

# פגיעות טכנו-דיגיטלית וכישלונות מודיעיניים

ד"ר אהוד ערן<sup>1</sup>

ההבטחה הגלומה בעוצמה דיגיטלית היא שיותר נתונים יביאו לראייה טובה יותר של המציאות ויאפשרו תגובה מהירה יותר. אולם עליונות דיגיטלית נושאת עימה גם פגיעויות עמוקות. ככל שמדינות ממשיכות להשקיע בארכיטקטורות דיגיטליות, לשלב בינה מלאכותית בתהליכי עבודה מודיעיניים ולהרחיב יכולות סייבר, הן ייתקלו לא רק בהזדמנויות חדשות אלא גם בסכנות חדשות. המשימה המרכזית עבור חוקרים ואנשי מקצוע היא להבין ולמתן את הפגיעויות הנובעות לא מנחיתות טכנולוגית, אלא מעליונות דיגיטלית עצמה

## מבוא

הדיגיטציה המואצת של תשתיות מדינתיות ושל ארגונים צבאיים נתפסת כמרכיב חשוב בעוצמה לאומית. מדינות מסתמכות יותר ויותר על רשתות תקשורת, חיילים, פלטפורמות, מערכות בינה מלאכותית ונתוני עתק לצורך הגנה על גבולות, זיהוי איומים והפעלת עוצמה צבאית. נשיא רוסיה ולדימיר פוטין ניסח תפיסה זו באופן חד כאשר אמר ב-2017 כי "מי שיהפוך למוביל בתחום הבינה המלאכותית יהפוך לשליט העולם".<sup>2</sup> טענת היסוד שעליה מבוססים המאמצים הלאומיים הללו היא כי ככל שיש יותר מידע, יכולות ניטור, ניתוח והפצה מהירות ומקיפות יותר, כך אפשר להשיג התרעה מוקדמת יותר, הרתעה יעילה יותר וקטלניות גבוהה יותר.

התאוריה הריאליסטית ביחסים הבין לאומיים סבורה מזה עשורים רבים כי יתרון טכנולוגי הוא מכפיל כוח של עוצמה מדינתית.<sup>3</sup> קונקרטי, בתחום חקר המודיעין מקובלת ההנחה כי הטכנולוגיה הדיגיטלית משפרת במידה ניכרת את יכולות האיסוף והניתוח.<sup>4</sup> אולם שני העשורים האחרונים מלמדים כי עליונות דיגיטלית אינה מאיינת את האפשרות של הפתעה אסטרטגית. כך, ארצות הברית לא הצליחה לצפות את קריסתה המהירה של ממשלת אפגניסטן ב-2021, אף שהחזיקה ביכולות מודיעין, מעקב וסיור חזקות. רוסיה שגתה בהערכת עמידותה של אוקראינה ובנחישותן של מדינות המערב ב-2022, חרף מערכי ניטור דיגיטליים נרחבים. מגפת הקורונה הפתיעה גם מדינות מתקדמות טכנולוגית, אשר הפעילו מערכות גלובליות מתוחכמות לניטור בריאותי. וישראל, "אומת הסטארט-אפ", בעלת יחידות סייבר מהמובילות בעולם ומערכת ביטחון המשולבת עמוקות בבינה מלאכותית, ספגה כישלון מודיעיני חריף ב-7 באוקטובר 2023.

מקרים אלה מערערים על ההנחה שלפיה יכולת דיגיטלית מתורגמת באופן אוטומטי לביטחון רב יותר. הם מחייבים בחינה מחודשת של הקשר שבין התקדמות טכנולוגית ובין פגיעות אסטרטגית. המאמר טוען כי התפיסה הרווחת בקרב חוקרי ביטחון ואנשי מקצוע, ובמיוחד הציפייה הבלתי ביקורתית שלפיה חדשנות דיגיטלית מעצימה באופן טבעי את עוצמת המדינה, מסתירה מציאות מורכבת יותר. תשתיות דיגיטליות אינן רק מקור ליתרון; הן יוצרות גם צורות חדשות של עיוורון, תלות, נוקשות וחשיפה אסטרטגית.

הטענה המרכזית של המאמר היא שככל שמדינה משלבת באופן עמוק יותר טכנולוגיות דיגיטליות במערכי המודיעין, הממשל והביטחון שלה, כך היא נעשית פגיעה יותר לצורות מסוימות של הפתעה אסטרטגית הנובעות מאותן טכנולוגיות עצמן. רעיון זה מגולם במושג פגיעות טכנו-דיגיטלית (Techno-Digital Vulnerability). זוהי מסגרת מושגית המבהירה כיצד מערכות דיגיטליות מעצבות מחדש את היסודות הקוגניטיביים, הארגוניים והמבניים של ההערכה האסטרטגית.

בחמשת חלקי המאמר אני מקדם את הטעון באופן הבא: תחילה, המאמר סוקר את ספרות היחסים הבין לאומיים העוסקת

1 ראש המחלקה ליחסים בין לאומיים באוניברסיטת חיפה וחוקר בכיר במכון הרבני לחקר המודיעין

2 ALLEN, G. C. (2017). PUTIN AND MUSK ARE RIGHT: WHOEVER MASTERS AI WILL RUN THE WORLD. CENTER FOR A NEW AMERICAN SECURITY

3 KEOHANE, R., & NYE, J. (2012). POWER AND INTERDEPENDENCE (4TH ED.). LONGMAN; FARRELL, H., & NEWMAN, A. (2019). WEAPONIZED INTERDEPENDENCE: HOW GLOBAL ECONOMIC NETWORKS SHAPE STATE COERCION. INTERNATIONAL SECURITY, 44, 42–79

4 BETTS, R. K. (1978). ANALYSIS, WAR, AND DECISION: WHY INTELLIGENCE FAILURES ARE INEVITABLE. WORLD POLITICS, 31, 61–89; ZEGART, A. (2022). SPIES, LIES, AND ALGORITHMS: THE HISTORY AND FUTURE OF AMERICAN INTELLIGENCE. PRINCETON UNIVERSITY PRESS

בטכנולוגיה ובעוצמה. הוא מראה כי המסורות התאורטיות המרכזיות מתייחסות להתקדמות טכנולוגית כאל גורם מייצב ומעצים יכולות. בחלק השני של המאמר מוצגת המסגרת המושגית של פגיעות טכנו-דיגיטלית, ובה ארבעת המנגנונים שבאמצעותם עליונות דיגיטלית עשויה דווקא להגביר את הסיכון להפתעה. בחלק השלישי המאמר מדגים את המסגרת באמצעות הדוגמה של כישלון ישראל לחזות את אירועי 7 באוקטובר 2023. בחלק הרביעי נדונות משמעויות הממצאים עבור תאוריות של יחסים בין לאומיים ותאוריות של הפתעה אסטרטגית. לבסוף, המאמר מציע סדר יום מחקרי חדש, הקורא לשלב את חקר המערכות הדיגיטליות כחלק בלתי נפרד מן המחקר על הפתעה אסטרטגית וביטחון בין לאומי.

## טכנולוגיה, עוצמה ותפיסה ביחסים בין לאומיים

הפרדיגמות המרכזיות של היחסים הבין לאומיים מתייחסות בדרך כלל להתקדמות טכנולוגית כמקור להעצמת יכולותיה של המדינה, או כמאפיין מבני של תלות הדדית בין מדינות. חלק זה בוחן כיצד התאוריות המרכזיות בחקר היחסים הבין לאומיים ממשיגות את הקשר שבין טכנולוגיה לביטחון, ומדוע הן נוטות להתעלם מן הפגיעויות שהמערכות הדיגיטליות עצמן מייצרות.

### ריאליזם ועוצמה

הספרות הריאליסטית ראתה מאז ומתמיד ביכולות תעשייתיות, שבמרכזן הטכנולוגיה, מרכיב יסודי של העוצמה החומרית. עם השתנות הטכנולוגיה לאורך השנים, השתנה גם סוג הטכנולוגיה שעמד במוקד הדיון. בתחילה התמקדו החוקרים במדע ובטכנולוגיה כמנועי התעשייה הכבדה. כך, בספרו הקלאסי פוליטיקה בין האומות כתב החוקר הנס מורגנטאו כי "טכנולוגיית הלחימה והתקשורת המודרנית הפכה את הפיתוח הכולל של התעשיות הכבדות לרכיב חיוני בעוצמתה של מדינה".<sup>5</sup>

לטענתו, התעשייה יוצרת את הבסיס הכלכלי הדרוש למדינה כדי לנהל מלחמה כוללת: החל מכבישים, מסילות רכבת, משאיות, אוניות ומטוסים, וכלה באמצעי לחימה מכל הסוגים. כאשר מרכז הכובד של הכלכלה העולמית עבר מן התעשייה הכבדה לטכנולוגיות מידע, במה שכונה לימים "המהפכה התעשייתית השלישית", גם התחרות בין מדינות עברה אל תחום זה. כך, משנות התשעים ואילך עברה תשומת הלב ליכולות הנובעות מטכנולוגיות מידע. בהמשך, עם כניסתה של הכלכלה למהפכה התעשייתית הרביעית, המאופיינת במיזוג שבין מערכות פיזיות, דיגיטליות וביולוגיות,<sup>6</sup> התחרות הגלובלית עברה למישור טכנולוגי זה. כך, מתארים רבים את התחרות האמריקנית-סינית כ"מלחמת טכנולוגיה", שבמסגרתה וושינגטון מבקשת לשמר את עליונותה הטכנולוגית ולמנוע מסין גישה לטכנולוגיות קריטיות.<sup>7</sup>

מנקודת מבט ריאליסטית, טכנולוגיה מתקדמת מייצרת יכולת כפייה עדיפה: צבאות יעילים יותר, נשק מדויק יותר ומודיעין איכותי יותר. החוקר ג'ון מירשהיימר סבר כי הטכנולוגיה משפיעה על יחסי הכוחות, משנה את מאזן העוצמה ומעצבת את תוצאות ההרתעה.<sup>8</sup> באופן דומה הדגיש החוקר בארי פוזן כי שליטה בטכנולוגיות של מעקב, ניווט ותקשורת מאפשרת למעצמות לשלוט במרחבים הגלובליים באמצעות שילוב של מערכות סיור עולמיות ויכולות תקיפה מדויקות. פוזן הזכיר כי המהפכה בעניינים צבאיים (RMA) של ארצות הברית נשענה בראש ובראשונה על יישום הישגי המדע וההנדסה, ובייחוד בתחומי הפיזיקה, הכימיה וטכנולוגיות המידע, בפיתוח ובהפעלת מערכות נשק. עליונותה המדעית והטכנולוגית של ארצות הברית היא שאפשרה את עליונותה הצבאית בשדה הקרב הקונבנציונלי.<sup>9</sup> במסורת זו נתפסת הטכנולוגיה כמעט תמיד כמקור להעצמת יכולתה של המדינה. על פי ראייה זו, כאשר מתרחשים כישלונות מודיעיניים, הם מוסברים בדרך כלל באמצעות פרשנות שגויה של מידע, הקצאת משאבים לקויה או פיגור טכנולוגי ביחס ליריב. לעומת זאת, האפשרות שעצם התחכום הטכנולוגי יוצר פגיעויות חדשות כמעט שאינה נבחנת.

### ליברליזם, ניאו-ליברליזם ותלות הדדית דיגיטלית

המסורות הליברליות והניאו-ליברליות מעניקות מקום מרכזי הרבה יותר למידע ולתלות הדדית בהשוואה לריאליסטים. קוהיין

MORGENTHAU, H. (1967). POLITICS AMONG NATIONS: THE STRUGGLE FOR POWER AND PEACE (4TH ED.). ALFRED A. KNOPF, P. 113 5

SCHWAB, K. (2016). THE FOURTH INDUSTRIAL REVOLUTION. CROWN BUSINESS 6

WINKLER, S. C. (2025). NEW AND OLD COLD WARS: THE TECH WAR AND THE ROLE OF TECHNOLOGY IN GREAT POWER POLITICS. GLOBAL STUDIES QUARTERLY, 5, KSAF038 7

MEARSHEIMER, J. (2001). THE TRAGEDY OF GREAT POWER POLITICS. NORTON 8

POSEN, B. (2003). COMMAND OF THE COMMONS. INTERNATIONAL SECURITY, 28, 5-46 9

ונוי<sup>10</sup> מדגישים כיצד זרימת מידע מעצבת את התלות ההדדית המורכבת ואת חלוקת "העוצמה הרכה" ו"עוצמת הרשת". מחקרים מאוחרים יותר, ובראשם מאמרם של החוקרים הנרי פארל ואברהם ניומן על "תלות הדדית מחומשת" (Weaponized Interdependence)<sup>11</sup>, מספקים תובנות חשובות בנוגע לאופן שבו מדינות המשולבות ברשתות דיגיטליות עולמיות מסוגלות לנצל את הקישוריות לצורכי מעקב, כפייה או שיבוש של מדינות אחרות.

## עוצמה קיברנטית, עמימות ושבריריות

חקר הסייבר התקדם רבות בהבנת האופן שבו מערכות דיגיטליות יוצרות זירות חדשות של עימות ושיבוש. חוקרים מציינים כי תשתיות דיגיטליות הן מטבען שבריריות,<sup>12</sup> אך גם מזהירים כי יכולות קיברנטיות מייצרות לעיתים קרובות השפעות עמומות וקשות לזיהוי,<sup>13</sup> וכי הטענה כי במרחב הסייבר יש יתרון להתקפה מוגזם לעיתים.<sup>14</sup> אולם, מחקר הסייבר מתמקד בעיקר בהגנה ובהתקפה במרחב הקיברנטי עצמו. הוא מסביר כיצד האקרים חודרים למערכות, אך אינו בוחן באופן שיטתי כיצד ההסתמכות על מערכות אלה מעצבת תפיסה, קבלת החלטות ויכולת התרעה מחוץ למרחב הסייבר.

## חקר המודיעין: הכרה במגבלות הקוגניטיביות

חוקרים כדוגמת בטס, היואר, ג'רוויס ובר-יוסף ומקדרמוט<sup>15</sup> טוענים שכשלי מודיעין אינם נובעים בהכרח ממחסור במידע, אלא מסגירות קוגניטיביות, מהטיית אישוש, מכשלים ארגוניים ומפוליטיזציה של תהליך ההערכה. תובנות אלה נוגעות גם לעידן הדיגיטלי, שהרי הטכנולוגיה אינה מבטלת הטיות קוגניטיביות. עם זאת, גם ספרות זו מתייחסת בדרך כלל לטכנולוגיה ככלי המשפר את האיסוף, את הפצת המידע ולעיתים גם את הניתוח. רוב המחקרים אינם רואים בטכנולוגיית המידע מקור לעיוות מושגי בפני עצמו. חוקרים אלה מכירים בכך שכמות גדולה יותר של מידע אינה מבטיחה פרשנות טובה יותר, אך אינם ממשיגים במלואן את ההשלכות המבניות והתרבותיות של שילוב עמוק של מערכות דיגיטליות בארגוני מודיעין.

## עליונות טכנולוגית והפרדוקס של העוצמה הצבאית המודרנית

בספרות הצבאית, הארגונית והמדינית מתגבשת בשנים האחרונות טענה משותפת שלפיה עליונות טכנולוגית היא חרב פיפיות אסטרטגית, ולא מקור ליניארי ליתרון. טכנולוגיות מתקדמות משנות את אופן החשיבה ואת ההתנהגות הארגונית באמצעות יצירת אשליות של שליטה, סגירות אפיסטמית וביטחון עצמי מופרז. מקבלי החלטות נוטים לזהות שפע של נתונים עם הבנה מלאה של המציאות, ובו בזמן להמעיט בחשיבותם של אי-ודאות, הסתגלות היריב ואינדיקציות שאינן דיגיטליות.<sup>16</sup> כתוצאה מכך נוצר פרדוקס: ההשקעות שנועדו להגביר דיוק, מהירות ועליונות מייצרות במקביל מערכות המחוברות זו לזו באופן הדוק, ולכן גם שברירות יותר, קשות יותר לבקרה ורגישות יותר לקריסות מערכתיות, במיוחד בסביבות של לוחמת סייבר ומידע.<sup>17</sup> יתר על כן, ההסתמכות על אופטימיזציה טכנולוגית שוחקת בהדרגה מנגנוני יתירות (redundancy) ואת המומחיות האנושית, ובכך מצמצמת את יכולתם של ארגונים להפגין גמישות ועמידות כאשר מערכות נפגעות או כאשר מתרחשת הפתעה אסטרטגית.

## לקראת מסגרת מושגית: פגיעות טכנו-דיגיטלית

חלק זה מפתח מסגרת מושגית, שנועדה להסביר מדוע גם מדינות מתקדמות מבחינה טכנולוגית נותרות פגיעות להפתעה אסטרטגית. המסגרת המוצעת, פגיעות טכנו-דיגיטלית, מבוססת על הטענה שמערכות דיגיטליות אינן רק משפרות את יכולותיהן של מדינות, אלא גם מעצבות מחדש את הסביבה הפוליטית והארגונית. דינמיקות אלה אינן תופעות לוואי שוליות של השימוש

KEOHANE AND NYE (2012) 10

FARRELL AND NEWMAN (2019) 11

SLAYTON, R. (2017). ARGUMENTS THAT COUNT: PHYSICS, COMPUTING, AND MISSILE DEFENSE, 1949–2012. MIT PRESS 12

LINDSAY, J. (2013). STUXNET AND THE LIMITS OF CYBER WARFARE. SECURITY STUDIES, 22, 365–404 13

GARTZKE, E. (2013). THE MYTH OF CYBERWAR. INTERNATIONAL SECURITY, 38, 41–73 14

HEUER, R. J. (1999). PSYCHOLOGY OF INTELLIGENCE ANALYSIS. CIA PRESS; HEUER, R. J., & PHERSON, R. H. (2015). STRUCTURED ANALYTIC TECHNIQUES FOR INTELLIGENCE ANALYSIS (2ND ED.). CQ PRESS; BAR-JOSEPH, U., & MCDERMOTT, R. (2017). INTELLIGENCE SUCCESS AND FAILURE: THE HUMAN FACTOR. OXFORD UNIVERSITY PRESS; JERVIS, R. (2010). WHY INTELLIGENCE FAILS: LESSONS FROM THE IRANIAN REVOLUTION AND THE IRAQ WAR. CORNELL UNIVERSITY PRESS 15

BRYANT, S. L. (2011). THE DANGERS OF AN OVER-RELIANCE ON TECHNOLOGY [MASTER'S THESIS]. JOINT FORCES STAFF COLLEGE; PEÑA, C. (2024, DECEMBER 5). IT'S EASY TO GET LOST: THE TEMPTATION OF OVERRELIANCE ON TECHNOLOGY. WARROOM 16

U.S. Government Accountability Office. (2018). DOD just beginning to grapple with scale of vulnerabilities. GAO; Serena, C. C., & Clarke, C. P. (2019). America's national defense strategy and the paradox of technology. RAND Corporation Commentary 17

בטכנולוגיה, אלא מאפיינים אינהרנטיים של האופן שבו מערכות דיגיטליות פועלות בתוך ארגונים בירוקרטיים.

## מערכות דיגיטליות כמייצרות אשליה

מערכות מודיעין דיגיטליות יוצרות באופן שגרתי אשליה קוגניטיבית וארגונית של שלמות אפיסטמית, תחושה שלפיה קיים ידע מלא ורציף על המציאות. ריבוי החיישנים, מאגרי הנתונים העצומים, האלגוריתמים לסינון מידע ומערכות הזיהוי האוטומטי של דפוסים יוצרים רושם של מודעות מצב מלאה בזמן אמת. נדמה כי שדה הקרב, ואף המרחב המדיני שבו מתקבלות ההחלטות, הפכו לשקופים לחלוטין. זוהי גרסה ייחודית לעולם הביטחון של מה שמכונה בספרות הטיית האוטומציה (automation bias). הטיה זו היא הנטייה השיטתית להסתמך יתר על המידה על תוצריה של מערכת אוטומטית, תוך הפחתת החיפוש העצמאי אחר מידע והפחתת הנכונות לאמת את ממצאיה, במיוחד כאשר המערכת נתפסת כסמכותית או כאשר קיימים עומס עבודה ולחץ זמן.<sup>18</sup> הטיית האוטומציה עשויה להתבטא בשני סוגי טעויות:

- טעויות פעולה (commission errors): קבלת המלצות שגויות של המערכת גם כאשר קיימות ראיות סותרות.
- טעויות הימנעות (omission errors): הימנעות מפעולה משום שהמערכת לא התריעה על בעיה. במקרים אלה נוצרת ההנחה שאם אין התרעה הרי שאין איום.

במקום לבחון באופן ביקורתי את המידע, מקבלי ההחלטות משתמשים בפלט של המערכת כתחליף לחשיבה עצמאית ולחיפוש פעיל אחר מידע. השפעה זו בולטת במיוחד בארגוני ביטחון הנשענים בעיקר על מודיעין אותות (SIGINT), מערכי חישה מתקדמים ופלטפורמות מודיעין, תצפית וסיור (ISR) הפועלות ברציפות. אולם מקור הפגיעות איננו טכני בלבד. זהו בראש ובראשונה כשל אפיסטמי וארגוני. מערכות דיגיטליות מטפחות אשליה של ידיעה מוחלטת. הן יוצרות תחושת סגירות כוזבת, מצמצמות את טווח הפרשנויות האפשריות, מדרות דרכי חשיבה חלופיות ומחזקות הערכות איום המבוססות על הטיית אישור. קציני מודיעין פועלים ממילא תחת עומס מידע כבד.<sup>19</sup> במצבים כאלה גוברת הנטייה להשתמש בקיצורי דרך קוגניטיביים ולהסתמך על הטכנולוגיה, שכן, כפי שצינו אפלטון ומנגיס,<sup>20</sup> עומס מידע פוגע בשיקול הדעת ומגביר את ההסתמכות על היוריסטיקות, במיוחד תחת לחץ זמן.

אחת ההשפעות החזקות ביותר של מערכות דיגיטליות על אנשי מודיעין היא המחשבה כי ביכולתן לצמצם את אי-הודאות. צילומי לוויין ברזולוציה גבוהה, פלטפורמות מעקב רציפות, חיישנים אוטומטיים וכלי בינה מלאכותית יוצרים רושם שלפיו העמימות כמעט נעלמה. מנהיגים ואנשי מודיעין המורגלים במערכות כאלה עלולים לפתח מצב שאפשר לכנותו רוויה אפיסטמית (epistemic saturation): תחושה עזה שהמידע הזמין אינו רק רב, אלא גם שלם. בסביבה כזו נדמה שהלא-נודע הצטמצם לשוליים. זו לא רק הטיה פסיכולוגית, אלא תכונה מתהווה של האופן שבו מערכות דיגיטליות משתלבות בשגרת עבודת המודיעין. הממשקים הדיגיטליים מציגים מידע רב באופן נקי, מסודר ובכמות רבה, בעוד מרווחי הטעות מוסתרים מאחורי שכבות של חישוב אלגוריתמי. עצם נפח הנתונים יוצר תחושה של כיסוי מלא. למערכות הדיגיטליות יש אפוא גם אפקט נסתר: הן מציגות את עצמן כמקיפות ושלמות, גם כאשר אינן כאלה.

התרעה אסטרטגית מבוססת לעיתים קרובות על פרשנות של אינדיקציות עמומות. אולם, מערכות דיגיטליות נוטות להציג מידע כעובדות אמינות שנאספו באמצעות חיישנים, ולא כשברים של מציאות אסטרטגית הנצפית באופן חלקי בלבד. החוקרים מפנימים את ההנחה שאם איום אכן מתפתח, הוא יופיע בנתונים. כאשר הנתונים שותקים, הם מסיקים שהמצב האסטרטגי יציב, גם כאשר היריב מסתיר במכוון את פעילותו באמצעות הימנעות מחתימות אלקטרוניות. תהליך זה יוצר את מה שהחוקר רוברט ג'רוויס כינה בהקשר אחר "סגירות קוגניטיבית מוקדמת".<sup>21</sup> המערכות הדיגיטליות מעודדות סיום מוקדם של תהליך הפרשנות באמצעות יצירת אשליה של שלמות. ברגע שארגון מודיעין מאמין שחיישניו מסוגלים לזהות כל פעולה מהותית, תרחישים חלופיים (במיוחד כאלה המבוססים על הונאה, על התנהגות אנלוגית או על שיטות פעולה פשוטות) נראים בלתי סבירים ואף בלתי הגיוניים. התוצאה היא

PARASURAMAN, R., & MANZEY, D. M. (2010). COMPLACENCY AND BIAS IN HUMAN USE OF AUTOMATION: AN ATTENTIONAL INTEGRATION. HUMAN FACTORS: THE JOURNAL OF THE HUMAN FACTORS AND ERGONOMICS SOCIETY, 52, 381-410

HEUER AND PHERSON (2015) 19

EPPLER, M. J., & MENGIS, J. (2004). THE CONCEPT OF INFORMATION OVERLOAD: A REVIEW OF LITERATURE FROM ORGANIZATION SCIENCE, ACCOUNTING, MARKETING, MIS, AND RELATED DISCIPLINES. THE INFORMATION SOCIETY, 20, 325-344

JERVIS, R. (1976). PERCEPTION AND MISPERCEPTION IN INTERNATIONAL POLITICS. PRINCETON UNIVERSITY PRESS 21

צמצום קוגניטיבי: חוסר יכולת לדמיין סוגים מסוימים של איומים, דווקא משום שהמערכת שאמורה הייתה לחשוף אותם אינה מציגה אותם. ספרות כשלי המודיעין תיארה דינמיקה זו גם בעידן הטרור-דיגיטלי,<sup>22</sup> אך המערכות הדיגיטליות מעצימות אותה באופן דרמטי.

## מערכות דיגיטליות כמבני תלות

כאשר ארגוני מודיעין וביטחון משלבים מערכות דיגיטליות באופן עמוק בשגרת עבודתם, הם נעשים תלויים בהן מבחינה מבנית. חוקרי מודיעין מתרגלים לעבוד מול זרמי נתונים ומפסיקים בהדרגה להשקיע מאמץ בהבנה עמוקה של היריב. במקביל, הם חדלים כמעט מלפקפק במערכות המייצרות את המידע שעליו הם מסתמכים. במצב כזה מקורות מידע אחרים, ובראשם מחקר מעמיק של תרבות היריב ומודיעין אנושי (HUMINT), נדחקים לשוליים. מקבלי ההחלטות מתרגלים לנראות רציפה בזמן אמת, ולכן כל שיבוש במערכות הדיגיטליות הופך לאירוע בעל השלכות קטסטרופליות. ארגוני מודיעין הם מערכות בירוקרטיות מורכבות, שהכלים שברשותן מעצבים במידה רבה את שגרת פעולתן. לאורך זמן, ארגונים הנשענים באופן אינטנסיבי על תשתיות דיגיטליות מפנימים את ההנחה שמערכות אלה ימשיכו לפעול תמיד כמתוכנן. המערכות הדיגיטליות משנות את ארכיטקטורת עבודת המודיעין בכמה אופנים. ראשית, הן משנות את ההיררכיה של שיטות האיסוף. מודיעין אותות (SIGINT), מודיעין חזותי (IMINT) וניתוח מבוסס נתונים דוחקים בהדרגה את המודיעין האנושי (HUMINT), את הדיווח האיכותני מן השטח ואת הפרשנות ההקשרית. הסיבה לכך נעוצה, בין היתר, בתפיסה שמידע דיגיטלי הוא אובייקטיבי, אמין ופחות מוטע ממידע אנושי. חוקרים הפועלים בסביבה זו לומדים להעניק עדיפות למה שמופיע בתמונה הדיגיטלית, ולהפחית מערכם של אותות הנשענים על פרשנות אנושית.

שנית, תשתיות דיגיטליות מייצרות צורות חדשות של אינרציה ארגונית. מכיוון שמערכות דיגיטליות מחייבות רציפות, סטנדרטיזציה ותחזוקה טכנית, שגרת העבודה הופכת נוקשה יותר ופחות גמישה. עם הזמן, הארגון מתרגל להסתמך על דפוסי איסוף קבועים, על אינדיקטורים מוגדרים מראש ועל התרעות אוטומטיות. במובן זה, המערכת מלמדת את המשתמשים שלה מה לראות ומה להתעלם ממנו. שלישית, התלות הדיגיטלית שוחקת את החוסן הארגוני. כאשר התשתיות הדיגיטליות נפגעות, עקב תקלה, מתקפה או הטעיה מצד היריב, החוקרים עלולים לגלות שאין בידיהם הכישורים האנלוגיים או מנגנוני היתירות המוסדיים הדרושים כדי לפצות על אובדן המידע. ככל שהמערכות הדיגיטליות מתפקדות טוב יותר בשגרה, כך כישלון בעת משבר הופך הרסני יותר. לפיכך, העליונות הדיגיטלית יוצרת פגיעות סמויה אך ניכרת: היא מצמצמת את יכולת ההסתגלות של ארגוני המודיעין. השגרה הבירוקרטית מותאמת לסביבה דיגיטלית יציבה ולא לאי-ודאות. כאשר היריב פועל בדרכים שאינן מייצרות חתימות דיגיטליות, למשל באמצעות תקשורת אנלוגית, ניידות פשוטה או הונאה מכוונת, מתקשה הארגון להסתגל.

## חברות דיגיטליות חשופות יותר ליריביהן

הטכנולוגיות הדיגיטליות אינן פועלות רק בתוך ארגוני המודיעין; הן מחלחלות אל כלל החברה. למעשה, בתחומי טכנולוגיית המידע מתקיים לעיתים גם התהליך ההפוך: סוכנויות המודיעין מאמצות טכנולוגיות אזרחיות לצורכיהן.<sup>23</sup> דמוקרטיה המאמצות פתיחות דיגיטלית, שימוש נרחב ברשתות חברתיות, שירותי מיפוי ציבוריים, מערכות ממשל שקופות ורמה גבוהה של אוריינות דיגיטלית מייצרות כמויות עצומות של מידע שיריבים יכולים לנצל. זוהי אסימטריה מבנית: חברות פתוחות חשופות הרבה יותר מחברות סגורות. לאסימטריה זו יש השלכות אסטרטגיות עמוקות. בעידן האנלוגי נדרש מן היריב להפעיל מערך מודיעיני נרחב כדי לאסוף מידע על מתחים חברתיים, תנועות פוליטיות, גיוסי מילואים או חולשות לוגיסטיות. כיום חלק ניכר מן המידע הזה זמין לציבור. המדינה הדיגיטלית חושפת לעיני העולם, לרבות לעיני אויביה, את דפוסי החיים שלה.

לעומת זאת, משטרים סמכותניים מסוגלים לצמצם את החשיפה באמצעות יצירת "חומות דיגיטליות": צנזורה של רשתות חברתיות, הגבלת שירותי מיקום, או הלאמת תשתיות דיגיטליות. הסודיות במשטרים אלה איננה מוחלטת, אך היא מצמצמת את היקף המידע ואת רמת הפירוט הזמינים ליריבים.

בכך משנה הפתיחות הדיגיטלית את חלוקת הנראות במערכת הבין לאומית. לא רק האזרחים רואים יותר את המדינה, גם יריביה.

HEUER (1999); BETTS, R. K. (2007). ENEMIES OF INTELLIGENCE: KNOWLEDGE AND POWER IN AMERICAN NATIONAL SECURITY. COLUMBIA UNIVERSITY PRESS 22

KATZ, B. (2020). THE COLLECTION EDGE: HARNESSING EMERGING TECHNOLOGIES FOR INTELLIGENCE COLLECTION. CSIS BRIEF 23

התפתחות זו מערערת על ההנחה המסורתית בדבר אסימטריה מודיעינית. במקרים רבים, שחקנים היברידיים, כמו ארגונים לא־מדינתיים חמושים, עשויים ליהנות מתמונה טובה יותר של חולשותיה המבצעיות של מדינה מתקדמת טכנולוגית מאשר להפך. לפיכך, פתיחות דיגיטלית הופכת לפגיעות מבנית במערכת הבין לאומית. היא יוצרת מה שאפשר לכנות אסימטריית מידע הפוכה: החזק נעשה גלוי יותר, בעוד שהחלש נותר נסתר יחסית.

### תרבויות דיגיטליות, לאומיות טכנולוגית ותחושת עליונות

לבסוף, התקדמות דיגיטלית מואצת מחזקת לעיתים קרובות תפיסות של לאומיות טכנולוגית (techno-nationalism) ונרטיבים של ייחודיות טכנולוגית.<sup>24</sup> נרטיבים כאלה מחלחלים אל התרבות האסטרטגית של האליטות ומשפיעים על הציפיות הפוליטיות, על הנהלים הארגוניים ועל ההנחות המוקדמות שבאמצעותן מתפרשים איומים. בסביבה קוגניטיבית זו נוטים מקבלי ההחלטות ואנשי המודיעין להמעיט באופן שיטתי ביכולתם של יריבים בעלי משאבים מוגבלים להסתגל, לחדש ולהפתיע. תפיסה יהירה זו מצמצמת את מגוון האפשרויות המיוחסות ליריב, ומטשטשת את יכולתו לפתח חדשנות מבצעית, להשתמש בהטעיה או להפתיע באמצעות אמצעים פשוטים יחסית. בכך היא מחזקת תחושת עליונות דיגיטלית כוזבת, מחלישה את היכולת להבין את דרך החשיבה של היריב, ופוגעת ביכולת ההתרעה האסטרטגית.

### הדגמת המסגרת: ישראל וההפתעה האסטרטגית של 7 באוקטובר 2023

חלק זה ממחיש את המסגרת המושגית באמצעות בחינת האופן שבו הפגיעות הטכנו־דיגיטלית באה לידי ביטוי בכישלונה של ישראל לחזות את מתקפת חמאס ב־7 באוקטובר 2023. זה אינו חקר מקרה מלא, אלא המחשה אנליטית שמטרתה להראות כיצד ארבעת המנגנונים, אשליה, תלות, נראות־יתר ותחושת עליונות טכנולוגית, פעלו יחדיו ותרמו לכישלון המודיעיני של ה־7 באוקטובר 2023.

ישראל היא מקרה מתאים במיוחד משום שהיא אחת המדינות הדיגיטליות ביותר בעולם. החברה, הצבא וקהילת המודיעין שלה מדגישים כולם את חשיבותן של טכנולוגיות מידע. תפיסת המודיעין הישראלית נשענה במשך שנים על מעקב מתמשך, ניתוח מהיר ותגובה מבצעית מיידית. במובנים רבים, ישראל מייצגת את דגם־האב של מדינה המועצמת באמצעות טכנולוגיה דיגיטלית.

למרות זאת, ב־7 באוקטובר 2023 הצליח חמאס, ארגון היברידי בעל משאבים מוגבלים בהשוואה לישראל, לבצע מתקפת פתע רחבת היקף במספר זירות בו־זמנית. המתקפה ניצלה חולשות במערך ההתרעה, בהגנת הגבול ובמערכת גיוס הכוחות של ישראל.

### ישראל וטכנולוגיות מידע מתקדמות: החברה, הצבא וקהילת המודיעין

התנועה הציונית העניקה לטכנולוגיה מקום מרכזי כבר מראשית דרכה. בהנהגת אליטה טכנוקרטית קטנה שהובילה את מפעל ההתיישבות בארץ ישראל בשלהי המאה התשע־עשרה תחת השלטון העות'מאני, שיחזרה התנועה הציונית, אם כי בקנה מידה קטן בהרבה, את דפוסי הפעולה של האליטות הטכנולוגיות באירופה באותה תקופה.<sup>25</sup>

היישוב היהודי בארץ, תחילה תחת השלטון העות'מאני ולאחר מכן בעיקר תחת המנדט הבריטי, העניק עדיפות גבוהה לחינוך מדעי וטכנולוגי. חוזה המדינה, בנימין זאב הרצל, שילב כבר בספרו האוטופי אלטנוילנד (1902) את מרכזיותו של המדע בפרויקט הציוני. גיבור הספר הוא מדען בהכשרתו, והמדינה העתידית מתקדמת בזכות מחויבותה לערכי המדע וליישומם.<sup>26</sup> גם חיים ויצמן, ממנהיגי הציונות הבולטים, היה מדען בעל שם, ששימש מרצה בכיר לכימיה באוניברסיטת מנצ'סטר לפני שנבחר לנשיאה הראשון של מדינת ישראל עם הקמתה ב־1948.<sup>27</sup> המוסד האקדמי הראשון שהקימה העלייה הציונית החדשה היה הטכניון, המכון הישראלי לטכנולוגיה. הרעיון להקמתו גובש בראשית המאה ה־20 והוא נוסד ב־1912, עוד בתקופה העות'מאנית. בראשית המאה

EDGERTON, D. E. H. (2007). THE CONTRADICTIONS OF TECHNO-NATIONALISM AND TECHNO-GLOBALISM: A HISTORICAL PERSPECTIVE. NEW GLOBAL STUDIES, 1(1), 24  
ARTICLE 1

PENSLAR, D. (1991). ZIONISM AND TECHNOCRACY: THE ENGINEERING OF JEWISH SETTLEMENT IN PALESTINE, 1870–1918. INDIANA UNIVERSITY PRESS 25

HERZL, T. (1902). OLD NEW COUNTRY. ZIONIST ORGANIZATION 26

REINHARZ, J., & GOLANI, M. (2024). CHAIM WEIZMANN: A BIOGRAPHY. BRANDEIS UNIVERSITY PRESS 27

ה־21 כבר התהדר הטכניון במספר חתני פרס נובל ואף דורג באחד הסקרים כמוסד המוביל בעולם בתחום ההוראה הדיגיטלית.<sup>28</sup> עם הקמת המדינה התחזק עוד יותר הדגש על מדע וטכנולוגיה. ראש הממשלה הראשון, דוד בן־גוריון, הצהיר ב־1949 כי "תחיית עם ישראל, בניית המדינה מתוך החורבן, פיתוח הכלכלה שתוכל לקלוט מיליוני עולים והשגת עצמאות כלכלית, כל אלה מותנים בפיתוח המרבי של המדע בישראל"<sup>29</sup>

האיום הביטחוני המתמשך סיפק תמריץ נוסף להשקעה במדע ובטכנולוגיה, כאמצעי לאיזון הפער במשאבים בין המדינה היהודית הקטנה לבין העולם הערבי שסביבה. כבר ב־1948 הקים צה"ל את חיל המדע, שממנו התפתחה בהמשך הרשות לפיתוח אמצעי לחימה (רפא"ל). מפקדו הראשון היה הביו־פיזיקאי אפרים קציר, ואחיו, הכימאי אהרן קציר, שהמשיך אף הוא לקדם את מרכזיותו של המדע בישראל.<sup>30</sup> עדות למרכזיות המדע בישראל היא העובדה שפרופ' אפרים קציר נבחר ב־1973 לנשיאה הרביעי של מדינת ישראל.<sup>31</sup> בהמשך השקיעה המדינה באופן שיטתי במחקר ופיתוח, וב־2025 הייתה אחת המדינות המובילות ב־OECD בהיקף ההשקעה הציבורית בתחום.<sup>32</sup>

עם המעבר העולמי לעידן טכנולוגיות המידע, החלה ישראל כבר בשנות השבעים לעודד את פיתוח התחום באמצעות מענקים ותמיכה בחברות הזנק, לרבות בתקופות משבר עולמי כגון משבר 2008.<sup>33</sup> החוקר דן ברזניץ סיכם מדיניות זו בקביעה כי "תעשיית ההיי־טק הישראלית היא הצלחה מרשימה".<sup>34</sup> הצלחה זו עיצבה גם את הדימוי העצמי והבין לאומי של ישראל כ"מדינת הסטארט־אפ".<sup>35</sup>

מרכזיותם של המדע והטכנולוגיה בחברה הישראלית באה לידי ביטוי גם במערכת הביטחון, שראתה בהם "מכפיל כוח" ואמצעי לאיזון העליונות המספרית של מדינות ערב. החוקר צ'ארלס פרייליך סיכם תפיסה זו וכתב שהחזון היה כי "היכולות הטכנולוגיות מבצעיות המתקדמות של ישראל יאפשרו לאותו מספר מטוסים לבצע יותר גיחות, לטנקים להשיג שיעור פגיעות גבוה יותר, ולכוחות היבשה לפעול בניידות רבה יותר".<sup>36</sup>

לשם כך הוקמו מוסדות ייעודיים למחקר ופיתוח ביטחוני, ונבנתה תעשייה ביטחונית רחבת היקף, שב־2024 כבר ייצאה ציוד ביטחוני בכ־15 מיליארד דולר בשנה.<sup>37</sup> בשלב הזה, על פי החוקר איתי שפירא, "התרבות האסטרטגית הישראלית, אימצה תכונות של טכנו־פיליה" (אהבת הטכנולוגיה).<sup>38</sup> עם זאת, היו שהזהירו מפני התלות בטכנולוגיה. תא"ל (מיל') ד"ר מאיר פינקל, למשל, הביע במאמר מ־2006 חשש מ"פולחן הטכנולוגיה" בצה"ל, העלול לבוא על חשבון מרכיבים חיוניים אחרים של הכשירות הצבאית, ובהם תורה, אימונים, פיתוח כוח אדם ולוגיסטיקה.<sup>39</sup>

מבין גופי מערכת הביטחון, קהילת המודיעין היא אולי הבולטת ביותר בשימוש טכנולוגיה. זאת, לצורכי איסוף, עיבוד והפצת מודיעין, ובשנים האחרונות גם לצורכי תקיפה. תהליך זה החל בעקבות הלקחים שהפיקה ישראל ממלחמת המפרץ הראשונה וממלחמת קוסובו, שבהן הודגמה יכולת האיסוף הרב־ממדית והשימוש במידע לצורך תקיפות מדויקות.<sup>40</sup>

TECHNION UK. (2024b). ISRAEL'S TECHNION RANKED #1 WORLDWIDE IN DIGITAL EDUCATION. [HTTPS://TECHNIONUK.ORG/NEWS-POST/ISRAELS-TECHNION-RANKED-1-WORLDWIDE-IN-DIGITAL-EDUCATION](https://technionuk.org/news-post/israels-technion-ranked-1-worldwide-in-digital-education) 28

בן־גוריון, ד' (1958). חזון ודרך. בתוך י' בקר, משנתו של דוד בן־גוריון (עמ' 582). יבנה 29

קציר, א' (1971). בבור המהפכה המדעית. עם עובד 30

ARNON, R., SELA, M., & SHINDLER, C. (2016). EPHRAIM KATCHALSKI-KATZIR. ROYAL SOCIETY 31

HARRIS, L. (2025). YOUR TAXES: ISRAEL'S R&D EDGE OVER OTHER OECD COUNTRIES. JERUSALEM POST 32

COHEN, E. (2011). THE DEVELOPMENT OF THE HIGH-TECH INDUSTRY IN ISRAEL, AND GOVERNMENT POLICY TO SUPPORT IT. IN E. COHEN & A. LEV-ON (Eds.), 33  
CONNECTED: POLITICS, TECHNOLOGY AND SOCIETY IN ISRAEL. ISRAELI ASSOCIATION OF POLITICAL SCIENCE

BREZNITZ, D. (2007). INNOVATION AND THE STATE: POLITICAL CHOICE AND STRATEGIES FOR GROWTH IN ISRAEL, TAIWAN, AND IRELAND. YALE UNIVERSITY PRESS, P. 41 34

SENROR, D., & SINGER, S. (2009). START-UP NATION: THE STORY OF ISRAEL'S ECONOMIC MIRACLE. COUNCIL ON FOREIGN RELATIONS 35

FREILICH, C. (2018). ISRAELI NATIONAL SECURITY: A NEW STRATEGY FOR AN ERA OF CHANGE. CORNELL UNIVERSITY PRESS, PP. 24–25 36

AZULAI, Y. (2025). ISRAELI DEFENSE EXPORTS AT NEW HIGH OF 15 BILLION USD. CALCALIST 37

SHAPIRA, I. (2026). ISRAELI DEFENSE AND INTELLIGENCE BEFORE AND AFTER OCTOBER 2023: THE CULTURAL ROOTS OF STRATEGIC SURPRISE AND RESILIENCE. 38  
ROUTLEDGE, P. 48

FINKEL, M. (2006). THE IDF'S CULT OF TECHNOLOGY: RESTORING BALANCE TO GROUND FORCE DEVELOPMENT. MAARACHOT, 407, 40–45 39

עמידור, י' (2002). הרהורים על צבא ובטחון: מאמרים, מכתבים והרצאות. עיצוב 40

באגף המודיעין של צה"ל התעצם המהפך בעיקר במהלך העשור השני של המאה ה-21, בהובלת האלוף אביב כוכבי (2010–2014). אמ"ן שינה את תפיסתו הארגונית סביב שילוב הולך וגובר של מערכי מודיעין, תצפית וסיור (ISR), סייבר, עיבוד נתונים ויכולות תקיפה מדויקות. טלטלות האביב הערבי, קריסת מדינות ועליית השפעתה האזורית של איראן הפחיתו את מרכזיותם של צבאות סדירים והעלו את חשיבותם של ארגונים היברידיים הפועלים מתוך אוכלוסייה אזרחית. אך מה שהפך שינוי זה למשמעותי מבחינה מבצעית היה בראש ובראשונה ההתפתחות הטכנולוגית שאפשרה רמות חסרות תקדים של גילוי, זיהוי ותקיפה מהירה.<sup>41</sup>

אמ"ן העריך יותר ויותר כי הסבירות למלחמות בין-מדינתיות רחבות היקף פוחתת, בעוד שעימותים תת-קונבנציונליים מתמשכים הופכים לצורת הלחימה המרכזית. בתוך מציאות זו הפכו ה"סיכול הממוקד" ופגיעות מדויקות אחרות ביכולות היריב לליבת פעילות המודיעין. ישראל הרחיבה את השקעותיה ביכולות סייבר התקפיות והגנתיות, במערכות עיבוד נתונים אוטומטיות, במערכי איסוף מתמשכים ובמערכות מיזוג מידע מבוססות אלגוריתמים. יחידה 8200 מילאה תפקיד מרכזי בהתפתחויות אלה נוכח שאיפת אמ"ן לקצר את משך הזמן שבין גילוי המטרה לבין הפעלת האש לכמעט זמן אמת.

### מתקפת ההפתעה של 7 באוקטובר 2023 וכשל המודיעין הישראלי

בבוקר ה-7 באוקטובר 2023 פרצו למעלה ממאה חוליות של חמאס את גדר הגבול המפרידה בין רצועת עזה לישראל ותקפו בסיסים צבאיים, יישובים אזרחיים ושתי מסיבות טבע. בסיומו של אותו יום נהרגו קרוב ל-1,200 ישראלים, ו-251 ישראלים חיים ומתים נחטפו לרצועת עזה. בתוך 24–48 שעות הצליח צה"ל להשתלט מחדש על כלל השטחים שנכבשו. זמן קצר לאחר מכן פתח צה"ל במתקפה רחבת היקף ברצועת עזה. בהמשך התרחבה המלחמה וכללה גם את חזבאללה בלבנון, את החות'ים בתימן ובהמשך גם את איראן. עד אוקטובר 2025 נהרגו כ-90,000 בני אדם, רובם ברצועת עזה, אך גם, כאמור, בישראל וכן בלבנון, סוריה, עיראק, תימן ואיראן.

המודיעין הישראלי כשל לחלוטין במתן התרעה מפני המתקפה. הכשל המודיעיני של ה-7 באוקטובר התרחש בשלוש הרמות גם יחד: הטקטית, האופרטיבית והאסטרטגית.

ברמה המיידית ביותר לא הצליח המודיעין הישראלי להפיק התרעה טקטית: התרעה ממוקדת ורגישה לזמן, שאמורה להינתן כאשר מתקפה עומדת להתרחש, וזאת למרות קיומם של סימנים מבצעיים ברורים בשעות שקדמו למתקפה. אינדיקציות שהיו אמורות להביא לשינוי מידיי בפריסת הכוחות זכו להתעלמות או פורשו באופן שגוי. גם לאחר שני דיונים שנערכו בשעות הלילה המאוחרות ולפנות בוקר טרם ההתקפה בהשתתפות בכירי מערכת הביטחון והמודיעין, לא הצליחה המערכת לתרגם את הסימנים המעורפלים להתרעה קונקרטיה.

המודיעין כשל גם ברמה האופרטיבית. שנים לפני המתקפה החזיקה קהילת המודיעין במידע משמעותי על תוכנית הפעולה של חמאס, ובכלל זה על התוכנית שכונתה בישראל "חומת ירחו". ואולם, מידע זה לא הוטמע באופן מספק בתכנון המבצעי של צה"ל ובאופן הפעלת הכוחות. כתוצאה מכך, מערך ההגנה של פיקוד הדרום לא הותאם להתפתחות יכולותיו של היריב ולשינוי בדוקטרינת הלחימה שלו. מצב זה משקף שילוב המוכר היטב בספרות על כשלי מודיעין: ביטחון עצמי מופרז, דימוי מראה והתקבעות בהנחות בנוגע לדפוסי הפעולה ה"רגילים" של היריב, שילוב שפגע קשות ביכולתה של המערכת להסתגל למציאות המשתנה.<sup>42</sup>

המערכת כשלה גם ברמה האסטרטגית. התרעה אסטרטגית נועדה להתריע בפני מקבלי ההחלטות על שינויים ארוכי טווח בהעדפותיו של היריב, במידת הנכונות שלו ליטול סיכונים ובתפיסת הניצחון שלו, גם כאשר שינויים אלה אינם גלויים במלואם. המודיעין הישראלי לא הצליח לזהות את המעבר של חמאס ממדיניות שהתבססה על סבבי ירי רקטות מוגבלים, שנועדו לשמור את שרידות הארגון, לאסטרטגיה עתירת סיכון ובעלת פוטנציאל רווח גבוה, שהתבססה על חדירה קרקעית רחבת היקף.

EIRAN, E., GUTERMAN, O., & SIMAN-TOV, D. (2025). THE VANISHING WATCHMAN: THE RISE AND DECLINE OF EARLY WARNING. INTELLIGENCE AND NATIONAL SECURITY, 40, 863–885

BOB, Y. J. (2025). NEW IDF PROBE REVEALS FAILURES IN FIVE OCTOBER 7 INVESTIGATIONS, WHICH NEED TO BE REDONE. JERUSALEM POST

כישלון זה נבע בחלקו מהטעיה מוצלחת ומשמירה קפדנית על ביטחון מידע מצד חמאס. אולם הוא שיקף גם כשל אנליטי עמוק יותר: היצמדות למסגרת תפיסתית מיושנת שראתה בחמאס שחקן זהיר, המבקש לשמר יציבות יחסית ולהימנע ממלחמה רחבת היקף. בפועל, המסגרת האפיסטמית שבאמצעותה פירשו גופי המודיעין את התנהלות חמאס נותקה מן ההתפתחות שחלה בדוקטרינה, בכוונות ובתפיסת ההפעלה של הארגון.<sup>43</sup>

שלוש רמות הכשל הללו, פרשנות טקטית שגויה, אי-התאמה אופרטיבית וניתוח אסטרטגי מוטעה, ממחישות היטב את הדינמיקה הקלסית של הפתעה מודיעינית המתוארת בספרות המחקר: קיבעון מחשבתי, פיצול ארגוני והטעיה מצד היריב חברו יחד ופגעו ביכולתה של מערכת ההתרעה לפעול בדיוק ברגע שבו הייתה נחוצה ביותר.

בחלקים הבאים ינותחו ארבעת מנגנוני הפגיעות הטכנו-דיגיטלית שהובילו לכשל מודיעיני זה.

### **אשליית העליונות הדיגיטלית: כישלונה של תפיסת "עליונות המודיעין"**

המודיעין הישראלי האמין שמערכות המעקב והאיסוף שלו מספקות חדירה עמוקה לכל אויביה של ישראל באזור, ובכללם חמאס. למעשה, התפיסה המארגנת של אמ"ן הוגדרה כ"עליונות מודיעינית" שנועדה לתמוך בלחימה המבוססת על מודיעין והפכה למשימתו המרכזית של הארגון, וזאת, בפועל, תוך תיעדוף נמוך יותר או אולי אפילו על חשבון משימת ההתרעה המוקדמת.<sup>44</sup>

ב-2022 הציג הרמטכ"ל אביב כוכבי (שכיהן קודם לכן כראש אמ"ן) בפורום ציבורי את הישגי המודיעין. הוא סיפר כי הודות ליכולות האיסוף והעיבוד של אמ"ן מסוגלת ישראל לדעת את תוכנה המדויק של כל משאית המובילה אמצעי לחימה מעיראק לסוריה. לדבריו, יכולת זו, בשילוב אמצעי התקיפה המדויקים שבידי ישראל, משקפת "יכולות מתקדמות מאוד".<sup>45</sup>

עם הזמן יצרו הצלחות אלה אמונה עמוקה כי אף אחד מאויביה האזוריים של ישראל, ובכלל זה חמאס, אינו מסוגל להתארגן, להתאמן או לשנות את דפוסי פעולתו מבלי להותיר חתימות מודיעיניות שהמערכת תוכל לזהות. בדרך זו חיזקה הארכיטקטורה הדיגיטלית תפיסה אסטרטגית מוטעית. ארגוני מודיעין נוטים לראות במערכות הטכנולוגיות שלהם מקור אובייקטיבי לאמת. כאשר המערכות משדרות יציבות, האנליסטים נוטים להסיק שגם המציאות האסטרטגית עצמה יציבה, אף שלמעשה השקט המודיעיני עשוי לשקף דווקא את הצלחתו של היריב להסתגל, להסתיר את פעילותו או להימנע מיצירת חתימות דיגיטליות ולא היעדר איום ממשי.

### **תלות דיגיטלית ושיתוק מערכתי**

המנגנון השני, התלות הארגונית במערכות דיגיטליות, בא לידי ביטוי באופן בולט במהלך המתקפה עצמה. כבר בשלבים הראשונים של המבצע הצליח חמאס לנטרל חלקים משמעותיים ממערך המעקב הדיגיטלי של ישראל. רחפנים השמידו מגדלי תקשורת ומצלמות, קווי חשמל נותקו, וחלקים מרכזיים של המכשול החכם לאורך הגבול הושבתו.<sup>46</sup>

התוצאה לא הייתה רק אובדן של יכולת התצפית, אלא שיתוק ארגוני רחב. יחידות שהתרגלו להסתמך על תמונת מצב דיגיטלית בזמן אמת לא החזיקו באמצעים חלופיים ליצירת תמונת מצב. מערכות הדיווח הידניות היו איטיות, מקוטעות ולא התאימו להיקף האירוע. תחקירי צה"ל קבעו כי "מרכז המבצעים של המפקדה לא הצליח להבין את תמונת המצב בשעות הראשונות [של המתקפה]..." יתרה מזאת, המפקדות התקשו להבין גם את מצבם של מרכזי הפיקוד הכפופים להן, ובמיוחד את מצבה של אוגדת עזה.<sup>47</sup> הכוחות שפעלו בשטח וחיל האוויר התקשו לתקשר ביניהם, להבין את היקף החדירה ולתאם תגובה אפקטיבית. המערכת כולה, מערכת ריכוזית, דיגיטלית ותלויה בחיישנים, לא הצליחה לשחזר תמונת מצב מבצעית לאחר שהתשתיות המרכזיות שעליהן נשענה קרסו. בכך המחשישה המתקפה כיצד תלות עמוקה במערכות דיגיטליות עלולה להפוך כשלים מקומיים לקריסה מערכתית

43 סימנטוב, ד' וגורמן, ע' (עורכים) (2025). המודיעין והשבעה באוקטובר. מערכות והמרכז למורשת המודיעין

44 (EIRAN, GUTERMAN AND SIMAN-TOV (2025

45 האמל"ח במשאית מספר 8: כוכבי אישר שצה"ל תקף שיירה בגבול סוריה-עיראק (14 בדצמבר 2022). מעריב

46 חלבי, ע' (8 באוקטובר 2023). השמידו את "העיניים של הלוחמים", פוצצו גדר – ופשטו: התיעוד ממתקפת הפתע, והסימנים המעידים שפוספסו. וואינט

47 זיתון, י' (27 בפברואר 2025). 1,175 מחבלים בגל הראשון, מול 671 לוחמים: "אל תופתעו אם יגיעו לת"א": הפקודות הדמטיות בבור, דקה אחר דקה. וואינט

רחבת היקף. הפגיעה לא התבטאה רק באובדן מידע, אלא גם באובדן יכולתה של המערכת לארגן, לעבד ולהפיץ מידע חלופי. התלות הדיגיטלית הפכה את השבתת כמה רכיבים טכנולוגיים לקריסה של מנגנון קבלת ההחלטות כולו.

במילים אחרות, לא עצם אובדן החיישנים היה הגורם המרכזי לכשל, אלא העובדה שהארגון התקשה לתפקד כאשר אותם חיישנים חדלו מלפעול. זהו ביטוי מובהק למה שמאמר זה מכנה פגיעות טכנולוגיות. מצב שבו העליונות הטכנולוגית עצמה יוצרת תלות כה עמוקה, עד שפגיעה נקודתית במערכת הופכת במהירות למשבר אסטרטגי.

## נראות-יתר (Hypervisibility) וניצול על ידי היריב

חמאס ניצל את פתיחותה הדיגיטלית של ישראל במספר דרכים. מאז השתלטותו על רצועת עזה ב־2007, פעילות איסוף המודיעין הגלויה של הארגון עברה תהליך של מיסוד, בעיקר באמצעות מחלקת המודיעין הצבאי של גדודי עז א־דין אל־קסאם. פעילות זו התבססה במידה רבה על סביבת התקשורת הפתוחה והנגישה בישראל, אשר סיפקה לארגון גישה נרחבת למידע על צה"ל, מערכת הביטחון, הפוליטיקה הישראלית והחברה בישראל. חמאס הקים מנגנון שיטתי למעקב אחר אמצעי התקשורת בישראל, שכלל, בין היתר, פרסומים קבועים. כך למשל, מאז 2007 פרסם הארגון דוח שבועי בשם "ענייני ישראל", שסקר מגוון רחב של סוגיות אזרחיות וביטחוניות בישראל. הדוח סיכם את ההתפתחויות המרכזיות, ניתח אותן והסתייג בהערכה אופרטיבית שנועדה לשימוש פנימי. הפרסומים שעסקו בצה"ל כללו מידע על מבנה הכוחות, תרגילים צבאיים ואמצעי לחימה חדשים. המידע נאסף מעיתונות מודפסת, משידורי טלוויזיה ורדיו ומאתרי אינטרנט. בנוסף, חמאס עשה שימוש גם בתיעוד וידאו של קרבות ברצועת עזה שצה"ל עצמו פרסם באמצעי התקשורת. כך למשל, תיעוד הקרב עם חטיבת גולני ביולי 2007 שימש להכשרת לוחמי הארגון בזיהוי הסכנות הנשקפות מתצפיות אוויריות וממערכות תצפית תרמיות של צה"ל.<sup>48</sup>

גם הרשתות החברתיות סיפקו לחמאס חלון אל תוך החברה הישראלית. הדיונים הציבוריים סביב הקיטוב הפוליטי, מחאות אנשי המילואים והמתחים הפנימיים בחברה הישראלית סיפקו לארגון אינדיקציות גלויות על מצבה של ישראל. במקביל, סרטוני רחפנים אזרחיים שהופצו ברשת חשפו דפוסי תנועה של סיורי הגבול, ואילו תצלומי לוויין מסחריים, שהיו זמינים לכל דורש, אפשרו ללמוד על תשתיות צבאיות, מאפייני השטח ואף על המבנה הפנימי של בסיסים שהותקפו מאוחר יותר.<sup>49</sup>

## הירות והערכת חסר של מי שאינם באותה רמה טכנולוגית

לבסוף, הדרג המדיני וגופי המודיעין בישראל העריכו הערכת יתר את יכולותיהם שלהם, ובה בעת העריכו הערכת חסר את יכולותיו של חמאס. הערכות אלה נשענו במידה רבה על הפערים הטכנולוגיים שבין שתי החברות. כך, ראש הממשלה לשעבר נפתלי בנט תיאר ב־2013 את הסוגיה הפלסטינית כבעיה כואבת אך ניתנת לניהול, "כמו רסיס"<sup>50</sup> בישבן. במילים אחרות, הוא רמז כי פערי העוצמה בין ישראל לבין הפלסטינים מאפשרים לישראל להכיל את שאיפותיהם הלאומיות לאורך זמן. תפיסת עולמו של בנט נשענה במידה רבה על אמונתו בעליונותה הטכנולוגית של ישראל. בנט, יש לציין, הוא ראש הממשלה הישראלי הראשון שהגיע מרקע של תעשיית ההיי־טק.

באופן קונקרטי יותר, ישראל השתכנעה כי יתרונה הטכנולוגי מונע מחמאס כל אפשרות ממשית לחדור דרך הגבול. מאז 2014 נתפס איום המנהרות כאיום המרכזי הנשקף מרצועת עזה. לפיכך, בשלהי העשור השני של המאה ה־21 החלה ישראל בבניית מכשול מתקדם עתיר טכנולוגיה, שכלל חיישנים ומערכת תת־קרקעית שנועדה לנטרל את איום המנהרות. בדצמבר 2021 הושלם הפרויקט, שעלותו הגיעה לכמיליארד דולר, והוכרז כמבצעי. המכשול, שצה"ל הגדיר כ"מערכת הגנתית", כלל: מכשול תת־קרקעי פיזי וטכנולוגי באורך של כ־65 ק"מ; גדר עילית שגובהה למעלה משישה מטרים, המשולבת במערכות ליירוט רחפנים, כלי טיס ואיומים אוויריים נוספים; מכשול ימי המצויד בחיישנים לגילוי חדירות מן הים; מערכת נשק המופעלת מרחוק; רשת של מכ"מים ומצלמות המספקת מודעות מצבית ויכולות לגילוי מנהרות; מרכזי שליטה ובקרה ברמת הגדוד, החטיבה והאוגדה.

48 FLAMER, N. (2024). THE HAMAS INTELLIGENCE WAR AGAINST ISRAEL. CAMBRIDGE UNIVERSITY PRESS, PP. 59–75

49 אשכנזי, א' (4 במרס 2025). האוצר שגנב חמאס מישראל: ההחלטה הדומטית של צה"ל ללוחמים. מעריב

50 שיף, ע' (23 ביולי 2024). קונספציית הרסיס בישבן. וואינט

עם השלמת הפרויקט בירכו שר הביטחון והרמטכ"ל על הישג זה. שר הביטחון תיאר אותו כפתרון "טכנולוגי ויצירתי, ראשון במעלה השולל מחמאס אחת מהיכולות שאותן ניסה לפתח, ומציב קיר ברזל, סנסורים ובטון, בינו לבין תושבי הדרום". הרמטכ"ל הילל את הפרויקט ככזה המשקף "חשיבה מחוץ לקופסה"<sup>51</sup>. ואולם, כאשר הגיעו לידי גורמי המודיעין תוכניות מפורטות של חמאס למתקפה קרקעית רחבת היקף, הן נדחו כ"התרברבות ריקה". גורמי המודיעין לא האמינו כי יריב הנחות מהם מבחינה טכנולוגית מסוגל להתגבר על מערכות ההגנה המתקדמות של ישראל.<sup>52</sup> העליונות הדיגיטלית יצרה אפוא דמיון אסטרטגי שלפיו אמצעים פשוטים יחסית כגון מצנחי רחיפה, דחפורים, מטעני חבלה ורחפנים מסחריים, אינם מסוגלים לגבור על מערכות דיגיטליות מתקדמות. כתוצאה מכך, החדשנות של היריב בתחום הטכנולוגיה הנמוכה לא שולבה בהערכות המודיעין, אף על פי שסימניה היו גלויים לעין. בכך יצרה העליונות הטכנולוגית דווקא עיוורון אסטרטגי: ככל שגבר הביטחון ביכולות הדיגיטליות של ישראל, כך פחתה היכולת לדמיין תרחישים שבהם יריב בעל משאבים מוגבלים מצליח לעקוף אותן באמצעות יצירתיות, הסתגלות ושימוש באמצעים פשוטים.

## דין ומסקנות

מאמר זה מבקש לקדם את הספרות הקיימת על הסתמכות יתר על טכנולוגיה, באמצעות מעבר מאזהרות נורמטיביות וביקורות ארגוניות אל הסבר שיטתי לשאלה מדוע עליונות דיגיטלית עלולה דווקא לייצר פגיעות אסטרטגיות. מאמר זה מציע מסגרת מושגית – פגיעות טכנולוגיות – המפרטת את המנגנונים שבאמצעותם מערכות דיגיטליות מעצבות מחדש את הקוגניציה, הארגון והאינטראקציה האסטרטגית, ובכך מגבירות את הסיכון להפתעה. זאת, באמצעות המשגה של ארבעה מנגנונים הקשורים זה בזה:

1. אשליית שלמות המידע;
2. תלות מבנית במערכות דיגיטליות;
3. נראות יתר של החברה;
4. הערכת חסר שיטתית של יריבים דלי-טכנולוגיה;

מבחינה אמפירית, המאמר מרחיב את הספרות באמצעות הדגמה כיצד פעלו ארבעת המנגנונים בזמנית ברמות הטקטית, האופרטיבית והאסטרטגית בכישלון המודיעיני של ישראל ב-7 באוקטובר 2023. בכך הוא מראה שהפתעה לא התרחשה למרות עודף המידע, אלא דווקא בגללו.

באופן זה מעביר המאמר את מוקד הדיון מן השאלה האם טכנולוגיה עלולה להיכשל אל השאלה כיצד ארכיטקטורות דיגיטליות עצמן מייצרות תפיסות שגויות, קיבעון ארגוני והזדמנויות ליריב, ובכך מציע מסגרת כללית לניתוח הפתעה אסטרטגית במדינות מתקדמות דיגיטליות.

## חשיבה מחדשת על הגישות המסורתיות להפתעה אסטרטגית

הספרות הקלסית על הפתעה אסטרטגית מספקת כלים אנליטיים רבי עוצמה להבנת הסיבות לכך שמדינות מופתעות מאיומים. חוקרים בתחום זה מדגישים הטיות קוגניטיביות, כשלים ארגוניים, בעיות בתיאום בין-ארגוני ולחצים פוליטיים. למרות ההבדלים ביניהם, משותפת לכל הגישות הללו הנחה בסיסית אחת: כישלונות מודיעיניים נובעים מכך שמידע מתפרש באופן שגוי, זוכה להתעלמות או מודחק, ולא מכך שהוא אינו קיים. העידן הדיגיטלי מוסיף רובד חדש של מורכבות.

מערכות דיגיטליות מייצרות כמויות עצומות של מידע, אך גם מעצבות את האופן שבו מידע נאסף, מעובד ומתפרש. המודלים המסורתיים של הפתעה אסטרטגית לא חזו מציאות שבה: חיישנים אוטומטיים שולטים באיסוף המידע ומודלים של בינה מלאכותית מעצבים ציפיות ומפיקים תחזיות בעוד אנליסטים מסתמכים על לוחות בקרה בזמן אמת ומקבלי ההחלטות מוצפים בזרמי מידע בלתי פוסקים.

לפיכך, אף שהספרות הקלסית נותרת חיונית, יש לעדכן אותה כך שתתחשב באופן שבו תשתיות דיגיטליות יוצרות הן צורות חדשות של עיוורון מודיעיני והן מסלולים חדשים להפתעה אסטרטגית.

51 הושלמה בניית המכשול סביב רצועת עזה: כך זה נראה (7 בדצמבר 2021). פיקוד הדרום, מערכת אתר צה"ל

52 אייל, נ' (11 באוקטובר 2024). הפצצה והמחדל. וואינט

ממסגרת הפגיעות הטכנו־דיגיטלית נגזר שהפתעה אסטרטגית עלולה להתרחש בעתיד לא למרות עודף המידע, אלא דווקא בגללו. מבני הנתונים עצמם עלולים להטעות. אלגוריתמים עשויים לקבע הנחות קיימות במקום לערער עליהן. האמונה בעליונות ובידיעה הדיגיטלית מצמצמת את מגוון התרחישים הנתפסים כסבירים, ובכך דווקא מגבירה את הסיכוי להפתעות מסוגים מסוימים.

### טכנולוגיה, עוצמה והפרדוקס של היכולת

אחת המסקנות המרכזיות של המסגרת התאורטית היא שהיכולת הטכנולוגית אינה פועלת באופן ליניארי. התאוריה הריאליסטית רואה באופן מסורתי ביכולת גורם מצטבר: ככל שלמדינה יש יותר עוצמה, כך היא בטוחה יותר. העליונות הדיגיטלית נראית לכאורה כאישור להיגיון זה. אולם, כפי שהראו החוקרת רבקה סלייטון ואחרים בתחום הסייבר, מערכות מתקדמות יוצרות גם צורות חדשות של פגיעות.<sup>53</sup> לדוגמה, פלטפורמות דיגיטליות רבות מבוססות על צימוד הדוק (tight coupling): רכיבים רבים התלויים זה בזה ופועלים בסנכרון מלא. מבנה כזה יעיל מאוד, אך גם שברירי מאוד. כך, כשל קטן במקום אחד עלול להתפשט במהירות לכלל המערכת.

רעיון זה מהדהד את התאוריה הקלסית של החוקר צ'רלס פר<sup>54</sup> על תאונות במערכות מורכבות, שלפיה דווקא המאפיינים המשפרים את ביצועי המערכת הם גם אלה המגדילים את הסיכון לכשל קטסטרופלי. כאשר מיישמים תובנה זו על יחסים בין לאומיים, מתקבלת הטענה כי עליונות דיגיטלית מייצרת גם חשיפה רחבה יותר לפגיעות. ככל שמדינה משקיעה יותר בכלים דיגיטליים לצורכי מודיעין, מעקב ותקיפה, כך היא נעשית תלויה יותר בשלמותם ובתקינותם של כלים אלה. מכיוון שיריבים מסוגלים לעיתים לשבש או לעקוף מערכות דיגיטליות באמצעים פשוטים וזולים יחסית, היתרון הטכנולוגי עצמו הופך למקור של פגיעות מבנית. דינמיקה זו מערערת על אחת מהנחות היסוד של הריאליזם. היא מצביעה על כך שהיכולת הטכנולוגית אינה רק מכפיל כוח צבאי וכפייה, אלא גם מחוללת סיכונים חדשים.

### פתיחות ליברלית, שקיפות וחשיפה אסטרטגית

התאוריה הליברלית ביחסים בין לאומיים מדגישה את יתרונותיה של הפתיחות. שקיפות מפחיתה אי־ודאות, מקלה על שיתוף פעולה ותומכת באחריותיות (accountability) דמוקרטית. בעידן הדיגיטלי, פתיחות נתפסת לעיתים קרובות הן כערך נורמטיבי והן כיתרון אסטרטגי. אולם, כפי שמראים פארל וניומן,<sup>55</sup> תלות הדדית יוצרת גם הזדמנויות לניצול התלות על ידי יריבים. המושג נראות־יתר (Hypervisibility), כלומר החשיפה המבנית של חברות דמוקרטיות ודיגיטליות, מציב אתגר להנחות היסוד של הגישה הליברלית.

מחאות ציבוריות, דיונים ברשתות חברתיות, שירותי מיפוי פתוחים, פלטפורמות דיגיטליות של שירותים ציבוריים והיקף עצום של מידע הנוצר באמצעות טלפונים ניידים מספקים ליריבים תמונה מפורטת של נקודות התורפה הפנימיות של המדינה. זאת, אף שמעולם לא נועדו לשמש מקור מידע עבור אויבים. לפיכך, הפתיחות הדיגיטלית אינה רק נכס; היא גם מקור לפגיעות אסטרטגיות. זו אינה טענה נגד דמוקרטיה דיגיטלית, אלא קריאה לשלב את שאלת החשיפה הדיגיטלית במסגרת הערכת הסיכונים הלאומיים. דמוקרטיות יצטרכו למצוא דרכים לשמר את יתרונות הפתיחות, ובמקביל לצמצם את הנראות המבנית שהיא יוצרת.

### קונסטרוקטיביזם, זהות ויהירות טכנו־לאומית

הגישה הקונסטרוקטיביסטית ביחסים בין לאומיים מדגישה את תפקידם של זהויות, נרטיבים ומשמעויות חברתיות בעיצוב התנהגותן של מדינות. מסגרת הפגיעות הטכנו־דיגיטלית משתלבת היטב בתובנות אלה. נרטיבים של עליונות טכנולוגית, הרווחים הן בדמוקרטיות מתקדמות והן בקרב מעצמות מתפתחות, מעצבים את הציפיות של ארגונים ואת האופן שבו הם מעריכים איומים. מדינות שזהותן הלאומית כרוכה בחדשנות טכנולוגית נוטות לראות בטכנולוגיה לא רק כלי עבודה, אלא גם מקור לגאווה לאומית ולעליונות מוסרית. לממד הזהוטי יש חשיבות רבה, משום שהתרבות הארגונית מפרשת את הטכנולוגיה דרך תפיסת העצמי הלאומית. כך עלולה להתפתח יהירות טכנו־לאומית המביאה להערכת יתר של היכולות הדיגיטליות של המדינה ולהערכת חסר של יריבים המאמצים אסטרטגיות פשוטות יותר: אנלוגיות, דלות טכנולוגיה או היברידיות. כאשר משלבים את הקונסטרוקטיביזם עם

SLAYTON (2017) 53

PERROW, C. (1984). NORMAL ACCIDENTS: LIVING WITH HIGH-RISK TECHNOLOGIES. BASIC BOOKS 54

FARRELL AND NEWMAN (2019) 55

מסגרת הפגיעות הטכנו־דיגיטלית, מתקבלת מסקנה רחבה יותר: הפתעה אסטרטגית אינה רק כישלון של מידע או של קוגניציה; לעיתים היא גם כישלון של זהות. במקרים כאלה, הנרטיבים שהמדינה מספרת לעצמה על עליונותה הדיגיטלית עשויים לעוות אותה מפני אפשרויות פעולה אחרות של היריב.

## לקראת תאוריה דיגיטלית של הפתעה אסטרטגית

כלל התובנות שהוצגו עד כה מצביעות על הצורך בפיתוח תאוריה מעודכנת של הפתעה אסטרטגית, אשר תשלב בלב הניתוח תשתיות דיגיטליות, מערכות סוציו־טכנולוגיות ונרטיבים תרבותיים.

תאוריה כזו תכיר בכך כי:

- מערכות דיגיטליות מעצבות את האופן שבו בני אדם תופסים את המציאות.
  - הן מעצבות את שגרות העבודה של ארגוני המודיעין.
  - הפתיחות הדיגיטלית משנה את דפוסי הפגיעות של מדינות.
  - הזהות הדיגיטלית של המדינה משפיעה על האופן שבו היא מדמינת ומעריכה איומים.
- תאוריה זו אינה מבקשת להחליף את הגישות הקלאסיות לחקר ההפתעה האסטרטגית, אלא להרחיב אותן. בעוד שהספרות המסורתית הדגישה את הגורם האנושי (לרבות קוגניציה, פוליטיקה ודינמיקה ארגונית) התאוריה הדיגיטלית מוסיפה ממד נוסף: השפעתה של הסביבה הטכנולוגית עצמה על תהליכי קבלת ההחלטות ועל הסיכוי להפתעה.

## השלכות למדיניות ולפרקטיקה

בעוד שמאמר זה הוא בעיקרו קונספטואלי, למסגרת התאורטית יש השלכות מעשיות עבור דמוקרטיות מתקדמות דיגיטליות. אם עליונות דיגיטלית יוצרת צורות של פגיעות, על מדינות לפתח אסטרטגיות למיתון סיכונים אלה מבלי לוותר על היתרונות של החדשנות הטכנולוגית.

### איזון מחדש של איסוף מודיעין

מערכות דיגיטליות הטו את איסוף המודיעין במידה ניכרת לכיוון SIGINT ואמצעי חישה אחרים. הדבר מעלה שאלה מעניינת: האם ההפתעה של ה־7 באוקטובר עדיין הייתה מתרחשת אילו היו לישראל יכולות מעקב ומודיעין פחות מתוחכמות? עד כמה פחות מתוחכמות היו צריכות להיות היכולות הללו כדי שלא להיתפס לא מוכנים על ידי חמאס?

לנוכח היתרונות המוכחים של הטכנולוגיות הללו, הפתרון צריך להגיע מכיוון אחר. מסגרת הפגיעות הטכנו־דיגיטלית מציעה כי יש להדגיש מחדש HUMINT (מודיעין אנושי), תובנות אתנוגרפיות ופרשנות הקשרית. שיטות אזהרה מבוססות־אדם מתאימות לרוב יותר לזהות אסטרטגיות יריב אנלוגיות או מטעות שמערכות דיגיטליות מפספסות. מדיווחים ראשוניים, נראה שאגף המודיעין הצבאי (אמ"ן) כבר אימץ לקח זה. קצין בכיר באמ"ן ציין לאחרונה כי "בעבר אולי הייתה תחושה שהטכנולוגיה יכולה להחליף חלק מהאנשים העובדים עם שפה, 'חרבות ברזל' הוכיחה שבסופו של דבר אין תחליף לאדם-לאוזן, לאדם שיודע לקרוא ולפרש ביטויים שונים. זו ההנחיה שלנו לשנים הבאות: גיוס והעצמה של מומחי שפה".<sup>56</sup>

### בניית חוסן באמצעות יתירות

תלות דיגיטלית הופכת ארגוני מודיעין לשבריריים. על מדינות להשקיע ביתירות אנלוגיות, בארכיטקטורות נתונים מגוונות ובתהליכים אנליטיים מבוזרים. יתירות נתפסת לרוב כבלתי יעילה, אך בעולם שבו תשתיות דיגיטליות עלולות לקרוס לפתע, יתירות היא מקור לחוסן. זה כולל תכנון מערכות שיכולות להמשיך לפעול במצבים מוגבלים, הכשרת אנליסטים לפעול ללא נתונים דיגיטליים בזמן אמת, והבטחת יכולתם של ערוצי אזהרה קריטיים לשרוד תקיפות על צמתים דיגיטליים.

### התייחסות לפתיחות דיגיטלית כאל חשיפה אסטרטגית

דמוקרטיות חייבות להכיר בכך שהפתיחות שלהן בתחומי המידע יוצרת גם פגיעות אסטרטגית. על קובעי מדיניות לעודד אוריינות דיגיטלית לא רק כדי להתמודד עם דיסאינפורמציה, אלא גם כדי להעלות מודעות לאופן שבו יריבים יכולים לנצל נתונים ציבוריים.

הדבר עשוי לחייב הנחיות ציבוריות בנוגע להגבלות מיקום גיאוגרפי, משמעת תקשורת פוליטית-צבאית, וחשיפות של תשתיות קריטיות. בניגוד למדינות אוטוריטריות, דמוקרטיות אינן יכולות לסגור את המרחב הדיגיטלי שלהן, אך הן יכולות לטפח נורמות ציבוריות שמצמצמות חשיפה מיותרת.

## מיסודו של פלורליזם הערכתי

ארגוני מודיעין צריכים למסד תרגילי "צוות אדום" (red-teaming) שמאתגרים באופן מפורש הנחות דיגיטליות רווחות. יש לעודד חוקרי מודיעין לשקול כיצד יריבים עשויים לנצל מערכות דיגיטליות, להתחמק מגילוי דיגיטלי, או לחדש באמצעות שיטות בעלות רמת טכנולוגיה נמוכה. המטרה היא ליצור תרבויות ארגוניות שמתייחסות לנתונים דיגיטליים כאל מקור אחד מבין רבים, ולא כאל הפוסק הסופי של האמת. באופן דומה, דוקטרינה צבאית ומודיעינית חייבת לשקף את המציאות שבה עליונות דיגיטלית אינה שקולה לשליטה. על מדינות להניח שיריבים ינסו לפגוע בתשתיות דיגיטליות, להטעות מערכות אוטומטיות, ולנצל שקיפות דיגיטלית. יש לעדכן את הדוקטרינה בהתאם. האפשרות של לחימה בסביבות שבהן מערכות דיגיטליות נכשלות אינה צריכה עוד להיחשב יוצאת דופן; יש להניח אותה כמובנת מאליה.

## סיכום

עליונות דיגיטלית היא בסיס משמעותי של עוצמה מדינתית בעת הזאת. מדינות תלויות יותר ויותר בחיישנים, במערכות נתונים ובניתוח מבוסס בינה מלאכותית כדי להבין סביבות אסטרטגיות מורכבות ולפעול בהתאם, לרבות פעולות קינטיות. ההבטחה הגלומה בעוצמה דיגיטלית היא שיותר נתונים יביאו לראייה טובה יותר של המציאות ויאפשרו תגובה מהירה יותר. אולם כפי שנטען במאמר זה, עליונות דיגיטלית נושאת עימה גם פגיעויות עמוקות. הפגיעויות הטכנו-דיגיטלית מציעה מסגרת קונספטואלית להבנת סיכונים אלה. היא מראה כיצד תשתיות דיגיטליות יוצרות אשליות של שלמות מידעית, מייצרות תלות ארגונית השוחקת חוסן, חושפות חברות דמוקרטיות לניצול על ידי יריבים, ומעצבות נרטיבים תרבותיים שמעוותים את הערכת האיום. דינמיקות אלה מסייעות להסביר מדוע מדינות מתקדמות דיגיטליות נותרות פגיעות להפתעה אסטרטגית במאה ה-21. החוויה הישראלית של ה-7 באוקטובר 2023 היא רק דוגמה אחת לתופעה רחבה יותר, אך היא דוגמה מגלה. היא מראה כיצד עוצמה דיגיטלית יכולה להפוך למקור של עיוורון אסטרטגי. היא מדגישה את הצורך של ארגוני מודיעין לטפח ענווה פרשנית, גיוון מוסדי, וחוסן תפעולי.

באופן רחב יותר, מאמר זה טוען כי על מחקר יחסים בין לאומיים לשלב מערכות דיגיטליות בחקר ההפתעה האסטרטגית. גישות מסורתיות נותרות חיוניות, אך יש להשלים אותן בהעמקת הדיון באופן שבו הטכנולוגיה מעצבת תפיסה, ארגון ופגיעות. ללא שילוב כזה, התחום מסתכן באי-הבנה של טבעם של איום וביטחון בעידן הדיגיטלי.

ככל שמדינות ממשיכות להשקיע בארכיטקטורות דיגיטליות, לשלב בינה מלאכותית בתהליכי עבודה מודיעיניים ולהרחיב יכולות סייבר, הן ייתקלו לא רק בהזדמנויות חדשות אלא גם בסכנות חדשות. המשימה המרכזית עבור חוקרים ואנשי מקצוע היא להבין ולמתן את הפגיעויות הנובעות לא מנחיתות טכנולוגית, אלא מעליונות דיגיטלית עצמה.

המאמר המלא פורסם במקור:

**Eiran, E. (2026). Techno-digital vulnerability and intelligence failures. Social Sciences, 15(1), 37**

- אהרון קציר, בכור. המהפכה המדעית (תל-אביב: עם עובד, 1971)
- בן גוריון, דוד. "חזון ודרך". בתוך: בקר, יעקב. משנתו של דוד בן גוריון (תל-אביב: יבנה, 1958)
- סימנטוב, דוד ועופר גוטרמן (עורכים). המודיעין והשבעה באוקטובר (מערכות והמרכז למורשת המודיעין, 2025)
- עמידור, יעקב. הרהורים על צבא ובטחון: מאמרים, מכתבים והרצאות (עיצוב, 2002)
- Allen, Gregory C. 2017. Putin and Musk Are Right :Whoever Masters AI Will Run the World. Center for a New American Security
- Arnon, Ruth, Michael Sela, and Colin Shindler. Ephraim Katchalski-Katzir) Royal Society(2016 ,
- Bar-Joseph, Uri, and Rose McDermott. Intelligence Success and Failure :The Human Factor) Oxford University Press(2017 ,
- Betts, Richard K". Analysis, War, and Decision :Why Intelligence Failures Are Inevitable ". World Politics 61-89 : (1978) 31
- Betts, Richard K. Enemies of Intelligence :Knowledge and Power in American National Security) Columbia University Press(2007 ,
- Breznitz, Dan. Innovation and the State :Political Choice and Strategies for Growth in Israel, Taiwan, and Ireland) Yale University Press(2007 ,
- Bryant, Steven L". The Dangers of an Over-Reliance on Technology ". Master's thesis. Joint Forces Staff College(2011)
- Cohen, Erez". The Development of the High-Tech Industry in Israel, and Government Policy to Support it ". In Erez Cohen and Azi Lev-on) Eds (.Connected :Politics, Technology and Society in Israel) Israeli Association of Political Science(2011 ,
- Edgerton, David E.H". The Contradictions of Techno-Nationalism and Techno-Globalism :A Historical Perspective ", New Global Studies : (2007) 1:1 Article 1
- Eiran, Ehud". Techno-Digital Vulnerability and Intelligence Failures ". Social Sciences , 15 no(2026) 1 .
- Eiran, Ehud, Ofer Guterman, and David Siman-Tov". The vanishing watchman :The rise and decline of early warning ". Intelligence and National Security 863-85 : (2025) 40
- Eppler, Martin J., and Jeanne Mengis". The Concept of Information Overload :A Review of Literature from Organization Science, Accounting, Marketing, MIS, and Related Disciplines ". The Information Society 325-344 : (2004) 20
- Farrell, Henry, and Abraham Newman". Weaponized Interdependence :How Global Economic Networks Shape State Coercion ". International Security 42-79 : (2019) 44
- Finkel, Meir". The Cult of Technology in the IDF :The IDF's Cult of Technology :Restoring Balance to Ground Force Development ". Maarchot(2006) 407
- Flamer, Netanel. The Hamas Intelligence War Against Israel) Cambridge University Press(2024 ,
- Freilich, Charles. Israeli National Security :A New Strategy for an Era of Change) Cornell University Press(2018 ,
- Gartzke, Erik". The Myth of Cyberwar ". International Security 41-73 : (2013) 38
- Herzl, Theodor. Old New Country) Zionist Organization(1902 ,
- Heuer, Richards J. Psychology of Intelligence Analysis) CIA Press(1999 ,
- Heuer, Richards J. and Randolph H. Pherson. Structured Analytic Techniques for Intelligence Analysis, 2nd ed) .CQ Press(2015 ,
- Jervis, Robert. Why Intelligence Fails :Lessons from the Iranian Revolution and the Iraq War) Cornell

- University Press(2010 ,
- Jervis ,Robert .Perception and Misperception in International Politics) .Princeton University Press, (1976
- Katz ,Brian .The Collection Edge :Harnessing Emerging Technologies for Intelligence Collection .CSIS Brief(2020)
- Keohane ,Robert ,and Joseph Nye .Power and Interdependence4 ,th ed) Longman(2012 ,
- Lindsay ,Jon" .Stuxnet and the Limits of Cyber Warfare ",Security Studies365-404 :(2013) 22
- Mearsheimer ,John .The Tragedy of Great Power Politics) Norton(2001 ,
- Morgenthau ,Hans .Politics Among Nations :The Struggle for Power and Peace4 ,th ed) Alfred A .Knopf, .(1967First published in1948
- Parasuraman ,Raja ,and Dietrich M .Manzey" .Complacency and Bias in Human Use of Automation :An Attentional Integration ".Human Factors :The Journal of the Human Factors and Ergonomics Society52 381-410 :(2010)
- Peña ,Carlos" .It's Easy to Get Lost :The Temptation of Overreliance on Technology ".Warroom) Decem-ber(2024 ,5
- Penslar ,Derek .Zionism and Technocracy :The Engineering of Jewish Settlement in Palestine1870- , ) 1918Indiana University Press(1991 ,
- Perrow ,Charles .Normal Accidents :Living with High-Risk Technologies) Basic Books(1984 ,
- Posen ,Barry" .Command of the Commons ".International Security5-46 :(2003) 28
- Reinharz ,Jehuda ,and Motti Golani .Chaim Weizmann :A Biography) Brandeis University Press(2024 ,
- Schwab ,Klaus .The Fourth Industrial Revolution) Crown Business(2016 ,
- Senor ,Dan ,and Saul Singer .Start-Up Nation :The Story of Israel's Economic Miracle) Council on For-eign Relations(2009 ,
- Serena ,Chad C .,and Colin P .Clarke" .America's National Defense Strategy and the Paradox of Technol-ogy ",RAND Corporation Commentary(2019)
- Shapira ,Itai .Israeli Defense and Intelligence before and After October :2023 The Cultural Roots of Stra-tegic Surprise and Resilience) Routledge(2026 ,
- Slayton ,Rebecca .Arguments That Count :Physics ,Computing ,and Missile Defense) 1949-2012 ,MIT Press(2017 ,
- Technion UK2024 .b .Israel's Technion Ranked 1# Worldwide in Digital Education .<https://technionuk.org/news-post/israels-technion-ranked-1-worldwide-in-digital-education/>
- U.S .Government Accountability Office GAO .DOD Just Beginning to Grapple with Scale of Vulnerabili-ties) GAO(2018 ,
- Winkler ,Stephanie Christine" .New and Old Cold Wars :The Tech War and the Role of Technology in Great Power Politics ".Global Studies Quarterly :(2025) 5 ksaf038
- Zegart ,Amy .Spies ,Lies ,and Algorithms :The History and Future of American Intelligence) Princeton University Press(2022 ,