הסייבר בצה"ל

גדי איזנקוט

מבוא

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

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

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

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

הסייבר כחלק ממעגלי האיום

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

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

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

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

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

התארגנות צה"ל לפעולה בסייבר

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

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

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

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

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

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

סיכום

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

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

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

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

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

---

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

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