

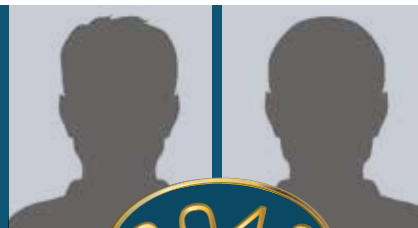
טכנולוגיה בשדה



יש חשיבות מכרעת לטכנולוגיה בעיצוב שדה הקרב העתידי. השילוב בין עולם המו"פ הצבאי לעולם הטכנולוגי האזרחי, יהיה זה שיביא לניצחון

כאשר מדמיינים את שדה הקרב כיום, עולה תמונה של לוחמים רצים, טנקים מתקדמים ודחפורי D9 בסיוע כוחות הנדסה מפלסים דרך לכוחות. בעוד 30 שנה ייתכן ותדמיינו דבר אחר לגמרי: נשקים אוטונומיים (לייזר או קלאסיים), המזהים אויב ופוגעים בו בשבריר שנייה; רחפנים שמטילים פצצות על עמדות אויב ומצלמים את שדה הקרב ממעוף הציפור; לוחמים בעלי יכולות ראייה וחישה עלי אנושיות בזכות מערכות שמחוברות לגופם. חלק גדול מהקרב יתנהל באמצעות תקיפות סייבר על הכלים האוטונומיים, ושימוש בפולסים (רפקים) אלקטרומגנטיים – EMP – כדי להשמיד את הרכיבים האלקטרוניים של האויב באופן רחביהיקף. השוני המהותי בין שדה הקרב העתידי המדומיין לזה הנוכחי, הוא המרכזיות של הטכנולוגיה המתקדמת בה נעשה שימוש. המגמה של שימוש בטכנולוגיה בשדה הקרב הולכת ומתרחבת.

איתמר, איתן,
ניר ואלישע
חניכי תוכנית
"תלפיות" מחזור ל"ז



הקרב העתידי



מל"ט בפעולה. המהפכה האוטונומית נמצאת היום בשיאה: מל"טים המצוידים במערכות זיהוי וירי עצמאיות שרק מחכות להחיצת כפתור כדי להשמיד את האויב (צילום: מור צידון)

כלים אוטונומיים

המהפכה האוטונומית נמצאת היום בשיאה: ממכונות אוטונומיות שהשוק האזרחי מציע ומסוגלות לנהוג ברמת דיוק שבני אדם לא מכירים, דרך רחפנים ביתיים המניידים עצמם למיקומים מוגדרים, ועד מל"טים בעולם המצוידים במערכות זיהוי וירי עצמאיות שרק מחכות להחיצת כפתור כדי להשמיד את האויב. העלויות ההולכות וקטנות מעוררות ומפשטות את השימוש במערכות אוטונומיות ונשלטות מרחוק. מהפכה זו דורשת שילוב של יכולות חישוב מתקדמות וזעירות, אלגוריתמים ומנגנוני למידה מתקדמים, וסוללות מתקדמות המאפשרות זמני הפעלה משופרים וטווחי הפעלה משופרים – יכולות המתפתחות כיום בעולם האזרחי, עבור סמארטפונים והוברבורדים (גלשני ריחוף).

אנחנו ממכנים כל מה שניתן, מוסיפים מחשבים ויחידות עיבוד לרכיבים ממוכנים ואף נותנים אוטונומיה ברמות שונות למערכות הממוחשבות. ניתן לראות זאת בשוק האזרחי בכל מקום, ותהליך בולט לדוגמה הוא של המכונית עם תיבת ההילוכים הידנית של המאה ה-20, שהתפתחה עד למכוניות אוטונומיות שלא צריכות בקרה אנושית דוגמת Waymo או מובילאיי, הנמצאות כעת בשלבי פיתוח אחרונים.

במאמר זה נסקור כמה מערכים טכנולוגיים, שלדעתנו עשויים לעצב מחדש את תמונת המלחמה העתידית: כלים אוטונומיים, העצמת אנוש, סייבר, נשק אלקטרומגנטי ופ"ש (פיקוד ושליטה) מתקדם. ננסה לגרות את הדמיון במחשבה כיצד הכיוונים שנראים לנו קריטיים כיום, עשויים להשפיע על האופן בו אנו נלחמים וחושבים על מלחמה, ולחזות את הבעיות המבצעיות איתן ניאלץ להתמודד.

סד"כ גדול אך זול, תקשה על האויב הפועל במתווה זה להישאר חשאי. בעידן בו מערכת אוטונומית מזהה לבד את האויב, ואז קובעת בעצמה האם מדובר במטרה לגיטימית לתקיפה ומקבלת אישור ירי מהיר, נחסך זמן ההתלבטות וניתן להגיע לדיוקים משמעותיים. זמן התקשורת והתיאום מפסיק להיות צוואר הבקבוק, ומרגע זיהוי האויב ניתן להשמירו תוך שניות בודדות. 3. אוטונומיות מאפשרת לבצע פעולות מורכבות בתיאום מוחלט, תוך שילוב יכולות רבות ומגוונות. פשיטה על בניין יכולה להתחיל מרכב אוטונומי עמוס חיישנים, המשלח לבניין רובוט סורק שמוזה ומפעיל בעצמו מל"ט להפצצת פתח בית. אחרי הסריקה הראשונה מתחילה התקפה באמצעות מיני-רחפנים, שמתפרשים ותוקפים כל איום בפנים – כשכל הנדרש מהמפעיל האנושי הוא לסמן את היעד ולבחור את אופן הפעולה. יכולות אלה מקטינות את כמות הלוחמים הנדרשת, ובכך מצמצמות אפשרות לנפגעים ונותנות למעט לוחמים מוכשרים ומנוסים להכריע את הקרב.

גם בטיפול באירועי טרור והגנת גבולות, מערכות אוטונומיות יכולות לשנות את אופי ההפעלה מהיסוד. במקום להציב כוח אדם מיומן באזורים מרכזיים ולהוביל לשחיקתו – ניתן לבצע מעקב רצוף, ערני ויעיל באזורי סיכון באמצעות מצלמות אבטחה, מיקרופונים ברחוב או תמונות לוויין, ולהקפיץ כוחות שיוצבו בסמוך כדי לטפל באירוע. כלים אוטונומיים יוכלו להתעדכן באופן מיידי בתמונת המצב, ולקבל החלטה על בסיס כל המידע תוך הבאה בחשבון את הסיכונים שבתקיפה במרחב אורבני. הם גם לא יחששו לסכן את עצמם ולהסתער על האויב.

פיקוד ושליטה מתקדמים

מכשול מרכזי איתו הצבאות מתמודדים הוא הצורך לדעת היכן החיילים בכל זמן נתון, עלימנת לתאם ביניהם. כבר כיום נכנסות לשימוש מערכות של שליטה ובקרה המאפשרות העברה של מידע טקטי וזיהוי של כוחות חברים, לדוגמה, צי"ד (צבא יבשה דיגיטלי).³

השוני המהותי בין שדה הקרב העתידי
המדומיין לזה הנוכחי, הוא המרכזיות של
הטכנולוגיה המתקדמת בה נעשה שימוש

2048

בעוד 30 שנה מערכות שליטה ובקרה אלה יהפכו מתקדמות יותר, ואנו מעריכים שנראה מערכת שליטה הקובעת בעצמה איזה אמל"ח להפעיל על איזו מטרה, מכוונת אותו באופן עצמאי ומפעילה. כאשר יכולת כלשהי יוצאת מכשירות, תדאג מערכת השליטה ליכולת חלופית או להפעלת אמצעי נגד. היא תאפשר למקבל ההחלטות לעסוק בעיקר ולא בפרטים הטכניים: יותר בחשיבה ובתכנון ופחות ביישום התוכניות ובחלוקת העבודה. מנגד, אנו לא מאמינים שבטווח זמן קצר ניתן יהיה להגיע למצב



רוב"ם (כלי רכב בלתי מאויש) בשטח פשיטה על בניין יכולה להתחיל מרכב אוטונומי עמוס חיישנים (צילום: תע"א)

כיום השימוש במערכות אוטונומיות מוגבל בחוק הבינלאומי, בשל החשש שמערכות אלה יוכלו, בגלל בעיה אלגוריתמית או באג בתוכנה, להפוך למכונות מלחמה הפוגעות בבלתי מעורבים. החששות מתחזקים, שכן רוב הקרבות המודרניים מתרחשים בתווך אורבני ובסביבה אזרחית. בעתיד, עם התחזקות השימוש בכלים אוטונומיים בעולם האזרחי, אמון החברה בכלים אלה יעלה. האמון בלחימה מבוססת כלים ומערכות אוטונומיות אולי אף יגבר על האמון הקיים בהפעלה מבצעית על בסיס אנשים, שכן היא נקיה מטעויות של עייפות, חוסר מקצועיות, חוסר ניסיון או הטיות פסיכולוגיות. בעולם בו מאמצים מערכות אוטונומיות, שדה הקרב והאיזמים שמציב האויב משתנים לחלוטין. ארגוני טרור יוכלו להיעזר בחשאינות כדי להקשות על תקיפת נגד, מדינות וארגונים יוכלו לחמוק מאחריות לפעולות לוחמניות. כמו כן כלים אוטונומיים יקלו באופן משמעותי על ביצוע פעולות טרור קטנות במרכזי אוכלוסין: בעזרת רחפנים מתאבדים עמוסי חומר נפץ,¹ מכוניות תופת אוטונומיות ובעזרת מערכות ירי עצמאיות.² פעולות שכדי לבצען יש צורך במפעיל בורד שאינו מסכן את חייו או נחשף בציבור, ללא תיאום מורכב או שכנוע מקדים הנדרש בהפעלת מחבל כיום. אויב בעל משאבים רבים יוכל לקנות לעצמו עוצמה צבאית גם ללא כוח פוליטי או תמיכת הציבור, ותקיפת סייבר משמעותית אחת יכולה לגרום לכוחות הצבא לירי דו"צ (דו צדדי), או גרוע מכך – לצעור חזרה ולתקוף את האוכלוסייה עליה הוא מגן. מנגד, גם אופי ההפעלה מתהפך:

1. מערכות לחימה אוטונומיות מאפשרות לקחת סיכונים רבים יותר, עקב נטרול החשש לחיי אדם. בכך הן משנות את ההפעלה של צבאות מערביים, המנהלים את מלחמתם תוך התחשבות בפגיעה בנפש, ולוקחים מקדמי בטיחות בעלויות גבוהות. עיקרון החתירה למגע יקבל דחיפה משמעותית כשנוכל לשלוח רחפנים ועירים להיכנס למבנה ולבצע פשיטה, או להיצמד לעמדות ממוגנות ולהתפוצץ בתוכן. הפעלה זאת מאתגרת את האויבים הנעלמים, ומציבה עליהם איום קל הרבה יותר למימוש.
2. מערכות אלה מאפשרות סגירת מעגל אש מהירה והגדלת קצב האש בסדרי גודל, מול אויב מורכב ונעלם הפועל בביזור משאבים. הפעלה של כלים אוטונומיים באופן מרחבי, על בסיס



ניסוי שילוח של טיל נגד טילים מסוג "חץ". יכולות חוזי מודיעיניות-טכנולוגיות, החל מלוינות מתקדמת ועד נחילי רחפנים ומל"טים, יאפשרו לנו לקבל תמונה מלאה של כל שדה הקרב בזמן אמת (צילום: ארנון בן ארי, לע"מ)

כמו כן ניתן יהיה לשרר בחזרה למוחו של החייל את הסביבה¹⁰ כאילו הוא רואה אותה דרך העיניים שלו. לטובת החיילים הספורים שבכל זאת יגיעו לשטח, נראה שינוי משמעותי בחויית הלוחם: כל חייל יוכל "להרגיש" את חברי הצוות האחרים, לראות באינפרא-אדום ולתקשר בעזרת צ'יפ שמחובר למרכז הדיבור שלו במוח (ולמרכזי השמיעה במוחות של שאר הכוח). הרפואה בצבא, כמו באזרחות, תתבסס על "תשתיות" בתוך הגוף, שיאפשרו ניטור מתמיד ושימוש בנתונים מפרקי זמן ארוכים. חיילים ייצאו לקרב כשהם מנוטרים על-ידי שבבים בכל גופם, ועם ערכות מיוחדות של "תיקון עצמי".

הטכנולוגיה הזאת תצמח, ככל הנראה,¹¹ מהתחום האזרחי. ארגונים צבאיים מתעסקים מעט מאוד במדע המוח, והשימושים באזרחות קרובים מספיק לצרכי הצבא עלי-מנת לספק מעבר יחסית פשוט. אנו רוצים להאמין שבעוד 30 שנה לצה"ל כבר יהיו לא מעט פרויקטים מבצעיים מסוג זה (גם אם ברמה ראשונית של מימוש הפוטנציאל בתחום), אך הדבר תלוי מאוד באופן בו נצליח להטמיע את הטכנולוגיות הללו.

סייבר

תקיפות סייבר, בשיח הצבאי והציבורי, הן כבר דבר שבשגרה בעשור האחרון. הפיתוח והשימוש ביכולות סייבר מתרחבים בקצב

של תוכנה המנהלת מלחמה באופן עצמאי לחלוטין. מקומם של אנשים ביכולות ניתוח, חשיבה יצירתית וקבלת החלטות במצבים מורכבים וחדשים לא יהיה קל להחלפה, גם תוך עשרות שנים ועם כוח חישוב אדיר.

יכולות חוזי מודיעיניות-טכנולוגיות, החל מלוינות מתקדמת ועד נחילי רחפנים ומל"טים, יאפשרו לנו לקבל תמונה מלאה של כל שדה הקרב בזמן אמת. סנסורים המאפשרים לראות דרך קירות, מצלמות תלת-מימד, תמונות תרמיות ושיטות מיוזג תמונות, יאפשרו לפזר את ערפל הקרב. שיטות שונות ימפו את מיקומי כוחות האויב וכוחותינו. טכנולוגיות העצמת אנוש יאפשרו למפקדים לקבל את המידע באופן חושי אינטואיטיבי. בעולם כזה יוכל לוחם יחיד לחוות את הקרב, ולהפעיל ישירות סד"כ אוטונומי בעל עוצמה גדודית או יותר. הגנרלים ישתמשו בטכנולוגיות מציאות מדומה כדי להביט ממעוף הציפור, או בגוף ראשון, בתמונת הקרב. הם יוכלו לתכנן את המערכה בזמן אמת ובקצב גבוה, ולגבש הערכה תוך ראייה רחבה אך גם היכרות אינטימית עם שדה הקרב.

כדי להיערך לשינוי באופן בו מתנהל הקרב, חשוב להמשיך במלאכת הדיגיטציה של אמצעי הלחימה, באיחודם לרשת שליטה אחת ובכניית תקנים המאפשרים הוספה מהירה של אמצעים חדשים. זאת תוך שמירה על הגנה בסייבר ול"א (לוחמה אלקטרונית). יש לייצר מרכזי מחקר ופיתוח שישכללו את המערכת המרכזית, ויבנו לה אופציות מורכבות יותר, בעיקר בתחום סגירת מעגלי אש.

העצמת אנוש

העצמת אנוש הוא העיסוק בשיפור האדם, לרוב באמצעים טכנולוגיים או ביולוגיים. שינויים ביחס שלנו לטכנולוגיה אפשר לראות כבר כיום – אנשים נעזרים במכשירי שמיעה שהופכים כמעט לחלק מהם, נכים משתמשים בכיסאות גלגלים חשמליים. יש הטוענים שבעתיד נוכל להרכיב עין שתוכל להגדיל את התמונה¹², ובשלב מתקדם יותר אולי גם להתקין לנו זיכרון נוסף¹³.

כבר היום יש טכנולוגיות בשלבי פיתוח מוקדמים, אך רוב התחום

האמון בלחימה מבוססת כלים ומערכות אוטונומיות אולי אף יגבר על האמון הקיים בהפעלה מבצעית על בסיס אנשים

2048

נמצא בשלבי הגייה. עם זאת, הדעה הרווחת¹⁴ היא שבי-30 השנים הקרובות נתחיל לראות שינויים מהותיים בחוויה האנושית. כיוון בולט הוא העצמת תכונות קיימות כמו: אורך חיים, כוח פיזי וקוגניציה¹⁵; ניצנים ראשונים של יצירת תכונות חדשות כמו להרגיש שדות מגנטיים¹⁶ והתממשקות עם הטכנולוגיות שסביבנו. לדוגמה, יהיה אפשר ליצור חייל רובוטי אליו מתחבר חייל אמיתי ממקום מרוחק, באמצעות קסדה המתחברת לראשו, ובכל פעם שהחייל (האנושי) ינסה להזיז את הרגל – תזוז הרגל של הרובוט ממקומה.¹⁷



מערכת צי"ד (צבא יבשה דיגיטלי). מעריכים שנראה מערכת שליטה הקובעת בעצמה איזה אמל"ח להפעיל על איזו מטרה, מכוונת אותו באופן עצמאי ומפעילת

היא בעלת פוטנציאל נזק קטסטרופלי, גם אם מדובר באויב פשוט עם חיבה למחשבים.

נשק אלקטרומגנטי

נשק פולסים אלקטרומגנטיים (EMP – Electromagnetic Pulse) הוא אמצעי שמאפשר ליצור גלים אלקטרומגנטיים עוצמתיים, שיכולים לפגוע במערכות אלקטרוניות מכל סוג. עוצמתו של כלי נשק כזה הולכת וגוברת עם הזמן באמצעות שני מערכים מרכזיים:

1. ההישענות ההולכת וגוברת של האנושות על אמצעים אלקטרוניים, מה שהופך את הצד המותקף לפגיע יותר ויותר.
2. המשך הפיתוח הטכנולוגי של נשקי EMP, שהופך אותם לאפקטיביים יותר ומתאימים יותר למתאר מבצעי. בנוסף, נשקים אלה מצמצמים את הפגיעה הישירה בחיי אדם, מה שהופך אותם לעדיפים כאשר יש צורך לפגוע באויב שמסתתר בתוך אוכלוסייה אזרחית, כמו בדרכי הפעולה של ארגוני הטרור.

נשק ה-EMP הראשון היה למעשה תופעת לוואי של פיצוץ גרעיני (NEMP – Nuclear EMP). הפיצוץ המכני ההרסני לוה בפולס אלקטרומגנטי חזק, שעוצמתו אדירה כאשר הפיצוץ מתרחש בגובה רב – מחוץ לאטמוספירה. ניסוי שנערך בארצות-הברית בשנת 1962 גילה כי טווח ההשפעה של הפולס הוא בסקאלה של למעלה מ-1000 ק"מ.¹³ ההערכה המקובלת היא שכיום, בזכות הבנה טובה יותר של התופעה ובזכות פצצות גרעיניות חזקות יותר, מעצמה יכולה להשתמש בפיצוץ גרעיני בשביל ליצור פגיעה משמעותית באלקטרוניקה ובתשתיות חשמל בסקאלה רבי-מדינית.

מלבד הפיצוץ הגרעיני, מדובר כיום גם על כלי נשק EMP שיוצרים פולסים אלקטרומגנטיים בטווח קצר הרבה יותר – מערכות ששולחות פולסים עוצמתיים מרוכזים (DEW – Directed Energy Weapon). מערכות כאלה נמצאות כיום בתהליכי מחקר ופיתוח באופן מוצהר בארצות-הברית,¹⁴ ברוסיה¹⁵ ובסין.¹⁶ ל-DEW יש פוטנציאל להיות נשק הרתעתי ומבצעי רבי-עוצמה. בניגוד לפיצוץ גרעיני בעל טווח ההשפעה האסטרטגי, DEW יתאים לשימוש טקטי בטווחים של קילומטרים בודדים ואף בטווחים של מאות מטרים. כלי נשק זה יאפשר פגיעה בתשתיות אויב, תוך

מסחר, וגם הדרג המדיני מבין את חשיבותו הגדולה של התחום: מיכולות איסוף המודיעין של ארצות-הברית שהודלפו לאחרונה,¹² ועד ההתקפות הלוחמניות נגד תשתיות אזרחיות שביצעה רוסיה נגד גיאורגיה תוך-כדי מלחמה.

לדעתנו, הסיבה המרכזית שעולם הסייבר יגדל בחשיבותו היא מהפכת הרשתיות. בשנים הקרובות אנחנו הולכים להתחבר יותר ויותר לרשת אחת גדולה. חזון המקרר שמומין כבר מצרכים, או המזגן שמחליט לחמם את הבית בטרם החזרה אליו, נראה קרוב מתמיד. לתופעה זאת מתייחסים בתור (IoT (Internet of Things, וצפויה לה פריחה בעיקר בעולם האזרחי.

עד היום, תקיפות סייבר היו מוגבלות בעיקר למכשירים אלקטרוניים מתקדמים כמו מחשבים פרטיים, שרתים וטלפונים חכמים. דרך פעולות אלה היה ניתן להשיג מידע על דואר אלקטרוני, לפגוע בתקשורת, להדליף מסמכים וכדומה. עם העלייה המשמעותית בכמות המכשירים שיש בהם מחשב קטן (שעונים, תנורים, מכוניות ובעתיד אולי אף אנשים) יוכלו צבאות להשתמש בתווך הסייבר לטובתם, ובהתאם גם להפיגע ממנו. איסוף המודיעין לגבי כוחות אויב או תופעות כמו "טרור היחידים", יהפוך קל הרבה יותר.

בדומה לסייבר, העוצמה של נשק EMP נשענת על התלות שלנו באלקטרוניקה. תלות זו ככל הנראה תתחזק עוד יותר בעתיד

למרכה הצער, השינוי בסכיבה משחק דווקא לטובת ארגוני גרילה וטרור. בעולם בו כל המכשירים שסביבנו מחוברים לרשת, יכולות סייבר מהוות סיכון בכל שלב בלחימה – לצבא ולאזרחים. ארגון טרור יוכל לשחק את המשק עם הזמנות פיקטיביות; להצית שריפות בכל הארץ; לגרום לתאונות דרכים; ואף לשבש מערכות העצמות אנוש המחוברות לאנשים. בחלק מן הסכנות הללו האפקט הפיזי לא נשמע יוצא דופן, אבל האפקט הפסיכולוגי הוא החשוב. אפשר ליצור מצב, בו אנו לא סומכים על הטכנולוגיה שלנו. המכשירים בבית "בוגדים" בנו, וכל זאת מבלי לסכן אף חבר בארגון הטרור.

מה שמגביר את הסיכון ואת הפגיעות של המערכות, הוא העובדה שבעולם שבו הכל מחובר – עוצמת הרשת כולה היא כזו של החוליה החלשה. כלומר פרצה אחת במכשיר "תמים" – עשויה להפיל תשתית לאומית.

הנחת היסוד שלנו כאשר אנחנו ניגשים לבחון טכנולוגיה חדשה כמו IoT, היא החשש מהיותה פגיעה לשימוש זרוני. בעולם הטכנולוגי לרוב קודם בא הפיתוח, ולאחר מכן באה האבטחה. צריך להביא מגמה זו בחשבון, כאשר אנו מנסים להבין לאן עולם הסייבר יצעד. עולם תקיפות הסייבר יאיים עלינו תמיד, במיוחד כאשר מדובר בטכנולוגיות חדשניות. חשיפה של התשתיות הלאומיות והצבאיות שלנו ושל העורף האינטרנטי הלאומי לתקיפות סייבר

ולהטמעה טכנולוגיות חדשניות בקצב גבוה, ולהתאים את עצמנו לעולם המשתנה.

בעבר היו המדינות הכוחות הגדולים במו"פ, וההשקעה הרבה שלהם באה לידי ביטוי בשדה הקרב – בטכנולוגיות שהקדימו את השוק האזרחי, וכנראה אף לא היו קורות בו מעצמן. לדוגמה: התפתחות המטוסים במלחמת העולם השנייה, הלוויינים, המחקר הפיזיקלי סביב פצצת האטום, ה-GPS ואפילו תחילתה של רשת האינטרנט.

בשנים האחרונות יש מגמה של התחזקות האזרחות על פני הצבא, ורבים מהחידושים הטכנולוגיים לא הגיעו ממדינות או מצבאות. קיימות כמה סיבות לכך, אך נראה שהעיקרית שבהן היא שכיום יש חברות ותאגידים גדולים יותר, שיכולים להחזיק בעצמם מו"פ מתקדם לא פחות משל רוב המדינות, לצד טיפוח של חברות סטארט-אפ שהן חממת החדשנות במדינות השוק החופשי.

מתוך מגמה זו יש כאלה הקוראים להשקיע פחות במו"פ הפנימי שנעשה בצבא, כיוון שהוא כמעט לא רלוונטי, ולהסתמך ככל האפשר על מיקור חוץ וקנייה מהתעשייה. לעומת זאת, יש הטוענים שגם כיום המדינות יכולות להיות כוח משמעותי בעולם ביחס לאזרחות. ככל שטכנולוגיה מעניינת יותר את העולם האזרחי ויש לה סיכוי להביא תפוקה מהירה – כדאי יותר לתת לאזרחות לפעול, ולקטוף



IoT (Internet of Things). חזון המקור שמזמין לבד מצרכים, או המזון שמחליט לחמם את הבית בטרם החזרה אליו, נראה קרוב מתמיד

הימנעות מפגיעה בבלתי מעורבים. הכוח ההרתעתי יכול להגיע מהאיום של שימוש נגד תשתיות אזרחיות, ואף מתרחיש מאון אימה שבו לשני הצדדים יש כלי נשק EMP, ושניהם נמנעים מהפעלתו מחשש לפגיעה קשה באורח החיים במדינה.

ברומה לסייבר, העוצמה של נשק EMP נשענת על התלות שלנו באלקטרוניקה. תלות זו ככל הנראה תתחזק עוד יותר בעתיד, עם הפיכת המערכות לאוטונומיות יותר והכנסת רכבים אלקטרוניים לגופנו (העצמת אנוש). נשק כזה צפוי להיות אמל"ח אסטרטגי הכרחי עבור צה"ל. ישראל, בתור מדינה בעלת מחקר ופיתוח (מו"פ) טכנולוגי מתקדם ביחס לשכנותיה, יכולה להשיג נשק EMP מוקדם יותר מאויבינו בסביבה הקרובה.

כיצד צריכה ישראל להיערך לשדה הקרב העתידי?

העתיד צופן משחק חתול ועכבר טכנולוגי של שיבוש מערכות אויב ויירוט השיבושים. למדינת ישראל יש מסורת טכנולוגית יפה שמביאה לנו יתרון יחסי במשחק זה. כדי להמשיך ולשמר יתרון זה בעתיד, אנו נדרש מצד אחד לקצב פיתוח מהיר ומנגד לרמת חסינות גבוהה.

ההתקדמות הטכנולוגית בעולם מחדדת את הצורך בפיתוח מגוון רחב של יכולות נגד, מגמה שרק תתעצם בעתיד. כבר היום, מול כל אמל"ח מפותח אמצעי נגד שנועד לעצור או להחליש אותו: מ"מעיל רוח" לטנק, דרך "כיפת ברזל" לרקטות ועד שיבושים בלוחמה אלקטרונית. גישה זו היא תגובתית בלבד, ותמיד תדרוף אחר האויב שיצר את האיום מלכתחילה.

היות שקצבי הפיתוח עולים ומתרחבים לתחומים חדשים, בעתיד נדרש לקצבי מו"פ מהירים אף יותר כדי לתת מענה לשלל האמצעים שהאויב יכול להשתמש בהם, ולפתח הגנות ועמידות לכל אמצעי נגד ששיג האויב. בעולם המחייב מעגלי מו"פ וייצור קצרים, יהיה צורך במצרי מדף גנריים. כמו כן תידרש שיפור היכולת לשלבם באמצעות תקנים וסטנדרטיזציה, ויכולת הטמעה שאינה אופיינית לצבא סבוך עם תהליכים ארוכים.¹⁷ עלינו ללמוד, כלובשי מדים, כיצד בעולם האזרחי מצליחים להביא לפיתוח

היות שקצבי הפיתוח עולים ומתרחבים לתחומים חדשים, בעתיד נדרש לקצבי מחקר ופיתוח מהירים אף יותר

2018

את הפירות כשיבשילו. מנגד, בנושאים שמעניינים בעיקר מדינות (לדוגמה, נשקי EMP), ובנושאים שדורשים תשתיות יקרות ואין בהם הבטחה לרווח כלכלי שיפצה על כך (לדוגמה, מערכת GPS דורשת השקעה בלוויינים) – נוכל להגיע להישגים טכנולוגיים חדשניים מתוך הצבא גם בעתיד.

העולם האזרחי יודע לתת פתרונות של ייעול ומזעור, ומשקיע מאמצים רבים בנוחות משתמש. אם ישיכיל צה"ל להיות מעורב במו"פ הנעשה בשוק האזרחי בדרך קבע, כל שיישאר הוא ליהנות מהתוצרים.

סיכום

אנו רואים חשיבות מכרעת לטכנולוגיה בעיצוב שדה הקרב העתידי. מלחמה בעור 30 שנה תכלול לוחמים שונים, פיקוד שונה, מתקפות שונות ושלל טכנולוגיות שקצרה היריעה מלהכיל וצורה תודעתנו מלרמיין. לדעתנו, השילוב בין עולם המו"פ הצבאי לעולם הטכנולוגי האזרחי, יהיה זה שיביא לניצחון בשדה הקרב העתידי. לישראל, כמעצמה טכנולוגית למודת קרבות הנשענת על איכות חייליה ונשקם, יש פוטנציאל להוביל את עולם הטכנולוגיות הצבאיות ולהיות חלוצה בתחומים רבים.

אנו מאמינים ביכולתה להגיע לשם.

ההערות למאמר הזה מתפרסמות באתר הוצאת מערכות.

