סייבר, מודיעין וביטחון

כרך 2 | גיליון 3 | דצמבר 2018

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

סייבר, מודיעין וביטחון

כרך 2 | גיליון 3 | דצמבר 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 2519-6677 (מודפס) • ISSN 2519-6685 (מקוון)

גניבת זהויות וחשיפה לתוכן פוגעני – סיכונים לבני נוער ברשת

לימור עציוני

ילדים ובני נוער משתייכים לקבוצת אוכלוסייה חלשה ופגיעה. פעילות של בני נוער וילדים ברשת חושפת אותם לשני סיכונים מהותיים: חשיפה לתוכן פוגעני וגניבת זהותם ושימוש בה לצורכי הכפשה ובריונות. מאמר זה בוחן את מאפייני התופעה ואת עוצמתה. המאמר מציע מספר דרכי פעולה במטרה למזער את הנזקים של סיכונים אלה לילדים ולבני הנוער, תוך התמודדות עם מגבלות הפרטיות הקיימות.

מילות מפתח: אינטרנט, בריונות רשת, גניבת זהויות, פורנוגרפיה, ילדים, בני נוער

מבוא

ההתפתחות הטכנולוגית טומנת בחובה יתרונות רבים, אולם לצידם יש לה חסרונות לא מעטים, החל בתלות המוחלטת של החברה בטכנולוגיה, הגוררת חשיפה להשבתת שירות ודליפת מידע בגין תקיפות סייבר, וכלה באפשרות להונאות פיננסיות ופגיעה פיזית בתהליכים קריטיים. על אף חומרתם של חסרונות אלה, ילדים ובני נוער ממשיכים להיות חשופים אליהם, ובמיוחד לשתי תופעות חמורות: גניבת זהות ברשת וחשיפה לתכנים פוגעניים.

גניבת הזהות ברשת הופכת להיות אחת הדאגות המרכזיות במרחב הדיגיטלי, כאשר בני נוער הם בין קבוצות הסיכון הפגיעות ביותר. גניבת הזהות והשימוש בזהות הבדויה נועדים, במקרים רבים, להכפשה ולמסעות ביוש (Shaming), העלולים להיות בעלי השלכות חמורות על בני הנוער שמהם היא נגנבה ולהשפיע על עתידם והתפתחותם. לצד תופעת גניבת הזהות מתקיימת חשיפה של ילדים

עו"ד ד"ר לימור עציוני הינה דקאנית משפטים במרכז האקדמי שערי מדע ומשפט, כותבת בימים אלה ספר אודות סייבר משפט רגולציה ומספקת ייעוץ וייצוג משפטי מקצועי, פלילי ואזרחי, לבני נוער ולבוגרים.

ובני נוער לתכנים פוגעניים. חשיפה מתמשכת לתכנים כאלה היא בעלת השלכות על ההתפתחות החברתית של בני הנוער, מגבירה את הנטייה לאלימות אצלם, ואף עלולה להשפיע על בניית מודלים מעוותים של יחסים בין־אישיים.

מהפכת המידע בכלל, ומהפכת התקשורת הדיגיטלית באינטרנט בפרט, מתבססות על שיטוח פערים בין חברות ותרבויות לטובת מטרות נעלות של פיתוח חינוכי, כלכלי וחברתי. החופש לעשות שימוש ברשת היה בשורה שסימנה הבטחה גדולה לפיתוח החברה והכלכלה גם במקומות הנידחים ביותר. בדרך זו התפתחה תופעת הגלובליזציה, שבמסגרתה מועברים מידע, ידע, קניין רוחני והון בין מדינות שונות באופן מיידי וללא כל קושי. עם זאת, מהפכת המידע יצרה שעבוד ליכולת לשנע מידע מסוגים שונים בקצב מהיר, בנפח גדול ועל גבי פלטפורמות שונות ומגוונות.[1]

ההתמקדות (ויש שיאמרו: ההשתעבדות) ביכולת לשתף מידע הדחיקה את הצורך לקיים מנגנוני בקרה על תוכן המידע. תחת הכותרת "ניטרליות הרשת" דוכאו הצורך והיכולת לקיים בקרת תוכן כלשהי. מבחינה תיאורטית, הצדק היה עם חסידי החופש ועם טענתם והבנתם שלגישה זו עשויות להיות תוצאות רצויות מבחינה חברתית ובעלות השפעה גם מעֵבר לתועלות המיידיות, כאלו המתבססות על תופעות לוואי רצויות (Externalities) של "ניטרליות הרשת". אלא שמבחינה מעשית, התנאים המצדיקים שימוש הוגן ברשת אינם מתקיימים במקום שבו פועל המודל של "ניטרליות הרשת".[2] כתוצאה מכך, נוצר מרחב פרוע, המאפשר העברה של תכנים פוגעניים מכל סוג שהוא ולכל משתמש.

היעדר מנגנוני בקרה, הן בצד המפיץ את המידע והן בצד המקבל אותו, הפך את האינטרנט לזירה של מציאות מופקרת, הפוגעת בעיקר בחלשים. בני נוער וילדים נחשפים לתכנים פוגעניים קשים, גם בעל כורחם. המצב הופך לבלתי נסבל כאשר, במקרים רבים, גם חיפוש ברשת אחר תוכן תמים מוביל לקפיצה של חלוניות עם תוכן פורנוגרפי, המזמינות את המשתמש להיכנס לאתר הפורנו. הזמינות הבלתי נתפסת של תוכן זה מקשה אפילו על ההורים להתמודד עם התופעה. כך, בלא כל בקרה, הופכים הילדים ובני הנוער לצרכני פורנו בעל כורחם.

ילדים ובני נוער משתייכים לקבוצת אוכלוסייה חלשה ופגיעה, הנתונה למניפולציה ולהשפעה מהירות. אלו יוצרות מצע רחב לשימוש פוגעני נוסף ברשת האינטרנט. התפתחותן של הרשתות החברתיות הביאה עימה תועלות רבות: השימוש ברשת יכול לסייע ביצירה של מערכת קשרים ענפה, באיתור עמיתים בעלי עניין משותף,

---

1 M. F. Mahmood & N. Hussin, "Information in Conversion Era: Impact and Influence from 4th Industrial Revolution", *International Journal of Academic Research in Business and Social Sciences*, 8 (9) (October 13, 2018): 320-328.

2 Keith N. Hylton, "Law, Social Welfare and Net Neutrality", *Review of Industrial Organization*, Vol. 50, No. 4 (June 2017): 417-429.

ביכולת להעביר מידע בזמן קצר ובתפוצה רחבה, ואף ביכולת לשווק שירותים ומוצרים עיסקיים באופן השווה לכל נפש ובתפוצה שהייתה בעבר שמורה רק לתאגידים עתירי משאבים. יחד עם זאת, השימוש הרחב ברשתות החברתיות הביא איתו בעיות לא קלות; גניבת זהויות בכלל וגניבת זהויות של בני נוער בפרט הפכו לרעה חולה, ששיטותיה משתכללות ומתפתחות, וכוללות, בין השאר, חדירה לחשבון קיים, השתלטות עליו ושימוש בו, לצד הקמת חשבון בדוי על שמו של הקורבן והתחברות לרשת המכרים שלו. כשמדובר בבני נוער, המטרה ברוב המקרים זהה: פרסום והפצה של פוסטים פוגעניים כדי לפגוע בבעל החשבון.

השאלה המרכזית המתעוררת בהקשר זה היא האם ניתן לאתר דרכים שיוכלו למזער את שני הסיכונים העיקריים לבני נוער ברשת – חשיפה לתוכן פוגעני וגניבת זהויות. זאת, תוך שמירת האיזון בין צורכי חופש המידע והפרטיות, שהינן נשמת אפה של דמוקרטיה ליברלית, ובין הצורך להגן טוב יותר על ילדים ובני נוער.

חסימת ילדים ובני נוער מפני תוכן פוגעני ברשת

הרעיון שלילדים יש זכות להגנה כאשר הם גולשים באינטרנט הוא עיקרון בסיסי בעולם הנשען על מגוון חוקים, שמטרתם היא למנוע התעללות וניצול באינטרנט. עם זאת, התנהלותם של ספקי תוכן מצד אחד, והקושי להטמיע הרגלי גלישה נורמטיביים לילדים מצד שני, מותחים את גבולות ההגנה ויוצרים דילמות חדשות בפני מחוקקים ברחבי העולם.[3]

לפי הבלוג Global Kids Online,[4] המאמצים להפוך את האינטרנט למקום בטוח יותר לילדים מחייבים יצירת איזון בין פיתוח מיומנויות דיגיטליות אצל בני הנוער מצד אחד, ובין גיבוש מדיניות כוללת להבטחת זכויות הילדים מצד שני. ניתוח שערך הבלוג הראה שילדים מתחילים להשתמש באינטרנט בגיל צעיר מאוד ומבלים ברשת זמן רב. כתוצאה מכך, עולה הסיכוי שלהם להיחשף לתוכן פוגעני כבר מגיל צעיר מאוד. התפוצה של מכשירי הטלפון החכמים מגבירה את הבעיה והופכת את החשיפה לזמינה במהלך כל שעות היממה, גם במצבים בהם אין נוכחות של הורה או מבוגר אחראי. שימוש מתון וקצוב ברשת יכול להועיל לרווחת הילדים, אולם שימוש רב ולא מרוסן בה עלול ליצור השפעה שלילית ארוכת טווח עליהם. ילדים שהם חסרי מיומנויות שימוש ברשת עלולים להיתקל בקשיים לימודיים וחברתיים, והניסיונות של הוריהם להפעיל עליהם הגבלות

3 Monica Bulger, Patrick Burton, Brian O'Neill, Elisabeth Staksrud, "Where Policy and Practice Collide: Comparing United States, South African and European Union Approaches to Protecting Children Online", *New Media and Society*, Vol. 19 No. 5 (January 16, 2017): 750-764.

4 "Making the Internet Safer for Children: The Global Evidence", *Global Kids Online*, February 6, 2018.

במטרה לצמצם שימוש שלהם ברשת עלולים להוות חרב פיפיות וליצור תגובת נגד הרסנית. לפי סקר שערך הבלוג, כ־14־36 אחוזים מבין הילדים ובני הנוער בגילים שבין 9־17 (בהתאמה) חווים חוויה פוגענית ברשת.[5]

בריטניה מתמודדת עם בעיה זו באמצעות החלטה שקיבלה ליצור מנגנון לאימות גיל לבני נוער באתרים פורנוגרפיים. האחריות על יישום מנגנון האימות היא של British Board of Film Classification (BBFC), שאמון על סיווג סרטים בבריטניה. גישה זו מבוססת על אילוץ ספקי אינטרנט בפס רחב ומפעילי רשתות סלולריות לחסום אתרי אינטרנט ויישומים שאינם משלבים אמצעי זיהוי לאימות גיל הגולש. עם זאת, לא ברור כיצד תופעל מערכת אימות הגיל וכיצד אפשר יהיה ליישמה באופן שלא ניתן יהיה לעקוף אותה, וכל זאת, מבלי לפגוע בפרטיות הגולשים ומבלי לשתף פרטים אישיים עם ספקי תוכן פורנוגרפי ופוגעני.[6]

אחת המפעילות של אתרי פורנו מרכזיים, דוגמת PornHub, YouPorn ו־RedTube, הציעה להשתמש בשילוב של פרטי כרטיס אשראי, מסרון SMS, פרטי דרכון או רישיון נהיגה כדי לאמת תאריך לידה של המשתמש.[7] נראה שגישה זו יוצרת בעיות פרטיות קשות במיוחד. מכל מקום, נכון לכתיבת שורות אלו, הפעלת המנגנון האמור נדחתה למועד כלשהו בעתיד.[8]

מדינת ישראל מתמודדת גם היא עם נושא זה, תוך ניסיון לחוקק חוק לחסימת תכָנים פוגעניים. מזה מספר חודשים מתקיים בישראל דיון הנוגע לדרכים לחסימת בני נוער בפני תוכן פוגעני ברשת האינטרנט. הצעת חוק ברוח זו אף אושרה בכנסת בדצמבר 2018, בוועדה משותפת לוועדת המדע ולוועדת הכנסת. נוסח החוק מאפשר למנויים על רשת האינטרנט לבחור אם ברצונם לחסום את החיבור שלהם לתכנים פוגעניים. הדיון בחוק, שקיבל את הכינוי "חוק הפורנו", נסב בעיקר סביב שני היבטים: הראשון נגע בצורך לסווג מהו תוכן פוגעני אותו נדרש יהיה לחסום, או באופן כללי יותר, בקושי ליצור רגולציה של תכנים באינטרנט, מרחב שבו בדרך כלל המדינה אינה מעורבת; ההיבט השני נגע בנושא הפגיעה בפרטיות. הצעת החוק השתנתה מספר פעמים, אולם ככלל, היא מבקשת מספקיות האינטרנט לשלוח הודעות למנויים, אשר יידרשו להשיב לאותן ספקיות במידה ויבקשו להפעיל שירות חסימה של תכנים פוגעניים.

בדיון על החוק עלו מספר נקודות, בהן הצורך לא להתייחס לכל קבוצת הילדים בגילאי 6־18 כמקשה אחת. זאת, מאחר וניתן להעריך כי הנזק הנגרם מחשיפה

5 שם.

6 Mark Jackson, "Age Verification and UK ISP Internet Porn Ban Quietly Delayed", *ISP News*, March 12, 2018.

7 Tom Allen, "Pornhub's 'AgeID' System will Require Punters to Hand Over their Date of Birth", *The Inquirer*, February 1, 2018.

8 Jackson, "Age Verification and UK ISP Internet Porn Ban Quietly Delayed".

לתכנים פוגעניים אינו זהה בכל קבוצת גיל. עוד עלה הצורך להטיל אחריות לא רק על ספקי האינטרנט, אלא גם על ספקי התוכן הפורנוגרפי, ובכלל זה לדרוש מהם להציב באתר שלהם חלונית אזהרה המטילה הגבלת גיל. במקביל, עלה הצורך לשמר את תשתית האינטרנט פתוחה וחופשית מצנזורה, כדי להגן על חופש הציבור. כמו כן, עלתה הצעה לאפשר למשתמש שלא השיב לדרישת ספק השירות לקבל סינון תכנים, להמשיך לקבל שירות מבלי שהסינון ייכפה עליו ללא הסכמתו.[9]

הצעת החוק, הדורשת מחברות שהן ספקיות שירותי אינטרנט לקבל תשובות בשאלות החסימה, תייצר בפועל רשומות שיאפשרו לדעת אלו מנויים ביקשו חסימה ואלו ביקשו לא לקבלה. הצעת החוק אמנם אוסרת על ספקיות האינטרנט לעשות שימוש במידע זה, אך עצם קיומה של הרשימה עלול להוות פגיעה חמורה בפרטיותו של אדם, במיוחד כאשר תוכן הרשימה עלול לדלוף לגורמים לא מורשים בשל תקלה או גניבה.

קיים קושי לקבוע תבחינים ברורים וחדים לצורך סינון חומרים באינטרנט. עוד בשנת 1964 התמודד עם נושא זה שופט בית המשפט העליון בארצות הברית, פוֹטר סטיוארט, שבמהלך משפט שנגע לחופש הביטוי אמר כי אינו יכול להגדיר מהי פורנוגרפיה, אולם הוא יכול לזהות אותה בבירור כשהוא רואה אותה ("I know it when I see it"). למרות הקושי, חברות האינטרנט הגדולות מסננות כבר כיום תכנים. כך, למשל, מסוננים תכנים ב"פייסבוק", ב"יוטיוב" ובפלטפורמות רשת נוספות. ניתן להניח שוועדה ציבורית שתוקם תוכל להציע קווים מנחים שיוכלו לאפשר סינון תכנים פוגעניים. קווים מנחים אלה ילכו וישתכללו במעלה הדרך.

הבעיה המרכזית של "חוק הפורנו" נותרה בעיית הפרטיות. כאן תוכל לסייע הטכנולוגיה שהתפתחה בעולם הפרסום הממוקד. האינטרנט שינה מהותית את שוק הפרסום ומאפשר פרסום ממוקד לקהלי יעד מוגדרים מראש. חברות האינטרנט הגדולות אוספות מידע רב על המשתמשים ברשת, הכולל עשרות מאפיינים, בכללם גיל, מגדר, שפה, מיקום, מצב משפחתי, מספר ילדים ועוד מאפיינים רבים. אלה נאספים ללא ידיעת המשתמש ונאגרים לצורך בניית פרופיל המאפשר פרסום ממוקד לקהלי יעד. כך, לדוגמה, פרסומת לתיקים יקרים לבתי ספר מתפרסמת היום רק באזור מסוים ורק להורים לתלמידים בגיל מסוים המתגוררים באותו אזור ועומדים במבחן הכנסה מסוים. טכנולוגיה זו משמשת גם לעריכת קמפיינים פוליטיים לקראת בחירות. בדרך זו ניתן לפנות עם מסרים ייעודיים לקהלים ממוקדים בכל פילוח וחתך.

שימוש בטכנולוגיה כזאת לצורך סינון יוכל להוות בשורה לילדים ולבני נוער. באמצעות טכנולוגיה זאת ניתן יהיה לזהות ילדים ברשת בכל חתך גיל ולאפשר חסימה מיידית של תכנים בהתאם לגיל המשתמשים. באותה שיטה ניתן יהיה

9 גדעון אלון, "'חוק הפורנו' אושר בוועדת השרים לחקיקה", **ישראל היום**, 12 בדצמבר 2018.

לקבוע גם מדרגות סינון בהתאם לקבוצת הגיל. לדוגמה, ניתן יהיה לקבוע חסימה מסוימת לגילאים 5־9, חסימה אחרת לגילאי 9־12 וכן הלאה, במקום לאכוף חסימה גורפת וכמקשה אחת לכל בני הנוער. בנוסף לכך, שיטה זאת תמנע פגיעה בפרטיות המשתמשים, מאחר והסינון לא יזהה את המשתמש בפועל, אלא רק את קבוצת התבחינים שלו.

אין טכנולוגיה החפה משגיאות. ניתן להניח שיתרחשו מקרים שבהם ילדים ייחשפו לתכנים פוגעניים בעקבות שימוש בטכנולוגיה המדוברת, או שמבוגרים ייחסמו בפני תכנים כאלה. אולם, הניסיון מעולם הפרסום מראה שחריגות כאלו יסתכמו באחוזים נמוכים. לפיכך, שימוש בטכנולוגיה המוצעת יפחית משמעותית את היקף התופעה ויאפשר איזון בין פגיעה בפרטיות ובחירויות אחרות ובין הצורך להגן על ילדים ובני נוער ולאפשר להם התפתחות בריאה וראויה.

גניבת זהויות של בני נוער ברשת

"היי נועה, אנחנו לא מכירות, אבל יש מישהי שמשתמשת בתמונה שלך ויצרה פרופיל ב'פֵייס'". זו הייתה הודעה שקיבלה נועה בנוש.[10] כך הבינה נועה שקמה לה מתחזה שעשתה שימוש בתמונותיה בחשבון "פייסבוק" בדוי. יריב (שם בדוי), נער בכתה י', התעורר בוקר אחד לגלות שבחשבון ה"אינסטגרם" שלו הועלו פוסטים אותם הוא לא כתב ותמונות שלא הכיר. מישהו הצליח, ככל הנראה, להיכנס לחשבון שלו ולהעלות פוסטים פוגעניים ומשפילים. הוא מצא עצמו מנסה לשתף את חבריו כדי למזער את הנזק, אך הצלחתו בכך הייתה מעטה. חלק ממכריו היו מהירי תגובה, והיו בהם מי שכבר ניצלו את האירוע כדי להעמיק את הפגיעה. אירועים דומים מתרחשים בקצב הולך וגובר.

רשתות חברתיות הפכו להיות פופולריות מאוד. לפי דוח של Global Social Media Research, מספר המשתמשים ברשתות חברתיות ברחבי העולם, נכון לשנת 2018, הינו קרוב ל־3.2 מיליארד, ומספר זה גדל בקצב של 13 אחוזים בכל שנה.[11] רובם המכריע של בני הנוער הם בעלי חשבונות ברשתות חברתיות, ו־45 אחוזים מהם מחוברים כמעט באופן קבוע.[12] נתונים אלה מדהימים בעוצמתם.

מלבד הפיכתה של הרשת החברתית לפופולרית בקרב בני נוער, היא פופולרית גם עבור פעילות לא חוקית, בריונית ופושעת. הפשעים העיקריים ברשת ניתנים לסיווג למספר קטגוריות: בריונות של הטרדות ואיומים מקוונים, וכן גניבת זהויות למטרות דומות. אירועים אלה נפוצים מאוד. בטבלה שלהלן ניתן לראות את היקף

10 נועה בנוש, "פתאום קם אדם ומגלה שגנבו את זהותו בטינדר", *Ynet*, 12 בינואר 2018.

11 Dave Chaffey, "Global Social Media Research Summary 2018", *Smart Insights*, November 23, 2018.

12 Monica Anderson and Jingjing Jiang, "Teens, Social Media & Technology 2018", *Pew Research Center, Internet & Technology*, May 31, 2018.

תופעת הבריונות ברשת במדינות שונות בעולם (לא כולל ישראל), שחלקה נגרם בשל גניבת זהות ומסעות בִּיוש. הטבלה מתייחסת (באחוזים) להורים שדיווחו על חשיפת ילדיהם לבריונות ברשת.[13]

מדינה	2011	2016	2018
הודו	32	32	37
ברזיל	20	19	29
ארצות הברית	15	34	26
בלגיה	12	13	25
דרום אפריקה	10	25	26
מלזיה	--	--	23
שוודיה	14	20	23
קנדה	18	17	20
טורקיה	5	14	20
ערב הסעודית	18	17	19
אוסטרליה	13	20	19
מקסיקו	8	20	18
בריטניה	11	15	18
סין	11	20	17

ניתוח הטבלה מראה את ממדיה המבהילים של התופעה. ניתן להניח שהיקף התופעה במדינת ישראל דומה להיקפה במדינות מערביות אחרות (דוגמת ארצות הברית, שוודיה ובריטניה).

בני נוער מרבים לעשות שימוש באינטרנט, אולם למרבה הצער, הבקרה אותה הם מפעילים כלפי התוכן המועלה לאתרים נמוכה מאוד. אותם בני נוער משתפים פרטים אישיים רבים ללא כל בקרה, ובכלל זה שמות מלאים, תמונות, שמות בני משפחה, מספרי טלפון, תאריכים חשובים, כתובות מגורים ועוד. כל אלה מהווים מצע טוב לגונבי זהויות, שיכולים להעלות בעקבות הגניבה פוסטים אמינים לכאורה. גם רמת המודעות לאבטחה אצל בני נוער הינה ירודה. הם עושים שימוש בחיבורי רשת אלחוטית שאינה מאובטחת, ובדרך כלל משתמשים באותן סיסמאות עבור חשבונות שונים. נמצא גם שבני נוער רבים משתפים ביניהם סיסמאות לא רק עם בני משפחה, אלא גם עם חברים.[14] הרושם הכללי בציבור הנו שבני נוער מודעים

13 Sam Cook, "Cyberbullying Facts and Statistics for 2016-2018", *Comparitech*, November 12, 2018.

14 Leigh, "Teenagers are Easy Victims of Identity Theft", *Homeschooling Teen Magazine*, 2018.

יותר ממבוגרים לבעיות האבטחה ברשת הינו שגוי. ברוב המקרים, נערים אינם מפעילים היגיינת רשת בסיסית, כגון ביצוע עדכוני אבטחה ומניעת העברת פרטים רגישים ברשת. תופעות אלו גורמות לבני הנוער להיות מטרה קלה מאוד לגונבי הזהויות, הן לצורך חדירה לרשתות החברתיות והן לצורך גניבת זהויות של בני משפחה לצורכי הונאה. מחקר שנערך בארצות הברית בקרב 500 הורים לילדים שזהותם נגנבה, הראה שקבוצת הסיכון הגדולה ביותר לגניבת זהויות הינה בגילים שבין 12־17 (44 אחוזים).[15]

כיצד ניתן להתמודד עם התופעה? גניבת זהות והתחזות ברשת הן עבירה פלילית בישראל, המוצאת ביטוי במספר חוקים: בחוק המחשבים (התשנ"ה–1995) נקבעה ענישה של שלוש עד חמש שנות מאסר למי ש"משבש את פעולתו התקינה של מחשב או מפריע לשימוש בו. מוחק חומר מחשב, גורם לשינוי בו... עושה פעולה לגבי מידע כדי שתוצאתה תהיה מידע כוזב או פלט כוזב. חודר שלא כדין לחומר מחשב הנמצא במחשב". הסעיף הרלוונטי לענייננו הוא, קרוב לוודאי, זה הנוגע לפעולה שתוצאתה מידע כוזב או פלט כוזב. לצידו של חוק זה עומד החוק להגנת הפרטיות (התשמ"א–1981). אף שחוק זה נוגע להגנתו של מידע פרטי של אדם במאגרי מידע, יש מקום לבחון אם חשבונות ברשתות חברתיות יכולים ליפול גם הם תחת הגדרה זאת, מה שירחיב את אחריותן של חברות האינטרנט הגדולות למידע, לאבטחתו ולמניעת שימוש במידע כוזב של משתמשים. לבסוף ניתן להישען על חוק איסור לשון הרע (התשכ"ה–1965). לפי חוק זה, לשון הרע היא דבר שפרסומו עלול "(1) להשפיל אדם (יחיד או תאגיד) בעיני הבריות או לעשותו מטרה לשנאה, לבוז או ללעג מצדם; (2) לבזות אדם בשל מעשים, התנהגות או תכונות המיוחסים לו; (3) לפגוע באדם במשרתו, אם משרה ציבורית ואם משרה אחרת, בעסקו, במשלח ידו או במקצועו; (4) לבזות אדם בשל גזעו, מוצאו, דתו, מקום מגוריו, גילו, מינו, נטייתו המינית או מוגבלותו." הִתחזות ברשת והעלאת פוסטים פוגעניים ומשפילים מאפשרות להגיש תביעה פלילית וגם ייחשבו כעוולה אזרחית, המקנה את הזכות לפיצוי הקורבנות.

קשה לראות כיצד מקטינים את חשיפת בני הנוער לרשתות החברתיות, המגיעה לעיתים לכדי התמכרות. לכן, לצד ההישענות על החוק, ראוי לפעול גם בדרכים נוספות. חיוני ללמד בני נוער כיצד להתנהל ברשת, הן בהקשרי אבטחת החשבונות והן בבקרת התוכן אותו הם מעלים, מתוך הבנת המשמעויות וההשלכות של שיתוף מידע אישי ברשת. ככל הנראה, לא ניתן יהיה למנוע לחלוטין את התופעה, ולכן, לצד פעולות אלו חשובה הקשבה לנפגעים וסיוע להם. מספר עמותות כבר החלו לפעול בכיוון זה.

15 Matt Tatham, "Survey: 12 Years Old Is the Average Age of a Child Identity Theft Victim", *Experian*, August 26, 2018.

האינטרנט, הרשתות החברתיות ותוכניות המסרים המיידיים יוצרים הזדמנויות חיוביות רבות בשיטוח פערים ובמתן הזדמנויות שוות. אולם, לצד זאת קיימים סיכונים עצומים לבני הנוער, המהווים אוכלוסיית סיכון פגיעה מאוד. טוב יהיה אם נשכיל לבנות מנגנוני הגנה משוכללים וטובים יותר למניעת פגיעה ובריונות באמצעות הִתחזוּת. גם ראוי שנתבע מחברות האינטרנט הגדולות לפעול באופן נחוש יותר כדי למנוע תופעות אלו.

סיכום

ילדים ובני נוער חשופים לסיכוני רשת רבים ואינם בעלי כלים מתאימים להתמודדות עם סיכונים אלה. מאמר זה ניתח שני סיכונים מרכזיים: חשיפת בני נוער לתכנים פוגעניים וגניבת זהותם לצורך ביזוי, ביוש והכפשה. מדינות שונות כבר החלו לפעול במטרה לספק כלים למזעור בעיית חשיפתם של בני נוער לתכנים פוגעניים. גם מדינת ישראל עושה זאת. אולם, הניסיונות הראשונים נתקלים בהתנגדויות משני כיוונים עיקריים: הראשון הוא הטיעון בדבר הצורך לשמר את הניטרליות של הרשת ולמנוע כל צנזורה על התכנים שבה; השני הוא הקושי לאתר מנגנון שימנע פגיעה בפרטיות. המנגנון המוצע במאמר זה יוכל לסייע לפתרון באמצעות חסימה של תכָנים פוגעניים, לפי קריטריונים של המשתמשים ברשת, כפי שהדבר כבר מבוצע על ידי חברות האינטרנט הגדולות בבואן לספק שירותי פרסום לקהלי יעד ממוקדים.

בני נוער אינם ערניים מספיק לאפשרות שזהותם תיגנב וייעשה בה שימוש בריוני. לרובם, הסיכון להפוך לקורבן אינו מוחשי, ולכן הם אינם מודעים להשלכות החמורות של אירועים כאלה. למרבה הצער, גניבת זהות יכולה להרוס את יכולתו של הצעיר להתפתח, או לפגוע בה אנושות. טוב יהיה לאמץ פתרון משולב לבעיית גניבת הזהות, שעיקרו העמקת המודעות של בני הנוער לסיכון, תוך הטמעת התנהלות מתאימה ברשת, אכיפה מחמירה ושימוש בחוקים קיימים, ולבסוף, סיוע למי שנפגעו מרעה חולה זו.

זוהי רק תחילתה של הדרך. הנזקים הנגרמים לבני נוער ולילדים ברשת עודם רבים. טוב וחשוב להעמיק את המחקר סביב הדרכים למזעור התופעה ולהתמודדות איתה.

דְּלֵית אֲתַר פָּנוּי מִנֵּיהּ – על הגנת הפרטיות ואיסור החדירה לרשומותיו של אדם במשפט העברי

אביעד הכהן וגבי סיבוני

התפתחות השימוש באינטרנט מעלה שאלות כבדות משקל באשר לזכותו של אדם לפרטיות ולחובתן של חברות לשמור על מידע פרטי שהופקד בידיהן. בפועל, מתרחשים אירועים רבים מדי בהם מידע פרטי חסוי זולג אל מחוץ לחברות האמונות על שמירתו, ולפעמים אף נמכר לגורמים פליליים. מערכת המשפט וגורמי הרגולציה המערביים עוסקים כיום לא מעט בנושא זה, אולם במשפט העברי התפתח דיון בתחום חשוב זה כבר משחר ההיסטוריה היהודית. מאמר זה מבקש לסקור התפתחות זו, במיוחד לאור המתרחש במרחב הסייבר בשנים האחרונות.

מילות מפתח: פרטיות, משפט עברי, סייבר, פרסום מקוון

מבוא

לאחרונה התפרסמו ידיעות מטרידות על שימוש שעושה הרשת החברתית הגדולה "פייסבוק" במידע פרטי של החברים בה. "פייסבוק" סובלת בתקופה האחרונה מפרסום שלילי לאור בעיות באבטחת פרטי המשתמשים בה, כמו גם בשל השימוש שהיא עושה במידע אישי שלהם כדי להגדיל את הכנסותיה מפרסום ממוקד. אולם נדמה שהבעיה חמורה הרבה יותר: מצד אחד, חברת "פייסבוק" מציעה להשתמש בהזדהות כפולה (Two Factor Authentication), כדי להגביר את הקושי לגנוב מידע אישי של המשתמשים בה. לצורך זה נדרשים המשתמשים לספק לחברה את

פרופ' אביעד הכהן הוא נשיא המרכז האקדמי שערי מדע ומשפט, דיקן בית הספר למשפטים וראש המרכז להוראת המשפט העברי ולימודו. פרופ' הכהן הוא מומחה למשפט חוקתי ועמית בכיר במכון ון ליר בירושלים.
ד"ר אל"ם (מיל') גבי סיבוני הוא ראש תוכנית ביטחון סייבר במכון למחקרי ביטחון לאומי.

מספר הטלפון הסלולרי שלהם; מצד שני, "פייסבוק" עושה שימוש מסחרי במספרי הטלפונים הסלולריים האלה לצורך העמקת הפרסום הממוקד של החברה עצמה.[1]

חוקרים הצליחו להוכיח כי חברת "פייסבוק" מאפשרת באופן שיטתי שימוש במידע מזהה, דוגמת מספרי טלפון אישיים, לצורך פרסומות ממוקדות המיועדות לבעלי אותם טלפונים. זאת, באמצעות פרופילים של משתמשים הנשמרים בחוסר שקיפות, שלמשתמשים עצמם אין כל גישה אליהם, וחמור מכך, אין להם יכולת לפעול בנדון.[2] פירוש הדבר הוא שגם אם המשתמש אינו מעוניין ש"פייסבוק" תאפשר למפרסם למקד אליו את הפרסום לפי מספר הטלפון שלו, החברה עדיין מוצאת דרך לעשות זאת ולכוון את הפרסום אליו באמצעות מגוון של פרטים אישיים.[3]

על דרך ההשאלה, ובלשון קדמונים, ניתן היה לומר "דְּלֵית אֲתַר פָּנוּי מִנֵּיהּ",[4] כלומר, כמעט ואין מקום שפנוי מעינו הבוחנת של "האח הגדול", הלוא הן חברות הענק שפועלות במרחב הסייבר, העושות שימוש במידע שנצבר בכליהן. ברובד המשפטי והמוסרי, ניתן לדַמות זאת למעשה שבו החוטא יוצא נשכר,[5] תחת שישלם על חטאו; לא רק שהוא עובר עבירה, אלא שהוא גם מקבל שכר עליה, מעין "הֶרָצַחְתָּ, וְגַם־יָרָשְׁתָּ".[6]

"פייסבוק" אינה יחידה בעניין זה. גם חברות אחרות עושות שימוש במנגנונים דומים, כשהמניע הכלכלי שמאחורי הדברים הוא ברור. כאשר מפרסם רוצה לפרסם מודעה, הוא מבקש למקסם את חשיפת המוצר שלו ולהציגו בפני קהל יעד רלוונטי למוצר שאותו הוא מבקש למכור. כך נוהגות חברות האינטרנט הגדולות, דוגמת "טוויטר" "גוגל" וכאמור "פייסבוק", וחברות אחרות. הן מספקות מנגנוני מיקוד לקהלי יעד, תוך שימוש במידע שנאסף על המשתמשים, כשברוב המקרים איסוף מידע זה והשימוש בו נעשים ללא ידיעתם או הסכמתם.

פעולותיהן של ענקיות אינטרנט אלו פוגעות בזכות לפרטיות, שהינה אבן פינה ויסוד מוסד בתורת זכויות האדם. עיקרה של הזכות לפרטיות היא זכותו של אדם ל"צנעת חייו" ולקיום מרחב פרטי, פיזי או וירטואלי, הנתון לשליטתו הבלעדית, שאינו מופרע על ידי אחר ללא הסכמתו ושלא ברצונו. יש הרואים את מקורה של זכות זו ב"זכויות הטבעיות", כגון הזכות לחיים וכבוד האדם וחירותו, הנתונות

---

1 Lowell Heddings, "Facebook is Using Your Phone Number to Target Ads and You Can't Stop It", *How to Geek*, September 28, 2018.

2 Ibid.

3 Kashmir Hill, "Facebook Is Giving Advertisers Access to Your Shadow Contact Information", *Gizmodo*, September 26, 2018.

4 תיקוני זוהר, תקונא שבע וחמשין, דף צב ע"ב.

5 ראו לדוגמה בבא קמא, לח, ע"ב.

6 **מלכים א'**, כא, י"ט.

לכל אדם באשר הוא אדם. אחרים רואים בזכות לפרטיות מעין "סעיף" של זכות האדם לכבוד, או אמצעי למימוש האוטונומיה שלו בהתאם לרצונו.

יש רבים בימינו הרואים את הזכות לפרטיות כזכות "צעירה" למדי בתורת משפט זכויות האדם, בהשוואה לשאר הזכויות. הם מציינים את "הולדתה" במאמרם המכונן של סמואל ווארן ושותפו למשרד לואיס ברנדייס, שכיהן לימים כשופט היהודי הראשון בבית המשפט העליון של ארצות הברית. עוד בשנת 1890 הם פרסמו, מאמר על "פרטיות" בכתב העת של בית הספר למשפטים באוניברסיטת הרווארד.[7] במאמר זה דיברו המחברים על מהות הזכות ומקורה, והרחיבו את מידותיה לא רק כלפי זכותו של אדם שלא יפגעו ב"סוד שיחו" ויחשפו פרטים ונתונים אישיים שלו (כגון פרטים על מצבו הרפואי, מצבו הכלכלי או עבירות שבהן הורשע בעבר), אלא גם כלפי זכותו של אדם להיוותר לבדו ו"להיעזב במנוחה", מבלי שזו תופרע בעל כורחו ושלא לצורך.

במשפט הישראלי נקבע עקרון יסוד חוקתי זה בסעיף 7(א) לחוק יסוד: כבוד האדם וחירותו, הקובע: "כל אדם זכאי לפרטיות ולצנעת חייו". מוסיף עליו סעיף 1 לחוק הגנת הפרטיות, התשמ"א–1981, הקובע: "לא יפגע אדם בפרטיות של זולתו ללא הסכמתו". כשאר זכויות האדם, גם זכות זו אינה מוחלטת. ניתן לסייגה מטעמים שבביטחון המדינה, בשמירה על חיי אדם, שלומו ובריאותו וכיוצא באלה.

הזכות לפרטיות והאיסורים שכרוכים בה הם משפחה גדולה של תת־זכויות ופרקי משנה. ביניהם: איסורים להאזנת סתר, לחיפוש בגופו ועל גופו של אדם, לחיפוש הכרוך בחדירה לצנעת ביתו של אדם, למעקב אחריו, איסור על עיון במסמכיו האישיים שלא ברשותו ובידיעתו, איסור חדירה למחשבו האישי ולפרטי התוכן האצורים בו וכיוצא באלה. בחינת מקורות הזכות לפרטיות במשפט העברי עשויה ללמדנו כי למרות המציאות המתחדשת לבקרים בנושא זה, עקרונות השמירה על פרטיות האדם וזכותו לצנעת חייו הם עתיקי יומין וניתן לעגן בהם פתרונות לסוגיה זו בימינו ולימֵינו.

מקורות הזכות לפרטיות במשפט העברי

יש הנוטים לעגן את הזכות לפרטיות במשפט העברי כבר בנבואת בלעם הנזכרת בספר במדבר: "וישא בלעם את עיניו, וירא את ישראל שֹׁכֵן לשבטיו... וישא משלו ויאמר... מה טֹבוּ אֹהליך יעקב, משכנותיך ישראל".[8] על אף שהקשרו של פסוק זה אינו משפטי־נורמטיבי, כופה ומצווה (דוגמת "לא תרצח" ו"לא תגנוב" שבעשרת

7 Samuel D. Warren, Louis D. Brandeis, "The Right to Privacy", *Harvard Law Review*, Vol. 4, No. 5 (December 15, 1890): 193-220.

8 **במדבר** כ"ד, ה'. מעניין לציין שדווקא פסוק זה, שנאמר על ידי לא יהודי – נביא מדְיָן – נבחר לפתוח את סידור התפילה היהודי והוצב בראש תפילת השחרית הנאמרת מדי יום. בדורנו קבע "קול ישראל" לפתוח את שידורי הרדיו שלו מדי בוקר בציטוט פסוק זה.

הדיברות), אלא בנבואה שירית של בלעם, שבא לקלל את ישראל ונמצא מברכם, שימש הפסוק כבר במקורות חז"ל הקדומים כמקור חוקי־משפטי שניתן לעגן בו את איסור הפגיעה בצנעת הפרט והחדירה לפרטיותו של אדם. בבואם להסביר מה בדיוק היה כה "טוב" ב"אהלי יעקב" שבהם צפה בלעם, אמרו חכמים: "מה טֹבוּ – על שראה פתחיהם, שאינן מכוונין זה מול זה".[9] שִׁבחָם של ישראל התבטא, אפוא, בעיניו בשמירתם הקפדנית על הזכות לפרטיות.

איסור הפגיעה בצנעת חייו של אדם נזכר באופן ספציפי במשפט העברי בהקשר לסוגיות רבות,[10] שמהן ובהן בא לביטוי מעמדו החשוב, הן במישור של "סור מרע ועשה טוב" – החובה למנוע מלכתחילה פגיעה בזכות הפרטיות ויצירת אמצעי מנע – והן במישור העניש שלאחר מעשה. כך, לדוגמה, נאמר כבר במשנה: "לא יפתח [אדם] לחצר השותפין פתח כנגד פתח וחלון כנגד חלון. היה [פתחו או חלונו] קטן – לא יעשֶׂנו גדול; אחד – לא יעשֶׂנו שניים".[11] התלמוד שואל: "מנהני מילי [היכן מקורם של דברים אלה]? אמר רבי יוחנן: דאמר קרא [הפסוק]: 'וישא בלעם את עיניו וירא את ישראל שכן לשבטיו'. מה ראה? ראה שאין פתחי אוהליהן מכוונין זה לזה. אמר: ראויים הללו שתשרה עליהם שכינה".[12] בפירושו לתלמוד מסביר הרשב"ם – רבי שמואל בר מאיר[13] – שאיסור פתיחת פתח חדש הפונה לחצרו של חברו (או אפילו לחצר המשותפת לשניהם) נועד למנוע "היזק ראייה", כלומר פגיעה בצנעת הפרט של הזולת.[14]

אליהו ליפשיץ מציין,[15] שמן המשנה עולה כי הפגיעה בפרטיות הנגרמת כתוצאה מפתיחת חלון לחצר המשותפת אינה נזק **מוחלט**, אלא רק נזק **יחסי**. זו הסיבה שאין דרישה לסתום חלון קיים, אף אם היה גדול, ורק נאסר לפתוח חלון חדש או להגדילו. אם החלון היה קיים עוד לפני שהגיעו השכנים למקום, אין הם יכולים להכריח את בעל החלון לשנות את מצבו לרעה, ועליהם להישמר בעצמם מפני הפגיעה בפרטיותם. הלכה זו סוכמה בידי הרמב"ם בחיבורו "משנה תורה": "מי שהיה לו חלון בכותלו, ובא חברו ועשה חצר בצִדו, אינו יכול לומר לבעל החלון: סתום חלון זה כדי שלא תביט בי, שהרי החזיק [בעל החלון] בהיזק זה".[16]

---

9 ראו, לדוגמה, **רש"י**, במדבר כ"ד, ה'

10 א' ליפשיץ, "הזכות לפרטיות במשפט העברי ובמשפט המדינה", בתוך: א' הכהן ומ' ויגודה (עורכים) **פרשת השבוע**, ירושלים, תשע"ב, כרך ד', עמ' 195; ש' אהרוני־גולדברג, "פרטיות באינטרנט בפריזמה הלכתית", **הפרקליט**, נב, תשע"ג, עמ' 151־234.

11 **משנה**, מסכת בבא בתרא, פרק ג, משנה ז.

12 **תלמוד בבלי**, בבא בתרא, ס, ע"א.

13 פרשן המקרא, התלמוד ומבעלי התוספות, נכדו של רש"י ותלמידו. חי במחצית הראשונה של המאה ה־12.

14 **רשב"ם**, בבא בתרא, נט, ע"ב, ד"ה "לא יפתח".

15 ליפשיץ, "הזכות לפרטיות במשפט העברי ובמשפט המדינה".

16 **רמב"ם**, הלכות שכנים, פרק ז, הלכה א.

חרם דרבנו גרשום על עיון בתוכן מכתב ללא רשות הכותב

צעד משמעותי ביותר בהגנה על צנעת חייו של אדם הנוגעת למסמכיו האישיים, כגון רשומותיו הרפואיות, מכתבים שכתב, ובימינו חומר האצור במחשבו האישי, נעשה במשפט העברי בעקבות תקנה שהתקין רבנו גרשום מאור הגולה, גדול חכמי אשכנז (גרמניה) במאה העשירית. בין שאר התקנות שתיקן,[17] קבע רבנו גרשום חרם על מי שמעיין במכתבי זולתו ללא רשותו, ובכך פוגע בפרטיותו. נוסח החרם הגיע אלינו ממקור מִשני, בין השאר אגב ציטוטו בספר השאלות והתשובות של המהר"ם – רבי מאיר מרוטנבורג.[18] וכך נאמר שם: "חרם שלא לראות בכתב חברו, ששולח לחברו, בלא ידיעתו".[19]

לימים נתקבע החרם של רבנו גרשום והיה לאבן יסוד בהלכה היהודית, עד כדי כך, שבעקבותיו החלו רבים לציין בראש מסמכים פרטיים שלהם כי החרם חל על העיון בהם. יש שנהגו להוסיף: ופגי"ן – "ופורץ גדר ישכנו נחש",[20] או נח"ש – ראשי תיבות של "נידוי, חרם ושמתא" דרבנו גרשום.[21] ביטויים אלה ממחישים את חומרת איסור הפגיעה בצנעת הפרט בעיני חכמי ההלכה.

טעמי האיסור במקורות המשפט העברי

כבר בדורות קדומים, שנים רבות לפני פרסום מאמרם של וורן וברנדייס, התחבטו חכמי המשפט העברי בדבר מקור האיסור לפגיעה בצנעת הפרט וטעמיו. אחדים מהם הפליגו למחוזות רחוקים וראו בפתיחת איגרת מעין "עשיית עושר ולא במשפט". לדעתם, הפוגע בצנעת כתביו של חברו מתכוון, בדרך כלל, להפיק מכך תועלת מעשית – כלכלית או אחרת – תוך עשיית שימוש בנכס של חברו שלא כדין. אחרים ראו בחדירה לצנעת כתביו של אדם ענף של האיסור "שאִילה שלא־מדעת", כלומר, מעשה שכמוהו כגזל, האסור אפילו לשם דבר מצווה.[22]

לימים הרחיב רבי חיים פלאג'י[23] את טעמו של איסור זה בכיוון אחר – לשדה ה"איסורי" ולא ה"משפטי" של המשפט העברי.[24] לדעתו,[25] מי שפותח וקורא

17 המפורסמות שבתקנות אלו הן האיסורים לגרש אישה בעל כורחה ולשאת יותר מאישה אחת.

18 מחכמי אשכנז (גרמניה) במאה הי"ב.

19 **שו"ת מהר"ם מרוטנבורג**, חלק ד, סימן אלף, סעיף כב.

20 פסוק שמקורו בספר קהלת י, ח. על מנהג זה, ראו המקורות בהערה הקודמת.

21 **תורת חיים**, ג, מז; **אנציקלופדיה תלמודית**, הערך "חרם דרבנו גרשם" (ובמהדורה המקוונת של "המיקרופדיה התלמודית" הנמצאת ברשת האינטרנט).

22 **תורת חיים**, שם; אנציקלופדיה תלמודית, שם.

23 מחכמי איזמיר, טורקיה, במאה הי"ט.

24 על הבחנה זו בין החלק ה"איסורי" לבין החלק ה"משפטי" שבתורת ישראל ראו בהרחבה: מ' אֶלון, **המשפט העברי**, הוצאת מאגנס, ירושלים תשמ"ח, עמ' 100–124.

25 רבי חיים פלאג'י, **שו"ת חקקי לב**, חלק יורה דעה, סימן מט.

מכתב של חברו ללא ידיעתו הוא כגונב את "מצפוני ומסתרי לבו", ובכך עובר על האיסור החמור של "גניבת דעת". לצד זה, מזכיר רבי חיים פלאג'י כמקור אפשרי להחלת איסור הפגיעה בצנעת הפרט גם את העיקרון הכללי ורחב היריעה של מצוות "וְ·הַבְתָּ לְרֵעֲךָ כָּמוֹךָ"[26], שכידוע התפרש בתורתם של חכמים ראשונים על דרך השלילה: "מה ששנוא עליך – אל תעשה לחברך".

נימוק מעניין אחר לאיסור החדירה לצנעת כתביו של אדם ומאגריו ניתן בפי חכם הלכה אחר, רבי ישראל יעקב חגיז.[27] גם לדעתו, איסור העיון ברשומותיו של אדם ללא רשותו נטוע בחלק ה"איסורי" שבתורת ישראל, והוא חלק מאיסור הליכת רכיל, שהוא מן האיסורים החמורים בתורה. וכך הוא כותב: "אסור לפתוח איגרת חברו, משום שיש איסור לבקש ולחפש מסתרותיו של חברו. ומה ההבדל בין 'לא תלך רכיל' לאחרים או לעצמו?"[28]

חכמי הלכה אחרים רואים את מקור האיסור בכלל האוסר על אדם לגלות כל מידע שהגיע אליו מחברו, אלא אם כן הלה נתן לו רשות מפורשת לעשות כן. כמקור לכך מובאת, בדרך כלל, ההלכה שמופיעה כבר בתלמוד הבבלי: "אמר רבי מוסיא בר בריה דרבי מסיא משמיה דרבי מוסיא רבה: מנין לאומר דבר לחבֵרו שהוא ב'בל יאמר' [ואסור לגלותו], עד שיאמר לו [הראשון] 'לך אמור!'?, שנאמר (ויקרא א, א): 'וידבר ה' אליו מאהל מועד לאמר'".[29] ופירש רש"י שהלימוד הוא מהמילה "לאמר", שהיא מילה מורכבת, מעין נוטריקון, ראשי תיבות של: "לא אמוֹר", כלומר, על דרך הכלל אסור לך לומר דברים שהגיעו אליך מאדם אחר, אלא אם כן הוא נותן לך רשות מפורשת להעבירם הלאה. ואם כך בדברים שנאמרו לך ישירות, קל וחומר בדברים שלא כוונו אליך, בין שמדובר בדברים שבכתב ובין שמדובר בדברים שבעל פה.[30]

משמעות האיסור בעידן המידע

שמירה על מידע פרטי של אדם היא חובה יסודית של כל המחזיק במידע מעין זה. על חברות האינטרנט הגדולות חלה החובה לשמור על מידע כזה מכל משמר ולפעול בכל הדרכים הסבירות כדי למנוע זליגה שלו לגורמים בלתי מורשים. בפועל, לא רק שחברות אלו מתרשלות לעיתים בשמירה על המידע – ויעידו על כך אירועי זליגת המידע האחרונים מחברת "פייסבוק", ולאחרונה גם הגילוי על דליפת הענק

26 **ויקרא** יט, יח.
27 מחכמי פאס שבמרוקו, ולימים ראש ישיבה בירושלים, המאה הי"ז.
28 רבי ישראל יעקב חגיז, **שו"ת הלכות קטנות**, חלק א, סימן רעו.
29 **תלמוד בבלי**, יומא ד, ע"ב.
30 אהרוני־גולדברג, "פרטיות באינטרנט בפריזמה הלכתית", עמ' 159־160.

של מידע לקוחות מרשת המלונות "מריוט"[31] – אלא שחלק מהחברות אף עושות שימוש מסחרי במידע הפרטי הנמצא בחזקתן ופועלות להשיג מידע ממקורות אחרים לצורך קידום עסקיהן. אותן חברות מתחרות על נגישות למידע מתוך כוונה לספק ללקוחותיהן המפַרסמים אצלן את אפשרויות המיקוד הטובות ביותר. הן אוספות נתונים ומידע מכל מקור אפשרי, לרבות מידע על צפייה בעמודים ברשת, הקלקת Like, שיתוף, חיבור לרשתות אלחוטיות, מאפייני מכשיר הקצה, שפה, מיקום ועוד עשרות (יש הגורסים מאות) פרמטרים נוספים. איסוף המידע אינו מוגבל רק למרחב הרשתי, אלא גולש גם למרחב הסלולרי. כך, למשל, משתמשי "אנדרואיד", העושים שימוש באפליקציית המסרים של "פייסבוק", מעניקים, בלא ידיעתם, את מספר הטלפון הסלולרי שלהם לחברה. מאגרי מידע עצומים – פרטיים וציבוריים, צבאיים, רפואיים ומסחריים – אוצרים בתוכם מידע עצום הנוגע לצנעת הפרט: למן כתובת מקום המגורים, מצב משפחתי ומצב בריאותי, ועד למצב הכלכלי, הרשעות בעבירות שונות, ציונים במהלך שנות לימוד, קורות חיים וכיוצא באלה.

עובד או גורם מורשה שנמסר לו מידע חסוי, אשר עיין בו ללא רשות או עשה בו שימוש, דינו כגזלן. מצב כזה עשוי לשמש פתח להגשת תביעת נזיקין אזרחית נגד אנשים או ארגונים המתרשלים בשמירת המידע שבידיהם ואינם נוקטים את כל אמצעי אבטחת המידע שהיה על אדם סביר כמוהם לנקוט, ועל אחת וכמה נגד ארגונים העושים שימוש במידע זה למטרות בצע כסף. במצבים מסוימים, מחדל אבטחת מידע מעין זה עשוי להגיע גם לכדי עבירה פלילית.

כאמור לעיל, בספרות המשפט העברי נקבעו הלכות שונות שנועדו להגן על צנעת מסמכיו של אדם. חלקן נקבעו על דרך של "סוּר מרע" – אם על ידי נקיטת אמצעי מנע בטרם תיעשה הפגיעה בצנעת הפרט, ואם לאחר מעשה, על ידי ענישת הפוגע בפרטיותו של חברו. במקרים אחרים נעשה המאבק בהפרת האיסור על דרך של "עשֵׂה טוב", כלומר, הבטחת תמריצים ושכר כלכלי או רוחני למקפיד על שמירת איסור הפגיעה בצנעת חייו של חברו.

לנוכח חומרת האיסור, קבעו חכמים כי חרם דרבנו גרשום, שכאמור אוסר על פתיחת מסמך או על עיון בו ללא רשות כותבו, חל מאליו גם אם לא צוין בראשו שהוא "סודי" או "מסווג".[32] במלים אחרות: הכלל הוא איסור לעיין במסמך ללא רשות מפורשת של כותבו. הדבר מותר רק במקרים חריגים, כאשר הוא נועד לתכלית ראויה (כגון הצלת חייו של אדם או לשם הגנה על ביטחון המדינה ושלום הציבור). גם אז הדבר מותר רק באופן מידתי, "במידה שאינה עולה על הנדרש". לדעת אחד מחכמי ההלכה, עצם החדירה למסמכי הזולת, אפילו ללא קריאת תוכנם,

31 Brian Krebs, "Marriott: Data on 500 Million Guests Stolen in 4-Year Breach", *KrebsonSecurity*, November 30, 2018.

32 ראו: פלאג'י, **שו"ת חקקי לב**, חלק יורה דעה, סימן מט.

כבר מהווה הפרה של חרם דרבנו גרשום.[33] גישה זאת משליכה באופן משמעותי על כל הקשור לניתוח מידע עתק (big data) על ידי חברות האינטרנט הענקיות.

השמירה על פרטיות ומידע פרטי אינה רק עניין טכני. יש לה מטרה עליונה. לדעת הרב אלפרד כהן, אדם זקוק לפרטיות מאחר שפרטיותו היא המקור והאמצעי למימוש יכולותיו וכישרונותיו הייחודיים.[34] הֵד לכך שהשמירה על הזכות לפרטיות אינה רק אמצעי למימוש זכויות אחרות אלא גם ערך עצמאי, חלק מכבוד האדם באשר הוא אדם, ניתן למצוא בתורת המשפט העברי.

לאיסור הפגיעה בצנעת הפרט בכלל, ולאיסור החדירה לרשומותיו של אדם שלא בידיעתו או הסכמתו בפרט, יש, אפוא, שורשים עמוקים בתורת המשפט העברי. ההתפתחות הטכנולוגית המואצת, חולשותיו של מרחב הסייבר וקשיי אבטחה מציבים בפני חכמי המשפט העברי אתגרים חדשים ומרתקים הנוגעים ליישום עקרונות עתיקי יומין במציאות של ימינו. מדובר במזיגת יינו הישן והטוב של המשפט העברי לקנקנה המתחדש של מערכת המשפט במדינת ישראל, שערכיה הם "ערכים יהודיים ודמוקרטיים" כאחד.

33 רבי יוסף דוד, **בית דוד**, יו"ד, קנח.

34 Rabbi Alfred S. Cohen, "Privacy: A Jewish Perspective", *Journal of Halacha and Contemporary Society*, Vol. 1 (1981): 57.

המרחב הקיברנטי: זירת העימות הסעודית-איראנית הבאה?

רון דויטש ויואל גוז'נסקי

השילוב של הערפול המובנה הגלום במבצעי סייבר נרחבים עם פוטנציאל הנזק הממשי הטמון בהם, הופך מרחב זה לאידיאלי לפעולה עבור ערב הסעודית ואיראן ותואם את ראייתן האסטרטגית ואת תפיסת הפעלת הכוח שלהן. הסיכון והסיכוי שמציב המרחב הקיברנטי בפני כל אחת משתי המדינות הופכים אותו למפתה, במיוחד כשהדבר נוגע להשקעת משאבים לטווח הארוך. נראה, לפיכך, שמרחב הסייבר צפוי להפוך לזירת התנגשות מרכזית עתידית נוספת עבור ערב הסעודית ואיראן, וזאת לאור מגבלות הכוח הקונבנציונלי שמנעו זאת מהן עד כה.

מילות מפתח: ערב הסעודית, איראן, לוחמת סייבר, לוחמה אסימטרית, ישראל, ארצות הברית

מבוא

מזה זמן שערב הסעודית ואיראן מקיימות ביניהן יריבות עזה. על אף ניסיונות שנעשו לאורך השנים להגיע להפשרה ביחסים, או לפחות להבנות אסטרטגיות מסוימות שיפחיתו את המתחים בין השתיים, ערב הסעודית ואיראן לא חדלו לראות האחת באחרת איום מרכזי. למרות זאת, ועל אף הסמיכות הטריטוריאלית בין שתי המדינות, מעולם לא פרץ ביניהן עימות צבאי ישיר בעל משמעות, ולכל היותר היו התנגשויות נקודתיות ובאמצעות כוחות של צד שלישי. סיבה מרכזית למצב זה עשויה להיות אופי הכוחות החמושים של השתיים ותפיסת ההפעלה שלהן.

סיבות היסטוריות, חברתיות וגיאופוליטיות הביאו לכך שהן ערב הסעודית והן איראן אינן מחזיקות ברשותן כוחות יבשה המסוגלים לבצע תמרונים נרחבים

רון דויטש הוא מתמחה במכון למחקרי ביטחון לאומי. ד"ר יואל גוז'נסקי הוא חוקר בכיר במכון למחקרי ביטחון לאומי.

מעבר לגבולותיהן, ובכלל זה לא האחת נגד השנייה. זאת ועוד, כוחות הצבא הסעודיים לוקים בחוסר יעילות משווע על אף תקציבי עתק, בעוד שהאיראנים משמרים תפיסת הפעלה של כוחותיהם הנובעת מרציונל של התנגדות ולוחמה אסימטרית, דבר המתבטא במעמדם ובתפקידם המרכזי של משמרות המהפכה, ובמיוחד של זרוע הטילים.[1]

תפיסת ההפעלה של הכוח הצבאי על ידי ערב הסעודית ואיראן מיתרגמת בתורה לראייה אסטרטגית־מדינית רחבה יותר, השמה דגש על לוחמה תודעתית ועל הפעלת טרור ו"שליחים" מאחורי הקלעים במטרה לערער את יריבותיהן. ייתכן וניתן לראות בתפיסת הפעלה זאת דמיון למושג חדש יחסית שהתגבש (בין אם בצדק ובין אם לאו) בשנים האחרונות – "דוקטרינת גראסימוב", ההולכת ותופסת מקום כגישה פוטנציאלית ללחימה ולמדיניות חוץ בכלל.[2] דוקטרינה זאת מיוחסת לגנרל הרוסי ואלרי גראסימוב ומבוססת על דברים שכתב בשנת 2013, ובהם תיאר מעין "זן חדש" של מלחמות. אלו כוללות, לדבריו, לצד מאמצים צבאיים קונבנציונליים, אפיקי פעולה נוספים, דוגמת שימוש בתקשורת, חתרנות פנימית, סייבר וכל אמצעי אחר המסוגל לזרוע כאוס בשורות האויב.[3]

גישה זו עשויה לקבל זווית מעניינת במיוחד כאשר היא נבחנת לאור התפתחות הלוחמה בסייבר. השילוב של הערפול המובנה עם פוטנציאל הנזק הממשי הגלום במבצעי סייבר נרחבים הופך מרחב זה לאידיאלי עבור תפיסת הפעלת הכוח של ערב הסעודית ואיראן.

מאמר זה מבקש לבחון באיזו מידה, אם בכלל, עשוי מרחב הסייבר להפוך לזירת ההתנגשות מרכזית בין ערב הסעודית ובין איראן. לצורך כך, המאמר משווה בין יכולות הסייבר של כל אחת משתי המדינות, הן ברמה ההגנתית והן ברמה ההתקפית, ומנסה להגיע למסקנה האם מרחב הסייבר עשוי להקנות לאחת מהן את היכולת להשיג את מה שנבצר ממנה לעשות באמצעים צבאיים קונבנציונליים.

הסייבר בערב הסעודית

תחום הסייבר לא זכה לתשומת לב ולא קיבל חשיבות רבה בערב הסעודית עד לשנים האחרונות. עם זאת, פגיעותה של הממלכה לאיומי סייבר העלולים להסב לה נזקים רבים הולכת וגוברת. מדובר בנזקים העשויים לבוא לידי ביטוי באמצעות שני ערוצים מרכזיים: הראשון, הערוץ ה"ישיר", כולל מתקפות אפשריות

1 עוזי רובין, **טילים כנושאי הדגל של חזון המשטר האיראני**, מכון ירושלים למחקרים אסטרטגים, 23 בנובמבר 2018.

2 Mark Galeotti, "I'm Sorry for Creating the 'Gerasimov Doctrine'", *Foreign Policy*, March 5, 2018.

3 Molly K. McKew, "The Gerasimov Doctrine", *Politico Magazine*, September/October 2017.

על תשתיות ומתקנים סעודיים, צבאיים ואזרחים כאחד, מה שעשוי לגרום לנזק כלכלי רב ואף למספר גבוה של אבדות בנפש. דוגמה בולטת לפוטנציאל ההרסני של התקפה מסוג זה ניתן היה לראות ב־2017, בהתקפת סייבר שכוונה לאחד המפעלים הפטרוכימיים בממלכה.[4] מטרת ההתקפה לא הייתה גניבת מידע או פגיעה בבסיסי נתונים סעודיים, אלא גרימת נזק פיזי של ממש ופיצוץ שישבש את מערכות המפעל. המבצע כשל בשל טעות בקוד התקיפה, ששיבש את פעולתו. חוקרים סבורים כי מי שעמדה מאחורי התקיפה הייתה איראן, שתיקנה מאז את הטעות שהכשילה אותה, וכי מדובר עתה רק בשאלה של זמן עד שהיא תפעל שוב נגד ערב הסעודית, הפעם בעוצמה ובתחכום רבים יותר.[5]

מעֵבר להתמקדות באיום על תשתיות קריטיות ועל מערכות בקרה במטרה לשבש את שרשרת האספקה ואף לפגוע בה פיזית, ניתן לזהות כיום איום הולך וגובר גם על מערכות מידע ארגוניות סעודיות, שמטרתו היא לשבש אותן ולרגל אחריהן. בשלהי 2016 הותקפו מספר יעדים ממשלתיים בערב הסעודית, בהם גם מערכות המחשב של הבנק המרכזי הסעודי, על ידי התוכנה הזדונית "שאמון". בווירוס זה נעשה שימוש כבר ב־2012, במתקפת הסייבר הרחבה נגד חברת הנפט הלאומית הסעודית, אראמק"ו. דוגמאות אלו הן חלק בלבד ממסכת תקיפות רחבה בהרבה, עליה רמז בכיר במגזר הסייבר הסעודי, שהעריך כי ב־2015 לבדה ספגה הממלכה כשישים מיליון תקיפות סייבר, בקצב של כ־164,000 תקיפות ליום.[6]

לצד ערוץ התקיפה הישיר בסייבר, קיים גם ערוץ "עקיף", שעשוי לבוא לידי ביטוי בשימוש בפלטפורמות אינטרנט פופולריות, כגון "פייסבוק" או "טוויטר", כתמיכה בגורמים המתנגדים למשטר בערב הסעודית וכדי לגרום לתסיסה פנימית בממלכה. היתרון שבאופן פעולה זה גלום בכך שהוא עשוי להיות בעל חתימה נמוכה עוד יותר מאשר מתקפות הסייבר הישירות, בשל יכולתה של המדינה התוקפת להסוות את פעילותה כמחאה פנימית אותנטית, בין היתר באמצעות שימוש בחשבונות פיקטיביים. אין גם להוציא מכלל אפשרות תסריט של פעולה משולבת: פעילות סייבר בחתימה נמוכה, שתגרום לאסון אזרחי רחב היקף שיזעזע את החברה הסעודית, ובמקביל, פעילות מוגברת של חתרנות קיברנטית, שתנצל את המצב הפנימי הרגיש כדי לעודד התקוממות אקטיבית נגד בית המלוכה.

בית המלוכה הסעודי מתחיל להבין את הפוטנציאל ההרסני של הממד הקיברנטי ומנסה לפעול כדי להתמודד איתו. יחד עם זאת, קיימים מספר גורמים פנימיים

4 Nicole Perlroth and Clifford Krauss, "A Cyber-attack in Saudi Arabia Failed to Cause Carnage, but the Next Attempt could be Deadly", *The Independent*, March 21, 2018.

5 Ibid.

6 Ibrahim al-Hussein, "60 Million Cyber-attacks Targeted Saudi Arabia in One Year", *Al Arabia*, May 2, 2018.

המהווים מכשלה בפני השגת מטרה זאת. בראש ובראשונה ניתן למנות את הפיצול המובנה בממשל הסעודי, שבמסגרתו מחולקות הסמכויות לטיפול באסטרטגיה הקיברנטית בין מוקדי כוח רבים המשתייכים למשרדים ולגופים שונים. מצב זה מקשה על גיבושה ויישומה של דוקטרינת סייבר אחידה, באופן שייתן מענה לצורכי הביטחון המגוונים של הממלכה.[7]

מכשול מרכזי נוסף ביכולתה של ערב הסעודית להתמודד עם איומי סייבר קשור לפיגור הטכנולוגי היחסי של החברה הסעודית. בעיה זאת אינה חדשה ואינה ייחודית לסוגיית הסייבר, אלא נוגעת בנקודות חולי עמוקות בהרבה מהן סובלת הממלכה. עושר הנפט של ערב הסעודית יִתר במשך עשורים רבים את הצורך בפיתוח מגזרים כלכליים נוספים. כמו כן, קניית "שקט תעשייתי" אצל התושבים באמצעות סובסידיות נדיבות וריבוי מיותר של משרות ממשלתיות, מנעה, במידה רבה, מהאוכלוסייה את התמריצים לעבודה קשה ולרכישת השכלה מתקדמת. כתוצאה מכך, ערב הסעודית חסֵרה את התשתית האנושית והטכנולוגית כדי להגיע ליכולות הדרושות לה בתחום הסייבר, בכלל זה לצרכים אזרחיים, ונאלצת להסתמך בעיקר על סיוע חיצוני (תעשיית טכנולוגיות המידע תופסות נפח של כ־0.4 אחוזים בלבד מהתמ"ג הסעודי).[8]

במטרה להתגבר על קשיים אלה נקטה ערב הסעודית בשנים האחרונות מספר צעדים, שבעקבותיהם הוטב מעט מצבה. כיום ניתן למנות שלוש זרועות מרכזיות בממלכה הקשורות לתחום הסייבר ופועלות במקביל האחת לרעותה: הזרוע הראשונה היא "הרשות הלאומית להגנת הסייבר" (NCA). גוף זה, אשר הוקם ב־2017 בצו מלכותי וכפוף למלך וליורש העצר, אמון על ריכוז המדיניות, ההנחיות וההכשרה בתחום הגנת הסייבר עבור כלל הגופים הממשלתיים, כמו גם הפרטיים.[9] זהו למעשה הגוף המרכזי האחראי על הטכנולוגיה ההגנתית בממלכה; הגוף השני הוא "הפדרציה הסעודית להגנה קיברנטית ולתכנות" (SAFCAP). גוף זה כפוף לוועד האולימפי הסעודי ואחראי בעיקר על הכשרת כוח האדם והתשתית הטכנולוגית עבור מגזר הסייבר והתכנות בערב הסעודית. חלק מפעולתה השוטפת של הפדרציה הוא לארגן כנסים ותחרויות, שמטרתם היא להגביר את המודעות לסוגיות ביטחון הסייבר ולעודד את הנוער הסעודי להתמחות בתחום זה ולהוות

7 Melissa Hathaway, Francesca Spidalieri and Fahad Alsowailm, *Kingdom of Saudi Arabia Cyber Readiness at a Glance* (Potomac Institute for Policy Studies, 2017), pp. 23-24.

8 Ibid., p. 3.

9 "Follow Basic Cyber Security Standards, Govt Agencies Told", *Saudi Gazette*, October 7, 2018.

עתודה טכנולוגית פוטנציאלית.[10] לשני גופים גלויים אלה ניתן להוסיף זרוע שלישית, התקפית וחשאית יותר באופייה, שנוהלה על פי הדיווחים, לפחות עד לאחרונה, בידי מוחמד אל־קטאני, שהיה יד ימינו של יורש העצר מחמד בן סלמן. זרוע זאת, "המרכז ללימודים ולתקשורת" (CSMA) בריאד מעסיק מאות סעודים המתַפקדים כ"צבא טרולים" בערוצי המדיה החברתית, ותפקידם הוא לנטר מתנגדי משטר, למחוק תגובות ביקורתיות בנושאים רגישים ולשתול תגובות אוהדות למדיניות בית המלוכה.[11] על אף שרבות מפעילויות הסיכול של המרכז נותרו מחוץ לאור הזרקורים במערב, רצח העיתונאי ג'מאל חשוקג'י העלה לקדמת הבמה את אל קטאני ומלחמת המידע המתבצעת תחת ניהולו, מלחמה אשר במסגרתה היה חשוקג'י איום משמעותי.[12]

למרות ההתפתחויות האחרונות בערב הסעודית בתחום הסייבר, יש לקחת בחשבון שיידרש עוד זמן רב עד שניתן יהיה לגשר באופן מלא על הפערים המשמעותיים הקיימים בתחום זה בממלכה. בטווח הזמן הקצר־בינוני, עד שהתהליכים הנזכרים לעיל יצברו תאוצה, ערב הסעודית עשויה לפצות על הפערים בתחום הידע והתשתית הטכנולוגית ברכש של ידע ממדינות זרות. בכל האמור לרכש צבאי, ערב הסעודית היא הלקוחה הגדולה ביותר של ארצות הברית, ומתקיים שיתוף פעולה פורה בין שתי המדינות גם בתחום הסייבר. במסגרת ההסכמים שחתם נשיא ארצות הברית, דונלד טראמפ, בביקורו בממלכה במאי 2017 היו גם הסכמים בתחום ההגנה בסייבר, שנועדו לכסות על הפערים הקיימים אצל הסעודים בתחום זה. כן דווח כי חברות קבלן מטעם הממשל האמריקאי עוסקות במתן ייעוץ והדרכה לערב הסעודית בתחום ההגנה בסייבר וגם פועלות ישירות במשרדי הממשלה הסעודיים כדי להגן עליהם מפני התקפות סייבר. אחת מחברות אלו, Booz Allen Hamilton, אף מצאה לנכון להדגיש כי המעורבות שלה בתחום הסייבר בערב הסעודית אינה כוללת בניית יכולות התקפיות.[13]

הפערים הסעודיים בתחום הסייבר עשויים לשמש גורם משפיע גם על יחסיה של הממלכה עם ישראל, שכמעצמת סייבר, יש לה הרבה מה להציע לערב הסעודית בתחום זה. על פי דיווחים שונים, ייתכן שקשרים כאלה כבר מתקיימים, או לפחות התקיימו בעבר. במסגרת זו דווח כי גורמי ממשל הקשורים לערב הסעודית השתמשו

10 האתר הרשמי של "הפדרציה הסעודית להגנה קיברנטית ותכנות", https://safcsp.org.sa/en

11 Adam Goldman and Karam Shoumali, "Saudis' Image Makers: A Troll Army and a Twitter Insider", *The New York Times*, October 20, 2018.

12 Ignatius, david "how a Chilling Saudi Cyberwar Ensnared Jamal Khashoggi" *The Washington Post* 07.12.2018

13 Michael Forsythe, Mark Mazzetti, Ben Hubbard and Walt Bogdanich, "Consultants Stick with the Saudis", *The New York Times*, November 8, 2018.

בתוכנת ריגול ("פגאסוס") של חברת NSO הישראלית בניסיון לצותת למתנגדי המשטר.[14]

אפיק אפשרי נוסף עבור ערב הסעודית הוא יצירת תשתית הגנה משותפת בסייבר למדינות המפרץ המאוגדות ב"מועצה לשיתוף פעולה במפרץ" (GCC), או לחלקן, המתמודדות עם איומים דומים. קריאות לשיתופי פעולה כאלה כבר נשמעות, אלא שהדרך עודנה ארוכה עד שהן יעברו לפסים מעשיים אפקטיביים, לאור המתחים המשמעותיים הקיימים בין חלק מאותן המדינות.[15]

יכולות הסייבר של איראן

בניגוד לערב הסעודית, איראן מחזיקה בתשתית מבוססת יחסית של יכולות סייבר, הן הגנתיות והן התקפיות. בין יעדי ההתקפה העיקריים של איראן בשנים האחרונות נמצאות ערב הסעודית, ישראל וארצות הברית.[16] פעילות הסייבר האיראנית מפוקחת על ידי הדרגים הגבוהים ביותר במשטר, ובהם הנשיא ומפקד משמרות המהפכה, ואת יכולות הסייבר שלה מתַחזקת איראן באמצעות מספר דרכים: ראשית, המשטר האיראני משקיע כספים במחקר ובהכשרה של כוח אדם בתחום הסייבר, מתוך תפיסה אסטרטגית של חשיבותו הרבה;[17] שנית, החתימה על הסכם הגרעין עם המעצמות בשנת 2015 פתחה בפני איראן הזדמנויות לשיתופי פעולה רבים עם אוניברסיטאות ומוסדות מדעיים מסביב לעולם. אפשרות זו נוצלה על ידיה כדי לקדם גם את תחום הסייבר שלה, וזאת באמצעות שיתוף פעולה מדעי עם אוניברסיטאות שברשותן ידע בנושא זה;[18] שלישית, הניצול האיראני של ידע זר בתחום הסייבר אינו מוגבל רק לשיתופי פעולה רשמיים. בשנת 2013 נוסד מוסד ה"מבנא" (Mabna) האיראני, שמטרתו היא השגת גישה למשאבים מדעיים מחוץ לאיראן.[19] אמנם, מטרה זו אינה ממוקדת בהכרח בתחום הסייבר, אולם מדובר באפיק אפשרי נוסף בעל פוטנציאל לתרום לגיבוש יכולות הסייבר האיראניות.

14 "Israeli Hacking Firm NSO Group Offered Saudis Cellphone Spy Tools – Report", *Times of Israel*, November 25, 2018.

15 Ramola Talwar Badam, "GCC Urged to Coordinate Cyber Security following Wannacry Attack", *The National*, May 21, 2017.

16 Collin Anderson, Karim Sadjadpour, *Iran's Cyber Threat, Espionage, Sabotage and Revenge* (Carnegie Endowment for International Peace, 2018), https://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf

17 גבי סיבוני וסמי קרוננפלד, "התפתחויות בלוחמת הסייבר של איראן 2013־2014", **צבא ואסטרטגיה**, כרך 6, גיליון 2, אוגוסט 2014, עמ' 84.

18 Levi Gundert, Sanil Chohan and Greg Lesnewich, "Iran's Hacker Hierarchy Exposed: How the Islamic Republic of Iran Uses Contractors and Universities to Conduct Cyber Operations", *Recorded Future*, May 9, 2018.

19 על פי נתוני ה־FBI, בין קורבנות פעילות ה"מבנא" ניתן למצוא 3,768 פרופסורים ב־144 אוניברסיטאות בארצות הברית לבדה, ו־4,230 פרופסורים הפזורים על פני 176 אוניברסיטאות

אירן חשה היטב בעבר את הסכנות הטמונות במרחב הקיברנטי. הדוגמה המובהקת ביותר לכך היא הנוזקה "סטקסנט", אשר פגעה בתשתיות גרעין אירניות ב־2012. אולם עוד קודם לכן התנסתה אירן בסכנה קיברנטית מסוג אחר: המחאה הנרחבת ברחובות טהראן ב־2009 המחישה את הפוטנציאל ההרסני הטמון בקבוצות אופוזיציה פנימיות ובזליגה של רעיונות חתרניים מבחוץ. בתקופה זאת פתח המשטר האירני בפרויקט של בידול רשתות, שמטרתו הייתה העברת כלל התקשורת האירנית לרשת פנים מדינתית המנותקת מהזירה הבין־לאומית, כך שבידי המשטר תהיה השליטה המלאה על התכנים הנכנסים למדינה, כמו גם הגנה טובה יותר מפני מתקפות סייבר.[20] יעד זה מגובה על ידי פעילות אכיפה אגרסיבית של אנשי "משטרת הסייבר" האירנית כלפי גורמים חתרניים הפעילים ברשת.[21]

מלבד זאת, אירן משקיע מאמצים רבים בפיתוח ובהטמעה של יכולות הגנה קיברנטיות, כמו גם בתרגול של תפיסות הפעלה. דוגמאות לכך ניתן לראות בתרגילים שנערכו בשנים 2012 ו־2013 ובדקו את מערכי ההגנה הקיברנטית האירניים בזרועות הים והיבשה (בהתאמה) של משמרות המהפכה.[22] לאחרונה דווח באירן על חשיפה של גרסה מתקדמת יותר של תולעת "סטקסנט", אולם נטען כי היא טרם הספיקה לגרום לנזק כלשהו. בהמשך לכך העריך ראש מערך הסייבר האירני, גנרל ג'ולאם רזא ג'לאלי, שאירן אינה נמצאת עוד תחת איום סייבר משמעותי, ועל כן היא מורידה את הנושא אל תחתית סדר העדיפויות. דיווח זה עשוי להוות אינדיקציה לשיפור ניכר ביכולות הסייבר האירניות בשנים האחרונות, אם כי אין לשלול את האפשרות שמדובר במהלך הונאה תודעתי ותו לא.[23]

לצד פיתוח יכולות הגנתיות מתקדמות, עברה אירן כברת דרך מרשימה בפיתוח יכולות התקפיות בסייבר. אין ספק שאירן נמצאת במקום מתקדם יותר מאשר ערב הסעודית בכל הנוגע ליכולות כאלו, אם כי נראה שהיא עדיין מפגרת מאחורי מעצמות הסייבר הגדולות דוגמת סין, רוסיה, ארצות הברית וישראל. מערך הסייבר ההתקפי האירני מצוי בעיקר תחת אחריות משמרות המהפכה ומשתייך לתת־גוף המכונה "צבא הסייבר האירני" (ICA). מערך זה סובל מחולשה מובנית בשל אופיו הקבלני למחצה: רובם של מבצעי הסייבר ההתקפיים של אירן אינם

---

21 מ־21 מדינות שונות, ובהן ישראל, גרמניה, סין, דרום קוריאה, בריטניה וטורקיה: Lior Tabansky, "Iran's Cybered Warfare Meets Western Cyber-Insecurity" in: *Confronting an "Axis of Cyber"? China, Iran, North Korea, Russia in Cyberspace*, ed. Fabio Rugge (Italia: ISPI, 2018), p. 130.

20 סיבוני וקרוננפלד, "התפתחויות ביכולות הסייבר של אירן", עמ' 85.

21 שם, עמ' 88.

22 שם, עמ' 87.

23 **אירן מאשימה חברה ישראלית במתקפת סייבר**, המרכז הירושלמי לענייני ציבור ומדינה, 5 בנובמבר 2018.

מבוצעים על ידי אנשי משמרות המהפכה עצמם, אלא על ידי יחידים וקבוצות האקרים עצמאיות למחצה, המקבלות שכר בהתאם למידת הצלחתם. היעדר מחויבות אידיאולוגית והחיפוש אחר רווחים כספיים הופכים חלק גדול מההאקרים האיראנים למועמדים בעייתיים מבחינת משמרות המהפכה. על כן, המשטר נוקט גישה רב־רובדית: בדרג הביניים מוצבים קצינים בעלי מחויבות אידיאולוגית למשטר, והם קובעים את היעדים הדרושים ומטילים משימות שונות על קבלני משנה אד־הוק, קרי קבוצות של האקרים אזרחיים המקבלים שכר לפי משימה.[24] יש להוסיף לכך כוחות של "שליחים" קיברנטיים, הפועלים בהקשר אידיאולוגי יותר. דוגמה מובהקת ל"שליח" כזה היא ארגון חיזבאללה הלבנוני, שקשריו עם הרפובליקה האסלאמית של איראן מקנים לו יכולות סייבר מתקדמות יחסית בהשוואה לארגוני טרור אחרים.[25] יכולות אלו מופעלות בשעת הצורך ומהוות זרוע קיברנטית התקפית נוספת עבור המשטר האיראני.

בנוסף לכך, מפעיל המשטר האיראני יכולות התקפיות "רכות", קרי לוחמה פסיכולוגית המתנהלת באמצעות מניפולציות מידע ברשתות החברתיות ובאתרי החדשות, בדומה לנעשה על ידי ערב הסעודית. דוגמה מובהקת ליכולת איראנית כזו, שנחשפה לאחרונה, היא מה שזכה לביטוי "אייתוללה BBC" – מבצע נרחב שבוצע מטעם המשטר האיראני ובו זויפו אתרי חדשות מכל רחבי העולם, ובראשם אתר ה־BBC בשפה הפרסית. האתרים המזויפים הכילו תוכן מניפולטיבי ומכוון, בהתאם לצורכי הלוחמה הפסיכולוגית האיראניים.[26]

סיכום ומסקנות

מאמר זה ביקש לבחון את ההיתכנות להתפתחותו של מרחב הסייבר לזירת עימות עתידית רחבה בין ערב הסעודית ובין איראן. למעשה, כבר היום מתקיימות התנגשויות בין השתיים בתוך המרחב הקיברנטי, אם כי היא לא הפכה עדיין לזירת החיכוך המרכזית ביניהן. על כן, כשדנים בעימות סעודי־איראני במרחב הסייבר, יש להבחין בין הטווח הקצר והבינוני ובין הטווח הארוך. כפי שעולה מניסיונן של שתי המדינות, שתיהן סובלות מנקודות תורפה קיברנטיות, שיש בהן פוטנציאל להסב נזק אסטרטגי משמעותי ביותר. נקודות תורפה אלו עלולות להתגלות כנקודות הבקעה שימוטטו את המשטר כולו, אם אחת מהשתיים תצליח להכות

24 Gundert, Chohan, Lesnewich "Iran's Hacker Hierarchy Exposed: How the Islamic Republic of Iran Uses Contractors and Universities to Conduct Cyber Operations", p. 5.

25 Ben Schefer, "The Cyber Party of God: How Hezbollah Could Transform Cyberterrorism", *Georgetown Security Studies Review*, March 11, 2018.

26 "Ayatollah BBC – An Iranian Disinformation Operation against Western Media Outlets", *Clearsky Cyber Security*, 2018.

בהן מספיק חזק. מכיוון שכך, הסיכון והסיכוי שמציב המרחב הקיברנטי בפני ערב הסעודית ואיראן כאחת הופך אותו למפתה, במיוחד כשמדובר בהשקעת משאבים לטווח הארוך.

לפי שעה, נראה כי היכולות הקיברנטיות הן של ערב הסעודית והן של איראן הן דלות מכדי להכיל עימות בקנה מידה מלא ביניהן. יכולות אלו ממלאות תפקיד תומך חשוב, אך עדיין לא מפותח דיו כדי לתת מענה לתפיסת הביטחון של השתיים. ר׳יה לכך הם האמצעים ההתקפיים הפשוטים יחסית המשמשים את ערב הסעודית ואיראן במרחב הקיברנטי. אלה כוללים בעיקר הפצת מידע כוזב ("פייק ניוז") וחתרנות דרך הרשתות החברתיות. לא ערב הסעודית ולא איראן מחזיקות ברשותן תשתיות סייבר התקפיות רחבות היקף: לראשונה אין עדיין, ככל הידוע, יכולת טכנולוגית עצמאית לכך, בעוד שבאיראן היא אמנם קיימת, אך נראה שהיא מבוססת בעיקר על "שכירי חרב" מזדמנים למחצה.

השאלה המעניינת יותר שצריכה להישאל נוגעת למגמות ארוכות הטווח. כפי שצוין לעיל, מקבלי ההחלטות בערב הסעודית ובאיראן מודעים היטב לפוטנציאל הנזק והתועלת שמגלם בתוכו המרחב הקיברנטי ונוקטים צעדים למיצוב שתי המדינות כשחקניות בעלות יכולת בתחום זה בטווח הארוך. לכך מצטרף שיווי המשקל האסטרטגי שמקיימות השתיים ביניהן: לא לערב הסעודית ולא לאיראן יש היכולות למוטט את הצד השני באמצעות מערכה צבאית קונבנציונלית. מכיוון שכך, הפנייה לאפיק הסייבר, על האפשרויות הגלומות בו, מהווה צעד מתבקש. במובן זה, אין לשלול את האפשרות שאנו חוזים בניצניו של מרוץ טכנולוגי סעודי־איראני (כמובן, בנוסף לשלל האיומים הקיברנטיים המעסיקים כל אחת משתי המדינות בנפרד).

קשה לחזות את תוצאותיו של מרוץ כזה: מחד גיסא, על אף שניתן להתווכח על מעמדה של איראן כמעצמת סייבר מן השורה, אין ספק שהיא נמצאת כיום בעמדת יתרון ביחס לערב הסעודית בתחום זה. לאיראן יש תשתיות הגנה מפותחות יחסית וניסיון רב ערך שנקנה בשנים של התמודדות עם מתקפות ישראליות ואמריקאיות. כמו כן, בניגוד לערב הסעודית, שנעדרת יכולות התקפיות "קשות" של ממש, לאיראן יש יכולות מוכחות של תקיפת יעדים סעודיים ומערביים (ואמריקאיים בפרט) דרך הרשת, גם אם נראה שהיא אינה יכולה לבצע מתקפה שיטתית ורחבה בדומה לישראל, לרוסיה ולארצות הברית. לבסוף, ומעל הכול, בעוד שערב הסעודית נעדרת תשתית טכנולוגית ואנושית בתחום הסייבר (ולכל היותר, תשתית כזאת נמצאת בה בחיתוליה), איראן השקיעה מאמצים רבים בהכשרת כוח אדם באוניברסיטאות השונות, כמו גם בשיתופי פעולה עם מוסדות זרים, ואף בגניבת ידע. כל אלה מציבים את איראן כמה צעדים לפני ערב הסעודית ועלולים להפוך עם הזמן לפער קטלני עבור הממלכה.

מאידך גיסא, ישנם שני גורמים משמעותיים העשויים לשחק לטובתה של ערב הסעודית במרוץ הטכנולוגי לטווח הארוך ולבלום את ההתקדמות האיראנית: הראשון שבהם הוא משאביה העדיפים של הממלכה. כוחות הביטחון הסעודיים נהנים מתקציבים שנתיים מן הגבוהים בעולם. אם הם יתועלו נכונה ותוגבר ההשקעה החכמה במרחב הקיברנטי (לצד השקעות בחינוך הטכנולוגי המקדים), תוכל ערב הסעודית להאיץ את תהליכי ההתקדמות הטכנולוגיים שלה. לעומת זאת, איראן, הכורעת תחת נטל הסנקציות הבין־לאומיות, מתקשה להקצות משאבים דומים לפיתוח ולרכישת יכולות חדשות.

גורם משמעותי שני היא מטריית ההגנה ושיתופי הפעולה המתקיימים בין ערב הסעודית ובין מעצמת הסייבר הגדולה בעולם – ארצות הברית. כבעלת ברית מרכזית, ארצות הברית עשויה לספק לערב הסעודית מטריית הגנה קיברנטית ויכולות טכנולוגיות, שיאפשרו לה להדביק את הפער מול האיראנים. לכך מצטרף מה שנראה כשיתופי פעולה חשאיים אך תדירים עם ישראל, שהיא, כאמור, מעצמת סייבר בפני עצמה. משקלם היחסי של יתרונות אלה יגבר ככל שיחלוף הזמן. אם הם ינוצלו בחוכמה על ידי הממלכה, הם עשויים להתגלות כנכס של ממש, שייצור לה יתרון על פני איראן.

בחינה של יכולות הסייבר הנוכחיות בערב הסעודית ובאיראן מראה כי עימות קיברנטי רחב היקף בין השתיים לא צפוי כנראה בטווח המיידי. עם זאת, אופיו של המרחב הקיברנטי והעמימות המובנית הקיימת בו, הופכים אותו למתאים במיוחד לתפיסת הפעלת הכוח של שתי המדינות. על כן, יש לצפות, בטווח הבינוני והארוך, לשימוש גובר של שתיהן במרחב זה, כנתיב וכדרך פעולה נוספת לפגיעה ביריב, וזאת בניגוד למגבלות הכוח הקונבנציונלי שמנעו זאת מהן עד כה.

"ג'ון הג'יהאדיסט" הבא: דמוקרטיה וירטואלית והמאבק בתעמולה המקדמת קיצוניות אלימה

מתיו קרוסטון

הספרות המחקרית מתעדת ומנתחת את הדרך בה ארגונים אסלאמיים קיצוניים מנצלים את הטכנולוגיה המודרנית כדי לגייס לשורותיהם אנשים חדשים שעמדותיהם קיצוניות. ניתוח זה של המתרחש מאחורי הקלעים מחמיץ ניתוח לא פחות חשוב של המתרחש בחזיתם, כלומר, כיצד ומדוע מצליחים כלי התעמולה והגיוס הווירטואליים לשכנע אוכלוסיות שלמות בחברה המערבית ומדוע אנשים הופכים לקיצוניים למרות שהם חיים בדמוקרטיות יציבות וחופשיות? מאמר זה משלב מרכיבים של הפסיכולוגיה הקוגניטיבית (ובמיוחד את המושג "המלחמה הקוגניטיבית הראשונה" שטבע גבי סיבוני) ושל הטכנולוגיה הווירטואלית עם מרכיבים מתחום המאבק בקיצוניות האלימה, כדי להסביר מדוע גופים במערב העוסקים בסיכול טרור – ממשלות, צבאות וסוכנויות מודיעין – מתקשים להיאבק בגיוס הווירטואלי. כישלון התוכניות של הדמוקרטיות המערביות להיאבק בקיצוניות הווירטואלית האלימה מציב שורה של שאלות הנוגעות לחוסר הצלחתה של הדמוקרטיה בעידן הדיגיטלי לממש את האידיאלים שלה ואת הבטחותיה, במיוחד בהשוואה ליכולות הטכנולוגיות שמפגינים הגורמים הקיצוניים. כישלון כזה פירושו המשך ההצלחה של הקבוצות הקיצוניות, המקדמות סדר יום אלים והרג של חפים מפשע, והמשך כישלונן של הדמוקרטיות המערביות במאבקן עם קבוצות אלו במסגרת "המלחמה הקוגניטיבית הראשונה".

מילות מפתח: רשתות חברתיות, תעמולת רשת, מדינה אסלאמית, CVE, מאבק בטרור

פרופ' מתיו קרוסטון הוא חבר בפקולטה לדוקטורנטים בכירים בבית הספר ללימודי ביטחון ונושאים גלובליים, האוניברסיטה הצבאית האמריקאית.

מבוא

המדינה האסלאמית אמנם לא הצליחה לשמור על הישגיה הגיאו־פוליטיים הפיזיים בעיראק ובסוריה, אולם יכולתה להשיג השפעה מרבית באמצעות פלטפורמות של רשתות חברתיות ולגייס אנשים לביצוע מעשי זוועה בערים גדולות במערב ממשיכה לעורר דאגה. הספרות המחקרית מתעדת היטב ובהיקף רחב כיצד ארגונים אסלאמיים קיצוניים מנצלים את הטכנולוגיה המודרנית כדי לגייס לשורותיהם אנשים בעלי דעות קיצוניות. עם זאת, ניתוח המתרחש מאחורי הקלעים אינו נותן מענה לתהליך חשוב לא פחות המתרחש על פני השטח, והוא: כיצד ומדוע מצליחים כלי התעמולה והגיוס הווירטואליים לשכנע אוכלוסיות של מהגרים המתגוררות בחברות מערביות ומדוע מהגרים אלה מועדים לקיצוניות למרות שהם חיים בדמוקרטיות יציבות וחופשיות?

מאמר זה משלב מרכיבים של הפסיכולוגיה הקוגניטיבית (ובמיוחד את המושג "המלחמה הקוגניטיבית הראשונה" שטבע גבי סיבוני) והטכנולוגיה הווירטואלית עם מרכיבים של המאבק בקיצוניות האלימה, במטרה לנסות ולהסביר מדוע גופים מערביים העוסקים בסיכול טרור – ממשלות, צבאות וסוכנויות מודיעין – מתקשים לנהל את המאבק בגיוס הווירטואלי.[1] המאמר עוסק בחברות המערביות שלא הצליחו להביא מבחינה פסיכולוגית את קהילות המהגרים שלהן להשתלב בערכיהן הדמוקרטיים. ההתנערות מאחריות לפיתוח אמצעי נגד למצב זה מסבירה מדוע קבוצות מסוימות של מהגרים מתגוררות "במערב", אבל נותרות "לא מערביות".

המאמר גם מנתח את השאלה כיצד האינטרנט הפך לכלי לניצול זדוני של כישלון הדמוקרטיה המודרנית לממש את התחייבויותיה. נושא זה חוצה תחומים רבים וחשובים הנוגעים לאינטרנט ולחברה, ובכלל זה תפקיד הרשתות החברתיות בקמפיינים פוליטיים ובניסוח מדיניות מודיעינית; נשיאה באחריות והזכות לפיצוי על עוולות ברשת; חידושים (שליליים וחיוביים כאחד) בהשתתפות ובמעורבות האזרחיות; תנועות חברתיות מקוונות; חוסר יציבות ותנודתיות בחיים הפוליטיים; עליית הקיצוניות והגברת הקיטוב.

המאמר מתמקד בניתוח האופן שבו פועלת התעמולה הווירטואלית הקיצונית, תוך התייחסות לאפקטיביות של הטכנולוגיה הווירטואלית שנמצאת בשימוש והעמדתה מול המדיניות הבלתי יעילה והמאכזבת של הדמוקרטיות המערביות הנאבקות בקבוצות הקיצוניות. כישלון התוכניות להתמודדות עם קיצוניות אלימה, מול המתקפה הווירטואלית של הגורמים הקיצוניים, מחייב להשיב על מספר שאלות לא קלות על האופן שבו הדמוקרטיה המודרנית אינה מצליחה לממש את

1 Gabi Siboni, "The First Cognitive War", in: *Strategic Survey for Israel 2016-2017*, eds. Anat Kurz and Shlomo Brom (Tel Aviv: Institute for National Security Studies, 2016).

האידיאלים שלה בעידן הדיגיטלי, במיוחד לנוכח המומחיות הטכנולוגית שמגלים גורמים קיצוניים. סביר להניח שאי־יכולת להתמודד עם מומחיות חדשה זו תביא לכך שקבוצות קיצוניות ימשיכו לקדם בהצלחה את סדר היום האלים שלהן ולהרוג עוד חפים מפשע. פירוש הדבר הוא שהדמוקרטיות המתקדמות ביותר ימשיכו להפסיד לקבוצות הקיצוניות ב"מלחמה הקוגניטיבית הראשונה".

"המלחמה הקוגניטיבית הראשונה"

גבי סיבוני היה הראשון לטבוע את המושג "מלחמה קוגניטיבית ראשונה" כביטוי לשימוש ההולך וגובר שעושים ארגונים תת־מדינתיים בטכנולוגיה וירטואלית במטרה לגייס אנשים למגוון רחב של פעילויות שנועדו לערער את החיים במדינה המודרנית. סיבוני מדגיש עד כמה רחבה מגמה זאת, הכוללת חרמות אקדמיים וכלכליים, ערעור הלגיטימיות של המערכות האלקטורליות והמשפטיות ואפילו ביצוע פעולות טרור של ממש. הוא מציין במפורש את השימוש היעיל בטכנולוגיות וירטואליות לא רק כדי לגייס את מה שמכונה "זאבים בודדים" לביצוע משימות טרור, אלא גם כדי להפוך אירועים אלה לספונטניים יותר ולפחות צפויים, ובדרך זו להימנע ככל האפשר מן הצורך בתשתית ארגונית פורמלית ובמערכות לוגיסטיות.[2]

עבודתו המקורית של סיבוני התמקדה באופן בלעדי בסיכון המיידי הנובע מיכולות כאלו כלפי תפקודה התקין של מדינת ישראל.

מאמר זה טוען כי המושג "מלחמה קוגניטיבית ראשונה" רלוונטי לא רק לישראל וכי ניתן להחיל אותו גם על הדמוקרטיות המערביות המתקדמות ביותר בעולם, עליהן הוא כבר השפיע רבות. מטריד במיוחד להיווכח עד כמה דמוקרטיות אלו אינן משלבות אסטרטגיות נגד חדשות במאבק בהתפתחותן של מגמות ההקצנה. הספרות המחקרית העוסקת בטרור הסייבר ובגיוס וירטואלי של גורמים קיצוניים היא רחבת היקף (כפי שיוצג בהמשך מאמר זה ביתר פירוט), אך מרביתה עוסקת בשיטות ובלוגיסטיקה של הגיוס וברקע האישי של המגויסים הפוטנציאליים. פירוש הדבר הוא שהיבט מכריע אינו מקבל את הדגש הראוי לו: מה השתבש מבחינה פסיכולוגית ו/או תפיסתית, עד שהביא לגיוס הווירטואלי של מהגרים המתגוררים בקהילות מהגרים בדמוקרטיות המערביות, שלכאורה היו אמורים להיות פחות פגיעים לתעמולה קיצונית.

היבט זה של עמדות המגויסים הפוטנציאליים כלפי הדמוקרטיות שבתוכן הם חיים הוא חשוב, משום שהוא עוסק בליבת היסוד הפסיכולוגי, שעשוי להיות הגורם שהופך אותם לבשלים לגיוס לשורותיהם של הגורמים הקיצוניים. במובן מסוים, זהו שדה הקרב הראשון ב"מלחמה הקוגניטיבית הראשונה", כלומר, זה המתייחס

2 Ibid.

לשאלה כיצד "ג'ון הג'יהאדיסט" הפוטנציאלי חווה את החיים בדמוקרטיה וכיצד חוויה זו טיפחה בו יחס שלילי כלפי המוסדות הדמוקרטיים.

זאת ועוד, גופים העוסקים בסיכול טרור צריכים להבין טוב יותר את ראשית תהליך "ההתפכחות" של המתגייסים הפוטנציאליים, משום שרק בשלב זה – השלב אותו אני מכנה "שלב הסמן המקדים" (pre-cursor phase) – יש לגופים ממשלתיים הזדמנות אמיתית להרתיע את המגויסים הפוטנציאליים ולעצור אותם מלהפוך ל"ג'ון הג'יהאדיסט" הבא. הספרות המחקרית העוסקת בגיוס באמצעות הסייבר נוטה להתעלם מחלק זה של התהליך, מתוך עמדה הגורסת שכל גישה ביקורתית כלפי החברה הדמוקרטית היא במידה רבה תפיסה לא נכונה, ולכן אינה בעלת ערך למחקר. זוהי עמדה שגויה. העיקרון של "המלחמה הקוגניטיבית הראשונה" הוא שיש ביכולתן של קבוצות לא מדינתיות להשפיע מבחינה פסיכולוגית על יחידים יותר מאשר גופי המדינה הרשמיים, ולכן יש חשיבות רבה לעמדותיהם של המגויסים הפוטנציאליים כלפי המדינות המארחות לפני שעברו תהליך של הקצנה. בטרם נצלול לעומקו של מרכיב חסר זה, יש לסקור את הספרות המחקרית העוסקת בגיוס גורמים קיצוניים.

המדיה החברתית, "ג'יהאד הסייבר" והאינטרנט ככלי נשק של קיצונים

הרעיון של "ג'יהאד אלקטרוני" או של ("www.mujahideen") אינו חדש. ארגון "אל־קאעידה" ניצל אותו היטב כבר לפני כעשרים שנה. ר' ל' תומפסון ערך ניתוח ביקורתי של הרשתות החברתיות שנפוצו במיוחד בקרב דור המילניום והראה כיצד הן הצליחו להגיע לרמת יעילות מסוכנת בפיתוי משתמשים ברשת בעזרת הבטחות לחברות ולהשתייכות. ההפגזה הווירטואלית במסרים קיצוניים יכולה למשוך בקלות מגויסים תמימים לתוך "מאורת הארנב" של ההיי־טק, מבלי שיידעו כיצד לצאת ממנה. תומפסון הראה כיצד שיעור החדירה הווירטואלית בחברות שונות במזרח התיכון ובצפון אפריקה גבוה מהממוצע, למרות התפיסה המערבית המקובלת שמדובר בשני אזורים נחשלים. החדירה הווירטואלית במזרח התיכון עולה ב־31.6 אחוזים על זו של סין, אף שהרוב במערב סבור שסין היא מדינה הרבה יותר מתקדמת מבחינה טכנולוגית, וכי אוכלוסייתה מחוברת לאינטרנט הרבה יותר מאוכלוסיות אחרות.[3]

3 R. L. Thompson, "Radicalization and the Use of Social Media", *Journal of Strategic Security* 4, no. 4 (2011): 167-190.

ס' ד' קין (Keene) עוסק בקשר בין האינטרנט ובין גיוס טרוריסטים.[4] הוא מכיר את הקושי לפקח על אתרי אינטרנט וחדרי צ'אט קיצוניים, לא כל שכן לסגור אותם, וזיהה את כוחה של המדיה הווירטואלית למצֵב קבוצות טרור כמובילות בנושאים בעלי חשיבות מרובה ואת האינטרנט ככלי העצמה שבאמצעותו יכולים מגויסים פוטנציאליים להשתכנע בקלות לתמוך בעמדות שהן שונות לחלוטין מאלו השגורות במדינות בהן הם מתארחים. עבודתו של קין היא דוגמה לספרות המחקרים המוקדמת בנושא הרדיקליות בסייבר, שראתה בעמדות ובגישות של המגויסים הפוטנציאליים כלפי החברה המארחת, לפני שהם נחשפו לאתרים ולתעמולה קיצוניים, לוח חלק. התמקדות במרחב זה תעזור לנו להבין את כוח המשיכה הראשוני של הרדיקליזם הווירטואלי בקרב חלק מהמוסלמים החיים במערב. ואכן, בריאן לוין מראה כיצד האינטרנט הפך במהלך השלבים המוקדמים של הרדיקליזציה הווירטואלית למעין מערכת שלמה, שבה אזרחים אמריקאים (כלומר, אנשים שנולדו בארצות הברית או התאזרחו בה לאחר פרק חיים ארוך שם, כך שקשה לאפיין אותם כבעיה של "האחר") נוטלים חלק מרכזי בגיבוש, בתחזוקה ובהפצה של תכנים מקוונים הגורמים להקצנת עמדות של מהגרים מוסלמים, ואפילו של ילידי ארצות הברית, ודוחפים אותם לבצע התקפות נגד מדינותיהם.[5] גם במקרה זה, המחקר לא בחן את העמדות המקוריות של המתגייסים הפוטנציאליים קודם לחשיפתם לתכנים הווירטואליים.

המאפיין המרכזי של האינטרנט, שהפך אותו למקובל כל כך בעיניהם של אנשי דת רדיקליים, הוא הנאמנות שהוא מעודד. שלא כמו נאומים בעל פה או מידע העובר מפה לאוזן, האינטרנט מאפשר להעתיק מסרים מילה במילה ולשלוח אותם כפי שהם לכל רחבי העולם מבלי לאבד מתוכנם. הוא גם מציע אתר וירטואלי קבוע שאנשים יכולים לחזור אליו ולמצוא אותו בלי קשר למשך הזמן שעבר מאז שנתקלו בו לראשונה.

מרטין רודנר (Rudner) הצביע לאחרונה, בסדר עולה של חומרה, על הפונקציות הרבות של הפעילות הווירטואלית מצד קבוצות אסלאמיות קיצוניות:

1. הפיכת קהילות מוסלמיות בדמוקרטיות מערביות לגורמים חתרניים, תוך הונאת הממשלות במדינות המארחות והסחת דעתן כדי שלא יגיבו לאיום הגובר.
2. טיפוח עמדות התומכות בפעולות טרור.
3. מתן הצדקה תיאולוגית למעשי אלימות פוליטית או לטרור.
4. מתן הנחיות טכניות והוראות פעולה למעשי טרור.

---

4 S. D. Keene, "Terrorism and the Internet: A Double-Edged Sword", *Journal of Money Laundering Control* 14, no. 4 (2011): 359-370.

5 Brian Levin, "The Original Web of Hate Revolution: Muslim and American Homegrown Extremists", *American Behavioral Scientist* 59, no. 12 (2015): 1609-1630.

5. קידום מעורבות ישירה בפעילויות מכינות המאפשרות פעולות טרור.
6. עידוד מעורבות אישית בביצוע פעולות טרור.[6]

מחקרים כמו זה של רודנר מתמקדים יותר מכל במרכיב ההמרה הפנימית שמביאה לגיוס. ואכן, מרטין רודנר הראה כיצד לימודי דת וירטואליים מילאו תפקיד גדול יותר בגיוס מאשר פילוסופיות פוליטיות טהורות, וכינה אותם "הסמן המקדים הנחוץ" בשלב ההכשרה. אני מבקש לטעון שהסמן המקדים האולטימטיבי בשלב ההכשרה של מגויסים מהמערב הוא תהליך ההתפכחות והאכזבה שלהם מהחברה המערבית, לאחר שהגירתם למערב הייתה מלווה בשלבה הראשון בתקוות גדולות ובאופטימיות רבה. על הספרות המחקרית להתמקד טוב יותר בתהליך זה, משום שספק אם גיוס וירטואלי בהיקף כלשהו היה מצליח במצב שבו "החיים האמיתיים" של המגויסים הפוטנציאליים במערב היו נחווים כהצלחה.

אנג'לה ג'נדרון (Gendron) צללה עמוק אפילו יותר בניסיון להבין את הניואנסים שנעשה בהם שימוש במסגרת הקריאה הווירטואלית לג'יהאד. אותן "טכניקות טיפוח" עשו שימוש בשורה של גורמים פסיכולוגיים, סביבתיים וחברתיים, שלכל אחד מהם יכולת השפעה בדרגות שונות. המחקר של ג'נדרון נשען, במידה רבה, על עבודתו החשובה של "המרכז ללכידות חברתית", שהתמקדה בשלוש פונקציות ליבה שממלאים האתרים הגי'האדיסטיים:

- **ספריות מקוונות**. אלו כוללות אתרים ג'יהאדיסטיים הממלאים תפקיד מרכזי כמאגרי הרצאות של דמויות מפתח בפנתיאון הג'יהאדי; סרטונים שהוכנו על ידי "אל־קאעידה" וקבוצות קיצוניות אחרות; נשידים, כלומר שירים ערביים מסורתיים המהללים אלימות אסלאמית. חלק גדול מחומר זה זמין באופן מקוון וכולל תרגום לאנגלית של המקורות הערביים.
- **זירה למטיפים**. אתרים ג'יהאדיסטיים מפרסמים דרשות והרצאות של מטיפים אסלאמיים רדיקליים בולטים ושל פרשנים המקדמים ג'יהאד, ואלו נגישות בקלות דרך האינטרנט.
- **פורומים לשיח**. אתרים ג'יהאדיסטיים רבים מארחים חדרי צ'אט, פורומים לדיונים וקבוצות דיון. אלה מקלים על קיום שיחות מקוונות בין מאמינים החולקים דעות דומות, ומשמשים כמוקדי התארגנות לתכנון ולתיאום פעילויות בנושאים מרכזיים. קשר חברתי ורשתות חברתיות יוצרים קהילות מקוונות ותומכים בהן, וכן מאפשרים לפעילי ג'יהאד ולאלה התומכים בהם לשתף מידע ולחזק את הקשר ביניהם.[7]

---

6 Martin Rudner, "Electronic Jihad: The Internet as Al Qaeda's Catalyst for Global Terror", *Studies in Conflict & Terrorism* 40, no. 1 (2017): 10-23.

7 Angela Gendron, "The Call to Jihad: Charismatic Preachers and the Internet", *Studies in Conflict & Terrorism* 40, no. 1 (2017): 44-61.

מ' האמבלט (Hamblet) הסתמך על עבודה זו של "המרכז ללכידות חברתית" ועל מחקרים רבים שהרחיבו בנושא זה, ובהם של מכון ראנד, אוניברסיטת ג'ורג' וושינגטון וממשטרת ניו יורק, כדי להדגיש שבהשוואה ל"אל־קאעידה", ארגון המדינה האסלאמית לא רק פעל בדרך שונה והפך למתוחכם בשימוש שהוא עושה באינטרנט, אלא גם נבדל מ"אל־קאעידה" במקורות הגיוס שלו, החל מהמוצא הגיאוגרפי וכלה בגיל הממוצע הכללי של המגויסים. ניתן לראות זאת היטב בארבעת השלבים של הרדיקליזציה שזוהו בדוח של משטרת ניו יורק:

- **טרום רדיקליזציה**: החיים לפני אימוץ האידיאולוגיה של הג'יהאד הסלפי.
- **הזדהות עצמית**: גילוי וחקירה של האסלאם הסלפי.
- **אינדוקטרינציה**: העצמת האמונה ואימוץ מלא של האידיאולוגיה.
- **ג'יהאדיזציה**: קבלה של החובה להילחם בשם הג'יהאד; תכנון וביצוע מתקפת טרור.[8]

למרבה הצער, הדוח של משטרת ניו יורק אינו מקדיש תשומת לב מחקרית שווה לכל אחד מארבעת השלבים. שלושת השלבים האחרונים – הזדהות עצמית, אינדוקטרינציה וג'יהאדיזציה – קיבלו בדוח הרבה יותר משקל מאשר השלב הראשון. כפי שנראה בהמשך, הסוכנויות והארגונים המעורבים ביותר בהרתעה ובמאבק בקיצוניות החמיצו הזדמנויות פז בשל ההתעלמות מהשלב המקדים, קרי, שלב החיים שלפני אימוץ האמונות הקיצוניות. הבנת הסיבה מדוע המתגייסים הפוטנציאליים לארגוני הג'יהאד עוברים התפכחות ואכזבה מהחברות המערביות המארחות אותם, במידה כזו שהופכת אותם לפרי בשל לגיוס בידי גורמים קיצוניים, היא מרכיב קריטי שרוב ארגוני האכיפה והמודיעין עדיין לא ניתחו לעומק ובצורה מספקת.

חשיבותן של עבודות דוגמת אלו של ג'נדרון והאמבלט היא בכך שהן מראות כיצד טכנולוגיית האינטרנט שינתה את הייעוד ואת המיתוג של האידיאולוגיה האסלאמית הרדיקלית, שלעיתים תכופות הוצגה על ידי התקשורת והפרשנים המערביים כארכאית, נחשלת ותקועה במאה ה־16, והפכה אותה לדבר הרבה יותר מודרני, כריזמטי ומושך. עם זאת, מאמר זה מבקש להראות שאין זה משנה עד כמה אטרקטיביים או כריזמטיים הם אימאמים קיצוניים מסוימים, וגם לא משנה עד כמה מסוגננים ומושכים הם אתרי האינטרנט הקיצוניים; הסגנון אינו הגורם היחיד בהמרת אנשים לג'יהאדיזם.[9] השיבוש המהותי שחל בחייהם של המגויסים

8 M. Hamblet, "The Islamic State's Virtual Caliphate", *Middle East Quarterly* 24, no. 4 (2017): 1-8.

9 Anne Aly, "Brothers, Believers, Brave Mujahideen: Focusing Attention on the Audience of Violent Jihadist Preachers", *Studies in Conflict & Terrorism* 40, no. 1 (2017): 62-76; Peter Wignell, Sabine Tan and Kay L. O'Halloran, "Under the Shade of AK47s: A Multimodal Approach to Violent Extremist Recruitment Strategies for

הפוטנציאליים (לפחות על פי תפיסתם), שנתפס בהמשך ככישלונה של החברה המערבית לממש את הבטחותיה, הוא הסמן המקדים המכריע החסר בכל אותם מחקרים. קל יותר לעצור את הדרך לעבר האידיאולוגיה הג'יהאדיסטית בשלב העוברי שלה, מאשר בשלב שבו היא כבר הצליחה ליצור תומכים מוצהרים בג'יהאד. מאבק וירטואלי בהקצנה בשלבה המקדים הוא יעיל והגיוני יותר מאשר מאבק כזה המתנהל בשלבי האימוץ הפעיל שלה. נקודה זו לא הודגשה מספיק בספרות המחקרית עד היום, ולכן היא נעדרת מהמדיניות העוסקת בנושא.

פיקאר (Picart) מתקרבת להכרה בפער זה כאשר היא מנסחת את מה שהיא מכנה ה"שִׁיק של הג'יהאד" או ה"קוּליוּת של הג'יהאד". במבט ראשון נראה כי המחקר של פיקאר תואם באופן מושלם את עקרונות "המלחמה הקוגניטיבית הראשונה" ואת הצורך להבין את התהליכים הפסיכולוגיים הפנימיים של המגויסים הפוטנציאליים. אכן, דומה שהרצון להיות רלוונטי – או מה שמכונה "טיפוס קשוח" – הוא בעל השפעה רבה על גברים צעירים הנחשפים לגיוס הווירטואלי.[10] גם אין ספק שסגנון הגיוס (קרי, לשוחח עם המועמד הפוטנציאלי בשפה שהוא מבין ולגרום לכך שהתנהגות קיצונית תיראה בעיניו כ"מגניבה") הוא מרכיב חשוב, אבל הוא מחמיץ את הסמן המקדים, שהוא־הוא המרכיב החיוני: מדוע תפיסת "הטיפוס הקשוח" שמציעה הקהילה הקיצונית תיראה כדבר אטרקטיבי למי שכבר מרגיש "טיפוס קשוח" בקהילה המארחת שלו? מאמר זה מבקש לטעון שתפיסת "הטיפוס הקשוח" לא אמורה להיות הגורם האטרקטיבי ביותר, ולכן חשוב יותר לנתח את חוסר ההצלחה של המגויסים הפוטנציאליים להשתלב בקהילה המארחת.

פוסט (Post), שדן בשאלה כיצד בני אדם מנוכרים מתפתים להצטרף ל"קהילה של שנאה",[11] הגדיר את הסכנות שבעולם האינטרנט הקיצוני. הוא גם בדק כיצד טרור, אפילו אם הוא "תוצרת בית", מכוון על ידי אסטרטגיות זרות וחיצוניות, דבר המקשה עוד יותר על האסטרטגיות הנגדיות שמפעילה המדינה, בשל מחויבותה לכבד את העקרונות המערביים של חופש וחירות אזרחית. הטיעון של פוסט משתמש בנימוק לקוי: מחקרים כמו שלו מיטיבים להכיר באי־הצלחתה של תעמולת הנגד המערבית, אך אינם טורחים לשאול מדוע הדבר הוא כך. אם המגויסים

Foreign Fighters", *Critical Studies on Terrorism* 10, no. 3 (2017): 429-452; Javier Argomaniz, "European Union Responses to Terrorist Use of the Internet", *Cooperation and Conflict* 50, no. 2 (2015): 250-268.

10 C.J.S. Picart, "Jihad Cool/Jihad Chic: The Roles of the Internet and Imagined Relations in the Self-Radicalization of Colleen LaRose (Jihad Jane)", Societies 5 (2015): 354-383.

11 J. M. Post, "Terrorism and Right-Wing Extremism: The Changing Face of Terrorism and Political Violence in the 21st Century: The Virtual Community of Hatred", *International Journal of Group Psychotherapy* 65, no. 2 (2015): 242-271.

הפוטנציאליים היו נהנים מחירויות אזרחיות, מחופש ומשאר היתרונות שהם סימן ההיכר של החברה הדמוקרטית המארחת, אזי הם לא היו דוחים בקלות כזאת את תעמולת הנגד המערבית, ולמעשה לא היו רואים בה תעמולה כלל. שוב ושוב מחמיצים המחקרים הקיימים את ההזדמנות לרדת לעומקו של פער זה.

מויר (Moir) ממשיך עם רעיון "קהילת השנאה" במחקרו על התפיסה, לפיה אתרים של רשתות חברתיות קיצוניות הם יותר מאשר זירה לתקשורת הדדית, ולמעשה הם גורם חיוני ליצירת תחושה של חוסר שייכות בקרב מגויסים פוטנציאליים, באופן שגורם להם להרגיש שהם נמשכים ומתפתים פחות לאפשרויות שיש למדינה המארחת אותם להציע.[12] מחקרים מסוג זה אמנם מתמקדים בתהליך האינדוקטרינציה ובפיתויים שמציעות רשתות חברתיות לקיצונים בפוטנציה, אך גם מחזקים את אמינות הטיעון שמובא כאן, לפיו הבנה נכונה של האופן שבו הקהילות המארחות לא מצליחות להגיע ל"זאבים בודדים", היא קריטית ליצירת אמצעי נגד מוקדמים ויעילים.

כמה מחקרים חדשים מתמקדים בהקצנה הגוברת ברחבי האיחוד האירופי ונוגעים, במסגרת זו, בגורם של הסמן המקדים. לוגן מקנייר וריצ'רד פרנק (Macnair and Frank) מתמקדים ספציפית בסרטוני הגיוס של מרכז התקשורת של המדינה האסלאמית – "אל־חיאת". הם מדגישים, ובצדק, כי לא מדובר רק באיכות המקצועית, המסוגננת והיחצנית של הסרטונים, אלא גם במשיכה הרגשית הטבועה בהם, שמדברת אל אנשים המתגוררים במערב אך מוטרדים או לא מרוצים מחייהם.[13] החוקרים מתמקדים באופן שבו הסרטונים של ארגון המדינה האסלאמית מבקשים לתקן תחושות אלו על ידי הבטחות לאושר, כבוד ותהילה, לא רק בעולם הזה, אלא גם בעולם הרוחני הבא. יש בכך החמצה מסוימת, שכן הנכונות של המגויסים הפוטנציאליים להיענות להקצנה אינה מתבססת רק על הבטחות עתידיות, אלא גם, ובעיקר, על חוסר שביעות הרצון שלהם כיום מהמדינה שבה הם חיים.[14] התבססות החוקרים על ההבטחות לתהילה מצביעה על כך שלדעתם ההתמרמרות על מה

12 N. L. Moir, "ISIL Radicalization, Recruitment and Social Media Operations in Indonesia, Malaysia and the Philippines", *Prism: A Journal of the Center for Complex Operations* 7, no. 1 (2017): 90-107.

13 Logan Macnair and Richard Frank, "To My Brothers in the West . . . : A Thematic Analysis of Videos Produced by the Islamic State's Al-Hayat Media Center", *Journal of Contemporary Criminal Justice* 33, no. 3 (2017): 234-253.

14 Mohammed Hafez and Creighton Mullins, "The Radicalization Puzzle: A Theoretical Synthesis of Empirical Approaches to Homegrown Extremism", *Studies in Conflict & Terrorism* 38, no. 11 (2015): 958-975; Levin, "The Original Web of Hate: Revolution: Muslim and American Homegrown Extremists"; Guy D. Golan, "Countering Violent Extremism: A Whole Community Approach to Prevention and Intervention" (master's thesis, California State University, 2016).

שנתפס כדיכוי המוסלמים היא הלהבה שהציתה את הרדיקליזם החדש. בניגוד לכך, מאמר זה טוען שבמקום לעסוק ברגשות מופשטים בדבר דיכוי פוליטי ברמה הגלובלית, הגיוני ומשכנע יותר להניח שהקצנה נולדת בקרב אנשים שחשים כמי שנפגעו באופן אישי מהמדינות שבתוכן הם חיים. תחושה זו של אכזבה אישית לא זכתה לניתוח מספק בכל מה שנוגע למשמעותה בהקשר לסיכול טרור.

ברזיקה (Brzica) הוא הקרוב ביותר מבין החוקרים "ליישר קו" בין הספרות המחקרית הקיימת ובין הגורם החברתי של הסמן המקדים. ברזיקה קישר בין האופי המבוזר והאוטונומי של האינטרנט ובין המאפיינים החברתיים של טרור "הזאבים הבודדים" והסיק מכך שקשה לגלות בתוך עשרות אלפי אתרים את אלה המשפיעים על היווצרותם של אותם "זאבים בודדים" ועל המוטיבציה שלהם לבצע פעולות טרור על אדמה מערבית, ובמקביל ליצור הרתעה כלפיהם.[15] ברזיקה סיווג את התומכים הפוטנציאליים באסלאם הקיצוני לפי מספר קטגוריות, שהרביעית שבהן רלוונטית לניתוח שבו עוסק מאמר זה: "... מהגרים שהגיעו לאיחוד האירופי ועלולים לעבור רדיקליזציה בשל תסכול מתנאי החיים שם, יחד עם חשיפתם לתעמולה ג'יהאדיסטית קיצונית באמצעות האינטרנט או באמצעות גורמים התומכים באידיאולוגיות קיצוניות ופועלים בקרב קהילות אסלאמיות מבוססות באירופה".[16]

ברזיקה מתקרב לענייננו, אך הוא עדיין רחוק ממנו, שכן הוא מנתח את התעמולה באינטרנט במקום לעסוק בממד אותו הוא מתאר כ"תסכול מתנאי החיים שם". היצמדות למושגים מופשטים, תוך התעלמות מהמקורות הישירים והמפורשים של כעס ותוקפנות, יוצרת קשר רופף בלבד בין גוף הידע על טרור "הזאבים הבודדים" ועל גיוס קיצונים במערב ובין תפיסת "המלחמה הקוגניטיבית הראשונה".

ארבע הקטגוריות של ג'יהאדיסטים פוטנציאליים על פי ברזיקה כוללות את "הפגיעויות" הבאות: מעמד סוציו־אקונומי, הבדלים תרבותיים, תחושת שייכות אתנית (או היעדרה), שכנוע דתי ו/או גורמים פסיכולוגיים.[17] אין ספק שכל הגורמים האלה משחקים תפקיד ביצירת ג'יהאדיסטים, אך ערוב של ארבעתם, ללא שום הבחנה או יצירת בידול מחקרי ביניהם, כמוהו כמלחמה בטרור באמצעות ירי לכל הכיוונים: הוא פוגע, אך לא מועיל לעיצוב אסטרטגיית הרתעה יעילה.

עבודתה של קארן גרינברג היא דוגמה טובה למחקר המבקש לבחון האם האינטרנט, שנוצל בצורה כה יעילה ככלי להקצנה, יכול לשמש באותה מידה

15 N. Brzica, "Potential Adherents of Radical Islam in Europe: Methods of Recruitment and the Age of Perpetrators in Acts of Terror", *Politička misao* 54, no. 4 (2017): 161-184.

16 Ibid., p. 170.

17 Ibid.

גם כנשק של תגובות נגד. למרבה הצער, הספרות המחקרית לוקחת את ממד ההרתעה שיש לאינטרנט בצורה פשטנית מדי, ומתמקדת בפתרונות פוטנציאליים המתייחסים מאוחר מדי למעגל ההקצנה. כך, למשל, גרינברג מתמקדת בשלוש טכניקות וירטואליות מרכזיות שעשויות להניב הרתעה: מאמצי שיבוש, המבוססים על התערבות טכנולוגית של חברות אינטרנט בשם הממשל האמריקאי; הטיה ויצירת עניין שונה; הפצה של נרטיבים או מסרים נגדיים.[18]

ככלל, למאמצי השיבוש יש השפעה קטנה בלבד, שכן האינטרנט הוא טכנולוגיה גמישה ובעלת כושר הסתגלות גבוה. אפילו משטרים אוטוקרטיים במיוחד, דוגמת סין, אינם מסוגלים "לסלק" גורמים רדיקליים באמצעות מהלכי שיבוש. הטיה ויצירת עניין שונה הולכות, במקרים רבים, יד ביד עם מסרים נגדיים. הגיוני להניח שמסרים נגדיים אפקטיביים ייצרו עניין אצל מגויסים פוטנציאליים, וכאשר הדבר אינו קורה, יש להפנות את הביקורת אל תוכנו של המסר הנגדי. במילים אחרות, ההנחה היא שאם המדינה רק תמצא את המסר הנכון, אסטרטגיית ההרתעה אכן תפעל. הבעיה בהנחה זו היא שאינה מתייחסת לעיתוי, שהוא ההיבט המכריע בסוגיה זאת: אפילו המסר הנגדי הטוב ביותר יתגלה כבלתי אפקטיבי כאשר המגויס הפוטנציאלי כבר נמצא הרחק בדרכו להקצנה. מכיוון שחלק גדול ממערך ההרתעה של המדינה מנסה להילחם בקיצונים זמן רב לאחר שהם הפכו למגויסים באמצעות התעמולה המקוונת, אין זה מפתיע לגלות שרבות מאסטרטגיות ההרתעה מופעלות מאוחר מדי. בנוסף לכך, אסטרטגיות אלו אינן מתייחסות בצורה ביקורתית לאשמתו של המצב החברתי, כגורם אפשרי ביצירת אווירה פסיכולוגית המכשירה את הגיוס באמצעות האינטרנט.

גרינברג מציינת כי תוכניות הנגד זכו עד היום לאמון מועט ביותר, למרות שיש עדיין נתונים ומדדים שטרם נותחו.[19] למרות כל זאת, היא מגלה אופטימיות לגבי האפשרות שהאינטרנט יהפוך, בסופו של דבר, לכלי רב עוצמה במאבק בטרור. אני מוכן להצטרף לאופטימיות זאת בתנאי שממשלות המערב יחדדו את שאלת העיתוי ויגבירו את הביקורת העצמית, כחלק מפיתוח אסטרטגיות הנגד.

הסקירה של הספרות המחקרית שהוצגה לעיל מצביעה על כישלונה לנתח את חייהם ודרך חשיבתם של המגויסים לארגוני הג'יהאד באמצעות האינטרנט בשלב שלפני הפיכתם לקיצונים. במקום הנטייה הנוכחית להתמקד בסיפורי תהילה הירואיים, בהצהרות רוחניות של קדושה ובמושגים מופשטים של טינה פוליטית, אני טוען שהערכה מעמיקה יותר של התסכול, הייאוש וחוסר הנחת הכללי שנוצרים אצל המגויסים הפוטנציאליים עקב אי־הצלחתם במדינות המערב שבהן הם חיים,

18 Karen J. Greenberg, "Counter-radicalization via the Internet", *The Annals of the American Academy of Political and Social Science* 668, no. 1 (2016): 165-179.

19 Ibid.

תצביע על גורמים אלה כבסיס וכסיבה לעמדות הקיצוניות המתגלות בקרב אותן אוכלוסיות של מהגרים. אם טיעון זה שלי נכון, הוא נותן למדינות המערב מושג ברור יותר מתי עליהן להפעיל את אסטרטגיות הנגד שלהן: כאשר המגויסים הפוטנציאליים עדיין חיים במערב וכאשר הם עדיין מקווים להיות חלק ממנו. שיבוש, הטיה ומסרים נגדיים כלפי מהגרים שאמנם חיים במערב, אך כבר אינם שואפים להיות "מערביים", הם מהלכים מאוחרים מדי ומהווים בזבוז של משאבי המדינה. מקרה המבחן של האחים צַרְנַיֶיב, שעשו את הפיגוע בריצת המרתון של בוסטון בשנת 2013, ישמש כדי להמחיש נושא זה.

האחים צרנייב: "חולמים" אמריקאים מתוסכלים?

לכידת שני האחים טמרלן וג'וחר צרנייב בעקבות הפיגוע במרתון בוסטון היא סיפור מתועד היטב. התהליך ההדרגתי של פניית טמרלן אל אימאמים מוסלמים כריזמטיים באמצעות האינטרנט והסתבכותו בתקריות אלימות עם אשתו האמריקאית זכו לכיסוי ברמה כמעט מציצנית.[20] ג'וחר, מצידו, תואר כאח הצעיר שהעריץ יתר על המידה את אחיו הבכור, ואף על פי כן הציבור האמריקאי לא חש כל אהדה כלפיו אפילו כאשר נגזר עליו עונש מוות.[21] הפיגוע במרתון בוסטון הוא, במידה רבה, אזהרה מפני מי שנראים לכאורה כצעירים נורמטיביים, העלולים לפנות ללא סיבה ברורה לקיצוניות, גם לאחר שקיבלו את כל ההזדמנויות האפשריות בחברה הדמוקרטית המערבית.[22] מוצאם הצ'צ'ני של שני האחים הוזכר מספר רב של פעמים, כאילו די בעובדה זו כדי לעורר את חשדן של הרשויות המקומיות בדבר הסכנה הפוטנציאלית הטמונה בהם.[23]

ניתוח כזה בדיעבד של תהליך הקצנה הוא אופייני למדי: מטיפים מוסלמים כריזמטיים המופיעים באינטרנט נחשבים לתופעה דתית בלבד, עד שהם הופכים לאמצעי לשטיפת מוח. מוצא צ'צ'ני אינו משנה דבר עד לרגע שבו מתברר שמהותם הרוחנית של האחים צרנייב הייתה מאז ומתמיד בעלת פוטנציאל של אלימות; זאת ועוד, גבר שמאלץ את אשתו להתלבש בהתאם לקוד הלבוש האסלאמי הקפדני נחשב לשמרן גרידא, עד לרגע שהדבר מתפרש כדחייה של עקרונות החופש המערביים. גם הפרטים שתיעדו את הניסיונות הראשוניים של האחים צרנייב להסתיר את

20 Peter Foster and Tom Parfitt, "Boston Bomber Arrested: Tamerlan Tsarnaev's Hateful Rage behind American Dream", *The Telegraph*, April 20, 2013.

21 Ron Borges, "Dead Suspect's Coach: 'I Never Saw any Hatred'", *Boston Herald*, April 19, 2013.

22 Marc Fisher, "The Tsarnaev Family: A Faded Portrait of an Immigrant's American Dream", *The Washington Post*, April 28, 2013.

23 Benjamin Lytal. "The Chechen Grievance: Tolstoy's 'Hadji Murad' after Boston", *Daily Beast*, April 21, 2013.

טיבם מפני החברה האמריקאית נתקלו בהתעלמות מסוימת, כאילו היה מדובר באירועים נקודתיים חסרי משמעות ובני חלוף.[24] אני סבור כי סוג כזה של ניתוח לא מאפשר לזהות את השלב שבו ניתן להפעיל אמצעי נגד אפקטיביים, וגם לא את הסימנים המעידים החשובים העשויים לסייע למשטרה, לארגוני המודיעין ולארגונים החברתיים ב"מלחמה הקוגניטיבית הראשונה".

המקרה של האחים צרנייב מוכיח עד כמה רבות ההזדמנויות ליצור הרתעה כבר בשלב הסמן המקדים. טמרלן, האח שנראה האתלט מבין מהשניים וכמי שנוטה פחות ללימודים, השקיע מאמצים רציניים בענף האִגרוף והתקדם בו די הצורך כדי לייצג את אזור ניו־אינגלנד באליפות האגרוף הלאומית "כפפות הזהב". במהלך תקופה זו הוא אפילו הצהיר כי אם מולדתו צ'צ'ניה לא תקבל עצמאות ותישאר אזור בעייתי בפדרציה הרוסית, הוא יעדיף לייצג את ארצות הברית באולימפיאדה מאשר להיות חלק ממשלחת רוסיה;[25] במונחים של "המלחמה הקוגניטיבית הראשונה", כאשר לקיצוניות הווירטואלית יש אחיזה חזקה כל כך, אמירות מסוג זה מהוות הזדמנות שניתן לבנות עליה. טינתו של טמרלן כלפי רוסיה מובנת למדי לכל מי שנמנה על הגולה הצ'צ'נית, אבל טינה זאת לא הופכת אוטומטית לרצון לייצג את ארצות הברית. כל מי שמתעניין במלחמות הצ'צ'ניות יודע שמה שמתואר כ"המאבק הצ'צ'ני לעצמאות" מוצג לעיתים קרובות גם כעימות בין רוסיה ובין קיצונים אסלאמיים. זאת, נוכח העובדה שתנועת העצמאות בצ'צ'ניה אכן נתמכת במידה רבה על ידי גורמים קיצוניים כאלה. הקיצוניות האסלאמית זלזלה מאז ומתמיד הן בחברה האמריקאית והן בחברה הרוסית והתייחסה אליהן בבוז, אלא שבשלבי ההקצנה המוקדמים שלו טמרלן עדיין עשה הבחנה בין יחסו לרוסיה (שהכעס שלו כלפיה היה יותר פוליטי מאשר דתי) ובין יחסו לארצות הברית (שאותה הוא היה מוכן עדיין לאמץ כמולדתו החדשה).

ההיטמעות של ג'וחר צרנייב בחיים האמריקאיים הייתה עמוקה עוד יותר. הוא תואר כתלמיד תיכון ידידותי, שאהב סקייטבורד והפך לקפטן קבוצת ההיאבקות בבית הספר שלו. בהמשך הוא נרשם לאוניברסיטת מסצ'וסטס בדרטמות'. בזמן לימודיו שם נחשב ג'וחר לסטודנט חביב, חברותי, אהוב, ורבים דיווחו שסיפר להם כי מטרתו היא ללמוד רפואת שיניים. כאמור, מרבית ההתייחסויות לפיגוע במרתון בוסטון פטרו את ג'וחר כצעיר חלש אופי, שלא היה לו הכוח לעצור את תהליך הגיוס של אחיו, ובסופו של דבר הלך בעקבותיו מתוך נאמנות משפחתית. השאלה

24 Peter Finn, Carol D. Leonnig and Will Englund, "Tsarnaev Brothers' Homeland was War-Torn Chechnya", *The Washington Post,* April 19, 2013.

25 Snejana Farberov, "He Dreamed of Being an Olympic Boxing Hero for the USA but then Turned to Radical Islam; Older Bomb Suspect was a 'Talented' Fighter with a Dark Side", *Daily Mail*, 20 April 2013, p. 4.

אם הניתוח הפסיכולוגי הפשטני הזה מדויק אינה משנה לענייננו; חשובה יותר השאלה עד כמה אפשר היה להתערב ולהרתיע את ג'וחר בשלב הסמן המקדים? כאמור, האח הצעיר נטמע בחברה האמריקאית טוב מאחיו המבוגר וביקש ללמוד מקצוע בעל משמעות חברתית כמו רפואת שיניים. אין לזלזל בסמנים מקדימים כמו אלה, כפי שלא ניתן לראות בהם אישוש לקיצוניות: גופים העוסקים בסיכול טרור נוטים להאמין שניתן לזהות את המגויסים הפוטנציאליים רק לאחר שהם יזמו קשר עם ארגונים קיצוניים, אולם במציאות הדבר אינו תמיד נכון. למעשה, בשנת 2011 ביקש שירות הביטחון הרוסי (ה־FSB) מה־FBI לפקוח עין על טמרלן, משום שהרוסים חשדו שבאחד מביקוריו המשפחתיים ברפובליקה של דגסטן (שיש לה היסטוריה ארוכת שנים של קיצוניות אסלאמית), ייתכן שיצר קשר עם ארגונים קיצוניים שם. ה־FBI אכן בחן את המקרה, אבל לא מצא שום בסיס לחשש הרוסי.

המקרה של האחים צרנייב מראה כי המודל הקיים לאיתור יעדים לגיוס, המתבסס על מעקב אחר ניסיונותיהם של מגויסים פוטנציאליים ליצור קשר עם ארגונים קיצוניים מוכרים, מתמודד עם הבעיה בשלב מאוחר מדי ואינו יעיל בגילוי גורמי איום ממשיים. אין ספק שמודל זה לא פעל במקרה של האחים צרנייב. תוכנית שתכלול אמצעי נגד פרואקטיביים, שתתבסס על התערותם החיובית של המועמדים הפוטנציאליים בתוך החברה המארחת, עשויה להיות יעילה יותר. אין פירוש הדבר שהיה צריך "לארגן" את אליפות "כפפות הזהב" כך שטמרלן יזכה בה, או לתת לג'וחר מלגה מלאה לאוניברסיטה כדי שיגשים ביתר קלות את רצונו ללמוד רפואת שיניים גם אם לא היה זכאי לה; יש לפתח תוכניות ליצירת קשרים עם אוכלוסיות שמגיעות מ"אזורי איום" כמו צ'צ'ניה, במטרה לסייע להן להשתלב ביתר הצלחה בחברה המקומית. תוכניות כאלו קיימות במספר רב של מדינות דמוקרטיות במערב ומיועדות לקבוצות אוכלוסייה שונות ומסיבות רבות ומגוונות. אין ספק שיהיה זה נכון להוסיף אליהן תוכניות שיתבססו על העיקרון של מניעת התפתחותה של קיצוניות רדיקלית מבית.

סוג כזה של תוכניות נגד יכול היה לגרום לשינוי במקרה של האחים צרנייב, משום שנראה שתהליך ההקצנה שלהם לא ניזון משנאת הערכים האמריקאיים מסיבות אנטי דמוקרטיות ואנטי מערביות. להיפך, נראה כי ההקצנה שעברו האחים התרחשה בדיוק ברגע שבו תהליך ההיטמעות שלהם בחברה האמריקאית החל לסטות מהדרך (התפתחותו של טמרלן כמתאגרף נעצרה, וציוני ג'וחר בשנת הלימודים הראשונה שלו במכללה העמידו את המשך לימודיו בסכנה). רוסלן צארני, דודם של האחים צרנייב, שהפך זמנית לידוען מקומי בעקבות ראיון טלוויזיוני מפורסם אחד, הסביר בפשטות שהם נגררו לקיצוניות משום "שהיו 'מפסידנים' ושנאו את אלה שהצליחו להסתדר טוב מהם".[26] נכון היה להתייחס להערה זו ביתר רצינות, שכן

26. Finn, Leonnig and Englund, "Tsarnaev Brothers' Homeland was War-Torn Chechnya".

היא רומזת על נקודת מפנה קריטית להתערבות, כאשר המגויסים הפוטנציאליים עדיין אינם שקועים ברומן עם האידיאולוגיה הקיצונית, למרות שהם חווים טלטלה בשל חוסר יכולתם "להצליח" במולדתם החדשה. סיוע בתקופה זו יכול להיות יעיל לא רק בהרחקת המגויסים הפוטנציאליים מרדיקליזציה, אלא גם ביכולת ליצור אצלם תחושה עמוקה ויציבה יותר של נאמנות למדינה החדשה, ובדרך זאת לבנות שכבת הגנה עבה יותר נגד הטרור. אפשר לראות בכך מקרה נדיר של "סיווג חיובי": הערכה ומיפוי של יחידים לצורך התערבות שנועדה לסייע, תוך התבססות על הרקע והמורשת שלהם במטרה להשיג רמת ביטחון גבוהה יותר נגד הטרור.

המאמץ למנוע הקצנה של אותם אנשים שאינם מצליחים בחברה המערבית צריך לעמוד במוקד מאמצי ההתערבות/המניעה של רשויות אכיפת החוק וגורמי המודיעין במערב. משמעותה של ההתערבות בשלב הסמן המקדים ב"מלחמה הקוגניטיבית הראשונה" היא יצירת הזדמנות שתגרום לכך שמצבי חוסר הברירה ייחשבו לבחירה הגרועה ביותר, כפי שהם אכן צריכים להיות. כאמור, תוכניות התערבות חיובית כאלו מתקיימות מזה זמן רב במקומות שונים ומיועדות לקהילות מגוונות רבות, והגיע הזמן לנסות אותן גם בתחומי המודיעין והביטחון הלאומי.

סיכום: "המלחמה הקוגניטיבית הראשונה" מתרחבת

בפברואר 2018 פורסם דוח חדש ופוקח עיניים מטעם התוכנית ללימודי רדיקליזציה באוניברסיטת ג'ורג' וושינגטון, תחת הכותרת: "הנוסעים: הג'יהאדיסטים האמריקאים בעיראק ובסוריה". הדוח משלב בצורה מרתקת בין מדע המדינה ובין סוציולוגיה, וחושף את הקוראים לנוסעים אמריקאים ואירופים ההופכים לג'יהאדיסטים. הראיות הקיימות בארצות הברית מצביעות על התפתחות איטית ורופפת של תהליך הקצנה, ששורשיו נטועים בסכסוך האתני בבלקנים בתחילת שנות התשעים של המאה העשרים. הדבר מהווה עדות נוספת ל"בלקניזציה החברתית" בארצות הברית, שהמשיכה להתקיים גם לאחר הגעתם של גלי אוכלוסיות מהגרים חדשות. הדוח של אוניברסיטת ג'ורג' וושינגטון מכיר בתחושות הניתוק של המגויסים הפוטנציאליים, אך אינו יוצר את הקישור בין תחושות אלו ובין הכישלון של המערכות הקהילתיות בארצות הברית לשלב את המהגרים בתרבות האמריקאית.[27] היכולת להבין מדוע חלק מהקבוצות המגיעות לארצות הברית אינן מפתחות זיקה חזקה לערכים הפוליטיים שם תוכל לסייע לרשויות אכיפת החוק בארצות הברית לזהות יחידים המהווים יעד נוח במיוחד לגיוס לארגונים הג'יהאדיסטיים. ככלל, הקהילה הדיפלומטית האמריקאית, שירותי הרווחה והאקדמיה לא עשו די

27 Alexander Meleagrou-Hitchens, Seamus Hughes and Bennett Clifford, *The Travelers: American Jihadists in Syria and Iraq* (Washington DC: Program on Extremism, George Washington University, 2018).

לחקר התופעה, שהדרך הנכונה ביותר לתאר אותה היא כתהליך הגירה שבסופו המהגרים אולי חיים "במערב", אך אינם הופכים ל"מערביים".[28]

למרבה הצער, שיטות הלחימה בטרור של ממשלים מערביים הופכות למיושנות, שכן הן ממשיכות להתמקד בשלבי האינדוקטרינציה והגיוס, שהם שלבים מאוחרים מכדי להצליח במלחמה זאת. במצב זה, ההופעה הבאה של "ג'ון וג'יין הגי'האדיסטים" תתרחש לא בעקבות נסיעתם לחו"ל או יצירת קשר אישי ישיר שלהם עם קהילות קיצוניות, אלא תהיה מקומית, חסויה ובלתי צפויה. המוטיבציה הרבה ביותר להתגייסות לשורות ארגוני הג'יהאד נמצאה עד כה בקרב גורמים קיצוניים שהיו קשורים ביניהם בצורה רופפת ומרוכזים סביב קהילות מזוהות היטב בערים מערביות גדולות.[29] אולם, כפי שעולה ממאמר זה, אסטרטגיה של התמקדות בשלבים המאוחרים של האינדוקטרינציה והגיוס אינה יעילה לצורך מניעת טרור. נדרשת חדשנות באסטרטגיה של צעדי הנגד, שתשים את הדגש על שלב הסמן המקדים, תקדם את "המלחמה הקוגניטיבית הראשונה" ותגלה את המגויסים לפני גיוסם ולא לאחר שכבר גויסו, אומנו והוכשרו היטב.

מאמר זה שואף להשלים פער בולט בספרות המחקרית, שבה ניתוח ההקצנה והגיוס במרחב הווירטואלי נוטה להיות ממוקד בפתרונות שגם הם וירטואליים. בניגוד לכך, המאמר טוען שכמה מאמצעי הלחימה הטובים ביותר נגד ההקצנה הווירטואלית מצויים בתוך המוסדות החברתיים־פסיכולוגיים־תרבותיים ובתוכניות שיכולות וצריכות להתקיים ב"עולם האמיתי". שלב הסמן המקדים הוא אידיאלי לסוג ההתערבות שיכולה להביא לתוצאות מוחשיות בחייהם של המגויסים הפוטנציאליים, במקום ללכוד אותם בהבטחות וירטואליות אזוטריות. אלא שמעט מאוד מחקרים עושים כיום את הקישור הזה. אל לנו ליפול למלכודת המניחה כי בעיות וירטואליות ניתן לפתור רק על ידי פתרונות וירטואליים. לסוכנויות הרווחה ואכיפת החוק יש יתרון בתוכניות ממשיות ובתקציבים, לעומת הארגונים הקיצוניים שנמצאים אי שם ומנסים ליצור קשר דרך האינטרנט. אסור שגופים חברתיים אלה יפנו עורף לאחד התחומים המעטים שבהם יש להם מומחיות ויכולת להשפיע בצורה פעילה וישירה.

מספר חוקרים בולטים העלו כבר לפני זמן רב את סוגיית ההדרה, הניתוק והקשיים האמיתיים של המוסלמים החיים במערב.[30] מאמר זה מסתמך על חוקרים

28 Matthew Crosston, "Jihad Selfie: The Evolving Strategy of Homegrown Radical Recruitment", *Homeland Security Today,* March 14, 2018.

29 Ibid.

30 Olivier Roy, *Globalized Islam: The Search for a New Ummah* (New York: Columbia University Press, 2004); Hale Afshar, "Islam, Globalization and Postmodernity", *International Affairs* 71, no. 4 (1995): 831; Carool Kersten, "Islam, Cultural Hybridity and Cosmopolitanism: New Muslim Intellectuals on Globalization", *Journal of*

אלה לצורך יצירת הקשר בין תובנותיהם הסוציולוגיות ובין תחום הביטחון הלאומי. אך החשוב מכל הוא הניסיון שעושה המאמר לצעוד את הצעד הראשון לקראת קביעת אסטרטגיות חדשות וחדשניות ב"עולם האמיתי", שיוכלו לצמצם או למנוע את התפתחות טרור "הזאבים הבודדים". הדבר חסר כיום, ומה שמטריד עוד יותר הוא שהסיבה לכך אינה רק פער בגוף הידע, אלא מדיניות בלתי יעילה של הגנה על החברות הדמוקרטיות במערב מפני סכנות מבית. מדובר במדיניות המפסידה במערכה על "המותג" שלה ומעוררת את השאלה כיצד מהגרים, החיים בקהילות הפגיעות לגיוס על ידי גופים קיצוניים, שהחיים במערב חדשים להם ועדיין אפשר להשפיע עליהם, אינם חווים את האידיאלים, הערכים, ההזדמנויות והיתרונות שמזמנת להם הדמוקרטיה המערבית. שלב זה, שלב הסמן המקדים, שבו מחברים את הגורם החברתי־פסיכולוגי־תרבותי עם הביטחון הלאומי, הוא השלב שבו יש לפתוח בהסתערות הראשונית במסגרת "המלחמה הקוגניטיבית הראשונה". כאן טמונה ההזדמנות הטובה ביותר לניצחון.

יש להרחיב את האזהרה המקורית של גבי סיבוני, לפיה על מדינת ישראל לשפר את מוכנותה והיערכותה לכל היבטי "המלחמה הקוגניטיבית הראשונה", ולדבר הן על מדינות נוספות שצריכות להיערך למלחמה זאת והן על האסטרטגיות שקהילות המודיעין והממשלים השונים צריכים ליישם. חדשנות בעולם של סיכול טרור אינה משימה קלה, במיוחד כאשר מדובר בהשקעה ב"סיווג חיובי", כפי שגורס מאמר זה, וכן בגילוי מעורבות יזומה בקהילות מסוימות, בהימנעות מאיומים ובהשקעה בהצלחה הקבוצתית של אותה אוכלוסייה. יתרון נוסף של גישת החדשנות טמון בכך שהיא אינה מציבה בפני חברות פרטיות ומסחריות תביעות שעשויות לפגוע בחירויות הווירטואליות או להגביל את הגישה לאינטרנט; במקום זאת, היא דורשת שהסוכנויות הממשלתיות הרשמיות יגלו תחכום ושכלול בפעילותן במרחב הווירטואלי, לפחות כמו הארגונים הקיצוניים, ויהיו פעילות ביצירת קשרים עם גורמים בעלי פוטנציאל לגיוס, בדיוק כפי שעושים זאת "הרָעים". יהיו מי שינסו לטעון שמדובר בתַגמול טרוריסטים פוטנציאליים או בשיחוד גורמים קיצוניים לשנות את דרכם. הנקודה החשובה שיש לזכור לקראת התמודדות עם תגובות בלתי נמנעות אלו היא שההצעות שמעלה מאמר זה הן בעלות הפוטנציאל הרב ביותר להצליח ולהשפיע על מניעת גיוסם של המגויסים הפוטנציאליים לארגוני הג'יהאד.

זאת ועוד, לאסטרטגיות חדשות שיתמקדו בשלב הסמן המקדים יש גם תועלת חיובית משנית, והיא יצירת קשר מעמיק יותר עם קהילות מהגרים, שבאופן מסורתי היו איטיות יחסית לאמץ את העקרונות המערביים ונטו להישאר מבודדות מבחינה

International and Global Studies 1, no. 1 (2009): 89-113; Akbar Ahmed, *Journey into Islam: The Crisis of Globalization* (Washington DC: Brookings Institution Press, 2007); Ali Mohammad, *Islam Encountering Globalisation* (London: Routledge, 2012).

חברתית ומנותקות מהרעיונות של חירות אזרחית. פעילות פרו־אקטיבית לחיסול "הבלקניזציה החברתית", על ידי השקעה של המדינה המארחת בהצלחתן של הקהילות הפגיעות לגיוס, אינה צריכה להיחשב לפעילות סעד ולהענקת שירותי רווחה. מדובר באסטרטגיה מקומית שמטרתה היא לנצח ב"מלחמה הקוגניטיבית הראשונה".

"ארגז הכלים" של האיחוד האירופי כחלק מדיפלומטיית הסייבר

אָנֶגְרֶט בֶּנדְיֶיק

בספטמבר 2017 עדכן האיחוד האירופי את אסטרטגיית ביטחון הסייבר שלו משנת 2013. הגרסה החדשה נועדה לשפר את ההגנה על התשתיות הקריטיות של אירופה ולהעצים את האסרטיביות הדיגיטלית של האיחוד מול אזורים אחרים בעולם. כדי למנוע מצבים שבהם עימותים במרחב הסייבר ייצאו מכלל שליטה, גיבש האיחוד האירופי באוקטובר 2017 את מה שכונה "ארגז כלים לדיפלומטיית סייבר", המגדיר מהם אמצעי הנגד האפשריים שיגבו מחיר מהתוקפים במקרה של מתקפת סייבר חיצונית. מסגרת הפעולה המתוכננת כוללת זימון דיפלומטים וסנקציות מדיניות, כלכליות ופליליות נוספות, לצד תגובות דיגיטליות. עם זאת, הבעיה הבסיסית – ייחוס המתקפה – קיימת גם בעולם של דיפלומטיית הסייבר. בנוסף לכך, השימוש ב"ארגז הכלים" אינו נתון להחלטה וולונטרית, אלא תלוי בתמיכתן פה אחד של כל המדינות החברות באיחוד. כל אלה מצטברים לכדי מכשולים המקשים על יצירת הרתעה הגנתית יעילה בסייבר.

מילות מפתח: סייבר, האיחוד האירופי, אסטרטגיה, הרתעה

מבוא

מאז שנודע דבר מתקפות הסייבר נגד רשתות מחשבים ומשרדי ביטחון והגנה של ממשלות אירופיות, מתעקשים קובעי מדיניות הביטחון שעל המדינות החברות באיחוד האירופי לפתח יכולות הגנת סייבר ותגובות סייבר הולמות יותר. האיחוד ממשיך, עם זאת, לדגול באסטרטגיית ביטחון סייבר שתתבסס על חוסנן של תשתיות טכנולוגיית המידע והתקשורת ועל דיפלומטיית סייבר. זאת, כחלק ממדיניות

ד"ר אנגרט בנדייק היא סגנית ראש החטיבה לאירופה במכון הגרמני לענייני ביטחון ועניינים בין־לאומיים בברלין.

החוץ והביטחון המשותפת שלו ומשאיפתו למצב את עצמו ככוח החותר לשלום. באוקטובר 2017 אימץ האיחוד את תוכנית "התגובה הדיפלומטית המשותפת של האיחוד האירופי לפעילות סייבר זדונית", המתמקדת בכלים לא צבאיים שמטרתם לתרום ל"צמצום האיומים בתחום ביטחון הסייבר, מניעת עימותים והגברת היציבות ביחסים הבין־לאומיים".[1] התרחבות רשת התשתיות הביאה את האיחוד האירופי לדבוק במדיניות של דיפלומטיית סייבר צעד אחר צעד, המבוססת על העיקרון של בדיקת נאותות (Due diligence).

מתקפות סייבר (דוגמת זו ששוגרה נגד תשתיות המידע והתקשורת של הממשלה הפדרלית הגרמנית[2]), ריגול סייבר, גניבת קניין רוחני, פשעי סייבר או הפצת מידע כוזב, לא רק משתקים את התקשורת ופוגעים בביטחון הסייבר, אלא גם יכולים להיות חלק מלוחמה היברידית. "היברידי" בהקשר זה פירושו שימוש מכוון, סמוי או גלוי, שעושים שחקנים מדינתיים ולא מדינתיים באמצעים אזרחיים וצבאיים במשולב. אמצעים אלה כוללים, לצד מתקפות סייבר, קמפיינים של דיסאינפורמציה, ריגול, לחץ כלכלי, שימוש ב"שליחים" (proxy) ופעילויות חתרניות אחרות. השימוש בגז עצבים שנעשה בלונדון הביאה את ראשי הממשלות וראשי המדינות של האיחוד האירופי להכריז, בסוף מארס 2018, על עמידה חד־משמעית לצד בריטניה, תוך איום על רוסיה שתישא באחריות. במסגרת זו נשקלו סנקציות נוספות, כמו גם פעולת תגמול בסייבר (hackback).[3]

הן האיחוד האירופי והן נאט"ו מיקדו את האסטרטגיות שלהם באירופה בהרתעה מבוססת חוסן, אם כי כל ארגון פנה לתחומים אסטרטגיים שונים. חלק ממעצמות הסייבר החלו לבנות את יכולות הסייבר ההתקפיות וההגנתיות שלהן, בעוד שהאיחוד האירופי ונאט"ו דוחפים את המדינות החברות לבנות יכולת הגנה משותפת. עם זאת, רק מספר קטן של מדינות באיחוד האירופי ובנאט"ו, וביניהן בריטניה, צרפת, אסטוניה והולנד, הן בעלות יכולות טכניות ותשתית משפטית להציב יכולות סייבר התקפיות.

1 "Draft Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities", 13007/17 LIMITE, *Council of the European Union*, Brussels, October 9, 2017, p. 2.

2 Thorsten Severin and Andrea Shalal, "German Government under Cyber Attack Shores up Defenses", *Reuters*, March 1, 2018.

3 "Conclusions on the Salisbury Attack", *European Council*, March 22, 2018, http://www.consilium.europa.eu/en/press/press-releases/2018/03/22/european-council-conclusions-on-the-salisbury-attack/pdf.

הגנת סייבר: מגננה או מתקפה?

השאלה אם על מדינות מותקפות לנקוט אמצעי נגד התקפיים, דוגמת פעולת תגמול בסייבר, כדי לנטרל את מקור מתקפת הסייבר, היא נושא פוליטי ושנוי במחלוקת. אסטרטגיית אבטחת הסייבר של גרמניה מ־2016[4] קוראת לביטחון סייבר הגנתי ולהקמת כוח תגובה מהירה נייד במסגרת המשרד הפדרלי לביטחון המידע (BSI), וכן להקמת צוותים דומים בתוך המשטרה הפדרלית ובסוכנות מודיעין הפנים, שיהיו מסוגלים להגיב לאיומי סייבר על מוסדות ממשלתיים ותשתיות קריטיות. ממשלת הקואליציה החדשה בגרמניה אימצה את העמדה שלפיה גרמניה זקוקה לאמצעי סייבר צבאיים ואסטרטגיים, וכן לבסיס משפטי לפריסתם, כדי להגיב על התקפות סייבר, כמו אלו שהיו על הפרלמנט הפדרלי בשנת 2015 או על רשת התקשורת הממשלתית בשנת 2018.[5]

נאט"ו רואה במתקפות המתרחשות במרחב הסייבר צורה של לוחמה, המצדיקה את הפעלת פסקת ההגנה ההדדית של סעיף 5 באמנה הצפון אטלנטית. נאט"ו דן בימים אלה בשאלה האם התכנון המבצעי של הארגון צריך לכלול מרכיב של פעולות התקפיות ברשתות מחשבים מצד המדינות החברות. מאז פסגת נאט"ו בוורשה ב־2016, התחזק שיתוף הפעולה בין הארגון ובין האיחוד האירופי, והוא כולל חילופי מידע ותרגילי ביטחון סייבר משותפים.

נייר עמדה של משרד ההגנה הגרמני משנת 2016, העוסק במדיניות הביטחון הגרמנית ובעתיד הבונדסוור, מצביע על הקמת יחידה ארגונית שישית במספר בצבא גרמניה – יחידת מרחב הסייבר והמידע – המונה כיום כ־13,500 איש.[6] הקמת היחידה תאפשר שימוש ביכולות סייבר הגנתיות והתקפיות גם יחד, במקרה של צורך בהגנה עצמית או בהגנה הדדית במסגרת נאט"ו. השאלה אם יכולות התקפיות נכונות גם לזמן שלום עדיין שנויה במחלוקת. המבקרים טוענים כי התפשטות של תוכנות זדוניות לכדי מתקפת סייבר אינה מצדיקה את היתרונות ההרתעתיים קצרי הטווח שיכולות התקפיות אלו מציעות. הם עומדים על כך שנושאים הנוגעים לבניית אמון, לאמצעים להגברת הביטחון ולבקרת נשק צריכים להיות מטופלים על ידי האו"ם ו"הארגון לביטחון ושיתוף פעולה באירופה" (OSCE), וכי כל פיתוח של יכולות ביטחון סייבר התקפיות יוצר סיכון של הגברת חוסר האמון, חוסר ביטחון הדדי וסיכוי לעימותים. לשיטתם, רק דיפלומטיית סייבר ארוכת טווח,

4 "Building and Community, German National Cyber Security Strategy", *Federal Ministry of the Interior*, 2016, http://www.bmi.bund.de/cybersicherheitsstrategie/.

5 Melissa Eddy, "Germany Says Hackers Infiltrated Main Government Network", *The New York Times*, March 1, 2018.

6 "White Paper on German Security Policy and the Future of the Bundeswehr", *The German Federal Government*, 2016, https://bit.ly/2zXvJuE.

המתואמת ברמת האיחוד האירופי, תוכל לסייע בהשגת ביטחון לאירופה ולמנוע הסלמת סכסוכים.[7] אין ספק שלאיחוד האירופי יש אינטרס למצב את עצמו כמכתיב הנורמות בתחום ביטחון הסייבר באירופה ולהדגיש את חשיבותם של צעדים בוני אמון וביטחון בדיפלומטיית הסייבר הבין־לאומית.

סוגים שונים של דיפלומטיית סייבר

דיפלומטיית סייבר, בניגוד להגנת סייבר כוללת, מציעה אפשרות למנוע הסלמה של עימותים, ובכך היא מחזקת את הסיכוי לשלום. נציבים המופקדים על מדיניות חוץ בתחום הסייבר פועלים כיום ביותר משלושים מדינות. דנמרק אף מינתה שגריר לדיפלומטיית סייבר. דיפלומטיית סייבר במובנה הרחב ביותר כוללת אמצעי בניית אמון, וכן היבטים מסוימים של בניית נורמות בין־לאומיות, הגנה על נתונים, חופש ביטוי, ממשל באינטרנט והעמדה לדין, מכוח הסכמים בין־לאומיים, בגין אי־מתן סיוע משפטי הדדי. עם זאת, לממשלות רבות אין את הידע או את המשאבים הדרושים כדי לשמור על סטנדרטים בסיסיים של ביטחון סייבר, או אפילו כדי לזהות מתקפה המתבצעת דרך שרתים הנמצאים בשטחן. למרות זאת, רוב המדינות מביעות הסתייגות רבה מהרעיון להקים גוף רגולטורי מרכזי וכולל לאבטחת מרחב הסייבר מחשש לריבונותן הלאומית, ולכן מסמנות אותו כדבר בלתי מציאותי בשלב זה. סביר יותר להניח שמרחב הסייבר ומרחב המידע יוכפפו בהדרגה לריבונות הלאומית.[8] כך או כך, הרגולציה הממשלתית תפגר תמיד אחרי ההתפתחות הטכנולוגית של המגזר הפרטי. שותפויות ציבוריות־פרטיות מסתמנות, אפוא, כצורת הפיקוח הבולטת ביותר בתחום ביטחון הסייבר.

במישור המולטילטרלי, קבוצה של 25 מומחי ממשל בין־לאומיים, שכונסה על ידי העצרת הכללית של האו"ם בשנת 2015, הגיעה להסכמה כי יש ליישם את המשפט הבין־לאומי, לרבות את הזכות להגנה עצמית, גם על מרחב הסייבר.[9] עם זאת, הקבוצה לא הצליחה להגיע בקיץ 2017 להסכמה אם להקים מעין "מועצת ייחוס" (attribution council). תנאי מוקדם לקביעת ייחוס (שהוא הזיהוי הטכני, המשפטי והפוליטי של מבַצע מתקפת הסייבר) הוא יצירת שיתוף במידע רגיש בין

7 André Barrinha and Thomas Renard, "Cyber-Diplomacy: The Making of an International Society in the Digital Age", *Global Affairs* 3, no. 4-5 (2017): 353-364; André Barrinha, "Virtual Neighbors: Russia and the EU in Cyberspace", *Insight Turkey* 20, no. 3 (2018): 29-41.

8 Milton Mueller, *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace*, (Polity, Cambridge, UK, Malden, MA., 2017).

9 "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", *United Nations General Assembly*, A/70/174, July 22, 2015, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

צוותי CERT (צוותי תגובה לאירועי חירום במחשבים) ובין השירותים החשאיים וסוכנויות הביטחון.

המסגרות המולטילטרליות הבלתי יעילות הביאו לכך שהנשיאים שִי ג'ינפינג וולדימיר פוטין חתמו ב־2016 על הצהרה בילטרלית משותפת בשנחאי, שהכריזה על שלב חדש בשותפות האסטרטגית הכוללת בין סין ובין רוסיה. בייג'ין ומוסקבה הביעו דאגה מהשימוש לרעה שנעשה בטכנולוגיות מידע ותקשורת לצורך התערבות בעניינים פנימיים של מדינות, וקראו לקהילה הבין־לאומית לשתף פעולה על בסיס של כבוד ותועלת הדדיים ושיקולי צדק, ולספק מענה משותף לאיומים על אבטחת המידע.[10] ארצות הברית מסתמכת גם היא על הסכמים בילטרליים כדי להילחם בפשעי סייבר, כמו ההסכם בעניין זה שחתמה עם סין.[11]

מאז כישלון השיחות המולטילטרליות שנערכו בחסות האו"ם ב־2017, קוראים מומחי ביטחון סייבר להקמת "קואליציה של המוכנים" מקרב מדינות ה־G20 או ה־G7, כדי לקדם גיבוש של נורמות בין־לאומיות בתחום הסייבר. מסגרות דו־מסלוליות כמו "הנציבות העולמית ליציבות מרחב הסייבר", הן המובילות כיום בתחום זה.

חיזוק יכולת הייחוס נוגע לא רק למדינות, אלא גם למגזר הפרטי. בפברואר 2017 קראה חברת "מייקרוסופט" לכינון "אמנת ז'נבה הדיגיטלית",[12] והיוזמה האחרונה בנושא זה היא "אמנת האֶמון" שהשיקה חברת "סימנס" בכנס האבטחה במינכן בפברואר 2018,[13] העוסקת ברעיונות דומים. הפורום הכלכלי העולמי מבקש להקים "מרכז עולמי לביטחון הסייבר" כדי להיאבק בפשיעה בסייבר, וחותר גם הוא לשיפור שיתוף הפעולה בין המגזר הפרטי ובין רשויות המדינה, במה שמכונה "שותפויות ציבוריות־פרטיות".

10 "China, Russia Sign Joint Statement on Strengthening Global Strategic Stability", *Xinhuanet*, June 26, 2016, http://www.xinhuanet.com/english/2016-06/26/c_135466187.htm.

11 Adam Greer and Nathan Montierth, "How Are US-China Cyber Relations Progressing?", *The Diplomat*, November 1, 2017, https://thediplomat.com/2017/11/how-are-us-china-cyber-relations-progressing/.

12 Brad Smith, "The Need for a Digital Geneva Convention", *Microsoft*, February 14, 2014, https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.

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

מדיניות ביטחון הסייבר ומדיניות החוץ בסייבר של האיחוד האירופי

ביטחון סייבר הוא בעיה לא רק עבור מדינות, אלא גם עבור האיחוד האירופי כארגון. הבעיה חורגת מעֵבר לשאלה של חוסן הרשתות, של השוק הדיגיטלי או של העמדה לדין של פושעי סייבר, ונוגעת גם למדיניות החוץ והביטחון המשותפת של האיחוד האירופי ולמדיניות ההגנה והביטחון המשותפת שלו (ראו טבלה 1 להלן). שורה של גורמים כבר מתמודדים עם סוגיות מדיניות החוץ וביטחון הסייבר של האיחוד האירופי: "התגובה המשולבת למשברים פוליטיים" (IPCR) של האיחוד, ובעיקר "הסוכנות האירופית לאבטחת רשתות ומידע" (ENISA), "המרכז האירופי לפשעי סייבר" (EC3) ביורופול, "מרכז המודיעין וחדר המצב של האיחוד האירופי" (INTCEN), "מינהלת המודיעין של הצוות הצבאי של האיחוד האירופי" (EUMS INT) וחדר המצב שלה (EU SITROOM), יחידת INTCEN של האיחוד לניתוח איומים היברידיים (הידועה בשם Hybrid Fusion Cell), "צוות התגובה לאירועי חירום במחשבים של מוסדות וסוכנויות האיחוד האירופי" (CERT-EU), וכן "מרכז תיאום המענה בחירום של הנציבות האירופית" (ERCC). יש לציין גם גופים ומנגנונים חדשים שהוקמו על פי "ההנחיה לביטחון רשתות ומידע" (NIS), כגון "רשת צוותי IT בחירום של המדינות החברות" (CSIRT).

טבלה 1. ביטחון סייבר באיחוד האירופי: תחומי אחריות

CFSP: דיפלומטיית סייבר	**CSDP: הגנת סייבר**	**שוק אחיד**	**חופש, ביטחון, משפט**	
EEAS SIAC (EU INTCEN, EUMS INT) EU SITROOM EU Hybrid Fusion Cell ERCC	EDA GSA	ENISA רשת CSIRT CERT-EU	יורופול (EC3) Eurojust EU-LISA	האיחוד האירופי
משרדי חוץ	גופי הגנה, צבא וביטחון	רשויות המופקדות על NIS, צוותי CSIRT לאומיים	רשויות ניהול והגנה על נתונים	**רמת המדינה**

קיצורים: EDA: "סוכנות ההגנה האירופית"; EEAS: "שירות פעילות החוץ האירופית"; EU-LISA: "הסוכנות האירופית לניהול מערכות IT רחבות היקף בתחום החופש, הביטחון והמשפט"; GSA: "הסוכנות האירופית למערכות ניווט לווייני גלובליות"; SIAC: יכולת יחידנית לניתוח מודיעין.

האיחוד האירופי הקים בשנת 2015 את "קבוצת העבודה האופקית לנושאי סייבר", במטרה לתאם את ההיבטים הפוליטיים של מרחב הסייבר. הקבוצה נוטלת חלק הן בפעילויות חקיקה והן בפעילויות שאינן קשורות לחקיקה. יתרה מכך, המדינות החברות החליטו בפברואר 2015 לחזק את דיפלומטיית הסייבר ברמת האיחוד כחלק ממדיניות החוץ שלו. המהלך אושר בנובמבר 2016 במסגרת "התוכנית ליישום ביטחון והגנה".[14] גופים מרכזיים המתאמים את הניתוח האסטרטגי עבור מדיניות החוץ והביטחון המשותפת הם: צוות דיפלומטיית הסייבר ב"שירות פעילות החוץ האירופית"; יחידת INTCEN, המופקדת על המודִיעִין למצב בפן האזרחי; "מינהלת המודיעין של הצוות הצבאי של האיחוד האירופי", העושה זאת בפן הצבאי. כדי להרתיע מפני מתקפות סייבר ולהשתקם בעקבותיהן, וכדי לזהות את העבריינים, תלויים מומחי מחשב פורנזיים במקורות רבים הפועלים בכל הרמות הפוליטיות במדינות ובארגונים השונים. האיחוד האירופי מסתמך על שיתוף הפעולה הטוב השורר בין משרדי הממשלה ובין גופי הביטחון כדי ליצור תיאום בתחום זה.

חוקים מיוחדים חלים על המאבק בטרור. עם זאת, טרם גובשה מדיניות מתואמת של האיחוד האירופי, המחברת בין החובה להחליף מידע ובין המעקב והשימוש במידע משותף זה, שתהיה מגובה בהסכמים, אם כי מדיניות כזו נמצאת בבחינה מחודשת. ההגנה על השוק הדיגיטלי הפנימי במדינות האיחוד מצדיקה את הגברַת היכולות של הנציבות האירופית בעניין זה. הנציב לביטחון של האיחוד, ג'וליאן קינג, מופקד על נושא זה וכבר השיק חבילת חקיקה מרחיקת לכת לחיזוק החוסן הפנימי.

נייר עמדה משותף של האיחוד האירופי, מספטמבר 2017, שכותרתו "חוסן, הרתעה והגנה: בניית ביטחון סייבר חזק עבור האיחוד האירופי", מציע נקודות מוצא לשיתופי פעולה בבניית אמון וביטחון. אלו מתבססות על ארבעת יסודות ביטחון הסייבר של האיחוד האירופי.[15] "קבוצת העבודה האופקית לסוגיות הסייבר", שהיושב ראש שלה מתחלף ברוטציה, וכן "הוועדה לביטחון ופוליטיקה" (PSC), אחראיות על אמצעי יישום הולמים. יש לזכור כי מבחינה משפטית, המדינות החברות באיחוד האירופי חופשיות להשיק יוזמות משלהן.

14 "Implementation Plan on Security and Defence, Factsheet", *European External Action Service*, 2016, https://eeas.europa.eu/headquarters/headquarters-homepage/34215/implementation-plan-security-and-defence-factsheet_en.

15 "Resilience, Deterrence and Defence: Building Strong Cybersecurity in Europe", *European Commission*, 2017, https://ec.europa.eu/digital-single-market/en/news/resilience-deterrence-and-defence-building-strong-cybersecurity-europe.

ארבעת יסודות ביטחון הסייבר של האיחוד האירופי הם:

- **היסוד הראשון**: ההנחיה בנושא מתקפות על מערכות מידע, משנת 2013,[16] לרבות הקנסות בגין מתקפות כאלו. הנחיה זו חלה על מקרים של שחקנים פליליים שאין להם קשר משמעותי עם מדינה נותנת חסות. כדי להתמודד עם האיום ההולך וגובר של פשעי סייבר חוצי גבולות, מתוכננים כלים חדשים, שניתן יהיה להפעילם לצורך העמדה לדין בצורה יעילה יותר. ההנחיה לגבי "ר•יות אלקטרוניות" ("e-evidence") נמצאת בשלב זה בדיונים, כשהמטרה היא לאפשר נגישות חוצה גבולות לראיות כאלו.[17] הנחיה נוספת שנמצאת בדיון עוסקת במאבק בהונאה ובזיוף בסביבה נעדרת מזומנים, דוגמת מטבע ה"ביטקוין". המטרה במקרה זה היא לשפר את שיתוף הפעולה בין הרשויות השונות של המשפט הפלילי.
- **היסוד השני**: שדרוג "הסוכנות האירופית לאבטחת רשתות ומידע" על ידי הגדלת צוות העובדים משמונים ל־125 איש והגדלת התקציב השנתי מ־11 ל־23 מיליון אירו. הסוכנות אמורה לארגן תרגילי ביטחון סייבר שנתיים כלל־אירופיים ולעודד שיתופי פעולה בין צוותי IT בחירום של המדינות החברות (CSIRT). בעבר הורחבו תרגילים אלה מדי פעם גם לבעלות ברית שאינן חברות. "הסוכנות האירופית לאבטחת רשתות ומידע" נועדה בעיקר ללוות את הקמתה ויישומה של מסגרת הסמכה כלל־אירופית. המטרה היא להפוך מוצרים ושירותים של טכנולוגיות מידע למאובטחים יותר באמצעות מתן תמריצים לשוק, ולאפשר למשתמשים לקבל החלטות מושכלות בבואם לרכוש מוצרים ושירותים כאלה. מערכות הסמכה שונות יעברו האחדה כדי לחזק את השוק הדיגיטלי האחיד למוצרים אמינים. צעדים אלה מבוססים על "ההנחיה לביטחון רשתות ומידע",[18] שאמורה הייתה להיכנס לתוקפה במאי 2018 ולשמש כאמת מידה להשגת שיפורים דומים גם ב"ארגון לביטחון ושיתוף פעולה באירופה"(OSCE).

16 "Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on Attacks against Information Systems and Replacing Council Framework Decision", *European Parliament*, 2005/222/JHA, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF.

17 "E-evidence – Cross-Border Access to Electronic Evidence", *European Commission*, https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en.

18 "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union", *European Parliament*, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN.

- **היסוד השלישי**: "שיתוף הפעולה המובנה והקבוע" (PESCO) שהוקם בדצמבר 2017 על ידי 25 שרי ההגנה של האיחוד האירופי.[19] נכון לנובמבר 2018, שבעה מתוך 34 פרויקטים של הגוף החדש מיועדים ספציפית לביטחון סייבר באירופה. על פי הדיווחים, פרויקטים אחרים שלו עוסקים בסטנדרטיזציה של מערכות לחיילים – ציוד אלקטרוני, תקשורת שפה ונתונים ותוכנה. יוון מתכננת לפתח צוות חירום אירופי לענייני טכנולוגיות מידע, וליטא מבקשת להיות אחראית על הקמת מערכת הגנת סייבר אירופית. הרעיון הוא ליצור מעֵין "אזור שנגן בסייבר", שיילחם בפשיעה באינטרנט ויפעל באופן שיחצה את הגבולות הלאומיים. הבנק האירופי להשקעות מתכוון להשקיע עד סוף 2020 יותר משישה מיליארד אירו בפיתוח מה שמכונה "טכנולוגיות כפולות שימוש", שנועדות לביטחון סייבר צבאי ואזרחי.
- **היסוד הרביעי**: ניהול דיאלוגים בילטרליים בנושא הסייבר בין האיחוד האירופי ובין גורמים חיצוניים, במסגרת הסכמי השותפות האסטרטגית שלו עם ארצות הברית, קנדה, סין, דרום קוריאה ומדינות נוספות. האיחוד גם מציע לנסח אסטרטגיה לשיתוף פעולה בין־לאומי במרחב הסייבר ולמניעת עימותים, באופן שיהיה תואם את רפורמת ביטחון הסייבר של ספטמבר 2017. כצעד ראשון, עדכן האיחוד את אמצעי דיפלומטיית הסייבר ושל הגנת הסייבר שלו, וכן את הנחיותיו בעניין הפיקוח על ייצוא סחורות בעלות שימוש כפול.

תגובה דיפלומטית משותפת לפעילות סייבר זדונית

העלייה במספר מתקפות הסייבר אילצה את השחקנים הבין־לאומיים השונים לשקול כיצד להגיב עליהן כראוי. ממשל אובמה הטיל ב־2014, לראשונה, סנקציות חד־צדדיות על צפון קוריאה, לאחר שחברה בת אמריקאית של תאגיד "סוני" נפלה קורבן למתקפת סייבר קטלנית, שבמהלכה הועתקו כל המידע והנתונים שלה.[20] שנתיים לאחר מכן חזרה ארצות הברית להטיל סנקציות לאחר שנתוני כוח האדם של הממשל האמריקאי "נשאבו", כחלק ממתקפת סייבר רחבת היקף. בעקבות ההתערבות הרוסית לכאורה במסע הבחירות לנשיאות ארצות הברית ב־2016,

19 "Permanent Structured Cooperation (PESCO) – Factsheet", *European External Action Service*, 2018, https://eeas.europa.eu/headquarters/headquarters-Homepage/34226/permanent-structured-cooperation-pesco-factsheet_en.

20 David E. Sanger and Michael S. Schmidt, "More Sanctions on North Korea after Sony Case", *The New York Times*, January 2, 2015, https://www.nytimes.com/2015/01/03/us/in-response-to-sony-attack-us-levies-sanctions-on-10-north-koreans.html.

הטיל הממשל האמריקאי, במארס 2018, סנקציות על חמישה ארגונים וחברות ו־19 חשודים, בנימוק של "פעולות סייבר זדוניות" מצידה של רוסיה.[21]

האיחוד האירופי דן לראשונה בפברואר 2015 בצורך בדיפלומטיית סייבר משותפת. ביוני 2017 הציע האיחוד לבנות "ארגז כלים לדיפלומטיית סייבר", כדי לספק מענה דיפלומטי משותף לפעולות סייבר זדוניות.[22] מטרתו העיקרית של "ארגז הכלים" הייתה להבטיח יכולת תגובה למדיניות החוץ והביטחון של האיחוד, שתהיה מתחת לסף של עימות מזוין. יכולת כזו נועדה להשלים את צעדי האיחוד מכוח "ההנחיה לביטחון הרשתות והמידע", על ידי דרישה לתקינת סף וחובת דיווח, וכן לבניית מערכות של טכנולוגיות מידע ותקשורת עמידות עבור "השוק הדיגיטלי האחיד". דיפלומטיית סייבר כזו ברמת האיחוד האירופי תאפשר להפעיל אמצעים פוליטיים, לרבות אמצעים מגבילים, במסגרת מדיניות החוץ והביטחון המשותפת, כתגובה על מתקפות סייבר.

באוקטובר 2017 אומץ "ארגז הכלים" המתוכנן לדיפלומטיית הסייבר תחת השם החדש: "טיוטה לקווים מנחים למסגרת לתגובה דיפלומטית משותפת של האיחוד האירופי נגד פעולות סייבר זדוניות". "הארגז" נועד לסייע למדינות האיחוד לשתף פעולה בבלימת איומים מיידיים וארוכי טווח ולהרתיע עבריינים ותוקפים פוטנציאליים בטווח הארוך. נראה שלכל אחת ממדינות האיחוד בנפרד לא הייתה יכולת מספקת להשפיע על חישובי עלות־תועלת של התוקפים; לעומת זאת, דיפלומטיית הסייבר של האיחוד האירופי הציעה ערך מוסף אסטרטגי, בשל יכולתה להטיל סנקציות, או לחילופין להציע תמריצים חיוביים.

האיחוד האירופי התחייב לפעול על פי העקרונות הבין־לאומיים, תוך שמירה על בדיקת נאותות במרחב הסייבר. בכוונתו גם לחזק את דיפלומטיית הסייבר שלו על ידי חילופי מידע עם צדדים שלישיים, כחלק מהמאבק במתקפות סייבר. צוות מומחי הממשל של האו"ם אימץ גם הוא את עקרון בדיקת הנאותות בדוח הסופי שלו, אותו הגיש ביוני 2015.[23] על פי דוח זה, מדינות אחראיות לוודא כי שטחן הריבוני ומערכות המחשוב והתשתית הממוקמות בו, או נמצאות בשליטת

21 "Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks", *US Department of the Treasury*, March 15, 2018, https://home.treasury.gov/news/press-releases/sm0312.

22 "Draft Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (Cyber Diplomacy Toolbox) 9916/17", *European Council*, June 7, 2017, http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf.

23 "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", *United Nations*, July 22, 2015, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

אותן מדינות בצורה אחרת כלשהי, אינם מנוצלים למתקפות על תשתיות של מדינות אחרות.

חמשת האמצעים של "ארגז הכלים"

האיחוד האירופי מסתמך בדיפלומטיית הסייבר שלו על "ארגז הכלים" של מדיניות החוץ והביטחון המשותפת. ניתן לחלק את כלי העבודה של "הארגז" לחמש קטגוריות: אמצעים מניעתיים; אמצעים שיתופיים; אמצעים מייצבים; אמצעים מגבילים; אמצעים לתגובות של הגנה עצמית מכוח החוק של כל אחת מהמדינות החברות. את האמצעים המדיניים קובעת מועצת האיחוד האירופי, בסיוע "שירות פעילות החוץ האירופית". במקרים חמורים, פעילויות סייבר זדוניות יכולות להביא לנקיטת אמצעי ענישה ולשימוש בכוח או אף בהתקפה חמושה, בהתאם לחוק הבין־לאומי ולמגילת האומות המאוחדות. במקרים כאלה, המדינה החברה מקבלת החלטה ריבונית להפעיל הגנה עצמית עצמאית, או קולקטיבית מכוח סעיף 51 של מגילת האו"ם, ובהתאם לדין הבין־לאומי וההומניטרי.

אמצעים מניעתיים

האיחוד האירופי מנהל דו־שיח בנושא הסייבר במסגרת דיאלוגים מדיניים עם מדינות שלישיות, שמטרתם להשפיע על ההתנהגות ועל העמדה של שותפיו לשיח. האיחוד גם תומך בצעדים בוני אמון, כמו אלה שפותחו על ידי "הארגון לביטחון ושיתוף פעולה באירופה". דיאלוגים עם ארגונים אזוריים, כגון האיחוד האפריקאי או ASEAN (איחוד מדינות דרום־מזרח אסיה), חשובים במיוחד. בדרך זו יכולים האיחוד האירופי והגוף האזורי שניצב מולו להגדיר כיצד ניתן לשכלל את יכולות האזור להשתמש במרחב הסייבר (המכונות "בניית יכולת סייבר"). זאת, באמצעות הסכמי התאגדות (אסוציאציה), הסכמי שותפות וכן שיתופי פעולה, או באמצעות "המכשיר ליציבות ולשלום" (IcSP).

אמצעים שיתופיים

כדי להקל על הטיפול בתקרית מתמשכת, המשלחת של האיחוד האירופי במדינה המארחת יכולה להעביר איגרת דיפלומטית (Demarche) לממשלה של אותה מדינה. מהלך כזה מחייב הוראה מהנציב העליון של האיחוד לענייני מדיניות חוץ וביטחון. במצב של עימות, ראש משלחת האיחוד יכול להעביר הצעה לערוך שיחות מקיפות, או להסתפק בהעברת מסרים בנושאי מפתח. האיגרת הדיפלומטית יכולה להתנסח ולהישלח גם בעזרת מדינה שלישית. סוג כזה של פתרון אינו אפשרי במקרים שבהם ראש המשלחת של האיחוד האירופי נקרא לחזור לארצו בשל מצב של עימות.

אמצעים מייצבים

אמצעים מסוג זה ממלאים תפקיד של מסר, בהיותם איתות אסטרטגי לתוקף הפוטנציאלי שעליו להימנע מלעסוק בפעילות סייבר זדונית. מועצת אירופה יכולה לקבוע פעולה או עמדה של האיחוד האירופי, אולם רק אם אלו התקבלו פה אחד. היא גם יכולה להעביר החלטה לממש פעולה כזו. במקרה כזה תידרש הצבעה ברוב קולות, למעֵט כשמדובר בפעולות הנוגעות לצבא או להגנה (סעיף 31, פסקה 2 באמנת האיחוד האירופי). הנציב העליון של האיחוד לענייני מדיניות חוץ וביטחון יכול גם למסור הצהרה "בשם האיחוד האירופי", אם כי תידרש לכך הסכמה מראש של כל מדינות האיחוד. הסכמה כזו תתקבל בדרך כלל, אלא אם יש צורך בתגובה מיידית, או אם האיחוד האירופי צריך תחילה לגבש את עמדתו לנוכח מצב חדש, או אם שונתה עמדה קיימת. במקרים שנדרשת תגובה מהירה, אך לא ניתן להגיע להסכמה בקרב 27 המדינות החברות, הנציב העליון יכול לפרסם את ההצהרה על אחריותו האישית.

סנקציות

האיחוד האירופי רשאי להטיל אמצעים מגבילים (סנקציות) בניסיון לקדם מטרות מדיניות בעקבות מתקפות סייבר חמורות. צעדים כאלה יהיו, בדרך כלל, מכוונים כלפי גורמים רשמיים של מדינות שלישיות, אך גם כלפי חברות ממשלתיות, ישויות משפטיות או אישיות טבעית אחרת. על מועצת אירופה להצביע פה אחד על הטלת הסנקציות, והן יהיו חייבות לעלות בקנה אחד עם מטרות מדיניות החוץ והביטחון המשותפת, לפי סעיף 24 של אמנת האיחוד האירופי.

ניתן לחלק את הסנקציות לשתי קטגוריות עיקריות: כאלו שנקבעות באופן עצמאי על ידי האיחוד האירופי, וכאלו שהאיחוד האירופי מחויב להטיל בעקבות החלטה של מועצת הביטחון של האו"ם. על פי חוקי האיחוד, סנקציות חייבות להיות ממוקדות. לדוגמה, ניתן להכניס חברות או אנשים מסוימים לרשימת הסנקציות כדי לחסום חשבונות בנק שלהם, כל עוד נשמרים כללי סף שקובע החוק. תנאים מוקדמים נוסחו כדי לשמור על החוקיות של מקרים כאלה, למשל, הקביעה כי המיועדים לסנקציות צריכים לקבל הסבר על הסיבות להכללתם ברשימה והזדמנות להגיש ערר.

תמיכה בתגובה חוקית של מדינה חברה

אמנת ליסבון כוללת סעיפי סולידריות וסיוע הדדי, אותם ניתן להפעיל בעקבות מתקפות סייבר חמורות. פסקת הסולידריות (סעיף 222 לאמנת התפקוד של האיחוד האירופי) קובעת כי המדינות החברות יעניקו תמיכה הדדית כאשר אחת או יותר מהן תיפול קורבן למתקפות טרור, לאסונות טבע או לאסונות מעשה ידי

אדם (כולל מתקפת סייבר חמורה). הנוהל ליישום סעיף זה באמנה הוגדר בהחלטה של מועצת אירופה מיולי 2014.

פְּסקת הסיוע ההדדי, המופיעה בסעיף 42 תת־סעיף 7 של אמנת האיחוד, מקבילה למדי לסעיף 5 באמנת נאט"ו, אם כי סעיף 5 נותן עדיפות לחברות נאט"ו. סעיף הסיוע ההדדי של האיחוד הופעל לראשונה על ידי צרפת בנובמבר 2015, בעקבות פיגועי הטרור בפריז. "התגובה הדיפלומטית המשותפת של האיחוד האירופי לפעולות סייבר זדוניות", מאוקטובר 2017, קובעת כי תגובות התואמות את הדין הבין־לאומי אינן מחייבות ייחוס חד־משמעי של מתקפת סייבר למקור או לתוקף ספציפיים. דבר זה עולה בקנה אחד עם הפרשנויות של מומחים למשפט בין־לאומי, המעוגנות ב"מדריך טאלין 2", בדבר החלת החוק הבין־לאומי על מרחב הסייבר.

פיקוח על הייצוא

האיחוד האירופי מתכוון לקדם את דיפלומטיית הסייבר שלו ואת שאיפתו לבדיקת נאותות באמצעות שליטה קפדנית יותר על ייצוא סחורות בעלות שימוש כפול. הנחיית השימוש הכפול, ממאי 2009, מסדירה את דרישות הרישוי המשותפות של המדינות החברות באיחוד האירופי במצבים של ייצוא, רכש והעברה של סחורות כאלו. באמצע דצמבר 2017 פרסמה הנציבות האירופית נוסח חדש לנספחים I, IIa עד IIg ו־IV של ההנחיה.[24] העדכון עסק בעיקר בפיקוח חדש על מוצרים מסוימים, כגון חומרות של טכנולוגיות מידע. הסחורות סווגו ככפופות לפיקוח (נספח I) על בסיס: (1) התנאים הקיימים באמנות ובהתחייבויות בין־לאומיות, ובמיוחד החלטת מועצת הביטחון של האו"ם 1540, אמנת הנשק הכימי ואמנת הנשק הביולוגי, וכן (2) רשימות פיקוח של משטרי ייצוא בין־לאומיים מולטילטרליים, ובראשם "הסדר ואסנאר", "קבוצת ספקיות הגרעין", "קבוצת אוסטרליה" ו"משטר הפיקוח על טכנולוגיית טילים" (MTCR). רשימות אלו מתעדכנות באופן תדיר. ייצוא סחורות ספציפיות למדינות הנתונות לסנקציות כפוף לא רק לפיקוח הדוק יותר; במקרים רבים יש לקבל אישור נפרד גם לייצוא סחורות בעלות שימוש כפול. אי־ציות לתנאים עלול לגרור עונשים או קנסות כבדים.

בדיקת נאותות – שלב אחר שלב

דרישת האיחוד האירופי להסכמה פה אחד מקשה על מיצובו ככוח משכין שלום. המדינות החברות מפגינות לא רק אמביוולנטיות אסטרטגית רבה (כמו, למשל,

24 "Commission Delegated Regulation (EU) 2017/2268 of 26 September 2017 amending Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items", *Official Journal of the European Union* 60, December 15, 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2017:334:FULL&from=EN.

במדיניותן כלפי רוסיה), אלא גם חוסר קוהרנטיות בפעולותיהן בענייני חוץ. שאיפת האיחוד האירופי לפעול ככוח משכין שלום מתבטאת ברצונן של המדינות החברות בו לחזק את עקרון בדיקת הנאותות באמצעות הכלים המדיניים שמציעה מדיניות החוץ והביטחון המשותפת.

בדיקת נאותות היא עיקרון מקובל היטב במשפט הבין־לאומי, המתבסס על הרעיון שהאיחוד האירופי לא רק חייב להבטיח שהכללים נשמרים בתחום השיפוט שלו, אלא גם לשאת באחריות לתוצאות מעשיו מחוץ לגבולותיו, למשל, באמצעות מדיניות ייצוא קפדנית יותר. כיום, יותר מתמיד, יש להחלטות האיחוד השלכות מעֵבר לתחום השיפוט שלו, ולכן עליו ליצור קוהרנטיות בתחום זה. כאשר הדבר נוגע למרחב הסייבר, לא די שהמדינות החברות יימנעו מהכרעות לא אחראיות הנעשות באופן עצמאי; חובתן היא גם ליטול על עצמן לפעול ביחד עם מדינות אחרות ולעשות כל מה שיתרום, בגבולות הסביר, ל"מרחב סייבר פתוח, כוללני, חופשי, שוחר שלום ובטוח".

השאלה עד כמה צריכות ממשלות המדינות החברות באיחוד האירופי להיערך לצעדי נגד טכנולוגיים, או אפילו לביצוע פעולות תגמול בסייבר, כפי שקורה כיום במקרה של רוסיה, נתונה לוויכוח. במידה שמדינה חברה תבחר להפעיל הגנה עצמית, כפי שהיא מוגדרת בסעיף 51 של מגילת האו"ם, ובהתאם למשפט הבין־לאומי ולמשפט ההומניטרי, הדבר יהיה בגדר מהלך מסלים ברמה הגבוהה ביותר של הסיוע ההדדי בקרב מדינות האיחוד האירופי. השלב הסופי של ניהול המשבר יהיה, לפיכך, עצירת המתקפה המתמשכת באמצעות הגנה אקטיבית, והמוצא האחרון יהיה פעולת תגמול בסייבר, כלומר פגיעה ממוקדת בשרת שממנו יצאה המתקפה. מהלך כזה יעמוד בעקרון בדיקת הנאותות רק אם המתקפה המתמשכת צפויה להסתיים בהשלכות חמורות שיאיימו על עצם קיומה של המדינה, ואם מוצו כל האמצעים האחרים. המסגרת המשפטית וחלוקת הסמכויות שפעולה כזו מחייבת לא הוגדרו עדיין, גם לא ברמה הלאומית.

הכלים החשובים והיעילים ביותר של האיחוד האירופי בהקשר זה הם מניעה וגילוי. המניעה כוללת את הצעדים הנכללים ב"הנחיה לביטחון רשתות ומידע", כגון אכיפה של תקינת סף ודרישות דיווח על מפעילי תשתיות קריטיות. ספקי תקשורת רשאים לנתח את תנועת הנתונים במקרה של שיבושים, ואם יש צורך, גם לחסום את העבריינים שזוהו.

חשיפה פירושה הבהרה וייחוס של המתקפה. גורם מכריע בהקשר זה היא ההערכה הפוליטית. עליה לקחת בחשבון את התמונה הכוללת של תקריות הסייבר ולחזות איומים היברידיים בעלי רלוונטיות צבאית. כאשר מדובר בהתקפות מקצועיות, נדרש שימוש בדיפלומטיית סייבר בין מדינות החולקות תפיסה דומה, כדי שגורמי הביטחון שלהן יחלקו מידע לצורך ניתוח חלקי הקוד ואופן התנהלותה של המתקפה.

ניתוחים מסוג זה מאפשרים להסיק מסקנות לגבי קבוצות ההאקרים ומקורן. "רשת צוותיIT בחירום של המדינות החברות" והיכולות הטכניות שלה נועדו לאפשר חילופי מידע דומים לצורך הגנה על תשתיות קריטיות. דיפלומטיית סייבר מחייבת החלפת מידע גם בין רשויות ועסקים. קבוצות CERT ציבוריות ופרטיות ושיתופי פעולה בתעשייה הכרחיים גם הם לאיגום ידע ומומחיות בדיפלומטיית סייבר.

דיפלומטיית סייבר היא מרכיב חשוב בביטחון הלאומי בסייבר. יחד עם זאת, עליה לשלב גם את הממד הכלל־אירופי ואפילו את הממד העולמי. אין די בחקירות שיתבססו אך ורק על מידע ברמה הלאומית. "מסגרת התגובה הדיפלומטית המשותפת של האיחוד האירופי לשנת 2017" מציעה מדיניות ביטחון סייבר שאינה צבאית. מדיניות כזו תסייע להתגבר על הדחף להגיב באופן מיידי על איומים במרחב הסייבר, ובמקום זאת נותנת עדיפות למהלכים מדיניים, כחלק ממדיניות החוץ והביטחון המשותפת של האיחוד, המבקש להטביע את חותמו ככוח משכין שלום. נכון יעשו שותפיו ויריביו של האיחוד ברחבי העולם כשיפרשו גישה זו שלו כמסר מדיני מובהק.

ישראל בפני שינויים עולמיים בתפוצת מל"טים חמושים: סכנות, אתגרים והזדמנויות

לירן ענתבי

במשך מספר עשורים הייתה מדינת ישראל בין המובילות בייצור, ייצוא והפעלת מל"טים. הדבר הִקנה לה יתרון בתחום הביטחוני והשפיע על יחסיה עם מדינות שונות. בשנים האחרונות מתחולל שינוי משמעותי בתחום זה, במסגרתו הופיעו יצרניות ויצואניות חדשות, כמו סין, איראן ורוסיה, חל שינוי במדיניות הייצוא של ארצות הברית ונעשה שימוש הולך וגובר בטכנולוגיות ובכלים אזרחיים, כמו רחפנים, המוסבים למשימות צבאיות הן על ידי מדינות והן על ידי ארגוני טרור. לשינויים אלה פוטנציאל להשפיע משמעותית על ישראל, הן מבחינה ביטחונית והן מבחינה מסחרית. מאמר זה סוקר את ההתפתחויות שחלו בתחום תפוצת המל"טים בעולם וממליץ למדינת ישראל על מדיניות הולמת להתמודד איתן, ובתוכה הרחבת המעקב המודיעיני אחר תפוצת מערכות ורכיבי מל"טים, השקעה במערכות נגד מתחומי הסייבר והל"א, הגברת השקיפות בתחומי הייצור והפיתוח ותמיכה בפיתוחים אזרחיים לצורך כניסה לשווקים חדשים.

מילות מפתח: מל"טים, כלים בלתי מאוישים, רחפנים, טכנולוגיה צבאית

מבוא

ישראל היא שחקנית מרכזית בתעשיית המל"טים העולמית. הדבר מתבטא בפיתוח ובייצור של מערכות מתקדמות, בצבירת ניסיון מבצעי מגוון ובייצוא של כלי טיס בלתי מאוישים. ישראל הפכה למשך כשבע שנים (2005־2013) ליצואנית המובילה בעולם בתחום זה, וזאת חרף היותה מדינה קטנה יחסית.

בשנים האחרונות מתחולל שינוי משמעותי בתפוצת מל"טים בעולם, ובהם גם מל"טים חמושים. הדבר נובע משינויים בתחום הטכנולוגי, מכניסתן של שחקניות

ד"ר לירן ענתבי היא עמיתת מחקר במכון למחקרי ביטחון לאומי ומרצה באוניברסיטת תל אביב ובאוניברסיטת בן־גוריון בנגב. המחברת מבקשת להודות לגב' מתן ינקו־אביקסיס, סטודנטית לתואר שני בלימודי דיפלומטיה באוניברסיטת תל אביב, המתמחה במכון למחקרי ביטחון לאומי.

חדשות לשוק כיצרניות ויצואניות, משינוי מדיניות של יצואניות ותיקות, וכן משינויים טכנולוגיים המאפשרים לעשות שימוש ברכיבים או מוצרים אזרחיים שונים, שעוברים התאמה והסבה לצרכים ביטחוניים. שינויים אלה הם בעלי פוטנציאל להשפיע באופן משמעותי על ישראל, הן בהיבט האיומים שהיא צריכה להיערך להתמודדות עימם במישור הביטחוני והן בהיבט האתגרים המסחריים שהמצב החדש יוצר.

המאמר פותח בהצגת הדומיננטיות הישראלית בתחום המל"טים בעשורים החולפים, וממשיך בהצגת השינויים שהתחוללו בתפוצת המל"טים בעשור האחרון, וכן בתיאור השינויים בדפוסי השימוש בהם. המאמר גם מציע דרכים להתמודד עם שינויים אלה: מלבד היערכות מול האיומים הביטחוניים הטמונים במצב החדש, יש צורך בשינוי המדיניות גם בתחום הפיתוח ובתחום המסחרי, במטרה לשמר את חוסנה של ישראל.

דומיננטיות ישראלית בתחום כלי הטיס הבלתי מאוישים

מזה מספר עשורים ישראל היא אחת השחקניות הדומיננטיות בתחום כלי הטיס הבלתי מאוישים. ישראל החלה לעשות שימוש במל"טים לצורכי צילום כבר בשנות השישים והשבעים של המאה העשרים, ועברה לשימוש במל"טים לצורכי הטעייה ואיסוף, שראשיתו במבצע "ערצב 19" בתחילת מלחמת לבנון הראשונה (1982). יש הטוענים שהצלחת הפעילות באמצעות מל"טים במבצע זה שימשה השראה להמשך פיתוחם של כלי טיס בלתי מאוישים בארצות הברית בשנות השמונים והתשעים של המאה.[1]

למרות המבצעים המרשימים שאפיינו את השימוש במל"טים בתחילת הדרך, השימוש העיקרי של ישראל בכלי טיס בלתי מאוישים היה למטרות איסוף מודיעין במסגרת עימותים אסימטריים, החל משורה של מבצעים בראשית שנות האלפיים, דרך מלחמת לבנון השנייה ומבצעים שונים נגד ארגון חמאס ברצועת עזה שבאו לאחר מכן ("עופרת יצוקה", "עמוד ענן" ו"צוק איתן"). שיא השימוש של ישראל במל"טים היה בשנת 2006, כאשר הפכה למדינה הראשונה בהיסטוריה שעשתה שימוש ביותר שעות טיסה של מל"טים לאורך המלחמה מאשר שעות טיסה של מטוסי קרב. יתר על כן, היה זה מקרה ראשון בהיסטוריה הצבאית שבו נשמר רצף של פעילות מל"טים מעל לאזור הלחימה לאורך מלחמה שלמה.[2]

---

1 Tamir Libel and Emily Boulter, "Unmanned Aerial Vehicles in the Israel Defense Forces", *The RUSI Journal*, 160:2 (2015): 68-75.

2 יצחק בן־ישראל, **מלחמת הטילים הראשונה**, נייר עמדה של בית הספר לממשל ולמדיניות: אוניברסיטת תל אביב, מאי 2007, עמ' 46.

ההובלה והדומיננטיות הישראליות בתחום המל"טים באות לידי ביטוי לא רק בניסיון המבצעי; על אף היותה מדינה קטנה יחסית, ישראל הפכה בשנים 2005־2013 למובילה העולמית של ייצוא מל"טים, עם נתח שוק של 4.62 מיליארד דולר.[3] על פי פרסומים שונים, ישראל ייצאה כלי טיס בלתי מאוישים למדינות רבות באירופה, באסיה ובאמריקה הלטינית,[4] ולאורך השנים גם ייצאה מל"טים רבים לארצות הברית, שעשתה בהם שימוש, בין היתר, במלחמה בעיראק.[5]

בסוף העשור השני של המאה ה־21 מייצרת ישראל ומייצאת מערכות אוויריות בלתי מאוישות שונות בהיקף נרחב ומסוגים שונים, החל במיני־מל"טים טקטיים המופעלים על ידי כוחות קרקעיים, כמו "רוכב שמיים" (skylark) של חברת "אלביט",[6] דרך כלים טקטיים רב־משימתיים לטווח בינוני, דוגמת "הרמס 450", גם הוא של "אלביט", בעל טווח טיסה של מאות קילומטרים ויכולת נשיאת מטענים ייעודיים במשקל של כמאתיים ק"ג,[7] ועד למל"טים לטווח ארוך, דוגמת "הרון" (Heron) של התעשייה האווירית לישראל, שמסוגל לשאת מטען ייעודי במשקל של עד 470 ק"ג.[8] על פי פרסומים זרים, חלק מהמל"טים הישראליים המופעלים מרחוק הם בעלי יכולות תקיפה מתקדמות.[9]

לצד המערכות הללו, המוטסות ומופעלות מרחוק, מייצרת ישראל ומייצאת גם מערכות אוויריות בלתי מאוישות מתחום "החימושים המשוטטים", שחלקן הן מערכות "שגר ושכח" הפועלות באופן אוטונומי: לחלק מן המערכות הללו יכולות טכניות המאפשרות להן לטוס, לשהות באוויר ולאתר מטרה, ובמידת הצורך גם להשמיד אותה באמצעות חומר הנפץ שהן נושאות, תוך שהן "מתאבדות". כל זאת במעורבות אנושית נמוכה, או ללא מעורבות אנושית כלל. בין המערכות

---

3 אורה קורן, "ישראל הינה יצואנית כלי הטיס הבלתי מאוישים הגדולה בעולם", **דה־מרקר**, המהדורה הדיגיטלית, 19 במאי 2013, https://www.themarker.com/news/macro/1.2023690

4 Harriet Sherwood, "Israel is World's Largest Drone Exporter", *The Guardian*, Digital Edition, May 20, 2013, https://www.theguardian.com/world/2013/may/20/israel-worlds-largest-drone-exporter

5 Amnon Barzilai, "U.S. Army Wants to Buy More Israeli Hunter Drones", *Haaretz*, July 8, 2003, https://www.haaretz.com/1.5494046.

6 Skylark^{tm} I – LEX, Elbit Systems Website, http://elbitsystems.com/products/uas/skylark-i-lex/

7 Hermes^{tm} 450, Elbit Systems Website, http://elbitsystems.com/products/uas/hermes-450/

8 Heron, Israel Aerospace Industries Website, http://www.iai.co.il/2013/18900-16382-en/BusinessAreas_UnmannedAirSystems_HeronFamily.aspx.

9 רון בן ישי, "עמימות תקיפות המל"טים מיותרת", *Ynet news*, 11 ביולי 2016, https://www.ynet.co.il/articles/0,7340,L-4826915,00.html

הבולטות בתחום זה ניתן למנות את "הארפי" (Harpy NG) ו"הארופ" (Harop) מתוצרת התעשייה האווירית.[10]

ייצוא המל"טים הוא תחום מסחרי חשוב עבור מדינת ישראל, והיווה בשלב מסוים כעשרה אחוזים מכלל הייצוא הביטחוני שלה.[11] מעֵבר לחשיבות הכלכלית, לייצוא המל"טים יש השפעה ניכרת על יחסיה של ישראל עם מדינות שונות, הן בתחום הדיפלומטי והן בתחום שיתופי הפעולה הביטחוניים. במסגרת זו בולטת עיסקת מל"טים שערכה ישראל עם רוסיה (שלא נתקלה בהסתייגות מצד ארצות הברית), שבתמורה לה ציפתה ישראל מרוסיה שתימנע ממכירת טילי נ"מ S–300 לאיראן.[12]

במשך שנים רבות שלטה ישראל בתחום ייצוא המל"טים, כשבמקביל לה מקיימת ארצות הברית דומיננטיות בייצור כלי טיס בלתי מאוישים. במשך תקופה ארוכה השקיעה ארצות הברית משאבים רבים בייצור מל"טים לצורך הגדלת סדר הכוחות שלה עצמה, אולם בשנים האחרונות החל תהליך שבו יצרניות מל"טים אמריקאיות מבקשות לייצא יותר כלים כאלה למדינות שונות ברחבי העולם. התפתחות זו מובילה, בין היתר, להגברת התחרות העולמית, ובראש ובראשונה לתחרות עם ישראל. במקביל מתחוללים שינויים נוספים בתפוצת מל"טים צבאיים ברחבי העולם, כפי שיתואר להלן. גם שינויים אלה עשויים להשפיע על ישראל.

שינוי בתפוצת מל"טים צבאיים

שוק המל"טים העולמי הולך וגדל משנה לשנה באופן משמעותי. בשנת 2015 הוערך שוק זה ב־5.93 מיליארד דולר, וההערכה היא כי בשנת 2022 יגיע שוויו ל־22.15 מיליארד דולר, כאשר הנתח הצבאי של השוק אמנם ימשיך לגדול, אך עיקר הגידול יהיה בתחום האזרחי.[13] חרף השינויים המתחוללים בעולם, ישראל וארצות הברית הן עדיין שתי המדינות המובילות בתחום ייצור וייצוא המל"טים הצבאיים. חידושים בתחום הטכנולוגיה, יחד עם השפעות מתחום הגלובליזציה והיעדר רגולציה, מובילים לשינוי משמעותי בתחום זה ומאפשרים הופעתן של

10 Harpy NG, Israel Aerospace Industries Website, http://www.iai.co.il/2013/36694-16153-en/Business_Areas_Land.aspx.

11 אורה קורן, "ישראל הינה יצואנית כלי הטיס הבלתי מאוישים הגדולה בעולם".

12 אנשיל פפר, "ישראל תמכור מל"טים לרוסיה כדי שתבטל עסקה עם איראן", **הארץ**, מהדורה דיגיטלית, 25 ביוני 2009, https://www.haaretz.co.il/news/politics/1.1267820.

13 Christopher Diamond, "Global Drone Market Expected to Surpass $22B by 2022", *Defense News*, May 3, 2017, https://www.defensenews.com/air/2017/05/03/global-drone-market-expected-to-surpass-22b-by-2022/.

שחקניות חדשות בשוק המל"טים,[14] המציעות את מרכולתן בשווקים חדשים, ובהם מדינות שבעבר לא נמצא גורם שהיה מוכן למכור להן מערכות מסוג זה.

התפתחות זו מובילה לשינויים משמעותיים בתפוצת מל"טים בכלל ומל"טים חמושים בפרט, וכן בדפוסי השימוש בהם. הדבר מתאים לתחזית שהוצגה לפני מספר שנים במחקר של מכון RAND האמריקאי, שם נטען כי תוך פחות מעשור תוכל כל מדינה לרכוש מל"טים חמושים ולעשות שימוש בהם.[15] בהתבסס על מחקר זה, וכן על השינויים שחלו בשנים שחלפו מאז פרסומו, ניתן לטעון כי השינוי המשמעותי ביותר בתחום המל"טים מתרחש כיום בתת־התחום של המל"טים החמושים.

אחת השחקניות המשמעותיות שנכנסה לשוק המל"טים החמושים בעשור האחרון וגורמת לשינויו מן היסוד היא סין, המהווה יצואנית בולטת בתחום זה. על פי דוח של משרד ההגנה האמריקאי משנת 2015, בכוונתה של סין לייצר 42,000 מל"טים מסוגים שונים עד שנת 2023.[16] בדוחות האמריקאיים שפורסמו מאז נאמר כי סין ממשיכה להשקיע משאבים בתחום זה במטרה לאפשר את מימוש התוכנית.[17] המל"טים הסיניים מסדרת CH (Cai Hong) Rainbow, המיוצרים על ידי התאגיד הסיני CASC (China Aerospace Science and Technology Corporation),[18] הפכו לנפוצים ברחבי העולם תוך שנים בודדות. בתוך סדרה זאת ניתן למנות את CH–3, המהווה את הדגם הנפוץ ביותר שלה, ואת CH–4, שניהם בעלי יכולת תקיפה, אך נבדלים זה מזה בגודל, ביכולת נשיאת המטען הייעודי ובמשך הטיסה. המל"ט החדש ביותר בסדרה זו, CH–5, הוא, לטענת היצרן, בעל יכולת נשיאה עד אלף ק"ג של מטענים ייעודיים וחימוש, יכולת שהייה באוויר של עד שישים שעות וטווח

14 לירן ענתבי, "שינוי מגמות בתחום כלי הטיס הבלתי מאוישים: אתגרים חדשים", **צבא ואסטרטגיה**, כרך 6, גיליון 2, אוגוסט 2014, עמ' 19־35, http://www.inss.org.il/he/wp-content/uploads/sites/2/systemfiles/%D7%9C%D7%99%D7%A8%D7%9F%20%D7%A2.pdf.

15 Lynn E. Davis, Michael J. McNerney, James S. Chow, Thomas Hamilton, Sarah Harting and Daniel Byman, *Armed and Dangerous? UAVs and U.S. Security* (Santa Monica, CA: RAND Corporation, 2014), https://www.rand.org/pubs/research_reports/RR449.html; Patrick Tucker, "Every Country Will Have Armed Drones Within 10 Years", *Defense One*, May 6, 2014, https://www.defenseone.com/technology/2014/05/every-country-will-have-armed-drones-within-ten-years/83878/.

16 Zachary Keck, "China Is Building 42,000 Military Drones: Should America Worry?", *The National Interest*, May 10, 2015, https://nationalinterest.org/blog/the-buzz/china-building-42000-military-drones-should-america-worry-12856.

17 "Military and Security Developments Involving the People's Republic of China 2018", *United States Office of the Secretary of Defense, Annual Report to Congress*, May 16, 2018, pp. 23, 33-34, 63-64, 83, https://media.defense.gov/2018/Aug/16/2001955282/-1/-1/1/2018-CHINA-MILITARY-POWER-REPORT.PDF

18 Clever Hawkl, China Aerospace Science and Technology Corporation's Website, http://english.spacechina.com/n16421/n17215/n17272/c125468/content.html

טיסה מרבי של 6,500 ק"מ.[19] מדובר בנתונים המבקשים להתחרות עם מל"טים מתקדמים מתוצרת המדינות שיש להן ותק רב בתחום זה.

במקביל לפיתוח הטכנולוגי ולייצור המהיר, סין מנהלת מדיניות ייצוא מתירנית וליברלית מאוד ביחס למדיניות השמרנית של ארצות הברית וישראל, ובין היתר אינה חתומה על הסכמים דוגמת משטר הפיקוח על טכנולוגיות טילים (Missile Technology Control Regime – MTCR), המהווה את אחד ההסכמים המגבילים יצוא מל"טים. הסינים גם מציעים את מגוון המל"טים מתוצרתם במחירים נמוכים באופן משמעותי ממחירי המל"טים האמריקאיים, מה שהופך את סין ליצואנית אטרקטיבית. כך, למשל, מל"ט סיני מסוג CH-5 עולה כמעט מחצית ממחירו של מל"ט MQ-1 Predator האמריקאי.[20] כתוצאה מכך, פקיסטן, עיראק וניגריה כבר הספיקו לבצע תקיפות באמצעות מל"טים חמושים שסופקו להן על ידי סין או יוצרו בשיתוף פעולה איתה. נכון לשנת 2018, סין אישרה ייצוא של מל"טים לעשר מדינות, ובתוכן ירדן, ערב הסעודית ואיחוד האמירויות הערביות.[21] מדיניות זו של סין היא בעלת השפעה על ישראל הן בהיבט הביטחוני והן בהיבט המסחרי.

שחקנית נוספת הגורמת לשינוי בתחום המל"טים העולמי היא איראן, המייצרת בשנים האחרונות סוגים שונים של מל"טים, אותם היא מציגה בפומבי בהזדמנויות שונות. חלק מהדגמים שהציגה איראן בתערוכות או במצעדים צבאיים לא הדגימו יכולת מבצעית. עד לשנים האחרונות נראה היה שהמל"טים שמייצרת איראן הם לשימושה ולשימושם של בני ובנות החסות שלה, דוגמת חזבאללה.[22] עם זאת, בשנתיים האחרונות החלה כנראה איראן לספק מל"טים גם לסוריה, מדינה כושלת הנמצאת במלחמת אזרחים הנמשכת כבר יותר מחצי עשור. התפתחות חדשה זאת מהווה גורם "משַנה כללי מִשחק" (Game Changer) עבור ישראל.

אחד הכלים המרכזיים הנמצא בשימוש איראן ובעלות בריתה הוא מל"ט בשם "שאהד 129", ששימש בין השאר לתקיפות על המורדים בסוריה.[23] מאז שנת 2017 מציעה איראן מל"ט בשם Hamaseh, שלדברי חוקרים בתחום המל"טים מזכיר

19 Zhao Lei, "Unmanned Combat Drone to be Exported", *China Daily*, January 11, 2016. http://www.chinadaily.com.cn/china/2016-11/01/content_27233618.htm.

20 Ben Brimelow, "Chinese Drones may Soon Swarm the Market – and that could Be Very Bad for the US", *Business Insider*, November 16, 2017, https://www.businessinsider.com/chinese-drones-swarm-market-2017-11.

21 "World of Drones", *New America*, https://www.newamerica.org/in-depth/world-of-drones/1-introduction-how-we-became-world-drones/.

22 Roi Kais, "Hezbollah has Fleet of 200 Iranian-made UAVs", *Ynet news*, November 25, 2013, https://www.ynetnews.com/articles/0,7340,L-4457653,00.html.

23 Jeremy Binnie, "Analysis: Syrian Rebel Video Corroborates Iranian UAV Strike Claims", *Jane's 360*, February 12, 2016, https://www.janes.com/article/57968/analysis-syrian-rebel-video-corroborates-iranian-uav-strike-claims.

בצורתו את מל"ט "איתן" של התעשייה האווירית של ישראל (אם כי הוא בעל ממדים קטנים יותר).[24] על פי הדיווחים האיראניים, מל"ט זה מסוגל לשאת חימוש וחיישנים מתקדמים ולשהות באוויר במשך 11 שעות, והוא בעל טווח טיסה מרבי של מאתיים ק"מ. האיראנים גם טוענים שמל"ט זה הוא בעל יכולות חמקניות, למרות שצורתו החיצונית ואופן תליית החימוש עליו מעידים אחרת.[25] לאיראן אין לוויינים צבאיים, ולכן יכולות ההפעלה שלה בתחום המל"טים הינן מוגבלות. זאת, משום שטווחי השידור של המל"טים שלה מוגבלים למרחקים קצרים יחסית, ובמקרים אחרים הם מאפשרים העברת המידע המודיעיני שהם אוספים רק לאחר הנחיתה.[26]

בד בבד עם השינויים בתפוצת המל"טים כתוצאה מהצטרפות שחקניות חדשות, גם ארצות הברית, שהיא כאמור יצרנית ותיקה של מל"טים, עומדת ככל הנראה לשנות את דרכי פעולתה במה שנוגע לייצוא מל"טים, בעיקר מל"טים חמושים. בכך תצטרף גם היא לגורמים המשפיעים על השינויים בתפוצת המל"טים ברחבי העולם. נמסר כי הנשיא דונלד טראמפ, בניגוד לקודמו, שוקל לאשר שינוי במדיניות הייצוא של מערכות טיס בלתי מאוישות. במסגרת המדיניות החדשה יצטמצמו, כמדווח, החסמים על מכירת מל"טים קטנים המאפשרים איתור ותקיפה, שהם בעלי טווח טיסה ויכולת נשיאת חימוש נמוכים יותר מאלה של המל"ט הוותיק מסוג MQ–1 Predator,[27] או של הדגם המתקדם יותר MQ-9A Reaper–. הדרישה להוריד את החסמים על מכירת מל"טים מגיעה מהתעשיות הביטחוניות האמריקאיות, המבקשות להרחיב את מעגל לקוחותיהן. לעומתן, יש בארצות הברית קולות היוצאים נגד שינוי המדיניות, בין השאר בטענה שגידול במכירת מל"טים תוקפים

24 Stephan Trimble, "Iran Puts Hamaseh UAV on Export Market", *FlightGlobal*, July 18, 2017, https://www.flightglobal.com/news/articles/iran-puts-hamaseh-uav-on-export-market-439414./

25 Kelsey D. Atherton, "Iran Unveils Absurd New Stealth Drone", *Popular Science*, May 13, 2013. https://www.popsci.com/technology/article/2013-05/iran-unveils-new-stealth-drone-isnt.

26 Yaniv Kubovich, "Iran's Army of Drones, Target of Syria Strike: Rising Force or Limited Threat?", *Haaretz*, April 12, 2018 https://www.haaretz.com/middle-east-news/iran/.premium.MAGAZINE-iran-s-drones-targeted-in-syria-rising-force-or-limited-threat-1.5992631.

27 Michael C. Horowitz and Joshua A. Schwartz, "A New U.S. Policy Makes it (somewhat) Easier to Export Drones", *The Washington Post*, Digital Edition, April 20, 2018, https://www.washingtonpost.com/news/monkey-cage/wp/2018/04/20/a-new-u-s-policy-makes-it-somewhat-easier-to-export-drones/?utm_term=.2f0fe76beefb.

עשוי לתת נשק בידי ממשלות הפועלות בצורה לא אחראית נגד שכנותיהן, ואף נגד אוכלוסיות מבית.[28]

מדינה נוספת שמנסה להפוך לשחקנית דומיננטית יותר בתחום המל"טים היא רוסיה. רוסיה מפגרת בתחום המל"טים יחסית לעוצמתה הצבאית ולתפקיד שממלא הייצוא הביטחוני ביחסיה האסטרטגיים עם מדינות רבות. יחד עם זאת, מקובל להחשיב אותה כאחת מחמש המדינות הבולטות בתחום המל"טים,[29] ככל הנראה בשל ניסיונה להשתלב בין המובילות בתחום זה על ידי השקעת משאבים בתוכנית לאומית לקידומו, בעלות של מיליארדי דולרים.[30] כמו כן, רוסיה מקדמת שיתופי פעולה בייצור מל"טים עם מדינות שונות, שאיתן היא קיימה בעבר שיתוף פעולה כזה.[31] רוסיה מפגרת עדיין מבחינה טכנולוגית ותעשייתית בתחום זה, אך פעילותה הגוברת בו מחייבת תשומת לב מיוחדת, בעיקר לאור העובדה שהיא מספקת ציוד צבאי למדינות סוררות דוגמת סוריה.

במקביל לשינויים הללו ניכרת מגמה נוספת בתחום המל"טים: מדינות רבות הופכות ליצרניות מל"טים, לרוב לצריכה עצמית. חרף העובדה שלרוב מדובר במל"טים שאינם תוקפים, לא ניתן להתעלם מההשפעה הפוטנציאלית של שינוי זה הן בתחום הביטחוני והן בתחום המסחרי. בין היצרניות החדשות יחסית ניתן למנות את הודו, פקיסטן, דרום אפריקה, ונצואלה ואוקראינה, אך יש עוד מדינות רבות המוזכרות בהקשר זה.[32]

לאור השינויים המתחוללים בעולם בתחום המל"טים, עולות מעת לעת יוזמות שמטרתן להגביל או לשנות את המצב הקיים. מחקר של מכון המחקר של האו"ם לענייני מניעת תפוצת נשק (UNIDIR) קורא להגברת השקיפות, הפיקוח והחבות המשפטית בכל הנוגע למל"טים חמושים. המחקר מתבסס על פגישות עם מומחים מתחומים שונים וממדינות שונות וכולל שורת המלצות, שהמרכזית

28 Mike Stone and Matt Spetalnick, "Exclusive: Trump to Boost Exports of Lethal Drones to More U.S. Allies – Sources", *Reuters*, March 18, 2018, https://www.reuters.com/article/us-usa-arms-drones-exclusive/exclusive-trump-to-boost-exports-of-lethal-drones-to-more-u-s-allies-sources-idUSKBN1GW12D.

29 Robert Farley, "The Five Most Deadly Drone Powers in the World", *The National Interest*, February 16, 2015, https://nationalinterest.org/print/feature/the-five-most-deadly-drone-powers-the-world-12255.

30 Jaroslaw Adamowski, "Russian Defense Ministry Unveils $9B UAV Program", *Defense News*, February 19, 2014.

31 Yaakov Lappin, "Report: Moscow Purchased 10 Israeli Drones", *The Jerusalem Post*, September 8, 2015, https://www.jpost.com/Israel-News/Politics-And-Diplomacy/Report-Russia-purchased-ten-Israeli-drones-415575.

32 Wim Zwijnenburg and Foeke Postma, "Unmanned Ambitions", *PAX for Peace*, July 2018, pp. 18-35, https://www.paxforpeace.nl/publications/all-publications/unmanned-ambitions.

שבהן היא לקיים דיון מולטילטרלי פתוח ומשתף במטרה לקבוע סטנדרטים ועקרונות לשימוש במל"טים חמושים.[33] בנוסף לכך יצאה ארצות הברית בשנת 2016 ביוזמה, שבמסגרתה היא ניסחה מסמך עקרונות להסדרת ייצוא מל"טים, עליו חתמו עד היום כארבעים מדינות. צרפת, רוסיה, סין וברזיל, שהן בין יצרניות המל"טים המרכזיות, סירבו לחתום על המסמך, כמו גם ישראל, החוששת שהוא יגביל את הפעילות העיסקית שלה בתחום זה ברחבי העולם.[34]

השינוי בדפוסי השימוש במל"טים חמושים

השינוי בתפוצת מל"טים מאפשר, בין היתר, שינוי בדפוסי השימוש בהם, במיוחד במל"טים תוקפים. השינויים העיקריים בשימוש במל"טים באים לידי ביטוי בשנים האחרונות בעיקר במזרח התיכון רווי הסכסוכים האלימים. דוגמה בולטת לכך היא השימוש שעשה צבא עיראק במל"טים תוקפים מתוצרת סין במאבק שניהל נגד ארגון הטרור המדינה האסלאמית (דאע"ש). הצבא העיראקי, שפורק ושוקם על ידי ארצות הברית לאחר מלחמת המפרץ השנייה, כמעט שב והתפורר לחלוטין בעקבות המתקפות הקשות של דאע"ש. יחד עם זאת, צבא עיראק מחזיק כיום בכלים בלתי מאוישים חמושים מתוצרת סין, בעלי יכולת תקיפה באמצעות טילים מונחים. כלים אלה מאפשרים לו להצטרף לקבוצה הולכת וגדלה של צבאות ברחבי העולם העושים שימוש מבצעי במל"טים חמושים, דבר שהיה נחלתן של מדינות בודדות בלבד עד לפני פחות מעשור. המקרה העיראקי מטריד במיוחד, לאור חוסר היציבות המאפיין את עיראק בכלל ואת הצבא העיראקי בפרט.

על פי מחקר של ארגון PAX, יצרניות חדשות של מל"טים, כמו איראן, סיפקו מל"טים, חלקם חמושים, למדינות שונות, שאף עשו בהם שימוש. מל"טים מתוצרת איראן נטלו חלק במספר עימותים וסכסוכים אזוריים, כולל בטורקיה, במפרץ הפרסי ובסוריה, וכן בפקיסטן, שם הופעלו מל"טים כאלה נגד המורדים בצפון־מערב המדינה.[35] יכולתן של חלק ממדינות אלו לרכוש ולהשתמש במל"טים הינה מדאיגה, במיוחד לאור אופי המשטרים בהן, יציבותן המעורערת ואיומי טרור הקשורים בהן.

מקרה נוסף של שימוש במל"ט תוקף בזירה המזרח תיכונית הוא המל"ט האיראני ששוגר מתחומי סוריה אל עבר ישראל בפברואר 2018. המל"ט, שלטענת גורמים

33 "Increasing Transparency, Oversight and Accountability of Armed Unmanned Aerial Vehicles", *UNIDIR*, July 2017, http://www.unidir.org/files/publications/pdfs/increasing-transparency-oversight-and-accountability-of-armed-unmanned-aerial-vehicles-en-692.pdf.

34 גילי כהן, "ישראל סירבה לחתום על מסמך עקרונות שהפיצה ארה"ב להסדרת יצוא מל"טים", **הארץ**, מהדורה דיגיטלית, 23 באוקטובר 2016, https://www.haaretz.co.il/news/politics/.premium-1.3101120.

35 Zwijnenburg and Postma, "Unmanned Ambitions", p. 11.

שונים מהווה חיקוי של מל"ט אמריקאי חמקן, בעל יכולת לשאת טילים מדויקים, יורט על ידי ישראל.[36] בהתאם לתחקיר שפורסם על ידי צה"ל, המל"ט נשא עליו חומר נפץ, מה שהפך את שיגורו למקרה הראשון שבו איראן ניסתה לפגוע באופן ישיר במדינת ישראל על אדמתה.[37]

מעבר לשימוש במל"טים מתוצרת התעשיות הצבאיות של מדינות שונות, נעשה כיום שימוש גם בכלים חמושים מאולתרים או בכלים אזרחיים שעברו הסבה. ההערכה היא כי למרות שמדובר בכלים שאינם מתוצרת צבאית, והם לעיתים קרובות קטנים, בעלי טווח קצר ורמות דיוק נמוכות, עדיין הם יכולים להוות איום ביטחוני משמעותי.[38] אחד המקרים הבולטים בהקשר זה התרחש בסוף דצמבר 2017, כאשר בסיס חיל האוויר הרוסי "חמימים" במחוז לטאקיה והמרכז הלוגיסטי "טרטוס", שניהם בסוריה, הותקפו על ידי קבוצה של 13 כלי טיס בלתי מאוישים. ההתקפה הביאה להרס ציוד צבאי רוסי משמעותי רב: מפציצים, מטוסי קרב, מטוס תובלה, וכן מאגר תחמושת. הטכנולוגיות ששימשו את התוקפים בכלים המאולתרים הללו, ובתוכן מערכות GPS שאפשרו את התקיפה המדויקת, הביאו גורמים רוסיים לטעון כי ההתקפה בוצעה בגיבוי של מדינה מפותחת.[39] לטענה זו לא נמצאה עדות ממשית, ולעומת זאת יש חוקרים הטוענים שגם ארגונים תת־מדינתיים מסוגלים לייצר כיום כלים דוגמת אלה ששימשו במתקפה, באמצעות רכיבים שניתן לרכוש מהמדף המסחרי או מתוצרת עצמית. ימים ספורים לאחר התקיפה הראשונה על יעדים רוסיים בסוריה, שכונתה "Novy-God Attack", סיכל הצבא הרוסי בהצלחה ניסיון נוסף לתקוף את בסיס "חמימים" באמצעות

36 Morris Loveday, "The Drone Shot Down by Israel was an Iranian Copy of a U.S. Craft, Israel Says", *The Washington Post*, Digital Edition, February 11, 2018, https://www.washingtonpost.com/world/israel-confirms-downed-jet-was-hit-by-syrian-antiaircraft-fire/2018/02/11/bd42a0b2-0f13-11e8-8ea1-c1d91fcec3fe_story.html?utm_term=.8ab82fb83acf.

37 יואב זיתון ורון בן ישי, "מל"ט הנפץ: ניסיון איראני ראשון לפגוע בישראל ישירות", *Ynet news*, מהדורה דיגיטלית, 14 באפריל 2018, https://www.ynet.co.il/articles/0,7340,L-5229485,00.html.

38 "Home-Made Drones Now Threaten Conventional Armed Forces", *The Economist*, Digital Edition, February 8, 2018, https://www.economist.com/science-and-technology/2018/02/08/home-made-drones-now-threaten-conventional-armed-forces.

39 Dave Majumdar "Russia Came Under Attack by a 'Swarm' in Syria, Says Report", *The National Interest*, January 8, 2018, https://nationalinterest.org/blog/the-buzz/russia-came-under-attack-by-swarm-syria-says-report-23987.

מל"טים חמושים.[40] מאז היו מספר התקפות נוספות על הבסיס, כשמערכות ההגנה האווירית הרוסיות מצליחות ליירט את המל"טים התוקפים.[41]

העובדה המרכזית העולה מהמתקפות הללו היא שטכנולוגיית מל"טים נפוצה כיום מאוד וכי האיום המרכזי לישראל מגיע לא רק ממדינות הרוכשות מל"טים תוקפים מתוצרת איראנית או סינית, אלא גם מצד כל גורם אחר המסוגל להרכיב לעצמו אמצעי תקיפה מתקדמים באמצעות רכיבי מדף. ארגוני המודיעין המדינתיים מתקשים לעקוב אחרי גורמים כאלה. האיום החדש הולך ומתעצם עקב תפוצה מתרחבת של טכנולוגיות מתקדמות מסוגים שונים, היוצרות היצע מדף של אמצעים שניתן לעשות בהם שימוש קטלני ללא קושי רב. בדרך זו הופכות טכנולוגיות שונות לבעלות שימוש דואלי (אזרחי וצבאי), למרות שהן אינן מוגדרות ככאלו, וכתוצאה מכך לא חלות עליהן רגולציה או חקיקה שיאפשרו להגביל את תפוצתן ולמנוע שימוש צבאי בהן. הדבר מהווה איום מהותי על ישראל, מכיוון שארגוני טרור המאיימים עליה נסמכים על הטכנולוגיות הללו יותר משעושים זאת צבאות סדירים.

מתקפות המל"טים בסוריה מדגישות פעם נוספת גם את איום הרחפנים, שמדינות רבות אינן ערוכות די כדי לטפל בו, הן מבחינת פריסת מערכות ההגנה האווירית סביב בסיסים ונכסים אסטרטגיים והן מבחינת יכולות ל"א או סייבר לשבש או להשתלט על הכלים העוינים מרחוק. פגיעה של קבוצת כלים מאולתרת כמו זו ששימשה במתקפות על בסיס "חמימים", או התקפה של רחפנים חמושים, אינן משפיעות, ברוב המקרים, מבחינה אסטרטגית על מדינה או על מערכה צבאית, אך הן עלולות לגרום פגיעה קשה מבחינה תודעתית.

השפעות אפשריות על ישראל

השינויים המתחוללים בתחום המל"טים הינם בעלי השפעה על הזירה הבין־לאומית כולה. מל"טים חמושים מקנים לגורמים שונים, יותר מאשר בעבר, יכולת לבצע מתקפות אוויריות מבלי לקבל אחריות עליהן ותוך שמירת חשאיות סביב הגורם המבצע. גם היכולת לבצע משימות איסוף מודיעיניות משתנה בצורה משמעותית נוכח השינוי בניהול הסיכונים על ידי מפקדים או מדינאים, שינוי הנובע מהעובדה שהמטוס פועל ללא מפעיל אנושי על סיפונו. התחרות הגוברת בשוק המל"טים היא גורם נוסף המשפיע באופן משמעותי, במיוחד על מדינות שהיו בעבר יצרניות ויצואניות מובילות בתחום זה.

---

40 סוכנויות הידיעות, "הבסיס הרוסי בסוריה שוב תחת אש: 'סוכלה מתקפת מל"טים חמושים'", **וואלה חדשות**, 7 בינואר 2018, https://news.walla.co.il/item/3125331.

41 Dmitry Kozlov and Sergei Grits, "Russia Says Drone Attacks on its Syria Base Have Increased", *The Times of Israel*, August 17, 2018, https://www.timesofisrael.com/russia-says-drone-attacks-on-its-syria-base-have-increased/.

ישראל מושפעת, יותר ממדינות אחרות, מהשינויים הללו, הן מבחינה ביטחונית והן מבחינה מסחרית. הדבר נובע ממעמדה כיצואנית מובילה של מערכות אוויריות בלתי מאוישות, מההשפעה של תפוצת המל"טים על סוגיות אסטרטגיות הקשורות אליה, ומעצם היותה מדינה הסובלת ממגוון איומים ביטחוניים מתמשכים, הן מצד חלק מן המדינות השוכנות לאורך גבולותיה והן מצד ארגוני טרור הפועלים מבית ומחוץ. להלן יפורטו ההשפעות העיקריות של השינויים בתעשיית המל"טים על ישראל.

איומים ביטחוניים

הגיוון ביצרניות ויצואניות המל"טים, ובתוכם גם מל"טים תוקפים, מביא לשינוי באופי הגורמים הפוטנציאליים המשתמשים במערכות אלו. העובדה שסין מייצאת מל"טים למספר מדינות שבעבר ידן לא הייתה משגת (הן מבחינה תקציבית והן מבחינת מערכות היחסים האסטרטגיים שלהן) לרכוש מערכות כאלו, עשויה להציב את ישראל בעתיד הקרוב או הבינוני בפני אתגרים הנובעים מהשימוש של אותן מדינות במל"טים. כמו כן, יש לקחת בחשבון את הסיכונים הכרוכים באפשרות שמערכות אלו יעברו, מסיבות שונות, מאותן מדינות לידיים לא מדינתיות. בין המדינות שבהן מדובר בהקשר זה ניתן למנות את עיראק, ירדן ופקיסטן. אלו מצטרפות לאיראן, וכן לארגון חזבאללה, המצויד במערכות איראניות.

ראוי לציין כי שינוי זה מתחולל לצד שינויים נוספים במזרח התיכון, ובהם המצב הרעוע בסוריה בעשור האחרון והנוכחות הרוסית והאיראנית בזירה, שמשפיעים גם הם על ישראל ויוצרים איומים שעליה ללמוד להתמודד איתם. לכך יש להוסיף את האיום האווירי הנובע משימוש ברחפנים וכלים מאולתרים ואת העובדה ששחקנים שונים משיגים כיום יכולות אוויריות משמעותיות באמצעות רכיבי מדף, כולל מל"טים תוקפים או כלי טיס מאולתרים מדויקים לצורך פעולות התאבדות.

אתגרים מסחריים

האתגר המסחרי של ישראל הנובע מתפוצת מל"טים הינו מורכב. ישראל זקוקה לייצוא הביטחוני, שמל"טים מהווים חלק מרכזי מתוכו, כדי לקדם פעילות נרחבת של התעשיות הביטחוניות שלה. הדבר נובע מכך שהשוק הישראלי קטן מכדי להתקיים עליו בלבד. בנוסף, ישראל מושפעת בייצוא המל"טים שלה מהשינויים העולמיים בתפוצת כלי הטיס הבלתי מאוישים, ובמיוחד מייצוא המל"טים של סין, המהווה תחרות מסחרית משמעותית.[42] אלא שבשונה מארצות הברית, הסובלת גם היא מהתחרות הסינית, ישראל חשופה לביקורת גדולה יותר בזירה הבין־לאומית על

42 "יצרני המל"טים הישראלים חוששים מהאיום הסיני", **דה־מרקר**, מהדורה דיגיטלית, 10 בפברואר 2018, https://www.themarker.com/wallstreet/1.5806899.

השימוש המבצעי שהיא עושה במל"טים, דבר שעלול להשפיע גם הוא על יכולות הייצור והייצוא שלה.[43] זאת ועוד, בניגוד לארצות הברית, שבתגובה לתחרות מצד סין וישראל יכולה להרחיב את ייצוא המל"טים שלה למדינות כמו ערב הסעודית,[44] שוק הייצוא של ישראל מוגבל יותר, שכן קיימת קבוצה של מדינות שהיא אינה מקיימת איתן קשרים דיפלומטיים רשמיים, ועל כן ייצוא ביטחוני אליהן עשוי להיות בעייתי יחסית למתחרותיה.

השפעה נוספת על יכולת הייצוא של ישראל נובעת מהסכמים בתחום הייצוא הביטחוני, המשפיעים במיוחד על ייצוא מל"טים. הסכם בולט כזה הוא משטר הפיקוח על טכנולוגיות טילים, שבמסגרתו המדינות החברות מתאמות ביניהן את מדיניות הפיקוח על הייצוא בתחום זה.[45] ישראל קיבלה על עצמה לפעול בהתאם להסכם זה וליישם אותו במדינות שאליהן היא מייצאת מאז שנת 1991.[46] יחד עם זאת, כמו בהסכמים בין־לאומיים אחרים, ישראל מתקשה להשפיע על העדכונים המתבצעים בהסכם מעת לעת, דבר המשפיע מבחינה מסחרית עליה יותר מאשר על ארצות הברית או על מדינות שמלכתחילה אינן חתומות על ההסכם או אינן מבצעות אותו לפרטיו.

הן האתגרים הביטחוניים והן האתגרים המסחריים מחייבים את ישראל לעדכן את מדיניותה בתחום המל"טים, במטרה להיערך בצורה מתאימה נוכח הסיכונים הטמונים בהפעלה עוינת של מל"טים על ידי אויביה, וכן כדי לשמר את יכולתה לייצא כלי טיס בלתי מאוישים למדינות שונות ולהפיק את התועלת הכלכלית והדיפלומטית הטמונה בכך.

המלצות לישראל

לאור השינויים שתוארו לעיל, ישראל חייבת לכלול בין האיומים האווירים האפשריים עליה הפעלה עוינת של מל"טים, רחפנים או כלים מאולתרים מתוך אחת המדינות הנחשבות לאויבותיה. הדבר כבר קרה בעבר, כאשר מל"טים שוגרו כלפיה מלבנון על ידי חזבאללה ומסוריה בהפעלה איראנית. כמו כן, עליה להיערך ליירוט ולתגובה גם במקרים שבהם יופעלו נגדה כלים כאלה מבלי שגורם כשלהו יקבל על עצמו

43 Damien Gayle, "Charges Dropped over Protest at Israeli Military Drones Factory in UK", *The Guardian*, Digital Edition, November 23, 2017, https://www.theguardian.com/world/2017/nov/23/charges-dropped-protest-israeli-military-drones-factory-uk-uav-engines.

44 דן ארקין, "ארה"ב תספק מל"טים חמושים בינוניים לסעודיה, קוריאה הדרומית ויפן", *ISRAEL DEFENSE*, 26 במארס 2018, http://www.israeldefense.com/he/node/33573.

45 MTCR Website, http://mtcr.info/ .

46 אתר האינטרנט של אגף הפיקוח על הייצוא הביטחוני של משרד הביטחון: http://www.exportctrl.mod.gov.il/Hakika/Pages/MTCR.aspx.

את האחריות לשיגורם. בנוסף לכך, על ישראל להיות מודעת לסיכונים הכרוכים בתפוצת המל"טים ולהיערך טכנולוגית ומבצעית להתמודדות גם עם איומים קטנים ובינוניים באמצעות כלי טיס בלתי מאוישים שעשויים להיות מופעלים בקבוצה או בנחיל.

על ישראל להשקיע מאמצים מודיעיניים במטרה לעקוב אחר תפוצת מל"טים בעולם, ובכלל זה אחר מל"טים חמושים תוצרת סין, איראן ומדינות נוספות שיופיעו בזירה המזרח תיכונית. בנוסף, עליה לעקוב אחרי מוצרי ורכיבי מדף, וכן אחר טכנולוגיות לשימוש דואלי שעשויות לסייע בייצור מערכות טיס בלתי מאוישות מאולתרות. הבנה מעמיקה של תמונת המל"טים העולמית, כמו גם מעקב אחר ייצוא או זליגת אמצעים בין מדינות ובין ארגונים תת־מדינתיים, מהווים נדבך חשוב בהיערכות להגנה על שמי המדינה ועל כוחותיה של ישראל בשגרה ובלחימה.

במקביל, על ישראל להשקיע בפיתוח אמצעי סייבר ול"א, בנוסף להתאמת מערכות ההגנה האווירית לאיומים מצד כלי טיס בלתי מאוישים. זאת, במטרה ליצור מענים זולים יותר מאשר יירוט באמצעות טילים, כמו, למשל, שיבוש או השבתה מרחוק של מל"טים עוינים. כמו כן, נחוצים לישראל אמצעים להתמודדות אפקטיבית עם ריבוי איומים בקנה מידה רחב, ובכלל זה עם קבוצות מל"טים ורחפנים או נחילים שלהם.

על ישראל לצאת מתוך הנחה שמדובר במגמה שתמשיך להשפיע על הזירה הבין־לאומית ואף עתידה להתחזק. על רקע זה מומלץ כי מדינת ישראל תעודד את התעשיות הביטחוניות להשקיע בפיתוח פתרונות בתחום ההגנה האווירית נגד כלי טיס בלתי מאוישים מסדרי גודל ומסוגים שונים. דוגמה לפיתוח כזה ניתן לראות בעיסקה שחתמה "רפאל" עם בריטניה לייצוא של מערכות נגד רחפנים.[47] תחום זה עשוי להפוך לאפיק ייצוא חשוב ומרכזי בפני עצמו, שייתן מענה לאתגר העולמי המתרחב, וכן יסייע בהגנה על ביטחונה של ישראל.

השקעה בפיתוח אמצעים להגנה נגד כלי טיס בלתי מאוישים היא בעלת חשיבות גדולה גם לאור השימוש האזרחי במל"טים, שעתיד להתרחב מאוד בעשורים הבאים. התפתחות כזו תציב אתגרים לא רק בתחום ההגנה האווירית, אלא גם בפני ניהול התעבורה האווירית בכל מדינה שתרצה לדבוק בקדמה ולאפשר הפעלת מערכות כאלו בשטחה לצרכים מדיניים, מסחריים ופרטיים.

במטרה לשמר את הייצוא, המהווה גורם מסייע להמשך פיתוחם של אמצעים חדשים, על ישראל להציב בקדמת הבמה יתרונות נוספים שלה מלבד הטכנולוגיה עצמה. במסגרת זו, ישראל יכולה להציע למדינות שונות גם שירותים, ויותר מכך ידע

47 Yuval Azulai, "Rafael to Sell 6 Anti-Drone Systems to UK for $20m", *Globes*, Digital Edition, August 16, 2018, https://en.globes.co.il/en/article-rafael-to-sell-6-anti-drone-systems-to-uk-1001250393.

המבוסס על ניסיון מבצעי וכוח אדם איכותי, כפי שעשתה בעיסקת המל"טים עם גרמניה. עיסקה זו כוללת חכירה (בשונה מרכישה) למשך תשע שנים של מל"טים ישראליים מסוג "הרון (Heron TP) " תוצרת התעשייה האווירית עבור כוחות הצבא הגרמני. במסגרת זו גם יוכשרו צוותים גרמניים בארץ להפעלת המל"טים.[48] שיטה זו תאפשר לשמר שותפויות אסטרטגיות ואף לכונן שותפויות חדשות.

דוגמה נוספת ליחסים אסטרטגיים של ישראל עם מדינה גדולה, המושפעים בצורה משמעותית מאוד מייצוא של טכנולוגיה צבאית ובתוכה מל"טים מתקדמים, הם היחסים עם הודו.[49] יחסים אלה מעידים גם הם כי לייצוא מל"טים חשיבות רבה יותר מאשר עצם ההכנסה הכספית שהדבר יוצר למדינת ישראל. לפיכך, על ישראל להמשיך להשקיע בחדשנות טכנולוגית וביכולת לתת מענה לצרכים מבצעיים וטכנולוגיים של לקוחותיה, תוך ייצור וייצוא בלוחות זמנים קצרים יחסית. זאת, כדי לשמר לעצמה יתרונות אחרים מאשר מחירי המוצרים שלה, שאינם זולים ביחס לסין או למתחרות אחרות. כמו כן, עליה לבחון אפשרות לספק תמיכה ולחלוק ידע מבצעי כחלק מהשירות שהיא נותנת ללקוחותיה – יתרון שחלק ניכר מן המתחרות האחרות אינן יכולות להציע.

חרף התחרות הגוברת בזירה הבין־לאומית, הנובעת מהצטרפותן של שחקניות חדשות לשוק, והמאמצים הגוברים של שחקניות ותיקות דוגמת ארצות הברית להגדיל את מכירותיהן, על ישראל להקפיד גם להבא לברור את המדינות והמשטרים שהיא מייצאת אליהם טכנולוגיות צבאיות, ובתוכן מל"טים, כפי שעשתה עד היום באמצעות אגף הפיקוח על הייצוא של משרד הביטחון (אפ"י). עליה להקפיד על הדבר גם במצב של כניסת אמצעים חדשים לשווקים, דוגמת רחפנים אזרחיים, שמספקים מענה לחלק מהצרכים הצבאיים הקיימים כיום ואינם מחייבים הפעלת מל"טים צבאיים, או אפילו מהווים נשק בידי ארגוני טרור.

לאור התחרות הקשה בתחום המל"טים הצבאיים והביקורת הנוקבת שתחום זה גורר עימו מצד אחד, ולאור הפוטנציאל הכלכלי העצום הטמון בשוק המל"טים האזרחי מצד שני,[50] מן הראוי שישראל תשקול להגדיל את השקעות המדינה בפיתוח ובייצור טכנולוגיות לצרכים אזרחיים. זאת, על בסיס היתרון היחסי והידע שהיא צברה בתחום המל"טים הצבאיים. בכך תתמוך המדינה ביצירת אפיק ייצוא מרכזי

48 Assaf Uni, "Bundestag Approves €1b Israeli UAV Deal for German Army", *Globes*, Digital Edition, June 13, 2018, https://en.globes.co.il/en/article-bundestag-approves-%E2%82%AC1b-israeli-uav-deal-for-german-army-1001241320.

49 Manu Pubby, "India all Set to get Missile Armed Drones from Israel", *The Economist Times*, July 14, 2018, https://economictimes.indiatimes.com/news/defence/india-all-set-to-get-missile-armed-drones-from-israel/articleshow/57980098.cms.

50 Diamond, "Global Drone Market Expected to Surpass $22B by 2022".

נוסף, שעשוי להוות גם הוא מקור הכנסה מרכזי ותמריץ לשותפויות אסטרטגיות עם מדינות נוספות.

על ישראל להמשיך לעקוב אחר המתרחש בתחום המל"טים בזירה הבין־לאומית, בעיקר בגופים השונים של האו"ם, ולנסות למנוע בדרכים דיפלומטיות מהלכים שיַצֲרו את צעדיה בתחום זה. כמו כן, על ישראל לשקול את הגברת רמת השקיפות שלה בנוגע לחלק מהשימושים שהיא עושה במל"טים, במטרה למנוע ביקורת בין־לאומית ואת השפעותיה, ובתוכן ניסיונות אפשריים של מדינות שונות באו"ם להגביל את השימוש במל"טים תוקפים ובתוך כך ופגיעה בייצוא מישראל מסיבות פוליטיות. הגברת השקיפות תאפשר לאשרר ולתקף את העובדה שישראל עושה שימוש במל"טים בהתאם לנורמות המקובלות והדין הבין־לאומי ולמנוע התקפות עליה מצד ארגוני זכויות אדם ומדינות שונות. הגברת השקיפות גם עשויה לסייע להציג באור חיובי של היכולות הישראליות, דבר שיהיה בו כדי להפוך אותן למוצר נדרש גם בקרב מדינות נוספות ברחבי העולם.

סיכום

ישראל היא אחת מיצואניות המל"טים המובילות בעולם וגם אחת המשתמשות הבולטות במערכות אלו, ויש לה ניסיון מבצעי ארוך שנים בהפעלתן. בשנים האחרונות ניצבת ישראל בפני אתגרים הנובעים משינויים בתפוצת המל"טים העולמית, הן בתחום הטכנולוגי והן כתוצאה מכניסת שחקניות חדשות לשוק ומשינוי מדיניות של שחקניות ותיקות. התפתחויות אלו מאתגרות מאוד את ישראל מבחינה מסחרית. נוסף לכך האתגר הביטחוני, הנובע מעצם ההתרחבות של תפוצת המל"טים בעולם וכן מאיומים אווירים חדשים כתוצאה משימוש בכלי טיס בלתי מאוישים בעלי יכולות חדישות.

המאמר תיאר את הדומיננטיות הישראלית בתחום המל"טים, בעיקר מראשית שנות האלפיים, וכן את השינויים המתחוללים בעשור האחרון בתפוצת המל"טים ברחבי העולם ובדפוסי השימוש בהם. במסגרת שינויים אלה הצביע המאמר על הפיכתה של סין ליצואנית מל"טים מרכזית, שמדיניות הייצוא שלה מתירנית, ובכך היא גורמת לשינויים בעלי השפעות מרחיקות לכת על כלל הזירה הבין־לאומית, ובתוכה גם על ישראל. בנוסף, תיאר המאמר את האתגרים שמציבים המל"טים האיראניים והשימוש הנרחב במל"טים בזירה המזרח תיכונית הבלתי יציבה. לצד זאת, סקר המאמר את ההשפעות המסחריות הנובעות מכניסתן של שחקניות חדשות לתחום כלי הטיס הבלתי מאוישים ומשינוי המדיניות של שחקניות ותיקות בתחום זה, דוגמת ארצות הברית.

המאמר קובע כי רצוי וניתן להתאים את המדיניות הישראלית לשינויים המתחוללים בתחום המל"טים. במסגרת זו הוא מציע שורה של צעדים: מעקב

מודיעיני אחר תפוצת מל"טים ורכיביהם בעולם כולו; פיתוח אמצעי נגד מתחום הסייבר והל"א, בנוסף להתאמה ושיפור של מערכות ההגנה האווירית של ישראל בהתאם לאיומים החדשים. כמו כן ממליץ המאמר לישראל להגביר את רמת השקיפות שלה בתחום המל"טים, במקביל להמשך הקפדה על ברירת הגורמים להם היא מייצאת אמל"ח. בנוסף ממליץ המאמר שישראל תבחן דרכים נוספות לשמר, ואף להגביר, את הייצוא הישראלי של כלי טיס בלתי מאוישים, תוך מקסום ההישגים האסטרטגיים שייצוא כזה מאפשר, ובמקביל לבחון את האפשרות לעודד את התעשיות הישראליות לפתח מל"טים לצרכים אזרחיים וכן אמצעי הגנה מפני מל"טים. זאת, בשל הפוטנציאל הכלכלי העצום הטמון בשווקים אלה וכחלק מהמטרה של שמירת חוסנה וביטחונה של מדינת ישראל.

הרצאות מאת

ראי"ל גדי אייזנקוט
ופרופסור יואל רונן

ב־24 באוקטובר 2018

בכנס שנערך בשיתוף המכון למחקרי ביטחון לאומי והמרכז האקדמי שערי מדע ומשפטים בהוד השרון לרגל השקת המזכר "רגולציה במרחב הסייבר" שנכתב על ידי ד"ר אל"ם (מיל') גבי סיבוני ועידו סיון־סבי‌ליה

הפעילות במרחב הסייבר בראי המשפט הבין־לאומי

יעל רונן

הדיון ברגולציה פנים־מדינתית של מרחב הסייבר שם את הדגש על הגנת מרחב זה. לעומת זאת, השיח בנושא הסייבר במשפט הבין־לאומי הינו היפוך גמור לכך, וזאת בשלושה מובנים: ראשית, המשפט הבין־לאומי עוסק בהסדרת יחסים בין־מדינתיים; שנית, רגולציה היא פעולת ארגון, פיקוח ואכיפה, שמטרתה היא לכפות באופן חוקי כללי התנהגות מחייבים. הנחת היסוד של הרגולציה היא קיומם של כללי התנהגות כאלה. לעומת זאת, המשפט הבין־לאומי נמצא עדיין בשלב של ניסיון לברר מהם כללי ההתנהגות הקיימים והראויים במרחב הסייבר, כלומר, ניסיון לברר מה מותר ומה אסור לעשות בתחום זה; שלישית, בעוד שהרגולציה עוסקת ב**הגנת** מרחב הסייבר, המשפט הבין־לאומי מתמקד ב**השלכות** של התקפות סייבר על הביטחון.

מרחב הסייבר מאתגר את המשפט הבין־לאומי בכמה היבטים: ראשית, המשפט הבין־לאומי, על כל ענפיו, עוסק בעיקר בהסדרת היחסים הקשורים לגופים מוחשיים (גוף, נכסים, קרקע). לעומתו, מרחב הסייבר אינו מוחשי. כתוצאה מכך מתעוררת השאלה אם הנורמות הקיימות במשפט הבין־לאומי מתאימות למרחב זה, או שיש צורך בעיצוב נורמות חדשות; שנית, המשפט הבין־לאומי מבוסס באופן ספציפי על חלוקה טריטוריאלית: הזירה העולמית מחולקת לשטחי אדמה – מדינות – ודגש רב מושם על חלוקת הסמכויות והזכויות – ריבונות. לעומת זאת, עולם הסייבר הינו במהותו חוצה גבולות; שלישית, המשפט הבין־לאומי מבוסס באופן מסורתי על עליונות המדינות כשחקניות בזירה הבין־לאומית: להן יש זכויות, והן נושאות באחריות. נדמה שבתחום הסייבר המדינות אינן השחקניות המרכזיות.

פרופסור יעל רונן היא פרופסור חבר במרכז האקדמי שערי מדע ומשפט בהוד השרון ועמיתת מחקר במרכז מינרבה לזכויות אדם, האוניברסיטה העברית בירושלים.

מאמר זה מתבסס על הרצאה בכנס של המכון למחקרי ביטחון לאומי, בשיתוף עם המרכז האקדמי שערי מדע ומשפט, שנערך ב־24 באוקטובר 2018 לרגל השקת המזכר "רגולציה במרחב הסייבר", שנכתב על ידי ד"ר אל"ם (מיל') גבי סיבוני ועידו סיון־סביליה

הבדלים אלה מעוררים שאלה בסיסית: האם המשפט הבין־לאומי חל במרחב הסייבר? העיסוק בשאלה זאת מתקיים בעיקר בזירה האקדמית. מדריך טאלין הראשון, מסמך שניסחה קבוצת אנשי אקדמיה והתפרסם בשנת 2013, התמקד בשאלה כיצד ניתן להחיל את המשפט הבין־לאומי על מרחב הסייבר, בראש ובראשונה בהקשר של פעולות המהוות הפרה של האיסור על שימוש בכוח ושל הזכות להגנה עצמית, או פעולות המתרחשות במהלך סכסוך מזוין. מדריך טאלין השני מ־2017 הרחיב את הדיון בסוגיה זאת לשאלת התחולה של המשפט הבין־לאומי על פעולות שאינן מגיעות לכדי שימוש בכוח או למצב של סכסוך מזוין בזירה המדינית. העיסוק של מדינות בתחולת המשפט הבין־לאומי במרחב הסייבר נותר מצומצם. אחת הסיבות לכך היא שהטכנולוגיה מאפשרת חדירה לתחומים רגישים, שבהם ממשלות נזהרות מלהתבטא. למרות זאת, יש כיום קונצנזוס שהמשפט הבין־לאומי חל גם על מרחב הסייבר. אחת ההתפתחויות הבולטות בהקשר זה היא ההסכמה שהושגה ב־2015 במסגרת קבוצת מומחים ממשלתיים שהתכנסה באו"ם, לפיה מגילת האו"ם חלה במלואה גם במרחב הסייבר. הקבוצה כללה, בין היתר, מומחים מארצות הברית, בריטניה, רוסיה וסין, שהן השחקניות הראשיות בזירה הבין־לאומית בתחום זה. להסכמה שהושגה ביניהם יש משמעויות שונות, שכמה מהן יפורטו להלן.

מגילת האו"ם מעגנת את האיסור להשתמש או לאיים להשתמש בכוח נגד העצמאות או השלמות הטריטוריאלית של מדינות, וקובעת כי פעולה כזאת תהיה חוקית רק כהגנה עצמית, או בהסמכה של מועצת הביטחון ובנסיבות מיוחדות. השאלה היא, כמובן, מה ייחשב "שימוש בכוח" כשמדובר בפעולות סייבר. פעולת סייבר בהקשר זה היא פעולה נגד מערכת מחשבים במטרה לאסוף, להחדיר, לשנות או לשבש נתונים בדרכים אחרות, או כדי לעשות מניפולציה בפעולה של המערכת. יש הסכמה רחבה שפעולת סייבר יכולה להיחשב כ"שימוש בכוח" או כ"התקפה מזוינת", אם תוצאותיה הצפויות יהיו מסוג בר־השוואה לאלו של התקפה קינטית, כלומר גרימת מוות או פציעה של אנשים ופגיעה ברכוש. למשל, אם פעולת סייבר תביא להסטת רכבת מפסי המסילה או לפריצת סכר מים באזור מיושב, היא תיחשב להתקפה מזוינת, בדיוק כמו הפצצת המסילה מהאוויר.

דוגמה להתקפה מסוג זה היא פרשת Stuxnet. ב־2010 חדר פוגען ("סטוקסנט") למערכות שעליהן התבססו הצנטריפוגות באחד המתקנים הגרעיניים של איראן. תולעת שהוחדרה למערכות במתקן הגרעיני גרמה לצנטריפוגות להסתובב, לצאת משליטה ולהיהרס. זו אחת הפעמים הראשונות שבהן נגרם הרס פיזי של רכוש על ידי פעילות סייבר. הפעולה הצביעה על הפוטנציאל של מרחב הסייבר כאמצעי להרס ולגרימת נזק ליריב, בדיוק כמו התקפה באמצעים קונבנציונליים.

לסיווג של מעשה כ"התקפה מזוינת" יש חשיבות, כי בהתקיים נסיבות מסוימות, "התקפה מזוינת" מקנה למדינה המותקפת זכות להגנה עצמית. אם פעולת סייבר יכולה להיחשב "התקפה מזוינת", אזי תיתכן גם תגובה כוחנית לה. לפי גישה זאת, ההתקפה על איראן באמצעות תולעת "סטוקסנט" עשויה הייתה להקנות לה זכות להגנה עצמית. שאלה חשובה המתעוררת בהקשר זה היא כלפי מי קיימת זכות ההגנה העצמית. גורמים באיראן ובמדינות נוספות ייחסו את התקפת "סטוקסנט" לארצות הברית ולישראל, אף שלא הוצגו ראיות של ממש למעורבות של מדינה מסוימת בייצור הפוגען או בהפצתו. שאלה נוספת היא איזו פעולת נגד תיחשב חיונית ופרופורציונלית, כנדרש על מנת שניתן יהיה לראותה כחוקית במסגרת זכות ההגנה העצמית.

הסוגיה המורכבת ביותר, לגביה עדיין אין קונצנזוס, קשורה לאותם מצבים שבהם פעולת סייבר גורמת פגיעה קשה ומשמעותית, אך ללא גרימת נזק פיזי לאדם או לרכוש. הפרשנות המקובלת היא שאיסוף מידע, גניבת מידע ואפילו השמדת מידע או שינויו אינם "התקפה מזוינת" בפני עצמם. כשאין מדובר ב"התקפה מזוינת", גם לא ניתן להגיב עליה במסגרת ההגנה העצמית. עם זאת, השפעתן המזיקה של פעולות כאלו יכולה להיות משמעותית מאוד. דוגמה אפשרית לכך היא התקפה על המערכת הכלכלית והפיננסית, למשל פעולת סייבר על הבורסה בניו יורק, שתגרום לה להתרסק בשל פגיעה באמינות המידע ובתשתית המחשבים. השאלה המתעוררת בהקשר זה היא אם מדובר בנזק כלכלי גרידא, או שהתוצאות הקטסטרופליות של הפעולה מצדיקות את התיוג שלה כ"התקפה מזוינת".

פעולת סייבר אחת כזאת עוררה את העניין הבין־לאומי בתחולתו של המשפט הבין־לאומי על מרחב הסייבר: באפריל 2007 הודיעה ממשלת אסטוניה על כוונתה להעביר אנדרטת זיכרון למלחמת העולם השנייה ממרכז עיר הבירה טאלין לבית קברות צבאי בפרברי העיר. בתגובה לכך החלו הפגנות אלימות של אזרחים אסטוניים ממוצא אתני רוסי. בהמשך בוצעו לאורך כחודש ימים התקפות על תשתיות אינטרנט ציבוריות וכלכליות באסטוניה. האינטרנט הוא כלי שימושי משמעותי ביותר באסטוניה: 95 אחוזים מהפעילות הבנקאית במדינה מנוהלת באופן דיגיטלי ו־98 אחוזים משטח המדינה היה מרושת, עד כדי כך שנאמר על אסטוניה כי האינטרנט חשוב בה כמעט כמו מים זורמים. ההתקפות על תשתיות האינטרנט באסטוניה כללו את האתרים של נשיא המדינה, ראש הממשלה, הפרלמנט, מפלגות, בנקים, אמצעי התקשורת ועוד. השפעתן הייתה משמעותית: שני הבנקים המרכזיים במדינה שותקו למשך מספר ימים, וחלק מסוכנויות החדשות המרכזיות נפגעו. קווי החירום במדינה נותקו למשך שעה, התקשורת הפרטית והציבורית נפגעה, ובעיקר נפגע האמון בכלכלת המדינה. מקובל לייחס את ההתקפות לרוסיה, וחלקן אכן בוצעו ממחשבים בשליטת מוסדות ממשלתיים רוסיים. עם זאת, עקבות

התוקפים הובילו ל־177 מדינות נוספות, ורוב ההתקפות בוצעו ממחשבים בעלי כתובת פרטית.

פוליטיקאים אסטונים השוו את ההתקפות לפלישה ולפעילות צבאית קונבנציונלית, אך הנזק הממשי שלהן היה מזערי, ובעיקרו כלכלי: לא הייתה פגיעה ברכוש או בנפש, חיילים לא נשלחו לחזית, ולא נעשה שימוש בתחמושת קונבנציונלית. מצד שני, הייתה פגיעה בתשתיות הכלכליות הבסיסיות של המדינה, דבר שהיווה פגיעה אנושה ביכולת התפקוד שלה.

קביעה אפשרית שמדינה שהייתה קורבן לפגיעה משמעותית באמצעות סייבר לא תוכל לנקוט צעדי הגנה עצמית בתגובה לכך, היא בעייתית מאוד. התעלמות מהתפתחויות טכנולוגיות עלולה להוביל לתוצאות אבסורדיות, וספק אם מדינות יצייתו לכלל שאינו עולה בקנה אחד עם צרכים מציאותיים. לכן, יש כיום מידה רבה של קונצנזוס בקרב אנשי האקדמיה שפעולות סייבר עלולות להוביל לתוצאות חמורות כל כך, עד שיהיה מוצדק להגדירן כ"התקפה מזוינת". השאלה היא מהן אמות המידה לכך. בתשובה לכך ניתן לבחון היבטים שונים, כמו השלכות על אינטרסים לאומיים חיוניים, מיידיות ההתממשות של התוצאות ומידת הישירות, החודרניות או המעורבות המדינתית.

עיקרון נוסף המעוגן במגילת האו"ם הוא האיסור להתערב בענייניהן הפנימיים של מדינות. איסור זה אינו מתייחס לאמצעים ספציפיים, ולפיכך כולל גם התערבות באמצעות הסייבר. האיסור על התערבות בעניינים פנימיים אינו בולט בדרך כלל בשיח הבין־לאומי, כי כאשר יש התקפה קונבנציונלית על מדינה, ה"התערבות" היא עניין שולי יחסית. דווקא כאשר אין שימוש באלימות, אלא נעשית מניפולציה חברתית או כלכלית, איסור ההתערבות הופך למרכזי.

ככלל, מעשה ייחשב "התערבות" כאשר יש כפייה או לחץ, מפורש או אחר. למשל, ריגול ואיסוף נתונים ממחשבים במדינה זרה אינם בגדר התערבות אסורה, כי אף שיש בהם מרכיב של חדירה לרשת מחשבים זרה, כשלעצמם הם אינם מהווים כפייה או הפעלת לחץ על אותה מדינה. המצב שונה כאשר יש מניפולציה של תוצאות בחירות או של דעת קהל ערב בחירות באמצעות מחשבים. יש תחומים שבהם המחלוקת רבה עוד יותר: למשל, מה דין פגיעה באמצעות אתרי תוכן בקמפיין פוליטי של מפלגה מסוימת, או יצירת פעילות פיקטיבית שמטרתה היא הטיית דעת קהל? אפשר לטעון שבכל התחומים האלה יש התערבות בליבה של ריבונות המדינה – אמנם לא מבחינה צבאית, אלא מבחינה חברתית ופוליטית – שהשפעתה יכולה להיות חמורה מאוד. אין ספק שמעשים מסוג זה אסורים; מה שעדיין מהווה שאלה פתוחה היא איך רשאית המדינה הנפגעת להגיב עליהם.

מרחב הסייבר יוצר דילמות נוספות למשפט הבין־לאומי. אחת מהן קשורה למגבלות על שימוש בסייבר הנובעות מכללי המשפט ההומניטרי. דילמה נוספת

קשורה לסיכונים שהשימוש בסייבר מציב בפני הגנה על זכויות אדם. בתחומים אלה ונוספים נמצא המשפט הבין־לאומי רק בראשית דרכו. הצורך לעבד ולגבש נורמות בעקבות התפתחויות טכנולוגיות אינו ייחודי למשפט הבין־לאומי. עם זאת, אין ספק שמושכלות היסוד המשפטיות של המשפט הבין־לאומי שרירות וקיימות גם במרחב הסייבר.

הסייבר בצה"ל

גדי איזנקוט

מבוא

הסייבר הוא התחום שהתקדם בצורה המשמעותית ביותר בצה"ל בעשור האחרון. בתקופה זו הפך הסייבר לנושא מרכזי ולתחום עיסוק נרחב בצה"ל בכל מה שנוגע לפיתוח הידע וליישומו. מרחב הסייבר והרגולציה הקשורה בו הם בעלי חשיבות רבה גם בצה"ל, וזאת בשל מספר סיבות: ראשית, הם נוגעים לשיח הציבורי העוסק בפיתוח הידע ובהסדרת היחסים בין המדינה ובין המערכת הכלכלית בנושא הסייבר הלאומי וחוסנו, ובחיזוק יכולתה של המדינה לקיים המשכיות תפקודית בכל מצבי החירום וגם תחת מתקפות של אויבים ויריבים; שנית, למרחב הסייבר יש חשיבות רבה גם בהקשר הבין־לאומי. מדינת ישראל רואה עצמה בחזית העולמית של פיתוח הידע בתחום הסייבר, ומשכָּך, היא תוכל לתרום לפיתוח הגנה כוללת על מרחב הסייבר גם במדינות אחרות.

צה"ל עוסק באופן אינטנסיבי בתחום הסייבר ומקצה לו משאבים רבים מאוד. עשייתו זאת נשענת על שלושה נדבכים: החשוב ביותר הוא הגנת מרחב הסייבר הצבאי וסיוע להגנת מרחב הסייבר האזרחי. צה"ל משקיע משאבים רבים בביצור ההגנה בסייבר; הנדבך השני נוגע ליכולת לאסוף מודיעין במרחב הסייבר. ההתפתחות הטכנולוגית הביאה לכך שיותר ויותר מידע מודיעיני חיוני הינו דיגיטלי. כתוצאה מכך מתקיימים מאמצי איסוף טכנולוגי רבים ביותר במרחב זה; הנדבך השלישי הוא התקיפה בסייבר, כלומר היכולת להשיג הישגים מבצעיים של ממש באמצעות פעולות במרחב הסייבר. צה"ל משלב את כלל הפעילויות שתוארו לעיל בעשייתו המבצעית בהיקף רחב ביותר.

רב־אלוף גדי איזנקוט הוא ראש המטה הכללי של צה"ל.

מאמר זה מתבסס על הרצאתו בנושא הסייבר בצה"ל בכנס של המכון למחקרי ביטחון לאומי, בשיתוף עם המרכז האקדמי שערי מדע ומשפט בהוד השרון, שנערך ב־24 באוקטובר 2018 לרגל השקת המזכר "רגולציה במרחב הסייבר" שנכתב על ידי ד"ר אל"ם (מיל') גבי סיבוני ועידו סיון־סביליה.

הסייבר כחלק ממעגלי האיום

צה"ל הוא צבא טכנולוגי מאוד, בוודאי בהשוואה לחלק מאויביה של מדינת ישראל, וההגנה נתפסת אצלו כחיונית ליכולתו התפקודית. מאז הקמת המדינה התמודד צה"ל עם שלושה מעגלי איום מרכזיים, שבשנים האחרונות הצטרף אליהם מעגל רביעי. הראשון בשלושת המעגלים הינו האיום הקונבנציונלי – איום מצד מדינות שיש להן צבאות עם יכולות מגוונות, בהם כוחות שריון, חי"ר וארטילריה, המסוגלים לבצע תמרון יבשתי, ולצידם כוחות אווריים התקפיים, כוחות הגנה אווירית לשיבוש פעילותנו ואף יכולות ימיות. כל אלה נבנו בעיקר למטרות התקפיות, כדי לכבוש חלקים ממדינת ישראל.

המעגל השני הוא האיום הבלתי קונבנציונלי, המלווה גם הוא את מדינת ישראל מזה שנים רבות. עיקרו של איום זה נוגע לניסיונות של גורמים שונים באזור לפתח יכולת גרעינית צבאית התקפית. ניתן לראות זאת בחזון האיראני לפתח נשק גרעיני ובניסיונה של סוריה לפתח נשק כזה, שסוכל בשנת 2007. יתכן שבעתיד יתגלו ניסיונות נוספים מסוג זה. לצד הנשק הגרעיני, אחדות ממדינות הטבעת סביב מדינת ישראל הן בעלות יכולות להפעיל נשק כימי. יכולת כזאת הייתה, לדוגמה, לסוריה, ולמרות שהיא צומצמה משמעותית לפני כחמש שנים, היא הופעלה מספר פעמים במהלך מלחמת האזרחים במדינה.

מעגל האיומים השלישי שמעסיק את צה"ל מאוד בעשור האחרון, וימשיך להעסיק אותו בעתיד הנראה לעין, הוא האיום התת־קונבנציונלי של ארגוני הטרור והגרילה הפועלים נגד ישראל. איום זה כולל, בין השאר, אש תלולת מסלול בהיקפים נרחבים, תוך הגדלת העוצמה והדיוק של הירי, ופיתוח יכולות פעולה בתוך התת־קרקעי, הן בהקשר ההגנתי ליצירת שרידות והן בהקשר ההתקפי במטרה לחדור לתוך מדינת ישראל לצורך ביצוע פעולות טרור התקפיות נגד יישובים. לצד אלה, צה"ל ושאר ארגוני הביטחון מתמודדים עם איומים של ארגוני ג'יהאד ועם פיגועי השראה של יחידים. איום הטרור קיים בצפון המדינה, בדרומה, ביהודה ושומרון וגם כלפי נכסים ישראליים ויהודיים בחו"ל.

המעגל הרביעי הוא איום הסייבר. זהו איום חדש יחסית, שגבר מאוד בעשור האחרון וצפוי לגדול באופן משמעותי בשנים הקרובות. עיקרו הוא איום על היכולות התפקודיות של מדינת ישראל – הן האזרחיות והן הצבאיות. לאורך שנים התמקד צה"ל בפיתוח שלושה ממדי לחימה: היבשתי, האווירי והימי. בשנים אחרונות הוא החל לפתח ממד לחימה נוסף – ממד הסייבר – מתוך הבנה שיש להתייחס לממד זה בצורה רחבה ומקיפה, תוך היערכות ברמה הלאומית וברמה הביטחונית גם יחד. בתהליך פיתוח הידע בוחן צה"ל כיצד ניתן לפעול כדי להגן על מרחב הסייבר הצבאי, כמו גם על מרחב הסייבר המדינתי. זאת, מתוך הבנה שמוטלת על צה"ל חובה להגן על התשתיות הביטחוניות, על מתקנים חיוניים, על יכולות כלכליות,

על בתי חולים, על שדות תעופה ועל המגזר הבנקאי במדינת ישראל, לצד הגנה על היכולות הצבאיות כדי לאפשר לצבא תפקוד מיטבי בהפעלת מערכות הפיקוד והשליטה שלו. יכולות אלו נשענות, כידוע, על אמצעים מתקדמים ביותר, ובהם מערכות נשק ומודיעין, יכולות אוויריות ויכולות ימיות.

התארגנות צה"ל לפעולה בסייבר

העיסוק המשמעותי בתחום הסייבר בצה"ל התחיל לפני כעשור. בשנים האחרונות התקיים בצה"ל מֶחשב מעמיק סביב הדרך הנכונה לפיתוחו ולארגונו של תחום זה. צה"ל אינו הצבא היחיד הפועל כך. מדינות נוספות בוחנות גם הן את הנושא: חשיבה עמוקה התקיימה בשאלת הסייבר בצבא האמריקאי, שבעקבותיה הייתה למידה הדדית בין ארצות הברית לישראל לגבי הדרך המיטבית לארגון העשייה הצבאית במרחב הסייבר. הדיון במסגרת זו נסב בעיקר על הדרך לארגן את שלושת מרחבי העשייה במרחב זה: יכולת ההגנה, יכולת האיסוף ויכולת ההתקפה.

תהליך הלמידה החל בצה"ל לפני כארבע שנים, ובמסגרתו התקיימו למידה ועבודת מטה שנמשכו כשנה. השאלה שהועמדה על הפרק הייתה: כיצד נכון להתארגן? נבחנו מספר חלופות, שחלקן היו קפיצת מדרגה ממשית, כמו ארגון כלל יכולות הסייבר של צה"ל תחת מפקדה אחת. חלופות אחרות היו שמרניות יותר. לאור העובדה שצה"ל מתמודד באופן שוטף ואינטנסיבי עם קשת רחבה של איומים, התגבשה לבסוף ההבנה שלא נכון יהיה לנקוט מהלך שהוא בגדר קפיצת מדרגה, תוך ניסוי ותעייה במרחב פעולה חיוני ביותר, במיוחד במקרה של הסלמה ביטחונית מהירה. לאור זאת, החלופה שנבחרה הייתה התקדמות איטית וארגון פעילות הסייבר בצה"ל באופן מדוד. כפועל יוצא מכך הורחבה הסמכות של אגף התקשוב, שקיבל עליו את האחריות הכוללת להגנה בסייבר, ושמו שונה לאגף התקשוב וההגנה בסייבר. במסגרת זו הוקמה באגף חטיבת הגנת הסייבר, המשלבת בתוכה אנשים בעלי רקע התקפי. במקביל, הוחלט לערוך ארגון מחדש באגף המודיעין, תוך איחוד יכולות האיסוף והיכולות הנוספות שלו, וזאת מתוך הבנה שהתשתית של יחידה 8200 והתשתיות הנוספות שנדרשות כדי לשרת את מרחב הסייבר צריכות לפעול באופן משולב. ההתקדמות בעשייה וצבירת הניסיון יביאו בעתיד, לפי ההערכה, למצב שבו יכולות ההגנה, האיסוף וההתקפה יאוגדו תחת מפקדה אחת.

גם בארצות הברית מתלבטים הגורמים הרלוונטיים מהי הדרך הנכונה להיערך בתחום הסייבר, ובכלל זה שוקלים לפצל בין פיקוד הסייבר (USCYBERCOM) והסוכנות לביטחון לאומי (NSA). כאמור, הדילמות המשותפות הובילו לשיתוף ידע בין צה"ל ובין הגורמים השונים בארצות הברית העוסקים בסייבר, ויש להניח שתהליך זה יימשך עוד שנים, שבמהלכן יישאר בתוקפו המודל הנוכחי המפוצל

של העיסוק בתחומי הסייבר השונים. עם זאת, בשלב מסוים במעלה הדרך יבשילו התנאים והיכולות, ואלה יאפשרו, כאמור, לאחד את מרחב הסייבר תחת מפקדה אחת. יש להניח שגם אז המהלך ייעשה בדרך מדודה ושקולה.

שינוי גדול מאוד נעשה בצה"ל גם במיון כוח אדם ובהכשרתו, בתשתיות הדיגיטליות, בבניין הכוח ובבתי התוכנה. השינוי שנעשה בתחומים אלה וחיזוק אגף התקשוב וההגנה בסייבר הביאו לשידוד מערכות ביכולות ההגנה של צה"ל במרחב זה. במסגרת זאת בולטת קפיצת הדרך הגדולה שנעשתה ביכולות התקשוב של צה"ל במסגרת הפרויקט "צבא יבשה דיגיטלי" (צי"ד), בו הושקעו יותר מעשרה מיליארד שקל במטרה לאפשר לכוחות היבשה של צה"ל אופטימיזציה ותפקוד טוב יותר בריכוז המידע על האויב, על כוחותינו ועל הפעלת הכוח המשולב של צה"ל. הרה־ארגון שבוצע באגף המודיעין הביא לשינוי מוחלט בתוך מערכי האגף במטרה להגיע לאופטימיזציה ולהקטין כפילויות. כן הוכנסו שינויים ושיפורים משמעותיים בשילוביות ובשיתופיות הבין־ארגונית בין צה"ל ובין השב"כ והמוסד, וכן ביכולות ברמה המדינתית.

צה"ל מקיים לא מעט תרגילים ואימונים משולבים הן בתוך עצמו והן עם ארגונים אחרים, ואפילו עם צבאות זרים, כדי ללמוד לחלוק מידע סייבר, מתוך הבנה שמדובר באתגר מתפתח הדורש שיתוף של ידע וחלוקתו. צה"ל גם משתתף באופן פעיל בתרגילים ובבניית היכולות להגן על המדינה במצבי חירום, תוך שיתוף פעולה הדוק עם מערך הסייבר הלאומי. עשייתו זאת של צה"ל נובעת מראייתו את עצמו כחלק בלתי נפרד מהגנת מרחב הסייבר הלאומי בחירום ובמצבי מלחמה. לצורך זה יש להמשיך לפתח ידע ולבנות שפה משותפת בין כלל הזרועות של מדינת ישראל, בנוסף ומעֵבר להתקדמות הרבה שהושגה בתחום זה עד היום. עדיין רב הנסתר במרחב זה על הגלוי, וכך נכון להשאיר את הדברים.

סיכום

צה"ל התקדם התקדמות אדירה בתוכנית "צבא יבשה דיגיטלי", המאפשרת למפקד המודרני בכל הדרגים לקבל מידע רב יותר וליצור תמונת מצב עדכנית יותר בנוגע למיקום האויב וכוחות צה"ל במרחב. התקדמות זו עשויה לגרום להצפת מידע בדרגי השדה, דבר שעלול להזיק יותר מאשר להועיל. ראוי לזכור שעודף מידע אינו ערובה לתהליכי פיקוד ושליטה טובים יותר. הדברים כבר נותחו בצה"ל, וחשוב להיות מודעים להם: "[אם] בעבר נאבק המפקד הטקטי להשיג נתונים על מיקום כוחותיו ועל מיקום האויב כדי שיוכל לקבל החלטות, הרי היום מוגשים לו נתונים אלה ורבים אחרים בשפע, וכתוצאה מכך עומד בפניו אתגר חדש: להפריד את

המוץ מהתבן ולמצוא את פריטי המידע הרלוונטיים שיאפשרו לו לקבל החלטות טובות יותר ולהשיג הכרעה בלחימה".[1]

לקדמה ולשקיפות במידע יש השלכות פסיכולוגיות נוספות על האופן שבו מפקדים מחלקים מידע. כמאמר קלאוזביץ, שדה הקרב הוא ממלכת האי־ודאות, וימשיך להיות ממלכת האי־ודאות,[2] וחשוב לפיכך שהשקיפות במידע לא תבלבל את הדרגים השונים בעת קבלת החלטות ושִמְדרגיות הפיקוד תישמר. העובדה שכל שרשרת הפיקוד – המ"פ, המג"ד, המח"ט ומפקד האוגדה – רואה את כל המידע באותו זמן, אסור לה שתגרום לתופעה של "מגדל בבל"; אסור שמערכות הפיקוד והשליטה המתקדמות, שמאפשרות לכולם לראות אותו מידע, יגרמו לכך שמפקד אוגדה או אלוף פיקוד יפעלו כאילו הם ברמת מפקד הפלוגה ויחשבו שהם מבינים טוב יותר את המצב ויודעים לקבל החלטות טובות יותר ממי שנמצא בשדה הקרב ממש.

צה"ל ימשיך להתפתח בתחום הסייבר, לבנות יכולות, לארגן את המפקדות ולפתח כלים טכנולוגיים חדשים. אולם, לצד הקִדמה הטכנולוגית, שמהווה מכפיל כוח של צה"ל ביחס לאויביו, חשוב מאוד לשמור תמיד על עקרונות ותפיסות הפיקוד הבסיסיות. תפיסות פיקוד אלו, הנשענות על אלפי שנות ניסיון אנושי, אינן תפיסות שמרניות גרידא; אדרבא, הן מסדירות בצורה טובה יותר את האופן שבו באה לידי ביטוי האומנות בשדה הקרב, את הדרך שבה מתקבלות החלטות ואת תהליכי הביצוע שלהן.

העשייה הצבאית תמשיך לחייב פעילות פיזית קשה ותובענית. ימי "מלחמות הכפתורים" הסטריליות עדיין רחוקים מאוד מאיתנו, אם בכלל יגיעו למקומותינו. לכן, על אף שצה"ל משקיע מאמצים רבים בפיתוח יכולות הסייבר שלו, נותר בעינו הצורך לשמר ולפתח את יכולותיו הקינטיות, מתוך הבנה שמלחמות העתיד ימשיכו להיות מוכרעות בשדה הקרב הפיזי.

---

1 גבי סיבוני, מורן מיורצ'יק, "קללת השפע", **מערכות**, גליון 459, פברואר 2015, עמ' 19.

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

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

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

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