



**"גרדיום" – כלי רכב בלתי מאויש, רכב אוטונומי של צה"ל על גדר הגבול ברצועה. רכבים עתירי סנסורים הפכו, זה מכבר, לסטנדרט בתעשיית הרכב, כחלק ממהפכת הרכב המקושר**



**סא"ל נורית כהן-אינגר < רע"ן סיגמא בלוט"ם  
 רס"ן יאיר אדיב < רמ"ד שו"ב במפא"ת  
 סרן זיו דיין < קמ"ד שו"ב במפא"ת**

# מלחמת ה"דברים" ההשפעה של מהפכת האינטרנט של הדברים על העולם הצבאי

## מבוא

העולם שלנו נמצא בעיצומה של מהפכה. המידע שנאסף בשנה האחרונה גדול מסך כל המידע שנאסף קודם לכן בהיסטוריה האנושית. הגידול המעריכי (אקספוננציאלי) במידע, מוכר לנו כמהפכת ה-Big Data, וזו נמצאת רק בתחילתה. אנו רגילים לכך שהמידע נוצר ונאסף מאנשים, המדווחים סטטוסים בכל רגע נתון. התופעה הזאת יצרה אתגרים טכנולוגיים חדשים, כמו אגירת כמויות גדולות של מידע במרכזי מחשוב עצומים. ואולם האתגרים המשמעותיים הם הבנת המידע והבחנה בין העיקר לטפל, שמצריכים שיטות עיבוד ומיצוי מידע חדשות והובילו להתפתחות של תחומי חקר ומדעי המידע.

מהפכת ה-Big Data התעצמה עם חיבורם של חפצים שונים, מערכות מרובות חיישנים ואביזרים, לרשת האינטרנט. אלה יצרו עולם חדש משלהם שבו כל חפץ וחיישן אוסף ומנטר, משתף ומדווח, מעבד ומסיק מסקנות בעצמו, מחליט החלטות ומבצע. זהו העולם של "האינטרנט של הדברים" (IoT - Internet of Things), המוכר גם בשם "האינטרנט של הכל" (Internet of Everything IoT).

מהפכת ה-IoT צפויה לשנות את החברה האנושית והדרך שבה אנו חיים. במאמר הזה נסקור את השימושים האפשריים בטכנולוגיה, ואת הפוטנציאל לסביבה הצבאית לצד האתגרים והסיכונים.

טכנולוגיית האינטרנט של הדברים, היא בעלת פוטנציאל להשפעה רבה על שדה הקרב העתידי ופניהם של הצבאות העתידיים. הצבא מחויב לאמץ תפישות הפעלה וחשיבה חדשים, ולשנות את אופן התנהלותו



## שימושי האינטרנט של הדברים

עד לפני עשור נעשה החיבור לאינטרנט מהמחשב הביתי בלבד. בשנים האחרונות גדלה עשרות מונים כמות ה"דברים" המחוברים לאינטרנט: הטלפון החכם, הטלוויזיה, שעונים חכמים, משקפיים, מכוניות ומוצרי חשמל ביתיים. כולם הופכים את עולמנו לעתיר מידע, לעולם שבו ניתן לדעת הכול על הכול בכל רגע ובכל מצב. כיום מחוברים לאינטרנט של הדברים כ-6 מיליארד חפצים, וההערכות הן שמספרן יגיע עד שנת 2020 לכ-21 מיליארד.<sup>1</sup> מדובר בכשלושה חפצים בממוצע לאדם באוכלוסיית כדור הארץ.

המהפכה החלה לפגוש אותנו בתחומים שונים ומגוונים בחיינו, בין היתר, בית חכם, רפואה ורכבים אוטונומיים.

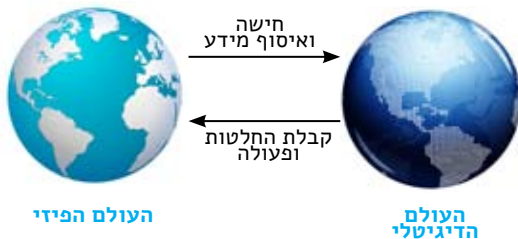
**הבית החכם** - יש גידול במספר החיישנים שמדווחים בזמן אמת לבעליהם על המצב בביתם, ומתריעים על כשלים כגון: עשן, נזילות, כניסת גורמים עוינים ואף מזהים את בעלי הבית בכניסה לביתם. שימושים תבונתיים יותר כוללים למשל מערכות השקיה בגינה, שפועלות עצמאית ומחליטות על כמות המים להשקיה בהתאם לסוגי הצמחים ולמזג האוויר.

**הרפואה** - כבר היום קיימות מערכות המסוגלות להתריע על שינויים במצב הפיזיולוגי (חום, לחץ דם, דופק וחמצן) עוד לפני שהמטופל חש בבעיה הן יכולות לסייע במניעת נזק בלתי הפיך. דוגמה לכך היא צמיד המתריע למטופל על סכנה, למשל חשש לאייספיקה של הלב ואובדן הכרה, ובמקביל מדווח באופן אוטומטי למרכז בקרה של שינוי במצב.

**הרכבים האוטונומיים** - רכבים עתירי חיישנים הפכו זה מכבר לסטנדרט בתעשיית כלי הרכב, במסגרת מהפכת הרכב המקושר. הרכב כולל עשרות חיישנים שונים ומערכות מחשוב מתוחכמות, בהן מחשב דרך בשילוב מערכת ניווט חכמה, מערכת מניעת תאונות

ומחשב מנוע, המאפשר ניצול אנרגיה אופטימלי וזיהוי מקדים של תקלות. עיבוד המידע הרב שנאסף בזמן אמת, בשילוב אלגוריתמים מורכבים מתחום הבינה המלאכותית, מייצרים את התנאים לנהיגה אוטונומית, כלומר שיכולת של הרכב לנהג את עצמו ליעד ללא מעורבות אדם, זאת תוך עמידה בחוקי התנועה המקומיים והתמודדות עם הפתעות בלתי צפויות בנסיעה. בשנים האחרונות התקיים ניסוי של חברת גוגל לרכבים אוטונומיים, שנוסעים באופן עצמאי בכבישי ארצות-הברית.<sup>2</sup> רכבים אלו כבר גמעו למעלה מ-2.5 מיליון ק"מ. לפי מחקר שנערך,<sup>3</sup> כ-3 אחוזים מכלי הרכב החדשים שייכנסו לשוק - יהיו אוטונומיים.

מהפכת ה-IoT משנה לנגד עינינו את אופן התפקוד של רכבים חשמליים, והופכת אותם לחכמים באמצעות המעבר מחישה לפעולה. למעשה, ה-IoT הוא הגשר בין העולם הפיזי לבין העולם הדיגיטלי, כאשר החיישנים מתרגמים את הסביבה הפיזית למרחב הדיגיטלי, ולאחר תהליך עיבוד וקבלת החלטות משפיעים על העולם הפיזי באופן אוטומטי ובמעורבות מינימלית של האדם.



## המהפכת טכנולוגיות השפיעו על צבאות מאז ומתמיד

תורות הלחימה הושפעו במשך ההיסטוריה מטכנולוגיות ששירתו את האנושות לצרכים הכלכליים והחברתיים, החל מהמצאת הגלגל בשנת 3500 לפנה"ס ועד למהפכת האינטרנט של הדברים.

המהפכות התעשייתיות<sup>4</sup> השפיעו על תפיסות, על שיטות ועל טכנולוגיות הלחימה. תהליך התיעוש יצר את התנאים למלחמה טוטלית המערבת את כל מרכיבי החברה במלחמה, ולא רק את הצבא והשליטים. בתי החרושת וקווי הייצור בעורף אפשרו לייצר בכמויות עצומות כלי נשק ובאופן מתמשך עבור המאמץ המלחמתי, ולכן גם הפכו לחלק ממטרות הלחימה של הצד שמנגד.

**מהפכת המחשוב**, שהחלה בשנות ה-40 של המאה ה-20,<sup>5</sup> הביאה לשינוי תפיסה ושימוש נרחב יותר ביכולות העיבוד והמחשוב המתקדם, זאת תוך ניצול התקדמות הטכנולוגיות האזרחיות. ארצות-הברית אימצה את התפיסה,<sup>6</sup> ובאמצעות שימוש בטכנולוגיות חדשות מהעולם האזרחי

והטמעתן הלכה למעשה בשדה הקרב, החל מהתו"ל, עבור דרך ההכשרות והאימונים וכלה באמצעי הלחימה עצמם - שיפר הצבא האמריקני באופן ניכר את יכולותיו, העצים את המודעות המצבית והפחית באופן משמעותי את ערפל הקרב.

**מהפכת המידע** מיצבה את המידע כמרכיב החשוב והמהותי בכל דבר ועניין. המידע מהווה מכפיל כוח בקבלת החלטות, ונותן יתרון ברור למי שמחזיק בו. מהפכת המידע הובילה לפיתוח מערכות שו"ב ומודיעין צבאיות. מערכות אלה מאפשרות הפעלה מדויקת של הכוח, פיזור ערפל הקרב, ניתוח והבנה של היכולות, של הפעולות של היריב ושל המוטיבציה שלו.

**מהפכת השיתופיות** העבירה כוח עצום להמונים שהפכו לשחקנים החדשים בזירה. דוגמה לכך היא "האביב הערבי" שמוטט משטרים בני עשרות שנים. מהפכת השיתופיות, או בשמה הצבאי מהפכת השילוביות, שינתה את מבנה הצבא ממערכים צבאיים כבדים ליחידות קטנות וזריזות, ואפשרה שיטות לחימה חדשות רב זרועיות מבוססות רשת. גם מהפכת ה-IoT צפויה לשנות את פני הצבא באופן ניכר.

## תורות הלחימה הושפעו לאורך ההיסטוריה מטכנולוגיות ששירתו את האנושות לצרכים הכלכליים והחברתיים, החל מהמצאת הגלגל ב-3500 לפנה"ס ועד למהפכת האינטרנט של הדברים

## IoT אופרטיבי

באחזקה מונעת לציוד, בייעול שרשרת האספקה ובמעקב אחר היסעים. מובן שאימוץ תרחישים הנמצאים בשימוש "ערים חכמות", יכול לשפר באופן משמעותי התנהלות בסיסים ואבטחתם. בצבא ארצות-הברית החלו לשלב טכנולוגיות IoT לניהול מלאים, וכן טכנולוגיות לניהול אנרגיה ותשתיות פיזיות,<sup>8</sup> שבאמצעותן הביאו בשנים האחרונות לחיסכון של כ-25 אחוזים בצריכת החשמל והמים במתקנים השונים. דוגמא נוספת לכך, היא השימוש במערכת החכמה של מטוסי ה-F35 להתייעלות משמעותית באחזקתם ובתפעולם.<sup>9</sup>

בדומה לרכבים האוטונומיים, קל לדמיין כיצד רק"ם עתיד עתיר חיישנים יבצע משימות באופן אוטונומי, למשל, פטרול צמוד לגדר, או אפילו הסתערות וירי בתנאים שונים, ובפרט בשטח בנוי. הרק"ם יספק תמונת מצב מלאה ובזמן אמת של כשירותו, ויתעדף את משימותיו בהתאם לרמת הכשירות והמשאבים הזמינים. השימוש בכלים אוטונומיים בשדה הקרב יאפשר הפחתת הסיכון של כוחות לוחמים אנושיים, ויצמצם את הפגיעה באזרחים בזכות פעולות כירורגיות ממוקדות.

באזורי אסון יוכלו רחפנים לשמש להקמת רשת תקשורת זמינה לכוחות המחלצים ללא תלות בתשתיות קיימות, זאת באמצעות יצירת רכבת ממסרים. רחפנים בשילוב כוחות רגליים יאפשרו לכוח לראות ולפעול רחוק יותר. כך למשל, במהלך המלחמה באפגניסטן, השתמש הצבא הבריטי בבנוי מסוקים<sup>10</sup> לאיתור חוליות של הטאליבן, מעקב אחריהן וכן לסגירת מעגלי אש מהירים. הלוחמים היו מצוידים באמצעים,

שידעו לתקשר ביניהם ולספק מודיעין מהיר ואמין בזמן אמת. באותו סבב לחימה השתמשו צלפים אמריקאים באפליקציית אייפון,<sup>11</sup> שפותחה במקור למטרות משחק, וחישבה את השפעת הרוח וסיבוב כדור הארץ על הבליסטיקה של הקליע, ובכך סייעה בצליפה למרחקים ארוכים. אלה דוגמאות ספורות לשינויים הצפויים בעידן ה-IoT.

## אתגרים וסיכונים בשילוב הטכנולוגיה

לשילוב טכנולוגיות IoT בסביבה צבאית יש אתגרים רבים שדורשים למענה. שימוש במעבדים זעירים, רבי עוצמה שצריכת ההספק שלהם נמוכה. מעבדים אלה יאפשרו את שילובם בכל תצורה החל ממחשוב לביש, עבור דרך מסכים גמישים וכלה בחיישנים חכמים, תוך עמידה בתנאי סביבה ושטח קשים. נוסף על כך, תינתן אפשרות לשימוש במאגר אנרגיה נישא שיהיה מסוגל לספק אנרגיה רציפה ולאורך זמן, ואפילו לייצר אנרגיה באופן עצמאי. תקשורת רחבת סרט לכל אורך שדה הקרב עתיר החיישנים, ועד רמת הלוחם הבודד.

קיימות כמה מגבלות לשימוש בטכנולוגיות ה-IoT. הראשונה, קיימת מגבלה פיזית<sup>12</sup> ללוחם בנשיאת עשרות חיישנים שלהם תפקודים שונים. מעבר לכך, בסביבה עתירת חיישנים, כאשר כל חיישן מייצר מידע, נוצרים היצף מידע ועומס על התקשורת וכן על יכולות עיבוד מרכזיות. הדור הבא של החיישנים יידרש לטייב את המידע ולבצע עיבוד מתקדם בתוך היחידה עצמה ובאופן מבוזר, ולשדר לאחור רק תוצרי מידע מעובדים רלוונטיים. הגישה

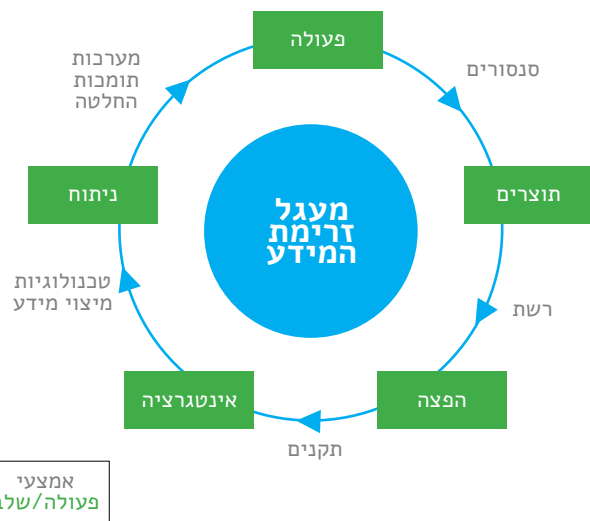
שימוש נכון בטכנולוגיות IoT, ישפר וידייק את שיטות הלחימה המוכרות ואת מעגל זרימת המידע בשדה הקרב. פעולה שמבצע משתמש הקצה, ומדווחת על-ידי אמצעים וחיישנים, בונה תוצרי מידע המופצים ברשת וגורמים להיצף מידע. באמצעות תקנים והגדרת שפת IoT צה"לית, יתאפשרו אינטגרציה והיתוך של המידע לכדי מידע אחיד גולמי. באמצעות טכנולוגיות מיצוי מידע, יתבצע ניתוח נוסף שממנו יופק ידע חדש. לבסוף, על-ידי מערכות תומכות החלטה, המידע והידע הרלוונטיים, המעודכנים והאפקטיביים ביותר מגיעים למשתמש הקצה בצורה של תובנות והמלצות לפעולה.

התקשורת בין הרכיבים מאפשרת שמירה על חשאיות יחסית לאמצעי הקשר האחרים, זאת הודות לשידור בעוצמות נמוכות מאוד ויעילות אנרגטית על-ידי שימוש בסטנדרטים חדשים בהם BLE,<sup>13</sup> שהיא גרסת Bluetooth חדשה ודלת הספק שתוקננה עבור תחום ה-IoT. רפואה קרבית מבוססת IoT תשלב חיישנים שימדדו פרמטרים פיזיולוגיים ואף פסיכולוגיים של הלוחם תוך כדי אימונים וקרב. מצב בריאותו של הלוחם ידווח בזמן אמת, ינותח, ובהתאם לכך תינתן התרעה למניעת מצב סכנה בריאותי - יכולת בעלת חשיבות רבה להגנת הלוחמים שנדרשים להגיע לסף יכולתם. יתרה מזו, שידור הסטטוס הבריאותי מהווה לחצן מצוקה, ומאפשר לאתר לוחם פצוע בזמן אמת ולשלוח אליו את הסיוע הדרוש. חיישנים

לזיהוי ריחות ורעלים יתריעו על סכנה עוד לפני שהלוחם מודע לה.

בתחום הלוגיסטיקה, כמות התרחישים לשילוב טכנולוגיית האינטרנט של הדברים היא אין-סופית: חיישנים מסוגים שונים יוכלו לשפר באופן משמעותי תהליכים לוגיסטיים, להתייעל ולחסוך - לסייע באיתור ציוד, בניהול מלאים במחסנים, בטיפול

## שימוש נכון בטכנולוגיות IoT, ישפר וידייק את שיטות הלחימה המוכרות ואת מעגל זרימת המידע בשדה הקרב



▶ הזאת הביאה להתפתחות של מחשוב ערפל,<sup>13</sup> כלומר, הורדת ענן המחשוב המרכזי קרוב יותר לקרקע וליחידות הקצה, וביצוע תהליכי היתוך ועיבוד מידע באופן מבוזר בין יחידות הקצה ורכיבי הרשת. באופן דומה יידרשו המערכות המבצעיות לשלב מנגנונים ומסננים, שייעבירו ללוחם שבקצה את המידע הרלוונטי עבורו לצורך עמידה מוצלחת ביעדיו. אי-הפעלה של מנגנונים כאלה עלולה להוביל לפגיעה ביכולת הפעולה של הלוחם, מכיוון שהוא יפנה את הקשב שלו לניתוח והבנת המידע ולא יוכל להתרכז בסביבה ובמשימה. כדי לסייע ללוחמים ולמפקדים עם היציג המידע,<sup>14</sup> נידרש לבחון לפיתוח מערכות תומכות החלטה שיכוונו באופן אקטיבי את המשתמשים על-ידי מתן התרעות והמלצות לפעולה, השוואת דפ"א אות שונות וכימות להישג או העלות של כל דפ"א לצורך השוואה.

אחד הסיכונים שיכולים להתפתח משילוב הטכנולוגיה, הוא יצירת תלות בין הלוחם או המפקד למידע המתקבל ולחיישנים השונים. אין ספק, כי לטכנולוגיה מקום מרכזי בלחימה של היום, וקשה לדמיין לחימה ללא אמצעים טכנולוגיים. עם זאת, חשוב שתורת הלחימה – אף שהיא מבוססת על טכנולוגיות מתקדמות – תדע לטפל ולתפעל "מעצורים", כלומר שיתורגלו מקרים שבהם הטכנולוגיה והחיישנים אינם זמינים מסיבות שונות, למשל, נתק בתקשורת, מחסור באנרגיה או אירוע של תקיפת סייבר. כפועל יוצא מכך, יש חשיבות רבה לשיקול הדעת של הלוחם ולהכשרתו. כך למשל, בדוגמה של רפואה קרבית: הרופא יכול להסתמך על תמונת מצב חיישנים פיזיולוגיים של הלוחמים, והמלצת מערכת תעדוף פצועים בעת אירוע רב נפגעים, אך המערכת אינה תחליף למקצועיותו, לתמונת המצב שהוא רואה בעיניו, ולשיקול דעתו בזמן האירוע.

## אתגרים בממד הסייבר

הגשר שה-LoT בונה בין המרחב הפיזי למרחב הדיגיטלי, מייצר חשיפה לתקיפות סייבר שמשמעותן פגיעה במרחב הפיזי, בתשתיות קריטיות, בבריאות וברכוש.

בפברואר 2015 התנהל שימוע בסנאט האמריקני<sup>15</sup> בנושא מגמת ה-LoT והמעורבות הממשלתית הנדרשת לשמירת האיזון, בין תמיכה בחדשנות לבין הגנה על המשתמשים. לשילוב יישומי LoT בשדה הקרב ללא מענה אבטחה ראוי יכולות להיות השלכות מרחיקות לכת, החל מפגיעות הכוח הבודד וכלה בפגיעה אסטרטגית בכלל הצבא.

המתקפה האחרונה (אוקטובר 2016),<sup>16</sup> שנחשבת לאחת המתקפות הגדולות בסייבר, יוחסה לאינטרנט של הדברים. היציג של מידע מאמצעי LoT ייצור (Distributed Denial of Service) attack DDOS – התקפת מניעת שירות מפוצלת באתרים ושירותים מרכזיים באינטרנט.

רק לשם המחשה, הצליחו חוקרי אבטחה לפרוץ לתוכנה של רובה צלפים יוקרתי<sup>17</sup> עם כוונת חכמה, שיכול להישלט מרחוק על-ידי מחשב. החוקרים הצליחו לשבש את הכוונת כך שתמיד תחטיא את המטרה, למנוע מהרובה לבצע ירי, ואפילו לגרום לפגיעה במטרה שגויה סמוכה על-ידי שינוי פרמטרים מהיר בזמן ביצוע הירי. כל זאת ללא ידיעת הצלף.

אתגרי האבטחה, הנלווים לחיבורם של רכיבים פיזיים לרשת האינטרנט, הם אתגרים מוכרים. עם זאת, בעולם ה-LoT היקף הרכיבים המחוברים, ביזורם, נגישותם הגבוהה בזמן אמת וכמות המידע המופקת על ידם, יוצרים בעיה בסדר גודל חדש. להלן כמה מגמות שמעצימות את אתגרי האבטחה בעולם ה-LoT:

• **גידול בביזורם של רכיבי קצה** – ריבוי רכיבים מבוססי מחשב מתבטא בריבוי וקטורי תקיפה, כלומר כל אמצעי מחשב יכול לשמש כדלת לתוקף. המגמה הזאת מחייבת גישות אבטחה חדשות, הגנה בכל נקודה ולא רק בהיקף.

• **הקטנת צריכת הספק של רכיבים** – רכיבי מחשב זעירים עם אילוצי צריכת הספק אינם מכילים לרוב זיכרון נרחב או יכולת עיבוד משמעותית, ולמעשה משיתים אילוצים על מורכבות ואיכות מערכת ההגנה המיושמת בהם.

• **האצת מגמת האוטונומיות** – לנוכח הקישוריות ההדדית והאוטונומיה הגוברת של רכיבי ה-LoT, מצטמצמת המעורבות האנושית בתהליך כך שנדרש לייצר יותר תהליכי בקרה, ניטור ואימות על תהליכי שיתוף המידע וקבלת ההחלטות.

ה-LoT מחייב שילוב מערך הגנה רב ממדי מקצה לקצה שפועל על האמצעים, על הרשת, על המידע, על הטרנסקציות ועל התהליכים, במשך כל תהליך המו"פ – החל מתכנון הרכיב ועד לייצור. הגישה נקראת "Security by Design".

סוכנות DARPA, הסוכנות הממשלתית של מחלקת ההגנה האמריקנית, העוסקת בפיתוחים הטכנולוגיים של צבא ארצות-הברית, התניעה לאחרונה את תוכנית LADS<sup>18</sup>, שנועדה לאפשר ניטור והגנה על מכשירי LoT על בסיס חומרה חיצונית למכשירים עצמם. כך מתאפשר ניתוק פיזי ולוגי, בין המכשירים שברשת ה-LoT לבין הגנת הסייבר שעוטפת אותם. השיטה מאפשרת לעשות שימושים צבאיים בפיתוחים טכנולוגיים אזרחיים, שנדרש רק להלביש עליהם את חליפת ההגנה ללא התאמות חומרה יקרות וארוכות. עם זאת,

השיטה הזאת עלולה להניב תוצר סופי גדול ומסורבל יותר במבנה הפיזי שלו, לעומת הרכיב המקורי.

גם סוכנות ה-NSA, ארגון הביון הממשלתי של משרד ההגנה האמריקני, זיהתה את ההזדמנות המודיעינית לצד הסיכון, והחלה להשקיע במחקר<sup>19</sup> העוסק בפריצה לאמצעים חכמים, בעיקר ביומטריים, כדי לאתר מיקום ולאסוף מידע אודות יעדים. השימוש באינטרנט של הדברים לצורך ריגול ומודיעין הנו אפשרות נוספת לניצול לרעה של התחום המתפתח.

לשם השלמת מגמת שילוב טכנולוגיות LoT באמצעים ללחימה ובאמצעים תומכי אמל"ח, חשוב לפתח תפיסת הגנה רחבה המשלבת הגנה רב שכבתית על כל מרכיבי הרשת – החל מרמת החיישן הבודד, עבור דרך מקורות האנרגיה, התקשורת, מערכי המידע וחזור לרובוטים הנדרשים לבצע משימות באופן אוטונומי.

## מבט לעתיד

שדה הקרב העתידי מורכב לאין שיעור ממה שהיה בעבר. אם פעם הייתה תמצית פעולתו של הלוחם השימוש בנשק, והכלים

## בדומה לרכיבים האוטונומיים, קל לדמיין כיצד רק"ם עתיד עתיר סנסורים יבצע משימות באופן אוטונומי כגון פטרול צמוד לגדר, או אפילו הסתערות וירי בתנאים שונים, ובפרט בשטח בנוי



מל"ט הרון אוסף מודיעין. פעולה שמבצע משתמש הקצה, ומדווחת על-ידי אמצעים וסנסורים, בונה תוצרי מידע שמופצים ברשת וגורמים להיצף מידע

ועל סגירת מעגלי התקיפה, ונעזר במערכות תומכות החלטה לחלוקת קשב ולפתרון בעיות בין הכלים. היכולות האלה מהוות מכפיל כוח על-ידי שבירת התלות בין גודל הסד"כ הלוחם לגודל האובלסוסייה, מאפשרות החזקת סד"כ לחימה בסדר גודל מעצמתי ומשנות את פניו של הצבא כפי שאנו מכירים אותו כיום.

### סיכום

טכנולוגיית האינטרנט של הדברים, היא בעלת פוטנציאל להשפעה רבה על שדה הקרב העתידי - החל משיפור יכולות האיסוף, המודיעין ופיזור ערפל הקרב, עבור דרך

הגברת האפקטיביות של הכוח תוך צמצום משאבים וסיוע בקבלת החלטות, וכלה בהכנסת כלים חדשים לזירה, בהם רובוטים אוטונומיים עתירי חיישנים.

העולם נמצא בעיצומה של מהפכה, שתשפיע על שדה הקרב העתידי ותשנה את פניו. המהפכה הזאת דורשת אימוץ של תפיסות הפעלה וחישיבה חדשות, שישנו את אופן ההתנהלות של חיי היום-יום שלנו ותשפיע על הכלכלה, על החברה ועל הביטחון.

קרל פון קלאוזביץ תיאר את שדה הקרב כ"ממלכת אי הוודאות". אנחנו מאמינים, כי שימוש מושכל בטכנולוגיות IoT, תוך מיצוי המידע שייאסף, יוכל לשפר את השליטה. השילוב בין חיישנים חכמים המייצרים מידע בדיסציפלינות שונות, ברובוטים (החל מרובוטים זעירים ועד פלטפורמות לחימה לא מאוישות) ובמאגרי מידע עצומים. זאת בשילוב עם יכולות עיבוד מבוזרות, אלגוריתמים מתקדמים של היתוך ומיצוי מידע, זמינות והנגשת המידע הרלוונטי לכל גורם בקרב- מהווים יחד את התנאים הדרושים לעידן חדש של מלחמות, עידן "מלחמת הדברים".

## אחד הסיכונים שיכולים להתפתח משילוב הטכנולוגיה, הוא יצירת תלות בין הלוחם או המפקד למידע המתקבל ולסנסורים השונים

שנעזר בהם היו חושיו ויכולותיו הפיזיות והקוגניטיביות, ואילו היום נמצאות ברשותו מערכות רבות שעוזרות לו למקסם את יכולותיו - מכשירי קשר, מערכות שו"ב, כוונות חכמות או מערכות נשק מתוחכמות. משימתנו לוודא שהטכנולוגיה לא הופכת את תפקיד הלוחם למורכב מדי, אלא משתלבת בהרמוניה באקוסיסטם של הלוחם העתידי.

כפי שבעולם האזרחי עולה השאלה האם נותר מקום למקצועות כמו נהג מונית<sup>20</sup> בעידן שבו המכוניות מנוהגות באופן אוטונומי, וצופים<sup>21</sup> כי עד שנת 2020 כ-5 מיליון אנשים יפוטרו ויחלפו על-ידי מחשבים ורובוטים

בעלי אינטליגנציה מלאכותית, בעולם הצבאי עולה השאלה מה תהיה ההשפעה על ממלאי תפקידים בצבא בעידן ה-IoT. האם ניתן לדמיין שליחת רובוטים למלחמה במקום לוחמים, והחלפת המפקדים במחשבים רבי עוצמה שיקבלו החלטות במקומם? חיישנים, כלים לא מאוישים אוטונומיים, רובוטים ומחשבים יכולים לסייע רבות בשדה הקרב, למנוע פגיעה בחיי אדם, למנוע מפגיעה לא מבוקרת ונזק אגבי ממוקד, מנוהל וכירורגי.

לטכנולוגיות האלה יש פוטנציאל להגביר את אפקטיביות הצבא ולהביא למקסום הישגיו, זאת תוך צמצום הפגיעה בחיי אדם, אך הן לא יוכלו להחליף את "האדם שבטנק" או היד שעל הג'ויסטיק.<sup>22</sup> עם זאת, יידרשו הלוחמים המתקשבים להרחיב את סט המיומנויות שלהם ולשלב יכולות כמו קריאת נתונים, ניתוח מידע, הפקת תובנות, הפעלת יכולות סייבר ושליטה על מערכי ולהקות כלים לא מאוישים.

בשדה הקרב העתידי, יוכל כל לוחם לשלוט על מערך של עשרות כלים המנוהלים היררכית ומסוגלים לבצע משימות צוותיות מורכבות באופן אוטונומי. הלוחמים יוכלו לפקח על משימת העל

