צבא ואסטרטגיה

כרך 3 | גיליון 3 | דצמבר 2011

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
INCORPORATING THE JAFFEE CENTER FOR STRATEGIC STUDIES
TEL AVIV UNIVERSITY
אוניברסיטת תל-אביב

צבא ואסטרטגיה

כרך 3 | גיליון 3 | דצמבר 2011

צבא ואסטרטגיה

כתב העת **צבא ואסטרטגיה** מיועד להעשיר, להפרות ולהעמיק את השיח הציבורי באשר למרכיב הצבאי של הביטחון הלאומי בישראל.

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

כתב העת **צבא ואסטרטגיה** רואה אור במסגרת תכנית המחקר 'צבא ואסטרטגיה', המתנהלת במכון למחקרי ביטחון לאומי.

כתובת
המכון למחקרי ביטחון לאומי
רח' חיים לבנון 40, ת"ד 39950, תל־אביב 61398
טל' 03-6400400, פקס' 03-7447590
דוא"ל: info@inss.org.il

המאמרים המתפרסמים בכתב העת **צבא ואסטרטגיה**
מוצגים באתר המכון: www.inss.org.il/

ISSN 1565-8880

השימושים האסטרטגיים בעמימות במרחב הקיברנטי

מרטין ס׳ ליביקי

לעמימות אסטרטגית שמור מקום של כבוד במוסכמות המדינאות. חוסר הנכונות המכוונת של מדינות להצהיר על מעשיהן (או על מה שבכוונתן לעשות), בצד העדר הוכחה שהן עשו זאת משחררת מדינות אחרות. הן יכולות לטעון כי משהו נעשה, אך אם צורכיהן מכתיבים זאת, באפשרותן להעמיד פנים כי הדבר לא נעשה. דרגת הספק עשויה להשתנות: מספק מוחלט (איש אינו יודע מה קרה או מה עתיד לקרות) לספק קטן מאוד (לא "עובדים" על אף אחד). עם זאת, בכל אחד מהמקרים, מבצעי המעשה סיפקו עלה תאנה, שקוף ככל שיהיה, שמדינות אחרות יכולות לאמץ.

דוגמאות לעמימות אסטרטגית במרחב הפיזי

דוגמה אחת שכבר שנים שמור לה מקום של כבוד, היא סירובה של ישראל להודות (או להכחיש) שהיא מחזיקה בנשק גרעיני. לא יימצא פרשן ראוי לשמו המאמין באמת ובתמים שישראל אינה מחזיקה בנשק גרעיני. אך מאחר שישראל מעולם לא הצהירה שברשותה נשק גרעיני, מדינות אחרות חופשיות להעמיד פנים שישראל לא 'חצתה את הגבול' בתחום הגרעיני. מצב זה נוח למדינות שיהיו נתונות ללחץ של בני עמם להגיב בתוכניות גרעין משלהן במקרה שהמעמד הגרעיני של ישראל יֵצא לאור. מצב זה גם מסייע למדינות שלא היו יכולות לייצא פריטים מסוימים לישראל לו מעמדה הגרעיני היה גלוי יותר.[1] עם זאת, אין אף מדינה המתנהגת כאילו אין לישראל יכולת תגובה גרעינית.

עמימות דומה נוגעת לשימוש המשוער שעושה ארצות־הברית בכטב"מ (כלי טיס בלתי מאוישים) מסוג "פרדטור" ובטילי שיוט כדי לפגוע באנשי אל־קאעדה במדינות כמו תימן או פקיסטן. המדיניות הרשמית היא להכחיש את קיומן של טיסות כגון אלה. מנהיג תימן טען, שאלה היו מבצעים של תימן, מה שנשמע לא

ד"ר מרטין ליביקי הוא מדען חבר בצוות הניהול הבכיר במכון ראנד, קליפורניה, ארצות הברית.

סביר, ורק פרשנים בודדים נפלו בפח והאמינו לטענות אלה. ואולם לפחות עד לאחרונה לא הודו ראשי המדינות האמורות בתקיפות שהתרחשו בשטחן, וכך לא נאלצו להתמודד עם הטענה בדבר פגיעה בריבונותן.

דוגמה אחרת היא מדיניות ארצות־הברית כלפי עצמאותה של טייוואן. ארצות־הברית הצהירה שהיא מתנגדת להכרזת עצמאותה של טייוואן וכן לכל ניסיון ליישב את עניין מעמדה של טיוואן בכוח. ארצות־הברית אינה מכירה בטייוואן כמדינה, ולפיכך אין לה הסכם סיוע הדדי איתה. לכן, נשאלת השאלה: האם במקרה שטייוואן תכריז על עצמאות וסין תחליט לכבוש את האי, ארצות הברית תתערב לטובתה של טייוואן? ברור שהאינטרס המובהק של ארצות־הברית הוא שסין תחשוב שזה אכן המצב כדי שלא תפתח במלחמה, וכמעט ודאי שהאינטרס של ארצות־הברית הוא, שגם טייוואן תחשוב שזהו המצב כדי שהיא עצמה לא תעודד את סין לפתוח במלחמה. הבה נניח שהסיכויים של התערבות ארצות־הברית משולים, פשוטו כמשמעו, להטלת מטבע, ונתפסים כך משני צדי המצָרים. בהתאם לכך, טייוואן עשויה להגיע למסקנה, שהערך הצפוי מהכרזת עצמאות הוא שלילי (הוא היה עשוי להיות חיובי אילו ידעה בוודאות שארצות־הברית תחוש לעזרתה) מאחר שארצות־הברית עשויה לא להתערב. בדומה לכך סין משיקולים שלה, עשויה להגיע למסקנה, שהערך הצפוי מפלישה וחציית המצָרים עלול להיות שלילי מכיוון שארצות־הברית עלולה לפעול. כל אפשרות עמומה פחות מזו עלולה לעודד צד זה או אחר לנקוט צעד טיפשי.

המרחב הקיברנטי מתאים לעמימות

מלחמה קיברנטית היא חשאית במהותה. כאשר פורצי מחשבים חודרים למערכת מחשב כדי לשבש את פעולתה, התוצאות הישירות הן על־פי־רוב בלתי נראות לעולם החיצוני. בהתאם לדרגת השיבוש במערכות האלה, גם התוצאות העקיפות עשויות להיות בלתי נראות לעין. תוצאות של מתקפת סייבר על רשת חשמל, הגורמת לכיבוי האורות, ניתנת לצפייה אפילו מהחלל; אבל בהעדר המשך חקירה וגילוי, לא יהיה ברור אם ההאפלה היא פועל יוצא של התקפה מכוונת, או של טעות אנוש, תוכנה לקויה, או (לעתים קרובות) של הטבע עצמו. גם אם יתברר שמערכת השתבשה בגלל התקפה, זהות התוקף עשויה להישאר אפופה במסתורין. לבסוף, אם עצם התקפת הסייבר וזהות מחוללה היו ברורים, מטרתה עשויה להיות מעורפלת ולא ברורה – אחרי הכול, מלחמה קיברנטית לבדה אינה יכולה להרוג איש, או אפילו להרוס יותר מדי (עיין ערך תולעת הסטקסנט – Stuxnet) ועוד פחות מכך לכבוש שטח או לשנות משטר (מלחמה קיברנטית אכן יכולה לאפשר שימושים אחרים בכוח, ושימושים אחרים אלה הם המוחשיים יותר). כמעט כל הפריצות הקיברנטיות נועדו לגנוב מידע או לעשות שימוש במחשב המטרה (כמו

ברובוט), ומעבר לכך להשאיר את המערכת כמות שהיא. אפשר לעצב התקפות כניסיונות להטעות בני אדם (למשל תמונות מכ"ם מסולפות) או את הציוד שלהם (ראו על תולעת הסטקסנט). במקרים האחרונים, המובן מאליו מטבע הדברים פועל כבומרנג; משעה שברור כי הצלחת להערים על מערכת, מנהלי המערכת אינם צפויים לאפשר לה לפעול כפי שפעלה בעבר.

האם תולעת הסטקסנט היא דוגמה יוצאת דופן?

אפשר היה לשער שמתקפת סייבר אשר שיבשה דבר מה בפועל עברה את השלב שבו הכול יכולים להצניע את קיומה. תולעת הסטקסנט התגלתה בחודש יוני 2010, ובספטמבר זוהתה מטרתה – מתקן גרעיני באיראן. החשדות המוקדמים ביותר סימנו את הכור בבושהר כיעד שלה,[2] אך איראן הכחישה שהכור ספג חבלה כלשהי. בתוך כמה שבועות זוהה מפעל הצנטריפוגות בנתנז כמטרת ההתקפה. הכחשות ראשוניות של איראן הופרכו בשלהי נובמבר 2010, ביום שבו חיסלו מתנקשים שני מדעני גרעין איראנים, וכאשר הודה אחמדינג'אד שהייתה תולעת שגרמה בעיות רבות, אך אלה תוקנו.[3] מהו הנזק הממשי שהסבה תולעת הסטקסנט לפיתוח הגרעין האירני? סטטיסטיקה של סבא"א (הסוכנות הבינלאומית לאנרגיה אטומית) מלמדת, כי ייתכן שהתולעת האמורה גרמה להתבלות מוקדמת של עשרה אחוזים מהצנטריפוגות של איראן, ולפיכך הקנתה ליוצרי התולעת כמה חודשי דחייה לכל היותר בלוח הזמנים המשוער שלפיו יהיה בידי איראן די חומר גרעיני לבניית הפצצה הראשונה שלה.[4] בדיווחים אחרים מצוטטים אישים בכירים, המתנבאים (נכון לינואר 2011) שהמועד המוקדם ביותר שבו איראן תוכל להרכיב התקן כזה הוא 2015, כלומר הושג עיכוב של כמה שנים.

רב הנסתר על הגלוי בכל הקשור לתולעת הסטקסנט (למעט מה שידוע שהיא הצליחה להשיג).[5] ראשית, לא ברור איך הצליחה התולעת לחדור למפעל ב־נתנז; דומה כי חשדות ולפיהם יוצרי התולעת קיבלו סיוע ביודעין או שלא ביודעין מקבלנים רוסים חיבלו ביחסי העבודה של האיראנים עם קבלנים אלה.[6] ומה שחשוב מכך – מי כתב את התולעת ומי שחרר אותה? האם היה זה אדם מסוים (התחכום שלה מרמז על אפשרות אחרת)? האם היו אלה ישראלים – כפי שאפשר לשער מכמה רמזים בקוד המקור – אך מי יידע אם רמזים אלה לא הושתלו כדי להטעות? האם היו אלה אמריקנים? האם מדובר בשיתוף פעולה – אמריקני־ישראלי?[7] האם היו אלה הסינים?[8] לנוכח העמימות הרבה, אין פלא שאיראן טרם הגיבה על האירוע הזה. גם סוריה לא הגיבה על ההתקפה על מה שנחשד כמתקן הגרעין שלה, ועיראק לא עשתה דבר חוץ מלהתלונן לאחר שהופצץ הכור שלה באוסיראק – ובשני המקרים הללו לא הייתה שום עמימות בנוגע למְבצעים. קשריה האיתנים של איראן עם חמאס ועם חזבאללה מרמזים כי ייתכן שעמדו לרשותה

כמה דרכים – שלא עמדו לרשותן של סוריה (בשנת 2007) או של עיראק (בשנת 1981) – להביע את חוסר הנחת שלה. יתרה מכך, איראן טרם עשתה "עניין גדול" מהתקרית, ואם לאחר חודשים של שתיקה והכחשות היא תראה בכך אקט של מלחמה, יהיה בכך משום תפנית של 180 מעלות.

יתרונות השימוש בתולעת הסטקסנט במקום בכוח אווירי לצמצום יכולתה הגרעינית של איראן, ברורים למדי (בהנחה שהתולעת אכן עשתה את מה שיוצריה ציפו): השפעה דומה, זריעת חוסר אמון בקרב קורבנותיה ואי־ודאות מי מבין הספקים או הציוד עדיין סובלים משיבושי התולעת, וכל זאת במידה פחותה בהרבה של גינוי (ואולי אף בהערצה כמוסה) ובפחות סיכונים אסטרטגיים מאלה הכורכים בהפעלת כוח אווירי.

שימושי העמימות

ההשערה המוצעת היא, שהתקפת סייבר המשמשת במקום שיטות קינטיות, יוצרת עמימות רבה יותר במונחים של תוצאות, מקורות ומניעים. לפיכך אם מתקפות סייבר פועלות בהצלחה – וסימן השאלה בעניין הזה הוא גדול – הן משנות את פרופיל הסיכון של פעולות מסוימות, כך ובדרך כלל בדרכים ההופכות אותן לחלופות מתאימות יותר. להלן כמה שימושים היפותטיים של מתקפות סייבר.

א. קורבן לתוקפנות בהיקף קטן עשוי להשתמש במתקפות סייבר כדי לבטא את אי־שביעות רצונו, אך הסיכון להסלמה קטן יותר לעומת זה הכרוך בתגובה פיזית. לדוגמה, בשלהי 2010 הפציצו כוחות צפון קוריאה אי בדרום קוריאה והרגו שני אזרחים ושני אנשי צבא. תגובה בדמות מתקפת סייבר, שנועדה לשבש מתקן תעשייה חשוב (אם מתעלמים מן העובדה שצפון קוריאה אינה ממוחשבת היטב ובעלת אפס חיבורי רשת לשאר העולם) הייתה עשויה להעביר את תחושת אי־שביעות הרצון של דרום קוריאה. לו רצתה צפון קוריאה להגיב היה עליה: (1) להודות שאחד ממתקניה נפרץ; (2) לנקוט צעדים שיוכיחו כי דרום קוריאה היא האחראית הבלעדית לכך (זו עשויה להיות ארצות־הברית או אפילו יפן, ואפילו סין). לחלופין, אם צפון קוריאה לא תגיב באופן פומבי, יש לה סיכוי טוב להגביל את מספר היודעים מדוע כמה ממתקניה חדלו מלפעול. תיאור זה מציג מאפיין חשוב נוסף של מלחמה קיברנטית, המעניק לה יתרון על פני לוחמה פיזית: אף־על־פי שהיותך מותקף עשוי להוות מקור לגאווה (תוכל לגלם את דוד לעומת האויב גוליית), העובדה שפרצו למערכות שלך פירושה שנכנסת למרחב הקיברנטי בלי לתת את הדעת על הגנה של מערכותיך. קורבנות איננה דבר הראוי להתגאות בו. לפיכך מומלץ למדינות היכולות להסתיר את העובדה שהותקפו לעשות זאת, וכך לשמור על כבודן – אך נתיב זה גם עושה את התגובה לאפשרית פחות. פתוחה לפניהן הדרך להגיב באופן דומה, וכך מאבק של עין תחת עין שהחל בעולמות

הפיזיים, עולה (או יורד) לעולם הקיברנטי. אך נתיב זה עשוי להיות בטוח יותר בכל ההיבטים לעומת הנחתת מכות פיזיות.

ב. מדינה עשירה בלוחמי סייבר עשויה להשתמש באיום בלוחמת סייבר להרתעה מפני הפיכתה למטרה אפשרית של אויביה. לדוגמה, באפשרותה של ישראל לאיים על איראן במתקפות סייבר אם תותקף על־ידי חזבאללה, ארגון בעל קשרים מוכחים עם איראן.[9] במצב עניינים שכזה, קיימת אפשרות שישראל לא תהיה מעוניינת לפרסם ברבים את האיום הזה. איום גלוי יאפשר לחזבאללה לכפות את רצונו על איראן בטענה שהוא מעוניין לתת ביטוי לסוג הפגיעה שתניע את ישראל לתקוף את איראן במרחב המדומה. אך יש מסלולים פרטיים להעברת האיום. יש היגיון באיום שכזה. הבעיה הרווחת בכל הנוגע להרתעת סייבר היא, שהייחוס של ההתקפה הפותחת מהווה בעיה, אך במקרה של התקפה פיזית – נניח, בדמות טילים של חזבאללה המשוגרים לעבר ישראל – יהיה קל מאוד לקבוע זאת. לחילופין, אף על פי שמדינה כמו איראן אינה עשויה בהכרח לחשוש מהתקפה ישראלית ישירה גם בתגובה להתקפה של חזבאללה, (התקפות שכאלה לא התממשו בשנת 2006, למשל), היא עשויה לחשוש ממתקפת־סייבר בהתחשב בעליונות הברורה של פורצי מחשבים ישראלים על פני עמיתיהם האיראנים. עליונות שכזו ממתנת (אם כי לא מבטלת) את החשש כי לאחר שהצהירה על הכוונה לבצע מתקפת־סייבר, לא יהיו לישראל מטרות נגישות באיראן. גם אם ההצלחה של מתקפה בודדה אינה ודאית, הסיכויים כי חלק מהן יצליחו ויגרמו נזק – טובים למדי. הפניית אצבע מאשימה של איראן כלפי ארצות־הברית לאחר מכן עלולה ליצור בעיה עבור ארצות־הברית, אך לעשות חיים קלים יותר עבור ישראל. הסלמה לאלימות איננה באמת אופציה עבור איראן בהתחשב בעליונותה של ישראל בתחום הלוחמה הקונבנציונלית (לפחות אם הקרב יהיה בסמוך לישראל). וליתר דיוק, כפי שצוין, איראן תיאלץ להודות כי המערכות שלה חובלו ולשכנע כי היא יודעת מי עומד מאחורי הפעולה. לבסוף, בעוד שישראל מרושתת יותר מאיראן, לאור יכולות הסייבר שלה, אולי לא יהיה בכך די כדי להטות את הכף לטובתה של איראן היה וזו תשיב מלחמה.

ג. מתקפות סייבר עשויות לשמש מדינה אחת כדי להשפיע על תוצאות סכסוך במדינה אחרת בלי שתצטרך להתחייב לכך בגלוי או אפילו במשתמע. לדוגמה, מלחמת האזרחים בלוב – אילו היה צבא לוב מחובר לאינטרנט באופן כזה שמתקפות סייבר היו יכולות להשפיע על ביצועיו,[10] אזי באמצעות נטרול כוחות הממשל המרכזי, היו פורצי מחשבים מן המערב יכולים להטות במידה ניכרת את כיוון המלחמה. אילו המורדים היו מנצחים, היו ממשלות המערב נשכרות מכך. אפשר שלא היה באפשרותם של כוחות המורדים לדעת שהם קיבלו סיוע, וייתכן שהדבר היה רק לטובה (בייחוד אם מדובר במורדים בעלי נטייה ג'האדיסטית מבין

המורדים בלוב, המקדמים בברכה את התערבות הכוחות האמריקניים). אפשרות אחרת היא לפזר רמזים (למשל, אם יכולת מסוימת תשותק מחר, אתם תדעו את הסיבה לכך). לחלופין, אילו ידה של הממשלה הייתה על העליונה, היא הייתה עשויה לחשוד שכוחות המערב חיבלו במערכות המידע שלה, אך הייתה מתקשה להוכיח זאת. היא הייתה עשויה להתלונן, אך היה צפוי מלוב להאשים את המערב במגרעותיה, ואז לתלונותיה, בהעדר הוכחות, לא היה ניתן לייחס חשיבות כלשהי. ליתר דיוק, היא לא הייתה רוצה לטעון כך אם רצונה היה להעמיד פנים לאחר מכן שאין לה כל סיבה לראות שוב במערב אויב. לו מלחמת האזרחים הייתה נמשכת, יכול היה המערב להעמיד פנים שהוא לא נתן סיוע לפני כן, וממילא גם לא התחייב להגדיל את הסיוע שלו (גם אם נשלחו רמזים למורדים, הם היו מתקשים מאוד להוכיח לאחרים שפורצי מחשבים מן המערב הציעו להם סיוע, שכן בשונה מהממשלה, אין לצפות שתהיה להם גישה למחשבים שחובלו). הבעיה הגדולה ביותר הטמונה בהצעת סיוע שכזה היא האפשרות של חשיפה, אבל אם היעד למתקפות שרוי בסכסוך עם שאר העולם, אין לצפות שהוא יזכה לסיוע ממשי באיתור התוקפים. סיוע שכזה הוא כה מושך (לפחות מנקודת המבט של נותן הסיוע), שהוא עשוי להפוך למאפיין שגרתי – משני הצדדים – בכל סכסוך שבו התוצאה אינה ודאית, ולרשתות יש חשיבות רבה במה שנוגע ליכולות לחימה. יודגש שוב, כי הודאה שהמערכות שלך נפרצו כרוכה תמיד במידה זו או אחרת של מבוכה.

ד. התקפות סייבר אינן צריכות להיות מכוונות בהכרח רק כלפי אויבים, אף־על־פי שהסיכונים שביצירת אויבים חדשים במקרה של חשיפת מקור המתקפות הם ברורים. דמיינו לעצמכם מצב שבו שתי מדינות ניטרליות מתקדמות באיטיות לעבר מלחמה. נניח שמדינה שלישית מסוגלת לגרום שיבושים במערכות המעקב, השליטה והבקרה של שני הצדדים, שיטילו ספק בדבר הצלחתן של שתי המדינות להתגבר על הסכסוך ביניהן. אם מערכות יוצאו מכלל שליטה, צפוי שכל אחת מהמדינות הללו תאשים תחילה את האחרת במקום לתלות את האשמה בצד שלישי. סביר ביותר שההנחה הראשונית – שהנזק נעשה על ידי הצד השני – תשפיע על התגובות ועל הפעילויות שלהן. יתר על כן, סיכוי גבוה הוא שהאשמה כזאת לא תוטח בפומבי עקב המבוכה הכרוכה בכך. עם זאת, תחבולות שכאלה עלולות להוביל מדינות למלחמה אם אחד הצדדים ישכנע את עצמו, למשל, שמתקפות הסייבר שמשגר כלפיו הצד האחר הן בגדר צעד מקדים להזזת כוחות מידית, או שהן מעידות שכוחות האויב אינם פרוסים במערך מסוים בלא סיבה.

ה. עמימות עשויה להועיל במדיניות הצהרתית, כזו המפרטת כיצד המדינה תגיב על מתקפת סייבר כנגדה. לעמימות יש חסרונות ויתרונות כאחד. החיסרון הוא, שאחרים עשויים לחשוב שהם יכולים להתחמק מאחריות לביצוע התקפות

שהם היו נמנעים מביצוען לו היה ברור להם שאלה יגררו פעולות תגמול. היתרון הוא, שסביר להניח שמדינת המטרה לא תרצה לתקוף בחזרה, בייחוד אם היא חוששת ליחס לעצמה את ההתקפה. מדינה הנמנעת מתקיפת־נגד מכיוון שאינה בטוחה, לא תאבד ממעמדה בעיניה שלה – ייחוס המעשה לצד מסוים הוא באמת משימה קשה. עם זאת, אם התוקף (ואחרים) יגיעו למסקנה שהמדינה האמורה ידעה מי התוקף אך העמידה פנים שאינה יודעת, מחשש להתלקחות מלחמה בהיקף מלא, אזי כל איום בנקמה מצדה יישמע לא אמין. אם מדינה ממהרת להבטיח פעולות תגמול בתגובה על מתקפות סייבר ואינה יכולה לעמוד בהבטחותיה, גם יכולתה לממש את איומיה האחרים, תוטל בספק.

מסקנות

העמימויות הטקטיות הרבות של לוחמת הסייבר מחזקות אסטרטגיה המבוססת על עמימויות אסטרטגיות. ייתכנו מקרים רבים שמדינה תוקפנית אינה מעוניינת לפרט מה היא עשתה. אפילו מדינת המטרה, במקרים מסוימים, עשויה להגיע למסקנה שלהעמיד פנים שלא הותקפה (אפילו אם עליה להעלים עין מהראיות) עדיף בעבורה מניסיון להבהיר עניינים.

ואולם יש גם חיסרון בעמימות אסטרטגית. מדינות עשויות ליטול על עצמן, שלא בדין, את הזכות לגרום סוגים שונים של נזקים במרחב הקיברנטי, בהניחן כי לעולם לא יידרשו לשאת באחריות על מעשיהן.. לעתים אין בכך הצדקה, והמדינה מרמה רק את עצמה; ואפילו אם יש הצדקה באי־לקיחת אחריות, היא מספקת לפורצי המחשבים דרגה של חופש שההיסטוריה מלמדת שהיא מסוכנת בפני עצמה.

הערות

1 בניגוד לכך היה צורך בחקיקה בשנת 2006, שתאפשר לארצות־הברית לשתף טכנולוגיה אזרחית עם הודו, שבדומה לישראל אינה חתומה על האמנה לאי־הפצת נשק גרעיני, אבל בשונה מישראל, היא מעצמה גרעינית מוצהרת. ראו: Peter Baker, "Signs India Nuclear Law: Critics Say deal to Share Civilian Technology could Spark Arms Race," Washington Post, December 19, 2006. www.washingtonpost.com/wp-dyn/content/article/2006/12/18/AR2006121800233.HTML

2 Robert McMillan, IDG News, "Was Stuxnet Built to Attack Iran's Nuclear Program?" taken from *PCWorld*, September 21, 2010.

3 William Yong, Alan Cowell, "Bomb Kills Iranian Nuclear Scientists," *New York Times*, November 30, 2010.

4 Joby Warrick, "Iran's Natanz nuclear facility recovered quickly from Stuxnet cyberattack," *Washington Post*, February 16, 2011. See also the report by the Institute for Science and International Security, http://media.washingtonpost.comqwp-srv/world/documents/stuxnet_update_15Feb2011.pdf

5 הדבר הברור ביותר על תולעת הסטקסנט הוא אופן פעולתה מכיוון שהתולעת נתפסה "בחיים" כביכול, בטרם יכלה להשמיד את עצמה (פעולה שהיה עליה לעשות במקרה שלא יעלה בידה למצוא התקן לוגי מסוים ניתן לתכנות, שעמד בפרמטרים מסוימים קבועים מראש, הקשורים לסוג מסוים של צנטריפוגה).

6 www.economist.com/blogs/babbage/2010/09/stuxnet_worm

7 William Broad, John Markoff, David Sanger, "Israel Tests on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, January 15, 2011.

8 Jeffrey Carr, "Stuxnet's Finnish-chinese Connection", December 14, 2010, www.blogs.forbes.com/firewall/2010/12/14/stuxnets-finnish-chinese-connection/

9 משקיפים רבים חולקים על האפיון של חזבאללה כבובה של איראן. עם זאת, יש הבדל בין חזבאללה הפועל אך ורק בהתאם להוראות מאיראן, לבין מצב שבו לאיראן יש השפעה מספקת על חזבאללה כדי להניאו מלנקוט פעולות לא חכמות.

10 במאמר רב השפעה, שסקר את האפשרויות של התערבות המערב בלוב נזכר הנושא של לוחמה אלקטרונית בדמות שיתוק התקשורת, אך לא צוין דבר בנוגע ללוחמת סייבר: Thom Shanker, "U.S Weighs Options, on Air and Sea," New York Times, March 6, 2011, http://www.nytimes.com/2011/03/07/world/middleeast/07military.html

התרת אפקט ה־'סטקסנט':
על המשכיות ושינוי בשיח על איומי הסייבר

מרים דאן קוולטי

מבוא

זה שנים אחדות שאיומי סייבר נמצאים על סדר היום הפוליטי והביטחוני. זמן לא רב לאחר שחוקרי מכון RAND, ג'ון ארקווילה ודויד רונפלדט, דיברו על כך ש"הלוחמה הקיברנטית (לוחמת סייבר) מגיעה!",[1] הפך צירוף המילים "לוחמת סייבר" לסיסמה הבולטת ביותר בשיח בנושאי מחשבים, ביטחון לאומי ומרחב קיברנטי (cyberspace). נתונה לחסדי האירועים וההתרחשויות שבכותרות, גברה ההתעניינות בנושא כל אימת שדווח באמצעי התקשורת על שימוש אגרסיבי במחשבים; היא שבה ודעכה כאשר נושאים אחרים תפסו את מרכז הבמה.

בשנת 2010 נפל דבר. הסטקסנט (Stuxnet), תולעת המחשב המתוחכמת שנוצרה כדי לחבל במערכות השולטות ומבקרות תהליכים תעשייתיים, הסעירה את הקהילה הבינלאומית במגוון דרכים והזניקה את נושא הסייבר אל מרחב החששות של הציבור ואל ראש רשימת האיומים. התוצאה היא, שעוד ועוד מדינות רואות במתקפות סייבר את אחד האיומים הביטחוניים העתידיים המרכזיים, אם לא הגדול שבהם. באיזו מידה מוצדקת ראייה זו, ומה באמת שינתה תולעת הסטקסנט בשיח?

מטרתו של מאמר זה לתת תמונה מאוזנת של תופעת לוחמת הסייבר. אדגים כיצד ומדוע התפתחה לוחמת הסייבר מהתפיסה הצרה, הנוגעת אך ורק לאינטראקציה צבאית, למשמעותה הרחבה, שנעשתה מנותקת ממלחמה במובנה הפשוט ומקיפה כמעט כל פעילות הנוגעת לשימוש אגרסיבי במחשבים. בעיקר תיעשה במאמר זה הבחנה בין צורות שונות של עימות סייבר, שתשמש בסיס להערכת סיכונים מיושבת ושקולה. בהמשך יודגם כיצד השיח על איומי הסייבר מתאפיין, ככל הנראה, בפחות מדי שינוי וביותר מדי המשכיות מכפי שנוטים

ד"ר מרים דאן קוולטי עומדת בראש יחידת המחקר 'הסכנה החדשה' במכון ללימודי ביטחון, ציריך, שוויץ.

להודות כיום. דימוי האיום נשאר יציב משלהי שנות התשעים של המאה ה־20, ותולעת הסטקסנט לא חוללה שינוי משמעותי במצב הזה. הדבר נכון גם בנוגע לאמצעי־נגד מתוכננים או חזויים.

הֶקשרים ומשמעויות של לוחמת סייבר

חשיבותו של המושג לוחמת סייבר והשפעתו ניתנים להבנה בצורה הטובה ביותר בהקשר הרחב של מהפכת המידע, שעיצבה – ועדיין מעצבת – את התפיסות בדבר הזדמנויות וסכנות. בייחוד דומה כי הטכנולוגיות של מהפכת המידע וחידושים ארגוניים נלווים בשנות השמונים והתשעים שינו את אופי העימות ואת סוגי המבנים, הדוקטרינות והאסטרטגיות הצבאיות. לפיכך נראה כי מושג זה מרמז על הופעתה של לוחמה מסוג "חדש", שבה גורם המידע נהפך בהדרגה לחשוב יותר ויותר. התפתחות זו התאפשרה (אם לא הונעה) מסיומה של המלחמה הקרה וההגדרות המחודשות שבאו בעקבותיה למונחים כמו אויבים, מחשבה אסטרטגית והוצאה על ביטחון.

מלחמת המפרץ הראשונה, בשנת 1991, יצרה קו פרשת מים בכל הנוגע לחשיבה צבאית על לוחמת סייבר. עימות זה נתפס בעיני אסטרטגים צבאיים (בעיקר אמריקנים) כעימות הראשון בדור חדש של עימותים, שבהם הניצחון איננו מובטח רק בכוח הזרוע, והוא גם פועל יוצא של היכולת לנצח במלחמת המידע ולהבטיח "דומיננטיות של מידע". בעקבות מלחמה זו פורסמו אינספור ספרים בנושא,[2] והתגובה להתפתחויות הטכנולוגיות אחרי מלחמת המפרץ מצאה ביטוי גם במאמרי דוקטרינה חדשים שמיסדו את מרכיב המידע.

תחילה התאפיין השיח באופוריה רבה. אבל זמן קצר אחר־כך ניתנה תשומת לב רבה יותר לסיכונים הכרוכים בהתפתחות זו: גיבוש אסטרטגיות שלא מוקדו עוד ביכולת האויב, אלא סימנו את "זרימת המידע של היריב", הדגישו את הפגיעות הגבוהה יחסית של כוחות אמריקניים מרושתים. עם התקדמות הדיון על התקפות על מערכות מידע עוינות אפשריות, נידונו בהרחבה גם הסכנות האפשריות לרשתות נתונים אזרחיות. ארצות־הברית, כמעצמת־העל היחידה שנותרה, נתפסה כמי שנועדה מראש להפוך למטרה ללוחמה א־סימטרית. חשש נרחב קנה לו אחיזה בקרב הקהילה האסטרטגית, ולפיו אלו הצפויים לנחול כישלון נגד מכונת המלחמה האמריקנית עלולים לתכנן לפגוע קשות בארצות־הברית באמצעות תקיפת נקודות חיוניות שלה מבית, דהיינו תשתיות חיוניות[3]. המושג תשתית חיונית מכיל מגזרים כמו מידע וטלקומוניקציה, שירותים פיננסיים, אנרגיה ותשתיות, תחבורה ועוד רכיבים המשתנים ממדינה למדינה ובמהלך הזמן.[4] רוב המגזרים הללו מסתמכים על מרחב שלם של מערכות בקרה מבוססות תוכנה לפעולתם החלקה, האמינה והרציפה.

עם גידולן של רשתות מחשב והתרחבותן לעוד ועוד היבטים של חיי היומיום, השתנתה מטרת ההגנה ממה שנתפס כרשתות קנייניות מוגבלות (ממשלתיות, בעיקר צבאיות), אל החברה בכללותה – או ליתר דיוק, אל דרך החיים שלה, המתאפשרת באמצעות תת־המבנה הבלתי מופרע של הטכנולוגיה.[5] על בסיס זה התפתח איום הכולל שני צדדים הקשורים בקשר גומלין זה לזה. ראשית, פרספקטיבה פנימית, ולפיה עצם הקישוריות של מערכות תשתית מציבה סכנות מכיוון שהפרעות בתוכן עלולות להתפתח לאסונות גדולים במהירות רבה. חידושים בטכנולוגיית מידע ותקשורת הגבירו אפוא את הפוטנציאל לאסון של ממש בתשתיות חיוניות באמצעות הגדלה ניכרת באפשרות שסיכונים מקומיים יהפכו לסיכונים מערכתיים. שנית, פרספקטיבה עם מבט כלפי חוץ מתמקדת בהגברת הנכונות של שחקנים זדוניים לנצל נקודות תורפה בלא היסוס או מגבלות. מאחר שמערכות תשתית חיוניות משלבות ערכים סמליים ואינסטרומנטליים, התקפתן הופכת לחלק חשוב בהיגיון המודרני של השמדה, המבקשת להשיג השפעה מרבית.

ממד הסייבר גם מעצב מחדש את המרחב למשהו שאינו נטוע עוד במקום או בנוכחות. "האויב" הופך לישות מרוחקת ונטולת פנים, נעלם גדול שכמעט בלתי אפשרי לאתרו. מצב זה מוביל לשני מאפיינים חשובים של ייצוג האיום: ראשית, יכולת ההגנה על מרחב מתבטלת – אין מקום מוגן מפני התקפה או מפני התמוטטות קטסטרופלית. שנית, האיום הופך אוניברסלי כביכול משום שהוא נמצא כעת בכל מקום.

הפנומנולוגיה של הסייבר

לאור האמור לעיל, אין זה מפתיע לגלות, כי החשש מפני איומי סייבר הוא גדול כל כך. אך כל משקיף יוכל להיווכח עד כמה האיומים הם בלתי מוגדרים. לאחר שחרג מגבולותיו הצבאיים, הפך המושג מטושטש מאוד: לוחמת סייבר מתייחסת כעת לכל תופעה הכרוכה בשימוש הרסני או משבש בצורה מכוונת את עבודת המחשבים.

ערפול קונספטואלי שכזה מקשה עלינו להבין מה קורה בעימותים "סייבריים",[6] ואילו סוגים של אמצעי־נגד נדרשים להתמודדות עם אירוע ספציפי. ברוס שנייר (Bruce Schneier), טכנולוג אבטחה ומחבר בעל שם בינלאומי, מבחין בין סייבר־ונדליזם (cybervandalism), כלומר השחתה של אתר אינטרנט; סייבר־פשע (cybercrime), תופעה של גנֵבת קניין רוחני, סחיטה המבוססת על איום בתקיפה מסוג מתקפה מבוזרת למניעת שירות (DDoS), מרמה המבוססת על גנבת זהות וכיוצא באלה; סייבר־טרור (cyberterrorism), פריצה למערכת מחשב כדי לגרום להתכת כור גרעיני, לפתיחת סכר, או כדי לגרום להתנגשות בין שני מטוסים; ולוחמת סייבר (cyberwar).[7] שנייר משתמש במונח לוחמת סייבר במובן של

שימוש במחשבים לשיבוש פעילויות של מדינת אויב, ובייחוד התקפות המכוונות על מערכות תקשורת.

הסיווג של שנייר בונה מערך של איומי סייבר מתעצמים ומסלימים – משלב אחד בסולם לזה שבא אחריו, ההשפעות האפשריות וכן ההיקף והעוצמה מסלימים. בשנים האחרונות נוכחנו לגלות כי סייבר־ריגול (cyberespionage) וסייבר־חבלה (cybersabotage) נעדרים מהסולם. עם זאת יצוין, שקווי הגבול בין הפעילויות השונות מטושטשים מאוד. כאשר מתרחש אירוע שגרם נזק, קשה לקבוע אם הנזק הוא תוצאה של התקפה זדונית, פגם ברכיב מסוים או תאונה. על אף המטרות השונות, הכלים והטקטיקות המשמשים צבאות, ארגוני טרור ועבריינים במרחב הסייבר – דומים מאוד, אם לא זהים. פירוש הדבר, במקרה של התרחשות התקפה, קשה מאוד לזהות מי עומד מאחוריה ובאיזה סוג של תופעה מדובר.

יודגש שוב, הקושי בהבחנה בין התופעות השונות אין משמעו שההבחנה איננה נחוצה; ההפך הוא הנכון. **ראשית,** היתרון בתפיסה של "חומרת ההשפעות" שהיא מסייעת לקובעי מדיניות לתעדף בתיאוריה – דבר חשוב ביותר. רק התקפות מחשב שתוצאותיהן הרסניות או גורמות שיבושים חמורים צריכות להיחשב סוגיה של ביטחון לאומי, ולפיכך מחייבות תשומת לב הניתנת לאירועים שמהווים איום קיומי. מתקפות הגורמות לשיבוש של שירותים לא חיוניים, או שהן בעיקר מטרד יקר, אינן נכללות בקטגוריה זאת.[8] **שנית,** הגדרה צרה ומדויקת מסייעת לעקוף סכנות אחרות הטמונות בתיוג אירוע מסוים כ"מלחמה", למשל לפטור קורבנות של התקפה מאחריותם להשלכות הנובעות מרשלנותם שלהם בכל הנוגע לאבטחת מחשב או יצירת לחץ להשיב מלחמה נגד "פורצי מחשבים", אמיתיים או מדומים.[9] **שלישית,** הגדרת התופעות מדגימה בבירור היכן מרכז הכובד – בחקירות מחשב קפדניות. יש לחקור כל אירוע בקפדנות. כפי שמציין שנייר: "בדיוק כשם שכל מקרה של ירי אינו בהכרח פעולה מלחמתית, כך כל מתקפת אינטרנט מוצלחת, בלי קשר למידת חומרתה, אינה בהכרח פעולה של לוחמת סייבר. מתקפת סייבר המשתקת את רשת החשמל עשויה להיות חלק ממערכה של לוחמת סייבר, אך היא גם עשויה להיות פעולה של סייבר־טרור, סייבר־פשע או אפילו – אם היא מבוצעת בידי נער בן ארבע־עשרה שלא מבין באמת מה הוא עושה – סייבר־ונדליזם. הסיווג הספציפי מותנה במניעים של מחולל המתקפה ובנסיבות ההתקפה [...] בדיוק כמו בעולם האמיתי".[10]

הערכת סיכונים

הדברים לעיל מעלים את השאלה: עד כמה נמצאים אנו במצב של סכנה? עימותים במרחב המדומה הם בבחינת מציאות זה יותר מעשור – בכל עימות פוליטי, כלכלי וצבאי יש היבטים המתרחשים בתוך האינטרנט וסביבו. יתרה מכך, פעילויות

פליליות ופעילויות ריגול בעזרת טכנולוגיות מידע ותקשורת מתרחשות בכל יום. אך בכל ההיסטוריה של רשתות מחשבים, היו רק דוגמאות בודדות להתקפות חמורות שהיה להן הפוטנציאל לשבש או אף שיבשו בפועל – בצורה חמורה – פעילויות של מדינה. בודדות יותר הדוגמאות למתקפות סייבר שגרמו לאלימות פיזית נגד בני אדם או רכוש. הרוב המכריע של התקפות הסייבר הן מדרגה נמוכה וגורמות אי־נוחות, ולאו דווקא לשיבוש חמור או לשיבוש לטווח ארוך. למעשה ברור כיום, כי הסבירות להתרחשותה של לוחמת סייבר "טהורה" (או אסטרטגית) נמוכה ביותר, וסבירות גבוהה יותר מיוחסת למתקפות על מערכות מחשבים בשיתוף עם צורות התקפה אחרות, פיזיות.[11]

האם הערכה זו השתנתה בשנה החולפת? סיווג התולעת סטקסנט אכן מהווה אתגר. מסתובבים אלפי סיפורים והשערות על התולעת, על מקורותיה ועל כוונותיה.[12] סיפורים כתובים ברמה זו או אחרת, וכולם מכילים חלקי תצרף (פאזל) שאינם ניתנים לחיבור מלא ושלם. חלקי התצרף מרמזים על כך שרק למדינה אחת או לכמה מדינות – ההיגיון הרגיל של "מי צפוי להרוויח" מצביע על ארצות־הברית או על ישראל – היו היכולת והאינטרס לייצר ולשחרר את תולעת הסטקסנט כדי לחבל בתוכנית הגרעין של איראן. אף־על־פי שהעולם לא יידע כנראה לעולם לבטח מי עומד מאחורי קוד התוכנה הזה, מרבית המתכננים האסטרטגיים נכונים להאמין כי "מהלומה דיגיטלית ראשונה" התרחשה, ותיבת פנדורה הווירטואלית נפתחה.

עם זאת, גם אם נניח את התרחיש הקיצוני ביותר, ולפיו רוב המדינות בעולם פיתחו נשק סייבר יעיל ורב עוצמה, או יצליחו לפתח נשק מסוג זה בעתיד הקרוב (הנחה המוטלת בספק), עצם קיומן וזמינותן של יכולות כגון אלה אין פירושו שייעשה בהן בהכרח שימוש. נראה כי תחום הסייבר מוביל בני אדם להניח, כי מאחר שיש להם נקודות תורפה הן בהכרח ינוצלו. בכל זאת, בנושאי אבטחה וביטחון יש לבצע הערכת איומים קפדנית. הערכה כזאת מצריכה העמקה יסודית בשאלה: "למי יש האינטרס והיכולת לתקוף אותנו, ומה הוא צפוי להרוויח מכך?" בעבור מדינות דמוקרטיות רבות, הסיכון של מלחמה נדחק לשוליים. הסיכון של מתקפת סייבר בהיקפים החמורים ביותר צריך להישקל באותה הרצינות.

התרת אפקט תולעת ה'סטקסנט'

פרסום הקוד של תולעת הסטקסנט ופרטים רבים נוספים כבר הובילו להתקפות של מערכות מחשבים רבות נוספות. לפיכך מערכות SCADA – מערכות מחשב המנטרות ומפקחות על תהליכים תעשייתיים ותשתיתיים – צפויות לשמש מטרה לכל פורץ מחשבים בעתיד הנראה לעין. למצב זה נלווית סכנה אינהרנטית של תופעות מכוונות ולא מכוונות – אם כי חשוב לציין כי השיח בנושא תשתיות

חיוניות עוסק באיום על מערכות ה־SCADA זה יותר מעשור. כמו כן, מזה זמן רב מצפים מומחים לאירוע בסדר גודל רציני במרחב הסייבר. מנקודת מבט זו, תולעת הסטקסנט איננה הפתעה גדולה, אלא דווקא אישור למה שדנו בו וחששו מפניו במשך שנים. אף־על־פי שהיא מיקדה את תודעת הפוליטיקאים בשלבים היותר חמורים של איומי הסייבר, באופן זמני לפחות אין היא משנה את הסבירות להתרחשות אירוע של סייבר־טרור או לוחמת סייבר.

תולעת הסטקסנט גם אינה משנה את השיטות והכלים הזמינים להתמודדות עם איומי סייבר. הכוונה למשל לאמצעי אבטחת מידע, או לפעילויות המגוונות והרבות, המושגים והתהליכים הנכללים ב"הגנה על תשתיות חיוניות" (CIP). ההתייחסות ל־CIP דומה למדי במדינות רבות:[13] מבוקשות שותפויות הדוקות עם המגזר העסקי ועם שותפים בינלאומיים, בעיקר כדי להחליף מידע בנוגע לאיומים שונים ולמגוון סוגיות. לאחרונה גם ניכרת התרחקות מהמושג "הגנה", ומעבר לשימוש במושג "גמישות".[14] גמישות איננה מושג חדש כמובן, אך עלייתו הנוכחית מלמדת על שינוי חשוב בחשיבה. בעוד אמצעי הגנה נועדו למנוע התרחשות של שיבושים, הגמישות מקבלת את העובדה ששיבושים מסוימים הם בלתי נמנעים.

לחשיבה כזאת נודעת חשיבות רבה, ועליה להיות מושרשת בתודעת הפוליטיקאים ובתודעת כלל האוכלוסייה. רשתות מידע לעולם אינן יכולות להיות "מוגנות" מן ההיבט של הביטחון הלאומי. ההפך הוא הנכון: שומה על תקריות סייבר להתרחש, מכיוון שאין דרך להימנע מהן. במילים אחרות: אפילו ההגנות המושלמות ביותר לא יוכלו להבטיח ששום דבר חמור לא יתרחש בעולם המרושת.

מדינות נוטות להגיב בכוח לאתגר כזה ומנסות להגביר את רמת הביטחון בכל האמצעים. אך אין לטעות ולראות במרחב הסייבר עוד "תחום" שאפשר לנקוט בו פעולה צבאית לפי שיקול דעת. כדי שיהיה אפשר להמשיך ליהנות מיתרונותיו של עידן הסייבר, חשוב ללמוד באופן מעשי איך לחיות עם חוסר ביטחון. מלבד מגבלות משפטיות ואסטרטגיות, שיובאו ודאי בחשבון בכל התלבטות אם להשתמש במתקפות סייבר ככלי נשק אם לאו, המכשולים הגדולים ביותר צריכים להיות חששות מפני השלכות שליליות שאינן ניתנות לשליטה. ראשית, השלכות עלולות להיווצר ישירות עקב התלות ההדדית בין משאבים חיוניים שונים. שנית, השלכות שליליות עלולות להיות מורגשות באמצעות ההשפעה של אמון מעורער במרחב הקיברנטי, מה שיגרום להשלכות מזיקות לכלכלה העולמית.[15]

באמצעות העברת סוגיה מסוימת, במשתמע או במפורש, לתחום של ביטחון לאומי ופעולות צבאיות, נוטים להכפיף אותה לכללי משחק סכום אפס, שבהם הרווח של צד אחד הוא ההפסד של הצד האחר. עם זאת, ההיגיון של מרחב הסייבר הוא אחר. בדומה לפיקוח על החלל והימים, הפיקוח של מרחב הסייבר מחייב נורמות עולמיות מוסכמות. הדרכים הזמינות כיום ל"בקרת נשק" בזירה זו הן בעיקר

חילופי מידע וגיבוש נורמות, בעוד הניסיונות לאסור לחלוטין את האמצעים של לוחמת סייבר, או להגביל את הזמינות של נשק־סייבר צפויים להיכשל. הקשיים לא צריכים למנוע מהקהילה הבינלאומית לאמץ מגבלות אחראיות וריסון עצמי בשימוש בנשק הסייבר, ולחשוב על דרכים חדשות וחדשניות לשפר את ההגנה על רשתות מחשב חיוניות בלי להפריע ליכולתו של הציבור לחיות ולעבוד בביטחון באינטרנט.

הערות

1 John Arquilla and David F. Ronfeldt, "Cyberwar is Coming!", *comparative Strategy* vol. 12, no. 2 (1993), pp. 141-165.

2 Greg Rattray, *Strategic Warfare in Cyberspace*, Cambridge 2001; Michael O'Hanlon, *Technological Change and the Future Warfare*, Washington 1999.

3 Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*, London 2008.

4 Elgin Brunner and Manuel Suter, International CIIP Handbook 2008/2009, Zurich: Center for Security Studies, 2009.

5 Myriam Dunn Cavelty, "Cyber-Security", in Peter Burgess (ed.), *Routledge Handbook of New Security Studies*, London 2010, pp. 154-162.

6 Chris Demchak, "Cybered Conflicts as a New Frontier", *Atlantic Council*, October 28, 2010, http://www.acs.org/new_atlanticist/Cybered-conflict-new-frontier

7 Bruce Schneier, "Schneier on Security: A Blog Covering Security and Security Technology," Post: "cyberwar," June 4, 2007, http://www.schneier.com/blog/archives/2007/06/cyberwar.html

8 Cf. Clay Wilson, *Computer Attack and Cyber-terrorism: Vulnerabilities and Policy Issues for Congress, Congressional Research Report for Congress*, Washington 2003; Dorothy Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," in John Arquilla and David F. Ronfeldt (eds.), *Networks and Netwars: The Future of Terror, Crime and Militancy*, Santa Monica 2001, pp. 239-288.

9 Martin Libicki, *Defending Cyberspace and Other Metaphors*, Washington 1997, p. 38.

10 Schneier, http://www.schneier.com/blog/archives/2007/06/cyberwar.html

11 Peter Sommer and Ian Sommer, "Reducing Systemic Cybersecurity Risk, OECD/IFP Project on Future Global Shocks, 2011," www.oecd.org/dataoecd/3/42/46894657.pdf

12 שתי דוגמאות בולטות הן:
Mark Clayton, Stuxnet malware is 'weapon' out to destroy ... Iran's Bushehr nuclear plant? September 21, 2010, http://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant; William J. Broad, John Markoff and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, January 15, 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

13 Myriam Dunn Cavelty and Manuel Suter, "Public-Private Partnerships are no Silver

Bulled: An Expanded Governance Model for Critical infrastructure Protection", *International Journal of Critical Infrastructure Protection* Vol. 2, No. 4 (2009), pp. 179-187.

14 Christine Pommerening, "Resilience in Organizations and Systems: Background and Trajectories of an Emerging Paradigm", in *Critical Thinking: Moving from infrastructure Protection to infrastructure Resilience*, *CIP Program Discussion Papers Series*, (Washington 2007), pp. 9-22.

15 Andrew Rathmell, "Controlling computer Network Operations", *Information & Security: An International Journal* 7 (2001), pp. 121-144.

מבט בינתחומי על אתגרי הביטחון בעידן המידע

יצחק בן־ישראל, ליאור טבנסקי

מבוא

התפתחות האלקטרוניקה והמחשב מאז מלחמת העולם השנייה השפיעה על מגוון תחומים רחב ויצרה את "עידן המידע". מאמר זה עוסק ביחסי הגומלין בין טכנולוגיות המידע, עידן המידע והביטחון, ומתמקד בתופעות החדשניות.

חלק ניכר מהדחף לפיתוח עולם המחשוב נגזר מהיישומים הצבאיים. במקביל התפתחה גם החשיבה על השפעת השינוי הטכנולוגי על סוגיות הביטחון. אולם, עידן המידע שממשיך להתפתח במהירות, וכך תקשורת המחשבים ושיבוץ המחשב בכל תחומי החיים יצרו מרחב קיברנטי. נראה שהשינויים מאתגרים את התפיסות הקיימות ומחייבים בחינה מחדש של מושגי יסוד. המאמר נועד לתרום לדיון בסוגיות הביטחון הלאומי הנובעות מהתפתחות טכנולוגיות המידע. הצורך בדיון ציבורי מושכל ובעיצוב מדיניות החלטי מתחזק לאור העובדה כי הסיכון כבר התממש. מספיק להזכיר את האירועים שקרו באסטוניה באביב 2007, ופרשת Stuxnet.[1] במקרה הראשון, אורח החיים של המדינה נפגע בעקבות התקפה פשוטה מבחינה טכנית אך מסיבית על שירותים מבוססי אינטרנט. במקרה השני נראה שהיה שימוש בנשק קיברנטי מורכב מאוד מבחינה טכנית, שעוצב כדי לפגוע במדויק במערכת בקרת תהליך תעשייתי במתקן מאובטח להעשרת דלק גרעיני באיראן. עיצוב הנשק ושיטת הפעלתו כללו הסוואת הפעילות לאורך זמן. נראה שהפעלת הנשק הקיברנטי הזה גרמה לנזקים פיסיים מצטברים בעלי משמעויות אסטרטגיות. בשני המקרים יש הסכמה רחבה שמדינות עמדו מאחורי ההתקפות הקיברנטיות; ובשני המקרים אין ראיות חד־משמעיות.

פרופ' יצחק בן ישראל עומד בראש סדנת יובל נאמן למדע, טכנולוגיה וביטחון, אוניברסיטת תל אביב
ליאור טבנסקי הוא חוקר בתכנית לחקר לוחמה קיברנטית, הנתמכת על ידי קרן ג'וזף וג'נט ניובאוואר, פילדלפיה, ארצות הברית

הבנת הבסיס העיוני של עידן המידע חיונית לליבון סוגיית הביטחון הקיברנטי. במאמר נשתמש בהגותם של הפילוסוף קרל פופר, הסוציולוגים העתידנים אלווין והיידי טופלר, והכלכלן פול רומר לביאור המאפיינים של עידן המידע, ולבירור סוגיות ביחסי הגומלין בין ההתפתחות הטכנולוגית לביטחון הלאומי. בהמשך ננתח את מאפייני המרחב הקיברנטי של היום, ונדון במשמעויות לענייני הביטחון הלאומי. בחלק השלישי נסקור את התחום המוכר כ"לוחמת מידע" ונתמקד בתופעה החדשנית: לוחמת המחשבים במרחב הקיברנטי. בהמשך המאמר נסקור את כלי הנשק הקיברנטיים ושיטות הלחימה, נדון בהגנה, בהתקפה, ובהרתעה. נציג סוגיות מרכזיות העולות בתחום הביטחון הקיברנטי. נראה שעל מנת לשמור על הביטחון והשלום, נדרשת בחינה רב־תחומית של הסוגיות והאתגרים החדשים.

הקדמה עיונית

השינוי הטכנולוגי מעסיק הוגים רבים שמתחבטים בהבנתו ובבחינת ההשפעות החברתיות שלו. נזכיר שלושה הוגים הרלוונטיים להבנת המציאות המשתנה, אולם מפאת מסגרת הפרסום לא נוכל להרחיב את הדיון בנושא.

המונח הגל השלישי לקוח מבית מדרשם של זוג הסופרים שחיבוריהם הם רבי־מכר, אלווין והיידי טופלר מתאר תקופה. לטענתם, אנו נמצאים בעיצומו של המעבר לגל השלישי, אשר בו מבוססת הכלכלה על ידע ושליטה במידע,[2] במקום על ייצור תעשייתי המוני.

טבלה 1: שלושת הגלים – לפי טופלר

	משאב עיקרי	מיהו עשיר?	סמל	כלי מלחמה	דרך המלחמה
הגל הראשון	חקלאות מאורגנת	בעל אדמות	מגל	חרב	קרב פנים אל פנים בטווח אפס; כיבוש (אדמה)
הגל השני מאמצע המאה ה־17 עד סוף המאה ה־20	תעשיה ממוכנת, ייצור המוני	תעשיין	מכונות של קווי יצור המוני	טנק, מטוס	קרב באמצעות מכונות, מטווח בינוני־רחוק; דיוק נמוך; ניסיון לפגוע בכושר הייצור
הגל השלישי מסוף המאה ה־20 ואילך	ידע	ביל גייטס	מחשב	לוחמת מחשב Cyber Warfare	ניסיון לפגוע במידע באמצעים ממוחשבים. פגיעה מרחוק בכושר התפקוד, מבלי להגיע פיסית אל היעד

גם צורת המלחמה משתנה. שם המשחק יהיה השגת מידע על האויב ומניעת מידע על עצמך. מי שישלוט בטכנולוגיות המידע ינצח במלחמה, גם אם יעמדו מולו כלים רבים שייפלטו מקווי הייצור של הגל השני.

שלושת העולמות של פופר

בנוסף לשימוש בתזה של הזוג טופלר, נעזר בכמה מושגים מבית היוצר של הפילוסוף **קרל פופר** אשר הלך לעולמו ב־1994. פופר בחן את עולם הידע כמושג הקיים נוסף על עולם החומר ועולם הרוח.[3] לטענתו, קיים "עולם" שלם של ידע אנושי (פופר מכנה אותו עולם־3) המאוכלס ב"יצורים" שהם תוכן אובייקטיבי של מחשבה, כמו משפט פיתגורס וחוקי הפיסיקה, שאינם "חומר" ואינם "חוויות מנטליות" סובייקטיביות. מרגע שנוצר משפט פיתגורס הוא אמת אובייקטיבית, שאינה תלויה עוד ברוח שיצרה (או גילתה) אותו. הידע הוא אובייקטיבי אף שהוא תוצר של הרוח האנושית (הסובייקטיבית).

טבלה 2: שלושת העולמות של פופר והמרחב הקיברנטי – מאפיינים עיקריים

	תכולה	מעמד	דוגמאות	דוגמה במרחב הקיברנטי
עולם – 1	חומר	אובייקטיבי	שולחנות, מטוסים	חומרה
עולם – 2	חוויות מנטליות	סובייקטיבי	כאב, שמחה	תצוגות (חוויית משתמש)
עולם – 3	ידע	אובייקטיבי	מתמטיקה, פיסיקה	תוכנה

כלכלת עידן המידע

שלא כמו בחומר, אפשר להשתמש בידע שוב ושוב, ולחלק אותו לצרכנים רבים בלי שהוא יתמעט. הידע הוא "סחורה" בלתי־נדלית. הכלכלן פול מ' רומר, ממובילי המחקר בתורת הצמיחה החדשה, דן בהשלכות הכלכליות של ידע, ובמאמרו בו הוא מניח יסודות לכלכלה "אחרת", מבוססת ידע.[4] מתברר שהכלכלה, הבסיס לעוצמה ולשגשוג, צומחת לא רק כתוצאה משינויי הון וכוח האדם, והתפתחות הידע היא מקור חדש לצמיחה. אופי הצמיחה מבוססת הידע שונה מהמוכר לכלכלה המסורתית.

אם ננסה לאחד עתה את הבסיס המטאפיסי של פופר עם הסוציולוגיה של טופלר ועם תורת הכלכלה של רומר, נוכל לטעון כי מלחמות הגל השני והראשון התנהלו בעיקר בעולם־1 ("חומר"). במלחמות אלו ניצח מי שהשכיל להעמיד

צבא גדול וחזק יותר, ומי שידע לגייס לעזרתו ולטפח את הגורמים המנטליים (עולם־2) של גייסותיו (כמו רוח־קרב, מוטיבציה, אומץ לב וכו'). לפי תיאור זה, מלחמות העתיד יתפשטו גם לעולם־3, עולם המידע. מבלי להפחית בערכם של גורמים אלו גם בעתיד, הרי בעוד מלחמות העבר (הגל הראשון) נשענו על כוח הזרוע, ומלחמות ההווה (הגל השני) נשענות על כוח המכונות, ישענו מלחמות העתיד יותר ויותר על כוח המוח.

התמודדות אינטלקטואלית עם עידן המידע בתחום הביטחון הלאומי

סמלו המובהק של עידן המידע – המחשב האלקטרוני – נבנה עם סיום מלחמת העולם השנייה כדי לעזור לצבא ארה"ב בחישובים בליסטיים לארטילריה. בשישים השנים שלאחר מכן, בייחוד אחרי המצאת הטרנזיסטור והמעגל המוכלל, הלכו מימדי המחשב וקטנו בהתמדה. גורדון מור, ממייסדי יצרנית המעבדים "אינטל", העריך בשנת 1965, שבכל שנה עד שנתיים יכפיל מספר הטרנזיסטורים את עצמו בשבב המוכלל, בעוד שהמחיר יישאר קבוע.[5] משהתברר שאכן הדבר מתקיים בתחום המוליכים למחצה, הניבוי זכה לכינוי "חוק מור". העתידן ריי קורצוויל מציג טיעונים משכנעים בעד הרחבת "חוק מור" לטכנולוגיות המידע בכללותן.[6]

עם התפתחות המחשב והקטנת ממדיו, עסקו מוסדות הביטחון בשיפור הביצועים של מערכות רבות באמצעות שיבוץ מחשב. התרומה המרכזית התבטאה במהפכת הדיוק של החימוש, וראשיתה בכוח האווירי. תחילה תרמו המחשבים לשיפור בתכנון המבצעים. כשהתאפשר להכניס מחשב למטוסי קרב, נרתם כוח החישוב למשימות התקיפה. שינוי אסטרטגי של ממש התחולל כאשר מימדי המחשב ומחירו קטנו עד שאפשר היה להכניסם לחימוש עצמו. כך נולד עידן "החימוש החכם", חימוש מונחה מדויק, שאומץ תחילה בחימוש אווירי. התוצאות המבצעיות היו מרחיקות לכת. מה שמסוגל לעשות כיום מטוס עם חימוש חכם, בתקיפת מטרת נקודה דוגמת טנק, שקול למה שיכלו לעשות 15 מטוסים לפני 30 שנה או 60 מטוסים לפני 40 שנה.[7] אין פלא כי למהפכה הטכנולוגית הזו יש השפעה מכרעת על תורת הלחימה.

כדי להתאים את אומנות המלחמה לטכנולוגיות המידע, פותחה בראשית שנות התשעים של המאה העשרים תורת לחימה חדשה, "המהפכה בעניינים צבאיים" (Revolution in Military Affairs – RMA). התפישה עומדת על ארבעה יסודות: תקיפה מדויקת; חלל; שליטה בתמרון; לוחמת מידע.[8] לוחמת מידע נוגעת לכמה היבטים שונים: לוחמת מחשבים (שהם האמצעי הטכנולוגי העיקרי לאחסון ושינוע מידע), לוחמה אלקטרונית (בעיקר נגד מערכות קשר ותקשורת), לוחמה פסיכולוגית וטיפול באמצעי תקשורת (החל מתדרוך עיתונאים, דרך עיתונאים

המשובצים בכוחות הלוחמים וכלה במניפולציה במידע המשוחרר לציבור). חשוב לדייק במושגים ולהבין היטב למה מתכוונים במונח "לוחמת מידע", וכפי שנראה בהמשך, המושגים הללו השתנו עם הופעתו והתפתחותו של המרחב הקיברנטי.

התוצאה הישירה של ה־RMA היא עליונות צבאית מוחלטת של צבאות המדינות המפותחות בשדה הקרב[9] – כפי שזו באה לידי ביטוי במלחמות ארצות־הברית בעיראק ואפגניסטן, ובמלחמות ישראל בלבנון ונגד ארגוני הטרור. תוצאה נוספת של ה־RMA היא היכולת חסרת התקדים לנהל לחימה בעצימות נמוכה מדויקת ויעילה, ואף היכולת לגבור על טרור באמצעים צבאיים – בלי לגרום נזק סביבתי רחב.[10]

ואולם התפתחות המחשוב ממשיכה, ומחייבת שינוי תפיסתי מתמשך. החלק הבא במאמר נועד לספק בסיס לתפיסה מעודכנת של הביטחון הלאומי במציאות הכוללת מרחב קיברנטי חדש.

המרחב הקיברנטי

התפוצה המתמשכת של המחשוב ורשתות התקשורת יצרה בראשית המאה ה־21 מצב חדש: שכבה ממוחשבת נוספה על המערכות הקיימות הוותיקות, והיא שולטת למעשה בתפקודן. תפוצת המחשבים, שיבוצם בהתקנים שונים וחיבורם ברשתות התקשורת – כל אלה יוצרים את המרחב הקיברנטי. המושג מאפשר לנו להבין את המתרחש בעולם־3,[11] תוך מיקוד ביחסי הגומלין עם סוגיות הביטחון הלאומי: רשתות הקשורות ביחסי גומלין של תשתיות טכנולוגיות מידע הכוללות רשתות בזק, רשתות ייעודיות, האינטרנט, מערכות מחשב ומערכות משובצות מחשב. המושג כולל גם את הסביבה הווירטואלית – המידע המאוחסן, המעובד והמועבר על הרשתות הללו וביניהן.[12]

שלא כמו יבשה, ים, אוויר, חלל או ספקטרום אלקטרומגנטי, המרחב הקיברנטי אינו תוצר הטבע. המרחב הקיברנטי נוצר בידי בני האדם, ולא היה קיים בלא טכנולוגיות המידע שפותחו בעשרות השנים האחרונות. הידע – שהוא אולי המרכיב החשוב ביותר במרחב הקיברנטי – הוא תוצר של פעילות אנושית מצטברת.[13] המבנה והעיצוב של המרחב הקיברנטי כפי שהוא היום טומנים בחובם השלכות משמעותיות לענייני הביטחון הלאומי.[14]

אפשר לתאר את המרחב הקיברנטי כמורכב משלושה רבדים.[15]

1. הרובד המוחשי ביותר, המשמש היום תשתית של עולם המחשוב, הוא הרובד הפיזי. הרכיבים הפיסיים הם אבני הבניין המוחשיים של המרחב הקיברנטי, אבני בניין עם מאפיינים טבעיים: רוחב, גובה, עומק, משקל, נפח.[16] הרובד החומרי – חופף את "עולם־1" בתפיסה של פופר.

2. הרובד השני הוא לוגיקה של תוכנה: מגוון מערכי הוראות שתוכנתו בידי בני אדם. הרכיבים הפיזיים נשלטים במידה רבה על־ידי התוכנה, והמידע המאוחסן במחשבים נתון לעיבוד באמצעות הוראות התוכנה. רובד התוכנה הוא בחלקו "פיסי" (עולם־1) ובחלקו "לוגי", דהיינו, שוב, עולם־3.
3. הרובד השלישי של המרחב הקיברנטי הוא רובד הנתונים שהמכונה מכילה ומעבדת. הנתונים ועיבודם יוצרים מידע וידע. הרובד הזה הוא הפחות מוחשי מהשלושה, בעיקר משום שמאפייני המידע שונים מאוד ממאפייני האובייקטים הפיזיים. זהו רובד השייך במובהק לעולם־3 של פופר.

טבלה 3 : מאפייני המרחב הקיברנטי ונקודות תורפה העולות מהם

מאפיין	תורפה
שינוי בקצב מהיר	התיישנות מהירה של אמצעים, כולל של מערכות הגנה.
מבנה הפרוטוקול TCP/IP	קשה להתחקות אחר האות ברשת ולזהות את מקורו.
רמת סיבוכיות גבוהה	קשה מאוד לקשר בין אירוע לתוצאה; קשה להבדיל בין תקלה לתקיפה.
שימוש רחב בציוד מסחרי סטנדרטי, מן־המדף	צמצום פערי היכולות בין שחקנים קטנים לגדולים. פגיעות של חומרה ומערכות הפעלה זהות מסכנת קשת רחבה של מערכות.
אמצעי הלחימה הבסיסיים – זולים יחסית	מחיר ההגנה הולך ועולה.
סביבה משפטית מעורפלת	"תחום אפור" עם סיכוי נמוך לענישה– מעודד חוסר יציבות.

מלחמת מידע ללוחמה קיברנטית

בספרות המקצועית האמריקנית והאירופית,[17] לוחמת המידע נתפסת כמאפיין מובהק של עידן המידע. בעגה הצבאית האמריקאית מכונה לוחמת המידע בשם Information Operations. החלק הממוחשב שלה קרוי Computer Network Operations (CNO).[18]

מבט בטבלה 4 מגלה שלמעשה אלו נושאים "קלאסיים", שהעיסוק בהם ימיו כימי המלחמה עצמה. במרוצת ההיסטוריה פותחו כמה שיטות לוחמה קלאסיות ל"לוחמת מידע", החל באיסוף מודיעין באמצעות "חיישנים" אנושיים (ראה פרשת המרגלים בימי יהושע בן־נון) וכלה בפיתוח טכנולוגיות איסוף מיוחדות (כמו חיישני מודיעין מוטסים, לוויינים וכו'). גם בתחום המניעה פותחו שיטות קלאסיות בלוחמת מידע, כמו הסוואה, דמיים ומיסוך, שיבוש וחסימה, הונאה והטעייה, תעמולה ועוד.

טבלה 4: נושאים הנכללים תחת הכותרת לוחמת מידע

נושא	מערכות וטכנולוגיות רלוונטיות
איסוף מידע	חיישנים שונים בכל תחומי הספקטרום האלקטרו־מגנטי
שינוע מידע לעיבוד ולצרכן	תקשורת רחבת סרט, דחיסה, הצפנה
אחסון ושליפה	בסיסי נתונים, De-Duplication, דחיסה
עיבוד וסינון מידע	עיבוד אותות דיגיטאלי (DSP), אלגוריתמים לזיהוי אוטומטי (ATR), מיזוג נתונים (Data Fusion), אינטליגנציה מלאכותית (AI)
הנגשת מידע	תקשורת רחבת סרט; מערכות תצוגה וממשק אדם־מכונה
מניעת מידע	הסתרה, שיבוש, לוחמה אלקטרונית (ל"א), הצפנה, הטעיה
הגנה על מידע	מניעת גישה למידע שלך מבלתי מורשים, הצפנה

עיון בטבלה 4 לעיל מוביל למסקנה, שהחידוש הכמעט יחיד בתחום זה הוא התלות הגוברת והולכת של מערכות המידע במחשב. במילים אחרות, בעוד שלוחמת מידע אינה תחום חדש, הרי שאין הדבר כך לגבי מערכות המידע משובצות המחשב. המרחב הקיברנטי מאפשר להגדיר מטרות, כלי נשק ושיטות לחימה חדשים. מה שייחודי למלחמת הגל השלישי, מלחמה בעידן המידע, אינו לוחמת מידע לכשעצמה אלא לוחמת מחשבים. משום כך ראוי לצמצם את תחום הדיון ולהתמקד בלוחמת מחשבים במרחב הקיברנטי. החדשנות במרחב הקיברנטי כה רבה, עד שמושגי היסוד כגון "מלחמה", "נשק", "התקפה" ו"הגנה" זקוקים לביאור מחודש.

לוחמת מחשבים במרחב הקיברנטי היא חדירה בלתי מורשית למערכות המחשב של היריב לשם איסוף מודיעין, שיבוש, הטעיה, מניעת שימוש והשהיית המידע. זאת במקביל למניעת הישג דומה של היריב במערכות המחשב שלנו. גם תקיפה מסורתית (הפגזה, הפצצה, חבלה פיזית) של מערכות מחשב תגרום ודאי שיבוש, מניעה והשהיית המידע. אולם תקיפה פיזית כזאת אינה נכללת בלוחמה קיברנטית.

מאפייני המרחב הקיברנטי[19] מגדירים גם את הלוחמה בתחום הזה. מאפייני המרחב הקיברנטי מקשים על ההבחנה בין פגיעה מכוונת לתקלה, ומקשים על האפשרות לייחס פעולה לגורם מסוים (attribution), ולכן גם מקשים להגיב על תקיפה. מאפייני המרחב הקיברנטי היום מעצימים שחקנים שוליים ומקנים יתרון לתוקף לעומת המגן.

בשנים האחרונות מתפתח דיון בפגיעות שנוצרה לאור חיוניות המרחב הקיברנטי לכל תהליכי החיים בחברה המפותחת.[20] לוחמת מחשבים אינה מוגבלת

למערכים צבאיים; עם תפוצת המחשוב ורשתות התקשורת היא הפכה ישימה בכל תחומי החיים. רוב המערכות במשק האזרחי – תלויות היום במחשבים ומחוברות למרחב הקיברנטי. עובדה זו יוצרת פגיעות, הפותחת אפשרויות חדשות ללחימה ודורשת הערכות הגנתית גם של המדינות המפותחות.

התקפה והגנה במרחב הקיברנטי[21]

כלי הנשק הקיברנטי הוא תוכנה זדונית או חומרה מזיקה, הפוגעת במשאב הממוחשב של הקורבן וגורמת לשיבוש נתונים, הטעיה, מניעת שירות או איסוף והעברת מודיעין. אנו מציעים תרגום עברי למונחים האנגליים בתחום:

malware– תוֹקעה. תוכנה זדונית שמיועדת לשבש בסתר פעילות תקינה של מערכת ממוחשבת, וכך לפגוע בתהליך שמנוהל באמצעות אותה מערכת.

spyware– רוֹגלה. תוכנה זדונית שמיועדת לאסוף נתונים בסתר ולעתים להעביר אותם ברשת;

phishing – דיוג. תרמית מבוססת תוכנה והנדסה חברתית על מנת להשיג במרמה נתונים אישיים של משתמשים ופרטי הזדהות.

השתלת חומרה יכולה להיעשות בהוספת רכיב אלקטרוני נוסף ליחידה קיימת או תוספת בתוך מעגל משולב. ההשתלה יכולה להתבצע בשלב הייצור, ההובלה, התפעול תחזוקה ותיקון.[22] השימוש בתוכנה כנשק לוגי נפוץ מהשימוש בחומרה. אפשרות זו מאפשרת את שיטות הלחימה החדשניות ביותר. הידע והטכנולוגיה הם מוצרים בלתי־נדלים, ובכך חשיבותם העצומה בכל הנוגע ללוחמת המידע, ולא כל ההשלכות כבר הובררו במלואן.[23]

בשעה שמתבסס החשד שמתרחשת התקפה קיברנטית, קשה מאוד לזהות את מקורה ואת זהות התוקף. כל הגורמים הפועלים במרחב הקיברנטי משתמשים באותם הכלים והשיטות. פעמים רבות קיים שיתוף פעולה מסחרי, מעין "מיקור חוץ", בין הגורמים הטכניים בעלי יכולת התקיפה (מתכנתים, פורצי הצפנה, בעלי רשתות שבויות), למזמיני שירותים (חוקרים פרטיים, פשע מאורגן, ארגוני ביון). כדי לקבוע שתקיפה קיברנטית היא מעשה מלחמתי, יש לבחון כמה מאפיינים:

- **מקור ארגוני וגיאוגרפי**: האם מדינה עומדת מאחורי הפעולה?[24]
- **מניע**: האם אפשר לזהות מניע אידיאולוגי, פוליטי, כלכלי, דתי למתקפה?
- **רמת המורכבות**: האם המתקפה דרשה תכנון מורכב ומשאבים מתואמים, אשר זמינים בעיקר לגופים מדינתיים?
- **תוצאה**: האם ההתקפה גרמה לנזק ונפגעים? האם הייתה גורמת נזק לולא פעולות ההגנה?

מאפייני המרחב הקיברנטי מקשים לתת תשובות לשאלות הללו, ודאי לא תשובות המספיקות לקביעת מדיניות.

כדי להתגונן צריך לזהות שמתרחשת מתקפה, וכאמור הדבר אינו פשוט כלל במרחב הקיברנטי. ככל שהחדרת כלי הנשק תעשה מוקדם יותר, ובייחוד לפני גיבוש תוכניות בדיקה, הסיכוי לגילוי קטן. ככל שהנשק הקיברנטי יהיה מדויק יותר, כך הוא יגרום פחות נזק סביבתי ויפחית הסיכוי שהמותקף יגלה את דבר ההתקפה. פעילות ההתגוננות מכילה שלושה מעגלים:[25]

1. **הגילוי**: זהו "עקב אכילס" של התחום – כיצד נדע שהתרחשה תקיפת מחשבים?
2. **המניעה**: הפעלת אמצעים לעצירת התוקף בשלב החדירה.
3. **התגובה**: בכלל זה אמצעי התאוששות לצמצום הישג התוקף, אמצעי זיהוי פלילי ואף "פעולת תגמול".

סוגיות מרכזיות בלוחמה קיברנטית

השינוי הטכנולוגי, הנמצא ביסוד מעבר ל"גל השלישי", להרחבה מהירה של "עולם־3" ולהתפתחות "כלכלת המידע", מעלה שאלות חדשות. אחת המרכזיות היא שאלת ההגנה על תשתיות חיוניות. בשנים האחרונות אנו עדים לדיון מתפתח על ההגנה על התשתיות חיוניות, המונחות ביסוד החברה המודרנית. היתכנות האיום הוצגה בניסויים, למשל מתקן לייצור חשמל הוצא מכלל שימוש והתפוצץ באמצעות שידור הוראות למערכת השליטה והבקרה.[26] נראה שהאיום התממש בפרשה שנתגלתה בקיץ 2010: וירוס תולעת המכונה Stuxnet התפשט במחשבי "חלונות" וחיפש בינם מחשבים המריצים תוכנת שליטה ובקרה תעשייתית תוצרת "סימנס" מסוג מסוים, המחוברים לבקר תעשייתי מדגם מוגדר. כאשר איתר את המחשבים הרלוונטיים, הפעיל הווירוס קוד תוכנה ששיבש את פעילות הבקר הממוחשב תוך הסתרת השינוי מתוכנת השליטה וממפעילי הציוד. נטען כי בסופו של דבר, פגע סטאקסנט בהפעלה התקינה של הצנטריפוגות להעשרת אורניום באיראן. משך התקיפה ומקורה – אינם ידועים.[27]

תשתיות חיוניות של המדינה הן יעד מתבקש במהלך סכסוך. מדוע אפוא עלה כעת החשש הזה, ודווקא במדינות החזקות ביותר? ארצות הברית שנהנית ממעמד של מעצמת־העל היחידה בעולם – היא החלוצה והמובילה בדיון על פגיעותה הקיברנטית.[28] התשובה נעוצה במעבר מ"מלחמות הגל השני" של טופלר אל מלחמות "הגל השלישי", גל המידע. הדיון המחודש בהגנה על התשתיות החיוניות נעוץ בהופעת איום חדש, שלא היה בר ביצוע לפני כן. התפתחות המרחב הקיברנטי מאפשרת, לראשונה בהיסטוריה, לתקוף מערכות תשתית חיוניות במרחב הקיברנטי, בלי להגיע פיזית אל מקום הימצאותן ובלי להיחשף במהלך התקיפה. נניח שיום אחד יתמוטטו מערכות המחשבים של הבנקים בישראל. נניח גם כי נצליח לקבוע בוודאות כי הנזק העצום נגרם במכוון, בחדירה מכוונת, ונניח שנצליח לאתר את התוקף בשטחה של מדינה שכנה. האם זו תקיפה מלחמתית?

לכאורה הנזק שנגרם הוא "רק" כלכלי ולא נפגעו חיי אדם (ישירות). פעמים רבות מדינות הבליגו על תקיפות מסורתיות שגרמו נזק כלכלי אך לא פגעו בחיי אדם.[29] אבל נזק כלכלי עלול לגרום לשיתוקה של מדינה שלמה. נושא ההגנה על תשתיות מידע לאומיות חיוניות הוא אחד המרכזיים בדיון על ביטחון קיברנטי. נושא ההגנה על תשתיות חיוניות חורג מגבולות מאמר זה, וראוי לטיפול ממוקד.[30]

"מלחמה מידע" מעלה מיד הרהור על מושג המלחמה עצמו: האם תקיפה קיברנטית של המידע הממוחשב, ללא שימוש באש – היא "מלחמה"? מהי מטרה לגיטימית במלחמה כזאת? השימוש הצבאי הנרחב בתשתיות אזרחיות (בעיקר לתקשורת) מקשה על ההבחנה בין מטרה צבאית לאזרחית. כך, תשתית המחשוב של משרד ההגנה האמריקני מורכבת מ־15,000 רשתות ושבעה מיליון התקנים הפזורים ברחבי העולם. אולם רוב התקשורת של משרד ההגנה מנותב ברשתות אזרחיות מסחריות.[31] אזרחים (גם ילדים ונשים) יכולים להיות יעילים כלוחמי מחשבים לא פחות מחיילים. האם זה הופך אותם מטרות פוטנציאליות לתגובה? כיצד יש לפעול במקרה של נזק כלכלי רחב? כיצד אומדים את הנזק העקיף שהתקיפה גרמה? נניח שתקיפה קיברנטית גרמה לשיבושים ממושכים באספקת חשמל. נניח שאחת התוצאות היא כיבוי מערכות התאורה והרמזורים בכביש, ושבעלטה אירעה תאונות דרכים קטלנית. האם להתייחס לקורבן התאונה כחלל במלחמה קיברנטית? כיצד יש להגיב: באש ובתמרון, או במכת־נגד קיברנטית? הבעיה סבוכה יותר מהתרחיש שתיארנו, משום שתקיפת מחשבים אינה זקוקה לבסיס מדינתי, והיא יכולה להיעשות גם על ידי ארגונים ואף יחידים.

לוחמת מחשבים מתנהלת גם בין מדינות ידידותיות בתחרות להשיג למודיעין דיפלומטי וכלכלי. האם ראוי לקרוא לזה "לוחמה"? האם ראוי להפעיל לוחמת מחשבים בימי שלום למטרות כאלה?

הבעיה המיוחדת בנושא הלוחמה הקיברנטית היא זיהוי התקיפה: בניגוד לתקיפה מסורתית המתרחשת בעולם־1, שהוא עולם החומר, איתור הפגיעה וזהות התוקף אינם בהכרח נחשפים לאחר התקיפה. ללוחמת מחשבים גם אין "קו חזית" מוגדר ואין בה כמעט משמעות למרחקים גיאוגרפיים. נוכח מאפייני המרחב הקיברנטי, עצם זיהוי התקיפה אינו מובן מאליו: לתקיפה ולתקלות יש תסמינים דומים. עם השתכללות עולם המחשבים, המתבטאת בריבוי התוכנות והיישומים, ובריבוי מספר הטרנזיסטורים בכל רכיב – הסבירות לתקלה אינה יורדת. ההסתברות הסטטיסטית לשגיאת תכנות (Bug) בתוכנה היא קבועה, וערכה הנומינלי עולה עם ריבוי המורכבות של תוכנות.[32]

כאמור, היכולת לזהות שהמחשבים שלך הותקפו ונפגעו, ולא התקלקלו באופן "טבעי" – לוקה בחסר. בלי היכולת להבחין בזמן אמת בין מתקפה לתקלה, נדרשת השקעה כבדה ב"כוננות קיברנטית" מתמדת. ההגנה מפני איומים קיברנטיים

חייבת להקיף את כל אפיקי התקיפה, להתעדכן עם פיתוחים חדשים, ומחיר ההגנה הולך ועולה. הטיעון על קושי ההגנה דומה לטיעון נגד הגנה אקטיבית נגד טילים, ולטיעון על עקרות הגנה נגד מחבל מתאבד. עם זאת, ניתן לייצר מענה לאיומים החדשים.[33] על ההגנה מוטלת מעמסה רבה מכיוון שבמאפייני המרחב הקיברנטי של היום יש יתרון ברור להתקפה על פני ההגנה.[34] תחום ההצפנה הוא אחד הבודדים במרחב הקיברנטי שבו המגן נהנה בינתיים מיתרון על התוקף.[35] בהינתן הקושי לזהות את עצם התקיפה, מקורה הגיאוגרפי וזהות התוקף, מתקבל מצב של חוסר וודאות המקשה על תגובה מסלימה. טבלה 3 לעיל מסכמת את המאפיינים ואת נקודות התורפה הרבות היוצרים את "בעיית הייחוס": קשה לדעת את מקור התוקף וזהותו, בשליחות מי פעל, וודאי שקשה להוכיח אשמה. בתחום הביטחון המסורתי מוקדש מאמץ רב לנושא המודיעין, ההתרעה, וההרתעה, כדי לצמצם ככל האפשר משאבים המופנים לקיום כוננות מתמדת. נושא ההרתעה הוא בעייתי במיוחד במרחב הקיברנטי בעיקר עקב בעיית הייחוס.[36] אם מתגברים עליה, ומוציאים לפועל תקיפה קיברנטית, מאפייני המרחב הקיברנטי מעלים בעיות נוספות. כיצד לזהות שהמחשבים שניסית לתקוף, בתגובה על מתקפה קיברנטית שאיתרת, אכן נפגעו? כדי שיהיה אפשר להסתמך על התקפה קיברנטית נדרשת בקרת תוצאות (battle damage assessment). מבחינה זו, לתקיפה המבוצעת "בחוג פתוח", כלומר כזו שלא ידוע אם הצליחה, יש תועלת מוגבלת. בעיה זו חריפה במיוחד בתקיפה קיברנטית.

בלוחמה קונבנציונלית התפתחו "חוקי משחק" המעוגנים באמנות בינלאומיות. אמנות אלו נוסחו לפני הופעת המרחב הקיברנטי, והן עוסקות ב"מאבק מזוין", ב"עימות פיזי", ב"פגיעה טריטוריאלית" וכדומה. המושגים האלה אינם רלוונטיים ללוחמת מחשבים, והאמנות הקיימות דורשות התאמה ללוחמה קיברנטית, מלחמה ב"גל השלישי". על אף המחקר הענף בתחום, סביר להניח שבחינת הסוגיות מזווית המשפט תמשך שנים רבות. העדר "חוקי משחק" מקשה על התמודדות היומיומית עם הבעיות המיוחדות של הלוחמה הקיברנטית. הסוגיות שסקרנו אינן משפטיות גרידא, אלא סוגיות מדיניות הכרחיות לקבלת החלטות ולביצוען. כך בימים אלה (סתיו 2011) שוקדים בנאט"ו על גיבוש מסגרת משפטית שתאפשר לארגון להגיב על מתקפות קיברנטיות בשיטות שחוקיותן מעורפלת במצב המשפטי הקיים. הבנת היסודות העיוניים של התחום חיונית לשיפור יכולת ההתמודדות.

סיכום

המרחב הקיברנטי הוא תוצר חדש למדי של עידן המידע. ביטחון קיברנטי הוא חלק מסוגיה חדשה: המעבר לעידן המידע. על מנת להתמודד עם השינוי המאתגר, יש לאמץ פרספקטיבה רב תחומית. לכן הצגנו בתחילת המאמר מקורות עיוניים

אחדים של עידן המידע. בחרנו לגייס למשימה מרעיונותיהם של הזוג טופלר, ושל קרל פופר ופול רומר, אולם ברור לנו שיש עוד מקורות, ואנו בטוחים שנראה מחקר בינתחומי נוסף בנושא "עידן המידע". לאחר מכן סקרנו את רכיבי הלוחמה הקיברנטית: נשק, הגנה, התקפה, מלחמה, תוך נגיעה הכרחית ביסודות הטכניים מתחום המחשבים.

הבעייתיות בהתמודדות עם אתגרי ביטחון נובעת ממאפייני המרחב הקיברנטי: מהירות הפעולה, קצב השינוי, מורכבות וסיבוכיות. ההגנה וההתקפה הקיברנטית מתרחשים בעולם־3, עולם הידע. יש לחקור לעומק את ההשלכות המהותיות הנובעות מהסוגיות המרכזיות של לוחמה קיברנטית, שתוארו בפרק האחרון במאמר.

החידוש המרכזי אינו "לוחמת המידע" אלא לוחמת המחשבים במרחב הקיברנטי. הדיון בפתרונות ל"ענייני מחשבים" נוטה להתרכז בתחום הטכני, המרוחק מהדיון הציבורי וממרחבי עיצוב המדיניות הציבורית. ברור שדרושה הבנה מקצועית בתחום הנדון, והוא מציב אתגרים כבירים הדורשים מענה ברמת המדיניות הציבורית הלאומית. סקירת הסוגיות המרכזיות של לוחמת המידע מציגה תמונה מורכבת, אל מעבר למקצועות המחשב. לפיכך כדי לספק ביטחון לאומי בסביבה המשתנה של עידן המידע, ראוי להשתמש בתשומות מכל תחום ידע רלוונטי: כלל מדעי החברה, פסיכולוגיה ופילוסופיה. אנו מקווים שהמאמר יעודד מחקר בינתחומי של אתגרי הביטחון הקיברנטי, יתרום לפיתוח מדיניות ביטחון לאומית מושכלת ובסופו של דבר יתרום לביטחון ושגשוג בעידן המידע.

הערות

1 "The Meaning of Stuxnet: A sophisticated "cyber-missile" highlights the potential—and limitations—of cyberwar," *Economist (GBR) Economist* 397, no. 8702 (2010). September 30, 2010, from the print edition.

2 ניתן להבחין בין מידע (Information) או נתונים (Data) ובין ידע (Knowledge) המחייב גם המשגה והבנה של המידע הגולמי. לצורך המאמר, ההבחנה אינה מהותית.

3 K. Popper, *Objective Knowledge - An Evolutionary Approach*, Oxford University Press, 1972. פרקים 4–3

4 Paul M. Romer, "Endogenous Technological Change", *Journal of Political Economy*, 1990, Vol. 86, no. 5, pt 2, pp. S71-S102.

5 Mollick, E. "Establishing Moore's Law." *Annals of the History of Computing, IEEE* Vol. 28, no. 3 (2006), pp. 62-75.

6 Ray Kurzweil, "The Law of Accelerating Returns" (2001).

7 יצחק בן־ישראל, "מלהב החרב אל זיכרון המחשב" **אודיסאה** 9, אוקטובר 2010.

8 לקורא המתעניין ב־RMA בהקשר של טכנולוגית המידע מומלצים הספרים הבאים: Michael E. O'Hanlon, *Technological Change and the Future of Warfare*. (Washington, D.C.: Brookings Institution Press, 2000). Stuart E. Johnson and Martin C. Libicki, *Dominant Battlespace Knowledge: The Winning Edge*. (Washington, DC:

National Defense University Press, 1995).

9 עליונות שהביאה לנסיגת האויבים לאסטרטגיה של הישרדות ולחימה א־סימטרית.

10 היכולת הוצגה לראשונה בניצחונה של ישראל על "אנתפאדת המתאבדים" הפלסטינית בשנים 2000–2005. ראה: ליאור טבנסקי, **המאבק בטרור בעידן המידע: 'אינתיפאדת המתאבדים' וההתמודדות הישראלית עמה בסיוע טכנולוגיות עילית.** אוניברסיטת תל אביב, תל־אביב (2007).

11 ראה לעיל על המושג מבית מדרשו של קרל פופר.

12 הדמיון הרב להגדרות אמריקניות מקורו בדמיון בין ארצות הברית וישראל בכל הקשור לערכים ולרמה מדעית וכלכלית. סין, רוסיה, הודו, צרפת ואחרות – מגדירות את המרחב הקיברנטי והאיומים הקיברנטיים בצורות שונות. אולם, העיסוק בנושא זה חורג מגבולות עבודה זו.

13 הדיון על מעמד הידע מופיע אצל קרל פופר, ומוזכר בפרק הקודם.

14 לדיון על המרחב הקיברנטי בהקשר לביטחון הלאומי ראו: ליאור טבנסקי, "לחימה במרחב הקיברנטי: מושגי יסוד", **צבא ואסטרטגיה**, כרך 3, גיליון 1, אפריל 2011.

15 Martin C. Libicki, "Cyberdeterrence and Cyberwar," (Santa Monica, CA: RAND Corporation, 2009).

16 אלקטרוניקה היא התשתית של עולם המחשוב היום. לפני האלקטרוניקה היו מכונות חישוב מכאניות. ובעתיד? כבר כיום הוכחה האפשרות לנצל תשתית ביולוגיות לצורכי המחשוב. מחשוב DNA משתמש בביולוגיה מולקולארית ו־DNA במקום הרכיבים האלקטרוניים. אפשרות נוספת היא מחשוב פפטידי Peptide: מחשוב ביו־מולקולארי המבוסס על תרכובות העשויה חומצות אמינו.

17 השווה ההגדרות של משרד ההגנה אמריקאי: "Joint Publication Jp 3-13: Joint Doctrine for Information Operations". edited by United States Department of Defense. Washington, DC, 2006.
לאלה של האיחוד האירופי כפי שמוגדרים במכרז של רשות ההגנה האירופית EDA Study "Computer Network Operations (CNO) for EU led military operations", 10-CAP-OP-37 (EU milops CNO Capability) - Annex, August 16, 2010.

18 שכוללת הגנה (Computer Network Defense (CND, ניצול Computer Network Exploitation (CNE) והתקפה Computer Network Attack (CNA). הבסיס הטכני לשלוש סוגי הפעולה הוא זהה.

19 ראה טבלה 2 לעיל.

20 ראה למשל: Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do about It*. New York: Ecco, 2010; Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz. *Cyberpower and National Security*. Washington, DC: Center for Technology and National Security Policy; National Defense University Press: Potomac Books, 2009; Lynn III, William. "Defending a New Domain", *Foreign Affairs* Vol. 89, no. 5 (September-October 2010); Coward, Martin. "Network-Centric Violence, Critical Infrastructure and the Urbanization of Security." *Security Dialogue* 40, no. 4-5 (2009), pp. 4-5; Sharp, Walter Gary. "The Past, Present, and Future of Cybersecurity", *Journal of National Security Law & Policy* 4, no. 1 (2010).

21 לדיון בסוגיות הטכניות ראה: Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld*. (O'Reilly Media 2009).
Lehtinen, Rick, Deborah Russell, and G. T. Gangemi. *Computer Security Basics*. Sebastopol, CA: O'Reilly & Associates, 2006.

22 נטען כי חומרה פגומה שהשתיל ה־CIA בציוד לבקרת מערכת הובלה של גז שרכשה

ברית המועצות, גרמה לפיצוץ אדיר בסיביר ב־1982
W. K. Clark and P. L. Levin, "Securing the Information Highway: How to Enhance the United States' Electronic Defenses," *Foreign Affairs,* Vol. 88, No. 6 (2009).

23 למשמעויות הכלכליות ראה הדיון אצל פול רומר, שהוזכר לעיל.

24 לאחר פיגועי 11 בספטמבר 2001, סף התמיכה המדינתי הוּרד: לעיתים, די בראיות נסיבתיות כמו תמיכה אידיאולוגית באויב או מתן שירות לוגיסטי למחבלים.

25 דיון מפורט בנושאים הללו חורג מגבולות המאמר.

26 "ניסוי אורורה" שנערך במעבדות הלאומיות באיידהו, ארצות הברית.
Lewis, James Andrew, "Thresholds for Cyberwar." Washington, DC: Center for Strategic and International Studies 2010.

27 ראה הערה 1. "The Meaning of Stuxnet." *Economist*. Chen, T. "Stuxnet, the Real Start of Cyber Warfare?" *IEEE Network* Vol. 24, no. 6 (2010).

28 United States. President's Commission on Critical Infrastructure, Protection. *Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection*. Washington, DC: US GPO, 1997.

29 כך נהגו ממשלות ישראל לאורך שנים, כאשר אלפי רקטות "טפטפו" מרצועת עזה ופגעו בשטחים פתוחים במערב הנגב.

30 ראה: ליאור טבנסקי, הגנה על תשתיות קריטיות מפני איום קיברנטי, **צבא ואסטרטגיה,** כרך 3, גיליון 2, נובמבר 2011. Myriam Dunn, "Securing the Digital Age: The Challenges of Complexity for Critical Infrastructure Protection and Ir Theory," in Johan Eriksson and Giampiero Giacomello, (eds.), *International Relations and Security in the Digital Age* (Routledge, 2007).

31 Lynn III, William. "Defending a New Domain".

32 אחד המדדים למורכבות התוכנה הוא מספר שורות הקוד Source Lines of Code (SLOC). "**חלונות** 3.1NT", מערכת ההפעלה מבית **מיקרוסופט**, יצאה לאור ב־1993 וכללה 4.5 מיליון שורות. "**חלונות** XP" יצאה לאור ב־2001 וכללה 45 מיליון שורות. הפצת לינוקס Fedora 9, כוללת 204 מיליון שורות קוד.

33 ראה: ליאור טבנסקי, **המאבק בטרור בעידן המידע**. (2007)

34 ראה לעיל, וגם: Lynn III, William. "Defending a New Domain"

35 שיטות ההצפנה הקיימות מבוססות על עקרון מתמטי הבא לידי ביטוי בקושי לפרק לגורמים מספר המורכב ממספרים ראשוניים. למחשוב קוונטי מאפיינים שיבטלו לחלוטין את היתרון של שיטות ההצפנה הקיימות. כאשר ייבנה מחשב קוונטי – תחום הביטחון יעבור זעזוע עקב התיישנות יסודות ההצפנה.

36 Libicki, Martin C. "Cyberdeterrence and Cyberwar." Santa Monica, CA., RAND Corporation, 2009. ראה גם מאמר של אמיר לופוביץ' בגיליון זה.

המרחב הקיברנטי וארגוני הטרור

יורם שוייצר, גבי סיבוני ועינב יוגב

מבוא

באחת הסצנות בסרט "מת לחיות 2" (ארצות־הברית 1990) משתלטים טרוריסטים על מערכות המחשוב, בקרת התעבורה, והתקשורת האווירית, מתחזים לפקחי טיסה, נותנים נתונים כוזבים ובתוך סופת שלגים מנחים את טייסי המטוס ויושביו להתרסקות קטלנית על מסלול הנחיתה. לא היה ביכולתם של גורמי הביטחון לתת מענה וסיוע, וגיבור הסרט ג'ון מקליין (בגילום ברוס ויליס), נותר חסר אמצעים להושיע מלבד עמידה חסרת תכלית בערפל על מסלול הנחיתה ונפנוף לעברו של המטוס בשני לפידים מאולתרים. לכאורה מדובר בעוד פנטזיה הוליוודית שאפשר לבטלה כגוזמה, וזו אף שודרגה בסרט המשך – "מת לחיות 4". ואולם פיגועי ה־11 בספטמבר 2001, והשינויים וההתפתחויות באיומים הביטחוניים בעשור האחרון, מצביעים על כך שגם התסריטים הדמיוניים ביותר שנרקמו באולפני הוליווד, יכולים למצוא ביטוי מעשי במרחב הציבורי והביטחוני של ימינו.

השימוש במרחב הקיברנטי כזירה מרכזית ללוחמה בין אויבים או בין מדינות יריבות היה מאז ומעולם קרקע פורייה לפנטזיות ולסצנות מרהיבות בקולנוע. ואולם מרחב זה, ששימש בעבר תפאורת רקע לסצנות מלחמה הוליוודיות, הולך ותופס מקום מרכזי כזירה חשובה, שבה, כך מסתמן, ינוהלו מלחמות העתיד, וכאחת הזירות שיתבצעו בה פעולות עוינות בין גורמים יריבים. יש אפשרות שבין גורמים אלה יימצאו גם ארגוני טרור, שעד כה השתמשו בעיקר בפעילות פיזית אלימה כדי לקדם את האינטרסים שלהם, ולעתים גם את אלו של שולחיהם. נוכח איומים אלו, הקימו מדינות במערב בשנים האחרונות רשויות מיוחדות שנועדו להיערך לקראת פעולות לוחמניות תוך שימוש באמצעים טכנולוגים חדשניים נגד יעדי תשתית אסטרטגיים. מאמר זה מתמקד בניתוח היתרונות והמגבלות העולים להביא לידי כך שארגוני טרור ישתמשו בכלים קיברנטיים כדי לתקוף תשתיות קריטיות של

יורם שוייצר עומד בראש פרויקט הטרור במכון למחקרי ביטחון לאומי
אל"מ (מיל.) ד"ר גבי סיבוני הוא ראש תכנית צבא ואסטרטגיה ותכנית לוחמה קיברנטית, הנתמכת על ידי קרן ג'וזף וג'נט ניובאוואר, פילדלפיה, ארצות הברית
עינב יוגב היא עוזרת מחקר בפרויקט הטרור במכון למחקרי ביטחון לאומי

מדינות, מוסדות וסמלי שלטון, תשתיות ומערכות עסקיות ותעשייה, וכן יעדים אזרחיים ציבוריים למיניהם. כן נבחן האם מדובר באיום ממשי ומידי, או שמא זהו איום פוטנציאלי רחוק, השב ועולה מעת לעת כחלק מהשיח הכללי בתחום זה.[1]

האיום הקיברנטי מצד קבוצות טרור

חמש קבוצות עיקריות משתמשות כיום, או שיש להן פוטנציאל לשימוש בעתיד, בכלי תקיפה קיברנטיים: (1) מדינות המפתחות יכולות התקפיות והגנתיות כחלק (גדל והולך) מיכולות הפעלת הכוח שלהן; (2) גורמים פליליים המונעים בעיקר מאינטרסים פליליים־עסקיים; (3) חברות עסקיות הפועלות בעיקר בתחום ההגנתי מכיוון שהיקף ההתקפות במרחב הקיברנטי בהקשרים עסקיים גדל והולך במידה ניכרת, אולם חלק מהן עלולות לפנות לאפיק של התקפה על חברות מתחרות; (4) ארגוני טרור, שמשום היתרונות הגלומים בשימוש במרחב זה ומשיקולי עלות־תועלת בעבורם עלולים לנסות ולבצע התקפות טרור קיברנטי; (5) גורמים "אנרכיסטיים", המתנגדים למערכת הממסדית הקיימת, מעוניינים לחבל בה מבפנים או מבחוץ, ויבקשו לתקוף את מערכת המחשוב, שהיא כיום הבסיס לניהולה, בכוונה לשבש ואף להרוס את הסדר החברתי ואת מרקם החיים במדינה.

תחום התקיפה הקיברנטית, שאליו עלולים להיכנס ארגוני הטרור נושא בחובו פוטנציאל לשינוי במאזן הכוחות בחברה, משום העוצמה שהוא מעניק לתוקפים, ובייחוד לארגוני טרור הפועלים בנחיתות ביחסי הכוחות הא־סימטריים בינם לבין יריביהם. בניית יכולת במרחב הזה עשויה לאפשר להם לתקוף מתקנים, תהליכים מערכתיים ואתרים של יריבים ולגרום נזקים פיזיים כבדים וליצור השפעה פסיכולוגית ניכרת בחברה ובציבור המותקפים, וזה תוך כדי יכולת פעולה בממדים נוספים על אלה המוכרים לנו כיום מפעולות הטרור הקונבנציונליות, כגון פיגועי התאבדות, הפעלת מטעני חבלה, התבצרות עם בני ערובה, חטיפות כלי תעבורה ובני אדם. לתקיפה קיברנטית יש כמה יתרונות: ראשית, הימנעות מנוכחות פיזית ביעד המותקף. אפשר לנסות ולפגוע מרחוק ברשתות תקשורת ובמערכות בקרה של מתקנים ותהליכים וכך להימנע מהצורך להתמודד עם מכשולים פיזיים ומערכות אנושיות. שנית, היקף הנזק – תקיפה קיברנטית איננה מתקיימת בחלל פיזי בלבד אלא יש לה פוטנציאל לפגיעה קשה ומתמשכת במערכות בקרה ותשתית. בעוד רוב פיגועי הטרור מתוחמים בזמן ובמקום,[2] הפיגוע הקיברנטי מעצים את היבטי החרדה וההפחדה הכרוכות בהשפעות הפסיכולוגיות של מעשה הטרור. שלישית, טשטוש זהויות ומקור ההתקפה – במרחב הקיברנטי קל יותר לעמעם ולטשטש זהויות וגבולות שבין מדינות. גורמי הטרור יכולים לתקוף קיברנטית תוך כדי טשטוש זהויות וביצוע הטעיות לגבי מקור התקיפה. למשל, לתקוף בתוך מדינת היעד תוך כדי שימוש בכתובות של מדינה ידידותית. כך יתקשה המותקף

לזהות את המקור האמיתי של התקיפה. רביעית, יחס עלות־תועלת מיטבי – השימוש בפלטפורמה קיברנטית לצורכי תקיפות טרור מגלם יחס עלות־תועלת מיטבי מבחינתו של ארגון הטרור, שהוא נחות ברמת המשאבים והיכולות לעומת המדינות שאותן הוא תוקף. בהנחה שארגוני טרור יעדיפו מטרות מוגנות פחות על פני אלה המוגנות היטב, הרי שהם יוכלו לתקוף תוך כדי יצירת נגישות על־ידי החדרת מפגעים שיחדירו קודים זדוניים לאתרי היעד, או תוך שימוש בטכנולוגיה העומדת להיות זמינה למדי לקהלים רחבים. חמישית, טרור אל־הרג – באמצעות תקיפות קיברנטיות יכול ארגון הטרור לגרום נזקים ניכרים בלי פגיעה פיזית והרג ישיר. כך הוא יוכל להשיג הישגים באמצעות הפחדה ושיבוש מרקם החיים בלבד, דבר שיעניק למבצעיו יכולת הגנה והסבר לוגי למעשיהם בלי ששפכו דם אלא רק גרמו לנזק בדמים. חדשנות הפעולה תבטיח אף היא פרסום רב לארגוני הטרור, ואף כניסה לתחום פיגועי מיקוח־אל־הרג, שלאחר הדגמות ידרשו תמורות באיימם בפגיעה קיברנטית.

מושמעת טענה שארגוני טרור אינם מעוניינים במרחב הקיברנטי משום שהם מעדיפים פעולות ראוותניות של שפיכות דמים, בעלות נראות גבוהה בהרבה מהאלמוניות המאפיינת כביכול פעולות חבלה באמצעות המרחב הקיברנטי.[3] ואולם טענה זו אינה מתיישבת עם התפיסה הבסיסית של השימוש באסטרטגיית הטרור, הגורסת שהפעילות הטרוריסטית צריכה להתמקד בניסיון לצמצם את פערי העוצמה במאבק עם יריב שעוצמתו רבה יותר, ביצוע פעולות הרסניות תוך כדי חיפוש נקודות תורפה במערכי ההגנה שלו כדי לחדור מבעדן, והשגת עמדת יתרון במחיר נסבל ההולם את האמצעים הדלים יחסית העומדים לרשות מחוללי הטרור. כבר היום אפשר לראות, שארגוני טרור מהג׳יהאד העולמי עושים שימוש רב, אם כי מוגבל ועדיין לא מפותח יחסית, במרחב הקיברנטי כדי להביא יתרונות אלו לידי מימוש. במחקר שבחן את היכולת ואת השימושים בתחום הקיברנטי של ארגוני ג׳יהאד,[4] נמצאו מאפיינים עיקריים המשמשים לבנייה ולשיפור התשתית הארגונית והמבצעית של ארגוני הטרור בתחומים האלה:

- **תעמולה** – שימוש לצרכי הפצת רעיונות, פסיקות, הנחיות, נאומים ודעות של אנשי דת ומנהיגי טרור;
- **גיוס ואימון** – שימוש לצורכי איתור וגיוס של חברים פוטנציאליים, וכן העברת חומרי הכשרה והדרכה באמצעות הרשת;
- **גיוס כספים ומימון** – שימוש ברשת לגיוס כספים במסווה של ארגוני צדקה וסיוע, ושימוש לגִּבת זהויות וכרטיסי אשראי;
- **תקשורת** – שימוש ברשת כגורם לתקשורת מבצעית תוך שימוש בכלים מגוונים ובהם כלי הצפנה זמינים;

- **איתור מטרות ומודיעין** – שימוש במידע ברשת לשם איתור מטרות ומחקר מודיעיני.

המעבר של ארגוני הטרור משימוש לוגיסטי ותעמולתי לשימוש אופרטיבי באמצעים קיברנטיים עלול לבוא לידי ביטוי בביצוע פיגוע דרמתי וחדשני, זול למדי בעלותו אך עם תהודה רבה ולעתים עם נזק בהיקף גדול ביותר, אפילו אם נעשה בחתימה נמוכה או אפילו בשמירה על אנונימיות של מבצעיו. לכן כל ארגון טרור, ובעיקר אלה השואפים לפרסום וליצירת אפקט פסיכולוגי על ציבור יריביהם, רואה בפיגוע כזה אתגר חשוב ושאיפה ראויה, שכדאי להתאמץ בעבורו. חדשנות גם תבטיח למבצעים פרסום בינלאומי ואת היותם דגם לחיקוי. לפיכך ארגונים תת־מדינתיים שיכולתם הטכנולוגית נמוכה משל מדינות שבהן הם נאבקים, עלולים להצטרף למגמה של ניצול הטכנולוגיה המתקדמת הנדרשת ללוחמה הקיברנטית, בייחוד, אבל לא כתנאי הכרחי, אם יזכו לסיוע של מדינות תומכות או אם יצליחו לרכוש בעצמם יכולת כזאת בעתיד על־ידי גיוס אנשים בעלי הכשרה מתאימה בתחום הזה, שיוכלו להביא לידי ביטוי כישורים יוצאי דופן בתחום.

גם למדינות תומכות טרור יש במרחב הקיברנטי כוח משיכה רב להפעלת ארגוני שליח: האנונימיות הטמונה בשימוש כזה, הקושי להוכיח את זהות המפעיל, יכולת ההכחשה (deniability) הגבוהה של מדינות בנוגע למעורבותן נוחה יותר, והגמול בדמות גרימת הנזק הרב ליריב. יתר על כן, גם אם יעלה כלפיהן חשד, יהיה קשה להוכיח את אשמתן, ובכל מקרה "פיגוע קיברנטי" עשוי להיחשב מקומם פחות את הציבור הנפגע מפיגוע טרור בנשק חם הגורם שפיכות דמים גדולה, אפילו שהנזק בעטיו של הראשון רב ביותר, ואף עלול לעלות בהרבה על הנזק לרכוש ולחיי אדם הנגרמים מפעולת טרור אלימה ומדממת.

למרות היתרונות של תקיפה קיברנטית שתוארו לעיל, עדיין לא נודעה תקיפה שהאחראים לה הם גורמי טרור. בניית יכולת ממשית בתחום התקיפה הקיברנטית מחייבת מעבר של סף מודיעיני וטכנולוגי לא מבוטל. בשלב זה סביר להניח שלארגוני הטרור יש קושי לאתר, לגייס ולתחזק יכולת ונגישות טכנולוגית גבוהה ביותר המאפשרת להגיע לסף הזה. אמנם הישענות על יכולת של מדינות תומכות טרור עשויה לספק מענה ולו חלקי למגבלה זאת, אולם אין בה, לפחות בשלב הנוכחי, כדי לייצר לארגוני הטרור מצע טכנולוגי יציב ומשמעותי הנדרש לקיומה של יכולת תקיפה קיברנטית אפקטיבית. כן ניצבים ארגוני הטרור בפני מגבלות הפעילות במרחב הקיברנטי הגלוי (רשת האינטרנט). זהו חיסרון מובהק ואתגר לא מבוטל לארגוני טרור, שכן יכולת המעקב והמודיעין הקיברנטי של מדינות ומעצמות טכנולוגיות מאפשרת להן לזהות התנהגויות חשודות ברשת, לאתר התארגנויות ולהתגונן מפניהן ומפני איומים ספציפיים.

נקודות תורפה ומענים

אף־על־פי שעד כה לא הצליחו ארגוני הטרור להתגבר על המכשולים להשגת יכולת תקיפה קיברנטית, המערכות האזרחיות והפגיעה במרקם החיים השגרתי נותרו ככל הנראה היעדים המועדפים שלהם. אלו הן נקודות התורפה העיקריות, ויכולת הגנתן פחותה מזו של המערכות הביטחוניות. סביר להניח שחיזוק ההגנה על תשתיות לאומיות חיוניות דוגמת מערכות אספקת חשמל, מים ותקשורת, תוביל את ארגוני הטרור לנסות לפגוע ביעדים מוגנים פחות השייכים למגזר האזרחי והעסקי. אף שבמקרים רבים מערכות ממגזרים אלה אינן נכללות בקבוצת התשתיות הקריטיות המוגנות, הרי מבחינת ארגוני הטרור המתקפה יכולה לספק תוצאה אפקטיבית בעיקר בהיבטי הדימוי והפגיעה בביטחון הבסיסי של התושבים.

חלק נכבד בבניית מערך הגנה כנגד תקיפת סייבר הוא כללי ואינו תלוי במקור האיום, בין שמקורו בארגוני טרור, ובין שמקורו בגורמים מדינתיים או בגורמים פליליים. כך בהיבטים הארגוניים דוגמת הרשות לאבטחת מידע בישראל ומשרדים המתמחים בהגנת סייבר במדינות שונות, וכך בחלק ממרכיבי ההגנות מתחום מערכות המידע והאבטחה הכוללת. לעומת אלה, אל מול ארגוני טרור המבקשים להפעיל כלים קיברנטיים, נדרשים שני רכיבים ייעודיים, המחייבים פיתוח ושכלול מתמשך.

מודיעין – איסוף אקטיבי של מודיעין מדויק ואיכותי מחייב פעילות איסוף ממגוון מקורות ובהם מקורות גלויים, וממוחשבים ומרשתות של ארגוני הטרור. לצורך זה יש לפתח יכולות לשהות במערכות האלה בצורה סמויה ולהזרים מידע בצורה פעילה ומתמשכת. לשם כך יש להתגבר על הפרישה הגלובלית הרחבה המאפיינת את ארגוני הטרור, המשתמשים בחדרי דיונים רבים ברשת, ומעבירים מסרים במילות קוד ייחודיות. גורמי המודיעין נדרשים לבנות יכולת ליירט תשדורות אלה ולפענחן בקבועי זמן רלבנטיים, ובה בעת לספק לגורמי ההגנה הקיברנטית את הכלים להגן מפני הפעולות המתוכננות ואף לשבש אותן.

שיבוש – בשונה מהקמה של מערכות הגנה, שאינן מנסות למנוע את התקיפה אלא למנוע את הצלחתה, מטרת השיבוש היא לסכל את ביצוע התקיפה או לפגוע במהלכיה. הקמת מערך שיבוש אפקטיבי כנגד תקיפות קיברנטיות של ארגוני טרור מחייב ניטור ובקרה מודיעיניים שיוכלו לזהות את ההתארגנות לתקיפה טרם התרחשותה, ולפעול ביעילות לסיכולה. היבט זה נשען בעיקר על יכולת איסוף של מודיעין טקטי הן במחשבים והן ברשתות התקשורת שארגוני הטרור משתמשים בהן.

לעתים, נעשים ניסיונות שיבוש שאינם מופנים לכוונת תקיפה מסוימת, אלא כניסיון לפגוע בתשתיות הארגוניות של ארגון היעד. ניסיון כזה אירע למשל באנגליה כאשר המודיעין הבריטי השחית את גיליונו המקוון של כתב העת האנגלי

Inspire של ארגון אל־קאעדה. בנוסף, בשנים האחרונות הג׳יהאד האלקטרוני על מרכיביו מהווה יעד לתקיפות סייבר מזדמנות, שרובן מיוחסות לממשלות של מדינות מערביות: אתר הטאליבן הושחת חדשות לבקרים, וכן הותקפו פורומים ג׳יהאדיסטיים אקסקלוסיביים ואתרים פונדמנטליסטיים עתירי פרופיל. מנגד רשויות אמריקניות, סעודיות והולנדיות דולות מידע מודיעיני יקר ערך על אודות טרור אסלאמי פוטנציאלי מאתרים ג׳יהאדיסטיים המשמשים ״מלכודות דבש״ (honeytraps) למודיעין איכותי.[5]

בצד אלה חובה להעמיק את הגנת המערכות האזרחיות שהן נקודות התורפה הגדולות ביותר, ולכן הן המטרות המועדפות על ארגוני הטרור. ממשלת בריטניה למשל החלה לנקוט אמצעים חקיקתיים רבים הכוללים אישור שימוש באמצעים פולשניים, כגון ציטוט לשיחות טלפון, מעקבים אחרי תנועות דואר אלקטרוני בתיקים משטרתיים הקשורים לעברות טרור, טרפוד תהליכי רדיקליזציה דרך האינטרנט ואימון ייעודי של יחידות משטרה להתמודד עם איום סייבר.[6] עם זאת, ברוב המדינות ההגנה על המערכות האזרחיות עודנה בחיתוליה. עיקר משאבי המדינות בתחום ההגנה הקיברנטית מוקצים למערכות הביטחוניות ולמה שקרוי תשתיות לאומיות קריטיות. העמקת ההגנה על המערכות האזרחיות מחייבת שידוד מערכות לאומי, החייב להיתמך ברגולציה מתאימה.[7]

סיכום

במפגש שהתקיים בניו יורק בדצמבר 2001, זמן לא רב לאחר מתקפת הטרור בארצות־הברית, שטח הפילוסוף ז׳אק דרידה את תפיסתו על התמורות שחוללו בעולם פיגועי ה־11 בספטמבר 2001. לשיטתו פיגועים אלו הם עדיין חלק מ״תיאטרון האלימות העתיק״, העולם הממשי והנראה, שבו דברים עדיין מתנהלים ב״סדר ברור וגדול״. ואולם לדבריו, המרחב הקיברנטי מציב איום חמור יותר על עולמנו הפוליטי והפיזי – הסכנות הטמונות בו משנות את היחס בין טרור, במובן הפסיכולוגי וההיסטורי של התקפה אלימה, לבין המושג טריטוריה. כעת, בעידן הטכנו־מדעי החדש, האיום שהכרנו בעבר כממשי, נהפך לאיום בלתי נראה, שקט ומהיר ובלא שפיכות דמים, שלדברי דרידה הוא גרוע יותר מפיגועי ה־11 בספטמבר, שכוונו כלפי מקום ידוע בזמן מסוים. כעת אנו ניצבים נוכח אתגר המאיים על מרקם החיים החברתיים־הכלכליים, מרקם שכולנו קשורים ותלויים בו, בכל נקודה ובכל רגע.[8]

ההתפתחויות והחידושים הטכנולוגים המהירים בשנים האחרונות במרחב הקיברנטי אכן יצרו שדה לחימה שבו חוברות ומאוגדות להן בו בזמן אוכלוסיות מגוונות ורבות, מקומיות ובינלאומיות, שהן יעד נחשק לפעילותם של ארגונים תת־מדינתיים. נכון לעת הזאת טרם נודעה תקיפה קיברנטית של גורמי טרור ולכן

האיום אינו נראה מיידי. הגורמים הרוצים לנצל את המרחב הקיברנטי למטרות זדון צריכים לעבור סף גבוה בשלושה רכיבים חיוניים: השגת מודיעין איכותי, נגישות ויכולת לפצח מערכות מחשוב המוגנות בטכנולוגיה גבוהה, וכן כושר חישוב ומחשוב גבוהים. ואולם היתרונות שבהשגת היכולת הקיברנטית, שפורטו במאמר זה, עלולים לשמש להם תמריץ לפתח, לרכוש או לגייס יכולת כזאת בעתיד. השגת שליטה ביכולות הטכנולוגיות והמודיעיניות המתקדמות הנדרשות במרחב הקיברנטי, צפויה להעניק לגורמים כאלה יכולת לשבש את אורח החיים התקין של אוכלוסיות הנחשבות יריבות, לערער את אמונתן בממשליהן ותזכה אותם בעוצמה ובחשיפה תקשורתית שחשיבותן רבה. לפיכך חייבות מדינות המערב להתכונן בהתמדה כדי לקדם את פני הרעה הצפויה הזאת ולשפר את יכולת המודיעין ואת יכולת ההגנה על המערכות האזרחיות. בד בבד עליהן לבנות מודיעין מדויק ויכולת הגנה על המערכות הביטחוניות ועל התשתיות הלאומיות הקריטיות ויכולת לשבש התארגנויות ותקיפות קיברנטיות של ארגוני טרור. הפקרתו של המרחב הקיברנטי האזרחי, שהוא מטרה לארגוני טרור, עלולה להביא בעתיד לידי תוצאות הרות אסון, שבשעת מבחן יציבו את גורמי הביטחון, כמו את גיבור הסרט "מת לחיות 2", בנסותם להציל מטוסים מתרסקים כשבידיהם לפידים בוערים בלבד.

הערות

1 השימוש במינוח טרור קיברנטי במאמר זה הוא בהקשר של השימוש בכלים קיברנטיים העלול לשמש ארגוני טרור לצורך תקיפת תשתיות כלכליות ומערכות אזרחיות במדינות יעד.

2 אפשר להחריג כאן פיגועים דוגמת התקיפה ב־11 בספטמבר 2001 בארצות־הברית, שהשפיעה גלובלית על מערכי הבטיחות בתעופה.

3 שמואל אבן ודוד סימן־טוב, **לוחמה במרחב הקיברנטי: מושגים, מגמות ומשמעויות לישראל**, המכון למחקרי ביטחון לאומי, מזכר 109, יוני 2011, עמ' 42.

4 *Examining the Cyber Capabilities of Islamic Terrorist Groups*, Institute for Security Technology Studies at Dartmouth College, Technical Analysis Group, March 2004.

5 Adam Rawnsley, "Stop the presses! Spooks hacked al-Qaida online mag," *Wired*, June 3, 2011, http://www.wired.com/dangerroom/2011/06/stop-the-presses-spooks-hacked-al-qaida-online-mag/June 4, 2011.

6 "Warning of rise in cyber-terrorism," *The Independent*, July 12, 2011, http://www.independent.co.uk/news/uk/crime/warning-of-rise-in-cyberterrorism-2312434.html, (July 14, 2011).

7 גבי סיבוני, "הגנת נכסים ותשתיות קריטיות מפני תקיפה קיברנטית – הממד הסטטוטורי", **צבא ואסטרטגיה**, כרך 3, גיליון 1, מאי 2011.

8 ז'אק דרידה, מתוך ג'יובנה בוראדורי, **פילוסופיה בזמן טרור – שיחות עם הברמאס ודרידה**, תל־אביב, הקיבוץ המאוחד, 2004, עמ' 173–174.

לוחמה קיברנטית והרתעה: מגמות ואתגרים במחקר

אמיר לופוביץ

מבוא

בשנים האחרונות מספר הולך וגדל של חוקרים הרחיבו את הדיון באסטרטגיית ההרתעה כדי לבחון התמודדות עם מגוון של איומים "חדשים". בשונה מתקופת המלחמה הקרה שבה התמקד המחקר בהרתעה בין מדינות, בין מעצמות ובהרתעה גרעינית, אנו רואים בשנים האחרונות – ובייחוד מאז פיגועי ה־11 בספטמבר 2011 – מחקרים רבים הבוחנים את אסטרטגיית ההרתעה כלפי איומים נוספים, כמו טרור, מדינות סוררות וכלפי הרתעה בסכסוכים אתניים. למחקרים אלה יש כמה מאפיינים משותפים: הם מתבססים ברובם על ניסיון לבחון את רלוונטיות התנאים להצלחת הרתעה כפי שפותחו בהקשר של המלחמה הקרה, והם שמים דגש חזק למדי על המלצות מדיניות (policy oriented), ובעיקר על המלצות הנוגעות להתמודדות עם האתגרים הניצבים לפני ארצות־הברית.[1] מאפיינים מחקריים אלה בולטים מאוד גם בדרך שבה התפתח הדיון בקשר שבין הרתעה לבין לוחמה קיברנטית.[2] כך, רבים מהמחקרים העוסקים באסטרטגיית ההרתעה ולוחמה קיברנטית, יוצאים מנקודת המבט האמריקנית ובוחנים את האפשרות של ארצות־הברית ליישם אסטרטגיה של הרתעה כדי למנוע התקפות קיברנטיות עליה, או את הדרך שבה ארצות־הברית יכולה להשתמש בלוחמה הקיברנטית כדי להרתיע מגוון של איומים אותם היא מבקשת למנוע.[3]

ממחקרים אלו עולה, כי האפשרות להרתיע התקפות של לוחמה קיברנטית היא מוגבלת בכל אחד מהממדים הדרושים להפעלה מוצלחת של אסטרטגיה זו: הימצאות היכולת (אמצעי נשק), אמינות האיום והאפשרות להעביר את המסר המאיים למאתגר הפוטנציאלי.[4] עם זאת, יש כמה גורמים העשויים בתנאים מסוימים לשמש בסיס להרתעה מוצלחת גם של לוחמה קיברנטית. במאמר זה אסקור את ספרות המחקר ואציע כיוונים להמשך המחקר בסוגיות האמורות.

ד"ר אמיר לופוביץ' הוא מרצה בחוג למדע המדינה, אוניברסיטת תל־אביב

בחלק הראשון של המאמר מוצגים התנאים להצלחת אסטרטגיית ההרתעה. בחלק השני נסקרים הטיעונים המרכזיים שהוצגו בנוגע לקשיים להפעיל הרתעה מוצלחת נגד לוחמה קיברנטית לגבי כל אחד מן התנאים הללו. החלק השלישי עוסק בכמה גורמים העשויים לחזק את ההרתעה כנגד לוחמה קיברנטית, ובמספר יתרונות וחסרונות שלהם. בחלק האחרון אצביע על החשיבות להמשיך את הדיון בקשרים שבין הרתעה ולוחמה קיברנטית, ואציע כיוונים אפשריים למחקר ולחשיבה בנושא.

התנאים להצלחת הרתעה

שחקנים יכולים לנסות לגרום לירי‌בם להימנע מפעולה לא רצויה במגוון דרכים. האסטרטגיה של הרתעה על־ידי איום בענישה (deterrence by punishment) היא אחת הנחקרות ביותר שבהן. סוג זה של הרתעה זכה למספר רב של ההגדרות,[5] כשביניהן הגדרתם של גורג' וסמוק זכתה לשימוש נרחב. לטענתם, הרתעה היא היכולת לשכנע יריב (פוטנציאלי) כי המחיר שהוא ישלם עקב ביצוע הפעולה הלא רצויה יעלה על כל רווח אפשרי.[6] סוג זה של הרתעה שונה מ**הרתעה על־ידי** מניעה (deterrence by denial),[7] המבוססת על הניסיון לשכנע תוקפן אפשרי שעליו להימנע מהפעולה מאחר שלא יצליח להשיג את מטרותיו.[8] המושג של הרתעה גם שונה מהמושג אכיפה (compellence), המבוסס על שימוש באיומים כדי לגרום ליריב לבצע פעולה, בעוד הדגש בהרתעה הוא כאמור לגרום ליריב להימנע מביצוע הפעולה הלא רצויה.[9]

סוגיה מרכזית שעסקו בה חוקרים שבחנו את אסטרטגיית ההרתעה על־ידי איום היא התנאים שבהם היא עשויה להצליח, כלומר לגרום ליריב פוטנציאלי להימנע מאתגור המגן. המחקר, שהתפתח ברובו בתקופת המלחמה הקרה ועסק בהרתעה בין מעצמות־העל, עמד על שלושה תנאים מרכזיים: יכולות המגן, אמינות האיום והעברת המסר של האיום למאתגר.

תנאי ראשון בכדי שהרתעה על־ידי איום בענישה תפעל, הוא שהמגן יוכל לגבות מחיר מהשחקן המאתגר. לא מפתיע אפוא שמחקרי ההרתעה התפתחו מאוד בעידן הגרעיני מאחר שנשק זה מאפשר להבהיר היטב את המחיר של מלחמה עתידית. הנשק הגרעיני נתן למנהיגים "כדור בדולח", שאפשר להם לראות את תוצאות המלחמה הגדולה הבאה, ולכן לנקוט משנה זהירות בהתנהגותם.[10] עם זאת חשוב להדגיש, כי אין מדובר רק ביכולת לא קונבנציונליות, וגם אמצעים קונבנציונליים עשויים לשמש לגביית מחיר ממאתגר.[11] יתרה מכך, חלק חשוב מממד היכולת הוא אמצעי העברה שיש בידי המגן, למשל מטוסים, טילים ואפילו כבישים או כלי רכב העשויים להיות חלק מנדבך היכולת בהקשר של הרתעה.

תנאי שני להצלחת הרתעה הוא אמינות האיום. כדי שאיום ההרתעה יהיה אפקטיבי, השחקן המגן צריך להיות נכון להשתמש באמצעים שברשותו. חוקרים

הציגו מגוון גורמים העשויים להגביל נכונות זאת, למשל דעת קהל פנימית או בינלאומית, או אפילו יכולת ההרתעה של היריב עצמו (השחקן המאתגר).[12] המשותף לגורמים אלה הוא, שהם מעלים, כל אחד בדרכו, את המחיר של הפעולה ומקטינים את האמינות של השחקן להוציא לפועל את האיום אם יידרש לכך.[13]

התנאי השלישי הוא העברת המסרים למאתגר בדבר שני התנאים הקודמים — היכולות והכוונות. כלומר, על המאתגר להיות מודע לאמצעים שיש בידי השחקן המגן ולנכונותו להשתמש בהם. יש הטוענים שתנאי זה הוא החשוב ביותר, כפי שרמזו לכך חוקרים שפיתחו את הגישות הפסיכולוגיות להרתעה. לטענתם, לתפיסות ולעיוותי תפיסה של מקבלי החלטות יש השפעה ישירה על הצלחת הרתעה.[14] במובן זה, מה שחשוב זה לא היכולות של השחקן המגן וכוונותיו, אלא כיצד אלו נתפסים בעיני המאתגר הפוטנציאלי.

לבסוף, אסטרטגיית ההרתעה עשויה לשמש למניעת סוגים שונים של איומים. לכן קשה לדון באופן אחיד בתנאים להצלחת הרתעה, שכן אלו צריכים להיות מותאמים לא רק לשחקן המאתגר, אלא גם לסוג הפעולה שמנסים להניא אותו מלבצע. למשל, בעוד נשק גרעיני עשוי להיות אפקטיבי בהרתעה מפני מתקפה כוללת ("הרתעה כללית"), מידת יעילותו תהיה נמוכה יותר כלפי איומים מוגבלים יותר.[15]

הרתעה ולוחמה קיברנטית – הקשיים בהרתעה

חלק גדול מן המחקרים שבחנו את אסטרטגיית ההרתעה בהקשר של לוחמה קיברנטית, ביקשו ליישם את התיאוריות של המלחמה הקרה בכל הנוגע להצלחת ההרתעה. חוקרים בחנו את התנאים המרכזיים להצלחת הרתעה שהוצעו בספרות (ונידונו בחלק הקודם): יכולת המגן, אמינות האיום ותקשורת, כלומר האפשרות להעביר אל המאתגר את המסר בדבר היכולות ואמינות האיום. מרבית החוקרים סבורים על סמך בחינת התנאים האלה, שאסטרטגיית ההרתעה צפויה להיכשל לנוכח האיומים שיוצרת לוחמה קיברנטית.[16]

היכולת

קושי מרכזי בהרתעת לוחמה קיברנטית נובע מכך שסוג לוחמה זה מאפשר גם לשחקנים חלשים להעתיק את העימות למרחב שבו יוכלו למקסם את רווחיהם ובמידת סיכון נמוכה. למעשה, ככל ששחקן מפותח יותר מבחינה טכנולוגית, כך הוא פגיע יותר להתקפות של לוחמה קיברנטית.[17] גורם זה מקטין את אפשרות התגמול, ולכן את היכולת לבסס איום הרתעה אמין. כך למשל, קשה מאוד להרתיע שחקנים, ובייחוד יחידים, שאין ברשותם מערכות מידע משל עצמם הניתנות לאיום בפגיעה בהן.[18] בעיה זו באה לידי ביטוי גם בהתמודדות עם מדינות שמידת

ההתבססות שלהן על מערכות מידע היא נמוכה. במצבים כאלה האפשרות של איום אפקטיבי באמצעים של לוחמה קיברנטית בלבד היא מוגבלת.

האמינות

בעיה שנייה בהרתעת איומי לוחמה קיברנטית היא אמינות המגן. לפגיעות המגן עשויה להיות השפעה המגבילה את נכונותו להפעיל את יכולותיו עקב חששו כי תגמול עלול להוביל להסלמה. הבעיה של המגן היא, שהסלמה כזאת עלולה להיות מסוכנת לו יותר מאשר למאתגר, ועל כן עלול לגדול חוסר האמון של המאתגר בנכונותו של המגן לפעול.[19] הבעיה אף מועצמת מכך, שעל־פי־רוב לצד החלש השוקל שימוש בלוחמה קיברנטית יש חסמי כניסה נמוכים (low entry costs).[20] במילים אחרות, העלויות של מאתגר פוטנציאלי לעשות שימוש באמצעים של לוחמה קיברנטית הם במקרים רבים נמוכות, מה שמגדיל עוד את הקשיים בהצגת האיום ההרתעתי הנדרש כדי למנוע פעולה כזאת.

גם דעת קהל פנימית ובינלאומית עשויה להגביל את אמינות איום התגמול עקב המאפיינים של הלוחמה הקיברנטית. במצבים שיהיה קשה לבסס את זיהוי מקור הפגיעה (כפי שיתואר בהמשך),[21] יהיו מגבלות גם על היכולת להפעיל תגמול שיגרום נזק.[22] מגבלות אלה יכולות להיחשב בעיני מאתגר פוטנציאלי למערערות את אמינותה של ההרתעה. וכך תוקפן פוטנציאלי, המעריך כי קטנים הסיכויים שהמגן יממש את איומיו בגלל נזק שעשוי להיגרם לו עקב כך, תוקפן כזה יהיה נכון להסתכן ולפעול.

העברת האיום

הבעיה השלישית נובעת מהקושי של המגן להעביר למאתגר את המסר בדבר יכולותיו ובדבר אמינות התגובה שלו. מלבד הבעיות הבסיסיות בנוגע לכל אחד מן ההיבטים הללו, שתוארו לעיל, מאתגרים יכולים להיות לא רק אנונימיים אלא אפילו יחידים, שפעמים רבות אין להם כתובת פיזית הניתנת לזהוי.[23] כך למשל, לטענת ליביקי, עד היום לא לגמרי ברור מה המקור להתקפה על שרתי האינטרנט של אסטוניה בשנת 2007, והאם הייתה זו פעולה מכוונת מלמעלה של ממשלת רוסיה, כפי שטענו גורמים אחדים שבדקו את הנושא.[24] מקור הפגיעה יכול להיות מדינה אחרת, ארגונים או יחידים הפועלים בתוך מדינה אחרת, וכן ארגונים או יחידים הפועלים בתוך גבולות המדינה שאותה רוצים לתקוף. למעשה, מצב זה מבטא את הטשטוש הקיים בין פשיעה, טרור ולוחמה.

יתרה מכך, לצורך הרתעה לא מספיק זיהוי בדיעבד של הגורם המאתגר, אלא נחוץ זיהוי שלו מבעוד מועד, בטרם התקפה, כדי שיהיה אפשר להפנות אליו את האיום המרתיע. זוהי סוגיה מרכזית, שכן הרתעה מבוססת כאמור על כך

שהמאתגר הפוטנציאלי יהיה מודע מראש ליכולתו של המגן ולנכונותו להפעיל את האמצעים שבידו. ואולם אם המגן מתקשה לזהות את מקור הפגיעה לאחר התרחשותה, קל וחומר שיתקשה בכך בטרם פגיעה. יתרה מכך, גם הפתרון של הצגת איומים כלליים שנועדו להקיף טווח רחב למדי של שחקנים שהמגן מעריך כמי שעלולים לנסות ולפגוע בו הוא מוגבל. זאת מכיוון שההרתעה יעילה יותר במקרה שהאיום, גם אם אינו מפורש לגמרי, מופנה לשחקן ספציפי ולא לשורה אנונימית ולא מוגדרת של שחקנים או סוגי שחקנים העלולים לנסות ולאתגרו.[25]

קושי אחר הקשור ישירות להעברת המסרים למאתגר נוגע לשאלת האמצעים להעברת מסרי האיומים לתוקף הפוטנציאלי.[26] קושי זה מתעצם משום ריבוי השחקנים היכולים ליצור איומים. שלא כמו בתקופת המלחמה הקרה, שבה מספר היריבים (שהיו מדינתיים) היה מוגבל ויכולותיהם היו ברורות למדי, בעידן המידע יש ריבוי של תוקפים אפשריים, מה שמקטין את האפשרות להציג הרתעה יציבה ואמינה.[27] במילים אחרות, בתקופת המלחמה הקרה — ובעימותים בין־מדינתיים מסורתיים בכלל — היריב היה ידוע, ולכן היה ברור מיהו הנמען של המסר ההרתעתי. מנגד, ריבוי האיומים של הלוחמה הקיברנטית וגיוונם יוצר זירה מורכבת יותר לפעולה, שבה לא ברור לגמרי כיצד יש להעביר את המסר המרתיע.

הרתעה ולוחמה קיברנטית – לעתים ההרתעה אפשרית

למרות הקשיים שצוינו, אין לפסול לגמרי את האפשרות שהרתעה כנגד לוחמה קיברנטית עשויה בתנאים מסוימים להצליח, חלקית לפחות. למשל, חוקרים הדגישו כי האיום בתגמול אינו חייב להיות מוגבל לחלל הקיברנטי, אלא יכול להיעשות באמצעים מסורתיים יותר. כך אם מדינה מאיימת לפעול באמצעים של לוחמה קיברנטית, האיום ההרתעתי כלפיה יכול להתבסס על קשת רחבה של אמצעים המצויים ברשותה של המדינה המבקשת להתגונן. איומים כלכליים, פוליטיים, דיפלומטיים או צבאיים עשויים להיות יעילים בהרתעת מדינה הרוצה להפעיל לוחמה קיברנטית נגד מדינה אחרת. בדומה, גם עם איומים שמציבים יחידים או ארגוני טרור המבקשים להפעיל לוחמה קיברנטית, יכולות מדינות – כפי שהציעו חוקרים (ואף כמה מקבלי החלטות) – להתמודד בעזרת אמצעי הרתעה שאינם מן המרחב הקיברנטי. למשל, איומים באמצעות מערכת המשפט (הפנימית והבינלאומית), ובאמצעות ארגונים לביטחון פנים, זאת למשל בשילוב עם איומים צבאיים מסורתיים.[28] באופן זה, אם יש שחקנים המעריכים שישיגו רווחים מהסטת העימות לחלל הקיברנטי, שבו הם נהנים מיתרונות, השחקנים העלולים להיפגע יכולים לפעול בזירות הנוחות להם ולא להגביל את עצמם לתגובה במרחב הקיברנטי בלבד.

אמצעי אחר הוא הרתעה על־ידי מניעה. היתרון הטמון באסטרטגיה זו הוא אפשרות ביסוסה על אמצעים הגנתיים, וכך לא רק להניא יריב מפעולה, אלא גם לתת פתרון במקרה שהמאתגר החליט לתקוף. יתרה מכך, לדברי מורגן, התבססות על אמצעים הגנתיים מגוונים, שיסייעו לביסוס הרתעה על־ידי מניעה, יוכלו לסייע לזהות את התוקפן ולחזק את היכולת להפעיל תגובת־נגד, מה שעשוי לחזק גם את ההרתעה באמצעות ענישה.[29] עם זאת, הפעלת אסטרטגיה זו כרוכה בהתגברות על בעיות דומות לאלו הקשורות להפעלה מוצלחת של הרתעה על־ידי איום. בשני המקרים, מחיר הכניסה הנמוך שנדרשים מאתגרים לשלם כדי להפעיל לוחמה קיברנטית נותר קושי מרכזי. עוד מציע מורגן, כי הרתעה סדרתית (serial deterrence)[30] יכולה גם היא להיות מועילה להתמודדות עם איומים של לוחמה קיברנטית. לטענתו:

> attacks are very likely to turn out to be manageable cyber repeated serial deterrence, primarily through applications of harmful responses over an extended period, to induce either eventually permanent suspensions of the most temporary or bothersome attacks or of attacks by the most obnoxious opponents.[31]

בעוד שזוהי דרך מקורית להתמודד עם איומים במרחב הקיברנטי, ויש בה ניסיון מעניין להשתמש במושגים קיימים בדרך חדשנית, אין היא אינה חפה מאתגרים. ראשית, לא ברור שהיריב יכול להיות מושפע לאורך זמן מאותם ניסיונות, שכן אלו עלולים ללמד את המאתגר כי ההרתעה שמפעיל המגן אינה עובדת (ועל כן הוא נדרש לאותן פעולות חוזרות).[32]

בעיה נוספת הקשורה לאסטרטגיה המבוססת על הרתעה סדרתית היא חשיפת האמצעים שבידי המגן. הבעיה של חשיפת היכולת באה אומנם לידי ביטוי בכל אחת מצורות ההרתעה במרחב הקיברנטי (הרתעה על־ידי איום, הרתעה על־ידי מניעה); ואולם עקב אופיים של האמצעים שמשתמשים בהם במרחב זה, הבעיה חריפה במיוחד בכל הקשור לניסיונות הרתעה לאורך זמן, כמו הדרישות המתחייבות מאסטרטגיה של הרתעה סדרתית.[33] במצב זה, חשיפת היכולות ההתקפיות כפועל יוצא של התקיפות החוזרות ונשנות עשויה לשמש מקור לידע או השראה בעבור המאתגר.[34] מורגן עצמו התייחס לסוגיה זו וטען, כי חשיפת היכולות עלולה לא רק להעניק השראה ליריבים ומוטיבציה להשגת יכולות דומות, אלא גם עלולה לאפשר ליריב להתכונן לאיום העתידי ולפגוע ביעילותו של האיום הזה.[35]

כיוונים לחשיבה ולמחקר נוסף

אומנם כמה חוקרים כבר החלו להציע כיווני מחקר מגוונים לבחינת הרתעה במרחב הקיברנטי, אך אני מבקש להצביע כאן על שני כיוונים מרכזיים שבהם אפשר להרחיב עוד את הספרות בנושא. ראשית, יש מקום למקד יותר את המחקר העוסק באיומים במרחב הקיברנטי. נראה שקיים פער הולך וגדל בין הפרקטיקות בזירה הבינלאומיות וסוגי האיומים בה לבין הדרך שהמחקר בתחום בוחן את אסטרטגיית ההרתעה. פער זה קיים בתחומי מחקר נוספים של הרתעה, אך הוא בולט במיוחד בנוגע למרחב הקיברנטי, המכיל מגוון רחב של סוגי אינטראקציות בין סוגים שונים ומגוונים של שחקנים המאיימים בדרכים שונות. לכן יש להרחיב את הדיון בסוגי השחקנים והאיומים שהם יוצרים, ובדרכים להרתעת כל אחד מהם. זאת ועוד, בדומה למחקר הרחב בנוגע לאסטרטגיית ההרתעה, קיימת נטייה להתמקד בהרתעה של מדינות כלפי סוגים שונים של שחקנים (ארגוני טרור, מדינות סוררות וכו'),[36] בעוד חלק חשוב שאינו זוכה לתשומת לב מספקת נוגע להרתעה של אותם שחקנים את המדינות שאותן הם מבקשים לאתגר. בעיות אלה של הרתעה קיימות גם בלוחמה קיברנטית, ומעצימות את הקשיים של מדינות המתמודדות בזירה מורכבת בהרבה ממה שידעו בעבר.

בדומה, המחקר העוסק בלוחמה קיברנטית נוטה לעסוק בהיבטים קלאסיים של ביטחון, בעוד זירת האיומים מורכבת ומגוונת.[37] למשל, מדינות מוטרדות מאוד מכוחם העולה של שחקנים כלכליים (למשל גוגל), או אידיאולוגיים (למשל יחידים או קבוצות חברתיות המבקשים לקדם רפורמות שלטוניות), המשתמשים במרחב הקיברנטי. בלי להיכנס לשאלה, האם ההגדרות הקיימות ללוחמה קיברנטית מכילות את האינטראקציות עם שחקנים אלה, עשויה להיות תרומה חשובה לניתוח יחסים אלה באמצעות התיאוריות של ההרתעה. לדוגמה, אפשר לחקור באמצעות הכלים והמושגים של אסטרטגיית ההרתעה את האינטראקציות בין גוגל לבין סין בנוגע לאיומים המרומזים או הישירים שהציגו שחקנים אלה זה לזה בסוגית הצנזורה על התוצאות המוצגות במנוע החיפוש. בנוסף, פירוק המחקר של הרתעה ולוחמה קיברנטית לסוגים שונים של איומים (cyberwar, cybercrime, cyber-terror, internetwar) ולסוגי השחקנים המפעילים אותם (מדינות, יחידים, ארגונים כלכליים) עשוי להיות לא רק מדויק יותר ופורה, אלא גם להצביע על התנאים לקיום סיכויים רבים יותר להצלחתה של אסטרטגיית ההרתעה של כל אחד מן השחקנים המעורבים כלפי יריבו.

שנית, אני סבור כי יש להמשיך ולבחון בגישה ביקורתית ומקורית את הספרות האסטרטגית המסורתית בנושאי הרתעה. הדבר כבר נעשה במידה לא מבוטלת בכמה מן המאמרים שפורסמו בנושא, אך יש מקום להמשיך ולבחון מושגים נוספים לגבי אסטרטגיית ההרתעה, כמו "הרתעה מידית",[38] "הרתעה כללית" ו"הרתעה

מורחבת".[39] יש לנסות להבין את המשמעות והרלוונטיות של יישום פרקטיקות כאלה במרחב הקיברנטי.

בדומה אפשר להשתמש במושגים כמו "עמימות". מושג זה עשוי לשמש מסגרת חשיבה להתמודדות עם הדילמה הכרוכה מחד גיסא בצורך בחשיפת היכולות,[40] ומאידך גיסא החשש שהיריב יוכל לנצל חשיפה זו להגדיל את עוצמתו ואת חסינותו מפני איומי ההרתעה. שימוש בתובנות שפותחו בהקשרים שונים עשוי להיות בסיס מעניין לפיתוח רעיונות של עמימות במרחב הקיברנטי, לא רק לגבי הכוונות והנכונות להפעיל את האיומים, אלא בכלל ביחס לשאלת קיומן של היכולות. באור זה אפשר למשל לנתח את המאמצים שעושות מדינות בשנים האחרונות בתחום הלוחמה הקיברנטית. לא רק שאמצעים אלה שמפתחות מדינות עשויים לחזק את אסטרטגיית ההרתעה שלהן כלפי איומים אלה, אלא שעצם הבולטות שזכו לה מאמצים אלה יכולה לשמש ככלי הרתעתי. כך הגם שלהקמת פיקוד אסטרטגי לניהול לוחמה קיברנטית של ארצות־הברית יש מגוון מטרות ותפקידים,[41] עצם אזכורו והבולטות שקיבל מאפשרים לא רק את שיפור היכולת, אלא גם מדגימים את הנכונות להשקיע משאבים בצמצום האיומים והנזקים. ייתכן שהבלטת הרצון להשקיע באמצעים מעין אלו, וחשיפה של היקף התקציבים, המשאבים וכוח האדם המופנה לנושא — גם בלי פירוט מדויק של האמצעים הנרכשים ויכולותיהם — יוכלו לסייע בהגדלת אמינות המסר ההרתעתי נגד איומים במרחב הקיברנטי, במיוחד כלפי איומים הכרוכים ברמות גבוהות של אלימות מצדן של מדינות אחרות. במילים אחרות, חשיפה חלקית של היכולות תוך שמירה על ערפול ועמימות לגבי מהותן, מאפשרת לצמצם את אותן השפעות מזיקות שתוארו לעיל, אך גם להעביר מסר תקיף. עם זאת, אפשר לצפות כי סף הכניסה הנמוך לפעולה במרחב הקיברנטי, במיוחד כשמדובר בעימותים א־סימטריים, ימשיך להציב אתגר לביסוס אסטרטגיה של הרתעה המבקשת למנוע איומים במרחב הזה.

סיכום

המחקר העוסק בהרתעה של לוחמה קיברנטית דן בעיקר בקשיים הטמונים בהרתעת יריבים מלעשות שימוש באסטרטגיה זו. הגם שבתנאים מסוימים הרתעה עשויה להתקיים, בכל זאת הקשיים הנוגעים ליכולת המגן, לנכונות שלו להשתמש באמצעים אלה וליכולתו להעביר את המסר המרתיע למאתגר הפוטנציאלי מגבילים מאוד את האפשרות להפעיל הרתעה מוצלחת. עם זאת, בשל היתרונות הגלומים באסטרטגיית ההרתעה בהקטנת היקפי אלימות בסכסוכים, חשוב לנסות ולפתח עוד את המחקר העוסק בקשרים בין הרתעה לבין לוחמה קיברנטית. במאמר זה ביקשתי להצביע על שני כיוונים מרכזיים להמשך החשיבה והפיתוח של רעיונות אלה. ואולם, וכפי שטוען כאמור מורגן, יש לנהוג זהירות בתובנות

הקיימות, שכן נדרש עוד ידע אמפירי על מהותה של הלוחמה הקיברנטית, הן על הנזק שהיא גורמת, והן על הדרך שאפשר להשתמש בה.

הערות

1 Lupovici Amir, "The Emerging Fourth Wave of Deterrence Theory–Toward a New Research Agenda," *International Studies Quarterly* 54, no. 1 (2010): 705-732.

2 בלוחמה קיברנטית הכוונה היא לסוג מסוים של לוחמת מידע, הגם שלעתים המושג לוחמת מידע משמש כמושג חליפי למושג לוחמה קיברנטית. סוג לוחמה זה מבוסס על הניסיונות השונים למנוע, לשבש, לנצל או להשמיד את מערכות המידע של האויב, תוך הגנה על מערכות המידע של המגן מפני איומים דומים. ראו: Harknett J. Richard, "Information Warfare and Deterrence," *Parameters* 26, no. 3 (1996), pp. 93-97; Wheatley F. Gary and Hayes, E. Richard, Infor*mation Warfare and Deterrence*. (Washington DC: National Defense University Press, 1996), pp. v-vi, 5-6; Molander, C. Roger, Riddile, S. Andrew, and Wilson, A. Petter (1996). "Strategic Information Warfare: A New Face of War," *Parameters* 26 No. 3 (1996), pp. 83, 86-90. לסקירה מקיפה של מושגים מרכזיים על לוחמה במרחב הקיברנטי ראו: טבנסקי ליאור, "לחימה במרחב הקיברנטי: מושגי יסוד". **צבא ואסטרטגיה**, כרך 3, גיליון 1 (2011). עמ' 65–80.

3 על הנטייה הכללית של המחקר העוסק בלוחמת מידע וביטחון לבחון שאלות מדיניות, ולהמעיט בשילוב היבטים תיאורטיים כלליים יותר, ראו: Eriksson Johan and Giacomello Giampiero, "The Information Revolution, Security, and International Relations: (IR)relevant Theory?" *International Political Science Review* 27, no. 3 (2006), pp. 221-244.

4 במאמר זה אשתמש במונחים הרווחים לתיאור השחקנים הנוגעים לאסטרטגיית ההרתעה: השחקן המגן, השחקן המבקש להפעיל את אסטרטגיית ההרתעה כדי למנוע פעולה שאינה רצויה לו; והשחקן המאתגר, השחקן המבקש לפעול נגד המגן. השימוש במושגים החלופיים, השחקן המרתיע או השחקן המורתע, כפי שנעשה לעתים, הוא בעייתי, שכן הוא מרמז על הצלחת האסטרטגיה.

5 לסקירה מצוינת של הגדרות המושג הרתעה על־ידי איום ראו: Morgan, M. Patrick, *Deterrence Now* (NY: Cambridge University Press, 2003), pp 1-2.

6 George Alexander and Smoke Richard. *Deterrence in American Foreign Policy: Theory and Practice* (New York: Columbia University Press, 1974), p. 11.

7 חשוב להבהיר כי אסטרטגיה של הרתעה על־ידי מניעה גם שונה מאסטרטגיה של הגנה. אף שקיימת חפיפה ביניהן, הרי הגנה מבקשת לספק פתרון למקרה שאסטרטגיית ההרתעה תיכשל, ואילו הרתעה על־ידי מניעה מבקשת למנוע את הפעולה על־ידי כך שהמאתגר יבין שאין ביכולתו לבצע את הפעולה עקב יכולותיו של המגן.

8 להבחנה זו ראו: Snyder Glenn, *Deterrence and Defense* (Princeton: Princeton University Press, 1961). עם זאת, הרתעה על־ידי איום והרתעה על־ידי מניעה עשויות עקרונית לחזק זו את זו. אם מאתגר פוטנציאלי יידע לא רק שסיכויו להצליח נמוכים, אלא שגם ייגבה ממנו מחיר יקר, גדלים הסיכויים שהוא יימנע מפעולה.

9 Schelling Thomas, *Arms and Influence* (New Haven: Yale University Press, 1966), p. 69.

10 Carnesale Albert, Doty Paul, Hoffmann Stanley, Huntington, P. Samuel, Nye, Jr. S. Joseph, and Sagan D. Scott, *Living with Nuclear Weapons*. (Cambridge: Harvard University Press, 1983).

11 לדיון בהרתעה קונבנציונלית ראו למשל Shimshoni Jonathan, *Israel and Conventional Deterrence: Border Warfare from 1953 to 1970* (Ithaca: Cornell University Press, 1988); Mearsheimer J. John, *Conventional Deterrence* (Ithaca: Cornell University Press, 1983).

12 כך למשל נטען, שהתפתחות נורמות בינלאומיות הקוראות לאיסור השימוש בנשק גרעיני ודעת קהל בינלאומית התומכת בכך, מחלישות את אסטרטגיית ההרתעה הגרעינית מאחר שהן מעלות את מחיר מימוש האיום של המגן Paul T.V., "Nuclear Taboo and War Initiation in Regional Conflicts," *Journal of Conflict Resolution* 39, no. 4 (1995), pp. 699-700, 711.

13 חוקרים דנו בשאלה כיצד להגדיל את אמינות האיום, ואף הציעו אמצעים לכך, למשל "מסרים יקרים" (costly signals) Fearon James, "Domestic Political Audiences and the Escalation of International Disputes," *American Political Science Review* 88, no. 3 (1994), pp. 577–592. עם זאת, היו חוקרים שהטילו ספק באפקטיביות של חלק מן האמצעים האלה. לדיון בנושא ראו למשל Huth, Paul, "Reputations and Deterrence: A theoretical and Empirical Assessment," *Security Studies* 7, no. 1 (1997), pp. 72-99.

14 Morgan, *Deterrence Now*, pp. 15-16.

15 לסקירה מצוינת המדגימה היטב את הסוגים השונים של ההרתעה הישראלית ראו: בר־יוסף אורי, "50 שנות הרתעה ישראלית: לקחי העבר ומסקנות לעתיד". **מערכות**, גיליון 366–367, 1999, עמ' 12–29.

16 Harknett, Ibid, pp. 93-107; Berkowitz D. Bruce, "Warfare in the Information Age," In Athena's Camp: Preparing for Conflict in the Information Age. eds. John Arquilla and David F. Ronfeldt (Santa Monica, CA: RAND Corporation, 1997), pp. 183-184; Goldman O. Emily, "Introduction: Security in the Information Technology Age," In *National Security in the Information Age,* ed. Emily O. Goldman (London: Taylor & Francis, 2004), p. 3; Arquilla, John, "Thinking About New Security Paradigms," in National Security in the Information Age, ed. Emily O. Goldman (New York: Routledge, 2004), pp. 210-213. למסקנות דומות מגיע מורגן, הטוען כי היבטים שונים הנוגעים לפרקטיקות של ההרתעה מתקופת המלחמה הקרה ומבוססים הן על אסטרטגיה זו והן על גורמים תומכים כמו אמצעי בקרת נשק, רלוונטיים פחות להרתעה במרחב הקיברנטי. עם זאת, אין הוא פוסל על הסף את האפשרות של שימוש בסוגים שונים של אסטרטגיית ההרתעה להתמודדות עם איומים אלה Morgan, M. Patrick, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm," in *Proceedings of a Workshop on Deterring Cyberattacks*, eds. John D. Steinbruner et al., (Washington: The National Academies Press, 2010) pp. 55-76. נוכח מגבלות היכולת לבסס הרתעה כנגד לוחמה קיברנטית הוצע – במיוחד בעבור ארצות־הברית, שבה עוסק כאמור רובו של הדיון המחקרי – לנקוט אמצעים חלופיים לאסטרטגיה זו, למשל שימוש באמצעים הגנתיים. Adams James, Wheatley and Hayes, Ibid, p. 9; "Virtual Defense," *Foreign Affairs* 80 (2001), pp. 107-112.

17 Harknett, Ibid, pp. 96-97, 103-104; Wheatley and Hayes, Ibid, p. 9; Berkowitz, Ibid, pp. 183-184; Libicki C. Martin, *Conquest in Cyberspace* (Cambridge, UK: Cambridge University Press, 2007), p. 272. על הפגיעות של חברות (societies) למתקפות אלקטרוניות ראו: Deibert Ron, "Circuits of Power: Security in the Internet Environment," in *Information Technologies and Global Politics: The Changing Scope of Power and Governance*, eds. J.P. Singh and James N. Rosenau (NY: Suny Press, 2002), p. 115. על נקודות הרגישות לאיומים חיצוניים ופנימיים של מערכות

מידע, ראו: Libicki C. Martin, *Cyber Deterrence and Cyber War* (Santa Monica, CA: RAND Corporation, 2009), pp. 13-23. Available at: www.rand.org/pubs/monographs/2009/RAND_MG877.pdf.
עם זאת, חשוב לציין כי לטענת ליביקי היקף האיום שיוצרת לוחמה קיברנטית בתקופה הנוכחית אינו ברור או ודאי. לטענתו, סוגיית היקף הנזק שעשויה לוחמה קיברנטית לגרום היא מרכזית ועומדת בבסיס הוויכוח בדבר חשיבות אסטרטגיית ההרתעה כלפי סוג לוחמה זה Libicki, *Cyber Deterrence and Cyber War*, p. 36.
מסיבות דומות, הנוגעות למיעוט המידע הקיים וחדשנות הנושא, ממליץ מורגן להיזהר ממסקנות חפוזות בנוגע לאפשרויות ההרתעה של איומים במרחב הקיברנטי, Morgan, "Applicability of Traditional Deterrence Concepts", pp. 61-62.

18 Libicki, *Cyber Deterrence and Cyber War*, p. 26.

19 Harknett, Ibid, p. 104.

20 Molander et al., Ibid, p. 87.

21 על הקשיים בזיהוי מקורן של התקפות של לוחמה קיברנטית ראו גם: Libicki, *Cyber Deterrence and Cyber War*, pp. 44-45.

22 על דעת הקהל הפנימית והבינלאומית המגבילות את אפשרות השימוש בכוח, ובכך משפיעות על ההרתעה של השחקן המגן, ראו למשל: Jervis Robert, "Deterrence, Rogue States, and the Bush Administration," in Complex Deterrence, eds. T.V. Paul, Patrick Morgan, and James Wirtz (Chicago: University of Chicago Press), p. 153.

23 Hayes and Wheatley, Ibid, p. 9; Harknett, Ibid, p. 104; Berkowitz, 1997, pp. 183-184; Cordesman Anthony, and Cordesman, Justin, *Cyberthreats, Information Warfare, and Critical Infrastructure Protection: Defending the US Homeland*. (Westport: Praeger: 2001), p. 7; Arquilla, Ibid, pp. 210-211.

24 Libicki, *Cyber Deterrence and Cyber War*, pp. 1-3.

25 הסיבה לכך היא שהאיום המרתיע צריך להיות מותאם כאמור לסוג האיום ולסוג הגורם המפעיל אותו. לכן נטען כי קיימת חשיבות לבסס את ההרתעה על איום ממוקד כלפי מאתגר מסוים. למשל, הרתעה כלפי שחקן מדינתי הנהנה מריבונית בטריטוריה מסוימת ואשר יש לו "מטרות ערך", שונה מהרתעה כלפי שחקן שאינו מדינתי, המחייבת אפוא שימוש בסוגים שונים של איומים. סוגיה זו זוכה בשנים האחרונות לדיון נרחב בהקשר של הרתעה "תפורה" (tailored deterrence), בעיקר בהקשר של הרתעת טרור. לדיון במושג ראו: Lantis S. Jeffrey, "Strategic Culture and Tailored Deterrence: Bridging the Gap between Theory and Practice". *Contemporary Security Policy* 30, no. 3 (2009), pp. 469-471. לדיון במושג ביחס ללוחמה קיברנטית ראו: Kugler, L. Richard, "Deterrence of Cyber Attacks," in *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), pp. 331-333.

26 Harknett, Ibid, pp. 98-100.

27 Libicki, *Conquest in Cyberspace* p. 272. לדיון נוסף בהשפעת המהפכה בענייני צבא (RMA) על הרתעה ועל היכולת להרתיע ראו: Morgan, *Deterrence Now*, pp. 219-224.

28 ראו, Hayes and Wheatley, Ibid, pp. 13, 19-20 Kugler, Ibid, p. 328.; וכן ראו ב־ Cordesman and Cordesman, 2002, p. 7.

29 Morgan, "Applicability of Traditional Deterrence Concepts", p. 59.

30 במושג דומה – הרתעה מצטברת (cumulative deterrence) – השתמש דורון אלמוג בנוגע לדרך להרתיע איומים של טרור שלא במרחב הקיברנטי, Almog Doron, "Cumulative Deterrence and the War on Terrorism," *Parameters* 34, no. 4

(2004-2005): pp. 4-19.

31 Morgan, "Applicability of Traditional Deterrence Concepts", p. 59.

32 Lupovici, Ibid, p. 722.

33 כך למשל עשוי המאתגר ללמוד על אמצעי הגנה (או לקבל השראה לאמצעים כאלה) מהאמצעים שמשתמש בהם השחקן המבקש להפעיל הרתעה על־ידי מניעה, וכך הוא עלול להגביל את היכולת להרתיע באמצעות אסטרטגיה זאת.

34 ביקורת דומה הועלתה לאחר הדיווחים על וירוס סטקסנט (Stuxnet), שעל פי הפרסומים שיבש את פיתוח הגרעין באיראן. החשש שהציגו מומחים לאבטחת מידע הוא, כי תקיפה קיברנטית זו תשמש לא רק השראה למה שאפשר לעשות באמצעות סוג לוחמה זה, אלא שחלקים מהקוד של הווירוס עצמו נחשפו ועלולים לסייע לשחקנים שונים לפגוע בתשתיות רגישות. ראו למשל: "Experts Fear Hackers Can Launch Stuxnet-Like Attacks on Power Plants, Prison Gates", *The Globe and Mail*, October 24, 2011.

35 Morgan, "Applicability of Traditional Deterrence Concepts", p. 63.

36 לאזכור של סוגיה זו בהקשר של לוחמת מידע ראו למשל: Goldman, 2004, p. 3.

37 לדיון במגוון איומים אלה ראו: טבנסקי 2011, ובעיקר עמ' 70, 75–77.

38 הבחנה בסיסית רווחת במחקר ההרתעה מבדילה בין הרתעה כללית, המבוססת על הניסיון למנוע מהיריב לשקול אפשרות של תקיפה (למשל כפי שבא לידי ביטוי בהרתעה גרעינית), לבין הרתעה מידית, הנוגעת למצב שבו שחקן מבקש לעשות פעולה (למשל מזיז כוחות) ובעזרת שימוש באיומים המגן מניא אותו מפעולה זאת. דיון חשוב ומעניין בהקשר זה יכול לעסוק במשמעות של כל אחת מצורות ההרתעה הללו במרחב הקיברנטי.

39 ליביקי, למשל, החל לבחון הרתעה מורחבת במרחב הקיברנטי, Libicki, *Cyber Deterrence and Cyber War,* pp. 104-106. ואפשר למקד ולפתח עוד את הדיון בסוגיות התיאורטיות שנידונו בנוגע לאסטרטגיה זו. לדיון במושג הרתעה מורחבת ראו למשל: Huth Paul, *Extended Deterrence and the Prevention of War* (New Haven: Yale University Press, 1988), pp. 15-27.

40 כאמור, הספרות בנושאי ההרתעה מדגישה את הצורך בהעברת המסר המאיים לצד היריב, ובכלל זה את המחיר שהוא יידרש לשלם. לכן מסרים לגבי יכולות המגן או חשיפת האמצעים שבידו הוזכרו כגורמים חשובים בהקשר הזה.

41 "ארצות־הברית מקימה פיקוד צבאי למלחמה בהאקרים", *Ynet*, 24 ביוני 2009, http://www.ynet.co.il/articles/0,7340,L-3736253,00.html

צבא המילואים שוקע[1]

יגיל לוי

מידי ל"ג בעומר נחגג ברוב הדר יום ההוקרה לחיילי המילואים וראשי הצבא והמדינה מעלים על נס את תרומתם של אנשי המילואים לביטחון המדינה. בשנת 2011 אף נלוו לאירוע זה טונים צורמים – המשך המחאה של ארגוני המילואים על הפער בין התחייבויות המדינה למימושן, מחאה של אנשי מילואים שהושמעה בעת ביקור הנשיא והרמטכ"ל באימון בצאלים ודיון סוער בכנסת.

לבל נטעה, מערך המילואים של צה"ל, בעבר התשתית העיקרית של הכוח הצבאי, נמצא בפרשת דרכים כשהפיקוד הצבאי עצמו והדרג המדיני אינם יודעים כנראה באמת כיצד לעצבו מחדש. אבקש לטעון כי השילוב של עלויות פוליטיות ועלויות כלכליות גבוהות הכרוכות בהפעלתו של מערך המילואים מאיץ את שקיעתו כחלק מצעידתו לעבר מודל של צבא מילואים מקצועי.

האמרת העלויות של מודל המילואים

מודל המילואים של צה"ל הוא מודל יקר, פוליטית וכלכלית. בראשיתו זה היה דווקא מודל זול: האתוס של אומה מגויסת הבטיח כי אנשי המילואים ימלאו את תפקידיהם בצייתנות פוליטית מלאה. בה בעת, שירות המילואים היה זול מהבחינה הכלכלית ככל שהמעבידים או אנשי המילואים נשאו בעיקר העול של הפיצוי למשרת על אובדן השתכרותו, בטרם התעצבה מערכת הפיצוי המלאה של הביטוח הלאומי, בעיקר לאחר 1967.

העלויות הפוליטיות עלו לאחר 1967. מצומת 'ההמתנה' ערב מלחמת ששת הימים, עת תססו אנשי המילואים לנוכח היסוסיה של הממשלה לצאת למלחמה, החלה לחלחל לתודעתם של מקבלי ההחלטות המודעות לעלות הפוליטית של גיוס המילואים. אנשי המילואים הם בעלי פוטנציאל למיקוח פוליטי, הן משום שהם 'אזרחים מחוילים' החיים בשני עולמות בעת ובעונה אחת,[2] והן משום מיקומם הטבעי במעמד הבינוני – אם במקור (שכן הם משקפים את צבא החובה

פרופ' יגיל לוי הוא חבר סגל האוניברסיטה הפתוחה

של העבר, שבו היה ייצוג גבוה יותר למעמד הבינוני) ואם כתוצאה של מוביליות חברתית. עלות פוטנציאלית זו (עלות כלכלית היכולה להיתרגם לפוליטית ערב בחירות 1973) נמנתה עם השיקולים המכריעים בהחלטה להימנע מגיוס המוני ערב מלחמת יום הכיפורים. זאת, על רקע גיוס הסרק היקר של חלק ממערך המילואים חודשים מעטים קודם לכן, מחשש להתקפה מצרית, מהלך אשר עורר ביקורת על הצבא.[3] הימנעות זו מגיוס המילואים עיצבה כזכור את תוצאות המלחמה.

התארגנויות שונות של אנשי המילואים לאחר 1973, ממוטי אשכנזי ועד ל'שלום עכשיו', תרמו להפקעת המונופול על קבלת החלטות צבאיות מידי האליטה הפוליטית ולהרחבה של גבולות השיח הפוליטי באופן ששחק בהדרגה את מרחב החופש של הממשלה בקבלת החלטות צבאיות ומדיניות. תהליך זה התעצם לאחר מלחמת לבנון הראשונה. התארכותה של המלחמה, הרחבת מטרותיה וההיגררות למלחמת התשה ממושכת הזינו התארגנויות חדשות של אנשי מילואים, המשולבות לראשונה בסרבנות סלקטיבית ומאורגנת, ובמרכזם 'יש גבול' ו'חיילים נגד שתיקה' לצד 'שלום עכשיו' הותיקה. פעולות המחאה שחוללו תרמו תרומה מכרעת לנסיגה החד־צדדית של צה"ל מלבנון בשנת 1985. זאת, שנתיים לאחר שהממשלה הורתה על נסיגה חלקית מאזור ביירות ומהרי השוף לנהר האוואלי; 'יצאנו מלבנון בגלל המילואימניקים' (כלומר מחאתם), אמר שר הביטחון משה ארנס.[4]

משלב זה הפנימו מקבלי ההחלטות את התובנה כי לפריסה של אנשי מילואים עלות פוליטית ניכרת המביאה לצמצום מרחב החופש של קבלת ההחלטות הפוליטיות. על רקע זה, משפרצה האינתיפאדה הראשונה בשנת 1987 והתפתחו לחצים של מפלגות הימין השותפות לממשלה, להורות לצבא לדכא את ההתקוממות האזרחית בכוח, בעוד השמאל שולל זאת, התייצב הרמטכ"ל דן שומרון מול הממשלה. הוא הכריז שלהתקוממות יש פתרון מדיני אך לא צבאי. בכך ביקש הרמטכ"ל למתן את אופי המשימות של הצבא בדיכוי ההתקוממויות. לצד אולי גם שיקולים אחרים, שומרון ביקש למנוע את התפוררות הצבא, שבו שירתו באותה עת חיילים משמאל ומימין בצורה מאוזנת למדי, ובעיקר כאשר פריסת הצבא בשטחים נשענה באופן משמעותי על כוחות המילואים, 'בוגרי לבנון'. קביעתו מיתנה, קרוב לודאי, התנגדות פוטנציאלית של החיילים משורות השמאל, בכך שהעניקה לתפקודם משמעות של מהלך זמני והכרחי שאינו מביא הכרעה – זו תושג על שולחנות הדיפלומטים. הריסון הצבאי סלל את הדרך לנסיגה חלקית משטחי הגדה המערבית ורצועת עזה בדמות הסכמי אוסלו. יתר על כן, ראש הממשלה יצחק רבין העיד, כי החשש שמא בעת מלחמה לא הסכמית תיכשל הממשלה לממש גיוס מלא של מילואים, מילא תפקיד בהחלטתו לעלות על נתיב אוסלו.[5]

מחאת המילואים גילמה חלק מהרגישות החברתית הגוברת לחללים צבאיים. בטאו זאת היטב 'חיילים נגד שתיקה', ארגון של חיילי מילואים משוחררים שהפגינו מול ביתו של ראש הממשלה מנחם בגין במחאה על מלחמת ההתשה הלבנונית, ונשאו שלטים ועליהם מספר החללים המעודכן. רגישות זו הביאה את הצבא לעיצוב מדיניות של מניעת נפגעים המצמצמת את העמדתם של חיילים תחת סיכון ואף נמנעת מביצוע משימות עתירות סיכון. זאת, בדומה לתהליכים דומים שפקדו את צבאות המערב בעיקר מאז מלחמת וייטנאם.

מרכיב אחד של מדיניות זו היה להרחיק את אנשי המילואים מזירות הלחימה הרגישות. אכן, מלחמת הגרילה לתוכה שקע צה"ל בלבנון בשנים 1985–2000 הושענה על הכוחות הסדירים. ההישענות על הסדירים גם צמצמה את הסיקור העיתונאי על הנעשה בזירה זו, כפי שהעיד ממקור ראשון משה (צ'יקו) תמיר ממפקדי הכוחות בלבנון.[6]

כך גם באינתיפאדה השנייה. אל ליבת הלחימה הוטלו חיילי המילואים בעיקר ב'חומת מגן', רק לאחר שהלגיטימציה של הלחימה נבנתה על בסיס לחימת הסדירים במהלך כמעט שנתיים. גם אם שיעורי ההתייצבות היו גבוהים, הרי שבאופן לא מפתיע, מחאת המילואים על אופי המשימות ועל חלוקת הנטל והתגמול, שבה והתעוררה כשהמבצע הסתיים, בעת שעדיין התנהלה 'מלחמה על הבית', כפי שלחימת הצבא בפלסטינים צוירה בשיח הציבורי. למשל, החלטת הממשלה להארכת מכסת המילואים (מ־30 ל־37 יום) לאחר מבצע 'חומת מגן', עברה, אך רק לאחר התנגדות ובהמשך נבלמה הצעה להארכה נוספת.[7]

מרכיב אחר של מדיניות מניעת הנפגעים קבל ביטוי בעיצובה של תורת הלחימה. מאז שנות התשעים, הצבא השעין את תורת הלחימה החדשה על טכנולוגיה, ועיצב אותה על בסיס 'אש מנגד', שעיקרה העתקת האש – בשונה מהגייסות – אל שטח האויב, בהבדל מתפיסת הלחימה המסורתית עד שנות השמונים. התורה בוססה על רכישת יכולת גבוהה של השמדת מטרות באמצעות אש אווירית וארטילרית, עם דגש על חימוש מדויק וללא כניסה הכרחית של כוח יבשתי לשטח האויב. במבצעי 'דין וחשבון' ו'ענבי זעם', נגד חזבאללה של שנות התשעים, יושמה לראשונה התורה החדשה, והיא השתכללה במלחמת לבנון השנייה ובמבצע 'עופרת יצוקה'. בדומה ל'מהפכה בעניינים צבאיים' (Revolution in Military Affairs) שקידם צבא ארצות הברית בשנות השמונים, התורה החדשה של צה"ל נועדה בין היתר לחסוך בנפגעים באמצעות שימוש אינטנסיבי בטכנולוגיה (דוקטרינה של 'הלם ומורא'), כך שניתן יהיה לקצר את משך הלחימה ולהביא להכרעה מהירה בהתחשב באילוצים הפוליטיים החדשים.

גישה זו באה לידי ביטוי במלחמת לבנון השנייה, המבטאת נקודת שבר משמעותית ביחסי הצבא עם אנשי המילואים, שנבטה על תשתית משברית

מוקדמת, כפי שיובהר בהמשך. הלחימה הושענה בתחילה על הפצצות מהאוויר כהפעלה של 'אש מנגד'. המילואים גויסו רק לאחר 16 ימי לחימה.[8] ההיסוס לגייסם ביטא את העלות הפוליטית הכפולה בה כרוך הגיוס: החשש כי מחיר דמים גבוה, בעיקר של חיילי מילואים, עלול לשחוק את התמיכה הציבורית בפעולה צבאית, ולפגוע בלגיטימיות של הממשלה והצבא,[9] לצד ההבנה כי מרגע בו גויסו המילואים, מצטמצם חופש הפעולה של הממשלה. כך התבטא הרמטכ"ל דן חלוץ, שניסה לשכנע את הממשלה לצאת למבצע יבשתי כולל ולא מדורג בסוף המלחמה: "אין פה דרכי ביניים – נעשה חצי, נעשה רבע, נעשה שליש בשביל לרצות חלק מהמאוויים שלנו... זה הכל או לא כלום, מן הטעם שיש גם אנשים מאחורי המוכנות הזאת ויש סד"כ מילואים שיושב דרוך ומוכן, ואיננו יכולים להחזיק אותו כפות תחת 'תמתינו, תמתינו'.[10] במילים אחרות, יש כאן הד למורשת תקופת ההמתנה של 1967, שמשעותה שהממשלה אינה יכולה להרשות לעצמה המתנה ממושכת העשויה לעודד תסיסה של אנשי המילואים.

עלות פוליטית זו אכן התגלתה כרלבנטית לאור המחאה של אנשי המילואים לאחר המלחמה. אנשי מילואים חברו להורים שכולים ולקבוצות אחרות שמחו על תפקודו הלקוי של הצבא במלחמה. המחאה תרמה להגבהת חסם נוסף בפני יכולת הצבא לסכן את חייליו, דרך גיבוש הציפייה שהממשלה תימנע מלסכן חיילים לשווא. סיכון כזה מתקיים בנסיבות שבהן אין לממשלה יכולת פוליטית להשלים את המשימה הצבאית, גם אם צדקת המשימה אינה מוטלת בספק פוליטי, ובנסיבות שבהן אין לממשלה יכולת לבצע את המשימה בשל אי־מוכנות הצבא. לא בכדי, אומדן גבוה של הרוגים, ובהם אנשי מילואים רבים, היו בין השיקולים המרכזיים שהנחו את הממשלה לדחות את הפעולה היבשתית בעזה לאורך זמן. היא אישרה זאת רק משבשלו התנאים להפעיל מדיניות אש שתקטין את חשיפת חיילי צה"ל לסיכון על חשבון הגברת הסיכון של אזרחי עזה.[11] לפינוי יישובי עזה בשנת 2005 כמעט ולא נקראו מילואים, ומשימה זו, השנויה במחלוקת פוליטית חריפה, הוטלה על חיילי החובה והקבע.

המחשה עדכנית לעלות הפוליטית הכרוכה בפריסת מילואים נתן גדוד מילואים ששירת בשנת 2011 בגבול ישראל־מצרים. חיילים וקצינים בגדוד הבהירו בתחילת שירותם למפקדי הגזרה שלא ישתתפו בנוהל 'החזרה חמה', הנוהל המסמיך את חיילי צה"ל ואת שוטרי מג"ב להחזיר מבקשי מקלט (כמו פליטים מסודן) למצרים ולמוסרם לשוטרים המצריים לאחר תשאול קצר, המוודא שאינם מבקשי מקלט מדיני אלא מסיגי גבול. אנשי המילואים פעלו כך משהבינו כי המוחזרים צפויים להתנהגות אלימה מצד המצרים. מפקד החטיבה המרחבית נענה לבקשת החיילים והורה כי בעת שירות הגדוד בגזרה לא יבוצע בה הנוהל השנוי במחלוקת, נוהל המבוצע תדיר כאשר גדוד 'קרקל' הסדיר מוצב בגזרה.[12] זוהי המחשה כיצד אנשי

מילואים יכולים להשפיע, גם אם זמנית, על הגבלת מרחב הפעולה העצמאי של הצבא.

מחאות אנשי המילואים חידדו עוד לפני מלחמת לבנון השנייה את התחושה שנוצר 'משבר מילואים', כפי שכונתה תופעה זו מאז שנות התשעים. תחושת המשבר המריצה את הממשלה, בלחץ ארגוני המילואים ובעידוד שדולת המילואים שקמה בכנסת, לאשר רפורמה במודל הגיוס. גיבושה החל בוועדה בראשות קצין מילואים ראשי, תא"ל אריאל היימן, נמשכה ב'ועדת ברוורמן'; ומוסדה בחקיקתו של 'חוק שירות המילואים, התשס"ח–2008'. החוק הגביל את סמכות המדינה לגייס אנשי מילואים והכפיפה לכללים מוגדרים יותר מבעבר. בין היתר נקבע כי חייל מילואים לא ייקרא לשירות מילואים למטרת תעסוקה מבצעית יותר מפעם אחת במהלך תקופה של שלוש שנים רצופות (סעיף 7, ג'2,), בעוד גרסאות קודמות של הרפורמה גִלמו הגבלה משמעותית עוד יותר. הוראה זו ביטאה את העלות הפוליטית של פריסת המילואים מעצם הקביעה כי התעסוקה המבצעית תתבסס על כוחות הסדיר בעוד פריסת מילואים היא חריג.

העלות הפוליטית של מערך המילואים האמירה במשולב עם העלות הכלכלית. הנסיגה הראשונה מלבנון אפשרה לממשלה להסב את מערך המילואים לברירני בחלקו, לאו דווקא בהחלטה מפורשת ומודעת. כחלק מהקיצוץ העמוק בתקציב הביטחון בשנת 1985, הוחלט על העברה הדרגתית של תקצוב ימי המילואים מהביטוח הלאומי לצבא. קודם לכן העלות של ימי המילואים, בעיקר הפיצוי למשרת על אבדן השתכרותו, לא הועמסה על תקציב הביטחון, ולכן מערך המילואים נוהל בעיקרו במנותק משיקולים כלכליים של מערכת הביטחון. בעקבות ההחלטה תומרץ הצבא לחסוך בימי המילואים, ולהשתמש בחיסכון למטרות אחרות. נוסף על המשמעויות התקציביות, ניהול מערך המילואים הוכפף לכלליה של כלכלת השוק, ולראשונה הודבק 'תו מחיר' כלכלי לשירותם של אנשי המילואים. התוצאה הייתה קיצוץ ניכר בימי המילואים, והקלה של נטל השירות. להמחשה: הבסיס התקציבי של שנת 1985, טרם השינוי, היה 10 מיליון ימי מילואים לשנה. עקב הקיצוץ ירדה צריכת ימי המילואים לכ־3 מיליון, נכון לשנת 2006.[13] מגמת הירידה הורגשה גם בשנים שבהם מערך המילואים הושקע בלחימה, בעיקר בשתי האינתיפאדות.

אולם צמצום הצריכה של ימי המילואים הגדיל את אי השוויון בחלוקת נטל השירות, ככל שהצבא איתר תחליפים לדרג המנהלה אך לא לדרג הלוחם. כשליש ממשרתי המילואים נשאו ב־80% מהנטל, נכון לראשית שנות ה־2000, ורק 10% מחייבי הגיוס (כלל חייבי הגיוס הם כמחצית מהגברים בישראל בגילאי הגיוס למילואים) ביצעו מדי שנה שירות מילואים העולה על 10 ימים.[14] כלומר, אחוזים בודדים משתתפים במה שפעם נחשב למוסד המגדיר את הגבריות

הישראלית.[15] אתוס 'צבא העם' נסוג מפני אתוס השוק. אי השוויון המחריף היה הרקע להתארגנויות אנשי המילואים באמצעות ארגונים שונים (פורום המגדי"ם היה החלוץ ואחריו פורום החפשי"ם ו־בלת"ם) בתביעה לחלוקת הנטל ולתגמול המשרתים, לצד מחאה בנושאים כמו ביטוח הסיכון של חיילים ובהם טייסים. לחצים אלה הניבו את חוק שירות המילואים.

העלות הכלכלית הגבילה את הכשרתם של אנשי המילואים למלא את משימותיהם בחירום ואמוני המילואים צומצמו משמעותית משנת 1989. בד בבד צומצמו באופן ניכר מאז שנת 2002 גם אימוני היחידות הסדירות, כתוצאה מהקושי לגייס יחידות מילואים שיחליפו את היחידות הסדירות, השקועות בלחימה בזירה הפלסטינית. הייתה בכך פגיעה נוספת בכשירות מערך המילואים המוזן מהיחידות הסדירות, לצד הפגיעה בכשירות היחידות הסדירות עצמן. בשנים 2003 עד 2005 דיווח צה"ל לדרג המדיני, שקיימת פגיעה מתמשכת באימוני מערך המילואים בכוחות היבשה עקב קיצוצים בתקציב.[16] על רקע זה, שכלול תורת 'אש מנגד' התקבע גם כתוצאה ממגבלות התקציב, שהביאו לירידה בכשירות צבא היבשה. בתורו – אימוץ התורה ועיצוב התוכניות המבצעיות על יסוד 'אש מנגד' השפיעו עוד על הקטנת ההשקעה של משאבים בצבא היבשה, שכן ההשקעה בו התייתרה בחלקה לנוכח הדגש על ממד האש. לכן, משהחליטה ממשלת ישראל להגיב בעוצמה על חטיפת חיילי המילואים ביוני 2006, תגובה שהפכה למלחמת לבנון השנייה, מכה אווירית הייתה המענה העיקרי והמועדף. המילואים גויסו באיחור, ונסיבות הגיוס וההפעלה הולידו, כאמור, מחאה.

חוק שירות המילואים ש'משבר המילואים' הוליד, העלה את העלויות הכלכליות של גיוס מילואים, בכך שקבע תגמול מיוחד למשרתי המילואים, מעבר לפיצוי עבור אבדן השתכרות. כבר בשנת 1998 נקבע לראשונה בחוק, שאנשי המילואים יפוצו לא רק על אבדן השתכרותם אלא גם כתגמול על עצם שירותם ('תגמול מיוחד') והחוק החדש מיסד זאת והוסיף 'תגמול נוסף' באמצעות רשות המסים. העיקרון של צבא מקצועי החל להתמסד מעבר לפרקטיקה שבאה לידי ביטוי עוד קודם לכן.

בתמצית, ההנהגה הפוליטית והפיקוד הצבאי הפנימו את העלויות הפוליטיות והכלכליות של גיוס המילואים והפנמה זו הניחה תשתית לתהליך המתגלגל שתואר כאן ושהביא בהדרגה לצמצום משאביו של מערך המילואים ולכן גם לצמצום תפקידיו בפועל. אין בזאת כדי לטעון למודעות מפורשת של מקבלי ההחלטות אלא להפנמה המעצבת את התרבות האסטרטגית של הצבא ובכך קובעת את גבולות המרחב של ההחלטות הזמינות. כך בהדרגה, הצבא הוגבל בהפעלתו של מערך המילואים. הפעלתו הושתתה על מיקוח כלכלי המשולב גם בהגברת המיקוח הפוליטי, המתנה את ביצוע המשימות בהתאמתו לערכי המגויסים, ובכך הגבילה את הפעלתו, גם אם לא נדרשה עוד במלואה.

מבט לעתיד

לכאורה, 'חוק שירות המילואים' וההשקעה המאסיבית באימוני מערך המילואים בשנים שלאחר מלחמת לבנון השנייה סמלו שינוי בגישת הצבא והדרג הפוליטי לגבי חשיבותו של מערך המילואים. אך על מערך זה נגזר לשקוע ככל שעלויותיו ימשיכו לעלות.

העלות הפוליטית תעלה ככל שתפקודו של הצבא יהיה שנוי במחלוקת פוליטית, אם על מטרות הפעלת הכוח ואם על העלויות הנדרשות למימוש מטרות יחסית מוסכמות. מחלוקת זו מועצמת בנסיבות של רגישות חברתית גוברת לחללים. רגישות שכזו מנמיכה את רף הביקורת הציבורית על תפקודו של הצבא ומביאה אותו ואת הדרג הפוליטי לנהוג במשנה זהירות בטרם ייקראו אנשי מילואים.

עלות זו נפגשת עם העלות הכלכלית. הלחצים של אנשי המילואים לשיפור חבילת התגמול, כדי להבטיח כי תכסה את מלוא עלויות שירותם, לא תמו עם הנהגתו של החוק. גם סקר של מחלקת מדעי ההתנהגות של הצבא הראה כי שליש בלבד מקרב המשרתים ביחידות לוחמות סבור כי ההטבות והתגמולים משמעותיות.[17] יתר על כן, בשיח אנשי המילואים עם הצבא והממשלה עולה שוב ושוב התופעה של אנשי מילואים המופלים לרעה במקומות עבודתם, בפרט מפקדים. מנקודת מבטם של מעסיקים רבים, שירות המילואים אינו עוד הון חברתי שאיש המילואים מביא איתו למקום העבודה האזרחי אלא משיא תשואה שלילית. לאורך זמן, הקושי להתמודד עם תופעה זו יגביר את הלחצים לתגמול ולפיצוי אנשי המילואים.

מקור אחר ללחצי תגמול הוא התרחבות שיעורי אי־השוויון בחלוקת הנטל. כאמור, חוק שירות מילואים מיסד את המעבר למודל שירות בררני. המשמעות היא שצעירים המתעקשים על שחרור ממילואים, יהיו פטורים משירות במרבית המקרים, גם אם חובת השירות הפורמאלית נותרה בעינה. יתר על כן, לא רק שמוסדה ההסמכה של הצבא לפטור משירות ביטחון את מי שאינם בשירות סדיר, החוק אף מניח תשתית לעידוד שחרור שכזה דרך שני מנגנונים: (1) הגבלת שירות המילואים להכשרה ואימון לשם מימוש יעדו של החייל בשעת חירום ולתעסוקה מבצעית מנפה מהשירות בעלי תפקידים במקצועות מנהלה שונים; (2) הטלת החובה על הצבא להבטיח את רמת הכשירות של אנשי המילואים מעודדת את פליטתם של אלה שהצבא לא ישקיע בשמירה על כשירותם אך גם לא יחזיקם במערך המילואים ללא שמירה שכזו, הסותרת את הוראות החוק. מכיוון אחר, ועדת ברודט, שמונתה על ידי הממשלה לאחר מלחמת לבנון השנייה, כדי לדון בגודל ובהרכב הרצויים של תקציב הביטחון לטווח הקצר והארוך, המליצה על אזרוח תפקידים צבאיים, לרבות אלה שמאוישים על ידי אנשי מילואים, הניתנים לרכישה בשוק.[18] בכך מתחזק התמריץ לצמצם תעסוקה של אנשי מילואים.

מנגד, בעוד ועדת ברוורמן וחוק שירות המילואים בקשו למתן את האפקט של אי השוויון על ידי צמצום היקף הקריאה למילואים, הצבא מפגין התנגדות שיטתית לכך. לאחרונה התבטא סגן הרמטכ"ל, יאיר נווה, בגלוי משקבע: "הצורך שלנו במשימות לאורך הגבול דורש מאיתנו להגדיל את הסד"כ בתעסוקה... אני באופן אישי המלצתי, וגם הרמטכ"ל מסכים, שעדיף לפגוע בחוק המילואים ולא לפגוע באימונים.."[19] יש בכך כדי להעיד על הדפוס רווי הסתירות של טיפול המדינה במערך המילואים: הכרה הצהרתית בחשיבותו לשעת חירום, ניסיון לתגמל את המשרתים אך גם העמקת אי־שוויון באופן שאינו סימטרי לתגמול.

התוצאה היא שהצבא יצטרך להגדיל את התגמול הכספי. אך ככל שיעשה זאת, הוא ייטה לחליפין בין תגמול ובין הקטנת היקף המגויסים כדי להפחית עלויות, עד כדי מעבר בלתי נמנע, כחלק מתנועה ספיראלית של תגמול מול בררנות, לצבא מילואים מקצועי (מהלך העשוי להתרחש במקביל גם בצבא הסדיר). הצורך למקצע את מערך המילואים יתמוך במגמה זו. לצד זה, הפיכת צבא המילואים למקצועי תפחית את העלויות הפוליטיות הכרוכות בהפעלתו ככל שיכונן דפוס יחסים המסב את מערכת היחסים החוזית בין הצבא ובין מגויסיו, מחוזה רפובליקני במישור מדינה – קבוצה, המקנה לאנשי מילואים את הזכות להביע קול פוליטי בשם תרומתם הצבאית, לחוזה העסקה במישור צבא־פרט. חוזה כזה מחליש את התשתית למחאה פוליטית היוצאת משורות צבא המילואים. ממשלות תמיד יעדיפו עלות כלכלית על פני פוליטית ובפרט עלות כלכלית המאזנת את העלות הפוליטית.

המחשה לכך הציעה מלחמת לבנון השנייה: הממשלה החליטה לתגמל את אנשי המילואים שהשתתפו במלחמה (8 ימים לפחות) בתגמול מיוחד, שכונה 'החזר הוצאות', בגובה של 400 שקל, ו־50 שקל נוספים לכל יום, מיום השירות התשיעי ומעלה.[20] תגמול זה היה מעבר לפיצוי המעוגן בחוק עבור אבדן ההשתכרות. במלחמות העבר, שבהן גויסו אנשי מילואים לתקופות ממושכות יותר ולשירות קשה יותר, לא הוענק תגמול שכזה, מעבר למנגנוני הפיצוי הפורמליים שהיו נוהגים תמיד. את התגמול המיוחד ניתן לקרוא כמנגנון לשיכוך המחאה של אנשי המילואים (שלא בכדי לא נדרש לאחר 'עופרת יצוקה', שהצטיירה כהישג). יש לזכור שהתגמול אושר באוגוסט 2006, לאחר שיחידות המילואים שוחררו ומחאתם על המלחמה החלה להישמע, בעיקר – בשלב ראשון – על הרמה הנמוכה של כשירות היחידות. ככל שמנגנון הגיוס מבוסס על שכירה ולא על גיוס, כלומר ככל שהתגמול הכספי ממלא תפקיד מרכזי יותר, כך נעקף הצורך להתמודד עם דרישות, ציפיות ומחאות בעלות ממד פוליטי, או עם כאלה שעשויות להתפרס לשדה הפוליטי. תגמול זה, ובהמשך לו מערכת התגמולים הכספיים ש'חוק שירות המילואים' הניח את יסודותיה – מערכת העתידה להתעצם ככל שהשירות יהיה בררני יותר – מחזקים את פרופיל השכירה על פני הגיוס של מערך המילואים,

ומפחיתים את הפוטנציאל לקול פוליטי. התודעה הפוליטית האזרחית ממלאת תפקיד משני. כך העלות הכלכלית מאזנת את העלות הפוליטית.

לטווח ארוך, מערך המילואים יצטמצם ויעמוד על מודל מקצועי המתבסס על שירות של מעטים יחסית, בהדרגה בהתנדבות, לתקופות ארוכות יחסית, שיבטיחו את השמירה על כשירותם בתמורה לתגמול כספי הולם, בדומה למודל שכמה צבאות מערביים אמצו על חורבות גיוס החובה. ישראל צועדת בכיוון זה. האוטונומיה המקצועית של הצבא ושל מפעיליו הפוליטיים תצא נשכרת מכך, אך הדמוקרטיה, שקולם של אנשי המילואים היה נדבך חשוב שלה, מעצם היכולת לרסן את הפעלת הצבא, תינזק.

הערות

1 תודתי לעלה מינקובסקי מפורום החפשי"ם (אחד מהארגונים הנאבקים על מעמד אנשי המילואים וזכויותיהם) על הערותיו המועילות על טיוטת המאמר.

2 ניר גזית, עדנה לומסקי־פדר ואייל בן־ארי, "המילואימניקים בין העולמות", **מערכות** 394 (מאי 2004), עמ' 87–94.

3 ראו: בני מוריס, **קורבנות – תולדות הסכסוך הציוני־הערבי 1881–2001**, עם עובד, תל־אביב, 2003, עמ' 375; אורי בר־יוסף, **הצופה שנרדם: הפתעת יום הכיפורים ומקורותיה**, זמורה־ביתן, תל־אביב, 2001, עמ' 225–226.

4 עפר שלח ויואב לימור, **שבויים בלבנון: האמת על מלחמת לבנון השנייה**, ידיעות ספרים, תל אביב, 2007, עמ' 319.

5 יורם פרי, "יחסי חברה–צבא בישראל במשבר", **מגמות**, כרך ל"ט, גליון 4 (1999), עמ' 394.

6 משה תמיר, **מלחמה ללא אות**, מערכות, תל אביב, 2005, עמ' 10–11, 274.

7 מהלכים אלה מתועדים באתר פורום החפשי"ם http://miluim.ipaper.co.il/1411

8 **הוועדה לבדיקת אירועי המערכה בלבנון, דין וחשבון סופי**, משרד ראש הממשלה, ירושלים, 2008, עמ' 250.

9 שם, עמ' 411, 526.

10 שם, עמ' 180.

11 יגיל לוי, **מי שולט על הצבא: בין פיקוח על הצבא לשליטה בצבאיות**, מאגנס, ירושלים, 2010, עמ' 168–170.

12 אנשיל פפר, "אנשי המילואים התנגדו להחזרה בכוח של מסתננים למצרים – והנוהל הוקפא", **הארץ**, 22 באפריל, 2011.
http://www.haaretz.co.il/hasite/spages/1225775.html

13 כנובע מניירות אלה: **פגיעה בעובדים בשל יציאתם לשירות מילואים**, מרכז המחקר והמידע של הכנסת, ירושלים, 2003; **אומדן העלות התקציבית של יישום הצעת חוק הביטוח הלאומי**, מרכז המחקר והמידע של הכנסת, ירושלים, 2007.

14 אריאל היימן, "מערך המילואים, צה"ל והחברה הישראלית – עבר, הווה, ועתיד", **מערכות** 394, (מאי 2004), עמ' 5.

15 כפי שהראתה: Sara Helman, "Militarism and the Construction of Community," *Journal of Political and Military Sociology,* vol. 25, no. 2 (1997), pp. 305-332.

16 מבקר המדינה, **דו"ח שנתי 58א**, משרד מבקר המדינה ונציב תלונות הציבור, ירושלים, 2007, עמ' 87–97.

17 ממד"ה, **עמדות מפקדים ומשרתי מילואים בדרג א' 2011**, 2011.
http://portal.knesset.gov.il/Com4bitachon/he-IL/CommitteeHistory/24052011.htm
18 **דו"ח הוועדה לבחינת תקציב הביטחון**, משרד ראש הממשלה, ירושלים, 2007, עמ' 105.
19 יוני שנפלד ונועה הורוויץ, "בשנים הקרובות נקרא למילואימניקים לא פחות, וכנראה גם יותר", **במחנה**, 25 במאי 2011.
20 צה"ל, **חוברת מידע לאיש המילואים**, 2006, עמ' 7.
http://www.aka.idf.il/SIP_STORAGE/files/4/59004.pdf

סוף מעשה במחשבה תחילה

על נסיגת צה"ל מלבנון בשנת 2000

גיורא אילנד

מאמר זה מציג כמה מהעובדות וכמה מהמסקנות הנובעות מהנסיגה של ישראל מלבנון ב־2000. כמו כן מובאים שני אירועים נוספים שהתרחשו לאחר מכן: מלחמת לבנון השנייה בשנת 2006, ואירוע קטן יחסית, אבל חשוב – יציאת כוחות סוריה מלבנון בשנת 2005. כל המאורעות הללו קשורים זה בזה.

לפני שהחליט ראש הממשלה ושר הביטחון דאז אהוד ברק לצאת מלבנון, וכדבריו אז, עם הסכם או בלעדיו, נראתה המערכה הצבאית של ישראל בלבנון באופן הבא: לחימה טקטית עם חזבאללה, כמעט כולה באזור הביטחון או בשוליו; צה"ל מנסה לשפר את יכולתו, אך גם האויב משפר את היכולות שלו; השיפורים בשני הצדדים התקזזו פחות או יותר, ומספר הנפגעים הישראלים בשנה היה קבוע למדי – בין 20 ל־25 הרוגים בשנה, בלי קשר, כמעט, לאירוע מסוים (להוציא את אסון המסוקים).

השאלות העיקריות שנדונו בצבא היו, האם אפשר לנהל את הלחימה בחזבאללה באופן שונה, והאם המצב הקיים נסבל. הדעה בצבא הייתה, שהמצב השורר הוא בגדר הנסבל, ואפשר להמשיך כך לאורך זמן. לא התקיים למעשה שום עיסוק יסודי ואמיתי בשאלה מה הן החלופות העומדות לרשות מדינת ישראל.

משה ארנס – שהיה שר הביטחון תקופה קצרה לפני שנת 1999 – ניסה להציג גישה אחרת, שלפיה כל עוד ישראל מצויה בהתמודדות עם חזבאללה, האפקטיביות שלה מוגבלת, ולכן לא בהכרח חזבאללה הוא היריב שנכון להתמודד איתו, היריב האחר אינו סוריה בהכרח. עימות ישיר עם סוריה טומן בחובו סיכונים גדולים יותר לישראל. לדברי ארנס, נכון היה להטיל אחריות על ממשלת לבנון, שעל אף חולשתה מחויבת באחריות מדינתית מלאה. לדעת ארנס, היה נכון להתמיד בתקיפת תשתיות בלבנון.

אלוף (מיל.) גיורא אילנד הנו חוקר במכון למחקרי בטחון לאומי.
מאמר זה מבוסס על הרצאה שנשא המחבר בכנס "10 שנים לנסיגה מלבנון", שהתקיים ב־28 ביוני 2010.

נראה שגישה זו לא מיצתה את עצמה לאורך זמן בגלל שינויים פוליטיים בישראל. בשנת 1999, כשנבחר אהוד ברק לראש הממשלה ולקח לעצמו גם את תפקיד שר הביטחון (קיץ 1999), הוא הכריז את הכרזתו המפורסמת: עד 1 ביולי 2000 ייצא צה"ל מלבנון, עם הסכם או בלעדיו.

אמירה זו לא מצאה חן בעיני ראשי הצבא; ההכנות בצבא ליציאה מלבנון התמהמהו מאוד, בעיקר משום שהיה הליך מדיני של משא ומתן עם סוריה, שהיה אינטנסיבי מאוד בסוף שנת 1999 ובתחילת 2000. הייתה הרגשה שאפשר להגיע להסכם עם סוריה. הצבא היה מעורב באופן ישיר במשא ומתן עם סוריה, והרושם היה כי משעה שהסכימה ישראל לרדת מרמת הגולן, אפשר להגיע להסכם; ואם אפשר להגיע להסכם, היה ברור שהוא כולל את לבנון, ולכן אין למהר לנקוט פעולות כלשהן.

השינוי הדרמטי קרה בתחילת מארס 2000. לאחר פגישת קלינטון־אסד היה ברור שאין הסכם. ברק דבק בהבטחתו, והיה ברור שהיציאה מלבנון תהיה חד־צדדית ובלי הסכם. נותרו ארבעה חודשים לכל היותר להכנות, והייתה מודעות לצורך ליצור הפתעות טקטיות כלשהן.

כשהחלו ההכנות לקראת היציאה מלבנון התגלע עוד ויכוח נוקב בין הצבא, הרמטכ"ל שאול מופז, לבין ראש הממשלה ושר הביטחון בשאלה מה היא יציאה חד־צדדית. ראיית הצבא את היציאה החד־צדדית הייתה שונה מאוד מראייתו של ראש הממשלה. הצבא הבין – או רצה להבין – שהיציאה החד־צדדית היא יציאה טקטית שמשמעה: קשה לנו להחזיק את אזור הביטחון מבחינת האפקטיביות של הלחימה, ויש לנו נפגעים רבים, והשהייה בלבנון במתכונתה כפי שהייתה נהוגה אז משמעותה הייתה שאנו בעיקר משמשים מטרות. לפיכך יש לסגת לקו טקטי אחר במרחק קילומטר אחד מהגדר. האמירות שהשמיע הצבא היו בנוסח: "לא יעלה על הדעת שנעזוב אזורים כמו רכס חממיס מעל מטולה או מקומות אחרים השולטים על היישובים שלנו". לפי ראיית הצבא, תהיה נסיגה לקו הטקטי האמור (מה שגם כונה "קיצור קווים*), אבל מבחינה אסטרטגית הכול יהיה אותו הדבר: צה"ל ימשיך לתמוך בצד"ל ככל האפשר; ברור שצה"ל ימשיך לתקוף בלבנון וימשיך לפעול מעבר לקו החדש. השינוי יבוא לביטוי, כאמור, בהיערכות טקטית אחרת.

ראש הממשלה ושר הביטחון הבין כי הנסיגה הטקטית הזאת לא תשנה דבר, ובמידה מסוימת היא תהיה דומה לנסיגה הטקטית הקודמת, בשנת 1985, לאותו אזור ביטחון. לדבריו, מדובר ברעיון אסטרטגי לסגת לקו הבינלאומי, לקבל לגיטימציה – לא מלבנון ומסוריה, כי מהן לא נקבל – ממדינות חשובות בעולם. הלגיטימציה היא שתביא בסופו של דבר לידי מציאות ביטחונית טובה יותר.

ההליכים המדיניים אכן נעשו בזמן קצר. אחד מהם היה להגיע לקו גבול מוסכם בין ישראל לבין לבנון. היה קו ייחוס לגבול בקטע שמהים עד ה־חצבני, שהתבסס

על הסכם סייקס־פיקו משנת 1916, קו גבול שנעשה רשמי ומוכר בשנת 1923. משמע, היה קו גבול, והיו צריכים לשחזר אותו.

מאזור החצבני ומזרחה לא היה מעולם קו גבול בין ישראל לבין לבנון. אם חוזרים לתקופת המנדט הצרפתי והמנדט הבריטי, הרי גם סוריה וגם לבנון היו חלק מהמנדט הצרפתי ולא היה גבול ביניהן, ולכן אין בסיס בינלאומי קודם לקו גבול בין ישראל ללבנון בקטע המזרחי (אזור רמת הגולן־הר דב).

לא הייתה אפשרות להידבר עם ממשלת לבנון, ולכן היה צורך לסגת לקו שהאו"ם יכיר בו כגבול הבינלאומי. השאלה הייתה איך ליצור את הקו הזה ולהביא לכך שיזכה לתמיכה בינלאומית? מי שהיה אז ראש מחלקת המיפוי בצה"ל, אלוף משנה חיים סרברו, מצא מפה של האו"ם משנת 1974 המגדירה את המנדט של כוח האו"ם ברמת הגולן (לאחר מלחמת 1973 הסכימו ישראל וסוריה על הפרדת כוחות, וניתן מנדט לכוח או"ם לפקח עליו. המנדט הזה הגדיר את גבולות האחריות של הכוח הזה, הכוללים את רמת הגולן). לפיכך רמת הגולן היא השטח שנכלל במפה, ולצורך העניין האמור כל שטח שאינו מצוי במפה אינו נכלל ברמת הגולן, דהיינו אם שטח כזה הוא בצפון, אזי הוא בתחום לבנון.

היות שהקו הזה, שתחם את רמת הגולן, השאיר בשטח ישראל את הרכס החשוב של הר דב, הקרוי בפי הלבנונים חוות שבעא, ובכלל זה בסיסי המודיעין החשובים הנמצאים עליו, הרי שמבחינת ישראל הקו הזה היה קו טוב. היות שהקו התבסס על מפת או"ם, טענה ישראל שמפה זו מגדירה בעצם את קו הגבול לאורך אזור הר דב. האו"ם אכן קיבל את הקו הזה. המחיר הבולט של הכרה זו מבחינת ישראל הוא הכפר ע'ג'ר, שקו הגבול הזה חותך אותו לשני חלקים.

הצבא נערך לקראת 1 ביולי 2000, מתוך כוונה לנצל את הזמן ליציאה מסודרת ככל האפשר. בכנס (עשור לנסיגה מלבנון) תואר, תהליך שנחשב לתחילת התמוטטותו של צד"ל, בעיקר בגזרה המערבית. הצבא לא צפה את התהלוכות האזרחיות שהתרחשו סמוך לנסיגה ואת משמעותן. ב־21 במאי 2000 ביקר הרמטכ"ל בפיקוד צפון בתרגיל גיס. כשהחלו להגיע הידיעות על התהלוכות. זו הייתה הפתעה. יום לאחר מכן, כשהתהלוכות האזרחיות התעצמו התקיימה פגישה מתוחה במוצב זרעית בה נכחו ראש הממשלה ושר הביטחון, הרמטכ"ל, אלוף פיקוד הצפון ואלופים נוספים מהמטה הכללי. נשאלה השאלה מה עושים עכשיו בשעה שצד"ל התחיל להתמוטט. היו אז שתי אפשרויות: האחת לשלוח אוגדה או שתי אוגדות של צה"ל במקום צד"ל כדי להחזיק את אותו הקו ולהילחם עליו. השאלה הייתה אם נכון להילחם על קו שחודש אחר־כך עתידים לצאת ממנו. האפשרות האחרת הייתה להתאים את עצמנו למצב שמתהווה ולהקדים את יציאת צה"ל מלבנון.

ההחלטה לא הייתה פשוטה כלל במעמד ההוא במוצב בפיקוד הצפון. מה שעזר לראש הממשלה להחליט שצה"ל ייצא מיד היה קשור לא רק למציאות הצבאית כפי שתוארה, אלא לצירוף מקרים של אירוע מדיני. באותו הבוקר התקיים דיון באו"ם, שסיכומו היה אישור למזכיר הכללי של האו"ם לסכם עם ישראל את נושא היציאה מלבנון ואת נושא קו הגבול הבינלאומי. משמעות הדבר הייתה, שראש הממשלה ושר הביטחון יכול להסתמך על החלטת האו"ם, המאפשרת לישראל לעשות את מה שבעצם התכוונה לעשות. כך חברו התנאים המדיניים אל המצב הצבאי. אכן היציאה הזאת מלבנון נעשתה בחיפזון רב, אבל יש לזכור שגם חזבאללה הופתע. העובדה שהיציאה נעשתה בלילה אחד הקשתה על חזבאללה לפגע בכוחות היוצאים. מכאן לשני האירועים המאוחרים יותר – בשנת 2005 ו־2006.

בשנת 2005 נוצר מצב, מסיבות שלא היו קשורות ישירות לישראל, שבכל העולם זעמו על סוריה, בעיקר לאחר רצח רפיק אל־חרירי. נוצרה קואליציה רחבה – ובכלל זה סעודיה, האו"ם, צרפת וארצות הברית – שהאשימה בכך את שלטון סוריה בלבנון, ולכן שליטי סוריה חייבים להוציא את צבאם מלבנון.

ישראל הייתה שותפה סמויה למהלך של יציאת סוריה מלבנון ותמכה בו בהתלהבות לאחר ויכוח פנימי שהתקיים במערכות הממשל בישראל שבמרכזו השאלה: האם יציאת סוריה מלבנון טובה לישראל. היו מי שחשבו (כולל כותב שורות אלה) שהמהלך הזה אינו רצוי לישראל. באופן מוזר, לישראל ולסוריה היה עניין בהימצאות הסורים בלבנון, וזה משלוש סיבות: (א) הסורים בלבנון הם כתובת מרסנת, והם התנאי לכך שאם תגיע ישראל להסכם עם סוריה, יכלול ההסכם גם את לבנון, וסוריה לא תוכל להתחמק מאחריות; (ב) לא ברור כלל אם יתחזקו הכוחות המתונים הדמוקרטיים אם סוריה תֵצא מלבנון, וייתכן שיתחזקו כוחות אחרים, כפי שאכן קרה, וחזבאללה ואיראן תפסו את מקומה של סוריה; (ג) ברגע שסוריה מוותרת כביכול על לבנון, מוקד העניין שלה יהיה רמת הגולן, ומי שחשב שאין לקיים עם סוריה משא ומתן על רמת הגולן, סבר כי עדיף שסוריה תיאבק על אחיזתה בלבנון ולא תתמקד במאבק על הגולן.

יציאת הסורים מלבנון גרמה לאנשים בישראל לחשוב, שאולי, באיחור של חמש שנים, תקטוף ישראל, בעקיפין לפחות, את הפֵּרות של היציאה מלבנון בשנת 2000 – צה"ל כבר אינו בלבנון, את הסורים שונאים, הסורים יוצאים מלבנון, ולבנון תהיה מדינה דמוקרטית, פרו־מערבית. כידוע, התקווה נגוזה במהירות. חזבאללה בעצם תפס את מקומה של סוריה, והמציאות בלבנון, מהבחינה הזאת, ודאי טובה פחות משחשבו שתהיה.

משנת 2000 עד 2006, כמו בנוגע לדברים רבים אחרים, לא התקיים דיון כלשהו בממשלת ישראל בשאלת המדיניות הנכונה ללבנון. המדיניות נקבעה דה־פקטו, בעיקר בידי הצבא. משמע, גם אם פעם בחודשיים־שלושה מתרחש אירוע טקטי,

מנסים לצאת מממנו בדרך המיטבית האפשרית, ולא מסלימים בעקבות האירוע מעבר למינימום הנדרש – "מדיניות הכלה", ואפילו הבלגה.

אי־קיומו של דיון אסטרטגי על לבנון אופייני לישראל. בדרך כלל כשהמצב רגוע כביכול, ואינו דורש החלטות, לא יוצרים חלופות מדיניות־אסטרטגיות משום שלא חייבים; כשמתרחש אירוע נקלעים למציאות המחייבת להגיב מהר.

והנה בשנת 2006 ניתנו בידי ישראל כל הכלים להעמיד את העימות במישור מדינתי. חזבאללה אינו עוד רק ארגון, הוא חלק מהפרלמנט, הוא חלק מהשלטון בלבנון, הוא חלק מהממשלה, ולכן ישראל צריכה לראות בממשלת לבנון אחראית לאש הנורית משטחה ויכולה להגיב בהתאם. זו ההחמצה הגדולה של מלחמת לבנון השנייה – ישראל הגדירה את האויב באמצעות הגדרה מצמצמת מדי. אילו מלכתחילה הייתה ישראל רואה בלבנון את האויב ולא רק בחזבאללה, הייתה אפשרות שהמלחמה הזאת הייתה קצרה בהרבה, וההרתעה שהייתה מושגת בסופה גם הייתה מוצלחת בהרבה מכפי שהיא היום.

אם חוזרים להחלטה של שנת 2000, לדעתי נכשלה ישראל בשנות התשעים בכך שבשום שלב לא ניסתה לפתח חלופה אמיתית, זולת שתי החלופות שלכאורה היו בנמצא: (1) להישאר במצב הקיים; (2) לסגת נסיגה חד־צדדית. גם בעניין ההינתקות מעזה הצטמצם הדיון הציבורי לשתי אפשרויות: האם אתה בעד ההינתקות או נגדה. האם זה היה כל מרחב האפשרויות? התשובות קשורות לעיתוי העלאת השאלה.

בשנות התשעים לא מיצתה ישאל את כל מרחב האפשרויות, וייתכן בהחלט שהיה בידי ישראל ליצור מציאות אחרת. נרמז כאן על צעדים בכיוון מסוים שניסה משה ארנס לקדם, אבל כאמור, מרחב הזמן במקרה שלו היה מצומצם מאוד עקב הבחירות.

אם מסכימים שהיו רק שתי אפשרויות – להישאר במצב שהיה אז או לצאת מלבנון, נראה שראש הממשלה ושר הביטחון אהוד ברק החליט החלטה אמיצה ונכונה. אני אומר זאת נוכח היותי אז אלוף במטה הכללי, שכמו רוב עמיתיו התנגד ליציאה חד־צדדית. אולי השיח הזה התנהל בקול רם מדי וגם בקול אחיד – ואכן מן הראוי לבחון כיצד נוצרת דינמיקה כזאת בתוך מטה כללי.

על אף כל הבעיות, בפרספקטיבה של עשר שנים נראה שההחלטה לצאת מלבנון הייתה החלטה נכונה. כאמור, ההחמצה הגדולה היא שבשנת 2006 לא ידעה ישראל למנף באופן מוצלח יותר את הלגיטימציה שניתנה לה שש שנים לפני כן.

No. 98, April 2009, Anat N. Kurz, *The Palestinian Uprisings: War with Israel, War at Home*.

No. 97, March 2009, Shmuel Even and Amos Granit, *The Israeli Intelligence Community: Where To?* [Hebrew].

No. 96, September 2008, Ron Tira, *The Struggle over the Nature of War* [Hebrew].

No. 95, August 2008, Anat N. Kurz, *The Palestinian Uprisings: Struggle on Two Fronts* [Hebrew].

No. 94, July 2008, Ephraim Kam, ed., *A Nuclear Iran: Implications for Arms Control, Deterrence, and Defense*.

No. 93, April 2008, Shmuel Even and Zvia Gross, *Proposed Legislation on the IDF: Regulating Civil-Military Relations in the Wake of the Second Lebanon War* [Hebrew].

No. 92, December 2007, Dani Berkovich, *Can the Hydra be Beheaded? The Campaign to Weaken Hizbollah* [Hebrew].

No. 91, July 2007, Benny Landa and Shmuel Even, *The Israeli Economy in the Age of Globalization: Strategic Implications* [Hebrew].

No. 90, May 2007, Yehuda Ben Meir and Dafna Shaked, *The People Speak: Israeli Public Opinion on National Security 2005-2007*.

No. 89, March 2007, Ron Tira, *The Limitations of Standoff Firepower-Based Operations: On Standoff Warfare, Maneuver, and Decision* [English and Hebrew].

No. 88, February 2007, Ephraim Kam, *A Nuclear Iran: What Does it Mean, and What Can be Done*.

No. 87, January 2007, Ephraim Kam, A Nuclear Iran: Analysis and Implications [Hebrew].

Memoranda 2007 — Present

No. 110, November 2011, Meir Elran, Owen Alterman, and Johannah Cornblatt, Eds., *The Making of National Security Policy: Security Challenges of the 21st Century— Conference Proceedings.*

No. 109, June 2011, Shmuel Even and David Siman-Tov, *Cyber Warfare: Concepts, Trends, and Implications for Israel* [Hebrew].

No. 108, May 2011, Emily B. Landau and Tamar Malz-Ginzburg, eds., *The Obama Vision and Nuclear Disarmament* [Hebrew].

No. 107, March 2011, Emily B. Landau and Tamar Malz-Ginzburg, eds., *The Obama Vision and Nuclear Disarmament*.

No. 106, November 2010, Yehuda Ben Meir and Olena Bagno-Moldavsky, *Vox Populi: Trends in Israeli Public Opinion on National Security 2004-2009*.

No. 105, August 2010, Meir Elran and Yoel Guzansky, eds., *Vision and Reality in the Middle East: Security Challenges of the 21st Century — Conference Proceedings*.

No. 104, June 2010, Gallia Lindenstrauss, *Mediation and Engagement: A New Paradigm for Turkish Foreign Policy and its Implications for Israel* [Hebrew].

No. 103, May 2010, Tamar Malz-Ginzburg and Moty Cristal, eds., *A Nuclear Iran: Confronting the Challenge on the International Arena* [Hebrew].

No. 102, December 2009, Michael Milstein, *Muqawama: The Challenge of Resistance to Israel's National Security Concept* [Hebrew].

No. 101, November 2009, Meir Elran and Judith Rosen, eds. *The US and Israel under Changing Political Circumstances: Security Challenges of the 21st Century — Conference Proceedings*.

No. 100, September 2009, Aron Shai, *Sino-Israeli Relations: Current Reality and Future Prospects*.

No. 99, June 2009, Meir Elran, ed., *The Civil Front* [Hebrew].