Shutterstock

הקיום הנעדר של הטכנולוגיה בחשיבה האסטרטגית־ביטחונית של ישראל

אביתר מתניה, אורן פודהורצר וניר דניאל
אוניברסיטת תל אביב

יציבתה המדעית־טכנולוגית של ישראל ויתרונה הטכנולוגי־צבאי הם תוצאה של אסטרטגיה וריכוז מאמץ לאורך שנים. להווי ידוע שהמשך בניית יתרון זה לאורך זמן תלוי בכיוון האסטרטגי ובהחלטות המתקבלות כיום, ולכך נדרש מאמר זה.

שיטה מקובלת לבחינת יכולות ויתרון טכנולוגי היא על פי השקעות תקציביות או על פי דירוגים מוחלטים ויחסיים של רמת מחקר אקדמי, מחקר ופיתוח (מו"פ) תעשייתי והשקעות בהון אנושי, אך במאמר זה בחרנו לגשת לנושא מזווית שונה ולבחון את מקומה של הטכנולוגיה כפי שהוא מתבטא באסטרטגיות ביטחון פורמליות של ישראל שפורסמו בשני העשורים האחרונים. ייחודה של פרספקטיבה זו שהיא מלמדת על האיכות ועל עומק ההבנה של התכנון האסטרטגי הלאומי בהקשר הטכנולוגי הצופה פני עתיד.

בהתאם לכך המאמר מתמקד בניתוח שלוש אסטרטגיות ביטחוניות מרכזיות שפורסמו בשני העשורים האחרונים – "תפיסת הביטחון של ישראל", "אסטרטגיית צה"ל" ו"האסטרטגיה הישראלית להגנת הסייבר". הוא מנתח את מקומה של הטכנולוגיה בהן על בסיס נורמטיבי של האופן שבו צריכות להיכתב אסטרטגיות טכנולוגיות שלמות, משווה אותן זו לזו וכן לאסטרטגיות ביטחון לאומי של ארצות הברית ובריטניה.

מהניתוחים עולה כי בשלוש האסטרטגיות **קיימת התייחסות מובהקת ליתרון טכנולוגי כאל יעד**, אך לצד זאת **בשתיים הראשונות חסר ניתוח מקיף של דרכי המימוש והכלים הנדרשים לבניית העוצמה הטכנולוגית, וגם השלישית אינה שלמה.** המאמר מסתיים בדיון במשמעויות ובהיבטים לעתיד של היעדרה (הדרך והאמצעים) של הטכנולוגיה (יעד) מן האסטרטגיות הללו.

מילות מפתח: טכנולוגיה וביטחון, אסטרטגיה לאומית, ביטחון לאומי, אסטרטגיה טכנולוגית, תפיסת הביטחון של ישראל.

מבוא

התפיסה השלטת בתרבות הישראלית בהקשר לטכנולוגיה בכלל ולטכנולוגיה צבאית בפרט, בקרב מקבלי ההחלטות, מלומדים ו"עמך ישראל", הן בהקשר לרובד הביטחון הלאומי והן בנוגע לרובד הביטחוני־צבאי שמתחתיו היא: המדע והטכנולוגיה הם תשתית חיונית למדינה מפותחת בכלל; המדע והטכנולוגיה הם רכיב מרכזי בביטחונה הלאומי של ישראל במובן הרחב ביותר; הטכנולוגיה היא מרכיב מכריע בהשגת יתרון מהותי בשדה הקרב לכל צבא וחיונית בייחוד לישראל, הסובלת מא־סימטריה כמותית חריפה מול אויביה לצורך השגת עליונות צבאית עליהם, החיונית לשרידותה של המדינה; לישראל יש כבר זמן רב יתרון טכנולוגי מובהק על הסביבה ויציבה טכנולוגית מתקדמת במונחים גלובליים (מדע ותעשיית היי־טק) בכלל, ובפרט בטכנולוגיה צבאית המבוססת על מו"פ עצמי איכותי. תפיסות אלו של עליונות טכנולוגית והון אנושי מדעי־טכנולוגי מעולה כמרכיב משמעותי בהשגת יתרון על היריבים הלכו והתעצמו עם השנים והפכו כאמור למרכיב יסודי בפועל בתפיסת הביטחון של ישראל, במובנה הרחב ובמובנה הביטחוני־צבאי כאחד (בן־ישראל, 2013; בן ישראל ועמיתיו, 2020, עמ׳ 8-21; מתניה 2022; פינקל ופרידמן, 2016; עילם, 2009, עמ׳ 497-508; עמידרור, 2020).

אך להווי ידוע שלשם יצירת יציבה טכנולוגית מובילה ושימורה נדרשת השקעה מתמדת וארוכת טווח בתשתיות מדעיות אקדמיות, בתשתית מערכתית טכנולוגית ובתשתית והון אנושי, המהוות בסיס מאפשר לאסטרטגיית בניין כוח טכנולוגי. כן יש לזכור שהשקעה כזו נושאת פרי רק שנים רבות לאחר שבוצעה, לעיתים רק לאחר עשור או שניים. למשל, ההשקעות בהון אנושי מדעי־טכנולוגי בישראל שבוצעו עוד לפני קום המדינה הן שאפשרו מו"פ עצמי בעשורים שלאחר הקמתה, וההשקעות בהון אנושי בעשורים הראשונים לקיום המדינה הן שעמדו ביסוד ההגעה לעליונות צבאית־טכנולוגית משנות ה־90 ואילך, והיו גם חלק מאבני הבניין שאפשרו את הפיכתה של ישראל למעין מרכז (hub) של חדשנות טכנולוגית (מתניה, 2022).

שאלת המחקר והגישה המתודולוגית

השאלה שאנו מעוניינים לעסוק בה במאמר זה היא עד כמה אנשי הרמה האסטרטגית של המדינה מבינים גם כיום את חשיבותם של המדע והטכנולוגיה כמרכיב אסטרטגי בביטחונה הלאומי של ישראל וכמרכיב מפתח ביתרונה הצבאי האזורי, ועד כמה הם מנהיגים תחומים אלו ביד מכוון ובראייה אסטרטגית מנהיגותית מובילה. ניתן לענות על שאלה זו במספר דרכים. שתיים נהוגות הן מדידה וניתוח של תקציבים המופנים לטכנולוגיה ומדדים לרמה ולהיקף המחקר והמו"פ. הראשונה מתמקדת כאמור בניתוח תקציבים המוקדשים לנושא הטכנולוגי בכיוונים שונים, החל מהתקציבים למו"פ כללי (כמו תקציב הות"ת ותקציב רשות החדשנות) וכלה בנתח תקציב הביטחון המוקדש לבניין כוח טכנולוגי, וכן תקציבי המגזר העסקי המופנים למו"פ, וזאת בהשוואה לאורך שנים ולמדינות אחרות, באופן מוחלט או יחסי. יתרונותיה של שיטה זו הם שבסופו של דבר יש מִתאם גבוה בין תקציבי המו"פ לבין היקף המו"פ המבוצע, אך הוא אינו מושלם משום שאינו מודד איכות ואינו רגיש לאסטרטגיות של מיקוד מאמץ או יתירות.

שיטה נהוגה שנייה היא לפי מדידה השוואתית של גופי המו"פ בישראל — האוניברסיטאות, תעשיית ההיי־טק והמו"פ הביטחוני בהשוואה למדינות אחרות בעולם, הן באופן יחסי (לנפש) והן באופן מוחלט. לגבי המגזר האזרחי אכן יש נתונים ודירוגים רבים המצביעים על מקומה הסביר של האקדמיה הישראלית בעולם המדע ועל מקומה הטוב של תעשיית ההיי־טק בהשוואה לעולם במספר מגזרים, כמו סייבר או מדעי הנתונים. בחלק הביטחוני המדידה מעט יותר מורכבת אך אפשרית. היתרונות של שיטה זו הם ביחסיותה מול העולם ובשימוש בדירוגים אובייקטיביים יחסית. חסרונותיה הם בכך שהיא מודדת מצב עכשווי הנשען על השקעות ומאמץ של עשור או שניים אחורנית, ובכך שהדירוגים לעיתים מחמיצים את הסיפור האמיתי של המו"פ ועלולים להטעות את מי שתוהה לאן להמשיך.

במאמר זה אנחנו מבקשים לנקוט גישה שלישית, כזו שאינה מסתמכת על תקציבים או נתונים אלא על הממד ההצהרתי האסטרטגי של המדינה, ולבחון עד כמה וכיצד הנושא הטכנולוגי עולה במסמכים אסטרטגיים מהותיים של ישראל, ברמת הביטחון הלאומי וברמה של ביטחון־צבא באופן ישיר. נתחיל בחסרונות המובנים של שיטה זו: ראשית, הצהרות אינן בהכרח מעשה ("בין אמר ועשה ת"ק פרסה"). יש מדינות שמצהירות אך בשטח עושות מעט מאוד, עקב חוסר ביכולת יישום של המגזרים השונים או משום שהתקציבים אינם עוברים על אף ההצהרות והתכנון. שנית, שיטה זו רגישה לעצם הגותן וכתיבתן של אסטרטגיות לאומיות ושל מי שכותב אותן. במדינת ישראל בפרט חסרות באופן מובהק אסטרטגיות לאומיות כתובות ומאושרות, והיא חזקה בעולם המעשה יותר מאשר בעולם התאוריה.

ואולם לשיטה זו גם מספר יתרונות. הראשון — כאשר נושא מסוים כבר מופיע באופן ברור וסדור באסטרטגיה הלאומית, הדבר מצביע על כך שהרמה האסטרטגית

של קבלת ההחלטות מודעת לו ומחויבת אליו, ולכן גם בדרך כלל תקדיש את מה שנדרש על מנת לממש אותו ולאורך זמן רב, ויש סיכוי לא רע שגם באופן חוצה ממשלות מתחלפות. זאת ועוד, הצהרתיות ברורה ומחויבת על כיוונים אסטרטגיים מחלחלת מטה לדרגי המקצוע והביצוע באופן ברור ואחיד וכמצפן לעשייה ארוכת טווח, משום שלביטויים הפורמליים יש משמעות בפועל באשר לעומק ההבנה של התכנון האסטרטגי ויעדיו, קביעת סדרי העדיפות האסטרטגיים והתכנון ארוך הטווח, תוכניות החומש של הגופים השונים, הקצאת משאבים ופיתוח כוח אדם מתאים. כמו כן, יתרון חשוב מאוד של דרך זו הוא שהדברים המופיעים באסטרטגיות קובעים את העתיד, שהוא־הוא העניין העיקרי שלנו, ולא רק מצלמים את תמונת ההווה, הנשען על מה שאחרים בנו במהלך העשורים שחלפו.

אי אפשר להתעלם מעוד יתרון גדול של בחינת אסטרטגיות לאומיות — המוטיבציה והחזון שהן מציבות בפני האומה כולה והעושים במלאכה, ופעמים רבות הן חשובות יותר מתקציבים. ישראל היא דוגמה טובה לכך שעל אף מחסור כבד בתקציבים של ממש, אך במאמץ לאומי שהקדיש את מיטב משאבי האומה למדע ולטכנולוגיה בעשורים הראשונים שלה בהתבסס על חזון ואסטרטגיה ברורה של המנהיגות בתחילת הדרך, הצליחה לבנות את עצמה כמובילה, יחסית לגודלה, בטכנולוגיה ביטחונית ובהמשך בטכנולוגיה בכלל, מה שתקציבים או דירוגים לא מדדו ולא הראו במדויק במשך עשרות שנים.

אלו הסיבות לכך שעל אף החסרונות וההסתייגויות שנכתבו כאן, אנו בוחרים בשיטה זו של בחינת אסטרטגיות לאומיות לצורך הבנת מקומה של הטכנולוגיה בסדר האסטרטגי של המדינה. דרך זו כאמור אינה חפה מחסרונות וגם אינה שלמה, אך מהווה מרכיב בבחינה כוללת של השאלה כמוסבר. לשם כך מאמר זה פונה לאסטרטגיות הביטחוניות של ישראל שנכתבו בעשורים האחרונים ובוחן אם הן אכן מבטאות באופן פורמלי שאיפה זו לקדמה טכנולוגית ולבנייתו של המרכיב הטכנולוגי כמרכיב יסוד באסטרטגיית הביטחון הלאומי של ישראל גם בראייה לעתיד; כיצד הטכנולוגיה באה לידי ביטוי בחשיבה הביטחונית האסטרטגית של מדינת ישראל; ואם הביטוי הפורמלי של חשיבה זו עולה בקנה אחד עם חשיבותה.

במאמר אנו מנתחים את ההתייחסות לטכנולוגיה בשלוש אסטרטגיות ביטחוניות מרכזיות של ישראל שפורסמו בשני העשורים האחרונים, המייצגות את מקומה של הטכנולוגיה בחשיבה הביטחונית הישראלית: הראשונה היא מסמך המלצה לאסטרטגיית ביטחון לאומי שהוכן על ידי ועדת מרידור בשנת 2006 והוגש לממשלת אולמרט. אף שלא אושר רשמית הוא נתפס כאחד מהמסמכים המכוננים בתחום הביטחון הלאומי בעשורים האחרונים. בניתוח במאמר זה נסתמך על הגרסה המופיעה במסמך הבחינה מחדש משנת 2018 של המסמך המקורי (מרידור ואלדדי, 2018); השנייה היא אסטרטגיית צה"ל בגרסתה הבלתי מסווגת שפורסמה בשנת 2018 (אסטרטגיית צה"ל, 2018), המבטאת את החשיבה הביטחונית־טכנולוגית ברובד הביטחוני־צבאי. זו הייתה הפעם הראשונה שצה"ל פרסם מסמך מסוג זה, שמטרתו לפרט את האסטרטגיה שלו בראייה כוללת כמתחייב מתפיסות הביטחון הלאומי של צה"ל. בכך הפך מסמך זה למסמך מכונן המצביע על תפיסות, דגשים, מיקוד ותובנות של דרג קבלת ההחלטות בצבא; השלישית היא האסטרטגיה הישראלית להגנת הסייבר (האסטרטגיה הישראלית להגנת הסייבר, 2017), שאומנם מתייחסת לנושא מסוים בביטחון הלאומי, אך עושה זאת בהיקף הנע מהרובד של ביטחון לאומי כולל ועד הפן ההגנתי עצמו.

במילים אחרות, האסטרטגיה הראשונה שאנו בוחנים היא ברובד הביטחון הלאומי (אם כי במובן הצר ולא במובן הרחב הכולל גם היבטים חברתיים וכלכליים, אלא ביטחון בלבד); השנייה היא הרובד שמתחתיו — ביטחוני־צבאי באופן מקיף ביותר; והשלישית היא אסטרטגיית הסייבר — המקבילה לשתיהן יחד מבחינת הרבדים אך ממוקדת בנושא אחד בלבד — הסייבר. בכך אנו מקיפים את נושא האסטרטגיות הלאומיות משני כיוונים (כללי וממוקד) ובשני רבדים (ביטחון לאומי וביטחוני־צבאי), תוך בחינת שלושה גופים שונים (ועדה ממונה, מטכ"ל וגוף ממשלתי, בהתאמה לשלוש האסטרטגיות). יצוין כי למיטב ידיעתנו, בשני העשורים האחרונים לא פורסמו אסטרטגיות לאומיות או לאומיות למחצה נוספות בהיבטי ביטחון או ביטחון לאומי, למעט מסמך חסוי של ראש הממשלה לשעבר נתניהו, שלא ניתן לגשת אליו. בכך עבודתנו מקיפה גם את האסטרטגיות הקיימות בתחום.

המתודולוגיה לניתוח האסטרטגיות וההשוואה ביניהן היא ניתוח לפי יעדים, דרכי מימוש ואמצעים (Ends, Ways, Means). אסטרטגיה ניתנת לתיאור כחיבור בין שלושה מרכיבים: יעדים (Ends), דרכי פעולה למימושם (Ways) ואמצעים לביצוע (Means), כפי שהגדירם הגנרל ליקה (Lykke) (Cancian, 2017). על פי תאוריה זו נדרש איזון בין שלושת המרכיבים לשם יצירת אסטרטגיה מוצלחת, ואילו בחוסר איזון טמון סיכון לאי־הצלחה במימושה (Yarger, 2008).

אנו מתבססים על שיטה זו ומנתחים את האסטרטגיות בשלושה אופנים שונים. הראשון —

ניתוח ההיבט הטכנולוגי באסטרטגיות הללו בהתאם למצופה מהן לפי יעדים, דרכי מימוש ואמצעים, מה שנותן לנו תצפית ראשונית **נורמטיבית** על הקיים ועל החסר בהיבט הטכנולוגי באסטרטגיות אלו, בהשוואה למה שהיינו מצפים מכל אחת מהן ברובד ובמיקוד שלה, ובהשוואה למה שיש בהן בתחומים אחרים שאינם טכנולוגיים; השני — **השוואת האסטרטגיות זו לזו** אך לא מבחינת תוכנן (שהרי הן מכוונות לרבדים ולנושאים שונים) אלא מבחינת התייחסותן לתחום הטכנולוגי, כל אחת בתחומה וברובד המצופה ממנה. כלומר משווים את אופי ההתייחסות לפן הטכנולוגי, שלמותו והיקפו; השלישי — השוואת התייחסותן של האסטרטגיות הישראליות לטכנולוגיה לעומת התייחסותן של שתי אסטרטגיות ביטחוניות מקבילות במדינות מערביות — ארצות הברית ובריטניה. באמצעות השוואה זו אנו מקבלים נקודת מבט יחסית של **פוליטיקה השוואתית** של שתי מעצמות ביטחוניות וטכנולוגיות שאנו רואים בהן מקור להשוואה בהתייחסות לטכנולוגיה בהיבט האסטרטגי הלאומי.

הסתייגויות ומגבלות הניתוח

נסתייג ונדגיש את מגבלות הניתוח כבר כאן. ראשית, מושא ההשוואה במאמר זה של האסטרטגיות האמריקאית והבריטית הוא ברובד הגבוה ביותר של אסטרטגיות לאומיות, ומתאים לכן בעיקר להשוואה לדוח ועדת מרידור בדבר אסטרטגיית הביטחון הלאומי של ישראל. עם זאת, בראייתנו הן נותנות פרספקטיבה מצוינת לגבי התייחסות כוללת לטכנולוגיה גם ברבדים נוספים של האסטרטגיות של צה"ל ומערך הסייבר הלאומי.

שוני מהותי נוסף בין מסמכי האסטרטגיה הישראליים לבין המסמכים האמריקאיים והבריטיים הוא היותם של האחרונים מסמכים מאושרים ברמה הלאומית על ידי מנהיגי המדינות, וזאת להבדיל מהמקרה הישראלי שבו מדובר במסמכים שלא אושרו ברמה הלאומית, כלומר בממשלה, ולכן אינם בהכרח מעידים או לא מעידים על התפיסה האסטרטגית המנהיגותית, לא כשנכתבו ולא כיום. הערה זו חשובה בייחוד לגבי אסטרטגיית הביטחון הלאומי (ועדת מרידור), שהצוות שכתב אותה הוקם על פי בקשת ראש הממשלה אריאל שרון ומסקנותיה הוגשו לראש הממשלה אהוד אולמרט כדי שהממשלה תאשר אותן, אך הן מעולם לא אושרו ולא תוקפו. הערה זו נכונה חלקית גם לאסטרטגיית צה"ל ולאסטרטגיה הישראלית להגנת הסייבר. אלו תוצרים של הארגונים המדוברים — צה"ל ומערך הסייבר הלאומי — שאושרו על ידי ראשיהם בעת פרסומם אך מעולם לא תוקפו על ידי הממשלה.[1]

חשוב לציין גם שרמת ההתייחסות לטכנולוגיה שאנו מצפים מכל מסמך היא שונה, בהתאם לרובד שהוא שייך לו ולמטרת כתיבתו. למשל אסטרטגיית צה"ל, שאכן מבטאת התייחסות לאומית אסטרטגית לביטחון, עושה זאת מנקודת המבט של אסטרטגיה צבאית של הרמטכ"ל, שהיא שילוב של תפיסת הפעלה והחלטות ארגוניות הנוגעות לצה"ל.

עם זאת ולאחר הסתייגויות אלו, אנו מוצאים כי השיטה שנבחרה במאמר זה לניתוח האסטרטגיה הישראלית לגבי היתרון הטכנולוגי בראייה עתידית, מרכיב מרכזי וחשוב ביותר כאמור בהיבטי הביטחון הלאומי, היא חזקה במיוחד. זאת בעיקר משום שהיא מקיפה שלושה מסמכי יסוד שונים במהותם, במהות הארגונים והכותבים שלהם וברבדים שלהם כפי שתואר, והתייחסות מקיפה זו משלושה כיוונים שונים ובאמצעות בסיס דוקטרינרי שווה לבחינתן מאפשרת ליצור מבט־על אובייקטיבי באשר לגישה האסטרטגית של ישראל למקומה של הטכנולוגיה בביטחון הלאומי.

למרות החשיבות והמרכזיות של היתרון הטכנולוגי וההסתמכות עליו במערכת הביטחונית האסטרטגית הישראלית ובקרב מקבלי ההחלטות, הדיון והעיסוק בו אינם שלמים ומקיפים, והם רחוקים ממה שהיינו מצפים ממדינה מובילה טכנולוגית כמו ישראל.

טענת המחקר

טענתנו העיקרית היא שלמרות החשיבות והמרכזיות של היתרון הטכנולוגי וההסתמכות עליו במערכת הביטחונית האסטרטגית הישראלית ובקרב מקבלי ההחלטות, הן ברובד הביטחון הלאומי והן ברובד הביטחוני הישיר, הדיון והעיסוק בו אינם שלמים ומקיפים, והם רחוקים ממה שהיינו מצפים ממדינה מובילה טכנולוגית כמו ישראל. כלומר קיים פער בין ההצבעה על חשיבות הטכנולוגיה לבין בניית אסטרטגיה טכנולוגית מקיפה למימוש היתרון הטכנולוגי. במאמר אנו בוחנים את שלוש האסטרטגיות הביטחוניות לאישוש טענתנו זו ומצביעים על כך שהיא בעיקר רלוונטית לאסטרטגיית הביטחון הלאומי ולאסטרטגיית צה"ל, ובאופן חלקי גם לאסטרטגיית הגנת הסייבר, ובייחוד בהשוואה לאופן המקיף שאסטרטגיות זרות (ארצות הברית ובריטניה) דנות בנושא. בחלק הדיון אנו מנסים לעמוד על הסיבות לכך ועל המשמעויות של פער זה.

חלק ראשון: אסטרטגיות ביטחוניות לאומיות של ישראל ומקומה של הטכנולוגיה בהן

תפיסת הביטחון של ישראל — ועדת מרידור בחלוף עשור

כללי

המסמך "תפיסת הביטחון של ישראל — דו"ח הועדה לגיבוש תפיסת הביטחון (ועדת מרידור) ובחינתו בחלוף עשור" (מרידור ואלדדי, 2018) ריכז ובחן בחלוף עשור את הדוח המסכם את מסקנות הוועדה לגיבוש תפיסת הביטחון של ישראל בראשות דן מרידור, אשר הוגש באפריל 2006 לראש הממשלה דאז אהוד אולמרט ולשר הביטחון שאול מופז. מטרת הדוח הייתה לשרטט את התובנות והעקרונות הבסיסיים בתפיסת הביטחון הלאומי של ישראל תוך התמקדות בתחום הביטחוני הצר וללא עיסוק כמעט בכלל מרכיבי הביטחון הלאומי במובנם הרחב, למעט נגיעה בסוגיות מרכזיות לאומיות שלהן ממשק עם עולם התוכן הביטחוני, כמו העיקרון "צבא העם" או חלקו של תקציב הביטחון בתקציב המדינה הכללי. המסמך זכה להסכמה נרחבת הן לגבי נחיצותו והן לגבי התכנים העיקריים שבו. התפיסה לא אושרה באופן פורמלי על ידי הממשלה אך חלק מהמלצות הדוח אומצו בפועל, כמו הוספת "רגל ההתגוננות" למשולש הביטחון הישראלי ושילובו באסטרטגיית צה"ל.

מקומה של הטכנולוגיה במסמך

כבר בעקרונות היסוד (מרידור ואלדדי, 2018, עמ׳ 18–19) ניתן לראות את מרכזיותה של הטכנולוגיה בתפיסה הביטחונית, כאשר שניים מבין תשעת העקרונות נוגעים באופן ישיר ביתרון האיכותי (עקרונות 4 ו־8): "העוצמה הביטחונית תיבנה על עוצמה לאומית הנשענת על שמירת היתרון האיכותי"; ו"קידום היתרון האיכותי מחייב למצות את היתרונות היחסיים ברמה הלאומית. לשם כך יש לטפח את האיכות האנושית, לנצל את ההזדמנויות הטכנולוגיות ולפתח את היכולת הארגונית".

משמעות העיקרון הראשון היא שחלק הארי של העוצמה הביטחונית הישראלית הוא היתרון האיכותי הטכנולוגי והאנושי, בעוד שהעיקרון השני מסביר בקווים כלליים כיצד יש לקדם את היתרון האיכותי. החתירה לשימורו ולחיזוקו של היתרון האיכותי נשענת על שני מאמצים עיקריים המשלימים זה את זה. הראשון — טיפוח התשתית האנושית ויצירת הבסיס הטכנולוגי; השני — תרגומם המעשי של אלה לעוצמה צבאית. הבסיס האנושי והטכנולוגי נבנה על יסוד האיכות האנושית בצה"ל ובתעשיות, על תשתית מתקדמת של מו"פ ביטחוני, על תעשיות ביטחוניות המפתחות ומייצרות אמצעי לחימה מתקדמים ועל שיתוף פעולה בינלאומי. תרגום התשתית הזאת לעוצמה צבאית מתבסס על פיתוחם של אמצעי לחימה מתקדמים ועל הצטיידות בהם, על רכישת יכולות מערכתיות המבוססות על תפיסות הפעלה מבצעיות, על טיפוח כוח אדם איכותי בתחומי הפיקוד, ההפעלה והאחזקה של אמצעי לחימה ועל יצירת תשתית ארגונית מתקדמת בתחומי הניהול, הידע והמידע.

בהמשך המסמך ישנן המלצות לאופן בניית היכולות הצבאיות (עמ׳ 28). לדעת כותבי המסמך, גישת בניין הכוח הצבאי צריכה לאזן בין בניית כוח לאיומים ספציפיים, כלומר גישת המענה — "בניין הכוח הוא סוג של ׳מענה׳ שניתן ל׳איום׳ הצפוי", כפי שמתאר יצחק בן־ישראל (בן־ישראל, 1997), לבין גישה גנרית של פתרונות ורסטיליים המאפשרים בנייה מהירה יחסית של יכולות צבאיות. גישה זו מזכירה את גישתו של יורם חמו, המתייחסת לבניין הכוח כאל מערכה דו־צדדית (חמו, 2016), בעוד שבסך הכול נדרש לשמור על היתרון היחסי מול צבאות סדירים במרחב. נוסף על כך המסמך כולל המלצות קונקרטיות לכיווני פיתוח טכנולוגיים, ביניהם קידום היכולות הלא־מאוישות (למשל כלי טיס בלתי מאוישים), התקדמות בחימוש המדויק, פיתוח תחום החלל, פיתוח יכולות ההגנה נגד רקטות ועוד.

המסמך ממשיך ומרחיב על הצורך בהסדרה לאומית של תהליכי קבלת ההחלטות בסוגיות היתרון האיכותי בראייה בין־תחומית ובין־ארגונית — גורם ביטחוני אחד האחראי על קביעת סדרי העדיפויות, קבלת ההחלטות המרכזיות ותיאום שוטף ומחייב של מערכות המו"פ, אשר לנוכח מגבלות המשאבים נדרש להיות ממוקד, רלוונטי, בעיתוי מתאים ובעל פוטנציאל להיות מתורגם למענה אפקטיבי שיקנה יתרון משמעותי בשדה הקרב (עמ׳ 35-36).

ניתוח

ניתן לראות כי הטכנולוגיה תופסת מקום חשוב ומרכזי בתפיסת הביטחון הלאומי הכוללת. בהתאם לסיווג המרכיבים באסטרטגיה, היתרון הטכנולוגי הוא אמצעי (Means) מרכזי ליצירת העוצמה הביטחונית הישראלית, שהיא הדרך (Ways) להשגת היעדים הלאומיים (Ends). יש פירוט חלקי על אופן שימורו של היתרון האיכותי הטכנולוגי, וכן הבנה כי כדי לשמרו יש צורך בטיפוח הון אנושי הבונה תשתית טכנולוגית, שעל גביה נבנים הפיתוחים הצבאיים. עם זאת בולט חוסר ההתייחסות לשאלה כיצד נדרש לטפח את ההון האנושי, וכן חוסר פירוט על הדרכים הקונקרטיות לשמירה על היתרון

האיכותי (לדוגמה, היקף ההשקעה הנדרש במו״פ ביטחוני, הקשר בין האקדמיה להון האנושי ועוד). חוסר זה בולט בייחוד בהשוואה לנושאים אחרים במסמך, שבהם דווקא קיימת התייחסות כוללת הן ל״מה״ והן ל״איך״ באופן מקיף יותר, כמו למשל לגבי הצגת אסטרטגיה מקיפה מול אתגר הטרור.

מסמך אסטרטגיית צה״ל

כללי

מסמך ״אסטרטגיית צה״ל״ הוא מסמך תפיסתי כולל שפורסם לראשונה לציבור הרחב בשנת 2015 ועודכן בשנת 2018 במטרה להוות את התשתית הרעיונית והמעשית לכל העשייה הצבאית (אסטרטגיית צה״ל, 2018). זו הפעם הראשונה שצה״ל פרסם מסמך מסוג זה, שמטרתו לפרט את האסטרטגיה שלו בראייה כוללת כמתחייב מתפיסות הביטחון הלאומי של צה״ל. בשל כך הוא הפך למסמך מכונן המצביע על תפיסות, דגשים, מיקוד ותובנות של דרג קבלת ההחלטות של הצבא. המסמך מפרט את האסטרטגיה של צה״ל כאמצעי להשגת האינטרסים הלאומיים, והיא נשענת על יסודות החשיבה והעשייה הצבאיות. המסמך בנוי מהכלל אל הפרט: המסגרת האסטרטגית — היעדים הלאומיים, הסביבה האסטרטגית, גורמי האיום ומאפייניו, עקרונות תפיסת הביטחון הלאומי והזיקה למטרות ולייעוד צה״ל (Ends), עקרונות וגישות הפעלת הכוח, תפיסת הפיקוד והשליטה ועקרונות בניין הכוח לטווח הקצר והארוך (Ways) והיכולות הנדרשות בצה״ל (Means). האסטרטגיה המובאת במסמך נשענת על ארבעה עמודי תווך, בהתאם להמלצת דוח תפיסת הביטחון של ישראל שנסקר לעיל — הרתעה, התרעה, התגוננות והכרעה, תוך יישומם באסטרטגיה ביטחונית הגנתית ובתפיסה צבאית אופרטיבית התקפית (עמ׳ 9).

מקומה של הטכנולוגיה במסמך

הטכנולוגיה במסמך אסטרטגיית צה״ל באה לידי ביטוי במספר היבטים. בהיבט הסביבה האסטרטגית מציג המסמך כי קצב התפתחות הטכנולוגיה המהיר, העלייה ביכולת המיצוי של טכנולוגיות לשימושים צבאיים ומהפכת המידע והסייבר משפיעים באופן מהותי על הסביבה האסטרטגית, וכנגזרת מכך — על הביטחון הלאומי ועל צה״ל בפרט (עמ׳ 10-11). בהיבט הצבאי המתייחס ליריבי צה״ל (״צד אדום״) מציג המסמך איום ניכר על צה״ל בעקבות מגמת התרחבות התפוצה של אמצעי לחימה טכנולוגיים מתקדמים והתעצמות האויב במרכיבים התקפיים ומודיעיניים, שתכליתם לשבש את יכולות צה״ל ואת עליונותו המבצעית בכל ממדי הלחימה (עמ׳ 12-13). כחלק מאסטרטגיית צה״ל יש צורך למנוע, לשבש ולשלול את ההתעצמות הטכנולוגית של אויבי המדינה בשגרה ובחירום על מנת לשמור על הפער והיתרון הטכנולוגי באמצעות גישת המניעה וההשפעה, הכוללת פעולות אקטיביות למניעת התעצמות זו ברגיעה (עמ׳ 15-16). אסטרטגיית צה״ל מתייחסת גם לעולם המודיעין ובפרט למודיעין הטכנולוגי כאל אבן יסוד בהבנת האויב, יכולותיו וכוונותיו, חלק מהתהליך ומתחרות הלמידה בין מדינת ישראל לבין אויביה ומרכיב מרכזי בהתאמת המענה והיכולות האופרטיביות והטכנולוגיות על מנת לשלול את יכולות האויב מחד גיסא, ולשמור על היתרון היחסי האיכותי מאידך גיסא (עמ׳ 10, 17, 20).

תכליתו המרכזית של הפן הטכנולוגי באסטרטגיית צה״ל היא שמירה על היתרון האיכותי היחסי ועל הרתעה כוללת כלפי האויבים בזירות השונות. על פי המסמך, שמירת היתרון האיכותי היחסי של מדינת ישראל נדרשת להתבצע תוך למידה מתמשכת של הסביבה האסטרטגית והמבצעית ומעקב אחר התעצמותם של צבאות במזרח התיכון במסגרת תחרות הלמידה, על מנת לוודא שהיתרון האיכותי נשמר (עמ׳ 21, 26).

בהיבט הפעלת הכוח נדרש צה״ל על פי המסמך לקיים תהליכי בניין כוח לשימור ולחיזוק מעמדה הצבאי של ישראל ולשימור היתרון האיכותי היחסי והעליונות הצבאית בכל הממדים (יבשה, אוויר, ים, מודיעין, סייבר), תוך התמודדות מתמדת עם אתגרי קצב ההשתנות המהיר והתכוף של הטכנולוגיה והאתגרים הכלכליים. בפרט מציין המסמך כי נדרשת טכנולוגיה מתקדמת המותאמת לצרכים האופרטיביים וכן אמצעים וכוח אדם המיומן המתאים להפעלתה, והוא אף מתעדף את כוח האדם הטכנולוגי בקבוצה א׳ בסדר העדיפויות, יחד עם הלוחמים ככוח איכותי למשימות הלחימה בשדה הקרב. המסמך ממשיך ומפרט את עקרונות בניין הכוח, ביניהם גמישות ורב־תכליתיות (ורסטיליות), שיתופיות, רשתיות ורב־זרועיות, מסה קריטית, קטלניות, חופש פעולה וחיזוק הלמידה (עמ׳ 25-30).

בשונה מתחום הפעלת הכוח, בתחום בניין הכוח הטכנולוגי מסמך אסטרטגיית צה״ל אינו מציג אסטרטגיה ומתודולוגיה סדורה המגדירה את היעדים, דרכי הפעולה להשגתם והאמצעים הנדרשים, ואת יחסי הגומלין ביניהם. המסמך מגדיר את היעדים (Ends) של בניין הכוח כשימור מעמדה הצבאי של ישראל וחיזוקו תוך אפשור הפעלת הכוח לפי גישות המענה, אך לא את יכולות הליבה הנדרשות לבניין כוח טכנולוגי. מעבר לעקרונות בניין כוח כלליים, המסמך אינו עוסק בדרכים

ובשיטות למימוש בניין הכוח הטכנו־מבצעי (Ways), כמו לדוגמה התייחסות להשקעה במחקר ופיתוח, לפיתוח ולטיפוח ההון האנושי, לשיתוף פעולה בין התעשייה, משרד הביטחון והאקדמיה, להכרעה בנושא 'לפתח או לרכוש' (Make or Buy) ועוד. פער זה מבטא **חוסר הלימה בחשיבה האסטרטגית בין תהליכים אופרטיביים ומבצעיים וגישות הפעלת כוח לתהליכי בניין כוח טכנולוגיים בראייה הוליסטית**, אשר פוגעים בשלמותה של התפיסה האסטרטגית הכוללת המובאת במסמך.

בפן הביטחוני־צבאי נשענת מדינת ישראל בין היתר על שיתוף הפעולה והסיוע הביטחוני האמריקאי לצורך שימור עליונות צבאית טכנולוגית.

ניתוח

אסטרטגיית צה"ל מבטאת את התשתית הרעיונית והמעשית לכל העשייה הצבאית כחלק מתפיסת הביטחון הלאומי של ישראל ומציגה היבטים יישומיים למימוש האסטרטגיה בדגש על הפעלת הכוח, אתגרי הלחימה והגדרת הצרכים המבצעיים והאופרטיביים, אשר מענה להם יתבסס בין היתר על טכנולוגיה מתקדמת.

עם זאת, בהיבט של שמירת היתרון האיכותי היחסי ובניין הכוח הטכנולוגי חסרה באסטרטגיית צה"ל התייחסות לתהליכי בניין הכוח הטכנולוגי (Ways), הבניית תהליך אסטרטגי לבניין הכוח הטכנולוגי הכולל תפיסת מימוש, ארגון תומך, הקצאת משאבים נדרשת, תעדוף, הגדרות 'לפתח או לרכוש', שיתוף פעולה ביטחוני־טכנולוגי, ובעיקר החיבור התפיסתי האסטרטגי בין הצורך והיעדים המבצעיים (Ends) לדרכים למימושם (Ways) ולמשאבים ולטכנולוגיות הנדרשים לשם כך (Means). עולה מכך שהביטוי של הממד הטכנולוגי במסמך זה חלקי וחסר ואינו מבטא כנדרש את המקום המרכזי והייחודי שאותו צריכה לתפוס הטכנולוגיה על כלל היבטיה (הפעלת כוח, בניין כוח, ארגון ומשאבים) באסטרטגיה זו, וזאת בשונה מהיבטים אחרים באסטרטגיה.

מרכיב מרכזי נוסף החסר בהקשר הטכנולוגי הוא שיתוף הפעולה הלאומי והבינלאומי כמרכיב מפתח במימוש האסטרטגיה, ובפרט שיתוף הפעולה הביטחוני־אסטרטגי עם ארצות הברית. בפועל, בפן הביטחוני־צבאי נשענת מדינת ישראל בין היתר על שיתוף הפעולה והסיוע הביטחוני האמריקאי לצורך שימור עליונות צבאית טכנולוגית, בעיקר באמצעות הצטיידות באמצעי לחימה מתקדמים (כדוגמת המטוס 'אדיר' — F-35I), אשר אין ברצונה וביכולתה הכלכלית של מדינת ישראל לפתח בעצמה (Rounds, 2019, p.36-37 — ביטול פרויקט ה'לביא'), אולם גם נושא זה לא בא לידי ביטוי במסמך האסטרטגיה.

מסמך האסטרטגיה הישראלית להגנת הסייבר[2]

כללי

מסמך זה של מערך הסייבר הלאומי (האסטרטגיה הישראלית להגנת הסייבר, 2017) מפרט את אסטרטגיית הגנת הסייבר הלאומית, שייעודה הוא "להסדיר את כלל המאמצים הלאומיים בתחום הגנת הסייבר, ליצור 'שפה משותפת' בין העוסקים במלאכה ולהבטיח מענה יציב וארוך טווח" (עמ' 8). המסמך מורכב משלושה חלקים: הראשון — פירוט של תפיסת הפעולה בהגנת הסייבר, המחולקת לשלוש שכבות הגנה; השני — פירוט אופן יישום האסטרטגיה על ידי שלושה מאמצי־על: בניית הסייבר כמרחב צמיחה בטוח על ידי מימוש שלוש שכבות ההגנה; הקמת זרוע אופרטיבית של מערך הסייבר להובלת מאמצי ההגנה על המשק הישראלי מפני תקיפות; ומחקר, פיתוח ויישום של טכנולוגיות הגנה מדינתיות; החלק השלישי — פירוט בניין הכוח המדעי־טכנולוגי הלאומי בסייבר וחיזוק היתרון היחסי הישראלי בנושא, וכן שותפויות בינלאומיות לעיצוב מרחב הסייבר.

מקומה של הטכנולוגיה במסמך

הפן הטכנולוגי בא לידי ביטוי בשלושת חלקי המסמך העיקריים. בחלק הראשון, הדן ברעיון הפעולה של הגנת הסייבר באמצעות מודל של שלוש שכבות הגנה, שהוא הדרך (Ways) להגשמת יעד ההגנה, מפורטות הטכנולוגיות הנדרשות בכל שכבה כחלק מהותי משכבת ההגנה (Means). בחלק השני של המסמך (עמ' 37-38) הפן הטכנולוגי בא לידי ביטוי בצורה בולטת במאמץ השלישי — מחקר, פיתוח ויישום של יכולות וטכנולוגיות הגנה מדינתיות. כחלק ממאמץ זה להגנת הסייבר הלאומית מושקעים משאבים במו"פ של טכנולוגיות הגנה מדינתיות מתקדמות, כמו גם יחידת מו"פ ממשלתית ייעודית (היחידה לטכנולוגיות סייבר), האמונה על בניין הכוח הטכנולוגי בהגנת הסייבר במדינה ועל מתן מענה לצרכים המבצעיים של הרשות להגנת הסייבר. כלומר, על פי האסטרטגיה המוצעת במסמך, ליישום הגנת סייבר לאומית יעילה נדרש מאמץ־על של מו"פ טכנולוגי מתקדם עבור טכנולוגיות הגנה לאומיות כאחד משלושה מרכיבים עיקריים בהגנה — עדות למקומה המרכזי של הטכנולוגיה באסטרטגיה זו.

בחלק האחרון של המסמך מפורטים המאמצים התומכים בביסוס יכולת הסייבר הלאומית, שאחד מהם הוא בניין כוח מדעי־טכנולוגי לאומי בסייבר (עמ׳ 42-46). המסמך מרחיב היבט זה של בניין הכוח וההון האנושי ועוסק בשני תחומים נוספים: הראשון, שילוב האקדמיה באקוסיסטם בתחום הסייבר, לצד התעשיה וההון האנושי; השני, העצמת ההון האנושי בכמות ובאיכות, גם בגיל צעיר (תלמידי חטיבת הביניים/תיכון), כבסיס להון האנושי בעתיד.

ניתוח

הטכנולוגיה מופיעה במסמך זה הן כאמצעי (Means) מובנה להשגת דרכי ההגנה (Ways) על פי מודל שלוש השכבות (החלק הראשון במסמך); הן כדרך להשגת הגנה יציבה לאורך זמן (Ways) באמצעות בניית יחידה ייעודית לטכנולוגיות ומו״פ בתחום (החלק השני); והן כיעד (Ends) בפני עצמו בבניית האקוסיסטם השלם של הסייבר בישראל (החלק השלישי). האסטרטגיה המוצגת במסמך זה נחשבת מקיפה ושלמה באופן ייחודי לאסטרטגיות ישראליות. היא קושרת באופן ברור בין היעדים (Ends) הדרכים (Ways) והאמצעים (Means), והטכנולוגיה שזורה בכל ההיבטים והחלקים שלה באופן מקיף ושלם (Adamsky, 2017). חלק מהותי ממנה הוא שמירת היתרון הטכנולוגי בנושא בידי ישראל.

מקומה של הטכנולוגיה באסטרטגיות השונות — ניתוח השוואתי

בשלוש האסטרטגיות לעיל הפן הטכנולוגי מופיע כמרכיב חיוני באסטרטגיה עצמה, ועליו מתבססת העוצמה הישראלית בכל אחד מתחומי העיסוק של האסטרטגיות. במסמך ״תפיסת הביטחון של ישראל״ היתרון האיכותי הטכנולוגי מופיע בשני עקרונות יסוד שעל פיהם נדרש לגבש את התפיסה; באסטרטגיית צה״ל הפן הטכנולוגי מתבטא בהופעת היתרון היחסי בתחילת המסמך כעיקרון לחיזוקה האסטרטגי של מדינת ישראל (ובהמשך המסמך היתרון היחסי מוצג כגורם עיקרי בהרתעה מול האויבים בזירות השונות); ובאסטרטגיה הישראלית להגנת הסייבר הפן הטכנולוגי אומנם לא מופיע כעקרון יסוד, אך הוא אחד משלושת מאמצי־העל ליישום האסטרטגיה הכוללת, כלומר הוא אחד ממרכיבי העוצמה הישראליים בהגנה בסייבר.

נוסף על כך, בשלוש האסטרטגיות ניתן דגש מפורט על המשך בניין הכוח באמצעות מו״פ טכנולוגי. עצם ההופעה של פירוט ייעודי מסוג זה בכל אחת מהאסטרטגיות מצביעה על המקום המרכזי שמחברי כל אחד מהמסמכים מייחסים לטכנולוגיה. כמו כן, בשלוש האסטרטגיות מודגש כי היתרון הטכנולוגי מתבסס על הון אנושי בעל הכשרה מתאימה.

עם זאת, **ההבדל העיקרי והעמוק** בהתייחסות לטכנולוגיה בשתי האסטרטגיות הביטחוניות לעומת אסטרטגיית הגנת הסייבר הוא **שבאחרונה יש התייחסות מקיפה ל״איך״ שומרים על היתרון הטכנולוגי ולא רק ל״מה״ נדרש**. באסטרטגיית הגנת הסייבר מפורטת בקווים כלליים אסטרטגיה לשמירה על היתרון הטכנולוגי, שהוא אחד האמצעים (Means) להשגת היעדים הכלליים (Ends), אך בהיותו כה משמעותי הוא אמצעי חשוב מספיק לצורך פירוט מיני־אסטרטגיה לשמירתו. מיני־אסטרטגיה זו שזורה לאורך כל המסמך ובולטת בייחוד במאמץ התומך ב״בניין הכוח המדעי־טכנולוגי הלאומי בסייבר״ (האסטרטגיה הישראלית להגנת הסייבר, 2017, עמ׳ 42-46). **היעד** הכללי שלה הוא בניין כוח איכותי להגנת הסייבר, או במילים אחרות שמירה והגברה של היתרון הטכנולוגי הישראלי בהגנת הסייבר, אך לא רק זאת. ההתייחסות לבניין כוח בסייבר ברמה הלאומית נוגעת להיבט של ביטחון לאומי במובנו הרחב בעולם הסייבר, כלומר בניין כוח ברמה מעצמתית ככלי ביטחוני־מדיני ולא רק לצורכי הגנת הסייבר של המדינה. **הדרכים** הן המאמצים לתרגום ההון האנושי ליתרון טכנולוגי, כמו למשל שילוב האקדמיה והתעשייה, או המאמצים להגדיל את ההון האנושי ולשפר את איכותו; **והאמצעים** הם ההון האנושי עצמו, משאבים, האקדמיה, התעשייה ועוד.

יש שיטענו כי אסטרטגיית הגנת הסייבר מתעמקת בנושא פרטני יחסית לעומת שתי האסטרטגיות הביטחוניות, ועל כן ניתן לטעון כי בשל עומק זה יש מקום באסטרטגיה לפירוט נוסף ולהעמקה בנושאים ספציפיים. אך אסטרטגיות דומות במדינות אחרות לאו דווקא מתייחסות לפן הטכנולוגי בצורה זו אלא להגנת הסייבר של המדינה באופן ישיר בלבד. בכך אסטרטגיה זו ייחודית הן בנוף העולמי והן בישראלי, ובפרט בהתייחסותה למרכיב הטכנולוגי שהוא־הוא היוצר המרכזי של היתרון האיכותי (Adamsky, 2017).

חלק שני: השוואה לאסטרטגיות ביטחוניות זרות

בחלק זה של המאמר נשווה את מקומה של הטכנולוגיה באסטרטגיות הישראליות למקום שהיא תופסת בשתי אסטרטגיות ביטחוניות זרות — אסטרטגיית הביטחון הלאומי האמריקאית שפורסמה בדצמבר 2017 בעת כהונתו של הנשיא טראמפ (The White House, 2017), ואסטרטגיית הביטחון הלאומי של בריטניה שפורסמה בשנת 2015 (HM Government, 2015). ארצות הברית

ובריטניה נבחרו להשוואה זו שכן הן ללא עוררין מעצמות ביטחוניות וטכנולוגיות מובילות עולמיות. שני המסמכים מקיפים ועוסקים בשלל הנושאים הקשורים לביטחון הלאומי של מדינות אלו במנעד רחב ביותר, ובכלל זה לדוגמה התייחסות להתמודדות עם איומים ספציפיים כמו טרור ופשיעה, אינטרסים במרחב העולמי והאזורי ודיפלומטיה בינלאומית או סוגיות בהקשר הכלכלי, וכן בהרחבה גם בנושא המדעי־טכנולוגי. תחילה נבחן את מקומה של הטכנולוגיה בשתי אסטרטגיית ביטחון לאומי אלו ולאחר מכן נשווה אותה למקומה של הטכנולוגיה באסטרטגיות הביטחוניות הישראליות שהובאו בחלק הראשון.

אסטרטגיית הביטחון הלאומי של ארצות הברית

מסמך אסטרטגיית הביטחון הלאומי האמריקאית מתפרסם אחת לארבע שנים, עם כניסתו של ממשל חדש בארצות הברית (המסמך הראשון פורסם בשנת 2002). הוא מפרט את תפיסת הממשל באשר לסוגיות הביטחון הלאומי של ארצות הברית וכיצד נכון להתמודד איתן. המסמך המעודכן האחרון פורסם בדצמבר 2017 בעת כהונתו של הנשיא טראמפ (The White House, 2017). הנשיא הנוכחי ביידן פרסם ב־2021 מסמך הכוונה לכתיבת אסטרטגיית ביטחון לאומי.

הטכנולוגיה מופיעה במסמך זה במספר רבדים. תחילה מוצגת הטכנולוגיה כמרכיב מרכזי בחיזוק ובהגברת שגשוגה של הכלכלה האמריקאית, כלומר הטכנולוגיה מוזכרת בהקשר הלאומי ככלי לשמירת היתרון האזרחי־כלכלי, בניגוד להקשר הצבאי המובהק שמוצג באופן כמעט בלעדי באסטרטגיות הישראליות. בהמשך מציג המסמך את ההקשרים הביטחוניים של הטכנולוגיה ואת מקומה בשמירת היתרון האיכותי הצבאי של ארצות הברית על פני יריבותיה, אשר הולך ונשחק (Ends).[3] הן בפן הכלכלי והן בפן הביטחוני המסמך מציג את דרכי הפעולה לשימור היתרון האיכותי היחסי הטכנולוגי (Ways), אשר במובנים רבים חופפות ומתבססות על אותן אבני בניין — כוח אדם מדעי וטכנולוגי, חדשנות, יזמות ותעדוף טכנולוגיות, השקעה במו״פ ובפיתוח תשתית ידע מדעית וטכנולוגית וקיום שיתופי פעולה פנימיים וחיצוניים. המסמך מעמיק בכל אחד מנושאים אלו ומפרט את האמצעים לקידומם ולחיזוקם. נעמיק בקצרה בכמה מהם.

בתחום כוח האדם המדעי והטכנולוגי מציג המסמך את הצורך בקידום חינוך מדעי וטכנולוגי, ובפרט חיזוק מקצועות ה־STEM (Science, Technology, Engineering, Mathematics) — מדעים, טכנולוגיה, הנדסה ומתמטיקה, ופיתוח וטיפוח כוח אדם אקדמי עם התמחויות והתמקצעות טכנולוגית. בפרט ובהקשר למגזר הביטחוני מציין המסמך בין היתר את הצורך בגיוס כוח אדם טכנולוגי מוכשר, חדשן וממציא ואת הסרת המחסומים לגיוסו, תמריצים לגיוס ולשימור עובדי STEM פדרליים ומשכורות המתחרות עם השוק האזרחי על מנת לייצר מסלולים קלים יותר לכניסה של כוח אדם טכנולוגי, מדענים ומהנדסים לשירות הציבורי (עמ׳ 19-20).

המסמך מציג חלק ייעודי (עמ׳ 20-22) העוסק בתחום החדשנות ומתאר את תכליתו המרכזית כשימור ההובלה העולמית בטכנולוגיה, המצאות וחדשנות לשימור היתרון התחרותי האמריקאי. חלק זה מציג תעדוף טכנולוגיות מפציעות החיוניות לצמיחה כלכלית ולביטחון, ובפרט טכנולוגיות בינה מלאכותית ומעקב והבנה של מגמות התפתחות מדעית וטכנולוגית בעולם, וכיצד אלו יכולות להשפיע על ארצות הברית או לחתור תחת האסטרטגיות והתוכניות האמריקאיות. עוד מציג חלק זה את מינוף המגזר הפרטי ואת המומחיות שלו בבנייה ובחדשנות. בפרט מציין המסמך את הצורך בהשגה מחדש של גורם ההפתעה בהקשר הטכנולוגי דרך שילוב של טכנולוגיות חדשות בשדה הקרב בקצב של התעשייה האזרחית המודרנית, תוך לקיחת סיכונים.

בהקשרי מו״פ ופיתוח ידע מדעי וטכנולוגי מציג המסמך את הצורך בשיפור ובהשקעה במו״פ בשלבים מוקדמים, את הצורך בהגברת האפקטיביות של השימוש במו״פ ובמומחיות הנבנית במגזר הפרטי לצורכי הכלכלה והביטחון הלאומיים, קידום והגנה על בסיס החדשנות האמריקאית בתחום הביטחון הלאומי.[4] בפרט מדגיש המסמך את הצורך בהגנה על הידע האמריקאי בתחום הביטחון, שלרוב צומח מתוך האקדמיה ומתעשיות אזרחיות שונות והוא חיוני לשימור היתרון האיכותי. עוד מציין המסמך (עמ׳ 22-23) את הצורך בהשקעה בטכנולוגיה בתחום האנרגיה, הגעה לעצמאות אנרגטית, טיפול בזיהום אוויר ובהשפעה על האקלים, אשר מבטא את מקומה של הטכנולוגיה ככלי להתמודדות עם בעיות כלל־עולמיות וליצירת עצמאות אנרגטית, לרבות בתחום אנרגיית הגרעין.

בתחום שיתופי הפעולה מדגיש המסמך לאורך חלקיו השונים את החשיבות של שיתופי פעולה טכנולוגיים חיצוניים עם בעלי ברית ושותפים, וכן שיתופי פעולה פנימיים בין הממשל האמריקאי, התעשיה והאקדמיה, וחיזוק הקשר בין מערכת הביטחון לחברות טכנולוגיה אזרחיות כמנוף מרכזי לקידום הטכנולוגיה ברמה הלאומית והביטחונית.

כמו כן מבטא המסמך את היכולת להשתמש בטכנולוגיה ככלי להפעלת עוצמה קשה ורכה ולשימור ויצירת השפעה כנגד איומים גלובליים המשתמשים בטכנולוגיה (עמ׳ 25-26), וכן מתייחס לטכנולוגיה בידי אויבי המעצמה, אשר מצמצמת ושוחקת את היתרון הטכנולוגי האמריקאי המובהק (עמ׳ 3).

עם זאת המסמך מסייג את התלות המוחלטת בטכנולוגיה ומציג הבנה שהתלות והאמונה בטכנולוגיה כגורם שיכול לפצות על סדרי כוחות הייתה מוחלטת ומוטעית. מול זה נאמר במסמך כי לצד התלות בטכנולוגיה נדרש חידוש יכולות צבאיות, מודרניזציה, הצטיידות מסיבית באמצעים והגדלת היקפי הכוחות (עמ׳ 29). כפי שמצוין במסמך, ״האמנו בטעות שטכנולוגיה תוכל לפצות על הקיבולת המופחתת שלנו — היכולת להציב בשטח מספיק כוחות כדי לגבור מבחינה צבאית, לייצב את הישגינו ולהשיג את יעדינו הפוליטיים הרצויים. שכנענו את עצמנו שכל המלחמות יתנהלו ויוכרעו במהירות, מרחוק ועם מינימום נפגעים״[5] (עמ׳ 7).

אסטרטגיית הביטחון הלאומי וההגנה האסטרטגית של בריטניה

מסמך אסטרטגיית הביטחון הלאומי וההגנה האסטרטגית הבריטי פורסם לראשונה בשנת 2008 ומאז פורסמו עוד שני מסמכים מעודכנים, האחרון בשנת 2015 (HM Government, 2015). מסמך זה, בדומה למסמך האמריקאי, מתאר את היעדים הלאומיים של בריטניה בתחום הביטחון, את האתגרים העומדים לפתחו של הביטחון הלאומי הבריטי ואת הדרכים להתמודד איתם.

גם מסמך זה מתאר בצורה מקיפה מאוד את מקומה של הטכנולוגיה כחלק מהביטחון הלאומי. המסמך מציג כי התקדמויות טכנולוגיות בעולם, בעיקר בעולמות ה־IT והסייבר, משפיעות מאוד על הביטחון הלאומי ומהוות הזדמנות מחד גיסא ואיום מאידך גיסא, וכי לקדמה הטכנולוגית במגוון תחומים יש פוטנציאל עצום בתחום הביטחוני והכלכלי (עמ׳ 19). המסמך טוען כי תעשייה ביטחונית המקדמת חדשנות ותחרותיות מהווה מרכיב מרכזי בהתמודדות עם האיומים על הביטחון הלאומי של בריטניה. חדשנות במוצרים ובשירותים שמספקת התעשייה הביטחונית מאפשרת שימור היתרון ביחס ליריבים. המסמך מתייחס גם להיקפי ההשקעה של משרד הביטחון (MOD) במדע ובטכנולוגיה.

המסמך מפרט מספר יכולות ביטחוניות מתקדמות שבהן נדרשת בריטניה להשקיע — מטוסי קרב, סייבר, חלל, תקשורת, לוחמה בטרור ועוד, תוך שיתופי פעולה אסטרטגיים עם מדינות ידידות ושותפות, לדוגמה שיתוף פעולה בתחום פיתוח כלי טיס בלתי מאוישים עם צרפת. בכל היכולות האלה מצוין כי נדרשת השקעה משמעותית בתחום הטכנולוגי על מנת לשמור על היתרון היחסי והתחרותי, יחד עם התבססות על מדע וטכנולוגיה ומחקר ופיתוח בשיתוף צבאי, אזרחי ותעשייתי.

גם במסמך זה, בדומה למסמך האמריקאי, יש חלק ייעודי העוסק בחדשנות (עמ׳ 73-75). נאמר בו כי החדשנות המתבססת על מיצוי יכולות מדעיות וטכנולוגיות חיונית לעוצמה הכלכלית, לפרודוקטיביות ולתחרותיות של בריטניה בשוק העולמי. עוד מצוין במסמך כי בעולם הטכנולוגי כיום הקטר הוא המגזר הפרטי ולא הציבורי, ושיתוף הפעולה בין המגזר הטכנולוגי הפרטי למגזר הציבורי הוא מרכיב מפתח באפקטיביות של המיצוי הטכנולוגי בתחומי הביטחון הלאומי. לדוגמה מציג המסמך התנעה של יוזמת חדשנות ביטחונית (Defense Innovation Initiative) ברמה הלאומית, בעבודה משותפת עם אוניברסיטאות, חברות סטארט־אפ וחברות קטנות ובינוניות, תוך הצבת המדע והטכנולוגיה במרכז החשיבה בתחום הביטחון הלאומי. ״ניצור גוף חדש חוצה משרדים לניתוח טכנולוגיות מפציעות וחדשנות, עם קישורים צמודים למגזר הפרטי ולאקדמיה כדי להבטיח שנזהה את ההזדמנויות״[6] (עמ׳ 74).

עוד מציין המסמך (עמ׳ 74) השקעה בטכנולוגיות חדשניות ובעלות פוטנציאל להפוך למשבשות מול היריבים — מהלך הכולל מחקר מתקדם במעבדות המדע והטכנולוגיה של משרד הביטחון והמרכז למדע וטכנולוגיה יישומית, העובדים בצמוד לתעשייה ולאקדמיה. בהקשר זה מצוין הצורך לקדם טכנולוגיות במהירות, לבחון רעיונות לא קונוונציונליים ונכונות לקחת סיכונים דרך שינוי תפיסות העולם המסורתיות בתחום. המסמך מתייחס גם למסחור של יכולות המפותחות לטובת היבטי ביטחון על מנת למנף צמיחה כלכלית, לדוגמה בעולם הסייבר, וכן הקמת תוכניות האצה (אקסלרטורים) בתחום הביטחון על מנת לסייע לכלל המגזרים להפוך רעיונות חדשניים למוצרים ולשירותים במהירות רבה יותר ולמסור אותם למשתמשים הביטחוניים (עמ׳ 75).

המסמך עוסק גם בצורך בהגדרה של הממשלה לגבי הטכנולוגיות הנדרשות לפיתוח עצמי, ואילו מהן נדרשות לרכש חיצוני או דרך שיתופי פעולה והשקעה משותפת עם בעלי ברית, האקדמיה והתעשייה (׳לפתח או לרכוש׳) (עמ׳ 74). לדוגמה, שיתוף פעולה טכנולוגי אסטרטגי בין בריטניה לבין ארצות הברית כמרכיב מרכזי בביטחון הלאומי, לצד שיתוף פעולה בתחומי מודיעין, גרעין, דיפלומטיה ויכולות צבאיות, בין היתר כחלק מ״אסטרטגיית ההיסט השלישית״ האמריקאית (שמואל, 2016), ושיתוף פעולה עם צרפת סביב יוזמות טכנולוגיות בתחומי התעופה, הים והחלל. בפרט מציין

המסמך את שיתוף הידע הטכנולוגי כמרכיב בחיזוק היחסים הביטחוניים (HM Government, 2015, p. 75).

בהקשר של כוח אדם טכנולוגי מציין המסמך את ההכרח בפיתוח ובטיפוח כוח אדם טכנולוגי (STEM ויזמות), הקלות במעבר בין האקדמיה, המגזר הפרטי, המגזר הביטחוני ובין מדינות, קידום התעשייה הביטחונית והיצוא הביטחוני ומיצוב התעשיות הביטחוניות כמתקדמות, חדשניות ותחרותיות, לרבות שילוב חברות חדשות, גם קטנות, בתחום הביטחוני, כולל צמצום מגבלות המכירה והיצוא (עמ׳ 75, 78).

למסמך המתואר קדם המסמך ״ביטחון לאומי באמצעות טכנולוגיה״ (National Security Through Technology) שפרסם משרד ההגנה הבריטי ב־2012 (Ministry of Defence, 2012). על פני 65 עמודים מפורטות במסמך הדרכים (Ways) להשגת יתרון זה, כאשר התכלית והיעד של התוכנית (End) הם לספק לכוחות המזוינים ולסוכנויות הביטחון את האמצעים (Means) הטובים ביותר שניתן לרכוש במגבלות התקציב, בטווח הקצר והארוך, בגישה פרואקטיבית ויוזמת.

מקומה של הטכנולוגיה כחלק מתפיסת הביטחון הלאומי — כפי שמוצג בשתי אסטרטגיות ביטחון לאומי מערביות, של ארצות הברית (2017) ושל בריטניה (2015) — הוא מרכזי ביותר.

השוואה בין האסטרטגיות הביטחוניות הזרות לאסטרטגיות הביטחוניות הישראליות

מקומה של הטכנולוגיה כחלק מתפיסת הביטחון הלאומי — כפי שמוצג בשתי אסטרטגיות ביטחון לאומי מערביות, של ארצות הברית (2017) ושל בריטניה (2015) — הוא מרכזי ביותר. המסמכים עוסקים באופן מעמיק ויסודי בשלושת מרכיבי האסטרטגיה (Ends, Ways, Means) — יעדי הטכנולוגיה ומימושיה לצרכים וליעדים הלאומיים והביטחוניים, הדרכים להשגת ושימור היתרון הטכנולוגי, והאמצעים להשגת יתרון זה.

שתי האסטרטגיות מוצאות כי הטכנולוגיה חשובה עד כדי הגדרתה כמטרה (Ends) ולא רק כדרך (Ways) להשגת ביטחון, כלומר רואות בה מרכיב מרכזי בביטחון הלאומי בפני עצמה ומרחיבות ומעמיקות בה בהקשר לשגשוג כלכלי וביטחון כאחד. בכך הן שונות מהותית מהאסטרטגיות של ישראל, שאף כי הטכנולוגיה נתפסת בה כמרכיב משמעותי בביטחון הלאומי, המדינה אינה מגדירה אותה כיעד בפני עצמו אלא כדרך (למעט בתחום הסייבר, שם אכן יש לישראל טביעת רגל גלובלית כבדת משקל).

שתי האסטרטגיות הזרות גם מפרטות את הדרכים (Ways) לקידום הטכנולוגיה בתחומי הביטחון הלאומי, לדוגמה חיזוק הקשר בין משרד הביטחון, התעשיות והאקדמיה, שיתופי פעולה פנים־מדינתיים וחוץ־מדינתיים, הקמת מרכזי חדשנות ותוכניות האצה טכנולוגיות ביטחוניות, פיתוח ידע בחזית הטכנולוגיה ושימוש בו לחיזוק שיתופי פעולה וקשרים ביטחוניים לצד שמירה על הידע המתקדם הייחודי, יצוא ביטחוני, הגדרת ׳לפתח או לרכוש׳ ועוד. שתי האסטרטגיות גם מפרטות את האמצעים (Means) לקידום הטכנולוגיה, לדוגמה פיתוח, טיפוח וניוד כוח אדם טכנולוגי והשקעות תקציביות נכבדות במדע ובטכנולוגיה. לעומתן האסטרטגיות הישראליות ברובד הביטחון הלאומי וברובד הביטחוני־צבאי, כל אחת ברמתה, מציגות באופן חלקי מאוד את דרכי הפעולה למימוש הטכנולוגיה כחלק מהחשיבה האסטרטגית הכוללת, דבר המהווה פער חשיבתי ותפיסתי בקשר ובחיבור בין היעדים והאמצעים. פער זה מייצר אסטרטגיות לא שלמות ולא מאוזנות ולוקה בביטוי בכתובים של מקומה המרכזי של הטכנולוגיה כחלק מאותן אסטרטגיות. לעומת זאת, אסטרטגיית הגנת הסייבר נוגעת, כפי שהוצג, בדרכים להשגת היתרון הטכנולוגי, אך בפירוש לא בהיקף המופיע באסטרטגיות הזרות.

באסטרטגיות הזרות יש הסתכלות רחבה על מקומה של הטכנולוגיה בכל שרשרת הערך שלה (השכלה טכנולוגית ומדעית, כוח אדם טכנולוגי, גופי מחקר ופיתוח) ובאקוסיסטם השלם לקידומה ולמימושה, וכיצד יש לפעול על מנת לשמור על ההובלה הטכנולוגית לאורך זמן. חסרונו של דיון רחב כזה בולט מאוד בשתי האסטרטגיות הישראליות של הביטחון הלאומי ושל צה״ל. בשונה מהן, אסטרטגיית הגנת הסייבר דומה לאלו הזרות מבחינת השלם שהיא דנה בו בעולם הטכנולוגי, כלומר יעדים, דרכים ואמצעים ובהסתכלות כוללת ושלמה, אך גם היא אינה מגיעה לאותו היקף ופירוט של שתי האסטרטגיות הלאומיות של ארצות הברית ובריטניה.

זאת ועוד, האסטרטגיות הזרות עוסקות בהרחבה גם במשאבים (תקציבים, כוח אדם, הקמת גופים ומסגרות ועוד) על מנת לממש את דרכי הפעולה לחיזוק היתרון הטכנולוגי, דבר שגם הוא חסר בשתי האסטרטגיות הישראליות הראשונות ובאופן חלקי גם בזו של הסייבר (לא מוזכרים תקציבים ומספרים). כמו כן נושא שיתוף הפעולה המדעי והטכנולוגי של מדינות אלה ביניהן לבין עצמן ועם מדינות נוספות מהווה מרכיב משמעותי בתפיסה האסטרטגית, אך הוא נעדר מהאסטרטגיות הישראליות כמעט לחלוטין.

לסיכום, באשר לשאלת המימוש בפועל של האמור באסטרטגיות אלה בנושא הטכנולוגי, ראוי לציין כי מתוך האסטרטגיות הלאומיות נגזרים מסמכי עבודה למימוש בפועל של היתרון הטכנולוגי, כדוגמת "ביטחון לאומי באמצעות טכנולוגיה" בבריטניה (Ministry of Defence, 2012), ו"אסטרטגיית ההיסט השלישית" בארצות הברית (שמואל, 2016), אשר ממומשים במשרד הביטחון ובגופים השונים.

חלק שלישי: דיון

כללי

הטכנולוגיה היא אחד המרכיבים המרכזיים בתפיסות ביטחון ובאסטרטגיות מודרניות בעשורים האחרונים, בעיקר בעולם המערבי, ככלי מרכזי לשמירת היתרון האיכותי היחסי. מבט על אסטרטגיה ביטחונית מגלה כי הטכנולוגיה היא באופן טבעי אחד האמצעים (Means) למימוש היעדים הביטחוניים, אך במובנים רבים היא יכולה להשפיע באופן מהותי על הדרכים (Ways) למימוש היעדים. למשל, מערכת כיפת ברזל אינה רק אמצעי להתמודדות עם איום רקטות (Means), אלא בעצם קיומה והצלחתה ביירוט שיעור נכבד של רקטות היא משנה את אסטרטגיית הלחימה של צה"ל במערכה לאסטרטגיה מגננתית (Ways). ואף יותר מכך: הטכנולוגיה יכולה להשפיע גם על היעדים עצמם (Ends). לדוגמה, עם כניסתו של העולם הביטחוני לפעילות בממד הסייבר, שהוא מרחב טכנולוגי בבסיסו, השתנו בעקבות כניסת הטכנולוגיה החדשה גם היעדים הביטחוניים ולא רק הדרכים להשגתם, כמו למשל יעד ביטחוני חדש של הגנה על תשתיות חיוניות מפני תקיפתן בסייבר. בבחינה ברובד נמוך יותר הדן באסטרטגיה טכנולוגית כשלעצמה, ניתן לראות את שימור היתרון האיכותי כיעד (Ends) של הטכנולוגיה שאותה אנו רוצים לפתח ולהשיג, ולשם כך נדרשים שיטות פיתוח, תעדוף, שיתופי פעולה, החלטות פיתוח עצמי או רכש/יבוא חיצוני (Make or Buy) ודרכים (Ways) נוספות, כמו גם תקציבים, תשתיות וכוח אדם (Means).

פערים באסטרטגיות הביטחון הישראליות

כפי שהראינו בחלקים הקודמים, תפיסות הביטחון האסטרטגיות הישראליות בהחלט רואות גם היום בטכנולוגיה מרכיב חשוב ומרכזי ביצירת היתרון האיכותי היחסי ובשימורו, מרכיב שהוא אחד הגורמים העיקריים בעוצמה הביטחונית הישראלית הן ברובד הביטחון הלאומי והן ברובד הביטחוני הישיר, לא רק בפועל אלא גם בביטוי שניתן לכך בכתובים. בהתאם קיים פירוט נרחב על "מה" שנדרש מהטכנולוגיה, תוך התייחסות ליכולות הטכנולוגיות הנדרשות.

עם זאת באסטרטגיות, בדגש על זו של הביטחון הלאומי ואסטרטגיית צה"ל, אין התייחסות מספקת ל"איך" משמרים את היתרון הטכנולוגי, מעמיקים אותו ומקדמים אותו, כפי שהיינו מצפים מאסטרטגיות השמות דגש על חשיבותה של הטכנולוגיה ובייחוד בהשוואה לנושאים אחרים הנדונים בהן, כפי שהראינו קודם לכן. חוסר זה אומנם קטן יותר באסטרטגיית הגנת הסייבר המתייחסת לכך, אך גם היא אינה מגיעה לרמת הפירוט המופיעה באסטרטגיות הלאומיות של ארצות הברית ובריטניה. שלוש האסטרטגיות הישראליות, כל אחת בתחומה ועם ההבדלים ביניהם, אינן מעמיקות בתחומים החיוניים לטווח ארוך שיש להשקיע בהם: מהי המדיניות הנכונה להעצמת היתרון היחסי ואיך מתגברים על חולשות בתחום; מדיניות מכוונת לפיתוח עצמי לעומת הישענות על טכנולוגיות מעצמתיות; היכן נכון להישען על טכנולוגיות אזרחיות ומתי יש להעצים את יכולות הפיתוח הפנימיות של מערכת הביטחון או של התעשיות הביטחוניות, וההבדלים ביניהן; או כיצד מתרגמים יתרון זה לעוצמה צבאית (במילים אחרות — העמקה בתהליך בניין הכוח הלאומי והביטחוני).

בהקשר לאסטרטגיית הביטחון הלאומי חסרה התייחסות לאקוסיסטם השלם של טיפוח הון אנושי מדעי־טכנולוגי, מקומה של האקדמיה בבניין הכוח הלאומי הזה וכיצד לחזק אותה בראייה לאומית כוללת מהיבט של ביטחון לאומי, השקעות במו"פ וכדומה, ועד יצירת העוצמה הצבאית. בהקשר זה נדרשת גם התייחסות לקידום המחקר המדעי והטכנולוגיה בהיבט האזרחי כמרכיב בביטחון הלאומי, בשמירה על היתרון האזרחי־כלכלי ועל תחרותיות בשוק העולמי, כמו גם הרחבה והקלה על המעבר בין המגזר הציבורי והביטחוני למגזר האזרחי. פערים אלו בולטים בייחוד על רקע ההתייחסויות המעמיקות של אסטרטגיות הביטחון הלאומי של ארצות הברית ובריטניה לפן הטכנולוגי באופן כה מקיף. מתמיה שדווקא במדינת ישראל, שהממד המדעי טכנולוגי שלה הוא עמוד תווך בכלכלתה, בעוצמתה הצבאית ובעוצמתה המדינית כיום בעולם, חסרה התייחסות מקיפה לטכנולוגיה במסגרת האסטרטגיות הלאומיות, או לחלופין אסטרטגיה טכנולוגית לאומית המאושרת על ידי הממשלה.

האם המעשה חשוב מהתאוריה?

יש שימעיטו בחשיבות אסטרטגיה כזו וידבקו במעשה, מתוך טענה שישראל הצליחה ליצור את עמוד התווך המדעי־טכנולוגי שלה גם ללא אסטרטגיה כתובה ברורה, כפי שגם תפיסת הביטחון הלאומי שלה אינה מאוגדת במסגרת כתובה מחייבת. אך אם כך הדבר, מדוע טורחים הגופים השונים לכתוב אסטרטגיה? משום שיש חשיבות לתפיסות אסטרטגיות כתובות בכלל, ובפרט לתפיסות הביטחון הפורמליות. ראשית, הן מהוות מסגרת מאגדת לכל העוסקים במלאכת התכנון האופרטיבי ובניין הכוח ולכל השותפים למאמץ הביטחוני בכך שהן משרטטות באופן קוהרנטי וברור את היעדים, את הדרכים למימושם ואת האמצעים להגשמתם, כך שכל אחד מהעושים במלאכה יכול לדעת היכן למקד מאמץ ומה חלקו בעשייה. שנית, לאסטרטגיות אלו חשיבות גבוהה במיוחד בהחלטות לא רק על מה עושים ובמה מתמקדים, אלא לא פחות חשוב מכך — על מה מוותרים. פערים באחד מהמרכיבים באסטרטגיה עלולים להוביל לביזור מאמץ מיותר, להקדשת משאבים ומאמצים לא ממוקדים ולטעויות קריטיות בכיוונים הנדרשים. כמו כן, לאסטרטגיות יש השפעה בפועל על הקצאת משאבים, כוח אדם וקביעת סדרי העדיפויות. בדיוק כפי שנדרש לקבל החלטות על מה לא כלול באסטרטגיה ומה לא נדרש עקב משאבים מוגבלים, כך יש חשיבות רבה למדיניות חלוקת המשאבים במה שאמור להיעשות. לבסוף, האסטרטגיות משקפות בכתובים את אופן ועומק החשיבה של צמרת קבלת ההחלטות במדינה ובמערכת הביטחון.

ראש ממשלת ישראל הראשון, דוד בן־גוריון, שלא היה לו רקע טכנולוגי פורמלי, ראה במדע ובטכנולוגיה את הבסיס לתקומת ישראל ומרכיב מרכזי בביטחונה הלאומי בהקשר הרחב ובהקשר הצבאי המיידי.

אם כן, החשיבות של פיתוח ושל כתיבת אסטרטגיות לאומיות ברורה והפן הטכנולוגי אינו יוצא דופן. מן האופן שבו מופיע הנושא הטכנולוגי כיום באסטרטגיות הביטחוניות עולה כי היתרון הטכנולוגי נחשב בעיקר אמצעי המשמש להרתעת האויבים ולהכרעתם בעת הצורך, אך הוא אינו נתפס כיעד אסטרטגי בפני עצמו, שמחייב בניית אסטרטגיה לשמירתו. יתרה מכך, נוצר הרושם כי הנחה סמויה באסטרטגיות היא שטיפוח ושימור היתרון הטכנולוגי מובנים מאליהם ויתבצעו בכל מקרה וכדרך אגב — רושם הבולט בייחוד באסטרטגיית צה״ל. ייתכן כי רושם זה של מקבלי ההחלטות נובע מהיותה של ישראל מדינה מתקדמת טכנולוגית בעלת תעשייה טכנולוגית חזקה, שבה השוק האזרחי מנביט ומקדם טכנולוגיות רבות, לרוב ליצוא, המשפיעות גם על המערכת הצבאית שנהנית מפירות התעשייה. רושם זה מתחזק לאור הפסיחה בתפיסת הביטחון של ישראל על הקשר בין הטכנולוגיה בשוק האזרחי (ככלי לשמירה על היתרון האזרחי־כלכלי) לבין היתרון הטכנולוגי הביטחוני (נזכיר כי בתפיסת הביטחון הלאומית האמריקאית והבריטית קשר זה מפורט ומודגש).

מנהיגות אזרחית אסטרטגית

האם לעובדה שמקבלי ההחלטות בצמרת הביטחונית הישראלית הם לרוב אנשי מבצעים ומעשה, רובם ללא הכשרה טכנולוגית או מדעית, עשוי להיות קשר הדוק להיעדרה היחסי של הטכנולוגיה מן האסטרטגיות? ייתכן, לא בהכרח. ראש ממשלת ישראל הראשון, דוד בן־גוריון, שלא היה לו רקע טכנולוגי פורמלי, ראה במדע ובטכנולוגיה את הבסיס לתקומת ישראל ומרכיב מרכזי בביטחונה הלאומי בהקשר הרחב ובהקשר הצבאי המיידי. הוא פעל בנחישות לקידומם ואף ביטא זאת באופן ברור בכתב ובמעשה (בן־ישראל, 2013). ניתן לומר שהמקום המרכזי שהוא נתן למדענים במערכת הביטחון ולמעורבותו האישית בהקמת המטה המדעי וחיל המדע בצה״ל עוד בעת מלחמת העצמאות (בראל, 2009) היה גורם מרכזי בהפיכתה של הטכנולוגיה למרכיב כה משמעותי בביטחון הלאומי של ישראל (מתניה, 2022).

אך גם אם בן־גוריון היה מאבות הקביעה כי המעשה המדעי־טכנולוגי הוא מרכיב כה מהותי בבניין העוצמה הישראלית, הוא לא היה היחיד, ומקבלי החלטות ומובילים אסטרטגיים נוספים בלטו בזיקתם למדע ולטכנולוגיה, בהבנתם את חשיבותם ובהחלטות שקיבלו בנושא. שמעון פרס (מחקר גרעין, לדוגמה), יצחק רבין (למשל במימוש חזון לוויינות על אף עמדה מתנגדת של צה״ל, וזאת מתוך ראייה ארוכת טווח של המשמעות המדינית הכוללת של התחום לביטחון הלאומי), משה ארנס (בייחוד עצמאות מו״פ ביטחוני) ובנימין נתניהו (למשל בתחום הסייבר, שאותו דחף כך שישראל תהיה בו מובילה עולמית לא רק במדד יחסי אלא באופן מוחלט — תחום טכנולוגי ראשון שבו ישראל הפכה למובילה כזו (מתניה ורפפורט, 2021, עמ׳ 12), וזאת תוך כך שלעיתים הוא נתפס כמשוגע לדבר) — כולם היו בעלי סקרנות וצימאון להכיר את התחום הטכנולוגי או בעלי זיקה טכנולוגית, או שפיתחו אינטואיציה טכנולוגית לאורך שנים של חיכוך עם התחום הטכנולוגי, מה שאפשר להם לשקול ולקבל החלטות בתחומים טכנולוגיים ביטחוניים.

עם זאת, מרבית ההחלטות הללו היו נקודתיות ובנושא מסוים, אשר חייבו בין היתר השקעת משאבים ותקציבי עתק ברמה הלאומית, ולכן חייבו החלטה עקרונית של בכירי המערכת המדינית והביטחונית. הנקודתיות שבהחלטות אלה הן היוצא מן הכלל שמעיד על הכלל — היעדר אסטרטגיה רחבה וכוללת בנושא הטכנולוגי.

הצורך במנהיגות עם זיקה טכנולוגית

תופעה נוספת שמעוררת תהייה בהקשר של מקומה העתידי של הטכנולוגיה בישראל היא מיעוטם, עד כדי היעדרות כמעט מוחלטת, של טכנולוגים או אנשים בעלי זיקה או הבנה טכנולוגית רצינית משולחנות קבלת ההחלטות האסטרטגיות במדינה שהטכנולוגיה היא מרכיב מרכזי בכלכלתה ובביטחונה הלאומי. במערכת הביטחון בפרט יש לכך השלכות על עומק המחשבה האסטרטגית בנושא, על היכולת לקבל החלטות חורצות גורל בתחום בניין הכוח הטכנולוגי, בהחלטה על סדרי עדיפויות, על ניצול ועל הקצאה של משאבים. כמה מהיושבים לצד שולחן המטכ"ל של צה"ל הם בעלי הבנה או זיקה לטכנולוגיה ולמימושה הנכון בבניין הכוח ובהפעלתו? עד כמה מפקדי זרועות שאין להם זיקה או ניסיון טכנולוגי יכולים להבין לעומק שינויים שטכנולוגיות משבשות יכולות להכניס לממדי הלחימה השונים ולשנותם באופן מהותי, ולהכין בשל כך את הזרועות השונות לזמנים משתנים, שבהם כנראה פלטפורמות מאוישות לאו דווקא יהיו העיקריות? כמה מראשי משרד הביטחון, למעט ראש מפא"ת (המנהל למחקר ולפיתוח אמצעי לחימה ותשתית טכנולוגית), הם בעלי יכולת קבלת החלטות בתחום הטכנולוגי? וכמה במערכת הממשלתית?

זו אולי אחת מהתובנות שיש להסיק ממאמר זה. מן הראוי ואף נחוץ שאלו האחראים על התפיסות האסטרטגיות של ישראל ועל ביטחונה הלאומי יבנו לאורך שנים זיקה ואינטואיציה טכנולוגית, מיוזמתם וגם על פי הנחיה, בהכשרות שהם עוברים.

אסטרטגיה טכנולוגית לישראל

עוד תובנה העולה ממאמר זה, ובפרט על בסיס ההשוואה לאסטרטגיות ביטחון לאומיות של ארצות הברית ובריטניה, היא שעל הסביבה האסטרטגית הישראלית לגבש תפיסת ביטחון לאומי טכנולוגית מקיפה כמסמך נלווה למסמכים האסטרטגיים הקיימים, לגיבוש אסטרטגיית־על לצורך המשך העצמת המרכיב המדעי־טכנולוגי בתפיסת הביטחון הלאומי ולשימור ולטיפוח היתרון האיכותי הטכנולוגי הישראלי כחלק מתפיסות הביטחון הרשמיות של המדינה.

אסטרטגיה זו צריכה להיות מקיפה, להתייחס לשמירה על היתרון הטכנולוגי הביטחוני והאזרחי כאל יעדים (Ends) מרכזיים ולקשור ביניהם לבין הדרכים (Ways) והאמצעים (Means) להשיגם. אסטרטגיה זו נדרשת להתייחס לסוגיות מרכזיות בנושא הטכנולוגי — גזרות וחלוקת אחריות באקוסיסטם הטכנולוגי האזרחי והביטחוני (למשל מי אחראי על פיתוח כוח אדם טכנולוגי במדינה, מוביל ומקבל את ההחלטות בנושא); איך נראה אותו אקוסיסטם שלם; איך מטפחים את כוח האדם הטכנולוגי במדינה (האזרחי והביטחוני); כיצד מייצרים בסיס מדעי וטכנולוגי; כיצד יוצרים שיתופי פעולה בין מערכת הביטחון, התעשיות והאקדמיה; כיצד מתרגמים את היתרון הטכנולוגי לעוצמה צבאית; מהם התקציבים הראויים להשקעה במחקר ופיתוח; מהו האיזון בין רכש אמצעי לחימה ישראליים לאמריקאיים ועוד. כל אלה בולטים מאוד בחסרונם באסטרטגיות הביטחוניות הקיימות כיום ומהווים בראייתנו מרכיב מכריע לשימור היתרון הטכנולוגי לאורך זמן.

נדרש לבחון את הטכנולוגיה בראייה אסטרטגית כמטרה וכיעד בפני עצמו, ולא רק כאמצעי להגשמת היעדים הלאומיים והצבאיים.

סיכום

מאז קום המדינה מהווה היתרון האיכותי היחסי, ובתוכו המרכיב הטכנולוגי, מרכיב מרכזי וחשוב בתפיסת הביטחון של מדינת ישראל. במאמר זה בחנו כיצד הטכנולוגיה באה לידי ביטוי פורמלי בחשיבה הביטחונית האסטרטגית של מדינת ישראל בעשורים האחרונים באמצעות ניתוח מסמכים ביטחוניים רשמיים ורשמיים למחצה, ואם הביטוי הפורמלי של חשיבה זו עולה בקנה אחד עם חשיבותה של הטכנולוגיה בתפיסה הביטחונית. הסיבה שבחרנו דווקא בפרספקטיבה זו לבחינת השאלה היא משום שלאסטרטגיות כאלו יש השפעה משמעותית על עתיד התחום בעשורים הקרובים, על יצירת מוטיבציה מתאימה אצל כל הנוגעים בדבר, על כוונן אסטרטגי ומיקוד של ההחלטות (מה כן ומה לא), על המאמצים, העדיפויות, הבחירות והמשאבים, על סימון משותף של וקטור לאומי ועל התייחסות קבועה למרכיב חיוני זה ביתרונה האיכותי של ישראל. כפי שהבהרנו, פרספקטיבה זו אינה היחידה וגם אינה מלאה, אך היא ייחודית בתובנות העולות ממנה ושאותן ביכולתה להאיר.

לשם כך התמקדנו בשלוש אסטרטגיות לאומיות שפורסמו בשני העשורים האחרונים: אסטרטגיית הביטחון הלאומי (ועדת מרידור מ־2006, מסמך מ־2018), שדנה ברובד העליון של הביטחון הלאומי, גם אם מזווית צרה של ביטחון וללא התייחסות לחוסן חברתי או עוצמה כלכלית, למשל; אסטרטגיית צה״ל (2018) הנמצאת ברובד הביטחוני־צבאי, קומה מתחת לרובד הלאומי; והאסטרטגיה הישראלית להגנת הסייבר (האסטרטגיה הישראלית להגנת הסייבר, 2017), שמצומצמת לנושא לאומי יחיד אך דנה בו הן ברובד של הביטחון הלאומי והן ברובד הביטחוני־צבאי הישיר. בחינת האסטרטגיות בוצעה ממספר כיוונים. ראשית, ניתוח מקומה של הטכנולוגיה במסמכים עצמם מול מה שהיינו מצפים לראות מנייר אסטרטגי, ובייחוד בהשוואה לתחומים אחרים בו (מבט נורמטיבי); ניתוח השוואתי של מקומה של הטכנולוגיה בכל אחת מהן; וניתוח השוואתי מול שתי אסטרטגיות ביטחון לאומי זרות — זו של ארצות הברית וזו של בריטניה.

מהניתוחים השונים עולה התובנה המרכזית של מאמר זה, הגורסת כי קיים פער משמעותי בין הביטוי הפורמלי הקיים בבירור של הטכנולוגיה כגורם בולט בעוצמה הביטחונית ישראלית, בחשיבותה ובמרכזיותה, לבין הפירוט הפורמלי על הדרכים להשגתה ולשימורה. בהיבט אסטרטגי פער זה בולט במיוחד בהיעדרה של אסטרטגיה מקיפה לשמירת היתרון הטכנולוגי היחסי, העמקתו ותרגומו לעוצמה צבאית וביטחונית בפועל ולאורך זמן. פער זה יכול לנבוע בראייתנו ממספר גורמים, כפי שהוצגו בפרק הדיון, הבולטים ביניהם הם ראיית הטכנולוגיה כאמצעי ולא כמטרה, והנחה סמויה כי הטכנולוגיה היא בבחינת ״מובנת מאליה״, ייתכן כתוצאה מהשפעות השוק האזרחי הטכנולוגי המתקדם בארץ או מחוסר הבנה מעמיקה של בכירי המערכת הלאומית והביטחונית בנושא.

בראייתנו, כפי שפורט לעיל, נדרש לבחון את הטכנולוגיה בראייה אסטרטגית כמטרה וכיעד בפני עצמו ולא רק כאמצעי להגשמת היעדים הלאומיים והצבאיים, וזאת לאור מרכזיותה וחשיבותה לביטחון הלאומי בראייה רחבה וכוללת, לרבות השפעתה על הכלכלה, ולא רק באופן ישיר על הביטחון. בחינה כזו מחייבת ניסוח של אסטרטגיה כוללת לשמירה ולטיפוח היתרון האיכותי הטכנולוגי הישראלי כחלק מתפיסות הביטחון הרשמיות של המדינה, כמרכיב חיוני לשימור היתרון הטכנולוגי לאורך זמן ולשימור העוצמה הביטחונית הלאומית.

אביתר מתניה הוא פרופסור בבית הספר למדע המדינה, ממשל ויחסים בינלאומיים באוניברסיטת תל אביב. הוא מכהן שם כראש התוכנית לתואר שני בלימודי ביטחון וכראש התוכנית לתואר שני בלימודי פוליטיקה, סייבר וממשל, וכן כראש המרכז לחקר מדיניות ואסטרטגיית אוויר וחלל. בין השנים 2012-2018 הקים את מערך הסייבר הלאומי ועמד בראשו. eviatarm@tauex.tau.ac.il

אורן פודהורצר וניר דניאל הם סטודנטים חוקרים בתוכנית לתואר שני בלימודי ביטחון באוניברסיטת תל אביב.

מקורות

אסטרטגיית צה״ל (2018). אתר צה״ל, https://bit.ly/3enE0yW

בן־ישראל, י׳ (1997). תורת היחסות של בניין הכוח. **מערכות, 352-353**, 33-42. https://bit.ly/3LxQMGm

בן־ישראל, י׳ (2013). **תפיסת הביטחון של ישראל**. האוניברסיטה המשודרת, מודן הוצאה לאור, משרד הביטחון — ההוצאה לאור.

בן ישראל, י׳, מתניה, א׳ ופרידמן, ל׳ (עורכים) (2020). **המיזם הלאומי למערכות נבונות בטוחות להעצמת הביטחון הלאומי והחוסן המדעי־טכנולוגי: אסטרטגיה לאומית לישראל — דו״ח מיוחד לראש הממשלה.** אוניברסיטת תל אביב, סדנת יובל נאמן למדע טכנולוגיה וביטחון. https://bit.ly/3QizS0g

בראל, א׳ (2009). המנהיג, המדענים והמלחמה: דוד בן־גוריון והקמת חיל המדע. **ישראל — כתב עת לחקר הציונות ומדינת ישראל — היסטוריה, תרבות חברה, 15**, 67-92. https://bit.ly/3x1lofE

חמו, י׳ (2016). בניין הכוח כמערכה — על אופטימיזציה ואסטרטגיה. **בין הקטבים, 6**: בניין הכוח — חלק א׳, 11-38. https://bit.ly/3CVfvU4

מערך הסייבר הלאומי (2017). **האסטרטגיה הישראלית להגנת הסייבר**. https://bit.ly/3PPkMzi

מרידור, ד׳ ואלדדי, ר׳ (2018). **תפיסת הביטחון של ישראל — דו״ח הוועדה לגיבוש תפיסת הביטחון (ועדת מרידור) ובחינתו בחלוף עשור**. מזכר 182, המכון למחקרי ביטחון לאומי. https://bit.ly/3CTwsOK

מתניה, א׳ (2022). האבולוציה של שירות החובה בישראל: מבניין המיליציה לעמוד התווך של העליונות הצבאית־טכנולוגית. **עדכן אסטרטגי, 25** (2), 12-3.

מתניה, א׳ ורפפורט, ע׳ (2021). **סייברמאניה — כיצד הפכה ישראל לכוח עולמי בזירה שמעצבת את עתיד האנושות**. כנרת זמורה דביר.

פינקל, מ׳ ופרידמן, י׳ (2016). שבעה עשורים ליתרון האיכותי של צה״ל — השתנות התפיסה לגבי מהות היתרון האיכותי של צה״ל על אויביו, השתנות היתרון האיכותי בפועל וכיוונים לעתיד. **בין הקטבים, 9**, 43-66. https://bit.ly/3q94bfw

עילם, ע׳ (2009). **קשת עילם: הטכנולוגיה המתקדמת — סוד העוצמה הישראלית**. ידיעות אחרונות וספרי חמד — משכל.

עמידרור, י׳ (2020). תפיסת הביטחון הלאומי של ישראל. **בין הקטבים, 28-30**, 19-34. https://bit.ly/3AOBV6S

שמואל, ש׳ (2016, 1 בנובמבר). **המסע לאסטרטגיית ההיסט השלישית במערכת הביטחון האמריקאית**. מרכז דדו. https://bit.ly/3qdkBne

הערות

1 למען השלמות והדיוק יצוין שחלקים מסוימים באסטרטגיה הישראלית להגנת הסייבר הדורשים החלטה של ממשלת ישראל לצורך הקמה או ביצוע אושרו על ידה במספר הזדמנויות, ובייחוד בהחלטותיה 2443 ו־2444 מיום 15 בפברואר 2015.

2 למען הגילוי הנאות נציין שאחד ממחברי המאמר (אביתר מתניה) היה מי שהוביל את פיתוחה וכתיבתה של אסטרטגיית הסייבר הישראלית במסגרת תפקידו כמקים וכראש מערך הסייבר הלאומי.

3 כפי שמצוין בעמ׳ 2 במסמך: "A belief emerged, among many, that American power would be unchallenged and self–sustaining. The United States began to drift. We experienced a crisis of confidence and surrendered our advantages in key areas. As we took our political, economic, and military advantages for granted, other actors steadily implemented their long-term plans to challenge America and to advance agendas opposed to the United States, our allies, and our partners."

4 רשת NSIB – National Security Innovation Base — אמריקאית של ידע, יכולות ואנשים, כולל אקדמיה, מעבדות לאומיות והמגזר הפרטי, ההופכת רעיונות לחדשנות ותגליות למוצרים מסחריים ולחברות.

5 "We also incorrectly believed that technology could compensate for our reduced capacity —for the ability to field enough forces to prevail militarily, consolidate our gains, and achieve our desired political ends. We convinced ourselves that all wars would be fought and won quickly, from stand-off distances and with minimal casualties."

6 "We will create a new, cross-government Emerging Technology and Innovation Analysis Cell, with close links to the private sector and academia to ensure that we identify these opportunities"

Adamsky, D. (2017). The Israeli Odyssey toward its national cyber security strategy. *The Washington Quarterly, 40*(2), 113-127, DOI: 10.1080/0163660X.2017.1328928

Cancian, M. F. (2017, October 6). Formulating national security strategy: Past experience and future choices. Center for Strategic and International Studies (CSIS). https://bit.ly/3TGUItp

HM Government(2015). *National security strategy and strategic defense and security review 2015: A secure and prosperous United Kingdom*. https://bit.ly/2vlh1hb

Ministry of Defence (2012). *National Security through technology: Technology, equipment, and support for UK defence and security*. https://bit.ly/3RgJqdf

Rounds, R. K., III. (2019). *Sourcing air supremacy: Determinants of change in the international fighter jet network*. [A Dissertation submitted to the Faculty of the Graduate School of Arts and Sciences of Georgetown University in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Government]. https://bit.ly/3cNRDHj

The White House (2017). *National security strategy of the United States of America*. https://bit.ly/3e41d95

Yarger, H. R. (2006). Toward a theory of strategy: Art Lykke and the US Army War College strategy model, in J. B. Bartholomees, Jr. (Ed.), *U.S. Army War College guide to national security policy and strategy*, 2nd Edition (pp. 107-114). https://bit.ly/3Rh5ogP