מה ניתן ללמוד מהמלחמה באוקראינה על מקומו הנכון של הסייבר ההתקפי (CNA) במארג היכולות של צה״ל, במלחמה רחבת היקף - תא״ל (מיל׳) ד״ר פינקל

תא״ל (מיל׳) ד״ר מאיר פינקל הוא ראש תחום מחקר במרכז דדו.

פורסם לראשונה ביולי 2022.

תקציר

לצבאות, בעיקר מערביים, יש נטייה ל״הקסמות״ מטכנולוגיה צבאית עולה שאמורה לשנות את מאפייני הלחימה ולעיתים יש הטוענים שגם את טבעה. תחום הסייבר הוא ללא ספק תחום שהביא ל״הקסמות״ כזו, בין היתר כי הפעולות בתחום זה חשאיות וחסויות, מה שמקשה על הצופה הביקורתי לבקרם. החשיבה בצה״ל לגבי השילוב של סייבר התקפי במלחמה עדיין לא מפותחת, והמלחמה באוקראינה מהווה הזדמנות טובה לדבר עליה. מלחמת רוסיה־אוקראינה מספקת הזדמנות למידה באשר לעוצמתם היחסית של מרכיבים שונים, ישנים וחדשים, שחלקם נתפסים כמשנים את פני תופעת המלחמה. למידה זו תאפשר לצה״ל, בראיה עתידית, ״לנרמל״ את מקומם של כל המלחמה החדשים בתרחיש של מלחמה כוללת.

מבוא – איך צבאות לומדים על עוצמתן של יכולות מתפתחות?

רעיונות ויכולות חדשות מתפתחות בתקופות שבין מלחמות והוגי דעות ופרקטיקנים מנסים לשער את מידת השפעתם במלחמה עתידית, כדי להשפיע על תקצוב הפיתוח של יכולות כאלה, הדומיננטיות שלהם בתוך תפיסות ההפעלה וכדומה. נראה כי הדוגמה המוכרת ביותר לגבי הניסיון לחזות את תפקידה העתידי של יכולת מתפתחת בשדה הקרב העתידי היא זו של ג׳וליו דואה, שצפה בשנות ה־20 של המאה ה־20 כי ההפצצה האסטרטגית תייתר את הצורך בצבאות. במלחמת העולם השנייה, בה נעשה שימוש מאסיבי בהפצצה אסטרטגית באירופה, ללא הכרעת גרמניה או בריטניה, קיבלה ההפצצה האסטרטגית את הפרופורציה הנכונה בתוך מכלול הכלים הצבאיים.

לעיתים, היכולות הללו נבחנות בעימותים קטנים או בפעולות בטחון שוטף, והניסיון הזה מנותח דרך המשקפיים של עימות רחב היקף כדי לשפר את יכולת החיזוי המדוברת. דוגמה מוכרת היא ההתנסות הגרמנית בהפעלת שיריון במלחמת האזרחים בספרד לפני מלחמת העולם השנייה.

ישנן גם תקופות בהן צבאות שקועים בלחימה מתמשכת מסוג מסוים, בה יש דומיננטיות של מרכיבים מסוימים, ונטייה להניח שהעימות הנוכחי הוא ״המלחמה״ ולא יהיו עוד ״מלחמות גדולות״. הלך רוח זה מביא להדגשה הולכת וגדלה של מרכיבים מסוימים על חשבון אחרים. צה״ל של תחילת שנות ה־2000, למשל, לחם בהצלחה באופן אינטנסיבי באיו״ש תוך דומיננטיות של לחימת חי״ר על גווניה השונים. במקביל בוטל תו״ל ההשתתפות של מטוסי קרב בלוחמת היבשה ובניין הכוח הוטה ללוחמה בטרור (פינקל, 2018, עמ׳ 44־48). במלחמת לבנון השנייה התברר כי זו היתה שגיאה.

מוכרת גם הנטייה בצבאות, בעיקר מערביים, ל״הקסמות״ מטכנולוגיה צבאית עולה שאמורה לשנות את מאפייני הלחימה ולעיתים יש הטוענים שגם את טבעה. רעיונותיו של דואה כבר הוזכרו, ומקרה חדש יותר הוא ה״מהפכה בעניינים צבאיים״ (RMA) שנביאיה טענו כי תהפוך את הלחימה לפעולה מנגד, באמצעות מודיעין ואש מנגד. אך היריבים של צבאות אלו, ובכלל זה גם יריביה של ישראל, נטרלו אפקטיביות פוטנציאלית זו באמצעות פעולות שונות.

לרוב, עליית טכנולוגיה מהסוג המדובר מייתרת, לכאורה, יכולות ותיקות. גם כאן, הניסיון צבאי בפועל מסייע ״לנרמל״ את האפקטיביות את טכנולוגיות שיוחסה להן השפעה גדולה על מעשה המלחמה. תחום הסייבר הוא ללא ספק תחום שהביא ל״הקסמות״ כזו, המצויה כנראה לקראת

שיאה, בין היתר כי הפעולות בתחום זה חשאיות וחסויות, מה שמקשה על הצופה הביקורתי לבקרם.
יש לציין כי בשנת 2015 הצהיר הרמטכ"ל איזנקוט על הקמת זרוע סייבר בפיקוד אלוף (אסטרטגיית צה"ל, 2015, עמ' 30) שתהיה אחראית על המרכיבים ההגנתיים וההתקפיים, על בניין הכוח ועל הפעלתו. יש בכך כדי להעיד על החשיבות הרבה שיוחסה לתחום העולה באותה עת ואולי גם ל"הקסמות" ממנו. תחליה מונה רמ"ט לתחום הסייבר תחת סגן הרמטכ"ל ובסופו של תהליך לא הוקמה זרוע עצמאית והתחום בוזר בין אגף התקשוב שהפך לאגף התקשוב וההגנה בסייבר לבין אמ"ן ליחידה 8200 בו הוקמה מחלקת התקפה בסייבר.
כבר יותר מעשור שצה"ל נלחם במב"ם באמצעים שונים ובמערכות שונות, ומפעיל סייבר לצרכי השגת מודיעין ולצרכי השפעה (תודעה), כאשר מול איראן נראה כי על פי פרסומים זרים מרכיב מרכזי הוא סייבר התקפי (לפירוט ההבדלים בין סוגי הסייבר ראה מטה). הסייבר ההתקפי הוא תחום עולה בכל העולם ומרכיב חשוב בעימותים ש"מתחת לסף מלחמה", הקרויים בלעז Gray Zone Warfare. יש כאלה הטוענים כי זו היא המלחמה עצמה, ולא המערכה בין המלחמות (סא"ל רועי, 2021, עמ' 36-37). גם אלה שחושבים כי יכולה להיות מלחמה, טוענים כי הפעולות במב"ם הקינטי, מחדדות ומשפרות את יכולת אמ"ן וחיל האוויר לקראת מלחמה. אחרים טוענים כי המב"ם מבלבל את צה"ל וכי הוא נשען בפועל על "מקל גדול" שבלעדיו, אין למב"ם היתכנות (אורטל, 2021, עמ' 90-91). החשיבה בצה"ל לגבי השילוב של סייבר התקפי במלחמה עדיין לא מפותחת, והמלחמה באוקראינה מהווה הזדמנות טובה לדבר עליה.
מלחמת רוסיה־אוקראינה היא המקרה הקרוב ביותר למלחמה מהדפוס ה"קלאסי" של פעולת כיבוש שטח והשמדת אויב, תוך הפעלת כלל האמצעים שיש בידי היריבים. גם אם לא החלה כמבצע הכרעתי, מספקת הזדמנות למידה באשר לעוצמתם היחסית של מרכיבים שונים, ישנים וחדשים, שחלקם נתפסים כמשנים את פני תופעת המלחמה. למידה זו תאפשר לצה"ל, בראיה עתידית, "לנרמל" את מקומם של החדשים בתרחיש של מלחמה כוללת.
המיקוד כאן יהיה בסייבר התקפי. תחום זה של פעולה בסייבר עוסק בפגיעה במערכות כדי להוציאן מתפקוד (CNA-Cyber Network Attack). התקפה בסייבר יכולה לבוא לידי ביטוי בשיתוק או שיבוש יכולת תקשורת של צבאות, ויכולה להיות לה גם תוצא של פגיעה פיזית במערכות עקב השתלטות עליהן מרחוק ושיבוש פעולתן. לא אעסוק כאן בסייבר ככלי להשגת מידע מודיעיני – גניבת מידע בסייבר (CNE) ובסייבר לצרכי השפעה (CNI). הסיבה לכך היא ששניהם הם כלים מוכרים לצה"ל והוא מפעיל אותם כבר שנים בהכנות למלחמה ובמב"ם.

השילוב של סייבר התקפי נגד מטרות צבאיות ומטרות תשתית לאומית במלחמה באוקראינה

מה חשבו המומחים שיעשו הרוסים בתחום הסייבר ההתקפי באוקראינה? נראה שהציפיות התבססו על פעולות רוסיות בשנים האחרונות. המלחמה בגיאורגיה ב־2008 היתה כנראה השילוב הראשון של התקפת סייבר עם הפעלת תמרון ואש. בפתיחת העימות הרוסים תקפו בסייבר אתרים ממשלתיים, בנקים ואתרי חדשות. נראה שהעניין הקשה על הממשלה הגיאורגית להגיב ולהתארגן, אם כי הפגיעה בכוחות הצבאיים היתה מוגבלת ולא היתה לכך השפעה משמעותית על תוצאות הלחימה (White, 2018). ב־2015 תקפו הרוסים והשביתו חלק ניכר מאתרי האנרגיה באוקראינה וב־2017 תולעת סייבר בשם NotPetya מחקה ושיבשה תוכנות הפעלה במחשבים רבים באוקראינה, בחברות אזרחיות וגופי ממשל. כל אלה, היוו רפרנס ליכולת הרוסית, ומומחים ציפו שהמלחמה תמחיש יכולות אלה, כבר מתחילתה.
מה קרה במלחמה באוקראינה? בתחילת העימות ולפני הפלישה הרוסית היו עדויות להתקפות סייבר רוסיות על שרתים של משרד ההגנה האוקראיני, בנקים, ספקי אינטרנט אזרחיים ועוד. מרגע שהחלה הפלישה, הכלים המרכזיים בתחום הסייבר ההתקפי אשר הופעלו על ידי הרוסים הם אש ול"א להשגת עליונות אווירית, תמרון יבשתי לכיבוש שטח בדרום וליצירת איום על הבירה בצפון, ובהמשך הפעלת אש לדיכוי התנגדות צבאית ולהטלת טרור על האוכלוסייה.
הסייבר ההתקפי נראה ככלי מוגבל בהיקפו במלחמה הנוכחית – היה שימוש ב־DDOS ובנוזקה שמחקה מידע משרתים – אך תקיפות אלה ככה"נ לא השפיעו משמעותית על תשתיות צבאיות ומערכות ממשלתיות קריטיות, כמו ייצור חשמל. יש מחלוקת בקרב הפרשנים על הסיבות לכך. חלק מהפרשנים טוענים, כי הבעיה היא שהכלים שהרוסים הכינו להתקפה משמעותית אינם ממוקדים דיים וכי הרוסים חוששים מהנזק האגבי שיזלוג למדינות נאט"ו, ומהסלמה בלתי רצויה מול נאט"ו

(Willett, 2022). פרשנים אחרים טוענים, כי הסיבה אינה העדר פעולה רוסית, אלא דווקא חיזוק ההגנות האוקראיניות על ידי ארה״ב, לאחר התקפות רוסיות שמהן הפיקו האוקראינים לקחים (Cristal, 2022; Rohozinski, 2022).

פרשנות נוספת אפשרית הינה, כי יתכן שעקב אופי המערכה, שהחלה בניסיון עריפת ההנהגה הפוליטית, הרוסים נזהרו בהפעלת כלים שיזיקו גם לאוכלוסייה. מנגד, יש פרשנים הטוענים, כי תקיפות חסויות של מדינות המערב על מערכות התקשורת הרוסיות פגעו באפקטיביות מאמצי הסייבר הרוסיים (Rohozinski, 2022). יש גם טענות לפיהן לרוסים יש כלי סייבר התקפי משמעותיים שעדיין לא הופעלו כיוון שהם נועדו למקרה של מלחמה מול נאט״ו, והרוסים לא מעוניינים לחשוף אותם. בניגוד לפרשנויות אלו, שני מומחי לתחום במטה נאט״ו בבריסל – העוזר לענייני סייבר לראש המודיעין של נאט״ו והאנליסט הבכיר לניתוח איום הסייבר בנאט״ו – אף פרסמו מאמר בכתב העת היוקרתי Foreign affairs לפיו בניגוד לקונצנזוס המחקרי הקיים, רוסיה הפעילה מאז תחילת הלחימה פעולות סייבר רבות, מסונכרנות ואפקטיביות שהיו בעלות תרומה רבה למאמץ המלחמתי הרוסי (Cattler and Black, 2022). בהקשר זה, יש לציין גם ניתוחים לפיהם תקיפות סייבר רוסיות של מערכות השליטה ברכבות בוצעו כ״ריכוך״ לפני תקיפה קינטית של תשתיות שינוע באמצעות רכבות (McLaughlin, 2022).

לסיכום חלק זה, ניכר כי בשלב זה של המלחמה עדיין קיימת חוסר בהירות לגבי מקום הסייבר ההתקפי הרוסי במאמצי הלחימה הרוסיים. כמו כן, קיימות מחלוקות מחקריות בתחום, הגם שנראה שמרבית הפרשנים מצביעים על כך שלסייבר ההתקפי הרוסי הייתה תרומה מוגבלת למאמצי הלחימה הרוסים, בוודאי ביחס לציפיות המוקדמות. בכל מקרה, לצורך מאמר זה, השילוב של סייבר התקפי עם תמרון ואש במלחמה, מאפשר פיתוח החשיבה הצבאית בישראל בעניין זה.

סייבר התקפי כחלק ממארג יכולות צה״לי במלחמה – היכן יתרונותיו וחסרונותיו

השאלה החשובה לצרכי בניין הכוח ופיתוח תוכניות המלחמה של צה״ל, תחת עיקרון של לחימה משולבת ומשותפת, שהסייבר ההתקפי משתלב לתוכה, היא היכן יתרונותיו המרכזיים בעימות רחב היקף. הסייבר הוא כלי מצוין למערכות מתחת לסף המלחמה, שכן הוא מאפשר פעולה במרחב ההכחשה, אך מה קורה כאשר אין צורך להכחיש? ניתן לזהות כאן כמה יתרונות וחסרונות, בראיה של מלחמה עתידית מול החזבאללה בלבנון או מול חמאס בעזה ובמלחמה במעגל שלישי מול איראן.

היתרון הראשון – והוא נכון הן למעגל ראשון והן למעגל שלישי – הוא בהפעלת סייבר התקפי במהלומה בפתיחת מלחמה כאשר ניתן להפתיע, כדי לשבש מערכות מסוגים שונים, בין אם מערכות תקשורת ונתונים, ובין אם מערכות פיזיות בעלות ערך גבוה לאויב. פעולה כזו היא בעלת אופי מערכתי, ונועדה ״לעצב״ את שדה הקרב כדי להקל על הפעולות בדרג הטקטי. ניתן לשער שמרגע שהמלחמה מתפתחת, האויב יצליח למזער סיכונים, בדומה לאופן שבו יפעל ביחס לפעולה אווירית (פיזור יכולות, מעבר לאתרי חירום סודיים וכדומה) ובהקשרי נגישות מודיעינית (מעבר למערכות חירום, הפסקת תעבורת תקשורת וכדומה). יש לזכור כי במקרים רבים הלחימה מתפתחת כהסלמה איטית, ולכן לא רצוי לבסס מרכיב משמעותי מהתפיסה בכלל ובתוכה מרכיב הסייבר ההתקפי, על תרחיש שבו תתאפשר מתקפת פתע ישראלית.

היתרון השני של סייבר התקפי במלחמה רחבת היקף הוא יכולת תקיפה של מערכות שמיקומן הפיזי אינו ידוע ולכן לא ניתן לתקפן קינטית, או שמיקומן ידוע וישנן מגבלות בתקיפה קינטית עקב נז״א או מגבלות אחרות. הסייבר ההתקפי מאפשר לחדור מערכים פיזיים של הסוואה, הגנה, וההסתתרות מאחורי האוכלוסייה. במלחמה עתידית, פגיעה קינטית במערכת הספקת חשמל בלבנון שהיא מערכת אזרחית־צבאית יכולה להביא לגינוי של ישראל בעולם. לעומת זאת, השבתה באמצעות פעולה בסייבר, תהיה כנראה לגיטימית.

יתרון שלישי של סייבר התקפי במלחמה הוא ב״אמנעת״ פעילות אויב. שיבוש פעולה של מערכות הגנה לסוגיהן כמו טק״א וטח״י, שיבוש יכולת הפעלת כטמ״מים וכדומה. גם כאן רצוי שהפעולה ההתקפית בסייבר תהיה בעל השפעה מערכתית על שדה הקרב, שתקל על צה״ל בהתנגשויות בדרג הטקטי.

החיסרון המרכזי של פעולות סייבר התקפיות הוא מחירן המשאבי. לכן, כל מטרה שניתן בעת מלחמה במעגל ראשון לתקוף קינטית, לא רצוי להשקיע בה משאבים לתקיפה בסייבר. תהיה זו כפילות ובזבוז של משאבים. דוגמה מהמלחמה באוקראינה – תקיפה פיזית של מגדל התקשורת בקייב זולה הרבה יותר מאשר הכנת כלי סייבר התקפיים לעניין זה. לעומת זאת, במעגל שלישי,

יתכן שהעניין הפוך – תקיפה בסייבר תהייה זולה יותר ועם פחות סיכונים מאשר תקיפה אווירית, אם כי גם כאן, עלות בניית ושימור יכולת תקיפה משמעותית בסייבר היא גבוהה מאוד.

סיכום: מה יכול צה"ל ללמוד מהמלחמה לגבי פיתוח יכולותיו ותוכניותיו בתחום הסייבר ההתקפי

הסייבר ההתקפי הולך ותופס מרכזיות בחשיבה הצבאית הישראלית, בעיקר בהקשרי מעגל שלישי במסגרת המב"ם, אך גם במעגל ראשון. החשיבה הצבאית הישראלית מוטה כבר כמה עשורים למענה צבאי מוכוון טכנולוגיה, ואופייה של הפעולה בסייבר, הופכת תחום זה למועד עוד יותר ל"הקסמות". אך מתוך הבנה, שרצוי לרעננה, שתרחיש הייחוס המרכזי הוא מלחמה, ולא מבצעים מוגבלים בעזה ומב"ם, יש ללמוד מהמלחמה באוקראינה מה יכול להיות מקומו היחסי בתרחיש כזה.

בהכללה, נראה כי במקרה של מלחמה עם חזבאללה וחמאס, כאשר תופעל אש ישראלית מאסיבית ואולי גם תמרון יבשתי, יש סיבה להאמין שמרכיב הסייבר ההתקפי יהיה מצומצם. החזבאללה אינו מדינת לבנון, ופגיעה במערכות דואליות (צבאיות ומדינתיות־אזרחיות) בהן חזבאללה עושה שימוש כמוה כתקיפה קינטית של מטרות כאלה, עם המגבלות הכרוכות בכך. רצוי למקד את היכולות בתחום זה בתחומים שאינם רגישים לעיתוי כמו מתקפת פתע, ובתחומים שהם השלמה הכרחית, אך לא גיבוי, לתקיפה קינטית שהיא זולה הרבה יותר.

לצורך ההמחשה, יתכן ורצוי להקביל את הסייבר ההתקפי לתחום היחידות המיוחדות/ייעודיות. אחרי כל מלחמה מתברר כי תרומתן קטנה ביחס להשקעה בהן, גם אם חשיבותן בשגרה גדולה. כך לאחר מלחמת יום הכיפורים, למשל, הוחלט לפרק את סיירת שקד שפעלה היטב במלחמת ההתשה בתעלת סואץ אך לא התאימה לתרחיש מלחמה. בהתאמה גם לפעולה המערכתית של הכוחות המיוחדים (סיירת מטכ"ל ויחידת שלדג) בבעל־בק במלחמת לבנון השנייה היתה השפעה מוגבלת בלבד על תוצאות המלחמה.

אפשרות אחרת היא להגדיר את הסייבר ההתקפי כ"סיוע קרבי" כמו סיוע אש, ולהקנות לו מעמד של חיל או מפקד מערך אשר לו יכולת משולבת של בניין כוח והפעלתו בחירום, בין אם באופן מטכ"לי ריכוזי ובין אם שילוב של יכולות בכמה דרגים, עליהם יהיה אחראי מפקד המערך. הקבלה כזו תאפשר דיון מושכל יותר ביכולות חשובות שמקומן במב"ם הולך וגדל, אך למידה מהמלחמה באוקראינה מעמידה אותן בפרופורציה הנכונה בתרחיש של מלחמה רחבת היקף. מן הצד השני, יתכן שבתרחיש של מלחמה במעגל שלישי, בו יכולת התקיפה הקינטית הישראלית סובלת ממגבלות שונות, מרכיב הסייבר ההתקפי צריך להיות מרכזי.

רשימת מקורות:

- אורטל, ערן (אפריל 2021). "הזבוב על גב הפיל: מקומה של המערכה בין המלחמות בתפיסת הביטחון של ישראל". **עדכן אסטרטגי**. כרך 24, גיליון 2, עמ' 86-91.
- לשכת הרמטכ"ל. אסטרטגיית צה"ל. 2015. גרסה בלמ"ס.
- סא"ל רועי (ינואר 2021). "ממב"ם למערכה רב־זירתית רציפה". **מערכות**, גיליון 489, עמ' 36-43.
- פינקל, מאיר (2018). **הרמטכ"ל**. מודן ומערכות.

- Cuttler David and Black, Dan (April 6, 2022). "The Myth of the Missing Cyberwar Russia: Hacking Succeeded in Ukraine—And Poses a Threat Elsewhere, Too". *Foreign Affairs*.
- Cristal, Moti. (March 13, 2022). "Five things we learned from the Russia-Ukraine cyberwar". *Ha'aretz*.
- McLaughlin, Jenna (April 27, 2022). "cyberwar is already happening in Ukraine, Microsoft analysts say". In: https://www.npr.org/2022/05/26/1101569979/a-cyberwar-is-already-happening-in-ukraine-microsoft-analysts-say?s=08. Refers to: Microsoft. Special Report: Ukraine: An overview of Russia's cyberattack activity in Ukraine.
- Rohozinski, Rafal. (March 9, 2022). "The missing 'cybergeddon': what Ukraine can tell us about the future of cyber war", *IISS*.
- Willett, Marcus (March 10, 2022). "Russia–Ukraine: Pressing the right button at the right time", *IISS*.

- White, Sarah P. (March 20, 2018). Understanding Cyberwarfare Lessons from the Russia-Georgia War. *Modern war Institute*.