כיצד הדיגיטל משנה את טבע החשאיות

שרון טל[1]

מבוא

פעילות חשאית, בדומה למלחמה או לדיפלומטיה, היא כלי שמדינות משתמשות בו כדי להשיג את יעדיהן. עוד מראשיתה היא הושפעה מהטכנולוגיה, אך לא בצורה אחידה ולא בכיוון אחד. הטכנולוגיה עיצבה את הכלים, שינתה את הזירה והגדירה מחדש את גבולות האפשר, אך נותר בעינו המתח הבסיסי בין המבקשים להסתיר למבקשים לחשוף. המעבר לעידן הדיגיטלי שינה מהותית את האיזון במתח זה: פיקוח נרחב (UTS – Ubiquitous Technical Surveillance), ריבוי שחקנים בזירה החשאית, כלי AI – כל אלה מצמצמים את מרחב ההסתרה אשר משרת את הפועלים בחשאי. חשיפות דוגמת הסיכול של מחמוד אלמבחוח בדובאי ב־2010, הדלפות המידע הסודי של אדוארד סנודן ב־2013 ולכידת מרגלים של ה־CIA בסין בין 2010 ל־2012 מדגימות את היכולת להשתמש בדיגיטל כאמצעי לשיבוש פעילות חשאית. אלא שהטכנולוגיה גם מאפשרת לבצע פעולות "ללא ייחוס", מגבירה את שיתוף הפעולה בין מדינות למגזר הפרטי ויוצרת כלים חדשים המרחיבים את גבולות הזירה החשאית.

מאמר זה מנסה לבחון כיצד הדיגיטל מעצב מחדש את טבעה של החשאיות, ומהי חשאיות בעולם שכל פעולה בו מותירה עקבות אשר אפשר לנתח. מהמטרה הזו נגזרות כמה שאלות: כיצד השתנו תנאי הפעולה החשאית במרחב הציבורי, ובאיזו מידה אפשר להסתיר זהות בעולם שאפשר לנתח בו כל "חתימה" גם בדיעבד? אילו דפוסי פעולה חשאית מתאפשרים בזירת הסייבר, ובמה הם נבדלים מדפוסי הפעולה בזירות האחרות? אילו שינויים חלו ביכולת ההכחשה, בהינתן שהייחוס עצמו זמין יותר? כיצד משתנים יחסי הכוחות והגבולות בין שחקנים מדינתיים לשחקנים תת־מדינתיים בזירה החשאית? האם ההמשגה הקיימת של חשאיות עדיין תקפה, ואם לא – כיצד יש להמשיגה מחדש? טענת המאמר היא שבעידן הטכנולוגי הנוכחי חשאיות כבר אינה מצב בינארי (הסתרה או חשיפה), ובמקום זאת יש ניהול מתמשך של פערי ידיעה. המאמר מתמקד בפעולות מדינתיות, אבל עוסק גם בגורמים תת־מדינתיים אשר פעילים במרחב החשאי. הוא נשען על מקורות גלויים העוסקים בעולם החשאי ועל ראיונות עם אנשי קהילת המודיעין לשעבר.

חשוב להבהיר כי על אף ההתמקדות בטכנולוגיה הגורם הקובע אינו הטכנולוגיה כשלעצמה, אלא הדרך שמדינות וגורמי ממסד בוחרים להפעיל ולהסדיר אותה (או להימנע מלעשות זאת). הטכנולוגיה לא פועלת בריק; החלטות מדיניות, כמו גם מסגרות משפטיות ובין־לאומיות, משפיעות עליה ומעצבות אותה. כך למשל בדיקות ביומטריות בגבולות היו קיימות שנים לפני שהן נפרשו בהיקף נרחב לאחר אירועי 11 בספטמבר; שוק כלי המעקב המסחרי (תוכנות דוגמת פגסוס) התפתח להיקפו הנוכחי בשל היעדר רגולציה בין־לאומית, ולא רק בגלל התקדמות טכנולוגית; בד בבד החלטות האיחוד האירופי, כמו גם פסיקות בנושא הפרטיות בכמה מדינות, מצמצמות את זמינות הנתונים ומגבילות את יכולת המעקב. מאמר זה מתמקד בפוטנציאל אשר הטכנולוגיה יוצרת, אך מכיר בכך שמימושו של פוטנציאל זה תלוי במשתנים שאינם טכנולוגיים.

המרחב החשאי: מושגים ושחקנים

בפעולה חשאית הגורם המבצע מנסה להסתיר את זהותו, את מעשיו, או את שניהם, כדי להשפיע על תפיסות, אירועים ותהליכים באמצעים שאין להם "ייחוס רשמי". נהוג להבחין בין שתי קטגוריות:

פעולה חשאית (clandestine). זו מתבצעת תוך כדי ניסיון להסתיר את הגורם המבצע, את המעשה עצמו, ולעיתים את שניהם. דוגמה לכך היא גיוסו של סוכן חשאי במדינה זרה;

פעולה חסויה (covert). הגורם המבצע נותר חסוי, או מתאפשרת יכולת סבירה להכחיש את זהותו (plausible deniability), אך הפעולה עצמה יכולה להיות גלויה לגורם המותקף. דוגמאות לפעולה כזו הן מבצעי תודעה והשפעה, פעילות חשאית כלכלית

---

1 לשעבר איש שב"כ, ביום חוקר במכון הרכבי לחקר המודיעין

ומבצעים של כוח פארא־צבאי.[2]

למרות ההבדל בין שתי הקטגוריות הגבול ביניהן מטושטש למדי: פעולות רבות כוללות את שני המאפיינים (הן חשאיות וחסויות), ולעיתים קשה לסווג אותן חד־משמעית לאחת משתי הקטגוריות.[3] הבחנה נוספת היא בסוגיה "מי יודע על הפעולה": פעולה מסוימת יכולה להיות גלויה לירי, סמויה עבור הציבור המקומי, ומוכחשת רשמית לכל הקהלים. מדינות משתמשות בפיצול הזה – הן מתכננות פעולות שיהיו גלויות לקהל ייעודי ועמומות לקהלים אחרים.[4]

החשאיות היא אפוא לא רק מאפיין של הפעולה עצמה, אלא גם פונקציה של קהל היעד: מה שחשאי לציבור הרחב עשוי להיות גלוי לחלוטין לשירות המודיעין שמנגד. לפיכך התווך החשאי משתנה ממרחב של הסתרה למרחב של תקשורת מכוונת בין כמה גורמים. בתווך הזה פעילים גורמים מדינתיים ותת־מדינתיים:

טבלה 1: שחקנים במרחב החשאי

גורם	גופים	מניע	סוגי פעולות
מדינתי	משטרה, גופי ביטחון פנים, גופי ביון, כוחות מיוחדים	אינטרסים של ביטחון לאומי	איסוף מודיעין, ריגול, סיכול, חבלה ומבצעים פארא־צבאיים
היברידי	צבאות פרטיים, ארגוני גרילה	כספי, אידאולוגי	
לא מדינתי	ארגוני פשע	כלכלי	פשיעה, פעולות טרור וחתרנות, מימון, גיוס ואינדוקטרינציה
	ארגוני טרור	אסטרטגי, אידאולוגי	

בזירה זו יש תחרות – בדרך כלל "מתחת לרדאר" – בין גורמי פשיעה לגורמי אכיפה, בין צבאות וסוכנויות ביון לגופי ביטחון פנים. ההסתרה גורמת לכך ששיטות הפעולה חופפות, והגבולות בין הגופים מיטשטשים: מדינות נוקטות דפוסים של גורמי טרור, ארגוני פשיעה מאמצים דרכי פעולה של גופי אכיפה, וסוכנויות ביון פועלות בשיטות של ארגוני פשיעה. התחרות הזו הייתה תמיד, אך דומה שהיא הואצה בעשורים האחרונים. ככל שהטכנולוגיה התקדמה, הפעילות החשאית נעשתה מתוחכמת יותר; פיתוח אמצעי מסוים גורם לפיתוח של אמצעי נגד וכן הלאה (פעולה ותגובה), והספירלה הזו מעלה את רמת המשחק החשאי כולו.

עד לעידן הדיגיטלי הפעילות החשאית התבצעה בעיקר במרחב הגאוגרפי הציבורי – ערים, גבולות ומעברי גבול היו זירות הפעולה העיקריות שלה. הטכנולוגיה שינתה זאת: היא אפשרה להקים דיסציפלינות חדשות מבוססות דיגיטל, כמו למשל סייבר ופיקוח מבוסס חיישנים (UTS); שיפרה מאוד את יכולות האיסוף; ובד בבד שינתה ללא הכר את פני החשאיות במרחב הציבורי.[5] כיום הפעילות החשאית מתנהלת במקביל בתווך הרשתי ובתווך הציבורי; השניים שלובים זה בזה ומשלימים זה את זה. פעולה מסוימת עשויה אפוא להתקיים בכמה ממדים במקביל – כל צד פועל בכל ממד כמגן על נכסיו וכתוקף את נכסי הצד שמנגד.

נדרשת הבחנה בין שני מושגים מרכזיים אשר מוצגים במאמר: עידן הדיגיטל ועידן הרשת. עידן הדיגיטל הוא שלב המעבר של נתונים לפורמט דיגיטלי: מאגרי מידע ממוחשבים, תיעוד בירוקרטי אלקטרוני, רשומות גבולות וכן הלאה. בשלב הזה הנתונים

2 Dennis Broeders, "Addressing the elephant in the room - Cyber intelligence and international security", Inaugural lecture at Leiden University (31 March, 2023); Carson, A., & Yarhi-Milo, K. (2017). Covert communication: The intelligibility and credibility of signaling in secret. Security Studies, 26(1), 124-156

3 בשל טשטוש הגבולות בין הקטגוריות לא תהיה הבחנה ביניהן בהמשך המאמר

4 Cormac, R., & Aldrich, R. J. (2018). Grey is the new black: Covert action and implausible deniability. International Affairs, 94(3), 477-494

5 מתנהל ברשת דיון ער בחולשות הדיסציפלינה היומינטית, בין השאר בשל עליית הדיגיטל. אלא שאחד הלקחים הבולטים של 7 באוקטובר הוא חשיבות היומינט ככלי לבירור כוונות האויב – ראו למשל אצל Egger, M. (2023, January 13). The relevance of HUMINT in the digital era. Lobo Institute

קיימים ונשמרים, אך כל מקור פועל כמערכת סגורה ועצמאית. עידן הרשת הוא שלב מאוחר יותר המתאפיין בחיבורים בין מקורות אלו – חיבור בין מכשירי קצה, חיבור בין מאגרים, חיבור בין שכבות ניטור. ההבחנה בין שני העידנים אינה טכנית בלבד: הדיגיטל יצר את חומר הגלם, אך הקישוריות והרשתיות עשו אותו לאִיום ממשי על הזירה החשאית (בשל היכולת להרכיב תמונה שלמה ממגוון של מקורות).

הזירה החשאית הקלסית (עד לשנות ה־90 של המאה ה־20)

הטכנולוגיה אינה גורם חדש בזירה החשאית. לווייני ריגול, יירוט ופענוח של תשדורות ועיבוד ממוחשב של מידע מילאו תפקיד מרכזי בעימותים של המאה ה־20. אולם האיום שנשקף מיכולות אלה לפעילות החשאית היה ממוקד: הוא הופנה אל הפעילות הצבאית־מדינתית ואל ערוצי התקשורת של הגורם החשאי, ולא אליו עצמו. פרשת אלי כהן ממחישה הבחנה זו. כהן נתפס ב־1965 לאחר שמשדרו אותר באמצעי איכון, בעוד שזהותו הבדויה עמדה במבחן במשך שנים. הזירה המבצעית, לעומת זאת, הייתה אנושית במהותה. הפעיל החשאי וגורמי הביון הנגדי פעלו להסתיר את עצמם זה מזה, ופעולות הזיהוי, המעקב והחקירה נשענו על יכולות אנושיות של תצפית ושל איסוף. גורמי הביון הנגדי חתרו לאתר חריגות בדפוסי התנהגות או ברשתות קשרים, ושילבו לשם כך אמצעים אנושיים, כגון מעקב ותשאול, עם מקורות סיגינטיים. הגורם החשאי, מצדו, נשען על יכולתו להיטמע בסביבת הפעולה ולהתאים אליה את פעילותו בלי לעורר חשד.

ניתן להצביע על שלושה תנאים מבניים שאפשרו את קיומה של החשאיות בזירה זו. התנאי הראשון הוא עלותו של הפיקוח. מעקב אחר אדם אחד חייב הקצאה של תשומות רבות של עיקוב, פיקוח טכני וכוח אדם, ולכן היה סלקטיבי, מותנה בזיהוי מוקדם של מושא החשד. כל עוד הפעיל לא עורר חשד, לא הייתה הצדקה להפנות אליו קשב ומשאבים. התנאי השני הוא אופייה האנלוגי והמפוצל של הסביבה. רשומות אזרחיות ונתונים על תנועה ועל פעילות פיננסית נשמרו על גבי נייר, במוסדות נפרדים ובמדינות נפרדות, והצלבתם הייתה איטית, יקרה ולעיתים בלתי אפשרית. התנאי השלישי הוא ארעיות החתימה. העקבות שהותירה הפעילות החשאית, היו מועדים לדעיכה: עקבות פיזיים נעלמו, זיכרונם של עדים התעמעם ורשומות אבדו או נותרו בלתי נגישות. משום כך חייבה החשיפה סנכרון בין הפעולה לבין גילויה, ופעילות שלא התגלתה בזמן אמת או בסמוך לו נותרה לרוב חסויה.[6]

תנאים אלה מסבירים מדוע ניתן היה לבסס תשתית חשאית, על אף שהדבר חייב מומחיות והשקעה ניכרת של זמן ומשאבים. סיפור כיסוי, דרכון מזויף, ביוגרפיה בדויה וקשרים תומכים נדרשו לעמוד בבדיקה נקודתית ומקומית בלבד, ולפיכך ברוב המקרים הספיקו סיפור כיסוי סביר וניירת תקינה. נקודת התורפה של הפעילות החשאית בעידן זה נבעה מאותו מקור שהעניק לה את כוחה: התלות בגורם האנושי. טעות מבצעית, עד מקרי או סוכן כפול עלולים היו לפרום את הכיסוי, כפי שאירע בפרשת לילהאמר (1973), שבה נחשף צוות מוסד לאחר שעדה מסרה למשטרה את מספר הרכב ששימש אותו. עם זאת, השלכות הרוחב של החשיפה היו מוגבלות בדרך כלל: המידור והיעדר הקישוריות בין מאגרי המידע מנעו מחשיפתו של פעיל יחיד להתגלגל לחשיפת הרשת כולה. מכלול זה, מהווה את קו הבסיס שממנו ייבחנו התמורות בפרקים הבאים.[7]

בשנות ה־90 של המאה ה־20 העידן הדיגיטלי והאינטרנט חדלו להיות מיזם אקדמי ומדינתי, והגלישה ברשת הייתה לתופעה גלובלית ונגישה לציבור הרחב. באותן השנים גם התרחב השימוש בטלפון הסלולרי, והוא היה למוצר נפוץ בכל בית. הנגישות לרשת ולתקשורת הגבירה את יכולת הפיקוח המדינתית על הפרט, מיקומו והתקשורת שלו, והרחיבה את היכולת לחשוף פעילות שהוא ניסה להסתיר. שתי פרשות ממחישות שני היבטים משלימים של התמורה הטכנולוגית באותן השנים. סיכול "המהנדס" יחיא עיאש בינואר 1996 הדגים את הפוטנציאל המבצעי הטקטי הגלום בתשתית הסלולרית, ובעקבותיו באה שורת סיכולים אשר התבססו על שימוש בטכנולוגיה; חשיפת רשת אשלון (Echelon)[8] הדגימה את ההיקף התעשייתי־מערכתי הרחב של השימוש באותה הטכנולוגיה למטרות של פיקוח חשאי – תשתית גלובלית שימשה בשיטתיות ל"יירוט" תקשורת אזרחית בקנה מידה המוני.[9]

---

6 Mayer-Schönberger, V. (2009). *Delete: The Virtue of Forgetting in the Digital Age*. Princeton University Press.

7 Bernath, E. (2019). To what extent have the developments of current information and communications technology (ICTs) affected espionage tradecraft used while conducting covert operations? [Master's thesis, Brunel University], pp. 34-35

8 אחת מפרשת הריגול האלקטרוני הגדולות בהיסטוריה. אשלון פעלה באמצעות ברית "חמש העיניים": ארצות הברית, הממלכה המאוחדת, קנדה, אוסטרליה וניו זילנד. סימנים ראשונים לקיומה של הרשת התקבלו במהלך שנות ה־90 של המאה ה־20, וב־2001 פורסם דוח של הפרלמנט האירופי אשר חשף פומבית ורשמית את קיומה

9 Campbell, D. (April 1999). Interception capabilities 2000. European Parliament; Gardham, D., & Kifner, J. (1996, January 6). Hamas bomb engineer slain by booby-trapped cellular phone. The New York Times

עידן הרשת

העשור הראשון של שנות האלפיים התאפיין במעבר לאינטרנט מהיר (דור 2.0), בהקמת רשתות חברתיות (מ־2004 ואילך) ובתפוצה נרחבת של הטלפון החכם (מ־2007 ואילך). טכנולוגיות אלו הצריכו שינוי בפעילות החשאית משני טעמים. הטעם הראשון היה הנגישות העצומה שהתאפשרה לגורמי המודיעין: איסוף ממקורות גלויים (רשתות חברתיות, פורומים, מסדי נתונים), ובד בבד יכולת לפרוץ לשרתים, למכשירי קצה ולמאגרי מידע. אלא שקפיצת המדרגה האמיתית נבעה מהטעם השני: הקישוריות. לא זו בלבד ששכבות הניטור הצטברו, אלא שכולן היו מחוברות ביניהן ואפשרו ליצור תמונה שלמה המורכבת ממגוון של מקורות. הודות לכך התאפשר לגורם האכיפה לשלב בין שורה של שכבות פיקוח למאגרי מידע ארכיוני, והתמונה שהתקבלה הייתה שלמה הרבה יותר מזו אשר הייתה בידיו בעבר.

להתפתחות זו נוספו עוד שתי "שכבות". הראשונה שבהן, דיגיטציה בתחום השירותים הבירוקרטיים (גבולות, בתי מלון, שירותים ממשלתיים), יצרה מאגרי מידע. אלו חייבו את הגורם החשאי להבטיח שזהותו לא תיחשף גם בבדיקה של מאגר מידע. השכבה השנייה, פריסה רחבה של מצלמות במעגל סגור (CCTV) במרחב הציבורי, צמצמה עוד יותר את היכולת לקיים פעילות שאינה מתועדת ויזואלית. האתגר הכפול הצריך הסתגלות לשכבת הניטור הוויזואלי: הגורם החשאי נדרש לגלות עקביות לא רק בזהות הבירוקרטית שלו, אלא גם בדפוס התנועה המתועד. מסלול שאינו עקבי, נוכחות חוזרת בנקודת עניין, שינוי פיזי בולט – כל אלו היו עלולים לעורר חשד.

הביטוי הבולט לשינוי זה היה שורת חשיפות; כולן התרחשו בתוך שנים ספורות והביאו לידי ביטוי את שחיקתו של מרחב ההסתרה. פרשת סיכולו של אלמבחוח ב־2010 הייתה אחת הפעמים הראשונות שנחשפה פעילות חשאית בהתבסס על ניתוח של נתוני הסביבה הדיגיטלית – מצלמות אבטחה, רישומי כניסה ויציאה, דרכונים, עקבות השימוש בכרטיסי אשראי; קריסת רשתות ה־CIA באיראן ובסין בשנים 2010–2012 חשפה בעייתיות ברובד אחר: תשתית התקשורת החשאית נפרצה, והדבר גרם לנפילה רוחבית ולחשיפת עשרות סוכנים; בשנים 2014–2015 המודיעין הסיני זיהה אנשי מודיעין אמריקנים בהתבסס על הצלבת מאגרי מידע אזרחיים (OPM, Anthem ו־Marriott), כמו למשל טופסי סיווג ביטחוני, ביטוחי בריאות ורישומי לינה במלונות.[10] הצלבת המאגרים אפשרה לסינים להכין פרופיל מודיעיני מקיף ושיבשה את היכולת של ארצות הברית להסוות את אנשי השטח והמודיעין שלה.

עידן הניטור הרחב

UTS הוא מונח רשמי שטבע הממשל האמריקני כדי לתאר רשת חיישנים אשר אוספת נתונים ללא הפסקה, ובאמצעות שיטות אנליטיות מתקדמות מאפשרת לחבר בין אנשים להתרחשויות ולמיקומים.[11] המונח מתאר מיזם שנבנה במשך כשני עשורים. הוא החל לאחר המתקפה ב־11 בספטמבר 2001, מתקפה שתוצאותיה הניעו גל של השקעות בתשתיות ניטור במדינות המערב. לאחר הפיגועים בלונדון ב־2005 הרחיבה בריטניה את רשת החיישנים והייתה לאחת המדינות המצולמות ביותר בעולם. באותן השנים השיקה סין את SkyNet, תוכנית שביקשה לכסות את כלל המרחב הציבורי בכלי ניטור ממוחשב.[12] קפיצת המדרגה ברשת זו התבססה על מהפכת הקישוריות: נתונים מטלפונים חכמים, מרשתות חברתיות, ממאגרים פיננסיים וממצלמות ציבוריות החלו לזרום לתשתיות אנליטיות משותפות. פרשת סנודן ב־2013 חשפה את ממדי התופעה: תוכנית המעקב של הסוכנות לביטחון לאומי בארצות הברית (NSA) הצליבה מקורות ממגוון ספקי אינטרנט, ותוכנת התחקור שלה אפשרה להעריך בזמן אמת את תעבורת האינטרנט הגלובלית.[13] בדרך זו התקבל כלי תחקור רב־עוצמה המבוסס על ניתוח של דפוסי חיים (pattern-of-life analysis). כך למשל אדם שנוסע בתדירות מסוימת, מתקשר בדפוס ספציפי ורוכש בשעות מסוימות אינו מעורר חשד בכל מאגר בנפרד, אך עלול להיות חשוד בהתבסס על הפרופיל שהאלגוריתם בנה.[14] קפיצת המדרגה הבאה התאפשרה לאחר פיתוח משטח אנליטי המבוסס על בינה מלאכותית: ב־2015 השיקה סין את Sharp Eyes, תוכנית המשך ל־SkyNet אשר מטרתה לכסות את המרחב

---

10 Bisson, D. (2015, June 29). The OPM breach: Timeline of a hack. Tripwire; Kovacs, E. (2018, December 6). Chinese government suspected in Marriott hack: Report. Security Week

11 Sherman, J. (2025, July 25). Ubiquitous technical surveillance demands broader data protections. Lawfare

12 הסינים והרוסים מתקדמים בתחום זה, והערים הסיניות נחשבות למפוקחות ביותר בעולם – הן במספרים מוחלטים של מצלמות, הן בעוצמת המעקב הטכנולוגי. אולם גם ערים מערביות דוגמת וושינגטון מנוטרות באופן נרחב, ונעשה בהן שימוש במערכות פיקוח מתקדמות (Bernath, 2019 , pp. 21-22)

13 Greenwald, G., Marquis-Boire, M., & Lee, M. (2015, July 1). XKEYSCORE: NSA's Google for the world's private communications. The Intercept

14 Gioe, D. V., & Manganello, T. (2025). Smart new world: Adapting human intelligence for the digital age. Intelligence and National Security 40(6), 1114-1128

הציבורי במצלמות המשלבות זיהוי פנים המבוסס על AI.[15] הבינה המלאכותית שדרגה את יכולת הניטור בשני מובנים: ראשית, היא הגבירה מאוד את מהירות העיבוד בשלוש השכבות – אגירה, רישות ותחקור. הארכיטקטורה הרשתית היא התנאי המאפשר, והבינה המלאכותית אפשרה לממש את הפוטנציאל של הרשת; שנית, היא אפשרה ליצור קטגוריה חדשה של תחקור נתונים שאינו אלפא נומרי (קול, תמונה וביומטריה). את הנתונים סיפקו המצלמות והחיישנים, אך לרובם לא התאפשר ניתוח אוטומטי. תוצר ישיר של מהפכת ה־AI הוא האפשרות לערוך זיהוי פנים אוטומטי, לנתח הליכה, לשלב בין נתונים ביומטריים מכמה מקורות ולנתח דפוסי תנועה במרחב.[16] היכולות האלה מעניקות לגופי אכיפה כלים חזקים המאפשרים לנטר ולפקח, כמו גם לזהות חשודים בפעילויות טרור וריגול. הוא גם מאפשר לגורמי מודיעין צבאי לזהות סימנים לפעילות צבאית התקפית. עבור הגורם שמבקש להישאר חשאי, המשמעות מרחיקת לכת: אין עוד הבחנה בין "להיראות" ל"להיות מזוהה". כל תנועה במרחב הציבורי נושאת חתימה פוטנציאלית, וגם בדיעבד אפשר לתחקר אותה.

טבלה 2: התפתחות אתגר הדיגיטל לפעילות החשאית

תקופה	מעצב דיגיטלי	הגורם המאתגר	השפעה על החשאיות	אירועים מכוננים
עד שנות ה־90	מחשבים מרכזיים	פיקוח אנושי וסיגינטי	השפעה מינורית	ריגול במלחמה הקרה, חשיפתו של אלי כהן
משנות ה־90 עד 2005	קישוריות רשתית (אינטרנט), סלולאר אישי	+ פיקוח סלולארי ורשתי	הרחבת יכולת הפיקוח המדינתית על הפרט	סיכול יחיא עיאש (1996), פרשת אשלון (1998–2001)
2005–2015	מחשוב אישי ורשתיות (סמארטפון, רשתות חברתיות)	+ פיקוח ויזואלי + סייבר	שחיקת החשאיות המסורתית, צמצום המונופול המדינתי, גיוון כלים ושיטות (סייבר)	פרשות מבחוח (2010) וסנודן (2013), סייבר מדינתי באסטוניה (2007) ואיראן (2010)
2015 - 2022	מחשוב אישי נרחב, רשתיות ואחסון זול (חיישנים, לבישים)	+ נתוני עתק + אוסינט	צמצום האנונימיות במרחב הציבורי, היכולת להתחזות, מתיחת משך הפעולה החשאית	פרשת סקריפל (2018), איסוף המודיעין של חמאס לקראת 7 באוקטובר
2022 והלאה	עידן הבינה המלאכותית	+ בינה מלאכותית	פירוק שיטתי של החשאיות ויכולת ההכחשה הסבירה, העצמת יכולות סייבר וזיוף עמוק (Deep Fake)	קמפיין ריגול סיני ראשון מנוהל AI (2025), כלי AI בשימוש מפעל המטרות של צה"ל

הסייבר כזירה חשאית

בהקשר של ההמשגה במאמר זה סייבר הוא סביבה דיגיטלית הכוללת רשתות מחשבים, מערכות תקשורת, מאגרי מידע ומכשירי קצה. זו זירה חשאית בפני עצמה, וגורמים מגוונים פועלים בה כדי להשיג מגוון מטרות - איסוף מידע, השפעה, או פגיעה ושיבוש. תנאי היסוד של הזירה הם אלה אשר עושים אותה מתאימה לפעילות חשאית; היעדר גבולות גאוגרפיים, ריבונות ברורה וכללי

15 NetAskari (2026, May 25). Sharp Eyes: Mass surveillance of foreigners in China – Part 2. https://netaskari.substack.com/p/sharp-eyes-mass-surveillance-of-foreigners

16 Ilia Antenucci, "Smart cities, smart borders. Sensing networks and security in the urban space," Nina Klimburg-Witjes (ed.) "Sensing In/Security: Sensors as Transnational Security Infrastructures", Mattering Press (January 2021), pp 76-100.

לחימה מוסכמים מוביל לכך שפעולות השחקנים מתאפיינות בעמימות ובהכחשה.[17]

הפעולה החשאית השתלבה בסייבר בהדרגה ושינתה את מפת השחקנים הפועלים בו. בשנות ה־90 פעלו בזירה זו בעיקר פצחנים (האקרים); אחריהם הצטרפו רשתות פשע מאורגן, ואלה בנו תשתיות להונאה פיננסית ולסחיטה דיגיטלית; מדינות נכנסו לתווך הזה בשלב מאוחר יותר – תחילה לצורכי ריגול, ובהמשך כדי לפגוע בתשתיות.[18] עם הזמן היה הסייבר למערכת מורכבת ומשולבת: הגבולות בין השחקנים הפעילים בו היטשטשו, והדבר הִקשה על ייחוס פעולה מסוימת לשחקן מסוים ואִפשר למדינות יכולת הכחשה סבירה. הפעולות בזירת הסייבר נחלקות לשלוש קטגוריות עיקריות. הקטגוריות האלה נבדלות באפשרויות לחשאיות ולייחוס:

איסוף מודיעין. חדירה למערכות מידע של יעד כדי לאסוף נתונים, ליירט תקשורת ולשתול אמצעי מעקב. הסייבר מאפשר להגיע מרחוק למידע אינטימי – בהיקפים חסרי תקדים, ובלי לסכן את חייהם של סוכנים. האיסוף בממד הזה יכול להיות פסיבי או אקטיבי; הוא יכול להתמקד בהגברת הביטחון הלאומי, בריגול תעשייתי וכלכלי, או בפעילות פלילית.

חבלה ושיבוש. מימוש הפוטנציאל ההרסני של הסייבר. המטרה היא לפגוע בתפקוד של מדינת היעד באמצעות שיבוש מערכות, חבלה בתשתיות חיוניות וגרימת נזק ממשי, וזאת ללא נוכחות אנושית בשטח וללא חשיפה של הגורם המבצע.[19] לקטגוריה הזו יכול להיות ממד צבאי מובהק – פגיעה ביכולת התפקוד של צבא האויב באמצעות שיבוש התקשורת שלו, או שיבוש פעולתן של המערכות הממוחשבות שלו. הפוטנציאל הזה הוביל את הקברניטים בארצות הברית להגדיר את המרחב הקיברנטי כמרחב לחימה עצמאי (בדומה לזרועות היבשה, האוויר, הים והחלל), ובהתאם לכך הצבא האמריקני נדרש לפעול בו לשמירת הביטחון הלאומי (בדומה לנדרש במרחבי הלחימה האחרים).[20]

השפעה וערעור. עריכת מניפולציות על כלי תקשורת ורשתות חברתיות מאפשרת לעצב את המציאות שהיעד פועל בה, וזאת באמצעות השפעה על תפיסות, על אמונות ועל קבלת החלטות. קטגוריה זו שונה מבנית משתי קודמותיה: איסוף וחבלה מצריכים הסתרה מלאה של הפעולה ושל המְבצע גם יחד; לעומת זאת פעולות ההשפעה אמורות מעצם טבען להגיע לידיעת הציבור, שכן התוכן חייב להיחשף כדי לאפשר פעולה. בקטגוריה זו אין הסתרה של הפעולה, אלא רק של הייחוס. בקצה האחד של "קשת ההסתרה" נמצאת תעמולה מדינתית גלויה, כזו שאינה מסתירה את מקורה; בקצה האחר נמצאות פעולות חשאיות ממש, כמו למשל שימוש בפרופילים מזויפים ו"זיוף עמוק" (deepfake), אשר מתאפיינות בכך שהשחקן וכוונתו מוסתרים. הסייבר והרשתות החברתיות הגדילו את הזמינות ואת היקף השימוש בממד ההשפעה, והבינה המלאכותית האיצה זאת עוד יותר (בשל הקלות של ייצור תוכן משכנע, פרופילים מזויפים ו"זיופים עמוקים" והקושי להבחין בזיוף).

שלוש הקטגוריות - איסוף, חבלה והשפעה - משתלבות ומשלימות זו את זו: איסוף משרת מְבצעֵי השפעה, השפעה יוצרת תנאים לחבלה, וחבלה מחזקת את אמינות ההשפעה הדיגיטלית.[21] המאפיין העיקרי של הסייבר כמרחב חשאי הוא היכולת לבצע את הפעולות בכל שלוש הקטגוריות, ולספק להן הכחשה סבירה, בצורה חשאית (הפעולה עצמה מוסתרת) או חסויה (הגורם המְבצע מוסתר). חלק מהחסרונות המבניים של קטגוריה מסוימת אינם נפתרים בתוכה, אלא באמצעות מעבר לקטגוריה אחרת: מבצע חבלה בסייבר יכול להיות חלופה למבצע קינטי המסכן חיי לוחמים; ארגון פשע המופעל כשלוח (פרוקסי) יכול להחליף גופים מדינתיים במבצעים רגישים; וסוכן נגיש יכול לגשר על פערי נגישות בסייבר. לעיתים קרובות אם פעולה נחסמת בממד אחד, אפשר לבצע אותה בהצלחה בממד אחר בעל פרופיל חשיפה אחר לחלוטין.

---

17 גוארינו, א' ואזיילו, א' (יוני 2017). אביפת גבולות או חציית גבולות בסייבר: דילמת הריבונות. סייבר, מודיעין וביטחון, 1(2), 3–18

18 פעולת הריגול המדינתי הגדולה הראשונה בתחום הסייבר הייתה בסוף שנות ה־90 של המאה ה־20: רוסיה חדרה למחשבי הפנטגון, צבא ארצות הברית, נאס"א, גופי ביון ואוניברסיטאות אמריקניות (Moonlight Maze). פעולת השיבוש המדינתי הראשונה כוונה ב־2007 נגד אסטוניה, התמקדה במניעת שירות ושיתקה את מוסדות המדינה

19 דוגמאות רלוונטיות הן תקיפת מתקני הגרעין באיראן ב־2010; תקיפה של רוסיה נגד מתקני תשתית באוקראינה לפני ובמהלך המלחמה ביניהן; ותקיפה של איראן ב־2015 וב־2016 אשר כוונה נגד תשתיות בערב הסעודית

20 U.S. Joint Chiefs of Staff (2018, June 8). Joint Publication 3-12: Cyberspace operations. https://nsarchive.gwu.edu/document/16681-joint-chiefs-staff-joint-publication-3-12

21 יסעור, נ' וסיטרינוביץ, ד' (2025). התערבות והשפעה זרה איראנית במהלך מלחמת "חרבות ברזל". בתוך ד' סימן טוב וי' קופרווסר (עורכים), השפעה והתערבות זרה כאתגר אסטרטגי ומודיעיני (עמ' 68–80). המכון למחקרי ביטחון לאומי

הסייבר ההתקפי ערער את אחת ההנחות הבסיסיות של הפעילות החשאית הקלסית, ולפיה חשאיות כרוכה בסיכון. בפעילות החשאית המסורתית נדרשו מסגרות מפקחות ומאשרות בגלל הסיכון לחשיפה, למעצר ולכישלון מדיני. אולם אם אין לוחם בשטח, פוחת משקלו של הסיכון בקבלת החלטות על פעולה – והדבר בא לידי ביטוי בתהליכי האישור. תחילה נדרשו בפעולות סייבר התקפיות אישורים ברמת "מבצע חוצה גבול"; ברם ככל שהתבררה יכולתו של הסייבר להשיג הישגים מבצעיים תוך כדי סיכון נמוך להיחשף, השתנו הנהלים בהתאם: רמת האישור הנדרשת ירדה, הואצלו סמכויות בנושא היציאה לפעולה, והתקצר משך הזמן שנדרש לאישור הפעולה.[22]

הפחתת הסיכון משנה את "כלכלת" הפעילות החשאית כולה. הפחתת רמת האישור הנדרשת הרחיבה את מרחב הפעילות החשאית האפשרית: מְבצעים שבעבר לא אושרו בגלל סיכון מוגזם לאנשי שטח, הפכו אפשריים ואף שגרתיים. יתרה מזאת, שילוב בין הסייבר לפעולה פיזית מגדיל את סיכויי ההצלחה: פעולות משולבות – הסייבר יוצר את התנאים, ופעולה קינטית מממשת את ההישג (או להפך) – מאפשרות להגיע להישגים שאף אחד מהרכיבים לא היה מסוגל להשיג לבדו. נטרול מערכות הגנה לפני תקיפה, שיבוש תקשורת של היעד בזמן מְבצע, שימוש בגישה פיזית להשתלת יכולת סייבר – כל אלו מדגימות סינרגיה אשר מניבה תוצאה הגדולה מסכום חלקיה.[23] שינוי זה מאיים על הפרדיגמה הישנה: הסייבר מתחרה בפעולות קומנדו, ולעיתים אף מייתר אותן; פעולה שהצריכה סיכון חיים, אפשר לבצע מרחוק בסיכון אפסי. בד בבד הפעולות הפיזיות הפכו מסוכנות יותר בשל שיפור יכולות הגילוי. הסייבר מספק הזדמנויות להתמודד עם האיום הנובע מיכולות הפיקוח הנרחבות, שכן אפשר לחדור ולתפעל את הארכיטקטורה הרשתית עצמה אשר הפיקוח מבוסס עליה. כך למשל אפשרית מניפולציה של סביבת הניטור עצמה באמצעות חדירה למצלמות האבטחה, מחיקת קטעי תיעוד ושיבוש (או החלפה) של רצף הצילום. אפשר גם לשנות בסיסי נתונים כדי למחוק רישומי כניסה ולעצב מחדש את החתימה הדיגיטלית של היעד, או של הגורם החשאי עצמו. אפשרות נוספת היא "לשתול" זהות כיסוי פעילה במאגרים הרלוונטיים – הצגת היסטוריה דיגיטלית עקבית, רישומי עבר ונוכחות ברשתות חברתיות שנבנית מראש.[24]

לא כל השחקנים מנצלים את האפשרויות האלה באופן זהה. מדינות מכוונות ליעדים בעלי הערך הגבוה ביותר (תשתיות לאומיות, מאגרי מידע, מערכות ביטחוניות), שהם גם המורכבים והמסוכנים ביותר בהיבט של חשיפה. לעומת זאת שחקנים א־סימטריים (ארגוני טרור, ארגוני פשע מאורגן ובודדים) מכוונים ליעדים שבהם סיכויי ההצלחה גבוהים, פוטנציאל הנזק או הרווח הכלכלי המיידי מהיר, וסיכון החשיפה נמוך יחסית.

תמורות בעולם החשאי

ניתוח של השפעות הדיגיטל על הפעילות החשאית מגלה שלא מדובר רק בשינוי של כלים וטקטיקות לחימה, אלא בשינוי עמוק אשר משפיע על טבע החשאיות עצמה. ארבע התמורות המתוארות בסעיף זה אינן מקבילות, וכל אחת עונה על שאלת משנה אחרת. התמורה הראשונה היא שחיקת המונופול המדינתי. הדיגיטל אִפשר לשחקנים חדשים להיכנס למרחב החשאי וטשטש את הגבולות בין מדינות לגורמים לא מדינתיים. בעבר יכולות מעקב, ריגול וחבלה היו מונופול של מדינות; אולם הזמינות והנגישות הטכנולוגית גרמו לכך שכיום ארגוני טרור ופשיעה מפעילים פיקוח אווירי, משתמשים בהאזנות ובכלי סייבר מתקדמים ורואים בהם רכיב מרכזי בפעילותם. מה שבעבר הצריך מערכי מודיעין של מדינות, הופך כיום זול ונגיש.[25] גם בזירת הסייבר הידע והיכולות כבר אינם נחלתם של ארגוני המודיעין בלבד. חברות עסקיות וארגוני פשע מחזיקים ביכולות שבעבר היו שמורים למעצמות, ויש שיתוף פעולה בין גורמי מודיעין מדינתיים לקבלנים חיצוניים למיניהם: גורמי פרוקסי, ספקי יכולות פורנזיקה דיגיטלית, ספקים של כלי מעקב ותקיפה וכן הלאה.[26]

כיום יכולות ייחוס שבעבר היו בלעדיות למדינות, נמצאות גם בידי גורמים אזרחיים. כך למשל בספטמבר 2018 סייע בלינגקאט

---

22 כך למשל בארצות הברית מסכת האישורים למבצעי סייבר התקפי ירדה בין 2012 (ממשל אובמה, PPD-20) ל־2018 (הממשל הראשון של טראמפ, NSPM-13)

23 Golding, J. (2022, November 11). Byte, with, and through: How Special Operations and Cyber Command can support each other. War on the Rocks; Keller, J. (2020, May 12). SOCOM chief: Door-kickers are out, cyber operators are in. Task & Purpose

24 Baker, S., Espionage Tradecraft in an AI-Saturated Surveillance World (2026), pp 2-4. https://www.stevebaker.info/wp-content/uploads/2026/02/Espionage-AI.pdf

25 כך למשל קרטלים במקסיקו מפעילים רחפני תצפית ומצלמות במעגל סגור כדי לעקוב אחר פעילות המשטרה. דרך הפעולה שלהם דומה לזו של מערכות צבאיות

26 על השימוש המדינתי בכלי סייבר מסחריים ראו אצל Broeders & Kavanagh (2023), pp. 21-23; Marczak, B., Scott-Railton, J., McKune, S., Abdul Razzak, B., & Deibert, R. (2018, September 18). Hide and seek: Tracking NSO Group's Pegasus spyware to operations in 45 countries. The Citizen Lab

(Bellingcat), גוף חוקר המתמקד בניתוח מידע ממקורות גלויים (כלי אוסינט פתוחים), לחשוף את זהותם של סוכני GRU שהרעילו בבריטניה את סרגיי סקריפאל ובתו יוליה.[27] חלק מהגורמים האזרחיים נהנים מיתרונות שאין למדינות: גמישות, אימוץ מהיר של טכנולוגיות, שחרור מאילוצים בירוקרטיים ומשפטיים. התרחבות השימוש בטכנולוגיית AI מאיצה את התהליך בגלל היתרון בתחום זה של חברות הענק הטכנולוגיות על הגורמים המדינתיים.[28] אולם לשחקנים הללו יש לא רק יתרונות, אלא גם חסרונות מבניים: סנכרון מוגבל בין מערכות, כמו גם חשיפה גבוהה לחדירה ולשיבוש של גורמי אכיפה. הגמישות מאפשרת להם לנוע מהר, אך גם מונעת מהם לשרוד לאורך זמן.[29]

טשטוש ההפרדה בין החשאי ללא חשאי וזליגת הידע הם חלק מתופעה רחבה יותר: היקף המידע אשר זמין לציבור גדֵל באופן חסר תקדים. מה שבעבר נרכש באמצעות איסוף מדינתי חשאי, זמין היום לכול ברשתות החברתיות – הנגישות למסדי נתונים רבה, רמת החשיפה גבוהה, איכות המידע גבוהה מאוד.[30] ריבוי השחקנים אינו רק שינוי בתנאי הזירה; הוא מגדיל את מספר הקהלים אשר יש לנהל מולם את פערי הידיעה, ובהתאמה מצטמצמת יכולתה של מדינה לשלוט במידע שנאסף עליה.

התמורה השנייה היא ביכולת להסתיר את הזהות, רכיב יסוד בתוך החשאי. אם בעבר אדם היה יכול להסתיר את זהותו, לזייף, להחליף ולבנות זהות חדשה ללא קושי רב, הרי בעידן ה־AI זהות היא תוצר שהמערכת מגבשת בהתבסס על מסקנותיה ממכלול הפעולות של האדם. כל תנועה, שיחה, תשלום וכניסה שלו למלון יוצרים חתימה דיגיטלית ייחודית. אי־אפשר לזייף חתימה כזו, כי היא מורכבת ממכלול נתונים שמצטבר לאורך זמן בכמה מערכות. בעבר החשאיות הייתה פיזית במהותה – לא להיראות ולא להשאיר עקבות. בעולם הדיגיטלי האדם מנוטר בקביעות (מצלמות, ביומטריה וכן הלאה), ללא תלות במסמכים פורמליים; ההתמקדות היא בנתון שהאדם מייצר ובמשמעות שהאלגוריתם מפיק מהנתון הזה. זהות טבעית היא כזו שיש לה חתימה דיגיטלית עקבית, היסטוריית גלישה, פרופיל רשת טבעי, דפוס רכישות וכן הלאה. בעולם מרושת לחלוטין אי־נראות היא סימן מעיד: מי שלא קיים דיגיטלית, יכול להפוך חשוד – היעדר נוכחות ברשת וניסיון לטשטש עקבות מוזָנים לאלגוריתם כחריגות.[31] אחד השינויים בעידן ה־UTS הוא ביטולו של מרחב ביניים, מרחב שהזירה החשאית פעלה בו מאז ומעולם – האפשרות להיות שונה בלי להיות חשוד. בעבר התנהגות הוגדרה כחריגה בהתבסס על שיקול דעת אנושי של המעריכים אותה, והדבר אִפשר לסוכנים להתנהל במרחב של דו־משמעות ועמימות. האלגוריתם לא מְפרש אלא מודד ומתריע על אנומליה, ולכן האנונימיות (את זו אפשרה בעבר המולת המרחב הציבורי עצמה) כמעט חדלה להתקיים כמרחב חשאי.

אחת הדרכים להתמודד עם תמורה זו היא אפוא לא להיעלם, אלא לנהל את החתימה הדיגיטלית (signature reduction) כדי "להיראות טבעי".[32] גורמים חשאיים משקיעים משאבים רבים ביצירת זהויות סינתטיות – פרופילים שנבנים לאורך זמן ומקיימים פעילות מתמשכת ברשת החברתית, קשרים אותנטיים והתנהלות דיגיטלית עקבית.[33] דרך אחרת היא היעלמות מלאה לפרק הזמן הנדרש לביצוע הפעולה. זיהוי בדיעבד אינו בהכרח כישלון, שכן מניחים כי הפעולה תושלם עד שהמידע ייאסף וינותח. זו פעילות חסויה ולא חשאית: מטרתה איננה הסתרת הזהות, אלא הסתרת הפעולה בעת ביצועה. לוגיקה כזו מאפיינת פעולות קומנדו חסויות, שָם הייחוס בדיעבד מקובל ולעיתים אף רצוי.[34] דרך נוספת היא להטביע את האות בתוך רעש ועומס מידע, כיוון שאלה מנטרלים את יכולת הניתוח של הצד הצופה.[35]
לצד ניהול החתימה הדיגיטלית, יש להתייחס בנפרד לביומטריה — קטגוריית מידע ששונה איכותית משאר סוגי החתימה שנסקרו לעיל. לא כל שיטות הזיהוי הביומטרי רלוונטיות באותה מידה לפעילות חשאית. שתיים בלבד מגיעות כיום לפריסה המונית שיוצרת

27 Bellingcat Investigation Team (2018, September 26). Skripal suspect Boshirov identified as GRU Colonel Anatoliy Chepiga

28 ריאיון עם אל"ם (מיל') גל שמואלי ב־18 ביוני 2026

29 אבן, ש' וסימן טוב, ד' (יוני 2011). לוחמה במרחב הקיברנטי: מושגים, מגמות ומשמעויות לישראל. המכון למחקרי ביטחון לאומי (מזכר 109), עמ' 22־23

30 לדוגמאות של שימוש נרחב באוסינט במלחמת רוסיה–אוקראינה – שיתוף אזרחים אוקראינים במאמץ האיסוף, איסוף ברשתות חברתיות, קבלת מידע מלוויינים מסחריים – ראו: Emily Harding, "Intelligence in a Transparent World", *CSIS* (September, 2025).

31 Baker, S. (2026, February 22). Espionage tradecraft in an AI-saturated surveillance world. Steve Baker FRSA

32 Bernath (2019), p. 33

33 ההתמקדות היא בעיקר בניהול הזהויות החשאיות בעידן הדיגיטלי ובפיתוח זהויות סינתטיות, או לחלופין בשימוש בביסוי אותנטי עמוק ובעריכת מניפולציות בבסיסי נתונים (Bernath, 2019, p. 40)

34 Baker (2026), pp. 2-4

35 Moede, C. (2026, May 29). Intervening in the attribution chain: Signature reduction under cross-domain surveillance. Small Wars Journal

סיכון ממשי לגורם המבקש להישאר חשאי: טביעת אצבע, הנפוצה בגבולות, במאגרי אכיפת חוק; וזיהוי פנים, שהתרחב במהירות ממתקני ממשל לשערי גבול אוטומטיים ולמצלמות עירוניות. בעוד שהיסטוריית גלישה, נוכחות ברשתות חברתיות ודפוסי תנועה הם תוצרים של פעולה, וככאלה ניתנים לזיוף ולהחלפה — ביומטריה היא תוצר של קיום. טביעת אצבע, ותבנית פנים לא ניתנות לבנייה מחדש באותו אופן שבו נבנית זהות דיגיטלית סינתטית. המשמעות המעשית של הבחנה זו היא שהביומטריה אינה עוד סוג של פער ידיעה שניתן לנהל, אלא נקודת הקצה שבה מושג הניהול עצמו מאבד את תוקפו - היא מגדירה את גבול היכולת להסתיר זהות מלכתחילה, ולא רק את הקושי לשמר הסתרה קיימת. אותה אי-הפיכות ניכרת בפרשת הפריצה הסינית למאגרי ה-OPM שהוזכרה לעיל. בעוד שפרטים כגון כתובת מגורים או היסטוריית תעסוקה של עובדי ממשל אמריקאים ניתנים להסתרה מחודשת, הנתונים הביומטריים שנחשפו — טביעות אצבע של מיליוני עובדים — נותרו חשופים לצמיתות, ללא כל אפשרות 'להנפיק' טביעת אצבע חדשה למי שזהותו נפגעה.

התמורה השלישית היא בייחוס הפעולה החשאית. בעולם החשאי הקלסי הכחשה סבירה הייתה מאמץ מודע ומכוון; מאחורי כל פעולה חשאית עמד גורם – אדם, ארגון או מדינה – שהשקיע מאמץ ממשי בהסתרת מעורבותו.[36] מאפייני הסייבר מאפשרים לגורם החשאי להכחיש את מעורבותו בלי להידרדר להסלמה. כך למשל קוד יכול לעבור דרך שרתים בעשרות מדינות, ומדינות עושות שימוש בגורמי פשע מאורגן (כפרוקסי) או בכלי תקיפה מסחריים (דוגמת פגסוס) כאמצעי ליצירת הכחשה. לעמימות תורמת העובדה שתכלית התקיפה יכולה להיות עמומה, גם אם התקיפה עצמה התגלתה.

לטכנולוגיה יש תפקיד כפול – מחד היא מספקת לתוקף מגוון כלים לפעולה חשאית ומאידך היא הופכת את ההכחשה הסבירה (plausible deniability) לבלתי סבירה (implausible deniability) שכן ככל שכלי הייחוס הדיגיטלי-פורנזי מצטברים, ההכחשה נאלצת לעמוד מול ראיות קונקרטיות, ולמרות זאת מדינות ממשיכות לנהל פעולות חשאיות תוך הכחשה בלתי סבירה בעליל. רוסיה ממחישה זאת באופן מובהק במקרה מתקפת הסייבר NotPetya (יוני 2017). ניתוח של הקוד הזדוני הוביל את ארה"ב ומדינות נוספות במערב, לייחס את המתקפה לרוסיה, ברמת ודאות גבוהה. חרף זאת, מוסקבה המשיכה להכחיש כל מעורבות, וכינתה את הטענות 'רוסופוביות'. [37] ההכחשה כאן לא נועדה לשכנע, איש אלא לשמר מעטפת שמאפשרת הימנעות מהסלמה גלויה, גם כשהצדדים כולם יודעים שהיא חסרת כיסוי עובדתי. הטכנולוגיה פועלת בשני כיוונים מנוגדים - מחד מקשה על הסתרת הפעולה עצמה, ומאידך מאפשרת ערפל ייחוס שלא היה קיים בעבר. המאבק על החשאיות בעידן הרשתי הוא מרחב מתחים דינמי שבו יכולות החשיפה וההסתרה מתפתחות במקביל, אולם לא כל השחקנים כורכים את פעולתם בחשאיות.

הסייבר מרחיב את ממדיה של תופעה שהייתה עוד קודם. פעולות של פרוקסי ומבצעי חבלה חשאיים נערכו גם בעבר, אך ממדיהן בעידן הסייבר חסרי תקדים. חבלה בתשתיות חיוניות ומבצעי השפעה פוליטיים יוצרים נזק אמיתי וממשי, אך אינם חוצים את הסף שמצדיק תגובה צבאית. נוצר אזור ביניים אפור: מדינות יכולות לפגוע זו בזו בחשאי באופן מתמשך, וזאת בלי שהצד המותקף ירצה להגיב בגלוי. עקב כך נוצרים מעגלי פעולה–תגובה מהירים וחסרי ייחוס, שהם מתחת לרף ההסלמה (הדברים אמורים גם בפעולה חסויה שאיננה בממד הסייבר, ואי-אפשר לייחס אותה חד־משמעית לצד התוקף).[38]

התמורה הרביעית היא במשך הפעולה החשאית. בעולם החשאי הקלסי הסיכון להיחשף היה ברגע הפעולה (מועד המפגש, מעבר הגבול וכן הלאה); החשאיות הייתה אירוע מוגדר בזמן ובמרחב. לעומת זאת בעולם הדיגיטלי הסיכון להיחשף קיים על ציר זמן שלם – לפני הפעולה, במהלכה ואחריה. כל נתוני המסגרת הדיגיטלית של הפעולה נשמרים ומאפשרים ניתוח. חשיפה יכולה להיות רטרואקטיבית, ופעילות שבוצעה לפני שנים יכולה להתגלות בהתבסס על נתונים אשר נותחו בדיעבד. דוגמה מובהקת לחשיפה בדיעבד היא ניסיון ההרעלה הכושל באפריל 2015 של אמיליאן גברב, סוחר נשק בולגרי. הפרשה נותרה בלתי פתורה במשך כארבע שנים, עד שב־2019 נחשף – בהתבסס על "הצלבת" נתוני טיסות, דרכונים ורישומי תקשורת סלולרית – כי מדובר בפעולה של המודיעין הרוסי.[39]

---

36 לניתוח של הפעולה החשאית בכלי לשליטה בהסלמה, לרבות הצגת מקרי בוחן במהלך המאה ה־20, ראו אצלו Austin Carson, "Secret Wars: Covert Conflict in International Politics", Princeton University press, (2018).

37 UK and US Blame Russia for 'Malicious' NotPetya Cyber-Attack," BBC News, February 15, 2018, https://www.bbc.com/news/uk-politics-43062113.

38 אבן וסימן טוב (2011), עמ' 23; Cormac & Aldrich (2018), pp. 491-492; להרחבה בנושא של מעגלי פעולה–תגובה בין מדינות טוטליטריות לדמוקרטיות בעידן ה־AI ראו אצל Prunckun, H. (2026). AI and the reconfiguration of the counterintelligence battlefield. International Journal of Intelligence and Counterintelligence, 39(3), 738-755.

39 Bellingcat Investigation Team (2019, November 23). The dreadful eight: GRU's unit 29155 and the 2015 poisoning of Emilian Gebrev. Bellingcat

בזירת הסייבר הפעולה החשאית עשויה לא להסתיים כלל. נוכחות חשאית במחשבי היריב יכולה להימשך חודשים או שנים, ללא הגדרת מועד של סיום מבצעי, וזאת בניגוד לפעולה הפיזית אשר מסתיימת עם השלמת הביצוע. כך למשל לפי דוח של CISA, לקבוצת תקיפה סינית הייתה דריסת רגל בתוך רשתות של תשתית חיונית בארצות הברית במשך חמש שנים לפחות.[40] דריסת רגל זו לא זוהתה, אך הקבוצה נמנעה במתכוון מגֵבת מידע ומגרימת נזק והמתינה למשבר עתידי. המשמעות היא שניהול של חשאיות בזירת הסייבר יכול להיות לא רק אירוע, אלא מצב מתמשך ללא נקודת סיום ברורה.

מכלול התמורות מצביע על שינוי עמוק בעולם החשאי, ונדרשת המשׂגה מחדש של הפעילות החשאית. המסגרת המסורתית של פעילות חשאית התבססה על ההנחה כי אפשר להסתיר את המידע על הפעולה, על מְבצעיה ועל מפעיליה. ההצלחה נמדדה ביכולת לשמור על פערי ידיעה. העידן הדיגיטלי לא ביטל את פערי הידיעה, אך שינה מהותית את אופיים: הם נעשו דינמיים, זמניים, וכאלה שקשה יותר לתכנן אותם מראש. דווקא בעידן המתאפיין בשאיפה של כולם לחשאיות, קשה מאי פעם לשמור עליה. ריבוי השחקנים, הדלפות (באישור וללא אישור), לחץ לפרסם הצלחות ולהרתיע – כל אלו חושפים את מה שאמור להישאר בצל. מדינות מתקשות לשמור על סודותיהן, ארגונים נחשפים באמצעות כלים שאמורים להיות חשאיים. החשאיות הייתה למשאב מתכלה אשר יש לנהל. המאמר פתח בהגדרת חשאיות כהסתרה של הגורם, הפעולה, או שניהם; ניתוח המציאות הדיגיטלית חושף שההגדרה הזו נשחקה: בעולם שכל פעולה בו משאירה עקבות אשר אפשר לנתח, מרחב ההכחשה הסבירה מצטמצם.

בהתאם לכך השתנה בעידן הנוכחי המדד להצלחת פעילות חשאית. היא לא נמדדת רק בהסתרה, אלא ביכולת הניהול: לשאלה "כיצד להימנע מחשיפה?" נוספה שאלת השליטה בעיתוי החשיפה ובמשמעותה הפוליטית. פרסום ארכיון הגרעין האיראני על ידי ישראל באפריל 2018 הוא דוגמה לפעולה חשאית ששירתה חשיפה מכוונת. גם מבצע תקיפת הכור הגרעיני הסורי ממחיש שליטה מכוונת בעיתוי החשיפה: ישראל תקפה את הכור בספטמבר 2007, שמרה על עמימות בנושא זה במשך למעלה מעשור, ורק במרס 2018 אישרה את אחריותה להפצצת הכור. עצם העיתוי של המעבר מעמימות להודאה היה כלי אסטרטגי עצמאי, כזה אשר מנותק מהמטרה המבצעית המקורית.[41]

ההמשגה המוצעת – ניהול פערי ידיעה במקום הסתרתם – לא מחליפה את הבידול בין פעולה חשאית לפעולה חסויה, אלא מרחיבה אותו: ההבחנה בין הסתרת הפעולה להסתרת המפעיל נשמרת, אך שתי הקטגוריות הן עתה חלק מהשאלה הרחבה יותר של שליטה בזרימת המידע ובמשמעותו לאורך זמן. ארבע התמורות שתוארו מסבירות יחדיו כיצד השתנה טבע החשאיות, ומה המשמעות (האסטרטגית והאופרטיבית) של השינוי הזה. החשאיות חדלה להיות מצב בינארי (הסתרה או חשיפה) והייתה לניהול מתמשך של פערי ידיעה.

סיכום והמלצות

בשנים האחרונות הזירה החשאית השתנתה ללא הכר. היא הפכה מגוונת, מורכבת ומלאה בשחקנים שלא היו בה מעולם, גבולותיה התמוססו, ויחסי הכוחות בתוכה משתנים ללא הרף. על אף מורכבותו של המרחב החשאי הוא מושך אליו עוד ועוד גורמים בשל זמינות הכלים החשאיים, השפעתו הגדולה והפוטנציאל לפעול ללא קבלת אחריות: אפשר לפגוע, להשפיע ולרגל בלי לשלם את המחיר הדיפלומטי, הפוליטי או הצבאי הנלווה לפעולה גלויה.[42]

קיים קשר עמוק בין חשאיות לשינוי המבני בעידן הביטחון העכשווי. "בין המלחמות" של המאה ה־21 אינו מצב זמני אלא מתמשך, ואפשר לנהל אותו מתחת לרדאר. הזירה החשאית מאפשרת "מלחמה מתמדת ללא מלחמה" – שחיקה שיטתית של יכולות לא חוצה את רף התגובה, ונוצר מרחב מבצעי בין מלחמה לשלום. במרחב זה פעולות כוחניות מתרחשות מתחת לרף ההסלמה, הגבולות בין צבאי ולא צבאי מיטשטשים, וטבע הזירה מאפשר היעדר ייחוס. המטרה אינה ניצחון צבאי, אלא יצירת יתרון תחרותי מצטבר ושחיקה שקטה של יכולת היריב.

40 Cybersecurity & Infrastructure Security Agency (2024, February 7). PRC state-sponsored actors compromise and maintain persistent access to U.S. critical infrastructure (Alert Code: AA24-038A). https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

41 Gross, J. A. (2018, March 21). Ending a decade of silence, Israel confirms it blew up Assad's nuclear reactor. The Times of Israel

42 Baram, G, & Sommer, U. (2019). Covert or not covert: National strategies during cyber conflict. In T. Minárik, S. Alatalu, S. Biondi, M. Signoretti, I. Tolga, & G. Visky (Eds.), 2019 11th International Conference on Cyber Conflict: Silent Battle (pp. 1-16). IEEE

הכניסה לזירה הפכה אפוא קלה יותר, אך ההישרדות בה מורכבת. מהגוף החשאי נדרש ניהול מתמיד של מתחים ללא פתרון: בין יעילות לחשאיות, בין ריכוזיות לביזור, בין נוכחות דיגיטלית לאנונימיות. השחקן שישרוד בסביבה הזו הוא לא בהכרח הגדול ביותר, אלא הגמיש. נוצר דרוויניזם חדש – הקצב הוא הגורם הקובע, ותגובה מאוחרת לשינוי טכנולוגי משמעה חשיפה.

הטיעון המרכזי במאמר הוא שהחשאיות השתנתה ממצב אשר אפשר לשמר למשאב אשר יש לנהל. בהתאם לכך נדרש עדכון של ארבעה עקרונות יסוד אשר קהילות מודיעין פועלים לפיהם:

ראשית, הכנה לחשיפה צריכה להיות חלק בלתי נפרד מהתכנון המבצעי, ולא תגובת חירום מאוחרת. המשמעות המעשית היא שכל תיק מבצעי צריך לכלול תרחיש חשיפה: מי חושף, מתי, באיזה ערוץ, ומהי התגובה המוכנה מראש. הדבר הכרחי לא מפני שהחשיפה רצויה, אלא כי כיום היא אפשרות סבירה.

שנית, בעבר הפעילות החשאית הסתמכה על אנשים אשר מסוגלים להסתיר את זהותם, אולם כיום הדרישות מהם השתנו מן היסוד. יצירת זהות בדויה אמינה מחייבת נוכחות דיגיטלית עקבית במשך שנים; לפיכך הפרופיל הנדרש אינו עוד של אדם אשר מסוגל לאמץ זהות לקראת פעולה, אלא של כזה המסוגל להחזיק בזהות מסוימת לאורך זמן תוך כדי שמירה על עקביות דיגיטלית. יש לכך השלכות על מסלול הקריירה של העובד – החל בשלב הגיוס, עבור בפיתוח המקצועי וכלה באופק הקריירה. המטרה היא לשמר זהות דיגיטלית בלי שהארגון יאלץ "לנתק אותה" לאחר כל מבצע.

שלישית, השימוש בגורמים חיצוניים לביצוע פעילות חשאית אינו חדש, אך העידן הדיגיטלי הרחיב מאוד את היקפו ואת סוגי הגורמים המעורבים. המשותף לכולם הוא שני יתרונות: יכולת מבצעית שהמדינה מעדיפה לא להפעיל בעצמה, ושכבת בידול המאפשרת הכחשה. המרד של קבוצת וגנר ברוסיה ביוני 2023 חשף את הסיכון שבגורם אשר אין שליטה מלאה בו: הוא עלול לפתח אינטרסים עצמאיים, ובנקודת משבר להיות מנכס לאיום.[43] מומלץ שמדינות אשר רוצות להשתמש בקבלני משנה חיצוניים יגדירו מראש אילו יכולות ליבה אי-אפשר להאציל להם, ואילו מנגנונים לניהול סיכונים ילוו את ההתקשרות ואת היום שאחרי.

רביעית, הפעילות החשאית בעידן זה לא יכולה להישען על הנחת יסוד של אי־ודאות מתמשכת באשר למידת החשיפה של הפעילות. יש לפתח יכולת שיטתית ללמידה מתמדת של המערכת על עצמה. על הארגון לפתח יכולת לערוך ניתוח מודיעיני "מכוון פנים" הכולל מעקב שיטתי אחר פרסומים ודוחות OSINT, כמו גם להיעזר בניתוחים של חברות אבטחה וארגוני מחקר עצמאיים (כמו למשל Mandiant, Bellingcat, Lab Citizen) אשר עוסקים בפעילותו שלו. בדרך כלל ניתוחים כאלה מבוססים על אותם החיישנים הדיגיטליים וכלי הניתוח שהארגון עצמו נדרש להכיר, והם מספקים תחקיר חיצוני על שיטות הפעולה ודפוסי ההתנהגות שלו. אם ניתוחים כאלה יהיו מקור למידה שיטתי, ולא ייבחנו רק בתגובה לאירוע מסוים, הארגון עשוי להבין איך הוא נראה מבחוץ ולזהות דפוסי חשיפה שאינם גלויים לו מנקודת המבט הפנימית. בד בבד נדרשת התאמה בין קצב הלמידה הארגונית לקצב ההשתנות של הסביבה הטכנולוגית. פעמים רבות מבנים ארגוניים חשאיים נוטים להיות מסורבלים בשל הירדכיה נוקשה, סגירות ותהליכי עבודה בירוקרטיים. היתרון הוא בהבטחת יציבות ובשמירת הסוד, אך מבנה ארגוני כזה מאט את הפצתם של לקחים ואת העדכון של שיטות הפעולה. לפיכך יש לאמץ מנגנוני למידה מהירים ומבוזרים יותר, כלומר להקנות לרמות הקרובות למקור השינוי סמכות לזהות ולשנות את שיטות הפעולה שלהן בסמוך ל"זמן אמת".

רשימת מקורות

אבן, שמואל ודוד סימן-טוב. לוחמה במרחב הקיברנטי: מושגים, מגמות ומשמעויות לישראל(תל אביב, המכון למחקרי ביטחון לאומי, 2011).

גוארינו, אלסנדרו ואמיליו אזיילו. "אכיפת גבולות או חציית גבולות בסייבר: דילמת הריבונות." סייבר, מודיעין וביטחון 1, גיליון 2 (2017).

יסעור, ניצן ודני סיטרינוביץ. "התערבות והשפעה זרה איראנית במהלך מלחמת חרבות ברזל." בתוך דוד סימן טוב ויוסי קופרווסר (עורכים), השפעה והתערבות זרה כאתגר אסטרטגי ומודיעיני (תל אביב: המכון למחקרי ביטחון לאומי, 2025), 68-80.

Advisory ,Joint Cybersecurity" .PRC state-sponsored actors compromise and maintain persistent access to US critical infrastructure ,AA24-038A *7".th Feb* (2024).

Baker, Steve. "Espionage Tradecraft in an AI-Saturated Surveillance World." *Steve Baker FRSA* (22 February 2026).

Baram, G, & Sommer, U. (2019). Covert or not covert: National strategies during cyber conflict. In 2019 11th International Conference on Cyber Conflict (CyCon), vol. 900, pp. 1-16. IEEE, 2019.

Bernath, Erik. "To What Extent Have the Developments of Current Information and Communications Technology (ICTs) Affected Espionage Tradecraft Used While Conducting Covert Operations?" (2019).

Bisson, Brian D. "The OPM Breach: Timeline of a Hack," *Tripwire*, (29 June 2015).

Bowen, Andrew S., "Wagner Group Mutiny in Russia," *Congressional Research Service*, IN12186 (28 June 2023).

Broeders, Dennis, and Camino Kavanagh. "Shades of Grey: Cyber Intelligence and (Inter) national Security." *Policy Brief, EU Cyber Direct* (2023).

Broeders, D. W. J. "Addressing the elephant in the room: cyber intelligence and international security." PhD diss., Leiden University, 2023.

Golding, Josh. "Byte, with, and through: how special operations and cyber command can support each other." *War on the Rocks* (November 2022).

Campbell, Duncan. "Interception capabilities 2000." *Report to the Director General for Research PE* 168 (1999).

Carson, Austin. *Secret Wars: Covert conflict in international politics*. Princeton University Press, 2018.

Carson, Austin, and Keren Yarhi-Milo. "Covert communication: The intelligibility and credibility of signaling in secret." *Security Studies* 26, no. 1 (2017): 124-156.

Cormac, Rory, and Richard J. Aldrich. "Grey is the new black: covert action and implausible deniability." *International Affairs* 94, no. 3 (2018): 477-494.

Egger, Matthew, "The Relevance of HUMINT in the Digital Era," *Lobo Institute* (13 January 2023).

Gardham, Duncan, and John Kifner, "Hamas Bomb Engineer Slain by Booby-Trapped Cellular Phone," *The New York Times*, (6 January 1996).

Harding, Emily. "Intelligence in a Transparent World," *CSIS* (September 2025).

Keller May, Jared. "SOCOM Chief: Door-Kickers Are Out, Cyber Operators Are In." *Task & Purpose* (12 May 2020).

Kovacs, Eduard. "Chinese Government Suspected in Marriott Hack: Report," *Security Week*, (6 December 2018).

Gioe, David V., and Tony Manganello. "Smart new world: adapting human intelligence for the digital age." *Intelligence and National Security* 40, no. 6 (2025): 1114-1128.

Gross, Judah Ari. "Ending a decade of silence, Israel confirms it blew up Assad's nuclear reactor." *The Times of Israel* 21 (2018).

Marczak, Bill, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert. "Hide and seek: Tracking NSO group's Pegasus spyware to operations in 45 countries." (2018).

Marquis-Boire, Morgan, Glenn Greenwald and Micah Lee, "XKEYSCORE: NSA's Google for the World's Private

Communications," *The Intercept* (July 2015).
Moede, Christopher, "Intervening in the Attribution Chain: Signature Reduction Under Cross-Domain Surveillance", *Small Wars Journal* (May 2026).
Prunckun, Henry. "AI and the Reconfiguration of the Counterintelligence Battlefield." *International Journal of Intelligence and Counterintelligence* 39, no. 3 (2026): 738-755.
"Sharp Eyes: Mass surveillance of foreigners in China," *NetAskari* (25 May 2026).
Sherman, Justin, "Ubiquitous Technical Surveillance Demands Broader Data Protections," *Lawfare* 25) July.(2025 U.S Joint Chiefs of Staff ,Joint Publication :3-12 Cyberspace Operations ,Washington ,DC) June ,(2018 II–1-II.4-
Team ,Bellingcat Investigation" .Skripal suspect Boshirov identified as GRU colonel Anatoliy Chepiga ".*Bellingcat .https//:www .bellingcat .com/news/uk-and-europe/2018/09/26/skripal-suspect-boshirov-identified-gru-colonel-anatoliy-chepiga* (2018).
Team, Bellingcat Investigation. "The dreadful eight: GRU's Unit 29155 and the 2015 poisoning of Emilian Gebrev." *Bellingcat. https://www. belli ngcat. com/news/uk-and-europe/2019/11/23/thedread ful-eight-grus-unit-29155-and-the-2015-poiso ning-of-emil i an-gebrev/Accessed* 11 (2023).
The Soufan Center, "Beyond the Drones: Confronting Russia's Expanding Hybrid War on Europe," *IntelBrief* (8 October 2025).