מעבר לטכנולוגיה: כיצד חדשנות צבאית הופכת להפתעה מודיעינית בעידן הדיגיטלי

עופר גוטרמן[1]

העידן הדיגיטלי אינו משנה מהותית את תופעת ההפתעה הטכנולוגית, אך הוא מעצים את התנאים להיווצרותה. בסביבה כזו אי אפשר לצפות מהמודיעין לאתר או לחזות במדויק כל יכולת וכל שימוש עתידי בה, אך עליו לזהות מערכות מתהוות, להעריך את קצב הבשלתן ולבחון כיצד הן משנות את תפיסת הלחימה של היריב, וכיצד הן שוחקות יתרון איכותי או יוצרות ומנצלות נקודות תורפה בצד שלנו. על המערכת הביטחונית לעסוק גם בשלילת יכולותיו המתפתחות של היריב ולפתח גמישות וחוסן שיאפשרו לה לספוג הפתעה, להסתגל אליה ולהתאושש ממנה

מבוא

בקרב מילאי ב־260 לפנה"ס התמודד הצי הרומי הצעיר עם הצי הקרתגי המנוסה. לפי פוליביוס, הרומאים התקינו בספינותיהם גשר השתלטות (קורבוס), שננעץ בספינת האויב ואפשר לחיילים לעבור אליה. הקרתגים הופתעו מן המתקן, והרומאים הצליחו להפוך את הקרב הימי למפגש הדומה ללחימה ביבשה.[2] בקרב טונדיבי ב־1591 הביס כוח משלוח מצומצם של הסולטנות הסעדית במרוקו את צבא סונגהאי, באמצעות נשק חם (רובי ארקבוז ותותחים) שלא היה מוכר לצבאה הגדול בהרבה של האימפריה האפריקנית.[3] ההצלחה המהירה של הוורמאכט בפלישה לצרפת ב־1940 נבעה, בין היתר, מאופן הפעלת השריון שהפתיע את הצרפתים: ריכוז עוצבות השריון וחיבורן לקשר רדיו, לסיוע אווירי ולפיקוד נייד שאפשרו חדירה מהירה וניצול מיידי של הצלחה.[4]

מקרים אלה ואחרים מלמדים שההפתעה הטכנולוגית עתיקת יומין והיא חלק בלתי נפרד מתופעת המלחמה. לעיתים מקורה באמצעי חדש, לעיתים בשימוש בלתי צפוי באמצעי מוכר, ולעיתים בפער בין היכרות עם הטכנולוגיה עצמה ובין הבנת האופן שבו היא משפיעה על שדה הקרב.

מיכאל הנדל הגדיר הפתעה טכנולוגית כיתרון חד־צדדי הנוצר באמצעות נשק חדש או שימוש חדשני בנשק מוכר, מול יריב שאינו מודע ליכולת או שלא הכין לה מענה יעיל.[5] מאיר פינקל הרחיב את ההגדרה והשתמש במונח הפתעה טכנולוגית ותורתית, המתייחס לשימוש באמצעי לחימה ובתורת לחימה שהצד המופתע אינו יכול לשבשם בזמן המפגש.[6] בשתי ההגדרות, החידוש הטכנולוגי מוביל להפתעה רק כאשר הוא מקנה יתרון במפגש עם היריב.

ההתייחסות להפתעה הטכנולוגית כהפתעה שהיא גם תורתית מגלמת הבנה שטכנולוגיה הופכת ליכולת צבאית באמצעות חיבור בין אמצעי, תפיסת ההפעלה שלו והארגון שמפעיל אותו, לרבות מבנה ארגוני, הכשרות, הטמעה והיבטים תפעוליים. אפשר להכיר אמצעי חדש, לעקוב אחר פיתוחו, לדעת שהיריב מצטייד בו, ובכל זאת להחמיץ את היכולת שנבנית סביבו ואת דרך הפעלתה.

להמשגה זו, הרואה בהפתעה הטכנולוגית תופעה מערכתית רחבה מן הפן הטכנולוגי לבדו, יש משמעות מעשית למודיעין. היא מבהירה כי יש להרחיב את המעקב גם לשאלות של תפיסה ובשלות מבצעית ולהשפעות מערכתיות על שדה הקרב, לרבות זיהוי נקודות תורפה במוכנות לאיום החדש.

---

1 אל"ם (מיל') ד"ר עופר גוטרמן, עמית בכיר במכון הרכבי לחקר המודיעין ובמכון למחקרי ביטחון לאומי, ומרצה במחלקה ליחסים בין־לאומיים באוניברסיטה העברית.

2 Polybius. (1922). The histories (W. R. Paton, Trans.; Vol. 1, Books 1–2). Harvard University Press. (Original work published ca. second century BCE). Book 1, §§ 22–23

3 Kaba, L. (1981). Archers, musketeers, and mosquitoes: The Moroccan invasion of the Sudan and the Songhay resistance (1591–1612). The Journal of African History, 22(4), 457–475. https://doi.org/10.1017/S0021853700019861

4 נווה, ש' (2001). אמנות המערכה: התהוותה של מצוינות צבאית. מערכות, עמ' 124; פינקל, מ' (2007). על הגמישות: הגמישות כמפתח להתמודדות עם הפתעה טכנולוגית ותורתית בשדה הקרב. מערכות

5 Handel, M. I. (1987). Technological surprise in war. Intelligence and National Security, 2(1), 1–53. https://doi.org/10.1080/02684528708431875

6 פינקל (2007), עמ' 10, 35

הקשר בין הטכנולוגיה ובין המערכת הנבנית סביבה הוא גם נקודת המוצא לבחינת ההפתעה הטכנולוגית בעידן הדיגיטלי. בעידן זה יכולת צבאית עשויה להיבנות באמצעות שילוב משתנה של רכיבי מדף, תוכנה, נתונים, קישוריות ומבנים ארגוניים רשתיים יותר, ולאו דווקא באמצעות פיתוחו של אמצעי לחימה ייעודי חדש. מכאן עולה שאלת המאמר: האם וכיצד משנה העידן הדיגיטלי את התנאים לזיהויה של התפתחות טכנולוגית שעל המודיעין להתריע מפניה?

המאמר יסקור שלושה מנגנונים מרכזיים התורמים להחמצת זיהויו של איום טכנולוגי: אסימילציה וראיית מראה, הטיה ארגונית־תרבותית ופער ההבשלה. השניים הראשונים מוכרים מהספרות הכללית על כשלי מודיעין, אך כאן הם נבחנים בהקשר של שינוי טכנולוגי – הנטייה לפרש יכולת חדשה באמצעות דפוסי הפעלה מוכרים, והקושי לזהות אצל היריב אימוץ טכנולוגיה והפעלתה בדרכים שונות משלנו. המנגנון השלישי ייחודי להפתעה הטכנולוגית־תורתית ונוגע לקושי לזהות מתי אמצעי ניסיוני, צירוף רכיבים או אלתור מקומי הופך ליכולת מבצעית של ממש. לאחר מכן אבחן כיצד מאפייני הסביבה הדיגיטלית מעצימים מנגנונים אלה, ולבסוף אדון בהתאמות הנדרשות בעבודת המודיעין.

מנגנוני כשל בזיהוי הפתעה טכנולוגית ותורתית

אסימילציה וראיית מראה

הטיית אסימילציה היא הנטייה לפרש תופעות חדשות על פי תבניות הידע והחשיבה הקיימות שלנו. בהערכת מודיעין, האסימילציה באה לא פעם לידי ביטוי ומתחזקת באמצעות ראיית מראה: שימוש בעצמנו כנקודת ייחוס להבנת האחר.[7] בהקשר הטכנולוגי, הטיה זו תוביל לבחינת היכולת החדשה לפי קצבי המו"פ וספי האמינות בתהליכי הפיתוח שלנו, במקום להבין את ניהול הסיכונים של היריב. היא גם תוביל לבחינת היכולת לפי האופן שבו אנחנו היינו משתמשים בה, במקום להבין אילו בעיות היריב מנסה לפתור באמצעותה, אילו אילוצים ניצבים בפניו וכיצד היא יכולה להשתלב במבנה הארגוני, בפיקוד ובשליטה ובלוגיסטיקה הייחודיים לו. תומס מאנקן מביא דוגמה לכך מן המעקב האמריקני אחר הצי היפני. ב־1940 קיבל הנספח הימי האמריקני בטוקיו מידע ממקור שנחשב מהימן על אודות טורפדו יפני שהונע בחמצן דחוס, ושנתוני הטווח, המהירות וראש הקרב שלו עלו במידה ניכרת על אלה שהכירו האמריקנים. המידע הועבר ללשכת החימוש של הצי האמריקני, אך נדחה כבלתי סביר. השימוש בחמצן נתפס כמסוכן מדי, ומומחי הלשכה לא האמינו שהיפנים השיגו יכולות שהצי האמריקני לא הצליח לפתח.[8]

באופן דומה, הטיית אסימילציה יכולה להתרחש גם בהקשר של טכנולוגיות העידן המודרני. כך, לדוגמה, במערב מקובל להבחין מבחינה מושגית בין סייבר טכנולוגי ובין השפעה פסיכולוגית, בעוד התפיסה הרוסית רואה בהם חלק ממרחב מידע שלם, ובו מתנהל עימות הכולל כלים טכנולוגיים, קינטיים ותודעתיים. ההבחנה התפיסתית של המערב יוצרת גם חלוקה ארגונית בין גופי סייבר, תודעה ומדיניות, ובשל כך קשה להבין את ההיגיון המחבר בין הרכיבים השונים במערכת הרוסית כמכלול.[9]

כדוגמה מתחום הבינה המלאכותית, מחקר שעסק באופן שבו היא מופיעה ונתפסת בספרות מקצועית ותורתית של צבא השחרור העממי הצביע על מאפיינים ייחודיים הנובעים מהתרבות האסטרטגית, מהמבנה הארגוני ומהצרכים המבצעיים של הצבא הסיני. מכאן שאימוץ הבינה המלאכותית לשימושים צבאיים בסין אינו צפוי לשחזר את הדפוסים האמריקניים, וניתוח המפרש את המאמץ הסיני כחיקוי מאוחר של השימוש האמריקני בבינה מלאכותית עלול להחמיץ את ההיגיון התורתי שהוא נועד לשרת.[10]

הטיה ארגונית־תרבותית

צבאות וקהילות מודיעין הם ארגונים בעלי משימות מוגדרות, אינטרסים פרטיקולריים, זהות מקצועית, זיכרון ארגוני והיררכיות של סמכויות ויוקרה. מאפיינים אלה משפיעים על נטייתם לייחס חשיבות לחידושים מסוימים ולהתעלם מאחרים. קרל בילדר ייחס

---

7 Jervis, R. (1976). Perception and misperception in international politics. Princeton University Press

8 Mahnken, T. G. (2002). Uncovering ways of war: U.S. intelligence and foreign military innovation, 1918–1941. Cornell University Press, pp. 70–71

9 אדמסקי, ד' (2015). אומנות אופרטיבית קיברנטית: מבט מזווית לימודי האסטרטגיה ומפרספקטיבה השוואתית (עשתונות, גיליון 11). מרכז המחקר של המכללה לביטחון לאומי; פלקוב, י' (2024). "לפרמט" את האויב והעולם לטובתנו: לוחמת התודעה הרוסית מהלכה למעשה. בתוך י' קופרוסר וד' סימן טוב (עורכים), השפעה והתערבות זרה באתגר אסטרטגי ומודיעיני (עמ' 19–32). המכון לחקר המתודולוגיה של המודיעין; המכון למחקרי ביטחון לאומי

10 Kania, E. B. (2021). Artificial intelligence in China's revolution in military affairs. Journal of Strategic Studies, 44(4), 515–542. https://doi.org/10.1080/01402390.2021.1894136

לכל זרוע צבאית "אישיות מוסדית" – דיוקן המכתיב אילו איומים וטכנולוגיות ייתפסו כנוגעים לה וכיצד הם יפורשו בתוך הארגון. לכן ארגון עשוי לפרש טכנולוגיה חדשה כמכפיל כוח של תפיסתו הקיימת, גם כאשר היא מאפשרת ארכיטקטורה אחרת לחלוטין ואולי טובה יותר. אותה הטיה עלולה לגרום לארגון המזהה את עצמו עם פלטפורמות ועם התמחות מסוימת להחמיץ השפעה מערכתית של טכנולוגיה המעבירה את מרכז הכובד הארגוני למקום אחר.[11]

סטיבן רוזן הדגיש את חשיבותם של מסלולי הקידום בארגונים. הוא הראה שחדשנות מקבלת כוח מוסדי כאשר קצינים המזוהים עימה מקודמים, כאשר מוקמות יחידות ייעודיות וכאשר ההכשרה, התקצוב והיוקרה משתנים. המודיעין צריך לראות במאפיינים אלה סימנים חשובים המעידים כי אמצעי ניסיוני הופך לחלק מהתפיסה המבצעית של היריב.[12]

מכאן גם חשיבותה של חדשנות הצומחת מלמטה. מי שמחפש אישור רשמי של הצמרת הצבאית או מסמך תורתי עלול להחמיץ תהליך המתחיל באלתורים, בניסויי שדה ובקבוצות מקצועיות שוליות, שרק בהמשך הדרך מקבל הכרה רשמית. השימוש הגרמני בתותח הנ"מ 88 מ"מ נגד טנקים ממחיש כיצד שימוש שלא תוכנן במקור עשוי להתפשט מהשטח ולהפוך לדפוס מערכתי.[13]

התרבות האסטרטגית הלאומית משפיעה במידה ניכרת על ההטיות הארגוניות. דימה אדמסקי הראה כי ברית המועצות, ארצות הברית וישראל פירשו את מהפכת המידע הצבאית בדרכים שונות: הסובייטים נטו להמשגה תאורטית ומערכתית אך התקשו לממשה, האמריקנים הדגישו עליונות במידע ודיוק של האמצעים הקינטיים, וישראל נטתה לאימוץ מעשי וטקטי של טכנולוגיות, לעיתים בלי לנסח את השינוי המערכתי המתחייב מהן.[14]

פער ההבשלה

פער ההבשלה (Latency gap) מתייחס למצב שבו המודיעין מצליח לזהות את הטכנולוגיה, ואף את היגיון השימוש בה, אך מחמיץ את העיתוי שבו הצטברות של מו"פ, הצטיידות והטמעה חוצה את הסף והופכת את הטכנולוגיה ליכולת מערכתית של ממש.
חדשנות צבאית כוללת תהליכי פיתוח, ניסויים, למידה ותיקון, לצד תהליכי אינטגרציה, הצטיידות, הכשרות והטמעה, וכן שינויים מבניים, תפעוליים ופיקודיים, שלעיתים נמשכים שנים רבות. שירותי מודיעין נוטים להמתין ל"הוכחת יכולת", כגון הפעלה מעשית במלחמה, אף שהשינוי המכריע התרחש זמן רב קודם לכן בבניין הכוח: בהקמת יחידות, בהכשרה, בתרגילים, בממשקים ובשיטות הגיוס והפיקוד.[15]

פער נוסף נובע מהשלכת ספי ההבשלה שלנו על היריב. ממסדים ביטחוניים מערביים נוטים לדרוש אמינות, בטיחות וביצועים גבוהים לפני הכרזה על יכולת מבצעית; מדינות כמו איראן או ארגונים לא־מדינתיים עשויים להסתפק במערכת "טובה דיה", במיוחד כאשר היא זולה ומופעלת במסה. המודיעין יכול אפוא להבין נכון את כיוון הפיתוח ובכל זאת לאחֵר בהערכת מועד הפיכתו לאיום ממשי.[16] נושאות המטוסים היפניות הן דוגמה להחמצה מודיעינית (אמריקנית במקרה זה) של המעבר מאימוץ פלטפורמה להבשלתה כחלק ממערכת לחימה. נושאות מטוסים פעלו בצי היפני עוד לפני 1941. באפריל אותה שנה הוקם הצי האווירי הראשון, שאיגד כמה נושאות מטוסים ואת קבוצות האוויר שלהן במסגרת מבצעית אחת. בחודשים שלאחר מכן גובשו ותורגלו השיטות להפעלתן המשולבת בהתקפה, ובדצמבר כבר הופעלו שש נושאות מטוסים בתקיפה המתואמת על פרל הארבור.[17]

---

11 Builder, C. H. (1989). The masks of war: American military styles in strategy and analysis. Johns Hopkins University Press

12 Rosen, S. P. (1991). Winning the next war: Innovation and the modern military. Cornell University Press

13 Westermann, E. B. (2001). Flak: German anti-aircraft defenses, 1914–1945. University Press of Kansas

14 Adamsky, D. (2010). The culture of military innovation: The impact of cultural factors on the revolution in military affairs in Russia, the US, and Israel. Stanford University Press

15 Murray, W., & Millett, A. R. (Eds.). (1996). Military innovation in the interwar period. Cambridge University Press; Horowitz, M. C. (2010). The diffusion of military power: Causes and consequences for international politics. Princeton University Press

16 Defense Science Board. (2010). Report of the Defense Science Board 2008 summer study on capability surprise: Volume II, supporting papers. Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, pp. 95–97; McKenzie, K. F., Jr., Spleeters, D., & Lincy, V. (2023, April 24). Iran's military drone program: Security implications and policy responses. The Washington Institute for Near East Policy

17 Till, G. (1996). Adopting the aircraft carrier: The British, American, and Japanese case studies. In W. Murray & A. R. Millett (Eds.), Military innovation in the interwar period (pp. 191–226). Cambridge University Press. https://doi.org/10.1017/CBO9780511601019.006; Parshall, J., & (Wenger, J. M. (2011, December). Pearl Harbor's overlooked answer. Naval History, 25(6

ההפתעה הטכנולוגית־תורתית בעידן הדיגיטלי

מנגנוני הכשל שתוארו אינם חדשים, אך העידן הדיגיטלי משנה את הסביבה הטכנולוגית שבה הם באים לידי ביטוי. יכולות צבאיות עדיין נשענות על פלטפורמות, אך חשיבות השילוב בין רכיבי חומרה ובין תוכנה, נתונים וקישוריות הולכת וגדלה. רכיבים מסחריים, טכנולוגיות דו־שימושיות וקוד פתוח מורידים את חסמי הכניסה ומעניקים יתרון למי שמסוגל לצרפם ולהטמיעם מהר יותר. דייב ונבל מציע להמשיג דינמיקה זו כ"אסימטריה סינתטית": בנייה מכוונת של חוסר איזון אסטרטגי באמצעות צירוף טכנולוגיות זולות, דו־שימושיות וזמינות, ליצירת עוצמה צבאית ניכרת שאינה חופפת למדדי העוצמה המסורתיים.[18]

שלושה מאפיינים של הסביבה החדשה משפיעים על יכולתו של המודיעין לאתר איום טכנולוגי מתפתח ולהבינו: דחיסת זמן, המצמצמת את מרחב ההתרעה; זמינות אזרחית, המפזרת את בניין הכוח בין המערכת הצבאית למגזר הפרטי; וצימוד פיזי־דיגיטלי בין רכיבים, המגדיל את העמימות ואת הקושי לזהות שינויים מערכתיים.

דחיסת זמן: קיצור מחזורי השינוי

דחיסת הזמן היא מאפיין של הסביבה הדיגיטלית המעמיק את הפער בהבנת הבשלתה של יכולת צבאית. בעידן הדיגיטלי, יכולת עשויה לעבור מניסוי להפעלה מבצעית בפרק זמן קצר בהרבה מבעבר, וכך להקשות עוד יותר על הצד השני להבין את משמעותה ולהיערך לה בזמן.

מקומן של מערכות מבוססות תוכנה ובעלות מבנה מודולרי הולך וגדל, והן מתאפיינות במחזורים קצרים יותר של פיתוח, ניסוי, הפעלה ותיקון. קצב השינוי בתוכנה מהיר מזה שבחומרה, ואילו תהליכי הפיתוח וההצטיידות הביטחוניים עדיין בנויים במידה רבה לפי מודלים שנועדו לפלטפורמות חומרה.[19] שינויים במערכות אלה יכולים להיעשות בהדרגה, להיבחן ולהזין את הגרסה הבאה, בלי להמתין להשלמתו של תהליך פיתוח אחד ארוך.

מקור נוסף לדחיסת הזמן הוא העברת חלק מתהליכי הפיתוח והאינטגרציה אל מחוץ לממסד הביטחוני. תוכנות, חיישנים, רכיבי תקשורת ומערכות בלתי מאוישות מפותחים במקרים רבים בידי חברות מסחריות, חברות הזנק ומהנדסים אזרחיים. שחקנים אלה יכולים לקיים קשר ישיר עם המפעילים ולשנות מוצר קיים בלי לעבור את מלוא תהליך הדרישות והפיתוח הצבאי. עם זאת, הבשלה מערכתית עדיין מחייבת התאמה של דפוסי ההפעלה, ההכשרה, התחזוקה והארגון, ולכן פיתוח טכני מהיר אינו שקול בהכרח ליכולת צבאית בשלה.

כך, לדוגמה, מחקר שבדק את המערכת האוקראינית מאז הפלישה הרוסית ב־2022 מתאר מעבר ממודל שנשען בעיקר על פיתוח ממשלתי ריכוזי למודל המשלב חברות פרטיות ומהנדסים אזרחיים. הקשר הישיר בין יחידות בחזית ובין המפתחים מאפשר לבצע התאמות בעקבות בעיות שהתגלו בהפעלה, לעיתים בלי להמתין לגיבוש דרישה רשמית במטה הכללי. שלב הפיתוח של רעיון ואב־טיפוס, שנמשך במערכת הממסדית 3–20 שנים, התקצר במגזר הפרטי לשבועות עד חודשים. תהליך האישור של מערכות בלתי מאוישות ולוחמה אלקטרונית הושלם לעיתים בתוך כשבועיים.[20]

דוגמה נוספת היא תגובתה המהירה של SpaceX לשיבוש רוסי של שירות Starlink בראשית המלחמה. בכיר בפנטגון מסר כי החברה זיהתה את הבעיה והפיצה עדכון תוכנה בתוך יום, והנגיד זאת לזמן הממושך שהיה נדרש למערכת ממשלתית כדי לנתח את התקלה, לגבש מענה ולהתקשר עם ספק.[21]

---

18 Horowitz (2010); Soare, S. R., Singh, P., & Nouwens, M. (2023, February 17). Software-defined defence: Algorithms at war. International Institute for Strategic Studies; Venable, D. (2026). Synthetic asymmetry: Intelligence advantage and strategic imbalance in the age of technological convergence [Preprint]. SSRN

19 Soare et al. (2023)

20 Bondar, K. (2025). How Ukraine rebuilt its military acquisition system around commercial technology. Center for Strategic and International Studies

21 Losey, S. (2022, April 20). SpaceX shut down a Russian electromagnetic warfare attack in Ukraine last month, and the Pentagon is taking notes. Defense News; Insinna, V. (2022, April 20). SpaceX beating Russian jamming attack was "eyewatering": DoD official. Breaking Defense

תרחיש הפתעת סייבר שתאגיד RAND בנה מציג ביטוי אפשרי לדחיסת הזמן בהקשר של בינה מלאכותית, המסוגלת ללמוד ולהשתפר במהירות רבה בלי צורך בהתערבות אנושית. בתרגיל השתפרה מערכת בינה מלאכותית במהירות, זיהתה חולשות אצל היריב וביצעה התאמות בקצב שעלה על יכולתם של מוסדות המדינה להבין את השינוי ולהגיב לו.[22]

מול מחזורי השינוי המקוצרים ניצבים ארגוני מודיעין (וגופים בוני כוח) שתהליכיהם נותרו במידה רבה מותאמים לעידן הקודם. חלק מההיגיון של מעגל המודיעין המסורתי עדיין תקף: מידע חדש צריך להיאסף, לעבור תהליכי עיבוד, אימות, הצלבה ובדיקה, להפוך להערכה מוסמכת ולהיתרגם לתוצרים מודיעיניים ולתהליכי הטמעה בקרב צרכנים ומקבלי החלטות. אך בעידן הדיגיטלי, התהליך הזה עומד במתח הולך וגדל עם קצב השינוי ונפחי המידע.[23] בהקשר הטכנולוגי, היריב עשוי לעבור כמה מחזורי ניסוי ותיקון של יכולת, עוד לפני שהמודיעין הספיק להשלים את הערכת הגרסה הקודמת שלה.

ירידת חסמי אימוץ וזמינות אזרחית

המאפיין השני הוא ירידת חסמי האימוץ והיכולת להפעיל מסה של אמצעים זולים, חלקם אף חד־פעמיים. מייקל הורוויץ הראה כי העלות הכספית הגבוהה של נושאות מטוסים או נשק גרעיני הגבילה את תפוצתם וביצרה את יתרון המעצמות.[24] לעומת זאת, האינטרנט, הניווט הלווייני, הבינה המלאכותית והרחפנים נשענים על השקעות אזרחיות ועל שרשראות אספקה עולמיות, ולכן זמינים לשחקנים רבים יותר. אפשר אולי לעכב את תפוצתם של תוכנה ורכיבים דו־שימושיים באמצעות בקרות יצוא, הגבלות גישה, תקינה ושליטה ברכיבי מפתח, אך אי אפשר למנוע אותה לאורך זמן.

המעבר מפלטפורמה יקרה למסה של רכיבים קטנים משנה גם את מדדי העוצמה. ספירת פלטפורמות ואיכותן הטכנית אינן משקפות בהכרח את רמת הקטלניות של רשת מבוזרת, שבה אובדן רכיב יחיד אינו פוגע בתפקוד הכולל והאפקט נוצר מהקישוריות, מהכמות ומהיכולת להחליף במהירות אמצעים שאבדו.

תפוצת השימוש ברחפנים אזרחיים זולים באוקראינה שינתה את יחסי העלות–תועלת: מסה של רחפני FPV, תוכנות אזרחיות ומידע גלוי מאפשרת לסגור מעגלי אש נגד מטרות יקרות ולהכביד על מערכי הגנה. דפוס זה, שהחל אצל שחקנים חלשים ופחות עתירי תקציב, הוכיח את עצמו ומחלחל בהדרגה גם לצבאות המעצמות שהחלו להסיט חלק ממאמצי הייצור וההצטיידות למאסות של מערכות זולות.[25]

אותו היגיון פועל גם במרחב המידע. פלטפורמות אזרחיות מאפשרות לשחקנים קטנים או אזרחיים להפעיל מאמצי גיוס, השפעה ולוחמה פסיכולוגית בקנה מידה שבעבר דרש תשתית מדינתית. היתרון היחסי של הממסד הביטחוני נשחק, והאיזונים והממשקים בין המדינה לאזרחים משתנים.[26]

מה המשמעויות למודיעין? הפיכתו של האקוסיסטם האזרחי למרכז כובד של חדשנות צבאית מחייבת את המודיעין הטכנולוגי לראות בו יעד מרכזי נוסף לכיסוי ולמעקב, לצד תעשיות ביטחוניות ופרויקטים צבאיים מסווגים. ירידת חסמי האימוץ מאיינת חלק מהיכולת המסורתית להעריך את כשירותו המבצעית של היריב: אומדן המלאי הקיים אינו מספיק, שכן היריב מסוגל לשנות או להחליף במהירות מערכות שנשחקו. לצד המלאי נדרש אפוא לבחון את קיבולת האינטגרציה וההתחדשות: היכולת לרכוש רכיבים

---

22 Smith, G., Hage, G., Heitzenrater, C., Chessen, M., & Girven, R. S. (2026). Infinite potential: Insights from the cyber surprise scenario: Post-series scenario report from a sequence of Day After artificial general intelligence exercises (RR-A4626-1). RAND Corporation. https://doi.org/10.7249/RRA4626-1

23 Stenslie, S., Haugom, L., & Vaage, B. H. (Eds.). (2021). Intelligence analysis in the digital age. Routledge. https://doi.org/10.4324/9781003168157

24 Horowitz (2010)

25 Kallenborn, Z. (2022, May 12). Seven (initial) drone warfare lessons from Ukraine. Modern War Institute; U.S. Department of Defense. (2023). Military and security developments involving the People's Republic of China 2023: Annual report to Congress. Office of the Secretary of Defense, pp. 97–98; Vergun, D. (2025, July 16). Pentagon to increase low-cost drone production in U.S. U.S. Department of Defense בנג'ו, י' (21 במאי 2025). מהפכת רחפני FPV ומשמעויותיה בלוחמת היבשה ובממדים נוספים. המכון למחקרי ביטחון לאומי

26 Singer, P. W., & Brooking, E. T. (2018). LikeWar: The weaponization of social media. Houghton Mifflin Harcourt; Libicki, M. C., Gompert, D. C., Frelinger, D. R., & Smith, R. E. (2007). Byting back: Regaining information superiority against 21st-century insurgents: RAND Counterinsurgency Study—Volume 1 (MG-595/1-OSD). RAND Corporation

ממקורות שונים, לחברם למערכת מבצעית, להפיק לקחים מן ההפעלה ולהכניס שינויים בגרסאות הבאות. ככל שהטכנולוגיה זמינה ומודולרית יותר, יכולות אלה נעשות מרכיב חשוב יותר בהערכת פוטנציאל הכוח של היריב.

צימוד פיזי־דיגיטלי וניידות בין ממדים

המאפיין השלישי הוא הצימוד בין תוכנה, נתונים וקישוריות ובין האפקט הפיזי. רכיבים דיגיטליים אינם עוד שכבה תומכת בלבד אלא רקמת החיבור של שרשרת הגילוי, העיבוד, ההחלטה והתקיפה. לכן עדכון קוד או שינוי בקישוריות עשויים לשנות את הדיוק, הקצב והקטלניות בלי להכניס לזירה פלטפורמה חדשה ובלי ליצור חתימה פיזית ברורה.[27]

הצימוד מגביר גם את הניידות התפקודית בין הממדים. אלגוריתם לזיהוי מטרות, פרוטוקול תקשורת או שיטה לחיבור חיישן לאמצעי תקיפה יכולים לעבור מן היבשה אל הים, האוויר, החלל או הסייבר. המעבר יחייב התאמות חומרה ותוכנה, ממשקים, נתונים והקשר המבצעי, אך הוא מפחית את התלות בין הזירה שהיכולת פותחה בה ובין הזירה שבה היא תיושם. חלוקה מודיעינית קשיחה לפי זרועות ופלטפורמות עלולה לכן להחמיץ תנועה רוחבית של דפוס פעולה.[28]

צימוד מערכתי מייצר גם עמימות וסיבוכיות. אותה תשתית תקשורת או שליטה עשויה לשרת מטרות טקטיות ואסטרטגיות, אזרחיות וצבאיות. תקיפה שנועדה לשבש יכולת קונבנציונלית עלולה להתפרש כהכנה למהלך אסטרטגי, בעוד פעילות איסוף דיגיטלית עשויה להיראות כהכנה לתקיפת סייבר.[29] כמו כן, ככל ששרשרת ההרג נעשית מהירה ואוטונומית יותר, ההתרעה הטקטית־מצבית המבוססת על עיבוד אנושי בלבד עלולה לאבד מערכה.

הרחפנים כמקרה בוחן של התפתחות מערכת לחימה בסביבה דיגיטלית

לאחר הפלישה הרוסית בפברואר 2022 הרחיבה אוקראינה במהירות את השימוש ברחפנים מסחריים וברחפני FPV. כלים שהופעלו בתחילה במסגרת יוזמות מקומיות של יחידות, מתנדבים וחברות פרטיות שולבו בהדרגה באיסוף, בהכוונת אש, בתקיפה ובהערכת תוצאותיה. ההתמסדות ניכרה בהקמת יחידות ייעודיות במסגרות הלוחמות, בפיתוח הכשרות ושיטות הפעלה ובייסודה של זרוע המערכות הבלתי מאוישות ב־2024. בתוך כשנתיים התפתח אפוא השימוש ברחפנים מאוסף פתרונות מקומיים למרכיב קבוע בבניין הכוח ובהפעלתו.[30]

דחיסת הזמן ניכרה גם במחזור החיקוי והתגובה שהתפתח בין הצדדים. אוקראינה הייתה חלוצה בהפיכת רחפני FPV מסחריים לחימוש תקיפה זול, אך רוסיה אימצה במהירות את דפוס ההפעלה. כבר בקיץ 2023 הפעילה רחפני FPV בהיקף נרחב, ועד סוף 2024 שילבה מחלקות רחפנים ביחידות מתמרנות, הרחיבה את הייצור וגיבשה הוראות ותורות הפעלה. בהמשך הפעילה רוסיה בהיקף הולך וגדל רחפנים הנשלטים באמצעות סיב אופטי, שפגעו ביעילותו של השיבוש האלקטרוני שההגנה האוקראינית נשענה עליו; אוקראינה מצידה פעלה בתוך חודשים לפיתוח ולייצור מערכות דומות. יתרון שנוצר בצד אחד נשחק במהירות, משום שרכיבי המדף, הידע הגלוי ורשתות היצרנים והמתנדבים אפשרו לצד האחר לחקות אותו ולהתאים לו מענה.[31]

המבנה המודולרי של הטכנולוגיה מאפשר גם להפיק מאותה פלטפורמה אפקט שונה באמצעות שינוי המערכת שסביבה. במבצע "קורי העכביש" ביוני 2025 תקפה אוקראינה בסיסי מפציצים בעומק רוסיה באמצעות רחפנים קצרי טווח שהוברחו לשטח המדינה,

---

27 פינקל (2007), עמ' 72

28 Soare et al. (2023)

29 Acton, J. M. (2018). Escalation through entanglement: How the vulnerability of command-and-control systems raises the risks of inadvertent nuclear war. International Security, 43(1), 56–99. https://doi.org/10.1162/isec_a_00320; Buchanan, B., & Cunningham, F. S. (2023). Preparing the cyber battlefield: Assessing a novel escalation risk in a Sino-American crisis. In R. Chesney, J. Shires, & M. Smeets (Eds.), Cyberspace and instability (pp. 60–98). Edinburgh University Press

30 Bondar, K. (2024, November 19). Why Ukraine is establishing unmanned forces across its defense sector and what the United States can learn from it. Center for Strategic and International Studies; Molloy, O. (2026, March 11). Drone warfare in Ukraine: From myths to operational reality, Part 1. Australian Army Research Centre

31 Pettyjohn, S. (2024, February 8). Evolution not revolution: Drone warfare in Russia's 2022 invasion of Ukraine. Center for a New American Security; Andreika, V. (2025, September–October). Russia's changes in the conduct of war based on lessons from Ukraine: Adapting technology, force structures, and the defense industry. Military Review; Sutea, V. (2026, February 24). Fiber-optic drones have emerged as critical kit for both Russia and Ukraine. Atlantic Council

הוסוו במבנים שהובלו על משאיות ושוגרו בסמוך לבסיסים. הטווח האסטרטגי של המבצע נבע משילובם במערכת שכללה מודיעין, לוגיסטיקה חשאית, הסוואה, תקשורת ותכנון מבצעי. המקרה מדגים שהערכת ביצועי הפלטפורמה לבדם אינה מספיקה להבנת היכולת הנבנית סביבה.[32]

הצימוד הפיזי־דיגיטלי ניכר גם ברחפן עצמו: יכולתו נקבעת לא רק על פי מאפייניו הפיזיים, אלא גם על פי התוכנה שעליו, קישור הנתונים והמערכות הדיגיטליות שהוא מחובר אליהן. מערכת DELTA האוקראינית, לדוגמה, משלבת שידורי וידאו מרחפנים וממצלמות נייחות עם מידע מחיישנים וממכ"מים בתמונת מצב משותפת. מודולים נוספים מאפשרים לתכנן נתיבי טיסה ואזורי אחריות, לתאם משימות בזמן אמת ולחבר את המידע לתהליכי איסוף ורכישת מטרות. הרחפן משמש לא רק כפלטפורמת צילום או תקיפה עצמאית, אלא כרכיב פיזי במערכת המופעלת באמצעות תוכנה, נתונים וקישוריות. משום כך אפשר לשנות את תפקידו ואת ערכו המבצעי באמצעות עדכון תוכנה, החלפת קישור הנתונים או חיבור למערכת ניהול קרב, גם בלי שינוי מהותי בפלטפורמה עצמה.[33]

הזירה הישראלית ממחישה את הקושי לפרש את משמעותם המערכתית של שינויים כאלה ולהיערך אליהם בזמן. ב־7 באוקטובר 2023 השתמשה חמאס ברחפנים מסחריים להטלת מטענים על מגדלי תצפית, חיישנים ומערכות נשק בגבול הרצועה, כחלק ממהלך משולב של פריצת המכשול ותקיפת מוצבים. ההפתעה לא נבעה מעצם השימוש ברחפנים, אלא מהפעלתם במסגרת משימה מערכתית לנטרול רכיבי הפיקוד והשליטה שצה"ל נשען עליהם בהגנת המרחב. מאוחר יותר, במרס 2026, החל חזבאללה להפעיל בדרום לבנון רחפני FPV הנשלטים באמצעות סיב אופטי, דפוס שהתפתח קודם לכן בזירת אוקראינה. החלפת קישור הרדיו בממשק סיב אופטי אפשרה לרחפנים לעקוף אמצעי שיבוש אלקטרוניים והציבה קושי חדש בפני מערכי הגילוי והשיבוש של צה"ל (שהמענה לו נותר חלקי נכון לכתיבת שורות אלה). בשני המקרים, עצם קיומם של הרחפנים והאפשרות לעשות בהם שימוש צבאי לא היו חדשים. הפער נגע להבנת האופן שבו ישולבו במערכת הפעולה של היריב, לקצב הבשלתה של היכולת ולתרגום ההכרה באיום למענה מבצעי בזמן.[34]

התפתחות השימוש ברחפנים במלחמות האחרונות ממחישה כיצד שלושת מאפייני הסביבה הדיגיטלית פועלים יחד: הזמינות האזרחית מספקת רכיבים, ידע ובסיס ייצור; דחיסת הזמן מאיצה את מחזורי הניסוי, הלמידה והחיקוי; והצימוד הפיזי־דיגיטלי מאפשר לשנות את תפקודה של הפלטפורמה באמצעות תוכנה, נתונים וקישוריות. הצבאות הכירו את האמצעי, אך הופתעו מהאופן ומהמהירות של הפיכתו לרכיב במערכת לחימה, באמצעות שינוי בממשקים, בשיטות ההפעלה ובהתארגנות. הדבר מדגיש את חשיבותה של הבנה מערכתית של הטכנולוגיה: הצורך לעקוב לא רק אחר סוגי הרחפנים וכמותם, אלא גם אחר מחזורי הלמידה והאופן שבו הם משתלבים במערכות רחבות יותר ומשנים את פני שדה הקרב.

המענה המודיעיני: מהכרת הרכיבים להבנת המערכת

התמודדות עם אתגר ההפתעה הטכנולוגית בעידן הדיגיטלי מחייבת התאמה של עקרונות המודיעין להתרעה לאופן שבו יכולות צבאיות נבנות, משתנות ומבשילות בעידן זה. השינויים נוגעים לשלושה רבדים: גבולות המודיעין, מושא המעקב וארגון תהליך הלמידה. יחד, הם עשויים לתרום לצמצום הפער בין הכרת רכיבי היכולת הטכנולוגית ובין הבנת המערכת שהיריב בונה בסיועה או על בסיסה.

הרחבת גבולות האיסוף והמחקר לסביבה האזרחית

המענה הראשון הוא הוספת שכבת איסוף ומחקר על האקוסיסטם האזרחי, לצד המשך המעקב אחר פרויקטים צבאיים רשמיים וסודיים. צי"ח המתמקד בתעשיות ביטחוניות ובפלטפורמות צבאיות מוכרות עלול להחמיץ טכנולוגיות ויישומים המתפתחים

32 Balmforth, T., & Hunder, M. (2025, June 1). To attack Russian air bases, Ukrainian spies hid drones in wooden sheds. Reuters

33 NATO Allied Command Transformation. (2024, July 12). Battlefield innovation: Ukraine's DELTA system paves the way for Allied interoperability at CWIX24; Ministry of Defence of Ukraine. (2025, January 27). Kateryna Chernohorenko: The Mission Control module is now accessible to all DELTA users

34 Page, J. M. (2025). Drones and the Hamas-led attack of 7 October 2023: Innovation and implications. Perspectives on Terrorism, 19(1), 1–33; Gebeily, M., Lubell, M., & Cartier, C. (2026, May 12). Evolving drone war in southern Lebanon clouds Iran peace prospects. Reuters; Stracquadanio, A. (2026, June 23). Frustrating Israel, fiber-optic killer drone technology has arrived in southern Lebanon. Defense News
ענתבי, ל' ואדר, א' (5 בפברואר 2024). רחפני FPV: משדה הקרב באוקראינה למזרח התיכון? מבט על, גיליון 1825. המכון למחקרי ביטחון לאומי

מחוץ לגבולות אלה. סריקת אופק נועדה להשלים את הכיסוי באמצעות איתור שיטתי של סימנים מוקדמים, מגמות מתהוות והתפתחויות שטרם נתפסו כאיום מגובש.[35] רכיבי מדף וטכנולוגיות דו־שימושיות מפותחים מחוץ לממסד הביטחוני ואפשר לרכשם בשוק החופשי, ולכן יש לעקוב גם אחר מגמות במגזר הטכנולוגי, שווקים וספקים, שרשראות אספקה, פורומים של קוד פתוח וקהילות מפתחים. הדבר מחייב גם גישה לידע ולמומחיות המצויים בסביבה האזרחית ופיתוח קשרים מתאימים עימם.[36]
הרחבת הכיסוי אינה יכולה להסתכם בזיהוי הרכיבים הזמינים או הנרכשים. במציאות של אסימטריה סינתטית, היתרון עשוי להיווצר מן האופן שבו היריב מחבר טכנולוגיות קיימות ומתרגם אותן בתוך המערכת הצבאית ליכולת מבצעית. לכן יש לחפש דפוסי התכנסות (patterns Convergence), כוונות שימוש וקצבי הרכבה, ולבחון באיזו תפיסת הפעלה משתלב הצירוף המתהווה ואילו התאמות ארגוניות נלוות אליו. הסריקה צריכה להשתלב בתהליך של מתן פשר (making-Sense): לא להסתפק בשאלה אילו טכנולוגיות היריב משיג, אלא לבחון לאיזו בעיה מבצעית נועד צירופן לתת מענה.[37]

הרחבת המעקב מאמצעים להבשלה מערכתית

בשלות אינה נמדדת רק לפי יכולתה של הטכנולוגיה או לפי ביצועיו של אמצעי בודד. היא תלויה במשימה שהיכולת נבנית לשמה ובשילוב בין האמצעי ובין תפיסת ההפעלה, המבנה הארגוני, כוח האדם, התקשורת, הנתונים והמערכים התומכים בו. יכולת עשויה להיות בשלה להפעלה מקומית או למשימה מוגדרת, אך עדיין לא להפעלה רחבה. לכן על המודיעין להעריך את רמת הבשלות הנוכחית, את כיוון ההתפתחות ואת קצב השינוי, באמצעות מעקב אחר כמה קבוצות של סימנים:

א. שינוי בשפה המקצועית, בתרחישי הייחוס, בניסויים ובתרגילים, שעשוי להעיד על גיבוש תפיסת הפעלה חדשה.
ב. חיבור האמצעי למערכות נוספות, ובהן חיישנים, תקשורת, נתונים, פיקוד ושליטה, אש ולוחמה אלקטרונית; וכן שינויים בתוכנה, בקישור הנתונים ובממשקים המרחיבים את תפקידו בלי לשנות בהכרח את הפלטפורמה עצמה.
ג. הקמת יחידות, שינוי משימותיהן של מסגרות קיימות, יצירת מקצועות והכשרות ומיסוד אחריות פיקודית ומקצועית; לצד הקצאת תקציב, סמכות ויוקרה לתחום וקידום בעלי תפקידים המזוהים עימו.
ד. התהוותם של מנגנוני למידה והסתגלות, ובהם קשר ישיר בין מפעילים, מפתחים ויצרנים, מעורבות של חברות ומתנדבים מן המרחב האזרחי, הפצת ידע בין יחידות וקצב השינויים בתוכנה, בחומרה ובשיטות ההפעלה בתגובה למעני היריב.
ה. עדויות ליכולת להפיק הישג מבצעי חוזר בתרגילים, בניסויים או בהפעלות מוגבלות, לרבות בתנאי הפרעה ומול אמצעי נגד, כדי להבחין בין הצלחה חד־פעמית ובין יכולת עקבית.
ו. מעבר מניסוי או מאלתור מקומי ליכולת שאפשר לשכפל ולהפעיל שוב בהיקף המתאים למשימה, לרבות ייצור והצטיידות, הפצה בין יחידות וזירות ויצירת מערכי הכשרה, תחזוקה, אספקה והחלפה המאפשרים להתמיד בהפעלתה.

לרוב, סימן יחיד לא יספיק כדי להוכיח שיכולת הבשילה. יש לבחון את הצטברות הסימנים ואת הקשרים ביניהם, לצד חסמים כגון מחסור במפעילים, קשיי תחזוקה, תלות בשרשרת אספקה, בעיות תקשורת או קושי להפיץ את היכולת מעבר ליחידות מצטיינות. ההערכה צריכה גם להבחין בין בשלות מקומית, בשלות בזירה מסוימת והטמעה רחבה בבניין הכוח.
לבסוף, יש להעריך את הבשלות לפי דרישות היריב ולא לפי הספים המקובלים אצלנו. יריב המוכן לקבל אמינות נמוכה יותר, שיעורי אובדן גבוהים וסיכוני בטיחות עשוי להגיע ליכולת יעילה מוקדם מכפי שנעריך באמצעות אמות המידה שלנו. מטרת המעקב היא לזהות את מסלול ההבשלה ולהתריע על התקרבות לסף המבצעי, ולא להמתין עד שהיכולת תוכח במלואה בשדה הקרב.

שילוביות בתהליך ההתרעה הטכנולוגית-תורתית

מאפייני הסביבה הדיגיטלית שנדונו במאמר – דחיסת הזמן, הזמינות האזרחית והצימוד הפיזי־דיגיטלי – מלמדים שהסימנים להתהוותה של יכולת צבאית, שאיתורם מוטל לכאורה על המודיעין, יהיו למעשה מפוזרים בין גופים שונים. גורמי האיסוף והמחקר עשויים לזהות את כוונות היריב ואת דפוסי ההצטיידות; גורמים טכנולוגיים ידעו לעמוד על בשלות הרכיבים והממשקים ביניהם; הכוחות בשטח את השפעתם המבצעית; גופי בניין הכוח את השינויים הארגוניים והתורתיים; והתעשייה והמחקר האזרחיים את

35 אלון, נ' (2018). סריקת האופק (Horizon scanning): תהליך מסייע בתהליכי קבלת החלטות ברמה הלאומית (מחקר עומק מס' 4). המכון לחקר המתודולוגיה של המודיעין, המרכז למורשת המודיעין

36 גוטרמן, ע' (16 בינואר 2023). מודיעין פתוח: מסגרת חדשה ליחסים בין ארגוני המודיעין לסביבה האזרחית. המכון לחקר המתודולוגיה של המודיעין

37 Cuhls, K. E. (2020). Horizon scanning in foresight: Why horizon scanning is only a part of the game. Futures & Foresight Science, 2(1), Article e23. https://doi.org/10.1002/ffo2.23; Habegger, B. (2009). Horizon scanning in government: Concept, country experiences, and models for Switzerland. Center for Security Studies, ETH Zurich

ההתפתחויות שמחוץ למערכת הביטחונית.

ממסקנה זו נגזר הצורך להטמיע דפוסי שילוביות בתהליכי הלמידה: מסגרת שבה הגורמים מנסחים יחד את שאלת המחקר, מחברים בין הידע והיכולות שברשותם ועוקבים אחר השינוי משלביו המוקדמים ועד הבשלתו המערכתית. אין הכוונה להקמתו של גוף קבוע סביב כל טכנולוגיה חדשה, אלא לגישה עקרונית (שלעיתים תתארגן במבנה זמני או קבוע) להתמודדות עם ידע מפוזר ומשתנה תדיר.[38]

במסגרת זו, למידה בחיכוך והערכת נטו הן פעולות משלימות. דיווחים מבצעיים וסימנים טכנולוגיים צריכים לעבור במהירות עיבוד וניתוח מחקריים, תיקוף בין יחידות וזירות וניסוי טכנולוגי־מבצעי, כדי להבין טוב ומהר יותר אם לפנינו יכולת מקומית או שמא עדות ליכולת מערכתית שמבשילה. בד בבד יש לבחון את היכולת המתהווה מול המערכת שלנו: אילו נקודות תורפה טכנולוגיות או מבצעיות היא עלולה לנצל, האם היא שוחקת יתרון איכותי, והאם קצב ההתאמה שלנו הולם את קצב השינוי של היריב. הערכת נטו זו מחייבת את השתתפות המודיעין, מפעילי הכוח ובוני הכוח, משום ששום גורם אינו מחזיק לבדו בתמונה המלאה של המפגש בין המערכות.[39]

השילוביות צריכה להימשך גם לאחר שניתנה התרעה. המודיעין צריך לעקוב אחר שינויים נוספים ביכולת ולהצביע עליהם, ולוודא שמפעילי הכוח ובוניו מבינים את השינויים ובוחנים את ההשלכות על תהליכי המוכנות ובניית המענה. מסגרות רב־ארגוניות שנבנו בתחומי הסייבר והראייה הממוחשבת מציעות דגמים אפשריים לחיבור בין מודיעין, טכנולוגיה, הפעלת כוח ותעשייה אזרחית, כדי לקצר את מחזור הזיהוי, הניסוי וההחלטה.[40]

סיכום: הפתעה טכנולוגית־תורתית בעידן הדיגיטלי

העידן הדיגיטלי אינו משנה מהותית את תופעת ההפתעה הטכנולוגית, שימיה כימי תופעת המלחמה למן העת העתיקה. אך הוא מעצים את התנאים להיווצרותה, בשל מאפייני ההאצה, הריבוי והמורכבות של העידן. יכולת עשויה להיבנות במהירות מחיבור של רכיבים גלויים וזמינים, להשתנות באמצעות תוכנה וקישוריות ולהתפשט בין זירות עוד לפני שהמודיעין הכיר בה כמערכת. בסביבה כזו אי אפשר לצפות מהמודיעין לאתר או לחזות במדויק כל יכולת וכל שימוש עתידי בה. אך עליו לזהות מערכות מתהוות, להעריך את קצב הבשלתן ולבחון כיצד הן משנות את תפיסת הלחימה של היריב, וכיצד הן שוחקות יתרון איכותי או יוצרות ומנצלות נקודות תורפה בצד שלנו.

האתגר הגובר מחייב להרחיב את מסגרת העשייה המודיעינית: להסתכל מעבר לצבאות ולתעשיות ביטחוניות, אל האקוסיסטם המדעי־טכנולוגי בסביבה האזרחית בצד השני; לבנות מודלים לאיתור הבשלה של טכנולוגיות לכדי מערכות מבצעיות המורכבות מממדים פיזיים־קינטיים ודיגיטליים כאחד; ולהקים קהילות ידע ורשתות של למידה המשלבות את המודיעין עם בוני הכוח ומפעיליו ועם גורמי מדע ותעשייה במגזר האקדמי ובמגזר הפרטי, כדי לאפשר למידה עמוקה ורוחבית הן של האיום והן של יכולת המענה לו.

המסגרת המוצעת אינה ממצה את מקורות ההפתעה הטכנולוגית, שחלקם קשורים בכשלים אוניברסליים של המודיעין שאינם נדונים במאמר. גם יישום מוצלח של העקרונות שהוצגו אינו מבטיח הצלחה: ההתרעה המודיעינית כרוכה מטבעה באי ודאות, והעידן הדיגיטלי מעצים אותה. משום כך, המענה הכולל אינו יכול להישען על התרעה בלבד. לצד שיפור היכולת לזהות מערכות מתהוות, על המערכת הביטחונית לעסוק גם בשלילת יכולותיו המתפתחות של היריב ולפתח גמישות וחוסן שיאפשרו לה לספוג

---

38 מיכאל, ק', סימן־טוב, ד' וויואלי, א' (2016). התפתחות תפיסת השילוביות בארגוני מודיעין. מודיעין הלכה ומעשה, 1, 6–24

39 ארנון, י' (2017). בניין הכוח בקהילת המודיעין במציאות משתנה. מודיעין הלכה ומעשה, 2, 27–35; קינן, א' (2021). בניין כוח משותף בקהילת המודיעין. מודיעין הלכה ומעשה, 7, 46–48; אל"ם י' (2021). ההשתנות הדיגיטלית במודיעין: פוטנציאל חדש למרחבי שילוביות. מודיעין הלכה ומעשה, 7, 49–59
Bowers, I., & Hiim, H. S. (2026). Measuring military competition in the 21st century: Toward a better understanding of how militaries are preparing for war. Comparative Strategy, 45(4), 573–592. https://doi.org/10.1080/01495933.2025.2611303; Bracken, P. (2006). Net assessment: A practical guide. Parameters, 36(1), 90–100; Krepinevich, A. F., & Watts, B. D. (2015). The last warrior: Andrew Marshall and the shaping of modern American defense strategy. Basic Books

40 אל"ם י' (2021); א' (2021). שותפות אסטרטגית: מכפיל כוח להתמודדות עם האיום המתגבר בממד הסייבר. מודיעין הלכה ומעשה, 7, 86–93; רס"ן י' (2021). "בשבל הכובבים מסתדרים": סיפורה של קהילה טכנולוגית רב־ארגונית משולבת תעשייה בתחום הראייה הממוחשבת. מודיעין הלכה ומעשה, 7, 94–102

הפתעה, להסתגל אליה ולהתאושש ממנה. אך אי היכולת למנוע כל הפתעה אינה הופכת את המאמץ לחסר תוחלת: איכות המעקב המודיעיני, מהירות הלמידה המשותפת והגמישות המבצעית עשויות לקבוע אם ההפתעה תהיה מוגבלת וברת הכלה או תהפוך לעמוקה ומשתקת.

רשימת מקורות

א' (2021). שותפות אסטרטגית: מכפיל כוח להתמודדות עם האיום המתגבר בממד הסייבר. מודיעין הלכה ומעשה, 7, 86–93

אדמסקי, ד' (2015). אומנות אופרטיבית קיברנטית: מבט מזווית לימודי האסטרטגיה ומפרספקטיבה השוואתית (עשתונות, גיליון 11). מרכז המחקר של המכללה לביטחון לאומי

אלון, נ' (2018). סריקת האופק (Horizon scanning): תהליך מסייע בתהליכי קבלת החלטות ברמה הלאומית (מחקר עומק מס' 4). המכון לחקר המתודולוגיה של המודיעין, המרכז למורשת המודיעין

אל"ם י' (2021). ההשתנות הדיגיטלית במודיעין: פוטנציאל חדש למרחבי שילוביות. מודיעין הלכה ומעשה, 7, 49–59

ארנון, י' (2017). בניין הכוח בקהילת המודיעין במציאות משתנה. מודיעין הלכה ומעשה, 2, 27–35

בנג'ו, י' (21 במאי 2025). מהפכת רחפני FPV ומשמעויותיה בלוחמת היבשה ובממדים נוספים. המכון למחקרי ביטחון לאומי

גוטרמן, ע' (16 בינואר 2023). מודיעין פתוח: מסגרת חדשה ליחסים בין ארגוני המודיעין לסביבה האזרחית. המכון לחקר המתודולוגיה של המודיעין

מיכאל, ק', סימן־טוב, ד' ויואלי, א' (2016). התפתחות תפיסת השילוביות בארגוני מודיעין. מודיעין הלכה ומעשה, 1, 6–24

נווה, ש' (2001). אמנות המערכה: התהוותה של מצוינות צבאית. מערכות

ענתבי, ל' ואדר, א' (5 בפברואר 2024). רחפני FPV: משדה הקרב באוקראינה למזרח התיכון? מבט על, גיליון 1825. המכון למחקרי ביטחון לאומי

פינקל, מ' (2007). על הגמישות: הגמישות כמפתח להתמודדות עם הפתעה טכנולוגית ותורתית בשדה הקרב. מערכות

פלקוב, י' (2024). "לפרמט" את האויב והעולם לטובתנו: לוחמת התודעה הרוסית מהלכה למעשה. בתוך י' קופרוסר וד' סימן טוב (עורכים), השפעה והתערבות זרה כאתגר אסטרטגי ומודיעיני (עמ' 19–32). המכון לחקר המתודולוגיה של המודיעין; המכון למחקרי ביטחון לאומי

קינן, א' (2021). בניין כוח משותף בקהילת המודיעין. מודיעין הלכה ומעשה, 7, 46–48

רס"ן י' (2021). "כשכל הכוכבים מסתדרים": סיפורה של קהילה טכנולוגית רב־ארגונית משולבת תעשייה בתחום הראייה הממוחשבת. מודיעין הלכה ומעשה, 7, 94–102

Acton ,J .M .(2018) .Escalation through entanglement :How the vulnerability of command-and-control systems raises the risks of inadvertent nuclear war .International Security .99–56 ,(1)43 ,https//:doi.org/10.1162/isec_a00320_

Adamsky ,D .(2010) .The culture of military innovation :The impact of cultural factors on the revolution in military affairs in Russia ,the US ,and Israel .Stanford University Press

Andreika ,V ,2025) .September–October .(Russia's changes in the conduct of war based on lessons from Ukraine :Adapting technology ,force structures ,and the defense industry .Military Review

Balmforth ,T & ,.Hunder ,M ,2025) .June .(1 To attack Russian air bases ,Ukrainian spies hid drones in wooden sheds .Reuters

Bondar ,K ,2024) .November .(19 Why Ukraine is establishing unmanned forces across its defense sector and what the United States can learn from it .Center for Strategic and International Studies

Bondar ,K .(2025) .How Ukraine rebuilt its military acquisition system around commercial technology. Center for Strategic and International Studies

Bowers ,I & ,.Hiim ,H .S .(2026) .Measuring military competition in the21 st century :Toward a better understanding of how militaries are preparing for war .Comparative Strategy .592–573 ,(4)45 ,https//:doi.org10.1080/01495933.2025.2611303/

Bracken ,P .(2006) .Net assessment :A practical guide .Parameters100–90 ,(1)36 ,

Buchanan ,B & ,.Cunningham ,F .S .(2023) .Preparing the cyber battlefield :Assessing a novel escalation risk in a Sino-American crisis .In R .Chesney ,J .Shires & ,M .Smeets) Eds ,(.Cyberspace and instability) pp .(98–60 .Edinburgh University Press
Builder ,C .H .(1989) .The masks of war :American military styles in strategy and analysis .Johns Hopkins University Press
Cuhls ,K .E .(2020) .Horizon scanning in foresight :Why horizon scanning is only a part of the game. Futures & Foresight Science ,(1)2 ,Article e23 .https//:doi.org/10.1002/ffo2.23
Defense Science Board .(2010) .Report of the Defense Science Board 2008 summer study on capability surprise :Volume II ,supporting papers .Office of the Under Secretary of Defense for Acquisition, Technology ,and Logistics
Gebeily ,M ,.Lubell ,M & ,.Cartier ,C ,2026) .May .(12 Evolving drone war in southern Lebanon clouds Iran peace prospects .Reuters
Habegger ,B .(2009) .Horizon scanning in government :Concept ,country experiences ,and models for Switzerland .Center for Security Studies ,ETH Zurich
Handel ,M .I .(1987) .Technological surprise in war .Intelligence and National Security.53–1 ,(1)2 , https//:doi.org10.1080/02684528708431875/
Horowitz ,M .C .(2010) .The diffusion of military power :Causes and consequences for international politics .Princeton University Press
Insinna ,V ,2022) .April .(20 SpaceX beating Russian jamming attack was" eyewatering :"DoD official. Breaking Defense
Jervis ,R .(1976) .Perception and misperception in international politics .Princeton University Press
Kaba ,L .(1981) .Archers ,musketeers ,and mosquitoes :The Moroccan invasion of the Sudan and the Songhay resistance .(1612–1591) The Journal of African History .475–457 ,(4)22 ,https//:doi.org/10.1017/S0021853700019861
Kallenborn ,Z ,2022) .May .(12 Seven) initial (drone warfare lessons from Ukraine .Modern War Institute
Kania ,E .B .(2021) .Artificial intelligence in China's revolution in military affairs .Journal of Strategic Studies .542–515 ,(4)44 ,https//:doi.org10.1080/01402390.2021.1894136/
Krepinevich ,A .F & ,.Watts ,B .D .(2015) .The last warrior :Andrew Marshall and the shaping of modern American defense strategy .Basic Books
Libicki ,M .C ,.Gompert ,D .C ,.Frelinger ,D .R & ,.Smith ,R .E .(2007) .Byting back :Regaining information superiority against21 st-century insurgents :RAND Counterinsurgency Study—Volume1)MG-595/1-OSD .(RAND Corporation
Losey ,S ,2022) .April .(20 SpaceX shut down a Russian electromagnetic warfare attack in Ukraine last month ,and the Pentagon is taking notes .Defense News
Mahnken ,T .G .(2002) .Uncovering ways of war :U.S .intelligence and foreign military innovation, .1941–1918Cornell University Press
McKenzie ,K .F ,.Jr ,.Spleeters ,D & ,.Lincy ,V ,2023) .April .(24 Iran's military drone program :Security implications and policy responses .The Washington Institute for Near East Policy
Ministry of Defence of Ukraine ,2025) .January .(27 Kateryna Chernohorenko :The Mission Control module is now accessible to all DELTA users
Molloy ,O ,2026) .March .(11 Drone warfare in Ukraine :From myths to operational reality ,Part.1 Australian Army Research Centre

Murray ,W & ,.Millett ,A .R) .Eds .(1996) .(.Military innovation in the interwar period .Cambridge University Press
NATO Allied Command Transformation ,2024) .July .(12 Battlefield innovation :Ukraine's DELTA system paves the way for Allied interoperability at CWIX24
Page ,J .M .(2025) .Drones and the Hamas-led attack of 7 October :2023 Innovation and implications. Perspectives on Terrorism33–1 ,(1)19 ,
Parshall ,J & ,.Wenger ,J .M ,2011) .December .(Pearl Harbor's overlooked answer .Naval History(6)25 ,
Pettyjohn ,S ,2024) .February .(8 Evolution not revolution :Drone warfare in Russia's 2022 invasion of Ukraine .Center for a New American Security
Polybius .(1922) .The histories) W .R .Paton ,Trans ;.Vol ,1 .Books .(2–1 Harvard University Press.)Original work published ca .second century BCE(
Rosen ,S .P .(1991) .Winning the next war :Innovation and the modern military .Cornell University Press
Singer ,P .W & ,.Brooking ,E .T .(2018) .LikeWar :The weaponization of social media .Houghton Mifflin Harcourt
Smith ,G ,.Hage ,G ,.Heitzenrater ,C ,.Chessen ,M & ,.Girven ,R .S .(2026) .Infinite potential :Insights from the cyber surprise scenario :Post-series scenario report from a sequence of Day After artificial general intelligence exercises) RR-A4626-1 .(RAND Corporation .https//:doi.org/10.7249/RRA4626-1
Soare ,S .R ,.Singh ,P & ,.Nouwens ,M ,2023) .February .(17 Software-defined defence :Algorithms at war .International Institute for Strategic Studies
Stenslie ,S ,.Haugom ,L & ,.Vaage ,B .H) .Eds .(2021) .(.Intelligence analysis in the digital age. Routledge .https//:doi.org10.4324/9781003168157/
Stracquadanio ,A ,2026) .June .(23 Frustrating Israel ,fiber-optic killer drone technology has arrived in southern Lebanon .Defense News
Sutea ,V ,2026) .February .(24 Fiber-optic drones have emerged as critical kit for both Russia and Ukraine .Atlantic Council
Till ,G .(1996) .Adopting the aircraft carrier :The British ,American ,and Japanese case studies .In W .Murray & A .R .Millett) Eds ,(.Military innovation in the interwar period) pp .(226–191 .Cambridge University Press .https//:doi.org/10.1017/CBO9780511601019.006
U.S .Department of Defense .(2023) .Military and security developments involving the People's Republic of China :2023 Annual report to Congress .Office of the Secretary of Defense
Venable ,D .(2026) .Synthetic asymmetry :Intelligence advantage and strategic imbalance in the age of technological convergence] Preprint .[SSRN
Vergun ,D ,2025) .July .(16 Pentagon to increase low-cost drone production in U.S .U.S .Department of Defense
Westermann ,E .B .(2001) .Flak :German anti-aircraft defenses .1945–1914 ,University Press of Kansas