סייבר, מודיעין וביטחון

כרך 1 | גיליון 1 | ינואר 2017

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
INCORPORATING THE JAFFEE CENTER FOR STRATEGIC STUDIES
TEL AVIV UNIVERSITY אוניברסיטת תל-אביב

סייבר, מודיעין וביטחון

כרך 1 | גיליון 1 | ינואר 2017

סייבר, מודיעין וביטחון

כתב העת **סייבר, מודיעין וביטחון** מיועד להעשיר, להפרות ולהעמיק את השיח הציבורי באשר למרכיב הצבאי של הביטחון הלאומי בישראל.

המאמרים המופיעים בכתב עת זה, הרואה אור שלוש פעמים בשנה, נכתבים על ידי חוקרי המרכז ואורחיו והדעות המובעות בהם הן של המחברים לבדם.

כתב העת **סייבר, מודיעין וביטחון** רואה אור במסגרת תכנית המחקר 'צבא ואסטרטגיה', המתנהלת במכון למחקרי ביטחון לאומי.

עיצוב גרפי: מיכל סמו־קובץ ויעל ביבר, המשרד לעיצוב גרפי, אוניברסיטת תל־אביב
דפוס: אליניר, פתח־תקווה

כתובת:
המכון למחקרי ביטחון לאומי, רח' חיים לבנון 40, ת"ד 39950, תל־אביב 6997556.
טל' 03-6400400, פקס' 03-7447590, דוא"ל: info@inss.org.il

המאמרים המתפרסמים בכתב העת צבא ואסטרטגיה
מוצגים באתר המכון: www.inss.org.il

ISSN 1565-8880 (מודפס) • ISSN 2307-9444 (מקוון)

דבר העורך

קוראים נכבדים,

כתב העת **סייבר, מודיעין וביטחון** יוצא לאור זו הפעם הראשונה כהמשך ישיר לכתב העת **צבא ואסטרטגיה**, שיצא לאור במהלך שמונה השנים האחרונות. כתב העת החדש יפנה לכותבים ולקוראים המתעניינים בתחום הסייבר או עוסקים בו, במגוון תחומי העשייה, בהם האקדמיה, גורמי מדיניות וממשל, הצבא, גופי המודיעין, הכלכלה והמשפט, וכמובן גורמים המפתחים ומספקים פתרונות לבעיות הקשורות בנושא זה, לצד גורמים בתעשייה המהווים לקוחות של פתרונות כאלה.

כתב העת החדש יעסוק במגוון נושאים, בהם: מדיניות גלובלית ואסטרטגיה בסייבר, רגולציה במרחב הסייבר, אבטחת החוסן הלאומי בסייבר והגנה על תשתיות לאומיות קריטיות. לצד אלה יעסוק כתב העת בנושאים הקשורים בבניין הכוח הקיברנטי על מרכיביו: המשאב האנושי, אמצעי לחימה, תורה, ארגון, הכשרה ופיקוד, וכן בהיבטים של לוחמת סייבר הגנתית והתקפית.

כתב העת יזמין כותבים המתמחים בהיבטים משפטיים ואתיים, וכן בהיבטי השמירה על הפרטיות ויחסי הגומלין של מדינות עם ענקי הטכנולוגיה העולמיים בתחום הסייבר. יוזמנו גם כותבים העוסקים בחשיבה צבאית ואסטרטגית, בהפעלת הכוח הצבאי במרחב הסייבר ובמבצעי תודעה, בניתוח תקריות ומשמעויות במרחב זה, וכן במאזן הרתעה ובניתוח איומים וסיכונים בתחום הסייבר, במודיעין, בשיתוף מידע ובשותפות ציבורית־פרטית לשיפור ההגנה במרחב הקיברנטי. מומחי טכנולוגיה יוכלו לכתוב על התפתחויות טכנולוגיות, מקרי בוחן, שיטות מחקר ופיתוח תהליכים הקשורים בסייבר.

קול קורא למאמרים והנחיות לכתיבה מצורפים בסוף כל גיליון של כתב העת ויהיו זמינים באתר המכון למחקרי ביטחון לאומי.

אני תקווה שתמצאו בכתב עת זה במה ראויה ללמידה ולפיתוח הידע בתחומי הסייבר, המודיעין והביטחון.

ד"ר גבי סיבוני
עורך

שילוביות בארגוני מודיעין – משמעויות תיאורטיות במבחן המעשה

קובי מיכאל, דודי סימנטוב, אורן יואל

המושג שילוביות, השגור בעשורים האחרונים במערכות צבאיות, מודיעיניות ואזרחיות, מייצג שינוי בדפוסי פעולתם של ארגונים בסביבות מורכבות ומאתגרות. סביבות אלו מתאפיינות ברשתיות, שפירושה ריבוי קשרים בין שחקנים וגורמים. ההבחנה הבולטת ביותר בין שיתוף פעולה ובין שילוביות היא תהליך ההיתוך המאפיין את השילוביות. בעוד ששיתוף פעולה משמר את המסגרות הארגוניות המובחנות ואת סמכויותיהן ותחומי אחריותן, בשילוביות מדובר בתצורות ארגוניות חדשות, המייצגות סינרגיה שהיא יותר מחיבור כל היכולות הקיימות.

מאמר זה מתמקד בשילוביות בתחום המודיעיני. זאת, לאור התפתחותן של תפיסות חדשות, שהובילו בשנים האחרונות לשבירת חומות מידור בין ארגוני המודיעין ולהתפתחות דגמי שילוביות בין ארגוני מודיעין לכוחות צבאיים ואזרחיים, לצורך ביצוע משימות מורכבות. המאמר סוקר את ההתפתחות התיאורטית והמעשית של תפיסת השילוביות ומציג ארבעה אבות טיפוס של שילוביות, על בסיס שורת מקרי בוחן מההקשר האמריקאי והישראלי. מניתוח מקרי הבוחן עולה שהשילוביות לא יושמה תמיד באופן הנכון. הצלחתה תלויה במספר מרכיבים, אותם ניתן להגדיר "אקולוגיה". הבולט שבהם הינו חופש ארגוני, היוצר מרחב שבו ניתן ואף מומלץ לאפשר לדרגי העבודה אוטונומיה, שמצידה מאפשרת גמישות ויצירתיות, גם אם תוך חריגה מתבניות העשייה המוכרות.

מילות מפתח: שילוביות, קהילת המודיעין, מודיעין, תהליכי למידה

ד"ר קובי מיכאל הוא חוקר בכיר במכון למחקרי ביטחון לאומי.
דוד סימן טוב הוא חוקר במכון למחקרי ביטחון לאומי.
אורן יואלי הוא מתמחה במכון למחקרי ביטחון לאומי.

מבוא

המושג שילוביות, השגור בעשורים האחרונים במערכות צבאיות, מודיעיניות ואזרחיות, מייצג שינוי בדפוסי פעולתם של ארגונים בסביבות מורכבות ומאתגרות. המדובר בסביבות המתאפיינות ברשתיות, כלומר בריבוי קשרים בין שחקנים וגורמים. ההבחנה הבולטת ביותר בין שיתוף פעולה לשילוביות היא בתהליך ההיתוך. שיתוף פעולה משמר את המסגרות הארגוניות המובחנות ואת סמכויותיהן ותחומי אחריותן; במציאות של שילוביות, מדובר בתהליך של היתוך היוצר תצורות ארגוניות חדשות וסינרגיה שהיא יותר מסך כל היכולות הקיימות. ארגונים לא נוטים בדרך כלל לשילוביות, אלא שבמציאות של משבר ותחרות, בה הם מוצאים עצמם מאוימים וחשופים לכישלון, עלול להתפתח פער ביכולתם לייצר מענה יעיל לאיומים ולאתגרים, דבר שעשוי לחזק את ההעדפה לשילוביות.

מאמר זה מתמקד בשילוביות בתחום המודיעיני לאור התפתחותן של תפיסות חדשות, שהובילו בשנים האחרונות לשבירת חומות מידור בין ארגוני המודיעין, חומות שאפיינו, יחד עם מאבקי יוקרה היסטוריים ותחרות, את היחסים ביניהם בעבר. התפיסות החדשות גם הובילו להתפתחות דגמי שילוביות בין ארגוני מודיעין לכוחות צבאיים לצורך ביצוע משימות מורכבות, ובהמשך – לדגמי שילוביות עם ארגונים מהמגזר האזרחי.

תחילה נציג את מושג השילוביות בהקשריו הרחבים ונסקור את תהליך התפתחות תפיסת השילוביות בממסד הביטחוני האמריקאי, את חדירתה לעולם האזרחי־עסקי ואת השפעותיה החוזרות על עולמות הצבא והמודיעין. בהמשך נעמוד על התייחסותם של מספר חוקרים בולטים למושג השילוביות ונצביע על דגשים שהם שמים עליו. החלק השלישי במאמר יפתח בדיון תיאורטי במושג השילוביות, מתוך ניסיון להרחיב את התשתית התיאורטית הקיימת, ולבסוף נתאר וננתח דגמים שונים של שילוביות בעולם העשייה המודיעיני, בדגש על תחום הפעלת הכוח, בעיקר בארצות הברית, ובאופן מצומצם יותר בישראל. כל זאת, בניסיון לבחון האם יש לשילוביות במודיעין ייחודיות משלה.

לצורך דיון בנושא, מבקש המאמר להתמודד עם השאלות הבאות:

- מהי שילוביות ומדוע נוצר הצורך בה?
- מהם יחסי הגומלין בין מאפייני השילוביות?
- מהם התנאים והחסמים בפני מימוש שילוביות?
- כיצד באה לידי ביטוי השילוביות בעולם המודיעין ומהם הדגמים השונים של שילוביות בעולם זה?

התפתחות רעיון השילוביות

המרחב הצבאי

רעיון השילוביות התפתח בממסד הביטחוני האמריקאי בשלהי שנות השבעים של המאה העשרים.[1] במהלך שנות השמונים, הוגדרה השילוביות באמצעות המושג Jointness, והתייחסה לפעולות, למבצעים, ולארגונים שבהם נטלו חלק גורמים שהיו שייכים לשתי זרועות צבאיות או יותר.[2] עד שנות השמונים, היה המבנה הפיקודי של הכוחות האמריקאים מבוזר בין חמש זרועות, אשר התנהלו באופן עצמאי לחלוטין בכל הנוגע לפיתוח תורות לחימה, הצטיידות ופיתוח כוח האדם. מאבקים סביב תקצוב הכוחות התקיימו בין המטות השונים, דבר שהביא לא פעם להקצאה תקציבית לא עניינית על בסיס יתרון הגודל של כוח מסוים והוביל להגדלה כוללת של תקציב הביטחון.[3] כאשר אחת הזרועות נתקלה בבעיית משאבים, היא העדיפה להתמודד אתה באמצעות שתדלנות בקונגרס על פני שיתוף וניצול משאבים קיימים שכבר פותחו בזרועות אחרות.[4]

ב־1986 נחקק חוק גולדווטר־ניקוֹלְס במטרה להתמודד עם מגוון הקשיים והבעיות שתוארו לעיל.[5] החוק הביא לשינויים מהותיים במבנה הכוחות המזויינים של ארצות הברית, שהתבססו על חיזוק תפיסת השילוביות, והעביר את הסמכות והאחריות לבניין הכוח ממפקדי הזרועות לידי ראשי המטות המשולבים, להקמת הפיקודים הגיאוגרפיים ופיקוד הכוחות המיוחדים. בשנת 1991 פורסמה לראשונה דוקטרינה צבאית אמריקאית, שהתייחסה באופן מפורט ומקיף לרעיון השילוביות, תוך יישום חוק גולדווטר־ניקולס.[6] הדוקטרינה קבעה קווים מנחים לכוחות המזויינים בנוגע לאופן יישום השילוביות במגוון ממדים, וזאת כדי להשיג אפקטיביות אופטימלית.[7]

פרסום הדוקטרינה ויישומה הובילו להקמת מספר מרכזי מחקר, אשר עסקו בפיתוח אסטרטגיות, תוכניות לוחמה ואימונים משולבים. לקחי מלחמת עיראק הראשונה, בה התגלו ליקויי שילוביות בין הכוחות השונים, ופערים בין הדוקטרינות הכתובות שהדגישו פעילות נפרדת ובין הממשקים שחייבו רמה גבוהה של שילוביות, הפכו זרז לפיתוח של דוקטרינות משותפות,[8] שקידמו את תפיסת השילוביות.

המרחב האזרחי

מספר שנים לאחר התפתחות רעיון השילוביות במגזר הצבאי האמריקאי, הגיע רעיון זה למרחב האזרחי־עסקי. תמורות, שהתחוללו בתחומי הניהול וטכנולוגיית המידע הובילו להתפתחויות תיאורטיות ויישומיות משמעותיות. "המהפכה הקיברנטית" אפשרה לארגונים עסקיים לרתום יישומי מחשוב מתקדמים לצורכיהם, הפכה את תהליכי העיבוד למהירים ומקבילים, הוזילה את עלויותיהם

והפכה את המידע והידע לנגישים לכל. במקביל, האצת תהליכי המחקר והפיתוח, המסחר ושיתוף הפעולה בין ארגונים ומדינות, הובילה לירידת קרנם של ארגונים גדולים שנוהלו בצורה היררכית וריכוזית, ולעליית קרנם של ארגונים גמישים (agile) ודינמיים. ארגונים אלה מאופיינים במטה בירוקרטי קטן ובחטיבות עצמאיות המנהלות רשתות של קשרי גומלין. המבנה ההיררכי והריכוזי המסורתי, שאפיין את הארגונים במהלך רוב שנותיה של המאה העשרים, נטש בהדרגה לטובת מבנה מבוזר, שטוח יותר, רשתי ודינמי, המדגיש את קשרי הגומלין בין הצמתים השונים ברשת.[9]

החברות המוצלחות ביותר התגלו כמשתפות הפעולה הגדולות ביותר, ונמצא שנתח גדל והולך מהפעילות העסקית בעולם מתבצע תוך שיתוף פעולה פנים־ארגוני ובין־ארגוני. תהליכי הייצור והפיתוח במגוון ענפים (טכנולוגיה, שיווק, ביו־רפואה וכדומה) נעשו מורכבים מאי פעם, והפכו את ההתמודדות של ארגון בודד עמם לבלתי אפשרית. כך, למשל, פיתוח מערכות מידע בימינו כמעט שאינו מתבצע כתהליך עצמאי נבדל; חברות מתחרות מעדיפות לשלב שירותים חיצוניים במוצר שלהן, על פני פיתוח עצמאי המחייב עמידה בסטנדרטים המתעדכנים ללא הרף.[10]

התפתחויות תיאורטיות של המושג שילוביות

צבי לניר, שעסק בפיתוח רעיון השילוביות בארגונים צבאיים, הגדיר אותה כ"יצירת יכולת מערכתית חדשה, המבוססת על היתוך הנכסים הייחודיים של הגורמים השונים ומעידה על זיקה עמוקה יותר מאשר תיאום או שיתוף פעולה".[11] לניר מדרג את הפעילויות המשותפות באופן היררכי לפי איכותן ולפי עומק ההשפעה המערכתית שהן משיגות בהקשר הצבאי. לשיטתו, יש להבחין בין "תיאום", "שיתוף פעולה" ו"שילוביות", כאשר כל אחד מהממשקים מאפיין רמה שונה של יחסי גומלין.

"תיאום" מוגדר על ידי לניר כ"רמת ממשק המאפשרת להשיג **יעילות** מערכתית באמצעות סטנדרטיזציה של התהליכים". למשל, תיאום במהלך הקרב בין כוח מרתק לכוח הולם, תיאום של זמן, של מקום ושל העצמה. את המושג "שיתוף פעולה" ממקם לניר רמה אחת מעל ה"תיאום". לטענתו, לצורך השגת **אפקטיביות** (רלוונטיות) מערכתית, לא די בחשיבה מערכתית מתואמת. זו אמנם מאפשרת לכוחות לפעול ביעילות, אך אינה מהווה ערובה להשגת האפקט הרצוי מול האויב. לכל מערכה מאפיינים ייחודיים ספציפיים, וכל אויב דורש הבנה מערכתית ייחודית. "החשיבה המערכתית המשותפת" מייצגת את שיתוף הפעולה כממשק, במסגרתו מתבצעת המְשגה של היגיון המערכת היריבה.

מעל למושגים "תיאום" ו"שיתוף פעולה" ממקם לניר את המושג "שילוביות".[12] לשיטתו, תכלית השילוביות היא להבטיח שהאפקטיביות המערכתית תיוותר כזו

גם בראי המציאות המשתנה. מכיוון שהמערכת החיצונית מצויה בסביבה המשתנה ללא הרף, הרלוונטיות ניתנת לשימור רק בהינתן מערכת דינמית, המתבססת על מעורבות של כל הדרגים בתהליך פיתוח הידע. הידע החדש נוצר במפגש בין הישויות השונות ומביא לטרנספורמציה ארגונית מתמדת. המרחב שבו הידע נוצר נמצא בנקודות החיכוך שבין הישויות, בּרִיק שמחוץ לטווח הניתן לכיסוי תפיסתי בלעדי על ידי ישות אחת, ולכן הוא מכונה "No Man's Cognitive Zone". הידע הנוצר במרחב זה הוא, לטענת לניר, "החשיבה המערכתית השילובית".[13]

עפרון רזי ופנחס יחזקאלי מבכרים את השימוש במונחים "שיתוף פעולה בין־מערכתי" ו"פעילות משותפת".[14] לגישתם, השילוביות היא ביטוי לדרגת חופש ארגוני, המאפשר מרחב בו ניתן ואף מומלץ לחרוג מהנהלים, מהחוקים ומתבניות העשייה המוכרות. חופש זה חיוני, מכיוון שבמציאות דינמית, המשתנה במהירות, ארגון בודד חייב לפתח ולרכוש ידע בזמן קצר. לטענתם, ידע רב נוצר בתווך שבין הארגונים, על בסיס קשרי הגומלין. לצורך השגת הידע הזה ופיתוחו, זקוקים הארגונים לשיתוף פעולה עם ארגונים אחרים.[15] הידע יכול להיווצר בכל אחד מהדרגים בארגון, וככל שזרימת המידע טובה יותר, יכולים התהליכים בארגון להיבנות מלמטה למעלה (Bottom Up), ואינם נותרים רק תוצאה של תכנון ריכוזי בדרג הקברניטים (Top Down).

ההגדרות של השילוביות, גם בצבא ארצות הברית וגם בצה"ל, מושפעות כיום מההתפתחויות הרעיוניות שתוארו לעיל, ומהוות רכיב מרכזי בתפיסותיהם. הדבר נכון במיוחד בנוגע לצבא האמריקאי, אשר מאז תחילת שנות התשעים מתייחס ל"Jointness" כאל מרכיב מרכזי באסטרטגיה שלו,[16] תוך הבחנה בין ממדי התפיסה ובין הביצוע.[17] בדומה לכך, גם ההגדרה הצה"לית מבחינה בין שילוביות כפעולה או תהליך כתוצאה של פעולה, ובין שילוביות כתפיסה וכתרבות ארגונית.[18]

ממדי השילוביות ושלביה

לשילוביות, שביסודה היא תהליך למידה מתמשך, שני ממדים עיקריים – הממד התפיסתי והממד הארגוני. עיצובה ומימושה באים לידי ביטוי בשלושה שלבים: העיצוב, התכנון והביצוע.[19] בספרות המקצועית מקובל להבחין בין שני סוגים עיקריים של למידה: למידה פשוטה־סיבתית (causal learning), המתרחשת כאשר אינפורמציה חדשה מובילה לשינוי באמצעים ודרכי פעולה, ולמידה אבחנתית־מורכבת (diagnostic learning), הנובעת מהבנת המתח בין ערכים ומושגים ומובילה לשינוי בהגדרת המטרות והאמצעים להשגתן כאחד. את הלמידה ברמה הפשוטה ניתן להגדיר כלמידה טקטית, שמהותה הסתגלות/התאמה, ואילו את הלמידה ברמה המורכבת ניתן להגדיר כלמידה אסטרטגית, שמהותה הבְּניה מחודשת של תפיסת המציאות. במונחים קוגניטיביים, ניתן להציג את הלמידה

הטקטית כעדכון מבנים קוגניטיביים קיימים, שתוצאתו היא הסתגלות והתאמה, ואת הלמידה האסטרטגית – כשינוי והרחבה של המבנים הקוגניטיביים, שתוצאתה היא שינוי תפיסות ואמונות.[20]

בבסיס תהליך הלמידה האסטרטגית נמצא רעיון ה"עיצוב", כתהליך חשיבתי מופשט, בו מתגבשת המסגרת התפיסתית. בשלב העיצוב, פרדיגמות קיימות מאותגרות, מעודכנות או מוחלפות, וחזון חדש מתעצב. שלב העיצוב נשען על חזון, המתייחס להחלטות עקרוניות "מה ברצוננו לעצב", בבחינת קריאת כיוון כללית המעניקה משמעות לתהליך. החזון "מנותק", לכאורה, מהקרקע המעשית־החומרית, המוגבלת לסך מסוים של משאבים, והוא מאתגר את הארגון לחשוב על פתרונות החורגים מגבולות אלה.

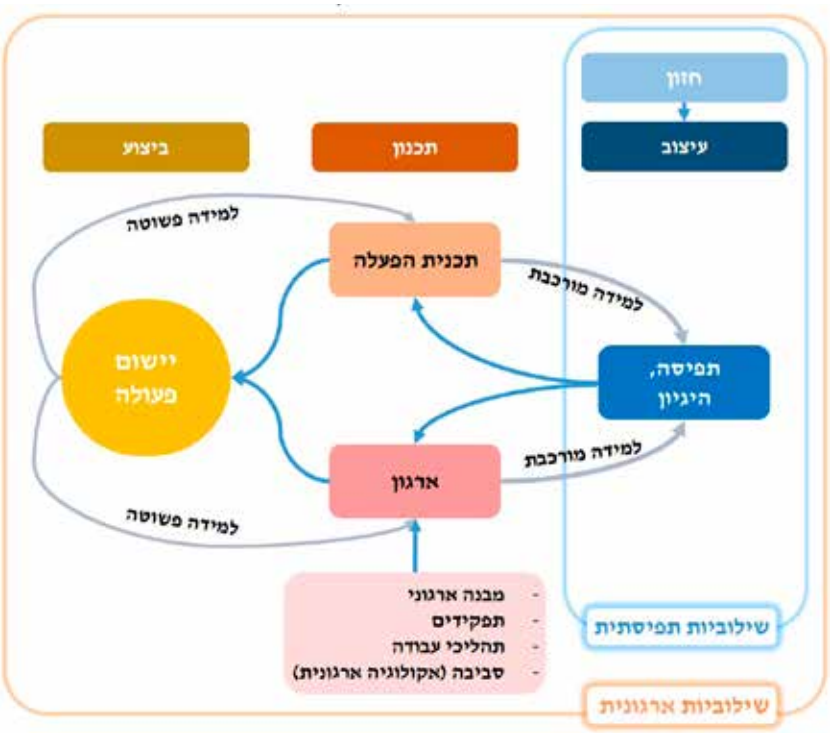
תפיסה הינה אחד מממדי השילוביות, ובו בזמן גם אחד מתוצריה. זאת, מכיוון שהיא אינה מהווה רק שלב או תשומה (כתפיסה ארגונית) בתוך תהליך ארגוני מקיף, אלא היא בעצמה תוצאה של שילוביות קוגניטיבית, במובן של שילוביות בשלב החשיבה המעצבת וגיבוש תפיסה (במובן של הבנייה קוגנטיבית לפירוש המציאות). לכן, נכון יהיה להמשיגה כ"שילוביות תפיסתית". שילוביות תפיסתית באה לידי ביטוי בממשקים ובתהליכי חשיבה משותפים בדרג של מנהלי הארגונים, ועניינה הוא ניתוח וחשיבה מחודשת על האתגרים הניצבים בפני הארגונים והגדרת ערכים משותפים. המפגש ביניהם נושק למרחב הבין־ארגוני, המאפשר יצירת ידע חדש במרחבים שנותרו מחוץ למרחבי החשיבה הארגוניים (No Man's Cognitive Zone). התפיסה בשלב העיצוב מתגבשת באמצעות תהליכי למידה דיאגנוסטית־אסטרטגית, מכיוון שמהותה היא אתגור פרדיגמות קיימות ועדכונן או החלפתן.

לעומת השילוביות התפיסתית, שילוביות ארגונית באה לידי ביטוי בממשקים ובעבודה המשותפת בין ארגונים. היא כוללת מבנים ארגוניים משותפים, תהליכי עבודה משותפים ואקלים ארגוני ("אקולוגיה"), המאפשרים למספר ארגונים/מסגרות לפעול באופן מסונכרן הממצה את היכולות של כל ארגון ויוצר שלם שהוא יותר מסך חלקיו ומסייע לקדם מטרות משותפות. שילוביות ארגונית נדרשת גם לבניין הכוח בהיבטים של הכשרת כוח אדם ובניית תשתיות ארגוניות, המסייעים למיצוי יעיל יותר של משאבי הארגונים ויכולותיהם, כדפוס קבוע ושיטתי בהתמודדות עם האתגרים המורכבים בפניהם הם ניצבים. שילוביות ארגונית באה לידי ביטוי מובהק יותר בשלב התכנון, בתוך מסגרת פרדיגמטית קיימת שהומשגה בשלב ה"עיצוב". הלמידה בשלב זה אינה "למידה מורכבת", אלא "למידה פשוטה", אשר מטמיעה אינפורמציה חדשה אל תוך מסגרות חשיבה קיימות.

השילוביות הארגונית מאפשרת זיהוי של האזורים הארגוניים בהם נדרשים שינויים. שינויים אלה יכולים להוביל להקמה, לפירוק או להתמזגות של מבנים ארגוניים, להגדרת תפקידים חדשים או תפיסות מקצועיות חדשות המשפיעות

על תצורת עבודתם של בעלי תפקידים קיימים, ולאפיון המרכיבים הסביבתיים הנדרשים ליצירת אקולוגיה שילובית. השילוביות הארגונית נדרשת גם לשלב הביצוע והיישום של התוכניות שגובשו בשלב התכנון. שלב הביצוע מהווה נדבך מהותי בשילוביות הארגונית, מכיוון שהוא מייצג את מבחן הרלוונטיות בהתמודדות עם האתגרים. גם בשלב זה הלמידה המתבצעת הינה "למידה פשוטה", מכיוון שמהותה היא בהתאמת האמצעים ודרכי הפעולה לאתגר נתון ועל בסיס תפיסה/פרדיגמה קיימת.

התרשים שלהלן מתאר את ממדי השילוביות (התפיסתית והארגונית), כפי שהם באים לידי ביטוי בכל אחד מהשלבים השונים (עיצוב, תכנון וביצוע), תוך התייחסות למאפייני תהליך הלמידה בכל אחד מהשלבים. השילוביות התפיסתית ממומשת בשלב ה"עיצוב", ואילו השילוביות הארגונית נדרשת בכל שלבי התהליך:



תרשים מס' 1: השילוביות כתהליך למידה – ממדים ושלבים

כפי שניתן לראות בתרשים, כל אחד משלבי השילוביות מחולל תהליכי למידה, המאפשרים את מימוש השלב העוקב. השלב הסופי של השילוביות – שלב

הביצוע – הוא השלב בו צפויים לעלות הבעיות והאתגרים בכל הנוגע למבחן היישום. במקרים בהם ההתמודדות עם בעיות ואתגרים היא ברמה של שינוי בתוכנית, באמצעים או בהיבטים הארגוניים, מדובר בהתאמה שהיא תוצאה של "למידה פשוטה". התמודדות המחייבת בחינה מחדש של המסגרת התפיסתית הרחבה מייצגת תהליך שהוא במהותו "למידה מורכבת".

מעבר ממשבר לרלוונטיות וחשיבות האקולוגיה הארגונית

את השילוביות ניתן למסגר כתהליך המתחיל ממשבר, מתפתח לפיתוח תפיסתי, ארגוני ואופרטיבי, ומוביל לשיפור הרלוונטיות של הארגון מול האתגרים הקיימים בסביבת פעולתו. הצלחת התהליך מותנית גם באקולוגיה של הארגון ושל סביבתו.

שלב ראשון – משבר

המשבר הוא גורם המחולל תהליכים ארגוניים המאפשרים לפתח את השילוביות כתפיסה וכדרך פעולה. המושג משבר מוגדר בספרות כמצב שבו מופיע שינוי עקב אירוע פתאומי, או שינוי חד במגמה ובכיוון או בזמן. במקרה כזה נדרשת הערכה מחדש של המצב, כלומר שיקול מחודש של האיומים, הערכים והמטרות של השחקן המעורב. השינוי יכול להיות בסביבה הפנימית או החיצונית, והאיום הינו על מטרות בעלות קדימות גבוהה או על ערכים ארגוניים בסיסיים.[21] תחילת המשבר היא בתחושת "חוסר אונים אסטרטגי", כביטוי לפער רלוונטיות של הארגון לאתגרי סביבתו, כלומר חוסר יכולת להתמודד עם בעיות חדשות ולעצב את המענה לאתגרים על בסיס התפיסה, המשאבים והיכולות הקיימים של הארגון.[22]

שלב שני – למידה מערכתית

לאחר הכרה במשבר בו הארגונים מצויים, או נוכח רצון להימנע ממשבר אפשרי, נדרשים תהליכי למידה מורכבת במטרה לעצב את המסגרת התפיסתית הרלוונטית להתמודדות. אלה נדרשים מכיוון שתהליכי למידה פשוטים, שנועדו לאפשר התאמת דרכי פעולה על בסיס תפיסה קיימת, לא הצליחו למנוע את פער הרלוונטיות שנוצר בגין חוסר הרלוונטיות של התפיסה הקיימת. כאשר תהליכי החשיבה והלמידה נערכים במשותף על ידי מספר גורמים ממספר ארגונים, תוך הבנה שתשתית הידע והפרדיגמה בכל ארגון כשלעצמו אינן מספיקות כדי לפתח תובנות משמעותיות, ניתן להגדירם כשילוביות תפיסתית.

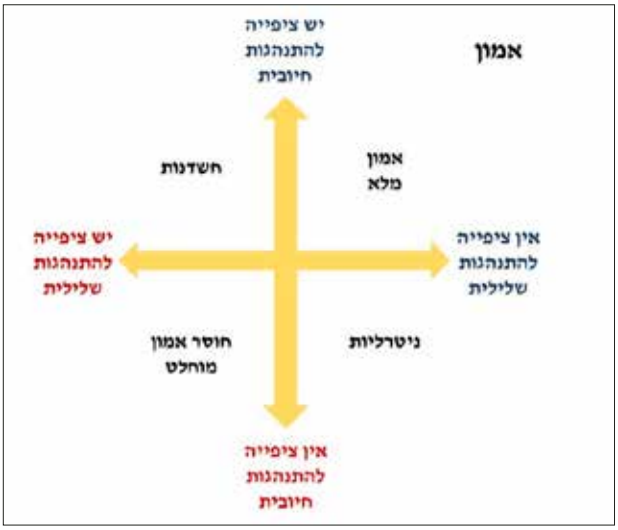
תהליך הלמידה בוחן מחדש את הארגון, את מטרותיו, את האפקט שהוא מבקש להשיג ואת הסביבה שבתוכה הוא פועל. השילוביות הארגונית עשויה להתגלות ככיוון אפשרי לפתרון המשבר בתהליך, אם כי לא הכיוון היחיד. לשם קידומו של

הפתרון השילובי עליו להיתפס כבעל פוטנציאל להעניק תועלת משותפת (payoff), העולה על התועלת שתופק כתוצאה מפעילות נפרדת, לא שילובית.

שלב שלישי – תהליכים ארגוניים ואקולוגיה ארגונית

הצלחת התהליכים ותוכנית הפעולה, שגובשו מתוך התפיסה החדשה, מושפעת ממספר מאפיינים ותנאים באקולוגיה הארגונית והבין־ארגונית, דוגמת נורמות עבודה, דינמיקה שהארגונים מייצרים, אמון בין השחקנים, וכן ממידת האוטונומיה המתאפשרת לדרגי העבודה. למרות שייתכנו מקרים בהם תהליכי האינקובציה של האקולוגיה הארגונית התחילו מלמטה למעלה, מתחייבים השלמה ומיסוד של אקולוגיה ארגונית חדשה מלמעלה למטה. ללא תמיכה, עידוד והרשאה של הדרג הניהולי בארגון, לא ניתן יהיה לעצב אקולוגיה ארגונית חדשה.

שילוביות יכולה להתאפשר רק כאשר המידע זורם באופן חופשי בין הארגונים ובתוכם. לכן, על דרגי הניהול להעניק לדרגי העבודה אוטונומיה לפתח ממשקים שילוביים ולאפשר זרימת מידע פתוחה וחופשית בתווך הבין־ארגוני. הצדדים הנוטלים חלק בממשק שילובי יסכימו לקחת את הסיכון בשעה שיש להם ציפיות להתנהגות חיובית מצד השותפים, ואין להם ציפיות להתנהגות שלילית מצד אותם שותפים. אמון הוא פונקציה של ציפיות ונכונות לקחת סיכונים.[23] במצב בו לצדדים אין היסטוריה משותפת, הם אינם יודעים מה ניתן לצפות מן הצד השני, ונקודת המוצא ליחסיהם תהיה ניטרלית. מצב כזה מחייב בנייה הדרגתית של אמון, באמצעות העצמת התנהגויות חיוביות ותִגמולן.



תרשים מס׳ 2: אמון כפונקציה של ציפיות[24]

השילוביות חייבת לבוא לידי ביטוי בנורמות העבודה ובסביבה המעניקה יחס אוהד לשיתוף מידע, לפיתוח קשרים ולתהליכים משותפים בהם נטל העבודה מחולק בין מספר גורמים. תודעת השילוביות מושפעת ממידת האוטונומיה המוענקת לעובדים שפועלים מטעם הארגון במסגרת שילובית. הניסיון מוכיח שבמקרים בהם עובדים נהנו מאוטונומיה, היה קל יותר לבנות סביבת עבודה של אמון בין הצדדים, וכתוצאה מכך גם יכולת לעבוד במשותף.[25]

השילוביות מחייבת ארגונים לוותר, במידת מה, על זהותם המקורית וליצור זהות מקצועית חדשה אל מול משימה. לכן, לצד היתרונות הרבים שיש להתארגנות רשתית מול אתגרים רשתיים, חשוב להקפיד ולמנוע נתק בין הזהות המקצועית המקורית של הפרטים בארגון החדש לבין ארגון האם שלהם, האמון על הכשרתם, קידומם וזהותם המקצועיים.

תרשים מס׳ 3: תהליך השילוביות – ממשבר לרלוונטיות

שילוביות בגופי מודיעין

התפתחות השילוביות בארגוני מודיעין היא תוצאה של למידה מתהליכים דומים בעולמות הצבאיים והעסקיים, וגם תוצאה של שינויים מהותיים באופי האתגרים המודיעיניים והשינויים הטכנולוגיים שאִפשרו זאת. כך, למשל, מתאר את התמורות הללו איתי ברון, אשר כיהן כראש חטיבת המחקר באגף המודיעין של ישראל: "בולטת המרכזיות של טכנולוגיית המידע בתקופתנו [...] בעולם כזה ניתן לאסוף מידע בכמות ובאיכות שלא ניתן היה לאסוף בעבר, לנתח ולעבד את המידע בקבועי

זמן שלא היו אפשריים [...] העולם החדש יוצר 'הצפה' במידע, מוביל לתחרות עם ספקי מידע וידע אחרים וחושף נקודות תורפה".[26]

שינויים בסביבה הטכנולוגית ובאתגרי המודיעין הביאו לתמורות באופי עבודת המודיעין ובתפוקות המצופות ממנה. ארגוני מודיעין נדרשים כיום לבצע מעקב אחר גופים "נעלמים" ולהפליל אותם, וכן לעקוב אחר תהליכים מתהווים, שבבסיסם לא היה תכנון מוקדם ואף לא הגדרה של מטרה ברורה מצד מקבלי ההחלטות באחד הצדדים.[27] כמו כן, קבועי הזמן העומדים לרשותם של אנשי מודיעין להתמודדות עם אירועים התקצרו משמעותית (למשל, כתוצאה מהשימוש בכלי מלחמה שהפעלתם אינה מחייבת היערכות מיוחדת, כמו הנשק תלול מסלול), כשבמקביל לכך הביאה "מהפכת המידע" את איש המודיעין לַצורך להתמודד עם היקפי מידע וידע הגדולים משמעותית מאלה להם נדרש בעבר.[28]

לדברי גורם ממלכתי בכיר המקורב לקהילת המודיעין הישראלית (דברים שנאמרו בפורום מודיעיני סגור) בשנים האחרונות חל שינוי תודעתי בקהילה זאת. במסגרת השינוי בוצעו מהלכים ארגוניים המשלבים מספר ארגונים, הונחלה תפיסה חדשה של "שבירת חומות" בין האיסוף ובין המחקר ונוצרו מרחבים מודיעיניים משותפים המאפשרים נגישות לכל שותף לפי צרכיו.

מנגנונים מחוללי שילוביות במודיעין – מסגרות ניהול של המערכת המודיעינית

מסגרות לניהול הקהילה המודיעינית מסייעות לחולל שילוביות באמצעות סנכרון בין הארגונים השונים בקהילה. אלה מצויים לא פעם בתחרות זה מול זה ובמאבק על משאבים ויוקרה ונוטים להתנהל בדרך בזבזנית ובתחרות הגורמות לכפילות ויתירות, שמצדן פוגעות בתרומתה הפוטנציאלית של הקהילה.[29] גוף־על עשוי לקדם את השילוביות בשני ממדיה: התפיסתי והארגוני. ביכולתו של גוף כזה לפעול בתהליכי Down Top ליצירת סטנדרטים כוללים של נורמות עבודה ולהנחות על הקמת מסגרות משימתיות שילוביות, שיאפשרו למספר גורמים שונים לעבוד במשותף.

דוגמה למסגרת לניהול קהילת מודיעין הינה Office of the Director of National Intelligence (או בקיצור המוכר DNI), שהוקם בארצות הברית לאור לקחי ועדות החקירה שהוקמו לאחר אירועי 11 בספטמבר 2001. עד אז עמד ראש ה־CIA בראש קהילת המודיעין האמריקאית. למסגרת החדשה ניתנו הסמכויות לגבש את מדיניות המודיעין של ארצות הברית, לנהל את תוכנית המודיעין ואת תקציבי המודיעין, להמליץ על מינויי בכירים בסוכנויות המודיעין ולהקים צוותים משותפים לשירותי המודיעין. ה־DNI מקדם תוכניות להגברת השילוביות בין גורמי המודיעין האמריקאי ופועל להטמעת סטנדרטים לביצוע הסנכרון

ביניהם. דוגמה לפעילות ה־DNI בהקשרי שילוביות ניתן לראות ב"תוכנית 500 הימים" משנת 2007. תכליתה המוצהרת של התוכנית הייתה לחזק את עקרונות השילוביות בקהילת המודיעין האמריקאית במגוון מישורים.[30] התוכנית נכתבה כחלק מיישום אסטרטגיית המודיעין הלאומית של ארצות הברית, המתעדכנת מדי כמה שנים ומציבה את השילוביות ואת האינטגרציה המערכתית כיעדים ארגוניים מרכזיים.[31] השילוביות מוגדרת בתוכנית כמכפיל כוח החיוני לתפקודם של כל תחומי העשייה והפעילות המודיעינית (טכנולוגיית מידע, שפה, ניתוח והערכה וכדומה). התוכנית דנה ביצירת סטנדרטים קהילתיים להפצה של מידע ומסמכים, לאבטחת מידע ולנגישות למקורות, תוך בניית ממשק אחיד ומשותף לשליפה ולעבודה מול פריטי ידע.

עיקרון נוסף שמקדם ה־DNI ומוזכר בפרסומי אסטרטגיית המודיעין האמריקאית נוגע לניהול מוכוון משימה.[32] תפיסה זו גורסת שהמשימה היא הרכיב שיכריע את צורת המבנים שבהם תתארגן העשייה המודיעינית, מבלי שההבחנות הפורמליות בין תחומי מומחיות ובין ארגונים שונים יהוו מכשול בפני ביצוע רה־ארגון ובפני יצירת מסגרות אינטגרטיביות מכוונות משימה. עיקרון זה מדגיש את הצורך בקביעת משימות קהילתיות כעיקרון מארגן וכבסיס לתכנון וביצוע משותף, תוך ניצול מיטבי של המשאבים והיכולות הייחודיות של כל ארגון והפחתת החסמים הנובעים מהנבדלות הארגונית.

כמו בארצות הברית, גם בישראל מנסים גופי המודיעין לקדם סדר יום של שילוביות ושל "שבירת חומות". צעד מרכזי בהקשר זה היה הקמתה ב־2007 של חטיבת הפעלה באגף המודיעין בעקבות לקחי מלחמת לבנון השנייה, כגלגול מודרני של מחלקת איסוף. ייעודה של החטיבה הוא ליצור חיבור טוב יותר בין מערכי המודיעין השונים באמ"ן, וכן חיבור טוב יותר בין המודיעין ובין דרגי השטח המבצעיים. חטיבת ההפעלה יועדה לשמש מעין מִפקדת מבצעים לכל גופי אגף המודיעין, ובידיה הופקדו הסמכויות לנהל את מִבצעי היחידות המיוחדות הכפופות לאמ"ן, להקצות משאבי איסוף בהתאם לתמונת המצב המודיעינית המשתנה ולהוביל תהליכים משותפים.[33] לקחי מלחמת לבנון השנייה הביאו את החטיבה לגבש תפיסת מידור חדשה, שאפשרה הטמעה מהירה ואיכותית יותר של המודיעין בקרב הכוחות הלוחמים. מרחב נוסף המסייע לקידום השילוביות הוא המרחב ההכשרתי. כך, למשל, בסוף שנות השבעים נוסד הקורס הבין־שרותי הבכיר למודיעין (הקב"ש), שמטרתו העיקרית הייתה לעודד שיתופי פעולה באמצעות העמקת ההיכרות בין בכירי קהילת המודיעין. בשנים האחרונות חל שינוי עמוק בקורס זה והוא ממוקד ביצירת ואיפשור שילוביות הן בדרג הניהול והפיקוד הבכירים (ראשי מחלקות) והן בדרגי עבודה בתחומים מקצועיים.[34]

לתמורות טכנולוגיות בעידן המהפכה הקיברנטית יש השפעה חשובה על האקולוגיה הנדרשת לקיומה של שילוביות בין גופי מודיעין שונים. השינויים שהתחוללו בעולם הניהול ובתחומי מערכות המידע זימנו לגופי המודיעין אתגרים חדשים לצד הזדמנויות חדשות. הביטוי לכך בעולם המודיעין הוא ביצירת ממדים חדשים לשיח בין גורמי המחקר והאיסוף דרך התווך הרשתי. דוגמאות לכך הן פלטפורמות "ויקי" המתבססות על רעיון של "ויקיפדיה" – אנציקלופדיה פתוחה בה הערכים נוצרים ונערכים על ידי המשתמשים, התורמים לה בהתאם למומחיותם – או פלטפורמות מבוססות רשת חברתית, בהן מגוון גורמים העוסקים בסוגיה מסוימת יכולים לדון ולתרום את פרשנותם ותובנותיהם הייחודיות. השיח ברשת החברתית המודיעינית מנטרל חסמים הנוגעים לשיוכם הארגוני של המשתתפים או לדרגתם, אשר לרוב תופסים משקל בשיח שאינו רשתי.[35] בהקשר זה מציעים חוקרים אמריקאיים את המושג "סביבה מודיעינית שיתופית" במאפייני הרשתות החברתיות, הכוללת פגישות וירטואליות, כתיבה משותפת של "מסמכים חיים" (כלומר, כאלה שניתן לעדכנם כל העת), בלוגים ועוד.[36]

דגמי השילוביות במודיעין במבחן המקרים האמריקאי והישראלי

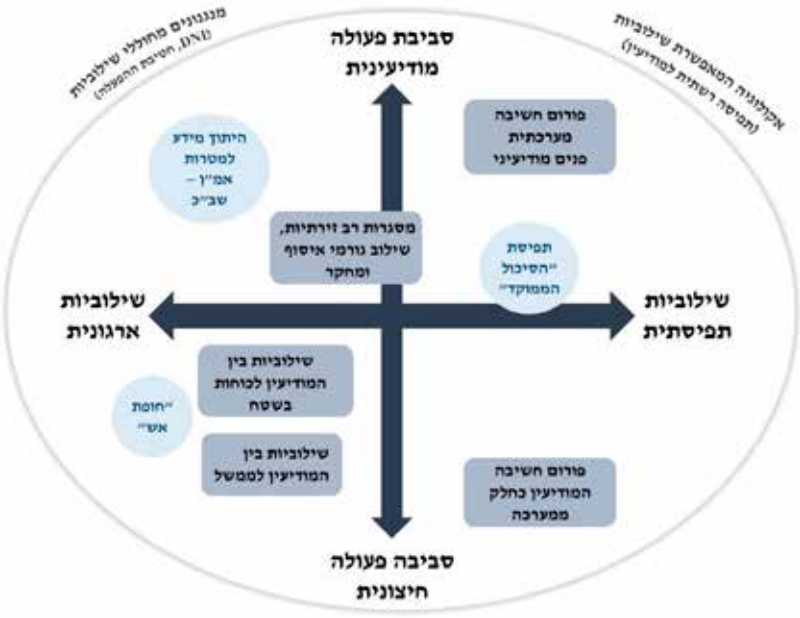
הצגת השיפולוגיה

את דגמי השילוביות ניתן לאפיין באמצעות שני משתנים: סביבת הפעולה והמהות. שני מאפיינים אלה מאפשרים טיפולוגיה של ארבעה אבות טיפוס. את המשתנה הראשון ניתן לתאר באמצעות ציר, שהקצה האחד שלו מייצג סביבת פעולה מודיעינית מובהקת, והקצה האחר מייצג סביבת פעולה מעורבת/מרובת גורמים (שהמודיעין הוא רק אחד השחקנים בה). בסביבת הפעולה המודיעינית נעשה שימוש במתודולוגיה מודיעינית ובמושגים מודיעיניים, והמידור מוגבל או אינו קיים. לעומת זאת, בסביבת פעולה מעורבת, המודיעין הוא שחקן אחד מני כמה שחקנים, הפועלים במתודולוגיות שונות ומתאפיינים בזהויות ארגוניות שונות. המודיעין נדרש אז להסתגל לכללי משחק חיצוניים, להתאים את עצמו אליהם מבחינה תפיסתית ומבצעית ולהקפיד על כללי המידור. המשתנה השני מתואר באמצעות ציר, שהקצה האחד שלו מייצג את המהות התפיסתית של השילוביות, והקצה האחר – את המהות הארגונית. הצלבת צירי המשתנים יוצרת מטריצה המייצגת ארבעה אבות טיפוס לדגמים של השילוביות המודיעינית:

- אב הטיפוס הראשון מייצג שילוביות תפיסתית, שמהותה חשיבה ולמידה משותפת של המערכה המודיעינית על ידי מספר שחקנים ממגוון ארגוני מודיעין, וגיבוש תפיסות מודיעיניות אחרות.

- אב הטיפוס השני עוסק גם הוא במסגרות שילוביות לחשיבה ולעיצוב המערכה, אלא שבמקרה זה ארגוני המודיעין מייצגים שחקן אחד מתוך קבוצת שחקנים, כשהדגש בתהליכי החשיבה והלמידה המשותפים הוא פיתוח ידע על המערכה כמכלול רחב יותר.
- אב הטיפוס השלישי מייצג שילוביות פנים־מודיעינית, הנערכת בין מסגרות המחקר, האיסוף, הסייבר והטכנולוגיה. שילוביות זו קשורה לליבת העשייה המודיעינית, והיא זו שמאפשרת למודיעין להפיק את המרב מתוך יכולותיו.
- אב הטיפוס הרביעי מייצג שילוביות בין המודיעין ובין מערכות וארגונים לא־מודיעיניים.

במאמר זה נרחיב לגבי שני אבות הטיפוס האחרונים.



תרשים מס׳ 4: טיפולוגיה של דגמי השילוביות

דוגמאות ליישום דגמי השילוביות המודיעינית והמודיעינית־מבצעית, מסגרות רב־זירתיות, שילוביות בין גורמי איסוף ומחקר

בקהילת המודיעין האמריקאית ניתן למצוא מגוון דוגמאות למסגרות מודיעיניות משולבות. הסיקור המחקרי הרחב ביותר ניתן ככל הנראה ל־National Counterterrorism Center (NCTC), שהוקם בעקבות המלצותיה של ועדת

החקירה לאירועי 11 בספטמבר 2001. הוועדה התמודדה עם הצורך ליצור תמונה מודיעינית אינטגרטיבית של איומי הטרור השונים ולהקים מסגרות מחקריות שירכזו את תמונת המודיעין המתגבשת בכלל גופי קהילת המודיעין האמריקאית. ה־NCTC מייצג את ההבנה כי הטרור מהווה זירת התמודדות ייחודית, המשלבת בין הפנים והחוץ, וכי לא ניתן לסכל טרור באמצעות קהילת מודיעין שאינה אינטגרטיבית. זאת, בשונה מהדיכוטומיה שאפיינה את סוכנויות המודיעין האמריקאיות עד אותה העת.

ה־NCTC כולל חטיבה גדולה למחקר מודיעיני, ובה ענפים המחולקים על פי זירות האיומים השונות. כל ענף כזה מורכב מנציגים ממספר סוכנויות ביון אמריקאיות.[37] ה־NCTC מקבל את המודיעין הגולמי המופק מכל אחת מסוכנויות הביון של ארצות הברית, ועל חוקריו מוטלת המשימה לבנות תמונה מקיפה והוליסטית של איומי הטרור השונים.

ממחקר שנכתב על ידי חוקר של CIA[38] שעבד ב־NCTC במשך כשנתיים, עולה כי הסביבה הארגונית והפוליטית שבה פועל ה־NCTC מְמַצבת אותו בעמדת נחיתות, כארגון שיוקרתו ומעמדו אינם משתווים לאלה של ארגוני האם השולחים את נציגיהם אליו.[39] ארגוני ביון ותיקים, דוגמת ה־CIA, מטפחים במשך שנים רבות מסורת של גאוות יחידה, המשרתת את המצוינות הפנים־ארגונית, אך מקשה על שילוביות עם ארגוני ביון אחרים, החיצוניים לארגון[40] עובדים המגיעים מסוכנויות הביון השונות של ארצות הברית לעבוד ב־NCTC משמרים באדיקות את זהותם הארגונית המקורית.

לאחרונה בוצע שינוי מבני מקיף ב־CIA שהוביל להקמת עשרה מרכזי משימה גיאוגרפיים ונושאיים, כאשר בכל מרכז פועלת נציגות של כל המקצועות המודיעיניים (מבצעים חשאיים, מחקר, טכנולוגיה וכדומה).[41] שינוי זה מהווה דוגמה לארכיטקטורה חדשה של ארגוני מודיעין, הנדרשת לאור הצורך בהתמודדות משולבת עם האתגרים המודיעיניים הנוכחיים. הוא אינו מהווה דוגמא לשילוביות בין ארגונית אלא לשילוביות פנים ארגונית.

"מרכזי היתוך" – שילוביות בין המודיעין למגזרים ממשלתיים ואזרחיים

"מרכזי היתוך" ("Fusion Centers") הינם חדרי מצב המשמשים את רשויות השלטון במדינות שונות לצורך שילוב פעילות של זרועות הממשל והמודיעין. בארצות הברית, מרכזים אלה פועלים בשיתוף עם המגזר האזרחי ומשרדי ממשלה נוספים, כחלק מהמאמץ לסכל ולהתריע מפני טרור, פשיעה ואסונות.[42]

בעשור שלאחר אירועי ספטמבר 2001 הוקמו בארצות הברית עשרות "מרכזי היתוך", אשר פעלו ברמה המחוזית, המדינתית והפדרלית.[43] מרכזים אלה כפופים למשרד להגנת המולדת (DHS) וכוללים נציגים מסוכנויות ממשלתיות, מהמגזר

האזרחי, ולעיתים גם גורמי צבא. בכל המרכזים קיימת נציגות מטעם סוכנות מודיעין אמריקאית אחת לפחות, בנוסף לנציגויות מטעם מערכות החוק והמשפט, המשטרה וגופי ביטחון הפנים (FBI), רשויות השלטון המקומיות, הרשויות המפעילות תשתיות לאומיות, וגם מהמגזר העסקי הפרטי. נוכחותם של גורמים מהמגזר הפרטי נועדה לאפשר ל"מרכזי ההיתוך" להשיג נגישות לנתונים של חברות פרטיות.[44] המרכזים מקבלים מידע ממגוון מקורות ומייצרים תמונה אינטגרטיבית, המאפשרת להם להתריע, לסכל, לחקור ולהעריך איומי טרור שונים, לרוב ברמה המדינתית.[45] שילוב הנתונים ממגוון מקורות מודיעיניים, משפטיים וממשלתיים מאפשר לגבש הערכות ולפרסם מסמכים עיתיים. כאשר מדובר באירוע "מתגלגל", "מרכזי ההיתוך" אחראים לתמוך בגורמים המבצעיים על ידי הספקת המידע הרלוונטי לאירוע וחיבור בין הגורמים המבצעיים השונים.[46]

הרעיון המארגן היה לחבר בין יכולותיהן של זרועות הממשל השונות, מתוך הבנה שההתמודדות עם טרור ופשיעה אפשרית רק על ידי יצירת חיבור כזה. עם זאת, בעשור החולף נמתחה ביקורת על עבודת "מרכזי ההיתוך", וועדות חקירה אף בחנו את פעילותן.[47] הביקורת התמקדה ברמה המקצועית הנמוכה של חלק מהדוחות שהופקו על ידי המרכזים, שהביאה להצפת קהילת המודיעין וביטחון הפנים האמריקאית בידיעות על פעילות אזרחית שלא נגעה כלל לטרור.[48] בעיה נוספת שהוזכרה במספר דוחות על "מרכזי ההיתוך" היא רמת האמון הנמוכה בין חברי הצוות השונים של המרכזים. אחת הסיבות לבעיה זו היא מגבלת השימוש בחומרים ברמת סיווג גבוהה, אשר לרוב ניתנים לחשיפה רק בפני גורמים מודיעיניים.[49]

שילוביות בין המודיעין ליחידות מבצעיות

בשונה מ"מרכזי ההיתוך" לעיל, הממשק המודיעיני־מבצעי נוגע לתהליכים מבצעיים ומודיעיניים בזירת הלחימה. ממשק זה מתבצע הן בשלבי האיסוף, העיבוד וניתוח המידע, והן בשלבי הפעילות המבצעית עצמה. הימצאות המודיעין במרחב הפעולה או בסמיכות לו מחברת אותו לשטח ומסייעת בהפקת מידע רלוונטי לביצוע פעולה מבצעית ובהטמעת המודיעין הנאסף בקרב הכוחות טרם הלחימה ובמהלכה.

המקרה האמריקאי

בצבא ארצות הברית פועלים צוותים המכונים (Joint Inter-Agencies Task Forces – JIATFs).[50] צוותים אלה הוקמו במטרה לשפר את יכולת המודיעין ומערכות הביטחון האמריקאיות בהתמודדות עם מליציות חמושות ותאי טרור המוטמעים בסביבה האזרחית. מדובר בצוותים שהורכבו מנציגים ממספר סוכנויות מודיעין

ויחידות מבצעיות ומנהליות שנכחו במרחב מסוים בו פעל הצבא האמריקאי. הנחת העבודה בהקמתם הייתה שאין ביכולתה של סוכנות אחת לספק תמונה מהימנה ומלאה דיה של גורמי טרור ותאים חמושים. רעיון ה־JIATFs מתייחס גם למסגרות הממוקמות במטה וגם למסגרות הממוקמות בשטח.

עדויות לפעילות מוצלחת של הצוותים הבין־סוכנותיים ניתן למצוא בבוסניה ובעיראק, שם היא מיוחסת לשילוביות שאפשרה לאתר חוליות טרור ולסכל פיגועים.[51] מניתוח פעילות הצוותים באזורים אלה, ניתן ללמוד, שהשהות המשותפת של נציגי היחידות השונות באזור רווי סכנה ומרוחק מיחידות האם הייתה גורם מרכזי שאִפשר הסרת חסמים, פתיחות ונכונות לשיתוף פעולה. ככל שהצוותים הבין־סוכנותיים היו קטנים יותר, נוצרה אינטימיות רבה יותר בין השותפים, וזו אפשרה תהליכי עבודה יעילים ותוצרים משמעותיים יותר.

אחד הגורמים המשתתפים בצוות הבין־סוכנותי נדרש להיות המוביל של המשימה, ובידיו ניתנת הסמכות לנהל את העשייה. ההכרעה מי יהיה הגורם המוביל עשויה להיקבע לפי גודל הסוכנות אותה הוא מייצג, או היקף התרומה של אותה סוכנות למשימה המדוברת. זאת, מתוך הנחה שגודל התרומה או חשיבות הארגון יעניקו לגיטימציה ותוקף להיותם הגורמים שיובילו את הצוות המשותף.

המקרה הישראלי במבחן ההתמודדות עם הטרור הפלסטיני

מאז תחילת שנות האלפיים ניצבים המודיעין הצבאי ושירות הביטחון הכללי של ישראל בחזית המאבק בטרור הפלסטיני. המשבר שחוותה ישראל בהתמודדות עם טרור המתאבדים של האינתיפאדה השנייה הביא להתפתחותה של שילוביות מודיעינית ומבצעית ברמת אפקטיביות גבוהה ביותר, אשר מופעלת מאז הן בשגרה והן במלחמה. במהלך שנות העימות הארוכות עם הפלסטינים הפך המודיעין הצבאי מגורם ה־מוּן על סיוע לקבלת החלטות, לגיבוש אסטרטגיה ולעיצוב מערכות צבאיות, לכלי מבצעי משמעותי,[52] המתמקד ב"סגירת מעגלים" מבצעיים כמשימה ראשית.[53]

המושג שרווח בקהילת המודיעין הישראלית בשנות התשעים להסדרת היחסים בין אמ"ן לשב"כ היה "מגנה כרטה". במידה רבה, ניתן לראות ב"מגנה כרטה" ביטוי הפוך לגישת השילוביות, שכן היא שרטטה גבולות אחריות בין שירותי המודיעין, הגדירה מרחבי פעילות וסמכויות ולא יצרה מרחב פעולה משותף. לאחר שנים ספורות של מאבק משותף בטרור, אשר תואר כ"שנים של מעצרים המוניים וסיכולים ממוקדים", התקרבו גופי הקהילה, ובמיוחד אמ"ן ושב"כ, אלה לאלה,[54] והחלה להיווצר ביניהם אווירה של אמון וקירבה, בניגוד לאווירת המחלוקת שאפיינה את יחסיהם עד אז.

יובל דיסקין, אז סגן ראש השב"כ, הוביל את "תפיסת הסיכול המשולב", שתכליתה הייתה מיצוי היכולות המודיעיניות והמבצעיות לסיכול ממוקד. תחת הובלתו ביטל השב"כ מידור שהיה קיים בין היחידות המרחביות של הארגון, וזאת נוכח העובדה שהתארגנויות הטרור חצו גבולות מרחביים שחייבו התייחסות כוללת אל המערכת הפלסטינית. דיסקין גם קידם את ערוצי ההידברות והתיאום עם יחידת הסיגינט המרכזית של חיל המודיעין (יחידה 8200) ושילב את נציגיה בחדרי הפיקוד של מרחבי השב"כ, באופן שאִפשר להשתמש בסיגינט ל"סגירת מעגלים" מבצעיים. כך הוא גם פעל בנוגע ליחידות מבצעיות של צה"ל שפעלו בשטחי יהודה ושומרון ורצועת עזה, וכן מול חיל האוויר. הסרת חסמי מידור ונוכחות משותפת בחדרי הפיקוד והשליטה יצרו אווירת אמון ופתיחות, וכן שפה משותפת שסייעה לפתח ולהטמיע תודעת שילוביות בין הארגונים. שילוב הכוחות בסביבה הפנימית של ארגוני המודיעין ובסביבה החיצונית, בין ארגוני המודיעין ובין יחידות מבצעיות, אִפשר להגיע להישגים מבצעיים חדשים. בהמשך הצליחו אמ"ן והשב"כ לפתח שילוביות ברמה גבוהה שהתבססה על היתוך מידע בין כל סוכנויות האיסוף והמחקר והביאה ליצירת "בנק יעדים" בהיקף ובאיכות גבוהים. דוגמה לכך ניתן לראות בשלושת סבבי הלחימה האחרונים (בשנים 2009, 2012, 2014) ברצועת עזה.[55] זוהי דוגמה למודל של שילוביות בין־ארגונית, המאפשר מיצוי של מידע הנדרש לייצור "בנק מטרות" ברמת דיוק ובכמות גבוהה.

ביטוי נוסף לרעיון השילוביות בין גורמי מודיעין ובין כוחות מבצעיים־לוחמים ניתן לראות בפרויקט "חופת אש" – גרסת צה"ל לרעיון הסיכול הממוקד שפותח בשב"כ. במסגרת הפרויקט, פועלים גורמי מודיעין וגורמים מחיל התותחנים או חיל האוויר בתאי תקיפה משותפים, לסיכול חוליות של משגרי רקטות ונשק נ"ט ולסיכול חדירות של מחבלים.[56]

סיכום ותובנות

בעשורים האחרונים חלו תמורות משמעותיות במושג השילוביות ובמאפייני יישומה הלכה למעשה. בתחילת המאה ה־21 הפכה השילוביות לכלי משמעותי יותר של קהילות מודיעיניות, וזאת בהשפעת שינויים שחלו בסביבה הביטחונית בה פועלות קהילות אלו, משברים שפקדו את קהילות המודיעין נוכח שינוי באופי האתגרים המודיעיניים, ושינויים טכנולוגיים ותרבותיים.

השילוביות מתארת ממשק מורכב ורב־ממדי בין ישויות, שבמהותו מייצג תהליכי למידה ברמות שונות ומתאפשר בזכות אקולוגיה מסוימת. ההבנה שסביבות עבודה רבות יכולות להיות רלוונטיות ויעילות יותר בזכות אותו ממשק שילובי אינה אינטואיטיבית, והיא מתאפשרת רק בתנאים ייחודיים, במסגרתם נדרשים ארגונים לוותר על חלק מסמכותם ולחלוק אחריות עם אחרים. האתגרים

שהזדמנו לפתחם של ארגונים, והמשברים שפקדו אותם כתוצאה מכך, חשפו אותם לפערים ברלוונטיות שלהם והפכו למחוללי השילוביות.

המאמר סקר את ההתפתחות התיאורטית והמעשית של תפיסת השילוביות, הבחין בין שילוביות תפיסתית לשילוביות ארגונית ועמד על יחסי הגומלין ביניהן ועל הזיקות ביניהן ובין סוגי הלמידה. מטריצה, הנוצרת מחיתוך של שני צירי משתנים (משתנה המהות ומשתנה הסביבה), אפשרה לזהות ולהגדיר ארבעה אבות טיפוס או דגמים של שילוביות, שאותם ניתח המאמר באמצעות שורה של מקרי בוחן מההקשר האמריקאי והישראלי.

השילוביות אינה פתרון קסם, ולא בכל המקרים בהם נוסתה היא התגלתה כפתרון הארגוני המוצלח ביותר. מקרי הבוחן מלמדים שלא תמיד יושמה השילוביות באופן הנכון. הצלחתה תלויה במספר מרכיבים, שהוגדרו במאמר כ"אקולוגיה". הבולט שבהם הינו החופש הארגוני, המאפשר מרחב שבו ניתן ואף מומלץ לאפשר אוטונומיה לדרגי העבודה. אוטונומיה זו מאפשרת גמישות ויצירתיות, גם אם תוך חריגה מתבניות העשייה המוכרות. גם לאמון בין השחקנים יש משקל רב בהצלחת הממשקים. השילוביות בין גורמי מודיעין לבין עצמם, ובמיוחד השילוביות של גורמי מודיעין עם גורמים חיצוניים, התאפשרו בעיקר במצבים בהם התפתחו בקרב אנשי המודיעין ציפיות להתנהגות חיובית של השותפים, וצומצם החשש מפני התנהגותם השלילית. במצב כזה נוצר אמון שהגדיל את נכונותם של השחקנים ליטול סיכונים, ובכלל זה להיחשף ולשתף.

הרעיון של "גוף־על" (דוגמת ה־DNI בארצות הברית), כגורם המחולל שילוביות וכגורם בעל השפעה על האקולוגיה הארגונית, מתברר כרעיון משמעותי, לפחות בקרב קהילת המודיעין האמריקאית. מנהל־העל יכול לעודד יצירת אקלים, תודעה וערכים של עבודה משותפת.

הביטוי המהותי של השילוביות המודיעינית קשור למסגרות הרב־זירתיות, המשלבות גורמי איסוף ומחקר. דגם זה מייצג היבטים של השילוביות התפיסתית והארגונית, החל מתהליכי המחשבה והלמידה הכרוכים בהתהוותו וכלה באופנים שבהם הוא בא לידי מימוש. השילוביות במקרים אלה, מצביעה על ההבנה כי קיים צורך לשנות את תצורת העבודה המודיעינית המסורתית, המפוצלת לדיסציפלינות שונות, לעֵבר ניהול מכוון משימה ו/או זירה.

לסיכום, תפיסת השילוביות מהווה מענה לסוגיות מרכזיות עמן מתמודדות קהילות המודיעין כיום, ואימוצה מאפשר להן לספק מענה טוב יותר לאתגרים החדשים. יחד עם זאת, לא מדובר בפתרון קסם המבטל את הצורך בתפיסות ובמבנים ארגוניים מסורתיים. מימוש תפיסת השילוביות במקומות ובהקשר בו היא נדרשת מחייב גם מאמצי בניין כוח משותפים דוגמת כוח אדם, תשתיות תקשורת ובקרה ועוד, שהם בסיס חיוני להשגת יעד זה.

הערות

1 את ניצניה של תפיסת השילוביות ניתן למצוא כבר בחשיבה הצבאית הסובייטית מתייחס לאמנות המערכה. להרחבה בנושא זה ראו: שמעון נווה, **אמנות המערכה, התהוותה של מצוינות צבאית** תל אביב: משרד הביטחון־ההוצאה לאור ומערכות, 2001.

2 Department of Defense Dictionary of Military and Associated Terms (US Department of Defense, Joint Publication 1-02, Washington D.C, amended through September 17, 2006), p. 132, http://www.fas.org/irp/doddir/dod/jp1_02.pdf

3 כדוגמה לכך מוזכרת תוכנית הגנתית של חיל הים האמריקאי (“600-Ship Maritime Strategy”) שכללה ספינות מלחמה, ועוררה זעם רב בקרב ראשי הזרועות האחרות כאשר היא הוצגה: Don M. Snider, “The US Military in Transition to Jointness: Surmounting Old Notions of Interservice Rivalry”, Airpower Journal, Fall 1996, http://www.airpower.maxwell.af.mil/airchronicles/apj/apj96/fall96/snider.html.

4 שם.

5 נוסח החוק: “Goldwater-Nichols Act of 1986”, U.S. Code Legal Information Institute, Cornell Law School, http://www.au.af.mil/au/awc/awcgate/congress/title_10.htm. להרחבה על החוק ראו: “Goldwater-Nichols Act”, Wikipedia, https://en.wikipedia.org/wiki/Goldwater%E2%80%93Nichols_Act.

6 Joint Warfare of the US Armed Forces, (Joint pub-1, Washington, D.C.: National Defense University Press, November 11, 1991), http://hdl.handle.net/2027/uiug.30112001695292.

7 הדוקטרינה גובשה באופן הירכי בתהליך Top - Down, וזאת לעומת דוקטרינת חיל הים, אשר גובשה על ידי הציים השונים בתהליך Bottom - Up. להרחבה ראו: Paul J. Bolt Damon V. Coletta, Collins G. Shackelford, *Defense Organization: The Need for Change: Staff Report to the Committee on Armed Services*, Washington D.C.: U.S. G.P.O., 1985, http://babel.hathitrust.org/cgi/pt?id=mdp.39015011556266;view=1up;seq=1

8 Snider, “The US Military in Transition”.

9 עפרון רזי ופנחס יחזקאלי, **מנהל ציבורי על פרשת דרכים – מאנוכיות לשיתוף פעולה** (צה”ל, המכללה לביטחון לאומי, המרכז למחקר אסטרטגי ולמדיניות, מאי 2007), עמ׳ 31.

10 גישה זו לפיתוח אפליקציות נקראת Service Oriented Architecture (SOA): Technical White Paper, “Service Oriented Architecture (SOA) and Specialized Messaging Patterns”, *Adobe*, 2007, http://www.adobe.com/enterprise/pdfs/Services_Oriented_Architecture_from_Adobe.pdf

11 צבי לניר, ״למה צריך את המושג ׳שילוביות׳״, **מערכות**, גיליון 401, יוני 2005, עמ׳ 20.

12 על ההבחנה בין תיאום, שיתוף פעולה ושילוביות ראו טבלת שילוביות: https://doalogue.co.il/wiki/

13 לניר, ״למה צריך את המושג ׳שילוביות׳״, עמ׳ 25.

14 רזי ויחזקאלי, **מנהל ציבורי על פרשת דרכים – מאנוכיות לשיתוף פעולה**, עמ׳ 59.

15 **שם**, עמ׳ 53.

16 “**Jointness of the Joint Force**. Jointness implies cross-Service combination wherein the capability of the joint force is understood to be synergistic, with the sum greater than its parts (the capability of individual components)”; “**Joint Operation Planning**. Joint operation planning provides a common basis

for discussion, understanding, and change for the joint force, its subordinate and higher headquarters, the joint planning and execution community, and the national leadership": Doctrine for the Armed Forces of the United States (United States Department of Defense, Joint Publication 1, March 2013), http://www.dtic.mil/doctrine/new_pubs/jp1.pdf

17 Department of Defense Dictionary of Military and Associated Terms, pp. 11, 13-14.

18 מח' תו"ל, מפקדות בטיחות והדרכה, "מונחון (2006)", בתוך: התכנון המערכתי, צה"ל, אמ"ץ–תוה"ד.

19 להרחבה על ההבחנה בין עיצוב לתכנון בעגה המערכתית, ראו: יותם הכהן, "עיצוב המערכה", **דואלוג**, https://doalogue.co.il/wiki/%D7%A2%D7%99%D7%A6%D7%95%D7%91_%D7%94%D7%9E%D7%A2%D7%A8%D7%9B%D7%94

20 קובי מיכאל, "כשל הלמידה במבחן ההתאמה בין מדינאות לצבאיות במאבק בטרור במזרח התיכון", **פוליטיקה**, כרך 25, האוניברסיטה העברית בירושלים, 2015, עמ' 6.

21 גבריאלה היכל, **קבלת החלטות בזמן משבר** (תל אביב: הוצאת מערכות, 1992), עמ' 75–79.

22 Kobi Michael, "Who Really Dictates What an Existential Threat Is? the Israeli Experience", Journal of Strategic Studies, 32(5)(2009): 687-713.

23 Roy J. Lewicki, Daniel J. McAllister and Robert J. Bies, "Trust and Distrust: New Relationships and Realities", The Academy of Management Review, Vol. 23, No. 3 (July 1998): 438-458.

24 המטריצה הוצגה לראשונה על ידי דניאל בר־טל, שהציג את המודל בסדנת אימון של מרכז שטיינמץ לשלום באוניברסיטת תל אביב.

25 Jeanne Hull, "'We're All Smarter than Anyone of Us': The Role of Inter-Agency Intelligence Organizations in Combating Armed Groups", Journal of International and Public Affairs (2008): 37-38.

26 איתי ברון, **המחקר המודיעיני – בירור המציאות בעידן של תמורות ושינויים** (המרכז למורשת המודיעין, המכון לחקר מודיעין ומדיניות, הוצאת אפי מלצר, 2015), עמ' 97.

27 על האתגר הכרוך במעקב אחר אויב נעלם ראו: **שם**, עמ' 93. על אתגר ההתהוות ראו: **שם**, עמ' 32.

28 **שם**, עמ' 12.

29 Bridget Rose Nolan, **"**Information Sharing and Collaboration in the United States Intelligence Community: An Ethnographic Study of the National Counterterrorism Center", a dissertation in sociology presented to the Faculties of the University of Pennsylvania, 2013, p. 158.

30 United States Intelligence Community, 500 Day Plan, Integration and Collaboration, October 10, 2007, https://wilsonml.wordpress.com/2007/10/16/dni-releases-the-500-day-plan-for-integration-and-collaboration; http://fas.org/irp/dni/500-day-plan.pdf

31 the National Intelligence Strategy of the United States of America (Office of the Director of National Intelligence, September 2014).

הרעיון זוכה להתייחסות במספר גרסאות של המסמך, לאורך השנים, מ־2005 עד 2014:
שנת 2005: http://fas.org/irp/offdocs/nis.pdf
שנת 2009: http://fas.org/irp/offdocs/nis2009.pdf
שנת 2014: http://www.odni.gov/files/documents/2014_NIS_Publication.pdf;

Joint Intelligence (Joint Publication 2-0, October 2013), http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf

32 הכינוי האמריקאי הוא: "Mission-Driven Intelligence Workforce". ראו למשל: *The National Intelligence Strategy of the United States of America* (Office of the Director of National Intelligence, August 2009), p. 11.

33 עמיר רפפורט, "טלטלה מודיעינית", Israeldefense, 6 במארס 2014, http://www.israeldefense.co.il/he/content/%D7%98%D7%9C%D7%98%D7%9C%D7%94-%D7%9E%D7%95%D7%93%D7%99%D7%A2%D7%99%D7%A0%D7%99%D7%AA.

34 שי שבתאי ועומרי גפן, **איך מקדמים שילוביות בקהילת המודיעין באמצעות הקב"ש**, הוצאה פנימית, 2015. הוצג בפורום מודיעין במכון למחקרי ביטחון לאומי.

35 דודי סימנטוב ועופר ג', "מודיעין 2.0 – גישה חדשה לעשיית מודיעין", **צבא ואסטרטגיה**, כרך 5 גיליון 3, דצמבר 2013.

36 **Living Intelligence** Chris Rasmuseen**. Toword** https://www.youtube.com/watch?v=nbgQ1V2BLEs

37 ביניהן CIA, NSA, DIA, FBI, NGA.

38 Nolan, **"**Information Sharing and Collaboration in the United States Intelligence Community".

39 שם, עמ' 59.

40 שם, עמ' 79.

41 Tom Ashbrook, "Reforming the American Intelligence System", On point Radio Show, March 11, 2015, http://onpoint.wbur.org/2015/03/11/cia-reform-john-brennan-senate-spies-national-security

42 Gudrun Persson, Fusion Centers – Lessons Learned – A Study of Coordination Functions for Intelligence and Security Services (CATS – Center of Asymmetric Threat Studies, National Defense College, 2013).

43 רשימת "מרכזי ההיתוך" הפועלים בארצות הברית, בכפיפות למשרד להגנת המולדת ראו:
Official website of the Department of Homeland Security, Fusion Center Locations and Contact Information, http://www.dhs.gov/fusion-center-locations-and-contact-information

44 Torin Monahan, "The Murky World of 'Fusion Centers'", Criminal Justice Matters, 75 (1) (2009): 20-21, http://publicsurveillance.com/papers/FC-CJM.pdf.

45 Considerations for Fusion Center and Emergency Operations Center Coordination Comprehensive Preparedness, Comprehensive Preparedness Guide (CPG) 502 (Federal Emergency Management Agency – FEMA, May 2010), p. 9, http://www.fema.gov/media-library-data/20130726-1828-25045-3917/cpg_502_comprehensive_preparedness_guide_considerations_for_fusion_center___eoc_coordination_2010.pdf

46 Use of Technology in Intelligence Fusion Centers, An Oracle White Paper, April 2007, p. 5, http://www.oracle.com/us/industries/046140.pdf.

47 דוח של ועדת חקירה פדרלית לבחינת פעילותם של "מרכזי ההיתוך":
Investigative Report Criticizes Counterterrorism Reporting, Waste at State & Local Intelligence Fusion Centers (U.S. Senate, The Permanent Subcommittee On Investigations, October 3, 2012), http://www.hsgac.senate.gov/subcommittees/

investigations/media/investigative-report-criticizes-counterterrorism-reporting-waste-at-state-and-local-intelligence-fusion-centers.

48 כתבה המתארת את פגיעתם של "מרכזי ההיתוך" בפרטיות האזרחים ראו: Robert O'Harrow, "DHS 'Fusion Centers' Portrayed as Pools of Ineptitude and Civil Liberties Intrusions", The Washington Post, October 2, 2012, http://www.washingtonpost.com/investigations/dhs-fusion-centers-portrayed-as-pools-of-ineptitude-and-civil-liberties-intrusions/2012/10/02/10014440-0cb1-11e2-bd1a-b868e65d57eb_story.html

49 Persson, Fusion Centers – Lessons Learned, p. 12.

50 Hull "We're All Smarter than Anyone of Us".

51 שם, עמ' 37.

52 סא"ל ע', "מקומו של המודיעין במשולש קלאוזוביץ", **מערכות**, גיליון 409–410, דצמבר 2006, עמ' 77–81.

53 אמיר אורן, אדון "הפרשנים או משרת המבצעים", **הארץ**, 24 ביוני 2005.

54 שם.

55 יוסי מלמן, "פלאי ההיתוך", **הארץ**, 1 באוגוסט 2008 (בהתייחסותו למבצע "עופרת יצוקה").

56 אמיר בוחבוט, "קצין איסוף: גלגולו של הסיכול הממוקד", **וואלה**, 28 בדצמבר 2012, http://news.walla.co.il/item/2601434.

לוחמת הסייבר בארצות הברית: השלכות על גופי סייבר מבצעיים ועל קביעת מדיניות הסייבר

עמרי הייזלר

מאמר זה מתמקד בשני מרכיבים מרכזיים של מרחב הסייבר ולוחמת הסייבר בארצות הברית. תחילה הוא יסקור שלושה אירועי סייבר בתקופות שונות, שבמהלכן חלה התפתחות הדרגתית בתשתיות, במנגנונים ובמדיניות ארצות הברית בתחום הסייבר. במסגרת זו ינתח המאמר את ההתפתחות התפיסתית, המבצעית והמשפטית שהובילה למבנה הארגוני של תחום הסייבר האמריקאי ולתהליך הנוכחי של קבלת ההחלטות בו. בהמשך יבחן המאמר את המדיניות ואת שיטות הפעולה של קהילת המודיעין האמריקאית וכן את המבנה של המערכת המבצעית של תחום הסייבר בארצות הברית. במסגרת זו ייסקרו הרקע, תחומי האחריות והמשימות של קהילת המודיעין של ארצות הברית לפני מתקפת סייבר, במהלכה ואחריה, תוך התעכבות על המבנה הארגוני, וספציפית על הארכיטקטורה הארגונית שלה. כמו כן יסקור המאמר בקצרה את איומי הסייבר הנוכחיים על ארצות הברית ויפרט כמה מהאסטרטגיות וכללי המדיניות שמשמשים אותה למתן מענה הולם לאיומים אלה. לבסוף, המאמר ינתח את מרחב הסייבר ברמת המקרו, תוך התייחסות לתיאום בין סוכנויות המודיעין האמריקאיות וביניהן למוסדות הפדרליים, המדינתיים והפרטיים הרלוונטיים לטיפול במשברי סייבר.

מילות מפתח: Moonlight Maze, תולעת מוריס, סטוקסנט, מתקפות סייבר, קהילת המודיעין האמריקאית, משבר סייבר, איומי סייבר, משילות אינטרנט, מדיניות אינטרנט, אסטרטגיית סייבר

עומרי הייזלר הוא קצין צה"ל ועובד משרד ראש הממשלה לשעבר. בוגר תואר שני מטעם בית הספר ליחסים בינלאומיים וציבוריים של אוניברסיטת קולומביה (SIPA).

תולדות לוחמת הסייבר

ניתן לחלק את התפתחות לוחמת הסייבר לשלושה שלבים היסטוריים: שלב התהוות, במהלך העידן המוקדם של האינטרנט; שלב הנסיקה, במהלך תקופת הביניים שלפני מתקפת 11 בספטמבר 2001 ואחריה, כאשר מתקפות הסייבר היו ברובן עדיין בעלות אופי של איסוף מידע; ושלב המיליטריזציה הנוכחי, שבו לוחמת סייבר יכולה לפגוע ביכולות אסטרטגיות ובתשתיות אמריקאיות קריטיות, בדומה למתקפה קינטית בקנה מידה נרחב.[1] הטבלה שלהלן מתארת שלבים אלה.

טבלה 1. שלבים היסטוריים בלוחמת הסייבר

שלבים	התהוות	נסיקה	מיליטריזציה
מסגרת זמן	1980–1998	1998–2003	2003 – כיום
דינמיקות	לתוקפים יש יתרון על המותקפים	לתוקפים יש יתרון על המותקפים	לתוקפים יש יתרון על המותקפים
למי יש יכולות?	ארה"ב ועוד כמה מעצמות־על	ארה"ב ורוסיה ועוד שחקנים קטנים רבים	ארה"ב, רוסיה, סין, ועוד שחקנים קטנים רבים עם יכולות משמעותיות
יריבים	האקרים	האקטיביסטים, האקרים פטריוטים, וירוסים ותולעים	ניאו־האקטיביסטים (Neo-Hakctivists), סוכני ריגול, תוכנות זדוניות, צבאות של מדינות, מרגלים ושלוחיהם, האקטיביסטים (Hacktivists)
אירועים מרכזיים	"ביצת הקוקייה" (1986), "תולעת מוריס" (1988), האקרים הולנדים (1991), מעבדות רומא (1994), "סיטיבנק " (1994)	"Eligible Receiver", "Solar Sunrise", "Moonlight Maze", "Allied Force",	"Titan Rain", אסטוניה, גיאורגיה, "Buckshot Yankee", "סטוקסנט"
הדוקטרינה האמריקאית	לוחמת מידע	מבצעי מידע	לוחמת סייבר

מתקפות סייבר כזרז להתפתחות ארגונית

כל אחת מהתקופות שתוארו בטבלה שלעיל מתאפיינת בדוקטרינה שונה מהותית, הן בהתייחס להתקדמות הטכנולוגית ולסוגי האיומים והן בהתייחס למדיניות

הסייבר של הממשל האמריקאי. חלק ממתקפות העבר רמזו על אתגרי הסייבר העתידיים ושימשו כסימני אזהרה לפגיעויות של ארגונים ולמצב האבטחה הבלתי מספק השורר בהם. ככל שהתלות של החברה בטכנולוגיה עלתה, כך גם גברו ההשלכות האפשריות של אבטחה בלתי מִספקת על פגיעויות ספציפיות במרחב הסייבר.

שלב ההתהוות – "תולעת מוריס"

אירוע סייבר זה שימש כקריאת ההשכמה הראשונה לקהילת המודיעין האמריקאית, לקובעי המדיניות ולחוקרים באקדמיה. אמנם, לא הייתה זו מתקפת הסייבר הראשונה על מערכות מחשב אמריקאיות (מתקפת ריגול הסייבר המשמעותית הראשונה הייתה החדירה בשנת 1986, שזכתה לכינוי Cuckoo's Egg בה היה מעורב הקג"ב הסובייטי), אולם הדעה הרווחת היא ש"תולעת מוריס" הייתה המתקפה הראשונה בקנה מידה גדול, וזאת מבחינת השתלשלות האירועים המהירה, היקפם והשלכותיהם. "תולעת מוריס" שוגרה במקור כמעשה קונדס ממעבדה באוניברסיטת קורנל, במטרה לפגוע בכמה שיותר מחשבים מבלי להתגלות. התולעת הביאה לקריסה של 6,000 מחשבים, שבשנת ההתקפה, 1988,[2] היוו כמעט עשרה אחוזים מרשת האינטרנט. המשרד לפיקוח על התקציב (US Accountability Office) העריך את הנזק שנגרם כתוצאה מ"תולעת מוריס" בין מאה אלף דולר לעשרה מיליון דולר – פער מספרי הממחיש את הקושי הקיים עד היום להעריך את הנזקים ממתקפות סייבר.[3]

ההשלכות החמורות של "תולעת מוריס" סיפקו אזהרה חשובה לקהילת המודיעין האמריקאית מעצם הפניית הזרקור לנזק הפוטנציאלי לרשתות מחשבים עתירות חיבורים, והדגישו את הצורך ליצור יכולות ארגוניות ומנגנונים בני הגנה במרחב הסייבר. למעשה, "תולעת מוריס" פעלה כזרז לגיבוש השלבים הראשונים בדרך לפיקוח טוב יותר על מרחב הסייבר והובילה לשינויים דרמטיים מבחינה תפיסתית ויישומית גם יחד:

- **שינוי בפרדיגמה**: במועד בו התרחש אירוע "תולעת מוריס" עשה האינטרנט את צעדיו המשמעותיים הראשונים ונחשב כ"מקום ידידותי". "תולעת מוריס" סייעה לחשוף את נוכחותם של אנשים בעלי כוונות זדוניות במרחב הסייבר. האירוע היה הפעם הראשונה שבה העיסוק בסייבר עבר מהתמקדות בנושא הקישוריות לחששות בתחום האבטחה.
- **מבצעיות**: בעקבות אירוע "תולעת מוריס" הקימה "הסוכנות לפרויקטי מחקר מתקדמים בתחום ההגנה" (DARPA) באוניברסיטת קרנגי מלון את "המרכז להתמודדות עם איומי סייבר" (CERT). מהלך זה המחיש את המעבר ממתן

פתרונות אד־הוק להקמת צוותים מקצועיים מאומנים ומצוידים כנדרש, לתיאום אירועים ולמתן הערכות ופתרונות למתקפות סייבר.[4]

- **רגולציה ותקנות**: במקביל לשינוי התפיסתי באבטחת הסייבר, חוקק הקונגרס האמריקאי בשנים שלאחר אירוע "תולעת מוריס" כמה חוקים, ביניהם חוק הפרטיות בתקשורת האלקטרונית ב־1986 וחוק ביטחון המחשבים ב־1987, שנועדו להבטיח, באמצעות הגנות משפטיות, את הפרטיות בתחומי הסייבר.[5] היוצר של "תולעת מוריס", רוברט טאפאן מוריס, היה האדם הראשון שהורשע על פי החוק נגד מעשי הונאה ושימוש לרעה במחשבים שנחקק בשנת 1986.[6]

שלב הנסיקה – אירוע "Moonlight Maze"

ב־1998 גילו גורמים אמריקאיים רשמיים בדרך מקרה דפוס של "גישוש" (probing) מתמשך במערכות המחשב של הפנטגון, באוניברסיטאות פרטיות, בנאס"א, במשרד האנרגיה ובמעבדות מחקר. עד מהרה הם הבינו כי פעולת הגישוש התרחשה באופן רציף במשך כמעט שנתיים. אלפי מסמכים שאמנם לא היו מסווגים, אך כללו מידע רגיש שקשור לטכנולוגיות בעלות יישומים צבאיים, נחשפו או נגנבו, לרבות מפות של מתקנים צבאיים, מערכי חילות ותוכניות חומרה.[7] למרות שמשרד ההגנה של ארצות הברית הצליח לזהות את עקבות הפולשים כמובילות למחשב מרכזי שנמצא בברית המועצות לשעבר, הגורמים שיזמו את המתקפה נותרו עלומים. רוסיה הכחישה כל מעורבות בה, והחשדות מעולם לא הוכחו חד־משמעית.[8]

המתקפה שקיבלה את הכינוי "Moonlight Maze" נחשבת בעיני רבים כמתקפת ריגול הסייבר הגדולה הראשונה מצד גורם מדינתי מאורגן וממומן. המתקפה תוכננה היטב, שכן התוקפים הותירו "דלתות אחוריות" כדי לאפשר להאקרים לחדור למערכת במועדים שונים, השאירו מעט מאוד עקבות ופעלו במשך זמן רב מבלי שהתגלו.[9] אירוע "Moonlight Maze" הבליט את התפקיד שממלאות רשויות מדינתיות בהפקה, במימון או לפחות בהשתתפות פסיבית באירועי ריגול מתוחכמים ורחבי היקף. יתרה מכך, האירוע ציין את הפגיעות של מרחב המידע, שבו יריבים יכולים לא רק לגרום לשיבוש השירות, אלא גם לשים את ידם על מידע רגיש. הוא הוכיח את הצורך החיוני ב"חומות אש" ובהצפנות, ומעל לכל – את הקושי בזיהוי מתקפה ובייחוסה לגורם עוין ספציפי.

אירוע "Moonlight Maze" היה שלב חשוב בהתפתחות לוחמת הסייבר ואבטחת הסייבר, וזאת בזכות ההשלכות האפשריות שלו על עימותים עתידיים.[10] הוא הצביע על השינוי הצפוי בשדה הקרב המודרני – ממלחמה קינטית, שבה לאויבים יש שמות, מיקומם הפיזי ידוע, המתקפות נראות בעין וניתן להעריך את נזקן, לעבר לוחמה אסימטרית המאופיינת במבצעי סייבר התקפיים, שהמתקפות בהם בלתי נראות, האויבים לא ידועים והנזק קשה לכימות. "Moonlight Maze"

הוביל לשינויים דרמטיים בגישתו של הממשל האמריקאי לאבטחת סייבר, כפי שיתואר בהמשך.

השינוי בפרדיגמה

המודעות של קובעי המדיניות בארצות הברית לאיומי טרור ותמיכתם ביוזמות למלחמה בטרור גם לאחר פיגועי 11 בספטמבר 2001 היו מוגבלות. אירוע "Moonlight Maze" הביא לחשיבה מחודשת על אסטרטגיית הגנת הסייבר האמריקאית, לוחמת סייבר, הרתעת סייבר וההגנה על רשתות רגישות ולא מוצפנות, כגון NIPERnet (רשת נתב פרוטוקול אינטרנט לא מאובטח – הרשת הלא מסווגת של הפנטגון). לראשונה התעוררו שאלות פוליטיות וחוקתיות בנוגע לביטחון, לפרטיות, לרעיונות בדבר ניטור אקטיבי ולסכנה של חשיפה לאיומים על־לאומיים.[11] אירוע "Moonlight Maze" הביא את ארצות הברית להבנה כי נדרשות מדיניות ואסטרטגיה ברורות ללוחמה האסימטרית, למרחב העתידי של איסוף מידע מודיעיני וריגול ולהשלכות הטכנולוגיות שנגזרות מכך.

פעולות חקיקה

הצו הנשיאותי מספר 63 להגנה על תשתיות קריטיות היה בחלקו תוצאה של אירוע "Moonlight Maze". היה זה מסמך מדיניות חלוצי שהגדיר את הכללים, תחומי האחריות והיעדים להגנה בתחום השירותים הציבוריים, תשתיות התחבורה והפיננסים וכל תשתית חיונית אחרת של ארצות הברית.[12] לצו הנשיאותי מספר 63 היו שתי השלכות אסטרטגיות מרכזיות: האחת, הקמת "מרכז ההגנה הלאומי נגד אירועים" (NIPC) – גוף חוצה סוכנויות, בעל סמכות לפקח על התשתיות הקריטיות הממשלתיות והאזרחיות של המדינה מפני מתקפות מחשב;[13] השנייה, הקמת "כוח המשימה המשותף להגנה על רשתות מחשב" (JTF-CND) – גוף שהופקד על הובלה ותיאום התגובות למתקפות סייבר ברמה הארצית, המרַכז תחתיו את ההגנה על רשתות מחשב צבאיות.[14]

פעולות מבצעיות

משרד ההגנה של ארצות הברית הוביל את בנייתם של מנגנוני תגובה לאירועי הסייבר והקים מוסדות לדיווח עליהם. דיווחים בנושאים צבאיים טופלו מאז ברמה המקומית, דרך מרכזי אבטחה ותפעול רשתות (NOSC) שפעלו בהכְוונה של "הסוכנות למערכות מידע של משרד ההגנה" (DISA). בנוסף לכך, מרכזי CERT אזוריים, שפעלו כמנגנוני פיקוד ושליטה, הפכו למובילים בתחום הערכת ההשלכות של מתקפות סייבר ברמות האישית והאזורית. גורמים נוספים שהוקמו לסיוע בתיעול מידע הם "כוח המשימה המשותף לתפעול רשתות מחשב" (JTF-CNO)

ו"המרכז הגלובלי לביטחון ותפעול רשתות" (GNOSC) של "הסוכנות למערכות מידע של משרד ההגנה".

שלב המיליטריזציה – "סטוקסנט"

מתקפת "סטוקסנט" נחשבת לאחת המתקפות המתוחכמות ביותר של תוכנות זדוניות עליהן נודע לציבור. מומחים רבים סבורים שרק מדינה יכולה הייתה ליצור ולשגר מתקפה כזאת, למרות שלא ניתן לאמת את הדבר. בערוצי תקשורת רבים אף הועלתה סברה שהיה זה שיתוף פעולה ישראלי־אמריקאי.[15]

התוכנה הזדונית, שנחשבת לאחת ממתקפות הסייבר ההרסניות ביותר שניהלו מדינות ריבוניות, הסבה נזק לצנטריפוגות של איראן ועיכבה את פעילות העשרת האורניום שלה. מרגע שהתוכנה הוחדרה לרשת, היא עשתה שימוש במגוון מנגנונים כדי להפיץ עצמה למחשבים נוספים בתוך אותה רשת ולהשתלט על הנעשה בה. המנגנונים שבהם השתמשה "סטוקסנט" כללו ניצול של פגיעויות מוכרות וכאלו שכבר טופלו ותוקנו, אך גם ארבע פגיעויות שלא היו ידועות ולא תוקנו עד למועד שחרור התולעת (וידועות בשם "מתקפות יום אפס" – zero-day exploits).[16] הקהילה הבין־לאומית ממשיכה לתהות מה היו המקור והמטרה המדויקים של וירוס ה"סטוקסנט", אך בכל מקרה האירוע העלה את המודעות לפגיעויות העיקריות הקיימות ברשתות המחשבים.[17]

"סטוקסנט" זוהה בשנת 2010. מקורו הלא ודאי והשפעתו המחישו את הקושי בזיהוי מתקפת סייבר והביאו למסקנה שלא ניתן להשיג הגנה מלאה ברמת המדינה על כל משאביה החיוניים.[18] כתוצאה מכך התעורר הכרח ללמוד את הדינמיקות של מצבים דמויי קרב בלוחמת הסייבר של העידן המודרני, שבהם אפילו מתקפת ענק לא בהכרח מיוחסת לתוקף ידוע ומוגדר, ואולי אף לא מותירה עקבות כלל. פירוש הדבר הוא שקובעי המדיניות עשויים לעמוד בפני השלכות של מתקפה בשדות הקרב הלא קינטיים של העידן הנוכחי (החל ממניעת שירות ועד הרס תשתיות קריטיות של מדינה) מבלי שיהיה להם "אקדח מעשֵן" או כלי פוליטי או חוקי להילחם בעזרתו. תופעה זו מחייבת את המחוקק והרשויות להתחיל לגבש אופציות תגובה כבר עתה, במקום לנסות לפתח אפשרויות התמודדות אד־הוק במהלך המשבר עצמו.

לוחמת הסייבר שלאחר שנת 2013 העתיקה את גישת מתקפת־הנגד מהרמה המבצעית[19] לרמה האסטרטגית־דיפלומטית, שבה המדיניות, החוק הבין־לאומי, המשילות באינטרנט והסכמים משחקים תפקיד משמעותי ביותר בסביבת הסייבר הפרוצה. שלושה הסכמים מרכזיים ומאמצי שיתוף פעולה בנושא המשילות באינטרנט ברמה הרב־לאומית גובשו מאז אותה שנה:

- **הסכם הסייבר בין ארצות הברית לסין**: הסכם זה קבע כי אף ממשלה "לא תבצע ולא תתמוך ביודעין בגניבה של קניין רוחני דרך הסייבר, לרבות סודות מסחריים או מידע עסקי סודי אחר, למען יתרון מסחרי".[20] אמנם, זהו הסכם בסיסי בלבד שאינו מבטיח סביבת סייבר בטוחה בין שתי המדינות, אולם חשיבותו נובעת מהיכולת להתבסס עליו בשנים הבאות ולהשתמש בו כמחווה של רצון טוב.
- **מפגש הפסגה העולמי של האו"ם בנושא חברת המידע (WSIS+10)**: פסגה זו חידשה את "פורום המשילות באינטרנט" (IGF) – מסגרת שבה המדינות החברות, החברה האזרחית והמגזר העסקי דנו בנושאי מדיניות האינטרנט, אבטחת סייבר, מעקב ופיקוח, קניין רוחני וזכויות יוצרים. המדינות החברות חיזקו במעמד זה ערוצים דיפלומטיים קיימים בתחום מדיניות הסייבר, ואשררו את מחויבותן לגשר על פערים דיגיטליים ולשפר את הגישה לטכנולוגיות מידע ותקשורת, וזאת באמצעות אישור המסמך שגובש בפסגת WSIS+10.[21]
- **הסכם "המעגן הבטוח" (Safe Harbor)**: הסכם זה נחתם בין משרד המסחר האמריקאי ובין האיחוד האירופי, והסדיר לראשונה את האופן שבו חברות אמריקאיות רשאיות לייצא ולטפל בנתונים אישיים של אזרחים אירופיים.[22]

מבנה מרחב הסייבר האמריקאי

מרחב הסייבר האמריקאי רווי במוסדות, בענפי צבא, במכוני מחקר ובגורמי אקדמיה, ממשל והמגזר העסקי. הדבר נובע ממורכבות התיאום, מתחומי האחריות המפוצלים ומגורמי פיקוח חופפים.

ברמה הלאומית ניצבת קהילת המודיעין האמריקאית, עם יכולות הגנה והתקפה במרחב הסייבר. קהילת המודיעין גם נושאת באחריות העליונה לטיפול בכל הסוגיות הקשורות בלוחמת הסייבר המודרנית, למתן מענה להן ולמעקב אחריהן. היא גם זו שמחזיקה למעשה באחריות המבצעית על כל היבטיו של מרחב הסייבר בארצות הברית, בין אם מדובר במתקפה נגד רשויות צבאיות או ממשלתיות, ובין אם מדובר במתקפה גדולה נגד מוסד פרטי או תשתית קריטית.

קהילת המודיעין האמריקאית במתכונתה הנוכחית הוקמה ב־1981 ומהווה פדרציה של 17 סוכנויות ממשל אמריקאיות הפועלות בנושאי מודיעין, הן ביחד והן בנפרד.[23] הארגונים החברים בקהילה כוללים סוכנויות מודיעין, את המודיעין הצבאי, את המודיעין האזרחי וכן גופי מחקר בתוך משרדי ממשלה פדרליים. בראש כל 17 הגופים עומד מנהל המודיעין הלאומי, שמדווח ישירות לנשיא ארצות הברית.[24] מרבית הסוכנויות המודיעיניות הן משרדים או לשכות בתוך משרדי הממשלה. תשע מתוכן פועלות במסגרת משרד ההגנה ואחראיות למימוש 85 אחוזים מסך כל תקציב המודיעין האמריקאי.

איסוף מסורתי של מידע מודיעיני למלחמה בטרור מבוסס על סדרה של דרכים ושיטות, הכוללת מודיעין אנושי (HUMINT), מודיעין אותות (SIGINT), מודיעין חזותי (IMINT) ומודיעין מדידות וחתימות (MASINT). כל הדיסציפלינות האלו דרושות כדי לבנות הערכת מודיעין כוללת, ויחד עם זאת, ככל שההון האנושי והמשאבים דורשים השקעות גדולות יותר מצד אחד, וההסתמכות האנושית על הטכנולוגיה הולכת וגוברת מצד שני, כך מתחזקת ההכרה ביכולותיו של מרחב הסייבר.

קהילת המודיעין האמריקאית מתמקדת כיום בשלושה היבטים בתחום אבטחת הסייבר: **ארגון**, **גילוי** ו**הרתעה**. גופים שונים בתוך הקהילה עוסקים במשימות שונות בתחום זה:[25] משרד מנהל המודיעין הלאומי עומד בראש כוח משימה המתאם את המאמצים לזיהוי מקורותיהן של מתקפות סייבר עתידיות; המשרד לביטחון המולדת (DHS) מוביל את מאמצי ההגנה על מערכות המחשוב הממשלתיות; משרד ההגנה מתכנן את האסטרטגיות למתקפות־נגד בסייבר; "הסוכנות לביטחון לאומי" (NSA) מנטרת, מזהה, מדווחת ומגיבה לאיומי סייבר; הבולשת הפדרלית (FBI) מובילה את המאמצים הלאומיים לחקירה ולהעמדה לדין של מבַצעי פשעי סייבר. בתקופת משבר, 17 הסוכנויות המרכיבות את קהילת המודיעין האמריקאית אחראיות הן לדווח והן להעריך את המודיעין שלהן, שלאחר מכן מתורגם להמלצות על ידי מנהל המודיעין הלאומי. יש ארגוני סייבר רבים נוספים הפועלים מחוץ למטרייה של קהילת המודיעין האמריקאית, הנותנים מענה לאיומי סייבר. הבולטת שבהם היא "מפקדת הסייבר האמריקאית" (USCYBERCOM).

ג'יימס קלאפר, מנהל המודיעין הלאומי של ארצות הברית, האחראי על קהילת המודיעין האמריקאית ועל התיאום המורכב בין כל זרועותיה, פרסם בתחילת 2015 הערכת סיכונים, לפיה איומי הסייבר עומדים בראש רשימת האיומים הגלובליים.[26] היה זה השינוי הראשון בהגדרת האיום הגלובלי הראשי, שמאז מתקפת 11 בספטמבר 2001 היה איום הטרור הפיזי. עם זאת, קלאפר התייחס לאפשרות של אירוע בממדים של "יום הדין של הסייבר" (מצב שקיבל גם את הכינוי "פרל הרבור של הסייבר" או "11 בספטמבר של הסייבר")[27] בסבירות נמוכה ורחוקה, למרות שמתקפות סייבר נגד ארצות הברית מתרחשות כל הזמן ומספרן נמצא בעלייה.[28]

במקום תרחיש של "יום הדין של הסייבר" שיפגע בכלל התשתיות האמריקאיות, קהילת המודיעין של ארצות הברית צופה שהאתגר בתחום הסייבר יהיה שונה. התחזית שהיא פרסמה כוללת סדרה ארוכה של מתקפות סייבר בעצימות נמוכה עד בינונית, ממגוון מקורות ולאורך זמן. סדרת מתקפות זו תגרום לעלויות מצטברות, שישפיעו על יכולת התחרות הכלכלית של ארצות הברית ועל ביטחונה הלאומי.[29]

התפוצה של תוכנות זדוניות ברחבי העולם מגבירה את הסיכון לרשתות המחשב האמריקאיות, לתשתיות רגישות ולנתונים. פעולת סייבר שנועדה לשבש

או להרוס לחלוטין, ומופנית נגד תאגיד פרטי, מערכת בקרה תעשייתית או מערכת הגנה, אמנם מחייבת שהאויב הפוטנציאלי יהיה בעל מומחיות ניכרת כדי להוציאה לפועל, אך היא לא דורשת מימון של מדינה או כישרון מבצעי ברמה בין־לאומית. שחקן מסוים, בין אם ברמת המדינה ובין אם ברמה של ארגון שאינו מדינתי, יכול לרכוש בשוק השחור תוכנה זדונית, תוכנת ריגול, תוכנת "יום האפס" (zero-day) או כל תוכנה אחרת, ולשלם למומחים כדי שיחפשו נקודות פגיעות ויפתחו יכולות לתקוף אותן.[30]

למרות העלייה בפעילות הסייבר מצד ארגונים כמו דאע"ש, בכירים במודיעין האמריקאי עדיין מאמינים כי גורמים מדינתיים הם האיום הגדול ביותר לאינטרסים האמריקאיים במרחב הסייבר. קהילת המודיעין של ארצות הברית מעריכה כי קיים סיכוי למשבר סייבר שייגרם על ידי שורה של גורמים, לרבות מדינות עם תוכניות סייבר מתוחכמות ביותר, כגון רוסיה או סין; מדינות עם יכולות טכניות נמוכות יותר אך בעלות כוונות הרסניות, כמו איראן או קוריאה הצפונית; גורמים לא מדינתיים עם יכולת גישה למשאבים ניכרים ומוטיבציה ליצור כאוס בסייבר; או עבריינים המונעים משאיפות לרווחים ופורצים או גורמים קיצוניים המונעים מאידאולוגיה.

לפי הערכתה של קהילת המודיעין האמריקאית, היעדים האפשריים למתקפות סייבר הם:

- **המגזר הפרטי**: לצד היותו קורבן למתקפות סייבר, המגזר הפרטי הוא גם שותף פעיל בחקירתן ובהתייחסות אליהן. לאור חשיבותם של המוסדות הפיננסיים (דוגמת "גולדמן סאקס") לכלכלה האמריקאית, קהילת המודיעין של ארצות הברית מגדירה מגזר זה כתחום חשוב להגנה במקרה של מתקפת סייבר חמורה.[31]
- **תשתיות קריטיות**: התשתיות הקריטיות – קרי הנכסים, המערכות והרשתות הפיזיים והווירטואליים החיוניים לביטחון, לבריאות ולבטיחות הכלכלה והחברה – פגיעות למתקפות סייבר מצד ממשלות זרות, גורמי פשע וגורמים הפועלים באופן עצמאי. מתקפה בקנה מידה גדול עלולה לשתק זמנית את אספקת המים, החשמל או הגז, לפגוע בתחבורה או בתקשורת ולהסב נזק למוסדות פיננסיים.[32]
- **הממשל**: חדירה למערכת קבלת ההחלטות הלאומית של ארצות הברית ולקהילת המודיעין האמריקאית תהיה תמיד יעד מרכזי עבור ישויות ריגול זרות. איום קבוע נוסף על אינטרסים אמריקאיים הוא הניסיון להשיג מידע בנושאי הביטחון הלאומי של ארצות הברית ומידע קנייני ממכוני מחקר אמריקאיים העוסקים בנושאי ביטחון, אנרגיה, כספים, טכנולוגיה בעלת שימוש כפול ותחומים נוספים.[33]
- **צבא וסוכנויות ממשל**: קו המגע הקדמי, שבאמצעותו יש להגן על משאבי ההגנה וההתקפה של הצבא האמריקאי, יותקף וייפגע במקרה של משבר סייבר.

מדיניות קהילת המודיעין האמריקאית

קהילת המודיעין של ארצות הברית מבצעת שורה של פעולות מודיעיניות מדי יום. במקביל, ארצות הברית נמצאת תחת מתקפת סייבר תמידית מצד גורמים מדינתיים ולא מדינתיים כאחד. ברמת המודיעין הלאומי, מתקפת סייבר מחייבת לא רק גיבוש מאמצי הגנה, אלא גם תכנון חלופות מבצעיות שונות לצורך פעולת גמול.

גודלה של קהילת המודיעין האמריקאית מביא אותה לקיים קשרים הדדיים ולשתף פעולה עם סוכנויות ממשל, הן ברמה המבצעית (צבא, משרד ההגנה, המשרד לביטחון המולדת) והן ברמה המדינתית (המגזר הפרטי, מחלקת המדינה, הבית הלבן).יעדי ההתכוננות וההיערכות האסטרטגית של קהילת המודיעין האמריקאית הם:[34]

- הקמה וניהול של כוחות ויכולות המוכנים להוציא לפועל מבצעי סייבר.
- הגנה על רשת המידע הפנימית שלה, אבטחת נתונים וצמצום סיכונים הניצבים בפני ביצוע משימותיה.
- היערכות להגן על אינטרסים אמריקאיים חיוניים מבית ומחוץ נגד מתקפות סייבר משבשות או הרסניות, שיש להן השלכות משמעותיות.
- הקמה וניהול של יכולות סייבר ותכנון השימוש ביכולות אלו כדי למנוע הסלמה של עימותים מצד אחד וכדי לשאוב ולאגור מידע לצורך הכנת "בנק מטרות" מצד שני.
- הקמה וניהול של שותפויות ובריתות בין־לאומיות איתנות במטרה להרתיע איומים משותפים ולחזק את היציבות והביטחון בזירה הבין־לאומית.

מדיניות קהילת המודיעין האמריקאית במענה למתקפות סייבר היא:

- **זיהוי המתקפה**: תוקפים מתוחכמים מנסים להסוות את מתקפת הסייבר שלהם. על גורמי המודיעין מוטל להכין את שדה הקרב ולהעריך במדויק את סיכויי ההצלחה והתועלת בכל סוג של מבצע נגד מתקפת סייבר, בדיוק כפי שהם עושים זאת בעימות קונבנציונלי.[35]
- **מידע**: תפקידה המרכזי של קהילת המודיעין הוא לספק מידע ולדווח, וזאת בנוסף ליכולות ההתקפיות המשמעותיות המצויות בידיה. היא חייבת להעביר מידע לזרועות המבצעיות עמן היא משתפת פעולה, וכן למחלקת המדינה. פירוש הדבר הוא שהצלחתה של קהילת המודיעין האמריקאית במהלך מתקפת סייבר תימדד בסימנים המעידים שהיא תיתן בשלב ההיערכות למתקפה, וביכולתה להיערך מולה באמצעות מתן התרעה ברגע התרחשותה.
- **הצגת חלופות**: המטרה המרכזית של קהילת המודיעין האמריקאית בזמן מתקפה היא לספק שורה של חלופות למקבלי ההחלטות ולאפשר להם גמישות אסטרטגית באמצעות הספקת מידע ערכי. במהלך מתקפה, על קהילת המודיעין

להצביע על דרכי פעולה אפשריות. המלצותיה והערכותיה נועדו לאפשר מרחב פעולה ותמרון מדיניים ואסטרטגיים־מבצעיים למקבלי ההחלטות.

- **הערכת נזקים**: שלא כמו בשדה הקרב המסורתי, מתקפת סייבר קשה לעתים לזיהוי, אפילו אם היא בקנה מידה גדול. על קהילת המודיעין מוטל לאמוד את הנזק שנגרם על ידי מתקפת הסייבר, כדי לאפשר לקובעי המדיניות לנקוט פעולת גמול מידתית. הדבר אינו מחייב אותה לבצע בהכרח מהלכים מבצעיים; אדרבא, עליה לקיים הערכות מודיעיניות ולפעול בתיאום עם משרדי ממשל אחרים, תוך החלפת מידע אתם, כך שתתאפשר זרימה הדדית שוטפת ויעילה של מידע רלוונטי.

תגובה רב־ממדית למתקפת סייבר

תפקידה של קהילת המודיעין האמריקאית חופף לא פעם לתפקידיהם של מוסדות, משרדי ממשל ויחידות צבאיות, שרבים מהם נמצאים מעבר לתחומי הסמכות והאחריות שלה. קהילת המודיעין אינה האחראית הבלעדית למתן מענה למתקפה בתחום הסייבר ברמה הארצית, המדינתית או ברמת התשתיות, ולפיכך היא תלויה במערכת הירכית ובשרשרת מורכבת של זרימת מידע. להלן מוסדות וגופים נוספים בארצות הברית המספקים מענה למתקפות סייבר:

- **המשרד לביטחון המולדת**: מופקד, במסגרת תפקידיו להגן על הטריטוריה של ארצות הברית ולהגיב למתקפות טרור, לתאונות מעשה ידי אדם ולאסונות טבע, והינו בעל אחריות על מודיעין "משמר החופים" (CGI) ועל "המשרד למודיעין ולמחקר" (I&A). "המשרד למודיעין ומחקר" אחראי לאיסוף, לניתוח ולעיבוד מודיעין, וכן להפצת המודיעין למשרד לביטחון המולדת ולשאר החברים בקהילת המודיעין האמריקאית. הוא גם הראשון להגיב על אירועים ברמה הארצית, המקומית והארגונית.[36] גופי הסייבר המרכזיים הפועלים בתוך המשרד לביטחון המולדת הינם המרכז הלאומי לאבטחת סייבר (NCSC) וחטיבת אבטחת הסייבר הלאומית ((NCSD. משרדו של מנהל המודיעין הלאומי אחראי לזרימה יעילה של מידע בין המשרד לביטחון המולדת ובין שאר גופי קהילת המודיעין, על מנת להבטיח סינרגיה של המידע במהלך מתקפת סייבר.
- **משרד ההגנה**: נחשב למוקד המבצעי של קהילת המודיעין האמריקאית ומופקד על תשע מסוכנויות הקהילה, כולל "הסוכנות לביטחון לאומי" (NSA). משרד ההגנה הוא גם המקור העיקרי למודיעין סייבר עבור משרד מנהל המודיעין הלאומי. חיוני שהמידע המבצעי יעובד באמצעות משרד מנהל המודיעין הלאומי ויועבר כהמלצות למדיניות ברמה הפדרלית. למעשה, מנהל המודיעין הלאומי מדווח למקבלי ההחלטות ולבית הלבן על סמך המודיעין שמשרדו מקבל ממשרד ההגנה (סביר מאוד להניח שמנהל המודיעין הלאומי והאדמירל מייקל רוג'רס,

שעמד הן בראש NSA והן בראש CYBERCOM, פועלים בצמידות במהלך מתקפת סייבר).

- **מחלקת המדינה**: הממשל תלוי בקהילת המודיעין במהלך משבר סייבר. שלא כמו בעימותים קונבנציונליים, בתרחיש של מתקפת סייבר סביר להניח שמקבלי ההחלטות אינם יודעים מה אירע, מי תקף, והיכן. אחריותה של קהילת המודיעין היא לספק הערכת מודיעין בזמן אמת, לעבד ולהעביר את המידע הלאה למקבלי ההחלטות. מחלקת המחקר והמודיעין (INR), העובדת עם הדיפלומטיה האמריקאית בנושאי מדיניות סייבר ומתווכת בין מחלקת המדינה לגורמי מודיעין לאומי היא הגורם המרכזי האמון על התיאום וההערכות עם קהילת המודיעין, ועל ניהול התקשורת בין המוסדות ברמה הדיפלומטית ובין הגורמים העוסקים בתחום מודיעין הסייבר.
- **המגזר הפרטי**: כאמור, מתקפות ופריצות סייבר לתשתיות הוגדרו על ידי מנהל המודיעין הלאומי כאיום מספר אחת על ארצות הברית. "המרכז לניתוח ושיתוף מידע" (ISAC) הוא הגורם המרכזי המפקח על איומי סייבר במגזר הפרטי, ומסייע לממשלים ברמה המדינתית ולממשל הפדרלי במידע הנוגע לאיומי סייבר. משברי סייבר במגזר הפרטי עשויים להשפיע על אינטרסים לאומיים (כמו במקרה של חברת "סוני"). לכן, המגזר הפרטי דורש לאמץ גישה מודיעינית מבצעית גם לגביו, וזאת בשיתוף פעולה עם המשרד לביטחון המולדת, מחלקת המדינה והבולשת הפדרלית.

מסקנות

ההיסטוריה של לוחמת הסייבר מלאה במסקנות ולקחים רבים, ויש בה כדי ללמד הן על ההתקדמות של מרחב הסייבר וכיוונו והן על תשומת הלב המקיפה שתחום זה מחייב בכל הרמות. ההתפתחות הטבעית של לוחמת הסייבר היא כלי חשוב בהתמודדות עם טעויות ואמצעי לחיזוי עתידו של מרחב המידע, הצורך בחוקים ותקנות בתחום הפרטיות, ריגול סייבר וכל הקשור באבטחת סייבר. קובעי המדיניות מתייחסים כיום למרחב הסייבר ברצינות רבה מאי פעם, ומוסדות בכל הרמות מפנים משאבים ניכרים כדי להתמודד עם איומי הסייבר הניצבים בפניהם. סוכנויות המודיעין משכללות ללא הרף את יכולות ההגנה וההתקפה שלהן בתחום הסייבר, בעוד שמוסדות פרטיים, במיוחד בתחומי הרפואה, הפיננסים, התשתיות הקריטיות והאנרגיה, וכן תאגידים מבוססי ידע, מקצים היום יותר מתמיד משאבים וכוח אדם להגנה על נתוניהם ולאבטחת הסייבר. הממשל האמריקאי מודע לסיכונים בפניהם עומדות רשתות המחשבים שלו, מה עוד והפרצות בהן נפוצות כיום יותר מתמיד. על רקע זה, ההשקעות ביצירת הגנה טובה יותר על מרחב הסייבר נמצאות כיום בשיא של כל הזמנים.

מספר הבנות מדיניות מהותיות הנוגעות לתחום הסייבר גובשו ברמה הבין־לאומית. עם זאת, מרבית קובעי המדיניות והמחוקקים אינם בעלי יכולת לטפל במתקפות סייבר בהיקף נרחב. לדוגמה, אין הגדרה כוללת אחת של "פעולה מלחמתית" במרחב הלא קינטי, וההגדרות הקיימות אינן ברורות, אינן משותפות לכול ואינן מוסכמות ברמה הבין־לאומית. זאת ועוד, אין בנמצא מנגנונים להתמודדות עם משברי סייבר בתחום הפיננסי. כתוצאה מכך, אין למדינות היכולת לקשור בין מתקפות סייבר גדולות ובין תוקפים מסוימים, דבר המאפשר לגורמים אחרים להסיר מעצמם אחריות.

יש צורך בשיתוף פעולה בין־לאומי בכל הרמות, במיוחד במישור הפיננסי, הדיפלומטי והמשפטי, שכן היעדר שיתוף פעולה כזה מונע יצירת בסיס יציב שעליו ניתן לבנות מנגנונים שיטילו את האחריות על האשמים האמיתיים. בשלוש השנים האחרונות הפכו מתקפות הסייבר למתוחכמות מאי פעם, וזאת למרות הגידול בהשקעות באבטחת סייבר בכל המגזרים. לכן, רק הסכמים מחייבים, כוללים ורב־לאומיים בתחום הסייבר, במקביל לחקיקה מתקדמת בתחום המשילות באינטרנט, יאפשרו להגיע למרחב סייבר בטוח יותר.

בהיבט הביטחוני, קהילת המודיעין האמריקאית יודעת להציג לקובעי המדיניות נרטיבים והמלצות מבצעיות, וזאת בזכות יכולות התיאום וטווח הסמכויות הרחב שלה. האתגר הגדול ביותר במהלך מתקפת סייבר הוא לזהות ולחבר את הנקודות השונות לכדי תגובה אחראית ומידתית. ללא גוף כמו קהילת המודיעין, הכמות האדירה של נתונים עתידה לרדת לטמיון במבוך המידע האינסופי. אויב עקשן עשוי לגרום לקריסתו של קו ההגנה במלחמה קיברנטית, בדומה למצב במלחמה קינטית. לעומת זאת, ובשונה משדה הקרב המסורתי, כאשר מתרחשת מתקפת סייבר, אי אפשר לראות אותה בעין, לא ניתן לייחס אותה לתוקף מסוים וקשה לזהות את השלכותיה.

ככל שחולף הזמן, טרור הסייבר עלול להפוך למקור גובר לחששות. מצב זה עשוי לחייב שיתופי פעולה מודיעיניים בין־לאומיים רחבים מתמיד. ייתכן שסוכנויות ביטחון ומודיעין לאומי במדינות שונות ייאלצו לשנות שיטות עבודה ולמקד מחדש את האסטרטגיות שלהן למלחמה באיום הסייבר. לאור כל זאת, אפשר כבר כיום לנבא שלא הנשק הגרעיני יהיה האיום העיקרי והגדול ביותר על האנושות בעתיד.

הערות

1 Jason Healey, ed. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Vienna, VA: Cyber Conflict Studies Association, 2013).

2 Ted Eisenberg et al., "The Cornell Commission: On Morris and the Worm", *Communications of the ACM* 32, no. 6 (1989): 706-709, http://portal.acm.org/citation.cfm?id=63526.63530.

3 בית הדין לערעורים של ארצות הברית העריך במהלך הערעור בנושא "תולעת מוריס" את העלות של הסרת הווירוס מכל התקן שנפגע בין 200 ל־53,000 דולר. נראה שעל נתונים אלה התבסס דובר אוניברסיטת הרווארד, קליפורד סטול, כאשר הערך את ההשפעה הכלכלית הכוללת של התולעת בין 100,000 ל־10,000,000 דולר.

4 Eisenberg et al., "The Cornell Commission: On Morris and the Worm".

5 Michael Rustad and Diane D'Angelo, "The Path of Internet Law: An Annotated Guide to Legal Landmarks", in *Duke Law & Technology Review 2011*, ed. Beatrice Hahn (Durham: Duke University School of Law, 2011).

6 United States v. Morris, (2d Cir. 1991), upholding the conviction of a computer science graduate student under the Computer Fraud and Abuse Act.

7 *Hearing before Committee on Governmental Affairs, US Senate* (March 2, 2000) (Testimony of James Adams, Chief Executive Officer, Infrastructure Defense Inc.).

8 Adam Elkus, "Moonlight Maze" in Healy, *A Fierce Domain: Conflict in Cyberspace*, *1986 to 2012.*

9 Ryan Richard Gelinas, *Cyberdeterrence and the Problem of Attribution*, Master Thesis, Georgetown University, 2010, http://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/historical/gelinasRyan.pdf.

10 Marcia McGowan, "15 Years after Presidential Decision Directive (PPD) 63", *Booz Allen*, May 22, 2013, http://www.boozallen.com/content/boozallen/en_US/media-center/company-news/2013/05/15-years-after-pdd63-blog-post.html.

11 "Moonlight Maze", *PBS, Frontline*, April 24, 2003, www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/.

12 Office of the Press Secretary, "Fact Sheet: Protecting America's Critical Infrastructures, PDD 63", May 22, 1998, http://fas.org/irp/offdocs/pdd-63.htm.

13 שם.

14 שם.

15 Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown Publishing, 2014).

16 Ralph Langner, "Stuxnet's Secret Twin: The Real Program to Sabotage Iran's Nuclear Facilities was Far more Sophisticated than anyone Realized", *Foreign Policy*, November 21, 2013, http://foreignpolicy.com/2013/11/19/stuxnets-secret-twin/.

17 שם.

18 Irving Lachow, "The Stuxnet Enigma: Implications for the Future of Cybersecurity", *Georgetown Journal of International Affairs Special Issue: Cybersecurity* (2011): 118-126.

19 לדוגמה, יצירת מוסדות נוספים המנטרים, מתאמים, מפקחים, מעריכים, מגנים ותוקפים.

20 Adam Segal, "The Top Five Cyber Policy Developments of 2015: United States-China Cyber Agreement", *Council on Foreign Relations, Net Politics (blog),* January 4, 2016, http://blogs.cfr.org/cyber/2016/01/04/top-5-us-china-cyber-agreement/.

21 Guest Blogger, "The Top Five Cyber Policy Developments of 2015: The WSIS+10 Review", *Council on Foreign Relations, Net Politics (blog)*, December

22, 2015, http://blogs.cfr.org/cyber/2015/12/22/the-top-five-cyber-policy-issues-of-2015-the-wsis10-review/.

22 Federal Trade Commission, "US-EU Safe Harbor Framework", July 25, 2016, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/u.s.-eu-safe-harbor-framework.

23 Executive Order No. 12333, United States Intelligence Activities (December 4, 1981), *Central Intelligence Agency*, https://www.cia.gov/about-cia/eo12333.html.

24 "The Organizational Arrangements for the Intelligence Community", *Federation of American Scientists*, February 23, 1996, http://fas.org/irp/offdocs/int009.html.

25 Eric Rosenbach and Aki J. Peritz, "Cyber Security and the Intelligence Community", in *Confrontation or Collaboration? Congress and the Intelligence Community*, ed. Eric Rosenbach (Harvard Kennedy School: Belfer Center for Science and International Affairs, 2009).

26 *Worldwide Threat Assessment of the US Intelligence Community*, Statement for the Record by James R. Clapper, Director of National Intelligence, before the US Senate Armed Security Committee, February 26, 2015, http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf.

27 Kristen Eichensehr, "Cybersecurity in the Intelligence Community's 2015 Worldwide Threat Assessment", *JustSecurity*, March 6, 2015, https://www.justsecurity.org/20773/cybersecurity-u-s-intelligence-communitys-2015-worldwide-threat-assessment/.

28 "Norse Intelligence Platform", *Norse*, http://map.norsecorp.com.

29 Eichensehr, "Cybersecurity in the Intelligence Community's 2015 Worldwide Threat Assessment".

30 Department of Defense, "The DoD Cyber Strategy", April 17, 2015, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_Cyber_ Strategy_for_web.pdf.

31 שם.

32 Andrew Meola, "Cyber Attacks against our Critical Infrastructure are likely to Increase", *Business Insider*, May 26, 2016, http://www.businessinsider.com/cyber-attacks-against-our-critical-infrastructure-are-likely-to-increase-2016-5.

33 שם.

34 שם.

35 Aaron Brantly, "Defining the Role of Intelligence in Cyber", in *Understanding the Intelligence Cycle*, ed. Mark Phythian (London and New York: Routledge, 2013).

36 שם.

לקחים מ"החליפות הוויראלית": אפקט ויראלי ככלי חדש ללוחמה פסיכולוגית?

מירון לָקוֹמִי

מאמר זה מבקש לנתח היבטים פחות ידועים במה שמכונה קמפיין הסייבר־ג'יהאד של המדינה האסלאמית, במטרה לחשוף את התרומה הפוטנציאלית של קמפיין זה ללוחמת מידע הנעשית במימון מדינתי. ראשית יוצגו המאפיינים המרכזיים של הקמפיין המקוון של "החליפות האסלאמית", אשר נועד ליצור "אפקט ויראלי". בהמשך יובא מבט כללי על עימותים צבאיים מהעבר, שבמהלכם ניתן היה להבחין בהיווצרותו של אפקט ויראלי. לבסוף, ובהסתמך על ניתוחים אלה, ינסה המאמר להשיב על השאלה כיצד שיטות ומנגנונים של שיווק ויראלי יכולים לשמש ככלי רב ערך ללוחמה פסיכולוגית.

מילות מפתח: סייבר־ג'יהאד, תעמולה בסייבר, לוחמת מידע, PSYOPS, לוחמה פסיכולוגית, אפקט ויראלי, שיווק ויראלי

רקע

לוחמת מידע[1] כובשת בהדרגה מקום מרכזי בעימותים צבאיים עכשוויים.[2] כפי שכבר הוכיחו דוגמאות עדכניות רבות, מניפולציה על מידע היא קריטית להשגת יתרון על היריב.[3] אחת הדרכים לעשות זאת היא באמצעות השימוש במבצעים פסיכולוגיים (psychological operations)[4] שמכוונת להשפיע על הגישות וההתנהגות של אוכלוסיות עוינות, להדוף תעמולה ודיסאינפורמציה של היריב ולבסס אמינות בקרב קהל היעד. עד תום המלחמה הקרה, יעדים אלה הושגו באמצעות שיטות מגוונות אם כי לא מתוחכמות, כמו רמקולים, עלונים מוצנחים, תוכניות רדיו, ספרי קומיקס, כרזות וכן סרטוני פרסומת ומבזקים בטלוויזיה.[5]

התפשטות רשת האינטרנט בסוף המאה העשרים הביאה לעידן חדש בלוחמת המידע. מרחב הסייבר, בהיותו זירה חדשה של פעילות אנושית רב־ממדית, התגלה

מירון לקומי הוא פרופסור אורח במכון למדעי המדינה ועיתונות, האוניברסיטה של שלזיה, קטוביץ, פולין.

כבעל מאפיינים רבים וייחודיים המאפשרים סוגים חדשים של פעולות מידע, תוקפות ומתגוננות גם יחד.[6] אחת הבסיסיות שבהן תוארה היטב על ידי Fitch: "כאשר אני תוהה לגבי ההשפעה של האינטרנט על חשיבתי, שב ועולה בי תמיד אותו דימוי. החידוש המהותי באינטרנט הוא טיפולוגיית הקשר של רבים מול רבים שהוא מציע. לפתע, כל שני אנשים המצוידים בכלי זה יכולים להעביר ביניהם מידע חיוני בצורה גמישה ויעילה. אנחנו יכולים להעביר מילים, קודים, משוואות, מוזיקה וסרטים בכל זמן לכל אחד, ולרוב גם בחינם".[7]

השימוש בלוחמת מידע במרחב הסייבר אינו תופעה חדשה. דוגמאות מהעבר, כמו הפלישה האמריקאית לעיראק או המלחמה בקווקז ב־2008, מעידות כי התעמולה בסייבר נשענה בדרך כלל על התאמת האמצעים של לוחמה פסיכולוגית מסורתית לסביבה האלקטרונית. במקום עלונים ורמקולים, נעשה שימוש רב בספאם בסיסי שהופץ בדואר אלקטרוני או כתגובות באתרי אינטרנט. כרזות הפכו לבאנרים ולהודעות שפורסמו באתרים שנפרצו וברשתות חברתיות.[8] מבזקי טלוויזיה הופיעו כסרטונים שהופצו דרך שירותי אירוח פופולריים כמו *YouTube* או *LiveLeak*.[9]

נכון להיום, מרחב הסייבר מאופיין במסיביות שלו (מעל 3.3 מיליארד משתמשים ב־2016) וביכולת הקישוריות ההדדית שהוא מציע, שביחד עם הדומיננטיות של המכשירים הניידים פותח אפשרויות ייחודיות ומשוכללות יותר לתעמולה במובנה הרחב. פוטנציאל זה כבר התממש ונוצל על ידי ארגון המדינה האסלאמית (דאע"ש): קמפיין הסייבר־ג'יהאד שבו החל ב־2014 הביא לכך שיעדיו המרכזיים של הארגון ידועים היום בכל רחבי העולם, או במילותיה של קריסטינה סקורי ליאנג (Schori Liang): "דאע"ש הביאו את הסייבר־ג'יהאד לרמה חדשה לחלוטין [...] הקמפיין שרשם הצלחה עצומה הפך לכלי אפקטיבי ללוחמה פסיכולוגית ולגיוס המונים".[10] כמובן שהפעילות המקוונת הזו הפכה למטרה למחקרים מדעיים נרחבים. לכן, מפתיע שחוקרי האקדמיה עדיין לא הבחינו בכך שדאע"ש מנצל מנגנונים וטכניקות ייחודיים לשיווק ויראלי לצורך הגברת יעילותה של תעמולת הארגון.

למאמר זה יש שלוש מטרות: ראשית, להציג את המאפיינים המרכזיים של הקמפיין המקוון של "החליפות האסלאמית", אשר יצרו את "האפקט הוויראלי"; שנית, להציג סקירה כללית של עימותים צבאיים מהעבר, שבהם ניתן לזהות אפקט ויראלי; שלישית, לאור תובנות אלו, לענות על השאלה כיצד השיטות והמנגנונים של השיווק הוויראלי יכולים לשמש ככלים רבי ערך בלוחמה פסיכולוגית. בסיכום, המאמר ינתח היבטים בקמפיין הסייבר־ג'יהאד של דאע"ש שעדיין לא זכו לתשומת לב מספקת, כדי להצביע על התועלת הפוטנציאלית שיש לקמפיין זה בלוחמת מידע המתנהלת בחסות מדינה.

המאמר מחולק לשלושה חלקים: החלק הראשון ינסה לשרטט את תופעת האפקט הוויראלי מנקודת המבט של התועלת הפוטנציאלית שלה ללוחמה פסיכולוגית; החלק השני יציג סקירה קצרה של העימותים שבהם תעמולה הפכה לוויראלית; החלק האחרון יתמקד ב"חליפות הוויראלית", כלומר בסיבות שהביאו לכך שהאפקט הוויראלי בפעילות הסייבר־גי'האד של דאע"ש הצליח במידה כה רבה.

אפקט ויראלי – הגדרה

האפקט הוויראלי הוא פונקציה של מחקר עומק בשיווק, שגילה כי מרחב הסייבר מאפשר את התפתחות המנגנון הידוע בכינוי "פה לאוזן". אפשר להגדיר זאת כשימוש בגורמים משפיעים "כדי ליצור 'באז' או המלצות למוצר בשיטת 'חבר מביא חבר'".[11] היסטורית, שיטת "פה לאוזן" הייתה תלויה לחלוטין בקשר פיזי ישיר בין אנשים, דבר שהגביל את הכיסוי הגיאוגרפי שלה ואת שיעור תפוצת המסר.[12] בעידן מהפכת המידע, "פה לאוזן" התפתח לכדי שיווק ויראלי, שמוגדר על ידי מריה וורנדל (Woerndl) ואחרים כ"העברה של מסרים שיווקיים דרך ערוצי אינטרנט שונים באמצעות חברים, במהלכה עובר המידע בין אנשים ללא מעורבות של מקור המסר המקורי, ומתפשט כמו וירוס המדביק את המארחים".[13]

טכניקות של שיווק ויראלי מכוונות אפוא לעורר את "האפקט הוויראלי". ניתן להגדיר אפקט זה באופן כללי כתהליך של התפשטות מעריכית (exponential) של המסר בצורה מקוונת, במהלכה אנשים ש"נדבקו" מהתוכן משתפים בו את חבריהם דרך הסביבה האלקטרונית. תבנית מסר כזה משתנה, ונעה מהודעות דוא"ל פשוטות, אתרי אינטרנט ותמונות (כמו "ממים"), עד משחקים, סרטונים, מוזיקה ומסמכים. בעיקרון, בהינתן התנאים המתאימים, כמעט כל צורה של תוכן לא מקובל יכולה להביא אנשים להפיץ אותו בקרב חברים, עמיתים ובני משפחה.

המונח "שיווק ויראלי" הוטבע על ידי סטיב ג'רוטסון (Jurvetson) וטים דרייפר (Draper) כדי לתאר את ההתרחבות הדינמית של *Hotmail* ב־1996, לאחר שהחברה פרסמה את שירותיה בדוא"ל היוצא של המשתמשים שלה, וכתוצאה מכך גדלה פי 25 במהלך תקופה של שנה אחת.[14] במאה ה־21, טכניקות של שיווק ויראלי מתמקדות בעיקר בשימוש בסרטונים קצרים, מעניינים ולא שגרתיים.

אחד הקמפיינים הראשונים של שיווק ויראלי נעשה על ידי חברת מערבלי המזון "BlendTec", שיצרה סדרה של סרטונים מקוונים תחת הכותרת "האם זה יתערבב?". הסרטונים הציגו מבחנים למוצרים של החברה, שעשו שימוש בפריטים לא רגילים, כמו סמארטפונים יקרים, לוחות עץ או שעונים. הגישה הייחודית קלעה היטב למטרה, והסִדרה הפכה לוויראלית. חשבון ה"יוטיוב" של "BlendTec" הפך עד מהרה לפופולרי מאוד (200,000 מנויים ב־2009) והמכירות קפצו ב־700

אחוזים.[15] מאז ניסו חברות רבות להשתמש בטכניקות של שיווק ויראלי, אם כי מעט מאוד הצליחו בכך. ביניהן כדאי להזכיר את "קפיצת החלל של רד בול", את "אני על הסוס" של "Old Spice", ואת "מתיחת המעלית" של LG.[16]

האפקט הוויראלי אינו מוגבל רק לפרסומות מקצועיות. אותם מנגנונים מנוצלים גם על ידי חובבנים. למעשה, חלק גדול מהתוכן שהופך לוויראלי נוצר לצורכי שעשוע ולא למטרות רווח, ומתפרסם ברשתות החברתיות כמו "יוטיוב", "פייסבוק", "רדיט", "טוויטר", "אינסטגרם", "טמבלר", ובמקבילות ממשלתיות שלהן (כמו *VKontakte*). מרבית המפרסמים מערבים אירועים ומצבים אקראיים, בדרך כלל מגוחכים, מעוררי עניין, חריגים, רגשניים או מושכים, שתופסים את עיניהם של "אזרחי הרשת" ("Netizens"), אשר בסופו של דבר הם אלה שאחראים להתפשטותו העתידית של התוכן. אחרים כוללים אזכורים יוצאי דופן שמתייחסים לתרבות ההמונים.[17]

בהקשר זה חשוב להדגיש שהמאפיינים שיוצרים את האפקט הוויראלי יכולים תיאורטית לשמש גם להגדלת ההיקף והיעילות של הלוחמה הפסיכולוגית: האפקט הוויראלי מבטיח תפוצה מהירה ומעריכית של מסרים ואת הגעתם לאוכלוסיות מגוונות, בזכות התכונה של הרשת החברתית ליצור אינטראקציות רב־שכבתיות. דבר זה אינו אפשרי בשיטות מסורתיות של לוחמה פסיכולוגית במרחב הסייבר. יתרה מכך, ההפיכה לוויראלי היא תהליך חמקמק ולא יקר מטבעו, שכן העברת המסרים תלויה אך ורק במקבלי המסר, שהם קהל היעד לתעמולה מקוונת בכל עימות צבאי.[18] לבסוף, בהשוואה לטכניקות קלאסיות, הן של לוחמה פסיכולוגית והן של פרסום מסורתי, שיטות שיווק ויראלי יכולות להיתפס כפחות מטרידות וכיותר אמינות, ובכך לצמצם השלכות שליליות אפשריות של קמפיין תעמולתי.[19]

הגדלת הסיכויים להתרחשות אפקט ויראלי בלוחמה פסיכולוגית תלויה במספר תנאים: הראשון הוא שהמראה ייגזר מתוכן המסר ויוצג בצורה מעניינת, לא שגרתית וקלה לקליטה. הומור, אלימות ומיניות הם בדרך כלל נושאים שמשפיעים על אנשים להעביר את המסר הלאה, שכן הם הדרך הקלה ביותר לעורר רגשות.[20] תכונה זו היא מכרעת בלוחמת מידע, שכן רגש יכול "להדביק" את הנמענים ברעיון ולעודד אותם להפיץ אותו. יתרה מכך, למרות שהאפקט הוויראלי נבחן בהצלחה ב"וב 1.0", שהכיל בעיקר תוכן סטטי ("רשת לקריאה בלבד"),[21] כיום הוא תלוי אך ורק בשימוש המתוחכם של הרשת החברתית. הודות לפופולריות של שירותים דוגמת "פייסבוק", "טוויטר", "אינסטגרם" או "יוטיוב", והחיבור ההדדי (פונקציית השיתוף) שהם מציעים, מסר מעניין דיו יכול להתפשט באופן מעריכי ולהגיע כמעט מיידית לקהלים בכל העולם. די בשיתוף אחד בחשבון פופולרי ברשת חברתית בכדי לעודד אלפים ואפילו מיליונים ללחוץ על הקישור.[22]

יש לכך קשר ישיר לסוגיה הרחבה יותר של טופולוגיית הרשת, שכמובן משפיעה על התפשטות המידע. Pastor-Satorras ו־Vespignani הדגישו בהקשר זה: "לטיפולוגיה של הרשת יש השפעה רבה על ההתנהגות הכוללת של תהליך התפשטותה של מגיפה. התנודות בקישוריות הרשת משחקות תפקיד מרכזי, בכך שהן מגבירות משמעותית את שכיחות ההידבקות".[23] אולם יש הבדל בין התפשטות וירוס להתפשטות מידע. לפי Barabási ואחרים, מידע מתפשט מתוך כוונה תחילה, בעוד שווירוס לא מתנהג כך, ולכן המידע מציג התנהגות מורכבת יותר.[24] כמו כן, יעילות ויראלית תלויה ברמת ההתפתחות של טכנולוגיית המידע והתקשורת של המדינה/החברה הרלוונטיות. מדינות לא מפותחות מבחינה אלקטרונית חשופות פחות לתעמולה מקוונת. לעומתן, חברות בעלות תלות גבוהה בתקשורת אלקטרונית מהוות יעד הולם יותר לתעמולה כזאת, שכן למסר המניפולטיבי יהיה סיכוי רב יותר להפוך לווירואלי הודות לכמות ולאיכות האינטראקציות המקוונות.

לבסוף, סביר להניח שאוכלוסיית היעד תיטה לעשות שימוש מופחת באינטרנט במהלך משבר או עימות, כאשר תשומת הלב מוסטת מהפעילות היומיומית ברשת, ואף תהיה אז הרבה יותר חשדנית כלפי תוכן מקוון בלתי מוכר, כך שהאפקט הווירואלי יהיה לכאורה קשה יותר להשגה. אולם, כפי שניתן ללמוד מהניסיון של "האביב הערבי",[25] אפילו במהלך משברים חמורים אנשים נוטים לעשות שימוש רב בתקשורת אלקטרונית לצורך איסוף מידע או תיאום פעילות. מסיבה זו, במרבית המצבים עדיין ניתן יהיה לחולל אפקט ויראלי שיהדהד בכל הסביבה האלקטרונית של קהל היעד.

לסיכום, מסרים ויראליים, בין אם למטרת רווח ובין אם לא, בין אם נעשו על ידי חובבנים ובין אם על ידי מקצוענים, הם בלתי שגרתיים מטבעם ובולטים בתוך גודש המידע באינטרנט, ומכאן ההסבר לפופולריות שלהם. פעמים רבות הם חורגים משיטות טיפוסיות של תקשורת מקוונת, וכך מושכים את תשומת הלב של משתמשי האינטרנט. האפקט הווירואלי מבקש למשוך את תשומת הלב של משתמשי הרשת במטרה להדביק אותם ברעיון, בתפיסה או במותג, שיועברו בתורם למשתמשים אחרים באמצעות שלל ערוצי הרשתות החברתיות. מגמה בקנה מידה כזה הייתה בלתי אפשרית ללא המדיה החברתית העכשווית ויישומיה. כתוצאה מכך, המסרים הווירואליים צמחו כתופעה עוצמתית וחדשה בתקשורת המקוונת. באמצעות ניצול רגשות וסקרנות, הם בעלי יכולת ברורה להשפיע על האופן שבו משתמשי האינטרנט תופסים סוגיות שונות ופועלים ברשת. מצב זה יכול להיות מנוצל בנסיבות מסוימות על ידי אנשי לוחמה פסיכולוגית מיומנים.

לוחמת מידע הופכת לוויראלית

בהמשך לשיקולים ולהסברים שפורטו לעיל, ראוי לציין שהאפקט הוויראלי אינו חדש בממד המקוון של המלחמות. מאז תחילת המאה ה־21 התלוותה לעימותים חמושים גם תעמולה בסייבר, בעיקר בעקבות התפשטות המכשירים הניידים המצוידים במצלמות, כמו הסמארטפונים, והתפתחות טכנולוגיות "וב 2.0".[26] שתי התפתחויות אלו הביאו לכך שהאינטרנט נשטף בתמונות ובסרטונים המתעדים אירועי מלחמה שונים, שחלקם היו כה חריגים, עד שהצליחו להפוך לוויראליים ברמות שונות. כמה מהדוגמאות הראשונות התרחשו במהלך הפלישה האמריקאית לעיראק ב־2003 והמלחמה בקווקז ב־2008. אולם השינוי האמיתי החל במהלך "האביב הערבי", שהוכיח את היכולת של הרשתות החברתיות להשפיע על גישות פוליטיות ועל מצב הרוח של אוכלוסיות. ב־2011 היו אלה אקטיביסטים במזרח התיכון שעשו שימוש נרחב בכלים של "וב 2.0" כדי להתארגן, לקדם סדר יום פוליטי ולעודד אוכלוסיות למרוד נגד משטרים רודניים.[27] לכן, אין זה מפתיע שאותם פעילים פוליטיים שנטלו חלק במהפכות "האביב הערבי" עשו שימוש בניסיון העשיר שצברו הרשתות החברתיות כדי לנהל תעמולה במהלך העימותים הצבאיים שהגיעו בהמשך. התוכן המניפולטיבי החדש ורחב־ההיקף ששוחרר לרשת יצר אפקט ויראלי בכמה אירועים מעניינים.

מלחמת האזרחים שהשתוללה בלוב ב־2011 בין המורדים שפעלו בגיבוי מדינות המערב ובין משטרו של מועמר קדאפי הייתה המקרה הראשון בהיסטוריה שבו נעשה שימוש ברשת החברתית בהיקף כה רחב, עד שהדבר השפיע על דעת הקהל הבין־לאומית. זמן קצר ביותר לאחר פרוץ הקרבות נשטף האינטרנט בסרטונים ובתמונות שתיעדו לחימה נגד משטר קדאפי. הסרטונים והתמונות הכילו לא פעם גם הצהרות או מניפולציות שנועדו להשיג תמיכה חיצונית. הצד הטכני והתוכני שלהם היה בדרך כלל חובבני, ולמרות זאת, בשני מקרים הם יצרו אפקט ויראלי: הראשון היה בתמונה המפורסמת של "גיבור הגיטרה מלוב", שעד מהרה הופצה דרך שירותי אירוח תמונות שונים[28] ותרמה לדימוי החיובי של המורדים הלובים. עקב החריגות של התמונה, שמיזגה שתי תמות שונות – ירי ומוזיקה – היא תפסה מהר למדי את תשומת לב התקשורת, שהפיצה את המסר גם במערב.[29] התוצאה הייתה, ככל הנראה, הפצת התמונה למאות אלפי אזרחי רשת.

השימושיות של האפקט הוויראלי לצורכי לוחמה פסיכולוגית זכתה לאישור גם במקרה נוסף – מותו של מועמר קדאפי באוקטובר 2011, שתועד מכמה זוויות והועלה לאינטרנט על ידי המורדים זמן קצר לאחר מכן. בתוך שעות ספורות בלבד הופצו בכל שירותי החדשות באינטרנט וברשתות החברתיות סרטונים שהראו את הלינץ' הברוטלי בדיקטטור לשעבר. עד מהרה הועתקו הצילומים גם בתחנות טלוויזיה מובילות כמו *CNN*, *BBC* ו־*NBC*.[30] למעשה, תיעוד האירוע הפך בשעתו

להיות התוכן הפופולרי ביותר לא רק באינטרנט, אלא גם בתקשורת העולמית. עשרות עותקים של הלינץ' הועלו ב"יוטיוב" בלבד וצברו מיליוני צפיות. לשם דוגמה, הגרסה של "אל־ג'זירה", שפורסמה ב־20 באוקטובר 2011 על ידי משתמש "יוטיוב" בשם xciter79, צברה יותר משישה מיליון צפיות עד 2016. הגרסאות שפורסמו על ידי חדשות רשת *ABC* ו"אל־ערביה" נצפו מעל מיליון פעם כל אחת.[31]

הסרטונים המציגים את הרגעים האחרונים של קדאפי נצפו בכל העולם עקב האפקט הווירואלי העצום שהם עוררו. האפקט הווירואלי הושג משום שצילומים אלה שילבו כמה מאפיינים חשובים: הם היו מזעזעים וכללו תוכן מפורש לחלוטין. תוכן מפורש לבדו לא מושך תשומת לב, במיוחד כאשר האינטרנט גדוש בחומרים המוגבלים לצפייה מגיל 18 ומעלה; אלא שסרטונים אלה הציגו בפירוט את מותו של דיקטטור שהיה שנוא ברחבי העולם – דבר חריג מאוד כשלעצמו. מותו של קדאפי סימן באופן סמלי את תום מלחמת האזרחים בלוב, שהייתה עימות אחריו עקבה מקרוב הקהילה הבין־לאומית כולה. כל הגורמים האלה חברו ביחד ליצירת האפקט הווירואלי הגדול והבולט ביותר שנרשם במהלך עימות צבאי עד היום.

לקח זה הופנם במהרה על ידי המורדים בסוריה, שהחלו לפרסם כמות אדירה של תעמולה מקוונת. למרות שהאופוזיציה למשטרו של חאפז אל־אסד עושה שימוש נרחב בסביבת "וב 2.0" כדי לעורר תמיכה מקומית ובין־לאומית, הניסיונות שלה כשלו ברובם, שכן הם כללו שחרור סרטונים ותמונות שהציגו לראווה פעולות טרור או פשעי מלחמה שהם עצמם ביצעו.[32] בורות זו באה לידי ביטוי בסרטון של מפקד המורדים אבו סקאר, שבו הוא נראה משחית גופה של חייל סורי ואוכל את בשרה. כפי שהסביר אבו סקאר מאוחר יותר בראיון לרשת *BBC*, הוא עשה זאת כדי לעורר אימה באויבים,[33] אך הסרטון הפך לווירואלי בשל האכזריות חסרת התקדים שהראה. השפעתו הייתה מנוגדת לחלוטין למה שרצו המורדים להשיג, שכן היא העמיקה את אי־האמון של מדינות המערב באותם מורדים שנחשבו ל"מתונים".

האפקט הווירואלי התגלה גם בלוחמת המידע שהתנהלה במהלך העימות האחרון באוקראינה. למרות שהתעמולה הרוסית הרשמית התמקדה בעיקר בתקשורת המסורתית, כמו ערוצי טלוויזיה, תחנות רדיו ועיתונים, מריה סנגובאיה (Snegovaya) מציינת כי האקרים, "בוטים" ו"טרולים" מילאו תפקיד חשוב בקידום התעמולה הרוסית בסביבת הרשת.[34] תועמלנים פרו־רוסיים העלו לרשת סרטונים מניפולטיביים וערכו תמונות בכל הרשתות החברתיות, כמו *VKontakte*,[35] במטרה לזרוע פחד בקרב האוכלוסייה באוקראינה, לאיים על מדינות המערב, לעוות את תפיסת המאורעות ולקדם את סדר היום של הקרמלין.

האפקט הווירואלי ניכר באופן מרשים בשני מקרים בולטים מתוך שפע צעדי התעמולה הרוסית ברשת: המקרה הראשון נגע לתמונה של חייל אוקראיני לכאורה, שטען בצורה לא נכונה את התחמושת ל־RPG־7. התמונה נערכה על

ידי תועמלנים פרו־רוסיים[36] ופורסמה ברשת כדי להגחיך את מאמצי המלחמה של אוקראינה. התמונה פורסמה באתרים כמו *reddit.com* ו־*epicfail.com*, שם היא נצפתה ושותפה על ידי אלפי משתמשי אינטרנט.[37] המקרה השני היה הוכחה לכך שגם לתעמולה פרו־רוסית יש חסרונות לא קטנים. אחד מה"מסמכים" שפורסם על ידי כלי תקשורת מטעם הקרמלין במרחב הסייבר תיאר את הטיפול הרע בשבוי אוקראיני בדונצק.[38] הכוונה המקורית הייתה לפגוע במורל האוכלוסייה האוקראינית, אולם במקום זאת המסמך עורר אפקט וירואלי מסוים, שכן עד מהרה הוא הופץ בכל שירותי החדשות המערביים באינטרנט וברשתות החברתיות, והפך לסמל לברוטליות ולפשעי המלחמה שמבצעים המורדים הנתמכים על ידי הקרמלין.[39]

המקרה של "החליפות הווירואלית"

הדוגמאות שפורטו לעיל מוכיחות שלושה דברים: ראשית, האפקט הווירואלי יכול בנסיבות מסוימות ללוות לוחמה פסיכולוגית; שנית, תוכן מניפולטיבי יכול להפוך לווירואלי ללא כוונה ספציפית, כתופעת לוואי של פעילות תעמולתית רגילה ברשת; שלישית, התועמלנים לא תמיד מודעים למנגנונים אלה.

ניתן להבחין כי הסייבר־ג'יהאד עושה שימוש מכוון באפקט הווירואלי לצורך הגברת היעילות והטווח של קמפיין התעמולה המתקדם שלו.[40] דאע"ש מוכיח כי הצליח לשנות את השיטות הרגילות שאפיינו את הסייבר־ג'יהאד ולהעצים את הסיכויים להתרחשות אפקט וירואלי. מי שאחראים לאימוץ גישה זו הם תאי דאע"ש העוסקים בלוחמה פסיכולוגית, קרי מרכז התקשורת "אל־חיאת" שהוקם ב־2014. המרכז מורכב מאנשי מקצוע מיומנים, כמו אמני גרפיקה ממוחשבת, מוזיקאים לשעבר,[41] צלמי קולנוע, עורכים ומומחים למניפולציות. למרות שמעט מאוד ידוע על כוח האדם שמרכיב את ארגון המדינה האסלאמית, מוצר המולטימדיה המתוחכם והמשוכלל מבחינה טכנולוגית שהוא מפיק מדבר בעד עצמו ומוכיח כישרון וידע.

למרכז המדיה "אל־חיאת" יש שתי מטרות עיקריות ידועות. האחת, לזכות בתמיכה כללית של חברות מוסלמיות ברחבי העולם, ובמיוחד במזרח התיכון ובאירופה. יעד זה נועד להיות מושג בכמה דרכים, כמו למשל סרטוני גיוס המעודדים את הצופים להצטרף לשורות ארגון המדינה האסלאמית או לקחת חלק בפעילות טרור במערב.[42] המטרה השנייה היא לזרוע פחד ובלבול בחברות המערביות. מטרה זו אמורה להיות מושגת בדרך כלל על ידי הצגה בוטה של זוועות ומעשים ברבריים של אנשי דאע"ש. עם זאת, כפי שטוענים גבי סיבוני, דניאל כהן וטל קורן, עריפות הראשים על ידי אנשי הארגון, שזכו לפרסום כה רב, יכולות להיתפס גם כחלק מהאסטרטגיה של דאע"ש המיועדת לפנות לאוכלוסיות

מוסלמיות ולזכות בתמיכתן. לדבריהם, "זהו מוקד משיכה למתגייסים פוטנציאליים, באמצעות פריטה על נימי המוסר האסלאמי הבסיסי, כחלק מהחזרה לעקרונות היסוד של האסלאם הקדום".[43]

מכונת התעמולה של המדינה האסלאמית פועלת כדי להשיג מטרות אלו על ידי תכנון מעשיה במרחב הסייבר באופן שימקסם את הסיכויים ליצירת אפקט וירואלי. כמה עובדות מעידות על כך: ראשית, קמפיין התעמולה של דאע"ש מתבסס על שימוש רחב ומתוחכם במיוחד ברשתות החברתיות.[44] מספר החשבונות ששיתפו תעמולה של דאע"ש בשנת 2014 ב"טוויטר" בלבד נע בין 46,000 ליותר מ־70,000. ממוצע העוקבים של חשבונות ה"טוויטר" התומכים במדינה האסלאמית עומד על כאלף לכל חשבון.[45] המדינה האסלאמית גם מנצלת רשתות חברתיות אחרות, אפליקציות עמית־לעמית (*Telegram* ו־*Surespot*) ושירותים של שיתוף תוכן (*JustPaste.it* ו־*Archive.org*).[46] כמו כן, הארגון עושה שימוש רב בשירותים שונים לשיתוף סרטונים, החל מהפופולרי ביותר דוגמת "יוטיוב" ועד לשנויים במחלוקת דוגמת *LiveLeak* והאתר הקנדי השנוי במחלוקת *BestGore.com*.[47] כתוצאה מכך, ההיקף והמגוון של פעילות הסייבר־ג'יהאד ברשתות החברתיות הוא חסר תקדים. זהו גם תנאי מפתח ליצירת האפקט הווירואלי, שכן הרשת החברתית מציעה נקודות כניסה רבות לתעמולת דאע"ש, וכך מתאפשרת העברה מהירה של מסרי הארגון.

שנית, הצד הטכני של פרסומי המדינה האסלאמית הוא כמעט מושלם, ורמתם הטכנית מושווה לעתים לזו של סרטים הוליוודיים.[48] מרכז התקשורת "אל־חיאת" עושה שימוש בשיטות ובציוד להפקה באיכות גבוהה במיוחד, כולל וידאו־גרפיקה, עריכה, גרפיקה ממוחשבת, אפקטים קוליים וצילומים. צ'רלי וינטר, המדגיש תופעה זאת, טוען כי "אין ספק שהמאמץ שהושקע בהפקת *Although the Disbelievers Dislike it* היה יוצא דופן. ניכר שתוכן הסרטון נבחר בקפידה, ומי שביים או ביימו אותו היו ללא ספק מקצוענים [...] הציוד שדאע"ש הקפיד לא לעשות בו שימוש – במיוחד המצלמות – המחיש את הרמה המקצועית של ההפקה".[49] כאן נכנס לתמונה גורם הייחודיות. האיכות הטכנית של תעמולת דאע"ש מבדלת עצמה מהפקות אחרות של הסייבר־ג'יהאד. לא ניתן להשוות את הגרסאות הגולמיות של "אל־קאעדה", "א־שבאב" או "בוקו חראם", לדוגמה, לסרטים שמפיק דאע"ש בסגנון הוליוודי, ברזולוציית HD ובתרגום רב־לשוני. יותר מכך, ההפקות של דאע"ש תואמות את הרגלי התקשורת של הקהל המערבי, כך שהן מעלות באופן טבעי את הסיכויים להיות בעלות אפקט וירואלי.

דאע"ש מרבה לאמץ צורות לא שגרתיות של תעמולה בהשוואה לרוב הפרסומים שנעשו במסגרת הסייבר־ג'יהאד, ואלו מושכות את תשומת הלב גם של אזרחי המערב. המסרים שמפיק מרכז התקשורת "אל־חיאת" מתייחסים תכופות ליצירות קאנוניות בתרבות ההמונים או בסייבר. לדוגמה, אחד הסרטונים

של הארגון עשה שימוש במותג הימורים פופולרי במיוחד.[50] דוגמאות אחרות הן *#mujatweets* ב"טוויטר",[51] שימוש נרחב ב"ממים", ופסקול של "נשידים" המעוצב בסגנון אמריקאי. אלה משולבים לעתים במצגים של אכזריות ברברית, כמו עריפת ראשים או התעללות בגופות, וזאת במטרה לעורר רגשות עזים. הניגוד החד בין קלישאות מוכרות מתרבות הסייבר ובין זוועות נוראיות הינו ייחודי לתעמולה של הסייבר־ג'יהאד. חיבור כזה מפתה במיוחד צעירים, המגיבים אליו יותר מאשר להצהרות המשעממות שפורסמו בעבר על ידי דמויות כמו אוסמה בן לאדן. האזכורים הברורים של תרבות הסייבר ותרבות ההמונים מאפשרים לקהלי היעד להבין טוב יותר את המסר ולאמץ אותו, ובכך הם גם תומכים במנגנון הוויראלי. ארגוני טרור לא שחררו מעולם סרטונים ותמונות עם תוכן בוטה, וגם לא מוזיקה כתעמולה המכוונת לקהל הצורך בידור מערבי. השימוש בכלים אלה על ידי דאע"ש כיום מושך מטבעו את תשומת לבם של אזרחי הרשת, דבר שהוא תנאי הכרחי להצתת האפקט הוויראלי.

כאמור, ארגון המדינה האסלאמית משלב בין השיטות האופנתיות ביותר בתקשורת המקוונת – רשתות חברתיות ואפליקציות פופולריות – ובין התקדמות טכנולוגית, ברבריות אכזרית ותחכום מניפולטיבי בהיקף חסר תקדים.[52] זהו המפתח להצלחה התעמולתית הגדולה שהארגון רשם, אשר באה לידי ביטוי בולט בהיקף ובתפוצה של סדרת הסרטונים המציגים עריפות ראשים של אזרחים מערביים (כמו ג'יימס פולי, סטיב סוטלוף, דיוויד היינס ואלן הנינג). עריפות ראשים אלו התפרסמו מאוגוסט 2014 ואילך והפכו לוויראליות בקנה מידה עולמי בתוך זמן קצר משחרורן לרשת. ישנן כמה תכונות שתרמו לאפקט הוויראלי של סרטונים אלה: הרמה הטכנית הגבוהה שלהם (שצוינה לעיל), הברוטליות הישירה שהוצגה בהם, והתוכן המניפולטיבי המתוחכם שניתן היה לראות בהצהרות של האסירים ושל "גון הג'יהאדיסט". ולבסוף, כל הסרטונים ניצלו את אותם שירותי שיתוף סרטים, לרבות "יוטיוב", *LiveLeak*, *BestGore* ורשתות חברתיות אחרות, שהבטיחו את תפוצתם המיידית באינטרנט. למעשה, הם שילבו את גורם הייחודיות עם תעמולה מקצועית, באמצעות נקודות כניסה מרובות לרשתות החברתיות.

סרטוני עריפות הראשים הפכו לקטעים המצליחים ביותר בהיסטוריה של תעמולת טרור וירלית. יש לכך מספר סיבות: ראשית, אף שקשה להעריך בדיוק כמה אנשים צפו באותם סרטונים או שמעו עליהם,[53] אפילו ההערכה הנמוכה ביותר עומדת על עשרות מיליונים. הצלחה זאת נבעה משני הווקטורים של התפוצה שהיו לקמפיין, שהיו קשורים ביניהם בקשר הדדי והפכו אותו לוויראלי: שירותי שיתוף סרטים והרשתות החברתיות. למרות שמנהלי המערכת מחקו לעתים קרובות את הגרסאות המקוריות, עותקים ערוכים או שלמים שלהן הופצו מיד ברשת, ככל הנראה כתוצאה מפעילותם של אזרחי רשת עצמאיים. ב"יוטיוב"

לבדו יש עדיין עשרות סרטונים מצונזרים של עריפת ראשים של דאע"ש שנצפו על ידי מיליוני משתמשים. שתי הגרסאות הפופולריות ביותר של ההוצאה להורג של ג'יימס פולי שפורסמו ב"יוטיוב" נצפו כמעט ארבעה מיליון פעמים (נכון למאי 2016). הגרסה המלאה של אותה הוצאה להורג פורסמה ב־*LiveLeak* ורשמה יותר ממיליון צפיות.[54]

עד מהרה זיהו גם עיתונאים את הסרטונים האלה, ואמצעי תקשורת מהמובילים בעולם, הן המסורתיים (חדשות בטלוויזיה) והן המקוונים (חשבונות "יוטיוב" רשמיים ואתרים ייעודיים) פרסמו תיעוד מצונזר ומקוצר שלהם במאות או אפילו באלפי עותקים, כשהם מלווים בפרשנות. רבים גם הכינו דיווחים משלהם על ההוצאות להורג, שלרוב כללו ציטוטים מההצהרות המניפולטיביות בסרטונים המקוריים. ניתן היה לראות מגמה זו כבר לאחר הפרסום הראשון של ההוצאה להורג של ג'יימס פולי, כאשר כל ערוצי התקשורת המקוונים והמסורתיים בעולם התמלאו בצילומי מסך, בגרסאות ערוכות ובתיאורים מפורטים. חיפוש סרטון ב"גוגל" עם המילים "James Foley" מעלה כ־322,000 תוצאות, שרובן קשורות להוצאה להורג.

חשוב לציין כי לשני הווקטורים האלה – שירותי שיתוף סרטים והרשתות החברתיות – יש יכולת הפצה עצמית: דיווחי התקשורת העלו את הסקרנות של אזרחי הרשת לצפות בסרטונים המקוריים, ואילו הפופולריות של הגרסאות הלא ערוכות העלתה את עניינם של הצופים בדיווחי התקשורת שבאו לאחר מכן. בדרך זו תרמה התקשורת בלא יודעין להצלחת הלוחמה הפסיכולוגית של דאע"ש, וחשפה קהלים למסרים שהארגון ביקש להעביר, גם אם אותם קהלים לא צפו בהקלטות המקוריות.

ההיבט הווירואלי של עריפות הראשים שביצעו אנשי דאע"ש בא לידי ביטוי בפופולריות של נושא זה בקרב המומחים והחובבנים בבלוגוספירה. פופולריות זו הביאה ליצירת כמות עצומה של תכנים המתייחסים לזוועות של דאע"ש. בתוכם אפשר לכלול ניתוחים שונים, פרשנויות ואפילו פרודיות. היקף המגמה מומחש בפופולריות של סרטון ה"יוטיוב" *ISIS Bloopers*, שהוא חיקוי (pastiche) של הוצאות להורג מבית היוצר של קומיקאים ישראלים. בין פברואר 2015 למאי 2016 נצפתה הפרודיה יותר מ־5.2 מיליון פעם.[55] שפע תוכן החובבים המתייחס לעריפות הראשים של דאע"ש מוכיח כי גורם "המגיפה" פעל במקרה זה היטב. אלמלא כן, משתמשי האינטרנט לא היו מקדישים זמן ומשאבים להכנת חומרים משלהם המתייחסים לאירועים אלה.

חשוב להדגיש שחשיפתם של מיליוני אזרחים מערביים לעריפות הראשים החריגות של דאע"ש, שהפכו לוויראליות בערוצים מקוונים ולא מקוונים וקיבלו חיזוק בדיווחים המדאיגים מהמזרח התיכון וממתקפות הטרור באירופה, תרמה

לחיזוק הפחד מפני ארגון המדינה האסלאמית, במיוחד במערב. הצלחת התעמולה של הארגון ניכרת בסטטיסטיקות של מכון המחקר פיו (Pew), המציין כי חברות מערביות רואות בדאע"ש את האיום מספר אחת על הביטחון העולמי.[56]

מסקנות

פעילות "החליפות הווירואלית" מציבה איום משמעותי בפני הביטחון הבין־לאומי, וספציפית מהווה סיכון מוגבר למיקרו טרור ולהעמקת הפחד והבלבול בקרב מדינות המערב. משום כך מעוניינות מדינות נאט"ו/האיחוד האירופי במדיניות אבטחת מידע שתטרפד מהר ככל האפשר את אסטרטגיית הסייבר של ארגון המדינה האסלאמית.

באופן פרדוקסלי, הצלחת השימוש באפקט הווירואלי על ידי המדינה האסלאמית במסגרת הלוחמה הפסיכולוגית שלה מובילה לכמה מסקנות באשר לשימושיות של אפקט זה: ראשית, אין כל דרך להבטיח כי מסר שנועד להפוך לווירואלי, כחלק מלוחמה פסיכולוגית, אכן יהפוך לכזה. מרקם היחסים האנושיים ברבדים השונים של האינטרנט הינו דינמי ומתעתע מכדי שניתן יהיה לנצל אותו בהצלחה בכל פעם. תכנון פעולות שיעמדו במאפייני התקשורת המקוונת המשתנים ללא הרף, כמו גם במגמות המשתנות ובמצב הרוח של אזרחי הרשת, אינו מלאכה פשוטה כלל ועיקר. ניסח זאת היטב דיוויד מירמן סקוט (Meerman Scott) כשאמר: "אין שום דרך להבטיח ויראליות".[57] למעשה, רק אחדים מתוך אלפי המסרים שדאע"ש שחרר לרשת בצורה של סרטונים, מוזיקה, הצהרות, באנרים ו"ממים", הפכו באמת ל"מגיפה".

שנית, המקרה של "החליפות הווירואלית" מראה כמה חשוב לבצע איסוף מידע נכון בתחום הסייבר. התאמת המסר לתרבות הסייבר של קהל היעד, וכן רמת הפיתוח של טכנולוגיית המידע והתקשורת, מעלות את הסיכויים לאפקט וירואלי.

שלישית, לוחמה פסיכולוגית המבקשת לנצל את האפקט הווירואלי צריכה להשתמש בהרבה "וקטורים לתקיפה", הן מבחינת התוכן והן מבחינת הטכנולוגיה. למסר יחיד המתפרסם ברשת יש סיכוי קטן בלבד להפוך לווירואלי, אולם מאות מסרים בצורות שונות יכולים לשנות את המצב, שכן אז עולה ההסתברות למשיכת תשומת לבו של הקהל. ניתן להסיק זאת מפעילות המרכז לתקשורת "אל־חיאת", שהציף את האינטרנט בתעמולתו. יותר מכך, המסרים צריכים להיות מופצים בטווח רחב של ערוצים – אתרי אינטרנט, רשתות חברתיות ושאר שירותים מקוונים, לרבות אלה שהם הפופולריים ביותר בקרב אוכלוסיית היעד.

רביעית, הקמפיין הווירואלי צריך להתנהל לפני ובמהלך אירועים צבאיים ופוליטיים, כפי שהוכח בהוצאות להורג שבהן "ג'ון הג'יהאדיסט" התייחס להצהרותיו של הנשיא אובמה. לקיחה בחשבון מראש של אירועים כאלה יכולה

לצמצם את הסיכויים שהמסרים יתקבלו כתעמולה עוינת על ידי אוכלוסיית היעד. במקביל, המסרים צריכים להתייחס אך ורק לאירועים החשובים ביותר לצורך הלוחמה הפסיכולוגית. מצב כזה עשוי לחזק את היעילות המבצעית של הלוחמה הפסיכולוגית, שכן הוא ימשוך את תשומת הלב לאותם מסרים שהם עדכניים, חריגים או מעוררי מחלוקת. דבר זה אכן נעשה בסרטוני ההוצאות להורג הידועים לשמצה.

חמישית, מקרה "החליפות הווירואלית" מוכיח שכדי לעורר אפקט וירואלי, על המסר לשמור על מבנה קומפקטי ונגיש. פירוש הדבר הוא שהחשיפה אליו לא תצריך התחברות, הזנת סיסמאות או התקנת תוספות לדפדפן. המשתמשים ברשת אינם ששים, בדרך כלל, להתחבר או להתקין תוכנה חדשה כדי להתעדכן, אפילו אם מדובר בתוכן המקוון המעניין ביותר. כמו כן, תוכן צריך לקבל שם פשוט, באופן שיעלה את הסיכויים למצוא אותו דרך רשת חברתית או מנועי חיפוש. בסביבת "וב 2.0", דבר זה תלוי מאוד גם בשימוש נכון בתו הסולמית (#), כמו בנושא #mujatweets של דאע"ש.

שישית, התוכן והמסר צריכים להיות כמה שיותר מסקרנים, חריגים וייחודיים. אין להבין מכך שלוחמה פסיכולוגית צריכה לעשות שימוש בטכניקות קלאסיות של שיווק וירואלי, כמו אלו המתבססות על נושאים מיניים. במקום זאת, ייתכן שהומור ואלימות (שני נושאים ששימשו את דאע"ש), אשר יוצגו בצורה ייחודית ולא רגילה, יכולים להיות הדרך הנכונה. הומור יכול להיות גמיש יותר, ובשימוש נכון עשוי להצית תגובות שונות אצל קהלי היעד, הן לחיוב והן לשלילה. לדוגמה, מרכז התקשורת "אל־חיאת" הִרבה ללעוג למאמצי הצבא האמריקאי במזרח התיכון באמצעות שימוש בהומור. גם אלימות עשויה למלא תפקיד ייחודי, שכן ביכולתה לזעזע או להפחיד את הנחשפים למסר. שימוש כזה באלימות יושם היטב ברבים מסרטוני ההוצאה להורג שדאע"ש פרסם ברשת.

לסיכום, מקרה "החליפות האסלאמית", וכן העימותים הצבאיים שתוארו לעיל, מלמדים שהאפקט הווירואלי אכן יכול להיות מנוצל ללוחמה פסיכולוגית במרחב הסייבר. למרות שמדובר בכלי אקראי מאוד, הרי שמאמצים מכוונים ומקיפים מספיק יכולים להגביר את הסיכויים להתרחשות וירואלית ולהקנות יתרונות ניכרים ליוצריה. הדוגמה הבולטת ביותר לכך היא התנהלות דאע"ש סביב תיעוד ההוצאות להורג על ידי אנשי הארגון.

הערות

1 Brian Nichiporuk הגדיר לוחמת מידע כ"תהליך של הגנה על מקורות מידע עצמיים משדה הקרב, ובמקביל ניסיון למנוע, לפגוע, להשחית או להשמיד את מקורות המידע של האויב משדה הקרב". על פי ניצ'יפורוק, לוחמת מידע כוללת ביטחון מבצעים, לוחמה אלקטרונית, לוחמה פסיכולוגית, הונאה, תקיפה פיזית של תהליכי

מידע והתקפות מידע על תהליכי מידע. ראו: Brian Nichiporuk, "U.S. Military Opportunities: Information-Warfare Concepts of Operation", in Strategic Appraisal. The Changing Role of Information in Warfare, eds. Zalmay Khalilizad, John White and Andy W. Marshall (Santa Monica: RAND Corporation, 1999), p. 180.

2 Catherine E. Theohary, "Information Warfare: The Role of Social Media in Conflict", CRS Insights, March 4, 2015; Scot Macdonald, Propaganda and Information Warfare in the Twenty-First Century (New York: Routledge, 2007); Edward Lucas and Ben Nimmo, "Information Warfare: What Is It and How to Win It?", CEPA Infowar Paper, no. 1 (2015); Margarita Jaitner and Peter A. Mattsson, "Russian Information Warfare of 2014", in 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace, eds. Markus Maybaum, Anna-Maria Osula and Lauri Lindström (Tallinn: NATO CCD COE, 2015); William Hutchinson, "Information Warfare and Deception", Informing Science 9 (2006): 213-223.

3 Paul Rosenzweig, Cyber Warfare: How Conflicts in Cyberspace are Challenging America and Changing the World (Santa Barbara: Praeger, 2013); Thomas Eljker Nissen, "Terror.com – IS's Social Media Warfare in Syria and Iraq", Contemporary Conflicts 2, no. 2 (2014).

4 Carnes Lord, "The Psychological Dimension in National Strategy", in Political Warfare and Psychological Operations: Rethinking the US Approach, eds. Carnes Lord and Frank R. Barnett (New York: National Defense University Press, 1989), pp. 13-14.

5 U.S. Department of the Army, Psychological Operations Tactics, Techniques and Procedures, FM 3-05.301 (FM 33-1-1), (Washington, DC, December 2003).

6 ראו למשל: Roger C. Molander, Andrew S. Riddile and Peter A. Wilson, Strategic Information Warfare: A New Face of War (Santa Monica: RAND Corporation, 1996); Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks", Journal of Strategic Studies 38, no. 1-2 (2015): 4-37.

7 W. Tecumseh Fitch, "Evolving a Global Brain," in How is the Internet Changing the Way You Think? ed. John Brockman (New York: Harper Collins, 2011), p. 184.

8 James Joyner, "Competing Transatlantic Visions of Cybersecurity", in Cyberspace and National Security: Threats, Opportunities and Power in a Virtual World, ed. Derek S. Reveron (Washington DC: Georgetown University Press, 2012); Giorgi Targamadze, Information Warfare against Georgia (Tbilisi: Georgian Foundation for Strategic and International Studies, 2014); Michael Kofman and Matthew Rojansky, "A Closer look at Russia's 'Hybrid War'", Kennan Cable, no. 7 (2015).

9 Cori E. Dauber, YouTube War: Fighting in a World of Cameras in Every Cell Phone and Photoshop on Every Computer (Carlisle, PA: US Army War College, Strategic Studies Institute, 2009).

10 Christina Schori Liang, "Cyber Jihad: Understanding and Countering Islamic State Propaganda", GSCP Policy Paper, no. 2 (2015): 2.

11 MindComet Corporation, Viral marketing: Understanding the Concepts and Benefits of Viral Marketing, The Relationship Agency White Paper (2008), p. 3, http://cmginteractive.com/uploads/viral_marketing.pdf.

12 שם.

13 Maria Woerndl, Savvas Papagiannidis, Michael Bourlakis and Feng Li, "Internet-Induced Marketing Techniques: Critical Factors in Viral Marketing Campaigns", International Journal of Business Science and Applied Management 3, no. 1 (2008): 34.

14 Victoria Fairbank, "A Study into the Effectiveness of Viral Marketing over the Internet" (University of Gloucestershire, 2008), pp. 12-13, http://ct-files.glos.ac.uk/mwd/modules/co333/showcase/MU303_08_FairbankV.pdf; Steve Jurvetson and Tim Draper, "Viral Marketing: Viral Marketing Phenomenon Explained", DFJ, January 1, 1997, http://dfj.com/news/article_26.shtml.

15 Christian Briggs, "BlendTec Will It Blend? Viral Video Case Study", SocialLens, January 2009, http://www.socialens.com/wp-content/uploads/2009/04/20090127_case_blendtec11.pdf.

16 Laura Crimmons, "Top Viral Marketing Campaigns of All Time", Branded3, December 2, 2014, https://www.branded3.com/blog/the-top-10-viral-marketing-campaigns-of-all-time/.

17 סוג זה של תוכן וירואלי תורם לפעמים לתרבות הסייבר הגלובלית. אחת הדוגמאות המוצלחות לכך נוגעת לסדרת תמונות "ממים" קומיות שהפכה לוויראלית לפני כמה שנים והשפיעה על הרגלי התקשורת ברשתות חברתיות בכל העולם. בהקשר זה אפשר לציין את "Neil deGrasse Tyson reaction", "Forever alone", "Trollface" ו"Yao Ming Face". ראו: "Neil deGrasse Tyson reaction", Knowyourmeme, http://knowyourmeme.com/memes/neil-degrasse-tyson-reaction; "Forever alone", Knowyourmeme, http://knowyourmeme.com/memes/forever-alone; "Trollface/Coolface/Problem?" Knowyourmeme, http://knowyourmeme.com/memes/trollface-coolface-problem; "Yao Ming Face", Knowyourmeme, http://knowyourmeme.com/memes/yao-ming-face-bitch-please.

18 Woerndl and others, "Internet-Induced Marketing Techniques", pp. 35-36.

19 MindComet Corporation, Viral marketing, p. 4.

20 Petya Eckler and Shelly Rodgers, "Viral Marketing on the Internet", in Wiley International Encyclopedia of Marketing, eds. Jagdish N. Sheth and Naresh K. Malhotra (New York: Wiley, 2010), http://onlinelibrary.wiley.com/doi/10.1002/9781444316568.wiem04009/pdf.

21 למידע נוסף על "Web 1.0" ראו: Sareh Aghaei, Mohammad Ali Nematbakhsh and Hadi Khosravi Farsani, "Evolution of the World Wide Web: From Web 1.0 to Web 4.0", International Journal of Web & Semantic Technology 3, no. 1 (2012): 1-10.

22 המנגנון הוא פשוט: חשבונות המקור משתפים את המסר בקרב העוקבים, והעוקבים שלהם יכולים להעביר את המסר הלאה, לעוקבים שלהם, וכן הלאה.

23 Romualdo Pastor-Satorras and Alessandro Vespignani, "Epidemics and Immunization in Scale-Free Networks", in Handbook of Graphs and Networks: From the Genome to the Internet eds. S. Bornholdt and H. G. Schuster (Wiley-VCH, Berlin, 2002), p. 19, http://arxiv.org/pdf/cond-mat/0205260.pdf.

24 Albert-László Barabási, Dashun Wang, Zhen Wen, Hanghang Tong, Ching-Yung Lin and Chaoming Song, "Information Spreading in Context", in Proceedings of the 20th International Conference on World Wide Web (Hyderabad: 2011), p. 2, http://www.barabasilab.com/pubs/CCNR-ALB_Publications/201102-10_WWW-Spreading/201102-10_WWW-Spreading.pdf.

25 Mirosław Lakomy, "Arab Spring and New Media", in The Arab Spring, ed. Beata Przybylska-Maszner (Poznań: Wydawnictwo Naukowe WNPiD UAM, 2011).

26 Dauber, YouTube War; "Social Networking Popular Across Globe: Arab Publics Most Likely to Express Political Views Online", Pew Research Center, Global Attitudes & Trends, December 12, 2012, http://www.pewglobal.org/2012/12/12/social-networking-popular-across-globe/.

27 Mikael Eriksson, Ulrik Franke, Magdalena Granasen, David Lindahl, ראו לדוגמה: Social Media and ICT during the Arab Spring, no. FOI-R--3702--SE (Swedish Defence Research Agency, July 2013); Lakomy, "Arab Spring and New Media".

28 "Man Plays a Guitar in the Middle of a Shootout in Libya", Imgur, http://imgur.com/r/HumanPorn/pyMmP.

29 Uri Friedman, "Libya's Fighting Guitar Heroes", Atlantic, October 12, 2011, http://www.thewire.com/global/2011/10/libyas-fighting-guitar-heroes/43584/; Ziad Al-Hasso, "The Story behind the Libyan Guitar Hero Photo", Channel 4, October 13, 2011, http://www.channel4.com/news/the-story-behind-the-libyan-guitar-hero-photo; Lee Moran, "Now that's a Real Guitar Hero: Libyan Soldier Strums away as Battle for Sirte Rages around him", Daily Mail, October 11, 2011, http://www.dailymail.co.uk/news/article-2047889/Libyan-soldier-strums-guitar-battle-Sirte-rages-him.html.

30 Moni Basu and Matt Smith, "Gadhafi Killed in Crossfire after Capture, Libyan PM Says", CNN, October 21, 2011, http://edition.cnn.com/2011/10/20/world/africa/libya-war; "Libya's Col. Muammar Gaddafi killed, says NTC", BBC News, October 20, 2011, http://www.bbc.com/news/world-africa-15389550; "Libya's Moammar Gadhafi Killed in Hometown Battle", NBC News, http://www.nbcnews.com/id/44971257/ns/world_news-mideast_n_africa/t/libyas-moammar-gadhafi-killed-hometown-battle/#.VyJ7k-SbSUk.

31 "Gaddafi death", YouTube, https://www.youtube.com/results?search_query=gaddafi+death.

32 "Syria", YouTube, https://www.youtube.com/results?sp=CAM%253D&search_query=syria&page=1&nohtml5=False.

33 Paul Wood, "Face-to-face with Abu Sakkar, Syria's 'Heart-Eating Cannibal'", BBC News, July 5, 2013, http://www.bbc.com/news/magazine-23190533.

34 Maria Snegovaya, "Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare", Institute for the Study of War, September 2015, pp. 13-14, http://understandingwar.org/sites/default/files/Russian%20Report%201%20Putin%27s%20Information%20Warfare%20in%20Ukraine-%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf.

35 Myroslav Shkandrij, "How Russian Propaganda Works through Social Media", Myroslav Shkandrij's Blog, May 9, 2014, http://www.ukrainianwinnipeg.ca/russian-propaganda-works-social-media/.

36 התמונה המקורית ראו: http://i.imgur.com/BuiPsTj.jpg.

37 "It's Gonna be a Short War", Epic Fail, December 31, 2015, http://www.epicfail.com/2015/12/31/its-gonna-be-a-short-war/; Reddit, https://www.reddit.com/r/pics/comments/3kh4o3/sorry_captain_i_am_of_still_learnings_how_to/.

38 "UAF Storm Donetsk Airport and Get their Assess Handed to them by NAF", YouTube, https://www.youtube.com/watch?v=3TZ9Q18HKlQ.

39 "Ukraine Rebels Launch Grisly Propaganda War", France24, January 28, 2015, http://observers.france24.com/en/20150128-ukraine-rebels-launch-grisly-propaganda-war.

40 Schori Liang, "Cyber Jihad: Understanding and Countering Islamic State Propaganda"; Adam Hoffman and Yoram Schweitzer, "Cyber Jihad in the Service of the Islamic State (ISIS)", Strategic Assessment 18, no. 1 (2015): 71-81; Erin Marie Saltman and Charlie Winter, Islamic State: The Changing Face of Modern Jihadism (London: Quilliam Foundation, 2014); Yannick Veilleux-Lepage, "Paradigmatic Shift in Jihadism in Cyberspace: The Emerging Role of Unaffiliated Sympathizers in Islamic State's Social Media Strategy", Journal of Terrorism Research 7, no. 1 (2016): 36-51, http://doi.org/10.15664/jtr.1183.

41 Hayley Cole, "German Rapper Turned Extremist behind Islamic State Beheading Videos and Uses Music to Recruit Young Jihadis", Mirror, November 9, 2014, http://www.mirror.co.uk/news/uk-news/deso-dogg-german-rapper-turned-4597188.

42 עוד בנושא זה ראו: Gabi Siboni, Daniel Cohen and Tal Koren, "The Islamic State's Strategy in Cyberspace", Military and Strategic Affairs 7, no. 1 (2015): 127-144; Charlie Winter, Documenting the Virtual 'Caliphate' (London: Quilliam Foundation, 2015).

43 Siboni and others, "The Islamic State's Strategy in Cyberspace", p. 137.

44 Charles Lister, "Profiling the Islamic State", Brookings Doha Center Analysis Paper, no. 13 (2014): 3, https://www.brookings.edu/wp-content/uploads/2014/12/en_web_lister.pdf; Veilleux-Lepage, "Paradigmatic Shift in Jihadism in Cyberspace".

45 J. M. Berger and Jonathon Morgan, "The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter", The Brookings Project on U.S. Relations with the Islamic World, Analysis Paper no. 20, 2015, https://www.brookings.edu/wp-content/uploads/2016/06/isis_twitter_census_berger_morgan.pdf.

46 Brendan I. Koerner, "Why ISIS Is Winning the Social Media War", Wired, April 2016, https://www.wired.com/2016/03/isis-winning-social-media-war-heres-beat/.

47 Miron Lakomy, Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw (Katowice: Wydawnictwo Uniwersytetu Śląskiego, 2015).

48 Michael S. Schmidt, "Islamic State Issues Video Challenge to Obama", The New York Times, September 17, 2014, http://www.nytimes.com/2014/09/17/world/middleeast/isis-issues-video-riposte-to-obama.html?_r=0.

49 Claire Davis and Charlie Winter, "Detailed Analysis of Islamic State Propaganda Video: Although the Disbelievers Dislike it", Quilliam Foundation and TRAC, December 19, 2014, p. 31, https://www.quilliamfoundation.org/wp/wp-content/uploads/publications/free/detailed-analysis-of-islamic-state-propaganda-video.pdf.

50 Michelle Malka Grossman, "Watch: Islamic State's Terror Video Game", The Jerusalem Post, September 21, 2014, http://www.jpost.com/Middle-East/IS-claims-it-created-a-terror-video-game-375935.

51 Mujatweets, https://twitter.com/hashtag/mujatweets.

52 Miron Lakomy, "Internet w działalności tzw. Państwa Islamskiego: nowa jakość cyberdżihadyzmu?", Studia Politologiczne 38 (2015): 156-182.

53 כמה מהגרסאות המצונזרות נצפו ב"יוטיוב" מעל מיליון פעם עד אמצע אפריל 2016. ראו: "Islamic State Execution", YouTube, https://www.youtube.com/results?search_query=islamic+state+execution.

54 "James Foley", YouTube, https://www.youtube.com/results?q=james+foley&sp=CAM%253D; "James Foley", LiveLeak, http://www.liveleak.com/browse?q=james%20foley&sort_by=views.

55 "ISIS Bloopers", YouTube, https://www.youtube.com/watch?v=Qz3oWmDUW1Q.

56 Jill Carle, "Climate Change Seen as Top Global Threat", Pew Research Center, Global Attitudes & Trends, July 14, 2015, http://www.pewglobal.org/2015/07/14/climate-change-seen-as-top-global-threat/.

57 David Meerman Scott, The New Rules of Viral Marketing: How word-of-mouse spreads your ideas for free (n.p. 2008), p. 16, http://www.davidmeermanscott.com/hubfs/documents/Viral_Marketing.pdf?_hstc=17524326.4476318ded53d9884be8e803282f82b2.1472783930977.1472783930977.1472783930977.1&_hssc=17524326.2.1472783930978&_hsfp=3082634171.

"מלחמת אזרחים" מודיעינית: מודיעין אנושי לעומת מודיעין טכנולוגי

מתיו קרוסטון ופרנק ואלי

מאז פיגועי 11 בספטמבר 2001 התפתח המודיעין בתוך אווירה חדשה שהתבססה על טקטיקות וטכניקות חדשניות לאיסוף מידע. אווירה זו, אליה התלוותה קפיצת ענק בתחום הטכנולוגיה, כמו הופעת הרשתות החברתיות, התקשורת הניידת, תהליכי עיבוד מידע, אחסון נתונים בממדים גדולים, חומרה וציוד תוכנה חדשים, דחפו את קהילות המודיעין בעולם כולו לתוך מרחב חדש ובלתי מוכר של מודיעין רב־ממדי. גם במצב החדש שנוצר, נותרו המדע והטכנולוגיה מצד אחד והיכולת האנושית מצד שני ההיבטים המרכזיים בעבודת המודיעין. ואף על פי כן, ניכרת מגמה הולכת וגוברת מצד כל אחד מהמחנות המנוגדים המיצגים היבטים מרכזיים אלה לתת עדיפות לשיטת איסוף אחת על פני האחרת. מאמר זה מבקש להסביר כיצד ניתן לנצל באופן מיטבי, בעבודת השטח ובשלבי העיבוד והניתוח של המידע המודיעיני, הן את המודיעין האנושי (HUMINT) והן את המודיעין הטכנולוגי (TECHINT). זאת, על ידי ביטול היריבות הכפויה ביניהם ויצירת שיתוף פעולה הדדי שלא קיים עתה.

מילות מפתח: סייבר, מודיעין, HUMINT ,TECHINT, מדע וטכנולוגיה, ביטחון לאומי

ד"ר מתיו קרוסטון (Crosston) הוא פרופ' למדעי המדינה, ועומד בראש התוכנית למחקרי מודיעין וביטחון לאומי באוניברסיטת בלוויו (Bellevue), נברסקה, ארצות הברית. פרנק ואלי הוא בעל תואר שני במדעים בתוכנית למחקרי מודיעין וביטחון לאומי של אוניברסיטת בלוויו.

גרסה מוקדמת יותר של מאמר זה פורסמה על ידי פרנק ואלי תחת הכותרת: "'HumInt' vs. 'TechInt': A Forced Intelligence Dichotomy", *The Security and Intelligence Studies Journal 1*, no. 3 (Summer 2014).

חלקים ממאמר זה פורסמו גם על ידי מתיו קרוסטון תחת הכותרת: "American UAV Apartheid and the 'Blowback' of New Drone Armies", *New Eastern Outlook*, April 3, 2015.

מבוא

מאז פיגועי 11 בספטמבר 2001 התפתח המודיעין בתוך אווירה חדשה של טקטיקות וטכניקות חדשניות לאיסוף מידע. אווירה זו, אליה התלוותה קפיצת ענק בתחום הטכנולוגיה, כמו הופעת הרשתות החברתיות, התקשורת הניידת, תהליכי עיבוד מידע, אחסון נתונים בממדים גדולים, חומרה וציוד תוכנה חדשים, דחפו את קהילות המודיעין בעולם כולו לתוך מרחב חדש ובלתי מוכר של מודיעין רב־ממדי. פריסתן של טכנולוגיות חדשות והתפשטותן לזירה הציבורית גרמו לכך ששיטות איסוף המידע שהיו פעם נחלתן הבלעדית של ממשלות או של ארגוני ענק, חורגות כיום הרבה מעבר ליכולות שאפיינו את המודיעין האנושי. תגובה נגדית למצב זה היא הקביעה שאסור לפגוע במעמדו של הגורם האנושי בזירה המודיעינית – קביעה שיצרה את הבסיס למתח שבו עוסק מאמר זה. ואכן, תהיה המלחמה מתקדמת מבחינה טכנולוגית ככל שתהיה, הגורם האנושי יישאר נוכח דרך קבע בעשייה המודיעינית בצורה זו או אחרת. לכן, יש לראות תמיד את המודיעין האנושי כראשון בין שווים.

ההתפתחויות הטכנולוגיות בתחום המודיעין, שנוצלו בהרחבה על ידי קהילת המודיעין בעבר, זמינות כיום לשימוש הציבור כולו. יתרה מכך, גם הגילויים האחרונים השנויים במחלוקת סביב שימוש במטא־דאטה להערכת סיכונים ולזיהוים (ובמילים אחרות – כל הקשור ב"פרשת סנודן") הם ביטוי לחדירת המרכיב הטכנולוגי לתוך מרחב המודיעין האנושי. טכניקות שנהוג ללמד כיום סטודנטים באוניברסיטה לצורך מחקר כמותני (כגון תוכנה מבוססת שיטות מעורבות, קידוד מחשב אוטומטי, ניתוח תוכן, כריית נתונים או אתחול), היו בדור הקודם טכנולוגיות שהגישה אליהן הייתה נתונה כמעט בלעדית בידי גורמים ממשלתיים. שילוב המדע והטכנולוגיה לכדי מה שמכונה "מודיעין טכנולוגי" (TECHINT), הפך לגורם מרכזי התורם משמעותית הן לנתונים והן לאסטרטגיה.[1]

המדע והטכנולוגיה מצד אחד והיכולת האנושית מצד שני נותרו שני היבטים מרכזיים של עבודת המודיעין. למרות זאת, קיימת מגמה הולכת וגוברת של התגבשות שני מחנות מנוגדים, שכל אחד מהם דוחף להעדיף שיטה אחת על פני האחרת. מאמר זה מבקש להסביר כיצד ניתן לנצל בעבודת השטח ובשלבי עיבוד וניתוח המידע המודיעיני הן את המודיעין האנושי (HUMINT) והן את המודיעין הטכנולוגי (TECHINT) כדי להפיק את המרב משיתוף פעולה הדדי ביניהם, שאינו בנמצא כיום. אנו סבורים שחובה לשים קץ לירִיבות הכפויה בין שתי שיטות איסוף המודיעין. יתר על כן, הימנעותן של המדינות המפותחות משילוב המודיעין האנושי עם המודיעין הטכנולוגי עלולה להציב אותן בעתיד בפני אתגרים בתחום הביטחון הלאומי שיהיו הרבה יותר מורכבים וקשים מאשר ניתן להעריך כיום, במיוחד ככל שמדינות אחרות בעולם נכונות ליישם את השילוב הנדרש.

היחסים בין מודיעין טכנולוגי למודיעין אנושי – תמונת מצב

זירת המודיעין המודרנית ממשיכה לעשות שימוש בטכניקות איסוף אנושיות, ואלו ממשיכות לזכות לאהדה במכלול המבצעים המודיעיניים. במקביל, הולך וגובר האתגר שמציב האיסוף באמצעות טכנולוגיות מדעיות חדשות. למרות היתרון של טכנולוגיות אלו הן לאוספי מידע מנוסים והן לטירונים שביניהם, יש עדיין דעות קדומות בנוגע לשיטות מדעיות "טהורות" לאיסוף מידע. דעות קדומות אלו באות לידי ביטוי בעיקר ברמת השטח והמבצעים, שם ניתנת עדיין עדיפות לקבלת החלטות ספונטנית – יכולת שהיא לכאורה ייחודית לגורמי האיסוף העוסקים במודיעין אנושי.

אלה המבקרים גישה זו מעלים את השאלה האם שווה לסכן לוחם כאשר ניתן לאסוף מידע דומה באמצעים הטכנולוגיים הנפוצים בחברה המודרנית, כמו כטב"מים, מתקני האזנה, חיישנים, מודיעין חזותי, חדירה אינטרא־נטית, מעקב אחרי דואר אלקטרוני או השתלטות על מחשבים מרחוק. אלא שהיריבות הנגרמת על ידי הדעות הקדומות הינה עמוקה, ומונעת את השילוב החיוני בין שתי הגישות – האנושית והטכנולוגית.

הדרך הטובה ביותר להבהיר את המתח שנוצר בין שתי הגישות הוא בעזרת דוגמה שנוהגים להציגה כמודל הנכון לשיתוף פעולה בין מודיעין אנושי למודיעין טכנולוגי: השימוש בכלי טיס בלתי מאוישים (כטב"מים). אמנם, קביעת היעדים לתקיפה על ידי הכטב"ם נעשתה במקורה על סמך ניצול יעיל של נכסים אנושיים באזור המטרה, אולם ההצלחה המרשימה של הכטב"מים הובילה במהלך השנים להפחתת השימוש בגורם האנושי, וכיום ישנן פעולות רבות של כטב"מים המבוססות על מודיעין טכנולוגי. ישנם גורמים בתוך קהילת המודיעין הטוענים שהסכנה הנובעת מפגיעה בשוגג היא נזק משני, שבהשוואה לסיכונו של נכס אנושי ניתן לספוג אותו. מה שלא תמיד נאמר הוא שחלק מהשינוי שחל בתפיסה נובע משיקולים של מיידיות ונוחות: הצורך באימות המטרות בשטח כשעושים שימוש בגורם האנושי מאט ומגביל את יכולות השימוש בכטב"ם.[2] מכל מקום, הנטייה למקסם את השימוש במודיעין טכנולוגי במקרים כאלה הפחיתה עם הזמן את מעמדו של המודיעין האנושי וגרמה לירידה בחשיבותו של השילוב הנדרש בינו ובין המודיעין הטכנולוגי.

בבואנו לדון ביריבות בין המודיעין האנושי ובין המודיעין הטכנולוגי, יש להזכיר את מה שמכונה "תסביך הנחיתות של הידע", שבמסגרתו כל התרחקות ממודיעין אנושי לטובת מודיעין טכנולוגי מביאה מומחי מודיעין רבים למצוא את עצמם במצב שבו הם "מתבוננים על התמונה מבחוץ". יתרה מכך, הצורך לשדרג את מיומנותו של איש האיסוף מהפעלה בגישת המודיעין האנושי המסורתית למומחיות במודיעין טכנולוגי, מחייב עקומת למידה שהיא מעבר ליכולתם של

רבים מהוותיקים והמנוסים בתחום האיסוף. היבט זה של היריבות בין המודיעין האנושי ובין המודיעין הטכנולוגי נדון רק מעט, כנראה משום שהוא נתפס כ"פיל בחנות חרסינה".

"חרדת המדע" שמייסרת רבות מהאוניברסיטאות במערב (שבעטיה סטודנטים מתרחקים מהתמחות בתחומים המחייבים ידע מדעי עתיר טכנולוגיות[3]) היא נושא לדאגה מבחינת ההשפעה שיש לו על יכולתן של מדינות דוגמת ארצות הברית להישאר בעלות כושר תחרותי בכלכלה הגלובלית. למציאות זו יש גם השפעה עמוקה על המוכנות הטכנולוגית של הדור הצעיר והחדש בקהילת המודיעין. למעשה, מדובר בבעיה כפולה: מצד אחד, אין מספיק אנשים חדשים המסוגלים לנצל את הכלים הזמינים לאיסוף מידע; מצד שני, ואולי החשוב יותר, נראה שלא מושקע כל מאמץ בבניית גשר בין שני תחומי המודיעין, שיהיה בו כדי להעצים את טווח יכולותיהם ולתת ביטוי מרבי לכישרונות הקיימים בזירה המודיעינית.

מודיעין אנושי: איסוף ומידע

הגורם האנושי באיסוף המודיעין הוא עתיק כמלחמה עצמה. זו השיטה היעילה והזמינה ביותר להשיג מידע, לעבד אותו ולפעול בצורה מהירה כלפי יעדים ומטרות שונים. ההטיה לטובת טכניקות אנושיות של איסוף מידע בולטת במיוחד בקרב קובעי מדיניות רמי דרג, אולם גם בקרב לוחמים וחוקרים ותיקים: חיילים חיוניים כדי לנצח במלחמה, כפי שנוכחות של הגורם האנושי בשטח חיונית למודיעין.[4] על פי פטריק מרפי, לשעבר מהנדס ראשי ביחידת התכנון והניהול של הסוכנות לפרויקטים ביטחוניים מתקדמים בחברת "Action Technologies": "אנחנו מדברים הרבה על טכנולוגיות, [אך] בסביבת הלוחמה האורבנית אי אפשר להתנתק מהגורם האנושי; אי אפשר לנהל לוחמה אורבנית ללא בני אדם".[5] אמירה זאת רלוונטית במיוחד בזירת הלוחמה המודרנית, שבפניה ניצבים אנשי האיסוף המודיעיני. הטיה זו לטובת המודיעין האנושי משפיעה גם על התפיסה התודעתית של צרכני המודיעין – קהל היעד שלו – במיוחד כאשר אותה שיטת מודיעין מתקדמת במעלות שרשרת המידע ומגיעה עד קובעי המדיניות. לא זו בלבד שקיימת ספקנות כלפי אלה מאנשי קהילת המודיעין שהם בעלי יכולות טכנולוגיות, אלא שקובעי מדיניות וגורמים ממשלתיים נוספים הנמנים על האסכולה המסורתית של העדפת הגורם האנושי (שתכופות הם מבוגרים בהרבה מאנשי המודיעין בשטח) עשויים גם הם להיות ספקנים כלפי ההסתמכות היתרה על מידע המושג באמצעים מכניים וטכנולוגיים ולא באמצעות הגורם האנושי בשטח.

האיסוף הוא רק היבט אחד של המודיעין האנושי. המידע שמופק מהמודיעין שנאסף חשוב לא פחות, שכן הוא מסייע גם לניסוח המדיניות וגם להתרעה ולפיתוח היכולות המבצעיות בשטח. מידע מודיעיני ממקור אנושי מתגלה לעתים תכופות

כבעל חשיבות מכרעת באיתור ובנטרול אויבים וככזה המאפשר פעולה ותגובה זריזות לשם השגת יעדים בתחום הביטחון הלאומי. לדוגמה, בתוכנית ששודרה ברדיו הציבורי האמריקאי ב־2013, ועסקה בנשים לוחמות, הודגש שפשיטות ליליות רבות שנערכו באפגניסטן היו תוצאה של מיומנותן וכישרונן של הנשים המגויסות לאסוף מידע מודיעיני מנשים אפגניות.[6] צודקים אנשי קהילת המודיעין הנוטים להעדיף את המודיעין האנושי, במיוחד כשהם טוענים שהשגת היעדים לא הייתה אפשרית אם הדרג הפיקודי היה מעדיף להתמקד ביכולות מודיעיניות טכנולוגיות ומוכן פחות מכך לערב מפעילים אנושיים, במיוחד במצבים מסוכנים ורגישים.

אין ספק שחלק מהסיבות להטיה לטובת המודיעין האנושי נובע משיקולים של הישרדות מקצועית. יחד עם זאת, יש גם היבטים מבצעיים של ממש הקשורים למלחמות של ימינו, המחזקים את הרלוונטיות של המודיעין האנושי. עלייתם של גורמים לא מדינתיים המתערבבים באוכלוסייה האזרחית ונטמעים בה, וחוסר הבהירות הנוצר כתוצאה מכך סביב היכולת לבודד ולזהות לוחמים ויעדים בצורה ברורה, גרמו לתוהו ובוהו ולכאוס כתוצאה מהשימוש הבלעדי במודיעין טכנולוגי שאינו מסתייע במודיעין האנושי.[7] גם ההתפתחויות בטכנולוגיית הכטב"מים ממחישות מצב זה: התפתחויות אלו אינן מתוחכמות מספיק כדי להטיס כטב"מים באופן סמוי לתוך אזורים מאוכלסים בצפיפות ולזהות ולאחר מכן לחסל יעדים ספציפיים. סרטים הוליוודיים עשויים להציג מבצעים כאלה להנאתם הרבה של הצופים, אולם היכולת הצבאית במציאות עדיין לא הגיעה לשלב כזה. באופן פרדוקסלי, דווקא מודיעין אנושי יכול לסייע במימושן של משימות בדרך שתהיה פחות כאוטית. במילים אחרות, יש כמה היבטים בלוחמה המודרנית שהופכים את השימוש הבלעדי במודיעין הטכנולוגי לכאוטי ולבלתי יעיל. הזרקת מודיעין אנושי לתוך הזירה תביא, ללא ספק, להגדלת שיעורי ההצלחה של המודיעין הטכנולוגי.

מדע וטכנולוגיה: איסוף ומידע

השימוש באמצעים טכנולוגיים בלבד לצורך איסוף מודיעין הוא חדש יחסית. אמצעי הייטק מרובים נוספו לכלי האיסוף המודיעיניים הקונבנציונליים בעידן הלוחמה המודרנית, והמדע והטכנולוגיה מציעים יכולות חדשות בעלות יתרונות טכנולוגיים־מדעיים ברורים לצורך השגת מידע מודיעיני.[8] זאת, אם באמצעות מעקב אחרי דואר אלקטרוני, טקטיקות לאיסוף בסייבר, ניתוח הדמיות לוויין או טכניקות למיקום יעדים ומטרות באמצעות כטב"מים. כך, למשל, הערכת היכולות הטכנולוגיות של ארגוני טרור (כמו האם הם יכולים לפתח ולהציב "פצצה מלוכלכת" או מטעני נפץ מסוג אחר) נעשית באופן היעיל ביותר על ידי ניתוח טכנולוגי ומדעי של המידע.

יתרון נוסף וערכי של המודיעין הטכנולוגי הוא היכולת להשאיר את המפעילים ואת הלוחמים מחוץ לטווח פגיעה. אלא שליתרון זה יש גם מבקרים, כפי שכתב על כך אחד החוקרים: "המעבר מפעילות מודיעינית המבוססת על הגורם האנושי לפעילות מודיעינית המבוססת יותר על גישה טכנולוגית, באמצעות מודיעין אותות (SIGINT), עורר ביקורת מיד לאחר פיגועי 11 בספטמבר 2001. מספר פרשנים, מומחים ואנשי ביטחון לאומי טענו אז כי בשנים האחרונות חלה ירידה ביכולות המודיעין האנושי של ה־CIA".[9]

קיים חשש שבהיעדר הערכה אנושית של המידע שנאסף, ניואנסים שונים בנתונים עלולים להיות מוחמצים, והניתוח שיתקבל יהיה שגוי. טענה זו זוכה בדרך כלל לטיעון נגדי, לפיו המודיעין הטכנולוגי יכול להגיע לרמת דיוק גבוהה מאוד בזכות קלות ההפקה שלו וכמות הנתונים שהוא יוצר. הנרטיבים המתחרים הנוגעים לטכניקות ההערכה של המידע המודיעיני, כפי שהם באים לידי ביטוי בעמדותיהם של משתמשי הקצה, מדגישים עוד יותר את האנטגוניזם בין מחנה המודיעין האנושי ובין מחנה המודיעין הטכנולוגי ומפריעים למיזוג הכול כך נחוץ בין שתי שיטות אלו. אם לא ניתן יהיה להשיג את הסינתזה הדרושה באמצעות איתור והכשרת כוח אדם שיוכל לפעול בשתי שיטות איסוף המודיעין, המאמצים יצטרכו להיות מושקעים במדיניות שתעודד סוכנויות מודיעין ליצור שילוב עקבי ויעיל יותר של מאמציהן־הן בכל אחד משני התחומים. למרבה הצער, עד היום מאמץ זה לא היה חזק או משכנע מספיק.

מודיעין טכנולוגי לעומת מודיעין אנושי: היבט המדיניות

התפתחות העידן הדיגיטלי בעשרים השנים האחרונות הביאה ליצירת ממד חדש לחלוטין במערכת המודיעינית, הן בתחום האיסוף והן בתחום המידע. התהליך הואץ עוד יותר בעקבות אירועי 11 בספטמבר 2001, שלאחריהם הגיעה תחושת חוסר הביטחון הלאומי של האמריקאים לשיא שלא הכירו בעבר. ככל שהעידן הדיגיטלי התפתח, כך הפכו טכנולוגיות שבעבר היו נחלתם הבלעדית של אנשים בעלי סיווג ביטחוני גבוה לזמינות להמונים, ואלה יכולים לרכוש אותן בכל חנות מחשבים, אמנם בגרסאות פשוטות יותר אבל בכל זאת עוצמתיות. מדובר בהצפנה, בקידוד, בכריית נתונים, בשלל האפליקציות החינמיות המשוכללות הנמצאות בכל סמארטפון, או בכמות הבלתי נתפסת של מידע, כולל מידע מסוכן, הזמין ברשת בלחיצת כפתור פשוטה.

התפשטות הטכנולוגיה ושקיפותה אפשרו יצירת כלים לאיסוף מסיבי של נתונים ממקורות גלויים (OSINT), וגרמו להשמעת קולות שקראו להגבלת השימוש במודיעין אנושי. קריאות אלו, שהן הרסניות לחסידי המודיעין האנושי, מתבססות על ההצלחה הכפולה הן בהשגת המשימה והן באבטחת הנכס המודיעיני: אם

המודיעין הטכנולוגי מאפשר את השגת המטרה ביעילות וללא התערבות אנושית, מדוע לטרוח ולשמור על מרחב פעולה כה רחב של המודיעין האנושי?[10]

המדיניות השלטת באיסוף המודיעיני הייתה רחוקה מלהיות מוכנה לטפל בהצפת המידע שיצר ה־OSINT. "זקני" הטכניקות הקלאסיות של המודיעין האנושי נאלצו להתעמת עם יכולת חדשה לאיסוף כמויות גדולות של מידע באופן שלא חוו אותו בעבר. זאת ועוד, התברר כי שימוש בשיטות המסורתיות לטיפול יעיל בטכניקת האיסוף החדשה הוא בעייתי. הצורך לגבש כללי מדיניות חדשים באווירה שנוצרה עם פיתוח היכולות החדשות הפך לאתגר שבו מעורבים כל הנוגעים בדבר.

המדיניות שגובשה בקהילת המודיעין האמריקאית ניצלה את העוצמה הטכנולוגית והמדעית החדשה וחרגה מגבולות הנורמות של חירויות האזרח המסורתיות של ארצות הברית. חקיקת חוקים כמו חוק הפטריוט משנת 2001, והגילויים שנחשפו בהדלפותיו של אדוארד סנודן ב־2013, מצביעים על כך שההזדמנות למקסם את היכולות הטכניות לצורך פיקוח ואיסוף מידע הייתה פיתוי גדול מכדי שניתן יהיה לוותר עליו.[11] בחינת הפן האתי והמוסרי של החלטות אלו חורג ממסגרתו של מאמר זה, אולם יש מקום להדגיש נקודה חשובה שלא הובהרה מספיק עד היום – הדרך שבה יכולות האיסוף החדשות כרסמו במה שעד עתה היה "סמכות השיפוט" הבלעדית של מפעילי המודיעין האנושי מצד אחד, והעצימו את הדעה הקדומה נגד אמצעי המודיעין הטכנולוגי מצד שני, בטענה שהם משקפים הבטחות ללא כיסוי ומשיגים פחות תוצאות מהמצופה.

לא ניתן להתכחש לעובדה כי טכנולוגיות מודרניות ומתקדמות מאפשרות חדירה קלה יותר לאזורים ולמקומות שסוכן אנושי התקשה להגיע אליהם. בנוסף, טכנולוגיות אלו מסייעות בפיתוח יכולות איסוף ומעקב קבועות, ולטווח ארוך. השגת רציפות כזאת באמצעות סוכני מודיעין אנושיים בלבד הייתה בעבר נטל כבד, מסוכנת, ולפרקים בלתי אפשרית.

אף אחד לא מרוצה: הדילמה התקציבית בין מודיעין אנושי למודיעין טכנולוגי

לוויכוח על המודיעין האנושי מול המודיעין הטכנולוגי היה מאז ומתמיד מרכיב כלכלי, שחשיבותו אולי אף עולה על מה שרוב המתדיינים נוטים לייחס לו. חסידי המודיעין האנושי יכולים לטעון כי מנקודת מבט תקציבית, מימון הגיוס וההכשרה של סוכן אנושי עבור קהילת המודיעין היא דבר הרבה יותר מועיל. המצדדים בגישה זאת גם יכולים לטעון כי השימוש הרב־תכליתי בסוכנים אנושיים, על יכולות ההמצאה שלהם והגמישות המאפיינת אותם, מהווה נימוק משכנע להשקעה גדולה יותר בהם מאשר במכשיר דומם ומנוכר המשרת מטרה אחת בלבד.

דילמת המימון עולה על הפרק לא פעם בדיוני התקציב, כאשר הצד התומך בהעדפת המודיעין הטכנולוגי מקונן על היעדר תקציב למימון ה"צעצועים" החדשים שלו, בעוד שמחנה התומכים במודיעין האנושי חש ששללו ממנו את התמיכה הכספית הדרושה כדי לשמר את עדכניותו של כוח האדם המגויס לצורך זה, את רעננותו ואת המרץ שמאפיין אותו. הדבר יוצר דילמה, שכן כל צד טוען למעשה שהוא לא מקבל מימון מספיק, ובמקביל סבור שהצד השני מבזבז כספים יקרים על שיטות פעולה פחות יעילות משלו.

דברים אלה עומדים בניגוד גמור לעובדה שהתקציב השנתי של המודיעין האמריקאי עלה בהתמדה במהלך עשר השנים האחרונות, במידה רבה בשל הדרישה למודיעין טוב ורלוונטי יותר, וכתוצאה מכך הדרישה למקורות אנושיים וטכנולוגיים שיתנו מענה לכך. מכיוון שההוצאות על פיתוחים טכנולוגיים כבר מהוות נתח גדול מתקציב המודיעין, ומכיוון שפיתוחים אלה נוהגים להתיישן או להפוך לבלתי רלוונטיים בתוך פרק זמן קצר יחסית, ישנו דחף בירוקרטי לפצות על כך באמצעות התמקדות במקורות מתחום המודיעין האנושי המתאפיינים בגמישות רבה יותר. דווקא המוניטין הידוע של קהילת המודיעין כמי שפועלת בחוד החנית של המחקר והפיתוח הטכנולוגי, הוא שמביא באופן פרדוקסלי למה שנתפס לפעמים כחוסר איזון תקציבי (אותו ניתן לפתור רק באמצעות ויתור על שיטות התאמה תקציביות מסורתיות). התוצאה היא שהמודיעין הטכנולוגי זוכה לעדיפות ולתשומת לב לא הוגנות מבחינה פיננסית, בהשוואה להשקעות ולתמיכה הכספית במודיעין האנושי.

גישה זו של העדפת המודיעין הטכנולוגי לוקה מאוד בחסר. יש ליצור איזון בין העדיפויות התקציביות, כך שהיכולות הטכנולוגיות יתרמו ויסייעו לטכניקות ולטקטיקות של המודיעין האנושי. בדרך זו ניתן יהיה להביא לצמצום הסיכונים עבור נכסים אנושיים הנמצאים במקומות מסוכנים, ובמקביל – להגביר את אמינות המודיעין שנאסף ואת הדיוק בניתוח ובהערכה שיתבססו עליו. לפיכך, התקציב לצורכי המודיעין הטכנולוגי צריך להיות כזה שיאפשר ניצול טוב יותר של המימון שניתן לצורכי המודיעין האנושי.

שדה הקרב הטכנולוגי, שלפי התחזיות יהיה קו האש העתידי, הוא גם וירטואלי וגם ממשי, בין אם מדובר במפעילים ברמת השטח שינצלו יכולות של כטב"מים, ובין אם מדובר בחוקרי סייבר שיעקבו אחר עקבות אלקטרוניות. לפיכך, יש לראות במודיעין טכנולוגי יעיל ורלוונטי

יתרון מכריע הן במבצעים והן במחקר והערכה מודיעיניים. המשך הנטייה הנוכחית לקבוע את העדיפות במימון מקורות מודיעיניים על סמך השוואה בין יכולות טכניות ובין כישרונות אנושיים, פירושו פגיעה ביכולות המודיעין והזנת יריבות מיותרת בין המודיעין הטכנולוגי ובין המודיעין האנושי. המימון צריך

להתמקד במחקר, בפיתוח ובמאמצים מבצעיים, שישלבו יחדיו את שתי שיטות האיסוף המודיעיני – הטכנולוגי והאנושי.

איך לגשר על הפער

המטרה של השגת מידע מדויק, ראוי ובעל משמעות אופרטיבית תתאפשר בצורה הטובה ביותר כאשר יחול שילוב בין יכולות המודיעין האנושי והטכנולוגי. הגישור על הפער הקיים בין שתי שיטות איסוף אלו הוא משימה לא פשוטה, שכן רק מעט מאוד מקרב אנשי האיסוף הם בעלי מיומנות בשני התחומים. החוקרים וקובעי המדיניות נוטים להעדיף אחת משתי השיטות כשיטה המפיקה את המידע הטוב והאמין ביותר, ולפיכך הם נותנים לה יחס מועדף, המתבטא בתחומים הפרוצדורלי, הבירוקרטי או הכספי.

התפשטות מרחב הלחימה לעבר תחום הסייבר ולשיטות טכנולוגיות של איסוף מידע, הופכת את השילוב בין המודיעין האנושי המסורתי ובין המדע והטכנולוגיה לצעד בלתי נמנע.[12] שילוב כזה אינו אמור להיות חוד החנית של איסוף המודיעין בעתיד, אולם הוא ייצור ללא ספק את הבסיס לטכניקות חדשות לאיתור כישרונות ולגיוס הדור הבא של אנשי מודיעין. לצורך זה יש להתעלם מסטיגמות ומדוגמות של העבר, בין אם כאלו שאפיינו את תחום המודיעין האנושי ובין אם את תחום המודיעין הטכנולוגי.

הדבר הראשון שיש לעשות במסגרת מאמצי השילוב בין שתי שיטות האיסוף הוא להכיר בעובדה שבני אדם ימשיכו להיות גם בעתיד חלק בלתי נפרד מהזירה המודיעינית. אין זה משנה עד כמה משוכללת תהיה הלוחמה העתידית מבחינה טכנולוגית ומדעית, היא תמשיך להסתמך גם אז בצורה זו או אחרת על ההון האנושי.[13] יחד עם זאת, יש להבין כי הטמעת כלים מדעיים ויכולות טכנולוגיות היא כלי עזר חיוני לסוכן האנושי כדי למנוע סכנות לחיילים ולשכלל את יכולותיו, וכי היא מאפשרת להעניק למפעילי השטח את האמצעים הדרושים להם להשגת יעדיהם ומשימותיהם.

למרבה המזל, ההטיה שגורמת להפרדה בין שתי גישות האיסוף המודיעיני היא תוצאה של עמדה אישית ולא של דיכוטומיה מוּלדת ובלתי ניתנת לשינוי. הטיה אנושית זו נשענת במידה רבה על הקושי של מפעילים ותיקים, המיומנים בטכניקות מסורתיות של מודיעין אנושי, לייחס את המקום הראוי לטכנולוגיה, שחשיבותה הולכת וגוברת. כאמור, החשש מפני חוסר היכולת לרכוש את המיומנויות הטכניות הדרושות אינו נובע אצל אותם אנשים רק מרצון לשמור על מקום העבודה שלהם, אלא גם ממחלוקת תיאורטית ומקצועית עמוקה על מידת היעילות של המודיעין הטכנולוגי ועד כמה יש ביכולתו להוות תחליף ליתרונות הייחודיים של הנכסים

האנושיים. זוהי סיבה נוספת לכך שהמיזוג והשילוב בין שתי שיטות האיסוף הם כה חיוניים.

המפתח להתקדמות בכיוון זה בטווח הקצר והבינוני הוא, מן הסתם, לא התעלמות ופסילה של אלה שאינם יכולים לרכוש את המיומנות הטכנולוגית, אלא התמקדות בדרכים שבהן כל אחד מהם יצליח לרכוש מיומנות בשפה, בגישות וביעדים של הצד האחר. בדרך זו, המודיעין הטכנולוגי והמודיעין האנושי יוכלו לתקשר ביניהם בצורה אפקטיבית, וכך יגבירו את השפעתו של התוצר המודיעיני ויתנו מענה מיטבי לצורכי הביטחון הלאומי.

דילמת השילוב בעולם – סקירה קצרה

מדינות מתקדמות מבחינה טכנולוגית הן אלו שחוות ביתר שאת את היריבות בין המודיעין האנושי למודיעין הטכנולוגי. עם זאת, הדילמה בין שתי שיטות המודיעין אינה נחלתן של מדינות מפותחות בלבד, והיא צפויה להתפתח ולהתרחב ככל ששיטות העבודה ושיתופי הפעולה המודיעיניים ימשיכו להפוך יותר ויותר לנורמה גלובלית.[14] רבות מהמדינות הפחות מפותחות נאלצות במידה מסוימת להעדיף מודיעין אנושי על פני שיטות מדעיות וטכנולוגיות חדשות, הן לאיסוף המידע והן להערכתו, וזאת בשל מחסור במשאבים טכניים ופיננסיים.

מדינות דוגמת בריטניה, אוסטרליה, רוסיה, סין וישראל החלו לשים את הדגש על מודיעין טכנולוגי במקום על מודיעין אנושי, כפי שניתן לראות מהשימוש שהן עושות באמצעי מודיעין טכנולוגיים מודרניים, כמו כטב"מים, צילומי לוויין וצילומי אוויר, וכן מודיעין אותות (SIGINT), מודיעין מדידות וחתימות (MASINT) ומודיעין חזותי/הדמייתי (IMINT). היריבות בין שיטות המודיעין האנושי והמדעי־טכנולוגי, אותה רואים בארצות הברית, צפויה להיווצר גם במדינות אלו (אם עדיין לא קיימת בהן). קהילות מודיעין במדינות מפותחות מבחינה טכנולוגית נוטות לפתח דילמות סביב המודיעין האנושי, מהסיבה הפשוטה שחדשנות מדעית היא תמיד מהירה יותר מהיכולת של בני אדם להדביק אותה.

בהיעדר סינתזה ושילוב נכונים בין שיטות המודיעין השונות, המדינה מסכנת את ביטחונה הלאומי. הדבר בולט במיוחד במדינות פחות מפותחות, אשר מוכנות לנקוט אמצעים לא מוסריים כדי להשיג את השילוב המדובר. סקירה קצרה של תפוצת כלי הטיס הבלתי מאוישים יכולה להוות דוגמה מצוינת לתופעה זו.

שילוב דה־פקטו במזרח התיכון

ב־2013 הצליח צה"ל להשמיד כלי טיס בלתי מאויש שאותר כשהוא טס מעל מתקנים צבאיים רגישים בישראל ומתקרב לאזור הכור הגרעיני בדימונה. הכטב"ם החודר היה לא חמוש, אולם הופעל על ידי מישהו מרחוק, וניסה לשדר תמונות

לבסיס האם שלו. ישראל לא פרסמה האם הגורם ששלח את הכטב"ם העוין הצליח להשיג את מבוקשו, אולם הודיעה חד־משמעית שהכטב"ם לא היה אמריקאי, סיני או רוסי, וטענה שמדובר בכלי טיס אירני שהורכב בלבנון ושוגר על ידי חזבאללה.[15] במקום אחר התייחסנו לכטב"ם שהשתתף באותו אירוע כאל "כטב"ם הסהר האסלאמי" הראשון בעולם, כביטוי לאופייה העל־לאומי של תפוצת טכנולוגיית הכטב"מים בעולמנו.[16]

ב־2013 הצהירה איראן כי היא פיתחה את כטב"ם Epic, שלטענתה הוא בעל יכולות לפעול הן ככלי קרבי והן ככלי למשימות סיור, וכן את כטב"ם Throne – מטוס קרבי ללא טייס, למרחקים ארוכים, בעל יכולות חמקנות. איראן לא חסכה ביחסי ציבור כדי לטעון לכתר ההגמוניה האזורית במודיעין טכנולוגי.[17] טענה זו בעייתית לאור מקומו של הגורם הישראלי, ולכן ראוי להתייחס אליה בספקנות מסוימת: ספק רב אם איראן מסוגלת להתחרות עם העליונות הטכנולוגית של צה"ל ועם הארסנל הטכנולוגי שלו, ולכן ניתן לקבוע כי חלק מאותם פרסומים היו למטרת יצירת רושם יותר מאשר ביטוי ליכולת אמיתית. ואכן, התגובה הכללית בעולם להודעות האיראניות הייתה ספקנית ביותר. יחד עם זאת, יש עדיין סוגיות חשובות בטענת האיראנים אותן צריך לבחון, במיוחד על ידי אלה שלא רוצים לראות את איראן מממשת את שאיפותיה. כך, למשל, יש לבחון את מהימנות טענותיה של איראן בדבר היכולת הכפולה של הכטב"מים שלה – הן קרבית והן לצורך סיורים ופעילות מודיעינית.[18] טענה נוספת של איראן אותה יש לאמת היא הצהרותיה על כך שהכשירה הון אנושי המסוגל לנצל את הטכנולוגיה המודרנית.

ה"הישגים" לכאורה של איראן הביאו, לא במקרה, הן את מצרים והן את ערב הסעודית להתחיל לגלות עניין ברכישת כטב"מים לצבאותיהן. שתי המדינות מחפשות מקורות השקעה כספית וטכנולוגית לפיתוח תוכניות משלהן ולגיוס כוח אדם בהיקף הנדרש לצורך זה.

המרוץ של מדינות שונות אחר כטב"מים טקטיים התמקד עד היום בהשגת מעמד אסטרטגי בזירה העולמית ובהקרנת עוצמה במדיניות החוץ שלהן, או לפחות ביכולת הפוטנציאלית של אותה הקרנת עוצמה. עם זאת, טורקיה, למשל, גילתה עניין בכטב"מים בשל שיקולים פנימיים, מה שיכול להוות תקדים מסוכן ביותר בעתיד. אמנם, טורקיה מצהירה שהשימוש שהיא עושה בכטב"מים בזירה הפנימית נועד למטרה חיובית של שמירה על השלום ופתרון סכסוכים, אולם דומה שהשימוש האלים בכלים אלה בתוך המדינה מיועד למעשה להמשך מאמצי החיסול של "מפלגת הפועלים של כורדיסטן" (PKK). הצבא הטורקי נמנע כמובן לחלוטין מלהזכיר את ה־PKK בהקשר של מדיניות הכטב"מים שלו, ובמקום זאת מתמקד בהדגשת יעילותם של כלי טיס אלה לצורך שמירה על ביטחון הגבולות, ללוחמה אורבנית ולשאר משימות מבצעיות. לכאורה, אין מקום למחות על מטרות כאלו,

אולם אם בוחנים את הדברים לעומק, מגלים שהן היו במשך שנים מילות קוד לטיפול בפעילות ה־PKK. ברור אפוא שפריסת כטב"מים חמושים בתוך שטחה הריבוני של טורקיה נועדה למעשה להשמדת המחתרת הכורדית.

הבחנה זו מצביעה על החשיבות הגוברת והולכת של הצורך לפתח יכולות אנושיות לצד רכישה של יכולות טכנולוגיות, וזאת במיוחד נוכח התפשטות השימוש בכטב"מים לצרכים פנים מדינתיים. עסקאות מסחריות־צבאיות פשוטות לכאורה, דוגמת אלו שהיו בין טורקיה לישראל בעבר, מסתירות שכבות נוספות, ובהן מאמצים מצד המדינות הרוכשות לעשות שימוש בטכנולוגיות החדישות לצורכי ביטחון פנים.

מעניין לראות כיצד יתפתח תחום זה בעתיד: כבר ראינו שיש מעט מאוד חוקים ונורמות בין־לאומיים המסוגלים למנוע מבצעים גלובליים שבהם מופעלים כטב"מים חמושים, במיוחד כאשר הדבר נעשה על ידי מעצמות־על דוגמת ארצות הברית. השאלה המתעוררת בהקשר זה היא, האם הפיקוח והתגובה הבין־לאומיים יהיו מצומצמים עוד יותר כאשר מדינות אחרות יעשו שימוש בכטב"מים חמושים כדי לטפל בבעיות בתוך גבולותיהן שלהן? אם כך יהיה, פירוש הדבר הוא שזירת כלי הטיס החמושים הבלתי מאוישים מתקדמת לכיוון קטלני יותר, במיוחד כאשר כלים אלה נרכשים על ידי מדינות כמו טורקיה.

שילוב דה־פקטו באסיה רבתי

לצד טורקיה, שיצרה תקדים של שימוש אלים בכטב"מים חמושים לצרכים פנימיים, סינגפור מציגה תקדים מסוג אחר: היא הצהירה באופן מפתיע, גלוי וישיר על יעדיה ומטרותיה לטווח הארוך ברכישת כטב"מים. סינגפור הודיעה בפומבי כי הרכישה של כלי טיס בלתי מאוישים מספקיות גדולות כמו ישראל היא רק הצעד הראשון בתוכנית אסטרטגית ארוכת טווח, שבמסגרתה תכשיר המדינה כוח אדם מקומי להפעלת צי הכטב"מים. מרכיב הכטב"מים נחשב לחלק מכריע, ואולי אף המכריע ביותר, בתוכנית הלאומית של סינגפור.[19] אם "המודל הסינגפורי" (בהיעדר מונח הולם יותר) יאומץ בקנה מידה עולמי, אזי קרֵב היום שבו יותר מדינות ינצלו רכישות של כטב"מים לא כדי לבנות תשתית של צי מקומי של מטוסים ללא טייס, אלא כדי להמריץ, לפתח ולהגדיל תעשיות מקומיות ולהכשיר מפעילים תוצרת בית. במילים אחרות, סינגפור היא הנחושה מכל המדינות בהצהירה על זכותה להשיג עצמאות הולכת וגדלה בתחום הכטב"מים, החל מבנייה, דרך חימוש והצטיידות, וכלה בבניית יכולות מבצעיות. אם היא תצליח במאמציה אלה, הדבר יהווה אתגר לדומיננטיות האמריקאית בתחום הטכנולוגי, אם לא לסיומה המוחלט.

למעשה, קיימת אפשרות שמדינות אחרות באזור אסיה והאוקיינוס השקט ילכו בעקבות המודל הסינגפורי, דבר שייצור פוטנציאל להקמתו של שוק הכטב"ם

השני בגודלו בעולם. עם זאת, אפשר לטעון שמדובר ב"תרגיל" סטטיסטי: אזור אסיה והפסיפיק ייקח אז אמנם מישראל את המקום השני, אולם רק אם ישולבו ביחד עסקות הרכש של כל המדינות באזור לנתון מסכם אחד. כאשר משווים בין ישראל ובין עסקות הרכש של כל מדינה באזור הפסיפיק בנפרד, ישראל עדיין שומרת בצורה ברורה על מקומה השני.[20]

הודו, קוריאה הדרומית, קוריאה הצפונית, מלזיה ואוסטרליה הן שחקניות גדולות בשוק הכטב"מים של אסיה רבתי, וזאת בנוסף למקומן המבוסס של סין וסינגפור באותו שוק. כל אחת מהמדינות הללו הביעה את רצונה לא רק לרכוש כטב"מים ממדינות אחרות, אלא גם להכשיר צוות מפעילים משלה ולפתח מאגר של הון אנושי חדש לצורך הכטב"מים הצבאיים. אותן מדינות חותרות במרץ ובשאפתנות רבים לשילוב בין מודיעין אנושי למודיעין טכנולוגי ואינן סבורות שעליהן להתאים את האינטרסים הלאומיים שלהן לאינטרסים האסטרטגיים של ארצות הברית. לכן, כאשר מדובר בפיתוחן של תעשיות כטב"ם מקומיות, על ארצות הברית להיות מודאגת לא רק ממדינות שאינן בעלות בריתה; אפילו בעלות בריתה עשויות למצוא עצמן במסלול התנגשות עם היעדים והמדיניות האמריקאיים, תוך שהן פועלות לקידום האינטרסים שלהן.

זוהי הבחנה שחשוב לעשותה, שכן עד עתה היא אינה זוכה לדגש הראוי במסגרת הדיונים והוויכוחים על תפוצת כלי טיס בלתי מאוישים: היכולת לשלב את העוצמה של המודיעין הטכנולוגי עם החיוניות של המודיעין האנושי מעניקה יכולת להקרין עוצמה חדשה למדינות שבעבר היו מוגבלות בכך. ארצות הברית וישראל חשו בעבר, ובצדק, ביטחון רב ביכולתן להקדים ולהביס כל מדינה אחרת במרוץ אחרי פיתוח יכולות ורכש צבאי, אולם ייתכן שתחושה זו שוב אינה מוחלטת באותה מידה: אין צורך שיריב חלש יותר יגיע בדיוק לאותה רמה טכנית ואנושית כמו ארצות הברית וישראל כדי לאתגר ולסכן באופן ממשי את האינטרסים של שתי מדינות אלו. הניסיונות שתוארו לעיל לשילוב מאמצים בזירת כלי הטיס הבלתי מאוישים, מוכיחים את הפוטנציאל השלילי שיש אפילו בשיפור יחסי של היכולות. כדי להסב נזק, אין צורך להגיע לשוויון מלא.

חילופי משמרות

מדיניות שתשים בראש מעייניה את צרכיו ודרישותיו של החייל, של המפעיל או של החוקר, תהיה מדיניות יעילה, בת־קיימא, המתפתחת בהתאם לצרכים. תהיה זו מדיניות המאמצת את התחום הטכנולוגי המתפתח יחד עם השינויים בהתפתחותו של הגורם האנושי, מדיניות המקדמת אינטרסים של הביטחון הלאומי הן בשדה הקרב והן בזירה המודיעינית. ההכרה בצורך זה וההסתגלות אליו משמעותן נקיטת הצעדים הדרושים למען הדורות הבאים של קהילת המודיעין.

לא פעם קורה שדווקא כוח האדם המיומן, הבקיא והמנוסה ביותר אינו מצליח להתקדם במעלה הסולם הבירוקרטי ולהתמנות למשרות של קובעי מדיניות. מצד שני, היעדר הניסיון המעשי בשטח בקֶרב קובעי המדיניות יכול להביא למתן עדיפות מודיעינית שגויה ולהיעדר חדשנות. כל עוד "טהרנים" ממשיכים לשלוט בדיוני התקציב והמדיניות, אזי כאשר הדברים יגיעו לקו המפריד בין המודיעין האנושי ובין המודיעין הטכנולוגי, עתידה להימשך ההפרדה השגויה והמוטעית בין שתי הגישות.

כיצד קהילות מודיעין במדינות כמו ארצות הברית וישראל צריכות לפעול כדי להתפתח מכאן ואילך? ראשית, עליהן לתת עדיפות לקידום ולעידוד כל מי שרואה צורך בשילוב חלָק בין מודיעין אנושי למודיעין טכנולוגי, הן במבצעים והן במדיניות. הדרך היחידה להביא לשינוי מהותי היא לאפשר לאנשים לחוש שהם מתוגמלים בנדיבות על גישות חדשות. הדילמה השגויה בשאלת העדיפות בין מודיעין אנושי למודיעין טכנולוגי יכולה להיפתר, אם ארצות הברית וישראל יחלו לקדם את אלה שרואים את הפוטנציאל הטמון בשילוב בין שתי הגישות, ויכשירו אנשים בעלי מיומנויות באמצעים ובמתודולוגיות הרלוונטיים.

שנית, ארצות הברית וישראל צריכות להתחיל לפתח גופי לימוד והכשרה משל עצמן, כדי להכשיר מומחים שישכילו להתנהל בשפה ובטכניקות של שתי הגישות המודיעיניות. ישנן אין ספור דוגמאות לתהליך דומה שכבר מתרחש בעולם, כאשר היריבות הבולטות של ארצות הברית וישראל בתחום זה הן סין ורוסיה. לא יהיה זה רעיון גרוע במיוחד לחקות במקרה זה את המתחרות. תוכניות הכשרה הדרגתיות יוכלו להקל על הדור הנוכחי של מומחי המודיעין לעקוב אחר השילוב בין השיטות המודיעיניות השונות ולהבין את הצורך בו.

אין לצפות שעובדים לא טכניים יהפכו למדעני מחשב, או שמומחים טכניים יהפכו לפתע ל"מרגלי־על" מוכשרים. במקום זאת, המאמצים צריכים להיות מופנים לקידום ולקיום תקשורת בין שתי הקבוצות, באופן שייצור שיח ושיתוף פעולה ביניהן, אפילו אם כל אחת מהן תמשיך להיות נעדרת מומחיות בתחומה של השנייה. הרעיון הוא לקדם יכולת יותר מאשר לתבוע מומחיות. מפתיע להיווכח שהיתרון הטמון בגישה זו הוחמץ עד היום. אם השילוב בין מודיעין אנושי למודיעין טכנולוגי לא יילקח ברצינות כחלק מהחשיבה על עתידו של המרחב המודיעיני, פירוש הדבר הוא שתימשך "מלחמת האזרחים" הסמויה ומשבשת הפעילות בין שתי הגישות, ויחסים שאמורים היו להפוך לברית, יישארו למרבה הצער יחסים של יריבות מסוכנת.

הערות

1 Intelligence Science Board, *The Intelligence Community and Science and Technology: The Challenge of the New S&T Landscape* (Washington, DC.: Office of the Director of National Intelligence, 2010), https://fas.org/irp/dni/isb/landscape.pdf.

2 Ashley J. Tellis, *Pakistan – Conflicted Ally in the War on Terrorism* (Washington, DC.: Carnegie Endowment for International Peace, 2007), http://carnegieendowment.org/files/pb56_tellis_pakistan_final.pdf.

3 Katherine Beard, "Behind America's Decline in Math, Science and Technology", *US News & World Report*, November 13, 2013, http://www.usnews.com/news/articles/2013/11/13/behind-americas-decline-in-math-science-and-technology.

4 Andy Savoie, "Boots on the Ground: HUMINT Needed for Urban Warfare", *Aerospace Daily & Defense Report*, December 8, 2004, http://aviationweek.com/awin/official-boots-ground-humint-needed-urban-warfare.

5 Ibid.

6 "Women in Combat, and the Price they Pay", *NPR, Morning Edition*, March 18, 2013, http://www.npr.org/2013/03/18/174444738/women-in-combat-and-the-price-they-pay.

7 WMD Commission, *Final Report of The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction* (Washington, DC.: Library of Congress, 2005), https://fas.org/irp/offdocs/wmdcomm.html.

8 Kevin M. O'Connell, "The Role of Science and Technology in Transforming American Intelligence", in *The Future of American Intelligence*, ed. Peter Berkowitz (Stanford: Hoover Institution Press, 2005), pp. 139-174, http://media.hoover.org/sites/default/files/documents/0817946624_139.pdf.

9 Rand C. Lewis, "Espionage and the War on Terrorism: Investigating U.S. Efforts", *Brown Journal of World Affairs* 11, no. 1 (2004): 175-182.

10 Ishmael Jones, *The Human Factor: Inside the CIA's Dysfunctional Intelligence Culture* (New York: Encounter Books, 2008).

11 Public Law Pub. L. 109-177, *USA PATRIOT Improvement And Reauthorization Act of 2005* (Washington, DC: Congressional Publications, March 9, 2006).

12 Denis O'Connor, *HMRC Handling of Human Intelligence Sources* (London: Inspectorate of HM Revenue and Customs, 2006), https://www.justiceinspectorates.gov.uk/hmic/media/hmrc-the-handling-of-human-intelligence-sources-20070325.pdf.

13 Robert K. Ackerman, "Defense HUMINT Needs Technology, Too", *Signal*, October 2006, http://www.afcea.org/content/?q=defense-humint-needs-technology-too.

14 Paul Todd & Jonathan Bloch, *Global Intelligence: The World's Secret Service Today* (New York: Zed Books, 2003).

15 Kristin Roberts, "When the whole World has Drones", *National Journal*, March 21, 2013.

16 Matthew Crosston, "American UAV Apartheid and the 'Blowback' of New Drone Armies", *New Eastern Outlook*, April 3, 2015, http://journal-neo.org/2015/04/03/american-uav-apartheid-and-the-blowback-of-new-drone-armies/.

17 East West Services, "Iran Announces New 'Epic' Combat UAV with Stealth Capability", *Geo-Strategy Direct*, May 22, 2013.

18 Crosston, "American UAV Apartheid and the 'Blowback' of New Drone Armies".

19 East West Services, "Singapore First East Asian Military to Deploy Israeli Strategic UAV", *Geo-Strategy Direct*, June 6, 2012.

20 "Asia UAV Acquisitions", *Defence Review Asia* 3*,* no. 7 (2009): 20.

רגולציה במרחב הסייבר בישראל – תשתית מושגית, אתגרים ודרכי התקדמות

גבי סיבוני ועידו סיון

בעיית ביטחון מרחב הסייבר (Cybersecurity) חוצה תחומים, מגזרים וגישות. מאמר זה מציג את עמודי התווך של הבעיה, מאמץ פרדיגמה לפיה המדינה היא מנהלת סיכונים עבור הציבור דרך רגולציה, וסוקר את הרקע וההסברים להתפתחות הרגולציה בעולם המודרני. בהמשך, המאמר עומד על הדומה והשונה בין ארצות הברית, האיחוד האירופי ומדינת ישראל באופן בו הן בוחרות להתמודד עם אתגר ביטחון מרחב הסייבר, ומדגיש את החשיבות והקשיים בהכלת רגולציה מדינתית בתחום זה על המגזר האזרחי. המאמר גם סוקר כיווני התקדמות אפשריים בשאלת ביטחון מרחב הסייבר ומעלה הצעות כיצד להבטיח את חוסנו הקיברנטי של המגזר האזרחי.

מילות מפתח: רגולציה, סיכונים, ביטחון סייבר, מגזר אזרחי

מבוא

ההתנהלות במרחב הסייבר הינה אתגר עבור מקבלי ההחלטות. האתגר נובע בראש ובראשונה מתלות המדינה והחברה במרחב הסייבר, שהוא מיסודו פגיע. מרחב זה מאפשר זרימת מידע, המסייעת ברוב המקרים לפריחה כלכלית, להגברת היעילות ולרווחה חברתית, אך הוא גם נתון לאיומים ביטחוניים, פליליים ומסחריים. האתגרים לחוסנו של מרחב הסייבר[1] נובעים ממספר סיבות עיקריות:

- ראשית, ישנה אסימטריה מובהקת בין חסמי הכניסה הנמוכים לתוקפים ובין עלויות הגנה גבוהות. בעוד שתקיפה מוצלחת זקוקה לווקטור התקדמות יחיד, מאמצי ההגנה מתיימרים לכסות את כלל הפגיעויות האפשריות.

ד"ר גבי סיבוני הינו ראש תוכנית ביטחון סייבר במכון למחקרי ביטחון לאומי. עידו סיון הינו חוקר ניובאואר בתוכנית ביטחון סייבר במכון למחקרי ביטחון לאומי.

- שנית, מרחב הסייבר נשען על פרוטוקולי תקשורת מיושנים המאפשרים אנונימיות רבה לתוקפים ומקשים על רשויות אכיפת החוק לזהות את מקור התקיפות.[2]
- שלישית, מרחב הסייבר מאפשר הן ניצול החולשות הרבות של חומרה/תוכנה והן שימוש בכלי תקיפה קיימים שכבר פעלו בהצלחה בתקיפות קודמות. תופעה זו גוררת מרוץ חימוש מואץ המדרדר עוד יותר את רמת האבטחה, וראיה לכך הוא השוק המשגשג לניצול חולשות zero-day.[3] לאחרונה נחשפה פעילות של חברות מסחריות הסוחרות עם ממשלות בחולשות תוכנה ובכלי תקיפה לצורכי ריגול נגד אזרחים ומתנגדי משטר.[4]
- רביעית, היעדר כלים לשיתוף מידע על האיומים במרחב הסייבר ועל אמצעי ההגנה שנוקטות חברות מסחריות מקשה על גיבושו של מאמץ קולקטיבי ופרו־אקטיבי למניעת תקיפות במרחב זה. הדבר נובע בראש ובראשונה משיתוף מידע חלקי ומשקיפות מוגבלת של חברות מסחריות במגזר האזרחי.[5] עם זאת, גם המגזרים הצבאי והמדינתי לא תורמים את חלקם בשיתוף מידע כזה.
- חמישית, יש מחסור בתמריצים כלכליים ובכלים טכנולוגיים לפיתוח הגנה נאותה. אמנם, נזקי הסייבר, המוערכים כיום במיליארדי דולרים, מתַמרצים את כוחות השוק להגן על עצמם, אך ברמה המדינתית המגזר האזרחי ברובו אינו חייב בדיווח במקרה של פריצה או של איום סייבר שהתממש. אי לכך, עלויות הנזק כתוצאה מפריצה מוצלחת ומוניטין החברה הנפרצת אינם מונחים על הכף באופן שיתמרץ חברות להגן על עצמן מבעוד מועד. למרות מודעות גוברת של בעלי מניות וקהל הלקוחות במגזר הפרטי לתחום הסייבר, אין הנחייה גורפת ומחייבת לפרסם אירועי סייבר ולדווח על נזק שנגרם. בנוסף לכך, יכולותיו של ארגז הכלים הטכנולוגי הקיים היום בשוק אינן מספיקות ליצירת הגנה הרמטית.[6]
- לבסוף, מרבית המשתמשים במרחב הסייבר אינם מודעים לסכנות שהוא טומן בחובו ומזינים אותו במידע רגיש וקריטי שאינו מוגן כראוי. בנוסף, משתמשים רבים נופלים קורבן לניסיונות חדירה באמצעות הנדסה חברתית, בוחרים סיסמאות באופן חלש מדי, ובמרבית התקיפות מהווים את החוליה החלשה דרכה נפרצות מערכות.[7]

אין זה מפתיע כי חדשות לבקרים מתקבלים דיווחים מרחבי העולם על חולשות חדשות שנחשפות ועל פריצות למאגרי מידע, גניבת מידע רגיש והסבת נזק למערכות ממוחשבות.[8] הקלות בה חברות מסחריות ומדינות אוספות ומאחסנות מידע קריטי אינה תואמת את יעילות המאמצים הנעשים כדי להגן על מרחב הסייבר, אף שהמדינה מנסה להתערב ולמנוע התממשותם של סיכוני סייבר, או לצמצמם בדיעבד. כך אנו מוצאים עצמנו תלויים לחלוטין בתפקודו התקין של מרחב שביסודו הוא פגיע.

הסיכונים הנשקפים ממרחב הסייבר הינם המשך טבעי של סיכוני המדינה המודרנית, כפי שתיאר הסוציולוג אולריך בק בספרו פורץ הדרך מ־1986, *Risk Society*.[9] לדברי בק, החיים המודרניים על פיתוחיהם הטכנולוגיים טומנים בחובם הזדמנויות רבות, אך גם יוצרים סכנות חדשות לאדם ולסביבה. הכלכלן דיוויד מוס (Moss) התייחס ב־2002 למורכבות של ניהול סיכונים אלה על ידי הממשלה.[10] מוס הראה כיצד ממשלת ארצות הברית, כמנהלת סיכונים עבור החברה האמריקאית, עברה דרך שלושה שלבי התפתחות עוקבים באסטרטגיית ניהול הסיכונים שלה. ראשיתו של התהליך הייתה במאה ה־19, כאשר ארצות הברית התערבה באופן אגרסיבי בניהול סיכונים לעידוד השקעות וצמיחת המשק (על ידי חוקים, כגון חוק חברה בע"מ, המגביל את הסיכון עבור המשקיעים בחברה, וחוק פשיטת רגל, המגן על משקיע מלרדת מכל נכסיו). בהמשך עברה המדינה לניהול סיכונים עבור בטיחות העובדים ויציבות חיי שוק העבודה (חוקים לפיצויים ולביטחון סוציאלי לעובדים כביטוי להולדתה של מדינת הרווחה האמריקאית). לבסוף, בשלב הנוכחי בעת המודרנית, המדינה עוסקת בניהול סיכונים עבור כלל החברה – תחילה סיכוני סביבה, בטיחות במזון וכדומה, וכעת סיכוני סייבר, הנובעים מפיתוחים מודרניים ומהסיכונים הכרוכים בהם.[11]

אסטרטגיות ניהול הסיכונים שנוקטת המדינה המודרנית נעות על הרצף שבין הפחתת הסיכונים ובין חלוקתם מחדש בחברה. מצד אחד, הפחתת סיכונים כוללת בעיקר מניעה של סיכונים מבעוד מועד (למשל, רגולציה לבטיחות, שלטים המזהירים מפני מהירות מופרזת, ובשדה הסייבר – דרישות אבטחת מידע למניעת פריצה למערכות), וכן צעדי צמצום נזקים (mitigation) שמטרתם להפחית את הנזק כתוצאה מסיכון שכבר התממש (למשל, רגולציית כיבוי אש; או בשדה הסייבר – צעדים לצמצום נזק מהתקפות סייבר[12] ודיווח לאזרחים וגורמים מדינתיים על פריצה שקרתה כדי שיתגוננו מפניה).

מצד שני, חלוקה מחדש של סיכונים עוסקת בהעברת האחריות לסיכון בין הישויות השונות. למשל, חוקי בטיחות מוצרים (Product Liability Laws) מסיטים את האחריות מהצרכן ליצרן. דוגמה עכשווית משדה הסייבר הם חוקי שיתוף מידע במרחב הסייבר (Cyber Information Sharing Act) המגבילים את האחריות של חברות מסחריות הבוחרות לשתף מידע עם הממשלה על פריצות סייבר. חלוקה מחדש של סיכונים יכולה לבוא לידי ביטוי גם כפיזור סיכונים על פני מבוטחים שונים, למשל בחברות ביטוח, כאשר כל מבוטח משלם פרמיה מסוימת כדי לכסות את הנזק מסיכון שיתממש אצל אחד המבוטחים. פיזור הסיכונים על ידי המגזר הפרטי בעולם הסייבר נעשה בעיקר עבור סיכוני צד שלישי,[13] עד כה ללא התערבות מדינתית.

על אף אסטרטגיות ניהול הסיכונים הרבות שעומדות בפני המדינה, היא טרם השכילה למצוא את האופן הראוי בו עליה להתערב, בעיקר במגזר האזרחי, כדי להבטיח את רציפותו התפקודית, חוסנו ויציבותו של מרחב הסייבר. החשיבות של המגזר האזרחי לחוסנו של מרחב זה היא עצומה: המגזר האזרחי מהווה את חלק הארי במרחב הסייבר, נחשף למרבית האיומים, ולפגיעה בו יש השלכות כלכליות וביטחוניות על חוסנה של החברה.

רגולציה מדינתית: רקע והתפתחות

רגולציה ברמה הבסיסית ביותר היא פעולת הסדרה, פיקוח ואכיפה המבוצעות על ידי המדינה או סוכנויות מדינתיות עצמאיות במטרה לכפות באופן חוקי כללי התנהגות מחייבים. רגולציה כזאת חלה על "נמעני רגולציה" שאותם הגוף הרגולטורי שואף להסדיר.

מושג הרגולציה נולד בארצות הברית בסוף המאה ה־19 כדרך פוליטית ומינהלית להסדיר את השוק. הרגולציה הפכה לכלי מרכזי בידי אנשי ממשל, שכן היא הייתה תגובה טבעית לכשלי שוק, להיעדר פיקוח ולהיווצרותם של "מונופולים טבעיים". לעומת זאת, באירופה הדגש היה לא על הרגולציה, אלא על הלאמה של השוק. פיקוח באמצעות הלאמה עיכב את התפתחות המסורת הרגולטורית באירופה לעומת ארצות הברית. יחד עם זאת, מסוף שנות השבעים של המאה הקודמת ואילך חלה התרחבות של השימוש ברגולציה והוקמו סוכנויות אכיפה עצמאיות בארצות הברית, וכן נעשה שימוש מסיבי בכלים רגולטוריים באירופה כחלק מהאצת האיחוד הכלכלי של היבשת.[14]

עם עלייתם לשלטון של מרגרט תאצ'ר בבריטניה (1979) ורונלד רייגן בארצות הברית (1981) חלה התרחבות בפעילות של סוכנויות רגולטוריות עצמאיות שפעלו להסדרת השוק, במה שזכה לכינוי "המדינה הרגולטורית".[15] תפקיד המדינה עבר אט־אט ממסבסדת שירותים ומסייעת לצמצום פערים, לייעול השוק באמצעות רגולציה (או דה־רגולציה)[16] מוגברת.

רגולציה נתפסת לרוב כחקיקה/חקיקת משנה על ידי המדינה או סוכנויות רגולטוריות עצמאיות. היא יכולה לבוא לידי ביטוי גם בהוראה/צו/הנחייה מחייבת. תפקיד הרגולציה הוא להסדיר את פעילות השוק, בעוד שקביעת המדיניות נעשית על ידי הדרג המדיני. ב"מדינה הרגולטורית" יש תפקיד מרכזי למומחים, והדרישה למומחיות גבוהה היא המוטיבציה הראשונית להקמת סוכנויות רגולטוריות עצמאיות.[17]

ניתן להסביר את חשיבותה של רגולציה עבור הציבור במספר אופנים:

- ראשית, הרגולציה שואפת להגן על ערכים ועל חירויות האזרח שעלולות להיפגע על ידי בעלי הכוח או איומים מבחוץ. משימה זו מסבירה את הצורך בכוחות צבא וביטחון מצד אחד, אך גם ברשויות שיבלמו ויאזנו אותם במידת הצורך מצד שני.
- שנית, רגולציה מוצדקת מבחינה כלכלית. תפקיד הרגולציה הוא לתקן כשלי שוק הנובעים מהתנהלות השוק החופשי באופן שלא משרת את האינטרס הציבורי.[18] לדוגמה, מונופול המתמחר ומספק מוצרים כראות עיניו, ועל כן יש להטיל עליו פיקוח.
- שלישית, רגולציה מתחייבת במצב של היעדר מידע או של אסימטריה במידע. מצב כזה גורם לצרכנים, לחברות או למדינות להתנהג בצורה שלא משרתת את האינטרס הציבורי, ובמקרה זה תפקידו של הרגולטור הוא לאפשר שקיפות וזרימת מידע.
- לבסוף, רגולציה נובעת מהרצון להבטיח את קיומם של משאבים ציבוריים מְתכלים שאי אפשר למנוע את השימוש בהם, החל מאיכות האוויר וכלה בכמות הדגים בים. על הרגולטור לדאוג שמשאבים כאלה ימשיכו להתקיים, על אף שכוחות השוק נוטים לכלותם.

אופן הפעילות של הרגולטור במדיניות הציבורית והיווצרותה של רגולציה מוסברים בספרות בצורות שונות ומגוונות. תיאוריית האינטרס הציבורי (פונקציונאליזם) גורסת כי רגולציה פועלת לקידום טובת הכלל ולהגדלת הרווחה החברתית.[19] לעומתה, תיאוריית האינטרס הפרטי גורסת כי הרגולטור מונע מתוך אינטרסים פרטיים במטרה להגדיל את רווחתן של קבוצות אינטרס מרוכזות המייצגות בדרך כלל פלח קטן באוכלוסייה. הרגולציה בהיבט הזה היא תוצר של היחסים בין קבוצות אינטרס ובין המדינה ובינן לבין עצמן.[20] בנוסף, אפשר לתת למשטרים רגולטוריים הסבר מוסדי. במקרה זה יכולותיו (capacity) של המוסד הרגולטורי[21] או מיקומו ההיסטורי בהליך המדיניות הציבורית[22] מסבירים את הבניית הרגולציה באופן בו היא נוצרה. בעשרים השנים האחרונות התפתח זרם נוסף, המסביר רגולציה מתוך תיאוריה רעיונית. על פי תיאוריה זו, לפרדיגמות יש תפקיד מרכזי בהליך העיצוב של המדיניות הציבורית.[23] רעיון מסוים נתפס כ"נכון" ב"חלון הזדמנות" מסוים וסוחף אחריו את מקבלי ההחלטות ליצירת רגולציה ברוח הפרדיגמה והאינטרסים העוטפים אותה.[24] קרי, רעיונות ואינטרסים שזורים במקרים רבים זה בזה, כאשר רעיון מסוים עוזר לתת לגיטימציה וביטוי לאינטרסים שבכוחם ליצור רגולציה שתשרת את מטרותיהם.[25]

גישות רגולציה במרחב הסייבר בעולם המערבי ובישראל

הרגולציה הולכת ומתרחבת בחיים המודרניים, וההסברים לקיומה והאופנים בהם היא מתהווה שונים ומגוונים. עם זאת, רגולציה במרחב הסייבר טרם נבחנה בספרות

באופן מספק. להלן יפורטו האתגרים שטומנת בחובה רגולציית מרחב הסייבר, דרכי ההתמודדות של רגולטורים עם בעיית ביטחון מרחב הסייבר, והאופן שבו ארצות הברית והאיחוד האירופי[26] מבַנות את משטרי הרגולציה שלהן במרחב זה בהשוואה לישראל. בהמשך יתמקד המאמר ברגולציה הישראלית על מרחב הסייבר ויצביע על הפער המהותי הקיים במשטר זה – המגזר האזרחי.

רגולציה במרחב הסייבר נוגעת להגנה לא רק במובן הקלאסי; היא טומנת בחובה היבטים רבים הקשורים באופן ישיר לביטחון הלאומי, להגנה על נכסים וקניין רוחני, למניעת פשיעה ולשמירת מידע והזכות לפרטיות. יחד עם זאת, הרגולציה מציבה אתגרים בפני הרגולטורים משלוש סיבות עיקריות:

- ראשית, העלויות המושתות על אלה הנדרשים להגנה על מרחב הסייבר הן גבוהות ויוצרות התנגדות נחרצת מצד המגזר הפרטי, המהווה את חלק הארי של מרחב זה, לרגולציה מכל סוג שהוא.[27]
- שנית, אין הנחייה מדינתית המורה על מידת השקיפות של חברות מסחריות בכל הנוגע לרמות ההגנה ולחומרת התקיפות המתרחשות בפועל. הן התוקפים והן המתגוננים משתפים ביניהם מידע,[28] אך מאמצי ההגנה אינם נהנים לרוב מהתארגנות קולקטיבית בקנה מידה נרחב. כאשר סודות מסחריים ומוניטין של חברות מונחים על כף המאזניים, אין זה מפתיע כי המגזר האזרחי אינו שש לשתף מידע על המתרחש במרחב הדיגיטלי שלו.
- שלישית, רגולציה במרחב הסייבר, כבכל מקום אחר, טומנת בחובה קונפליקט בין אינטרסים, שהבולטים הם המאבקים בן אטטיזם[29] לליברליזם ושל הזכות לפרטיות מול הזכות לביטחון.[30] מאבקים הקשורים לאינטרסים של הביטחון הלאומי מול הרצון בפיתוח כלכלי (המשתקפים בפיקוח על ייצוא מוצרים), כמו גם מכשולים בשיתוף מידע בין חברות הנובעים מהוראות מחמירות מצד הממונה על ההגבלים העסקיים, משקפים רק במעט את הקשיים בכינון רגולציה בתחום הסייבר. הקונפליקטים הללו נותנים דרור לאינטרסים מנוגדים ולמאבקי כוח סביב האופן בו יש להבנות את הרגולציה במרחב הסייבר.

נוכח אתגרים אלה, רגולציה של מרחב הסייבר כוללת בדרך כלל ארבע דרכי התמודדות עם בעיית האבטחה של מרחב זה.[31] הדרך הנפוצה היא התוויה של סטנדרטים ודרישות בתחום אבטחת המידע, הכוללים בין היתר הצפנה, ניטור, גיבויים, הזדהות חזקה וכיוצא באלה. בנוסף, בעיקר בארצות הברית, הרגולציה עוסקת בעידוד וביצירה של מכניזמים לשיתוף מידע בין חברות מסחריות ובין המדינה מתוך רצון להתמודד עם בעיית חוסר המידע, ועל ידי כך להתגונן מבעוד מועד מפני התקפות ולצמצם נזקים של התקפה שכבר התרחשה. שדה הרגולציה מתאפיין גם ביצירה של סוכנויות רגולטוריות ובמתן סמכות למוסדות מדינתיים לאכיפת סטנדרטים ופרקטיקות הגנה בתחום ביטחון מרחב הסייבר.[32] לבסוף,

משטרים רגולטוריים כוללים בתוכם צעדים לצמצום נזקי פריצה עבור צד שלישי, הכוללים דיווחים ל־CERT הלאומי[33] וללקוחות שמידע אישי עליהם נגנב. הדבר עולה בקנה אחד עם "מעגל ההגנה השלם",[34] הכולל צעדי מניעה, שיתוף מידע וצמצום נזקים אחרי מתקפה, היוצרים מעטפת הגנה קוהרנטית לארגונים במרחב הסייבר.

כלי הרגולציה המשמשים דרכי התמודדות אלו הינם לרוב חקיקה, הנחיות מדינתיות מחייבות מצד סוכנויות רגולטוריות[35] ורגולציה עצמית שמקורה באימוץ תקנים מומלצים – תקני ISO לאבטחת מידע[36] או תקני PCI עבור חברות מקוונות העוסקות בשירותי סליקה[37] – או מומחיות פנים־ארגונית הכוללת הנחיות להגנת רשתות המחשבים של הארגון אך אינה מפורסמת ברבים. גם המדינה מפרסמת סטנדרטים והנחיות על האופן בו מומלץ להגן ועל האסטרטגיות אותן יש לנקוט. בארצות הברית, למשל, מכון התקנים הלאומי (National Institute of Standards and Technology – NIST) מקפיד לפרסם סטנדרטים להגנה והצפנה של מערכות מידע.[38] במגזר הפיננסי, (The Financial Industry Regulatory Authority (FINRA סוקרת עבור חברות פיננסיות אמריקאיות את האסטרטגיות הרצויות להגנה במרחב הסייבר.[39]

בעולם המערבי יש שתי גישות עיקריות להתמודדות המדינה עם סיכוני מרחב הסייבר. בארצות הברית הרגולציה מבוססת בעיקר על מודלים וולונטריים, סקטוריאליים, מרובי סוכנויות, עם משקל נכבד לכוחות השוק.[40] האיחוד האירופי מציג גישה היררכית עם מוסדות רוחביים בעלי סמכות אכיפה חזקה, כאשר המדינה נמצאת במרכז וחלקים גדולים במגזר הפרטי כפופים לרגולציה. ארצות הברית מאמינה כי האינטרס העסקי יוביל חברות להגן על עצמן, בעוד שהאיחוד האירופי דוגל בגישה מתערבת יותר, בה המוסד המדינתי דואג להגנת המגזרים השונים לרווחת האזרחים. שקיפות כלפי אירועי סייבר נאכפת הן בארצות הברית והן באיחוד האירופי: בארצות הברית הדבר מבוצע ברמה המדינתית, כאשר ישנן 47 גרסאות של Data Breach Notification.[41] האיחוד האירופי, מצדו, קיבל לאחרונה את דירקטיבת הגנת המידע המשודרגת שלו (General Data Protection Regulation), שנכנסה לתוקף במאי 2016 ותיושם החל ממאי 2018. דירקטיבה זו מבטיחה סטנדרט אחוד לדיווח ופיצוי על אירועי סייבר. הלוגיקה של מקבלי ההחלטות באירופה הינה ליצור תמריצים עבור השוק להגן על עצמו מבעוד מועד, כדי שלא לשאת בהוצאות הדיווח והפיצוי הנוקשות.[42] לבסוף, בארצות הברית מסתמנת הרחבה של אסטרטגיות הסיכון אותן נוקטת המדינה – לא רק מניעה וצמצום נזקים כתוצאה מפגיעות סייבר, אלא הסטת האחריות מחברות מסחריות במטרה לעודד שיתוף מידע. גישה זו טרם אומצה באיחוד האירופי, וספק אם תאומץ נוכח הפגיעה האפשרית בזכות לפרטיות, הנתפסת באירופה כזכות אזרחית

בסיסית עליה המדינה צריכה לשמור. שיתוף המידע כולל מתן לגיטימיות לאיסוף מידע מוגבר על ידי חברות מסחריות והעברתו למדינה, וקשה להאמין שגישה כזאת תאומץ על ידי האיחוד האירופי מבלי שיתלוו לה אחריותיות ושקיפות מתאימות.

שתי הגישות נותנות מענה חלקי בלבד. הן אינן כוללות הסדרה של המגזרים הביטחוניים־ממלכתיים (צבא, גופי מודיעין וכדומה), שבדרך קבע פטורים מרגולציה ממשלתית ובעיקר מיישמים מודל של "רגולציה עצמית", וגם לא מענה כולל למגזר האזרחי על רבדיו השונים, הכוללים חברות מסחריות, גופי תעשייה והאזרחים עצמם.

ישראל מהווה מעין ייצור כלאיים בין שתי גישות אלו. מצד אחד, רוב המגזר האזרחי בה אינו נתון תחת רגולציה מחייבת כלשהי, והמדינה (כמו בארצות הברית) מסתמכת על כוחות השוק שימצאו את האיזון הנכון בין צורכי ההגנה על מרחב הסייבר ובין ההשקעה הכלכלית הדרושה לשם כך; מצד שני, הגישה האטטיסטית באה לידי ביטוי בחברות פרטיות כמו הבנקים, שבשל חשיבותן האסטרטגית מדינת ישראל החליטה להתערב באבטחתן. המדינה אף מטילה סנקציות על חברות פרטיות במקרה שהן לא עומדות בתנאי הסף הרצויים. יש לכך יוצא מן הכלל בדמות חוק הגנת הפרטיות, הכולל בתוכו היבטים של הגנת מידע ומוכל על מחזיקי מידע אישי באשר הם בכל המגזרים. יחד עם זאת, חוק הגנת הפרטיות נחקק ב־1981 והיבטי הגנת המידע שבו טרם עודכנו.

תהליך התגבשות הרגולציה במרחב הסייבר בישראל כוללת שני שלבים עיקריים, שהתגבשו ללא אסטרטגיה לאומית שחלה על כלל המגזרים במשק.[43] ראשיתו של משטר הסייבר בישראל הוא בחוק להסדרת הביטחון בגופים ציבוריים (1998), שפירט את הדרישות להגנה על מערכות המידע של גופים שהוגדרו כ "חיוניים" למדינה. אלה כללו את גופי התעופה, תשתיות המים, החשמל והתקשורת. ב־2002 נקבע כי המנחה המקצועית של גופים אלה תהיה הרשות הלאומית לאבטחת מידע (רא"ם) הכפופה לשירות הביטחון הכללי (שב"כ).[44] כמו כן נקבע כי גופים "חיוניים" הזוכים להנחיה מרא"ם ייבחרו בקפידה על ידי ועדת היגוי ייעודית. רשימת הגופים החיוניים הלכה והתרחבה עם השנים. גופים שהוגדרו כחיוניים עבור המדינה על סמך עוצמת הנזק שהם עלולים להסב (למשל, ביחס לתל"ג) קיבלו הנחיה מדינתית, בעוד שגופים רבים שלא הוגדרו כבעלי פוטנציאל נזק גבוה נותרו ללא הנחיה, והגנתם נגזרה בעיקר משיקולים כלכליים של כוחות השוק. ראוי לציין כי הגופים המונחים הינם פרטיים וציבוריים כאחד (למשל, בתי הזיקוק, חברת אל על, חברת החשמל, חברת רכבת ישראל).

ישראל נכנסה בשנת 2011 לשלב ב' בפיתוח הרגולציה במרחב הסייבר, כאשר הממשלה שינתה את גישתה והחלה לתת את הדעת לעבודה הנדרשת מול המגזר האזרחי. הרצון ליצור אינטגרציה מוצלחת יותר עם כוחות השוק הוביל להקמת

הדומה והשונה בין המשטרים הרגולטוריים בארצות הברית, בישראל ובאיחוד האירופי

	ארצות הברית – משטר רגולטורי ליברלי – נשען על כוחות השוק וברובו וולונטרי	**ישראל – בין ליברליזם לאטטיזם – תשתיות קריטיות תחת פיקוח המדינה, והשוק נתון לכוחותיו**	**האיחוד האירופי – משטר רגולטורי אטטיסטי – ריכוזי ומחייב**
נוכחות מדינתית	במגזרים קריטיים בלבד – אנרגיה, בריאות, חשמל, מים וכדומה	במגזרים קריטיים בלבד – אנרגיה, בריאות, חשמל, מים וכדומה	במגזרים קריטיים ובספקי שירותים מקוונים
אסטרטגיות ניהול סיכונים	אסטרטגיה מתקדמת – מניעת תקיפות סייבר וכן חלוקה מחדש של האחריות כלפי סיכונים במגזר האזרחי	לא קיימת רגולציה המגבילה אחריות ומסיטה סיכון בין הישויות השונות, או כזו המחייבת צמצום נזקי סייבר לחברות וללקוחותיהן בהינתן פריצה מוצלחת	אסטרטגיה של מניעת התקפות וצמצום נזקים, ללא חלוקה מחדש של האחריות כלפי סיכונים בחברה
שקיפות כלפי צרכנים בעת אירוע סייבר	קיימת ברמת המדינות בצורה לא אחודה וב־47 גרסאות שונות	לא קיימת	קיימת באופן קוהרנטי ואחיד תחת הדירקטיבות שאושרו ב־2016 ויגיעו למימוש ב־2018
קונפליקט עם הזכות לפרטיות	מנוהל ברובו על ידי כוחות השוק, פרט למגזרים ספציפיים (רישומי בריאות, מידע על קטינים וכדומה)	מנוהל ברובו על ידי כוחות השוק, עם דרישות מחמירות יחסית שלא נאכפות במלואן על ידי הרשות למשפט וטכנולוגיה (רמו"ט)	מנוהל על ידי המדינה עם חוקים מחייבים, מוסדות בעלי כוח, ומונע מתוך אינטרסים של שמירה על פרטיות, כזכות האדם הגוברת על אינטרסים כלכליים. ברמת מדינות האיחוד, הזכות לפרטיות מתערערת אל מול סוכנויות המודיעין המקומיות

מטה הסייבר הלאומי במשרד ראש הממשלה. בהמשך, הוקמה ב־2015 הרשות הלאומית להגנת הסייבר, כגוף הביצועי להגנה על מרחב הסייבר במדינה, אשר הציב לעצמו כמטרה לעבוד ישירות עם המגזר האזרחי. באופן סכמטי ניתן לתאר את ההסדרה המדינתית במרחב הסייבר בישראל באופן הבא:

תרשים 1: אופן הפיקוח על הגנת הסייבר בישראל, 2016

שני היבטים עיקריים עולים מתרשים 1: ראשית, כפי שנטען תחילה, המגזר האזרחי בישראל ברובו אינו מונחה. ישנם "איים" שונים, כמו המגזר הפיננסי, מגזר האנרגיה ומגזר הבריאות, המונחים בעיקר על ידי יחידות הסמך שפועלות תחת הנחיית רשות התקשוב הממשלתית. עם זאת, רובו ככולו של המגזר האזרחי מתבסס על הנחייה עצמית, לוקה בשיתוף ידע ומבַצע צמצום נזקים מול הלקוחות כראות עיניו.

בנוסף לפיקוח הסלקטיבי על המגזרים השונים, מדינת ישראל הוציאה לאחרונה שתי הנחיות רגולטוריות משמעותיות. ההנחיה הראשונה, שמטרתה להגביר את הפיקוח שכבר מבוצע על ידי האגף לפיקוח על ייצוא ביטחוני במשרד הביטחון, עסקה בהרחבת היריעה[45] של מוצרים שידרשו פיקוח מדינתי, מתוך רצון של המדינה לפקח על ייצוא הסייבר ולשמור על היתרון היחסי הישראלי. המדינה החליטה להקפיא את המהלך, להמשיך את ההיוועצות עם תעשיית הסייבר ולהמשיך להיצמד לעת עתה להסדרי פיקוח בין־לאומיים בלבד. זאת, נוכח התנגדות התעשייה, שחששה כי לא תוכל להתחרות בתעשיות של מדינות שאינן מפוקחות.[46] הרצון לשמור על מעמדה של ישראל בעולם כיצואנית סייבר מובילה ביחס לגודל האוכלוסייה במדינה,[47] הביא בין היתר לשמירת הסטטוס קוו בנושא הפיקוח. ניתן ללמוד מכך על עומק ההבנה ההדדית ושיתוף הפעולה הנרחב בין התעשיות השונות בישראל ובין משרד הביטחון.[48] המשרד בא לקראת התעשייה,

אך עדיין מקבל דריסת רגל בה ונמצא במעגל קבלת ההחלטות עבור כל מוצר סייבר בעל אפיון התקפי מובהק.

ההנחיה הרגולטורית השנייה שהוציאה המדינה שמה לה למטרה לטפח את ההון האנושי העוסק בהגנת סייבר וליצור סטנדרטים עבורו. זוהי, המלצה רשמית, בה המדינה מפרטת את רמת המקצועיות הנדרשת לעוסקים בהגנת סייבר על רבדיה השונים.[49] מדובר בהנחיה משמעותית, שטרם נוסתה בהרחבה בעולם, ועשויה להעלות את רמת המקצועיות של המעורבים בהגנת מרחב הסייבר בטווח הקצר בדמות מסלולי הכשרה שונים שיפותחו במיוחד, אך גם לייתר את האופן האוטו־דידקטי בו מרבית המומחים בתחום דינמי זה צוברים ידע.[50]

רגולציית סייבר במגזר האזרחי: חשיבות וקשיים

על אף שלל המאמצים שנעשו עד כה, המגזר האזרחי בישראל אינו נתון לרגולציה בתחום הסייבר ונעדר פיקוח מדינתי על אבטחתו.[51] מדובר במצב הקיים גם במדינות אחרות ונותן את אותותיו בין השאר בארצות הברית ובאיחוד האירופי (לפחות עד לשתי הדירקטיבות האירופיות האחרונות, שלראשונה כוללות תעשיות מהמגזר האזרחי).

קשה להפריז בחשיבותו של המגזר האזרחי לעמידותו של מרחב הסייבר, וזאת מכמה סיבות: ראשית, המגזר האזרחי מהווה את חלק הארי של מרחב זה. הוא נחשף למרבית האיומים עליו ומהווה באופן מסורתי את החוליה החלשה דרכה מתחילות תקיפות רחבות על מגזרים נוספים העושים שימוש בסייבר; שנית, חברות פרטיות מספקות שירותים באופן תדיר למשרדי ממשלה וגופים מדינתיים רגישים, ועל כן עמידותן הינה אינטרס ראשון במעלה; שלישית, פגיעה במגזר הפרטי פירושה פגיעה ביציבות המשק, שעלולה בתנאים מסוימים להידרדר לפגיעה חמורה יותר בחוסן הלאומי. מדיניות ההפרטה ההולכת ומתרחבת העמיקה את הבעיה והפכה את המגזר הפרטי לגורם מרכזי עוד יותר, דבר המשליך על מאמצי הרגולציה של המדינה; רביעית, המגזר האזרחי אחראי לפיתוחים הטכנולוגיים עליהם נשענים מגזרים רגישים יותר, ופגיעה בו עלולה להוות "דלת אחורית" וכר פורה לתקיפת מידע רגיש.[52] הדבר נכון במיוחד לחברות הזנק הדלות במשאבי הגנה, אך לעיתים קרובות מפתחות מוצרי הגנה לשימוש הכלל.[53]

התנגדותו העקרונית של המגזר הפרטי לרגולציה אינה מפתיעה, שכן היא חוצה תחומים ונושאים שונים. רגולציה מדינתית ופיקוח נתפסים כמגבילים חברות מסחריות וכמביאים עמם עלויות נכבדות שאין מאחוריהן תועלת משמעותית.[54] בנוסף, המגזר הפרטי תופס את המדינה כגורם שמגיב לאט לשינויים טכנולוגיים ואינו יכול לעמוד באתגרים הניצבים בפני פיקוח על מרחב טכנולוגי דינמי ומשתנה כמו מרחב הסייבר.[55] לפי תפיסתו של המגזר האזרחי, במקום להגביר את עמידות

החברות המסחריות, רגולציה מדינתית עלולה לפיכך לאלץ אותן לאמץ סטנדרטים שאינם תואמים עוד את האיומים הנוכחיים ולמנוע מהן את הגמישות ממנה הן נהנות כיום. לבסוף, הרעיון של התערבות מדינתית אינו עולה בקנה אחד עם גישת הניאו־ליברליזם שהתפשטה כאש בשדה קוצים בחברות קפיטליסטיות במאה העשרים.[56] הפרדיגמה השלטת היא פרדיגמה של הפרטה ודה־רגולציה, לפיה על המדינה להתערב באופן מזערי, אם בכלל, בנעשה בשוק, וזאת כדי למקסם תועלות עבור החברה המסחרית.[57]

תובנות מסכמות

על אף שמדינת ישראל מקדמת את הקמתה של הרשות הלאומית להגנת הסייבר, מגזרים רבים במשק עדיין נעדרים כל הנחיה ופיקוח שיבטיחו הגנה ראויה. חסרה מפת דרכים שתבטיח את חוסנו של המגזר האזרחי ותהווה מודל שיאומץ על ידי השחקנים השונים במשק.

מודל כזה יידרש לתת מענה למספר נקודות מפתח. ראשית, יהיה עליו ליצור תהליך מובנה שיתמרץ גופים אזרחיים לאמץ הגנה קיברנטית. "רגולציית כניסה" דרך חוק רישוי עסקים ברשויות המקומיות היא דרך אחת, אך ניתן לחשוב על דרכים נוספות. השאיפה היא לייצר מעין "חותמת סייבר" מקצועית שתעיד כי הגוף האזרחי מוגן כראוי. המדינה עמלה בימים אלה על חוק הסייבר, שיקבע סטנדרט הגנה אחוד לצורך קבלת תו תקן.[58] ייתכן שהצורך בחותמת אבטחה כזאת יתמרץ גופים להגן על עצמם טוב יותר.

שנית, יש לתת את הדעת לשכבות השונות במגזר האזרחי, שכן אין פתרון אחד שמתאים לכולם ויש צורך בהתאמה מדוקדקת של "חליפת" הרגולציה בהתאם לעיסוק, לרגישות המידע, להליכי הייצור ולשרשרות האספקה של החברות השונות במשק. על כן, יש לבצע מדרוג של המגזר האזרחי על פי חשיפתו לסיכונים והנזק שפריצה למערכותיו עלול לגרום. דין חברת ביטוח אינו כדין חברת תרופות, והמודל המוצע יצטרך לתת את הדעת על הבדלים מהותיים אלה.

שלישית, יש לשקול הרחבה של אסטרטגיות הסיכון אותן נוקטת המדינה. מהסתכלות רוחבית על סקירת הרגולציה הישראלית ניתן ללמוד כי המדינה עוסקת בעיקר במניעת התממשותם של סיכוני סייבר. ייתכן שמגנוני שיתוף המתפתחים בארצות הברית[59] במטרה לעודד שיתוף מידע, מחברות מסחריות, אך עם אי־פגיעה מרבית בזכות לפרטיות, יאפשרו לפתוח את צוואר הבקבוק של העברת המידע וייצרו הגנת סייבר פרו־אקטיבית ויעילה יותר.

לבסוף, יש לפעול להגברת השקיפות על אירועי סייבר בשגרה, תוך חיוב של כל המגזרים לדווח ל־CERT הלאומי, ושיתוף מידע עם האזרחים. הדבר יסייע ללמוד ממה להיזהר ולהבין עד כמה מידע רגיש נמצא בסיכון.

כל הנקודות שנמנו לעיל עשויות ליצור תמריצים יעילים יותר להגנה ולמזעור נזקים (mitigation). חברות מסחריות יחששו מלשאת בהוצאות הכרוכות במזעור הנזקים המעוגנות בחוק, ויש להניח כי יגנו על עצמן בצורה מרבית מבעוד מועד.

לסיכום, הצורך ברגולציית סייבר במגזר האזרחי בישראל הינו ברור. עם זאת, הקשיים בפיתוח רגולציה כזאת הם רבים, החל בקשיים ובמאבקים בין מוסדות המדינה, דרך נקודות חיכוך בין אינטרסים שונים ועלויות הכרוכות בציות לרגולציה, ועד לרצון למצוא את האיזון הנכון בין שקיפות לסודיות ובין ריכוזיות לביזור.

מרחב הסייבר בישראל הוא אזרחי במהותו – רובו המכריע מבוסס כיום על תשתיות, מערכות וטכנולוגיות אזרחיות המופעלות על ידי ארגונים אזרחיים. אף על פי כן, המגזר האזרחי טרם הוסדר וסונכרן אל תוך משטר הרגולציה בישראל. אחריות ההגנה על מרחב הסייבר במגזר זה נתונה כיום בידי הארגונים האזרחיים בלבד. אין בכוחו של הארגון הבודד להעמיד את המומחיות והמשאבים הדרושים כדי להתמודד עם האיומים במרחב הסייבר ללא יצירת תשתית לשיתוף פעולה עם שאר המגזרים במשק.

ישראל פועלת באופן לא מבוטל להגנה על מרחב הסייבר ברמה המדינתית. המדינה הקימה יחידות סמך במשרד ראש הממשלה, קיבלה החלטה על הקמת זרוע סייבר והקימה מסגרות למחקר ופיתוח ומרכזי מחקר לאומיים בתחום הסייבר. עם זאת, המדינה טרם עשתה די להגנת אותם גופים במגזר האזרחי שפגיעה בהם עלולה לפגוע מהותית גם בה. מצב זה מחייב את ממשלת ישראל להמשיך את החתירה ליצירת מסגרת שתאפשר הגנה יעילה על המגזר האזרחי הרלוונטי, וזאת באמצעות מגוון כלים ויכולות בתחום הגנת הסייבר.

הערות

1 המושג "חוסנו של מרחב הסייבר" מתייחס לעמידותו לפגיעות אפשריות כתוצאה מחולשות תוכנה/חומרה, פרוטוקולים לא מאובטחים וגישה לא מורשית למידע.

2 פיתוחם של פרוטוקולים אלה תאם את הצרכים עם ראשיתה של רשת האינטרנט בשנות השישים של המאה הקודמת. הצורך באותם ימים היה לאפשר קישוריות בין כמה עשרות מחשבים, כאשר אף אחד לא חזה כי על פרוטוקולים אלה תישען רשת של מיליארדי משתמשים.

3 חולשות zero-day הן חולשות חומרה או תוכנה שלרוב אינן ידועות ליצרן וטרם תוקנו. לעיתים אלו חולשות מוכרות שטרם הופץ להן תיקון בכל המערכות הרלוונטיות. על השוק המשגשג בתחום זה ראו: Andy Greenberg, "New Dark-Web Market is Selling Zero-Day Exploits to Hackers", Wired.com, April 17, 2015, https://www.wired.com/2015/04/therealdeal-zero-day-exploits.

4 בחודשים האחרונים נחשפו מסמכים פנימיים של חברת Hacking Team האיטלקית שעסקה בניצול חולשות ובפיתוח כלי תקיפה. המסמכים חשפו את היקף המסחר של החברה עם משטרים שונים בעולם. על התופעה הכוללת ראו: Nicole Perlroth, "Governments Turn to Commercial Spyware to Intimidate Dissidents", The New York Times, May 29, 2016, http://www.nytimes.com/2016/05/30/

technology/governments-turn-to-commercial-spyware-to-intimidate-dissidents.html?ref=topics&_r=0.

5 Jason Mallinder and Peter Drabwell, "Cyber Security: A Critical Examination of Information Sharing versus Data Sensitivity Issues for Organizations at Risk of Cyber Attack", Journal of Business Continuity & Emergency Planning, Vol. 7 (2) (2014): 103-111.

6 גבי סיבוני ועופר אסף, "קווים מנחים לאסטרטגיה לאומית במרחב הסייבר", מזכר 149, תל אביב: המכון למחקרי ביטחון לאומי, 2015, עמ' 17, 40.

7 Bruce Schneier, "Credential Stealing as an Attack Vector", Xconomy.com, April 20, 2016, http://www.xconomy.com/boston/2016/04/20/credential-stealing-as-attack-vector/.

8 Nate Lord, "The History of Data Breaches", digitalguardian.com, September 28, 2015, https://digitalguardian.com/blog/history-data-breaches.

9 U. Beck, Risk Society: Towards a New Modernity (Sage Publishing, 1986).

10 David Moss, When All Else Fail: Government as the Ultimate Risk Manager (Harvard University Press, 2002).

11 שם.

12 ראו את "מעגל ההגנה השלם": Gabi Siboni, "An Integrated Security Approach: The Key to Cyber Defense", The Georgetown Journal of International Affairs, May 7, 2015.

13 סיכוני צד שלישי בעולם הסייבר הינם סיכונים לפרטיות לקוחות של חברות מסחריות הנפגעים כתוצאה מפגיעת סייבר וגניבת מידע אישי. חברות הביטוח לא ששות לבטח סיכוני צד ראשון, מאחר ויש חוסר במידע אקטוארי שיסייע לתמחר פרמיות ביטוח עבור סיכוני סייבר לחברות עצמן (קרי, סיכוני צד ראשון).

14 שם.

15 Giandomenico Majone, "The Rise of the Regulatory State in Europe", West European Politics, Vol. 17 (1994): 77-101.

16 פרופ' לוי־פאור מסביר במאמרו "Regulation and Regulatory Governance" מדוע דה־רגולציה מזמינה עוד סוכנויות ופקידים לפיקוח על הפרטות ולשמירה על האינטרסים של המדינה: David Levi-Faur, "Regulation &Regulatory Governance", Department of Political Science & The Federmann School of Public Policy & Government, The Hebrew University, Mount Scopus, Jerusalem, February 2010.

17 שם.

18 שוריק דריישפיץ, "רגולציה – מה, איפה ומתי? מבט תאורטי ומשווה", **פרלמנט**, גיליון 64, מארס 2010: **מי הפריט את המדינה שלי? הפרטה, רגולציה, והמגזר השלישי: תיאוריה ומעשה**, המכון הישראלי לדמוקרטיה.

19 ראו לדוגמה: Harlod Demsetz, "Why Regulate Utilities?", Journal of Law and Economics, Vol. 11 (1968): 55-65.

20 למחקר אמפירי שבחן את הפעילות של קבוצות אינטרס בארצות הברית ראו: F. R. Baumgartner, and B. L. Leech, "Interest Niches and Policy Bandwagons: Patterns of Interest Group Involvement in National Politics", Journal of Politics, Vol. 63 (2001): 1191-1213.

21 מחקר לדוגמה על האופן בו המדיניות להגנת הפרטיות באירופה יצרה מוסדות חזקים שהעבירו חוקי פרטיות נוקשים שנגדו את רוח התקופה: A. L. Newman, "Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive", International Organization, Vol. 62 (01), (2008):103-130.

22 מחקר העומד על העקביות של מדינת הרווחה המודרנית: P. Pierson, The New Politics of the Welfare State (Polity Press, 2006).

23 מחקר על שבירת הפרדיגמה הקיינסיאנית ומעבר לכלכלה מוניטרית בבריטניה: Peter Hall, "Policy Paradigms, Social Learning and the State: the Case of Economic Policymaking in Britain", Comparative Politics, Vol. 25 (3) (1993):275-296.

24 מחקרו של John Kingdon הטביע מושגים כגון "חלון הזדמנויות" ו"יזם מדיניות" שמסבירים בצורה מדויקת להפליא את הליך המדיניות הציבורית: John Kingdon, Agendas, Alternatives and Public Policy, 2nd edition (Boston: Little, Brown, 1995).

25 D. Béland & R. H. Cox eds., Ideas and Politics in Social Science Research (Oxford University Press, 2010), Introduction.

26 אמנם, האיחוד האירופי שונה מהמוסד המדינתי הקלאסי, אך יחד עם זאת הוא מהווה אובייקט חיוני למחקר השוואתי בתחום הסייבר. ההחלטות ברמת האיחוד האירופי הובילו למדיניות הגנת מידע נוקשה בכל רחבי האיחוד, והדירקטיבות המתקבלות ברמת האיחוד מתוות את הדרך למדינות השונות. הדברים תקפים לא רק בהקשרי סייבר. ניתן לראות את השפעת האיחוד האירופי גם בהקשרים של רגולציה על בטיחות מזון ואימוץ מוצרים מהונדסים גנטית במדינות השונות. על חשיבותו הרגולטורית של האיחוד האירופי ראו: David Bach and Abraham L. Newman, "The European Regulatory State and Global Public Policy: Micro-institutions, Macro-influence", Journal of European Public Policy, Vol. 14:6 (2007): 827- 846.

27 Amitai Etzioni, "The Private Sector: A Reluctant Partner in Cyber Security", Georgetown Journal of International Affairs, International Engagement on Cyber, Vol. IV (October 2014): 69-78.

28 לאופן בו האקרים משתפים מידע ב־Darknet ראו ראיון עם Stuart Madnick מ-MIT: Linda Tucci, "Stuart Madnick: Dark Web Hackers Trump Good Guys in Sharing Information", techtarget.com, April 30, 2016, http://searchcio.techtarget.com/news/450295259/Stuart-Madnick-Dark-Web-hackers-trump-good-guys-in-sharing-information.

29 התערבות מוגברת וריכוזית של הממשלה.

30 ראו דיון פילוסופי המאתגר את המושגים "משחק סכום אפס" ו"איזון נדרש" בין ביטחון לחירויות הפרט: Jeremy Waldron, "Security and Liberty: The Image of Balance", Journal of Political Philosophy, Vol. 11 (2) (2003):191-210.

31 דרכי התמודדות אלו עולות כאשר בוחנים את הדרך בה מבוצעת רגולציה לאורך השנים בארצות הברית (ברמה הפדרלית וברמת המדינות) ובאיחוד האירופי (ברמת האיחוד וברמת המדינות החברות בו).

32 למשל, בית המשפט בארצות הברית העניק לאחרונה סמכות ל־Federal Trade Commission (FTC) לאכוף חוקי הגנת מידע במגזר הפרטי. לפרטים נוספים ראו: Brent Kendel, "Appeals Court Affirms FTC Authority over Corporate Data-Security Practices", The Wall Street Journal, August 24, 2015, http://www.wsj.com/articles/appeals-court-affirms-ftc-authority-over-corporate-data-security-practices-1440425754.

33 Cyber Emergency Readiness Team (CERT) – סוכנות רגולטורית הקיימת היום כמעט בכל מדינה. הסוכנות מרכזת את כל אירועי הסייבר החייבים בדיווח ומתכללת תגובה לאירועים משמעותיים שקורים במרחב.

34 Siboni, "An Integrated Security Approach".

35 למשל, הנחיות של הרשות לאבטחת מידע בישראל על האופן בו יש לאבטח רשתות ארגוניות.

36 להסבר על תקני ISO ראו האתר הרשמי: http://www.iso27001security.com/html/27032.html.

37 להסבר על תקני PCI ראו האתר הרשמי: https://www.pcisecuritystandards.org/.

38 ראו לדוגמה סטנדרטים שהפיץ הארגון: http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf.

39 למשל, דוח אחרון של FINRA שהוצא בנושא זה: https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf.

40 Richard J. Harknett, James A. Stever, "The New Policy World of Cybersecurity", Public Administration Review, Vol. 71 (3) (May/June 2011): 455-460.

41 ראו פירוט: "Security Breach Notification Laws", National Conference of State Legislators (NCSL), April 1, 2016, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

42 לפירוט בנושא ההשפעה של הרגולציה האירופית על רמת האבטחה של חברות מסחריות ראו: Warwick Ashford, "Breach Notification the Biggest Impact of EU Data Law Overhaul, Says Law Firm", computerweekly.com, November 27, 2015, http://www.computerweekly.com/news/4500258249/Breach-notification-the-biggest-impact-of-EU-data-law-overhaul-says-law-firm.

43 סיבוני ואסף, "קווים מנחים לאסטרטגיה לאומית במרחב הסייבר", עמ' 22.

44 בשנת 2015 הוקמה הרשות הלאומית להגנת הסייבר שקבלה על עצמה את האחריות על הנחיית עיקר גופי התשתיות הקריטיות במדינת ישראל.

45 הרחבה הכוללת בעיקר מוצרי חדירה, ניתוח פריצות וידע על קיומן של חולשות חומרה/תוכנה.

46 לפרטים נוספים ראו כתבה של כתב אורח, "מאחורי הקלעים של ביטול צו הסייבר החדש", **אתר גיק־טיים**, אפריל 2016, http://www.geektime.co.il/the-decline-of-the-israeli-cyber-law/ .

47 למהפכה בעיר באר שבע, שהמדינה שמה לה למטרה להפוך לבירת ייצוא הסייבר האזורית, ראו: Warwick Ashford, "Israel's Cyber Security Frontier", computerweekly.com, May 2016, http://www.computerweekly.com/opinion/Israels-cyber-security-frontier.

48 Matthew Waxman and Doron Hindin, "How Does Israel Regulate Encryption?", lawfareblog.com, November 30, 2015, https://www.lawfareblog.com/how-does-israel-regulate-encryption.

49 למסמך ההסדרה הרשמי ראו: "מדיניות אסדרת מקצועות הגנת הסייבר במדינת ישראל", **משרד ראש הממשלה – מטה הסייבר הלאומי**, 31 בדצמבר 2015, http://www.pmo.gov.il/SiteCollectionDocuments/cyber/hagana.pdf.

50 ראו דוח בנושא: Professionalizing the Nation's Cybersecurity Workforce (Washington D.C., The National Academy of Sciences, 2013), http://www.nap.edu/catalog/18446/professionalizing-the-nations-cybersecurity-workforce-criteria-for-decision-making.

51 פרט לישויות ספציפיות כמו הבנקים, או לחוק הגנת הפרטיות שחל על כלל המשק אבל לא מספיק מעודכן בהיבטי אבטחת מידע. ראו סקירה בכתבה של רפאל קאהאן,

"נתניהו משווק את הסייבר הישראלי אבל החקיקה בארץ פרוצה", **כלכליסט**, 25 ביוני 2015, http://www.calcalist.co.il/internet/articles/0,7340,L-3662815,00.html.

52 לסקירה מעמיקה יותר של חלק מהסיבות הנ"ל ראו: Etzioni, "The Private Sector: A Reluctant Partner in Cyber Security".

53 גבי סיבוני, דוד ישראל, "הריגול בסייבר והשפעתו על שיקולי חברות עסקיות", **צבא ואסטרטגיה**, כרך 7, גיליון 3, דצמבר 2015.

54 Etzioni, "The Private Sector: A Reluctant Partner in Cyber Security".

55 שם.

56 לסקירה על הגישה הניאו־ליברלית בחברות קפיטליסטיות ראו: John Dryzek, Democracy in Capitalist Times: Ideas, Limits and Struggles (Oxford University Press, 1996).

57 האם הפרטה באמת מובילה לדה־רגולציה? על אתגור הצידוקים להפרטה ראו: יצחק גל־נור, **מדיניות ההפרטה – על מי נטל ההוכחה?** (ירושלים: האוניברסיטה העברית ומכון ון ליר, 2014). על רגולציה בעידן של הפרטות ראו: דוד לוי־פאור, נעם גדרון, סמדר מושל, **הגרעון הרגולטורי של עידן ההפרטה** (ירושלים: מכון ון ליר, 2014).

58 ראו: יוסי מלמן, "קוד סגור: המדינה מקדמת חוק הגנת הסייבר על רקע התגברות התקיפות", **אתר מעריב**, 6 בפברואר 2016, http://www.maariv.co.il/journalists/Article-524985.

59 Andy Greenberg, "Congress Slips CISA into a Budget Bill that's Sure to Pass", Wired.com, December 16, 2015, http://www.wired.com/2015/12/congress-slips-cisa-into-omnibus-bill-thats-sure-to-pass/; Tim Greene, "CISA Legislation would Fit Liability for Businesses Sharing Cyber Threat Information", networkworld.com, October 28, 2015, http://www.networkworld.com/article/2998815/security/cisa-legislation-would-lift-liability-for-businesses-sharing-cyber-threat-information.html

בינה מלאכותית בתחום אבטחת הסייבר

נאדין וירקוטיס והדס קליין

תחום ביטחון הסייבר יכול לצאת נשכר משמעותית משימושים בבינה מלאכותית (AI). טכניקות בינה מלאכותית יכולות לשפר את ביצועי האבטחה הכוללים במקומות שבהם מערכות אבטחה קונבנציונליות עלולות להיות איטיות ובלתי מספקות, ובכך לספק הגנה טובה יותר מפני המספר העולה של איומי סייבר מתוחכמים. לצד ההזדמנויות הרבות שניתן למצוא בשימוש בבינה מלאכותית לאבטחת סייבר, עולים גם סיכונים וחששות. כדי לחזק את בשלותה ומוכנותה של אבטחת הסייבר, יש צורך במבט כולל על סביבת הסייבר של הארגון, מבט שישלב בינה מלאכותית עם תובנות אנושיות, שכן רק בני אדם או רק בינה מלאכותית אינם מספיקים להשגת הצלחה מלאה בתחום זה. שימוש אחראי בטכניקות של בינה מלאכותית הינו חיוני כדי להמשיך ולמתן את הסיכונים והחששות הנלווים לטכנולוגיה זו.

מילות מפתח: אבטחת סייבר, בינה מלאכותית (AI), מודיעין ביטחון, גישת אבטחה משולבת (ISA), שרשרת התקיפה בסייבר

מבוא

מאז שפורסמה מתקפת מניעת השירות (denial-of-service) הראשונה ב־1988,[1] הכמות, התחכום וההשפעה של מתקפות הסייבר עלו במידה ניכרת. ככל שמתקפות הסייבר הפכו לממוקדות וחזקות יותר, כך השתכללו אמצעי ההגנה. כלי האבטחה הראשון אמנם הוגבל לאיתור חתימות של וירוסים ולמניעת הפעלתם, אך כיום אנו עדים לפתרונות שתוכננו להעניק הגנה מקיפה נגד טווח רחב של סוגי מתקפות ולמגוון מערכות המהוות יעד למתקפה. יחד עם זאת, ההגנה על נכסי מידע בעולם הווירטואלי עדיין מהווה אתגר הולך וגדל.

נאדין וירקוטיס, דוקטורנטית במכון האוניברסיטאי למדעים וטכנולוגיה של אוקינאווה ומתמחה לשעבר בתכנית ביטחון סייבר של המכון למחקרי בטחון לאומי. הדס קליין, מנהלת תכנית בטחון סייבר במכון למחקרי בטחון לאומי.

כדי ליישם הגנה רציפה וחסונה, על מערכות האבטחה לדעת להתאים עצמן ללא הרף לסביבה, לאיומים ולגורמים המעורבים בשדה הסייבר, המשתנים בהתמדה. למעשה, המציאות בתחום אבטחת הסייבר שונה במקצת מהרצוי: גישות האבטחה מותאמות בדרך כלל לאיומים ידועים, וקשיחות והיעדר גמישות גורמים לכך שמערכות אבטחה מתקשות להסתגל באופן אוטומטי לשינויים החלים בסביבתן. גם כשקיימת אינטראקציה אנושית, תהליכי ההסתגלות צפויים להיות איטיים ובלתי מספקים.[2]

מאפייני הטכניקות של בינה מלאכותית, כמו גמישות, יכולת הסתגלות והתנהגות מערכת עמידה, יכולים לסייע בהתגברות על חסרונות שונים הקיימים בכלי אבטחת הסייבר של ימינו.[3] עם זאת, ולמרות שבינה מלאכותית כבר שיפרה במידה ניכרת את אבטחת הסייבר,[4] היא מעוררת חששות, ויש מי שרואים בה אפילו סיכון קיומי לאנושות.[5] בהתאם לכך, מדענים ומומחי משפט הביעו את חששם מהתפקיד ההולך וגדל של ישויות בינה מלאכותית אוטונומיות במרחב הסייבר, והעלו ספק אם השימוש בהן מוצדק מבחינה אתית.[6]

מטרת מאמר זה היא להתמקד בחסרונות של אמצעי האבטחה המסורתיים בתחום הסייבר ולהדגיש את ההתקדמות שנעשתה עד היום ביישום טכניקות של בינה מלאכותית באבטחת באותם אזורים. בנוסף, המאמר מסכם את הסיכונים והחששות הנלווים להתפתחויות בתחום הבינה המלאכותית, וזאת באמצעות בחינת הסטטוס הנוכחי, התייחסות לבעיות הקיימות והצבעה על כיווני התפתחות לעתיד.

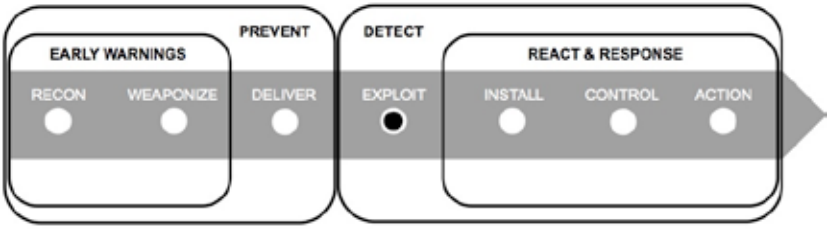
אתגרים באבטחת הסייבר

למרות הגברת המודעות לאיומי הסייבר והשקעת סכומים גדולים של כסף ומאמצים כבירים כדי להילחם בפשעי סייבר, היכולת של ארגונים לספק הגנה נאותה לנכסים הווירטואליים שלהם הינה עדיין סוגיה פתוחה.[7] הגורמים המעורבים במרחב הסייבר נעים מיחידים וארגונים פרטיים, דרך גורמים לא מדינתיים ועד ארגונים ממשלתיים. אלה מבקשים להגן על נכסי הסייבר שלהם, לתקוף נכסי סייבר של אחרים, או לעשות את שני הדברים גם יחד. המקורות לאיומי הסייבר הם מגוונים ונובעים מפעולות זדוניות פוטנציאליות העשויות לבוא מסיבות פיננסיות, פוליטיות או צבאיות, ואפילו מסוגים מסוימים של תחביבים.[8]

למרות ההטרוגניות והדינמיות של מרחב הסייבר, ניתן לאתר קווי דמיון מסוימים של מתקפות סייבר ושל אמצעי־נגד להן, כדי שאפשר יהיה לבנות מסגרת אבטחה מקיפה והוליסטית לתחום זה. מרבית מתקפות הסייבר מתאפיינות בשלבי מתקפה, אותם ניתן לתאר כ"שרשרת התקיפה בסייבר" (cyber kill chain).[9] מסגרת האבטחה מניחה שכל רצף של מתקפות מתחיל בשלב איסוף המידע, שבו

התוקף מנסה לאתר פרצות ופגיעויות ביעד המותקף (מערכת מטרה). השלב הבא במתקפה הוא התחמשות (weaponizing), שבו נקודות התורפה שהתגלו משמשות לפיתוח קוד זדוני ממוקד מטרה. לאחר מכן מגיע שלב החדירה (delivery), שבו התוכנה הזדונית מוחדרת למטרה הפוטנציאלית. לאחר שהתוכנה הזדונית הוחדרה בהצלחה, מגיע שלב הביצוע, שבו אותה תוכנה זדונית מפעילה את ההתקנה של הקוד הפולש. כתוצאה מכך, ניתן להתקין במערכת המארחת שנחשפה ערוץ פיקוד ושליטה, המאפשר לתוקף ליזום דרכו פעולות זדוניות. אמצעי־הנגד ייגזרו מהמקום שבו התגלתה הפעולה הזדונית בשרשרת התקיפה בסייבר.

גישת האבטחה המשולבת[10] (ISA) מציעה רעיונות מרכזיים ומסגרת כוללת לטיפול בהגנת סייבר. המטרה המרכזית של גישה זאת היא להפיק התרעות או אזעקות, רצוי לפני שהמתקפה משוגרת (לפני שלב הביצוע). ההתרעה אמורה לחולל הודעת אזהרה שתדע לתרגם את הנתונים החדשים שנאספו על האיום למשימות יישומיות. ההודעה גם אמורה לתמוך בבחירת אמצעי־הנגד, או לכלול בתוכה אמצעי־נגד ייעודיים שימנעו מהארגון ליפול קורבן למתקפה. אם לא ניתן למנוע מראש את המתקפה, יש לנסות לאתר את היקפה ולאחר מכן להגיב בהתאם. אמצעי־הנגד צריכים לכלול פעולות לעצירת הפורץ או אף לביצוע מתקפת־נגד עליו, וזאת בנוסף להגדרת נוהלי שיקום שיאפשרו שחזור מהיר של המערכת והשבתה למצבה הקודם.



תרשים 1. השלבים בשרשרת תקיפה בסייבר מול אמצעי־הנגד במסגרת גישת האבטחה המשולבת

תרשים 1 מתאר את הקשר ההדדי המתקיים בין מתקפת סייבר על פי שרשרת התקיפה בסייבר ובין אמצעי־הנגד המופעלים על פי גישת האבטחה המשולבת. התרשים מפרט את שרשרת התקיפה בסייבר, כפי שהיא מומחשת על ידי החץ האפור, ואת גישת האבטחה המשולבת, המומחשת על ידי המסגרות.

שרשרת התקיפה בסייבר כוללת את שבעת השלבים של מתקפת הסייבר כמפורט בתרשים, ואילו גישת האבטחה המשולבת מורכבת מארבעה שלבי פעולת־נגד. כדי לזהות ולחסום מתקפות מוקדם ככל האפשר, יש לקחת בחשבון

במסגרת גישת האבטחה המשולבת הכוללת את כל שלבי מתקפת הסייבר בשרשרת התקיפה.[11] כאמור, הדגש מושם על מניעת מתקפה ואיתור פעילויות זדוניות במהלך שלושת השלבים הראשונים של הפריצה, המוצגים בתרשים – איסוף המידע (recon), ההתחמשות (weaponize) והחדירה (deliver). לאחר המתקפה המתוארת בתרשים כשלב הביצוע (exploit), יש להפעיל את אמצעי גישת האבטחה המשולבת כדי לשבש את פעילות התוכנה הזדונית. המדובר בזיהוי (detection), תגובה (reaction) ומענה (response).

טיבו המורכב והדינמי של מרחב הסייבר מוביל למגוון אסטרטגיות ואתגרים טכנולוגיים שמעכבים ומסבכים את יכולת הארגון להגן על עצמו בצורה מספקת בסביבה הווירטואלית. אתגרים אלה כוללים את הצורך בהשגת נתונים, סוגיות הקשורות בטכנולוגיה, וכן פגמים ופערים ברגולציה ובניהול תהליכים.

אתגרים באיסוף מודיעין סייבר

העובדה שהתוקפים מותירים אחריהם עקבות לאחר הניסיון לתקוף מערכת מסוימת היא המפתח המאפשר להכיר אותם טוב יותר. על רקע זה, גישת האבטחה המשולבת והכוללת מחייבת איסוף וניתוח של מידע רב כדי להפיק ממנו מודיעין סייבר.[12] יחד עם זאת, ישנם אתגרים הניצבים בפני השגת נתונים רלוונטיים, כמו גם עיבודם, ניתוחם ושימוש בהם. לפיכך, המאמצים הקשורים למניעה, לזיהוי ולתגובה יעילים לפריצות זדוניות נעזרים כיום תדיר בכלי אבטחה שמבקשים להכניס אוטומציה בתהליכי האבטחה.

האתגרים המרכזיים הניצבים בפני השגת נתונים רלוונטיים הם:[13]

- **כמות הנתונים**: כמות הנתונים עלתה באופו מעריכי (exponential) מאז שהתקנים אלקטרוניים והשימוש בהם הפכו לחלק בלתי נפרד מהעבודה ומחיי היומיום. כדי ליישם גישת אבטחה משולבת, יש לתת את הדעת לכל הנתונים מכל המערכות ובכל הארגונים.
- **הטרוגניות של נתונים ומקורותיהם**: השונות בנתונים ובמקורותיהם מקשה על זיהוים ואיסופם. יתרה מכך, הנתונים והמקורות חוצים גבולות ארגוניים, גאוגרפיים ותרבותיים. גם אם זוהתה ההטרוגניות הרלוונטית של סביבת הסייבר, הטופולוגיה וההתנהגות של מערכות ורשתות עשויות להשתנות, ולפיכך לחייב התאמה מתמדת.
- **מהירות נתונים גבוהה**: הקצב הגבוה שבו מופקים ומעובדים נתונים מציב אתגרים בתחומי האחסון והעיבוד שלהם. נתונים אלה חיוניים להמשך הניתוח.

כאשר מדובר בעיבוד, ניתוח ושימוש בנתונים שהושגו, מערכות מניעה ואיתור של פריצות (IDPS) הן כלי רב ערך באבטחת סייבר – אחד מרבים בארסנל אבטחת הסייבר כיום.[14] מערכת IDPS יכולה להיות חומרה או תוכנה, שהוגדרה כמיועדת

להגן על מערכות בודדות או על רשתות שלמות. מערכת זו מבוססת על שני עקרונות מרכזיים: זיהוי שימוש חריג (misuse detection), שמזהה פעילות זדונית באמצעות הגדרת דפוסי התנהגות חריגה של מערכת ו/או רשת; איתור אנומליות (anomaly detection), שמתבסס על הגדרת דפוסים של התנהגות נורמלית במערכת ו/או רשת. מומחי אבטחה מגדירים שני דפוסים אלה תוך הסתמכות בעיקר על ניסיונם וכן על ידע קיים בדבר איומי סייבר.[15]

לבטחון סייבר יש אופי מורכב ודינמי במיוחד. איומים חדשים מופיעים חדשות לבקרים, ומתקפות נתפרות באופן ספציפי, כך שיערימו על תרחישי הגנה מוכרים. אמנם, המאפיינים של מערכת IDSP הם ביצועים מיטביים, הגנה מרבית ומספר מזערי של שגיאות,[16] אך מערכות האבטחה המסורתיות אינן מסוגלות עוד למלא דרישות אלו במלואן. להלן נקודות התורפה הטכנולוגיות הקריטיות ביותר של מערכת IDSP:[17]

- **שיעור זיהוי נמוך**: כל אי־דיוק בהגדרת דפוסים של נורמליות או חריגות בהתנהגות הרשת ו/או המערכת עלולים להשפיע על שיעור הזיהוי של מערכת IDPS. סביבת הרשת המשתנה תדיר הופכת משימה זו למאתגרת אף יותר. שגיאות בהגדרת דפוסים חריגים יכולות להוביל לשיעורים גבוהים של תוצאה שלילית שגויה (false negative). במקרה כזה, פעילות הרשת לא תזוהה מראש כניסיון תקיפה, משום שההנחה תהיה שאין מדובר בהתנהגות רשת זדונית. מנגד, הגדרה שגויה של דפוסים נורמליים תוכל לגרום לשיעורים גבוהים של תוצאה חיובית שגויה (false positive), ולהביא לכך שפעילות רשת שאינה זדונית תסווג ככזו בטעות.
- **קצב העברה איטי**: מערכות IDPS יכולות לסבול ממגבלות בעיבוד וניתוח ג'יגה־ביתים של נתונים לכל שנייה. מנגנונים שמתייחסים לסוגיה זו מתבססים בעיקר על התפלגות של עיבוד הנתונים, וכך הם יכולים להשפיע עוד יותר על פעולת המערכת, על תחזוקתה ועל העלויות הנלוות.
- **היעדר מדרגיות וחוסן**: סביבות סייבר הן דינמיות. התשתיות והתנועה ברשת משתנות ומתרחבות ללא הרף, וכמויות עצומות של נתונים הטרוגניים זקוקים לעיבוד וניתוח. דינמיקות כאלו תורמות לבעיות בתחום הביצוע ואף לאובדן יעילות, שכן מערכות IDPS לא תמיד מסוגלות לספק ולממש את הפונקציונליות שלהן כאשר הן מתמודדות עם דינמיקות מסוג זה.
- **היעדר אוטומציה**: מערכות IDPS אינן מסוגלות לפי שעה להסתגל אוטומטית לשינויים בסביבה. התוצאה יכולה להיות צורך בניתוח נתוני יומן על בסיס פרטני, התאמה ידנית של מערכות לשינויים בסביבת רשת, או מומחים שיקבעו מה התגובה המתאימה לכל הודעת אזהרה בנפרד. היעדר אוטומציה מביא לצורך מתמיד בפיקוח אנושי, גורם לעיכובים וכן מוסיף תקורות בעלויות ובמשאבים.

אתגרי הטכנולוגיה גורמים לארגונים להיתקל בשלב מסוים בליקויים באבטחה. ייתכן שאותם ארגונים ישתמשו אז בכמה מערכות אבטחה, או ירכשו מודיעין אבטחה בצורה של ייעוץ על ידי ספקים חיצוניים.[18]

אתגרים נוספים

מלבד הצורך בהשגת נתונים כוללת ובשימוש בטכנולוגיות אבטחה מוצקות להגנה קבועה על כל טווח המידע, יש לשקול גם את הצורך בתהליכים תומכים. הקמה ותחזוקה של תהליכים תומכים הן חשובות בדיוק כמו השגת הנתונים והשימוש בטכנולוגיות אבטחה הולמות. תהליכים פנים־ארגוניים ובין־ארגוניים יכולים לסייע לשפר ולשמר את גישת האבטחה המשולבת בארגונים, וזאת בנוסף לשיפור רמת המוכנות של אבטחת הסייבר שלהם.[19] זאת ועוד, יצירת מה שמכונה "סביבת הסייבר העסקית"[20] מעודדת שותפויות בין גורמים מגוונים לכל אורך סביבת הסייבר, במטרה לטפל ולשתף באיומים ביטחוניים, בניסיון שנרכש ובמשאבים.

ארגונים המגיעים מענפים שונים צפויים להציג דרישות שונות לאבטחת סייבר. הבדלים אלה יכולים להיות תוצאה של דרישות אבטחה הטרוגניות או של תגובות משתנות לנוכח מתקפות סייבר דומות.[21] כאשר ארגונים צריכים להגן על תשתיות קריטיות, כמו מתקני אספקת מים או מתקני חשמל גרעיניים, הם יתמקדו באבטחה מוגברת במקום בהיבטים הכלכליים. ארגונים פרטיים נוטים להתמקד בהפסדים הכספיים ולא לייחס חשיבות רבה מדי לסכנה לביטחון הציבור.[22]

אלה רק מקצת האתגרים שמטרידים ארגונים בבואם לגבש את אסטרטגיית האבטחה שלהם. לנוכח התפקיד החשוב שממלאות מערכות בטחון הסייבר בהקשר זה, נתמקד להלן באמצעים הטכנולוגיים.

טכניקות מודיעין לסיוע לאמצעי אבטחה

מכונות חכמות הן פתרון המבטיח שיפור אמצעי האבטחה העכשוויים במסגרת ההתמודדות עם סוגיות של איסוף מודיעין לאבטחת סייבר. מכונות חכמות יכולות לבצע כמה מהיכולות הקוגניטיביות האנושיות (כמו ללמוד או לנמק) וכן לכלול פונקציות חישה (יכולת לשמוע או לראות). מכונות כאלו מפגינות את מה שאנו מכנים אינטליגנציה[23] או בינה. בינה מלאכותית כזו מאפשרת למכונות להתנהג בתבונה ולחקות בינה אנושית – אם כי במידה מוגבלת.

התפתחות מערכות הבינה, בין אם בחומרה ובין אם בתוכנה, אפשרה לפתח שיטות לפתרון בעיות מורכבות, כמו סיווג או הקבצה (clustering), שלא ניתן היה לפתור מבלי לעשות שימוש בסוג כלשהו של אינטליגנציה.[24] לעומת מערכות מחשב מסורתיות, המבוססות על אלגוריתמים[25] קבועים ומחייבות תבניות נתונים ידועות מראש לקבלת החלטות, מומחים בתחום הבינה המלאכותית במדעי המחשב

פיתחו טכניקות שונות וגמישות, כגון רשתות עצבים מלאכותיות או רשתות עצבים עמוקות, שמאפשרות למחשבים ללמוד[26] ולהתאים את עצמם אוטומטית לדינמיקות של הסביבה. במרחב הסייבר, אימוץ אוטומציה יכול לכלול תבניות נתונים הטרוגניים, מקורות נתונים משתנים, או "רעש"[27] בפעילויות הסייבר.

אבטחת סייבר היא לכאורה התחום שיכול להשיג את הרווח הגדול ביותר מהכנסה לשימוש של הבינה המלאכותית הממוחשבת. מערכות בינה מלאכותית אוטונומיות אמורות להתגבר על האתגרים הניצבים בפני מערכות אבטחה קונבנציונליות.[28] התוצאה הצפויה משימוש בבינה מלאכותית היא מיתון בעיות הקשורות להשגת נתונים (כמות, הטרוגניות ומהירות הנתונים), וכן מיתון בעיות בכלים הקשורים לכך (שיעור זיהוי נמוך, קצב העברה איטי, היעדר מדרגיות וחוסן והיעדר אוטומציה). כך ניתן יהיה לשפר את היעילות והאפקטיביות של אבטחת הסייבר ושל הכלים הנלווים אליה.

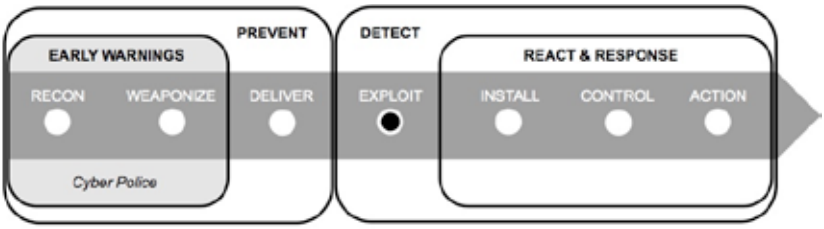
תחום הבינה המלאכותית פיתח ועדיין מפתח מספר רב של טכניקות שיתנו מענה להתנהגות מערכות חכמות. טכניקות רבות כאלו כבר הותקנו במערכות לאבטחת סייבר. אותן מערכות יכולות לעבד ולנתח מידע בהיקפים עצומים בתוך פרק זמן סביר, ובמקרה של ניסיון למתקפה הן יכולות לנתח את המידע ולבחור פעולות־נגד ייעודיות. ישנם תרחישים אפשריים שונים ליישום טכניקות של בינה מלאכותית לצורכי אבטחה, וזאת בארבע הקטגוריות של גישת האבטחה המשולבת. באמצעות אותם תרחישים ניתן להמחיש את מגוון האפשרויות שמציעים ענפי הבינה המלאכותית השונים.

"סוכני משטרה" חכמים ואינטראקטיביים לניטור רשתות שלמות

הפרדיגמה של "סוכנים חכמים" (intelligent agents) היא ענף של בינה מלאכותית שצמח מתוך הרעיון לפיו ידע בכלל, וידע לפתרון בעיות בפרט, אמור להיות משותף לישויות שונות. "סוכן יחיד" הוא ישות קוגניטיבית אוטונומית[29] עם מערכת קבלת החלטות משלה ויעד אישי. כדי להשיג את היעד שלו, הסוכן היחיד פועל בצורה פרו־אקטיבית במסגרת סביבתו ומול סוכנים אחרים. לסוכנים היחידים יש גם התנהגות ריאקטיבית: הם מבינים שינויים בסביבתם ומגיבים עליהם, וכן יוצרים אינטראקציה עם הסביבה ועם סוכנים מבוזרים אחרים. בחלוף הזמן, הסוכנים מתאימים עצמם לשינויים הדינמיים בסביבתם על פי הניסיון שצברו.[30]

עקב טבעם המבוזר והאינטראקטיבי, "סוכנים חכמים" נועדו לאסוף מידע על רשתות שלמות והמערכות ההיקפיות. נדמה כי מאפיין זה שימש לא רק כאמצעי הגנה, אלא גם לצורך איסוף מידע וביצוע פריצות (ראו לעיל שרשרת התקיפה בסייבר) במערכות המהוות יעד פוטנציאלי למתקפה.[31] מכיוון שההתנהגות של כל

סוכן מתעצבת על פי ניסיונו בתוך סביבתו האישית, לא פשוט להגן מפני איומים פרטניים מסוג זה.



תרשים 2. "סוכנים חכמים" של משטרת הסייבר המפיקים התרעה מוקדמת על פי גישת האבטחה המשולבת

דרך מוצלחת להשתמש בסוכנים נגד מתקפות סייבר מבוזרות היא באמצעות בניית "משטרת סייבר" של "סוכנים חכמים". גישה כזו מתבססת על הרעיון של "סוכני משטרה" מלאכותיים בסביבת סייבר מוגדרת, שמטרתם היא לזהות פעילות זדונית הנעשית בדרך מבוזרת.[32] כפי שהומחש בתרשים 2 לעיל, "סוכני משטרה" כאלה יכולים לסייע בהגנה כבר בשלבים הראשונים של מתקפת הסייבר.

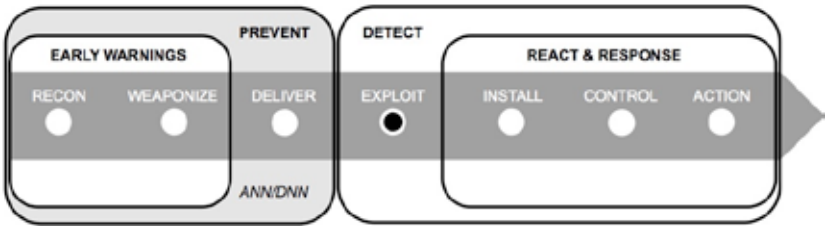
נוכחות של "סוכנים חכמים" ניתן למצוא גם במערכות חיסון מלאכותיות (AIS). שימוש בשני סוגים שונים של סוכנים – "סוכן זיהוי" ו"סוכן מתקפת־נגד" – מאפשר לחקות את המאפיינים היעילים של מערכת החיסון האנושית. סוכני הזיהוי מנטרים את סביבות הסייבר ומנסים לאתר פעילות חריגה. כאשר סוכנים אלה מזהים פעילות זדונית, הם שולחים בצורה יזומה הוראות מבוזרות לסוכני מתקפת־הנגד, שמופעלים כדי למנוע, למתן או אפילו להדוף את הפולשים לרשת.[33]

רשתות עצבים מלאכותיות למניעת פריצות זדוניות

טכניקה נוספת שצמחה מהתחום של בינה מלאכותית היא רשת העצבים המלאכותית (ANN). רשתות עצבים מלאכותיות הן מודלים של למידה סטטיסטית, המחקים את המבנה והתפקוד של המוח האנושי. הן יכולות לסייע בלמידה ובפתרון בעיות, במיוחד בסביבות שבהן האלגוריתמים או הכללים לפתרון הבעיה קשים לניסוח או לא ידועים. מכיוון שהתנהגות מערכת של רשת עצבים מלאכותית הינה חמקמקה וקשה להגדרה, מערכות כאלו נחשבות ל"קופסה שחורה" בלתי מוגדרת.[34]

רשתות עצבים מלאכותיות שימשו בהצלחה בכל השלבים של גישת האבטחה המשולבת לאבטחת סייבר, והן יכולות להכיל גם את כל השלבים של שרשרת התקיפה בסייבר. רשת עצבים מלאכותית המשולבת באבטחת סייבר יכולה

לשמש לניטור התנועה ברשת. כפי שמתואר בתרשים 3 להלן, ניתן לזהות פריצות זדוניות כבר בשלב החדירה ולפני שההתקפה עצמה יוצאת לפועל.[35] זוהי אחת המטרות שאבטחת הסייבר שואפת אליה, שכן היכולת למנוע מתקפות סייבר עוד קודם להתרחשותן היא הישג משמעותי שעשוי לקדם את הרעיון המרכזי של הגנה היקפית.[36] רשתות עצבים מלאכותיות גם יכולות לשמש בהצלחה ללמידה מפעילויות וממתקפות שהרשת עברה, כדי למנוע התממשות של מתקפות עתידיות.



תרשים 3. רשתות עצבים מלאכותיות למניעת מתקפות במסגרת גישת האבטחה המשולבת

היתרון הגדול של שימוש ברשת עצבים מלאכותית, בהשוואה לטכניקות קונבנציונליות המשמשות להגנת סייבר, הוא יכולת הלמידה שלה. כאמור, המצב הרגיל הוא שדפוסים המתארים פעילויות רשת נורמליות וחריגות כאחת מוגדרים באופן ידני על ידי מומחי אבטחה, בהתבסס על הידע המקצועי שלהם. ניתן לאמן את רשתות העצבים המלאכותיות כך שיזהו דפוסים כאלה באופן אוטומטי, באמצעות נתוני עבר שהועברו ברשת.

גישת IDPS המתבססת על אנומליות הוכיחה כי ניתן להשתמש בהצלחה ברשת עצבים מלאכותית להערכת מידע כותרת של חבילות נתונים ברשת,[37] וזאת במטרה ללמוד דפוסים של התנהגות רשת נורמלית.[38] בשלב ההכנה הראשון, רשת העצבים המלאכותית מאומנת לזהות ולהכיר דפוסים של תכונות כותרת השייכים לתנועת רשת נורמלית. משלב זה והלאה, כל חבילת נתונים עתידית העוברת ברשת המנוטרת מושווית לדפוסים שנלמדו. כאשר תכונות של כותרות חבילת נתונים תואמות לדפוס הרגיל, הן מועברות כרגיל. חריגות במידע של כותרת חבילת הנתונים, באופן שלא מתאים לדפוס שנלמד, יסווגו על ידי IDPS כאירוע זדוני ויידחו. נמצא כי גישה ייעודית זו משיגה שיפור בשיעור הזיהוי הכולל של ניסיונות פריצה, מבלי להפיק התרעות על תוצאות חיוביות שגויות או תוצאות שליליות שגויות. יתר על כן, בעוד שמערכות IDPS מסורתיות, המבוססות על חתימה או על אנומליות, פועלות בעיקר נגד פריצות מוכרות, גישת מערכת העצבים המלאכותית

מגינה בהצלחה מפני מקרים של פריצות שאינן מוכרות עדיין. בסיכומו של דבר, רשתות עצבים מלאכותיות אמורות לתמוך באופן מעשי בבניית מערכת IDPS איתנה, מסתגלת ומדויקת.[39]

ניטור רשתות עצבים מלאכותיות אינו מוגבל לשימוש במערכות IDPS. ניתן לעשותו באמצעות כל מערכת שמנטרת פעילויות רשת. גם "חומות אש", מערכות לזיהוי פריצה או "מרכזיות רשת" עושות שימוש ברשתות עצבים מלאכותיות כדי לסרוק תנועה נכנסת ויוצאת ברשת. סימולציה ניסיונית המבוססת על רשת עצבים מלאכותית הראתה שגם מאמץ מחשובי קטן למדי יכול לזהות מראש תשעים אחוזים מתוכנת ריגול.[40]

רשתות עצבים עמוקות (DNN), שהן צורה מפורטת, ממוחשבת ויקרה יותר של רשתות עצבים מלאכותיות,[41] שימשו לאחרונה לא רק כדי להגן על ארגונים מפני מתקפות סייבר, אלא גם כדי לנבא מתקפות כאלו. השיפורים בחומרה הובילו להתקדמות בעיבוד נתונים במסגרת תשתיות רשת ולשיפור קיבולת אחסון, כך שטכנולוגיות רשתות עצבים עמוקות הפכו לנפוצות ולישימות יותר. פלטפורמת אבטחה ייעודית המבוססת על בינה מלאכותית, שעושה שימוש בגישה של רשת עצבים עמוקה, הוכיחה שהיא יכולה לנבא בהצלחה כ־85 אחוזים ממתקפות הסייבר.[42] בעוד שגישות מסורתיות של אבטחת סייבר עברו מזיהוי מתקפה למניעת מתקפה, טכניקות רשתות עצבים עמוקות יכולות אפוא להוביל לשלב חדש של אבטחת סייבר – חיזוי מתקפה.

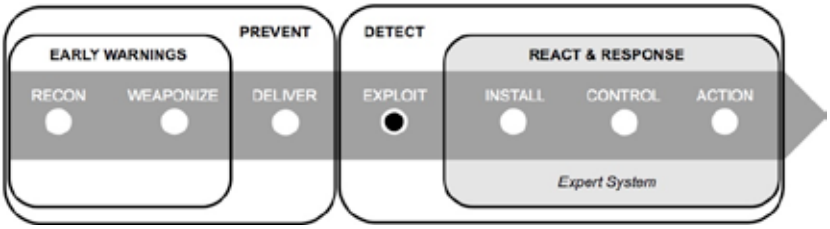
מערכות מומחות כספקיות תמיכה בהחלטות של מומחי אבטחה

מערכות מומחות (Expert systems) הן תוכניות מחשב שנועדו לספק תמיכה בקבלת החלטות סביב בעיות מורכבות בתחום מסוים, ועושות שימוש רחב מאוד ביישומי בינה מלאכותית. הרעיון של מערכות מומחות מורכב מבסיס ידע שמאחסן את הידע המומחה, וממנוע הסקת מסקנות המשמש להפקת תובנות לגבי ידע שהוגדר מראש וכן לאיתור תשובות לבעיות שעל סדר היום.[43]

מערכות מומחות מתייחסות לסוגים שונים של בעיות, וזאת בהתאם לאופן ההגעה לתובנות. גישה של גיבוש תובנות מבוססות־מקרים (case-based reasoning) מאפשרת פתרון בעיות באמצעות שחזור של מקרים דומים מהעבר, בהנחה שהפתרון של מקרה העבר יכול להיות מאומץ ומיושם גם על המקרה החדש. בהמשך נשקלות הצעות לפתרונות חדשים, ואם נדרש הן מעודכנות, וכך מביאות לשיפור מתמשך ברמת הדיוק וביכולת להתמודד עם בעיות חדשות לאורך זמן. מערכות מבוססות־כללים (rule-based systems) פותרות בעיות באמצעות כללים שהגדירו מומחים. הכללים מורכבים משני חלקים: תנאי ופעולה. הבעיות

מנותחות בשני שלבים: בשלב הראשון התנאי מוערך, ובשלב השני נקבעת הפעולה שיש לנקוט. שלא כמו במערכות מבוססות־מקרים, מערכות מבוססות־כללים אינן מסוגלות ללמוד כללים חדשים או לשנות אוטומטית כללים קיימים. עובדה זו קשורה ל"בעיית רכישת הידע", שהיא מכרעת לצורך התאמה לסביבות משתנות.[44]

מומחי אבטחה עושים שימוש נרחב במערכות מומחות לצורך תמיכה בהחלטות בסביבות סייבר. הערכת נתוני הביקורת של מערכות אבטחה יכולה לקבוע באופן כללי אם פעילות של רשת או מערכת היא זדונית או תקינה. הכמות העצומה של הנתונים גורמת לכך שמומחי אבטחה עושים שימוש קבוע בדוחות סטטיסטיים כדי לסרוק ולנתח את כל מידע הביקורת בתוך פרק זמן סביר. מערכות מומחות המבוססת על בינה מלאכותית הוכיחו בהצלחה שהן יכולות לתמוך במאמצים אלה באמצעות ניטור בזמן אמת של סביבות הסייבר, אפילו במספר מערכות רב או במערכות הטרוגניות.[45] במקרים שבהם מזוהה פריצה זדונית, מופקת הודעת התרעה. ההודעה מספקת מידע רלוונטי שמאפשר למומחי האבטחה לבחור את אמצעי האבטחה ביתר יעילות (react & respond – תגובה ומענה בתרשים 4 להלן). למרות כל הנאמר, חיוני לזכור כי אף שמערכות מומחות הצליחו לסייע למקבלי החלטות, הן אינן מסוגלות להחליף אותם.[46]



תרשים 4. מערכות מומחות לתמיכה באמצעי תגובה ומענה על פי גישת האבטחה המשולבת

חסרונות הבינה המלאכותית בעולם אבטחת הסייבר

עד עתה דנו ביתרונות הבינה המלאכותית וכן בטכניקות השונות שיכולות לתת מענה לסוגיות טכנולוגיות חשובות בתחום אבטחת הסייבר. למרות היבטים חיוביים אלה, קיימים חששות וסיכונים המתלווים לשימוש בבינה מלאכותית בתחום אבטחת הסייבר:

- **חוסר יכולת לשמר אוטונומיה באבטחת הסייבר**: אף שנרשמה התקדמות עצומה באימוץ טכניקות של בינה מלאכותית באבטחת הסייבר, מערכות אבטחת

הסייבר עדיין אינן אוטונומיות במלואן ולא יכולות להוות תחליף מוחלט לקבלת החלטות אנושית. לכן, יש עדיין משימות שמחייבות התערבות של בני אדם.[47]

- **פרטיות הנתונים**: טכניקות בינה מלאכותית, כמו רשתות עצבים מלאכותיות ועמוקות, הופכות למשוכללות יותר הודות להתקדמות בתחום החומרה. טכניקות חדשות כאלו צצות מדי יום. אולם לצורך הגובר בנתוני עתק (big data) יש גם צד שלילי כאשר הדברים מגיעים לפרטיות הנתונים: ניתוח כמויות עצומות של מידע עשוי לעורר בארגונים פרטיים וציבוריים גם יחד דאגה מפני פגיעה בפרטיות המידע האישי שהם מחזיקים, וחלקם אינם מוכנים על רקע זה לשתף את הנתונים שברשותם.[48] שאלות שיכולות להישאר ללא מענה עבור ארגונים שפרטיותם נפגעה הן: באילו נתונים אישיים נעשה שימוש? מדוע נעשה בהם שימוש? ואלו מסקנות מסיקים מהם במסגרת פתרונות מבוססי בינה מלאכותית?
- **היעדר רגולציה**: ישנם חששות משפטיים שונים בנוגע לבינה מלאכותית, אולם החשש הבולט ביותר הוא איבוד השליטה מצד בני האדם על ההשלכות הנובעות מבינה מלאכותית אוטונומית. טיבה הייחודי והקשה לחיזוי של הבינה המלאכותית גורם לכך שאין עדיין מסגרות משפטיות שיתנו מענה לתחום זה.[49]
- **חששות מתחום האתיקה**: מערכות אבטחה מבוססות בינה מלאכותית מבצעות יותר ויותר החלטות עבור אנשים ספציפיים או מסייעות להם להגיע להחלטות (למשל, במקרה שנדון לעיל בנוגע למערכות מומחות). לנוכח התפתחות זו, מדאיג במיוחד שאין עדיין קוד אתי למערכות כאלו. התוצאה היא שהחלטות שמתקבלות עבורנו באמצעות בינה מלאכותית אינן בהכרח החלטות שאנו היינו מקבלים כבני אדם.[50]

מסקנות

בינה מלאכותית נחשבת לאחת ההתפתחויות המבטיחות ביותר בעידן המידע, ונראה כי אבטחת סייבר הוא התחום שיכול להפיק מכך את המרב. אלגוריתמים, טכניקות, יוזמות וכלים חדשים המציעים שירותים המבוססים על בינה מלאכותית צצים ללא הרף בשוק האבטחה הגלובלי. בהשוואה לפתרונות אבטחת סייבר קונבנציונליים, מערכות מבוססות בינה מלאכותית אמורות להיות גמישות, מסתגלות ועמידות יותר, ובכך לסייע לשפר את ביצועי האבטחה ולספק הגנה טובה יותר למספר הולך וגובר של איומי סייבר מתוחכמים. נכון להיום, טכניקות של "למידה עמוקה" (deep learning) מסתמנות ככלים העוצמתיים והמבטיחים ביותר בתחום הבינה המלאכותית. רשתות עצבים עמוקות יכולות לחזות מתקפות סייבר מראש ולא רק למנוע אותן, וכך לפתוח שלב חדש באבטחת הסייבר.

במקביל להבטחה הגלומה בבינה מלאכותית, היא גם מתגלה כסיכון גלובלי לאנושות. לסיכונים ולחששות המתלווים לבינה המלאכותית יש על מה להתבסס.

ניתן לזהות במסגרתם ארבע בעיות מרכזיות: היעדר אוטונומיה מלאה של הבינה המלאכותית; חשש לפגיעה בפרטיות הנתונים; היעדר מסגרת משפטית מספקת לטיפול בסוגיה; חששות אתיים שמקורם בהיעדר קוד מוסרי למערכות קבלת החלטות אוטונומיות. עקב המהירות בה מתפתח תחום הבינה המלאכותית, חיוני לפתור סיכונים וחששות אלה מהר ככל האפשר, אך נוכח האפשרות הסבירה שפתרונות בני קיימא לא יימצאו במהרה, מומלץ לעשות בשלב זה שימוש מושכל בבינה מלאכותית במסגרת אבטחת סייבר. דבר זה יסייע לפחות למתֵן חלק מהסיכונים והחששות.

עד עתה לא נרשמה הצלחה גורפת בתחום הגנת הסייבר הנעשית על ידי בני אדם בלבד או על ידי בינה מלאכותית בלבד. למרות השיפורים הרבים שהבינה המלאכותית הכניסה לתחום זה, מערכות קשורות לא מסוגלות עדיין להתאים את עצמן באופן מלא ואוטומטי לשינויים בסביבתן, ללמוד את כל סוגי האיומים והמתקפות ולבחור וליישם באופן אוטומטי אמצעי־נגד ייעודיים שיגנו מפני מתקפות אלו. לכן, בשלב הטכנולוגי הנוכחי, כדי שניתן יהיה להגיע לבשלות באבטחת הסייבר, יש לשמור על התלות ההדדית החזקה בין בינה מלאכותית ובין הגורם האנושי, ויותר מכך, נדרש מבט כולל על סביבת הסייבר של ארגונים.

אבטחת סייבר אינה רק סוגיה טכנולוגית. היא נוגעת גם לרגולציה ולאופן שבו סיכוני אבטחה מטופלים. כדי להשיג ביצועי אבטחה אופטימליים, חיוני לשלב בין כל הפתרונות הטכניים, התהליכים הרלוונטיים ובני האדם, וכך להגיע למסגרת אחת של אבטחה משולבת. בסופו של דבר, הגורם האנושי הוא זה שקובע עדיין, ולא (רק) הטכנולוגיה.

הערות

1. סטודנט בוגר מדעי המחשב בשם Robert Tappen Morris כתב ב־1988 את תוכנת המחשב הראשונה שהופצה דרך האינטרנט: התולעת מוריס. התוכנה לא נועדה לגרום נזק אלא רק לאמוד את ממדי האינטרנט, אך שגיאה קריטית יצרה שינוי בתוכנה וגרמה לה לשגר את מתקפת מניעת השירות הראשונה.
2. בנוגע לחסרונות של מערכת מניעה ואיתור של פריצות (IDPS), ראו: Amjad Rehman and Tanzila Saba, "Evaluation of Artificial Intelligent Techniques to Secure Information in Enterprises", Artificial Intelligence Review 42, no. 4 (2014): 1029-1044, במיוחד הפרק "Performance Issues: IDS".
3. Selma Dilek, Hüseyin Çakır and Mustafa Aydın, "Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review", International Journal of Artificial Intelligence & Applications 6, no. 1 (2015): 21-39.
4. Enn Tyugu, "Artificial Intelligence in Cyber Defense", in Proceedings of 3rd International Conference on Cyber Conflict (ICCC), 7-10 June 2011, Tallinn Estonia, eds. C. Czosseck, E. Tyugu and T. Wingfield (Tallinn, Estonia: CCD COE, 2011), pp. 95-105; Xiao-bin Wang, Guang-yuan Yang, Yi-chao Li and Dan

Liu, "Review on the Application of Artificial Intelligence in Antivirus Detection System", Cybernetics and Intelligent Systems (2008): 506-509.

5. הקרן לאתגרים גלובליים מצביעה על בינה מלאכותית כאחד הסיכונים הגוברים שעלול לאיים על האנושות בעתיד. עוד בנושא זה ראו: Dennis Pamlin and Stuart Armstrong, "Global Challenges – Twelve risks that threaten human civilisation" (Global Challenges Foundation: 2015), http://globalchallenges.org/wp-content/uploads/12-Risks-with-infinite-impact.pdf.
6. Stuart Russell, Tom Dietterich, Eric Horvitz, Bart Selman, Francesca Rossi, Demis Hassabis, Shane Legg, Mustafa Suleyman, Dileep George and Scott Phoenix, "Research Priorities for Robust and Beneficial Artificial Intelligence: An Open Letter", AI Magazine 36, no. 4 (2015): 105-114.
7. "A History of Cybersecurity: How Cybersecurity Has Changed in the Last 5 Years", My Digital Shield, October 5, 2015, http://www.mydigitalshield.com/history-cyber-security-cyber-security-changed-last-5-years/.
8. Rehman and Saba, "Evaluation of Artificial Intelligent Techniques".
9. ישנן גישות שונות לתיאור השלבים השונים של מתקפת סייבר. מאמר זה מתייחס אל "שרשרת התקיפה בסייבר" (Cyber Kill Chain®), כפי שהוגדרה על ידי חברת "לוקהיד מרטין" ושימשה בהרחבה את קהילת הביטחון האמריקאית. עוד בנושא זה ראו: www.lockheedmartin.com.
10. Gabi Siboni, "An Integrated Security Approach: The Key to Cyber Defense", Georgetown Journal of International Affairs, May 7, 2015, http://journal.georgetown.edu/an-integrated-security-approach-the-key-to-cyber-defense/.
11. Tony Sager, "Killing Advanced Threats in Their Tracks: An Intelligent Approach to Attack Prevention", A SANS Analyst Whitepaper (2014), https://www.sans.org/reading-room/whitepapers/analyst/killing-advanced-threats-tracks-intelligent-approach-attack-prevention-35302.
12. המושג מודיעין סייבר הוא יותר מאשר נתונים גולמיים זמינים. הוא עוסק בהשגת מידע יישומי של נתונים ממוינים, מעובדים ומוערכים. עוד בנושא מודיעין על איומי סייבר וההגדרה של מודיעין סייבר ומידע סייבר, ראו: "What Is Cyber Threat Intelligence and Why Do I Need It?" iSIGHT Partners Inc. (2014), http://www.isightpartners.com/wp-content/uploads/2014/07/iSIGHT_Partners_What_Is_20-20_Clarity_Brief1.pdf.
13. Siboni, "An Integrated Security Approach".
14. Ahmed Patel, Mona Taghavi, Kaveh Bakhtiyari and Joaquim Celestino Junior, "An Intrusion Detection and Prevention System in Cloud Computing: A Systematic Review", Journal of Network and Computer Applications, 36, Issue 1, January 2013, pp. 25-41, http://dx.doi.org/10.1016/j.jnca.2012.08.007.
15. Susan M. Bridges and Rayford B. Vaughn, "Fuzzy Data Mining and Genetic Algorithms Applied to Intrusion Detection", 12th Annual Canadian Information Technology Security Symposium (2000): 109-122.
16. Patel and others, "An Intrusion Detection and Prevention System in Cloud Computing: A Systematic Review".
17. Rehman and Saba, "Evaluation of Artificial Intelligent Techniques".
18. Sager, "Killing Advanced Threats in Their Tracks: An Intelligent Approach to Attack Prevention".

19. המועצה הפדרלית לבדיקת מוסדות פיננסיים (FFIEC) פיתחה את הכלי להערכת אבטחת סייבר כדי שיסייע לארגונים לזהות סיכונים ולקבוע היערכות נכונה לאבטחה. רמת המוכנות מסייעת לארגונים לקבוע האם ההתנהגויות, הנהלים והתהליכים שלהם תומכים בצורה נאותה בהיערכותם לאבטחת סייבר. היא גם מזהה פעולות אפשרויות שיגבירו את יעילות ההיערכות. עוד בנושא זה, ראו: https://www.ffiec.gov/cyberassessmenttool.htm.
20. Abdul Wahab Amirudin, "Facing Cyberattacks in 2016 and Beyond", The Star, January 28, 2016, http://www.thestar.com.my/tech/tech-opinion/2016/01/28/facing-cyber-attacks-in-2016-and-beyond/.
21. Rehman and Saba, "Evaluation of Artificial Intelligent Techniques".
22. Linda Ondrej, Todd Vollmer and Milos Manic, "Neural Network Based Intrusion Detection System for Critical Infrastructures", 2009 International Joint Conference on Neural Networks (Atlanta, GA, 2009): 1827-1834.
23. Yoshua Bengio, "Learning Deep Architectures for AI", Foundations and Trends® in Machine Learning, 2, no. 1 (2009): 1-127.
24. Tyugu, "Artificial Intelligence in Cyber Defense".
25. לאלגוריתמים קבועים חיווט לוגי קשיח, ברמת קבלת החלטות, לטובת ניתוח נתונים. ראה שם.
26. Olin Hyde, "Machine Learning for Cybersecurity at Network Speed & Scale", an Invitation to Collaborate on the Use of Artificial Intelligence against Adaptive Adversaries, ai-one (2011), www.ai-one.com/.
27. "רעש" – מידע לא מדויק או לא רלוונטי בנתונים שנאספו.
28. "Cybersecurity and Artificial Intelligence: A Dangerous Mix", INFOSEC Institute, February 24, 2015, http://resources.infosecinstitute.com/cybersecurity-artificial-intelligence-dangerous-mix.
29. אפשר לפרש ישות סייבר קוגניטיבית כתוכנית יחידה, בין אם חומרה או תוכנה, שיש לה יכולות קוגניטיביות בדומה לאדם. בתחום הבינה המלאכותית, יכולות קוגניטיביות של "סוכן חכם" יכללו תפיסה של סביבת הסייבר, השגה וניתוח של נתונים שנאספו במרחב הסייבר, והסקת מסקנות מנתונים אלה.
30. Stan Franklin and Art Graesser, "Is It an Agent, or Just a Program? A Taxonomy for Autonomous Agents", Third International Workshop on Agent Theories, Architectures and Languages (London: Springer-Verlag, 1997): 21-35.
31. Alessandro Guarino, "Autonomous Intelligent Agents in Cyber Offence", in 5th International Conference on Cyber Conflict, eds. K. Podins, J. Stinissen and M. Maybaum (Tallinn, Estonia: NATO CCD COE, 2013): 377-388.
32. Tyugu, "Artificial Intelligence in Cyber Defense".
33. Xia Ye and Junshan Li, "A Security Architecture Based on Immune Agents for MANET", International Conference on Wireless Communication and Sensor Computing (2010): 1-5.
34. Christian Bitter, David A. Elizondo and Tim Watson, "Application of Artificial Neural Networks and Related Techniques to Intrusion Detection", World Congress on Computational Intelligence (2010): 949-954.
35. שם.
36. Tyugu, "Artificial Intelligence in Cyber Defense".

37. כותרת של חבילת נתונים מכילה תכונות כמו אורך נתונים שהועברו, סוג פרוטוקול הרשת או כתובות המקור והיעד של חבילת הנתונים. לכן, כותרת החבילה נושאת מידע שיכול לשמש כדי להבדיל בין התנהגות רשת רגילה ובין ניסיונות חדירה.
38. Ondrej and others, "Neural Network Based Intrusion Detection System".
39. Bitter and others, "Application of Artificial Neural Networks and Related Techniques to Intrusion Detection".
40. ההדמיות הניסיוניות של זיהוי תוכנת הריגול שמו דגש על זיהוי תולעים וספאם. עוד בנושא זה, ראו: Dima Stopel, Robert Moskovitch, Zvi Boger, Yuval Shahar and Yuval Elovici, "Using Artificial Neural Networks to Detect Unknown Computer Worms", Neural Computing and Applications, 18, no. 7 (2009): 663-674.
41. Geoffrey E. Hinton, Simon Osindero and Yee-Whye Teh, "A Fast Learning Algorithm for Deep Belief Nets", Neural Computation, 18, no. 7 (2006): 1527-1554.
42. Victor Thomson, "Cyber Attacks Could Be Predicted With Artificial Intelligence", iTechPost, April 21, 2016, www.itechpost.com/articles/17347/20160421/cyber-attacks-predicted-artificial-intelligence-help.htm.
43. Tyugu, "Artificial Intelligence in Cyber Defense".
44. Serena H. Chen, Anthony J. Jakeman and John P. Norton, "Artificial Intelligence Techniques: An Introduction to Their Use for Modelling Environmental Systems", Mathematics and Computers in Simulation, 78, no. 2-3 (2008): 379-400.
45. שם.
46. Debra Anderson, Thane Frivold and Alfonso Valdes, "Next-Generation Intrusion Detection Expert System (NIDES): A Summary", SRI International, Computer Science Laboratory, May 1995.
47. Katherine Noyes, "A.I. + Humans = Serious Cybersecurity", Computerworld, April 18, 2016, www.computerworld.com/article/3057590/security/ai-humans-serious-cybersecurity.html.
48. Tom Simonit, "Microsoft and Google Want to Let Artificial Intelligence Loose on Our Most Private Data", MIT Technology Review, April 19, 2016, https://www.technologyreview.com/s/601294/microsoft-and-google-want-to-let-artificial-intelligence-loose-on-our-most-private-data/.
49. Bernd Stahl, David Elizondo, Moira Carroll-Mayer, Yingqin Zheng and Kutoma Wakunuma, "Ethical and Legal Issues of the Use of Computational Intelligence Techniques in Computer Security and Computer Forensics", The 2010 International Joint Conference on Neural Networks (IJCNN) (2010): 1-8.
50. Nick Bostrom, "Ethical Issues in Advanced Artificial Intelligence", in Cognitive, Emotive and Ethical Aspects of Decision Making in Humans and in Artificial Intelligence, eds. Iva Smit and George E. Lasker (Windsor, ON: International Institute for Advanced Studies in Systems Research/Cybernetics, 2003), 2, pp. 12-17.

עד כמה ללחוץ על דוושת הגז – המרוץ לפיתוח מכונית אוטונומית בטוחה

אנדרו טאבאס

להופעת המכונית האוטונומית יש השלכות מרחיקות לכת בתחומים שונים, כמו הבעלות על הרכב, מערך התחבורה והבטיחות. כבר כיום יכולים האקרים להשתלט על מכונית אוטונומית דרך מערכות הניווט או הבידור שלה. חיבור מכוניות אוטונומיות לרשת יאפשר להשתלט עליהן במספרים גדולים. לפיכך, מקבלי ההחלטות חייבים לפעול כבר עתה כדי ליישם מנגנוני אבטחה טכניים ומשפטיים שימנעו מצב כזה. פתרונות אפשריים הם הקמה של מערכת אישורים, מאמץ ליצור "מרווח אוויר" בין רשתות המחשב השונות ברכב האוטונומי וחקיקת חוקי עונשין להאקרים. למרות הסיכונים הכרוכים במכונית האוטונומית, אל ליצרנים להירתע מפיתוחן. במקום זאת, עליהם להיות המובילים במרוץ לפיתוח טכנולוגיה שתתגבר על סיכונים אלה.

מילות מפתח: מכונית אוטונומית, מכונית ללא נהג, V2V, V2I, מערכות תחבורה חכמות, האינטרנט של הדברים, הצפנת מפתח ציבורי, אבטחת סייבר, האקר, מרווח אוויר

מבוא

בסיפור הקצר "סאלי" שכתב אייזק אסימוב ב־1953, הוא מתאר מכוניות "פוזיטרוניות" שנוסעות בעצמן. המכוניות גם מתקשרות ביניהן (ברשת של כלי רכב אוטונומיים), מגינות על עצמן (בתגובה לחששות אבטחה) והורגות (דבר הממחיש את הבעיות האתיות המתעוררות סביב רכבים אוטונומיים).[1] "סאלי" הוא נקודת פתיחה טובה לדיון במכוניות אוטונומיות (AV), מכיוון שהסיפור מצביע על סוגיות שחברות טכנולוגיות ויצרני רכב מתמודדים אתן כבר היום.

אנדרו טאבאס הוא בעל תואר ראשון ביחסי חוץ משעם אוניברסיטת ג'ורג'טאון, ואנליסט בקבוצת קדמוס.

רכב אוטונומי הוא בעל פגיעויות ייחודיות שמצריכות פתרונות אבטחה חדשניים. ראשית, מכונית אוטונומית תלויה בחיישנים לקבלת הקֶלט. חיישנים אלה יכולים לקבל קלט מוטעה וכך לסכן את ביטחון הרכב ונוסעיו; שנית, מכונית אוטונומית מקבלת מידע הנוגע למצבים של חיים ומוות – מערכות GPS, עדכוני חומרה קריטיים ותקשורת עם כלי רכב אחרים. מידע זה נובע ממערכת שנשענת על תשתית ענן, ויכולה לפיכך להיות חשופה להשתלטות של האקרים. יצרני מכוניות אוטונומיות אינם צריכים להירתע מאתגרים אלה, שכן המנצח במרוץ לפיתוח מכונית אוטונומית בטוחה ומוגנת יצליח להציל חיים ולשנות את העולם.

הטכנולוגיה

כדאי להבחין בין "מכונית אוטונומית" ובין "מכונית ללא נהג" (self-driving car). מכוניות אוטונומיות יכולות לנהוג לבד בתנאים מסוימים, אולם שומרות על יכולת הנהיגה האנושית. מכוניות אוטונומיות חייבות להציע "נסיגה חלקה" ממצב אוטונומי, דהיינו מעבר חלק לנהג האנושי.[2] פיתוח של מכוניות אוטונומיות מיטיב עם יצרני הרכב, משום שהוא מאפשר להם להתפאר ולפרסם כי כלי הרכב שהם מייצרים הינם בעלי טכנולוגיות מתוחכמות.

לעומת המכונית האוטונומית, מכוניות ללא נהג לא יאפשרו לבני אדם לנהוג בהן. הן גם ייראו שונות במובהק מהמכוניות של ימינו, בכך שיהיו נטולות הגה, דוושות ומראות. מכוניות ללא נהג אף יוכלו ליצור "צי של רכבים שיתופיים" שישים קץ לבעלות המסורתית על כלי רכב.[3] מכוניות ללא נהג יהוו איום על יצרני הרכב המסורתיים, ויביאו לכך שמכוניות משפחתיות יהפכו לפריט יוקרה. חברת "טסלה", המפתחת מכונית אוטונומית, כבר הציעה שבעלים של מכונית אוטונומית יוכלו להרוויח כסף באמצעות שילובה בצי של כלי רכב אוטונומיים כאשר היא לא תהיה בשימוש של בעליה. לדברי החברה, רעיון זה יסייע להוזיל את מחיר המכונית האוטונומית.[4]

מינהל בטיחות הדרכים האמריקאי (NHTSA) מציין חמש רמות של אוטומציה: "ללא אוטומציה" (0); "אוטומציה בפונקציה ייחודית" (1); "אוטומציה בפונקציות משולבות" (2); "אוטומציית נהיגה מוגבלת" (3); "אוטומציית נהיגה מלאה" (4). רמה גבוהה יותר פירושה יותר פונקציות של המכונית שאינן דורשות התערבות של נהג אנושי. רמה 0 מייצגת את המכונית המסורתית; ברמה 1 המכונית יכולה לבצע בעצמה כמה משימות ספציפיות; ברמה 2 היכולות האוטונומיות של הרכב מסוגלות להשתלב זו בזו, אולם הנהג עדיין חייב להיות פעיל. לדוגמה, מכונית ברמה 2 יכולה לשלב "בקרת שיוט מותאמת" עם "מרכוז נתיב"; כלי רכב ברמה 3 יכולים לנהוג בעצמם בסביבות מסוימות, אולם הנהג חייב להישאר ערני[5] (אם כי ייתכן שנהגים יתקשו להישאר מרוכזים כאשר המכונית האוטונומית עושה את מרבית

העבודה); ברמה 4 הנהג אינו צריך להישאר ערני ואף אינו צריך להישאר ברכב.[6] מכוניות ברמה 4, שהן למעשה מכוניות ללא נהג, אינן זקוקות כאמור להתקנת הגה, דוושות או שאר המרכיבים המוכרים לנו במכוניות כיום.

במכונית המסורתית, נהגים אנושיים הם הקישור בין הרכב לסביבתו: הם משגיחים על תמרורים ורמזורים, שמים לב לתנאי הדרך, נמנעים מלהתקרב לכלי רכב אחרים, מתקשרים עם נהגים אחרים ומנווטים את דרכם. כדי למלא פונקציות אלו, המכונית האוטונומית עושה שימוש בחיישנים, בתקשורת "רכב לרכב" (V2V) ובתקשורת "רכב לתשתית" (V2I). כמו האינטרנט של הדברים (IoT), גם המכונית האוטונומית מסתמכת על תשתית ענן.

"מערכות החישה" שמספקות את המידע למכונית האוטונומית, המתוארות על ידי אנדרסון ושותפיו, כוללות את המצלמות שאוספות נתונים על העולם שבחוץ[7] אך מוגבלות בשל תנאי מזג אוויר ויכולת התוכנה להמיר תמונות לנתונים,[8] וכן חיישנים – חיישני מכ"ם ולידאר, המפיקים אות ועוקבים אחר הזמן שלוקח לו לפגוע באובייקט ולחזור לחיישן כדי לקבוע את המרחק ממנו.[9] לשתי טכנולוגיות החיישנים יש מגבלות, משום שחלק מהמשטחים אינם מחזירים כהלכה גלי רדיו ואור.[10] חיישנים על־קוליים מזהים אובייקטים קרובים, ואילו חיישני אינפרא־אדום מזהים אובייקטים בלילה.[11] מכוניות אוטונומיות יכולות להשתמש גם במערכות GPS ובמערכות ניווט פנימיות (INS) לצורך השגת מידע על מיקומן.[12] מערכת INS נשענת על ג'ירוסקופים, מדי גובה ומדי תאוצה.[13] בנוסף, למכונית אוטונומית יש גישה למפות שכוללות מידע על רמזורים.[14] לדוגמה, חברת "גוגל" תכננה כלי רכב שאוספים מידע ובונים מפות וירטואליות של מאפייני הדרך תוך כדי הנסיעה.[15]

מכוניות אוטונומיות מתקשרות עם רשתות כלי רכב זמניות (VANET).[16] רשתות VANET "הן הבסיס למערכות תחבורה חכמות (ITS)".[17] טכנולוגיות של "רכב לתשתית" (V2I) משתפות בין המכוניות מידע על רמזורים ושאר גורמים חיצוניים ומסייעות לרכב האוטונומי להבין את העולם מסביבו. ניתן להשתמש בבלוּטוּת' כדי לשפר תקשורת V2I.[18] טכנולוגיות "רכב לרכב" (V2V) מאפשרות למכוניות לשתף ביניהן מידע בנוגע למיקום ולמהירות של כל אחת מהן, ובכך לצמצם את הסיכוי לתאונה. מכוניות אוטונומיות מתקשרות האחת עם השנייה באמצעות תקשורת ייעודית לטווח קצר (DSRC).[19] לאחרונה פרסם מבקר המדינה של ארצות הברית מחקר על היישום האפשרי של טכנולוגיות במכוניות עם נהגים אנושיים.[20]

מכונית אוטונומית מתבססת על "חישה־תכנון־פעולה".[21] המכונית מזהה מידע, מריצה אלגוריתמים כדי לקבוע את התגובה המיטבית ומוציאה לפועל את הפעולה הדרושה. מכונית אוטונומית היא דוגמה ל"מערכות עם שילוב מסיבי של מתמרים

חכמים" (MIST), אשר "עושות שימוש ברעיונות הענן כדי לקלוט מידע, לחוש את הסביבה ולהשתלב בצורה פעילה במצב במטרה להשיג את התוצאה הרצויה".[22]

מכוניות אוטונומיות מציבות אתגר ייחודי, משום שעליהן להבטיח את בטיחות הנוסעים בכל מחיר. לפיכך, על מהנדסי המכוניות האוטונומיות להבטיח כי החיישנים שבהן יהיו אפקטיביים בכל מצבי מזג אוויר ותנאי דרך. כמו כן, עליהם להגן על חיישנים אלה מפני התערבות חיצונית שעלולה לאיים הן על בטיחות הנוסעים ברכב האוטונומי והן על אלה שבכלי הרכב שסביבו. מסיבה זו, אבטחת הסייבר הופכת לגורם מרכזי בייצור מכוניות אוטונומיות.

לקראת רשת קולקטיבית של כלי רכב

תקשורת מסוג "רכב לרכב" (V2V) או "רכב לתשתית" (V2I) מאפשרת ליצור רשת קולקטיבית של כלי רכב. כדי ליצור מכונית יעילה, על בני האדם, המכוניות והתשתיות לדבר אלה עם אלה. המכוניות יִלמדו על תנאי מזג האוויר ומידע נוסף דרך תשתית הענן. בשלב הראשון הן ייאלצו להתמודד עם נהגים אנושיים, אולם בסופו של דבר הן יתקשרו אך ורק האחת עם השנייה. ברשת נטולת נהגים אנושיים יידרשו המתכנתים לקבוע שיטות להגדלת זרם התנועה. לפי Riener, עתיד המכונית האוטונומית הוא בצי שיתופי שבו הנוסע יוכל להזמין רכב לנסיעה, ולאחר מכן לשחרר אותו ולאפשר לו לחזור למיקום מרכזי ייעודי.[23]

בדומה לחיישנים, גם תקשורת "רכב לרכב" או "רכב לתשתית" מציבה אתגרים של אבטחת סייבר. תקשורת זדונית עלולה להסתיר סיכוני דרך או להמציא כאלה. סיכונים מומצאים מסוג זה יגרמו למכונית להתנהג באופן בלתי צפוי. האקרים משוכללים יותר עלולים לנצל את מערכת התקשורת של המכונית האוטונומית כדי לקבל דרכה גישה למחשב המרכזי שלה, וכך להשיג שליטה על ההיגוי והבלמים של הרכב. לכן, חיוני לאבטח את כל מסרי התקשורת ששולחת המכונית האוטונומית.

מגמות עכשוויות בתעשייה

המרוץ לפיתוח מכונית אוטונומית בטוחה משותף הן ליצרני הרכב המסורתיים והן לחברות טכנולוגיה, ובהן "פולקסווגן", "מרצדס בנץ", "טסלה", "בוש", "אובר", "לוקהיד מרטין", "גוגל", "אפל" ואחרות. הפיתוח של מכוניות אוטונומיות התרחב, וכיום הוא כולל משאיות וכלי רכב צבאיים.[24] אלון מאסק, מייסד "טסלה", העריך לא מכבר שעד שנת 2030 או 2035 מרבית המכוניות יהיו אוטונומיות.[25] חברת "אובֶר" הקימה לאחרונה מעבדה בפיטסבורג, שם שוקד מספר רב של בוגרי אוניברסיטת "קרנגי מלון" על חקר מכוניות ללא נהג. חברת "גוגל" שיגרה בינתיים לכבישים מכוניות ללא נהג שכבר גמאו 300,000 מיילים מבלי לגרום לאף תאונה.[26]

לכל אחד מיצרני הרכב המסורתיים ולחברות הטכנולוגיה יש יתרונות שונים, הגורמים לוויכוחים מי מהם יצליח יותר. חברות הרכב המסורתיות מותאמות טוב יותר לטפל באתגרים הייחודיים הנוגעים לייצור מכוניות, ויכולות לשלב בהן בהדרגה מאפיינים חדשים. לעומתן, חברות הטכנולוגיה המבקשות להשתלב בשוק הרכב עשויות להיתקל בקשיים מצד המשתמשים. למרות זאת, אחד ממנהלי "גוגל" טוען שתוכנית החברה לעבור למכירה של מכוניות אוטונומיות מלאות עשויה להתגלות כאסטרטגיה עסקית יעילה.[27]

יצרני המכוניות האוטונומיות יהיו חייבים להשיג את הסכמת המשתמשים, וזאת באמצעות עיצוב חדשני, בטיחות מתקדמת ונתונים סטטיסטיים שיובאו לידיעת הציבור: ראשית, צריך שהתצוגה שתחליף את ההגה במכוניות ללא נהג (מכוניות ברמה 4 לפי סולם NHTSA) תשרה תחושת ביטחון ברכב;[28] שנית, מומחי אבטחה יהיו חייבים לקחת בחשבון את הסיכונים של פריצה לנתונים ושל מתקפה ישירה על מערכות הרכב. בשימוע בקונגרס האמריקאי שהוקדש לנושא זה הכירו הדוברים בכך ש"השתלטות האקרים עלולה לאיים על היכולת להגיע לשיעור הסכמה גבוה" כלפי מכוניות אוטונומיות, וזאת ככל שיתגבר החשש מפני אבטחת נתונים ובטיחות אישית.[29] במצב כזה, המשתמשים יהיו מודאגים מהאפשרות שהתקשורת "רכב לרכב" בכלי הרכב שלהם לא מוגנת,[30] וגם יחששו מפני מתקפות שיפגעו בבטיחות הפעולה של המכונית עצמה; שלישית, יצרנים יוכלו להדגיש את העובדה שמכוניות חכמות בטוחות יותר ממכוניות שנהוגות בידי אדם.[31] 93 אחוזים של תאונות הדרכים בארצות הברית בשנת 2012 נגרמו בשל טעות אנוש, גבו את חייהם של 34,080 בני אדם[32] ועלו כמעט 230 מיליארד דולר למשק האמריקאי.[33] מכוניות אוטונומיות יוכלו לסייע במעבר ל"מטרת העל", שהיא "מערכת התחבורה היעילה והבטוחה ביותר שניתן להעלות על הדעת".[34] עם זאת, במקרה שמכונית אוטונומית בכל זאת תעשה תאונה, סביר להניח שאמצעי התקשורת ידונו באירוע זה יותר מאשר במקרה של תאונה עם מכונית רגילה. לדוגמה, המוות הראשון אי פעם בתאונה שעירבה מכונית אוטונומית התרחש ביוני 2016, כאשר מכונית "טסלה" התנגשה בנגרר של טרקטור בעת פנייה.[35] התאונה קיבלה כיסוי תקשורתי ניכר, אך חברת "טסלה" הזדרזה להרגיע את הציבור כי אפילו לאחר התאונה, שיעור מקרי המוות של מנגנון הנהג האוטומטי נמוך יותר מזה של הנהג האנושי.[36]

דרך נוספת להעלות את שיעור "הסכמת המשתמש" היא באמצעות הדגשת היתרונות הנוספים של המכונית האוטונומית. באלה ניתן לכלול ניידות רבה יותר של אנשים שאינם מסוגלים לנהוג, הקטנת התלות בחניה וכן יתרונות סביבתיים פוטנציאליים.[37] היצרנים צריכים להדגיש שיתרונות אלה עולים במשקלם על

העלייה הפוטנציאלית בסך הקילומטרים שניסע ועל הירידה הצפויה במספר מקומות העבודה עבור נהגים מקצועיים.[38]

פגיעויות

השתלטות של האקרים על מכוניות כיום הינה גם לא יעילה וגם יקרה, משום שהמכוניות של ימינו עושות שימוש במערכות מחשב שונות. אולם, ככל שמכוניות יתחברו ביניהן באמצעות מערכות תקשורת מתקדמות ורשתות כלי רכב, כך תגבר האפשרות להשתלטות נרחבת של האקרים עליהן. למעשה, פריצות בודדות של האקרים למכוניות הן אפשרות הקיימת כבר היום. לדוגמה, צמד האקרים הצליח להשתלט על מערכות ההיגוי, הבלמים והתאוצה של ג'יפ באמצעות מערכת Uconnect של הרכב. מערכת הבידור של הג'יפ הייתה מחוברת לבקרות ההיגוי והבלמים שלו באמצעות רשת המחשב המכונה "CAN bus".[39] במכונית אוטונומית יש יותר חיבורים עם העולם החיצוני ויותר בקרה ממוחשבת של מערכות הרכב מאשר בג'יפ שעבר השתלטות, וכך גדֵלה הפגיעות של כלי רכב מסוג זה. חברת "אובר" אף שכרה לאחרונה את שירותיהם של שני ההאקרים שפרצו לג'יפ במטרה לשפר את האבטחה של כלי הרכב שלה.[40]

יצרני הרכב חייבים להגן בצורה פרו־אקטיבית על מכוניות אוטונומיות מפני השתלטות של האקרים על עדכוני תוכנה, חיישנים ורשתות תקשורת: ראשית, עדכוני תוכנה דרושים כדי שהמכונית האוטונומית תפעל ביעילות, אך הם מהווים גם נקודת תורפה מרכזית,[41] ואם הם יותקנו בצורה מקוונת, המערכת תהיה נתונה לסיכון גבוה אף יותר;[42] שנית, אפשר להערים על חיישני המכונית. אם החיישן מזהה בטעות הולך רגל על הכביש, המכונית תעצור במפתיע.[43] אפשר להטעות חיישני לידאר (Lidar) באמצעות לייזר שעולה בסך הכול שישים דולר,[44] וישנו גם סיכון שנהגים "יפרצו" למכוניות שלהם עצמם או למערכת של המכונית שלהם במטרה לשנות את אופן ההתנהגות של הרכב.[45] בעלים שיפרצו למכוניות של עצמם במטרה להגביר את שליטתם ברכב יסכנו את ביטחונם.[46] הסיכון יגבר כאשר נהג במכונית הפרוצה ימצא עצמו נוסע ליד מכונית רגילה, שנהגה מצפה שהמכונית שנפרצה תנהג בצורה מסוימת; לבסוף, העובדה שמכוניות אוטונומיות יהיו מקושרות אחת לשנייה באמצעות רשתות תקשורת, תיצור נקודות פגיעות נוספות. מתקפות על מערכות "רכב לרכב", "רכב לתשתית" ו־GPS עלולות לפגוע בבטיחות, ב"הסכמת המשתמש" ובפרטיות.[47] תקשורת "רכב לרכב" פגיעה הן למתקפות מסוג של גניבת נתונים מרשת המחשב (CNE) והן למתקפות של השתלטות על רשת המחשב (CNA). מתקפת CNE כנגד תקשורת של מכונית אוטונומית עלולה לפגוע בפרטיותו של קורבן המתקפה,[48] שכן הנתונים של נסיעת הנהג המסוים יכולים לשמש נגדו. מתקפת CNA נגד מכונית אוטונומית יכולה

ליצור פעילות לא חוקית מזויפת ולדווח עליה, ובכך לגרום להשלכות לא נעימות לנהג.[49] האקרים שיפרצו לתקשורת "רכב לרכב" יכולים לשים את ידם על מפתחות, תוכנה, חיישנים ותשדורות יוצאות.[50] מתקפות DoS עלולות ליצור עומס יתר של מידע על המכונית, או לחילופין למנוע ממנה לשלוח מידע.[51]

Lacey מזהה שלושה סוגים של מתקפות נגד תקשורת מסוג "רכב לרכב" ו"רכב לתשתית". האקר יכול להשתמש ב"קישור הודעות" ולעקוב אחר "הודעת בטיחות בסיסית" של "רכב לרכב" כדי לגלות את מיקום המכונית. ב"מתקפת הפללה", ההאקר גונב תחילה את האישור המקוון של המכונית, ולאחר מכן שולח הודעות מזויפות שמעידות על נהיגה לא חוקית לכאורה. "מתקפת הפללה" עלולה לגרום למאסרו של נהג חף מפשע. ב"מתקפת סיביל", האקר גונב אישורים של מכוניות רבות, ולאחר מכן שולח הודעות מכל אחת מהן שמצביעות על נהיגה לא חוקית של מכונית מסוימת.[52] "מתקפת סיביל" עלולה גם היא להפליל נהג המציית לחוק. כל אחת מפגיעויות אלו מהווה מכשול במרוץ לפיתוח מכונית אוטונומית בטוחה. ככל שהיצרנים וחברות הטכנולוגיה ימציאו פתרונות חדשים לאותן פגיעויות, כך הם יתקרבו למטרה שהציבו לעצמם.

מניעים להשתלטות של האקרים

טרור הוא איום מרכזי על מכוניות אוטונומיות. דרך מצוינת לבצע פיגוע ראווה על ידי טרוריסט שיש לו מומחיות טכנית ושאיפות לפרסום בין־לאומי, היא השתלטות על מכונית אוטונומית אחת או יותר. אפילו השתלטות בקנה מידה קטן על כמה מכוניות בלבד עלולה להשבית את מערך התחבורה. מתקפה כזאת תזרע חשש בקרב הנוסעים במכוניות האוטונומיות ובכלי הרכב הרגילים גם יחד, משום שאם מכונית אוטונומית שהאקר הצליח להשתלט עליה נוסעת בכביש, אף מכונית לידה אינה בטוחה. חשש מפני מצב כזה עלול להביא לירידה כוללת בשימוש במכוניות, וכתוצאה מכך לקריסה של הכלכלה האמריקאית. לדוגמה, לאחר מתקפות הטרור על ארצות הברית ב־11 בספטמבר 2001, מספר הטסים במטוסים שם ירד באופן דרמטי ולא חזר לעצמו עד 2004.[53] מכוניות אוטונומיות יכולות לשמש טרוריסטים גם כדי לפגוע במטרות ספציפיות. מתקפה על מכונית יחידה, שתהיה מוסווית היטב, אף עשויה להיראות כמו כשל טכני.

האקרים יכולים לנסות לפגוע במכונית אוטונומית גם כדי לסחוט צרכנים או אפילו את ממשלת ארצות הברית. אם צרכן מקבל הודעה מהמכונית שלו שהיא תבצע תאונה מכוונת, אלא אם יועבר כסף לחשבון מקוון כלשהו, אותו צרכן ייאלץ, קרוב לוודאי, לציית לדרישה. באופן דומה, ארגון פשע יכול להודיע לממשלת ארצות הברית כי השתלט על כמה מכוניות לא מזוהות, ואז לאלץ אותה להיענות לדרישותיו, שאם לא כן יפתח הארגון במתקפה מסיבית. למרבה המזל, האקר

שהמניע שלו הוא כספי יגלה שהתהליך של השתלטות על מכוניות אוטונומיות יקר למדי.[54] השתלטות על מכונית אוטונומית תהיה אטרקטיבית רק אם האקרים יגלו דרך להרוויח מכך כסף.[55] בנוסף, כפי שציין אחד ההאקרים המזהה עצמו כ"כובע לבן", אנשים שיש להם את הידע הטכני הדרוש כדי להשתלט על מערכות תקשורת של מכוניות, בדרך כלל לא רוצים להרוג אנשים אחרים.[56] סיכון חמור יותר הוא סחיטה פוליטית. למשל ארגון "אנונימוס", יכול להשתלט על מכוניות אוטונומיות כדי לתבוע ממשלת ארצות הברית לשנות מדיניות מסוימת.

ממשלות זרות הן איום פחות חמור מאשר טרוריסטים ופושעים. הן יכולות לכוון לפגיעה ברשת תקשורת של מכונית אוטונומית, אולם סביר להניח שהשיבושים שייגרמו כתוצאה מכך בכלכלה האמריקאית ישפיעו גם על אותן ממשלות עצמן. עם זאת, קשה לסמוך על כך שממשלות זרות אכן יפעלו על פי שיקול זה.

פתרונות אפשריים

כדי לצמצם את הסיכוי למתקפות סייבר על מכוניות אוטונומיות, חיוני לאבטח את תשתית הענן, להגן על הטלקומוניקציה ולבחון את הפגיעויות הספציפיות של מכוניות אוטונומיות. יש שורה של פתרונות טכניים ומשפטיים לפגיעויות האופייניות למכוניות כאלו.

כאמור, הגנה על תשתית הענן מפני מתקפות סייבר חיונית לצורך אבטחת המכוניות האוטונומיות. חברות הטכנולוגיה צריכות להיצמד ל"שיטות עבודה מומלצות לאבטחת יישומים", וכך הן יוכלו לקבל גישה לרשת כדי לאבטח את הענן.[57] נוהלי דיווח ובדיקות מחמירים יסייעו גם הם לוודא קיומה של רשת מאובטחת.[58] ולבסוף, צוותי אבטחת הסייבר חייבים לפעול כמו מכבי אש, ולהיות מוכנים להגיב במהירות למתקפות סייבר.[59]

הגנה על הטלקומוניקציה, לרבות תקשורת "רכב לרכב" ו"רכב לתשתית", חיונית לשמירה על הפרטיות והביטחון. חינוך, שיתוף פעולה שמכבד זכות לפרטיות, חוקים ומנהיגות יכולים לסייע להגן על תשתית הטלקומוניקציה מפני מתקפות סייבר.[60] כדי להשיג תקשורת יעילה של "רכב לרכב" ו"רכב לתשתית", המכוניות צריכות לשדר הודעות בטיחות בסיסיות חד־סטריות ולא מוצפנות, שיהיו זמינות לקריאה על ידי כלי הרכב הסמוכים, וזאת בנוסף לתקשורות מאובטחות ואמינות מוצפנות.[61] לדוגמה, חברת הזנק ישראלית בשם "ארגוס" מַפתחת דרך שמאפשרת לקבוע אילו הודעות הן חוקיות ואילו זדוניות.[62]

יש גם פתרונות אפשריים ספציפיים למכונית אוטונומית. פתרונות אלה, כאשר הם ישולבו ביחד, יפחיתו את הסיכוי להצלחתה של מתקפה על הרכב האוטונומי. לצורך זה יש לנקוט את הפעולות הבאות: ראשית, על המפתחים להכיר היטב את דפוסי התנועה והדרך שבה מכונית אוטונומית מתקשרת עם מכוניות אחרות, עם

רוכבי אופניים ועם הולכי רגל. הבנה כזאת תאפשר להם להבחין בין התנהגות נהיגה רגילה לבין התנהגות נהיגה שנתונה להשתלטות עוינת.

שנית, על מפתחי המכוניות האוטונומיות להבטיח אפשרות של זיהוי חיובי של מכונית ספציפית כזו או של מקור העדכון של התוכנה שלה. "תשתית מפתחות ציבוריים" (Public Key Infrastructure – PKI) יכולה לנהל את אישורי הזיהוי של המכוניות האוטונומיות באופן מקוון,[63] בעוד ש"רשות אישורים" תהיה אחראית להקצאת אישורים מקוונים למכוניות כאלו.[64] המערכת שתקצה אישורים מסוג זה תוכל להיות "ממורכזת, מבוזרת או היברידית",[65] והאישורים עצמם יזהו מכוניות שמשתייכות למערכת זאת.[66] בשלב הבא, חברות יתבקשו להבטיח שהמכוניות יוכלו לזהות עדכוני תוכנה חוקיים. מכוניות אוטונומיות יהיו מסוגלות להבחין בין עדכוני תוכנה חוקיים למזויפים באמצעות מנגנוני "לחיצת יד" (handshake).[67] יש גם שורה של פתרונות טכניים שיאפשרו למערכות המחשב של המכוניות האוטונומיות לוודא שהן מחוברות למכונית הנכונה וכי הן מריצות תוכנה חוקית.[68] "בדיקות סבירות" יגבילו את התוכנה שניתן להפעיל על יחידת הבקרה האלקטרונית (ECU) של המכונית,[69] ו"זיהוי רכיב" יוצמד ליחידת הבקרה האלקטרונית.[70] חלק נוסף של התוכנה ינסה לזהות נתונים חריגים.[71]

שלישית, מפתחי מכוניות אוטונומיות צריכים להפריד בין מערכות מחשב חיוניות לבלתי חיוניות. השתלטות ההאקרים על הג'יפ, שתוארה לעיל, ממחישה את הפגיעות של מכוניות שהפונקציות שלהן מקושרות כולן בצורה אלקטרונית. Camek ואחרים ממליצים שיצרני הרכב יבנו מכוניות עם "שכבות אבטחה מרובות ובלתי תלויות" (MILS), שיש להן יכולות "מסתגלות" ו"מבוזרות".[72] ארכיטקטורת MILS בונה מחסום בין מחשבים חיוניים למחשבים לא חיוניים במכונית. ההפרדה בין מערכות המחשב יכולה למנוע מווירוס להגיע לפונקציות חיוניות ברכב.[73] מערכת מבוזרת תאפשר לארכיטקטורת MILS לפעול על מספר רב של מחשבים. מערכת מסתגלת תאפשר עדכון של יכולות חדשות.[74] מרכיבים אלה יסייעו לצמצם את הסיכוי של מתקפה על מכוניות אוטונומיות בעתיד.

רביעית, יצרנים צריכים לחפש אחר פתרונות טכניים נוספים. "קופסאות שחורות", שבמקור הן משמשות במטוסים, יוכלו להקליט נתונים על תאונות מבלי שיקליטו בהכרח נתוני GPS פרטיים.[75] נתונים אלה יוכלו לשמש ללימוד הטעויות שהובילו לתאונה ולספק רמזים לשאלה אם הייתה השתלטות על כלי הרכב. יש לצייד מכוניות אוטונומיות גם ב"מצב בטוח", שיאפשר להשבית את התכונות האוטונומיות שלהן,[76] כך שבמקרה של השתלטות, הנהג יוכל להחזיר לעצמו בבטחה את השליטה על הרכב. כדי לאפשר "מצב בטוח", יהיה צורך לשמר במכונית האוטונומית את ההגה המסורתי ואת דוושת הבלמים. יצרנים יידרשו גם להיצמד לתקני התעשייה ולבדיקות מקיפות של כלי הרכב.[77]

חמישית, לצד המאמצים הרבים להגנה על רכב אוטונומי מפני אתגרים טכניים, חשוב גם לבחון פתרונות משפטיים. חוקים נכונים יכולים הן להרתיע האקרים והן להקשות עליהם בניסיונותיהם להשתלטות עוינת. ואמנם, מדינות שונות כבר מיישמות חוקים בנוגע לבדיקת מכוניות אוטונומיות.[78] על המדינות לפעול ליישום חוקים המחייבים יצרני מכוניות אוטונומיות להיצמד לשיטות עבודה מומלצות בכל הנוגע לאבטחה. המחוקק המקומי והממשלתי גם יכול ליזום חקיקה שתגן על רישיונות. מכיוון שבלתי אפשרי לתכנן מכונית שהחומרה שלה חסינה באופן מוחלט מפני פריצות, החוק יצטרך להרתיע אנשים שהשיגו גישה פיזית לרכב מגניבת מפתחות תוכנה.[79] בנוסף, ניתן לעשות שימוש בחוקים המגנים על מערכות אוטונומיות קיימות, כגון אלו המשמשות במערכות בקרה אווירית. ניתן להרחיב חוקים אלה כך שיכסו גם מכוניות אוטונומיות, ככל שאלו יהפכו לנפוצות יותר.

שישית, גם חברות פרטיות ובתי המשפט יכולים למלא תפקיד במציאת פתרונות אפשריים לפגיעויות של כלי רכב אוטונומיים. בתי המשפט חייבים לקבוע כיצד להגיב לתאונות שנגרמו בעקבות השתלטות של האקרים. חברות שאוספות נתונים על מכוניות אוטונומיות צריכות לשאת באחריות משפטית להגנה על נתונים אלה.[80] דרישות מסוג זה יעודדו אותן חברות להשקיע באבטחת נתונים.

דילמות אתיות

מכוניות אוטונומיות משתמשות בתשתית ענן במצבים שיש להם נגיעה לחיים ומוות, ולכן הן מעלות שאלות אתיות רבות. אמנם, אין מקום לדיון אתי מפורט במאמר זה, אך בכל זאת כדאי לסקור כמה מהשאלות הנפוצות המופיעות בספרות בסוגיה זאת. מערכות אתיקה יכולות להתמקד בתועלתנות, זכויות, צדק, "הטוב המשותף" או תכונות טובות.[81] אפתח בגישה התועלתנית, שכן המכוניות האוטונומיות מבקשות להציל כמה שיותר חיי אדם, או כפי שציין אלכסנדר קוט (Kott): "מכוניות ללא נהג יהרגו אנשים, אבל פחות".[82] מנקודת מבט תועלתנית, הבחירה המתבקשת היא, אפוא, לעשות שימוש במכוניות אוטונומיות. Turek הולך צעד נוסף קדימה וטוען כי מכונית אוטונומית צריכה להיות מתוכנתת לא רק להצלת חיים, אלא גם כדי לשמור שהתנועה של מיליוני נהגים תזרום ללא הפרעה.[83]

מכיוון שהאלגוריתמים של המכוניות האוטונומיות נכתבים מראש, כל שינוי הנוגע לחיים ולעניינים שבנוחות נקבע גם הוא מראש. כאשר המתכנתים מקודדים את האלגוריתמים של המכונית, עליהם לדאוג שאלה יהיו "עקביים", להימנע מלעורר "זעם ציבורי" ו"לא לרפות את ידי הרוכשים".[84] יצרני המכוניות האוטונומיות גם יצטרכו לבחור בין הרג של הולך רגל ובין הריגת הנהג. Frowe טוען שבעצם הבחירה להיכנס לכלי הרכב, הנהג מקבל על עצמו אחריות, ולכן הוא צריך להסתכן בכך שחיי הולך הרגל יקבלו עדיפות גבוהה יותר על חייו שלו.[85] במקרה

כזה יהיה צורך בפסיכולוגים ובנתוני סקרים כדי לבנות אלגוריתמים קבילים, שכן אנשים עשויים להסתייג מלהיכנס למכונית אוטונומית "תועלתנית" שתבחר להרוג אותם ולהציל את הולך הרגל.[86] העקביות באלגוריתמים חיוניות גם היא. אחרת תיתכן אפליה כלכלית, שכן אלה המסוגלים להרשות לעצמם לרכוש רכב שיגן על הנהג בוודאי יעשו זאת.

אתגר נוסף שיש לבחון הוא מי אחראי לתאונה. ככל שהמכונית האוטונומית תהפוך לנפוצה יותר, כך יהיה צורך לקבוע מי אחראי לתאונות – היצרנים או האדם היושב ברכב.[87] התשובה יכולה להיות תלויה בשאלה אם המכונית היא אוטונומית (רמה 3) או ללא נהג (רמה 4). לבסוף, ישנה הסוגיה של רשת כלי רכב אוטונומיים הנוטלים את חופש הבחירה מהאדם: ממשלה השולטת ברשת יכולה לקבוע לא רק את מהירות הנהיגה של כלי רכב אוטונומיים, אלא גם את יעדיהם. רשת כזאת יכולה, לפיכך, לאפשר לממשלה לשלוט בניידותם של בני אדם.[88]

השלכות ונושאים למחקר נוסף

האם כל מה שנכתב לעיל מוביל למסקנה שיצרני הרכב האוטונומי צריכים "להרים ידיים"? האם האתגרים הטכניים והבטיחותיים הייחודיים של רכב מסוג זה הם כה גדולים, עד שחברות הטכנולוגיה והיצרנים צריכים להקפיא את פיתוח המכונית האוטונומית עד שתהיה בטוחה יותר? התשובה לשאלות אלו היא שלילית לחלוטין. מפתחי המכונית האוטונומית צריכים להמשיך בהתקדמותם, משום שמכוניות אוטונומיות, על כל הליקויים הנוכחיים שקיימים בהן, יכולות למנוע תאונות ולהציל חיים. אלון מאסק, מייסד "טסלה", התייחס לכך לאחרונה, כשכתב כי החברה שלו אינה מתעכבת במאמציה להוציא לשוק מכוניות אוטונומיות, משום ש"כאשר נעשה שימוש נכון [במכונית אוטונומית, היא תהיה] בטוחה משמעותית יותר מאשר אדם הנוהג בעצמו, ולכן תהיה זו שגיאה מוסרית לעכב את יציאתה לשוק רק בשל החשש מפרסום שלילי או חישוב מסחרי כזה או אחר הנוגע לאחריות משפטית".[89] במקביל לפיתוח המכונית האוטונומית, חייבים המתכננים להמשיך ולפתח אמצעי בטיחות יעילים יותר.

למכונית האוטונומית יש השלכות רבות שיכולות להוביל למחקרים נוספים. השלכות אלו כוללות, בין השאר, את המחלוקת סביב הזכות להשתמש בתקשורת ייעודית אלחוטית לטווח קצר (DSRC),[90] אבטחת סייבר של כטב"מים,[91] התאמת המכונית האוטונומית להתנהגות הבלתי מושלמת של הנהג האנושי,[92] והצמיחה של תעשיית הבידור הקשורה למכוניות. חששות משפטיים שיש לחקור את משמעויותיהם והשלכותיהם כוללים את האחריות על תאונות,[93] את החוקיות של שירותי מעקב משטרתי כגון אלה שמציעה תוכנת "ווייז", ההשפעה של המכונית

האוטונומית על חברות הביטוח, והסיכון מהפעלת מניפולציה על נתוני המכונית כדי ליצור מצג שווא.

כך או כך, כדאי שנהדק את חגורות המושב בעודנו מאיצים את מכוניותינו לעבר עולם האינטרנט של הדברים.

הערות

1 Isaac Asimov, "Sally", in Nightfall Two (Frogmore: Granada, 1976).

2 James M. Anderson, Nidhi Kalra, Karlyn D. Stanley, Paul Sorensen, Constantine Samaras and Oluwatobi A. Oluwatola, Autonomous Vehicle Technology: A Guide for Policymakers (Santa Monica: RAND, 2014), p. 66.

3 "Why Autonomous and Self-Driving Cars Are Not the same", Economist, July 1, 2015, http://www.economist.com/blogs/economist-explains/2015/07/economist-explains.

4 Elon Musk, "Master Plan Part Deux", Tesla (blog), July 20, 2016, https://www.tesla.com/blog/master-plan-part-deux.

5 "U.S. Department of Transportation Releases Policy on Automated Vehicle Development", NHTSA, May 30, 2013, http://www.nhtsa.gov/About+NHTSA/Press+Releases/U.S.+Department+of+Transportation+Releases+Policy+on+Automated+Vehicle+Development.

6 שם.

7 Anderson and others, Autonomous Vehicle Technology, p. 60.

8 שם, עמ' 61.

9 שם, עמ' 61–62.

10 שם.

11 שם, עמ' 62.

12 שם, עמ' 64.

13 "How Does a Self-Driving Car Work?", Economist, April 29, 2013, http://www.economist.com/blogs/economist-explains/2013/04/economist-explains-how-self-driving-car-works-driverless?fsrc=scn/fb/wl/bl/tr/st/howdoesaself-drivingcarwork.

14 Anderson and others, Autonomous Vehicle Technology, p. 64.

15 "How Does a Self-Driving Car Work?"

16 Christoph Ponikwar and Hans-Joachim Hof, "Overview on Security Approaches in Intelligent Transportation Systems: Searching for Hybrid Trust Establishment Solutions for VANETs", Secureware (2015): The Ninth International Conference on Emerging Security Information, Systems and Technologies, eds. Rainer Falk, Carla Merkle Westphall and Hans-Joachim Hof (Wilmington, DE: IARIA, 2015), http://toc.proceedings.com/27725webtoc.pdf.

17 שם, עמ' 1.

18 Anderson and others, Autonomous Vehicle Technology, p. 80.

19 Douglas Lacey, Vehicle-to-Vehicle Technologies for Intelligent Transportation Systems: Development, Challenges and Security Proposals (New York: Nova Science, 2014), p. 10.

20 "Intelligent Transportation Systems: Vehicle-to-Vehicle Technologies Expected to Offer Safety Benefits, but a Variety of Development Challenges Exist", United States Government Accountability Office (2013).

21 Anderson and others, Autonomous Vehicle Technology, p. 58.

22 Jerry L. Archer, "International Engagement on Cyber V: Securing Critical Infrastructure", Georgetown Journal of International Affairs (2015): 168.

23 Andreas Riener, "Who Cares about Trust, Grade of Traveling and Quality of User Experience in a World of Autonomous Cars?", AutomotiveUI '14, Adjunct Proceedings of the 6th International Conference on Automotive User Interfaces and Interactive Vehicular Applications (2014): 1-3.

24 Nick Lavars, "Self-driving Truck Hits the Highway in World First", New Atlas, October 4, 2015, http://newatlas.com/daimlers-production-autonomous-truck-debuts-public-roads/39701/; David Sedgwick, "Army Eyes Self-Driving Convoys", Automotive News, August 4, 2015, https://www.autonews.com/article/20150804/OEM06/308059984/army-eyes-self-driving-convoys.

25 Benjamin Snyder, "Tesla CEO Elon Musk just told us When all Cars will be Self-Driving", Fortune, November 4, 2015, http://fortune.com/2015/11/04/tesla-elon-musk-self-driving-cars/.

26 "Intelligent Transportation Systems: Vehicle-to-Vehicle Technologies Expected to Offer Safety Benefits, but a Variety of Development Challenges Exist", p. 7.

27 "Upsetting the Apple Car", Economist, February 21, 2015, http://www.economist.com/news/business/21644149-established-carmakers-not-tech-firms-will-win-race-build-vehicles.

28 Nikhil Gowda, Wendy Ju and Kirsten Kohler, "Dashboard Design for an Autonomous Car", AutomotiveUI '14, Adjunct Proceedings of the 6th International Conference on Automotive User Interfaces and Interactive Vehicular Applications (2014): 1-4.

29 "Intelligent Transportation Systems: Vehicle-to-Vehicle Technologies Expected to Offer Safety Benefits, but a Variety of Development Challenges Exist", p. 8.

30 Lacey, Vehicle-to-Vehicle Technologies for Intelligent Transportation Systems, p. 25.

31 Anderson and others, Autonomous Vehicle Technology, pp. 15-16.

32 "How Autonomous Vehicles will Shape the Future of Surface Transportation", United States Subcommittee on Highways and Transit (2013), p. vii.

33 שם.

34 שם, עמ' 7.

35 The Tesla Team, "A Tragic Loss", Tesla (blog), June 30, 2016, https://www.tesla.com/blog/tragic-loss.

36 שם.

37 Anderson and others, Autonomous Vehicle Technology, p. 9.

38 שם, עמ' xvii.

39 Andy Greenberg, "Hackers Remotely Kill a Jeep on the Highway – With Me in It", Wired, July 21, 2015, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

40 Roberto Baldwin, "Jeep Hackers Get New Jobs at Uber's Autonomous-car Lab", Egadget, August 28, 2015, https://www.engadget.com/2015/08/28/uber-jeep-hackers/.

41 Anderson and others, Autonomous Vehicle Technology, p. 70.

42 שם.

43 שם, עמ' 71.

44 Anna Peel, "Self-Driving Cars Can Be Disabled with Lasers", ValueWalk, September 8, 2015, http://www.valuewalk.com/2015/09/self-driving-cars-can-be-disabled-with-lasers/.

45 Anderson and others, Autonomous Vehicle Technology, p. 71.

46 שם.

47 Lacey, Vehicle-to-Vehicle Technologies for Intelligent Transportation Systems, p. 54.

48 שם, עמ' 72.

49 שם.

50 שם, עמ' 68–69.

51 שם, עמ' 69.

52 שם, עמ' 72–73.

53 "Airline Travel Since 9/11", United States Department of Transportation, Bureau of Transportation Statistics Issue Brief, no. 13, December 2005, http://www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/publications/special_reports_and_issue_briefs/issue_briefs/number_13/html/entire.html.

54 James Guy and Mat Greenfield, "Can Driverless Cars Ever Be Made Hack-Proof?", The Guardian, March 9, 2015, https://www.theguardian.com/technology/2015/mar/09/driverless-cars-safe-hackers-google.

55 שם.

56 שם.

57 Jerry L. Archer, "Dynamic and Effective Security in the Rapidly Evolving Global Cloud Computing Cyberspace", Georgetown Journal of International Affairs (2015): 173.

58 שם, עמ' 174.

59 שם, עמ' 175.

60 Tarek Saadawi and Haidar Chamas, "Securing Telecommunications Infrastructure against Cyber Attacks", Georgetown Journal of International Affairs (2015): 58-69.

61 Lacey, Vehicle-to-Vehicle Technologies for Intelligent Transportation Systems, p. 64.

62 Kobe Liani, "Israeli Start-Up Will Protect your Car [from] Cyber Terrorism", Walla, March 23, 2015, http://cars.walla.co.il/item/2839940.

63 Lacey, Vehicle-to-Vehicle Technologies for Intelligent Transportation Systems, p. 63.

64 שם, עמ' 81.

65 Ponikwar and Hof, "Overview on Security Approaches in Intelligent Transportation Systems: Searching for Hybrid Trust Establishment Solutions for VANETs", pp. 160-165.

66 שם.
67 Anderson and others, Autonomous Vehicle Technology, p. 70.
68 Lacey, Vehicle-to-Vehicle Technologies for Intelligent Transportation Systems, p. 79.
69 שם, עמ' 78.
70 שם, עמ' 79.
71 שם.
72 Alexander Georg Camek, Christian Buckl and Alois Knoll, "Future Cars: Necessity for an Adaptive and Distributed Multiple Independent Levels of Security Architecture", HiCoNS '13, Proceedings of the 2nd ACM International Conference on High Confidence Networked Systems (2013): 17-24.
73 "Five Star Automotive Cyber Safety Program", I Am the Cavalry, February 2015, https://www.iamthecavalry.org/domains/automotive/5star/.
74 Camek and others, "Future Cars: Necessity for an Adaptive and Distributed Multiple Independent Levels of Security Architecture".
75 "Five Star Automotive Cyber Safety Program".
76 שם.
77 שם.
78 Anderson and others, Autonomous Vehicle Technology, pp. 41-52.
79 Lacey, Vehicle-to-Vehicle Technologies for Intelligent Transportation Systems, p. 77.
80 Archer, "International Engagement on Cyber V: Securing Critical Infrastructure", p. 174.
81 Manuel Velasquez, Dennis Moberg, Michael J. Meyer, Thomas Shanks, Margaret R. McLean, David DeCosse, Claire André and Kirk O. Hanson, "A Framework for Thinking Ethically", Markkula Center for Applied Ethics, August 1, 2015, https://www.scu.edu/ethics/ethics-resources/ethical-decision-making/a-framework-for-ethical-decision-making//.
82 Alexander Kott, Cybersecurity, Lecture at Georgetown University, Washington, D.C., 2015. (צריך להוסיף כותרת ההרצאה)
83 Mitch Turck, "An Autonomous Car might Decide you should Die", Backchannel, March 10, 2015, https://backchannel.com/reinventing-the-trolley-problem-85f3d1730756#.lnpj44f1l.
84 Jean-François Bonnefon, Azim Shariff and Iyad Rahwan, "Autonomous Vehicles Need Experimental Ethics: Are We Ready for Utilitarian Cars?", arXiv:1510.03346v1 [cs.CY], October 12, 2015, http://arxiv.org/pdf/1510.03346v1.pdf.
85 Olivia Goldhill, "Should Driverless Cars Kill Their Own Passengers to Save a Pedestrian?", Quartz, November 1, 2015, http://qz.com/536738/should-driverless-cars-kill-their-own-passengers-to-save-a-pedestrian/.
86 Bonnefon and others, "Autonomous Vehicles Need Experimental Ethics".
87 Alexander Hevelke and Julian Nida-Rümelin, "Responsibility for Crashes of Autonomous Vehicles: An Ethical Analysis", Science and Engineering Ethics 21, no. 3 (2015): 619-630.
88 ראיון של המחבר עם Fr. Dennis McManus, 8 בדצמבר 2015.

89 Musk, "Master Plan Part Deux".

90 Anderson and others, Autonomous Vehicle Technology, p. 80.

91 Jon Fingas, "The U.S. Navy wants to Protect its Drones against Hacks", Egadget, May 20, 2015, https://www.engadget.com/2015/05/20/us-navy-wants-hack-resistant-drones/.

92 Matt Richtel and Conor Dougherty, "Google's Driverless Cars Run into Problem: Cars with Drivers", The New York Times, September 1, 2015, http://www.nytimes.com/2015/09/02/technology/personaltech/google-says-its-not-the-driverless-cars-fault-its-other-drivers.html?_r=0.

93 "Safer at any Speed?", Economist, March 3, 2012, http://www.economist.com/node/21548992.

סייבר, מודיעין וביטחון
קול קורא להגשת מאמרים לכתב העת

כתב העת **סייבר, מודיעין וביטחון** הינו כתב עת **שפיט** היוצא לאור שלוש פעמים בשנה בעברית ובאנגלית. עורך כתב העת הינו ד"ר גבי סיבוני העומד בראש תכנית צבא ואסטרטגיה ותכנית ביטחון בסייבר במכון למחקרי בטחון לאומי.
פנייה זו הינה קול קורא להגשת מאמרים ומחקרים שיפורסמו במסגרת כתב העת, על-פי שיקולי המערכת.

ייבחנו מאמרים הנוגעים לתחומים הבאים:

- מדיניות גלובלית ואסטרטגיה בסייבר
- רגולציה במרחב הקיברנטי
- אבטחת החוסן הלאומי בסייבר
- לוחמת סייבר והגנה על תשתיות חיוניות
- בניין הכוח הקיברנטי על מרכיביו: המשאב האנושי, אמצעי לחימה, תורה, ארגון, הכשרה ופיקוד;
- היבטים אתיים, מוסריים ומשפטיים במרחב הקיברנטי.
- טכנולוגיה במרחב הקיברנטי
- הרתעה במרחב הקיברנטי
- ניתוח איומים וסיכונים במרחב הקיברנטי
- ניתוח תקריות ומשמעויות במרחב הקיברנטי
- חשיבה צבאית ואסטרטגית, הפעלת הכוח הצבאי במרחב הסייבר ומבצעי תודעה
- מודיעין, שיתוף מידע, ושותפות ציבורית-פרטית (PPP)
- שיטות מחקר, פעולה והליכים (TTPs)

ניתן לעיין במאמרים בתחומים קרובים שנכתבו בגיליונות כתב העת **צבא ואסטרטגיה**, באתר האינטרנט של המכון: http://www.inss.org.il

ייבחנו מאמרים בהיקף של עד 5,000 מילים בעברית (עד 6,000 מילים באנגלית) כולל הערות שוליים ומראי מקום. המאמרים יכללו תקציר בהיקף של 100-120 מילים ורשימת מילות מפתח בהיקף של עד 10 מילים.

להגשת מאמרים ולפרטים נוספים ניתן לפנות לח"מ.

בברכה

הדס קליין, מתאמת כתב העת: **סייבר, מודיעין וביטחון**
hadask@inss.org.il

המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
INCORPORATING THE JAFFEE CENTER FOR STRATEGIC STUDIES
TEL AVIV UNIVERSITY אוניברסיטת תל-אביב

המכון למחקרי ביטחון לאומי – תכנית ביטחון סייבר
רח' חיים לבנון 40, ת"ד 39950, רמת אביב, תל אביב 61398 | טל': 03-6400400 | פקס: 03-7447588