23 בדצמבר 2015 השביתה התקפת סייבר יותר מחמישים תחנות חשמל משניות במערב אוקראינה והותירה יותר מ־230,000 תושבים ללא חשמל. היה זה המקרה הראשון של אירוע סייבר שהוביל לשיבוש ברשת החשמל של מדינה כלשהי.[1] שלוש

מיגל אלברשו גומס הוא חוקר בכיר במרכז ללימודי ביטחון, ETH Zurich, ודוקטורנט באוניברסיטת קרדיף, ויילס.

1 Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid", *WIRED*, March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

שנים מאז תחילת הסכסוך האוקראיני־רוסי מתחזקת ההבנה שאירועים מסוג זה משמשים בימינו כאמצעי כפייה במצבים של סכסוך.[2]

יש מומחים הסבורים כי ככל שתלותן של הפוליטיקה, הכלכלה והחברה הגלובלית במרחב הסייבר הולכת וגוברת, כך גובר באופן פוטנציאלי האיום במרחב זה.[3] נראה כי במצב זה אכן גוברת "הרוח הגבית" לכפייה באמצעות הסייבר, וזאת בשל העלאת המחיר הפוטנציאלי של אי־ציות לאיומים על תשתיות הסייבר הבסיסיות. עם זאת, ולמרות דעותיהם של המומחים, היו גם מקרים שבהם המותקפים בחרו להתנגד לתוקף ולא לציית לדרישותיו.[4] יתר על כן, גם כאשר מבצעי הכפייה בסייבר היו מתקדמים מבחינה טכנית, הם לא הביאו לשינוים משמעותיים במדיניותו של הצד המותקף.[5]

אלה המותחים ביקורת על גישה זאת מייחסים את הביצועים החיוורים של מבצעי סייבר בכפייה למגבלות המובנות בתחום זה. עם זאת, אין למהר ולבטל במחי יד את התועלת האסטרטגית הטמונה בכפייה באמצעות סייבר. כפי שמציינים גרטצקה ולינדסי, "הפוטנציאל של מרחב הסייבר מוגבל יותר ממה שמוערך בדרך כלל, אולם הוא אינו זניח...".[6] לפיכך, מן הראוי להוסיף ולחקור את השימוש שמדינות עושות במבצעי כפייה בסייבר.

מאמר זה חורג מן הדעה הרווחת, שלפיה הצלחות של מבצעי סייבר בכפייה, או כישלונן, נגזרים מאסטרטגיות נורמטיביות של קבלת החלטות, שבאמצעותן החלטה לציית או להתנגד לכפייה בסייבר מתקבלת כפונקציה של הרווח או ההפסד הצפויים. תחת זאת עושה המאמר שימוש בהאוריסטיקה קוגניטיבית, המאפשרת תובנה ברורה יותר באשר לשאלה מדוע מדינות מתנהלות לעיתים באופן המנוגד לציפיות, לפיהן הן יישמו אסטרטגיות "יותר רציונליות". ההסבר המצומצם שאותו

---

2 "Analysis of the Cyber Attack on the Ukrainian Power Grid", *SANS*, March 18, 2016, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

3 Myriam Dunn-Cavelty, "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse", *International Studies Review* 15, no. 1 (2013): 105–122; Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare", *Security Studies* 22, no. 3 (2013): 365–404; Jon R. Lindsay and Erik Gartzke, "Coercion through Cyberspace: The Stability-Instability Paradox Revisited", in *Coercion: The Power to Hurt in International Politics*, eds. Kelly Greenhill and Peter Krause (New York: Oxford University Press, 2016).

4 Benjamin M. Jensen, Brandon Valeriano and Ryan Maness, "Cyber Victory: The Efficacy of Cyber Coercion" (Paper presented at the Annual Meeting of the International Studies Association, Atlanta, GA., 2016).

5 Emilio Iasiello, "Cyber Attack: A Dull Tool to Shape Foreign Policy", in *Fifth International Conference on Cyber Conflict*, eds. Karlis Podins, Jan Stinissen and Markus Maybaum (Tallinn: NATO CCD COE, 2013), pp. 451–468.

6 Lindsay and Gartzke, "Coercion through Cyberspace".

מציעות גרסאות שונות של פרדיגמת הבחירה הרציונלית מסייע לנו להבין את הסביבה המורכבת; הוספת ממד קוגניטיבי משקפת את הצורך בחיפוש אחר נרטיבים המסבירים טוב יותר את תופעת הכפייה באמצעות סייבר. בעשותו זאת, מכיר המאמר בצורך שהעלו דין ומק־דרמוט להבין כי התנהלות של מדינה במרחב הסייבר מתבססת על אינטראקציה בין גורמים הפועלים ברמות פעולה שונות.[7]

על רקע זה, המאמר בודק את מידת הסבירות של השימוש בהאוריסטיקה קוגניטיבית כאסטרטגיה לקבלת החלטות במענה לניסיונות כפייה בסייבר. לצורך זה מחולק המאמר לארבעה חלקים. החלק הראשון מביא סקירה כללית קצרה של תופעת הכפייה במרחב הסייבר. לאחר מכן באה ביקורת על התפיסה הרווחת לפיה מרחב הסייבר הוא תחום של סיכון המתבטא ביישום לקוי של אסטרטגיית "התועלת הצפויה" כדי לפרש באמצעותה תגובה של מדינות לניסיונות כפייה בסייבר. במקום אסטרטגיה זאת מציע המאמר כחלופה את ההאוריסטיקה הקוגניטיבית, מתוך הבנה שהחלטות מתקבלות על ידי ניצול של המאפיינים הסטטיסטיים הייחודיים של מרחב הסייבר. בחלק השלישי בודק המאמר את מידת ההתאמה של גישה זו על ידי בחינתה על מבצע תולעת Stuxnet. המאמר מסתיים בדיון על המגבלות של מסגרת תיאורטית זו.

כפייה ומרחב הסייבר

ההתעניינות האסטרטגית במרחב הסייבר גברה במהלך שני העשורים האחרונים בעקבות צמיחתן של תשתיות הסייבר והגידול בתפוצתן.[8] התפתחות זו הועמדה בצלם של חששות מפני מידת הפגיעות של מערכות ותת־מערכות ואפשרויות הניצול לרעה שלהן על ידי תוקפים המשתמשים באסטרטגיות של מניעה או ענישה למטרות כפייה.[9] מצב זה מדגיש את הפגיעות המובנית של מרחב הסייבר יחסית לערכו החברתי־פוליטי והכלכלי, ומציג עתיד שבו מרחב הסייבר, המתבטא במבצעי סייבר, יהפוך לכלי כפייה עיקרי בידיהם של שחקנים המסוגלים לעשות בו שימוש. מכיוון שכפייה מוגדרת כשימוש בכוח או כאיום בשימוש בכוח כדי להפיק שינוי

7 Benjamin Dean and Rose McDermott, "A Research Agenda to Improve Decision Making in Cyber Security Policy", *Penn State Journal of Law and International Affairs* no. 5, January 1, 2017.

8 Stuart Starr, "Toward a Preliminary Theory of Cyberpower", in *Cyberpower and National Security*, eds. Franklin Kramer, Stuart Starr and Larry Wentz (Washington DC: Potomac Books, 2009), pp. 43–88.

9 Robert A. Pape, *Bombing to Win: Air Power and Coercion in War* (New York: Cornell University Press, 1996); John Stone, "Cyber War Will Take Place!", *Journal of Strategic Studies* 36, no. 1 (2013): 101–108.

בהתנהגותו של יריב,[10] המצב שנוצר בפועל מאשש את התפיסה שמבצעי סייבר מתאימים לצורך השגת מטרה זו. מאחר שהתוצאה של כפייה בסייבר מתבטאת בהפסד או ברווח, עצם האיום על תשתיות התומכות באינטרס האסטרטגי של מדינה יוביל אותה להערכה מחודשת של עמדתה.

למרות שחקר הכפייה במרחב הסייבר מעורר עניין בחוגים אקדמיים, הספרות המחקרית בנושא זה הינה עדיין מועטה. מחקרים ראשוניים המצביעים על פוטנציאל הכפייה בסייבר משקפים את היתרון ההתקפי שלו. לפי זלצמן, יתרון זה מתאפשר על ידי הרב־צדדיות ו"כוח הבייט" של מבצעי הסייבר. לדבריו, הרב־צדדיות היא היכולת של הצעדים הננקטים במרחב הסייבר להשפיע באופן שלילי על האינטרסים האסטרטגיים של מדינה.[11] "כוח בייט" הוא כמות הנזק הנגרמת על ידי פעולות הננקטות במרחב הסייבר. בנוסף לכך, היעדר מגבלות חומריות מעניק גם הוא יתרון אסימטרי למבצעי הסייבר. בעוד שגישה לכלי נשק קונבנציונליים (וגרעיניים) מוגבלת לעיתים קרובות משיקולים כלכליים, הזמינות של כלים הפועלים באמצעות רשתות מחתרתיות מעניקה יתרון דווקא לתוקפים המוגבלים מבחינה חומרית. עם זאת, התוצאות של מקרים שאירעו בעבר מעמידות בסימן שאלה את פוטנציאל ההצלחה של מבצעי כפייה בסייבר.

מתוך 164 מבצעי כפייה בסייבר שזוהו בעבר, 64 אחוזים בלבד הובילו לשינויים שניתן היה להבחין בהם בהתנהלותו של היריב.[12] יתר על כן, ניסיונות להכריח יריב באמצעות מניעה עלו יפה באחוז אחד בקירוב בלבד מן המקרים. אם התנאים הבסיסיים של מרחב הסייבר, כשהם משולבים עם היתרון ההתקפי של מבצעי סייבר, אכן מגבירים את פוטנציאל הכפייה בסייבר, נשאלת השאלה מהי, אם כן, הסיבה לשיעור ההצלחה המאכזב של מבצעי כפייה אלה?

הצלחת הכפייה או כישלונה

הראיות מצביעות על הפוטנציאל המוגבל של כפייה באמצעות הסייבר, אך אינן מבטלות לחלוטין את התועלתיות הטמונה בה. למרות הצורך לטפח ציפיות, הגורמים להצלחתה של כפייה בסייבר או לכישלונה נותרו בלתי ברורים. מחקרים העוסקים במימוש הכפייה בסייבר עושים שימוש באסטרטגיית "התועלת הצפויה" כדי להעריך את התנהלות המדינה מול ניסיונות כפייה כאלה. אסטרטגיה זו מניחה כי החלטתה של מדינה להתנגד או לציית לכפייה מבוססת על מִקסום ומזעור של

10 Daniel Byman and Matthew Waxman, *The Dynamics of Coercion: American Foreign Policy and the Limits of Military Might* (New York: Cambridge University Press, 2002).

11 Ilai Saltzman, "Cyber Posturing and the Offense-Defense Balance", *Contemporary Security Policy* 34, no. 1 (2013): 40–63.

12 Jensen, Valeriano and Maness, "Cyber Victory: The Efficacy of Cyber Coercion".

רווחיה והפסדיה האפשריים. ככל שמדינות ממשיכות להשקיע במרחב הסייבר כדי לעמוד ביעדיהן האסטרטגיים, כך גוברת ההשוואה שהן עושות בין איומי הכפייה ובין יעדיהן הכלכליים, המדיניים, החברתיים או הצבאיים, וקבלת ההחלטה אם לציית או להתנגד לכפייה נעשית בהתאם לעוצמת האיום על יעדים אלה.[13]

הגורם המכריע בפוטנציאל הכפייה בסייבר הוא היכולת לנצל את הפגיעויות הטכנולוגיות.[14] איום נפוץ במרחב הסייבר הוא זה הנובע מאותן פגיעויות, מאי־ידיעה ומתרחישים בלתי נמנעים אחרים המגולמים במרחב זה, אותם מנצלים מבצעי הסייבר. קֶבֶלטי מצביע על ההמשגה של האיומים הנובעים מהפגיעויות ומן ההיקף שבו מערכות נתפסות כחשופות לאיומים אלה ומושפעות על ידם.[15] הקישוריות והתלות ההדדית בין המערכות מאפשרת ליחידים ולארגונים לרענן אותן כל העת ולהרחיב את תחומיהן, אך במקביל הן מגבירות את ההשלכות השליליות על אותן מערכות במקרה של ניצולן לרעה. המורכבות של טכנולוגיות אלו ומגבלות האנוש הבסיסיות לא מאפשרות לסלק את האיומים באמצעות פיתוח המוצר וניהול איכות בלבד.

נסיבות אלו מובילות לשרשרת של מצבים הפועלים לטובתה של הכפייה באמצעות הסייבר. הראשון שבהם הוא אובדן תחושת הביטחון. מורכבותו של תחום הסייבר מגבירה את סיכויי התקיימותם של מצבי פגיעות הניתנים לניצול. הדבר הופך את יכולתו של תוקף לזהות פגיעויות לכמעט בלתי נמנעת ומאפשר לו לנצל אותן כדי להשיג יתרון לעצמו. מכאן שכל אימת שפגיעות זו מתקיימת במערכות ובתת־מערכות הנחשבות לקריטיות, החברה האזרחית נתונה בסיכון פוטנציאלי.[16]

יישום אסטרטגיית "התועלת הצפויה" על תרחיש של איומים בכפייה מצביע בסבירות גבוהה יחסית על צפי להפסדים, וכתוצאה מכך על צפי לציות. עם זאת, תקפותה של טענה זו תלויה לא רק בהכרה בתהליך של סיבה ומסובב ובאפשרות התממשותו, אלא גם ביכולתו של היריב המותקף למתן את האיומים. האמור לעיל יוצא מהנחה כי שחקן במרחב הסייבר פועל בסביבה ממורכזת סיכונים וכי הוא בעל ידע על איומים, יכולות והשלכותיהם.

---

13 Starr, "Toward a Preliminary Theory of Cyberpower".

14 Ronald J. Deibert and Rafal Rohozinski, "Risking Security: Policies and Paradoxes of Cyberspace Security", *International Political Sociology* 4, no. 1 (2010): 15–32.

15 Dunn-Cavelty, "From Cyber-Bombs to Political Fallout".

16 Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security and the Copenhagen School", *International Studies Quarterly* 53, no. 4 (2009): 1155–1175; James Lewis, "National Perceptions of Cyber Threats", *Strategic Analysis* 38, no. 4 (2014): 566–576.

סביבת מרחב הסייבר

הספרות בנושא הכפייה בסייבר נוהגת לשלב בין מושגי הסיכון ואי־הוודאות הנגרמים מיישום לא נכון של אסטרטגיית "התועלת הצפויה". המונחים "סיכון" ו"אי־ודאות" מגלמים תאימות מושגית מסוימת, אך כל אחד מהם מתאר למעשה סביבת מידע ייחודית המשפיעה על תהליכי קבלת ההחלטות ואיכותן. אם נאמץ את המינוח המשמש את סבֶג', הסיכון מתייחס ל"עולם קטן", שבו מקבל ההחלטה מודע להסתברויות של כל התוצאות והחלופות האפשריות. בניגוד לכך, אי־ודאות משקפת "עולם רחב", שבו ההסתברויות אינן ידועות או שאי אפשר לבטא אותן במידה כלשהי של ודאות מתמטית.[17]

אם נוהגים במרחב הסייבר כבתחום שבו הקישוריות והתלות ההדדית מגבילות את היכולת לחזות נקודות כישלון אפשריות ואת ההשלכות הנובעות מהן, משתמע מכך שמקבלי החלטות פועלים בהקשר של אי־ודאות יותר מאשר בהקשר של סיכון. בעניין זה הובהר זה מכבר כי אסטרטגיות נורמטיביות (כלומר, אסטרטגיית "התועלת הצפויה"), המשמשות בסביבות של אי־ודאות במקום בסביבת סיכון, נוטות להתאפיין בביצוע חסר. נושא זה מוצא ביטוי בדילמת bias-variance, המחמירה כאשר אסטרטגיות נורמטיביות מיושמות על סביבות לא מתאימות.

הדיוק ביכולת החיזוי של קבלת החלטות מאותגר על ידי שני גורמים חשובים: הטיה ושונות. המושג הראשון מתייחס למידת החריגה של מודל מן המצב האמיתי של סביבה מסוימת. מכיוון שאין לדעת מראש את מצב העניינים האמיתי, מודל שהוא נטול הטיה לחלוטין אינו יכול להתקיים. עם זאת, הטיה ממותנת על ידי שונות גוברת, הנובעת מהוספת פרמטרים המאפשרים מגוון רחב יותר של מצבים. בהתנהלות כזאת קיים סיכון של overfitting ושל הקטנת דיוק החיזוי. אסטרטגיות נורמטיביות כמו "התועלת הצפויה" מקזזות לעיתים קרובות את ההטיה על ידי הכללת פרמטרים כמו אלה שהוזכרו לעיל. זוהי גישה המתאימה לסביבות שבהן ניתן למצוא בקלות מקרים לדוגמה, או כאשר מקרים כאלה אינם דו־משמעיים. אסטרטגיות נורמטיביות עשויות להיות מסוגלות לתאר במדויק הבחנות קודמות, אך הן ייכשלו בחיזוי תוצאות עתידיות. במצבים כאלה, האוריסטיקה קוגניטיבית עשויה להתברר כמתאימה יותר להשגת המטרה.

האוריסטיקה מוגדרות כ"אסטרטגיות המתעלמות מחלק מן המידע, מתוך מטרה לקבל החלטות מהר יותר ובצורה חסכונית ו/או מדויקת יותר מאשר על

17 Kirsten G. Volz and Gerd Gigerenzer, "Cognitive Processes in Decisions Under Risk are not the Same as in Decisions Under Uncertainty", *Frontiers in Neuroscience* no. 6, July 12, 2012.

בסיס שיטות מורכבות יותר".[18] בהשוואה לאסטרטגיות הנורמטיביות, טעויות באסטרטגיית ההאוריסטיקה נובעות אך ורק מתוך הטיות. גם אם השגת דיוק באמצעות פחות מידע נראית כמנוגדת לאינטואיציה, בסביבות של אי־ודאות ההאוריסטיקה טובה יותר למעשה מן האסטרטגיות ה"רציונליות". דוגמה לכך הוא תחום ההשקעות. בורחֶס ואחרים מראים כי אפשר להשתמש בזיהוי שמה של חברה בלבד כדי לבנות תיק השקעות עם תשואות הגבוהות בעשרה אחוזים לפחות בהשוואה לשימוש באסטרטגיות אחרות.[19] במחקרם קיימת קורלציה חיובית חזקה בין החברה ובין ביצועיה בשוק, המנוצלת על ידי מקבלי ההחלטות העושים שימוש ביכולתם לזהות יחס זה מן הזיכרון (כלומר, כיסוי תקשורתי חוזר של חברה בעלת ביצועים טובים). מצב זה מאפשר לבחור חברה מסוימת על פני אחרת כאשר מרכיבים תיק השקעות.

דיון מעמיק בהאוריסטיקה נמצא מחוץ לטווח הטיפול של מאמר זה. אף על פי כן, חיוני לציין כי היתרונות של ההאוריסטיקה מבוססים על היכולת לנצל את המאפיינים הסטטיסטיים של סביבה העושה שימוש ביכולות קוגניטיביות אינהרנטיות, כגון זיכרון. במילים אחרות, ההאוריסטיקה היא מדויקת רק באותה מידה שהיא מתאימה למבנים קיימים.[20] נושא זה מוכר בהקשרים אחרים כרציונליות אקולוגית.

הרציונליות האקולוגית של מרחב הסייבר

אסטרטגיית ההאוריסטיקה מתאימה לסביבות המתאפיינות באי־ודאות, ביתירות, במחסור בנתונים ובשונות.[21] החלקים הקודמים במאמר עסקו בטבעו הבלתי ודאי של מרחב הסייבר. נושא זה דורש הסבר נוסף. שימוש מורחב בתזה של פרו (Perrow), המופיעה בספרו *Normal Accidents*, מאפשר לטעון שהקישוריות והתלות ההדדית שאותן מאפשר מרחב הסייבר גם מגבילות את היכולת לחזות את הסיבות של אירועים גורמי שיבוש ואת השלכותיהם. ללא מערכת יחסים פרדוקסלית זו לא הייתה מתקיימת האפשרות של "אסונות מתגלגלים", שהם

18 Gerd Gigerenzer and Wolfgang Gaissmaier, "Heuristic Decision Making", *Annual Review of Psychology* no. 62, January 10, 2011.

19 Bernhard Borges, Daniel G. Goldstein, Andreas Ortmann and Gerd Gigerenzer, "Can Ignorance Beat the Stock Market", in *Simple Heuristics That Make Us Smart*, eds. Gerd Gigerenzer, Peter M. Todd and the ABC Research Group (New York: Oxford University Press, 1999).

20 Laura Martignon and Ulrich Hoffrage, "Why Does One-Reason Decision Making Work?", in *Simple Heuristics That Make Us Smart*.

21 Peter M. Todd, Gerd Gigerenzer and the ABC Research Group, *Ecological Rationality: Intelligence in the World* (New York: Oxford University Press, 2011).

הבסיס לפוטנציאל הכפייה באמצעות הסייבר.[22] מעבד תמלילים, לדוגמה, הפועל בנפרד ובאופן עצמאי (stand-alone), מאפשר למומחים לאבטחת מחשבים, על בסיס ניסיונם עם תוכנות דומות, לחזות את מספר נקודות התורפה לכל אלף שורות קוד. במצב זה, הפעולה נעשית בסביבה של סיכון, תוך הכרת הפגיעויות האפשריות שנגזרות מן הגישה הישירה לקוד הבסיסי של התוכנה ו/או מן הניסיון. כדי להגביר את הפריון, משתמשים יוכלו ליצור קשר הדדי בין מעבדי התמלילים שלהם, שיאפשר להם לעבוד תוך שיתוף פעולה. אם יעשו כן, יצטמצם הידע הקודם על מאפייני הפגיעות, שכן מצבן של המערכות האחרות שאליהן הם מתחברים אינו מוכר. עקב כך, מסובך יותר ויותר לחזות היכן, מתי או כיצד עלול להתרחש כשל, מה שמציב את המשתמשים בסביבה של אי־ודאות.

כאשר מיישמים דוגמה זו על שאלת הכפייה בסייבר, מדינות התלויות במערכות סייבר אינן יכולות לחזות את ההיקף האמיתי של הנזק שתוקפים עלולים לגרום, והדבר מונע את היכולת להעריך במדויק את ההשלכות של ציות לכפייה או התנגדות לה. יש מי שטוענים כי נקודה זו מציבה אתגר בפני עצם התועלת שבכפייה במרחב הסייבר. מאמר זה טוען, לעומת זאת, כי אין בכך כדי לצמצם בהכרח את יכולת הכפייה באמצעות הסייבר, וכי המצב שתואר לעיל מצביע בעצם על כך שהיעדר מידע משפיע על בחירתה של האסטרטגיה הנכונה לקבלת החלטות באירועים מסוג אחר.

כפייה במרחב הסייבר אינה מתקיימת בחלל ריק, וחוסר הוודאות לגביה מושפע ממאפייני היתירות הקיימים. יתירות היא הקשר הקיים בין סימנים או רמזים בתחום המידע שבהם משתמשים בתהליך קבלת ההחלטות. חשוב לציין כי במבצעי כפייה בסייבר מעורבים לעיתים קרובות יריבים ותיקים עם היסטוריה של התנהלות אגרסיבית זה כלפי זה,[23] ולפיכך קיימת ציפייה להתרחשותן של פעולות מסוימות בין שני הצדדים, בין אם במרחב הפיזי ובין אם בתחום הווירטואלי. ריגול הסייבר הסיני נגד ארצות הברית, לדוגמה, אינו מפתיע במיוחד, והוא קשור בקורלציה חיובית לאינטרס הסיני להשיג יתרון במידע. בניגוד לכך, נראה כי מתקפת תוכנת הכופר WannaCry, המיוחסת לקוריאה הצפונית, אינה קשורה ליעדים האסטרטגיים או המדיניים של המשטר שם. הדבר מצביע על כך שאירועים מסוימים במרחב הסייבר מוגדרים מלכתחילה על ידי יחסים בין־מדינתיים הקיימים זה מכבר. בהתאם לכך, מקבלי החלטות עשויים לנצל מערכת יחסים זו ואת מידת ההיכרות שלהם עם הנושאים כדי להעריך את יכולתם לממש מבצעי כפייה בסייבר ואת השלכותיהם.

---

22 Charles Perrow, *Normal Accidents: Living with High-Risk Technologies* (Princeton: Princeton University Press, 1999).

23 Brandon Valeriano and Ryan C. Maness, "The Dynamics of Cyber Conflict Between Rival Antagonists, 2001–11", *Journal of Peace Research* 51, no. 3 (2014): 347–360.

אפשר אמנם לראות את מרחב הסייבר כהארכה של המרחב הפיזי שבו מבוטאת מערכת יחסים, אך מצבים כאלה הם נדירים למדי. לכן, המידע בדבר היעילות הכוללת של מבצעי כפייה בסייבר, מבחינת הכלים המועדפים, הטקטיקה והתוצאות, כמו גם מידע רלוונטי אחר, הוא מצומצם בהיקפו. למרות שההתקדמות בטכניקות פורנזיות מאפשרת ניתוח טוב יותר של מאפיינים טכניים, מאפיינים כאלה לבדם מאפשרים להגיע לתובנה אסטרטגית מוגבלת בלבד.[24] כתוצאה מכך, חוסר הוודאות ברמה הטכנולוגית מצטרף לחוסר הוודאות ברמה האסטרטגית/מדינית ומגדיל את הספק באשר לתועלתה של כפייה באמצעות הסייבר. עם זאת, נראה כי הדבר נכון רק אם מתבוננים בו דרך העדשה של גישות נורמטיביות, כגון זו של אסטרטגיית "התועלת הצפויה". מכיוון שהחלטות מתקבלות על בסיס רווח והפסד, אין במיעוט המידע די כדי להגיע למסקנה שלא יהיו הפסדים בעתיד, או שתימשך ההצלחה באמצעות השגת פשרה, שכן מקבלי ההחלטות אינם יכולים להיות מודעים לכל התוצאות והחלופות האפשריות.

לבסוף, רמת הביצוע של אסטרטגיית ההאוריסטיקה תלויה במשקלם או בתוקפם של הרמזים הקיימים בסביבה. התוקף הוא השיעור שעל פיו סימנים או רמזים יכולים להבחין באופן נכון בין אפשרויות שונות. לדוגמה, האם היערכות קדומנית של כוחות צבא הובילה בעבר לציות של המדינה שהייתה מאוימת על ידי אותם כוחות? בתרגום דוגמה זו לעיקריה של תיאוריית הכפייה בסייבר, ניתן לומר כי התוצאה של כפייה כזאת תלויה הן ביכולתו של הכופה לגבות מחירים מן היריב על ידי איום על נכסיו, והן באופן שבו המאוים הפוטנציאלי מעריך נכסים אלה שלו. הספרות המדעית עוסקת בנקודה הראשונה של טענה זו. לעומת זאת, היא מטפלת רק לעיתים רחוקות בשונות הקיימת בין יריבים בתפיסתם את מרחב הסייבר, דבר המשפיע עליהם בבואם להעריך את נכסיהם.[25] במילים אחרות, מה שעשוי להיות רמז תקף לציות במקרה אחד, עלול לא להיות כזה במקרה אחר. דבר זה מגביר את חוסר הוודאות.

בחירת האסטרטגיה ההאוריסטית

כאמור, האסטרטגיה ההאוריסטית יכולה להיות חלופה טובה יותר מהאסטרטגיות הנורמטיביות כדי להסביר את תוצאותיה של כפייה במרחב הסייבר, וזאת בהתבסס על הרציונליות האקולוגית של מרחב זה. יתרונותיה של האסטרטגיה ההאוריסטית נובעים ממספר סיבות: ראשית, אי־ודאות מונעת ממקבלי החלטות את היכולת

24 Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks", *Journal of Strategic Studies* 38, no. 1 (2015): 4–37.

25 Forrest Hare, "The Cyber Threat to National Security: Why Can't We Agree", in *Conference on Cyber Conflict Proceedings*, eds. Christian Czosseck and Karlis Podins (Tallinn: CCD COE, 2010).

לקיים הערכה אמפירית של כל התוצאות והחלופות האפשריות; שנית, הקורלציה בין אירועים במרחב הסייבר ובין יריבויות קיימות מפצה על אי־הוודאות ומאפשרת שימוש בניסיון העבר במרחב הסייבר לצורך קבלת החלטות; שלישית, הנדירות של מבצעי סייבר בכפייה מגבילה עוד יותר את השימוש באסטרטגיות נורמטיביות, שכן היא מונעת ממקבלי ההחלטות נקודות ייחוס שעליהן הם יוכלו לבסס את החלטותיהסף; לבסוף, חוסר היכולת לזהות מאפייני שונות בתוקפם של רמזים מוביל לגישה ספציפית מוטעה. כאשר מודעים לנקודות אלו, השאלה הנותרת היא איזו אסטרטגיה האוריסטית היא המתאימה ביותר לטיפול במבנים ארגוניים סביבתיים (environmental structures).

המאמר מניח כי האוריסטיקה המבוססת על נימוק יחיד (one-reason) היא זו המאפשרת להבין את תוצאותיו של מבצע כפייה בסייבר. משפחה זו של האוריסטיקה פועלת היטב במקרים שבהם הרמזים משתנים במידה רבה, קיימת יתירות, וכמות המידע מצומצמת.[26] שימוש בהאוריסטיקה של נימוק יחיד כדי להחליט האם לציית או להתנגד לדרישות שנעשות בכפייה מוביל לתהליך קבלת החלטות המתנהל בהתאם לכללים של "חיפוש, עצירה וקבלת החלטה". כללים אלה קובעים את דרך החיפוש של הרמזים הנכונים, את התנאים שבהם יש להפסיק את החיפוש ואת הדרך שבה רמזים אלה ייושמו ויובילו לקבלת החלטה ספציפית.

למרות פשטותה של האסטרטגיה ההאוריסטית, ביצועיה טובים יותר מאלה של אסטרטגיות מורכבות יותר, כגון "רגרסיה רבת משתנים" (multiple regression), רשתות עצביות וכדומה. עם זאת, חשוב לקבוע כי האסטרטגיה ההאוריסטית אינה באה במקום האסטרטגיות האחרות, שכן היא נמנעת מחיפוש ראיות סותרות ומתבססת על הערכה סובייקטיבית יותר מאשר אובייקטיבית של מצב נתון. מאפיין זה עלול להתברר כבעייתי, ואפילו כמסוכן, בסביבות מסוימות. לדוגמה, מבצע הנערך על ידי צד שלישי תחת "דגל כוזב", ומחקה את התנהגות היריב, עלול להוביל, בנסיבות מסוימות, להסלמה בלתי מכוונת.

ישימות ההאוריסטיקה – המקרה של Stuxnet

כדי לתמוך בטיעונים התיאורטיים שצוינו לעיל, להלן תודגם ישימותה של אסטרטגיית ההאוריסטיקה. מספר אירועים שהתרחשו מאז שנת 2007 עשויים לשרת מטרה זו, אך המאמר ידון רק במקרה של מתקפת Stuxnet, שיוחסה הן לארצות הברית והן לישראל. ההחלטה לעשות שימוש במקרה זה לצורך הדגמה מבוססת על זמינות המידע לגביו, המאפשרת לערוך השוואה בין שתי אסטרטגיות של קבלת החלטות.

---

26 Gerd Gigerenzer, "Why Heuristics Work", *Perspectives on Psychological Science* 3, no. 1 (2008): 20–29.

את האינטראקציה בין ארצות הברית לאיראן במרחב הסייבר ניתן לאפיין כסדרה של מעשי כפייה הנעשים באינטנסיביות, בחומרה ובהיקף משתנים.[27] מבין אלה, סטאקסנט הוא המקרה המפורסם ביותר של כפייה בסייבר. על קיומו נודע לראשונה ב־17 ביוני 2010, כאשר בוצעה פנייה לחברת האנטי־וירוס VirusBlokAda בבלרוס כדי שתיתן מענה לאתחולים מחדש בלתי מוכרים של מערכות שהתרחשו באותה העת באיראן.[28] למרות "גילויה" לראשונה בשנת 2010, אנליסטים סבורים כי תוכנת סטאקסנט הייתה מבצעית כבר בחודש יוני 2009, כאשר הדביקה עשר פעמים חמישה ארגונים בתוך איראן וגרמה ל־12,000 הדבקות בסך הכל עד למועד שבו זוהתה בשנת 2010.

התכונות המתקדמות של סטאקסנט מצביעות על מעורבותן של ישויות מדינתיות, או של כאלו הממומנות על ידי מדינה, בפיתוחו ובהפצתו. תכונות אלו העניקו לסטאקסנט את ההכרה כתוכנה הזדונית "החמושה" הראשונה בהיסטוריה. מגוון התכונות של התוכנה ויעדיה (מערכות בקרה תעשייתיות) גם הצביע על שינוי ביכולות, במורכבות ובכוונות של שחקנים הפועלים במרחב הסייבר.[29] החל עידן חדש בדו־שיח על השימוש באמצעי לחימה בסייבר.

למרות מאפייניו המבצעיים ותכונותיו, סטאקסנט לא הצליח לכפות על המשטר האיראני את סיום תוכנית ההעשרה הגרעינית שלו. התחושה הרווחת היא כי כישלון זה של סטאקסנט נבע מן הנזק המוגבל שנגרם לתשתית ההעשרה האיראנית. למעשה, עד שההדבקה בווירוס נבלמה, ניזוקו יותר מאלף סרכזות ששימשו את איראן להעשרת אורניום, אך ניתוח שנעשה לאחר האירוע העלה כי מספר הסרכזות שניזוקו לא עלה על בלאי ופחת תפעוליים רגילים. הסבר זה עולה בקנה אחד עם הבנת מושג הכפייה דרך האסטרטגיה של "התועלת הצפויה". במילים אחרות, לפי אותה אסטרטגיה, הנזק שנגרם לסרכזות האיראניות לא הגיע לממדים משבשים, מחלישים או כאלה המחייבים הערכה מחדש של המדיניות האיראנית. כדי שטיעון זה יהיה תקף, יש לאמץ הנחה חיונית אחת: כי למשטר האיראני היה מידע נכון על יכולותיו ופגיעותו במרחב הסייבר, מה שנתן לו את הביטחון שהוא יכול להסתכן בהתמודדות עם ניסיונות פגיעה נוספים בתשתית הסייבר שלו. אם אכן כך הדבר, הוא מרמז על קבלת ההחלטה להתנגד לניסיונות הכפייה בסביבה של סיכון. אלא שהתגובה האיראנית מאתגרת הנחה זו, הן אמפירית והן תיאורטית.

---

27 Jason Healey, "Winning and Losing in Cyberspace", in *Eighth International Conference on Cyber Conflict*, eds. Nikolaos Pissanidis, Henry Roigas and Matthijs Veenendaal (Tallinn: CCD COE, 2010).

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

29 Lindsay, "Stuxnet and the Limits of Cyber Warfare".

יהיה זה בלתי סביר להניח שהאחראים על ביטחון הסייבר באיראן החזיקו במידע מושלם על כל כיווני ההתקפה האפשריים על מערך הסייבר האיראני. תוכנית אבטחה מתאימה הייתה נוקטת לכל הפחות צעדים כדי למתן את האיומים שהיו מוכרים הן מניסיון עצמי והן ממידע שהיה זמין לכלל הציבור. במקרה של סטאקסנט, הדיווחים על פניית הרשויות האיראניות לגורמים שלישיים זרים כדי להיטיב להבין את ההתנהגות החריגה של המערכות שלהם, מצביעים על כך שהם לא צפו אירוע מסוג זה וגם לא העריכו את השלכותיו האפשריות. למעשה, המורכבות של סטאקסנט, שהייתה ללא תקדים, לא אפשרה לגזור ממנו חישוב כלשהו של נזקים והפסדים אפשריים.

ניתן לטעון כי מידע נוסף על יכולות הסטאקסנט ופוטנציאל הנזק שלו היה מתגלה עם התקדמות החקירה, דבר המרמז על מומחיות טכנולוגית ומערכת ארגונית מוגדרת המאפשרות קיומם של מאמצים כאלה. ארגונים זקוקים למנגנון המאפשר לבצע סינתזה של מידע בין יחידות שונות כדי להבין את מכלול ההשלכות של אירועים. עם זאת, לא ניתן לצאת מתוך הנחה שמבנה ארגוני כזה קיים בכל המדינות, וגם יעילותו אינה בבחינת דבר מובן מאליו.[30] התלות של איראן בסיוע חיצוני במהלך תקרית הסטאקסנט, יחד עם דיווחים מוקדמים יותר על יכולותיה במרחב הסייבר, מעמידים בספק את יכולתה להבין באופן מלא את השלכותיו של וירוס זה ומאתגרים עוד יותר את מידת ישימותן של אסטרטגיות נורמטיביות לצורך מתן הסבר להחלטת איראן להתנגד לכפייה באמצעותו.

אילו המשטר האיראני היה בטוח ביכולתו להתגונן מפני סטאקסנט או מפני צעדי כפייה אחרים, מדוע הוא לא הגיב תגובה חזקה יותר? הן גרטצקה והן לינדזי טוענים כי מבצעים המסתכמים בפשרה, אך למעשה נבלמים, מסתיימים לבסוף בסחרור של הסלמה.[31] לעומת זאת, מודל המשחק התיאורטי של אדוארדס ואחרים, למרות שהוא פחות קיצוני, גורס כי אלה המודעים לפגיעויות של עצמם והצליחו למתן אותן, צריכים, לפחות ברמה הציבורית, לייחס מעשי כפייה ליריביהם.[32] שום דבר מאלה לא קרה בכל מה שנוגע לסטאקסנט. אמנם, מספר חוקרים טוענים כי התגובה האיראנית התבטאה במבצעי סייבר איראניים במועד מאוחר יותר, אך לא נראה כי המאפיינים המבצעיים של התגובות היו בעלי ממדים שיכלו לשמש כמענה הולם לסטאקסנט, או שנתפרו על פי מידותיו.

---

30 Rebecca Slayton, "What is the Cyber Offense-Defense Balance?", *International Security* 41, no. 3 (2017): 72–109.

31 Erik Gartzke and Jon R. Lindsay, "Thermonuclear Cyberwar", *Journal of Cybersecurity* 3, no. 1 (2017): 47–48.

32 Benjamin Edwards, Alexander Furnas, Stephen Forrest and Robert Axelrod, "Strategic Aspects of Cyber Attack, Attribution and Blame", in *Proceedings of the National Academy of Sciences* (forthcoming).

אם בוחנים בצורה יסודית יותר את הגרסה הרווחת באשר לכישלון מבצע סטאקסנט, המאשרת לכאורה את התועלת של השימוש באסטרטגיות הנורמטיביות, מתברר כי היא ניצבת למעשה על קרקע לא יציבה. למרות שמדובר בספקולציה, הנובעת מהיעדר מידע ממקור ראשון על הנעשה באיראן, נראה שהמשטר שם היה חסר הבנה מלאה של מיני הפגיעויות שלו בתחום הסייבר. במצב זה לא היה ראוי שמקבלי ההחלטות באיראן יסתמכו על אסטרטגיית "התועלת הצפויה" או על אסטרטגיות דומות לה כדי לגבש את תגובתם, וזאת נוכח העובדה שהמידע שהיה בידיהם על ההשלכות האפשריות של התנגדות או ציות לכפייה היה חלקי בלבד או לא זמין לחלוטין. יתר על כן, הישימות של אסטרטגיות נורמטיביות מאותגרת גם במקרים אחרים של כפייה בסייבר. כך, למשל, מבצע "BoxingRumble" נגד ריגול הסייבר הסיני לא גרם לנזק משמעותי, ולמרות זאת, תגובת סין הייתה עצירה זמנית של פעילות הריגול.[33] נראה כי סתירה לכאורה זו מעמידה בסימן שאלה את תוקף המסקנות המבוססות על שימוש באסטרטגיות הנורמטיביות.

סגירת הפער

בהנחה שאסטרטגיות נורמטיביות כמו "התועלת הצפויה" אינן מתאימות לסביבת הכפייה באמצעות הסייבר, נשאלת השאלה האם אסטרטגיית ההאוריסטיקה עשויה להיות התשובה לכך. אם מרחיבים את הטענה שכפייה באמצעות הסייבר מתרחשת בין יריבים וכי מבנים ארגוניים סביבתיים מעדיפים את אסטרטגיית ההאוריסטיקה של החלטה יחידה, ניתן להוכיח הנחה זו על ידי שימוש בהאוריסטיקה "קח את האחרון" (Take the Last – TTL).

האוריסטיקה של TTL פועלת בדרך כלל תוך שימוש באסטרטגיה המוכרת כמערך *Einstellung*. מאז שנות השלושים של המאה העשרים הבחינו פסיכולוגים כי יחידים פותרים בעיות הנראות קשורות זו בזו באמצעות אסטרטגיות שפעלו היטב בעבר.[34] מכאן נובעת ההנחה כי האוריסטיקה של TTL משמשת בסביבות שבהן ההחלטות שמתקבלות עוסקות באירועים הקשורים בדרך זו או אחרת אלה באלה. קורלציה זו מתבטאת באופן עקיף ביכולתו של מקבל ההחלטה לזהות קווי דמיון בין משימות שונות. הזיהוי במקרה זה אינו בהכרח שווה ערך לזיכרון, אלא מתייחס למאפיינים אינטואיטיביים של אירועים – מאפיינים המתחזקים על ידי חשיפה נמשכת להם.

---

33 Sean Gallagher, "NSA secretly hijacked existing malware to spy on N. Korea, others", *arsTechnica*, January 19, 2015, https://arstechnica.com/information-technology/2015/01/nsa-secretly-hijacked-existing-malware-to-spy-on-n-korea-others/.

34 Gerd Gigerenzer and Daniel G. Goldstein, "Betting on One Good Reason: Take the Best Heuristic", in *Simple Heuristics That Make Us Smart*.

מכיוון שמבצעי סייבר בכפייה מערבים יריבים משכבר הימים המקיימים אינטראקציה קבועה זה עם זה, TTL מהווה אסטרטגיה אידיאלית לטיפול בהם, לא רק בגלל המבנים הסביבתיים, אלא גם בשל יעילותה. שלא כמו אסטרטגיית "התועלת הצפויה", המחייבת חישוב אינטנסיבי (דבר המגביר את העומס הקוגניטיבי), TTL מסתמכת אך ורק על ההכרה לצורך זיהוי החלופות. יתר על כן, במצבים קריטיים מבחינת הזמן, כגון סכסוכים בין מדינות, המהירות שבה מיושמת אסטרטגיית TTL הופכת אותה לבחירה מועדפת על פני אסטרטגיות חלופיות. שיטת TTL פועלת באופן הבא: איתור הרמז שהביא לעצירת החיפוש בבעיה הרלוונטית האחרונה והשוואתו לחלופות. אם תוצאת ההשוואה שונה מבעבר, יש להשתמש באותו רמז. במקרה שהדבר אינו כך, יש לחזור לבעיה לפני האחרונה ולאתר את הרמז שהביא לעצירת החיפוש באותה בעיה.

כאשר מסבירים את תוצאות הסטאקסנט על ידי שימוש בהאוריסטיקה של TTL, התהליך מתחיל על ידי בניית מאגר של כלל האירועים הדומים שהתרחשו בעבר. מכיוון שיעדו של סטאקסנט היה מערכות הבקרה של סרכזות גרעיניות האחראיות על העשרת אורניום, מאגר האירועים כולל, במידה גבוהה של ודאות, ניסיונות קודמים לכפות על איראן את עצירת העבודה בתוכנית הגרעין שלה. אין זו בהכרח הנחה בלתי מבוססת, לנוכח המאמץ הרב שהושקע על ידי יריביה של איראן, שביקשו להשיג בדיוק מטרה זאת. בנוסף, העובדה שאירוע הסטאקסנט התרחש במרחב הסייבר, אינה אמורה לפגוע ביכולתם של מקבלי ההחלטות לאתר נקודות דמיון בין האירועים השונים, נוכח העובדה שמדובר במטרה זהה (כלומר, סיום תוכנית הגרעין של איראן).

ברגע שבו נבנה מאגר מנטלי זה, נדרש מקבל ההחלטות לזהות את המקרה האחרון שבו הרמז גרם להבחנה בין החלופות השונות. מכיוון שאין בידינו גרסאות ממקור ראשון, המאמר מתייחס לאירועי כפייה שהתרחשו לפני יוני 2010. בין השנים 2006–2010 נערכה שורה של דיונים עם איראן, ואף על פי כן מועצת הביטחון של האו"ם הטילה עליה שש סנקציות שנועדו לשבש את תוכנית ההעשרה הגרעינית שלה. בנוסף לכך, ארצות הברית החלה אז לשקול ברצינות שימוש במהלומות אוויריות נגד איראן, וישראל איימה בנקיטת פעולה צבאית נגדה. אי אפשר לקבוע איזה מן האירועים הללו שימש כנקודת התייחסות של איראן, והדבר אינו משנה למעשה, שכן התוצאה הייתה זהה מבחינתה – התנגדות.[35]

ההקשר המשותף של אירוע סטאקסנט ושל אירועים דומים בעבר מוביל למסקנה שמקבלי ההחלטות באיראן בחרו להישאר עקביים בהתנהלותם המתנגדת לכלל

35 Shreeya Sinha and Susan Campbell Beachy, "Timeline on Iran's Nuclear Program", *New York Times*, April 2, 2015, https://www.nytimes.com/interactive/2014/11/20/world/middleeast/Iran-nuclear-timeline.html?_r=0#/#time243_10809.

צעדי הכפייה שננקטו נגדם. המאפיינים של סטאקסנט מגבילים את מידת הדיוק של אסטרטגיות מורכבות יותר לקבלת החלטות, בשל היעדר מידע על יכולותיה האמיתיות של התוכנה ועל מידת הפשרה. יתר על כן, אם ההתנגדות לניסיונות הכפייה פעלה היטב כאשר האיום היה גדול יותר (כלומר, כאשר על הפרק עמדה אפשרות של התנגשות פיזית של ממש), היא הייתה אמורה לפעול גם במצב הפחות קיצוני הזה.

לקראת העתיד

מאמר זה הציג את הטענה כי האוריסטיקה קוגניטיבית יכולה לשמש ככלי אנליטי להערכת תוצאותיו של מבצע כפייה בסייבר. אסטרטגיות נורמטיביות נותרות אמנם אבן היסוד להערכת התנהלותה של מדינה, אך המאפיינים הייחודיים של מרחב הסייבר מעמידים בסימן שאלה את מידת ההלימות שלהן למרחב זה. בתחום הפיזי, הניסיון מאפשר לגבש הערכה אובייקטיבית של רווחים והפסדים. לעומת זאת, חוסר הוודאות הטבוע במרחב הסייבר מגביל את יכולת החיזוי המדויקת של אסטרטגיית "התועלת הצפויה" ושל אסטרטגיות קשורות אחרות. במקום זאת, אסטרטגיות פשוטות וממוקדות מטרה, כגון האוריסטיקת TTL, מאפשרות לגבש תמונה ברורה יותר של צעדי כפייה בתחום וירטואלי זה.

ההסתמכות על האוריסטיקה בלבד אינה מאפשרת, עם זאת, להגיע למסקנה חלוטה. מכיוון שאין בנמצא אסטרטגיה לקבלת החלטות המתאימה לכל, מידת הישימות של אסטרטגיית האוריסטיקה או של אסטרטגיות נורמטיביות היא פונקציה של מבנים סביבתיים ושל היכולות הקוגניטיביות של יחידים גם יחד. תלות הדדית זו מבוטאת באופן מיטבי באנלוגיה שמביא הרברט סיימון, לפיה רציונליות דומה ללהבי מספריים, כאשר להב אחד מייצג את מגבלותיהם הקוגניטיביות של יחידים, בעוד שהלהב השני מייצג את המבנים והתנאים הסביבתיים. כשם שמספריים אינם יכולים לפעול באמצעות להב יחיד, באותה מידה הבנתנו את מושג הרציונליות אינה יכולה להיות מוגבלת להיבט יחיד כזה או אחר.

על רקע הנאמר לעיל, יש לציין שלוש נקודות חשובות. הראשונה היא שאין להציג את השימוש בהאוריסטיקה קוגניטיבית בתחום היחסים בין מדינות ככישלון הרציונליות. למרות ממצאים מן התקופה האחרונה בפסיכולוגיה קוגניטיבית, אנשי אקדמיה בתחום היחסים הבין־לאומיים ומדע המדינה ממשיכים להגדיר האוריסטיקה קוגניטיבית כאסטרטגיה בעלת עלות נמוכה שמובילה להחלטות שאינן מיטביות. במקום זאת, המאמר הנוכחי מדגיש את חשיבות התאמתן של אסטרטגיות לסביבה ההולמת אותן, וזאת מתוך הבנה שאפילו גישות מורכבות עלולות להוביל לתוצאות עלובות אם נעשה בהן שימוש לא נכון.

שנית, על אף השימוש המוצלח באסטרטגיה של האוריסטיקה לצורך הערכת התוצאות של צעדי כפייה במרחב הסייבר, לא ניתן לעשות הכללה מתוצאות אלו על כלל צורות האינטראקציה במרחב זה. נראה כי האוריסטיקה פועלת טוב יותר כאשר מסבירים באמצעותה כפייה בסייבר. אז היא עושה זאת בזכות הניצול היעיל והנכון של מבנים ארגוניים באמצעות תהליכים קוגניטיביים בסיסיים. תנאים אלה עלולים לא להתקיים בפעולות של שיבוש באמצעות הסייבר, המהוות חלק ניכר מן האינטראקציות הקיימות במרחב זה. במקרים כאלה, סביבת האי־ודאות מפנה את מקומה לסביבה של סיכון, וזאת בשל ההשפעות המתועדות היטב של הכלים והטקטיקות הנמצאים בשימוש באותם מקרים. האמור לעיל מאפשר, אפוא, שימוש באסטרטגיות נורמטיביות המסוגלות לנצל טוב יותר את המידע הזמין.

שלישית, אין להניח שהחלטות המתקבלות בזמנים של משבר נובעות ממחשבותיו של אדם אחד בלבד. מה שתורם לאיכותן של ההחלטות המתקבלות הם סוגי דינמיקה הייחודיים לאותו ארגון. יתר על כן, גורמים נוספים, כגון עלויות הקהל (שבהם אין מאמר זה עוסק), עשויים להיות משמעותיים במה שנוגע לאופן התגובה הננקטת אל מול ניסיונות כפייה. מן הראוי לציין גם גורמים אלה לנוכח חשיבות הנושאים המשפיעים על אינטראקציות שונות במרחב הסייבר.

תחום ביטחון הסייבר נמצא עדיין בחיתוליו. אולם, נוכח האיומים המתפתחים, הן במורכבותם והן בהיקפם, קיימת דחיפות שאנשי אקדמיה ופוליטיקאים כאחד יבינו את התנהלותה של מדינה בתגובה לאירועים המתרחשים במרחב הסייבר. המאמר בא לתרום למאמץ זה על ידי כך שהוא מציע דרך לניתוח הדברים, אף שדרך זו נשקלה אך לעיתים רחוקות על ידי העוסקים בתחום הסייבר, אלה שהבנתם עשויה לסייע בשמירה על יציבותו של תחום וירטואלי זה.

פיתוח יכולות ארגוניות לניהול משברי סייבר

גבי סיבוני והדס קליין

מספר גדל והולך של אירועים בתחום ביטחון הסייבר ומורכבותם הביא ארגונים רבים לפתח נהלים ויכולות לטיפול בתקריות סייבר. אלה מתבשאים ביכולות לתגובה מיידית לאירועים, ביכולות טכנולוגיות ובהקמת צוותים לתחזוקת מערכות המידע בארגון. יכולות אלו עשויות להיות בלתי מספקות, שכן לעיתים הן חסרות התייחסות להיבטים ניהוליים, לכישורים ולכלים הנדרשים מהצוות הטכנולוגי לניהול המשברים במהלך ההתמודדות עם תקרית סייבר. מצב זה עלול לגרום להידרדרות מהירה וחסרת שליטה של המצב ולהפוך למשבר חמור בעל היבטים פיננסיים, משפטיים ותדמיתיים, המשפיע על נכסי הארגון כולו. מאמר זה יבחן את הדרכים לפיתוח יכולות ארגוניות שיאפשרו להתמודד ביעילות עם משברים במערכות המידע, התקשוב והסייבר.

מילות מפתח: סייבר, משבר סייבר, ביטחון סייבר, התאוששות, ניהול משברים, המשכיות עסקית

מבוא

במאי 2017 התרחש משבר חמור בחברת התעופה British Airways. לדברי החברה, כֶּשל בחוות שרתים, שנגרם מנחשול חשמלי שנבע מפעולת כיבוי והדלקה של המערכת, השבית את יכולת החברה להפעיל את טיסותיה במשך שעות ארוכות. כתוצאה מכך התבטלו טיסות רבות ולמעלה מ־75,000 נוסעים לא יכלו להגיע ליעדיהם. הנזק לחברה התעצם כתוצאה מהקושי של הגורמים המקצועיים להבין את מהות התקלה ולטפל בה באופן שימזער את הנזק הן לחברה והן לנוסעים.[1] כתוצאה מכך, הנזק לחברה בכסף ובמוניטין היה ועודנו עצום. אירוע זה היווה

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

1 Nicola Harley, "British Airways IT Crisis Mystery as Energy Suppliers Say there Was No Power Surge", *The Guardian*, May 31, 2017.

תזכורת עד כמה חיוני להקים ולתרגל מערך ניהול משברים בחברות הנשענות על תשתיות מחשוב לצורך פעולתן.

מרבית המנהלים מבינים כיום כי אירוע סייבר הינו בלתי נמנע. אין זה משנה עד כמה מקצועי יהיה צוות ההגנה של הארגון, סביר להניח כי במוקדם או במאוחר יימצא הארגון תחת מתקפת סייבר ויחווה ניסיונות פריצה או פגיעה בתפקוד מערכות המחשוב שלו. אשר על כן, חברות וארגונים משקיעים כיום רבות ביכולות הגנה פרו־אקטיביות שמטרתן היא לאתר מתקפות בשלבים המוקדמים ביותר, עוד בטרם הצליח אירוע הסייבר להתממש ולגרום נזק של ממש. במסגרת זו משקיעים ארגונים גם בגישות ובכלים חדשים, כגון: מודיעין סייבר, ניטור רציף של רשתות וכלים לזיהוי התנהגות אנומלית. יחד עם זאת, ועל אף אמצעי ההגנה, על ארגונים להמשיך לוודא שיש ביכולתם להתמודד עם משברים שמקורם באירועי סייבר חמורים.

בשנים האחרונות התרחשו בקרב מגזרים שונים מספר משברי סייבר שהתפתחו לממדים משמעותיים, לעיתים עקב כשלים בניהולם. משברי סייבר מסוג זה עשויים לגרום לפגיעה באמון הלקוחות, בהכנסות החברה, במוניטין שלה ועוד. משברי סייבר מאיימים לעיתים גם על מנהלים באופן אישי ועשויים לגרום להם לאבד את תפקידם.

דוגמה לכשלים בניהול משבר סייבר בשל היערכות לא נאותה ניתן לראות במשבר אותו חוותה ספקית התקשורת הבריטית TalkTalk באוקטובר 2015. אופן ניהול המשבר שאיתו התמודדה החברה מעיד כי היא פעלה באופן מבולבל, עמום ולא עקבי, דבר המוביל למסקנה כי לא הייתה לה תוכנית ניהול משברים ברורה.[2] יומיים לאחר היוודע דבר התקיפה, החברה לא הצליחה לבודד את הנזק, לאמוד אותו ולזהות את התוקף וגם לא את הסיבה לתקיפה. על פי הערכות, הנזק לחברת TalkTalk כתוצאה ממשבר זה עמד על שישים מיליון ליש"ט וכָלל הן נזקים ישירים והן נזקים עקיפים, שהתבטאו בפגיעה במוניטין, באיבוד לקוחות ועוד. כשנה וחצי לאחר האירוע, ולאור בדיקת הרגולטור הבריטי, פוטרה מנכ"לית החברה. מדוח הרגולטור עולה בבירור כי המנכ"לית הייתה אחראית לחוסר המוכנות של החברה להתמודד עם משבר סייבר.

להבדיל מהמקרה של חברת TalkTalk, חברת התשתיות האמריקאית DYN, שחוותה באוקטובר 2016 מתקפת מניעת שירות מהחמורות שנראו עד היום, הצליחה בתוך שעות ספורות להדוף את המתקפה ולמנוע את הסלמתה למצב משברי. עובדי החברה העידו כי הם מתאמנים ומתכוננים לתרחישים מסוג זה על

2 Lucas Fettes, "What Lessons Can All Organizations Learn from the TalkTalk Security Breach?", November 12, 2015, http://www.lucasfettes.co.uk/what-lessons-can-all-/organisations-learn-from-the-talktalk-security-breach.

בסיס קבוע, וכי התרגול אינו ממוקד אך ורק בהיבטים טכנולוגיים, אלה כולל גם תהליכי הערכת מצב, קבלת החלטות תחת לחץ ותקשורת עם הדרג הניהולי.[3]

בניית יכולת ארגונית להתמודדות עם משבר מחשוב וסייבר ראוי שתהיה רכיב חיוני בבנייה הכוללת של יכולות ההגנה וההמשכיות העסקית של כל ארגון. מאמר זה מנתח את הרקע התיאורטי של ניהול משברים ומציע לבחון פיתוח של ארבעה רכיבי יסוד שיאפשרו לארגון להתמודד בהצלחה עם משברי מחשוב וסייבר: פיתוח תפיסה ארגונית להתמודדות עם משבר מחשוב וסייבר; פיתוח כוח האדם וארגונו במסגרת צוות ניהול משברים; רכישה או פיתוח של כלים טכנולוגיים ותהליכים ארגוניים שיוכלו לסייע למימוש התפיסה הארגונית; בניית תוכנית הטמעה, הכוללת אימונים, תרגילים וסימולציות.

קלאוזביץ כתב בשעתו כי "המלחמה היא ממלכת אי־הוודאות".[4] כלל זה נכון גם למשברים במרחב הסייבר, שכן אי־הבהירות, הערפל השורר במהלכם והקושי לגבש תמונת מצב מקשים על קבלת החלטות ועל ביצוע הפעולות שיביאו לפתרון המשבר ולהתאוששות מהירה ממנו. פיתוח יכולות כאלו יביא בהכרח להתמודדות טובה יותר עם המשבר, לניהולו בצורה טובה יותר, ומכאן גם לתוצאות טובות יותר עבור הארגון.

רקע תיאורטי – אסטרטגיה של ניהול משברים

בתחום הסייבר, כמו בתחומים אחרים, יש חוסר אחידות באשר למושג "משבר" ולאופן השימוש בו. לעיתים קרובות נעשה שימוש נרחב מדי במושג זה. ככלל, לא כל אירועי הסייבר בארגון מובילים בהכרח למשבר תפקודי המחייב התייחסות מיוחדת. רוב אירועי הסייבר מטופלים באמצעות תהליכי שגרה, כגון טיפול בהדבקה של נוזקות, התמודדות עם מתקפות מניעת שירות קלות וכדומה. בדרך כלל, אירועים אלה אינם פוגעים בארגון בטווח הבינוני והארוך, וההתמודדות איתם הינה לחם חוקם של צוותי ביטחון הסייבר או אבטחת המידע. אולם, יש ואירועי סייבר חמורים יגרמו לפגיעה מתמשכת ביכולת הארגון לתפקד ולספק שירות ללקוחותיו. במצב כזה מדובר באירוע משברי המחייב התמודדות מיוחדת.

אולגה קוליקובה ועמיתיה[5] מנתחים את משמעות חשיפתו של משבר סייבר בארגון וטוענים שלחשיפה כזאת יש ארבעה היבטים משמעותיים: הראשון נוגע

---

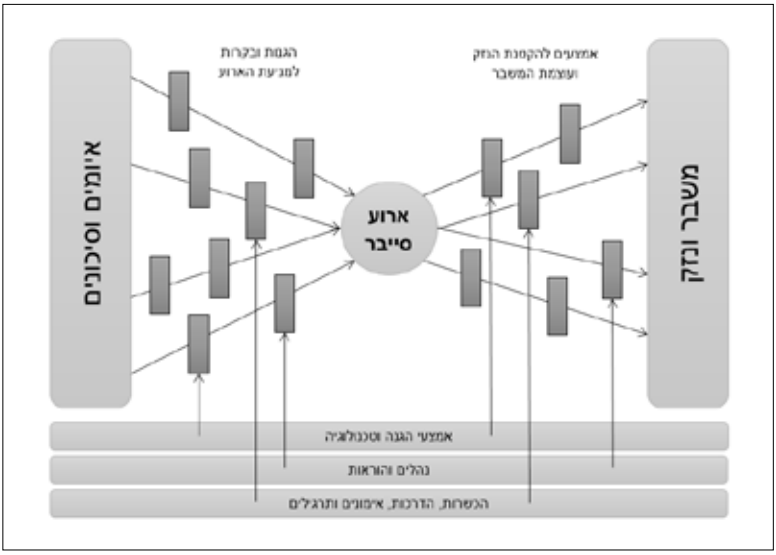
3 Christopher Roach, "Lessons Learned from the Dyn Attack", *CFO.com*, February 9, 2017, http://ww2.cfo.com/cyber-security-technology/2017/02/lessons-learned-dyn-attack.

4 רוג'ר אשלי לאונרד, **על המלחמה – מדריך קצר לקלאוזביץ**, משרד הביטחון־ההוצאה לאור, תל אביב, 1977, עמ' 79.

5 Olga Kulikova, Ronald Heil, Jan van den Berg, Wolter Pieters, "Cyber Crisis Management: A Decision-Support Framework for Disclosing Security Incident

לשיפור ההגנה ושיפור היכולת לבנות תמונת מצב; השני נוגע לעובדה שהחשיפה תאפשר לשפר את העמידה ברגולציות ובתקנים; השלישי נוגע לאפשרות שהחשיפה עשויה לפגוע בחוסן הכספי של הארגון; הרביעי נוגע למוניטין של הארגון העשויים להיפגע כתוצאה מהמשבר, דבר שמצידו עלול להקרין על התוצאות העסקיות של אותו ארגון.

אחד המודלים המנתחים את תהליך ההתמודדות עם אירוע משברי הינו מודל "עניבת הפרפר" (Bow-tie) שפותח כבר בשנת 1979.[6] מודל זה מציב את האירוע במרכז ומאפיין את ההגנות והבקרות שנועדו למנוע אותו, וכן את האמצעים שיש לנקוט להקטנת הנזק כאשר האירוע התרחש. התרשים שלהלן ממחיש את המודל בהקשר לאירוע סייבר:



תהליך ההתמודדות עם אירוע משברי מחייב בניית יכולות לגיבוש תמונת מצב מתמשכת במהלך המשבר. זהו תהליך המחייב מעקב קבוע אחר הפרמטרים המתפתחים של המשבר. "תמונת מצב" הינה ביטוי בו משתמשים בעת ניהול משבר בכדי לתאר את ההערכה הטובה ביותר למתרחש ברגע נתון, מה עשויות להיות ההשפעות של התרחשות זו, מידת חוסר הוודאות בהערכה, מידת יכולת ההכלה

Information", *IEEE, Computer Society, 2012 International Conference on Cyber Security*, pp. 103-112.

6 Steve Lewis and Kris Smith, "Lessons Learned from Real World Application of the Bow-tie Method, Prepared for Presentation at American Institute of Chemical Engineers", *6th Global Congress on Process Safety*, San Antonio, Texas, March 22-24, 2010.

של המשבר, כיצד הוא עשוי להתפתח ולהחמיר ומה עשוי להתרחש בהמשך. עוד מתארת תמונת המצב את ההגנות הפעילות והזמינות לארגון אל מול האיומים. תמונת המצב משמשת כבסיס להערכת המצב לצורך קבלת החלטות אופרטיביות ותעדוף האירועים והטיפול בהם, וזאת בהתחשב ברמת הסיכון ובפוטנציאל הנזק הגלום בהם.

החשיבות של תהליך בנייתה של תמונת המצב מתוארת במאמר של עלי רשידי ועמיתיו.[7] המאמר מנתח תהליך זה במהלך אירוע סייבר כמרכיב קריטי ביכולת לקבל החלטות מושכלות. מחברי המאמר מציעים מודל להיתוך מידע כדי לאפשר תהליך רציף של התעדכנות, תוך התבססות על מערכות מומחה.

מאמרם של בארפורד ועמיתיו מנתח את השלבים של תהליך בנייתה של תמונת המצב.[8] בשלב הראשון נדרשת הבנה של מה שקורה באותו רגע. שלב זה מותנע לאחר שמתקיים תהליך ראשוני של מיון ההתרעות שמתקבלות וניתוח הנתונים הקיימים. התהליך נמשך במטרה להבין את משמעות האירוע ואת מידת השפעתו על התהליכים הקריטיים בארגון. בשלב הבא מציעים הכותבים לגבש הבנה באשר לתהליך התפתחותו של האירוע, ולבסוף לגבש הבנה באשר לשאלה כיצד הוא התרחש. כל אלה הינם שלבים מקדימים לתהליך הערכת המצב, שמטרתו היא לקבל החלטות לפעולה לצורך הכלת האירוע ומזעור הנזק שהוא גורם.

ממד הזמן יוצר מורכבות נוספת. פעמים רבות קיים קושי להגדיר את המעבר מאירוע סייבר בעל עצימות נמוכה, שכדי להתמודד איתו מופעלים בשגרה אנשי הצוות הטכנולוגי והאירוע כולו נשאר בגבולות אלה, לבין אירוע סייבר בעל עצימות גבוהה, שמתפתח למשבר בעל השלכות משמעותיות לארגון כולו ומצריך מעורבות של יכולות נוספות. ניתן לתאר את נקודת המעבר מאירוע סייבר שגרתי לאירוע סייבר משברי באופן הבא: בשלב ראשון נוצר פער סמוי בין אופן התפקוד של מערכות המחשוב ובין המצב הרצוי, כפי שהוא מוגדר ברמות השירות הארגוניות. הטיפול בשלב זה נעשה על ידי גורמי השגרה. במידה והאירוע מידרדר, הפער גדל, צובר תאוצה ועלול להתרחב לתחומים נוספים, נדרש טיפול רחב ועמוק יותר.

הוראה 361 של בנק ישראל מגדירה מספר שלבים בהתמודדות עם אירוע סייבר:[9] שלב הזיהוי (Detection), במהלכו מתבצע בירור ראשוני בדבר קיומו של אירוע סייבר; שלב הניתוח (Analysis), הנוגע לבירור מקיף ומעמיק ככול האפשר

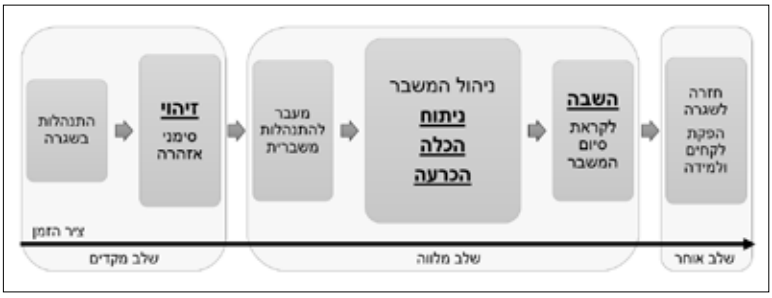
7 Ali J. Rashidi, Kourosh D. Ahmadi, Mostafa Heidarpour, "Cyber Situational Awareness Using Intelligent Information Fusion Engine (IIFE)", *Cumhuriyet University Faculty of Science, Science Journal (CSJ)*, Vol. 36, no. 3 (Special Issue), 2015.

8 P. Barford et al., "Cyber SA: Situational Awareness for Cyber Defense", *Cyber Situational Awareness* (Springer US, 2010).

9 המפקח על הבנקים, הוראה 361, ניהול בנקאי תקין [1] (3/15), **ניהול הגנת הסייבר**, מארס 2015.

לגבי אירוע הסייבר, וזאת לצורך קבלת החלטות בדבר כיווני פעולה אפשריים לבלימת התקיפה; שלב ההכלה (Containment), שנועד להשיג שליטה ראשונית באירוע לצורך הכלתו ועצירת החמרתו, עד להשלמת ההכלה; שלב ההכרעה (Eradication), שמטרתו נטרול האירוע כדי למזער ככול הניתן את הנזק שגרם; שלב ההשבה (Recovery), במהלכו חוזר הארגון לתקינות פעולה מלאה.

ניתן לאפיין את היכולות הנדרשות להתמודדות עם המשבר על פי שלביו הכרונולוגיים: הראשון הינו השלב המקדים בשגרה. בשלב זה על הארגון לקיים פעולות להפחתת ההיתכנות להתפתחות משבר ולהגברת המוכנות וההיערכות לניהולו. בספרו של סיימון בות', **אסטרטגיה של ניהול משברים**, הוא מונה מספר פרמטרים המקרינים על יכולת הארגון להתמודד עם משבר, אותם יש לפתח בשלבים המקדימים. הפרמטר הראשון הוא תכנון. בשלב המקדים נדרש הארגון להשקיע משאבים בתכנון ההתמודדות עם משבר.[10] משהוטל הארגון לתוך מציאות משברית, עוברים לשלב השני – השלב המלווה הכולל את ניהול המשבר בפועל – שם נדרש מגוון של יכולות שיסייעו לארגון בהתמודדות עם המשבר ובמזעור הנזק. השלב השלישי הוא שלב ההתאוששות לאחר האירוע, הכולל את תחקיר האירוע והפקת לקחים ממנו. הצגת שלבים אלה על ציר הזמן מומחשת בתרשים שלהלן:



פיתוח תפיסה לניהול משברים

אבן הדרך הראשונה הינה פיתוח תפיסה ארגונית לניהול משברים. תפיסה זו צריכה לכלול מספר מרכיבי יסוד: הראשון שבהם נוגע לקביעת מדדים לזמן השבתה נסבל ולרמות התפקוד הנדרשות לכול מערכת מחשוב בארגון. תהליך זה מחייב הסתמכות על ניתוח מערכות המחשוב והקריטיות שלהן לתפקודו הכולל של הארגון. ניתוח זה נקרא Business Impact Analysis (BIA), והינו רכיב בבניית תוכנית ההמשכיות העסקית. באמצעות כלי זה ניתן לנתח ולקבוע את ממדי

10 Simon A. Booth, *Crisis Management Strategy: Competition and Change in Modern Enterprises* (Routledge, Taylor and Francis Group, 1993), p. 13.

התפקוד של כל מערכת ואת הזמן הנדרש לה לחזרה לפעולה תקינה. קביעה כזאת מקרינה באופן מיידי על הקצאת המשאבים לצורך ניהול המשבר בארגון, שהרי לא דין ארגון שיכול להרשות לעצמו ניתוק מלקוחותיו למספר שעות, כדין בנק שהפסקת השירות המקוון שלו עלולה להסב נזק כספי ולפגוע במוניטין, או כדין חברת תעופה הנאלצת לבטל טיסות.

פיתוח התפיסה נדרש גם לצורך הגדרת מצבי משבר וליצירת שפה משותפת וכללים ברורים לניהולו. לקביעת מצבי המשבר וחומרתם יש השלכה מיידית על המשאבים אותם נדרש הארגון להקצות לצורך ניהול המשבר. משאבים אלה אמורים להתייחס להיקפו של צוות ניהול המשברים, למיומנויות הנדרשות ממנו, לאמצעים הטכנולוגיים והאחרים שיש להקצות לצורך הפעלתו, ולבסוף להיקף ההכשרות והאימונים של צוות זה. לאחר הגדרת מצבי המשבר נדרשת התפיסה לקבוע את תהליכי העבודה בארגון בשגרה, טרם המשבר, וכן במהלכו, ולבסוף לקבוע את תהליכי התחקור והלמידה בעקבותיו. התפיסה גם נדרשת לקבוע את אחריותם של בעלי התפקידים בארגון במצבי משבר.

פיתוח התפיסה והמורכבות של משברי סייבר ושל משברים ארגוניים בכלל מצריכים שיתוף גורמים רבים בארגון, בנוסף לצוותים המספקים מענה טכנולוגי לשירותי המחשוב ולאמצעי התקשורת. שיתוף זה דורש תיאום וניהול של מספר דיסציפלינות, ובהן ניהול ההשלכות המשפטיות הקשורות בתפעול והשגחה על מאגרי מידע, ניהול חבויות רגולטוריות הנכנסות לתוקף מרגע הכרזת המשבר, ניהול הפגיעה במוניטין, שיתוף הממונה על הסיכונים, עירוב גורמים הממונים על הגנת הסייבר בקרב רשויות האכיפה ועוד. לפיכך, חשוב לקבוע ועדת ניהול משברים ארגונית כחלק מההיערכות לניהול משבר סייבר, ולכלול בה את הצוות הניהולי הבכיר בארגון, כגון המנכ"ל, מנהל הכספים, היועץ המשפטי וגורם יחסי ציבור.

היתרונות הבולטים של שילוב מנהלים בכירים בוועדה לניהול משברי סייבר הם היכולת והסמכות לפעול בשני מישורים משלימים: בשגרה תפעל הוועדה לבחון היבטים רגולטוריים ומשפטיים בתרחישי משבר שונים ולהגדיר היבטים פיננסיים הקשורים בניהול משברים, תתקף את תוכניות ההסלמה במעלה מדרג הניהול ואת תוכניות המגירה לניהול ערוצי התקשורת והמדיה השונים בעת התרחשות משבר; בעת משבר תסייע הוועדה לאזן בין המתרחש בתוך הארגון ומחוץ לו ולשמור על המוניטין שלו, וכן תפעל להקטנת ההתחייבויות המשפטיות המתעוררות במהלך אותו משבר. כל זאת, תוך שמירה על אובייקטיביות ועל תהליכי תעדוף.

פיתוח כוח אדם וארגונו בצוות ניהול משברים

אחד היתרונות בהכשרת צוות פנים ארגוני לטיפול במשברים הינו היכולת של צוות כזה לנתח את מכלול האפשרויות ודרכי הפעולה באופן מיטבי. סביר להניח

כי אף גורם חיצוני, עתיר ניסיון ככול שיהיה, לא מכיר את הארגון כמו הצוותים המקצועיים, מנהלי התהליכים העסקיים והנהלת הארגון. זאת ועוד, חברי הצוות הפנים ארגוני הם, על פי רוב, בעלי סמכות מקצועית וזוכים להכרה ככאלה, דבר האמור להקל עליהם בעת ניהול האירוע.

כדי לנצל את המשאבים הפנימיים של הארגון ולממש את התפיסה הארגונית, יש צורך בהכשרת כוח אדם. תהליך בחירתם של בעלי התפקידים השונים מחייב הגדרה ברורה של מכלול התפקידים, של אחריות הצוות לניהול משברים ושל הממשקים שלו עם בעלי עניין בארגון ומחוצה לו. כמו כן, יש להגדיר את הכישורים הנדרשים מבעלי מקצוע אלה.

הדרישות מכול בעל תפקיד במהלך משבר צריכות לכלול קביעה של תחומי האחריות, ניתוח מערכת הכישורים הנדרשת והגדרה של הידע והניסיון הדרושים. בשלב הבא יש להגדיר את המיומנויות והכישורים הניהוליים הנדרשים מחבר הצוות כדי שיוכל למלא את תפקידו. הגדרה זאת צריכה לענות על השאלה "איזה מיומנויות וכישורים נדרשים כדי לנהל את המשבר באופן יעיל, ומה צריך חבר הצוות כדי לפעול ביעילות?". בשלב השלישי יש להגדיר את הידע והניסיון שצריכים להיות מצויים אצל כל חבר בצוות ניהול המשברים. כל אחד מאלה צריך להכיר היטב את הסביבה העסקית ולא רק את הסביבה הטכנולוגית, ולכן חייב להיות בעל היכרות עם הפעילות העסקית של הארגון, לפחות ברמה של הבנה בסיסית. הבנה כזאת תספק לו את היכולת לתעדף את אופן הטיפול במשבר על בסיס הבנת הקריטיות של התהליכים העסקיים שנפגעו.

הצוות הטכנולוגי של הארגון נדרש להתמודד עם מגוון אתגרים בעת משבר סייבר, בהם: גיבוש תמונת מצב, בדרך כלל על בסיס מידע חלקי, וגיבוש המענה המיטבי במטרה להתאושש במהירות ולשוב לתפקוד סביר. במקרים בהם המשבר מלווה בלחץ ציבורי נרחב, נדרשים מנהלי הארגון לתת תשובות לציבור הלקוחות ולבעלי עניין אחרים, דבר שמגדיל עוד יותר את תחושת הלחץ בה נתונים הגורמים המקצועיים.

הצוות הטכני לניהול משברים הוא הגוף הממונה על ניהול המשבר בארגון בהיבטים הטכנולוגיים והוא זה שמנחה את הגורמים המקצועיים כיצד לטפל בו באופן שיצמצם את הנזק והפגיעה במוניטין של הארגון. השאיפה היא שהצוות הטכני גם יצליח למנף את המשבר לטובת הארגון. תפקידיו של צוות זה כוללים גם היבטים של הערכה ראשונית של הנזק, תקשור המצב הקיים והשלכותיו העסקיות, גיבוש תוכנית פעולה למנהלי התהליכים העסקיים ולהנהלה, הכרזה על מצב חירום וניהול האירוע. אלו הן משימות מורכבות שאינן מסתכמות בהיבטים טכנולוגיים ובהבנה והיכרות של מערכות המחשוב והתקשורת הקיימות בארגון, אלא מצריכות גם הבנה עסקית, משפטית ותקשורתית רחבה.

צוות ניהול המשברים נמצא בעת משבר תחת לחץ רב שעשוי להקשות על תפקודו. תחושת הלחץ גוברת ככול שגדֵל הפער בין האמצעים והכישורים הדרושים לצורך התמודדות עם המשבר ובין היכולת והמשאבים העומדים בפועל לרשות הצוות. ניתן לאפיין שני סוגים של כישורים הנדרשים לצוות: כישורים מקצועיים/טכנולוגיים שעניינם התמצאות עמוקה במערכות הטכנולוגיות והניהוליות של הארגון; כישורים רכים שעניינם פיתוח יכולות אישיות וקבוצתיות המסייעות בתהליך ניהול המשבר.

פיתוח הכישורים המקצועיים/טכנולוגיים הינו תהליך המחייב הכשרה והתמקצעות במגוון המערכות הטכנולוגיות של הארגון, ובכלל זה מערך התשתיות והתקשורת, שרתי הנתונים ויישומי הקצה של הארגון. זאת, לצד הבנה עמוקה במערך הניהולי, ובכלל זה בתהליכי קבלת ההחלטות, במערך הסמכויות ובמקורות הידע בארגון, ובנוסף לכך הבנה של כלל המערכות והתהליכים הקריטיים בארגון ברמה שתאפשר ניתוח אירוע ומיפוי הגורמים הרלוונטיים לטיפול בו. כדי לשפר את ההבנה העסקית/ארגונית של צוות ניהול המשברים, מומלץ לקיים מפגשים קצרים עם מנהלי התהליכים העסקיים הקריטיים בארגון ולחשוף את צוות ניהול המשברים למורכבות, לחשיבות ולאתגרים הקשורים באותם תהליכים.

ראש צוות ניהול המשברים צריך להימנות על הדרג הניהולי וחשוב שיהיה בעל היכרות עמוקה עם ההיבטים הטכנולוגיים והשלכותיהם על התהליכים העסקיים. הייס ואומודיי קובעים כי מה שנחוץ לראש צוות ניהול המשברים הוא שילוב של תכונות אישיות ותכונות בין־אישיות. מדובר בתכונות של סובלנות ללחץ, במודעות עצמית ובמודעות כלפי כל אחד מחברי הצוות, וכן במיומנויות תקשורת טובות.[11]

צוות ניהול המשברים צריך לכלול חבר צוות שיהיה ממונה על היבטים הקשורים בתיאום המשבר בין היחידות העסקיות. על חבר צוות זה להיות בעל היכרות טובה עם מבנה הארגון ועם היבטים מינהליים הקשורים בתפקודו. הצוות אמור לכלול גם אנשי טכנולוגיה בעלי ידע מצטבר בתחומי התשתיות, התקשורת, השרתים, היישומים ובסיסי הנתונים. במקרים בהם המשבר חולש על מספר אתרים של הארגון, יש חשיבות להצבת נציגים של צוות ניהול המשברים בכול אתר, והתיאום העליון צריך להתבצע באופן מרוכז.

המאפיינים האישיים של אנשי הצוות לניהול משברים צריכים לכלול, כאמור, גם כישורים רכים, ובהם מיומנויות ותכונות כמו תקשורת בין־אישית, יכולת הקשבה, אינטליגנציה רגשית, כושר שכנוע, יצירתיות, קפדנות, יכולת לפתרון בעיות, יכולת

11 P. A. Hays & M. M. Omodei, "Managing Emergencies: Key Competencies for Incident Management Teams", *The Australian and New Zealand Journal of Organizational Psychology*, February 2012.

לעבודה בצוות, יכולת לקבל החלטות תחת לחץ ועוד. תכונות אלו ניתנות לפיתוח ולשיפור, כשהמטרה היא להביאן לידי ביטוי במסגרת ניהול המשבר.

שכנולוגיה

כלים רבים מסייעים בתהליך ניהול האירועים. במסגרת התפיסה הארגונית יש להחליט האם לעשות שימוש בכלי מדף או לייצר כלי ייעודי, הכול בהתאם לצרכים הייחודיים של הארגון.

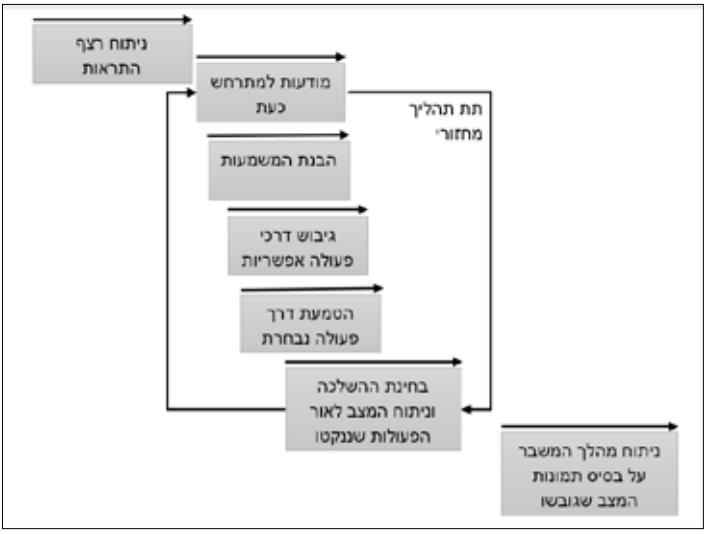
לכלים הטכנולוגיים יש חשיבות רבה בתמיכה בתהליך ניהול המשברים בארגון. כלים אלה נדרשים לתת מענה למגוון השלבים בתהליך, בכללם תהליכי גיבוש תמונת המצב וביצוע הערכת המצב, ולספק מערכת תומכת לניהול משברים, כולל יכולת שימור ואחזור מידע ממאגרי ידע מאירועים קודמים בארגון עצמו ובארגונים אחרים, וכן יכולות תיעוד לצורכי למידה. המערכת לניהול משברים מאפשרת מעקב ממוכן אחר הנהלים והתהליכים השונים ומדגישה את סדרי העדיפויות בניהול האירוע באמצעות תרחישים המוזנים מראש ומתבססים על תהליכים עסקיים קריטיים. היא גם מעצימה את התקשורת הפנים־צוותית והפנים־ארגונית.

ככלל, הכלי לניהול המשבר נועד לתת מענה למספר צורכי יסוד:

- ליצור יומן מבצעי שיהיה מאורגן באופן טבלאי ויפרט את מהלך ההתרחשויות והאירועים. שימוש ביומן מבצעי מאפשר לתעד את האירוע מהרגע הראשון ולשקף את המתרחש במהלכו. מטרתו היא לאפשר גיבושה של תמונת מצב, לתמוך בתהליכי קבלת החלטות ולתחקר את המשבר עם סיומו. יומן כזה צריך לכלול מועדי התרחשויות מדויקים, תיאור עדויות, עובדות והנחות עבודה.
- להוות פלטפורמה לתקשורת בין אנשי המפתח בארגון ובין בעלי העניין בעת האירוע. לעיתים נדירות בלבד נמצאים אנשי המפתח בו־זמנית בחדר ניהול המשבר, ועל כן נדרש לספק להם כלי שמאפשר תקשורת והבנת תמונת המצב מכול מקום ובכול עת.
- ליצור מרחב וירטואלי מרכזי אחד, בו יהיה מרוכז כל המידע על ההתרחשויות. יצירת מרחב כזה נועדה להבטיח שהצוותים הטכנולוגיים ומקבלי ההחלטות פועלים על בסיס אותן עובדות.
- לסייע בהבנת תמונת המצב בעזרת טווח הפרשנויות השונות של סיבה ותוצאה המאפיינות את עולם מערכות המידע, וזאת תוך התמודדות עם כמות ההתרחשויות ועם קצב האירועים המהיר.
- לסייע בהפחתת הלחץ לצורך קבלת החלטות אובייקטיביות והפעלה מובנית של תהליכי העברת הטיפול לדרג ניהולי גבוה יותר.

- לתמוך בתקשורת על פי מטריצת התקשורת וההסלמה הארגונית. מערכות לניהול משברים מאפשרות להזין מראש את מטריצת התקשורת ושולחות באופן אוטומטי עדכונים בעת התממשות התנאים שהוגדרו במערכת מראש.
- לסייע בהבנת משמעות האירועים, כך שפיסות המידע שנאספו ממקורות שונים יצורפו לכדי תמונה שלמה. זאת, תוך הערכת איכות המידע, הפרדה בין עיקר לטפל וארגון המידע בדרך שתאפשר לשלוף אותו בקלות בהמשך.
- לתמוך בתהליך הניסוח של דרכי פעולה אפשריות על בסיס הנתונים הידועים ותוך פירוש העובדות הרלוונטיות וניתוחן, וזאת כדי להבין כיצד המצב עשוי להתפתח.
- לבחון את ניתוח המצב ואת השלכותיו לאור הפעולות שננקטו. בשלב זה מתחיל מסלול חדש של גיבוש תמונת מצב והערכת מצב, המבוססות על השינויים שהתרחשו כתוצאה מהפעולות שננקטו ועל נתונים חדשים שהגיעו מבחוץ.

שימוש בכלים טכנולוגיים שיוכלו לסייע בתהליכים שתוארו לעיל יאפשר הגברה משמעותית של היעילות בעבודת הצוות לניהול המשברים. התרשים שלהלן מציג באופן סכמתי את התהליך אותו המערכות הטכנולוגיות נדרשות לתמוך:



משפחה נוספת של כלים טכנולוגיים נוגעת ללמידה מתוך אירועים קודמים בארגון ומחוצה לו. במהלך משבר אין מצפים מצוות ניהול המשברים לבצע ניתוחים שורשיים בכדי לזהות מדוע אירעה התקרית. ניתוח כזה צריך וחשוב שייעשה בתהליך התחקור אחרי האירוע, כחלק מהסקת המסקנות והלמידה הארגונית. ההתמקדות במהלך ניהול המשבר צריכה להיות בלימת אירוע הסייבר וסיכולו

ובהשבה מהירה של המערכות הארגוניות לתפקודן מלפני המשבר, תוך קביעת סדר עדיפויות. לפעמים נדרש פתרון זמני, או שימוש באמצעים שעוקפים את הבעיה, עד לפתרונה המלא.

כלי חשוב באבחון אירוע משברי הוא מסד הנתונים של האירועים והמשברים ההיסטוריים בארגון, אינדקס דומה המתאר את האירועים שהתרחשו במגזר העסקי אליו משתייך הארגון ברמת פירוט מרבית ככול הניתן, וכן אירועים שהתרחשו בסביבה הגיאופוליטית אליה משתייך אותו ארגון. למשל, ראוי שבנק ינהל רישום של אירועי סייבר חריפים שהתרחשו בבנקים אחרים ברחבי העולם. כלי כזה יאפשר לצוות ניהול המשברים בבנק לזהות בעיות או טעויות מוכרות שגרמו לאירועים דומים בעבר, ובכך לקבל מידע על דרכים לעקיפת הבעיות כשאלו זוהו. מדובר בכלי ממוכן ומובנה שצריך לכלול מנוע חכם לאחזור נתונים, כולל נתונים שנכתבו בפורמט של טקסט חופשי.

כלי ניהול המשברים גם נדרשים לתעד את המשבר ואת תהליכי העבודה במהלכו, וזאת כדי להזין את מערכת הלמידה הארגונית ולאפשר שימוש בה הן תוך כדי המשבר והן במשברים עתידיים. תיעוד המשבר חשוב שיכלול את השתלשלות העניינים, תיאור של ההתרעות שהתקבלו ואופן הדיווח עליהן, וכן ההחלטות שהתקבלו בכול שלב. לדבר זה יש חשיבות בכמה מישורים: למקרה ותרחיש דומה יתפתח בעתיד או למקרה בו, למרות הצעדים שננקטו ובכללם גיבוש תמונת המצב והערכת המצב, המשבר טרם הסתיים למעשה. בנוסף לכך, יש להקפיד על הכנת דוח מסכם שיופץ לבעלי העניין מבית, ובהם ההנהלה וגורמים נוספים בהתאם לעניין, וכן לבעלי עניין חיצוניים, על פי הנחיות הרגולציה המתאימות.

השמעה – הכשרה, אימונים ותרגילים

שיפור היכולות והשגת רמת מוכנות גבוהה מבוססים במידה רבה על אימונים, תרגילים והכשרות, כחלק מובנה בתהליך מימושה של התפיסה הארגונית. ניתן לאפיין מספר רכיבים בתהליך ההטמעה.

צוות ניהול המשברים כולל, בדרך כלל, עובדים בעלי הכשרה וידע עמוקים בתחום מערכות המחשוב ומרחב הסייבר הארגוני, שתפקידם בצוות בא בנוסף לתפקידם השגרתי. למרות זאת, כל מועמד לצוות ניהול המשברים צריך, טרם הפיכתו לחבר בו, לעבור הכשרת "שער כניסה", כלומר הכשרה בסיסית וראשונית. הכשרה זו צריכה לכלול את הכללים והעקרונות של הארגון לניהול משברים, את התוכניות והנהלים הארגוניים למצב כזה, הבנת הסביבה העסקית והיכרות עם כלים טכנולוגיים לניהול משברים. על ההכשרה גם לכלול היבטים של זיהוי, תיעוד, סיווג ותעדוף, אבחון (דיאגנוסטיקה) ראשוני של המשבר, חקירת התפתחותו, אמצעי התקשורת וההסלמה (העברת דרג הטיפול לרמה בכירה יותר), מקורות

המידע והאיסוף הקיימים בידי הארגון, ולבסוף אופן סגירת האירוע, תחקורו והפקת לקחים ממנו.

לצד ההכשרה הבסיסית, יש לקיים על דרך השגרה תרגילים, בכלל זה "תרגילי שולחן" (Tabletop Exercises) ואימונים לצוות בתנאים הקרובים ככול הניתן לתנאי אמת, וכן תרגילים רחבי היקף שישלבו גם את הרמה הניהולית בארגון. מטרתם של "תרגילי שולחן" היא לנתח תרחישי ייחוס רלוונטיים באופן שיאפשר למשתתפים בהם לבחון את התרחישים ללא הלחץ של סביבת העבודה. תרגילים כאלה מוסיפים באופן משמעותי לרמת הידע, מרחיבים את השפה המשותפת ומגבירים את רמת שיתוף הפעולה בין חברי צוות ניהול המשברים. במסגרת זו ניתן לעודד תהליכי חשיבה צוותיים, למקד את חברי הצוות בהתמודדות עם מגוון תרחישים ולשלוט על כיווני התפתחותם. זאת, תוך העמקת ממשקי התקשורת והאינטראקציה הפנימיים והחיצוניים עם בעלי עניין ושיפור ההבנה ההדדית באשר לסמכותם ואחריותם של חברי הצוות. תרגילים כאלה גם מאפשרים לתקף את המדיניות והנהלים של הארגון.[12] רצוי שהם יכללו הנחיה מקצועית[13] במטרה לסייע בהגברת רמת המוטיבציה של אנשי הצוות ובנכונותם להשתתף באירוע ולאפשר להם להתמודד איתו בהצלחה.[14] סט התרגילים מאפשר להוציא את צוות ניהול המשברים מחשיבה בתבניות כושלות, כגון חשיבה במושגים של הסתרה וטשטוש וניסיון לתת פתרון מיידי כדי לבצע "כיבוי שריפה".

לצד "תרגילי שולחן", יש לקיים אימונים ותרגילים רחבי היקף המדמים ככול האפשר את המציאות. ניתן לאפיין מספר עקרונות אותם יש לממש בתרגילים אלה:

- **אופי התרחישים** – גיבוש תרחישים הנוגעים לתקלות במערכות החיוניות של הארגון, תוך התבססות על ניתוח תוכנית ההמשכיות העסקית ועל ניתוח המערכות הקריטיות של הארגון (BIA). פעולה זו תבטיח התמודדות עם הליבה המבצעית של מרחב הסייבר הארגוני. מומלץ שתרחישי התרגילים ורמת מורכבותם ינוסחו באופן ספיראלי, כך שצוות ניהול המשברים ייחשף לתרחישים בעלי רמת מורכבות הולכת וגוברת.
- **סביבה טכנולוגית לתרגיל** – בניית סביבה טכנולוגית תרגילית שתאפשר דימוי קרוב ככול הניתן של המציאות. זאת, תוך מזעור השפעתו של התרגיל על התפקוד המבצעי של הארגון. הסביבה הטכנולוגית התרגילית צריכה לאפשר

12 Brent D. Ruben, "Simulations, Games and Experience-Based Learning", *Simulation & Gaming*, Vol. 30, 1999.

13 "Intrinsic Motivation, Extrinsic Rewards and Divergent Views of Reality", Book Review, *Educational Psychology Review*, Vol. 15, no. 3, September 2003.

14 A. J. Faria and W. J. Wellington, "A Survey of Simulation Game Users, Former Users and Never Users", *Simulation & Gaming*, June 2004.

תקשורת, הזרמת אירועים והקמת סביבת חיישנים למערכות המחשוב והתשתיות הטכנולוגיות.

- **בניית התרחיש** – התרגיל צריך להיבנות על בסיס האירועים המגיעים לצוות ניהול המשברים מהמערכות התפעוליות והמבצעיות וממפעיליהן. צוות ניהול המשברים יידרש לנסות לזהות את מקור התקלות מתוך בחינת האירועים והחיישנים הטכנולוגיים העומדים לרשותו (לדוגמה, עומס על משאבי מחשוב, תקלה בהעתקת נתונים ובקבצי לוג וכיוצא באלה). התרחיש נדרש לכלול את סיפור הרקע ואירועים המוזרמים במהלך האימון, שחלקם יהיו הזרמות "רעש" שאינן נוגעות ישירות לתקלות.
- **התאמות במהלך התרגיל** – צוות ניהול המשברים והמערכת הניהולית התומכת נדרשים לזהות את מקור הבעיה במערכות המחשוב ואת מהותו של אירוע הסייבר בו הם אמורים לטפל. לצורך זה יש להכין בנק אירועים שיוזרם בהתאם להתפתחות הטיפול בתרחיש, וזאת במטרה למצות את התרגיל ולאמן את כלל המעורבים באופן מיטבי.
- **בקרה וחניכה** – חיוני לקיים מערך בקרה צמוד לתרגילים. מערך זה יוכל להבחין במהלך התרגילים בחוזקות ובחולשות של כל חבר צוות ושל הצוות כמכלול, ובכך למקד את הלמידה ואת הפיתוח האישי והקבוצתי. במהלך התרגיל חשוב לכייל את היכולות הבסיסיות הקיימות ולהשתמש בנתונים שייאספו לצורך קביעת מדדי השיפור הנדרשים ולבחינת מידת ההצלחה של התרגילים הבאים. תוצאות התרגיל יאפשרו למקד את תוכנית ההשתלמויות והאימונים לחברי הצוות.

לצד אימון הצוות הטכנולוגי וכחלק מתהליכי האימון להתמודדות עם משבר, יש חשיבות לערוך אימון גם לרמה הניהולית בארגון. אימון כזה חשוב לצורך בניית שפה משותפת, להבנת האילוצים בכול הקשור לשיתוף בעלי עניין מחוץ לארגון במהלך משבר, וכן כדי לתת לצוות הטכנולוגי את השקט והמרחב הדרושים לטיפול במשבר ללא לחץ ניהולי. לחץ כזה לא רק שאינו תורם, אלא שברוב המקרים אף מפריע.

סיכום

ריבוי תקריות סייבר ומשברי סייבר הגביר מאוד את הצורך לפתח יכולות ארגוניות להתמודדות עם משברים כאלה. ניהול נכון של משבר סייבר יכול לצמצם נזקים ולהוביל את הארגון להתאוששות מהירה, ואילו כישלון בהתמודדות עם משבר כזה עלול להוביל לקריסת הארגון.

ניהול אירוע סייבר הינו משימה ארגונית הכוללת פונקציות רבות בארגון, החל מאנשי הסייבר ואבטחת המידע וכלה בחברי ההנהלה והדירקטוריון. לניהול האירוע יש השפעה שאינה נופלת מהשפעתן של היכולות הטכניות להתמודד איתו. יש

חשיבות מכרעת להכללת מדיניות לניהול משברי סייבר באסטרטגיית הסייבר הארגונית. על מדיניות זו לשקף את צורכי הארגון ויעדיו.

יכולת הארגון להתמודד עם משבר תלויה במידה רבה גם ביכולות האלתור והעמידה שלו בלחצים. נהוג ליחס יכולות כאלו לתרבות הניהול הישראלית, אולם אין בהן די במציאות המורכבת של משברי סייבר ובמצב הכאוטי שהם עלולים לגרום – מצבים שבהם נדרש צוות ניהול המשברים לתפקד. על כן, יש להתבסס על מתודולוגיות סדורות לניהול משברי סייבר ומחשוב ועל מערך מיומן שיוכן לצורך זה בעת שגרה. לאור זאת, מומלץ לנסח תוכנית מתאימה לפיתוח הכלים והמיומנויות בארגון, כפי שתואר במאמר זה, לרבות קביעת תוכנית סדורה לאימונים, סימולציות ותרגילים.

טורקיה – האתגרים למדיניות המאבק באיומי סייבר

אופיר איתן

טורקיה היא אחת המדינות המפותחות ביותר במזרח התיכון מבחינה טכנולוגית, כלכלית ומוסדית, ויחד עם זאת היא אחת המדינות המאוימות ביותר בעולם בממד הסייבר. הממשל הטורקי פועל בשנים האחרונות כדי לגשר על הפערים הקיימים באמצעי ההתגוננות מפני איומי הסייבר, אך המאמצים שהוא עושה בתחום זה טרם הניבו את הפירות הרצויים.
מאמר זה מנתח את תמונת המצב של ההיערכות הלאומית הטורקית להגנה בסייבר ומצביע על מספר אתגרים מובנים הניצבים בפני היערכות זו, שמקורם במדיניות טורקית ארוכת שנים. הממשל הטורקי ייאלץ למצוא פתרונות לאתגרים אלה כדי שיוכל לעמוד ביעדי תוכניות הביטחון הלאומי שלו להגנה בסייבר.

מילות מפתח: סייבר, טורקיה, מדיניות, ביטחון לאומי, כלכלה פוליטית

מבוא

איומי הסייבר משפיעים בשנים האחרונות באופן הולך וגובר על חיינו, ובתוך כך גם על מדיניותן של ממשלות רבות. על רקע זה החלו מדינות רבות לנקוט צעדים שמטרתם לגבש אסטרטגיה לאומית במרחב הסייבר ולהקים תשתיות הגנה נגד תקיפות ברשת. מאז שנשמעו באמצעי התקשורת השמות Stuxnet, Flame ו־Shamoon ופורסם דבר התקפות מניעת שירות (DDOS) נגד המגזר הפיננסי בארצות הברית, נראה כי גם המזרח התיכון הפך להיות גורם פעיל בזירת המלחמה התוססת בסייבר. זהות התוקפים במרחב הסייבר הינה סוגיה מעורפלת, ועם זאת שורבבו בה בשנים האחרונות שמותיהן של ארצות הברית, ישראל, איראן ומדינות נוספות במפרץ הפרסי.

אופיר איתן הוא מנהל אבטחת מידע והגנת סייבר מוסמך וקצין מודיעין סייבר בדרגת רס"ן (מיל') באגף המודיעין. בעל תואר ראשון ושני בהיסטוריה של המזרח התיכון מאוניברסיטת תל אביב.

טורקיה הינה אחת המדינות המפותחות ביותר במזרח התיכון, מעצמה אזורית וחברה מרכזית בנאט"ו. למרות זאת, קיים פער ניכר ביכולותיהם של מוסדותיה להתמודד עם התקפות סייבר. לראיה, רק בשנת 2016 הוקם מרכז לאומי לתיאום ולשיתוף פעולה להתגוננות בפני מתקפות סייבר ורק בחודש יולי 2017 הוצגה בפני הקבינט הטורקי טיוטת חוק לחיזוק ההגנה על מרחב הסייבר בגופים הציבוריים, תוך שילוב מומחי אבטחה מדיסציפלינות שונות, לרבות האקרים מסוג "כובע לבן" (White Hat Hackers), כלומר אנשי מקצוע שתפקידם לשפר את רמת האבטחה של רשתות ואמצעי מחשוב באמצעות ניסיונות תקיפה מבוקרים וסקרי מערכות. מטרת המהלך הייתה להרחיב את סמכויותיו של המרכז הלאומי להתערבות נגד התקפות סייבר (NICC), שהינו מחלקה הכפופה למועצת טכנולוגיית המידע והתקשורת (Bilgi Teknolojileri ve İletişim Kurumu – BTK) ונושא באחריות לטיפול בתקיפות סייבר ברחבי המדינה והכלתן, וכן להפצת ידע ולסיוע בהגנה על כלל הגופים הציבוריים.[1]

טורקיה טרם מיסדה מעטפת הגנה לאומית בסייבר המאגדת את מוסדות המשטר, גופי הביטחון, התשתיות הלאומיות וגופים אזרחיים. זאת, הגם שהיא גיבשה זה מכבר מתווה אסטרטגי לאומי בעניין זה – National Cyber Security Strategy and Action Plan 2016–2019.[2] המתווה הטורקי דומה לתהליכים דומים שהבשילו במדינות אחרות בעולם המערבי, תוך שהוא מתייחס למציאות הפרטנית של טורקיה, הנדרשת להתמודד עם איומי סייבר מגוונים ורציפים על תשתיות המדינה.

נראה כי מעֵבר לחסמים הביורוקרטיים, קיימים בטורקיה אתגרים מובְנים הבולמים את הצעדים הדרושים לצמיחתה של תשתית מקומית איכותית בתחום הסייבר. ענף האינטרנט ותקשורת הנתונים, הנכלל בין ענפי התעשייה עתירת הידע, הוא בעל מאפיינים ייחודיים ושונים משאר ענפי התעשייה במשק. כפועל יוצא מכך, תחום הלחימה בסייבר, קרי עולם התקיפות וההגנות הווירטואליות על רשתות ומערכות מחשוב, מחייב הפנייה מיוחדת של משאבים, בראש ובראשונה לפיתוח ההון האנושי.

על רקע הבנות יסוד אלו, ברצוני לטעון כי מדיניותה הריכוזית של טורקיה לאורך השנים היא שהובילה לאתגרים היסודיים הניצבים בפניה כיום, בבואה להתמודד עם איומי הסייבר על תשתיותיה הלאומיות. ניתן לחלק אתגרים אלה

1 Seyma Nazli Gurbuz, "Turkey Adopts Cybersecurity Strategy, Fights Cyberterrorism", *Daily Sabah*, August 10, 2017, https://www.dailysabah.com/war-on-terror/2017/08/11/turkey-adopts-cybersecurity-strategy-fights-cyberterrorism.

2 Merve Seren, "Turkey Steps Up Counter-Cyber Attack Efforts", *The New Turkey*, January 24, 2017, https://thenewturkey.org/turkey-steps-up-counter-cyber-attack-efforts/.

לשני רבדים שהם בעלי השפעה רבה על מסוגלותה של טורקיה לפתח עוצמה בסייבר: אתגר המדיניות והביורוקרטיה ואתגר התרבות הארגונית.

הניתוח שיוצג בעמודים הבאים יפתח בתיאור קצר של תמונת המצב של המדיניות הלאומית הטורקית בתחום הגנת הסייבר. לאחר מכן ינותחו שני הרבדים שהוזכרו לעיל, המכילים את כלל האתגרים המובנים הניצבים בפני מקבלי ההחלטות הטורקים בדרך לפיתוח עוצמה בסייבר. המאמר יעשה שימוש במספר הנחות יסוד מן הגישה הכלכלית הקפיטליסטית לצורך ניתוח תיאורטי של התפתחות האתגרים הניצבים בפני המדיניות הטורקית.

המדיניות הלאומית הטורקית להגנה בסייבר

מחקרים מן השנים האחרונות מציגים נתונים שצריכים להדיר שינה מעיניהם של מקבלי ההחלטות בצמרת הביטחונית הטורקית. כך, למשל, כבר בשנת 2012 פורסם כי טורקיה נמנית על עשר המדינות המותקפות ביותר בעולם בתחום הסייבר.[3] חברות אבטחת מידע ותקשורת מהמובילות בעולם, כמו Trend Micro, Fortinet ו־Akamai, פרסמו בשנים 2016־2017 כי טורקיה עומדת בראש רשימת המדינות המותקפות בסייבר באירופה ובעולם.[4]

ניתוח מפת איומי הסייבר מצביע על שלושה שחקנים מרכזיים המאיימים על רשתות האינטרנט הממשלתיות והמסחריות של טורקיה: גורמי הכוח הכורדים, האופוזיציה למשטר (FETO) ותשתיות הפשע המאורגן (Cyber crime, על פי המונח המקובל כיום). כדוגמה לאיום הסייבר הכורדי ניתן להביא מתקפה שזכתה להדים נרחבים בתקשורת, כאשר ארגון ה־PKK תקף את אתר משרד האוצר הטורקי עד שהביא לנפילתו, תוך השחתת תוכן האתר בתכני תעמולה התואמים את סדר היום של ארגון המחתרת הכורדי.[5] באירוע זה היה ברור מה היה השיקול שעמד מאחורי התקיפה "הרועשת", אף ששאלת זהותו של התוקף בעולם הסייבר נשארת בדרך כלל עלומה. בהקשר זה ניתן למנות רשימה ארוכה של תקיפות מפורסמות אחרות שכוונו נגד אתרי ממשל טורקיים, כמו אלה של משרד האוצר,[6] המשטרה

3 Aydin Albayark, "Turkey among Top 10 Countries Subjected to Cyber Attacks", *Sunday's Zaman*, July 1, 2012, https://www.todayszaman.com/news-285120-turkey-among-top-10-countries-subjected-to-cyber-attacks.html.

4 Seren, "Turkey Steps Up Counter-Cyber Attack Efforts".

5 Umit Kurt, "Cyber Security: A Road Map for Turkey", in *Strategy Research Project* (Pennsylvania: U.S. Army College, 2012), pp. 8-9; Umit Enginsoy, "Turkey Centralizes Efforts for National Cyber Security", *Hurriyet Daily*, November 21, 2011, https://www.hurriyetdailynews.com/turkey-centralizes-efforts-for-national-cyber-security.aspx?pageID=238&nID=7307&NewsCatID=344.

6 Kurt, "Cyber Security: A Road Map for Turkey".

הלאומית וחברת התעופה Turkish Airlines.[7] סביר ליחס תקיפות אלו ודומות להן לגורמי הכוח הכורדים וכן לגופי פשיעה בסייבר.

ככול שגובר השימוש של המוסדות והחברות בטורקיה ברשתות המחשוב והתקשורת, כך גדל האיום על תפקודם התקין. ההערכה היא כי מתוך כשמונים מיליון תושבים בטורקיה – המדינה העשרים בעולם מבחינת גודל האוכלוסייה[8] – קרוב ל־43 מיליון משתמשים ברשת האינטרנט. בכך הם תופסים את המקום ה־19 בעולם בשימוש באמצעי תקשורת זה.[9] מכאן עולה שטורקיה ניצבת בשורה הראשונה בעולם, לצד המדינות המפותחות ביותר במשפחת האומות, ביחס בין מספר התושבים ובין היקף השימוש באינטרנט. לעומת זאת, טורקיה מפגרת מאחור במה שנוגע למאמץ הלאומי להגנה על רשתות מפני תקיפות סייבר, בהשוואה לצעדים שיוזמות המדינות המפותחות.

באוקטובר 2010 פרסם הצבא הטורקי את "הספר האדום", המאפשר חלון הצצה, אחת למספר שנים, לנבכי אסטרטגיית הביטחון הלאומי הטורקית. מתוכן הספר ניתן להסיק כי הסייבר נתפס, בראייתה של טורקיה, כאיום בלתי קונבנציונלי. בהמשך לכך, המועצה הטורקית לביטחון לאומי אשררה בשנת 2011 אסטרטגיה לאומית חדשה, הכוללת לראשונה גם את היבט האיומים בסייבר.[10] כאמור, לאחרונה אף פורסמה תוכנית לאומית לאסטרטגיית הגנה בסייבר לשנים 2016־2019.[11] אסטרטגיה זו מגדירה שני יעדים מרכזיים: הראשון, הכרה טורקית בכך שהגנה בסייבר הינה מרכיב אינטגרלי של הביטחון הלאומי; השני, עמידת טורקיה בכשירות הנדרשת בכול הקשור לצעדים המינהלתיים והטכנולוגיים הדרושים כדי להשיג ביטחון מוחלט לכלל נכסיה בממד הסייבר.

מוסדות הממשל הטורקי מקיימים פונקציות הגנה בסייבר שהן פרי יוזמות מקומיות. למעשה, אין כל רשות אחודה או גוף עליון מתאם בטורקיה לנושא ההגנה בסייבר, והפעילות בתחום זה מסתמכת על מוצרים מיובאים. בין הגופים הקיימים ניתן למנות את ה־CERT הלאומי[12] הטורקי (TR-CERT) הפועל תחת רשות המידע והתקשורת, וכן את ה־Cyber Fusion Center (CFC) הראשון של

7 Albayark, "Turkey among Top 10 Countries Subjected to Cyber Attacks".

8 הנתון נכון לשנת 2009 ולכן, בסבירות גבוהה, היקף המשתמשים כיום רחב יותר. על כל פנים, אין בכך כדי לשנות מהותית את התמונה.

9 Central Intelligence Agency, *The World Factbook: Turkey*, January 7, 2013, https://www.cia.gov/library/publications/the-world-factbook/geos/tu.html.

10 J. A. Lewis and K. Timlin, *Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization* (Washington: CSIS, 2011), p. 20.

11 Seren, "Turkey Steps Up Counter-Cyber Attack Efforts".

12 CERT – Computer/Cyber Emergency Response Team – תפיסה שגובשה לראשונה על ידי אוניברסיטת קרנגי־מלון ומתייחסת לצורך בהקמת מרכזים לאומיים, מוסדיים או מגזריים שתפקידם הוא לסייע לקהלי יעד להיערך מול איומי סייבר ולהתמודד איתם.

משרד ההגנה הטורקי.[13] לעומת זאת, צבא טורקיה וארגון הביון הלאומי (MIT) נשענים על פתרונות טכנולוגיים מקומיים להגנה בסייבר, אותם מפתחת ומספקת "החברה הממשלתית לתוכנה ומערכות" (Havelsan).

בעקבות עבודת מטה שנערכה בשנים 2010־2011, גיבשה טורקיה תוכנית להקמת "מפקדת סייבר" במטה הכללי של הצבא הטורקי, שייעודה הוא להדוף מתקפות רשת נגד המדינה. המטות המשולבים של צבא טורקיה הכריזו על הקמת מפקדה זו בשנת 2013.[14] על פי הפרסומים בתקשורת, וכן מעדותו של קצין בכיר בצבא הטורקי השופך אור על הנעשה מאחורי הקלעים של המפקדה החדשה, גוף זה בנוי על פי המודל של מקבילו האמריקאי ותפקידו הוא לנטר את כל רשת האינטרנט הציבורית בטורקיה במטרה לספק מעטפת הגנתית למוסדות המדינתיים.[15] "מפקדת הסייבר" הטורקית אמורה לפעול בשיתוף פעולה עם משרד ההגנה הטורקי, המועצה הלאומית למחקרי מדע וטכנולוגיה (TÜBİTAK) והאוניברסיטה הטכנולוגית של המזרח התיכון (METU). המפקדה, שבראשה עומד קצין בדרגת גנרל, נשענת על תקציב ייעודי, הינה עצמאית מבחינת המבנה הארגוני וכוללת יחידה מיוחדת להגנה בסייבר.[16] על פי הצהרת שר התקשורת והתחבורה הטורקי, תוכנית ההגנה בסייבר של טורקיה יושמה בפועל בשנת 2013.[17]

המודעות בטורקיה לצורך בהגנה במרחב הסייבר ולפוטנציאל האיומים בממד זה אמנם גוברת בשנים האחרונות, כפי שניתן ללמוד מהתוכניות המדיניות ומהיוזמות המקומיות השונות, אולם מבחינה מעשית, טורקיה נמצאת בפער משמעותי בהיערכותה הלאומית להגנה בסייבר בהשוואה למדינות מערביות אחרות. צ'טין קיה קוץ', פרופסור לקריפטוגרפיה מאוניברסיטת קליפורניה, היטיב לתאר את מצבה בתחום ההגנה בסייבר: "מכיוון שטורקיה טרם השלימה את השינוי הקיברנטי בתשתיותיה [...] במקרה של תקיפת התשתיות בעתיד, דוגמת מערכות הרכבת התחתית או החשמל, אין בנמצא תהליכים מקדימים כדי להתמודד עם איום זה".[18]

---

13. Seren, "Turkey Steps Up Counter-Cyber Attack Efforts".
14. Burak Ege Bekdil, "Cyber Defense 'Indispensible Part' of Turkey's National Security: Senior Official", *Atlantic Council, Defense News*, December 13, 2013, http://www.atlanticcouncil.org/blogs/natosource/cyber-defense-indispensible-part-of-turkey-s-national-security-senior-official.
15. Kurt, "Cyber Security: A Road Map for Turkey", p. 14; Enginsoy, "Turkey Centralizes Efforts for National Cyber Security".
16. Lewis and Timlin, *Cybersecurity and Cyberwarfare.*
17. "Turkey's Cyber Defense Plan to be Ready in 2013", *Hurriyet Daily*, March 2, 2012, https://www.hurriyetdailynews.com/turkeys-cyber-defense-plan-to-be-ready-in-2013.aspx?pageID=238&nid=15054.
18. Gurbuz, "Turkey Adopts Cybersecurity Strategy, Fights Cyberterrorism".

תמונת המצב באה ללמדנו כי קידום מנגנוני ההגנה של טורקיה בסייבר מחייב לא רק זירוז התהליכים הביורוקרטיים, אלא גם התבססות על שתי אבני יסוד מההיצע הלאומי הטורקי – כוח אדם מקומי מיומן ותשתית מקומית של מחקר ופיתוח. עם זאת, כפי שכבר צוין בראשית המאמר, טורקיה נאלצת להתמודד עם אתגרים רבים נוספים, שמקורם במדיניות הריכוזית שהנהיגו ממשלותיה מאז היווסדה – אתגרים היוצרים חסמים ובלמים המעכבים את ההתבססות על שתי אבני היסוד הללו.

האתגרים הניצבים בפני טורקיה בדרך לפיתוח עוצמה במרחב הסייבר

הגישה הקפיטליסטית לכלכלה הפוליטית גורסת כי מדיניות ריכוזית מהווה את אחד מכשלי השוק המעכבים התפתחות יצרנית וטכנולוגית וצמיחתה של יזמות פרטית. הפילוסוף והכלכלן אדם סמית' טען כי חלוקת העבודה בין כלל גורמי השוק מביאה להתמקצעות, חוסכת זמן במעבר בין שלבי הייצור השונים ומניעה אנשים לשכלל תהליכי ייצור. בנוסף לכך, הגישה הקפיטליסטית אינה חולקת על כך שלמדינה יש תפקיד חשוב בפיתוח המשק ובייצובו גם בעידן השוק החופשי של ימינו. במסגרת זו, המדינה משפיעה דרך רגולציה של שוק העבודה, החינוך, הכשרות מקצועיות ועוד, תוך נקיטת מדיניות כלכלית וצעדי חקיקה ואכיפה במסגרת המתח שבין ביזור השוק לריכוזו.[19]

בכלכלת שוק ליברלית פירמות פותרות כשלי שוק באמצעות יחסי הגומלין בין השוק החופשי, חוזים (הסדרים) והיררכיה (יחסים בין הפירמות). במילים אחרות, על פי הגישה הליברלית הקלאסית, כשלי שוק נפתרים על ידי הדינמיקה של "היד הנעלמה" של כוחות השוק. לעומת זאת, בכלכלת שוק מתואמת, המאפיינת את הכלכלה הטורקית, הפירמות מסתמכות פחות על תחרות ויותר על רשתות עסקיות ויחסי גומלין אסטרטגיים ("חוזה לא מושלם"). למעשה, גם תחת תכתיבי השוק החופשי נשמרת ריכוזיות במשק – בידיהן של המדינה ושל קבוצות כוח בודדות.[20]

אתגר המדיניות והביורוקרטיה

עד שלהי שנות התשעים של המאה העשרים, ממשלות טורקיה לא נקטו מדיניות מוכוונת לדרבון וקידום יזמות פרטית בכלל, ובענף התעשיות עתירות הידע בפרט. הדבר היה פועל יוצא של מדיניות ארוכת שנים הנעוצה עוד בימי המעבר

19 Peter A. Hall, David Soskice, "Varieties of Capitalism", *The Political Economy Reader: Markets as Institutions*, eds. N. Barma and S.K. Vogel (Indiana: Routledge, 2007), pp. 292-303, 307-312.

20 שם.

מהאימפריה העות'מאנית לרפובליקה הטורקית המודרנית. הגם שהרפובליקה הטורקית ירשה מסורת בת למעלה ממאה שנים של אימוץ טכנולוגיה מערבית, ירושה זו כללה גם מדינה עניה שכלכלתה נשענת על יבולים חקלאיים ונעדרת תשתית ממוסדת כלשהי של מגזר פרטי.[21]

הממשלה הטורקית הראשונה חתרה אמנם למדיניות של פיתוח כלכלי וחברתי, אך משמעות הדבר בראייתה הייתה הקמת תעשייה כבדה ממוקדת ייצור. לשם כך, וכחלק מהמדיניות הריכוזית בכלל, הקימה ממשלת טורקיה חברות ממשלתיות בבעלותה ובניהולה, תוך אימוץ תוכניות חומש פרי המודל הסובייטי. מלבד המדיניות הריכוזית, שבלמה כל אפשרות ליזמות פרטית, ממשלות טורקיה לדורותיהן אימצו מדיניות פיתוח שאינה מקדמת דרישה לפיתוח מקומי. בתוך כך, טורקיה ביססה את הקמת התשתיות שלה על ייבוא מבחוץ מן המסד ועד הטפחות. הממשל הטורקי חתם על הסכמים עם תאגידים זרים כדי שאלה יתכננו, יקימו ויתפעלו מיזמים רחבי היקף, שבסופו של התהליך יועברו לידיים טורקיות. תהליך זה מתקיים למעשה עד ימינו. מדיניות זו הובילה לתלות בלעדית בטכנולוגיה חיצונית ולהיעדר צורך ביזמות מקומית.[22]

המתווה של הקמת חברות ותאגידים ממשלתיים הועתק במרוצת הזמן על ידי הממשל הטורקי גם למגזר הפרטי, כשהיעדים המדיניים ואופן הביצוע נשארו זהים. לכן, עד שלהי שנות התשעים של המאה העשרים התמקד העידוד הממשלתי של המגזר הפרטי בתעשיות כבדות, שתכליתן הייתה לייצר כמה שיותר מקומות עבודה. מדיניות זו הייתה בעלת השלכות נוספות, שמתוכן שתיים קשורות לענייננו: הראשונה, הזנחת ענפי התעשיות עתירות הידע, להן נדרש על פי רוב כוח אדם מיומן, משכיל ואיכותי, לצד הפחתה במספר המשרות בענפים אלה בהשוואה לענפים אחרים; השנייה, עליית שכבה של אוליגרכים, הלוא הם ראשי ובעלי התאגידים הגדולים. המדובר בקונגלומרט של משפחות המתוות את הביקוש בשוק הטורקי על פי צרכיהן, כאשר ברוב המקרים קיימת חפיפה כמעט מלאה בין האינטרסים שלהן ובין האינטרסים של המדינה. תאגידים אלה אינם זקוקים לרוב למהנדסים ולאנשי היי־טק, ובכך הם מחשקים את הקיבעון הטכנולוגי, הנחשלות בקרב האוכלוסייה ומיקודה בתעשיות "צווארון כחול".[23]

גם לאחר פתיחת השוק הטורקי, בשלהי שנות התשעים של המאה העשרים, ניצבו יזמים מקומיים בפני מסכת תלאות של ביורוקרטיה, שהקשתה ואפילו בלמה

---

21 Arnold Reisman, "Why Has Turkey Spawned so Few High-Tech Startup Firms? Or, Why is Turkey so Dependent on Technologic Innovations Created Outside its Borders?", *SSRN*, May 26, 2006, pp. 1-4, https://ssrn.com/abstract=904780.

22 שם, שם.

23 שם, עמ' 1־4, 9.

כל ניצן של יזמות מקומית. מדובר באתגר משמעותי לענפי התעשייה עתירת הידע בכלל ולענף הסייבר והאינטרנט בפרט. היזם הטורקי, המבקש להקים חברת הזנק, נתקל עוד מראשית דרכו במצב שבו כמעט ואינו יכול לגייס כספים מלבד הון אישי או משפחתי. רוב האשראי הפוטנציאלי ליוזמות מסוג זה מצוי בידי הבנקים, אולם אלה נוקטים מדיניות זהירה נוכח המשברים התכופים שפקדו את שוק ההון הטורקי בשלושים השנים האחרונות.[24] הנתונים הסטטיסטיים מראים כי מתן האשראי הבנקאי לעסקים הקטנים והבינוניים בטורקיה עומד על שלושה־ארבעה אחוזים בלבד מכלל האשראי הניתן למגזר הפרטי.[25] יש בכך אירוניה מסוימת, מפאת העובדה שהתאגידים הקטנים והבינוניים מהווים כ־99 אחוזים מענף התעשייה בטורקיה, אך נותנים תעסוקה לכ־66 אחוזים מסך העובדים בענף ומספקים כ־34 אחוזים מהערך המוסף היצרני בו.[26]

גם כאשר הבנקים בטורקיה מחליטים לתת אשראי ליזמות עסקית, רבים מהם לא מסוגלים לגבש תוכנית מימון ראויה ולמצוא את המקורות הכספיים הרלוונטיים למימונה. גם מקורות מימון חלופיים, כגון קרנות הון־סיכון, משקיעים עצמיים ("איינג'לים" – Angels) וגיוס הון ממניות, אינם מפותחים דיים בטורקיה בהשוואה לנדרש במדינות מערביות. יתרה מכך, מי שמספק את מרבית ההלוואות לפירמות היזמיות בשוק הטורקי הוא הבנק הלאומי הטורקי, Halk Bank (המצוי תחת הליכי הפרטה).[27] זאת, בשונה ממקורות המימון של יזמים במדינות מערביות, המגיעים מקשת רחבה של אפיקי מימון וסיוע, בהם הממשלה עצמה, השקעות חוץ, פירמות לעידוד צמיחה, ארגונים חוץ ממשלתיים (NGO's), ארגוני סחר בין־לאומיים וכיוצא באלה.[28] כאמור, מנופי צמיחה כלכליים מסוג זה אינם מפותחים דיים בטורקיה. מצב זה מעמיד אתגרים וחסמים רבים בפני ענף התעשיות עתירות הידע במדינה, ובתוכן תעשיית הסייבר.[29]

כשמדובר בתהליכי הביורוקרטיה הניצבים בפני היזם הטורקי, ראוי להביא את דברי הפרופסורית לניהול מאוניברסיטת סבנג'י באיסטנבול, דילק צ'טינדמר, המתארים אתגר מהותי זה: "טורקיה היא המדינה ה־13 הכי ביורוקרטית בעולם. מומחים טוענים כי יזם זקוק ל־172 חתימות ממגוון מוסדות ממשלתיים כדי לקבל

24 שם, עמ' 8־9.
25 שם, שם.
26 "Small and Medium-Sized Enterprises in Turkey: Issues and Policies", *OECD Report* (Paris: OECD Publications, 2004), pp. 29-33.
27 שם.
28 Reisman, "Why Has Turkey Spawned so Few High-Tech Startup Firms?", pp. 8-9.
29 "Small and Medium-Sized Enterprises in Turkey".

אישור להשקיע [...] בטורקיה, יזם מבזבז לא פחות מעשרים אחוזים מזמנו בנושאים ביורוקרטיים, כאשר באיחוד האירופי הדבר עומד על שמונה אחוזים בלבד".[30]

היבט קריטי נוסף בעידן השוק החופשי הוא היעדר הנגישות של חברות הזנק טורקיות למידע. על פי עקרונות הכלכלה הניאו ליברלית, קידום צמיחה במשק מחייב פתיחות מרבית של ערוצי המידע והידע. ממחקר שערך ארגון OECD בשנת 2004 על פלח העסקים הקטנים והבינוניים, עולה כי בשוק הטורקי קיים חוסר בסוכני ידע ובערוצי תקשורת לשיתוף מידע. בתוך כך, ארגון OECD המליץ לממשל הטורקי להימנע מעימותים בין גופי החקיקה ומערכות האכיפה על רקע ניגוד אינטרסים, וזאת כדי לאפשר שקיפות לטובת העסקים הקטנים והבינוניים.

בשנת 2001, עם התנעת התוכנית הלאומית למימוש אמנת האיחוד האירופי, התחייבה טורקיה להנהיג רפורמות יסודיות במערכות הרגולציה המקומיות, על פי אמות המידה הבין־לאומיות המקובלות. תהליך זה, יחד עם צעדים נוספים שממשלת טורקיה מנסה לקדם, אמורים לשפר, בין היתר, את תהליכי הביורוקרטיה ואת מערכות הרגולציה במדינה.[31]

אתגר התרבות הארגונית

עולם הסייבר מתייחד בהון האנושי שלו, המבדיל את מוקדי הידע והמומחים בענף זה משאר התעשיות עתירות הידע. בין היתר, דרושים מספר מאפיינים או תכונות מקצועיות כתנאי להתפתחותם, לקידומם ולהגעתם לרמה מקצועית נאותה של מהנדסי תוכנה, מומחי רשתות תקשורת ואבטחת מידע, וכן של פצחנים (Hackers). אין מדובר במדדים מדעיים, אלא בסביבה ממסדית וארגונית היוצרת אקלים המאפשר צמיחתם של פיתוחים ופתרונות טכנולוגיים חדשניים. קשה לנתק בין מרכיב חיוני זה של עולם הסייבר ובין מדיניות ממסדית ריכוזית המאפיינת את טורקיה, שכן לפחות על פי הגישות הליברליות לכלכלה פוליטית, מדיניות ריכוזית יוצרת חסמים להתפתחות של פירמות ויחידים גם בענפי האינטרנט ותקשורת הנתונים המבקשים לפרוץ דרך ולחדש בתחומם.

כדי לבחון את אתגרי התרבות הארגונית העומדים בפני יצירת שכבת הון אנושי בענף הסייבר הטורקי, יש להתמקד בשני מאפייני יסוד של טורקיה: יחסי צבא־מדינה ותרבות המחקר והפיתוח. כל זאת, תוך התבססות על הנחת היסוד, לפיה הריכוזיות בממסד הטורקי חוסמת תהליכים מבניים (כשלי שוק – Market Failure) הנחוצים לצמיחת תעשיות הסייבר במדינה.[32]

30. Reisman, "Why Has Turkey Spawned so Few High-Tech Startup Firms?", pp. 8-9.
31. "Small and Medium-Sized Enterprises in Turkey".
32. Hall and Soskice, "Varieties of Capitalism".

מקובל על רבים שהתעשיות הביטחוניות הן כור מחצב וזרז לפיתוחים טכנולוגיים בענפי תעשייה רבים, ובמיוחד בענף התעשיות עתירות הידע. בהתחשב בהנחת יסוד זו, הגיוני להסיק כי טורקיה, בה הצבא מהווה עמוד תווך מרכזי של המשטר והחברה, צריכה למצב את עצמה כחלוצה גם בממד הסייבר, או לכול הפחות להיות בעלת "סל כלים" איכותי בתחום זה. אולם, תמונת המצב מורכבת יותר, ולכן המציאות בממד הסייבר הטורקי שונה בתכלית. פרופסור ארנולד רייזמן טוען כי טורקיה לא הצליחה לתעל את ניסיונה הצבאי ואת תעשיותיה הביטחוניות לפיתוחים טכנולוגיים משמעותיים בשוק האזרחי, דבר שכאמור הינו הכרחי לצמיחה בממד הסייבר. כדי להוכיח את טענתו, ערך רייזמן השוואה תיאורטית בין שלוש מדינות שיש ביניהן קווים משיקים לדיוננו: טורקיה, ישראל והודו. שלוש מדינות אלו עומדות מאז הקמתן באופן רצוף בפני איומים ביטחוניים משמעותיים על ריבונותן, ושלושתן התנסו בקליטה והטמעה של אמצעי לחימה איכותיים המאופיינים בטכנולוגיה ברמה גבוהה.[33]

התעשיות הביטחוניות של טורקיה מייצאות כיום תוצרי פיתוח עצמאיים הדורשים התמקצעות טכנית גבוהה בתחומי האוויר, הים, הלוחמה האלקטרונית ומערכות השליטה והבקרה.[34] אולם, יחסי הגומלין בין התעשיות הביטחוניות הטורקיות ובין הפירמות הפרטיות בטורקיה (יחידים וארגונים) בממד הסייבר לא הביאו לפיתוח "סל כלים" איכותי דיו. זאת, מכיוון שתעשיות הסייבר הממשלתיות, בדומה לכול תעשייה טכנולוגית אחרת בטורקיה, אינן מפותחות די צורכן. ממצאיו של רייזמן מראים כי ישראל הצליחה לתעל את הפיתוחים הצבאיים שלה גם לטובת הפירמות הכלכליות במדינה וגם להפצת טכנולוגיות וידע בשוק האזרחי. לעומת זאת, טורקיה כמעט ואינה נהנית מתהליך דומה. בדומה למדינות מתפתחות, טורקיה למדה כיצד לייצר אמצעי לחימה קלים ותחמושת, אך את הנשק המתוחכם יותר המצוי בארסנל הצבאי שלה היא רכשה באופן קבוע מבחוץ (בין היתר מישראל).[35]

פרופסור רייזמן מציג תיאוריה להבנת מציאות זו. הוא משווה בין המארג הצבאי־חברתי של ישראל לזה של טורקיה, תוך הדגשת ייחודיותה של ישראל כ־"Startup Nation", וזאת למרות שגם שבטורקיה, כמו בישראל, נהוג שירות חובה צבאי. מרבית תהליכי המו"פ הפנים ארגוניים של צה"ל מתבססים על אוכלוסיית המשרתים בצבא, אך הייחודיות הישראלית היא בכך שתכתיבי הביקוש הארגוניים מביאים את שכבת הפיקוד הצבאית לאפשר מרחב יצירתיות ופעולה רחב, והתרבות הארגונית מעודדת את צמיחתם של רעיונות ויוזמות "מלמטה למעלה". כאשר

---

33 Reisman, "Why Has Turkey Spawned so Few High-Tech Startup Firms?", pp. 10-15.

34 Ibrahim Sunnetci, "High-Tech in Turkey – Special Report", *Military Technology*, Vol. 35, No. 3 (2011): 107-110.

35 Reisman, "Why Has Turkey Spawned so Few High-Tech Startup Firms?", pp. 10-15.

מצרפים לתרבות ארגונית זו את העובדה שצה"ל הוא שמאתר וממיין את המועמדים מתוך מרבית האוכלוסייה המגיעה לגיל 18 וששיעור המתגייסים לצבא הוא גבוה, מתגבשים יחסי גומלין מפרים בין הצבא ובין החברה האזרחית.

ואכן, אזרחים רבים בישראל יוצאים לאחר שירותם הצבאי לשוק האזרחי עם מטען ידע איכותי וניסיון תעסוקתי. במצב זה נפתחות בפניהם דלתות רבות במטרה לתעל את יצרנותם לטובת חברות אזרחיות, שבראש חלק מהן עומדים בוגרי המערכת הביטחונית. לעומת זאת, בטורקיה אין מסורת כזאת וגם לא תהליך דומה של הפריה הדדית בין המערכת הצבאית ובין השוק האזרחי. כך, גם כאשר הממסד הביטחוני הטורקי מאתר גורם איכותי במערכת, רוב הסיכויים הם שהוא יעשה בו שימוש רק אם אותו גורם יבחר להישאר בתוך מסגרת התעשיות הביטחוניות שבבעלות המדינה, ואלו פועלות על פי רוב תחת אילוצים ותכתיבים ארגוניים וביורוקרטיים המעכבים צמיחה.[36]

חרף הנאמר לעיל ניתן לטעון, ובצדק רב, כי אין הכרח בקיומם של יחסי צבא־חברה הדוקים כדי ליצור שכבת הון אנושי איכותית לענף הסייבר. הגם שמדובר בציר המצמיח פיתוח, מדינות שונות ידעו להגיע בעבר ובהווה להישגים גם ללא הצורך למצוא פתרון לאיומים ביטחוניים. אלא שבמקרה הטורקי, המחקר והפיתוח טעונים שיפור ניכר גם בשוק האזרחי. ההשקעות של הממסד הטורקי, כמו גם של הפירמות הפרטיות, במחקר אקדמי או מסחרי הינן דלות ביותר. לכך יש לצרף את העובדה כי משכורותיהם של החוקרים באקדמיה בטורקיה אינן גבוהות, דבר הפותח פתח לרמת איכות אקדמית נמוכה. מדובר בתרבות ארגונית מוסדית שאינה מהווה קרקע פוריה לפיתוחים, לשיתוף רעיונות, ליצירת מידע וידע וכדומה, שהם אבני יסוד להתקדמות וצמיחה בתעשיית הסייבר.[37]

הן הממסד הטורקי והן בעלי ההון בטורקיה לא עשו ככלל די לאורך השנים כדי לטפח מחקר, פיתוח ויזמות טכנולוגית. חשוב להדגיש כי האוליגרכים הטורקים אמנם דואגים להזרים הון חזרה לציבור ולשוק הטורקי, אך רוב התרומות וקרנות ההשקעה מנותבות להקמת בתי ספר, אוניברסיטאות ומוזיאונים. אין בנמצא בטורקיה מנגנון ממוסד להעצמת מחקרים אקדמיים על ידי השוק הפרטי, לא כל שכן לעידוד יזמות טכנולוגית באשר היא. לשם המחשה, הפארק הטכנולוגי הראשון בטורקיה נוסד בשנת 1985 על ידי האוניברסיטה הטכנולוגית באיסטנבול ולשכת המסחר העירונית. מוסד דומה הוקם באנקרה רק בשנת 1991, על ידי האוניברסיטה הטכנולוגית של המזרח התיכון (METU). לעומת זאת, פרופסור רייזמן מצביע

36 Hall of Soskice "Varieties of Capitalism"; Reisman, "Why Has Turkey Spawned so Few High-Tech Startup Firms?", pp. 5-8.

37 Reisman, "Why Has Turkey Spawned so Few High-Tech Startup Firms?", pp. 5-8, 10-12.

על כך שמכון ויצמן – מוסד שהוקם בישראל בין השאר במטרה לייצא ממצאים אקדמיים לשוק המסחרי – החל לפעול כבר בשנות החמישים של המאה העשרים.[38]

מצאתי לנכון לסכם דיון זה בציטוט של פרופסור רייזמן: "הגם שטורקיה שינתה את מדיניותה משנת 1923 והתניעה רפורמות נרחבות, היא לא שינתה את [אופי] אנשיה, השקועים במסורתיות. היסטורית, המשכילים הטורקים בתקופת האימפריה העות'מאנית היו מנהלים וביורוקרטים, אך לא היו בעלי 'ראש עסקי',[39] ובמיוחד לא בעלי אוריינטציה טכנית".[40]

סיכום

עיון במקורות שונים מראה כי הדיון האקדמי בסוגיית הסייבר בטורקיה, לפחות בשפה האנגלית, טרם הגיע לבשלות. הגם שניתן למצוא ברשת האינטרנט לא מעט דיווחים חדשותיים ותקשורתיים על תקיפות סייבר שחוותה טורקיה, ניכר כי הדיון בכך מסתכם על פי רוב במאמרי דעה שנכתבים על ידי גורמים שונים. על כן, בבואי לבחון את עיקרי התהליכים שטורקיה חווה בתחום הסייבר, בחרתי להתמקד באתגרים הניצבים בפניה, ובעיקר בבעיית הליבה, שבראייתי היא החוסר בהון אנושי איכותי מהיצע מקומי. לשם כך, בחרתי להשעין את ניתוח תמונת המצב בעיקר על ממצאיו ומסקנותיו של פרופסור ארנולד רייזמן, לצד שימוש במקור נוסף – ממצאי דוח ארגון OECD משנת 2004, שהתמקד במחקר הכלכלה הטורקית ובמתן הצעות לפיתוחה. הגם שהדיון האקדמי והניתוח שפרסתי בעמודים אלה אינם שלמים, הם מצביעים על הצורך להעמיק בהבנת יסודותיה של התרבות הטורקית כדי לפענח את הבסיס לאתגרים העומדים בפני פיתוח תעשיית הסייבר המקומית.

ההבחנה שהצעתי בין ההשפעה של המדיניות הטורקית הריכוזית על האתגר המדיני־ביורוקרטי מצד אחד ועל אתגר התרבות הארגונית מצד שני, הינה הבחנה מלאכותית בלבד לצורך הבהרת הטיעון הלוגי. למעשה, מדובר ביחסי גומלין סימביוטיים בין תרבותה של החברה הטורקית ובין מדיניותן של ממשלותיה. תמונת המצב החברתית־כלכלית הנוכחית במדינה מראה שאחוז גדול מהאוכלוסייה הטורקית מתגורר במרחב הכפרי ומשמר חברה מסורתית, אסלאמית ופטריארכלית, דבר המשפיע על מדיניותן ותפקודן של הממשלות הטורקיות.

דבריה של הפרופסורית דילק צ'טינדמר מיטיבים להעביר את המסר: "[...] האופק התעסוקתי בראי בוגרי האוניברסיטאות [הטורקיות] כולל תעסוקה בחברות

38 שם, עמ' 12, 15.

39 רייזמן משתמש במונח "Business-minded". בכך הוא מכוון להערכתי לחשיבה עסקית ויזמות בשוק החופשי.

40 Reisman, "Why Has Turkey Spawned so Few High-Tech Startup Firms?", pp. 8-9.

גדולות, שכן הקמת פירמה פרטית נחשבת לסיכון גדול. על כן, אין בנמצא מסורת של יזמות פרטית".[41] משפט זה מבטא היטב את המסקנה המרכזית העולה מהמאמר, לפיה כדי לטפח הון אנושי איכותי בקהילת הסייבר הטורקית יש צורך בסביבה הבשלה לכך, קרי תשתית המעודדת יוזמה וחדשנות. אולם נראה כי טורקיה אינה "חממה" המעודדת יזמות פרטית, אשר על פי הנוסחה המקובלת הינה תנאי הכרחי להעצמת אנשי היי־טק ומהנדסים פורצי דרך. יתר על כן, כאשר טורקיה נדרשת לפתרונות טכנולוגיים ייחודיים, סביר להניח שתבחר בייבוא ידע חיצוני, וכול אחד משחקני המשולש מדינה־אוליגרכים־חברה יעדיף לנתב את ההון האנושי לחברות הגדולות והיצרניות, בעוד שהמקום למקוריות וליזמות, ההכרחיות בעולם הסייבר, יישאר מוגבל.

41 שם, עמ' 14.

אסטרטגיית הסייבר של גרמניה – היערכות ממשלתית וצבאית מול איומי הסייבר

עמרי וקסלר

גרמניה היא מדינה מובילה באיחוד האירופי ואחת מהכלכלות החזקות בעולם. כתוצאה מכך היא מהווה מטרה מרכזית למתקפות קיברנטיות מצד מדינות, ארגוני טרור וארגוני פשע. התגברות האיום על הדמוקרטיה הגרמנית באמצעות קמפיינים של הפצת מידע כוזב, לצד האיום עליה מצד רוסיה, הובילו לשינוי בתפיסת הביטחון הגרמנית והביאו את ממשלת גרמניה לחתור להגברת עצמאותה בתחום הסייבר ולהתבססות על יכולות התקפיות במרחב זה. הבנת דרכי התמודדותה של גרמניה עם איומי הסייבר ותוכניותיה העתידיות בנושא זה חשובה לצורכי למידה והשוואה, וכן כדי לספק תובנות חדשות בסוגיה זו, במיוחד עבור מדינות דמוקרטיות אחרות.
בחלקו הראשון של המאמר מתוארים ההיערכות של ממשלת גרמניה בתחומי האבטחה הקיברנטית, שיתוף הפעולה בין הרשויות הגרמניות וכן היערכויות הקשורות בכוח אדם ובחיזוק המוסדות הרלוונטיים. בחלקו השני מתוארות ההיערכות ברמה הביטחונית־צבאית והדרך שבה מתאימה עצמה גרמניה לאתגרים החדשים. החלק האחרון במאמר בוחן את תמונת המצב בפן הבין־לאומי וכיצד רואה גרמניה את תפקידה כמובילה בתחום הסייבר בזירה הבין־לאומית.

מילות מפתח: אבטחה קיברנטית, גרמניה, אסטרטגיה, היערכות ממשלתית, היערכות צבאית.

רקע

ב־23 בפברואר 2011 פרסמה גרמניה אסטרטגיה מקיפה לתחום הסייבר. המסמך מגדיר את תפיסת האיום הקיברנטי, קובע קווים מנחים לאסטרטגיית אבטחה קיברנטית ומגדיר מטרות וצעדים ליישומם. הצעדים אותם נקטה גרמניה מאז

עמרי וקסלר הוא חוקר בסדנת יובל נאמן למדע, טכנולוגיה וביטחון ובמרכז למחקר סייבר בינתחומי ע"ש בלווטניק, אוניברסיטת תל אביב.

פרסום האסטרטגיה משנת 2011 עסקו בהגנה על תשתיות קריטיות, בהגברת מודעות האזרחים ובהטלת אחריות על יצרנים לספק מוצרים מאובטחים, בחיזוק אבטחת ה־IT בקרב הרשויות, בהקמת המרכז הלאומי להגנה קיברנטית (Cyber Abwehrzentrum – Cyber A-Z), בהקמת מועצה לאומית לאבטחה קיברנטית, בייעול המאבק בפשיעה במרחב הקיברנטי ובהתייצבות גרמניה כגורם מפתח בחזית המאמצים להגנת הסייבר באירופה וברחבי העולם.

בנובמבר 2016 אישר הקבינט הגרמני מסמך אסטרטגיה חדש בנושא אבטחת הסייבר, שפורסם מטעם משרד הפנים. האסטרטגיה החדשה הרחיבה את קודמתה מ־2011 ופורטו בה ארבעה תחומים מרכזיים שבהם על גרמניה לפעול: שימוש בטוח ועצמאי בסביבה הדיגיטלית; שיתוף פעולה בין המדינה והמערכת הכלכלית הגרמנית בתחום הסייבר; בניית מערך אבטחה קיברנטית יעיל בקרב המגזר הציבורי; הפיכת גרמניה לגורם מרכזי במדיניות הסייבר האירופית והעולמית.

תפיסת האיום

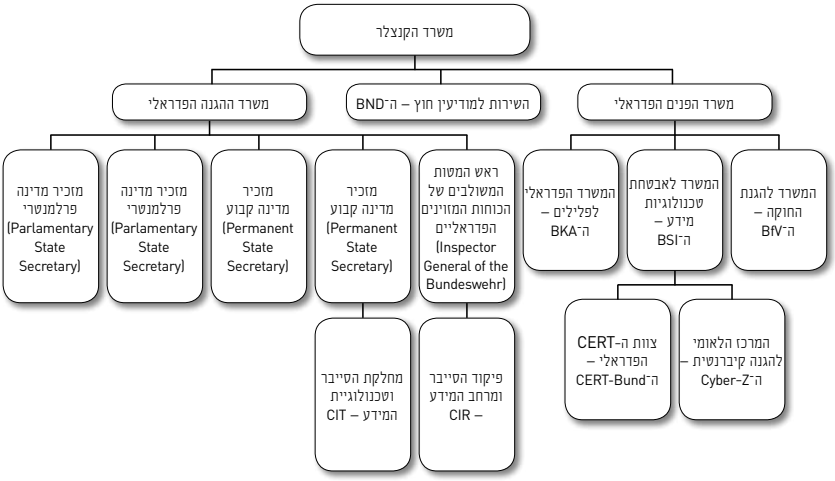
מסמך האסטרטגיה הגרמני משנת 2011 הציג את האיום הקיברנטי באופן כללי למדי ותיאר את מורכבות המתקפות הקיברנטיות. לעומתו, המסמך שפורסם בשנת 2016 הצביע על החשיבות הגוברת שמעניקה גרמניה לתחום הסייבר לאור העלייה במספר המתקפות הקיברנטיות ובמורכבותן. מסמך האסטרטגיה משנת 2016 עוסק, בין השאר, בנזק הנגרם ממתקפות קיברנטיות בתחומים החברתי, הכלכלי, הפוליטי והאישי, ומתאר אותן כאיום על היציבות, הסדר הציבורי והדמוקרטיה. המסמך מ־2016 גם מגדיר מטרות שפגיעה בהן תגרום לנזק ציבורי ופרטי רב. ביניהן:

- מתקפה על תשתיות קריטיות, ובמיוחד על תשתיות האנרגיה ורשת החשמל.
- מתקפה על תשתיות בנקאיות ומוסדות פיננסיים וביצוע מניפולציה על הבורסה.
- מניפולציה של מערכות אוטונומיות, השתלטות על תעבורת מידע הנשלטת על ידי מערכות IT, וכן מניפולציות על מערכות IT בתחום הבריאות.
- הפצה של מידע כוזב, דיווחים מטעים וחדשות מזויפות, המאפשרת לבצע מניפולציה של דעת הקהל, ועל כן מהווה סכנה לחברה החופשית ולדמוקרטיה.

משרד הפנים הגרמני, שהיה כאמור האחראי לניסוח האסטרטגיה, זיהה סוגים שונים של תוקפים ושל מניעים לביצוע מתקפות במרחב הקיברנטי: הרקע למתקפות הוא רחב ויכול להיות אידיאולוגי או פלילי. המבַצעים עלולים להיות ארגוני טרור, ארגוני פשע מאורגן, יחידות צבא או שירותי מודיעין של מדינות. הרקע המגוון של התוקפים ומקצועיותם מקשים על יכולות הגילוי והמעקב וכן על ניתוח המתקפות. מחברי המסמך מזהירים מפני עימותים פוליטיים או צבאיים שעלולים להיות מלווים

בעימות במרחב הקיברנטי. עימות במרחב זה עשוי להסלים למלחמת סייבר של ממש, או אפילו למתקפות סייבר שמתחת לסף של עימות מזוין.

תמונת מצב האיומים מורכבת ממספר רב של שחקנים בעלי יכולות ומניעים שונים. על כן, מחברי המסמך מסַכמים כי אמצעי ההגנה הקלאסיים על מערכות ה־IT הקיימות אינם מספיקים. הם מניחים כי מספר תקיפות הסייבר צפוי לעלות, כי מורכבותן תגבר וכי המטרות המרכזיות של התקפות הסייבר יהיו החברה הגרמנית, הכלכלה והתעשייה הגרמניות, וכן הדמוקרטיה הגרמנית.



תרשים: גופי הביטחון והסייבר בגרמניה

היערכות ממשלתית

גופי הממשל האחראים על תחום הסייבר בגרמניה הם: המשרד לאבטחת טכנולוגיית מידע (BSI), המשרד להגנת החוקה, המשמש כסוכנות ביטחון הפנים (BfV), שירות מודיעין החוץ (BND), המשרד הפדרלי לפלילים (BKA), משרד ההגנה (BMVg), משרד הפנים (BMI) והמשרד להגנת הציבור וסיוע למקרי אסון (BBK), המקביל לפיקוד העורף בישראל.

המשרד לאבטחת טכנולוגיית מידע

ה־BSI (Bundesamt für Sicherheit in der Informationstechnik) הוא משרד פדרלי הנמצא תחת סמכותו של משרד הפנים ומתפקד גם כרשות הלאומית לאבטחה קיברנטית. ה־BSI הוקם בשנת 1991 במטרה לספק שירותי IT לגופי ממשלה, ליצרני מערכות IT וכן לספקים ולמשתמשים. כיום אחראי ה־BSI להגנה על טכנולוגיית המידע של גרמניה ועל יישום מדיניות אבטחת המידע הלאומית. כן הוא אחראי

על מגוון פעילויות, כגון התרעה, מניעה ותגובה לתקריות, אזהרות מפני נקודות תורפה במוצרים ומפני תוכנות נוזקה, בניית ערוצי הדרכה והעלאת מודעות בקרב גופי ממשלה והציבור. כמו כן אחראי המשרד על חילופי מידע עם משרדי ממשלה, מוסדות וארגוני המגזר הפרטי, על ניסוח תקני אבטחה למפעילי תשתיות קריטיות ולמוצרים וכן על תהליכי הסמכה והכשרה של ארגונים ומוצרים.[1]

ה־BSI אחראי על גופים נוספים העוסקים בהתמודדות עם איומי סייבר, כגון המרכז הלאומי להגנה קיברנטית (Cyber A-Z) צוות ה־CERT הפדרלי (CERT-Bund) וה־CERT האזרחי (Bürger-CERT). הגוף האחרון אחראי על הגברת מודעות הציבור והעסקים הקטנים לאיומי סייבר.[2]

חיזוק המרכז הלאומי להגנה קיברנטית

Cyber A-Z הוא מוסד פדרלי להגנה מפני מתקפות אלקטרוניות על תשתיות ה־IT של גרמניה ועל המגזר הכלכלי שלה. המרכז הוקם על בסיס החלטת קבינט מפברואר 2011 והחל לפעול ביוני אותה שנה תחת המשרד לאבטחת טכנולוגיית מידע (BSI). Cyber A-Z ממוקם בעיר בון.[3]

המרכז הלאומי להגנה קיברנטית אינו מהווה ישות עצמאית והוא פועל יוצא של שורת הסכמי שיתוף פעולה בין הרשויות הגרמניות העוסקות בהגנה קיברנטית. על כן, ההפרדה בין תחומי השיפוט והאחריות של הרשויות השונות, ובעיקר בין המשטרה לשירותי המודיעין, נשמרת גם במהלך שיתוף הפעולה במסגרת המרכז.

המשימות המרכזיות של המרכז הלאומי להגנה קיברנטית הן מניעת מתקפות סייבר, אספקת מידע והתרעה מוקדמת על מתקפות כאלו. המרכז משתף מידע על הפרופילים והזהויות של השחקנים העומדים מאחורי מתקפות הסייבר, וכן משתף מידע סביב נקודות תורפה של מוצרי IT.

במסמך האסטרטגיה מ־2016 הומלץ כי Cyber A-Z ימשיך להתפתח כמרכז תיאום וכי תוקנה לו בעתיד יכולת ניתוח עצמאית ויכולת בניית תמונת מצב שתתאר במדויק את המתרחש. כמו כן הומלץ כי המרכז הלאומי להגנה קיברנטית יפעל גם כמרכז לאימונים ולתרגולים משותפים של צעדי התמודדות עם התקפות סייבר.[4]

---

1 Melissa Hathaway et al., "Germany: Cyber Readiness at a Glance", *Potomac Institute for Policy Studies*, October 2016, pp. 5-7, http://www.potomacinstitute.org/images/CRI/CRI_Germany_Profile_PIPS.pdf; "Cyber-Sicherheitsstrategie für Deutschland 2016", *Bundesministerium des Innern*, 2016, p. 17.

2 Hathaway et al., "Germany: Cyber Readiness at a Glance", pp. 5-7.

3 הרשויות הממלאות תפקיד מרכזי בתפעול המרכז הלאומי להגנה קיברנטית הן המשרד להגנת החוקה, המשרד לאבטחת טכנולוגיית מידע והמשרד להגנת הציבור וסיוע למקרי אסון. רשויות נוספות המעורבות במידע ושיתוף פעולה במסגרת פעילות המרכז הן המשרד הפדרלי לפלילים, שירות מודיעין החוץ הגרמני, המשטרה הפדרלית והצבא (הבונדסוור).

4 "Cyber-Sicherheitsstrategie für Deutschland 2016", p. 28

חיזוק יכולות הניתוח והתגובה של משרדי הממשלה

גרמניה משקיעה בהקמת צוותי תגובה ניידים (Mobile Incident Response Teams – MIRT), הכפופים למשרד לאבטחת טכנולוגיית מידע. מטרתם של צוותים אלה היא לנתח את המצב בזמן מתקפה ולסייע לצוותים המקומיים להתמודד עם האירוע והשלכותיו. הצוותים הניידים נועדו לתת מענה על פי בקשה, כדי לסייע לגופים חוקתיים, לרשויות פדרליות, למפעילי תשתיות קריטיות ולמתקנים חשובים. מטרת הסיוע היא בעיקר התמודדות עם האירוע, התאוששות וחזרה לשגרה.[5] צוותי התגובה הניידים אמורים לקבל סיוע מיחידות מיוחדות של המשרד הפדרלי לפלילים ומהמשרד להגנת החוקה.

צוותים נוספים אמורים לקום תחת המשרד הפדרלי לפלילים. צוותים אלה, שייקראו "כוחות לתגובה מהירה" (Quick Reaction Force), יהוו יחידה משפטית שתפקידה יהיה לאפשר תגובה מהירה למתקפות סייבר באמצעות תיאום צמוד עם פרקליטות המדינות השונות בגרמניה או עם משרד הפרקליטות הפדרלית. הצוותים אמורים לאפשר זירוז תהליכי אכיפה והבאה לדין, בשיתוף עם רשויות האכיפה הגרמניות.

גם המשרד להגנת החוקה הקים "צוותי סייבר ניידים" (Mobile Cyber Teams) המורכבים ממומחי IT וממומחי מודיעין בעלי ניסיון בניתוח מתקפות קיברנטיות. צוותים אלה יכללו עובדים הבקיאים בשפות זרות ויסייעו בהתמודדות עם מתקפות קיברנטיות של גופי מודיעין זרים או מתקפות של ארגוני טרור.[6]

חיזוק צוותי **CERT** הקיימים והקמת צוותים נוספים לתגובות חירום

כאמור, צוות ה־CERT הפדרלי מסונף למשרד לאבטחת טכנולוגיות מידע ואחראי על סיוע לרשויות ולמפעילי תשתיות קריטיות, לעסקים, לארגוני המגזר הפרטי, לרשויות מקומיות ולמוסדות מחקר וידע. כמו כן, ה־CERT הפדרלי אחראי על שמירת קשר ותיאום עם צוותי CERT זרים ובין־לאומיים.[7]

ממשלת גרמניה אמורה להשקיע משאבים נוספים כדי להגדיל את צוות ה־CERT הפדרלי ולהרחיב את הידע והמומחיות של אנשיו. כמו כן אמורים לקום צוותי CERT חדשים.

חיזוק יכולות ההתרעה של שירות מודיעין החוץ הגרמני

שירות מודיעין החוץ הגרמני (BND) אחראי, בין השאר, על מעקב ורישום של ניסיונות מצד גורמים חיצוניים – מדינות, ארגוני טרור או פושעים – לתקוף

5 שם, עמ' 29.
6 שם.
7 שם, עמ' 34.

קיברנטית את התשתיות של גרמניה ושל המגזר הכלכלי והאזרחי בה. המעקב אחר ניסיונות תקיפה והתיעוד שלהם אמורים לאפשר ל־BND לבנות דפוס פעולה של התוקפים, וכך לספק התרעה מוקדמת בעת זיהוי פעילות חשודה מצידם.

ה־BND משתף פעולה עם מומחי IT ואנליסטים במטרה לבנות מערכת התרעה מוקדמת מפני מתקפות קיברנטיות. מערכת כזאת אמורה לזהות מתקפות מסוג זה מבעוד מועד, לנתח אותן ולבנות תמונת מצב של מפת האיומים. מאמצי הגילוי המוקדם מתבססים על מודיעין סיגינטי, הנאסף באמצעות ביצוע סריקות יזומות ברשת, כחלק ממדיניות המכונה Signals Intelligence Support to Cyber Defence.[8] פיתוח מערכת ההתרעה המוקדמת נגד מתקפות קיברנטיות החל ב־2014, ועד שנת 2020 יושקעו בפרויקט זה כ־300 מיליון אירו. הפרויקט מתבצע בשיתוף עם סוכנויות מודיעין של בעלות בריתה של גרמניה וצפוי לספק מענה גם לניסיונות ריגול ברשת.[9]

ה־BND משתמש בחיישנים המותקנים בסיבים אופטיים ברחבי העולם. אלה מקנים לשירות מודיעין החוץ הגרמני יכולת לעקוב אחר תעבורת מידע במדינות אחרות ולנטר מתקפות סייבר מבעוד מועד. שיטה זו גם מאפשרת איסוף מידע על תוכנות זדוניות והקמת מאגר מידע על כלי התקיפה.[10]

חיזוק המסגרות המשפטית והחוקית במרחב הקיברנטי

הממשלה הפדרלית הגרמנית פועלת לחזק את רשויות האכיפה והשיפוט במטרה להיאבק בפשיעה הקיברנטית. החיזוק יבוצע במספר דרכים:

- ראשית, הממשלה תהיה האחראית להקצאת משאבים לרשויות הרלוונטיות וכן לתוספת כוח אדם מיומן בתחומים של זיהוי מצבים, קרימינולוגיה במרחב הקיברנטי וזיהוי פלילי במרחב הדיגיטלי.
- שנית, הממשלה תסייע לרשויות הביטחון והאכיפה בפיתוח ובבנייה של מערכות ניתוח והערכה.
- שלישית, יושם דגש מיוחד על התאמה בין הטכנולוגיה לבין הסמכויות והאמצעים הניתנים לגופי האכיפה והשיפוט על פי החוק. פיתוח של שני התחומים זה לצד זה נועד למנוע פערים בין החוק ובין הטכנולוגיה.

---

8 שם, עמ' 32.

9 "300 Millionen für Frühwarnsystem gegen Cyber-Attacken", *Spiegel Online*, May 16, 2014, http://www.spiegel.de/netzwelt/netzpolitik/bnd-arbeitet-an-fruehwarnsystem-gegen-cyber-attacken-a-969899.html.

10 Frederik Obenmaier and John Goetz, "Geheimdienst verstärkt Kampf gegen Cyber-Angriffe", *Süddeutsche Zeitung*, May 9, 2014, http://www.sueddeutsche.de/politik/abwehr-von-schadsoftware-geheimdienst-plant-fruehwarnsystem-fuer-cyber-angriffe-1.1956067#redirectedFromLandingpage.

- רביעית, הממשלה תשים דגש על שיתוף פעולה בין הרשויות הגרמניות ובין מדינות אחרות בעולם. כמו כן, יושם דגש על חילופי מידע ועל חילופי ידע מקצועי וניסיון בין הרשויות הגרמניות ובין רשויות מקבילות להן במדינות אחרות, וכן בין הרמות הפדרלית והמקומית בתוך גרמניה עצמה.[11]

דוגמה לשיתוף פעולה שגרמניה רוצה לחזק היא שיתוף הפעולה עם האיחוד האירופי בכלל ועם גופים ספציפיים שלו, כמו סוכנות ביטחון הרשתות והמידע (ENISA) ומרכז הפשיעה הקיברנטית של יורופול.

חיזוק הסמכויות של גופים בגרמניה המתמודדים עם איומי סייבר מוצא ביטוי, בין השאר, בחיזוק סמכויותיהם של המשרד הפדרלי לפלילים ושל המשטרה הפדרלית בתחומי הפשיעה הקיברנטית, הריגול במרחב הקיברנטי ועוד. כמו כן, ממשלת גרמניה התחייבה לחזק את מרכז הפשיעה הקיברנטית הפועל במסגרת המשרד הפדרלי לפלילים ולהרחיבו. המטרה היא לחזק את יכולות החקירה וההערכה של המרכז וכן לעדכן את החוק הפלילי ולהחמיר את הענישה על פשיעה במרחב הקיברנטי.

כדי להתמודד עם הריגול במרחב הקיברנטי, יחוזקו סמכויותיו של המשרד להגנת החוקה. במסגרת זו ישופרו יכולותיו לקיים מעקב וניתוח יעילים יותר אחר דפוסי פעולה משתנים של טרוריסטים וגורמים קיצוניים ברשת.[12]

היערכות צבאית

שני צעדים ארגוניים משמעותיים ננקטו בתחום הביטחוני־צבאי במטרה לחזק את היערכותה של גרמניה להתמודדות עם האיום הקיברנטי: הקמת מחלקת הסייבר וטכנולוגיית המידע (CIT) תחת משרד ההגנה והקמת פיקוד הסייבר ומרחב המידע (CIR) העצמאי לצד זרועות הצבא. צעדים אלה נועדו לספק הגנה קיברנטית למערכות ה־IT הצבאיות, וכן לגבש אסטרטגיות צבאיות בתחום הסייבר כדי להפוך את כוחות הביטחון לרלוונטיים בעידן הדיגיטלי באמצעות הקניית יכולות קיברנטיות הגנתיות והתקפיות.

מחלקת הסייבר ושכנולוגיות המידע

בספטמבר 2016 הורתה שרת ההגנה של גרמניה, אורסולה פון דר ליין (Ursula von der Leyen) על הקמת מחלקה חדשה במשרד ההגנה, שתיקרא Cyber und Informationstechnik (CIT). לראש המחלקה החדשה מונה קלאוס הארדי מולק

11 "Cyber-Sicherheitsstrategie für Deutschland 2016", p. 30.

12 "Digitale-Agenda: Mehr Sicherheit im Cyberraum", *Bundesregierung*, 2014, https://www.digitale-agenda.de/Webs/DA/DE/Handlungsfelder/6_Sicherheit/6-5_Cyberraum/cyberraum_node.html.

(Klaus Hardy Muehleck),[13] והיא כוללת כ־130 משרות. מחלקת הסייבר וטכנולוגיות המידע תבנה את מערך האבטחה הקיברנטית הצבאי בהתאם לאסטרטגיית האבטחה הקיברנטית הלאומית. כמו כן, המחלקה תוביל את תהליכי ההתמקצעות של הצבא הגרמני בתחום אבטחת המידע ותהיה אחראית על הסייבר וה־IT בתחום הצבאי. מחלקת הסייבר וטכנולוגיות המידע כוללת שתי מחלקות משנה: אחת בברלין, שתעסוק במשילות בסייבר וב־IT, בתכנון ובאסטרטגיה בתחום טכנולוגיית המידע. משימותיה יהיו, בין השאר, מדיניות דיגיטלית בתחום הסייבר וניהול יוזמות IT. כמו כן, המחלקה תהיה אחראית לבנות את מערך ה־IT של משרד ההגנה והצבא הגרמני. מחלקת המשנה השנייה תוקם בעיר בון ומטרתה היא לתת שירותי IT ולעסוק ביישום ובתפעול שוטפים של מערכות ה־IT הצבאיות. תחומי אחריות נוספים של המחלקה הם הגנה על מערכות IT, הגנה קיברנטית פסיבית ואבטחת הצפנה.[14]

פיקוד הסייבר ומרחב המידע

פיקוד הסייבר ומרחב המידע (Cyber und Informationsraum – CIR) הוקם כחלק מהצבא הגרמני עוד בנובמבר 2015. משימתו הייתה לבחון את ההיבטים הארגוניים, את תחומי האחריות ואת המשימות של הצבא הגרמני (הבונדסוור) בתחומי הסייבר והמידע. באפריל 2017 החל ה־CIR לתפקד כפיקוד צבאי לכול דבר, וצפוי להפוך למִבצעי באופן מלא החל משנת 2021. בראש ה־CIR עומד גנרל בעל שלושה כוכבים. באוקטובר 2016 מונה לעמוד בראשו גנרל מאייר לודויג ליינהוס (Maier Ludwig Leinhos), שהכריז על הפיכת הפיקוד למבצעי בתחילת אפריל 2017.

פיקוד הסייבר ומרחב המידע החל את פעילותו עם צוות התחלתי של כ־260 איש, ועד יולי 2017 גדל מספר המשרתים בו לכ־13,500 איש. כוח האדם של CIR צפוי לגדול לכ־14,500 איש עד מועד ההפעלה המבצעית המלאה שלו ב־2021. 1,500 משרות ישוריינו לאזרחים.[15]

תפקידיו של CIR מוגדרים כהגנה פסיבית והגנה אקטיבית במרחב הסייבר והמידע. הצבא הגרמני מהווה מטרה רגישה למאות מתקפות קיברנטיות מדי יום, שמטרתן היא בראש ובראשונה לגנוב מידע ונתונים ולשבש מערכות נשק

13 לפני מינויו לתפקיד זה עבד מוֶלק כמנהל מערכות המידע של חברת "טיסנקרופ", כמנהל מערכות המידע של יצרנית הרכב "פולקסווגן" (2004־2011) וכאחראי טכנולוגיות מידע של יצרנית הרכב "אאודי" (2001־2004).

14 "Verteidigungsministerin stellt neue Cyber-Abteilung auf", *Bundesministerium der Verteidigung,* October 5, 2016.

15 "German Military to Unveil New Cyber Command as Threats Grow", *Reuters*, March 30, 2017, http://www.reuters.com/article/us-germany-military-cyber/german-military-to-unveil-new-cyber-command-as-threats-grow-idUSKBN1712MW.

נתמכות IT. מרכזיותו של הבונדסוור בברית נאט"ו תורמת אף היא להפיכתו ליעד משמעותי לפריצה. בשל רגישותו זו, מטרתו הראשונית של פיקוד הסייבר ומרחב המידע היא הגנה על הרשתות ועל מערכות ה־IT של הבונדסוור. הגנה פסיבית זו מתבצעת באמצעות ניטור, גילוי מוקדם, ניתוח והערכת נזקים, וכן נטרול האיום ויכולת סיוע בחזרה לשגרה. תפקידים נוספים של CIR הם הגנה על מוסדות ממשלה, גופים ציבוריים ותשתיות קריטיות מפני מתקפות קיברנטיות מצד גורמים זרים, כגון מדינות או ארגוני טרור, וכן מאבק בתעמולה, במידע כוזב ובחדשות כוזבות (Fake news).

בנוסף להגנה הפסיבית, בונה הבונדסוור יכולות התקפיות, אותן הוא מגדיר כ"הגנה אקטיבית". אלו מתבטאות ביכולת לאסוף מודיעין על רשתות ומערכות זרות ולשבש את פעילותן. יכולות התקפיות אלו נמצאות עדיין בתהליכי פיתוח תחת אחריותו של צוות "מבצעי רשתות מחשב" (Computer Network Operations – CNO). הצוות מורכב מכשמונים מומחים בוגרי מחלקות מדעי המחשב באוניברסיטה הצבאית של מינכן, המתמחים בחדירה לרשתות ולשרתים, בביצוע מניפולציות ובגרימת נזק.[16] צוות ה־CNO קיים מאז שנת 2009, אולם תחת פיקוד הסייבר ומרחב המידע הוא יורחב ויועבר ממחלקת המבצעים של הפיקוד האסטרטגי של הבונדסוור אל "מרכז מִבצעי סייבר" חדש, ויכולותיו בתחום סריקת רשתות, איסוף מודיעין ודימוי אויב יגדלו.

יכולות אלו של הצבא הגרמני מעוררות ויכוח ער בקרב מחוקקים בגרמניה וגוררות ביקורת מצד הציבור הגרמני, הסולד מפני שימוש בכוח וחושש מפני כניסה ל"מלחמת סייבר" או מרוץ חימוש קיברנטי, ולכן מגלה חשדנות כלפי הרעיון של מתן סמכויות וכוח נוספים לכוחות הביטחון. ואכן, היכולות ההתקפיות מהוות שינוי עמוק בתפיסת הביטחון הגרמנית, אשר הופך אותה ליותר פרו־אקטיבית מאשר בעבר.[17]

בניית מערך גיוס לפיקוד הסייבר ומרחב המידע

הבונדסוור משתף פעולה עם המשרד לרווחה ופיתוח בתחום גיוס כוח אדם חדש לפיקוד הסייבר ומרחב המידע. הכוונה היא ליצור מנגנון גיוס והעסקה שיכלול מסלולי קריירה למגויסים ויפעל בהתאם לדינמיות ולגמישות המאפיינות את שוק ה־IT. במטרה להגיע למספר היעד של המגויסים ולהכשיר כוח אדם יוזם

16 Christian Kahl, "Vom Kampf in der fünften Dimension", *Bundeswehr Journal*, May 3, 2013, http://www.bundeswehr-journal.de/2013/vom-kampf-in-der-funften-dimension.

17 Isabel Skierka, "Bundeswehr: Cyber Security, the German Way", *Observer Research Foundation*, October 20, 2016, http://www.orfonline.org/expert-speaks/bundeswehr-cyber-security-the-german-way/.

וגמיש מבחינה מחשבתית, נשקל הרעיון לפנות לאוכלוסיות ולקבוצות יעד שעד לא מזמן לא היו מועמדות לגיוס, ובהן אנשים שנמצאו לא מתאימים למסגרת צבאית, מועמדים מרקע של משפחות מהגרים, בעלי אזרחות כפולה, מועמדים שנשרו ממסגרות החינוך הפורמליות ומועמדים מרקע מקצועי אחר. מכשירי גיוס חדשים למציאת מועמדים מתאימים הם קיום תחרויות וטורנירים לגילוי כישרונות בתחום ה־IT, תחרויות סטארט־אפ, גיוס מועמדים מתחום הגיימינג וכן מתן מלגות ללימודים רלוונטיים.[18] בנוסף, הקים הבונדסוור מחלקת מחקר בשם Cyber Cluster באוניברסיטה הצבאית במינכן והשיק תוכנית לימודי תואר באבטחה קיברנטית, אותה צפויים לסיים כשבעים בוגרים כל שנה.[19]

הזירה הבין־לאומית

גרמניה רואה בזירה הבין־לאומית הזדמנות לחיזוק האבטחה הקיברנטית באמצעות שיתופי פעולה ויוזמות משותפות, אך גם כפלטפורמה לחיזוק הכלכלה והתעשייה הגרמנית, המבוססת ברובה על ייצוא. התייצבותה של גרמניה במרכז הזירה הבין־לאומית בתחום הסייבר וה־IT תורמת לחיזוק המוניטין והמעמד הפוליטי שלה ברחבי העולם.

במסמך האסטרטגיה משנת 2016 מתחייבת ממשלת גרמניה לפעול להתייצבותה בחזית המאמץ האזורי־אירופי והבין־לאומי כדי לבנות חסינות ויכולת התמודדות עם איומים קיברנטיים ולקבוע תקנים לאבטחה בתחום הסייבר.

את הזירות שבהן מתכוונת גרמניה לקדם את מדיניות האבטחה הקיברנטית ניתן לחלק לארבע: אירופה והאיחוד האירופי; נאט"ו; הזירה הבין־לאומית; שיתופי פעולה בילטרליים.

אירופה

ביטחון השוק האירופי וההמשכיות הסדירה של המסחר ביבשת הם אינטרסים עליונים של ממשלת גרמניה. עם צמיחת המסחר הדיגיטלי עולה גם חשיבותה של האבטחה הקיברנטית עבור השוק האירופי המשותף. ישנה חפיפה בין האינטרס הגרמני לאבטחת הכלכלה המקוונת, הרשתות ומערכות המידע שבהן נעשה שימוש, לבין האינטרס של הנציבות האירופית, ששמה לה למטרה ליצור אמון וביטחון בפרויקטים של האיחוד, ובהם השוק המשותף הדיגיטלי.

אינטרס נוסף של גרמניה הוא שמירה על זכויות אדם ועל פרטיות בשימוש באינטרנט. על רקע זה הודיעה ממשלת גרמניה על תמיכתה ברגולציה מטעם

18 "Abschlussbericht Aufbaustab Cyber- und Informationsraum", *Bundesministerium der Verteidigung*, April 2016, pp.31-33.

19 שם, עמ' 35־36.

הנציבות האירופית, אשר תסדיר אבטחה של העברת נתונים ומידע בתוך אירופה ותסייע לשמירה על הפרטיות ועל מסחר תקין.[20]

בנוסף, פועלת הממשלה לחזק את מעמדה של גרמניה במסגרת מדיניות הסייבר האירופית, וזאת באמצעות מעורבות גדלה והולכת שלה במדיניות החוץ והביטחון של האיחוד האירופי. ממשלת גרמניה גם תומכת בקידום מחקרים של חוקרים גרמנים בתחום אבטחת ה־IT ופועלת לקשר ביניהם ובין מוסדות מחקר מקבילים ברחבי אירופה, וכן לקדם את תעשיית ה־IT המקומית. חלק ניכר מקידום התעשייה הגרמנית, כמו גם הגדלת מעורבותה של גרמניה בעיצוב מדיניות האבטחה הקיברנטית של האיחוד האירופי, באים לידי ביטוי בתמיכה בשורת פרויקטים של האיחוד העוסקים בסוגיות חוקיות וטכניות הקשורות למרחב הסייבר, כגון שימוש בזיהוי אלקטרוני ובחתימות אלקטרוניות של עסקים ורשויות. שימוש זה יאפשר זיהוי אמין של המשתמש וכן שיתוף פעולה מלא עם הסוכנות האירופית לאבטחת רשתות ומידע (European Union Agency for Network and Information Security – ENISA).[21]

נאט"ו

מדיניות החוץ והביטחון של גרמניה רואה בנאט"ו את עמוד התווך עליו נשענת הברית האירו־אטלנטית. חברותה של גרמניה בברית מבטיחה הן את ביטחונה שלה והן את ביטחון אירופה. לפי האסטרטגיה הגרמנית, תפיסת הביטחון הקולקטיבי של נאט"ו תקפה גם במרחב הקיברנטי, ועל כן מוטל על הברית הצפון אטלנטית להתחזק גם במרחב זה, כפי שהוא עושה בים, באוויר וביבשה. גרמניה היא שותפה מרכזית ומובילה בתהליכי הבנייה של מערך האבטחה הקיברנטית של נאט"ו ושל מדיניות הרתעה אפקטיבית במרחב הקיברנטי אל מול איומי הלוחמה ה"היברידית", כלומר זו המשלבת לוחמה קינטית וקיברנטית.[22]

הזירה הבין־לאומית

גרמניה הציבה את עצמה כמובילת הדיונים בארגונים הבין־לאומיים, ובראשם הארגון לביטחון ושיתוף פעולה באירופה (Organization of Security and Cooperation in Europe – OSCE) והאו"ם, בנושאים הנוגעים לשמירה על החוק הבין־לאומי במרחב הקיברנטי, לסגירת פערים בחוק הבין־לאומי בתחום הסייבר, לפיתוח נורמות, רגולציות ועקרונות הנוגעים להתנהגות מדינית אחראית בתחום זה, וכן לחיזוק היכולות והסמכות של האו"ם במרחב הקיברנטי.

---

20 "Cyber-Sicherheitsstrategie für Deutschland 2016", p. 40.
21 שם.
22 שם.

תחומים נוספים שבהם גרמניה לוקחת חלק הם העלאת המודעות לסכנות במרחב הקיברנטי, הרחבת מסגרות שיתוף המידע סביב מתקפות ותקריות קיברנטיות, החרפת המענה הבין־לאומי והחמרת הענישה על ריגול כלכלי ועל מתקפות סייבר, וכן תמיכה אקטיבית בחיזוק הפיקוח על ייצוא טכנולוגיות היכולות לשמש להתנהגות תוקפנית במרחב הקיברנטי.[23]

קשרים בילטרליים

גרמניה פועלת לתמוך בשותפותיה ולסייע להן בבנייה של יכולות גילוי, מניעה ותגובה לתקריות קיברנטיות, וכן לתמוך בחיזוק תשתיותיהן הדיגיטליות. כחלק משאיפתה של גרמניה להיתפס כשחקן אמין בזירה הבין־לאומית, היא מעודדת גורמים שונים בזירה זאת לבצע רפורמות חוקיות בתחום הסייבר, לחתום על אמנות בתחום זה ולנקוט צעדים בוני אמון שיחזקו את הביטחון הקיברנטי.[24]

אתגרים והשלכות פוטנציאליות של ההיערכות הגרמנית

על אף ההיערכויות השונות, הגידול בכוח אדם והרחבת הסמכויות של הרשויות והגופים השונים, ממשיכה ממשלת גרמניה לעמוד בפני מספר אתגרים במרחב הסייבר. חלק מהם הן מגבלות חוקיות הנוגעות לשימוש ביכולות סייבר התקפיות ולשיתוף פעולה בין הצבא ובין גופי המודיעין והביון, ואחרים נוגעים לפערים בתחום כוח האדם. כמו כן, להיערכות הגרמנית בתחום הסייבר יש מספר השלכות פוטנציאליות על מדיניות החוץ והביטחון השאפתנית של גרמניה בזירה הבין־לאומית.

פערים חוקתיים הנוגעים לשימוש בכוח

כחלק מהריסון הצבאי שמאפיין את גרמניה מאז תום מלחמת העולם השנייה, החוקה הגרמנית קובעת שכול שימוש בכוח צבאי למטרות שאינן הגנתיות גרידא מחייב את אישור הפרלמנט. בדוח של משרד ההגנה הגרמני נכתב כי הצורך במנדט פרלמנטרי תקף גם במבצעים במרחב הקיברנטי.[25] בשל המורכבות של מרחב זה, שבו לא תמיד ניתן להבדיל בין צעדים הגנתיים ובין צעדים התקפיים, נשאלת השאלה כיצד ובאילו מקרים על הצבא לפנות לפרלמנט כדי לקבל את אישורו. נראה כי גם הסעיף בחוקה הדורש את אישור הפרלמנט למהלכים של הגנה אקטיבית או מכה מקדימה עלול להוות אתגר בפני ביצוע מבצעים קיברנטיים, במיוחד כשמדובר בביצועם באופן מהיר וחשאי. עד היום לא נמצאה הדרך לגישור על פערים אלה.

ביצוע מתקפות קיברנטיות מצריך מודיעין מדויק על הרשתות והמערכות של היעד וכן על נקודות התורפה שלו אותן ניתן לנצל. מודיעין כזה, כמו גם פעולות

23 שם, עמ' 41.
24 שם, עמ' 42.
25 "Abschlussbericht Aufbaustab Cyber- und Informationsraum", p. 5.

ריגול והכנה אחרות לצורך ביצוע מתקפות קיברנטיות, הם תחום הפעולה של שירותי מודיעין. לכן, הצבא הגרמני ייאלץ לשתף פעולה ומידע בנושא זה עם שירותי הביון והמודיעין של גרמניה. בעוד שבארצות הברית שיתוף פעולה כזה הוא מובן מאליו, מה גם ופיקוד הסייבר האמריקאי חולק את אותה הנהגה עם סוכנות הביטחון הלאומית (NSA) ועושה שימוש בנכסיה ובמודיעין שהיא מספקת, שיתוף פעולה כזה בגרמניה ניצב בפני מגבלות חוקיות חמורות. הממד המשפטי של שיתוף הפעולה בין גופי המודיעין ובין הצבא וגופי האכיפה בגרמניה חורג ממסגרתו של מאמר זה. עם זאת, ניתן לציין כי מתנהל ויכוח משפטי באשר לסוגי המידע שמותר לגופי הביון, ובפרט ל־BND, לשתף עם רשויות גרמניות אחרות.[26] בנוסף לכך, ה־BND כפוף למשרד הקנצלר, בעוד שהצבא הגרמני כפוף למשרד ההגנה, והמשרד להגנת החוקה כפוף למשרד הפנים. לא ברור לפיכך כיצד ניתן לקיים שיתוף פעולה ביניהם. זאת ועוד, לפי שעה טרם הוגדרה חלוקת הסמכויות בין שלושת הגופים בכול הנוגע לאיסוף מידע הנוגע למבצעים קיברנטיים.

אתגרים בגיוס כוח אדם מיומן

בעיה נוספת, שאינה מיוחדת דווקא לגרמניה, היא גיוס והכשרת כוח האדם המתאים למילוי ואיוש המשרות החדשות בצוותי ה־CERT, ובמיוחד בפיקוד הסייבר ומרחב המידע בבונדסוור. על אף הכרזת הצבא הגרמני כי פיקוד הסייבר כבר אויש על ידי חיילים שנבחרו מתוך ענפים אחרים של הצבא, הבונדסוור עודנו ניצב בפני האתגר של הקמת מאגר מילואים של הפיקוד החדש. במכתב שנשלח מהמשרד הפדרלי האחראי לחימוש ולהצטיידות הצבא[27] לחיילי מילואים מתחום ה־IT, הם התבקשו למסור שמות של עמיתיהם לתחום ה־IT האזרחי. כן נכתב בפניה כי הצבא זקוק להאקרים, למפתחי IT, למומחים לאבטחת IT, למְבַצעי בדיקות חדירות (Penetration testers) ועוד.[28]

מעֵבר לקושי בגיוס אנשי IT מוכשרים ומנוסים, סובל הבונדסוור מאחוזי גיוס נמוכים ומתדמית של מעסיק לא אטרקטיבי. כמו כן, נמתחה ביקורת על התוכניות השאפתניות של הצבא, תוך טענה כי הוא אינו גמיש מספיק וכי קצב ההכשרות,

26 Kai Biermann, "BND-Überwachung: Warum schickt der BND der Bundeswehr abgehörte Daten?", *Zeit Online,* March 18, 2015, http://www.zeit.de/politik/deutschland/2015-03/bnd-bundeswehr-daten-ueberwachung/komplettansicht.

27 The Federal Office of Bundeswehr Equipment, Information Technology and In-Service Support.

28 Matthias Monroy, "Herausforderungen im Cyber- und Informationsraum: Bundeswehr sucht Tips für Aufbau einer Cyber-Reserve", *Netzpolitik,* April 26, 2016, https://netzpolitik.org/2016/herausforderungen-im-cyber-und-informationsraum-bundeswehr-sucht-tips-fuer-aufbau-einer-cyber-reserve/

הרכש וההצטיידות שלו אינו עולה בקנה אחד עם קצב היוזמה והחדשנות בשוקי החומרה והתוכנה, וכן עם קצב השינויים המהירים החלים במרחב הקיברנטי.[29]

תוכנית הלימודים האקדמית שהשיק הבונדסוור לצורך הכשרת אנשי IT היא צעד חיובי בכיוון הנכון, אך נוכח הצפי, לפיו כשבעים בוגרים אמורים לסיים את התוכנית כל שנה, ניתן להעריך כי יעבור זמן רב עד שהתוכנית תוכל לספק את צורכי הצבא. במצב זה קיים חשש שהבונדסוור ייאלץ לפנות לחברות קבלן פרטיות כדי שימלאו חלק ממשימותיו. אפשרות זו גורמת לחששות רבים של פגיעה בביטחון הלאומי, כפי שהודגם מספר פעמים בהדלפות מצד עובדי קבלן שפעלו עבור ה־NSA בארצות הברית.

הזדמנויות בזירה הבין־לאומית

שאיפותיה של גרמניה ורצונה למנף את מעמדה הבין־לאומי, כמו גם את כלכלתה ותעשייתה, אינן חדשות. בשנים האחרונות השתתפה גרמניה באופן פעיל ועקבי בפורומים בין־לאומיים שעסקו באבטחה קיברנטית ובטכנולוגיות מידע ותקשורת, כגון האו"ם, האיחוד האירופי, נאט"ו, פסגת ה־G–7, הארגון לביטחון ולשיתוף פעולה באירופה ועוד. כמו כן, גרמניה השתתפה בדיאלוגים בנושאי פיתוח ובניית יכולות קיברנטיות ולקחה חלק פעיל בדיוני קבוצת המומחים הממשלתיים של האו"ם (GGE) לקביעת נורמות התנהגות במרחב הקיברנטי.

פעילותה הבין־לאומית הבילטרלית של גרמניה התאפיינה ומתאפיינת בסיוע למדינות מתפתחות בתחום הסייבר, וכן בשיתופי פעולה בתחום זה עם מדינות מפותחות.[30] דוגמאות לשיתופי פעולה ודיאלוגים כאלה ניתן לראות, למשל, בדיאלוגים שנערכו בברלין עם משלחות מהודו,[31] בחתימת הסכם שיתוף פעולה עם

29 Nina Werkhäuser, "German Army Launches New Cyber Command", *Deutsche Welle*, April 1, 2016, http://www.dw.com/en/german-army-launches-new-cyber-command/a-38246517

30 Hathaway et al., "Germany: Cyber Readiness at a Glance", p. 13.

31 "Indo-German Intergovernmental Consultations in Berlin - Strengthening Cyber Cooperation", *German Missions in India*, May 31, 2017, http://www.india.diplo.de/Vertretung/indien/en/__pr/Politics__News/Merkel__Modi__2017__update2.html.

איגוד תעשיות הביטחון של אסטוניה,[32] ובהסכם שיתוף פעולה בתחום האבטחה הקיברנטית עם סינגפור.[33]

לצד מגמות אלו, הצפויות להימשך, נפתחו בפני גרמניה הזדמנויות נוספות בזירה הבין־לאומית: מדיניות ה"אמריקה תחילה" של הנשיא טראמפ, חוסר הבהירות המתמשך הנוגע לדרכה של ארצות הברית והתרחקותה היחסית מהאיחוד האירופי ומנאט"ו, לפחות בהשוואה לממשל אובמה, יכולים להוות הזדמנות עבור גרמניה למלא תפקיד מרכזי יותר בהנהגת מדינות המערב. באופן ספציפי, סגירת משרד המתאם לענייני אבטחה קיברנטית במחלקת המדינה של ארצות הברית ב־2017, שיכולה להיחשב כפגיעה ביכולותיה הדיפלומטיות של ארצות הברית בתחום האבטחה הקיברנטית, עשויה להוות הזדמנות עבור מדיניות החוץ השאפתנית של גרמניה.[34]

עזיבתה האפשרית של בריטניה את האיחוד האירופי תיצור, ככול הנראה, פערים בנושאי ביטחון ומודיעין באיחוד. הדבר נכון גם בתחום האבטחה הקיברנטית. הוואקום העלול להיווצר בעקבות עזיבתה של בריטניה – הנחשבת כשחקן מרכזי בתחום זה – עשוי לעודד את גרמניה לנסות למלא אותו ביכולותיה שלה. עם זאת, עזיבתה של בריטניה צפויה לפגוע לא רק באבטחה הקיברנטית, אלא במכלול שיתוף המידע בין מדינות האיחוד, ובכלל זה עם גרמניה.

סיכום

גרמניה רואה באיום הקיברנטי איום מרכזי ובעקבות זאת נערכת להגנה על כלכלתה, תעשייתה, כוחות הביטחון והתשתיות הקריטיות שלה. היא עושה זאת באמצעות שורה של פעולות במספר חזיתות: המשפטית, החוקתית, הצבאית, הפדרלית והמקומית. האסטרטגיה המקיפה של גרמניה שפורסמה בשנת 2016 מפרטת את הצעדים המרכזיים שנועדו לספק מענה לאיום הקיברנטי עליה. אסטרטגיה זו

32 "Cyber-Security Council Germany and Estonian Defence Industry Association sign cooperation agreement, agreeing upon fostering transnational cooperation in the area of cyber security together", *Cyber-Security Council Germany*, September 14, 2017, http://www.cybersicherheitsrat.de/data/PRESS-RELEASE-Cyber-Security-Council-Germany-and-Estonian-Defence-Industry-Association-sign-cooperation-agreement.pdf.

33 Prashanth Parameswaran, "What's in the New Singapore-Germany Cyber Pact?", *The Diplomat*, July 11, 2017, https://thediplomat.com/2017/07/whats-in-the-new-singapore-germany-cyber-pact/.

34 Morgan Chalfant, "Tillerson moves to close State cyber office", *The Hill*, August 29, 2017, http://thehill.com/policy/cybersecurity/348438-tillerson-moves-to-close-state-cyber-office.

תומכת בחיזוק ובהרחבה של הגופים והיחידות להגנה קיברנטית, וכן בהיערכות צבאית מחודשת, הכוללת הקמת גופים ייעודיים לתחום הסייבר.

בתחום ההיערכות הממשלתית, גרמניה שמה דגש על הרחבת הגופים הקיימים וחיזוק יכולותיהם. דוגמה בולטת לכך היא הרחבת המרכז הלאומי להגנה קיברנטית (Cyber A-Z), המשמש כגורם מקשר בין משרדי הממשלה השונים האחראים מבחינה חוקית על תחום הסייבר, וכן הקניית יכולות עצמאיות לגוף זה לצורך ניתוח, הערכה וגיבוש תמונת מצב, כמו גם הוספה של פלטפורמת אימון והדמיית מצבי חירום. דוגמאות נוספות הן חיזוק יכולות התגובה והיכולות המקומיות באמצעות סיוע פדרלי.

בזירה הצבאית, גרמניה הקימה את מחלקת הסייבר וטכנולוגיות המידע הפועלת תחת משרד ההגנה. המחלקה אחראית על תכנון האסטרטגיה הקיברנטית הצבאית ועל בניית מערך הסייבר של הבונדסוור. כמו כן, הוקם פיקוד הסייבר ומרחב המידע הצבאי (CIR), האחראי על הגנת הרשתות ומערכות ה־IT של הצבא ואמור להיות מצויד ביכולות הגנתיות והתקפיות. יכולותיו ההתקפיות הפוטנציאליות של הפיקוד מהוות שינוי מהותי במדיניות הגרמנית, שעד כה נמנעה משימוש בכוח ומבניית יכולות התקפיות, דבר שעשוי לעורר ביקורת ציבורית.

בזירה הבין־לאומית, נראה כי גרמניה רואה בשיתוף הפעולה הבין־לאומי והבילטרלי לא רק צעד אסטרטגי לחיזוק האבטחה הקיברנטית הלאומית, אלא גם הזדמנות למנף ולחזק את מעמדה הכלכלי והפוליטי בזירה האירופית מול מדינות שאיתן יש לה קשרים בילטרליים ומול ארגונים בין־לאומיים, וזאת על ידי הובלה ולקיחת חלק מרכזי במאמץ המשותף להתמודדות עם אתגרי סייבר. מיצובה של גרמניה כמעצמת סייבר מהווה ניסיון שלה לחזק את מעמדה הבין־לאומי, הפוליטי והדיפלומטי, וכן לחזק את התעשייה הטכנולוגית ואת הכלכלה הגרמנית מבוססת הייצוא.

גרמניה מצטרפת לשורה של מדינות אירופיות, ובכלל זה בריטניה וצרפת, החוששות מריגול, מגניבת מידע, מחוסר יציבות, מהשפעה חיצונית על הלך הרוח הציבורי ומהתערבות זרה בתהליכי הבחירות שלהן, ולכן הן בוחרות להשקיע מאמצים ומשאבים כדי להיות מוכנות להתמודדות עם איומים אלה. עם זאת, ישנם אתגרים חוקיים העומדים בפני התעצמותה של גרמניה בתחום הסייבר הצבאי, ובייחוד בתחום השימוש בנשק קיברנטי התקפי ובעקרונות ההגנה האקטיבית – חלק מתפקידיו של פיקוד הסייבר ומרחב המידע החדש. אתגרים נוספים הם בתחומי ההצטיידות וכוח האדם, אך אלה אינם מיוחדים לגרמניה. הצעדים החלקיים שננקטו כדי להתמודד עם אותם אתגרים הם מהלך בכיוון הנכון, אך אינם צפויים להוות פתרון מלא של הבעיה.

התהליך שעוברת גרמניה מעניין, בעיקר בשל עוצמתה ומרכזיותה בפוליטיקה ובכלכלה האירופית והבין־לאומית. ייתכן כי אירועים בעלי השפעה בין־לאומית, כגון מדיניות "אמריקה תחילה" של ממשל טראמפ, ידחקו בגרמניה להגדיל את הוצאות הביטחון שלה, הכוללות גם את תחומי הגנת הסייבר ולוחמת הסייבר. אירועים נוספים, כגון יציאת בריטניה מהאיחוד האירופי, צפויים לפגוע בביטחונה של גרמניה בכלל ובאבטחה הקיברנטית שלה בפרט, וזאת נוכח העובדה שביטחונה קשור לביטחון האיחוד האירופי כולו.

תהליך מעניין נוסף הוא השינוי העמוק שחל בתפיסת הביטחון הגרמנית, שעל אף האתגרים החוקיים מתבססת יותר ויותר על הגנה אקטיבית ואמצעים התקפיים. זהו שינוי גדול עבור מדינה שנמנעה בשבעים השנים האחרונות משימוש בכוח. עם זאת, שינוי זה צפוי להמשיך להיתקל במתנגדים רבים, הן מקרב הציבור והן מקרב המחוקקים בגרמניה, דבר שיקשה על מימושו.

הסייבר מחייב ומאפשר מהפכה בענייני מודיעין

דודי סימן טוב ונעם אלון

ההיסטוריה עשירה בדוגמאות של מעצמות, מדינות וצבאות שלא הצליחו לזהות פוטנציאל מהפכני של טכנולוגיה חדשה, וכתוצאה מכך איבדו את יתרונם ואת הרלוונטיות שלהם. מאמר זה מצביע על הפער בין השינויים הטכנולוגיים המהותיים שהסייבר יוצר ומאפשר ובין האופן שבו מתפקדים ארגוני המודיעין, אשר נותרו נשועים בתפיסות, בארכיטקטורה ובאתוסים שמקורם בפרדיגמת "מעגל המודיעין" שכוּננה בין שתי מלחמות העולם.[1] פער זה יוצר צורך בשינוי מערכתי ותפיסתי, אולם שינוי כזה מתעכב בשל היעדר תחושת משבר ודחיפות בקהילת המודיעין ובשיח הציבורי וזאת, למרות שהשיח על הפערים בין תפקוד גופי המודיעין בעידן הסייבר ובין התפיסות, התרבות והמבנה שלהם קיים כבר יותר מעשור. הסיבה העיקרית לכך היא שהמודיעין ממשיך לתפקד ומביא להישגים טובים גם בצורתו הנוכחית, במיוחד במישורים האופרטיבי והטקטי. ייחודו של מאמר זה הוא בהצגה שיטתית וברורה של הפערים והמתחים הקיימים בשל העיכוב באימוץ פרדיגמה חדשה על ידי קהילת המודיעין. המאמר מצביע על הסייבר כגורם המעצים פערים ומתחים אלה עד כדי חוסר יכולת לשמר את המערכת המודיעינית בצורתה הקיימת. בה בעת, המאמר מצביע על הסייבר כמרחב שמאפשר להיחלץ מפרדיגמת "מעגל המודיעין" ולפתח פרדיגמה חדשה.

מילות מפתח: מודיעין, סייבר, מהפכה בעניינים מודיעיניים, קהילת המודיעין, פרדיגמה, מעגל המודיעין

דודי סימן טוב הינו חוקר במכון למחקרי ביטחון לאומי. נעם אלון הוא מומחה בתחומי אסטרטגיה ומודיעין.

1 **תפיסת "מעגל המודיעין" הגדירה מספר שלבי יסוד המרכיבים את התהליך המודיעיני: איסוף ידיעות, עיבוד ידיעות (כלומר, מחקר) והפצת המודיעין המוגמר לצרכנים השונים. להרחבה בנושא זה ראו: דודי סימן טוב ועופר ג', "מודיעין 2.0 – גישה חדשה לעשיית מודיעין", צבא ואסטרטגיה, כרך 5, גיליון 3, דצמבר 2013, עמ' 27-29.**

מבוא

ההיסטוריה עשירה בדוגמאות של מעצמות, מדינות וצבאות שלא הצליחו לזהות פוטנציאל מהפכני של טכנולוגיה חדשה, וכתוצאה מכך איבדו את יתרונם ואת הרלוונטיות שלהם.[2] ההיסטוריה של חברות עסקיות עשירה בסיפורים דומים, שהובילו גם הם לנפילתן של חברות ענק ולעלייתן של חברות אחרות על פניהן.[3] היסטוריה זו מלמדת שזיהוי ואימוץ טכנולוגיות חדשות אינם מספיקים, שכן נדרשים שינויים תפיסתיים, תרבותיים, מבניים וערכיים שיאפשרו למצות את הפוטנציאל הטכנולוגי ולגבשו לכדי מהפכה היוצרת מרחב פעילות פרדיגמטי חדש.

מאמר זה מצביע על הפער שנוצר בין השינויים הטכנולוגיים המהותיים שהסייבר במובנו הרחב מאפשר, ובכלל זה גישות חדשות לייצור מידע וידע וגישות חדשות לגבי האינטראקציה של ארגונים מודיעיניים עם הסביבה ועם יעדיהם המודיעיניים, ובין האופן שבו מתַפקדים ארגוני המודיעין. אלה נותרו נטועים במידה רבה בתפיסות, בארכיטקטורה ובאתוסים שמקורם בפרדיגמת "מעגל המודיעין" שכוננה בין שתי מלחמות העולם. פער זה יוצר צורך בשינוי מערכתי ותפיסתי, אלא ששינוי זה מתעכב בשל היעדר תחושת משבר בקהילת המודיעין ובשיח הציבורי. זאת, בעיקר משום שהמודיעין ממשיך לתפקד ומציג הישגים טובים, במיוחד במישורים האופרטיבי והטקטי. סיבה נוספת להיעדר שינוי בפרדיגמה הקיימת היא שהמודיעין נתפס בציבור ובקרב רבים ממקבלי ההחלטות כ"קופסה שחורה", דבר המקשה על שיח ביקורתי שיניע שינוי מבחוץ.

פרדיגמת המודיעין הנוכחית: "מעגל המודיעין"

פרדיגמה היא תפיסת עולם הקובעת את הפרספקטיבה המושגית, וממנה נגזרים המבנה וההיגיון של התפקוד הבסיסי של רכיבי המערכת. הפרספקטיבה מבוססת על מוסכמה חברתית וארגונית שקובעת את יחסי הגומלין בין הגורמים השונים, וכן מסבירה ומפרשת את הסביבה שבה הפרט והארגון פועלים.[4] פרדיגמות מאותגרות ומשתנות באופן טבעי כשמתרבים הפערים בין הפירוש המקובל ובין התופעות שאותן הוא נועד לפרש, ואולם, כל שינוי כזה יוצר משבר בשל הקושי לאמץ פרספקטיבות חדשות ולזנוח את הישנות. ברגע שמתגבשת פרדיגמה חדשה,

---

2 מקס בוט, **חדשנות במלחמה: כלי נשק, לוחמים ויצירת העולם המודרני**, הוצאת מערכות, תל אביב, 2015.

3 דוגמאות מוכרות הן נפילתן של החברות "קודאק" ו"בלוקבסטר" בעקבות אי־הסתגלותן לעידן הדיגיטלי, ואיבוד הבכורה של חברת "בלקברי" כתוצאה מהקיבעון שלה סביב מבנה המכשיר הסלולרי.

4 תומס ס' קון, **המבנה של מהפכות מדעיות**, הוצאת ידיעות ספרים, תל אביב, 2005, עמ' 46־54; A. Levi, U. Merry, *Organizational Transformation: Approaches, Strategies, Theories* (Greenwood Publishing Group, 1986), pp. 10-14.

היא נושאת עימה מערכת מושגית של אמונות, ערכים ותפיסות, ואלה באים לידי ביטוי במבנים, בתהליכים, באתיקה ובגבולות המותר והאסור. דוגמאות בולטות לפרדיגמות שהשתנו הן המעבר מהתבססות על אמונה ומיתוסים לצורך בהוכחת דברים באמצעות ניסויים מדעיים, והמעבר מההנחה שכדור הארץ הוא מרכז היקום ושהוא שטוח להכרה במרכזיותה של השמש ולהיותו של כדור הארץ בעל צורה עגולה.[5]

בהקשר הצבאי מקובל להצביע על ה"מהפכה בעניינים צבאיים" (RMA) כמהפכה המרכזית של עידן המידע אשר שינתה מבחינה תפיסתית את האופן בו צבאות נלחמים.[6] בהקשר המודיעיני, המודיעין בעולם הישן נוהל ישירות על ידי מצביאים. כך היה משה בפרשת המרגלים בתנ"ך וכך היה גם נפוליאון. במסגרת פרדיגמה זאת, המודיעין התבסס על יחסי אמון בין המנהיג ובין המרגלים האנושיים אותם הפעיל. פרדיגמה חדשה התבססה בעידן התעשייתי, שהביא, בין היתר, להמצאתם של הטלגרף ושל מכשירי הקשר האלחוטיים. פרדיגמה זאת שמה במוקד את היכולת לאסוף אותות ולפענח אותם (ה"אניגמה", כמפעל המודיעיני המרכזי במלחמת העולם השנייה, היא דוגמה מייצגת לכך).[7] הפרדיגמה החדשה חייבה להקים ארגון מודיעיני מקצועי יותר, שלא יתבסס רק על קשר ישיר עם המצביא. כך התפתח מקצוע המודיעין ברמה המדינתית. הגידול המשמעותי בכמות האותות ובלוחמה האלקטרונית חייב את הקמתם של ארגוני מודיעין שעוסקים לא רק באיסוף ובפיצוח מידע, אלא גם בסידורו, בפרשנותו ובהנגשתו למקבלי ההחלטות. זו הפרדיגמה שלאורה הוקמו ארגוני מודיעין אסטרטגיים לאחר מלחמת העולם השנייה, שאחד מעקרונותיה המרכזיים הוא רעיון "מעגל המודיעין", כהיגיון מסדר של היחסים בין גופי האיסוף לגופי המחקר ובין ארגון המודיעין והקברניט.[8]

פרדיגמת "מעגל המודיעין", השולטת בכיפה במידה רבה עד היום, מבחינה בין הרכיבים השונים של המערכת המודיעינית ומגדירה את דפוסי הקשר ביניהם:

- בין צורות התפקוד השונות של המערכים בתוך ארגון המודיעין, ובייחוד בחלוקה היסודית בין יחידות ואנשי האיסוף ליחידות ואנשי המחקר.

---

5 להרחבה על משמעותה של פרדיגמה והשפעת שינויים בה על כלל אורחות החיים ראו: קון, **המבנה של מהפכות מדעיות**.

6 Deborah G. Barger, *Toward A Revolution in Intelligence Affairs* (RAND Corporation, Santa Monica, Ca., 2005).

7 David Kahn, *Seizing the Enigma: The Race to Break the German U-Boats Codes* (Houghton Mifflin Harcourt, 1991).

8 ההוגה המרכזי של רעיון "מעגל המודיעין" היה שרמן קנט, שעמד בראש גוף המחקר של ה־C.I.A, ועוד קודם לכן פיתח את תפיסת עולמו באקדמיה: Sherman Kent, *Strategic Intelligence for American World Policy* (New Jersey: Princeton University Press, 1949).

- בתוך מערך האיסוף היא יוצרת חלוקות משנה המבחינות בין צורות איסוף המידע השונות: איסוף אותות (סיגינט), איסוף מחומר גלוי (אוסינט), איסוף חזותי (ויזינט) ואיסוף אנושי (יומינט).
- מגדירה את דפוס הקשר בין הרכיבים השונים של הגוף המודיעיני ובינו לבין דרג מקבלי ההחלטות. קשר זה מאופיין בשאלות ותשובות ובהכוונה של המערכת המודיעינית על ידי הדרג האסטרטגי (צי"ח).[9]
- קובעת גבולות ברורים בין מושא המודיעין – מדינה אחרת או יריב המהווה מושא לפעילות המודיעינית – לבין המדינה בה מתפקדים אותם ארגוני מודיעין.[10]
- תפקידו המרכזי של המודיעין הוא לתת תשובות עובדתיות ולחשוף סודות על המציאות ב"צד השני של הגבעה", ובעיקר לספק התרעה.[11]

ניסיונות להתאמות כביטוי להתמודדות עם המציאות המשתנה

שליטתה של פרדיגמת "מעגל המודיעין" גם בימינו באה לידי ביטוי במבנה הארגוני, בחלוקה התפקודית, באתוסים ובלוגיקה שמושלת במעשה המודיעיני. ואולם, בשנים האחרונות החלה הסביבה המודיעינית לתפקד באופן שונה, שבמקרים רבים אינו עולה בקנה אחד עם עקרונות "מעגל המודיעין". כך נוצר מצב שבו, מצד אחד, הרכיבים המודיעיניים ויחסי הגומלין המוגדרים ביניהם ובין עצמם וביניהם לבין הסביבה החיצונית נותרו כשהיו, אך מצד שני החלו להופיע רכיבים ודפוסים חדשים ושונים המאתגרים את הפרדיגמה הקיימת. הדבר אופייני למצב שבו המערכת הפרדיגמטית נמצאת בשלב ביניים: היא אינה משנה את המערכת המושגית הבסיסית שמגדירה אותה, אולם בה בשעה היא נותנת ל"גידולי פרא" לגדול, תוך ניסיון לגדרם כך שלא יאתגרו את הזרם המרכזי.

למעשה, כבר לפני יותר מעשור הופיעו בשיח המודיעיני בעולם קריאות לבצע "מהפכה בעניינים מודיעיניים". ברקע לקריאות אלו עמדה טענה מרכזית, לפיה הכישלונות הגדולים של ארגוני המודיעין בעשורים האחרונים נבעו מהִשתנות

---

9 שם.

10 לתיאור ממקור ראשון של הפרדיגמה ויישומה במקרה הישראלי ראו: יהושפט הרכבי, **המודיעין כמוסד ממלכתי**, הוצאת מערכות, תל אביב, 2015. ערב הקמתה של מדינת ישראל, ובהיעדר גבולות מוגדרים, נהגו אנשי הש"י (שירות הידיעות – ארגון המודיעין של היישוב) לנסוע באופן תדיר לבירותיהן של מדינות ערב בכדי למצוא שם מענה לשאלות שהטרידו את ראשי היישוב. הם גם ראו במודיעין "גשר לשלום". משימה זו נעלמה לאחר הקמת המדינה, ובמקומה הופיעה המשימה הראשית של פיתוח ידע על יריבים והסביבה האסטרטגית והתרעה למלחמה כביטוי ראשי לכך.

11 Joseph S. Ney, "Peering into the Future", *Foreign Affairs*, Vol. 73, No. 4 (August 1994): 82-93.

הסביבה האסטרטגית ומהשינוי באופי האתגרים והאיומים.[12] מחקר מקיף שבוצע במכון RAND בראשית האלף הנוכחי הביע חשש כי המהלכים שבוצעו לאחר המשבר במודיעין האמריקאי, בעקבות כישלונו באירועי הטרור של ספטמבר 2001 ובמתן ההערכה השגויה לגבי הנשק בלתי קונבנציונלי של עיראק, הם רפורמות בלבד בפרדיגמה המודיעינית הישנה ואינם מספיקים כדי להביא לשינוי של ממש בתפקוד קהילת המודיעין.[13] המהלכים שננקטו בארצות הברית כללו, כידוע, הקמת ארגון־על שאמור לקבוע את האסטרטגיה המודיעינית ולכוון את קהילת המודיעין האמריקאית (מנהל המודיעין הלאומי – DNI), וכן הקמת גופים משולבים למחקר. כמו כן הוחל בעידודו של שיתוף מידע בין ארגוני המודיעין השונים.[14]

ניסיונות לשפר את התפקוד המודיעיני נעשו גם בקהילת המודיעין הישראלית, בין היתר באמצעות שימוש ברעיונות מערכתיים חדשים, שכללו שינויים מבניים ותפקודיים. כאלה, למשל, היו תהליכי שינוי ארגוניים שהובילו ראשי אמ"ן, ובהם תהליך "הרעיון המכונן" בהובלת אלוף אהרון זאבי (פרקש) ו"מעשה אמ"ן" בהובלת האלוף אביב כוכבי.[15] התהליך שהוביל אלוף זאבי כלל הקמת פורומים מודיעיניים משותפים, בהובלה של ראש זירה בחטיבת המחקר, לצורך עיצוב "מערכה מודיעינית". תהליך זה גווע לאחר שנים ספורות. בין השינויים שהוביל האלוף כוכבי הייתה הקמת רשת מודיעינית חברתית (שכונתה "טרייסובק" ואשר מערכת "פייסבוק"

---

12 David T. Moore, "Sensemaking: A Structure for an Intelligence Revolution", *Dissertation for National Defense Intelligence College*, March 2011; Russell E. Travers, "Waking Up on another September 12th: Implications for Intelligence Reform", *Intelligence and National Security*, Vol. 31, No. 5 (2016): 746-761.

13 Barger, *Toward a Revolution in Intelligence Affairs*; Gregory F. Treverton and Peter A. Wilson, "True Intelligence Reform Is Cultural, Not Just Organizational Chart Shift", *The RAND Blog*, January 13, 2005.

14 Gordon Nathaniel Lederman, "Restructuring the Intelligence Community", in *The Future of American Intelligence*, ed. Peter Berkowitz (Hoover Press, 2005), pp. 65-102.
ראסל טרוורס, במאמרו "Waking Up on another September 12th: Implications for Intelligence Reform", מבקש להרחיב מגמה זו כדי שתכיל את כל קהילת המודיעין האמריקאית. לגישתו, יש שלושה מהלכים משמעותיים שצריכים להתבצע: להכפיף את כל הסוכנויות המודיעיניות של ארצות הברית למנהל מודיעין אחד בעל אחריות וסמכות מלאות; להקים מעל סוכנויות המודיעין הקיימות צוותי משימה על־ארגוניים שיטפלו בכול האתגרים הלאומיים; לאפשר זרימה חופשית יחסית של מידע וידע בין הסוכנויות השונות ובינן לבין צוותי המשימה העל־ארגוניים.

15 אביב כוכבי וערן אורטל, "מעשה אמ"ן – שינוי קבוע במציאות משתנה", **בין הקטבים**, מרכז דדו, גיליון מס' 2, 2014; אהרון זאבי פרקש, דוב תמרי, **ואיך נדע**, הוצאת ידיעות אחרונות, 2011; נעמי פסה יוסף ושרית שפירא, "גשר על פני מים סוערים – המסע של אמ"ן בעידן המורכבות", **מודיעין הלכה ומעשה**, גיליון 2, המרכז למורשת המודיעין, 2017; חגי הוברמן, "ראש השב"כ: להתאים הערכותנו למציאות המשתנה", 15 במאי 2011, *www.inn.co.il*.

היוותה מקור השראה שלה), אולם מעדותם של אנשי מודיעין בתוך המערכת המודיעינית כיום עולה כי הרשת מממשת רק מקצת מהפוטנציאל שלה וכי השיח המודיעיני בה מוגבל. הקמת חטיבת ההפעלה על ידי ראש אמ"ן אלוף עמוס ידלין נועדה לשפר את היכולת של אגף המודיעין לעסוק בסוגיות אופרטיביות וכן לשפר את התפקוד המשותף של גורמי האיסוף והמחקר.[16] לעומת זאת, הניסיונות לגבש באמ"ן צוותים משימתיים משולבים לאורך זמן נתקלו בקשיים ובמתח מתמיד מול מערכי האיסוף. בשיח המודיעיני בישראל עלה גם הרעיון של יצירת מרחבים משותפים לייצור ידע מודיעיני והצורך לפרוץ את "מעגל המודיעין" באמצעות מיצוי יכולות טכנולוגיות חדשות כדי לשפר את תפקוד המודיעין ולאפשר לו להתמודד ביתר קלות עם האתגרים החדשים בסביבה. רעיונות אלה טרם מומשו במלואם, וכתוצאה מכך, פיתוחו של רוב הידע המודיעיני ממשיך להתבצע בכול ארגון מחקר בנפרד.[17]

בשנים האחרונות הועלו טענות נוספות נגד האופן בו מתפקדת קהילת המודיעין והודגש הצורך בשינוי מערכתי שלה. למשל, יש המצביעים על כך שעידן המידע וה"ביג דאטה" מחייב את ארגוני המודיעין לבצע התאמות מערכתיות שאינן מתיישבות עם המבנה והתפקוד הנוכחיים שלהם.[18] אחרים קוראים לשינוי בתחום האיסוף המודיעיני, בין השאר על ידי מתן ביטוי לרעיון של מודיעין מרובה מקורות (All-Source Intelligence).[19] בנוסף לכך גברה ההכרה בעליית חשיבותו של המודיעין הגלוי ובצורך להקים מרכזים מודיעיניים חדשים שיתמחו בתחום זה.[20] כן גוברת הקריאה להקמת מרכזים מודיעיניים להתכת מידע ממקורות מרובים.[21]

חוקר המודיעין ויליאם להנמן קרא לשינוי פרדיגמטי בקהילת המודיעין האמריקאית, הן בשל השינוי בנגישות למידע והן בשל השינוי באופי האיומים (עלייתו של האיום העל־מדינתי והתת־מדינתי). לגישתו, נדרשים שינויים ארגוניים,

16 עמיר רפפורט, "טלטלה מודיעינית", *Israel Defense*, מארס 2014.

17 סימן טוב ועופר ג', "מודיעין 2.0 – גישה חדשה לעשיית מודיעין", עמ' 27–42.

18 Kevjn Lim, "Big Data and Strategic Intelligence", *Intelligence and National Security*, Vol. 31, No. 4 (2016): 619-635.

19 Roberto Mugavero, "Challenges of Multi-Source Data and Information New Era", *Journal of Information Privacy and Security*, Vol. 11 (2015): 230-242.

20 Hamilton Bean, *No More Secrets: Open Source Information and the Reshaping of U.S. Intelligence* (Santa Barbara: Praeger, 2011); Michael Glassman and Min Ju Kang, "Intelligence in the Internet Age: The Emergence and Evolution of Open Source Intelligence (OSINT)", *Computers in Human Behavior*, Vol. 28 (March 2012): 673-682; "The DNI's Open Source Center: An Organizational Communication Perspective", *www.collectionservice.info*.

21 Christopher G. Pernin, Louis R. Moore and Katherine Comanor, *The Knowledge Matrix Approach to Intelligence Fusion* (RAND Corporation, Santa Monica, Ca., 2007).

תפיסתיים ותהליכיים, אשר ישקפו תפיסה יותר מבוזרת ופחות ממודרת, ובכך יוכלו לסייע לפיתוח גמישות אל מול המציאות המִשתנה.[22] להנמן מנה במחקר מקיף שערך את הסיבות לכך שלא די ברפורמות שבוצעו בקהילת המודיעין האמריקאית לאחר פיגועי ספטמבר 2001, וטען כי הן היו שינויים אבולוציוניים בלבד וכי גופי המודיעין של ארצות הברית המשיכו גם לאחר מכן לפעול לפי הפרדיגמה המסורתית מעידן המלחמה הקרה. לשיטתו, נדרש שינוי מודיעיני מערכתי לאור השתנות אופיים של האיומים ונוכח ההזדמנויות שנוצרו משילוב כוחות ושיתוף ידע עם הסביבה האזרחית. להנמן הציע לקיים במקביל שתי פרדיגמות: האחת, המסורתית, שתתמקד בפתרון חידות ("פאזלים") באמצעות מקורות חשאיים ומסווגים; השנייה, חדשה, שתתמודד עם מגמות גלובליות ואיומים חדשים המאתגרים הן את קהילת המודיעין והן ארגונים אזרחיים מדינתיים וגלובליים, וכמו כן תשתף פעולה עם גורמים עסקיים פרטיים באמצעות תפיסה חדשה של זרימת מידע. לצורך בשיתוף גורמים אזרחיים גלובליים במידע מודיעיני התייחס גם רוברט סטיל.[23]

הסייבר פורץ את גבולות הפרדיגמה

הטענה במאמר זה היא כי למרות ההצלחה החלקית של הניסיונות שתוארו לעיל ובחלוף יותר מעשור הבשילו כיום התנאים לבצע מהפכה של ממש באופן בו בנויות ופועלות קהילות המודיעין בעולם וביחסים בינן לבין הסביבה הלא מודיעינית. מה שמאפשר מהפכה כזאת, ולמעשה מחייב אותה, הוא הסייבר במובנו הרחב, שהינו "החלק החסר" ברעיונות שהועלו בעבר.[24]

הסייבר כולל את המרחב הפיזי והלא פיזי שנוצר מהגורמים הבאים – מחשבים, מערכות ממוכנות ורשתות, תוכנות, מידע ממוחשב, תוכן והמשתמשים עצמם.[25] מדובר בתופעה אנושית טכנולוגית ותרבותית שהתהוותה לפני יותר מעשור. הסייבר הוא מרחב מלאכותי (בניגוד לים, לאוויר וליבשה), והתקשורת בין רכיביו

22 William J. Lahneman, *Keeping U.S. Intelligence Effective: The Need for a Revolution in Intelligence Affairs* (Lanham: The Scarecrow Press, 2011); William J. Lahneman, "The Need for a New Intelligence Paradigm", *International Journal of Intelligence and Counter Intelligence*, Vol. 23 (2010): 201-225.

23 Robert Steele, "Foreign Liaison and Intelligence Reforms: Still in Denial", *International Journal of Intelligence and Counterintelligence*, Vol. 20, no.1 (2007): 167.

24 "מלחמת מידע היא יותר מאשר לוחמה מבוססת מידע – ביטוי המייצג, אמנם, שימוש משמעותי במידע או בסייבר לשם לחימה, אך אינו מכיל את המשמעות הטוטאלית שלו. לוחמת סייבר [צריכה להיתפס] כעניין אסטרטגי לצורך השגת מטרות אסטרטגיות, ובהתאם להגדרתו של לוטוואק את המלחמה האסטרטגית, להקיף את כלל רמות הפעולה – החל מרמת האסטרטגיה רבתי וכלה ברמה הטקטית". הציטוט לקוח מתוך: Amit Sharma, "Cyber Wars: A Paradigm Shift from Means to Ends", *Strategic Analysis*, Vol. 34 (February 2010): 62-73. (תרגום על ידי המחברים).

25 ההגדרה מתוך מסמך ארגון התקשורת העולמי – *ITU Cybersecurity Gateway*.

מתבצעת באמצעות "ביטים". הדבר מאפשר ליצור חיבורים ומרחבים משותפים בין דיסציפלינות מודיעיניות, שבעבר היו נפרדות ואשר הדרך היחידה לחבר ביניהן הייתה במוחו של האדם.

הסייבר, כסביבה מודיעינית חדשה, משנה הנחות יסוד בתחום המידע והידע. כמות המידע הזמין לאיש המודיעין, בין אם הוא נמנה על יחידות המחקר או על יחידות האיסוף, שמה לאל כל ניסיון לדעת כמה מידע קיים בנושא מסוים, מהו החלק היחסי של המידע שבידינו מתוך סך המידע הקיים, והאם אנו מחזיקים בכול המידע הרלוונטי.[26] יתרה מכך, ארגוני המודיעין אינם מסוגלים למצות את מרבית המידע שברשותם, בין אם בשל הצפת מידע וידע מחיישנים ובין אם בשל הקושי להתמודד עם מאגרי מידע מסווגים ובלתי מסווגים אליהם הם נגישים. מצב עניינים זה מטיל צל כבד על היכולת לשמר את הרעיון הבסיסי העומד ביסוד הארכיטקטורה והתפקוד של המודיעין בעידן "מעגל המודיעין", שבמרכזו היכולת לסנן מידע עד למציאת "ידיעת הזהב" או שורה של פרטי מידע מוגבלים המעידים, לכאורה באופן אובייקטיבי ומבוסס נתונים, על המציאות המתפתחת בצד השני.[27]

כאמור, בעידן הנוכחי יש לאנשי המודיעין נגישות פוטנציאלית כמעט אין סופית למידע, אולם בפועל, מרבית אנשי המחקר בחלק גדול מארגוני המודיעין ממשיכים לפעול לפי פרקטיקות מסורתיות ו"לרוקן תורים", כלומר לקרוא את הידיעות המודיעיניות לפי סדר אקראי למדי המבוסס על תעדוף של אנשי האיסוף. גם הקמת "רשת מודיעינית חברתית",[28] שסימלה גישה חדשה לעשיית מודיעין, לא שינתה, לפחות לא באמ"ן, את ההרגלים הישנים ולא יצרה צורה אחרת של צריכת מידע או של פיתוח ידע. כך, בעוד שאנשי המחקר המודיעיניי בסביבה האזרחית צורכים ומפתחים ידע בהתאם לתרבות הדיגיטלית ו"העולם הפתוח",[29] כאשר הם שוהים במערכת המודיעינית המסווגת הם חוזרים לצרוך מידע ולפתח ידע כאילו הם בשנות התשעים של המאה הקודמת – באופן "תורי" וטורי, בהתאם ל"מעגל המודיעין".

---

26 Barger, *Toward a Revolution in Intelligence Affairs*; Michael Warner, "Intelligence in Cyber and Cyber in Intelligence", in *Understanding Cyber Conflict: 14 Analogies*, eds. George Perkovich and Ariel E. Levite (Washington, DC: Georgetown University Press, 2017), pp. 17-31.

27 Bruce Berkowitz, "The Big Difference Between Intelligence and Evidence", *The RAND Blog*, February 2003.

28 כוכבי ואורטל, "מעשה אמ"ן – שינוי קבוע במציאות משתנה".

29 מחקרים מראים שדור המילניום יוצר את המגע הראשוני שלו עם מידע חדשותי באמצעות הרשתות החברתיות, ורק אם הוא מגלה עניין בנושא מסוים הוא פונה להרחבה באמצעות ערוצי חדשות מסודרים. ראו לדוגמה: Roy Greenslade, "How the Different Generations Consume their Daily News", *The Guardian*, July 22, 2015.

המגבלה הראשית הבולמת השתנות היא תפיסתית ולא טכנולוגית, שכן רעיונות על "ווביניט לכול חוקר", הבנה כי יש לאפשר לו נגישות לאינטרנט ולמאגרי המידע המסווגים, ומערכות טכנולוגיות שמאפשרות זאת, הופיעו בקהילת המודיעין בישראל כבר בראשית שנות האלפיים. המגבלה התפיסתית גורמת לכך שחוקרי המודיעין אינם ממצים את הפוטנציאל הכמעט אין סופי שכול חוקר אחר שאינו מודיעיני (באקדמיה או בעולם העסקים) נהנה ממנו.

הסייבר מאפשר, כאמור, ליצור מרחב מודיעיני משותף. החלוקה מן העבר בין מערכי האיסוף, שהתבססה על אורכי גל ומאפייני הפקה שונים, מתחלפת במהירות במרחב דיגיטלי משותף המבוסס על ביטים. למעשה, איש האיסוף החדש הינו טכנולוג, ושאר תפקידני המודיעין, בין אם בקטגוריית האיסוף ובין אם בקטגוריית המחקר, מבצעים פעולות מחקריות ברמות ובאיכות שונות ולצרכים שונים. הבעיה המרכזית של המודיעין בעידן הסייבר אינה עוד מציאת המידע "הנכון" והפקתו לצורך גילוי ה"סוד", אלא שאילת השאלה הנכונה, היוצרת ידע חדש[30] ועוסקת בהגדרות וביצירת קטגוריות תפיסתיות חדשות.[31] משימה זו אינה עוד נחלתו של החוקר בלבד, כשם שהיכולת לאתר מידע רלוונטי ולהפיקו אינה עוד נחלתו של האוסף בלבד. הן האוסף המודיעיני והן החוקר המודיעיני חולקים כיום ידע בסיסי משותף ויכולות חיפוש, איתור ועיבוד מידע משותפות.

הסייבר מייצר מרחב משותף עם היריב בעוד ש"מעגל המודיעין" נשען, במידה רבה, על הגבולות הגיאוגרפיים בינינו לבין יריבינו.[32] גבולות אלה אפשרו ליצור הפרדה תפיסתית ותפקודית בין מחקר, איסוף, פעולה חשאית התקפית וביטחון מסכל. ואולם, ההפרדות הללו הן מלאכותיות ומיותרות בעידן הסייבר. פעולה "איסופית", הכוללת הבאת מאגר מידע, אינה שונה במהותה מפעולה חשאית התקפית בסייבר.[33] עצם פעולת חיפוש המידע יוצרת עקבות ושינויים במרחב הרשתי עצמו. שינויים אלה משפיעים באופן ישיר הן על היריב והן על הצד של מבצע הפעולה, כמו גם על אזרחים, מדינות יריבות אחרות ומדינות ידידות. חוקר אינו נדרש עוד (וגם אינו יכול) להגביל עצמו לקריאה פסיבית של מידע ברשת. כניסתו לפורומים מחייבת אותו להניח שהוא שותף ונראה, גם אם הוא משתמש בזהות

30 א"ה, "האם המחקר המודיעיני צריך להשתנות וכיצד?", **מודיעין הלכה ומעשה**, גיליון 2, המרכז למורשת המודיעין, 2017.

31 איתי ברון, **המחקר המודיעיני: בירור המציאות בעידן של תמורות ושינויים**, הוצאת המרכז למורשת המודיעין, 2015, עמ' 58-59. להרחבה על יצירת קטגוריות חדשות וחשיבותן להבנת המציאות ראו: צבי לניר, **ליצור קטגוריות חדשות בעולם**, מכון "פרקסיס", 2008.

32 Robert D. Williams, "(Spy) Game Change: Cyber Networks, Intelligence Collection and Covert Action", *The George Washington Law Review*, Vol. 79 (2010): 1162-1200.

33 הבנות אלו הובילו למחשבות בארצות הברית לאחד את פיקוד הסייבר עם סוכנות הביטחון הלאומי (NSA). ראו לדוגמה: Jason Healey, "Shaking Up the Top of Cyber Command", *The CIPHER Brief*, October 22, 2017.

בדויה. מגמה זו מאתגרת מאוד את היכולת להפריד בין התפקודים המודיעיניים הפסיביים והאקטיביים, מחייבת לתת לחוקר כלים מתקדמים לניהול זהויות ברשת ומאפשרת לו להיות שותף פעיל ליצירה ולצריכה של ידע ברשת הגלויה.

הסייבר מאיץ את קצב ההשתנות של הסביבה: קצב תחלופת הטכנולוגיה, הקלות שבהפצתה ומחיריה הנמוכים יוצרים תשתית להִשתנות מתמדת של האויבים, היריבים, הידידים, הזירה המודיעינית הפנימית והסביבה האזרחית והעסקית כאחת. ההזנה ההדדית של כלל השינויים הללו יוצרת מציאות של תנועה מתמדת ושינוי מהיר, שפעמים רבות מתרחש באופן שאינו צפוי ואינו ליניארי. קצב השינויים הזה מאתגר מאוד שני תפקודים בסיסיים של "מעגל המודיעין": ראשית, הוא מקשה על היכולת לדעת מהי השאלה הנכונה, ומכאן גם על היכולת לשמר את ה"מנוע" של "מעגל המודיעין" – שאלות ברורות ומתועדפות של צד אחד (מקבל החלטות או חוקר) ותשובות ברורות ומתועדפות של צד שני (חוקר או אוסף); שנית, הוא מאתגר מאוד את היכולת לשמר "תו תקן" שלם של מוצר מודיעיני, שכן התהליך הסדור והטורי של ייצור ידיעה, בניית תמונת מודיעין יציבה והפצתה הינו ארוך וחורג פעמים רבות מגבולות הזמן של האירועים המהירים. בנוסף, הסייבר משנה את מאפייני המומחיות הנדרשת מאנשי המודיעין: אם בעבר איש המודיעין נדרש למומחיות בתחום המחקר בו עסק, הרי שבעידן הסייבר החוקר נדרש, בנוסף למומחיות דיסציפלינרית זו, גם להיכרות מעמיקה עם טכנולוגיות מידע, שפות ויכולות מתחום המידענות, היכרות עמוקה עם רשתות, סטטיסטיקה ועוד.

הסייבר והמודיעין: משבר פרדיגמטי

בשני החלקים הקודמים הוצגו השינויים שארגוני המודיעין ביצעו כדי לנסות לשמר את הפרדיגמה הנוכחית של "מעגל המודיעין". להלן יוצגו מספר ביטויים המאפיינים את חוסר ההתאמה של פעולת המודיעין לעידן הסייבר, חרף אותם שינויים.

כאמור, "מעגל המודיעין" מחלק את המפעל המודיעיני ליחידות איסוף ולגוף מחקר מרכזי. אולם, למרות שמרבית יחידות האיסוף עוסקות בעידן הסייבר ב"ביטים" ובחיבור ביניהם עוד לפני הגעת התוצר הלא מעובד לחוקר, הן ממשיכות לעשות את עבודתן באופן נפרד האחת מהשנייה, והחיבור ביניהן, אם מתרחש, מבוצע באופן מכני או כפוי ולא כזה המבטל חציצות והופך ל"טבעי".[34] מושגי ביניים שנוצרו בשנים האחרונות, כמו "יומינט קיברנטי" (יצירת ישויות אנושיות וירטואליות) ו"יוגינט" (חיבור של יומינט וסיגינט), או הצבה של אנשי יחידת הוויזינט ביחידת

34 להרחבה ראו: סא"ל א', "מודיעין גיאוגרפי – ממפת הנייר לגיאו־רשת", בתוך: שמואל אבן ודוד סימן טוב (עורכים), **אתגרי קהילת המודיעין בישראל**, המכון למחקרי ביטחון לאומי, תל אביב, 2017; אבי טל ודוד סימן טוב, "יומינט בעידן הקיברנטי – משחקים בין עולמות", **צבא ואסטרטגיה**, כרך 7, גיליון 3, דצמבר 2015.

הסיגינט, ולהפך, לצורך מיצוי תחום הסייבר הגיאוגרפי,[35] מלמדים על מורכבות המצב הנוכחי ועל ההכרח לבחון מחדש האם הארכיטקטורה האיסופית הקיימת עודנה תקפה.

היווצרות סדקים בחומות התפיסתיות ערערה את ה"חומה" בין המודיעין לצרכניו. ואמנם, כבר לפני כעשור קרא מפקד יחידה 8200 דאז "לשבור את החומות" בין יחידתו – יחידת האיסוף המובילה של חיל המודיעין – ובין גורמי המחקר.[36] למרות זאת, הארכיטקטורה של קהילת המודיעין, הן בישראל והן בעולם, נותרה כשהייתה, והחומות הארגוניות והפוליטיות ממשיכות לקבוע את קצב השינויים ובולמות למעשה יוזמות לשינויים עמוקים.

תהליך ייצור הידיעה המודיעינית בעבר התבסס על מומחיות הפרט – המתחקר ביומינט, המתרגם או איש הבינה הרשתית בסיגינט והחוקר המומחה לאותו תחום. כיום רווחת בקהילות המודיעין בעולם ההבנה כי יש צורך לשתף פעולה באופן החורג לעיתים משיחות טלפון או מהעברת מיילים. כתוצאה מכך, נוצרים גופי אד הוק הנשענים על עבודת צוות החוצה ארגונים, אלא שחלק ניכר מהם קמים מראש כהתארגנויות זמניות ונסגרים עד מהרה משהושגה המשימה. ניתן אמנם להצביע גם על ניסיונות מהפכניים, כמו זה של ראש ה־C.I.A. לשעבר, אשר הקים גופים משימתיים במקום האגפים המקצועיים של הארגון.[37] אולם ניתן לקבוע, ככלל, שהארכיטקטורה הבסיסית של חלוקה בין ארגוני האיסוף לארגוני המחקר ובין ארגוני האיסוף לבין עצמם מונעת הקמת ארגונים משולבים קבועים שיכללו גם נציגים מחוץ לקהילת המודיעין. מצב זה יוצר תסכול רב בקרב מי שמנסים להקים ארגונים כאלה.

מרחב נוסף העומד במרכז השיח הוא אופי הקשר בין גורמי המחקר בקהילות המודיעין. בין השאר מדובר בהקמת ארגונים שישלבו נציגים מכול גופי המחקר של קהילת המודיעין,[38] וכן בקריאה, בישראל כמו בארצות הברית, להקים מרחב מחקרי משותף. באמצע העשור הראשון של המאה הנוכחית הופיעה לראשונה באמ"ן קריאה להקמת "ויקיפדיה מודיעינית". קריאות דומות הופיעו גם בקהילת

35 סא"ל א', "גוף טקטי כמחולל שינוי במערך השטח", **מודיעין הלכה ומעשה**, גיליון 2, המרכז למורשת המודיעין, 2017.

36 סימן טוב ועופר ג', "מודיעין 2.0 – גישה חדשה לעשיית מודיעין".

37 דוד שטרנברג, "על השינוי ב־CIA: שילוביות משימתית כרעיון ארגוני מסדר", **מודיעין הלכה ומעשה**, גיליון 1, המרכז למורשת המודיעין, 2016.

38 על מושג השילוביות ויישומו במערכות צבאיות, מודיעיניות ואזרחיות ראו: קובי מיכאל ודוד סימן טוב, "שילוביות בארגוני מודיעין – משמעויות תיאורטיות במבחן המעשה," **סייבר, מודיעין וביטחון**, כרך 1, גיליון 1, ינואר 2017.

המודיעין האמריקאית.[39] למרות זאת, גופי המחקר השונים בשתי הקהילות ממשיכים עד היום לפתח את הידע שלהם בנפרד.

מגמה אחרת בשיח היא הקריאה להפיק תוצר מודיעיני משותף במסגרת מה שמכונה Living Intelligence. הרעיון היה שכול גורם מודיעיני יוכל לעדכן את התוצר ולחסוך את שרשרת התיאומים והכפילויות הבלתי נגמרת.[40] לפי שיטה זו, הצרכן אמור היה לקבל תוצר אינטגרטיבי "נושם" המתעדכן באופן שוטף ובזמן קצר בהרבה מהמקובל כיום. למעשה, מרבית הרעיונות האלה נותרו ללא יישום ממשי וכנראה הקדימו את זמנם, שכן המסורות ודפוסי העבודה הקבועים של קהילות המודיעין עצרו את רובם.

אחד התחומים שבהם מורגש ונדון מזה תקופה ארוכה הצורך בשינוי יסודי הוא המודיעין הגלוי.[41] בתחום זה הולכת ומתגבשת הסכמה רחבה שאין מדובר עוד בדיסציפלינה איסופית גרידא. כתוצאה מכך מתקיים ויכוח על מיקומו הארגוני של המודיעין הגלוי, כשעל הפרק עומדות בדרך כלל שתי אפשרויות: האחת, למקם אותו במרחב האיסופי; השנייה, לשלב אותו במרחב המחקרי. קיים קושי מעשי לבצע שינויים אלה. כך, השארת היחידה במרחב האיסופי, לפחות בישראל, יוצרת לא מעט אנומליות: החוקרים ממצים את המידע בצורה מהירה לכדי תוצרים מחקריים עוד לפני שהוא עובד והופץ על ידי יחידת האיסוף; מאגרי המידע הזמינים ברשת נחקרים עוד בטרם קוטלגו על ידי יחידת האיסוף; תוצרים מחקריים ואיסופיים אזרחיים ועסקיים רלוונטיים אינם ממוצים בשל חוסר רצון לבסס מערכת יחסים הדדית ברשת.[42]

הרושם העולה מניתוח המגמות הוא שקיימים ניצנים של שינוי, אך לצידם גם בלמים וחסמים – רובם ארגוניים ותפיסתיים. ניתן להצביע על ממדים פוטנציאליים

---

39 D. Calvin Andrus, "The Wiki and the Blog: Toward a Complex Adaptive Intelligence Community", *Studies in Intelligence* 49, no. 3 (September 2005): 63-70, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=755904.

40 David Schroer, "Efficacy and adoption of central web 2.0 and social software tools in U.S. intelligence community" (Thesis dissertation), www.amu.apus.edu (March 2011).

41 Hamilton Bean, "The DNI's Open Source Center: An Organizational Communication Perspective", *International Journal of Intelligence and Counterintelligence*, Vol. 20, No. 2 (February 2007): 240-257; Robert David Steele, "The Open Source Program: Missing in Action", *International Journal of Intelligence and Counterintelligence*, Vol. 21, No. 3 (May 2008): 609-619.

42 דוגמה מעניינת למיצוי הרשת הגלויה כמרחב ללמידה ולא רק כמרחב לאיסוף מידע ניתן למצוא בפרסומים העיתיים של מועצת המודיעין הלאומי האמריקאית (NIC) *Global Trends* ושל הגוף הבריטי לגיבוש מגמות אסטרטגיות גלובליות (STP) *Global Strategic Trends*. גופים אלה משתפים פעולה ומתייעצים עם מומחים ועם הציבור הרחב בפורומים יעודיים, כחלק מתהליך הכנת הדוחות שלהם.

של שינוי כמעט בכול תחום מודיעיני, אך בסופו של דבר השינוי בפועל הינו מוגבל בהיקפו. טענתנו הנובעת מכך היא כי ללא שינוי פרדיגמטי לא יחול שינוי מהותי ברבדים השונים של התפקוד המודיעיני הפנימי והחיצוני, וכי המודיעין, בתור גוף האמון בראש ובראשונה על פיתוח ידע, יחמיץ את המהפכה המתחוללת בנושא זה במרחב האזרחי.

בין הגורמים שבולמים את השינוי ניתן להצביע, כאמור, על מסורות ארגוניות ועל תפיסות פעולה שקשה להשתחרר מהן, וכן על מאבקים על יוקרה ומשאבים ששינוי דרמטי כזה עשוי לעורר.[43] בנוסף, יש רבים שיכולים לטעון כי עדיפה הדרך ההדרגתית אותה נוקט המודיעין כיום, שאינה מסכנת את הנכסים הקיימים. סיבה מרכזית נוספת שמקשה על שינוי היא היעדר תפיסת משבר, הן בראייה חיצונית והן בראייה פנימית. כפי שהוצג קודם לכן, השינוי בקהילת המודיעין האמריקאית אירע לאחר המשבר של אירועי הטרור בארצות הברית בספטמבר 2001 והמשבר בעיראק ב־2003. בישראל חלו שינויים משמעותיים בקהילת המודיעין בעקבות דוח ועדת אגרנט לאחר מלחמת יום הכיפורים. היעדר תודעת משבר, לצד תפיסת המודיעין כמוצלח, בעיקר עקב הצטיינותו במודיעין אופרטיבי וטקטי ונוכח הצלחותיו של האיסוף הקיברנטי, מהווים חסמים קשוחים המקשים על השינוי הנדרש.

קווים לדמותה של פרדיגמה חדשה: מהפכה קיברנטית בענייני מודיעין

אנו מצויים כיום בשלב מעבר מפרדיגמה ישנה, שהיכולת לשמרה הולכת ומאותגרת, לפרדיגמה חדשה שעדיין לא עוצבה, אך ניצנים ראשונים של מאפייניה כבר מיושמים בשטח. בחלק זה ננסה להתוות מספר עקרונות של הפרדיגמה החדשה, שנקרא לה "מהפכה קיברנטית בענייני מודיעין" (Cybernetic Revolution in Intelligence Affairs –CRIA).

מערכת פתוחה בשינוי מתמיד

איתי ברון, לשעבר ראש חטיבת המחקר באמ"ן, נהג להדגיש שהמודיעין, ובייחוד המחקר המודיעיני, מצויים בחזית ההתמודדות עם חוסר הוודאות הנובע מהִשתנות המציאות.[44] מציאות זו, של שינוי מתמיד ומואץ, מחייבת את קהילת המודיעין לפתח גישה ומבנה פתוחים:

- תרבות המעודדת זרימה מהירה של מידע וידע בתוך המרחב המודיעיני ובין המרחב המודיעיני למרחב האזרחי. המחקרים מראים שככול שהארגון מאורגן

43 לדיון בסוגיית מאבקי היוקרה והפוליטיקה הארגונית, כמו גם להיעדרה של תחושת משבר בקהילת המודיעין, ראו: מיכאל וסימן טוב, "שילוביות בארגוני מודיעין".

44 ברון, **המחקר המודיעיני: בירור המציאות בעידן של תמורות ושינויים**, עמ' 11–18.

באופן פחות פורמלי, פחות הירכי ופחות צנטרליסטי ויותר מבוזר, גמיש ומאציל סמכויות לדרגים נמוכים, כך משתפרות יכולת ההתמודדות שלו עם שינויים מהירים בסביבה, יכולת ההתאמה שלו ויכולתו למצוא פתרון לבעיות מורכבות.[45]

- מבנים משימתיים עצמאיים – הארכיטקטורה הבסיסית של קהילת המודיעין צריכה לעבור ממבנה אורכי, המבוסס על יחידות עצמאיות שאחראיות על כלל המשימות שבתחומן והקשרים שביניהן, למבנה מטריציוני שיהיה מבוסס על מבנים רב־דיסציפלינריים האחראים על בעיה מסוימת. בנוסף לכך, מבנים משימתיים אלה צריכים לקבל חופש פעולה מרבי להשגת צורכיהם, וזאת באמצעות פיתוח קשרים עם מבנים משימתיים אחרים ויכולת לפתוח מבנים משימתיים נקודתיים לתת־משימות נדרשות. בהתאם לכך, צריך לתת למבנים משימתיים אלה חופש פעולה יחסי לבחירת המשימה והדרך להשיגה. קיימות שתי מגבלות עיקריות למבנה כזה: הראשונה קשורה בצורך של ראשי הארגון ודרגי הביניים לנהל אותו באופן ריכוזי. לעניין זה יש לפתח תרבות ניהול מטריציונית;[46] המגבלה השנייה קשורה לבניין כוח שיזין אותם מבנים משימתיים ויאפשר את המשך פיתוח דיסציפלינות היסוד. מערכי האיסוף החדשים שיתמקדו בבניין הכוח יכולים לאחד מספר תחומים, כגון איסוף חזותי וסיגינטי או מבצעים מיוחדים ויומינט. שינוי כזה יכול לאפשר גם יצירת מרחבים משותפים משמעותיים בין ארגוני מודיעין שונים בקהילת המודיעין לטובת בניין הכוח.[47]
- שותפות עם המרחב האזרחי, העסקי והאקדמי – שותפות זו צריכה להישען על שיח פתוח והזנה הדדית של מידע, תובנות והערכות. הקשר בין המרחב המודיעיני למרחב האזרחי מבוסס כיום על שיח חד־צדדי, במסגרתו מועברים מידע וידע המגיעים מחוץ לקהילת המודיעין אל גופי הקהילה, אך התהליך אינו הדדי וסינרגטי. שותפות בין המרחב המודיעיני למרחב האזרחי תאפשר יצירת חיישנים חדשים והזרמה הדדית של מידע וידע, שמצידם יובילו לחשיבה רעננה על בעיות מוכרות וללמידה של בעיות שאינן מוכרות. שותפות כזו גם תרחיב את היכולת לתת מענה לבעיות השונות ותשפר את הפתרונות הקיימים.

---

45 P. R. Lawrence, J. W. Lorsch, "Differentiation and Integration in Complex Organizations", *Administrative Science Quarterly*, Vol. 12, No. 1 (January 1967): 1-47; H. Mintzberg, *The Structuring of Organizations* (McGill University, Prentice-Hall International, 1979).

46 סא"ל נ', "קהילת ידע מודיעינית כמנגנון פעולה המספק גמישות אסטרטגית ומערכתית לאמ"ן," **מודיעין הלכה ומעשה,** גיליון 1, המרכז למורשת המודיעין, 2016, עמ' 45־54.

47 יהל ארנון, "בניין כוח בקהילת המודיעין במציאות מִשתנה", **מודיעין הלכה ומעשה**, גיליון 2, המרכז למורשת המודיעין, 2017.

מערכת אקטיבית

כפי שראינו, הסייבר מחייב היפרדות מפרדיגמת "מעגל המודיעין", ובראש ובראשונה הפרדה בין מודיעין אקטיבי (המשויך לפי הפרדיגמה המסורתית לאיסוף) לבין מודיעין פסיבי (המשויך בדרך כלל לעיבוד ולמחקר). יש לפתח תפיסה, תורה ודוקטרינה בהן החוקר, לצד תפקידו להבין את המציאות, נדרש להיות אמון גם על חלקים ניכרים מהאיסוף (בעיקר במרחב הגלוי) והעיבוד. הדבר מחייב את יחידות האיסוף להגדיר את תפקידן מחדש ואת יחידות המחקר להקנות לחוקרים מיומנויות חדשות של "קמ"נות מידע".[48] יתכן שהחלוקה הארגונית המסורתית שבין חלק מיחידות האיסוף ליחידות המחקר תשתנה גם היא.

מערכת מבוססת טכנולוגיית היתוך, בינה מלאכותית ולמידת מכונה

הטכנולוגיות הללו, המצויות רק בתחילת דרכן בארגוני המודיעין הלאומיים (בניגוד למודיעין עסקי, למשל), עתידות לייתר חלק משמעותי מליבת עבודת המודיעין האיסופית והמחקרית בפרדיגמת "מעגל המודיעין". זאת, בעיקר במה שקשור לקטגוריזציה של מידע וסיווגו לתחומי ידע, פרשיות, תחומי עניין וכדומה, להמלצות לפעולה המבוססות על מקרי עבר, אנלוגיות ותרחישים ולמציאת דפוסים במידע (Clustering).[49] בה בעת, מערכת מבוססת טכנולוגיות מחייבת לפתח תפקידים חדשים (דוגמה אפשרית היא חוקרי דפוסים) ותהליכים חדשים (למשל, בקרת איכות במקום חיפוש במידע). גם מערכת מסוג זה מייתרת את ההפרדה בין איסוף למחקר, שכן חלק מתהליכי העיבוד והמחקר הבסיסיים הופכים גם הם לטכנולוגיים ואוטומטיים.

סיכום

חלק מהתובנות העולות ממאמר זה אינן חדשות. השיח על הפערים ההולכים ורבים בין התפקוד הנדרש מקהילות המודיעין ובין התפיסות, התרבות והמבנה שלהן קיים כבר יותר מעשור, הן בקהילת המודיעין האמריקאית והן בקהילת המודיעין הישראלית. גם הניסיונות ליצור שינויים והתאמות אינם חדשים. ובכול זאת, קהילות המודיעין נותרו ביסודו של דבר נאמנות לפרדיגמת "מעגל המודיעין" ולא הצליחו לחולל שינויים מהפכניים. דומה שהסיבה העיקרית לכך קשורה להיעדר תחושת דחיפות ומשבר.

ייחודו של מאמר זה הוא בהצגה שיטתית וברורה של הפערים והמתחים שכבר קיימים בשל העיכוב באימוץ פרדיגמה חדשה, ובהצבעתו על תופעת הסייבר

---

48 רס"ן (מיל') ד"ג, "קמ"ן המידע – תפיסה חדשה למחקר מודיעיני", **מודיעין הלכה ומעשה**, גיליון 2, המרכז למורשת המודיעין, 2017.

49 Paul Santilli, "Applying Machine Learning to Intelligence Problems", *linked in.*

המעצימה פערים אלה ומגבירה את המתחים עד כדי חוסר יכולת לשמר את המערכת במתכונתה הקיימת. בה בעת, המאמר מצביע על הסייבר כמרחב המאפשר להיחלץ מפרדיגמת "מעגל המודיעין" ולפתח פרדיגמה חדשה. דומה שתהליכים בכיוון זה כבר מיושמים בחלקם, הגם שהם אינם מגובשים לכדי תפיסה שלמה.

ברי שזניחת פרדיגמה ישנה ואימוץ פרדיגמה חדשה, עוד בטרם זו עוצבה באופן שלם, אינה מהלך פשוט ונטול סיכונים. אולם, נראה שגם הבחירה להישאר נטועים בפרדיגמת "מעגל המודיעין" אינה נטולת סיכונים. יותר מכך, דומה שכבר כיום ניתן להבחין בכך שהמשך האחיזה בפרדיגמה הישנה בעידן הסייבר יוביל תוך זמן קצר לכישלונות מודיעיניים משמעותיים ולאי־מיצוי הפוטנציאל הגדול שמזַמן העידן החדש למעשה המודיעיני.

פיתוח דוקטרינה ללוחמת סייבר במערכה הקונבנציונלית

רון טירה

תחום הסייבר נמצא בתהליך שיהפוך אותו לענף נוסף בלוחמה המדינתית, בדומה לענפי היבשה, הים, האוויר או החלל. ככזה, הוא עתיד להנביט דוקטרינת הפעלה מלאה ובשלה שתשאב מרכיבים מדפוסים והגיונות צבאיים כלליים ותשתלב במערכה הקונבנציונלית באופן סינרגטי עם מאמצים אחרים. כמה ממעצמות הסייבר כבר פיתחו דוקטרינות ויכולות מתאימות, אך רוב מדינות העולם ממוקדות עדיין באבטחת סייבר ולא בלוחמת סייבר, הגנתית והתקפית כאחת. אבטחת הסייבר מבוססת על פרקטיקות ומוצרים גנריים, המיועדים לאבטח בפני איומי ייחוס גנריים, שבמקרים רבים הם תת־מדינתיים. לעומת זאת, לוחמת סייבר מתמודדת עם יריב ספציפי, בהקשר ספציפי ועל בסיס מודיעין על היריב המאפשר את ההתמודדות איתו.

מילות מפתח: סייבר, ישראל, ארצות הברית

רקע: לקראת נורמליזציה של לוחמת הסייבר המדינתית

הסייבר נמצא בתהליך של התפתחות[1] לכדי ענף נוסף בלוחמה המדינתית, בדומה לענפי היבשה, הים, האוויר או החלל. ככזה, הוא עתיד להנביט דוקטרינת הפעלה מלאה ובשלה שתשאב, ולו חלקית, מתוך דפוסים והגיונות צבאיים כלליים ותשתלב במערכה הקונבנציונלית העיקרית, וזאת באופן סינרגטי עם מאמצים אחרים.

לוחמת הסייבר נמצאת בשלבי התפתחות שונים במדינות שונות,[2] בחלקן בתהליך סדור וקוהרנטי מעלה־מטה (top-down) ובחלקן בהתפתחות אינקרמנטלית, שבה

1 עמית שיניאק, "יתרון שאינו רק טכנולוגי – השינוי הארגוני בארצות הברית", **סייבר, מודיעין וביטחון**, כרך 1, גליון 3, דצמבר 2017.

2 גבי סיבוני ועופר אסף, **קווים מנחים לאסטרטגיה לאומית במרחב הסייבר**, מזכר 149, תל אביב: המכון למחקרי ביטחון לאומי, 2015.

סא"ל (מיל') רון טירה הוא איש עסקים ומשרת במילואים בחיל האוויר בתחום תכנון המערכה.

מכלול של צעדים נקודתיים, הננקטים לעיתים כמענה לצורך "בוער", מתחברים מטה־מעלה (bottom-up) לתמונה כוללת כלשהי. חלק ממעצמות הסייבר נמצאות בשלבים מתקדמים של פיתוח דוקטרינה ללוחמת סייבר,[3] העשויה להשתלב במערכה הקונבנציונלית. לפי פרסומים שונים, חמש מעצמות הסייבר המובילות בעולם הן ארצות הברית, רוסיה, סין, בריטניה וישראל.[4]

לוחמת הסייבר וההיערכות אליה מתרחשות בעיקרן בהסתר, והמקורות הגלויים בתחום זה מועטים. ארצות הברית חשפה בשנת 2010 טפח מתפיסת לוחמת הסייבר שלה,[5] אך מרבית הפרסומים הגלויים עוסקים בהקצאת המשאבים הלאומיים לסייבר, בקביעת המבנה הארגוני שלו (כמו מסמך "המיזם הקיברנטי הלאומי" בישראל),[6] ברגולציה או באבטחת מידע, ופחות מכך בעולם התוכן של דוקטרינת לוחמת הסייבר.

ניתן לקבוע בהכללה כי לוחמת הסייבר טרם הבשילה במרבית המדינות.[7] הסיבות לכך הן, בין היתר:

- התמקדות באבטחת סייבר[8] והבשלה איטית של רעיון המערכה ההתקפית וההגנתית בסייבר.
- היעדר דוקטרינה מלאה ובשלה ללוחמת סייבר התקפית והגנתית.
- הסתכלות על הסייבר כענף מבודד, שאינו משולב במערכה הקונבנציונלית.

---

3 "Cyberspace Operations", Joint Publication 3-12 (R), *US Joint Chiefs of Staff*; "Electronic Warfare", Joint Publication 3-13.1, *US Joint Chiefs of Staff*; William J. Lynn III, "Defending the New Domain, the Pentagon's Cyber Strategy", *Foreign Affairs*, September/October 2010; Cheryl Pellerin, "Cybercom Chief: Cyberspace Operations Key to Future Warfare", *US Department of Defense*, June 16, 2014; "The Department of Defense Strategy", *US Department of Defense*, April 2015.

4 Keith Breene, "Who are the Cyber Superpowers?", *World Economic Forum*, May 4, 2016.

5 "Cyber Command Fact Sheet", *US Department of Defense*, October 13, 2010.

6 לדוגמה, "קידום היכולת הלאומית במרחב הקיברנטי", *ממשלת ישראל*, החלטה 3611, 7 באוגוסט 2011, וכן "קידום ההיערכות הלאומית להגנת הסייבר", *ממשלת ישראל*, החלטה 2444, 15 בפברואר 2015. ראו גם "נייר מטה לדיון הוועדה העליונה למדע וטכנולוגיה בנושא: המיזם הקיברנטי הלאומי", יולי 2013, וכן "המרחב הקיברנטי והגנה על תשתיות חיוניות", *הכנסת*, 12 במאי 2013.

7 אסטרטגיית אבטחת סייבר דומה קיימת במספר רב של מדינות. להלן שתי דוגמאות להמחשה:
"Cyber Security Strategy for Germany", *German Federal Ministry of the Interior*, February 2011; "Cybersecurity Strategy", *The Government of Japan*, September 2015.

8 "National Cyber Security Strategies", *European Network and Information Security Agency*, December 2012.

- התמקדות בסייבר בסביבת ה־IT (מחשבים ומכשירים סלולריים הנגישים מהאינטרנט), לעומת מתן משקל חסר ללוחמת הסייבר בסביבת ה־OT[9] (שליטה במערכות תפעוליות) ונגד מערכות נשק.[10]
- התמקדות באיום הייחוס הפלילי, ההאקטיביסטי, הטרוריסטי, החתרני (כמו שיבוש ההליך הדמוקרטי או שוק ההון) או ה"פארה צבאי" (קרי, במקומות בהם המדינה התוקפת מבקשת להתכחש לפעולה), לעומת מתן משקל חסר לאיום הייחוס המדינתי/מעצמתי־צבאי.
- התמקדות יתר באנקדוטות, כמו למשל בשאלת ייחוס התקיפה (attribution),[11] כאילו היה זה מגדיר עיקרי של תחום הסייבר, והעלאת הטענה שסוגיית הייחוס קוטעת את הרצף ההגיוני הקלאוזביציאני (למעשה, סוגיית הייחוס אינה חדשה, שכן גם כוחות מיוחדים, צוללות או אפילו כלי טיס מסוגלים לתקוף ללא ייחוס, בלי שהדבר יהווה ערעור או שינוי בתבניות האסטרטגיות והמערכתיות המוכרות). לעומת זאת, מתן משקל חסר לנורמליזציה הצפויה של הסייבר ולהשתלבותו בזרם המרכזי (mainstreaming) של הלוחמה.

לוחמת הסייבר נמצאת בשלבי התפתחות טכנולוגית ומבצעית ראשוניים, שבאנלוגיה להתפתחות התעופה הצבאית אפשר להשוותם להופעת מטוס התצפית הדו־כנפי במלחמת העולם הראשונה. כבר אז הובהר הפוטנציאל הטמון באפשרות הטיסה אל מרכזי הכובד של האויב, מעל מערכי ההגנה הקרקעיים ומכשולי הקרקע, ולכן מצביאים כמו ג'וליו דואה ובילי מיצ'ל גיבשו את תפיסת ההפצצה האסטרטגית עוד בטרם פותחו מטוסים המסוגלים לממשה. גם דוקטרינת לוחמת הסייבר צריכה להמשיך ולהתפתח אל מול הפוטנציאל העתידי ולשמש כמצפן הטכנולוגי והמבצעי, אפילו אם אין כיום עדיין את כל הכלים הדרושים למימוש מלא של מרכיביה.

מאפייני לוחמת הסייבר

כפי שיובהר בהמשך, לוחמת הסייבר מאמצת בהדרגה דפוסים והגיונות צבאיים כלליים, אך, כבכל ענף בלוחמה, גם לסייבר מאפיינים ייחודיים שיש לאבחנם.

---

9 Nate Beach-Westmoreland, Jake Styczynski, Scott Stables, "When The Lights Went Out", *Booz Allen Hamilton*, November 2016.

10 LTG Larry Wyche, USA Ret. and Mr. Greg Pieratt, "Securing the Army's Weapon Systems and Supply Chain against Cyber Attack", *Institute of Land Warfare*, November 2017.

11 John S. Davis II, Benjamin Adam Boudreaux, Jonathan William Welburn, Jair Aguirre, Cordaye Ogletree, Geoffrey McGovern, Michael S. Chase, **"**Stateless Attribution, Toward International Accountability in Cyberspace", *RAND Corporation*, 2017; Martin C. Libicki, **"**It Takes More than Offensive Capability to Have an Effective Cyberdeterrence Posture**"**, *RAND Corporation*, March 1, 2017.

הסייבר מאפשר השגת שליטה בתוכנה או לפחות שיבוש פעולתה, ובמקרה של תוכנה המאפשרת שליטה במערכת מכנית, הוא עשוי לאפשר גם גרימת נזק פיזי לציוד או לאדם. במקרה בו תוכנה מאפשרת שליטה במספר רב של מערכות מכניות, ניתן להשיג פגיעה פיזית נרחבת ואף המונית. הסייבר מאפשר לפיכך הרג ופגיעה בנכסים, השקולים לפגיעה קינטית. כמובן שהסייבר גם מאפשר פגיעה בתפקודה של התוכנה או בנתונים, לרבות כאלה של מערכות נשק או מערכות תפעוליות קריטיות.

הפעלת נשק הסייבר כרוכה בסיכון אופרטיבי ישיר נמוך. ככזאת, היא עשויה להציג בנסיבות המתאימות יחסי עלות־תועלת אטרקטיביים בהשוואה לתקיפה פיזית, בעיקר במקרים בהם אין צורך במבצע עזר מורכב לשם יצירת נגישות לרשתות מבודדות (air gapped) או למערכות שמשיקולים טכנולוגיים או מבצעיים מאתגר לתקוף אותן מרחוק. מצד שני, כאשר התקפת הסייבר לא הוכנה מראש בשגרה, עלול להתעורר קושי לבצעה בחירום כשההתרעה היא קצרה.

המרחק הגיאוגרפי מאבד ממשמעותו בממד הסייבר, ולכאורה ניתן לתקוף בסייבר לכל טווח. מאפיין זה מרחיב מצד אחד את קשת אויבי הייחוס ואיומי הייחוס, ומצד שני מהווה לעיתים תחליף או משלים נוח יותר למבצע קינטי מורכב נגד מדינות לא גובלות ומרחיב את אפשרויות הפעולה נגד קואליציות של יריבות. ניתן למדוד את יחסי הכוחות חזק־חלש בממד הסייבר בנפרד מממדים אחרים (כפי שמעצמה ימית עשויה, לדוגמה, להיות בעלת עוצמה צבאית יבשתית צנועה).

בחלק מהמקרים, האתגר הטכנולוגי והמבצעי של החדרת נשק סייבר הינו מורכב וכרוך בזמן, ויש להניח שבאותם מקרים התוקף ישאף להתגבר על אתגר זה עוד בטרם יפרוץ העימות (מבצעי יום ה־"ע" מינוס). החדרת נשק סייבר למערכות קריטיות של יריבים פוטנציאליים היא לפיכך שגרה של טרם מלחמה, החיונית במקרים מסוימים להפעלה אפקטיבית של הסייבר ההתקפי מאוחר יותר, בלחימה עצמה. כלומר, בניגוד למרבית ענפי הלחימה, הפעלת הסייבר במערכה הקונבנציונלית מצריכה במקרים רבים ניהול מבצעים מקדימים בתקופת השגרה של טרם הלחימה. יש להניח שחשיפת ניסיון להחדיר נשק סייבר בשגרה לא תהווה, לפחות בחלק מהמקרים, קאזוס בלי ולא תוביל בפני עצמה להסלמה, וזאת בניגוד לחשיפת חדירה צבאית פיזית למדינה אחרת בעת שגרה.

לתוקף הסייבר יש כיום, ובעתיד הנראה לעין, יתרון משמעותי על המגן.[12] המגן חייב להגן על מספר רב של נכסים – מפלטפורמות לחימה ומערכות נשק, דרך מערכות שליטה ובקרה צבאיות, מערכות תקשורת צבאיות, תשתיות ממשל,

12 "Information Technology and Cyber Operations, Modernization and Policy Issues to Support the Future Force", *Hearing Before the Subcommittee on Intelligence, Emerging threats and Capabilities, House of Representatives*, March 13, 2013.

תשתיות לאומיות קריטיות, תשתיות שאינן קריטיות אך כאלו ששיבושן יוצר אפקט מורלי, תאגידים מסחריים בעלי חשיבות לאומית כמו בנקים או בורסות, ועד לכלל העורף הדיגיטלי האזרחי. תהליכי הרישות והדיגיטליזציה של העולם, הצפויים לעלות מדרגה עם כניסת "האינטרנט של הדברים" (IOT) והרֶכב האוטונומי, מזניקים מעלה הן את מספר הנכסים שניתן לפגוע בהם (או לפגוע באחרים באמצעותם) והן את הנגישות וכיווני התקיפה (attack vectors) האפשריים. התוקף יכול לבחור למעשה מתוך אינספור אפשרויות תקיפה, וכדי לחדור למערכת הנתקפת, עליו להצליח רק פעם אחת ובכיוון תקיפה בודד. לעומתו, המגן צריך להצליח להגן כל הזמן על כל כיווני התקיפה הקיימים במערכותיו.

שני יתרונות נוספים נמצאים בידי התוקף. הראשון, מאחר והמגן צריך להגן על "הכל", והתוקף יכול למקד את מאמצי התקיפה שלו באשר יבחר, הרי שהיקפי כוח האדם הדרושים להגנה בסייבר גדולים הרבה יותר מהיקפי כוח האדם התוקף (בניגוד ללוחמה הקונבנציונלית). מכאן שניתן לרכז כוח אדם איכותי יותר בהתקפה בהשוואה לממוצע של איכות כוח האדם המגן. בתחום הסייבר ישנה חשיבות מכרעת לאיכות כוח האדם, כישוריו, יצירתיותו, הידע והעדכניות שלו. לכן, בהתמודדות האופיינית בין תוקף ובין מגן על כיוון תקיפה מסוים, ניתן להניח שהתוקף (המציב לצורך זה את טובי אנשיו) יהנה מיתרון איכותי על המגן (המציב, בהיעדר התרעה ממוקדת, כוח אדם ממוצע ברמתו); היתרון השני של התוקף, שהוא במידה מסוימת פועל יוצא של הנקודה הקודמת, הוא שלפחות בעת הנוכחית, התורפות של מערכות שונות רבות יותר מהמודעות של המגן להן. גם רמת המודעות של המגן למידת הנגישות אליו אינה מספקת – למשל, היכולת להגיע אליו באמצעות תקיפת מערכות שכנות או צדדים שלישיים בשרשרת האספקה שלו.

בסייבר קיים דמיון ניכר בין האיסוף ובין ההתקפה, עד כדי טשטוש הגבולות ביניהם. בשני המקרים יש לחדור לרשת היריבה ולהשתלט על תוכנה. קצה תהליך האיסוף הוא המידע שנאסף, בעוד שקצה תהליך התקיפה הוא שינוי או שיבוש המידע. גם התהליך הטכנולוגי והמבצעי של איסוף והתקפה בסייבר זהה ברובו, ויתכן שאותו כלי סייבר ישמש הן לאיסוף והן, במקרה הצורך, לתקיפה.

כמו כל ענף לוחמה אחר, הסייבר הוא גם צרכן של המודיעין הנחוץ לשם ניהול מערכה הגנתית או התקפית. המודיעין הדרוש לסייבר אינו חייב להיאסף דווקא בממד הסייבר. המודיעין הרלוונטי ביותר, המאפשר את ניהול המערכה בסייבר, ייאסף לעיתים באמצעים אחרים (יומינט, קומינט וכדומה), או יהיה תוצאה של מחקר מודיעיני הנעשה בשיטות קונבנציונליות.

המערכה ההגנתית בסייבר

מוצע לאבחן בין אבטחת סייבר ובין ניהול מערכה הגנתית בסייבר, על בסיס ההמשגה וההגדרות שלהלן: אבטחת סייבר היא פעילות אותה עשוי לנקוט כל גורם המבקש לאבטח את עצמו בממד הסייבר, לרבות גורמים מסחריים ופרטיים. אבטחת הסייבר מבוססת על פרקטיקות ומוצרים גנריים[13] המיועדים להגן בפני איומי ייחוס גנריים. עיקרה של אבטחת הסייבר הוא בהתבוננות של הצד המאבטח (או ה"כחול") על עצמו, ובכלל זה על הדרך בה הוא מגן על "הגדר" (מניעת חדירת נשקי סייבר למערכת ה"כחולה"), התנהגותו האבטחתית השגרתית (מהצבת "מלכודות דבש" ופיתויים, דרך הונאת התוקף באמצעות ארכיטקטורת רשת מזויפת ועד לשינויים עיתיים בטופולוגיית הרשת ה"כחולה"), ניטור הפעילות בתוך הרשת ה"כחולה", ניטור המידע המוזרם מתוך הרשת ה"כחולה" החוצה, הצפנת המידע ה"כחול" והיערכות להתאוששות הרשת ה"כחולה" מתקיפה, מחקר חולשות עצמיות של הרשת ה"כחולה" וכדומה.

לעומת זאת, הגנה בסייבר היא מערכה שמנהל גורם מדינתי (או מעֵין מדינתי) במטרה להתגונן נגד תקיפה. הגנת הסייבר אינה גנרית, אלא נעשית על פי ההקשר – מול מאמץ התקפי מסוים של תוקף מוכר או מזוהה. כבכל מערכה הגנתית, עיקרה של ההגנה בסייבר הוא בהתבוננות על התוקף (או ה"אדום"), תוך נקיטת מגוון פעולות אופרטיביות מול המאמצים המזוהים שלו. כאשר ה"אדום" נערך לתקיפה, עשוי ה"כחול" לבצע תקיפה מקדימה שתמנע את התקיפה ה"אדומה". כאשר התקיפה של ה"אדום" החלה, יכול ה"כחול" לבצע אמנעה שלה, לרבות ברשתות תקשורת של מדינות שלישיות (לרוב תמימות) שה"אדום" עושה בהן שימוש.

כמו באבטחת סייבר, גם במערכה הגנתית ינסה ה"כחול" להדוף את ה"אדום" מלחדור לתוך הרשת ה"כחולה", וכן ינטר את הרשת ה"כחולה" כדי לזהות תקיפות "אדומות" שחדרו בהצלחה. עם זאת, ניתן לנקוט צעדים אופרטיביים קונקרטיים מול מערכה התקפית מזוהה, שיסייעו לסכלה. צעדים כאלה אינם עומדים לרשותו של מי שרק מאבטח את הרשת ה"כחולה" נגד איומים גנריים. לאחר זיהוי התקפה "אדומה" מוצלחת בתוך הרשת ה"כחולה", יש צורך בכלים לעקירת כלי התקיפה, אך במקרים מסוימים יש גם מקום להערכת פוטנציאל הנזק והחשיפה שבהתקפה, הכלת ההתקפה והותרתה בתוך הרשת ה"כחולה", לעיתים תוך ניהול מבצע הונאה מולה. יש מקרים שבהם נכון להתנהל מול תקיפה מוכרת ומוכלת, יותר מאשר ליצור את המוטיבציה אצל ה"אדום" לבצע תקיפה נוספת, שיתכן שלא תתגלה. במקרים אחרים נכון לבצע תקיפה אוחרת נגד ה"אדום" כדי לשבש את יכולתו

13 "NCSS Good Practice Guide", *European Network and Information Security Agency*, November 2016.

להפיק מודיעין מכלי התקיפה שהחדיר, או לשבש את יכולתו להעביר פקודות לאותו כלי תקיפה.

ניהול מערכה הגנתית כזאת מחייב הישענות על מודיעין המצביע על התוקף, מזהה את היערכותו וכוונותיו ואת צעדיו האופרטיביים, יוצר תמונת מערכה התקפית מתוך מגוון צעדים אופרטיביים התקפיים ומנתח את היכולות הטכנולוגיות ואת כלי התקיפה של התוקף, לרבות זיהוי כלי תקיפה לא מוכרים (קרי, מתקפת אפס ימים – zero-day). בד בבד, יש צורך בכלים לזיהוי תקיפות שחדרו את הרשת ה"כחולה", לאומדן היקף הנזק הפוטנציאלי מהחדירה ולאפשרויות הכלה שלה.

המערכה ההתקפית בסייבר

מערכה התקפית בסייבר מורכבת ממספר התקפות ומבצעי עזר המבוצעים תחת היגיון אסטרטגי אחד. בכך היא שונה מתקיפה נקודתית גרידא, המאפיינת לא אחת את איום הייחוס הפלילי, ההאקטיביסטי או הטרוריסטי.

רשתות ומחשבים של מערכות קריטיות – צבאיות או של תשתיות לאומיות – הן לא אחת מבודדות (air gapped), ומגמה זו צפויה להתעצם. כיום, הרוב המכריע של תקיפות הסייבר מתבצע בסביבת ה־IT, הנגישה ברובה לרשתות תקשורת פתוחות (כמו האינטרנט), אך מבט לעתיד מחייב להתייחס גם להתקפה על מטרות איכותיות ומבודדות. אחד האתגרים העיקריים בהתקפה מסוג זה הוא יצירת נגישות לרשת או למחשב הנתקפים. יצירת נגישות למטרה מבודדת מצריכה, במקרים רבים, מבצע עזר שאינו בתחום הסייבר, כמו שימוש בכוחות מיוחדים, יומינט, כלי טיס או שיט וכדומה. נקודה זו מהווה מבדיל מרכזי בין איום הייחוס המדינתי או המעצמתי, שבו מדינות מסוגלות לבצע מבצע עזר ליצירת נגישות, ובין איום הייחוס התת־מדינתי, שיתקשה במקרים רבים לנהל מבצע עזר ליצירת נגישות.

מבצע עזר ליצירת נגישות מצריך התבוננות על היריב כ"מערכת של מערכות" (system of systems), ניתוח כיווני הנגישות האפשריים, וכמובן הוצאה לפועל של מבצע העזר ליצירת הנגישות. במסגרת זו ניתן לנצל, בין היתר, נקודות תורפה הנובעות מתתי־המערכות המרכיבות את היריב:

- כבכל התקפת סייבר, יש לנתח את הארכיטקטורה של רשת המחשבים של היריב, את נקודות התורפה של התוכנות שברשותו, את נקודות התורפה של ההצפנה, את האפשרויות של אסקלציית פריבילגיות, כשלים של היריב ביישום מדיניות האבטחה שלו וכיוצא באלה.
- כדי ליצור נגישות, יש לבחון את הפריסה הגיאוגרפית של רשת המחשבים של היריב ולבחון דרכי גישה פיזיות אליה. לעיתים ניתן ליצור נגישות באמצעות רשתות סמוכות גיאוגרפית או מערכות מקומיות שהרשת הנתקפת, או מרכיבים בתוכה, תלויים בהן.

- יש לבחון את רשת התקשורת עליה פועלת רשת המחשבים היריבה ולנסות לזהות נקודות תורפה הקיימות בה, כמו למשל מִקטעים שבהם היא הופכת לאלחוטית.
- יש לבחון אם ניתן לתקוף באמצעות שרשרת האספקה של היריב, כלומר את מקורות הרכש של רכיבי החומרה, הקושחה והתוכנה שלו.
- יש למפות ולנצל את האינטראקציה של היריב עם רשתות או ארגונים אחרים, הידידותיים לו, שבהם רמת האבטחה נמוכה יותר.

שילוב לוחמת הסייבר במערכה הקונבנציונלית

מטרת המלחמה היא כפיית רצוננו המדיני על היריב חרף התנגדותו, וזאת בכוח או באמצעות איום בשימוש בכוח, או שלילת ניסיונו של היריב לכפות עלינו את רצונו המדיני, גם זאת בכוח או באמצעות איום בשימוש בכוח. אסטרטגיית המלחמה עשויה להיות הכרעה – פגיעה בכושרו של היריב לפעול נגדנו ביעילות בהקשר הרלוונטי – או התשה – גביית מחיר מלחמה בלתי משתלם ביחס למטרותיה – או אסטרטגיה אחרת הרלוונטית להקשר הייחודי של המלחמה. האסטרטגיה מיושמת באמצעות מערכה או מערכות. מערכה היא סדרה של הפעלות כוח שיש ביניהן קשר רציונלי, פונקציונלי, גיאוגרפי, סינרגטי או אחר. הפעלת כוח בהקשר זה משמעותה שימוש בכלים צבאיים, לרבות הפעלות כוח שאינן קינטיות, כמו איסוף מודיעין, לוחמה אלקטרונית, מבצעי עזר (כמו תדלוק אווירי או מבצעים לתספוק כוחות קרקעיים) וכיוצא באלה. הגדרות אלו הן צבאיות כלליות, ומן הסתם יחולו גם על לוחמת הסייבר.

לוחמת הסייבר עשויה לתרום למערכה הקונבנציונלית בשני אופנים: הראשון, כמאפשרת את פעולתם של אחרים, למשל בשיבוש מערך ההגנה האווירית כך שיקל על מטוס הקרב לבצע את משימתו, או בשיבוש מערך הפיקוד והשליטה של המערך הקרקעי של היריב כך שיקל על כוחות הקרקע ה"כחולים" להילחם בכוחות הקרקע ה"אדומים". יחד עם זאת, מערך הסייבר עצמו עשוי להזדקק לפעולה של אחרים כדי לאפשר את פעולתו שלו, לפחות במקרה של תקיפת סייבר על מערכות מבודדות. האופן השני בו לוחמת הסייבר עשויה לתרום למערכה הקונבנציונלית הוא בפעולה ישירה שלו להשגת תכלית מערכתית או אסטרטגית, כמו למשל גביית מחיר מלחמה מן היריב, שיביא אותו לוותר על ניהול המלחמה ועל מטרותיה המדיניות.

נראה כי דרך ההפעלה האופטימלית של לוחמת הסייבר, לפחות במקרים מסוימים, היא בסינרגיה עם ענפי לחימה אחרים ובמסגרת מערכה משולבת. כך, לדוגמה, במקרים המתאימים ניתן להשמיד או לדכא מערך הגנה אווירית באמצעות שילוב של מטוסי קרב, מסוקי קרב, כוחות מיוחדים, לוחמה אלקטרונית וסייבר.

במקרים אחרים ניתן להתיש ולכפוף את רצונה המדיני של מדינה יריבה באמצעות שילוב של תקיפות אוויריות, סגר ימי ולוחמת סייבר.

קיימת טענה לפיה סוגיית הייחוס (attribution) קוטעת את הרצף הקלאוזביציאני בין מדיניות ובין לוחמה, שהרי אם רשתות מחשבים במדינה מסוימת "סתם" קורסות, והדבר אינו ניתן לייחוס לשחקן מסוים, אותו שחקן יתקשה לממש את מדיניותו באמצעות סייבר. זאת, מאחר והמדינה המותקפת לא תזהה את התוקף, לא תזהה את ההקשר ואת רצונו המדיני של התוקף ממנה, ולכן לא תוכל להיענות ללחץ (כפי שהייתה עשויה להיענות ללחץ המופעל באמצעות סגר ימי גלוי, כדוגמה). טענה זו אינה נכונה, שכן סוגים רבים של לוחמה – מבצעים מיוחדים, צוללות ולעיתים אפילו הפעלת כלי טיס – אפשריים ללא ייחוס טקטי ישיר. מדינה המצויה תחת סגר ימי אינה צריכה להכיר כל צוללת יריבה ולהבין את הנסיבות הטקטיות של כל הטבעת ספינת סחר שלה כדי להבין את הסיטואציה האסטרטגית בכללותה, והיריב עשוי להצליח לכפות את רצונו המדיני עליה באמצעות סגר ימי גם ללא ייחוס של כל אירוע הטבעה יחידני. כך גם בסייבר: אין צורך בפורנזיקה קיברנטית לכל אירוע סייבר כדי שהמדינה המותקפת תבין את הסיטואציה האסטרטגית שיצרה המדינה התוקפת. ברוב המקרים, לפחות אלה של עימות בין־מדינתי, הצד הנתקף אינו זקוק לפורנזיקה קיברנטית שתפוגג את ערפל הייחוס כדי לבצע הערכת מצב מודיעינית קונבנציונלית ולהבין את הסיטואציה האסטרטגית.

שאלה הנשאלת לעיתים קשורה לבידודו של ממד הסייבר משאר הממדים. למשל, האם התקפת סייבר עלולה להביא לתגובה קינטית, או שמא סייבר ייענה רק בסייבר, והאם התקפת סייבר עלולה להוות קאזוס בֶּלי. התשובה המוצעת במאמר זה היא שדין סייבר כדין כל ענף אחר בלוחמה וכי הסייבר אינו ענף מבודד וייחודי. כבכל מקרה אחר, גם כאן על מקבל ההחלטות לבצע הערכת מצב ולקבל החלטה בהתאם לנסיבות. מתקפת סייבר נגד בית חולים שתהרוג מאות אנשים, או נגד תחנת כוח שתחשיך חלקים ניכרים מהמדינה המותקפת, אינה שונה ממתקפה קינטית היוצרת אותו אפקט. הצד המותקף יבצע את הערכת המצב שלו ויגיב בהתאם לאפקט שיצר התוקף. הוא עשוי להגיב בסייבר או באמצעים אחרים, בהתאם לנסיבות וליתרונו היחסי. אם האפקט שיצר התוקף מצדיק זאת, התקפת סייבר עשויה להיות גם קאזוס בלי.

סיכום: אבטחה מול מערכה הגנתית

באנלוגיה לעולם הפיזי, אם נבקר בתחנת כוח נמצא בה, קרוב לוודאי, גדרות, מגדלי שמירה, מצלמות, זרקורים, מספר רכבי אבטחה ותריסר מאבטחים החמושים בנשק קל. השאלה היא נגד איזה איום ייחוס זהו כוח אבטחה ראוי. התשובה היא שאמצעי אבטחה אלה יעילים מול איומי פשיעה או טרור. טענת מאמר זה

היא שבאנלוגיה לכך, זהו שלב ההתפתחות הנוכחי של הסייבר במרבית המדינות, למעט אולי בכמה מעצמות סייבר.

אך מה אם איום הייחוס על אותה תחנת הכח הינו צבאי – למשל, פשיטה של גדוד קומנדו, תקיפה של מפציץ אסטרטגי, או צוללת המשגרת טיל שיוט כשהיא משייטת במרחק מאתיים מייל מתחנת הכוח? במקרה כזה, ברור שאבטחת תחנת הכוח אינה רלוונטית. יתרה מכך, ברוב המקרים מדינה יריבה לא תתקוף "סתם" תחנת כוח בודדת, אלא כחלק ממערכה שיש מאחוריה היגיון מדיני ואסטרטגיה והיא משולבת במבצעים נוספים. למשל, תקיפת תחנת הכוח האמורה עשויה להיות חלק ממערכה רחבה יותר לפגיעה במערך החשמל ובתשתיות לאומיות אחרות במטרה לממש אסטרטגיה של התשה ולכפות מדיניות מסוימת. היא גם עשויה לכלול מבצעים מאפשרים שונים, כמו תקיפת מערך ההגנה האווירית או הימית קודם לתקיפת מערך החשמל. ההתגוננות נגד מערכה התקפית כזאת היא במערכה הגנתית, המתנהלת הרחק מתחנת הכוח האמורה ובעצימות גבוהה הרבה יותר מזו של כוח האבטחה שלה. מערכה כזאת תכלול הפעלה של כל אמצעי העוצמה הלאומית וכל הכלים הצבאיים, כמו, לדוגמה, תקיפה מקדימה על צבא האויב או אמנעתו בדרכו לתקיפת מערך החשמל של המדינה המתגוננת. באנלוגיה, זוהי לוחמת סייבר מדינתית ועצימה.

מרבית הגופים המדינתיים והמסחריים בעולם עוסקים באבטחת סייבר. לוחמת הסייבר, ההגנתית וההתקפית כאחת, נמצאת עדיין בשלבי התפתחות מוקדמים, אך היא זו שתעצב את פני העתיד.

הדרך להבנה טובה יותר של מודיעין הסייבר

מתיאו א׳ בונפנטי

בדומה למונחים אחרים הקשורים לתחום הסייבר, אין כל הגדרה מגובשת למונח "מודיעין סייבר" ואין בנמצא די מחקרים המתמקדים באופן בו הוא נוצר. לאור זאת, מטרתו של מאמר זה היא לצייר תמונה ברורה יותר של ענף מודיעין הסייבר הנמצא בצמיחה, וזאת באמצעות סקירה של המחקרים האנליטיים הקיימים בנושא. המאמר סוקר את הספרות המדעית הזמינה העוסקת במודיעין הסייבר, דן במושג זה ובוחן כיצד הוא מגובש באמצעות "מעגל המודיעין" (בסייבר). המאמר מסתיים בהדגשת החשיבות של פיתוח הבנה ברורה ומשותפת לבעלי העניין הרלוונטיים בתחום הביטחון, ובייחוד בתחום אבטחת הסייבר, לגבי מודיעין הסייבר.

מילות מפתח: אבטחת סייבר, מודיעין, מודיעין סייבר, תהליך מודיעין סייבר, מודלים

מבוא

במהלך העשור האחרון גובר הלחץ לאימוץ גישות ופתרונות מבוססי מודיעין לצורך טיפול באיומי סייבר. לחץ זה מגיע מצד חברים בקהילת אבטחת הסייבר הבין־לאומית (הבלתי פורמלית), המורכבת מנציגים של מוסדות וסוכנויות על־לאומיים, גופים ציבוריים מקומיים, ארגונים פרטיים והאקדמיה. גורמים אלה יזמו, בין היתר, את אימוצם של תפיסות ופתרונות אד־הוק שמטרתם לספק "מידע/מודיעין על איומי סייבר" – מוצר המספק לצרכניו הבנה (טכנית) של מבצעים ופעילויות זדוניות ברשתות התקשורת ומאפשר להם לנקוט אמצעי תגובה על בסיס

ד"ר מתיאו א׳ בונפנטי הוא חוקר בכיר במרכז ETH ללימודי ביטחון בציריך.

הבנה זו.[1] עם זאת, "מודיעין על איומי סייבר" לא הוכיח עצמו כפתרון הולם שניתן להסתייע בו למניעה מראש של איומי סייבר,[2] עקב האופי הטכני והאופרטיבי שלו ("מבט מבפנים"). ניתן לומר באופן כללי כי "מודיעין על איומי סייבר" אינו בנוי לספק, וגם אינו מספק בפועל, ידע על ההקשר הרחב יותר שבמסגרתו מתהווים איומי הסייבר.[3] למעשה, מוצרי המודיעין על איומי הסייבר אינם מאפשרים הבנה טובה יותר של סביבת האיומים וגם אינם מאפשרים חיזוי שלהם ומניעתם מראש.

נציגים שונים של קהילת אבטחת הסייבר תומכים כיום באימוץ הרעיון לפיו ארגונים צריכים לעבור מעמדה של ניהול אבטחה תגובתי לצעדים פרו־אקטיביים. אותם גורמים מתנגדים לגישה המתייחסת לאבטחת הסייבר בעיקר כ"צעדים הננקטים לאחר האירוע" ו"הגנה היקפית סטטית", ודוגלים באימוץ תפיסות, כלים ופרקטיקות ליצירת מודיעין חובק כל על איומי סייבר ושיתופו.[4] מודיעין כזה אמור לאפשר לצרכנים להבין את ההקשרים המבצעיים, הטקטיים והאסטרטגיים של האיומים (סוכנים, יכולות, מוטיבציות, מטרות, השפעה והשלכות, לא רק מנקודת מבט טכנית), לחזות את ההתפתחויות בטווח הקצר, הבינוני והארוך ולקבל החלטות מודעות לגבי צעדי המנע הנדרשים. שילובו של מודיעין זה בתהליכי קבלת ההחלטות בנושאי אבטחה אמור לאפשר לארגונים העושים זאת לנקוט עמדה של "חיזוי" או "ראיית הנולד" במקום גישה מכוונת עבר – גישה שתהיה "דינמית במקום סטטית" ו"זריזה וניתנת להתאמה מהירה במקום קשיחה ומסתגלת" לסיכונים הקשורים לסייבר.

המודיעין המתואר לעיל מכונה לעיתים קרובות "מודיעין סייבר" (CYBINT), מתוך כוונה להבדיל בינו ובין "מודיעין על איומי סייבר", שכאמור הוא בעל אופי טכני וצר. הביטוי "מודיעין סייבר" משמש באופן כללי להעברת הרעיון של ידע נרחב

---

1 שיתוף מידע על איומים, דפוסי מתקפה עדכניים, נקודות תורפה בתוכנות וכיוצא באלה עברו תהליך של תיקנון באמצעות יצירת רשת של "צוותי תגובה לאירועי אבטחת מחשב" (CSIRT). הם זכו לחיזוק באמצעות יצירתן ופיתוחן של מספר יוזמות, כגון STIX/TAXII, CyBox ו־MISPs (פלטפורמה לשיתוף מידע על נוזקות). ראו, לדוגמה: http://stixproject.github.io/supporters/.

2 Brian P. Kime, "Threat Intelligence: Planning and Direction", *SANS Institute InfoSec Reading Room*, 2017, p. 3, https://www.sans.org/reading-room/whitepapers/threatintelligence/threat-intelligence-planning-direction-36857. כפי שמודגש על ידי המחבר, "סימנים מעידים לסכנה" (IOCs), כגון חתימות של וירוסים וכתובות IP, סולמיות ("האשים") של קבצי נוזקה, כתובות URL או שמות אתרים ושרתי שליטה ובקרה אינם מהווים כשלעצמם מודיעין, אלא נחשבים למידע שימושי לצורך הגנה סטטית של הרשת.

3 Michael Montecillo, "Why Context is King", *Security Intelligence*, April 22, 2014, https://securityintelligence.com/enterprise-it-security-context-king/.

4 פירוש המונח "פרו־אקטיבי" בהקשר הנוכחי הוא היכולת לתת מענה לאיומי סייבר פוטנציאליים באמצעות חיזוק אמצעי ההגנה והתגובה.

ואיכותי יותר על אירועים אמיתיים או פוטנציאליים הנוגעים למרחב הקיברנטי ועלולים לסכן את הארגון.

בדומה למונחים אחרים הקשורים לתחום הסייבר, אין כל הגדרה מגובשת או פרשנות אמיתית משותפת בקרב קובעי מדיניות, ארגונים העוסקים בתחום, חוקרים ודעת הקהל למונח "מודיעין סייבר" כתוצר ו/או כתהליך. אם בוחנים את המדיניות או המנגנונים הרלוונטיים שיושמו לאחרונה (בייחוד ברחבי אירופה) ומסמכים אחרים שפורסמו על ידי ארגונים פרטיים או ציבוריים, וכן במסגרת האקדמיה, מתברר כי המונח "מודיעין סייבר" לא תמיד זוכה להגדרה כוללנית ומקיפה, אלא יש לו מגוון של פירושים והגדרות.[5] חרף השימוש ההולך וגובר בביטוי זה או אחר על ידי התקשורת, וכן על ידי חוקרים ואנשים העוסקים בתחום זה (במיוחד ספקים בתחום אבטחת הסייבר), החשיבה הקיימת בנושא הינה מוגבלת ואינה מפותחת דַיָה. הדבר נכון במיוחד כאשר בוחנים את העבודות האקדמיות או את המחקרים האחרים שנכתבו עד היום באותו נושא באירופה.[6] למעשה, אין כיום באירופה אף מחקר מעמיק שיתמקד בנקודת המבט התיאורטית והמעשית כאחת של נושא זה.

בניגוד לאירופה, החשיבה של המעורבים בתחומי האבטחה ואבטחת הסייבר בארצות הברית בסוגיית מודיעין הסייבר הינה מתקדמת יותר, הן במישור האקדמי והן במישור המעשי.[7] ייתכן כי הדבר נובע מאימוץ מוקדם יותר של תפיסות, פרקטיקות ופתרונות טכנולוגיים הקשורים למודיעין הסייבר על ידי ארגונים שבסיסם הוא בארצות הברית.[8] עם זאת, הדחף לאימוץ תוכניות הקשורות במודיעין

---

5 Matteo E. Bonfanti, "Another INT on the Horizon, Cyber Intelligence is the New Black", Paper Presented at the Intelligence in the Knowledge Society Conference, Bucharest, October 26-27, 2017 (אנתולוגיה של מאמרים מהכנס צפויה להופיע ב־2018).

6 נראה כי זה המקרה לפחות בחלק מן הספרות שנבחנה לצורך כתיבת מאמר זה. ראו, לדוגמה:
Mario Caligiuri, *Tra libertà e sicurezza* (Roma: Donzelli, 2016); Mario Caligiuri, "Cyber Intelligence, la Sfida dei Data Scientist", June 2016, https://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/cyber Intelligence-la-sfida-dei-data-scientist.html; Antonio Teti, "Cyber Intelligence e Cyber Espionage. Come Cambiano i Servizi di Intelligence nell'Era del Cyber Spazio", *Gnosis, Rivista Italiana d'Intelligence* 3 (2013):95-121; Umberto Gori and Luigi S. Germani, *Information Warfare 2011. La sfida della Cyber Intelligence al sistema Italia* (Bologna: Franco Angeli, 2012).

7 בנוסף לספרות המצוטטת להלן, ראו גם דיון שנערך על ידי בעלי עניין בתחום אבטחת הסייבר בארצות הברית ב־*Cyber Intelligence Blog* בכתובת https://cyberintelblog./wordpress.com.

8 ראו, לדוגמה: "The National Intelligence Strategy of the United States of America", *Office of the Director of National Intelligence*, 2014, https://www.dni.gov/files/documents/2014_NIS_Publication.pdf. לפי אותה אסטרטגיה, ההגדרה של מודיעין סייבר היא כדלקמן: "איסוף, עיבוד, ניתוח והפצה של מידע מכל המקורות המודיעיניים על התוכניות, הכוונות, היכולות, המחקר והפיתוח, הטקטיקה, הפעילויות המבצעיות והסימנים

הסייבר נמצא במגמת עלייה גם בקרב המעורבים בתחום אבטחת הסייבר שאינם מארצות הברית, מצב המצדיק את הרחבת הדיון בנושא. בהקשר זה, מן הראוי לבחון בפירוט רב יותר את המושג "מודיעין סייבר" ולנסות להבין את ההשלכות על סוכנויות וארגונים לאומיים שיעשו שימוש בגישות, במתודולוגיות, בכלים ובמסגרות לשיתוף פעולה שיהיו מבוססים על מודיעין סייבר.

מאמר זה מבקש לתרום תרומה ממוקדת לדיון על מודיעין הסייבר. במסגרת זו הוא מנסה לשרטט תמונה ברורה יותר של ענף מתפתח זה באמצעות סקירה של העבודה המחקרית הקיימת בנושא. המאמר סוקר את הספרות המדעית הזמינה העוסקת במודיעין הסייבר, דן במושג "מודיעין סייבר" ובוחן כיצד הוא נוצר, וזאת באמצעות הפריזמה של "מעגל המודיעין" (בסייבר). המאמר מסתיים בהדגשת החשיבות שבפיתוח הבנה ברורה ומשותפת של בעלי העניין הרלוונטיים בתחום הביטחון, ובמיוחד בתחום אבטחת הסייבר, לגבי מודיעין הסייבר.[9]

על שרמינולוגיה ומושגים (משותפים)

המונח "מודיעין סייבר" משמש בשפת היומיום בעיקר כביטוי מקיף וחובק כל. לפיכך, השאלה היא מהי ההגדרה המדויקת של מודיעין סייבר? בהיותו הן תוצר והן תהליך, יש לשאול האם מדובר במודיעין **הנובע** מהמרחב הקיברנטי, במודיעין **על** מרחב זה, במודיעין **במסגרת** המרחב או במודיעין **עבורו**, או שמדובר בשילוב של כל אלה? בנוסף לכך יש לשאול באיזו מידה מתמקד מודיעין הסייבר רק במרחב הסייבר ובאיזו מידה הוא מכסה אירועים/תופעות המתרחשים במרחב הפיזי? וכן, מהם המקורות העיקריים של מודיעין הסייבר וכיצד הוא נוצר? שאלות נוספות הן האם "מעגל המודיעין" "המסורתי" חל גם על מודיעין הסייבר ומהן הסוגיות הקשורות ביצירתו של מודיעין זה ובשיתופו? התשובות לשאלות אלו ולשאלות ספציפיות אחרות אינן מובנות מאליהן.

היעדר הסכמה כוללת סביב המונח "סייבר" מונע כל אפשרות להגיע להסכמה על מושג מקיף ואחיד של "מודיעין סייבר". בעוד שאין כמעט מחלוקת באשר למושג "מודיעין" (כתוצר וכתהליך), הגדרתו בהקשר למרחב הקיברנטי קשה יותר

המעידים של שחקנים זרים בתחום הסייבר; השפעתם הפוטנציאלית על הביטחון הלאומי, מערכות מידע, תשתיות ומאגרי נתונים; אפיוני רשת או מבט לתוך המרכיבים, המבנים, השימוש ונקודות התורפה של מערכות מידע זרות", שם, עמ' 8; ראו גם: "Resilient Military Systems and the Advanced Cyber Threat", *US Department of Defense Science Board*, January 2013, pp. 46, 49, http://www.dtic.mil/docs/citations/ADA569975; "The Department of Defense Cyber Strategy", *Department of Defense Science US Board*, April 2015, p. 24, https://www.defense.gov/Portals/1/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

9 המאמר מבוסס על מחקר מקדים המתבצע כעת כחלק מפרויקט מחקר בן שלוש שנים שהוגדר ומנוהל על ידי המחבר.

ויוצרת אתגר לא פשוט. באופן כללי ניתן לקבוע כי החשיבה על מודיעין סייבר כוללת תפיסות, מסגרות מושגיות ומינוחים הנובעים מהמערכת המודיעינית, תוך החלתם והתאמתם למרחב הקיברנטי.[10] הדבר נראה הגיוני, במיוחד בהתחשב בעובדה שחלק מהתפיסות מבוססות מספיק, ולכן אין כל צורך "להמציא את הגלגל מחדש ". ניתן לתהות, עם זאת, על היקף תחולתן של תפיסות אלו על מרחב הסייבר, הנבדל כאמור מן המרחבים המסורתיים והמוכרים. הסייבר הוא סביבה מעשה ידי אדם, המתפתחת בקצב מהיר, מעוצבת באופן טכנולוגי וכזו שאי אפשר לחוש אותה במלואה. על רקע זה, ייתכן שיש לפרש אותה באמצעות פרדיגמות אחרות. למעשה, האינטראקציות בין סביבת הסייבר ובין המרחב הפיזי/ממשי עדיין אינן ברורות לחלוטין.

זאת ועוד, מודיעין הסייבר הינו ענף חדש יחסית, הטעון עדיין מידה רבה של בחינה, הערכה ופיתוח. אין לפי שעה מספיק ניסיון משותף היכול להגדיר את הדרך בה הוא פועל ומהן היכולות הטובות ביותר הדרושות כדי לעשות בו את השימוש האפקטיבי ביותר. גם מצב זה מקשה על כל ניסיון ליצור מודל מקיף שיפרש את המושג "מודיעין סייבר".

הניתוח והשיקולים דלעיל חשובים להבנת המושג והבעייתיות סביבו. הם גם מסייעים להבין מדוע לא קיימת עדיין הגדרה מוסכמת ומגובשת של מודיעין הסייבר. כל מי שמבקש לאמץ גישה פחות מוטה מראש או יותר ודאית לחקר מודיעין הסייבר חייב להתחשב בשיקולים אלה.

מודיעין סייבר: ידע המאפשר פעולה, המופק מהסייבר או מיועד עבורו

קיימות שתי דרכים להתבונן על מודיעין הסייבר או לפרש אותו. זאת, בהתאם להיקף הפעילות לאיסוף המידע, האמצעים בהם נעשה שימוש כדי לבצע פעילות זו והמטרה הסופית אותה היא משרתת.[11] דרך אחת היא לחשוב על מודיעין הסייבר כמודיעין המגיע מהסייבר, כלומר, ידע המופק באמצעות הניתוח של כל המידע הערכי הנאסף "במסגרת" או "באמצעות" המרחב הקיברנטי. זהו מודיעין סייבר במובן הצר של המילה. מנקודת מבט זו, המונח "סייבר" מתייחס הן למרחב ממנו מגיעים הנתונים, או במילים אחרות, אותו מאגר דיגיטלי עצום של מידע הניתן

10 Robert M. Lee, "An Introduction to Cyber Intelligence", *Tripwire*, January 16, 2014, https://www.tripwire.com/state-of-security/security-data-protection/introduction-cyber-intelligence/; Stephanie Helm, "Intelligence, Cyberspace and National Security", paper given at EMC Chair Symposium.

11 Matthew M. Hurley, "For and From Cyberspace Conceptualizing, Cyber Intelligence, Surveillance and Reconnaissance", *Air & Space Power Journal* 26, no. 6 (2012): 12-33.

לשליפה או לעיבוד, והן לכלים/טכניקה/אמצעים המשמשים לאיסוף נתונים אלה (לדוגמה, באמצעות טכנולוגיות וטכניקות לניצול רשתות מחשבים).[12] בהתאם לפרשנות זו, יש ביכולתו של מודיעין הסייבר לתמוך עקרונית בקבלת החלטות בכל תחום, ולא רק בתחום ההתמודדות עם איומי סייבר. מודיעין הסייבר יכול אז לתמוך במגוון רחב של משימות במסגרת הממשלתית, התעשייתית והאקדמית, לרבות קביעת מדיניות, תכנון אסטרטגי, משא ומתן בין־לאומי, ניהול סיכונים וכן תקשורת אסטרטגית בתחומים המצויים מעבר לאבטחת סייבר.[13] במילים אחרות, מודיעין הסייבר עשוי לפעול "באופן בלתי תלוי ואינו צריך בהכרח לתמוך במשימת אבטחת הסייבר".[14] עם זאת, בהתחשב בעובדה כי מודיעין הסייבר נדון לעיתים קרובות בהקשר לאבטחת סייבר או למניעה של איומי סייבר ותגובה להם, ברור שאלו הן המטרות העיקריות (אם כי לא הבלעדיות) שלו.

דרך שנייה לפרש מודיעין סייבר היא לראות בו מודיעין המיועד "עבור" הסייבר, כלומר, תובנה הנובעת מפעילות מודיעין הכוללת את כל סוגי המקורות ומתרחשת הן במסגרת המרחב הקיברנטי והן מחוצה לו. זהו מודיעין סייבר במובן הרחב של המילה. המודיעין "עבור" סייבר יכול במצב זה גם לכלול (או להתבסס על) מודיעין "הבא מן" הסייבר. למעשה, מודיעין כזה עשוי לשאוב מידע מכל דיסציפלינה מודיעינית המספקת מידע חיוני, ללא קשר לזהות המקור, השיטה או האמצעים בהם נעשה שימוש לצורך גיבושו.

מודיעין הסייבר עשוי, אפוא, לנבוע משילוב של מודיעין ממקורות גלויים (OSINT), מודיעין אותות (SIGINT), מודיעין גיאו־מרחבי (GEOINT), מודיעין מרשתות חברתיות (SOCMINT) ומודיעין אנושי (HUMINT).[15] מנקודת מבט זו, מודיעין הסייבר הינו פחות בגדר דיסציפלינה כשלעצמה ויותר בגדר פרקטיקה אנליטית המסתמכת על מידע/מודיעין הנאסף גם באמצעות דיסציפלינות אחרות ומיועד לאספקת מידע למקבלי ההחלטות בסוגיות המתייחסות לפעילויות בתחום

12 Ross W. Bellaby, "Justifying Cyber-Intelligence?", *Journal of Military Ethics* 15, no. 4 (2016): 299-319; Hurley, "For and From Cyberspace", p. 13.
ניצול מערכות מחשבים או ניצול סייבר מתייחס לאיסוף ולשכפול חשאי של נתונים דיגיטליים ממחשבים או מרשתות.

13 Troy Townsend, Melissa K. Ludwick, Jay McAllister, Andrew O. Mellinger and Kate A. Sereno, "SEI Innovation Center Report: Cyber Intelligence Tradecraft Project: Summary of Key Findings", January 2013, pp. 2.01-2.20, spec. 2.5, https://resources.sei.cmu.edu/asset_files/WhitePaper/2013_019_001_40212.pdf.

14 שם.

15 Aaron F. Brantly, *The Decision to Attack: Military and Intelligence Cyber Decision Making* (Athens GA: University of Georgia Press, 2016), Ch. 7, pp. 103-108, 116-121.

הסייבר.[16] מה שהופך סוג זה של מודיעין ל"סייבר" הוא המטרה לשמה הוא מגובש: תמיכה בקבלת החלטות בסוגיות הקשורות למרחב הקיברנטי.

שתי נקודות המבט על מודיעין הסייבר – מודיעין "המופק" מן הסייבר ומודיעין "עבור" הסייבר – נדחסות לעיתים קרובות לתוך מושג אחד כולל. זאת, גם בשל העובדה כי מודיעין "עבור" הסייבר כולל בתוכו למעשה גם את המודיעין "המופק" מהסייבר. התוצאה היא מושג נרחב יותר של מודיעין סייבר הכולל את האיסוף, העיבוד, ההערכה, הניתוח, האינטגרציה והפרשנות של מידע הזמין "בתחומי" המרחב הקיברנטי, "באמצעותו" ו/או "מחוץ" לו, וכל זאת לשם שיפור תהליך קבלת ההחלטות בנושא האיומים הקשורים לסייבר.

ראוי לציין, כי כאשר בוחנים את הדיסציפלינות המודיעיניות "המסורתיות" הנכללות במושג "מודיעין סייבר" במובנו הרחב, רואים כי השלכותיהן על המרחב הקיברנטי הובילו להתפתחות מושגים וגישות אד־הוק, כמו אלו המכונות לעיתים קרובות בשם HUMINT וירטואלי, OSINT וירטואלי או מבוסס אינטרנט, COMINT וירטואלי וכן הלאה. שם התואר "וירטואלי" מציין פעילויות מודיעיניות המבוצעות בתחומי המרחב הקיברנטי או באמצעות כלים הנוצרים באמצעות מחשב. החיבור בין תפיסות ופרקטיקות "וירטואליות" לתפיסות ופרקטיקות "מסורתיות" של מודיעין מתייחס לאימוץ השיטות, הגישות והכלים בהם נעשה שימוש בפרקטיקות המסורתיות, תוך התאמתן למרחב הקיברנטי.[17] SOCMINT הוא מושג שונה במעט מן המושגים שצוינו לעיל, ולדברי מספר חוקרים ואנשי מקצוע, הוא דיסציפלינה עצמאית שיש לה מאפיינים ספציפיים.[18]

מידע המיועד ליצור מודיעין סייבר עשוי לכלול נתוני רשת טכניים (לדוגמה, נתוני חומרה ותוכנה), נתונים על ארגונים עוינים ויכולותיהם, נתונים על פעילויות

16 "Operational Levels of Cyber Intelligence", *Intelligence and National Security Alliance*, September 2013, pp. 1-14, https://www.insaonline.org/operational-levels-of-cyber intelligence; "Cyber Intelligence: Setting the Landscape for an Emerging Discipline", *Intelligence and National Security Alliance*, September 2011, pp. 1-20, https://www.insaonline.org/cyber-intelligence-setting-the-landscape-for-an-emerging-discipline. לעניין הדיסציפלינות המודיעיניות הקיימות, ראו, בין היתר: "Understanding and Intelligence Support to Joint Operations", Joint Doctrine Publication 2-00, *UK Ministry of Defence*, August 2011, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/311572/20110830_jdp2_00_ed3_with_change1.pdf.

17 לדוגמה, גישת ה־HUMINT הווירטואלי מיועדת לאיסוף מודיעין טקטי/מבצעי מן המידע הנוצר על ידי חברים בקהילות וירטואליות.

18 David Omand, Jamie Bartlett and Carl Miller, *#Intelligence* (London: Demos Publishing, 2012); Matteo E. Bonfanti, "Social Media Intelligence a Salvaguardia dell'Interesse Nazionale. Limiti e Opportunità di una Pratica da Sviluppare", in *Intelligence e Interesse Nazionale*, eds. Umberto Gori and Luigi Martino (Rome: Aracne, 2015), pp. 231-262.

סייבר נמשכות, או כל נתון רלוונטי אחר על אירועים גיאו־פוליטיים.[19] סוג זה של נתונים, כמו גם סיווגם, אינם ייחודיים למושג "מודיעין סייבר". נתונים כאלה יכולים להגיע באופן גולמי או בצורה של מידע שכבר עבר עיבוד; הם יכולים להתקבל באופן חוקי או באמצעות פעולות חדירה/ניצול בלתי חוקיות, הן ממקורות גלויים, הן ממקורות שהם קניין של גורם כלשהו והן ממקורות מסווגים אחרים.[20]

כפי שעולה מן הספרות המקצועית, נדרשים מקורות מידע מרובים כדי לפתח הבנה הוליסטית יותר של סביבת האיום ולגבש מודיעין סייבר מקיף.[21] ההיבט החשוב ביותר של הנתונים הוא היכולת שלהם לקבל תוקף וממשות. ניתוח המידע צריך לאפשר למקבלי ההחלטות לזהות, לעקוב ולחזות יכולות, כוונות ופעילויות בתחום הסייבר המחייבות פעולה מצידם.[22] זהו למעשה המאפיין העיקרי של מודיעין הסייבר. מטרתו היא לספק לצרכנים תובנות על פעילויות עוינות פוטנציאליות העלולות להתרחש במרחב הסייבר, כאלו שעלולות להתבצע באמצעותו של מרחב זה או כאלו שעלולות להתבצע נגדו, וכן לאפשר להם לתכנן צעדי מנע (פרו־אקטיביים) או אמצעי נגד (תגובתיים).

מודיעין סייבר עשוי להיות אסטרטגי, טקטי או אופרטיבי, בהתאם להיקפו או למידת היכולת לפעול על פיו.[23] לא קיימת הסכמה באשר לרמות השונות של מודיעין הסייבר. על פי הספרות הקיימת, מודיעין הסייבר עוסק בטווח הארוך, סוקר מגמות ואיומים מתפתחים ובוחן הזדמנויות להכלתם. הוא משמש לקבלת החלטות בדרגים הגבוהים ביותר, שמטרתן היא מימוש משימותיו של הארגון וקביעת כיוונו ויעדיו. מודיעין סייבר אסטרטגי מכסה את אופק האיומים ברמת המאקרו (איומים פוליטיים, חברתיים וכלכליים) המשפיעים על הארגון ומזהה את הגורמים המאיימים, מטרותיהם והאופן בו הם עלולים לנסות להשיגן. מודיעין הסייבר האסטרטגי עשיר במידע הֶקשֶרי.[24]

---

19 Jung-ho Eom, "Roles and Responsibilities of Cyber Intelligence for Cyber Operations in Cyberspace", *International Journal of Software Engineering and Its Applications* 8, no. 9 (2014): 137-146. המאמר עוסק במודיעין סייבר למטרות צבאיות.

20 Robert M. Lee, "Cyber Intelligence Collection Operations", February 25, 2014, https://www.tripwire.com/state-of-security/security-data-protection/cyber-intelligence-collection-operations/.

21 "Cyber Intelligence: Setting the Landscape for an Emerging Discipline", p. 1.

22 Townsend et al., "SEI Innovation Center Report".

23 ראו לדוגמה: Randy Borum, "Getting 'Left of the Hack': Honing Your Cyber Intelligence Can Thwart Intruders", *InfoSecurity Professional*, September/October 2014, https://works.bepress.com/randy_borum/63/.

24 Randy Borum, John Felker, Sean Kern, Kristen Dennesen and Tonya Feyes, "Strategic Cyber Intelligence", *Information & Computer Security* 23, no. 3 (2015): 317-332; "Strategic Cyber Intelligence", *Intelligence and National Security Alliance*, March 2014, pp. 1-16, https://www.insaonline.org/strategic-cyber-intelligence/.

מודיעין סייבר טקטי עוסק במה שמתרחש ברשת. בנוסף לכך הוא בוחן את החוזקות ואת נקודות התורפה של הארגון, וכן את הטקטיקה, הטכניקות והנהלים המשמשים את הגורמים המאיימים עליו.[25] עקב אופיו והטווח שלו, קיימת ככלל הלימה בין מודיעין סייבר טקטי למודיעין העוסק באיומי סייבר.[26] מודיעין הסייבר הטקטי, בהיותו בדרך כלל בעל אופי טכני יותר, משמש מקור מידע לצעדים ולפעולות מבוססי רשת אותם יכול הארגון לנקוט לצורך הגנה על נכסיו, שמירה על רציפות פעילותו וחידושה.

מודיעין סייבר אופרטיבי מורכב מידע על איומים מיידיים או ישירים על הארגון. מודיעין זה מאפשר את הפעילויות והתפוקות היומיומיות ותומך אותן. ברמה זו, מודיעין הסייבר בוחן את התהליכים הפנימיים בארגון ואת נקודות התורפה שלו.[27]

ראוי לחזור ולציין כי האבחנה המתוארת בין הרמות השונות של מודיעין הסייבר הינה לצורך אקדמי בעיקרו. בפועל, לא קיימת הבחנה ברורה בין רמה אחת של מודיעין סייבר לרמה האחרת, ולעיתים קרובות הן חופפות או אף משולבות ביניהן. יתרה מזאת, קרוב לוודאי כי משמעות המושגים "אסטרטגי", "טקטי" ו"אופרטיבי" תשתנה בין ארגון לארגון עקב גודלם, מורכבותם, משימתם ומאפייניהם.[28] כך או כך, חשוב שלארגון תהיה יכולת להביא בחשבון את הרמות השונות של מודיעין הסייבר ולעצב את המודיעין בדרך שתאפשר לו להבין את האתגרים וההזדמנויות בהם הוא עשוי להיתקל בסבירות גבוהה בטווחים הקצר, הבינוני והארוך. בכל מקרה, נראה כי אין בנמצא מתכון קבוע להצגת המוצר הסופי של מודיעין הסייבר בפני מקבלי ההחלטות.

תהליך יצירתו של מודיעין הסייבר: מודלים חלופיים מול מודלים מסורתיים

כמו במקרה של דיסציפלינות ומוצרים מודיעיניים אחרים, מודיעין הסייבר נוצר באמצעות מערך של פעילויות/פונקציות, המוצא את ביטויו ומוסבר באופן מסורתי באמצעות המודל של "מעגל המודיעין".[29] מודל זה נלמד, נבחן והועמד בספק מספר

25 "Tactical Cyber Intelligence", *Intelligence and National Strategic Alliance*, December 2015, pp. 1-16, https://www.insaonline.org/strategic-cyber-intelligence/.

26 שם.

27 "Operational Levels of Cyber Intelligence", *Intelligence and National Security Alliance*, September 2015, pp. 1-16, https://www.insaonline.org/strategic-cyber-intelligence/.

28 "Strategic Cyber Intelligence", p. 4.

29 "מעגל המודיעין" מופיע בכמה צורות. הנפוצות שביניהן מורכבות מחמש פעולות נפרדות: תכנון והכוונה, איסוף, עיבוד, ניתוח והפצה. חלק מפעולות אלו עשויות לכלול פעולות משנה, ובכך ליצור מעגל המורכב מתכנון והכוונה, איסוף, בחינה והשוואה, הערכה, ניתוח, אינטגרציה, פרשנות והפצה. לגבי "מעגל המודיעין" ראו: Mark Phythian, ed. *Understanding*

פעמים על ידי אנשי מקצוע ואנשי אקדמיה, עד שהוצעו לו מודלים חלופיים.[30] אותם ספקות לגבי התקפות והתחולה של "מעגל המודיעין" המסורתי קיימים גם בהקשר של מודיעין הסייבר. כפי שציין אחד המומחים הבולטים, "ככל שהמודיעין הופך ליותר דיגיטלי ו'סייברי' (בנושאי הטיפול, בשיטותיו ובצורותיו), הבנה כי 'מעגל המודיעין' הוא למעשה אמצעי למידה ולא חלק מתהליך הבנייה של המודיעין, עשויה לאפשר לעוסקים בנושא לחשוב על המודיעין בדרכים חדשניות יותר".[31] חוקרים ומומחים אחרים שותפים גם הם להשקפה זו. הם מדגישים כי מודל "מעגל המודיעין" חל רק בצורה מוגבלת על מודיעין הנוצר "מסייבר" ו"עבור הסייבר" ומצביעים על חוסר יכולתו של המודל לייצג ולהסביר את הליך יצירתו של מודיעין הסייבר. המודל המסורתי, שנועד לשמש כמעגל לינארי החוזר ונשנה, אינו מדגיש את ההדדיות של הפעולות מהן מורכב תהליך יצירתו של מודיעין הסייבר (תכנון, איסוף, עיבוד וכן הלאה) ואת הרלוונטיות שלהן האחת לשנייה. במילים אחרות, מודל "מעגל המודיעין" מתעלם מהתלות ההדדית ומההשפעות ההדדיות הקיימות בין פעולות אלו.

המבקרים המצוטטים לעיל מסתמכים למעשה על טיעונים המשמשים נגד "מעגל המודיעין" באופן כללי, ללא קשר לדיסציפלינה מודיעינית ספציפית.[32] על רקע זה, מתעוררת השאלה האם יש צורך במודל פרשני נפרד שיסביר את תהליך מודיעין הסייבר, ובמילים אחרות, האם תהליך מודיעין הסייבר הינו כה שונה מהתהליכים הנכללים בדיסציפלינות מודיעיניות אחרות, עד כדי כך שהוא דורש מודל חלופי שיתאר אותו. מתן תשובות משמעותיות לשאלות אלו מחייב הבנה ברורה, מקיפה ומעמיקה של מודיעין הסייבר כתפיסה, ומעל הכל כפרקטיקה בפני עצמה. אלא שקשה להגיע להבנה כזאת נוכח היעדר דיון וניסיון מספיקים בנושא מודיעין הסייבר. לפיכך, קביעת מודל ייחודי למודיעין הסייבר מהווה בשלב הנוכחי בעיקר סוג של תרגיל או ניסוי אינטלקטואלי, שתוצאותיו מחייבות עדיין תיקוף.

---

the Intelligence Cycle (London and New York: Routledge, 2013); Philip H. J. Davies, Kristian Gustafson and Ian Ridgen, "The Intelligence Cycle is Dead, Long Live the Intelligence Cycle", ibid., p. 56.

30 החסרונות של "מעגל המודיעין" המסורתי כמייצג את תהליך המודיעין נדונים בשורה של מאמרים בספר *Understanding the Intelligence Cycle*. ראוי לציין כי המודלים אינם מדויקים, משום שהם מנסים לפשט מציאות מורכבת. בנוסף לכך, מודלים אינם תהליכים אלא ביטויים מצומצמים שלהם. לפיכך, אין טעם לצפות מהמודל של "מעגל המודיעין", או מכל מודל פוטנציאלי אחר, לייצג את תהליך המודיעין באופן הוליסטי, חובק כל ומפורט לחלוטין. מודלים כאלה יהיו מסובכים וערכם המעשי יהיה נמוך.

31 Michael Warner, "The Past and Future of the Intelligence Cycle", in *Understanding the Intelligence Cycle*, p. 19.

32 *Understanding the Intelligence Cycle.*

אף על פי כן, נראה כי יש מספר טיעונים המצדיקים הגדרה של מודל אד־הוק שיסביר את תהליך גיבושו של מודיעין הסייבר.

המאפיין העיקרי של מודיעין הסייבר טמון בעובדה כי הוא "ממורכז סייבר", כלומר, עוסק בידע על סוגיות הקשורות לסייבר. מודיעין סייבר כרוך בניתוח של מידע הנאסף מן המרחב הקיברנטי, וכן ממקורות אחרים, לצורך השגת מטרות הקשורות לסייבר. ברמה הבסיסית ביותר, המושג "סייבר" מתייחס לתחום שהוא מעשה ידי אדם, תחום המתפתח במהירות, מעוצב באופן טכנולוגי ולא לגמרי מוחשי.[33] זהו תחום בו המידע נוצר, מעובד, מופץ, משותף, נשמר, עובר שינוי, נצרך ומושמד על ידי מספר רב של שחקנים ובקצב מהיר.[34] קשה לחזות את ההשלכות של קבלת החלטות מוכוונות מטרה על סוגיות הקשורות לסייבר ועל התחומים הווירטואלי והפיזי כאחד. מצב זה משפיע על אופן היצירה של מודיעין הסייבר וצריכתו ומאתגר את פונקציות הליבה של התהליך המודיעיני, קרי האיסוף, ההערכה, הניתוח, האינטגרציה, פירוש המידע והפצת המודיעין.

כאשר מדובר באיסוף ובהערכה, מודיעין הסייבר מסתמך גם על מידע המגיע ממקורות בלתי מבוקרים, דוגמת האינטרנט.[35] מידע זה דורש סינון, הערכה ותיקוף (במידה מסוימת). חשיבות מכרעת יש לסינון המידע, כדי שניתן יהיה לבחור מתוך המרחב הקיברנטי את פריטי המידע המשמעותיים בלבד. גם ההערכה היא משימה מאתגרת, וזאת עקב ההפכפכות הרבה, האנונימיות וחוסר הוודאות של הנתונים הזמינים במרחב הקיברנטי וההטרוגניות של מקורות המידע. מכאן, שכדי לתקף נתונים, יש חשיבות רבה לאימות המידע המופק ממקור אחד אל מול מידע המופק ממקורות אחרים, ועדיף שלפחות אחד ממקורות אלה יהיה מבוקר.

סינון, הערכה ותיקוף מיועדים למתן את מה שמכונה בשם "אנרכיית המידע", הנוצרת מן השילוב בין הנפח הגדל של הנתונים הזמינים ובין היעדר הבקרה עליהם. העובדה שתהליך היצירה של מודיעין הסייבר עשוי להתבסס גם על מידע/מודיעין המופק באמצעות דיסציפלינות אחרות, גורמת לכך שהשילוב בין כל החלקים

---

33 תחום זה הינו גם מרכיב וגם תוצר של המהפכה הדיגיטלית. ראו: Luciano Floridi, *Information: A Very Short Introduction* (Oxford: Oxford University Press, 2010); Luciano Floridi, *The Fourth Revolution: How the Infosphere is Reshaping Human Reality* (Oxford: Oxford University Press, 2016).

34 Warner, "Past and Future of the Intelligence Cycle", p. 16.

35 ניתן להגדיר איסוף כניצול מקורות ואספקת מידע המופק מהם לצורך עיבודו וניתוחו. מקור יכול להיות אדם, אובייקט, תהליך או מערכת מהם ניתן להשיג מידע. מקורות הינם בלתי מבוקרים כאשר הם אינם נמצאים תחת פיקוח והכוונה רשמיים של ארגון. דוגמה לכך הוא מידע הנוצר על ידי משתמשי אינטרנט או שחקנים אחרים במרחב הקיברנטי. הערכה ניתנת להגדרה כשלב בפונקציית הניתוח בו מתבצעת הערכה של המידע במה שנוגע לאמינות המקור ולמהימנות המידע. ראו, לדוגמה: "Understanding and Intelligence Support to Joint Operations", Joint Doctrine Publication 2-00, pp. 3-14, 3-20.

הרלוונטיים של הידע והפיכתו למוצר עקבי אחד יוצרת תופעה מאתגרת. זאת, עקב השוני בצורה, באופי ובמידת אי־הוודאות של המידע והמודיעין המתקבלים מהמרחב הקיברנטי (לדוגמה, מידע או נתונים טכניים אחרים המגיעים מרשתות חברתיות, פורומים ברשת וכן הלאה) בהשוואה למקורות "בלתי וירטואליים" אחרים.[36] מידת אי־הוודאות משפיעה גם על הפרשנות הניתנת למידע המעובד, כלומר, על הסקת המסקנות המבוססת עליו, הנכללות בדרך כלל במסגרת המוצר הסופי של מודיעין הסייבר. אי־ודאות זו צריכה להיות מובהרת גם לצרכן של מודיעין הסייבר, שחייב להיות מודע למגבלותיו העיקריות, ובעיקר בכל מה שנוגע לרמת הדיוק שלו.

היבט רלוונטי נוסף אותו יש להביא בחשבון בעת הגדרת מודל פרשני עבור תהליך מודיעין הסייבר הוא לוח הזמנים הצפוף הנדרש לעיתים תכופות לשם ביצוע משימות מודיעיניות. הדבר מחייב שהפעולות המודיעיניות יתבצעו בו־זמנית, או לחילופין שיימצאו קיצורי דרך כדי להוציאן אל הפועל. במילים אחרות, הפעולות הכרוכות במודיעין הסייבר אינן נעשות בצורה מעגלית, אלא מהוות "רשת רב־ערוצית" שלהן עצמן.[37]

נראה כי התנאים ליצירת מודיעין הסייבר שנדונו לעיל והאתגרים הכרוכים בהם מזרזים את הצורך בהגדרה של מודל ספציפי שיתן ביטוי טוב יותר לייחודיות של תהליך זה. צוות של מומחים ואנשי אקדמיה מן המכון לתוכנה ולהנדסה (SEI) של אוניברסיטת "קרנגי־מלון" בחן לפני מספר שנים את הספרות הקיימת בנושא זה והציע מודל המבוסס עליה.[38] המודל של SEI נבדל מ"מעגל המודיעין" המסורתי במינוח בו הוא עושה שימוש, בלוגיקה הבלתי לינארית והתוצאתית של הפעולות מהן מורכב התהליך, בחלוקה של פעולת הניתוח לשתי התמחויות נפרדות (ניתוח טכני או פונקציונלי וניתוח אסטרטגי) וביכולת של מודיעין הסייבר לתת מענה הן למטרות הטכניות "הצרות" של אבטחת הסייבר והן למטרות "הרחבות יותר" של מניעת איומי סייבר. המודל החדש מפרש את מודיעין הסייבר כתהליך אנליטי המסתמך על מידע/מודיעין הנאסף גם באמצעות דיסציפלינות אחרות ומיועד לספק מידע למקבלי ההחלטות בסוגיות המתייחסות לפעילויות בתחום הסייבר.[39]

המודל של SEI מורכב מחמש פונקציות: (1) הגדרת "הסביבה" שעל פיה נקבע היקף המאמץ להשגת מודיעין הסייבר, והמשפיעה גם על טיב המידע הנדרש

36 ניתן להגדיר אינטגרציה כפונקציה במסגרת התהליך המודיעיני, שבה המידע ו/או המודיעין המנותחים מנופים ומשולבים בתוך תבניות בתהליך יצירתו של מודיעין נוסף, שם, עמ' 3–22.

37 ראו, לדוגמה: Davies, Gustafson and Ridgen, "The Intelligence Cycle is Dead, Long Live the Intelligence Cycle" p. 64 ff.

38 Townsend et. al., "SEI Innovation Center Report".

39 שם.

כדי להשיגו;[40] (2) "איסוף הנתונים", או חקר המקורות ואיסוף וסינון של מידע באמצעות שימוש בכלים אוטומטיים ועתירי עבודה;[41] (3) "ניתוח פונקציונלי", כלומר ביצוע ניתוח טכני המותאם למשימה (לרוב, לצורך תמיכה במשימת אבטחת סייבר), שמטרתו היא להפיק את ה"מה" וה"איך" של איומי הסייבר;[42] (4) "ניתוח אסטרטגי", הכרוך בסקירה של מודיעין הסייבר הפונקציונלי, בשילובו עם מידע בעל הקשרים דומים ובהבהרה נוספת שלו, וזאת במטרה לענות על השאלות "מי" ו"מדוע";[43] (5) "דיווח ומשוב", כלומר הפצת מודיעין הסייבר למקבלי ההחלטות וקבלת משוב מהם.[44]

להלן פירוט של התחומים העיקריים שבהם קיימות תלות הדדית והשפעות הדדיות בין הפעולות השונות הכרוכות ביצירת מודיעין הסייבר: איסוף הנתונים מתבצע בהתאם להגדרת הסביבה, וזו מצידה מושפעת מן ההחלטות המתקבלות על ידי הארגון על בסיס מודיעין הסייבר שנצרך על ידו. המודיעין המתקבל מן הניתוח הפונקציונלי יכול לשמש כבסיס לקבלת החלטות בדבר פעולות שיינקטו ברמה הטכנית של רשת הארגון, שמצידן ישפיעו על הגדרתה של הסביבה הפנימית. אותו כלל חל גם על מודיעין המתקבל מן הפונקציה האסטרטגית, המשפיע על הסביבה הפנימית והחיצונית כאחת. הפונקציה האסטרטגית הופכת את המודיעין

40 שם, עמ' 2.9. המונח "סביבה" מתייחס לסביבה פנימית וחיצונית כאחת. הגדרת הסביבה הפנימית כוללת את חקר הנוכחות של הארגון בעולם הסייבר, את התשתית הנגישה באמצעות האינטרנט ואת הגדרת הנתונים אותם יש לאסוף כדי לשמור על ערנות באשר למתרחש ברשת. לצורך הגדרת הסביבה החיצונית יש לדעת אילו גופים הינם בעלי יכולת להשפיע על הרשתות של הארגון. הארגון חייב לגלות ולמפות את נקודות התורפה של המערכת, את כיווני החדירה או המתקפה עליה ואת הטקטיקה, הטכניקות, הנהלים והכלים המשמשים את הגורמים הרלוונטיים המאיימים עליה. כפי שנטען על ידי טאונסנד ואחרים, "השקעת הזמן והאנרגיה להגדרת הסביבה אפשרה לארגונים לשפר במידה משמעותית את פעולת איסוף הנתונים שלהם, וכתוצאה מכך להפוך את תוכניות מודיעין הסייבר ליעילות ולאפקטיביות יותר".

41 שם, עמ' 2.11. על איסוף המידע לכלול הן מקורות פנימיים (זרימת מידע ברשת, יומני תנועות, נתונים דמוגרפיים על המשתמשים) והן מקורות חיצוניים (ספקי מודיעין מצד שלישי, מידע ממקורות גלויים, רשתות חברתיות). על האיסוף להתמקד בסיכונים הרלוונטיים ובצרכים האסטרטגיים אשר זוהו במהלך לימוד הסביבה בה פועל הארגון. איסוף נתונים אפקטיבי צריך להתבסס על הגדרה של הסביבה. עליו להיות מכוון לנתונים הדרושים לצורך ביצוע ניתוח משמעותי של איומי סייבר קריטיים.

42 שם, עמ' 2.13. פונקציה זו כוללת אימות/תיקוף של נתונים על בסיס איכות המקור, היסטוריית הדיווח שלו ואימות בלתי תלוי באמצעות מקורות מאמתים אחרים.

43 שם, עמ' 2.15. ניתוח אסטרטגי מוסיף פרספקטיבה, הֶקשר ועומק לניתוח הפונקציונלי. הוא נטוע בסופו של דבר בנתונים טכניים, אך כולל גם מידע המגיע מחוץ למקורות הטכניים המסורתיים. הניתוח האסטרטגי מתאר פרופילים של גורמים מאיימים, יוצר את הערנות הנדרשת באשר למתרחש ברשת ומספק למקבלי ההחלטות מידע על ההשלכות האסטרטגיות של איומי הסייבר על ארגונים, תעשיות, כלכלות ומדינות.

44 שם, עמ' 2.17.

המתקבל מן הניתוח הפונקציונלי לשימושי יותר עבור מקבלי החלטות בכירים, שייתכן שהם נעדרים רקע טכני. מנקודת מבט זו, מדובר בסוג של יישום נוסף התורם לגישור על פערי התקשורת בין החוקרים בארגון ובין מקבלי ההחלטות בו. האחרונים מספקים משוב על המודיעין שהתקבל, ומשוב זה מסייע לעצב את הפעילות המחקרית של הארגון ולהסדיר ולכוון את דרכו. בכך משפיעים הבכירים בארגון על הסביבה.

מאמר זה לא מטפל בשאלת "תקפותו" של המודל של SEI. המודל גובש והוצג בעקבות עבודה אמפירית למיפוי והערכה של פרקטיקות קיימות בתחום מודיעין הסייבר בארצות הברית. הוא מבוסס על נתונים ומהווה את "המילה האחרונה" אצל ארגונים נבחרים שבסיסם הוא בארצות הברית. המודל הוא גם בעל השפעה נורמטיבית, כלומר, הוא מתאר כיצד תהליך גיבושו של מודיעין הסייבר אמור לפעול כדי שיהיה אפקטיבי. יתרה מזאת, יתרונו הוא בהיותו פשוט יחסית, ובה בעת מייצג את הפרקטיקות שאומצו על ידי ארגונים מסוגים שונים, כגון תאגידים קטנים, תעשיות גדולות יותר וסוכנויות ממשלתיות. יחד עם זאת, מידת הייצוג של מודל SEI צפויה להתפוגג ברמה הנמוכה ביותר וברמה הגבוהה ביותר של תהליך מודיעין הסייבר, כלומר ברמת הפרט מצד אחד וברמת השותפים המרובים, או הרמה העל־לאומית, מצד שני. סביר להניח כי המורכבות הארגונית/המוסדית ברמה העל־לאומית ומרובת השותפים הופכת את המודל המודיעיני של SEI לבלתי מתאים לרמה ארגונית זו. בנוסף לכך, יש להניח כי פיתוחים טכנולוגיים חדשים בתחום הסייבר ישפיעו על מודל זה ויחייבו הכנסת שיפורים שוטפים נוספים בו.[45] לפי המודל של SEI, האיסוף והניתוח הם תהליכים המתבצעים באופן עוקב, כלומר, שלב הניתוח יכול להתחיל רק לאחר השלמתו של שלב האיסוף. אלא שבפועל, קיימת אינטראקציה בין שתי הפונקציות והן יכולות להתרחש בו־זמנית. חרף האמור, יש להכיר בעובדה שהמודל המוצע על ידי המכון לתוכנה ולהנדסה הינו ניסיון מבוסס ראשוני להסביר בצורה טובה יותר את תהליך היווצרותו של מודיעין הסייבר ואת הדרכים העדיפות לגיבושו.[46]

מסקנות

יש חשיבות רבה להבנת התהליך של מודיעין הסייבר. הבנה כזאת יכולה לסייע לבעלי עניין לשמור על עקביות בכל הנוגע לקידום תוכניות או לנקיטת פעולות

45 מקדמיו של המודל מכירים בצורך זה במיוחד כשמדובר ביכולות האנליטיות: "מכיוון שהטכנולוגיה משתנה בקצב כה מהיר, הליך הפקתו של ניתוח מודיעין הסייבר צריך להיות דינמי דיו כך שיוכל להסתגל לכלים חדשים, ליכולות ולתחכום של היריבים המתפתחים במהירות".

46 דיון מעמיק יותר בתהליך מודיעין הסייבר ובגיבושו של מודל חלופי יתקיים במסגרת פרויקט המחקר.

הקשורות למודיעין הסייבר, וזאת ברמת המדיניות, ברמה המשפטית, במישור המבצעי ובתחומים נוספים. כדי להבין את תהליך מודיעין הסייבר יש להתבסס תחילה על הגדרה ברורה של המושג "מודיעין סייבר". המסגרת המושגית תשמש כשלד ליצירת הבחנות מושגיות, לארגון רעיונות ולקישור ביניהם, דבר שיאפשר הבנה מקיפה וכוללת של מודיעין הסייבר. אימוצה של מסגרת כזאת גם יהווה מרכיב חשוב בהפיכתו של מודיעין הסייבר לדיסציפלינה, כלומר, לתחום לימוד או פעילות מודיעיניים ספציפיים.

מרבית הספרות המקצועית מתייחסת כבר היום אל מודיעין הסייבר כאל דיסציפלינה מבוססת, או כזו שתתבסס בקרוב, אך נראה כי הדבר אינו כך. הבוסריות של הניתוח התיאורטי של מודיעין הסייבר, לצד הניסיון המוגבל יחסית בתחום זה, מקשים על ראייתו כתחום או כענף מודיעיני מוכר. במילים אחרות, אין לראות בשלב זה במודיעין הסייבר דיסציפלינה, משום שהוא עדיין אינו מוגדר דיו מבחינה תיאורטית ולא נוסה מספיק באופן מעשי. יתר על כן, אופיו של מודיעין הסייבר ותהליך יצירתו, כפי שתוארו לעיל, הופכים אותו לפרקטיקה אנליטית יותר מאשר לדיסציפלינה – פרקטיקה המסתמכת על מידע/מודיעין הנאסף גם באמצעות דיסציפלינות אחרות. יחד עם זאת, אין דבר שצריך למנוע ממודיעין הסייבר מלהפוך לדיסציפלינה, שתהליך גיבושה יעשה שימוש במשאבים טכניים או אנושיים ספציפיים לה.

תנאי מוקדם ליצירת מנגנוני שיתוף פעולה בתחום מודיעין הסייבר הוא הבנה משותפת של בעלי העניין לגביו. מדובר בהיבט חשוב, שכן תהליך יצירתו של מודיעין הסייבר דורש שיתוף פעולה הדדי ושיתוף ידע. כדי ששיתוף פעולה כזה יהיה אפקטיבי ומלא, עליו להתבסס לפחות על שפה משותפת ועל הבנת המושגים והמרכיבים של מודיעין הסייבר ושל תהליך גיבושו.

מאמר זה תורם להגדרת המושג "מודיעין סייבר" הן במובנו הצר והן במובנו הרחב (על בסיס הידע שכבר קיים בנושא), לזיהוי והבנייה של רכיבים מושגיים שלו ולפירושם באמצעות מסגרת תיאורטית בסיסית (וראשונית) ביותר. אין ספק כי יש להרחיב מסגרת תיאורטית זאת כדי שתכיל היבטים שונים נוספים של מודיעין הסייבר ותאפשר לפרקטיקה צומחת זו להתבסס ולהמשיך להתפתח.

סייבר, מודיעין וביטחון
קול קורא להגשת מאמרים לכתב העת

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

ייבחנו מאמרים הנוגעים לתחומים הבאים:

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

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

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

להגשת מאמרים ולפרטים נוספים ניתן לפנות לח"מ.

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

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