צבא ואסטרטגיה

כרך 7 | גיליון 3 | דצמבר 2015

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

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

צבא ואסטרטגיה

כרך 7 | גיליון 3 | דצמבר 2015

צבא ואסטרטגיה

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

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)

בין מציאות מדומה לטרור ממשי

דניאל כהן

מאמר זה מתמקד בשימוש של "המדינה האסלאמית" ושחקנים לא מדינתיים אחרים באמצעי תקשורת וטכנולוגיה כדי להשפיע על יחידים או על קבוצות, תוך שילוב בין רשת האינטרנט ובין עולם המציאות שמחוץ לרשת. אופן השימוש של "המדינה האסלאמית" ברשת בכלל ובמדיה החברתית בפרט לעיצוב המציאות דרך עיניה ולקידום מטרות הטרור שלה, שונה במהותו מהשימוש שעשו ארגוני טרור בעבר. שחקנים לא מדינתיים וארגוני טרור נוספים לומדים ומפיקים לקחים מהצלחת מודל הפעולה של "המדינה האסלאמית" כדי להשתמש באמצעי תקשורת וטכנולוגיה לצורך השפעה על יחידים או על קבוצות. המאמר בוחן את השימוש שעושה "המדינה האסלאמית" למינוף יתרונות הרשת, תוך שהוא מזהה שלושה מרחבי פעולה – גיאוגרפי, קיברנטי ותודעתי – המשמשים אותה לתקשורת, לתעמולה, ללוחמה פסיכולוגית, לגיוס פעילים ולשימוש ברשת במטרה להשפיע על בודדים או קבוצות ולהסית אותם לביצוע פעולות טרור בצורה ספונטנית.

מילות מפתח: סייבר, רשתות חברתיות, טרור, תודעה, "אל־קאעדה", המרחב הקיברנטי, "המדינה האסלאמית", דאע"ש, רשת האינטרנט.

מבוא

"אבולוציית הטרור" הנוכחית, המתגלמת בדמותה של "המדינה האסלאמית" (דאע"ש), מתאימה את עצמה לשינויים המהירים אותה חווה החברה האנושית ומצליחה "לדחוס מרחב וזמן" באפקטיביות רבה.[1] "המדינה האסלאמית" פועלת בשלושה מרחבי פעולה – גיאוגרפי, קיברנטי ותודעתי – ועושה זאת באמצעות יכולות לעיצוב תודעתי. זה בא לידי מימוש במרחב הקיברנטי, בשימוש

דניאל כהן הינו עמית מחקר ומתאם תכנית ביטחון סייבר במכון למחקרי ביטחון לאומי

באידיאולוגיה סלפית, בהשתלטות על מרחבים גיאוגרפיים ובכינון "הח'ליפות האסלאמית":

א. **מבחינה גיאוגרפית**, מדובר בהתבססות פרוטו מדינתית בסוריה ובעיראק ובשליחת גרורות לזירות לחימה בלוב, בניגריה, בתימן ובאפגניסטן. בנוסף, עוסקת "המדינה האסלאמית" בפעילות צבאית ובפיגועי טרור נגד מטרות המזוהות עם יריביה בזירות שונות.

ב. **מבחינה קיברנטית**, "המדינה האסלאמית" פועלת באופן שיטתי במרחב הסייבר, שם היא יצרה לעצמה תשתיות פעולה המשמשות אותה לקידום מטרותיה.

ג. **המרחב התודעתי** נמצא בין המרחב הגיאוגרפי ובין המרחב הקיברנטי. במרחב זה מבצעת "המדינה האסלאמית" פעולות פיזיות וקיברנטיות, כגון: שימוש בסמלים היסטוריים ודתיים ובסממני ריבונות, מחיקת דתות ואידיאולוגיות אחרות והצגת אכזריות קיצונית ומוחצנת.

כמטאפורה מעולם המחשוב ניתן לומר כי המרחב הקיברנטי והפיזי הם ה"חומרה" בשימוש "המדינה האסלאמית", בעוד שהתודעה הינה ה"תוכנה" בה היא עושה שימוש למניפולציות של עיבוד מידע וסמלים.

מאמר זה מתמקד בשימוש שעושים "המדינה האסלאמית" ושחקנים לא מדינתיים נוספים באמצעי תקשורת וטכנולוגיה כדי להשפיע על יחידים או על קבוצות, תוך שילוב בין העולם המקוון לעולם הלא מקוון – בין עולם רשת האינטרנט לזה שמחוץ לרשת.[2] הניתוח שעושה המאמר מתמקד במקרה בוחן – השימוש של "המדינה האסלאמית" באמצעי הטכנולוגיה והתקשורת לעיצוב תודעתי ותקשורתי שנועד לקדם את מטרות הטרור שלה, וזאת באופן השונה במהותו מהשימוש שעשו ארגוני טרור ברשת בעבר.

"המדינה האסלאמית" פונה לקהל רחב של קהילות מוסלמיות ברחבי העולם, תוך הצגת מציאות מעוותת. היא עושה זאת באמצעות מנגנוני תוכן והפצה של קמפיינים במדיה וברשתות החברתיות. במקביל, "המדינה האסלאמית" מהווה מוקד משיכה לגיוס בשטחים שבתחום שליטתה. שחקנים לא מדינתיים וארגוני טרור, כגון "אל־קאעדה", חמאס וחזבאללה, לומדים מהטכניקות השונות שלה ופועלים גם הם להשגת כלים יעילים יותר במרחב הווירטואלי. כמו בתחומי חיים רבים אחרים, ובעיקר בתחומים עסקיים, גם שחקנים אלה מרחיבים את ארגז הכלים שלהם לפעילות ברשת באופן הממצה את יכולותיהם. פעילותם ברשת תומכת את פעילותם במרחב הפיזי, ויש לה השפעות גם על פעולות טרור שלהם בעולם הממשי.

השינוי שיצרו האינטרנט ומהפכת הרשתות החברתיות

העולם המכני, המבוזר והאיטי, שהחל עם המהפכה התעשייתית השנייה, כלל תיעוש של מרבית תחומי הפעילות האנושית והמרת שרירי האדם והחיה על ידי מכונות. עולם זה הוחלף בשנים האחרונות בעולם רשתי, אלקטרומגנטי, מהיר, בו־זמני ומאוחד, המחבר בין גבולות פיזיים ובין גבולות התודעה ומטשטש אותם. הופעת הרשתות החברתיות בשנת 2005 מסמלת שלב חדש בהתפתחות הרשת. טכנולוגיית המידע המודרנית, שבאה לידי ביטוי בשימוש שעשו תנועות המחאה השונות ברחבי העולם ברשתות החברתיות, היא בעלת השפעה משמעותית ביותר. היא מאפשרת מעבר של ידע בצורה מהירה ושקופה ושימוש בו ככלי מרכזי לקידום ושינוי תהליכים פוליטיים וחברתיים. קבוצות קטנות יחסית וחסרות מבנה היררכי מוגדר מצליחות להפגין גמישות ותחכום ומגיעות במהירות להמונים באמצעות המרחב הווירטואלי.

בחינת התהליכים שהובילו לגל המחאות ששטף את העולם בשנים האחרונות, החל מ"האביב הערבי" במזרח התיכון[3] וכלה במחאות החברתיות על רקע כלכלי־חברתי ברחבי העולם, מצביעה על חשיבותן המכרעת של הרשתות החברתיות ככלים המשנים את פני החברה. ברמה הארגונית אף נעשתה קפיצת מדרגה מאז "האביב הערבי", והנגישות הטכנולוגית מאפשרת פיתוח אתרים ויישומים, כולל אזורים מוגנים בסיסמאות הנגישים למעגלי השפעה קרובים, שימוש ביישומי מובייל לשיתוף מסרים מידיים ועוד.[4] עוצמה זאת מוחזקת היום ברמה כזו או אחרת בידי מיליארדי אנשים, והיא שינתה מן היסוד את כללי המשחק.[5] כמעט שני מיליארד מאוכלוסיית העולם גולשים כיום ברשתות החברתיות, ונתון זה נמצא במגמת עלייה וצפוי להמשיך ולעלות בשנים הקרובות.[6]

האדם יצר את מרחב הסייבר, ובכך הקים רשת תקשורת גלובלית שצמצמה מאוד את הממדים הפיזיים של סביבת חייו. פירוש הדבר הוא ששינויים טכנולוגיים ותודעתיים הביאו להאצת מהירות התנועה והחישה האנושית במרחב באמצעות רשתות המחשבים של ימינו. בעת גלישה באינטרנט, התגובה העצבית (פעולת תאי העצב במוח בתגובה לגירויים שונים) של הגולש, וכן המידע מהרשת, מגיעים אל תודעת הגולש באותו הזמן.[7] הרשת מאפשרת למשתמש בה להיות בו־זמנית "בכל מקום ובשום מקום".[8] החיבור בין האינטרנט ובין הטלפון החכם הפך את האדם לזמין בכל רגע לכל מידע ותקשורת, ללא קשר למרחב הפיזי שבו הוא נמצא.

"המדינה האסלאמית" והשינוי המחשבתי והמעשי בארגונים הסלפיים־ג'יהאדיים

פנייתן של קבוצות פונדמנטליסטיות לציבור הרחב נעשתה על פי רוב במסגרת עקרונות מוסריים כלליים, בהם הוקרנו תחושות של משמעת, אותנטיות, מחויבות

וביטחון. התנועות האסלאמיסטיות וההתפשרות על עקרונות יצרו קבוצות שוליים חדשות, אשר הקצינו לא רק את אמצעי האלימות והטרור, אלא גם את הדיכוטומיה בין האסלאם ובין המערב.[9] ד"ר עבדאללה עזאם וממשיך דרכו אוסמה בן לאדן פיתחו תפיסה לפיה מלחמת הקודש (הג'יהאד) בכופרים חייבת להפוך למסלול מקביל, ולעתים חלופי, למלחמה במשטרים הכופרים השולטים בעולם האסלאמי; הג'יהאד צריך להיות חובק עולם, ויש להכות בכופרים שהשתלטו על שטחים השייכים לאסלאם (כגון צ'צ'ניה, הבלקן ופלסטין). בנוסף לכך, יש לפגוע בכלכלת המערב, שהוא מקור החוסן של המשטרים הכופרים בארצות האסלאם. חזונו של עבדאללה עזאם שבה לבבות, בעיקר אצל בני הדור השני והשלישי של המהגרים מהמזרח התיכון וצפון אפריקה לאירופה המערבית. צעירים אלה לא הצליחו לעבור את המשוכה המעמדית של בני הדור הראשון להגירה, ולכן בשורתם של עזאם ובן לאדן הייתה להם כ"טל על אדמה צחיחה".[10]

הטלטלה שאחזה במדינות המזרח התיכון בשנת 2011 ומוטטה כמה מהמשטרים "הכופרים" הביאה את ארגון "אל־קאעדה" לקרוא להמונים להמשיך את המהפכות עד סילוק המשטרים "המושחתים" כולם.[11] "האביב הערבי" אפשר ל"אל־קאעדה" לשנות את סדר העדיפויות שלו ולמקד אותו בג'יהאד "פנימי", וזאת כדי להשפיע על עיצוב המשטרים החדשים ברחבי המזרח התיכון והמגרב על פי הדגם הסלפי.[12]

פלג סורר של "אל־קאעדה" בעיראק, בשם "המדינה האסלאמית בעיראק וא־שאם" (דאע"ש), ניצל את חולשת השלטון הריבוני בעיראק ואת התפרקות סוריה כחלק מאירועי "האביב הערבי", ומיהר לפעול, תוך שהוא מעביר חלק מפעילותו לשטחה של סוריה. הארגון המזוהה עם "אל־קאעדה" בסוריה, "ג'בהת א־נוסרה", וכן יורשו של בן לאדן בהנהגת "אל־קאעדה", איימן א־זוואהירי, התנערו מצעד זה, וכך נוצר פיצול בין דאע"ש לבין "אל־קאעדה". בהמשך, במארס 2014, הושק קמפיין ברשת טוויטר, ובו דרישה להכתיר את מנהיג דאע"ש, אבו בכר אל־בגדאדי, לח'ליף.[13] קריאה זו לא נשארה בחלל הריק, אלא שימשה כניסוי כלים בידי מנהלי קמפיין המדיה החדשה של דאע"ש, אשר רצו לבחון כיצד תפורש ההצהרה בקרב קהילת הג'יהאד הסלפי הפועלת ברשתות החברתיות. ביוני 2014 כבר הכריז דובר דאע"ש, אל־עדנאני, על הקמת ח'ליפות אסלאמית בשטחים שנכבשו על ידי הארגון בסוריה ובעיראק, ואבו בכר אל־בגדאדי הוכרז כ"ח'ליף המדינה האסלאמית" (עיראק וא־שאם נשמטו משם הארגון).[14]

כבר במהלך המחצית השנייה של שנת 2014 חלשה "המדינה האסלאמית" על טריטוריה עצומה בצפון־מזרח סוריה ובחלקה המערבי והצפוני של עיראק. בנוסף לכך, היא זכתה לקבל את שבועות האמונים של ארגונים סלפיים ג'יהאדיים שונים באפריקה, באסיה ובמזרח התיכון והקימה תאי תמיכה ברחבי העולם המוסלמי,

כולל בקהילות מוסלמיות במערב. "המדינה האסלאמית" הטמיעה ושילבה בצורה ייחודית בין אידיאולוגיה סלפית לבין פרקטיקה פרגמטית, המשרתת את כינון מדינת ההלכה על פי דגם אידיאלי של ראשית ימי האסלאם וארבעת הח'ליפים הראשונים.

הגישה המעשית של ארגון "המדינה האסלאמית" לכינון המדינה אסלאמית מבדילה אותו מהגוף ממנו יצא – "אל־קאעדה" – שמצידו מציג חזון של הקמת מדינה אסלאמית כלל עולמית בטווח הארוך. ההוויה של "המדינה האסלאמית" היא ה"כאן ועכשיו". רק כך היא הצליחה להגשים את המטרה ארוכת הטווח שמעולם לא הושגה על ידי "אל־קאעדה" ושאר חסידי האידיאולוגיה הרדיקלית של הסלפיה – להשליט משטר אסלאמי לפי חוקי השריעה באמצעות קביעת עובדות בשטח והקמת מגנונים של ריבונות.

השימוש המושכל שעושה "המדינה האסלאמית" במרחב הקיברנטי אפשר לה "להיות בכל מקום" ברשת והביא ליצירת תחושות הזדהות ומשמעות רגשית בקרב תומכיה ולהתגייסות של צעירים רבים מכל רחבי העולם לאזורי הלחימה בסוריה ובעיראק. באותה דרך זכתה "המדינה האסלאמית", כאמור, בהבעת נאמנות של ארגונים סלפיים ג'יהאדיים שונים והקימה תאים של תומכיה ברחבי העולם המוסלמי ובקהילות מוסלמיות במערב.

השימוש של "המדינה האסלאמית" ברשת והשפעתו על המרחב הפיזי

מאז אמצע שנות השישים של המאה העשרים ישנה מגמה של חזרה לאסלאם במזרח התיכון. מגמה זו ניזונה משורה של תהליכים ונסיבות ששיקפו את חולשת האידיאולוגיות החילוניות, הלאומיות והסוציאליסטיות ואת אי־יכולתן להתמודד עם אתגרי המציאות החברתית והפוליטית בארצות ערב. בעקבות זאת התפתחה מגמה של השתלטות זהות אסלאמית על־מדינתית חזקה בחברה האזרחית (בעיקר באמצעות פעילות בשטח – מסגדים, מנגנוני צדקה ומרכזים קהילתיים), בעוד שהמסגרת המדינתית המשיכה לשלוט במדינות המוסלמיות והערביות באמצעות שפע כלים ששימשו לעיצוב נפשות הנתינים (חינוך, תקשורת ועוד).

תנועות סלפיות, בהובלת "האחים המוסלמים", שמו דגש על הטפה ופעילות חברתית מתוך המערכת השלטונית, תוך כדי שיתוף פעולה עם השליט והשלטונות והכרה לכאורה בהכרח שבקיומם, כחלק מתהליך השינוי הנדרש. בהמשך, על בסיס האידיאולוגיה של התנועה הסלפית שקידמה את רעיונות האסלאם הפוליטי, הלכה והתפתחה אידיאולוגיה קיצונית ואלימה בהרבה – הסלפיה־ג'יהאדיה.[15] אידיאולוגיה זו התאפיינה, בין השאר, באקטיביזם רבתי, כולל אלימות וג'יהאד מיליטנטי. כתוצאה מכך, ארגונים שזוהו עם תנועת הסלפיה־ג'יהאדיה נרדפו על

ידי מנגנוני הביטחון המדינתיים ונאלצו לעבור לפעילות חשאית וממודרת, תוך הקפדה על צמצום עקבות, כולל אלקטרוניים, שיכלו להביא לזיהוי פעילים. רוב התקשורת התנהלה במחשכים, בפורומים ג'יהאדיסטיים מאובטחים ובאמצעות רשתות תקשורת אנונימיות ומוצפנות. פעילי "אל־קאעדה", למשל, הרבו להשתמש למטרות תקשורת וגיוס בחדרי צ'ט מוצפנים, כולל בצ'טים של משחקי מחשב, כרטיסי "סים" חד־פעמיים וטלפונים לווייניים.[16] אוסמה בן לאדן אף השתמש בשליחים להעברת מידע, צעד שהקשה על המודיעין האמריקאי לאתרו במשך שנים.[17]

פיטר סינגר טוען כי מלחמת קרים הייתה המלחמה הראשונה בה נעשה שימוש בטלגרף, מלחמת וייטנאם הייתה מלחמת הטלוויזיה הראשונה, והמלחמות של ימינו הנערכות במקומות כמו סוריה ועיראק הן מלחמות בהן נעשה שימוש רחב בטכנולוגיית המדיה. לדברי סינגר, הצמיחה של פעילות ארגוני הג'יהאד ברשתות החברתיות מקבילה בהיקפה לצמיחה של השימוש שעושה הציבור הרחב במרחב הווירטואלי.[18]

היתרונות הגלומים בשימוש במרחב הסייבר נוצלו בעבר על ידי גורמי טרור במטרה להעביר מסרים מוצפנים, לגייס תומכים, לרכוש מטרות, לאסוף מודיעין, להסוות פעילות וכדומה. בעידן הרשת, ארגון טרור שרוצה לגדול ולגייס תומכים זקוק לפיתוח יכולות שיאפשרו לו להתגמש ולהשתנות במהירות, תוך התאמת מסריו לקהל יעד ממוקד או רחב. פעילי "המדינה האסלאמית" זיהו ברשתות החברתיות וביישומונים להעברת מסרים מיידיים כלי חיוני המאפשר לתקשר בין קבוצות ומכשירים שונים. כתוצאה מכך, הרשת משמשת את צורכי "המדינה האסלאמית" הן לתקשורת בין חברי הארגון והן כתשתית לתעמולה, ללוחמה פסיכולוגית ולגיוס פעילים. בנוסף, הרשת מאפשרת להשפיע על בודדים או קבוצות ולהסית אותם לביצוע פעולות טרור. יכולות אלו נותנות גמישות ומהירות, מאפשרות חתימה נמוכה, משמשות כמכפיל כוח להגברת התודעה ומאפשרות "להיות בכל המקומות כאשר אינך באמת בשום מקום".[19]

קמפיין עיצוב התודעה והתעמולה במרחב הסייבר אִפשר ל"מדינה האסלאמית" למתג עצמה בתוך זמן קצר כראש החץ של הג'יהאד העולמי. האסטרטגיה התקשורתית שלה היא בעיקרה פעילות ברשת בצורה מוחצנת, שמטרתה לגרום להפיכתה של הח'ליפות האסלאמית למוקד של משיכה והזדהות עבור אוכלוסיות מוסלמיות פוטנציאליות ברחבי העולם.

מסמך פנימי של מחלקת המדינה של ארצות הברית,[20] שדלף ל"ניו יורק טיימס" ביוני 2015, חשף את האתגרים הרבים של הממשל האמריקאי בבואו להילחם עם "המדינה האסלאמית" ברשת. ההערכה של גורמי מחלקת המדינה מצביעה על כך שהמדינות המעורבות בלחימה ב"מדינה האסלאמית" ברשת לא פועלות די

הצורך במשותף כדי לסכל את המשך הפצת ההודעות של הארגון. המסמך מצביע על חוסר אחידות במסרים, על היעדר שיתוף פעולה ועל קצב איטי ומסורבל של המאבק. מנגד, "המדינה האסלאמית" מגלה יעילות וזמן תגובה מהיר ברשת הרבה יותר מאלה של מעצמות טכנולוגיות כמו ארצות הברית, בריטניה ובעלות בריתן, ומצליחה בקלות יחסית לשמור על אחידות של מסרים.

מחקר של אהרון זלין (Zelin) מצביע על כך ש"המדינה האסלאמית" מפעילה יותר משלושים מרכזי מדיה שונים, הפעילים ב־24 מחוזות שבשליטת הארגון.[21] מרכזי המדיה מפרסמים בממוצע כ־18 מסרים תקשורתיים ביום (תמונות, סרטונים, באנרים, דוחות חדשותיים, שידורים ברדיו ונאומים) בלפחות שש שפות (הרוב בערבית, ולאחר מכן בסדר יורד באנגלית, רוסית, כורדית, צרפתית ואורדו).[22] מרבית המדיה שיצאה ממערך ההסברה והסייבר של "המדינה האסלאמית" ב־2013 הופקה והופצה על ידי מרכז תקשורת אחד ("אל־פורקאן מדיה"), ומאז היא נעשית בצורה מבוזרת. כיום ישנם כחמישה מרכזי מדיה מרכזיים הפועלים תחת זרוע ההסברה והתקשורת של "המדינה האסלאמית", והשאר הינם מרכזי מדיה מחוזיים.[23] לאחר הכנת המסרים, המשך הפעילות נעשה באמצעות הפצה דרך הרשתות החברתיות, פורומים ג'יהאדיסטיים, בלוגים ומיקרו בלוגינג, אתרי שיתוף סרטים ואתרי שיתוף תוכן. במהלך שנת 2014, אחד הכלים המרכזיים להפצת התכנים הוא באמצעות רשת טוויטר.

על פי מחקר של ברגר ומורגן (Berger & Morgan), מספר החשבונות הפעילים בשיא פעילותה של "המדינה האסלאמית" ברשת טוויטר, היה לא פחות מ־46,000 חשבונות של תומכים. מעגל פנימי של בין 500 לאלפיים חשבונות הוא של משתמשים "כבדים", הפועלים בצורה מתואמת ביניהם כדי למנף את היקף החשיפה של "המדינה האסלאמית" ולקדם את ההפצה הוויראלית שלה למעגלים חיצונים – ממוצע של עשרות שיתופים והעברות של מסרים ביום.[24] אמצעי נוסף להפצה הם אתרי מסרים מיידיים (כגון ווטסאפ וסנאפצט'), בהם ניתן להעלות ולהפיץ תמונות ובאנרים. אחד היתרונות הגדולים הנובעים משימוש בשיטה מבוזרת ומסוכרנת על ידי מערך ההסברה של "המדינה האסלאמית" הוא שימוש בפלטפורמות השונות שמציעה הרשת כ"פונדקאיות". כלומר, מיצוי המשאבים ברשת חברתית אחת (למשל בשל חסימת חשבונות הארגון ברשת חברתית מסוימת) מובילה למציאת רשת חברתית "פונדקאית" חדשה וחוזר חלילה. כך עברו פעילי "המדינה האסלאמית" משימוש ברשת טוויטר לרשתות חברתיות כגון KIK[25] ו־VK[26] ובהמשך לרשת החברתית טלגרם[27] (Telegram).[28]

דרכי ההפצה של "המדינה האסלאמית" במדיה החדשה נתמכות על ידי סיקור תקשורתי קבוע במדיה המסורתית, וזאת באמצעות ערוצי החדשות המסקרים אותה בצורה רציפה ומפרסמים את מסריה. במרבית הפעמים אין לעיתונאים

ולמערכות החדשות נגישות למידע ממקור ראשון על הנעשה בתוך אזורי השליטה של "המדינה האסלאמית", והם נאלצים להסתפק במסרים המוזנים על ידי מרכזי המדיה המרכזיים ומרכזי המדיה של המחוזות השונים. גם במקרים הנדירים שבהם מתאפשרת סקירת הנעשה במרחב הגיאוגרפי של "המדינה האסלאמית" בסוריה ובעיראק, ישנו פיקוח על התכנים, שלא מאפשר לעיתונאים סיקור אובייקטיבי של המציאות.

"המדינה האסלאמית" מנהלת "משטרת מחשבות" פנימית לדיכוי וסיכול ניסיונות של פעילי זכויות אדם ואחרים להוציא מתוך שטחי השליטה שלה חומרים מצולמים ואף עדויות של אזרחים.[29] מסריה מוצגים במונחי שחור ולבן, טובים ורעים והאסלאם נגד המערב. בסרטוני ההוצאה להורג של "המדינה האסלאמית", למשל, הקורבנות ייראו חלשים ומתועבים (הנשחט כורע על הברכיים כאשם כביכול במוות שהביא על עצמו), בעוד שהמוציא לפועל ייראה ויזואלית כגדול מהחיים. "המדינה האסלאמית" משיגה הצלחה תודעתית על ידי שליטה בצינורות המידע באזורים בהם היא נוכחת, והעולם נחשף אליה בדרך בה היא בוחרת. כמו כן, "המדינה האסלאמית" אוכפת את השימוש בויי פיי (Wi-Fi) בטריטוריה בשליטתה ולא מאפשרת שימוש ברשתות אלחוטיות פרטיות בתחומיה.[30]

בעבר, רוב התקשורת בין החברים בארגוני טרור ג'יהאדיסטיים לבין עצמם ובינם לבין מתגייסים פוטנציאליים הייתה נעשית במחשכים, באמצעות תקשורת מאובטחת. כיום, "המדינה האסלאמית" (ושחקנים לא מדינתיים אחרים) היא משתמשת "כבדה" בתקשורת גלויה, וזאת לגיוס, לתעמולה, ללוחמה פסיכולוגית ולשימושים נוספים. העידן הדיגיטלי מאפשר ל"מדינה האסלאמית" לפעול ברשת בדרכים שונות ומגוונות, כאשר השימושים העיקרים הם:

א. **עידוד הקצנה דתית** – פעילות זו מתבצעת במקביל לפעילות במסגדים ובמרכזים קהילתיים. התכנים העיקריים מועברים באמצעות כתבי עת,[31] סרטונים,[32] כרוזים ושירי דת (נשידים).[33] בשטחי השליטה של "המדינה האסלאמית" מתקיימים ערבי צפייה משותפת בסרטונים היוצאים ממרכזי המדיה של זרוע ההסברה שלה. בנוסף לכך, "המדינה האסלאמית" הקימה נקודות מדיה במספר ערים מרכזיות הנמצאות תחת שליטתה, והציבה בהן ישנם דוכנים להפצת חוברות, דיסקים ומכשירים לאחסון נתונים (USB) המיועדים להשפעה על ילדים ונוער.[34]

ב. **גיוס** – הרשת משמשת כמוקד משיכה לצעירים רבים בקהילות המוסלמיות ברחבי העולם. הטקטיקה אותה נוקטת "המדינה האסלאמית" לצורך גיוסם היא שיגור מסר אחיד ופשטני, הקורא לצעירים להגר למדינה האסלאמית או לבצע ג'יהאד במדינות המוצא שלהם.[35] פלטפורמות צ'טים מאפשרות למגייסי הארגון נגישות לצעירים רבים הנמשכים לסיפר (נרטיב) אותו מקדמת "המדינה

האסלאמית", וכן גיוס דרך הרשתות החברתיות, כולל גיוס של "אחד על אחד".[36] אמצעי נוסף לגיוס הוא מתן מענה למתעניינים חדשים בפורומים הפתוחים לקהל הרחב ובפורמט של שאלות ותשובות. "המדינה האסלאמית" משמשת מודל לחיקוי ולהשראה למספר רב של צעירים מקהילות מוסלמיות ברחבי העולם. מאז ההכרזה על כינונה ביוני 2014, ועד מארס 2015, הייתה עלייה של יותר משבעים אחוזים במספר הלוחמים הזרים שהיגרו לסוריה ולעיראק. מוקד משיכה אל "המדינה האסלאמית" נוצר מאז ביותר ממחצית ממדינות העולם.[37]

ג. **תקשורת בין חברים** – תוכנות מוצפנות מאפשרות לחברי "המדינה האסלאמית" לתקשר ביניהם ברשת בצורה מאובטחת ואנונימית.

ד. **לוחמה פסיכולוגית** – זו פועלת במספר ממדים, ובכלל זה פנייה אל אזרחים המתגוררים בשטחי השליטה של "המדינה האסלאמית" לצורך דיכוי והרתעה של חתרנות, וכן לסיכול ריגול פנימי, והפעלה בשדה הקרב באמצעות מנגנוני לוחמה פסיכולוגית ברשתות חברתיות, שיתוף סרטונים ופרסומים שנועדו להוריד את המוראל ואת רוח הלחימה של היריב.[38] הלוחמה הפסיכולוגית באה לידי ביטוי גם בסרטונים ובפרסומים (כתבי עת, שבועונים, באנרים וכדומה) המשמשים ככלים להשפעה על הציבור ועל מקבלי החלטות במדינות הנלחמות ב"מדינה האסלאמית".

ה. **איסוף מודיעין** – המדובר באיסוף נגד גורמים חתרניים, וכן להפעלת הרתעה ולוחמה פסיכולוגית נגד הכוחות הנלחמים ב"מדינה האסלאמית". הדבר נעשה, בין השאר, על ידי איסוף מידע ברשתות החברתיות, ולאחר מכן הפצתו כ"רשימת מטרות" של חיילים ומשפחותיהם (שמות, כתובות ומיילים). פעילות זו נתמכת על ידי תקיפות סייבר נגד אתרי מדיה ואתרים המזוהים כסמלי שלטון של היריב, וזאת כדי למנף את הסיקור התקשורתי ולהביא לחשיפה תקשורתית של "רשימת המטרות". הדבר נועד ליצור אצל המופיעים באותן רשימות חרדה ומורא מפני תקיפות טרור.[39]

ו. **סייבר טרור** – "המדינה האסלאמית" מפעילה זרועות של לוחמת סייבר נגד אתרים המזוהים עם השלטון ונגד ערוצי תקשורת שנבחרו לתקיפה, וזאת במטרה למקסם את החשיפה התקשורתית בחתימה נמוכה יחסית.[40] עד כה הסתכמה לוחמת הסייבר של הארגון בתקיפות פשוטות יחסית, שכללו השחתת אתרים והתקפות מניעת שירות.

ז. **הפעלת טרור מאורגן** – הרשת מאפשרת תקשורת בטוחה יחסית לצורך הקמה של תאי טרור, וכן תקשורת בין פעילים החוזרים למדינות המוצא שלהם משטחי הלחימה בסוריה ובעיראק. כך נעשה שימוש בטלפונים סלולריים לתקשורת בין המפגעים שביצעו את סדרת פיגועי הטרור בפריז בחודש נובמבר 2015.[41]

ח. **הסתה והשפעה על פיגועי טרור ספונטני ולא מאורגן** – דפוס הפעולה של ביצוע פיגועי טרור המכונה "טרור זאבים בודדים" נטוע עמוק בארגונים הנמנים על זרם האסלאם הסלפי. חברי זרם זה רואים חובה וייעוד להשתתף במאבק אלים נגד "אויבי האסלאם", הן במדינתם והן מחוץ לגבולותיה.[42] פיגועי טרור על ידי מעריצי "המדינה האסלאמית", שאירעו בארצות הברית, בקנדה, באוסטרליה, בדנמרק, בכווית, בתוניסיה ובצרפת בשנים 2014–2015, משקפים את יכולת הארגון להשפיע באמצעות המדיה החברתית על יחידים או קבוצות קטנות לבצע פיגועי "זאבים בודדים" בעולם המערבי. המכנה המשותף למבַצעי פיגועים אלה הוא גלישה ברשתות חברתיות, בהן הם מושפעים ממסרי הארגון. ואכן, רוב הפיגועים מסוג זה אירעו מאז ש"המדינה האסלאמית" קראה למוסלמים במערב לבצע פעולות טרור נגד כוחות הביטחון של מדינות המערב ואזרחיהן.[43] יש לציין, כי גם במקרי רצח שבהם המפַגעים לא קיבלו על עצמם את האחריות בשם "המדינה האסלאמית", ניתן לראות בהשפעתם של תכני ההסתה של הארגון מוטיבציה לביצוע הרצח.[44]

האסטרטגיה של זרועות המדיה והסייבר של "המדינה האסלאמית" לא שונה מזו של חברות עסקיות, בכך שהיא הטמיעה בפלטפורמות התקשורת השונות שלה את השימוש ברשת לטובת פעולה במרחב הפיזי. כך יכול הארגון לעודד רדיקליזציה במסגדים ובמרכזי קהילה מוסלמיים תוך כדי פעילות ברשתות החברתיות, ולהפיץ ברשת האינטרנט את המסרים שנועדו ליצור הרתעה ולוחמה פסיכולוגית. הוא עושה זאת תוך שימוש בקמפיינים לגיוס המונים, כגון הקמפיין בעל הכותרת "מיליארד מוסלמים תומכים ב'מדינה האסלאמית'".[45] היה זה קמפיין ששיקף את בחירתה של "המדינה האסלאמית" לפעול בגלוי ובצורה ממוקדת בערוצי המדיה החברתית למטרות גיוס לשורותיה, תוך הקמת תשתית של מגייסים הפועלים בשטח ומסייעים למתגייסים הפוטנציאליים במידע, במשאבים ובהכוונה.

"המדינה האסלאמית" מצליחה לשלוט במאבק על התודעה באמצעות הוויה שהיא מעצבת בעצמה. כך, העולם רואה את הנעשה בסוריה ובעיראק דרך העיניים של "המדינה האסלאמית", ואין למעשה מנגנונים אחרים שיאפשרו הסתכלות אובייקטיבית יותר על המציאות. בכך היא מצליחה לייצר פער תודעתי בין ה"ראייה" במובנה התפיסתי הצר לבין מתן פרשנות ל"מה שרואים", תהליך המחייב תהליכים קוגניטיביים רחבים יותר.

שינויים מבוססי רשת בארגוני טרור

ארגוני טרור שהביעו נאמנות ל"מדינה האסלאמית", כגון "בוקו חראם" בניגריה ו"אנצאר בית אל־מקדס" בחצי האי סיני, החלו גם הם לנהל עד מהרה מערכות תקשורתיות, כולל הפקה והפצה של סרטונים דומים לסרטוני ההוצאה להורג של

"המדינה האסלאמית".[46] גם ארגוני טרור אחרים החלו בתהליך למידה של שיטות הפעולה של "המדינה האסלאמית" ופרסמו סרטונים, כתבי עת ומסרים כחלק מקמפיינים תודעתיים, תעמולה ולוחמה פסיכולוגית.[47] ארגון חזבאללה בלבנון, למשל, בנה תשתית תקשורתית למאבק על התודעה. תשתית זו כוללת למעלה מעשרים אתרי אינטרנט בשבע שפות, חלקם אתרים חדשותיים וחלקם אתרים ייעודיים. חזבאללה גם עושה שימוש ברשתות החברתיות הזרות וביוטיוב, אך בהיקף נמוך יחסית ל"מדינה האסלאמית".[48] חזבאללה גם מקשה על אופן הסיקור התקשורתי בשטחים שבשליטתו ורודף פעילי זכויות אדם ואופוזיציה המנסים להפיץ תמונה אובייקטיבית יותר של המציאות.

ארגוני טרור המזוהים עם "אל־קאעדה" מנצלים את שלל האפשרויות הגלומות ברשתות החברתיות והגבירו את נוכחותם ברשת. "אל־קאעדה" כבר מפעיל מזה מספר שנים כתבי עת מקוונים בשפה האנגלית, כגון "Inspire" (שיצא לאור לראשונה ב־2010), וזאת לצורכי תעמולה, גיוס, הכוונה ולימוד של תומכים המעוניינים להצטרף לשורות הארגון.[49] ככלל, "אל־קאעדה" פעיל מאוד ברשת, ותכניו מופצים באתרי שיתוף תוכן וכן בפורומים סגורים.[50] אוסמה בן לאדן, מייסד "אל־קאעדה", נחשב לדור הראשון בהתפתחות התעמולה הג'יהאדיסטית המודרנית. קלטות של נאומיו הופצו לחברות החדשות והביאו לחשיפה גבוהה שלו ושל ארגונו בציבור. מערכת ההפצה והשיווק של דימוי העוצמה של הארגון השתכללה עם השנים כאשר, בנוסף לפעילות חברת ההפקה של הארגון – "אל סחאב" – טרחו חברי הארגון ואוהדיו להפיץ מספר רב של תקליטורי תעמולה ולהקרינם במאות רבות של אתרי אינטרנט.[51]

הדמות הבולטת ביותר בדור השני של "אל־קאעדה" היה אנוור אל־עולקי, שפנה אל אנשי המערב באנגלית באמצעות סרטוני יוטיוב, בלוג ועמוד פייסבוק.[52] "ג'בהת א־נוסרה" (כאמור, זרוע של "אל־קאעדה" בסוריה) מפיצה סרטונים ופעילה ברשתות החברתיות, וכמוה גם ארגוני מורדים סוריים "מתונים", כגון "ג'יש אל־אסלאם" ("צבא האסלאם"), שאף הפיץ ברשת סרטון הוצאה להורג של פעילי "המדינה האסלאמית".[53]

"המדינה האסלאמית" משמשת השראה גם לארגוני טרור פלסטיניים. אלה לומדים משיטות הארגון כיצד ליצור חשיפה מרבית ברשת ובמדיה כדי להעביר מסרים ולגייס תומכים ופעילים. ארגוני הטרור הפלסטיניים אף החלו לפרסם קמפיינים של הסתה ברשת, שמטרתם להשפיע על מַגָעים לא מאורגנים ("טרור זאבים בודדים" או "טרור ספונטני"). כך, חמאס והג'יהאד האסלאמי ניהלו קמפיינים ברשתות החברתיות, שכָּללו הפצת סרטונים ותמונות עם קריאה לדקור אזרחים יהודים, וחיילי צה"ל בפרט.[54] חמאס גם מפעיל מנגנוני בקרה על חומרים תקשורתיים היוצאים מתחומיו במטרה לשלוט במאבק התודעתי נגד ישראל.

לדוגמה, בינואר 2015 התרחש פיגוע דקירה באוטובוס קו 40 בתל אביב. בחקירתו טען המחבל הדוקר כי יצא לבצע את הפיגוע על רקע תסכול ממבצע "צוק איתן" ואירועים אלימים להם נחשף בתקשורת במזרח ירושלים, ולאחר צפייה בתכנים אסלאמיים קיצוניים שבהם שודרו התבטאויות בשבח "ההגעה לגן עדן".[55]

שני הקמפיינים הגדולים ביותר ברשתות החברתיות בזירה הפלסטינית בחודשים נובמבר ודצמבר 2014 היו "אדעס" (מהמילה בערבית "דריסה", שצלילה דומה ל דאע"ש) ו"אטען" (מהמילה בערבית דקירה). סִמלו של קמפיין זה היה תמונה של צעירים פלסטיניים העורפים ראשים בגרזן. הקמפיינים אפשרו לעומדים מאחוריהם ליצור השפעה פסיכולוגית של טרור ולערער את תחושת הביטחון בציבור הישראלי, וזאת תוך השקעת מאמץ מינימלי וללא צורך ביצירת מסה קריטית של התארגנות פעילים ובניית תשתית מודיעינית לביצוע פיגועים.[56]

בהשוואה לארגוני הטרור האחרים, "המדינה האסלאמית" ביצעה את קפיצת המדרגה הטכנולוגית והתקשורתית המתקדמת ביותר. היא הקימה תשתית מאורגנת היטב ברשתות החברתיות, כגון פיתוח יישומונים, פרסום מדריכים שונים ב־JustPaste, הפצת הודעות שמע ב־SoundCloud, שיתוף תמונות ב־Instagram ו־Snapchat, הפצת סרטונים ב־WhatsApp והעלאת שירי דת (נשידים) ב־YouTube. למרות ניסיונות של מדינות, תאגידי מדיה וחברות אינטרנט להילחם בתופעה זו, "המדינה האסלאמית" משתמשת בכלים טכנולוגיים לעקיפת החסמים ונשארת רלוונטית ולאורך זמן בתודעה התקשורתית ובמדיה החברתית. בכך היא מקדימה בשנות אור את ארגוני הטרור האחרים, שטרם למדו לשווק ולהפיץ תכנים בצורה ויראלית רחבה וחסרים את המשאבים הרבים המצויים בידי "המדינה האסלאמית".

ניתן להניח כי "המדינה האסלאמית" פועלת במדיה החברתית בצורה ממוקדת כלפי אוכלוסיות יעד מפולחות, תוך שימוש בכלים לניהול קמפיינים, אופטימיזציה תמידית ומעקב אחר ביצועים. גורמים נוספים מעורבים שלא בידיעתם בקמפיינים אלה במרחב הקיברנטי ומשמשים ככלי משמעותי לקידומם. המדובר בחברות מדיה חברתית (כגון פייסבוק) ובחברות מנועי חיפוש (כגון גוגל). חברות אלו מנתחות את הקלדות המשתמשים ובונות מאגרי מידע עצומים לניתוח ההתנהגותי של הגולשים ברשת. "הלקוחות" הופכים להיות נתונים שיניבו רווחים. הדבר נעשה על ידי החלפת מידע עם חברות עסקיות המעוניינות בקטגוריות של התנהגות צרכנית כזו או אחרת, כמו דעות, תשוקות ורצונות. מידע זה יכול לשמש כאמצעי נוסף להפצה ויראלית גם עבור "המדינה האסלאמית" על ידי הצעת העדפות לצרכנים, כולל תכנים הקשורים לארגון, כגון סרטונים, שירים, דפי תוכן וכדומה.

סיכום

רשת האינטרנט בכלל והרשתות החברתיות בפרט הפכו לגורם המשפיע ביותר על התנהגות החברה האנושית במציאות של ימינו. החיים ברשת והחיים מחוץ לרשת נהיו חלק ממארג אחד. במציאות בה מוסרות המחיצות בין העולם הפיזי לעולם הקיברנטי, השילוב בין רגשות לתכנים ברשת יכול להשפיע על התודעה. באותו אופן, פעילות ארגוני הטרור במרחב הקיברנטי משפיעה על פעולות טרור בעולם הפיזי. בעידן הרשת, ארגון טרור שרוצה להשיג מטרות פוליטיות ולגייס תומכים, זקוק לפיתוח יכולות שיאפשרו לו להתגמש ולהשתנות במהירות, תוך התאמת מסריו לקהל יעד ממוקד או רחב.

"המדינה האסלאמית" פועלת בשלושה מרחבי פעולה – גיאוגרפי, תודעתי וקיברנטי. היא זיהתה ברשתות החברתיות צורך חיוני, והדבר משמש אותה לתקשורת בין פעילים, אך גם כתשתית לתעמולה, ללוחמה פסיכולוגית ולגיוס פעילים. הרשת גם מנוצלת על ידיה להשפעה ולהסתה של בודדים או קבוצות לביצוע פעולות טרור. ארגוני הטרור האחרים לומדים ממודל מצליח זה ופועלים להשגת יכולות דומות.

ככל שיגברו מאמצי מדינות שונות לחסום את ההגירה הפיזית לתוכן ולסגור את גבולותיהן בפני המתגייסים ל'המדינה האסלאמית', כך תגדל הסבירות להגברת מאמציה במרחב הקיברנטי חסר הגבולות. מאמצים אלה עשויים לכלול הפניית משאבים לבניית יכולות לוחמת סייבר התקפיות אסטרטגיות ולגיוס קהילות של פצחנים (האקרים) במדינות המוצא של המתגייסים לארגון. מגמה נוספת שעלולה להתפתח כתוצאה ממאמציהם של ארגוני מודיעין לנטר ולזהות פעילות רשתית של פעילי "המדינה האסלאמית" במרחב הקיברנטי, היא מעבר של פעילי הארגון ותומכיו מפעילות מוחצנת ברשת לפעילות "מתחת לפני השטח". המדובר בהסתמכות על טכנולוגיות להצפנה מסחרית שהן בעלות מאפיינים דו־שימושיים, וכן על רשתות "אפלות" (Darknet/TOR), ושימוש מסיבי בהן.

אחד האתגרים העיקריים הניצבים בפני סוכנויות ביון וארגוני מודיעין כתוצאה מהתגברות השימוש ברשת על ידי ארגוני טרור, הוא גיבוש כלים חדשים לדליית מידע, לניטור ולאכיפה ברשתות החברתיות. זאת, לצורך סיכול טרור והסתה המובילה לפיגועי טרור, וכן לקידום פעילות אופרטיבית מול מַפגִעים פוטנציאליים. לכן, יש צורך לנהל מערכה פרו־אקטיבית, שתדע לאתר באמצעות כלים טכנולוגיים את בעלי הפוטנציאל לביצוע פיגועי טרור ותפעל בצורה התקפית לפגוע במקורות ההסתה ברשת ולסכל אותם. במקומות רבים בעולם לא קיימת הנחייה ברורה כיצד לפעול נגד פעילות טרור ברשת, והדרך לפעילות משפטית ולאכיפה משמעותיות בתחום זה, כולל גיבוש חקיקה ואכיפה נגד הקצנה והסתה לטרור המבצעת ברשת, עודנה ארוכה. השלב הראשון בגיבוש מדיניות שתטפל בכך הוא בהוכחת הקשר

בין הסתה לטרור דרך הרשת ובין הפיכתה ל"מנוע" לביצוע פיזי של פיגועי טרור מצד גורמים שאינם משויכים לארגוני טרור.

"המדינה האסלאמית" הצליחה לבנות סיפּר וזוכה לתשומת לב תקשורתית וציבורית מחוץ לנעשה בשטחים שבשליטתה. היא גם הצליחה להסיט את הקשב התקשורתי והציבורי מהמציאות הקיימת בשטחים אלה (דיכוי אוכלוסייה, הוצאות להורג, בעיות כלכליות ורעב, הפסדים בקרבות וכדומה). כדי לצמצם את מרחבי ההשפעה והנוכחות הגלובלית של "המדינה האסלאמית", יש למצוא מנגנונים וכלים ל"ריווח המרחב והזמן", שיחזירו לגודלו המקורי את הנפח התודעתי הגלובלי שהיא תופסת. זאת, תוך כפייה עליה לפעול במרחבים מוגבלים, בהם השפעתה תלך ותפחת ותופנה כלפי קהלי יעד מצומצמים.

"המדינה האסלאמית" הינה תופעה גלובלית, ולכן גם מהווה איום גלובלי. כמענה לאיום זה יש להרחיב את היריעה מבחינה תפיסתית ולהבין שלא מדובר רק באתגר מודיעיני־צבאי, אלא בתופעה חברתית ותרבותית רחבת ממדים, שאין אפשרות לטפל בה רק באמצעים קיברנטיים או קינטיים. אמנם, כבר מתבצעת פעילות של מדינות שונות להציב "סיפר נגדי" (Counter Narrative) מול השימוש של "המדינה האסלאמית" במרחב הקיברנטי, אך פעילות זו מוגבלת ומתרכזת בעיקרה בצמצום הגיוס ל"מדינה האסלאמית" ממדינות המערב ובהקצנה הדתית המתרחשת ברשת. במציאות הנוכחית, בה ההוויה של "המדינה האסלאמית" היא שקובעת את התודעה, יש להקצות משאבים לעיצוב התודעה ולהשפעה תודעתית. במסגרת זו נדרשת מערכה תודעתית וקיברנטית שתכלול פעילות אופרטיבית במרחב הגיאוגרפי שנמצא בשליטת "המדינה האסלאמית". פעילות כזו יכולה לכלול קמפיינים של לוחמה פסיכולוגית, אך בעיקר הכשרת אנשי אמון מקומיים המתנגדים ל"מדינה האסלאמית" והפיכתם ל"סוכני ידע" שישתמשו בכלים טכנולוגיים בעלי חתימה נמוכה, אנונימיות ואיכות ויזואלית גבוהה להפקת חומרי תוכן, מודיעין ודיווחים אובייקטיביים. אלה יופצו בצורה גלובלית, אך גם בצורה ממוקדת לקהילות ברחבי העולם בהן יש פוטנציאל להתגברות השפעתה של "המדינה האסלאמית".

גיבוש כלים יעילים לשימוש נגד "המדינה האסלאמית" יוכל לסייע כמענה גם לאתגר שמציבים שחקנים לא מדינתיים וארגוני טרור אחרים, המקבלים השראה מתופעת "המדינה האסלאמית" ומאמצים טכניקות דומות לפעילות טרור, ובכלל זה בשלושת מרחבי הפעולה שלה – הגיאוגרפי, הקיברנטי והתודעתי. הפצצות הקואליציה נגד "המדינה האסלאמית" מצליחות לסכל פעילות בשטחי הלחימה בסוריה ועירק, כולל חיסול של מספר גדול של פעילי "המדינה האסלאמית". אך פעילות זו לא מצליחה להוריד את מספר הפעילים בשל זרם המתגייסים החדשים שממלאים את השורות. על מנת להוריד את מספר המתנדבים המתגייסים לשטחי

"המדינה האסלאמית" לא מספיק לסגור גבולות פיזיים, פעילות שלא הוכיחה עצמה עד כה, אלא יש להוריד את המוטיבציה של מתגייסים פוטנציאליים לפנות לדרך הג'יהאד. ניתן להשיג יעד ברמה התודעתית, על ידי קעקוע הנרטיב של "המדינה האסלאמית" וה'אוטופיה' המעוותת שהיא מציגה. לצורך כך ישנו צורך בניהול מערכה שתכלול פעילות פרו אקטיבית של לוחמת סייבר משולבת עם לוחמת נרטיב.

הערות

1 להרחבה על המושג "דחיסת מרחב וזמן" ראו: David Harvey, *The Condition of Postmodernity* (Mass: Blackwell, 1989); אבי רוזן, **דחיסת מרחב וזמן באמנות הסייברספייס**, חיבור לשם קבלת התואר "דוקטור לפילוסופיה", אוניברסיטת תל אביב, אלול תשס"ט, http://www.sipl.technion.ac.il/~avi/tsc/avi_rosen_TSC.pdf.

2 המושג "אונליין־אופליין" בעולם העסקי מתייחס לשילוב בין אסטרטגיית השיווק והמיתוג בעולם האמיתי (מחוץ לרשת) ובין אסטרטגיית השיווק באינטרנט (בתוך הרשת). המטרה היא ליצור אחידות במרחבי הפעולה, ובכך להשיג חשיפה מרַבית עבור קהל יעד מוגדר.

3 Mahmoud Salem, "You Can't Stop the Signal," *World Policy Journal*, Fall 2014, http://www.worldpolicy.org/journal/fall2014/you-can't-stop-the-signal

4 דניאל כהן ורן לוי, "מחאת המטריות הוירטואליות", **שורטי**, המכון למחקרי ביטחון לאומי, 26 בפברואר 2015, http://heb.inss.org.il/index.aspx?id=5193&Blogid=8860

5 אשר עידן, "ההמון מסתער", **אודיסאה**, גיליון 16, יולי 2012, http://odyssey.org.il/224643.

6 "Number of social network users worldwide from 2010 to 2018 (in billions)," *Statista*, http://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/.

7 רוזן, **דחיסת מרחב וזמן באמנות הסייברספייס**, עמ' 16.

8 Roy Ascott, "From Appearance to Apparition: Communications and Consciousness in the Cybersphere," in *FISEA*, ed. Roman Verostko (Minneapolis College of Art and Design, 1993), pp. 1-8.

9 דניאל כהן, **בין מדינה אסלאמית דתית למדינה לאומית חילונית**, עבודת גמר לקראת התואר "מוסמך אוניברסיטה", אוניברסיטת תל אביב, אוקטובר 2012, עמ' 43.

10 ע' סיוון, "התנגשות בתוך האסלאם", בתוך: **הקרב של המאה ה־21: דמוקרטיה נלחמת בטרור**, חיים פס, עורך (ירושלים: המכון הישראלי לדמוקרטיה, תשס"ז, 2006), עמ' 48–51.

11 "ראש 'אל־קאעדה' למפגינים הסורים: צאו נגד ישראל", וואלה, 28 ביולי 2011, http://news.walla.co.il/item/1845055

12 יורם שוויצר ואביב אורג, **האודיסיאה של "אל־קאעדה" אל הג'יהאד העולמי**, מזכר 132, תל אביב: המכון למחקרי ביטחון לאומי, ינואר 2014, עמ' 47, http://www.inss.org.il/uploadImages/systemFiles/memo132f.pdf

13 Jessica Stern and J. M. Berger, *ISIS: The State of Terror* (Harper Collins Publishers, 2015), p. 157.

14 תרגום לאנגלית של נאום ההכתרה של מנהיג "המדינה האסלאמית": https://ia902501.us.archive.org/2/items/hym3_22aw/english.pdf

15 שוויצר ואורג, **האודיסיאה של "אל־קאעדה"**, עמ' 18.

16 Frank Gardner, "How do terrorists communicate," *BBC*, November 2, 2013, http://www.bbc.com/news/world-24784756

17 שם.

18 Mustapha Ajbaili, "How ISIS conquered social media," *Al Arabiya*, June 24, 2014, http://english.alarabiya.net/en/media/digital/2014/06/24/How-has-ISIS-conquered-social-media-.html

19 Celeste Olalquiaga, *Megalopolis: Contemporary Cultural Sensibilities* (Minneapolis: University of Minnesota Press, 1992), p. 6.

20 Mark Mazzeti and Michael Gordon, "ISIS Is Winning the Social Media War, U.S. Concludes," *The New York Times*, June 12, 2015, http://www.nytimes.com/2015/06/13/world/middleeast/isis-is-winning-message-war-us-concludes.html?_r=0

21 על פי המחקר שפורסם באוגוסט 2015, "המדינה האסלאמית" טוענת לשליטה על כ־32 מחוזות הכוללים: עשרה מחוזות בעיראק, שבעה בסוריה, שניים בגבול עיראק־סוריה, חמישה בתימן, שלושה בלוב, שניים בערב הסעודית, אחד באלג'יריה, אחד בגבול אפגניסטן־פקיסטן ואחד בניגריה. ראו:
Aaron Y. Zelin, "Picture or It Didn't Happen: A Snapshot of the Islamic State's Official Media Output," *Perspectives on Terrorism*, Volume 9, Issue 4 (August 2015), p. 87, https://www.washingtoninstitute.org/uploads/Documents/opeds/Zelin20150807-Perspectives.pdf

22 שם. עמ' 88.

23 שם.

24 J.M. Berger and Jonathon Morgan, "The ISIS Twitter census: Defining and describing the population of ISIS supporters on Twitter," Brookings, March 2015, http://www.brookings.edu/~/media/research/files/papers/2015/03/isis-twitter-census-berger-morgan/isis_twitter_census_berger_morgan.pdf

25 http://www.kik.com

26 https://vk.com

27 Pamela Engel, "ISIS has figured out ways to get around restrictions on one of the main apps it uses for propaganda," *Business Insider*, November 24, 2015, http://www.businessinsider.com/isis-telegram-channels-2015-11

28 https://telegram.org

29 "ISIS publically executes Iraqi human rights activist for Facebook posts condemning terrorists' destruction: UN," *New York Daily News*, September 25, 2014, http://www.nydailynews.com/news/world/isis-publically-executes-human-rights-activist-article-1.1952281

30 Pamela Engel, "How ISIS monitors and restricts internet access in the 'caliphate'," November 7, 2015, http://www.businessinsider.com/how-isis-governs-its-caliphate-2015-11

31 Aaron Y. Zelin, "al-Ḥayāt Media Center presents a new issue of the Islamic State's magazine: 'Dābiq #10'," *Jihadology*, July 13, 2015, http://jihadology.net/category/dabiq-magazine

32 "Videos: How ISIS Recruits Around the World," *The New York Times*, August 21, 2015, http://www.nytimes.com/interactive/2015/08/21/world/videos-isis-recruits.html?_r=0

33 מ' שמש, "שירי המדינה האסלאמית – מכשיר לקידום רעיון הח'ליפות", ממר"י, 13 באוגוסט 2015, http://www.memri.org.il/cgi-webaxy/sal/sal.pl?lang=he&ID=875141_memri&act=show&dbid=articles&dataid=3941.

34 Zelin, "Picture or It Didn't Happen," p. 86.

35 "Canadian ISIS Fighter to Muslims in Canada: You Have a Religious Duty to either Emigrate to The Islamic State, or else Carry Out Attacks in Canada," MEMRI, December 8, 2014, http://www.memrijttm.org/canadian-isis-fighter-to-muslims-in-canada-you-have-a-religious-duty-to-either-emigrate-to-the-islamic-state-or-else-carry-out-attacks-in-canada.html

36 Rukmini Callimachi, "ISIS and the Lonely Young American," *The New York Times*, June 27, 2015, http://www.nytimes.com/2015/06/28/world/americas/isis-online-recruiting-american.html

37 United Nations Security Council, "Analysis and recommendations with regard to the global threat from foreign terrorist fighters," May 19, 2015, http://www.un.org/en/ga/search/view_doc.asp?symbol=S/2015/358

38 Jillian Kay Melchior, "ISIS Tactics Illustrate Social Media's New Place in Modern War," *techCrunch*, October 15, 2014, http://techcrunch.com/2014/10/15/isis-tactics-illustrate-social-medias-new-place-in-modern-war/

39 Dugald McConnell and Brian Todd, "Purported ISIS militants post list of 1,400 U.S. 'targets'," *CNN*, August 14, 2015, http://edition.cnn.com/2015/08/13/world/isis-militants-american-targets/

40 Josh Constine, "ISIS 'Cyber Caliphate' Hacks U.S. Military Command Accounts, *techCrunch*, January 12, 2015, http://techcrunch.com/2015/01/12/cyber-caliphate/

41 The Monde.fr, On est parti on commence »: le SMS trouvé dans le téléphone portable d'un membre du commando, November 18, 2015, http://www.lemonde.fr/attaques-a-paris/article/2015/11/18/le-telephone-portable-d-un-membre-du-commando-trouve-pres-du-bataclan-a-permis-de-remonter-a-alfortville_4812515_4809495.html

42 על שיטות הפעולה ויתרונותיה ניתן ללמוד ממסה שנכתבה על ידי אבו מסעב אל־סורי, אחד מאנשי המבצעים המשפיעים ביותר על שיטות הפעולה של "אל־קאעדה" ושל ארגוני ג'יהאד עולמי אחרים: https://archive.org/stream/TheGlobalIslamicResistanceCall/The_Global_Islamic_Resistance_Call_-chapter_8_sections_5_to_7_LIST_OF_TARGETS#page/n0/mode/2up

43 John Hudson, "FBI Director: For Would-Be Terrorists, Twitter is the 'Devil on their Shoulder'," *Foreign Policy*, July 8, 2015, http://foreignpolicy.com/2015/07/08/fbi-director-for-would-be-terrorists-twitter-is-the-devil-on-their-shoulder/?utm_source=Sailthru&utm_medium=email&utm_term=*Editors%20Picks&utm_campaign=New%20Campaign

44 "דנמרק: בת 15 צפתה בתוכנית ההסתה של דאע"ש ורצחה את אמה", *Ynet*, 16 בספטמבר 2015, http://www.ynet.co.il/articles/0,7340,L-4700789,00.html

45 המדובר בקמפיין שיזם תומך דאע"ש ב־19 ביוני 2014 באמצעי המדיה השונים, זמן קצר לאחר הכיבוש האסטרטגי של העיר מוסול בעיראק ומספר ימים לפני ההכרזה על הקמת הח'ליפות האסלאמית. הקמפיין זכה להצלחה ולגילויי תמיכה ברחבי העולם, שפורסמו על רקע צילומים של אתרים שונים. ראו: Henri Tartaglia, "German ISIS Supporters Started a Jihadist Social Media Campaign," *VICE News*, June 20, 2014, http://www.vice.com/read/german-jihadi-internet-meme-campaign

46 Jay Akbar, "Like master, like servant: Nigerian terror group Boko Haram releases first beheading video since pledging allegiance to ISIS," *Daily Mail*, July 10, 2015, http://www.dailymail.co.uk/news/article-3156551/Like-master-like-servant-Nigerian-terror-group-Boko-Haram-releases-beheading-video-pledging-allegiance-ISIS.html#ixzz3kaEa4HBS

47 ראו למשל סרטון של חמאס כחלק ממסע תעמולה ולוחמה פסיכולוגית: ירון שניידר, "חמאס מציג: תיעוד חדש של יחידת לוחמי המנהרות", ערוץ 2, 27 באוגוסט 2015, http://www.mako.co.il/news-military/security-q3_2015/Article-ad8d86659ad6f41004.htm

48 מרכז המידע למודיעין וטרור ע"ש אלוף מאיר עמית, "טרור ואינטרנט: תשתית אתרי האינטרנט של חזבאללה והחברות התומכות בה", 4 במארס 2013, http://www.terrorism-info.org.il/he/article/20488

49 אלינור פוקס, "מסמרים, צינור ביוב וסיר לחץ: כך אל־קאעידה מלמדים להכין פצצה ביתית", מאקו, 17 באפריל 2013, http://www.mako.co.il/nexter-internet/Article-c04fbab1a771e31006.htm

50 ראו לדוגמה הפצת סרטונים על מנגנוני תקשורת המזוהים עם "אל־קאעדה": אוריאל קוך, "וידאו חדש של אל־שבאב אל־מג'אהדין: תיעוד המתקפה על בית המשפט ובניין הפרלמנט במוגדישו", *Online Jihad Exposed*, 9 בינואר 2015, http://www.onlinejihadexposed.com/2015/01/blog-post_9.html

51 יורם שוייצר ואביב אורג, **האודיסיאה של אל־קאעדה אל הג'יהאד העולמי**, עמ' 25.

52 סקוט שיין ובן האברד, "הנשק הלא כל כך סודי של המדינה האיסלאמית" (תרגום מ"ניו יורק טיימס"), **הארץ**, 31 באוגוסט 2014, http://www.haaretz.co.il/captain/net/.premium-1.2420978

53 "סוריה: 'ג'יש אל־אסלאם' הוציא להורג 18 מאנשי דאע"ש", *Arab Sensor*, 1 ביולי 2015, http://www.arabsensor.co.il/%D7%A1%D7%95%D7%A8%D7%99%D7%94-%D7%92%D7%99%D7%A9-%D7%90%D7%9C-%D7%90%D7%A1%D7%9C%D7%90%D7%9D-%D7%94%D7%95%D7%A6%D7%99%D7%90-%D7%9C%D7%94%D7%95%D7%A8%D7%92-18-%D7%9E%D7%90%D7%A0%D7%A9%D7%99

54 מתן חצרוני, "למה לנסראללה אין טוויטר?", ערוץ 2 באינטרנט, 1 בינואר 2015, http://www.mako.co.il/news-military/security-q1_2015/Article-a01a488571aaa41004.htm

55 אמיר בוחבוט ואבי אשכנזי, "המחבל מתל אביב: 'עשיתי את הפיגוע בגלל צוק איתן'", וואלה, 21 בינואר 2015, http://news.walla.co.il/item/2821840

56 אודי דקל, "הטרור בבית הכנסת בירושלים – ממאבק לאומי למלחמת דת?", **מבט על**, גיליון 633, המכון למחקרי ביטחון לאומי, 20 בנובמבר 2014, http://heb.inss.org.il/index.aspx?id=4354&articleid=8133

תפקידן ואחריותן של ממשלות בהגנה על קניין רוחני דיגיטלי

רון שחר

ההתפתחות המהירה של מרחב הסייבר הובילה להתגברות האיום של גניבת קניין רוחני בכלל וסודות מסחריים דיגיטליים פרטיים ומסחריים בפרט. המדובר בגניבה המתרחשת בדרך קיברנטית ונובעת ממניעים פליליים. לסוג זה של פשעי סייבר יכולה להיות השפעה קריטית על המערכת המקרו־כלכלית הבין־לאומית, לרבות פוטנציאל לאובדן של הכנסות עתק ממסים ולצניחה בתמ"ג. מרבית המדינות ניסחו דוקטרינה אסטרטגית להגנת סייבר במטרה להגן על התשתיות הקריטיות הפיזיות שלהן כנגד לוחמת סייבר פוליטית. לעומת זאת, למרביתן אין עדיין דוקטרינה, חקיקה ואמצעים מתאימים להגנה על קניין רוחני דיגיטלי כנגד פשעי סייבר הנעשים ממניעים פליליים. הגישה המיושנת של ענישה על פשעי סייבר לאחר התרחשותם אינה רלוונטית, שכן מרחב הסייבר מקשה בכל מקרה על זיהוי גניבת הקניין הרוחני בזמן אמת.

מאמר זה בוחן האם ההשלכות המקרו־כלכליות של המגמות הגוברות והולכות של גניבה במרחב הסייבר יביאו להגדרת הקניין הרוחני הדיגיטלי, הפרטי והמסחרי, כתשתית קריטית, כזו הזקוקה להגנה ממשלתית פרואקטיבית.

מילות מפתח: קניין רוחני דיגיטלי, גניבת סייבר, תשתית קריטית, אחריות ממשלתית, פשעי סייבר, CNE, הגנה פרואקטיבית, דוקטרינות הגנת סייבר, השלכות מקרו־כלכליות.

רון שחר הינו יועץ אסטרטגי בתחום הסייבר. שירת בצה"ל כראש מדור תכנון סייבר־אסטרטגי וכעוזר לראש מחלקת הגנת הסייבר של צה"ל.

מבוא

"התשתית הדיגיטלית שלנו – הרשתות והמחשבים שאנו תלויים בהם מדי יום ביומו – תקבל מעתה ואילך את היחס הראוי לה ותהפוך לנכס לאומי אסטרטגי".[1]

"אנו מתכוונים להגן בצורה אגרסיבית על הקניין הרוחני שלנו. הנכס הגדול ביותר שלנו הוא החדשנות, כושר ההמצאה והיצירתיות של העם האמריקאי. הגנה כזו חיונית לשגשוגנו, ומגמה זו רק תלך ותתחזק במאה הנוכחית". [2]

נשיא ארצות הברית, ברק אובמה

קניין רוחני פרטי ומסחרי בכלל וסודות מסחריים בפרט נתפסים כיום כמרכיב חשוב בכלכלת המדינה המודרנית. במקביל, מרחב הסייבר מתפתח במהירות והופך מקור להזדמנויות מרתקות, ולצד זאת מקור לאיומים, המתבטאים בלוחמת סייבר ובפשעי סייבר.[3] חלק מאיומי הסייבר שמאחוריהם מסתתר מניע פלילי מכוונים ישירות לגניבת קניין רוחני פרטי או מסחרי. גניבה כזו עלולה לגרום לאובדן ניכר של הכנסות ממסים, וכתוצאה מכך להקטנת תקבולי המדינה ולירידה בתוצר המקומי הגולמי של מדינה, וכן להשפיע משמעותית על המערכות המקרו־כלכליות הבין־לאומיות.[4] מרבית המדינות ניסחו דוקטרינות להגנה אסטרטגית על מרחב הסייבר וחוקים להגנה על תשתיות קריטיות פיזיות מפני מתקפות סייבר שמקורן ביריבות פוליטית. לעומת זאת, אותן מדינות נוטות להתעלם מהצורך להגן על קניין רוחני דיגיטלי במרחב הסייבר מפני התקפות בעלות כוונות פליליות.

מאמר זה בוחן את השאלה מדוע ממשלות צריכות להתייחס לכלל הקניין הרוחני שלהן – המסחרי והפרטי כאחד – וספציפית לסודות מסחריים דיגיטליים, כאל תשתית לאומית קריטית שראויה להגנה פרואקטיבית הולמת מצדן. המאמר גם יבחן האם ההשלכות המקרו־כלכליות של גניבת קניין רוחני דיגיטלי פרטי ומסחרי יכולות לסייע להגדיר קניין רוחני זה כתשתית קריטית הראויה להגנה לאומית מפני גניבת סייבר. המאמר אינו מתיימר להציג אמצעים ספציפיים להגנה כזאת, וגם אינו מציע שהגנה ממשלתית על קניין רוחני פרטי צריכה להיות שוות ערך להגנת סייבר על תשתיות קריטיות לאומיות; כל שהוא מבקש להציע היא מסגרת כללית להשגת איזון טוב יותר בין ההגנה על תשתיות קריטיות לאומיות ובין ההגנה על הקניין הרוחני במרחב הסייבר.

תשתיות פיזיות קריטיות – הגדרה והיקף

מתקפות סייבר הן פריצות של האקרים, בעיקר מחוץ לרשת, במטרה להשיג שליטה מסוימת או מלאה על הרשת.[5] שליטה כזו משמשת לשתי מטרות: תקיפת רשתות מחשבים (CNA), או ניצול (Exploitation) של רשתות מחשבים (CNE).[6]

מתקפות סייבר מבקשות לחדור לרשתות מחשבים מסיבות פוליטיות או פליליות, או ממניעים של ביטחון לאומי.[7] סוכנויות ממשלתיות, חברות בשוק הפרטי או יחידים יכולים להיות בעלי מניעים למעורבות בגניבת סייבר או בהשגת קניין רוחני דיגיטלי.

ממשלות אחראיות לספק הגנה וביטחון לאזרחים ולנכסים הלאומיים שלהן,[8] אולם הדָרגה שבה אחריות זו מתממשת משתנה בין מדינות בהתאם למשטר הנהוג בהן. על פי ג'יימס לואיס (Lewis) וקתרינה טימלין (Timlin) מהמכון ללימודים אסטרטגיים בין־לאומיים בוושינגטון די. סי., ככל שהאינטרנט הופך לתשתית גלובלית מודרנית לעסקי סחר בין־לאומיים ולפעילות ממשלתית, כך אבטחת הסייבר הופכת לעניין לאומי ובין־לאומי גם יחד.[9] ד"ר קריסטין לורד (Lord) וטרוויס שארפ (Sharp) מציינים כי מספרן של מתקפות הסייבר שנובעות ממניעים פליליים ופוליטיים גדל במהירות. הערכתם היא כי מדי חודש מתרחשות 1.8 מיליארד מתקפות סייבר, בדרגות חומרה שונות של תחכום, נגד הקונגרס של ארצות הברית וסוכנויות פדרליות אמריקאיות בלבד.[10] אריק סטרנר (Sterner) ממשרד ההגנה של ארצות הברית גורס שמספר מתקפות הסייבר גדול הרבה יותר מכך, במיוחד אם כוללים בהן גם מתקפות בין־לאומיות על ממשלות זרות ומגזרים פרטיים.[11] פרופ' אריק טלבוט ג'נסן (Talbot Jensen) מעריך כי אלפי חברות בכל העולם נמצאות תחת מתקפה בכל רגע נתון, וכי הקניין הרוחני שלהן, ובמיוחד סודותיהן המסחריים, נפגעים כתוצאה מכך.[12] למעשה, רק אם הממשלה וסוכנויותיה הרלוונטיות מיידעות את החברות המסחריות והפרטיות בנוגע למתקפה, הן מוּדעות לה. במקרים אחרים, חברות אינן מוּדעות כלל לכך שהן מותקפות, וכשהן מגלות זאת, כבר מאוחר מדי לטפל באיום, שכן נתוני החברה והקניין הרוחני שלה כבר נגנבו.[13]

מכל מתקפות הסייבר האפשריות, מתקפות ניצול (CNE), שבמגזר הפרטי באות לידי ביטוי בעיקר כגניבת קניין רוחני, הן המטרידות ביותר. על פי מרטין ליביקי, מתקפות CNE מעוררות דאגה רבה, בעיקר משום שהן מתמקדות בגניבת נתונים וסודות דיגיטליים ועושות זאת "מתחת למכ"ם" של הבעלים, מבלי שהן נחשפות ובשיטות שקשה לזהות.[14] לכן, גניבת קניין רוחני ומתקפות ניצול הן האיום הגדול ביותר על שמירה וניהול של קניין רוחני פרטי או מסחרי, דוגמת סודות מסחריים.

הגידול המהיר במתקפות סייבר בזירה הבין־לאומית, והאיום שהן מטילות על מערך האבטחה הגלובלית ועל מערכות כלכליות בכלל, הפכו למצב קבוע ומתמשך של פשעי סייבר ולוחמת סייבר. מתקפות סייבר אלו נעשות מצד אחד על ידי יחידות צבאיות מיומנות הפועלות מסיבות פוליטיות, ומצד שני על ידי פושעים מומחים המונעים מכוח אינטרסים מסחריים ופליליים.[15] התפתחות מתקפות הסייבר הביאה ממשלות בכל רחבי העולם להקים סוכנויות ייעודיות להגנת סייבר

ולגבש דוקטרינות בתחום זה, וזאת כדי להתמודד בדרך אפקטיבית עם האיומים החדשים ההולכים ומתרחבים במרחב הסייבר. כך, למשל, "סוכנות פיקוד הסייבר" (Cyber Command Agency) בארצות הברית מופקדת על התמודדות עם כל סוגי האיומים על תשתיות סייבר – קריטיות וצבאיות – המגיעים ממקורות פוליטיים. גופי ממשל אחרים, כמו ה־FBI, עוסקים באיומי סייבר שמקורם בפלילים.[16] מצב זה הוא תוצאה של ההסתמכות הגוברת של העולם המודרני על מערכות מידע מרושתות, ששולטות בתשתיות הקריטיות ובמערכות התקשורת והפכו חיוניות לאורח החיים הנוכחי.[17]

האחריות הגוברת של ממשלות במרבית המדינות המערביות על תחום הסייבר מתבטאת בעיקר בהגנה על תשתיות ואינטרסים בין־לאומיים, תוך התעלמות מהצורך להגן גם על קניין רוחני, מסחרי ופרטי. צרפת[18] וגרמניה[19] רואות באיומי הסייבר על תשתיות לאומיות קריטיות איום אסטרטגי, שזכה לעדיפות בדוקטרינת ההגנה שלהן. בבריטניה, הדגש מושם בעיקר על נכסים ממשלתיים, פעילויות, ארגונים לאומיים ותשתיות קריטיות, כמו המערכת הפיננסית.[20] בישראל, המשטרה היא האחראית על טיפול בפשעי סייבר, בעוד שמטה הסייבר הלאומי במשרד ראש הממשלה אחראי על הגנה התשתיות הקריטיות של המדינה, ואף זוכה למשאבים ולתשומת לב ממשלתית רבים יותר.[21]

הדגש הדומה ששמות ממשלות מערביות על הגנת תשתיות לאומיות מפני התקפות סייבר שונות מצביע על הסכמה רחבה בדבר הצורך לתת עדיפות להגנה פיזית על תשתיות לאומיות קריטיות במרחב הסייבר. הסכמה זו קיבלה דחיפה נוכח מספר מתקפות סייבר נגד תשתיות לאומיות קריטיות שזכו לחשיפה רבה בשנים האחרונות והעלו את המודעות לסוג זה של מתקפות. מתקפת הסייבר הגדולה על אסטוניה בשנת 2007,[22] ומתקפת "סטקסנט" על תוכנית הגרעין של איראן בשנת 2010[23] גרמו למרבית המדינות לתת עדיפות, במסגרת דוקטרינות ההגנה שלהן, להגנה ממשלתית פיזית על תשתיות קריטיות.

על פי ברוס ברקוביץ (Berkowitz), תשתיות קריטיות ונכסי מפתח הם מרכיבים חיוניים בכל מדינה: אם יותקפו דרך מרחב הסייבר, תימצא המדינה הנתונה למתקפה במצב קיצוני של פגיעות.[24] לדבריו, ההתפתחות הטכנולוגית והתלות הגוברת של תהליכים צבאיים וממשלתיים במרחב הסייבר הביאו לכך שההגדרה של תשתיות קריטיות הלכה והתרחבה. ברקוביץ גם סבור כי העובדה שקניין רוחני דיגיטלי ומערכות מידע הם כה חיוניים לממשלות, לחברה האזרחית ולצבאות המודרניים, עשויה להפוך אותם למטרות מרכזיות בעת מלחמה.[25] המסקנה היא שיֵש מקום לעדכן את ההגדרה של המושג "תשתית קריטית", כך שתכלול את מרכיבי הליבה הדיגיטליים.[26]

לוחמת סייבר, והאיום הישיר שהיא מטילה על היציבות ואורח החיים של מדינות שונות, הביאו את הקהילה הבין־לאומית לגבש דוקטרינות לאומיות להגנת סייבר. דוקטרינות אסטרטגיות אלו מבקשות להתמודד עם האיום הפוליטי באמצעות הגנה פיזית על התשתיות הקריטיות, אולם אינן נותנות מענה מספק לאיומים של גניבה פלילית של קניין רוחני ומתקפות ניצול על נכסים מסחריים ופרטיים. מצב זה מעלה את השאלה האם ההשלכות המקרו־כלכליות של העלייה בהיקף גניבות הסייבר צריכות להניע ממשלות לראות בקניין רוחני דיגיטלי, הן פרטי והן מסחרי, חלק מהתשתית הקריטית שראוי להגן עליה פרואקטיבית מפני גניבת סייבר, פוליטית ופלילית גם יחד.

קניין רוחני דיגיטלי, מסחרי ופרטי, כתשתית לאומית קריטית

למרות השוני בהגדרה הפורמאלית של קניין רוחני במדינות שונות, יש הסכמה על שלושה קריטריונים החייבים להתקיים כדי שקניין רוחני ייחשב כסוד מסחרי מבחינה משפטית: ראשית, על שמירת הנתונים כסוד להעניק יתרון תחרותי; שנית, חובה שהנתונים אכן יישמרו כסוד: קריטריון הסודיות הוא מוחלט ומחייב שלא ניתן יהיה לקחת או לחלץ את הסוד בקלות מהמוצר הזמין בשוק; שלישית, על הנתונים השמורים להיות מוגנים באמצעות מנגנון הגנת סודיות סביר[27] (לרבות טכנולוגיות הגנת סייבר), שמרחיק מהם פולשים. ישנם בתי משפט שמכירים גם בקריטריון רביעי של חבות, ותובעים שהמידע הסודי יימצא בשימוש מתמיד בעסקי החברה.

כפי שצוין קודם לכן, פעמים רבות חברות אינן יודעות שהנתונים שלהן נגנבו דרך מרחב הסייבר, וכאשר הן מגלות זאת, הן נמנעות לא פעם מלדווח על האובדן מתוך חשש לנזק מסחרי פוטנציאלי לִשמן.[28] גניבת סייבר של קניין רוחני מסחרי או פרטי יכולה להיות ממניעים פוליטיים, שמכוונים "ריגול כלכלי" (ביוזמת מדינה),[29] או ממניעים פליליים שחותרים להשיג יתרון בשוק המסחרי, המכונים "ריגול תעשייתי".[30] ההשלכות הפוטנציאליות המקרו־כלכליות של גניבה כזו על החברה ממנה נגנב הקניין הרוחני הן עצומות והרסניות, ללא תלות במניע או במטרה המקוריים. חברות שהקניין הרוחני נגנב מהן מסתמכות על שיטות שונות כדי לאמוד את הנזק הכספי הנובע מכך. חלקן מבססות את ההערכות שלהן על העלויות בפועל של פיתוח הנתונים הסודיים שנגנבו, ואילו אחרות מחשבות את אובדן ההכנסה העתידי שנגרם להן בגין הגניבה.[31]

מלבד הנזק שנגרם לחברה מסוימת מגניבת הקניין הרוחני שלה, השאלה המתעוררת היא האם גניבת סודות מסחריים מסוימים יכולה להביא לפגיעה מקרו־כלכלית בחוסן (resilience) של מדינה. גניבת סייבר של קניין רוחני דיגיטלי פוגעת ביכולת של המגזר הפיננסי המקומי לייצר הכנסות ומשרות חדשות או

לפתח חידושים,[32] וצפויה לגרום להפסדים בהכנסות ממסים, שיקטינו את תקבולי המדינה ואת התמ"ג שלה.[33] כתוצאה מכך, גניבת סייבר של קניין רוחני פרטי או מסחרי, בקנה מידה גדול ורחב היקף, יכולה להיות מתורגמת להפסד מקרו־כלכלי משמעותי, שיסתכם במיליארדים וישתקף בצניחה בתוצר הלאומי הגולמי.[34] גניבת סייבר משוכללת ומתוכננת היטב של סודות מסחריים דיגיטליים (ללא קשר למניע שמאחוריה) עלולה אפילו לגרור פשיטת רגל פתאומית של מדינה כתוצאה מאיבוד הכנסות עתק בעקבות אובדן תקבולים והכנסות ממיסוי החברות המחזיקות בבעלות על הקניין הרוחני שנגנב דרך מרחב הסייבר. ניתוח כלכלי שנערך על ידי גורם אמריקאי רשמי מעריך כי ההפסדים שנגרמו כתוצאה מגניבת סודות מסחריים בסייבר בארצות הברית בלבד, נעים בין שני מיליארד דולר ל־400 מיליארד דולר ויותר מדי שנה.[35]

המוטיבציה הראשונית לגניבת הסייבר אינה רלוונטית במיוחד כאשר שוקלים גישות שונות של הגנת סייבר. זאת, מכיוון שאין קשר בין מטרותיה של מתקפת הסייבר מצד אחד ובין השלכותיה המקרו־כלכליות ההרסניות ושיטות המניעה המקיפות (מבחינה טכנולוגית ודוקטרינרית) של הגנת הסייבר מצד שני. יחד עם זאת, ההשפעה הכלכלית שיש לגניבת סייבר על החוסן הלאומי היא בכל מקרה משמעותית.

קצב החדשנות, המחקר והפיתוח במגזר הפרטי והמסחרי במאה הנוכחית האיץ את צמיחת הסודות המסחריים ואת מספר הפטנטים שנרשמים בארצות הברית ב־40.6 אחוזים, עובדה הממחישה יותר מכל את התפקיד רב העוצמה שממלאים סודות מסחריים בכלכלה הגלובלית.[36] על פי נתוני הארגון האמריקאי של מנכ"לים בענף ההייטק (Technet), יותר משישה מיליון מקומות עבודה ושליש מהכלכלה האמריקאית (שהיקפה 15 טריליון דולר) מבוססים על חדשנות, ולכן על סודות מסחריים וקניין רוחני.[37] גנרל קית' אלכסנדר, לשעבר ראש סוכנות הביטחון הלאומי ופיקוד הסייבר של ארצות הברית, העריך שההפסדים לתמ"ג האמריקאי בעקבות גניבת סודות מסחריים במרחב הסייבר עומדים על כ־205 מיליארד דולר לשנה, וכינה זאת "העברת ההון הגדולה בהיסטוריה".[38] דוגמה בולטת לכך היא גניבת התוכניות של מטוס הקרב החמקן F–35 מחברת "לוקהיד מרטין" ב־2007, לכאורה על ידי חברה סינית שפיתחה אז מטוס קרב דומה (J–20).[39] המניעים מאחורי גניבת סייבר זאת היו אמנם פוליטיים, אך הייתה לה השפעה כלכלית רבה.

אחת הדרכים להבין את ערכם המקרו־כלכלי של סודות מסחריים, ובהתאם לכך את הפוטנציאל לאובדן ההכנסות למדינה מגניבתם, היא באמצעות סקירת ההשקעות שמשקיע המגזר הפרטי והמסחרי במחקר ופיתוח. אמנם, ישנם סודות מסחריים רבים וחשובים שאינם קשורים למחקר ופיתוח (כמו, למשל, נתוני מכירות, רשימות לקוחות, אסטרטגיות שיווק וכדומה), אולם תחום המחקר והפיתוח מייצג

השקעה בטכנולוגיות החדשות ביותר, ברעיונות ובהמצאות, שכולם הם מרכיבים חיוניים בסודות מסחריים רבים.[40] ההשקעות במו"פ בארצות הברית מהוות 2.7 אחוזים מהתמ"ג, ומסתכמות בכ־447 מיליארד דולר לשנה. השקעות במו"פ בגרמניה מהוות 2.9 אחוזים מהתמ"ג, בסין – שני אחוזים מהתמ"ג, בבריטניה – 1.8 אחוזים וברוסיה – 1.5 אחוזים.[41] כל השקעה במו"פ מייצרת גרסאות נוספות של סודות מסחריים חדשים (דולר אחד של השקעת מו"פ יצר עד 69 דולר של סודות מסחריים חדשים במהלך העשור האחרון), כך שערכם הכלכלי של סודות מסחריים גדול אפילו יותר מאשר ההשקעה הבסיסית במו"פ.[42]

במציאות שבה מרבית הנכסים בעלי הערך, וכן התשתיות, הם דיגיטליים, בלתי מוחשיים וקלים להעברה ברשת, גניבת סייבר של קניין רוחני מקבלת חשיבות קריטית נוספת.[43] בדוח משנת 2001, שהקיף 14 סוכנויות ביון אמריקאיות, הוערך כי גניבת סייבר עתידה להפוך ל"איום מתגבר ומתמשך",[44] וראש קהילת המודיעין האמריקאי דירג אותה כאיום קונקרטי משמעותי יותר אפילו מאיום הטרור.[45] על פי דוח של מכון Ponemon, יש עלייה בהיקף גניבת קניין רוחני במרחב הסייבר, כאשר חלק מהחברות חוות מעל 72 מתקפות סייבר בשבוע.[46]

ככל שקניין רוחני הופך לגורם דומיננטי ומכריע בכלכלה המודרנית (כפי שניתן להבין מהסטטיסטיקות שהובאו לעיל), כל גניבה שלו או נזק שייגרם לו יביאו להפסדים כספיים כבדים למדינה לה הוא שייך. לפיכך, כלכלות לאומיות ימצאו עצמן בסיכון כלכלי עצום, אם יקרה דבר מה לקניין הרוחני הדיגיטלי הפרטי או המסחרי שלהן. דוח של הקונגרס האמריקאי בנושא הריגול התעשייתי ציין בהקשר זה כי גניבת קניין רוחני מחברות פרטיות ומסחריות עלולה להשפיע על היכולת של המגזר הפרטי לייצר הכנסות ומקומות עבודה, לעודד חדשנות ולהניח את התשתית הכלכלית לצמיחה עתידית ולביטחון לאומי.[47] ואכן, החשיבות הגוברת של קניין רוחני דיגיטלי לכלכלה המודרנית מצד אחד, והנזק ההרסני הפוטנציאלי לכלכלה של אותה מדינה במקרה של גניבתו מצד שני, הופכים את האיום של גניבת קניין רוחני במרחב הסייבר למסוכן ביותר לחוסנה הכלכלי של המדינה. זאת ועוד, העלייה במספר מתקפות הסייבר שמתמקדות בגניבת קניין רוחני דיגיטלי, וההפסדים המקרו־כלכליים הכבדים הנובעים מכך, מכניסים את הקניין הרוחני הדיגיטלי המסחרי והפרטי לתוך ההגדרה של תשתיות לאומיות קריטיות שראויות להגנה על ידי המדינה. הדבר מחייב ממשלות ליישם את אמצעי הזהירות הנדרשים ולהפעיל גישת הגנה פרואקטיבית נגד מתקפות סייבר על התשתית הקריטית של קניין רוחני פרטי או מסחרי.

הגנה על קניין רוחני פרטי ומסחרי מפני גניבת סייבר היא קריטית לרווחיות החברה ולצמיחתה,[48] אולם יש להתייחס אליה גם כאל גורם בעל חשיבות לאומית. הסיבה לכך היא שקניין רוחני מסחרי משפיע על הכלכלה הלאומית באמצעות

הכנסות ממסים, הכנסות בלתי ישירות אחרות והתמ"ג, ולפיכך כל גניבה של קניין רוחני מסחרי בקנה מידה גדול במרחב הסייבר עלולה לפגוע בחוסן הכלכלי של המדינה ואף לגרום לתגובת שרשרת העלולה להיות חמורה פי כמה מכל מתקפת סייבר על תשתית קריטית בודדת. לכן, על ממשלות ליטול אחריות, ולו מסוימת, על הגנת קניין רוחני מסחרי ופרטי, ולאמץ גישה מעורבת ופרואקטיבית להגנתם. מהלך כזה עלול לעורר דילמה, שכן לצד החשיבות של קניין רוחני לחוסנה של המדינה מבחינה מקרו־כלכלית, הוא גם ישות הנמצאת בבעלות פרטית, ואינו שייך לממשלת אותה מדינה.

מודלים של זכויות יוצרים במדינות שונות

לאחר שאִפיֵנו את הבעיה והצבענו על המצב שבו ממשלות נמנעות מקבלת אחריות על הגנת קניין רוחני פרטי ומסחרי מפני מתקפות סייבר, נפנה להגדיר מודלים קיימים של זכויות יוצרים במדינות שונות ולהמליץ על פתרון שיתבסס עליהם. למרות שזכויות יוצרים הן רק סוג אחד של קניין רוחני, חלק מהמרכיבים בשיטות ההגנה עליהן עשויים להיות רלוונטיים גם להגדרת האחריות הממשלתית להגנה אופטימלית על קניין רוחני דיגיטלי פרטי ומסחרי באופן כללי, ועל סודות מסחריים באופן ספציפי.

המודל האנגלי־אמריקאי נועד להבטיח את טובת הציבור ורווחתו באמצעות הפעלת תמריצים כלכליים עבור בעלי הזכויות – דבר שמעודד יצירת מוצרים חדשים.[49] לפי מודל זה, הגנה ממשלתית פרואקטיבית על קניין רוחני דיגיטלי תעודד ישויות מסחריות ואנשים פרטיים להמשיך לייצר סודות מסחריים חדשים. לעומת זאת יש מי שטוען כי אין כל עדות אמפירית לכך שהגנה חזקה על קניין רוחני מגדילה את היקפו.[50] זוהי טענה שעשויה להיות נכונה כאשר מדובר בזכויות יוצרים בתחום האמנות והמדעים; לעומת זאת, סודות מסחריים מושפעים יותר מתמריצים כלכליים, שכן אלה משמשים גורם חשוב בצמיחתה הכלכלית של מדינה. הגנת סייבר פרואקטיבית של המדינה על סודות מסחריים תמשוך ממציאים חדשים הודות לתמריצים הכלכליים שהיא מעניקה. בדרך זו, הגנת סייבר ממשלתית על קניין רוחני דיגיטלי יוצרת רווח כפול: מניעת נזקים מקרו־כלכליים בקנה מידה לאומי כתוצאה מגניבת סייבר של קניין רוחני מסחרי, ועידוד צמיחה של קניין רוחני מסחרי חדש. שני יתרונות תוצאתיים אלה משקפים, כאמור, את המודל האנגלי־אמריקאי, שתורם לציבור בזכות העידוד שהוא נותן להמצאות נוספות ובזכות חיזוק החוסן הכלכלי הלאומי.

המודל הצרפתי לזכויות קניין משלים את המודל האנגלי־אמריקאי ומנסח את תפקידה של הממשלה בשמירה על הקניין הרוחני בידי בעליו. על פי המודל צרפתי, ובהתבסס על זכויות היוצרים, לא ניתן לנתק בין היצירה ליוצרה, שמחזיק

בזכויות הקניין על עבודתו.[51] היבט זה של המודל הצרפתי מטיל על הממשלה אחריות להבטיח שהקניין הרוחני הדיגיטלי יישאר מוגן כנכס של היוצר, ומונע הפקעת נכסים מסוג זה מבעליהם. במילים אחרות, המודל הצרפתי מבטיח שהגנה ממשלתית על קניין רוחני דיגיטלי פרטי ומסחרי לא תוביל להלאמה של קניין רוחני המצוי בבעלות פרטית וגם לא תביא להתערבות ממשלתית מוגזמת במגזר הפרטי. מודל זה מסייע לקביעת המידה הראויה והמאוזנת של הגנת סייבר ממשלתית על קניין רוחני פרטי ומסחרי. כמו כן, יש בו כדי לסייע להשגת מצב כלכלי לאומי איתן יותר, שיגביל כל חדירה מוגזמת מצד הממשלה למגזר הפרטי.

לסיכום, גישת המודל האנגלי־אמריקאי מסייעת לדרבן ממשלות לקבל על עצמן אחריות להגנה על קניין רוחני דיגיטלי פרטי ומסחרי, מתוך הבנה שההשלכות המקרו־כלכליות הלאומיות של נטילת אחריות כזאת ישרתו את טובת הציבור. מרכיבים במודל הצרפתי מבטיחים שחדירה ממשלתית למגזר הפרטי במסגרת ההגנה על הקניין הרוחני לא תפקיע את הבעלות על קניין זה מידי בעליו. הסינתזה המשפטית בין המודל האנגלי־אמריקאי והמודל הצרפתי יוצרת אחריות ממשלתית פרואקטיבית מאוזנת, מבלי שייחָצה הקו הדק המפריד בין המגזר הפרטי למגזר הציבורי.

האחריות והתפקיד הפרואקטיבי של הממשלה

לאור העקרונות והמודלים שהוצגו לעיל, נתמקד בשני מרכיבי ביצוע מרכזיים הנובעים מהאחריות הממשלתית הכוללת להגנה על קניין רוחני דיגיטלי, שכאמור, נועדה להשיג הגנה פרואקטיבית על קניין זה, כולל צדדיו הפרטיים והמסחריים. המרכיב הראשון הוא חקיקה של חוקי הגנת סייבר ייעודיים, שיספקו הגנה על קניין רוחני דיגיטלי פרטי וציבורי מכל הסוגים. בחלק מהמדינות קיים חוק מקיף ואחיד בנושא זה, ואילו מדינות אחרות מסתמכות על מערך של חוקים שונים, שבצירופם יחד משיגים הגנה משפטית מלאה על הקניין הרוחני. לדוגמה, בארצות הברית חוקקו שני חוקים בעניין סודות מסחריים, האחד בעל אוריינטציה אזרחית והשני בעל אוריינטציה פלילית: הראשון הוא חוק Uniform Trade Secrets Act (UTSA) משנת 1979, שמספק הגדרה רשמית וקריטריונים לסודות מסחריים ומגדיר מהי גניבה שלהם ומהו הסעד ההולם בעקבות גניבה כזו (כגון מתן צו מניעה, פיצוי כלכלי, תשלום שכר טרחת עורך דין וכיוצא באלה).[52] החוק השני נחקק ב־1996 ונקרא Economic Espionage Act (EEA), ובעקבותיו הפכו גניבה של סודות מסחריים וריגול כלכלי לפשעים פדרליים שעונשיהם נקבעו בהתאם.[53] שני החוקים מתמקדים בתוצאה ובהשלכות של גניבת סודות מסחריים דיגיטליים, אך אינם מנסים למנוע מראש ובזמן אמת את מעשה הגניבה עצמו.

חקיקת חוקי סייבר ייעודיים עשויה להרתיע במידה מסוימת תוקף סייבר פוטנציאלי, אולם אין בה כשלעצמה די כאמצעי מונע, מכיוון שמרחב הסייבר מספק לתוקפים אנונימיות יחסית, לרבות סיכון נמוך לזיהוי וקושי בהטלת האשמה על תוקפים ספציפיים.[54] לאור זאת, המרכיב השני של האחריות הממשלתית להגנה פרואקטיבית על קניין רוחני דיגיטלי הוא עיצוב דוקטרינת הגנת סייבר מקיפה, שמכירה ברמת האחריות האסטרטגית של הממשלה ובתעדוף הנובע ממנה לגבי הגנה על קניין רוחני דיגיטלי פרטי ומסחרי. דוקטרינות הגנת סייבר לאומיות כאלו לא יהיו הצהרתיות בלבד, אלא יגלמו בתוכן את העדיפות הלאומית במונחים של הקצאת משאבים (תקציבים, כוח אדם, יישום פתרונות טכנולוגיים ייעודיים וכיוצא באלה), כדי להגן על נכסים דיגיטליים חיוניים. לדוגמה, נשיא צרפת, פרנסואה הולנד, פרסם בשנת 2013 דוקטרינת הגנת סייבר לאומית כללית שמתייחסת לאיום גניבת סייבר. הדוקטרינה הצרפתית מדגישה את החשיבות שיש להגנה על נכסיה הטכנולוגיים והמדעיים של צרפת ולמניעת גניבה של ידע ומידע צרפתיים בעלי אופי פרטי וציבורי כאחד.[55] דוגמה טובה נוספת אפשר למצוא בדוקטרינת אסטרטגיית הסייבר של בריטניה, שמדגישה את החשיבות שיש להגנה על הקניין הרוחני הדיגיטלי של המדינה, לצד הגנה על תשתיות קריטיות צבאיות ולאומיות אחרות.[56] הדוח *Digital Britain* משרטט את חזון הדיגיטליזציה של בריטניה ומדגיש את החשיבות של הגנת סייבר כחלק מחזון אסטרטגי לאומי.[57]

שני מרכיבים מוצעים אלה – חוקים ודוקטרינות אסטרטגיות – גם הם אינם מספיקים כדי לפתור את בעיית גניבת הקניין הרוחני הדיגיטלי, ועדיין יש צורך בגישה ממשלתית פרואקטיבית כדי למנוע גניבת סייבר כזאת. על פי פרופ׳ לורנס לסיג (Lessig), האחריות הפרואקטיבית של הממשלה להגנה על נכסים פרטיים ומסחריים יכולה להתבצע ללא הסכמת הבעלים או ידיעתם,[58] אם כי סוג כזה של פעילות ממשלתית פירושה הפרה של זכויות אדם, ובמיוחד של זכות האדם לפרטיות. גלן גרינוולד (Greenwald) מצידו סבור כי המעורבות הממשלתית הגוברת במרחב הסייבר לא רק שתפגע בפרטיות הציבור, אלא תעשה מעט מאוד לשיפור אבטחת הסייבר.[59]

הפתרון הנכון צריך להיות פתרון מאוזן: על הממשלה להפעיל הגנה פרואקטיבית על קניין רוחני דיגיטלי פרטי ומסחרי, ובמקביל לדאוג להגבלה מרבית של כל אפשרות להפרת פרטיות במה שנוגע לנתונים ונכסים שאינם עונים על ההגדרה של קניין רוחני. במקום להסתפק בהגנה על רשתות צבאיות בלבד כדי למנוע חדירה עוינת, על הממשלות לפרוס את אמצעי הגנת הסייבר שלהן בכל המרחב הדיגיטלי האזרחי/ציבורי, ובכך להגן על רשתות ציבוריות וציבוריות־אזרחיות משותפות, וכן על נתבי ומתגי תעבורה לאומיים, כדוגמת ספקיות אינטרנט.

הפתרון האופטימלי להגנה על קניין רוחני פרטי ומסחרי צריך להיות באמצעות חקיקת חוקים הולמים וגיבוש דוקטרינות הגנת סייבר אסטרטגיות לאומיות, שביחד יניחו את היסודות שיעניקו לממשלות את הכלים והלגיטימיות הנכונים להגן בצורה פרואקטיבית על נכסים דיגיטליים חיוניים, פרטיים ואזרחיים. בנוסף להגנת סייבר ממשלתית, על חברות מסחריות ופרטיות להשקיע מאמצים ולעשות שימוש במשאבים ובהשקעות שבידיהן כדי למנוע ולאתר כל פרצה בתוך הרשתות שלהן וכל ניסיון לגניבת סייבר מתוכן.

מסקנות

> "החוק החדש לריגול כלכלי יסייע לנו לפצח עבירות כגון פירטיות תוכנה והפרת זכויות יוצרים, שעולות למשק האמריקאי מיליארדי דולרים באובדן הכנסות, ובכך יחזק את הביטחון הלאומי שלנו".[60]
>
> נשיא ארצות הברית, ביל קלינטון

הרבה השתנה מאז השמיע נשיא ארצות הברית את דבריו אלה על התקווה לעצור מעשי פירטיות והפרת זכויות יוצרים של סודות מסחריים וסוגים אחרים של קניין רוחני. מרחב הסייבר התפתח במהירות בעשרים השנים האחרונות, כשהוא מצמיח איומים אסטרטגיים חדשים, כמו גניבה של קניין רוחני דיגיטלי פרטי ומסחרי. במקביל, הקניין הרוחני הדיגיטלי הפרטי והמסחרי בכלל, וסודות מסחריים בפרט, הפכו לגורמים קריטיים ודומיננטיים בכלכלה בת־זמננו.

הגישה המיושנת של הטלת עונשים לאחר מעשה ועל בסיס התוצאות כמעט שאינה רלוונטית כיום, נוכח הקושי לאתר גניבות במרחב הסייבר בזמן אמת והיכולת הבו־זמנית להטיל את האחריות למניע הזדוני על כל אדם, ארגון או מדינה. המסקנה הנובעת מכך היא שממשלות בכל רחבי העולם צריכות לשנות את תפקידן ואחריותן בתחום ההגנה מפני גניבות במרחב הסייבר ולעבור לגישה פרואקטיבית שתתבסס על דוקטרינות, חקיקה ותקנות. עליהן ליטול על עצמן אחריות מסוימת להגנה על קניין רוחני דיגיטלי מסחרי ופרטי, וזאת בשל הפוטנציאל לכשל כלכלי עמוק במקרה של גניבות כאלו, וההשלכות שלהן על המערכות המקרו־כלכליות. ההפסדים המקרו־כלכליים הצפויים מגניבות במרחב הסייבר מגבירים את החשיבות של הגנה על הקניין הרוחני הפרטי והמסחרי של המדינה בכל תחומיו של מרחב זה. לפיכך, עליה להתייחס אל ההגנה על הקניין הרוחני בצורה דומה להתייחסותה להגנה על תשתיות קריטיות פיזיות וצבאיות. המודל האנגלי־אמריקאי יוכל להביא לכך שההגנה הממשלתית על הקניין הרוחני תכיל תמריצים כלכליים ליצירת קניין רוחני חדש; המודל הצרפתי יכול לעזור בניסוח זכותו האינדיבידואלית של היוצר לשמור ברשותו את הקניין הרוחני שפיתח.

הערות

1 President Barack Obama, "Remarks on Securing Our Nation's Cyber Infrastructure," Office of the Press Secretary, May 29, 2009, http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure

2 President Barack Obama, "Remarks by the President at the Export-Import Bank's Annual Conference," Office of the Press Secretary, March 11, 2010, http://www.whitehouse.gov/the-press-office/remarks-president-export-import-banks-annual-conference

3 מרחב הסייבר הוא מדיום וירטואלי המורכב מצבר של התקנים ממוחשבים ומרושתים המחוברים לעולם שבחוץ (האינטרנט למשל). ראו: Martin C. Libicki, *Cyber Deterrence and Cyberwar* (Santa Monica: RAND Corporation, 2009).

4 Pamela Passman, Sanjay Subramanian, George Prokop, *Economic Impact of Trade Secret Theft: A Framework for Companies to Safeguard Trade Secrets and Mitigate Potential Threats* (Washington, DC: The Center for Responsible Enterprise and Trade, 2013), p. 8.

5 Libicki, *Cyber Deterrence and Cyberwar*.

6 המושג CNA (Computer Network Attack) מתייחס למתקפה על הרשת והתהליכים העסקיים בה באמצעות שיבוש, מניעת שירות או הרס של מידע המאוחסן בה. המושג CNE (Computer Network Exploitation) מתייחס לגניבת נתונים מהרשת. ראו: US Department of Defense, *Dictionary of Military and Associated Terms* (Joint Education and Doctrine Division, 2014).

7 Oona A. Hathaway and others, "The Law of Cyber-Attack," *Cal if or nia Law Review*, 100, no. 4 (2012), p. 827.

8 Gareth Evans, Mohamed Shanoun, *The Responsibility to Protect: Report for the International Commission on Intervention and State Sovereignty* (Ottawa: International Development Research Centre, 2001), p. 13.

9 James A. Lewis, Katrina Timlin, *Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization* (Washington, DC: Center for Strategic and International Studies, 2011), p. 3.

10 Kristin M. Lord, Travis Sharp, *America's Cyber Future: Security and Prosperity in the Information Age* (Washington, DC: Center for a New American Security, 2011), p. 7.

11 Eric R. Sterner, "Deterrence in Cyberspace: Yes, No, Maybe?" in *Returning to Fundamentals: Deterrence and U.S. National Security in the 21st Century*, ed. Robert Butterworth (Arlington, VA: George C. Marshall Institute, 2011), pp. 28-35.

12 Eric Talbot Jensen, "Cyber Warfare and Precautions against the Effects of Attacks," *Texas Law Review*, 88 (2010), p. 1536.

13 Kim Zetter, "Report Details Hacks Targeting Google, Others," WIRED, February 3, 2010, http://www.wired.com/threatlevel/2010/02/apt-hacks/

14 Libicki, *Cyber Deterrence and Cyberwar*, p. 23.

15 Abraham R. Wagner, "Cybersecurity: From Experiment to Infrastructure," *Defense Dossier*, 4 (2012), p. 17.

16 Lewis and Timlin, *Cybersecurity and Cyberwarfare,* p. 22.

17 The White House, International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World (2011), p. 9.

18 Lewis, Timlin, *Cybersecurity and Cyberwarfare,* p. 11.

19 Federal Ministry of the Interior, *Cyber Security Strategy for Germany* (Berlin, 2011).

20 UK Office of Cyber Security and UK Cyber Security Operations Centre, *Cyber Security Strategy: Safety, Security and Resilience in Cyber Space* (London, 2009), p. 9.

21 Israel's Prime Minister's Office, *Advancing National Cyber Space Capabilities – Decision Number 3611* (August 7, 2011).

22 Michael N. Schmitt, "Cyber Operations and the Jus Ad Bellum Revisited," *Villanova Law Review*, 56 (2011), p. 569.

23 Thomas M. Chen, "Stuxnet, the Real Start of Cyber Warfare?," *IEEE Network*, 24, no. 6 (2010), p. 3.

24 Bruce D. Berkowitz, "Warfare in the Information Age," In *Athena's Camp: Preparing for Conflict in the Information Age*, eds. John Arquilla, David Ronfeldt (Santa Monica: RAND National Security Research Division, 1997), p. 181.

25 שם. עמ' 177, 181.

26 Myriam A. Dunn, "Securing the Information Age: The Challenges of Complexity for Critical Infrastructure Protection and IR Theory," *International Relations and Security in the Digital Age* (ETH Zurich: Center for Security Studies, 2007), p. 11.

27 Robert G. Bone, "A New Look at Trade Secret Law: Doctrine in Search of Justification," *California Law Review*, 86 (1998), pp. 248-249.

28 Office of the National Counterintelligence Executive, Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011 (2011), http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

29 שם. עמ' 7.

30 שם. עמ' 8.

31 שם. עמ' 2.

32 שם. עמ' 3.

33 Passman, Subramanian, Prokop, *Economic Impact of Trade Secret Theft*, p. 8.

34 Shahar Argaman, Gabi Siboni, "Commercial and Industrial Cyber Espionage in Israel," *Military and Strategic Affairs*, 6 (2014), p. 51, http://media.wix.com/ugd/d48d94_a62f01468dc8448ebe635f8d962c410f.pdf

35 Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets*, p. 4.

36 Passman, Subramanian, Prokop, *Economic Impact of Trade Secret Theft*, p. 7.

37 Dennis C. Blair, Jon M. Huntsman, *The IP Commission Report: The Report of the Commission on the Theft of American Intellectual Property* (The National Bureau of Asian Research, 2013), p. 23.

38 Carrie Lukas, "It's Time for The U.S. to Deal with Cyber-Espionage," *U.S. News and World Report*, June 4, 2013, http://www.usnews.com/opinion/articles/2013/06/04/chinas-industrial-cyberespionage-harms-the-us-economy

39 Cyber Warfare Challenges and the Increasing Use of American and European Dual-Use Technology for Military Purposes by the People's Republic of China: Hearing on the Communist Chinese Cyber-Attacks, Cyber-Espionage and Theft of American Technology, Before the Oversight and Investigations Subcommittee of the Foreign

Affairs Committee of the U.S. House of Representatives (2011) (statement of Richard D. Fisher, Jr., Senior Fellow, International Assessment and Strategy Center), p. 5.

40 Passman, Subramanian, Prokop, *Economic Impact of Trade Secret Theft*, p. 8.

41 שם.

42 שם.

43 Blair and Huntsman, *The IP Commission Report*, p. 43.

44 Siobhan Gorman, "China Singled Out for Cyber Spying," *Wall Street Journal*, November 4, 2011, http://allthingsd.com/20111104/china-singled-out-for-cyberspying/

45 Argaman, Siboni, "Commercial and Industrial Cyber Espionage in Israel," p. 54.

46 Ponemon Institute, *Second Annual Cost of Cyber Crime Study: Benchmark Study of U.S. Companies* (Ponemon Institute, 2011).

47 Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets*, p. 3.

48 שם. עמ' A–2.

49 Neil Netanel, "Copyright Alienability Restrictions and the Enhancement of Author Autonomy: A Normative Evaluation," *Rutgers Law Journal*, 24 (1993), p. 9.

50 Richard Watt, "An Empirical Analysis of the Economics of Copyright: How Valid are the Results of Studies in Developed Countries for Developing?" in *The Economics of Intellectual Property* (WIPO, 2006), p. 68.

51 Netanel, "Copyright Alienability Restrictions," p. 15.

52 Uniform Trade Secrets Act §§ 1-12 (amended 1985).

53 The Economic Espionage Act, 18 U.S.C. §§ 1831-1839 (1996).

54 Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets*, p. 1.

55 President of the French Republic's Office, *French White Paper: Defense and National Security* (2013), p. 102.

56 United Kingdom's Prime Minister's Office, *Cyber Security Strategy: Safety, Security and Resilience in Cyber Space* (2009), p. 9.

57 The United Kingdom's Department of Culture, Media and Sport & the Department for Business, Innovation and Skills, *Digital Britain: Final Report* (2009), pp. 189-207.

58 Lawrence Lessig, "The Law of the Horse: What Cyber Law might Teach," *Harvard Law Review*, 113 (1999), p. 5.

59 Glenn Greenwald, Ewen MacAskill, "Obama Orders US to Draw up Overseas Target List for Cyber-attacks," *The Guardian*, June 7, 2013, http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas.

60 President Bill Clinton, "Statement on Signing the Economic Espionage Act of 1996," October 11, 1996, Weekly Compilation of Presidential Documents, 32, no. 41 (October 14, 1996), http://www.gpo.gov/fdsys/pkg/WCPD-1996-10-14/html/WCPD-1996-10-14-Pg2040.htm.

הריגול בסייבר והשפעתו על שיקולי חברות עסקיות

גבי סיבוני ודוד ישראל

מרחב הסייבר הופך לכלי העיקרי והיעיל לריגול עסקי ולגניבת מידע וקניין רוחני. הוא מאפשר לתוקף קיצור דרך טכנולוגי, ההופך ליתרון תחרותי ועסקי בשוק בכלל ומול הנתקף בפרט. מאמר זה בוחן את מידת ההשפעה של הצורך להתמודד עם סיכוני הסייבר בכלל ועם אבטחת המידע הארגוני בפרט על השיקולים של מקבלי ההחלטות בחברות עסקיות. מדובר בהחלטות הקשורות לשיקולים של כדאיות הכניסה לפיתוח, תשומות ההגנה על המידע, אורך חיי המוצר ועצם הכדאיות העסקית בכניסה לתחומים חדשים. המאמר גם מעלה מספר רעיונות לסיוע בתחומים אלה ברמה הלאומית.

מילות מפתח: סייבר, ריגול, ריגול עסקי, אבטחת מידע, קניין רוחני, פשיעת סייבר, גניבת סייבר, טכנולוגיה.

רקע

ריגול עסקי אינו דבר חדש, וקיים בגלגולים שונים מאז שחר ההיסטוריה. ידועות מהפכות תעשייתיות היסטוריות אשר התבססו על העתקת ידע. כך, למשל, מכונות תעשייתיות מבריטניה מצאו את דרכן לארצות הברית וסייעו בהפיכתה למעצמה תעשייתית על חשבון פטנטים בריטיים.[1] בעולם העסקי, ריגול תעשייתי נחשב בדרך כלל כאחד האיומים הגדולים על היכולת של ארגון להתקיים בתוך השוק התחרותי בו הוא מתמודד. הנחת היסוד בעולם זה הייתה שהסיכון של גניבת מידע ואובדן מידע המשמש כקניין רוחני יכול להתממש בעיקר כתוצאה מאיום פנימי, כמו עובד ממורמר, סוכן מושתל או אף שיטוי של עובד נאמן. איום

ד"ר גבי סיבוני הוא ראש התוכנית לביטחון סייבר במכון למחקרי ביטחון לאומי.
דוד ישראל הוא מומחה לאבטחת מידע בחברת "מוטורולה ישראל" ומתמחה בתוכנית לביטחון סייבר במכון למחקרי ביטחון לאומי.

זה יכול להתממש גם כתוצאה מהעתקת מוצר ו"הנדסה לאחור" שלו (Reverse Engineering).

ההתגוננות מפני ריגול תעשייתי התמקדה עד לפני כעשור בהגנת המרחב הפיזי, למשל באמצעות מתחמים ממודרים, בקרות כניסה ומצלמות אבטחה. זאת, לצד בחינת המהימנות של עובדים וגורמים בשרשרת הפיתוח והייצור, ובכלל זה תחקירים ביטחוניים, בדיקות אמינות של עובדים, בחינת ספקים ועוד. ההגנה התבססה בעיקר על מניעת גישה למידע ולקניין רוחני הנמצאים בתוך המתחם הפיזי של הארגון ועל צעדים למניעת האפשרות להדליף מידע זה על ידי גורם פנימי מורשה או על ידי גורם זר שחדר את מעטפת ההגנה הפיזית.

ההגנה על המידע הארגוני ועל הקניין הרוחני נשענה וממשיכה להישען גם על רישום פטנטים והסכמים משפטיים, דוגמת הסכמי סודיות בין חברות וספקים, וזאת בהנחה שארגון יוכל לתבוע את זכויותיו מגופים שיפגעו בקניינו הרוחני. המידע הרגיש כולל לא רק קניין רוחני, אלא גם מידע העלול לפגוע בארגון במגוון דרכים, כמו פרטי חוזים, מרכיבי שכר (לצורך ציד של כישרונות מיוחדים), מידע לגבי מכרזים והצעות מחיר, תוכניות אסטרטגיות, תוכניות שיווק, רשימת לקוחות וספקים ועוד.

התפתחות השימוש במרחב הקיברנטי לצורכי פיתוח טכנולוגי ולצורכי ייצור[2] חושפת מרחב סיכון משמעותי לדליפת מידע רגיש וקניין רוחני. למעשה, התפתחות זאת שינתה את כללי המשחק בתהליכי אבטחת המידע והקניין הרוחני והפכה את ההגנה עליהם למורכבת יותר, עתירת משאבים ובעלת השפעה משמעותית על תהליכי העבודה וזרימת המידע בארגון. ההבנה הקיימת בקרב הנהלות בכירות בארגונים היא כי ידו של התוקף הינה על העליונה וכי סיכויי ההצלחה שלו גבוהים. זאת, לעומת המגבלות של המתגונן במרחב הקיברנטי. באחד המחקרים של חברת ייעוץ גדולה אף נטען כי כשישים אחוזים מהמנהלים הבכירים מאמינים שהתקפות הסייבר יגברו ויהפכו למתוחכמות ובעלות קצב מהיר יותר מאשר יכולת הארגונים להתמודד איתן.[3]

על רקע דברים אלה, מתחולל כיום שינוי עמוק בתהליכי קבלת ההחלטות הקשורות במחקר ופיתוח ובשיקולים שארגונים עסקיים ומסחריים נדרשים לשקלל בכל הקשור להשקעות בתחומים אלה. עוצמת האיום לגניבת מידע וקניין רוחני מחייבת את הארגונים להתייחס בצורה רצינית לנושא ההגנה עליהם. הגנה כזאת מחייבת הקצאה של משאבים לא מעטים, ובכלל זה משאבים טכנולוגיים, כמו גם יישום תקנים ונוהלי עבודה מתאימים. אלה מעמיסים על המשאבים האנושיים ועל עלויות הפיתוח, ובכך מצמצמים למעשה את ההשקעות בפועל בפיתוח עצמו. בהקשר זה על הארגון לשאול מספר שאלות יסודיות, כמו: מהן החולשות הקריטיות בתהליך העסקי ואיך יש להגן מפניהן? מה צפויה להיות העלות הנוספת

הכרוכה בהגנה על המידע ובמערך האבטחה שיידרשו בתהליך המחקר והפיתוח? האם ניתן יהיה להקים את מערך האבטחה הנדרש קודם להתנעת הפיתוח, והאם כתוצאה מכך גדל הסיכון העסקי של כניסה מאוחרת לשוק? מכיוון שברור שכל הגנה עלולה להיפרץ, יש גם לשאול מה תהייה היכולת להתאושש מפגיעה בתהליך העבודה במהלך הפיתוח ומה תהייה ההשפעה של הפריצה על ההשקעה הכוללת, וכן אילו עיכובים צפויים בתהליכי הפיתוח כתוצאה ממגבלות שיתוף מידע ומה תהיה השפעתם? כל תהליך פיתוח מחייב שותפות של גורמים חיצוניים, ולעיתים מיקור חוץ. בהקשר זה יש לשאול באיזו מידה נדרש יהיה להשקיע משאבים בהגנה במצבים כאלה, או לחייב ספקים חיצוניים לממש הגנות נוספות, דבר שעשוי לייקר את השירות?

א. זוהי רשימת שאלות חלקית, אולם היא מבהירה עד כמה השתנה תהליך קבלת ההחלטות בעידן איומי הסייבר ועד כמה משמעותית ההשקעה בתהליכי האבטחה שנועדו להתמודד איתם. שיקולים של איומי סייבר, המתווספים כנדבך רב־משמעות לכלל השיקולים העסקיים, עשויים להביא ארגון לקבל החלטה להימנע מכניסה לפיתוח טכנולוגי בתחומים המועדים להיות מטרה אטרקטיבית לריגול מסחרי. רגיש במיוחד בהקשר זה הוא מצבה של תעשיית חברות ההזנק. אלו נמצאות בדרך כלל במצוקת משאבים ומשקיעות את כל הונן בפיתוח הטכנולוגי, כך שיתקשו מאוד להשקיע את המשאבים הנדרשים כדי להגן בצורה מספקת על נכסי הקניין הרוחני שלהן. כתוצאה מכך, תעשיית החדשנות הינה התעשייה החשופה ביותר לאיומי סייבר הנוגעים לגניבת קניין רוחני.

ב. ישראל הינה מדינה בעלת תשתית טכנולוגית ענפה הכוללת, בין השאר, חברות הזנק רבות המפתחות מוצרים ופתרונות חדשניים. על רקע זה ראוי לבחון את תפקידה של המדינה בסיוע לאבטחת הקניין הרוחני המפותח בה, במיוחד זה המפותח כתוצאה מהשקעות הממומנות על ידי המדען הראשי של משרד הכלכלה.

ג. חברות חשופות לפגיעה במרחב הסייבר לא רק בהקשרי ריגול מסחרי, אלא גם בהקשרים של תקיפות סייבר הנעשות לצורך פגיעה, השבתה וגרימת נזק. גם התקפות כאלו מחייבות התייחסות והגנה. עם זאת, לצורך המיקוד, מאמר זה מבקש לבחון את משמעות הצורך להשקיע באבטחה והגנה על מידע קניין רוחני ועל תהליכי הפיתוח והמחקר, וכיצד שיקולי אבטחה אלה עשויים להשפיע על היקף ההשקעות במו"פ בכלל. כמו כן, המאמר מבקש לבחון כלים שיסייעו לחברות לעמוד בצורכי ההגנה שלהן על ידי מאמצים משותפים ויוזמות בין חברות עסקיות שונות. לצד זאת בוחן המאמר את תפקיד המדינה ביצירת

תשתית אבטחה שתוכל לסייע לחברות קטנות וגדולות לשפר את ההגנה על מידע קניין רוחני ואת מוכנותן להתמודד עם איומי הסייבר.

מורכבות ההגנה על תהליכי יצירת קניין רוחני

אחד ממוקדי המידע הרגישים ביותר להגנה הינו הקניין הרוחני, המהווה את הנכס העיקרי של חברות טכנולוגיות וחברות הזנק. כדי להבין את מורכבות ההגנה על תהליכי יצירתו של קניין רוחני – הווה אומר מורכבות אבטחתו של חוד החנית העסקי ושמירה על היתרון התחרותי הקריטי לקיומו של ארגון – נדרש לנתח את מחזור חייו של המידע. לצורך זה נתייחס למחזור חייו של פיתוח מוצר בחברת היי־טק.

פיתוח מוצר טכנולוגי מתאפיין בשלבים העיקריים הבאים: ייזום הרעיון, אפיון, יצירת אב טיפוס, בדיקות מעבדה ומעבר לייצור. מיותר לציין שכל השלבים המלווים את ייזום ופיתוח הרעיון, עד הבשלתו כמוצר סופי וייצורו, הינם תהליכים דיגיטליים מבוססי מערכות מידע שונות ומגוונות, הנותנים מענה לכל אחד משלבי הפיתוח והיצירה של הקניין הרוחני. כפועל יוצא מכך, כל אחד מהשלבים בתהליך יוצר מוטיבציה לתוקף והינו רלוונטי למתקפת סייבר אפשרית, אם באמצעות רשת האינטרנט ואם באמצעות גורם פנימי הפועל בשוגג או בזדון.

עקרונית, ובצורה מופשטת ביותר, מטרת הארגון היא לאתר את הנקודות הרגישות בתהליך ולמקד את הגנות הסייבר באזורים אלה. בפועל, ניתוח הסיכונים, המתבסס על תהליכי זרימת המידע וחשיבותו בתהליך הפיתוח, הופך מהר מאוד לתמנון רב־זרועות המצריך התייחסות אבטחתית מעמיקה. הזנחתו של ערוץ מסוים, או הערכת חסר של חשיבותו, עלולות להיות נקודות התורפה של מערך ההגנה בכללותו. המורכבות של ההגנה על כל אחד משלבי הפיתוח מושפעת מהעובדה כי כל אחד מהתהליכים מתאפיין בשימוש בכלים ובטכנולוגיות מגוונים ובעבודה בסביבה שונה ומצריך תמיד יכולות של שיתוף מידע. בכל אחד מהשלבים נדרש הארגון להעריך את הצורך במתן מענה לסיכונים הנוגעים לסודיות המידע, לאמינותו ולזמינותו (Confidentiality, Integrity, Availability).

נבחן לדוגמה את מורכבות ההגנה על מידע רגיש של ארגון המעוניין לפתח מוצר טכנולוגי המוגדר כפרויקט אסטרטגי ואשר עלול להוות מטרה למתקפות סייבר. כבר בשלב ייזום המהלך נוצרים מסמכים המוגדרים כחסויים ומוגבלים לעיניהם של מורשים בלבד: סיכומי פגישות, מצגות, ניתוחים טכנולוגיים, תרחישי שוק, קביעת מפת דרכים טכנולוגית וכדומה. אלה נשמרים בצורה דיגיטלית, המצריכה מעטפת הגנה אשר תבטיח גישה למורשים בלבד. משמעות הדבר היא בדרך כלל יישום מערכות למניעת זליגה של מידע,[4] שהן יקרות ומורכבות לתפעול. מורכבות ההגנה על מידע ארגוני רגיש דורשת ניתוח תהליכי יצירתו של המידע

בארגון, מיפוי המערכות, הבנת מחזור החיים, איתור המידע המסווג בבסיסי נתונים, בשרתי קבצים ובמחשבי קצה, וקביעות מדיניות ארגונית להגדרות סיווג. כל זאת, עוד בטרם נבחרו הכלים הטכנולוגיים אשר יאכפו את המדיניות אותה יש להטמיע, להדריך בהם את המשתמשים ולתמוך בהם לאורך כל חיי הפרויקט.

מעֵבר לצורך לאבטח שיתוף מידע פנים ארגוני, קיים צורך לנהל ולאבטח גם את המידע היוצא מהארגון. כמעט בכל ארגון מתקיים שיתוף מידע עם גורמים חיצוניים, כגון יועצים, ספקים ונותני שירותים למיניהם, וכמעט כל גורם בארגון נדרש לשתף מידע עם גורמים חיצוניים כדי לקדם את התהליכים העסקיים: החל ממהנדס הפיתוח המשתף במידע את קבלן המשנה החיצוני המומחה לתחום ספציפי ורגיש בפרויקט, דרך עורכי הדין הנדרשים לקבל ולשלוח חוזים עסקיים סודיים לשותפים, לספקים או ללקוחות פוטנציאליים, וכלה בעובדי הלוגיסטיקה והייצור המקבלים ושולחים מידע לנותני שירותים חיצוניים כחלק מניהול שרשרת האספקה.[5]

שמירה על אבטחת המידע הרגיש היוצא מתוך הארגון היא אחד האתגרים המורכבים ביותר ליישום, מאחר ומגוון הערוצים הדיגיטליים האפשריים להוצאה והכנסה של מידע הוא כמעט אינסופי. עובד עלול להוציא מידע על ידי שליחתו בדואר האלקטרוני הארגוני, דרך הדואר האלקטרוני הפרטי שלו, באמצעות העתקתו לרכיב זיכרון נייד כגון Disk on Key, צריבתו על כונן תקליטורים, שימוש בשירותי ענן לשיתוף קבצים חינמיים,[6] והגרוע מכל – באמצעות שירותי Peer-to-Peer, בהם המשתמש מתקין על מחשב בארגון תוכנה המקשרת אותו ישירות לרשת מחשבים המשתפים קבצים. כל אחד מאמצעים אלה מהווה סיכון משמעותי לקניין הרוחני של החברה. כל אחד מערוצי המידע מחייב ליישם טכנולוגיה אשר תגביל, תמנע, תחסום ותנטר את כל המידע העובר בה.

ארגונים רבים השקיעו משאבים רבים בחסימת התקנים חיצוניים אוגרי זיכרון, כגון Disk On Key ודומיהם, במניעת גלישה באינטרנט לשרתי שיתוף קבצים ועוד. אולם הצורך העסקי ביעילות, ושיתוף מידע בצורה מהירה וזמינה מתוך המשרד ומחוצה לו, מאלצים את הארגון ליצור ולאפשר ערוצי שיתוף מידע מאובטחים ומבוקרים מתקדמים. אחת האופציות הינה אימוץ של טכנולוגיות ענן, המאפשרות לארגונים להתייעל ולהנגיש את המידע מכל מקום באמצעות טלפונים סלולריים, מחשבי לוח ומחשבים ביתיים. שירותי הענן הם פתרון מצוין לארגון, אולם רמת האבטחה המובנית בהם לא מסַפקת לפי שעה תשובות לדרישות המחמירות להגנה על מידע וקניין רוחני.

תוצאות מחקר של חברת הייעוץ האסטרטגי "מקינזי"[7] מצביעות על כך שהדאגה מפני התקפות סייבר גורמת להאטה משמעותית באימוץ טכנולוגיות ענן ושירותי מובייל. כשבעים אחוזים מהנשאלים במחקר דיווחו כי דחו אימוץ

טכנולוגיות ענן בשנה ויותר מסיבות של אבטחת מידע, וארבעים אחוזים דיווחו כי דחו שימוש בשירותי מובייל בשנה ויותר מאותה סיבה. בתחום ההיי־טק, חמישים אחוזים מהנשאלים דיווחו כי יידרשו לבצע שינויים בתהליכי המחקר והפיתוח שלהם. עובדה נוספת המשקפת את השפעתן של הגנות סייבר על תפקודם של ארגונים היא שחמישים אחוזים מהמנהלים הבכירים מתחום ההיי־טק שהשתתפו במחקר דיווחו כי הנושא מהווה "נקודה כואבת", המגבילה את יכולת העובדים לשתף מידע.

מתברר, אפוא, כי טכנולוגיות המבטיחות התייעלות עסקית, כגון שירותי ענן יעילים וזולים, וכן טכנולוגיות שיתוף מידע וניידות, נתפסות כסיכון עסקי גבוה, עד כדי כך שהארגון מעדיף למעשה לספוג עלויות תפעול גבוהות ולא להסתכן ולהמתין עד אשר מערכות אלו יבטיחו לו בשלות ואבטחה איתנה. במצב כזה, ארגונים עלולים להתעלם מסיכוני סייבר בשל העדפתם יעילות תהליכים וקיצור זמן להשלמת המוצר על פני יישום בקרות והשלמה עם ההגבלות הנובעות מתהליכי האבטחה.

נקודת חולשה נוספת הקשורה לצורך של ארגונים לנתח וליישם מדיניות אבטחת מידע כאשר מדובר בגישה למידע וקניין רוחני, הינו הצורך לתת לגורמים חיצוניים גישה לרשת החברה. במקרים רבים מוצא הארגון לנכון לאפשר לספקים חיצוניים גישה מרחוק לרשת שלו, ובכך הוא נחשף למעשה לסיכונים המגיעים מכיוון הספק ומרמת אבטחת המידע הנהוגה אצלו.[8]

בין הגורמים שעשויה להיות להם גישה אל לב מערכות המידע והרשת הארגונית ניתן למצוא חברות המספקות תמיכה מרחוק למערכות מחשוב פנים ארגוניות, ספקים הנדרשים לעדכן מערכות מידע לוגיסטיות פנים ארגוניות וספקי משנה ושותפים עסקיים המתחברים מרחוק כדי לבצע פעילות במערכות החברה. גורמים אלה מחייבים את הארגון להקים, לתחזק ולנהל תשתית תקשורת מאובטחת ומוצפנת, בעלת הזדהות חזקה מול הארגון המקבל גישה. בנוסף, הארגון נדרש להגביל את הגישה הרשתית של הגורם החיצוני אך ורק למשאבים החיוניים לביצוע עבודתו, ולמנוע מצב בו גורם חיצוני יוכל לשוטט בצורה חופשית בתוך רשת החברה ולהיחשף למידע רגיש המצוי בשרתיה ובבסיסי הנתונים שלה. כל גישה של גורם חיצוני מצריכה ניתוח תהליכי, כגון: שם השרת אליו נדרשת הגישה, אילו תוכנות ופרוטוקולים יהיה עליו להפעיל, יצירת שם משתמש ייעודי, הפעלת מערכת ניטור ובקרה על כל תהליך ההתחברות והפעילות המתבצעת ברשת, יישום חוקי Firewall, וכמובן מעקב שוטף אחר הצורך בקישור החיצוני וטיפול בתקלות.

יש לתת מענה גם לרמת אבטחת המידע המיושמת אצל הגורם החיצוני ולסיכון האבטחתי הנובע מחולשה אפשרית בתחנת הקצה של נותן השירות. בין השאר יש לבחון האם המחשב שלו הוא בעל תוכנת אנטי־וירוס מעודכנת? האם קיבל

את עדכוני האבטחה האחרונים? האם הוא נגוע ב"סוס טרויאני" או בכל קוד עוין אחר? מחשב של ספק המתחבר לרשת הארגון הופך לחלק אינטגרלי ממנה. במקרים רבים הוא החוליה החלשה במערכת, אשר דרכה ניתנת האפשרות לגורם עוין לקבל אחיזה ברשת לצורך התקפת סייבר. במצב זה, לא משנה אם מדובר בארגון מסודר בעל מדיניות אבטחה עדכנית, המנהל את אבטחת תחנות הקצה בתאימות למדיניות הארגון בכל האמור לעדכוני אבטחה שוטפים, אנטי־וירוס ומניעת תוכנות בעלות סיכון אבטחתי; ברגע שניתנה גישה לגורם חיצוני בעל מדיניות אבטחה נחותה מזו של הארגון, הרי שהוא הופך לסיכון ממשי ומיידי.

נדבך נוסף שיש להתייחס אליו מבחינה אבטחתית הוא תהליך היצירה של אב טיפוס ושלב ביצוע הניסויים. זהו נדבך רגיש, שכן כאן נחשפים למעשה לראשונה הטכנולוגיה החדשנית, המוצר והיכולות החדשות העתידות לאפשר לארגון את פריצת הדרך העסקית. כאן מתגבש הקניין הרוחני לכדי ישות מגובשת, שאם גורם עוין ישים עליה את ידו, הוא יוכל לזכות ביתרון משמעותי. לפיכך, הצורך האבטחתי מכתיב ברוב המקרים הקמת מעבדות ואזורי פיתוח ממודרים על ידי בניית רשתות נפרדות, ניתוק מוחלט מרשת האינטרנט ויישומם של מוצרי אבטחה ותשתית נוספים המקבילים לאלה הנמצאים ברשת הארגונית. מיותר לציין את העלות הכלכלית הגבוהה של בניית רשתות נפרדות מסוג זה, כמו גם את הקשיים התפעוליים המתעוררים כתוצאה מכך בכל הקשור להוצאת מידע מתוך הרשתות המסווגות והכנסתו אליהן.

אחד ממעגלי האבטחה המשמעותיים ביותר הוא מערך הניטור והבקרה של אירועי אבטחה. ללא מערך ניטור אין לארגון יכולת לזהות אירועי אבטחה במערכותיו, אי־עמידה במדיניות האבטחה ואירועי סייבר פוטנציאליים, לא כל שכן יכולת להגיב לאירועים כאלה ולפעול במהירות להקטנת הסיכון. מערכות לניטור אירועי אבטחת מידע (SEIM)[9] הן בדרך כלל מערכות יקרות, המצריכות תחזוקה ועדכון שוטפים כדי להתאימן לאיומים חדשים, לתהליכים עסקיים ולמערכות אבטחה מדווחות חדשות. מערכת לניטור אירועי אבטחת מידע יודעת לקבל התרעות אבטחת מידע שמקורן בדרך כלל ברישומי אירועים מתוך המערכות הפנים ארגוניות (Audit Log / Security Log), כגון שרתים, ציוד תקשורת, מערכות Firewall, שרתי הזדהות, מערכות גישה מרחוק, בסיסי נתונים, שרתי קבצים ועוד. בנוסף לכלים הטכנולוגיים נדרש כוח אדם מיומן, המבין את משמעות האירועים המתקבלים במערכת ויכול לנתח את הפעילות ולקבל החלטה לגבי דרכי התגובה. יתרה מזו, שימוש במערכות לניטור אירועי אבטחת מידע מאפשר שילוב של מידע מודיעין סייבר חיצוני, המספק מידע עדכני על אופיין של התקפות סייבר ידועות, מקורות התקיפה וכלים הנמצאים בשימוש התוקפים. מידע מודיעיני זה מוצלב עם מידע הקיים ברשת הארגון ומאפשר זיהוי מוקדם ותגובה מהירה לאירוע.

החשיבות של יישום מערכות לניטור אירועי אבטחת מידע בתהליך ההגנה מפני התקפות סייבר עולה גם מתוך תוצאות מחקר של PoneMon Institute.[10] לפי מחקר זה, חברות שיישמו מערכות כאלו היו יעילות יותר בזיהוי והכלה של התקפות סייבר. כתוצאה מכך, אותן חברות חסכו כארבעה מיליון דולר של נזק, בהשוואה לחברות שלא יישמו מערכות לניטור אירועי אבטחת מידע.

הצעד החשוב ביותר בהתגוננות מפני איומי סייבר הוא השקעה בחינוך ובמודעות העובדים לסיכוני סייבר. אירועים של התקפות קיברנטיות מוצלחות על ארגונים התאפיינו, בין השאר, בחדירה לארגון דרך נקודת התורפה שלו – העובד, ולו הזוטר ביותר, שבאמצעותו ניתן להגיע לנקודת אחיזה ברשת הארגון הקורבן, וממנה להתחיל במתקפה. בהקשר זה יש עניין מיוחד בדוח מחקר על התקפות ממוקדות מבוססות דיוג (phishing) שנעשו על עובדי חברות.[11]

בכך לא מסתיימות הפעילויות שהארגון נדרש לבצע כדי להגן על קניינו הרוחני. לא די בהגדרת הנקודות הרגישות בתהליך ובהגנה עליהן; על הארגון להשקיע ולפתח לעצמו גם יכולות הגנה רשתית ולהקים מערכות ניטור ובקרה, שמצידן מצריכות רכישה, הטמעה ותחזוקה שוטפת, וכל זאת כדי לזהות אירועי אבטחה והתקפות סייבר בזמן אמת.

נוכח כל הנאמר לעיל, ברור כי הגנה על הקניין הרוחני הינה תהליך טכנולוגי, ארגוני ומינהלי מורכב ומשמעותי עבור הארגון. לתהליך זה ולעלותו הכספית השפעות עסקיות שליליות, כפי שינותח להלן.

השפעות כלכליות שליליות

החשש הכבד מפני התקפות סייבר ופוטנציאל הנזק הגבוה שיש בהן גורמים להשפעות כלכליות שליליות על ההתייעלות התפעולית של הארגון, על קיצור תהליכי הפיתוח והייצור ועל ההגעה לשוק לפני המתחרים. לפי הערכות המחקר של חברת "מקינזי",[12] כל עוד איומי הסייבר ימשיכו להתגבר והיכולת ההגנתית לא תסַפק את המענה ההולם, ההשפעות הכלכליות השליליות הנובעות מסיכוני סייבר יגרמו בחמש עד שבע השנים הבאות נזק למשק העולמי שיתבטא בפגיעה ביצירת ערך לחברות בסכומים שבין תשעה ל־21 טריליון דולר. משמעות הדבר היא כי תשומות ההגנה מפני סיכוני סייבר, וכן אובדן מידע וקניין רוחני כתוצאה מריגול מסחרי מבוסס סייבר, יגרמו לפגיעה משמעותית בכלכלה העולמית. המספרים דלעיל מושפעים כמובן מהתפתחות חוסנן של מערכות ההגנה. לצד זאת קיימת השפעה כלכלית ספציפית על כל חברה, בעיקר בשל הצורך שלה להגדיל את תקציב אבטחת הסייבר על חשבון תקציב המחקר והפיתוח, וכתוצאה מכך גם הקטנת הרווחיות התפעולית.

מעֵבר לעובדה שסיכוני הסייבר גורמים להשפעות כלכליות שליליות המתבטאות בהאטה עולמית ובצורך של חברות להשקיע בצורה מוגברת בתקציבי הגנת הסייבר, הסיכון המשמעותי לארגונים הוא של פגיעה ממשית בקניין הרוחני, על כל ההשלכות הכלכליות של הדבר. פגיעה בקניין רוחני עלולה להשפיע על שינוי מאזן הכוחות המסחריים בעולם, ליצור תחרויות לא הוגנות ולפגוע כלכלית ברווחיות חברות עד כדי חדלות קיומן. חברות רבות שחוו פגיעה בקניין הרוחני שלהן דיווחו על אובדן מכירות, רישיונות ותמלוגים, ירידה ברווחים ופגיעה במוניטין המותג והמוצר.

אחת הדוגמאות המשמעותיות בתחום גניבת קניין רוחני הוא מטוס החמקן הסיני J–31, הדומה בצורה מפתיעה למטוס החמקן F–35 של חברת "לוקהיד מרטין" האמריקאית. החברה האמריקאית נפלה בעבר קורבן להתקפת סייבר סינית, במהלכה נגנבה ממנה טכנולוגיית החמקן האמריקאי.[13] מטוס החמקן F–35 נחשב למטוס המתקדם ביותר בעולם, וכיום נמצאים בידי הסינים מידע טכנולוגי יקר ערך הקשור למטוס זה, כגון תרשימי מנוע מפורטים, מערכות מכ"ם וטכנולוגיות ייצור מתקדמות. קניין רוחני שהושקעו בו מיליארדי דולרים הפך במקרה זה למידע החשוף לגורם מתחרה, שעשה בו שימוש מיידי ויצר את המטוס J–31, הדומה להפליא לחמקן המקורי. מידע טכנולוגי מתקדם, הנופל לידי גורם מתחרה, מעניק לו קפיצת דרך טכנולוגית והופך אותו לשחקן משמעותי בשוק שנשלט בעבר על ידי מספר מצומצם של חברות.

הבעיה העיקרית בגניבת מידע וקניין רוחני היא העובדה שהארגון הנפגע מתקשה לזהות שנפל קורבן למתקפת סייבר שמטרתה גניבת מידע וקניין רוחני, שהרי מידע זה ממשיך להיות קיים בשרתים שלו והוא ממשיך לתפקד לכאורה כאילו לא קרה דבר. למעשה, הארגון כבר אינו שולט במידע, ועליו להתמודד עם מתחרה חדש שיפתיע אותו עם טכנולוגיה דומה או משופרת מזו שלו ויזכה ליתרון יחסי יקר ערך. מחקרים מראים כי הזמן שלוקח לחברה לגלות שהיא קורבן להתקפת סייבר הוא כ־230 ימים בממוצע.[14] משמעות הדבר היא כי במשך זמן זה התוקף שוהה בתוך מערכות הארגון, ותקופה זו ארוכה מספיק כדי לחקור את המידע המגיע לידיו, לנתחו מבחינת הרלוונטיות שלו לצרכיו, להסיק מסקנות ואף לשפר את התקיפה. המידע הנאגר אצל התוקף מאפשר לו להבין את מבנה הרשת של הארגון, להכיר שמות של מערכות הנמצאות בשימושו, לזהות שרתי קבצים ובסיסי נתונים, לפצח סיסמאות של עובדים בעלי הרשאות בסיווג גבוה ולחדור למאגרי המידע המעניינים אותו. מעבר לכך, המידע המועתק מהארגון מאפשר לתוקף להבין את המבנה הארגוני, להכיר את אנשי המפתח, את בעלי התפקידים ואת מקבלי ההחלטות, ולהמשיך להתקפה ממוקדת יותר במטרה לשלוף את המידע הספציפי בו הוא מעוניין.

כאמור, הארגון המותקף כלל אינו מודע לעצם קיומה של ההתקפה עליו וגם לא למשך השהייה של התוקף ברשת שלו. גם אם יש לו חשדות, יעבור זמן רב עד שהוא יידע פרטים מדויקים לגבי עומק ההתקפה ואיכות המידע שנגנב ממנו. פרק הזמן הארוך בטרם זיהוי ההתקפה הינו אחד היתרונות המשמעותיים ביותר של התוקף, וקיצור זמן הגילוי הוא אחד האתגרים המשמעותיים ביותר בהגנה מפני מתקפות סייבר. יכולת זיהוי של התקפת סייבר ותגובה עליה תלויות בצורה ישירה ברמת ההשקעה של הארגון במערכות מתקדמות לזיהוי והתרעה על פעילויות חריגות, בהגנה על עמדות קצה ומאגרי מידע, ביישום תקני אבטחה ובמודעות עובדים.

יש לזכור שהתקפת סייבר הממוקדת בגניבת מידע אינה דומה להתקפת סייבר שמטרתה מניעת שירות (DoS). במקרה האחרון, חברה מאורגנת תוכל להפעיל את תהליכי ההתאוששות עם סיום ההתקפה ולחזור לפעילות רגילה, תוך כדי הסקת מסקנות לגבי תיקון הפרצות. לעומת זאת, התקפה שבמהלכה נגנב מידע וקניין רוחני מצריכה מהקורבן לבצע תהליך מורכב של קבלת החלטות לגבי האסטרטגיה של המשך פעילותו העסקית, כמו למשל: איך לאמוד את מידת הנזק שנגרם לחברה כתוצאה מגניבת הקניין הרוחני? האם להמשיך לפתח מוצר שהמידע הטכנולוגי לפיתוחו וייצורו כבר אינו בשליטת החברה? האם להמשיך את האסטרטגיה העסקית בהתאם לתוכניות המקוריות, או שמא לשנות אותה מהקצה לקצה?

לפי הערכות ממקורות שונים,[15] הנזק לכלכלה העולמית הנובע מהתקפות סייבר הממוקדות בריגול תעשייתי הוא בסדר גודל של מיליארדי דולרים כל שנה. האפקט הכלכלי של גניבת מידע וקניין רוחני מתבטא במספר פרמטרים הנוגעים ישירות לארגון עצמו, ובצורה עקיפה גם למצב הכלכלי במדינה. בכל מקרה, היכולת להעריך מספרית את הנזק הכלכלי מהווה אתגר בפני עצמו, שקיים קושי אמיתי להעריכו בצורה כמותית, ועל כן הוא בגדר השערה.

את המשמעות הכלכלית המצטברת כתוצאה מגניבת מידע קניין רוחני ניתן לסכם במספר מאפיינים, ובראשם היכולת של התוקף לצבור יתרון טכנולוגי, באמצעותו הוא יוכל להציע מוצר זהה במחיר זול יותר, וזאת מאחר ולא השקיע בפיתוח ולפעמים גם עלויות הייצור שלו הן נמוכות. התוצאה לגבי הקורבן יכולה להיות ירידה במכירות, ירידת מחירים, ירידה ברווחים, ירידה בערך המניות שלו ואף סגירת החברה. בכל מקרה, קיימות עלויות גבוהות לחברה, הנובעות מהצורך לטפל באירוע התקיפה והשקעה בשיפור מערכות ההגנה שלה. דוגמה מפורסמת לחברה שחדלה להתקיים בשל גניבת מידע היא חברת DigiNotar ההולנדית, שפשטה את הרגל אחרי שמידע קריטי נגנב ממנה.[16]

הנזקים במישור הלאומי מהתקפות סייבר לצורך גניבת מידע קניין רוחני עלולים להתבטא בירידה בתוצר ובאובדן מקומות עבודה, במיוחד במדינה בה הכלכלה מוּטת טכנולוגיה ומו"פ. השקעות בטכנולוגיה מתקדמת עלולות לרדת לטמיון

ולהניב רווח כלכלי דווקא לתוקף. זאת ועוד, מידע טכנולוגי ביטחוני רגיש עלול לזלוג לאויבים ולהשפיע על מאזן הכוחות מול אויבים ויריבים. הערכה כמותית של השפעה כזו יכולה להישען על תחזיות כלכליות שונות, אולם בכל מקרה ברור כי האפקט הכלכלי הנוצר מהתקפות סייבר, הן ברמת החברה הפרטית והן ברמה הלאומית, דורש התייחסות אסטרטגית מעמיקה.

בבואנו לבדוק את השפעת הריגול המסחרי בעולם הסייבר על קבלת החלטות עסקיות של ארגונים, נדרש לבחון תחילה שלושה היבטים בסיסיים: הראשון נוגע לרמת המודעות של מקבלי ההחלטות לסיכוני ריגול סייבר; השני נוגע לשאלה האם יש בחברות השונות כלים להערכת הסיכונים ולקבלת החלטות בנושא; השלישי נוגע לאופן שבו החלטות שהתקבלו כמענה לאיומי הסייבר מיושמות בארגון. מחקרים[17] מראים כי רוב החברות מִתקשות להעריך את הסיכון, וכתוצאה מכך מתקשות לגבש תוכניות להקטנתו. קיימת תמימות דעים כי איומי הסייבר וההתקפות המתוחכמות ילכו ויתגברו, מבלי שלארגונים תהיה יכולת אפקטיבית להתגונן מפניהם.

דליפת מידע שהוא קניין רוחני הינה אחת הדאגות המרכזיות בחברות הי־טק, והיא נתפסת כחמורה ביותר יחסית לדליפת סודות של מִפרטי המוצרים. לעומת זאת, חברות שירותים מודאגות בעיקר מדליפת מידע המזהה את לקוחות החברה ומפגיעה בשירות אותו הן מספקות. סקירת בשלותן של חברות לנתח סיכוני סייבר (cyber risk-maturity) מצביעה על כך שגם בארגונים גדולים קיימים פערים ניכרים ביכולתם לבצע ניהול סיכונים. תשעים אחוזים מהחברות דורגו כבעלות תהליך ניהול סיכונים "מתפתח" או "בתחילת דרכו", ורק חמישה אחוזים מהחברות שהשתתפו בסקר הוגדרו ככאלו שבהן מתקיים תהליך ניהול סיכונים "בוגר".[18]

מעניין לציין כי לא נמצאה קורלציה בין ההוצאה הכספית על ניהול סיכונים לבין בשלות התהליך של ניהול אותם סיכונים. נמצאו חברות שהשקיעו מעט משאבים בתחום זה, אך ביצעו תהליך ניהול סיכונים אפקטיבי, בעוד שאחרות השקיעו משאבים רבים בתהליך ניהול הסיכונים, אולם ללא תְחכום, דבר שהשאיר מקום רב לשיפורים. מנהלים בכירים בתחום הפיננסי, שלא היה להם ידע טכני, התקשו לשלב סיכוני סייבר בתהליך ניהול הסיכונים ולקבל החלטות מושכלות בשל חוסר מידע. זאת ועוד, למרות העיסוק של ארגונים גדולים בהגנה על המידע ובהשקעות כספיות בתחום זה לאורך שנים, הנתונים משקפים את גודל הפער הקיים בין האיומים המתוחכמים בעולם הסייבר ובין יכולתן של חברות להגן על עצמן.

למעשה, ניתן להסיק כי הבעיה העיקרית אותה חווה העולם בהיבט של סיכוני סייבר היא היכולת להעריך את הסיכון, וכפועל יוצא מכך הקושי לתת לו מענה אבטחתי הולם. הקושי להתמודד עם איומי סייבר מורכבים, ומבחן התוצאה העגום

נכון להיום, הובילו למסקנה כי יש צורך בהגברת המומחיות בתחום הסייבר בתוך הארגונים עצמם. כיום ישנה מגמה[19] גוברת בחברות אמריקאיות גדולות למנות מומחי סייבר לתפקידים בכירים בארגון. חברות הנמנות על רשימת Fortune–500 ממנות מומחי סייבר המדווחים ישירות למנכ"ל, לעומת המבנה הנפוץ בו ממונה אבטחת המידע הארגוני (CISO) היה כפוף לסמנכ"ל מערכות המידע הארגוני (CIO). יתר על כן, הדרישות ממי שממלא את תפקיד מומחה הסייבר נוגעות כיום לא רק להבנה טכנית בתחום אבטחת המידע, אלא גם להיכרות מעמיקה עם התהליכים העסקיים והבנה בניהול סיכונים.

בעוד שחברות גדולות מקבלות החלטות אסטרטגיות בנושא אבטחת סייבר ומקימות גופים בעלי ידע וטכנולוגיות שנועדו לנתח את הסיכונים ולשפר את רמת האבטחה סביב נכסי המידע, חברות בינוניות וקטנות מתקשות לעשות זאת בכוחות עצמן. הסיבה לכך היא שאין להן את הגודל והמשאבים ליישם את כלל התהליכים, הטכנולוגיות וההתאמות התכופות הנדרשות בתחום הגנת הסייבר. חברות בעלות משאבים מוגבלים עומדות בפני מספר אפשרויות: יישום הגנות סייבר מינימליות, כמיטב הבנתן ויכולתן התקציבית, וכתוצאה מכך חשיפה לאיומים של גניבת מידע וקניין רוחני, שהרי הן יהיו ככל הנראה חדירות לתוקף נחוש, בין אם במודע ובין אם לא במודע. חברות קטנות רבות, המצומצמות במשאבים, ימנו ברוב המקרים את איש המערכת (System) כגורם המקצועי האמון על אבטחת המידע. טיפולו של אדם כזה יתמקד, במקרים רבים, בנושאים הנמצאים בתחום אחריותו הטכנית, כגון אבטחה של שרתים ותחנות קצה, ניהול משתמשים, אבטחת שרת הדואר ותשתית הרשת. אדם זה לא יקים מערך של אבטחת מידע התואם ניתוח מקצועי של סיכוני הסייבר הרלוונטיים לארגון.

אפשרות אחרת היא שהארגון יגדיל את תקציב הגנת הסייבר שלו כדי לתת מענה הולם לרמת האיומים, ובהתאם לכך גם לניהול הסיכונים. ניתן להניח שהדבר יחייב השקעות משמעותיות בתשתית אבטחת הסייבר, רכישת מוצרים רלוונטיים, הקמת צוות מומחים, הכשרה מקצועית, עמידה בתקנים ועוד. השקעות בתחום זה יקרינו על הרווחיות של הארגון ועל יכולתו להתמודד בשוק תחרותי, תוך ציפייה שלו שהן יחזירו את עצמן. זאת, בראש ובראשונה בהקטנת ההסתברות להיפגע מהתקפות סייבר וביכולת שהן יקנו לארגון לפתח תהליכים עסקיים בסביבה שתהייה מאובטחת כנדרש.

אפשרות נוספת היא להסתמך על שירותי אבטחה מנוהלים. פירוש הדבר הוא לקבל שירותי אבטחה נקודתיים מחברות מיקור חוץ, שבמקרים רבים אינן רואות את התמונה הכוללת של הארגון ואינן נמצאות בתוך התהליכים הקריטיים שנסקרו לעיל. שיטה זו טומנת בחובה יתרון, בעיקר בכך שהיא מאפשרת קבלת שירותים מקצועיים בתחום שלארגון אין ידע או יכולת טכנולוגית וכלכלית להטמיע או

לנהל בעצמו. זאת ועוד, גם העלויות יהיו נמוכות יחסית, מכיוון שנותן השירות מפזר את העלויות על פני מספר רב של לקוחות. מצד שני, גורם חיצוני, שאינו חי את הארגון בצורה יומיומית ואינו שותף לתהליכים העסקיים שלו המשתנים מדי יום, הוא בעל יכולת נמוכה לספק מענה אינטגרטיבי התפור בדיוק לצורכי הארגון. יתר על כן, מיקור חוץ מספק בדרך כלל מגוון שירותים מתומחר, מוגדר, סגור ובדרך כלל גנרי, כך שיתאים לרוב לקוחותיו, דבר היוצר קושי לקבל שירותי אבטחה ספציפיים לצורכי הארגון ובצורה דינמית. שירותי אבטחה מנוהלים יכולים להוות קפיצת מדרגה אבטחתית משמעותית לארגונים קטנים בעלי צרכים ברורים, אולם רק עד גבול מסוים, שבו התהליכים העסקיים הופכים למורכבים.

נראה כי חברות קטנות, המתבססות על הקניין רוחני שלהן, יתקשו להגן על המידע הקנייני ועל תהליכי העבודה שלהן מפני התקפות סייבר מתוחכמות. אותן חברות יסתפקו בפתרון אבטחתי חלקי, מתוך הנחה כי הן לא מהוות מטרה מועדפת לתקיפות מתוחכמות כאלו. פתרון מסוג זה יציב אותן על הקצה העליון של סולם החברות הנמצאות בסיכון גבוה להיפגע מאיומי סייבר, וכן מריגול עסקי ומגניבת מידע וקניין רוחני.

המצב קשה במיוחד במקרה של חברות ההזנק הישראליות. תעשיית המחקר והפיתוח בישראל הינה תעשייה ענפה. מאות חברות נסמכות על תקציב המו"פ של המדען הראשי במשרד הכלכלה ועל גיוסי הון מקרנות למיניהן כדי לפתח ידע, טכנולוגיה ומוצרים. חברות ההזנק הישראליות מאופיינות בכך שהקניין הרוחני שלהן הינו המנוע החשוב ביותר לקיומן ולהתפתחותן. חברות אלו יידרשו לבחור באחת משלוש החלופות שתוארו לעיל. ניתן להניח כי בשל מצוקה תקציבית, ואולי גם מתוך חוסר מודעות, הן יבחרו ליישם הגנות סייבר מינימליות. משמעות הדבר היא שנכסי המידע המתקדמים ביותר ומנוע הצמיחה הפוטנציאלי לכלכלה הישראלית יקבלו הגנות סייבר ברמה הנמוכה ביותר במשק. אפשרות כזאת מהווה נתון מטריד הדורש התייחסות מעמיקה ברמת הלאומית.

נקודה נוספת התומכת בצורך לגבש התייחסות ואסטרטגיה לאומית בתחום הגנת הסייבר של חברות הזנק בישראל היא העובדה כי אחת מדרכי המימון הנפוצות למחקר ופיתוח הינה קבלתו ממשרדו של המדען הראשי במשרד הכלכלה. המדען הראשי מאפשר הקמה של חממות טכנולוגיות על ידי חברות יזמיות ומימון של עד 85 אחוזים מתקציבן, בסכום כולל שנתי של 1.5 מיליארד שקל. הציפייה היא שפירעון המימון הממשלתי יתממש על ידי תשלום תמלוגים למדינה מכל הכנסה הנובעת מהמוצר שפותח במסגרת פרויקט החממה, או ממוצר הנובע ממנו, לרבות שירותים הנלווים למוצר או כרוכים בו. השקעתו של המדען הראשי במחקר ופיתוח מונחת למעשה על קרן הצבי בשל החשיפה העצומה של הטכנולוגיות המפותחות לגניבת הקניין הרוחני. הנזק הצפוי במקרה זה הוא בלתי ישוער: החברות מסַכנות

את יכולתן לממש את תוצרי המחקר והפיתוח, וכפועל יוצא מכך גם את יכולתן לשלם תמלוגים למדינה בגין המימון הממשלתי לאותו מחקר.

תובנות מסכמות

הגנה על מידע וקניין רוחני היא צורך קריטי של כל ארגון עסקי, אזרחי או לאומי. תהליך ההגנה על מידע קניין רוחני הינו מורכב מבחינה טכנולוגית ותהליכית ובעל השפעה משמעותית על תקציבי הפיתוח של הארגון. יישום מוצלח של מעטפת הגנה אפקטיבית על מידע ועל קניין רוחני תלוי בעיקר במודעות הארגון לסיכונים וליכולתו ליישם את מעטפת ההגנה בצורה מיטבית. כל זאת, כפועל יוצא של יכולותיו הכלכליות של הארגון, בשלות התרבות הארגונית בנושא אבטחת מידע, קיומן של פונקציות ארגוניות וכוח אדם מיומן. נדמה שהיכולת הכלכלית לממש פתרונות הגנה מתקדמים מהווה את אחת המגבלות העיקריות בהתמודדות של חברות קטנות ובינוניות עם סיכוני הגניבה של מידע קניין רוחני. עם זאת, קיומה של יכולת כלכלית הינו תנאי הכרחי אולם לא מספיק להתמודדות יעילה עם סיכוני מתקפות סייבר.

מתברר כי לארגונים קשה להעריך את סיכוני הסייבר, וזאת בשל חוסר ידע עדכני, מורכבות הנושא, היעדר משאבים כלכליים, חוסר במיומנויות או מבנה ארגוני לא מתאים (כגון חסרונה של פונקציה האמונה על תחום ניהול הסיכונים והגנת סייבר). מצב זה משפיע על עצם המודעות לסיכוני סייבר ועל המוכנות לפעול נגדם. גם ארגונים עתירי משאבים וכוח אדם מקצועי לא תמיד מצליחים ליישם הגנות מיטביות מול איומי סייבר, המסוגלות לתת מענה אפקטיבי באמצעים השונים של אבטחת המידע. חמור במיוחד הוא מצבן של חברות הזנק, המאופיינות מצד אחד כבעלות קניין רוחני פורץ דרך ובעל פוטנציאל כלכלי אדיר, ומצד שני כבעלות יכולות תקציביות מוגבלות המונעות מהן להקים מערכי הגנה אפקטיביים על הקניין הרוחני יקר הערך שלהן. יתר על כן, חברות הזנק, מעצם טבען, ממוקדות בפיתוח הטכנולוגי ואינן נוטות להקים גופי טכנולוגיית מידע (IT) ואבטחת מידע משמעותיים.

גופים ביטחוניים ותשתיות אזרחיות קריטיות בישראל מוגדרים כגופים מונחים על ידי הרשות לאבטחת מידע (רא"ם) ועל ידי הממונה על הביטחון במשרד הביטחון (מלמ"ב). לעומתם, המרחב האזרחי במדינת ישראל נותר ללא הכוונה או סיוע ברמה הלאומית, ולמעשה אמור להתנהל לפי הבנתו ויכולתו. מטה הסייבר הלאומי אמנם נדרש להתוויית מדיניות כוללת להגנה על מערכות ממוחשבות בישראל ("מדיניות קיברנטית לאומית") ולפיתוח תפיסת הפעלה מדינתית שלה בשגרה,[20] אך הגנה על מידע וקניין רוחני בגופים אזרחיים שאינם מוגדרים כתשתית קריטית אינה חלק עיקרי בפעילותו של מטה זה.

חובה על מדינת ישראל לפעול לשיפור תפקודה בהגנה על ידע שהיא מממנת באמצעות כספי מו"פ, וכן לקדם מהלכים להגנה על מידע וקניין רוחני של המגזר הטכנולוגי והעסקי, שהרי פגיעה בו תקרין ישירות על הכלכלה והתחרותיות של המשק הישראלי כולו. בנוסף לאמור לעיל, יש מקום להקים גוף מייעץ בתחום ההגנה על הידע והקניין הרוחני למגזר האזרחי בכלל ולחברות טכנולוגיות, כגון חברות הזנק, בפרט. יתכן וניתן לעשות זאת באמצעות מטה הסייבר הלאומי.

מענה, ולו חלקי, לאתגרים שתוארו לעיל יוכל להינתן על ידי דרישה של המדינה להגן על ההשקעות שלה מכספי מו"פ. דרישה כזו תוכל לייצר יוזמות אזרחיות עסקיות לאספקת מענה ברמה של מומחיות, ובעלות סבירה, לחברות הממומנות על ידי המדען הראשי של משרד הכלכלה, ולכן טוב יהיה אם יינתן סיוע מדינתי מסוים לבניית תשתית אבטחה שתיועד לחברות הנזקקות. דוגמה לסיוע כזה יכולה להיות בניית יכולות פיתוח ופעולה בענן מאובטח, בסטנדרטים של המערכת הביטחונית או קרובים אליה.

חברה עסקית שתיקח על עצמה לספק פתרונות אבטחה ויכולות פיתוח בתשתית מאובטחת תוכל לעשות זאת רק אם תעריך שיהיו לה מספיק לקוחות וכי המודל העסקי שלה יהיה רווחי. דבר זה יקרה אם חברות הממומנות על ידי המדען הראשי של משרד הכלכלה יונחו לאבטח את הקניין הרוחני שלהן ברמה מספקת, כפי שתיקבע על ידי הגורמים המקצועיים. הפעולה הנדרשת תיצור שילוב בין הדרישה מצד הגורם המממן לפעול בסביבה מאובטחת ובין מתן מענה על ידי חברות אזרחיות, שיספקו סביבה כזאת לשוק מאובטח.

הקמת תשתית ענן מאובטח תיצור "מרחב מוגן" שייתן מענה לצורכי הפיתוח הטכנולוגי של חברות טכנולוגיות, ובהן חברות הזנק. תשתית כזאת תתבסס על מערכות אבטחה שיתמקדו בהגנה על מידע וקניין רוחני ותאפשר לאותן חברות לנהל את המידע הרגיש תחת מעטפת אבטחתית גבוהה בהרבה מזו שיכלו ליצור לעצמן. לשכת המדען הראשי, המתקצבת חממות טכנולוגיות במיליוני שקלים, היא מנוע ההאצה לשימוש בתשתית הענן המאובטח. לשכת המדען הראשי גם שותפה לתוכנית קידמ"ה (קידום מו"פ הגנת הסייבר),[21] יחד עם מטה הסייבר הלאומי, ומתעדפת בתקצוב משופר מחקר ופיתוח בתחום הסייבר במטרה לקדם ולמצב את ישראל כמובילה עולמית בתחום זה. קבלת תקציבים מהמדען הראשי אינה מותנית כיום בהצגת תוכנית הגנה על המידע והקניין הרוחני הנוצר, והחברות המתוקצבות במיליונים ומפתחות טכנולוגיות האמורות להיות מנוע הצמיחה הכלכלי של מדינת ישראל חשופות למעשה להתקפות סייבר, שהנזק הגלום בהן הינו עצום.

בעולם בו התקפות סייבר מתוחכמות ממוקדות בגניבת מידע שמטרתה היא לקצר תהליכים טכנולוגיים, נראה כי הקמת גוף מייעץ מקצועי לחברות טכנולוגיות

אזרחיות, וכן פיתוח תשתית ענן ייעודית מאובטחת ברמה גבוהה, ישנו בצורה דרמטית את סיכוייהן של חברות ההזנק לשרוד ולהגן בהצלחה על הקניין הרוחני שלהן. מדינת ישראל תוכל, באמצעות מהלך כזה, לקיים מנגנון אבטחה מחייב ולוודא החזר ההשקעה שלה במחקר ופיתוח.

הערות

1 Doron S. Ben-Atar, Trade Secrets: Intellectual Piracy and the Origins of American Industrial Power (New Haven: Yale University Press, 2004).

2 במקרים רבים מועברות תוכניות ייצור של מכלולים במוצר (מארזים, מעגלים מודפסים, רכיבים אלקטרוניים ועוד) לגורמי הייצור הקבלניים באמצעות מדיה מגנטית. הדבר נעשה אם בהעברה פיזית של מדיה כזאת ואם באמצעות תקשורת מחשבים.

3 Tucker Bailey, Andrea Del Miglio, Wolf Richter, "The rising strategic risks of cyberattacks," *McKinsey Quarterly*, May 2014, http://www.mckinsey.com/insights/business_technology.

4 מערכות כאלו מכונות בשם: Data Leakage Prevention

5 שרשרת האספקה בארגון מנהלת את תהליכי הרכש, הייצור, האחסון, ההפצה והתובלה, ותפקידה הוא לקשר בין היצרנים, הספקים ולקוחות הקצה. ניהול שרשרת האספקה מצריך גמישות ותיאום גבוהים מול גורמים חיצוניים ומהווה מרכיב חשוב ביצירת הערך לחברה.

6 שירותי ענן דוגמת: Jambo Mail, Google Drive, DropBox ודומיהם.

7 Bailey, Del Miglio, Richter, "The rising strategic risks of cyberattacks."

8 ההתקפה על רשת Target האמריקאית, שבמהלכה נגנבו מיליוני כרטיסי אשראי, החלה בגניבת הרשאות הגישה של ספק מערכות תחזוקה שנתן שירותים לרשת זו. ראו: Brian Krebs, "Target Hackers Broke in Via HVAC Company," Krebs on Security, February 14, 2015, http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

9 SEIM - Security Event Information Management

10 "2013 Cost of Cyber Crime Study: United States," Ponemon Institute, October 2013.

11 "APT1 Exposing One of China's Cyber Espionage Units," Mandiant Report, February 2013, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

12 Bailey, Del Miglio, Richter, "The rising strategic risks of cyberattacks."

13 Franz-Stefan Gady, "New Snowden Documents Reveal Chinese Behind F-35 Hack," *The Diplomat*, January 27, 2015, http://thediplomat.com/2015/01/new-snowden-documents-reveal-chinese-behind-f-35-hack./

14 "Mtrends: Beyond the Breach," Mandiant 2014 Threat Report, https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf

15 McAfee, "The Economic Impact of Cybercrime and Cyber Espionage," Center for Strategic and International Studies, July 2013, http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf

16 ראו ניתוח מפורט של מתקפה זו בתוך: גבי סיבוני וסמי קרוננפלד, "לוחמת הסייבר של איראן", **צבא ואסטרטגיה**, כרך 4, גיליון 3, דצמבר 2012, http://media.wix.com/ugd/d48d94_1f8bd495a0554e44967b99e25e931eae.pdf

17 Bailey, Del Miglio, Richter, "The rising strategic risks of cyberattacks."

18 שם.

19 Nadia Damouni, "U.S. companies seek cyber experts for top jobs, board seats," Reuters, May 30, 2014, http://www.reuters.com/article/2014/05/30/us-usa-companies-cybersecurity-exclusive-idUSKBN0EA0BX20140530.

20 מתוך דף הבית של מטה הסייבר הלאומי באתר נציבות שירות המדינה: http://www.csc.gov.il/DataBases/NewsLetters/NewsLetters3/Pages/CyberHeadquarters.aspx

21 ראו חוזר המדען הראשי במשרד הכלכלה: "תוכנית קידמ"ה (קידום מו"פ הגנת הסייבר (לקידום יכולות התעשייה הישראלית בתחום הגנת הסייבר", 21 בנובמבר 2012, http://www.moital.gov.il/NR/rdonlyres/89646959-5455-4A5A-99FD-C4B07D07E8E5/0/syber122012_3.pdf

האמנם קרסה תיאוריית "קורי העכביש"? – על הרגישות לחללים ב"צוק איתן"

יגיל לוי

השיח הציבורי במהלך מבצע "צוק איתן" סימן רמה גבוהה של נכונות חברתית להשלים עם חללים צבאיים בהשוואה למלחמות או למבצעים קודמים, במיוחד ביחס למלחמת לבנון השנייה. במאמר זה אבקש לברר את הטענה הרווחת באשר לחיזוק הנכונות החברתית להשלים עם חללים צבאיים, ולהראות שאין לקבלה כפשוטה. טענתי היא שהרגישות לחללים קיימת, אבל היא מורכבת יותר מכפי שהיא נראית וגם מושפעת מנסיבות משתנות. כאשר, כמאפיין את "צוק איתן", הפעולה הצבאית הינה אינטנסיבית, קצרה ונתפסת כמוצלחת, וכאשר הקרבתן של הקבוצות החברתיות המבוססות אינה ניכרת, ואף מוצדקת בנסיבות של בחירה מרצון, הצדקתו של המוות הצבאי קלה יותר והוא אינו מעורר התנגדות של ממש.

מילות מפתח: העברת סיכון, מוות צבאי, מיפוי הרוגים, מניעת נפגעים, פעולה קולקטיבית, רגישות לחללים, שיח השכול

מבוא

השיח הציבורי במהלך מבצע "צוק איתן" (יולי–אוגוסט 2014) סימן רמה גבוהה של נכונות חברתית להשלים עם חללים צבאיים בהשוואה למלחמות או למבצעים קודמים, במיוחד ביחס למלחמת לבנון השנייה – הסבב האלים האחרון שבו נפלו עשרות חיילים. מבצע "צוק איתן", שארך חמישים יום, היה תגובה של ישראל להסלמה שחלה בירי רקטות וטילים מרצועת עזה לישראל, הסלמה ששני הצדדים לא שלטו בהתפתחותה.[1] במשך עשרת הימים הראשונים של המבצע תקף צה"ל מהאוויר, מהיבשה ומהים את הרצועה, חמאס ירה רקטות על יישובים ישראליים

פרופ' יגיל לוי הוא חבר סגל האוניברסיטה הפתוחה

ונעשו מספר ניסיונות של כוחות חמאס לחדור לישראל דרך מנהרות שחפר הארגון. הצעה של מצרים להפסקת אש נתקלה בסירוב של חמאס לקבֵּלה. אז פתחה ישראל במבצע קרקעי שנועד להרוס את המנהרות. הפעולה הקרקעית ארכה כשבועיים וחצי נוספים, ורק לאחר עוד שלושה שבועות של הפגזות של צה"ל מהאוויר, מהיבשה ומהים, הושגה הפסקת אש.

65 חיילים נהרגו במבצע "צוק איתן", אך מותם לא עורר מחאה ציבורית או ביטויי התנגדות להמשך הלחימה. על רקע זה נשמעה טענה כי קרסה תיאוריית "קורי העכביש" – התיאוריה על כושר העמידה הרעוע שמזכ"ל חזבאללה, חסן נסראללה, ייחס לחברה בישראל. חדה במיוחד בהקשר זה הייתה הבחנתו של חוקר התרבות פרופסור ישי רוזן־צבי, שבדברים שנשא בכנס באוניברסיטת תל אביב אמר: "מוות של חיילים לא מייצר יותר אותו לחץ ציבורי כשהיה בעבר. זהו מנגנון חדש ואחר מזה שהכרנו, שבו ארונות קבורה יצרו תחושת מיאוס שהביאה ביקורת ולחץ תקשורתי".[2]

התרשמותו של פרופ' רוזן־צבי קיבלה ביסוס במחקר של ציפי ישראלי ואלישבע רוסמן, שבדק את הסיקור התקשורתי במהלך מבצע "צוק איתן". לפי המחקר, אמנם סוקרו במהלכו נפגעים, אך לא בצורה ביקורתית כבעבר, וגם אם הושמעה ביקורת כלפי הדרג המדיני על אופן ניהול המבצע, היא לא שילבה את המחיר האנושי שלו. הקורבן הוצג כהכרח, החיילים שהקריבו את חייהם הוצגו כגיבורים והשיח לא חזר לדפוס העבר של התמסרות לשכול.[3] עמדה מנוגדת השתקפה בעדויות של ארגון "שוברים שתיקה" על המבצע. סיכום התחקירים שערך הארגון קבע כי העיקרון שהנחה את המדיניות הצבאית במהלך "צוק איתן" היה מינימום סיכון לכוחותינו, גם במחיר פגיעה באזרחים חפים מפשע. מדיניות זו הביאה, לפי "שוברים שתיקה", לפגיעה ניכרת באוכלוסייה האזרחית ברצועת עזה.[4]

לפנינו שתי גישות שונות, שלכאורה לא סותרות זו את זו. ועדת וינוגרד, שחקרה את מלחמת לבנון השנייה, מצטטת את ראש המוסד דאז, מאיר דגן, שאמר בדיון במהלך המלחמה כי "לדעתי, הטראומה של לבנון יושבת יותר אצל הדרג המדיני מאשר אצל הציבור".[5] בכך הוא קלע להבחנה המקובלת בתיאוריה כי המנהיגים חוששים לעיתים שהציבור לא ישלים עם קורבנות, וחשש זה מביא לצמצום סיכונם של החיילים עד כדי ביטול משימות, או לחילופין למדיניות אש אגרסיבית שתצמצם אף היא את סיכון החיילים. כלומר, מקור המחשבה כי מראה ארונות המתים מחולל התנגדות, הוא לא אחת בשיח הפוליטי ולא בדעת הקהל, וודאי שאינו נובע מהתנהגות קבוצתית מאורגנת. הפוליטיקאים תופסים את הציבור כרגיש מכפי שהוא באמת, ולכן נוטלים על עצמם אילוצים, לכאורה מרובים מדי.[6] למרות זאת, הסתירה שהוצגה לעיל מצדיקה ברור.

במאמר זה אבקש לברר את הטענה הרווחת באשר לחיזוק הנכונות החברתית להשלים עם חללים צבאיים, ולהראות שאין לקבלה כפשוטה. טענתי היא שהרגישות לחללים קיימת, אבל היא מורכבת יותר מכפי שהיא נראית וגם מושפעת מנסיבות משתנות. כאשר הפעולה הצבאית הינה אינטנסיבית, קצרה ונתפסת כמוצלחת, וכאשר הקרבתן של הקבוצות החברתיות המבוססות אינה ניכרת, ואף מוצדקת בנסיבות של בחירה מרצון, הצדקתו של המוות הצבאי קלה יותר והוא אינו מעורר התנגדות של ממש.

החלק הראשון של המאמר יציג את הרקע לדיון ואת מסגרתו התיאורטית. החלק השני יציג מספר היגדים הבוחנים הסברים שונים לאי־התפתחותה של התנגדות פעילה להקרבת חיים במהלך מבצע "צוק איתן".

רקע ותיאוריה

רגישות לחללים צבאיים התפתחה בחברה בישראל בעיקר מאז מלחמת לבנון הראשונה (1982), בדומה לתסמונת שהתפתחה בדמוקרטיות אחרות. שיח השכול שיקף את השינוי. עד מלחמת לבנון הראשונה, מותם של חיילים נתפס כהכרח, כחלק מ"מגש הכסף" שעליו ניתנה עצמאות המדינה. שיח השכול ההגמוני התאפיין אז בהשלמת המשפחות השכולות עם אסונן. המדינה העניקה להן כבוד ויוקרה והפכה את הנופלים לסמלי הנצחה לאומיים, ובתמורה לכך קיבלו המשפחות את קורבנן בהשלמה. ביקורת או תהייה על נסיבות נפילתו של הבן לא היו חלק מהשיח.[7] גישה זאת החלה להשתנות כבר במלחמת יום הכיפורים, כאשר מקצת המשפחות השכולות נכנסו לזירה הפוליטית והצטרפו לתביעה לפטר את שר הביטחון משה דיין, שנתפס כאחראי ל"מחדל" במלחמה. עם זאת, רק בעקבות מלחמת לבנון הראשונה החלו להישמע קריאות תגר ממשיות, שקעקעו את ההסכמיות סביב תביעת המדינה להקרבת חיים בשדה הקרב, והשיח הפך לביקורתי ואף למתריס.

"משפחת הבופור" – ההורים השכולים שמחו על מות בניהם בקרב על מוצב הבופור בלילה הראשון של מלחמת לבנון הראשונה – הייתה מהקבוצות הראשונות שהטילו ספק בצדקת המלחמה. קריאות תגר אלו המשיכו עם "חיילים נגד שתיקה", שמחו על מחיר הדמים של מלחמת ההתשה בלבנון (1982–1985). אותם חיילי מילואים משוחררים הניפו שלטים מול ביתו של ראש הממשלה מנחם בגין, עליהם צוין מספר החללים העדכני. לשיא הגיעה התופעה בתנועת "ארבע אימהות", שמחתה על מחיר השהייה בדרום לבנון בעקבות אסון המסוקים של 1997 ומילאה תפקיד בהוצאתו של צה"ל משם בשנת 2000. דומים להם היו ארגוני המחאה שפעלו בעקבות מלחמת לבנון השנייה (2006), כמו ארגונים של חיילי מילואים והורים שכולים. אלה מחו על תפקודו של הצבא במלחמה, שלטענתם

גרם לקורבנות שהיה אפשר למנוע, או, לחילופין, ניתן היה להצדיק אם מטרות המלחמה היו מושגות.

תנועות המחאה מינפו את הלגיטימיות של הדרישה להשמעת קול בזירה הציבורית בשם ההקרבה בצבא, הן כחיילי מילואים והן כהורים לחיילים. שני מהלכי הנסיגה החד־צדדית מלבנון, בשנים 1985 ו־2000, שנעשו בהשפעת המחאה על הקרבת החיים בזירה זו, היו ביטוי מובהק לשינוי בשיח השכול ולהשפעתו על פריסת צה"ל.[8]

התעצמות השיח הביקורתי הטילה מגבלות על חופש הפעולה של הממשלות ושל מפקדי צה"ל לסכן חיילים. שיאן של מגבלות אלו הגיע במלחמת לבנון השנייה, כאשר הממשלה נמנעה עד לרגע האחרון מלצאת לפעולה יבשתית נרחבת בעומק לבנון. ועדת וינוגרד, שחקרה את המלחמה, קבעה בהקשר זה: "צה"ל התנהל במלחמה כמי שהחשש מנפגעים בקרב חייליו שימש מרכיב מרכזי בהליכי התכנון ובשיקוליו המבצעיים. עם כל הרגישות שיש לייחס לחיי החיילים, והצורך להביא גורם זה בין השיקולים המנחים, קשה לקבל את ההשפעה יוצאת הדופן שהייתה לשיקול זה על ההחלטות של המפקדים הבכירים (ושל מקבלי ההחלטות בדרג המדיני)".[9]

גם מפקדי צה"ל נתנו ביטוי להבנתם כי החברה מתקשה יותר מבעבר לשלם את מחיר הנפגעים וכי שינוי זה מגביל את הפעלת הצבא.[10] החשש מנפגעים הרתיע מראשית שנות האלפיים ייזום של מבצעים יבשתיים ברצועת עזה, ומשאֵלָה בוצעו, הופעלה מדיניות אש אגרסיבית שצמצמה את הסיכון לחיילים והעבירה אותו בחלקו לתושבי הרצועה. מִתאם ברור מזוהה מאז בין הגברַת הרגישות החברתית לחללים ובין הנטייה למדיניות אש אגרסיבית. גישה זו חייבה את מקבלי ההחלטות להשתמש בכוח רק משניתן היה לתבוע לגיטימיות גבוהה להפעלת מדיניות אש אגרסיבית שתעביר חלק מהסיכון מחיילי צה"ל לאזרחים העזתיים. כאשר לא הושגה לגיטימיות כזו, העדיפו מקבלי ההחלטות ריסון צבאי (כמו הסדרי הפסקת האש עם חמאס, בדומה לאלה שהושגו עם חזבאללה בלבנון) במקום שימוש מוגבל בכוח שיגביר את הסיכון לחיילי הצבא.[11]

לכאורה, תסמונת זו של רגישות לחללים לא שבה והופיעה ב"צוק איתן". גם אם צה"ל דבק בגישה של העברת הסיכון מחיילים לאזרחי האויב מתוך הפנמה של רגישות חברתית לחללים, כפי שטוענים אנשי "שוברים שתיקה", יהיה מי שיטען כי הממשלה וצה"ל יכלו ליטול סיכונים גדולים יותר לאור השינוי בנכונות החברתית לקבל מספר גבוה יותר של הרוגים מקרב החיילים. את מידת הרגישות ב"צוק איתן" אבקש לברר בהמשך מאמר זה.

תסמונת הרגישות לחללים (casualty sensitivity) התפתחה בדמוקרטיות המתועשות מאז שנות השישים של המאה העשרים. מלחמת וייטנאם סימנה נקודת

מפנה בסוגיה זאת, וממנה ואילך נטבע המושג של מדיניות מניעת נפגעים (casualty aversion), כלומר הפחתת הסיכון לחיילים. זאת, אם על ידי הימנעות מביצוע משימות עתירות סיכון ואם על ידי ביצוען באופן המגביר את מיגונם של החיילים, לרבות על ידי הגברת השימוש בטכנולוגיה, או באופן המרחיק חלק מהסיכון אל עבר אזרחי האויב באמצעות מדיניות אש אגרסיבית.[12] תסמונת זו התפתחה ככל שהתחזקה התרבות הליברלית, על יסודותיה החומרניים, וירדה תחושת האיום הקיומי, בפרט עם סיום המלחמה הקרה.[13] הדבר הוביל להתפתחותה של תרבות פוסט־הירואית, שבה סיכון חיילים מהווה אילוץ מרכזי בהתווייתה של המדיניות הצבאית.[14]

לצד ההסבר הסוציולוגי, חוקרי יחסים בין־לאומיים ומדע המדינה מציעים הסברים המזהים את המשתנים המגבירים או מחלישים את הרגישות לחללים, וזאת בהינתן תרבות פוליטית שאינה סובלנית לקורבנות. אני מבקש להציע תבנית המבוססת על שתי שכבות, כמסגרת תיאורטית שתנחה את הדיון האמפירי: השכבה הראשונה היא טיעונם של אנשי מדע המדינה האמריקאיים, גֶלְפִּי, פִּיבֶּר ורַייפְלֶר, לפיו המשתנה המסביר רגישות לחללים במצב תרבותי־פוליטי נתון אינו מספרם המצטבר של החללים או האיום שמותם נועד לסלק (ומשתנים אחרים שהסבירו מחקרים קודמים); לפי מחקרם של השלושה, הציבור האמריקאי יתמוך בהמשכה של פעולה צבאית גם כאשר מספר חלליה ילך ויגדל. התמיכה תנבע מאינטראקציה של שני משתנים: הציפייה כי הפעולה הצבאית תשיג את מטרותיה והאמון בצדקתה של ההחלטה הבסיסית להשתמש בכוח.[15]

המשתנה של גלפי, פיבר ורייפלר מהווה הסבר משכנע, בפרט אם נזכור כי במציאות הישראלית מספר החללים לא תמיד מסביר את המחאה, או לחילופין, את ההסכמה שהתפתחה סביב השכול. עם זאת, חולשתו של משתנה זה היא בכך שהוא נשען בלעדית על מחקרי דעת קהל ולא נותן משקל ראוי לכך ששינויים בה, בעיקר כאלה המשפיעים על מקבלי ההחלטות, מתפתחים לא אחת כאשר מתעוררת מחאה, כלומר מתפתחת פעולה קולקטיבית נגד מחיר המלחמה. כך היה במקרה האמריקאי בווייטנאם, וכך היה גם במקרה הישראלי שבו, כפי שנסקר למעלה, תנועות מחאה חוללו תפנית בדעת הקהל, ובעקבות כך גם הביאו לשינוי במדיניות.

פעולה קולקטיבית חתרנית מתפתחת בעיקר מקרב שורותיהן של הקבוצות המבוססות, בעלות הזמן, המשאבים, הכישורים והתעוזה לחולל מחאה, בנסיבות שבהן הן נושאות בנטל ניכר. לכן יש מקום לשלֵב משתנה נוסף ולשאול מי הן הקבוצות החברתיות הנושאות בנטל החללים, ועל כן קורבנן עשוי לעודד אותן לפתח תובנות ביקורתיות ביחס להקרבתן ולתרגם תובנות אלו לשיח שכול ביקורתי, וממנו למחאה. מחקרים מראים מִתאם בין התנגדות פעילה למלחמה

ולקורבנותיה ובין מוצא חברתי מבוסס של הנושאים בנטל ההקרבה. ממצא זה מביא לכך שהמעבר מגיוס חובה לצבא של מתנדבים מחליש את הפוטנציאל למחאה במרבית הדמוקרטיות (בשל המדרג החברתי הנמוך יותר של המתנדבים), גם כשמספר החללים גדֵל.[16]

לטיעון זה שני יתרונות: ראשית, הוא הופך את הטיעון של גלפי וחבריו כי "ההצלחה קובעת" למורכב יותר ומעניק משקל לפרשנותן של קבוצות שונות – פרשנות המושפעת ממעמדה החברתי של כל קבוצה – לשאלה האמנם הפעולה הצבאית משיגה את יעדיה והאם הקורבן הולם את היעדים המושגים; שנית, הוא פותח אפשרות שדעת קהל ביקורתית לא תתורגם למחאה, בעיקר בנסיבות שבהן קבוצות חברתיות ממדרג נמוך נושאות בנטל ההקרבה. במצב כזה, דעת הקהל גם לא תגרום לשינוי בפריסת הצבא (דוגמת הפעלת לחץ אפקטיבי להפסקת הפעולה הצבאית).

השילוב של שני הטיעונים התיאורטיים המשלבים את משתני ההצלחה, הצידוק, וההרכב החברתי מוביל להנחה כי ההכרה בצדקת השימוש בכוח והציפייה להצלחתו יגבירו את הנכונות החברתית לקבל מספר גבוה של חללים, וזאת ככל שהקבוצות המקריבות אינן ממדרג גבוה. לעומת זאת, ככל שהקבוצות המקריבות הן ממדרג גבוה, ניתן לצפות לקריאה ביקורתית יותר של המציאות, כלומר, לקריאה ביקורתית את צדקת השימוש בכוח ואת מידת ההצלחה של התממשותו ביחס למספר החללים (וביחס לקורבנות אחרים, כמו המחיר הכלכלי הכרוך בלחימה). לקריאה ביקורתית זו יש פוטנציאל של תרגום להתנגדות פעילה למדיניות הצבאית.

להלן כמה היגדים שיאירו מגוון היבטים של הרגישות לחללים ב"צוק איתן" וינסו לענות על השאלה מדוע לא התפתחה בישראל רגישות לחללים במבצע זה.

היגד ראשון – מלחמה אינטנסיבית לא הביאה להתפתחות רגישות למחאה

מחאה התפתחה בעבר רק לאחר סיום הקרבות. כך, למשל, "משפחת הבופור" הופיעה לאחר ימי הלחימה הראשונים של מלחמת לבנון הראשונה, עם סיום החלק "הרשמי" שלה. כך גם היה במלחמת לבנון השנייה. בניגוד למצטייר בזיכרון הקולקטיבי, סימני השאלה סביב נסיבות המוות של החיילים בשתי מלחמות אלו הופיעו רק כשבוע לאחר סיום הקרבות, עם הצטרפותם של הורים שכולים למעגל המחאה המתפתחת. המסקנה הנובעת מכך היא שארונות מתים אינם מעוררים תגובה ביקורתית מיד עם הופעתם.

מחאה התפתחה בעבר גם בנסיבות של מלחמת התשה ממושכת. כך היה במלחמת ההתשה הלבנונית (1982–1985), וכך היה עם ארגון "ארבע אימהות", או עם המחאה שפיתחה תנועת "שובי" בשנת 2004 נגד הקרבת חיילים ברצועת עזה במהלך האינתיפאדה השנייה.

את מבצע "צוק איתן" ניתן לשייך לקטגוריה של מלחמה אינטנסיבית. רוב החללים במבצע זה נפלו במהלך כשבועיים בלבד, במיוחד בפעולה הקרקעית, במה שיכול היה להיתפס כלחימה אינטנסיבית אך גם תחומה בזמן וביעדים (ראו בהמשך). בנסיבות אלו, הפוטנציאל להתפתחותן של רגישות ומחאה היה נמוך. סביר להניח שהרגישות והמחאה היו גוברות ככל שהפעולה הקרקעית הייתה מתארכת ועימה גדֵל מספר ההרוגים, או שהן היו מתעוררות לאחר הלחימה, אם זו הייתה מצטיירת כמי שהחמיצה את יעדיה, סוגיה שנברר מיד.

היגד זה מאמץ חלקית את טענתו הקלאסית של ג'ון מוּלר, לפיה עלִיה במספר המצטבר של חללים תגביר רגישות, ובכך תחליש את התמיכה הציבורית בפעולה הצבאית.[17] עם זאת, כפי שהראו מחקרים אחרים המצוטטים במאמר זה וכפי שאחדד בהמשך, מִספרים בלבד אינם מחוללים שינוי, אלא אם מפרשים אותם בהקשר לאופן שבו מתנהלת הפעולה, למטרותיה ולהישגיה.

היגד שני – רגישות המעוררת מחאה תלויה באופי הלחימה ובפרשנותה הפוליטית

רגישות משמאל יכולה להופיע בצורה של התנגדות להקרבה כאשר זו נראית כחסרת תכלית פוליטית, כמו הטענה כי מלחמת לבנון הראשונה הייתה "מלחמת ברירה" – טענה שתדלקה את המחאה משמאל. רגישות כזו אפיינה את המחאות של "משפחת הבופור", "ארבע אימהות", "חיילים נגד שתיקה" ו"שובי", אם כי למעשה, אפילו תנועת "ארבע אימהות" לא שללה את צדקת נוכחותה של ישראל בדרום לבנון, אלא רק את יעילותה לנוכח המחיר שגבתה. מחאות מהסוג שתואר לעיל יכולות להציע חלופה מדינית או חלופה לא אלימה או כזו הכרוכה בפחות אלימות להקרבה הצבאית (דוגמת התביעות של "ארבע אימהות" או "שובי" להגן על גבולות המדינה מהקו הירוק ובכך גם להפחית את אלימות הצד הערבי).

רגישות מימין יכולה לעודד מחאה על קורבן שאינו מוצדק בשל אי־השגת התכלית, כאשר התכלית עצמה, שבעטיה הוקרבו החיים, נתפסת כצודקת. זה סוג הרגישות שהתפתחה בעקבות מלחמת לבנון השנייה. מחאתם הבולטת של מקצת ההורים השכולים בעקבות מלחמה זו לא ביקשה בהכרח לחסוך את הקורבן, אלא להפוך אותו למשמעותי, לכזה המשיג תכלית. הורים שכולים, שִמָחוּ על ההסכמה להפסקת אש ללא פעולה קרקעית מאסיבית שתחסל את איום הטילים והרקטות על ישראל, אפילו הביעו (אם כי במשתמע ובדיעבד) נכונות לקורבן גדול יותר, ובלבד שישיג תכלית צבאית משמעותית.[18]

המשותף לימין ולחלק מהשמאל הוא, אפוא, הנכונות להקריב, ובלבד שלהקרבה יהיו ערך והכרח. לכן, ארונות המתים לא מעוררים תחושת מיאוס אוטומטית; התחושה מותנית בנסיבות, כטענתם של גלפי וחבריו. במילים אחרות, האמון כי

הלחימה היא הכרחית ומשיגה את יעדיה יגביר את הנכונות לקבל חללים, וההיפך. זה אשר אירע ב"צוק איתן".

הממשלה והצבא לא רצו מלכתחילה בפעולה קרקעית במבצע "צוק איתן". חשש מנפגעים הניא את ההנהגה הישראלית מפני יציאה למבצע יבשתי, מתוך הנחה שמבצע כזה יחייב הפעלת אש אגרסיבית כדי להקטין את הסיכון לחיילי צה"ל, אך בכך יחשוף את ישראל לביקורת בין־לאומית.[19] לבסוף נגררה ישראל למבצע היבשתי בשל סירוב חמאס להצעה המצרית להפסיק את האש בתום עשרת ימי הלחימה הראשונים. התגלותו של מה שנתפס כאיום המנהרות לא רק העניקה לגיטימיות מבית (ואפילו לחץ פנימי) ובזירה הבין־לאומית לפעולה קרקעית, אלא גם אפשרה למקד את הפעולה באיום שיש לו יעד קונקרטי.

בשונה ממלחמת לבנון השנייה, הפעולה הקרקעית במבצע "צוק איתן" לא נועדה להפסיק את ירי הרקטות והטילים על העורף. פעולה קרקעית שזוהי תכליתה הייתה נכשלת ומצטיירת כלא אפקטיבית, בוודאי בשלביה הראשונים, דבר שהיה מכרסם בצידוק להקרבת חיי חיילים. להבדיל, הקורבן ב"צוק איתן" הוצדק בצורך להסיר איום מוחשי יותר – איום המנהרות – שהשיח הציבורי הציג אותו בצורה דמונית שפרטה על נימי הפחד של הישראלי הממוצע.[20]

מאמץ לשתק ירי על העורף הוא מעשה שההצלחה שלו מדידה, ולכן גם חשוף לביקורת. לעומת זאת, מאמץ לסלק איום עתידי הוא מהלך שהצלחתו אינה מדידה. מה שהיה מדיד במהלך זה במבצע "צוק איתן" היא הערכת המאמץ הצבאי ביחס למספר המנהרות שנהרסו ולזמן שהדבר דרש. זוהי מדידה של תשומות (מנהרות הרוסות) ולא של תפוקות (שיפור הביטחון) והיא מקלה על היכולת של מקבלי ההחלטות לשכנע את מובילי דעת הקהל בדבר האפקטיביות של הפעולה הנמדדת. לכן, פרויקט כזה כמעט שאינו יכול שלא להצליח, ומעצם טבעו הוא מספק לגיטימיות להקרבה.

ואכן, בציבור היהודי בישראל הייתה עם סיום המבצע הקרקעי הסכמה רחבה (של 92 אחוזים) כי היציאה למבצע הקרקעי הייתה מוצדקת, וכמחצית מהנשאלים בסקרים סברו כי מטרותיו הושגו, לפחות בחלקן.[21] גם אם במהלך המבצע היבשתי נשמעה ביקורת, הרי שזו התמקדה בזמן שלקח להרוס את המנהרות ובאופן הניהול הטקטי של המבצע, אך לא בעצם צדקתה של הפעולה והמחיר שהיא דרשה.[22] סביר להניח שאם המבצע הקרקעי היה מתארך, בעוד שגרף החללים עולה, הייתה מתפתחת רגישות מצמיחת התנגדות, לא כל שכן לו מטרת המבצע הייתה לשתק את הירי על העורף ולא לטפל במנהרות. שונה המצב כשמדובר במבצע בן שבועיים וחצי שלו מטרות בנות השגה.

הממשלה כך תרמה להבניה של שיח ציבורי המנתק את המאמץ הכושל לשתק את הירי על העורף מהמאמץ שנראה מוצלח להרוס מנהרות. מרבית החללים, 44

חיילים, נפלו בפעולה הקרקעית (האחרים נהרגו מהתקפות על ריכוזי הצבא מחוץ לרצועת עזה), אך מותם לא העלה סימני שאלה. לכן, משהפעולה נגד המנהרות מיצתה את עצמה והפוליטיקאים נדרשו לבחור בין סיום הלחימה ובין פעולה קרקעית רחבה לכיבוש רצועת עזה, שתְגבה את חייהם של מאות חיילים, הם בחרו באפשרות הראשונה.[23]

בנסיבות אלו, הפוטנציאל למחאה לא היה גבוה גם לאחר שתמה הלחימה. בהשוואה בין מבצע "צוק איתן" למלחמת לבנון השנייה, נמצא כי שבעים אחוזים מהציבור היהודי סברו בשבועות שלאחר סיום "צוק איתן" והשגתה של הפסקת האש כי המבצע לא השפיע על הביטחון הלאומי של ישראל או אף הרע אותו; בשבועות שלאחר מלחמת לבנון השנייה סבר שיעור דומה של הציבור היהודי (68 אחוזים) כי המלחמה הסתיימה בהחלשה מסוימת או רבה של כוח ההרתעה הישראלי אל מול העולם הערבי. כלומר, עוצמת הביקורת לאחר מלחמת לבנון השנייה עלתה על זו שלאחר מבצע "צוק איתן", כשרוב הציבור סבר לאחר המלחמה שהמצב הביטחוני הורע בעוד שלאחר "צוק איתן" הדעות על כך היו חלוקות בקרב שיעור דומה של נשאלים.[24] ההבדל בין יעדי שתי המלחמות ואופן האמידה של מימושן הוא שגרם לשוני זה, הגם שבשני המקרים כשלה ישראל במאמציה לשתק בדרך צבאית את הירי על אוכלוסייתה, וזה פסק רק בעקבות הסדר של הפסקת אש.

זאת ועוד, במלחמת לבנון השנייה נפלו חיילים במקביל להיפגעות אזרחים מירי חזבאללה ולפגיעה כבדה ברכוש. לעומת זאת, היפגעות אזרחים ורכושם ב"צוק איתן" הייתה מצומצמת הודות ל"כיפת ברזל": שבעה אזרחים נהרגו ב"צוק איתן" (כולל עובד זר וחייל בחופשה) לעומת 44 אזרחים שנהרגו במלחמת לבנון השנייה. כך נותק עוד יותר צידוקו של המוות הצבאי ממידת הצלחתו להסיר את האיום המיידי על העורף. "ההצלחה", במונחי גלפי ושותפיו, הייתה מובטחת, ועימה גם הרחקת התפתחותה של הרגישות למוות הצבאי.

הצדקת המוות הצבאי ניזונה בנסיבות אלו גם מגורם נוסף. אם שוב נידרש למחקר השוואתי, הצגה של נתונים על אובדן חיי אדם אצל האויב מסייעת לריכוך המידע על מות חיילים ולשיפור הדימוי הציבורי של הפעולה הצבאית כמי שאכן מצליחה לממש את מטרותיה.[25] כך היה גם במבצע "צוק איתן": סיקור נרחב של הנזק וההרג שנגרם לצד הפלסטיני מילא תפקיד בהצדקת הקורבנות של הצד הישראלי, שמספרם היה נמוך בהרבה מזה של הצד השני. "דובר צה"ל", כתב רביב דרוקר, "מעוניין שנראה את מה שקורה בעזה, כי זה יראה מה צה"ל עושה, יקטין את הלחץ של הציבור על מקבלי ההחלטות לעשות משהו, כאילו שאינם עושים".[26]

הקושי להצדיק את המוות הצבאי בדמוקרטיות גובר במצבים שבהם חיילים נתפסים כמי שסיכנו את חייהם כדי להגן על אזרחי האויב.[27] המדובר במוות שניתן

היה לחסוך לו הופעלה מדיניות אש אגרסיבית יותר. לכן, בעקיפין, הצגת אובדנו של האויב מחלישה את הפוטנציאל לביקורת, בפרט בנסיבות שבהן הציבור מצדיק מאוד את השימוש בכוח. כ־93 אחוזים בציבור היהודי האמינו במהלך מבצע "צוק איתן" כי צה"ל עשה שימוש מתאים בכוח, ואפילו בפחות מדי כוח.[28] לכן, ניתן להבין איך מראות ההרס וההרג מרצועת עזה לא אוזנו בביקורת פנימית, אלא אף תורגמו במישרין לתחושת הישג.

המצב שתואר לעיל היה הרקע לכך, שכאשר חיילים החלו להיפגע בפעולה הקרקעית במבצע "צוק איתן", מדיניות האש הפכה לאגרסיבית יותר, וזאת כדי להגן עליהם ולו במחיר פגיעה באזרחים עזתיים.[29] הנטייה להעברת סיכון מחיילים לתושבי הרצועה גברה במבצע זה ביחס לסבבי אלימות קודמים שם.[30] הפוליטיקאים ואנשי הצבא יודעים כי רגישות לחללים מבית תאיץ את סיום המלחמה מהר יותר מאשר לחץ בין־לאומי המושפע מרגישות לפגיעה באזרחי אויב. בדומה לעבר, הנטייה להעברת סיכון חייבה את מקבלי ההחלטות להשתמש בכוח רק משניתן היה לתבוע לגיטימיות גבוהה, בעיקר בזירה הבין־לאומית, להפעלת מדיניות אש אגרסיבית. במקרה זה נשענה הלגיטימיות על סירוב חמאס לקבל את ההצעה המצרית להפסקת אש ועל מיקוד המבצע היבשתי בסילוקו של מה שצויר כאיום המנהרות על יישובי הדרום.

מהיבט אחר, הרגישות לחללים קטֵנה ככל שתחושת האיום גוברת וההבנה שהשימוש בכוח נועד לסילוקו של איום זה.[31] אמנם, ב"צוק איתן" הוצבה מרבית האוכלוסייה הישראלית תחת איום החימוש של חמאס, אך היה זה במידה נסבלת. לעומת זאת, במלחמת לבנון השנייה הוצב רק חלק מהאוכלוסייה תחת איום חזבאללה, אבל היה זה איום אינטנסיבי, שהביא אפילו להגירה פנימית. מכאן שקשה להבחין בין רמות משמעותיות שונות של איום, ולכן לא זה המשתנה העיקרי המסביר את ההבדלים בין המלחמות בכל הנוגע ליחס לקורבנות, ובפרט את הצדקתם במבצע "צוק איתן" ואת הביקורת על ריבוי הקורבנות במלחמות לבנון השנייה. יש בכך כדי להעניק תוקף לטיעון באשר לחשיבות הצטיירותה של ההצלחה הצבאית.

כזכור, חשש מנפגעים הניא את ההנהגה הישראלית מפני יציאה למבצע יבשתי ברצועת עזה במהלך מבצע "צוק איתן". זאת מתוך הנחה שמבצע כזה יחייב הפעלת אש אגרסיבית כדי להקטין את הסיכון לחיילי צה"ל, אשר תחשוף את מדינת ישראל לביקורת בין־לאומית.[32] לבסוף נגררה ישראל למבצע היבשתי בשל סירוב חמאס להפסיק את האש בתום עשרה ימי לחימה. אך ההנהגה הישראלית יצרה במקביל את הנסיבות המתאימות שנועדו לצמצם את החשש מפני התנגדות ציבורית להקרבת חיילים וזאת באמצעות הפעלת מדיניות אש אגרסיבית, מדיניות שהעבירה כזכור חלק מהסיכון מחיילי צה"ל לאזרחים העזתיים. כאמור, מדיניות

זו זכתה ללגיטימציה בשל סירוב חמאס לקבל את ההצעה המצרית להפסקת אש ונוכח התמקדות המבצע היבשתי בסילוקו של מה שנראה כאיום המנהרות. לכן, ייתכן שחופש הפעולה שעמד לרשות הפוליטיקאים ואנשי הצבא היה רחב מכפי שהעריכו.

היגד שלישי – רגישות לחללים מושפעת מזהות המקריבים ולא רק מקריאה "אובייקטיבית" של המציאות

כפי שהראו מלחמות קודמות, נפילת חיילים מקבוצות חילוניות מבוססות מעודדת קריאה ביקורתית של המציאות. קריאה כזאת עשויה לפתח רגישות שתוביל למחאה, יותר משעושה זאת מותם של חיילים מקבוצות שוליות, מהגרות או דתיות. במילים אחרות, המשתנים המשפיעים על מפלס הרגישות לחללים, כמו תחושת איום, הערכת הצלחה או כישלון של הפעולה הצבאית, ההכרה בצדקת המלחמה ועוד, מתווכים באמצעות מעמדה ומאפייניה של הקבוצה הקוראת אותם. הפוטנציאל לקריאה ביקורתית גובר ככל שהקבוצה מבוססת, ואז גם הצלחה צבאית לכאורה יכולה לקבל פרשנות ביקורתית.[33] יתר על כן, כפי שנאמר בדיון התיאורטי, רגישות תמריץ קבוצות מבוססות לפעול, בעוד שרגישות שתתפתח בקרב קבוצות ממעמד נמוך עשויה להוביל להשלמה פסיבית עם ההקרבה. ואכן, ביטויי מחאה שהונעו מִרגישות לחללים הופיעו בעבר בישראל אצל משפחות מבוססות יחסית.

ברוח זו נדרש מיפוי חברתי של החיילים שנהרגו במבצע "צוק איתן".[34] להעמקת המשמעות של מיפוי זה מתבקשת השוואה בין "צוק איתן" ובין מלחמת לבנון השנייה (בה נפלו 119 חיילים), וזאת בשל הרכב דומה של הכוח הלוחם ומספר גבוה של חללים, שבמלחמת לבנון השנייה עורר מחאה. ההשוואה מראה שהמגמה החברתית הכללית של ירידה בנוכחות של הקבוצות החילוניות המבוססות במפת החללים – ירידה המשקפת את השינוי בהרכבו החברתי של הצבא – נותרה בעיקרה בעינה. שיעור הנפגעים מקרב קבוצות המעמד הבינוני והחילוני – הקבוצות בעלות הפוטנציאל להצמיח מחאה – היה זהה במלחמת לבנון השנייה וב"צוק איתן". בשני המקרים מדובר בכמחצית מהחללים, אך בכ־15 אחוזים פחות מאשר בשבוע הראשון והקריטי של מלחמת לבנון הראשונה, שהצמיח את המחאה התקדימית. מכאן שלא היה כל בסיס לתחושה הציבורית, לפיה החלוקה של "מנת הדם" במבצע "צוק איתן" הייתה מאוזנת יותר מבעבר. אמנם, בתי הספר התיכוניים של העילית התל אביבית יוצגו במפת חללי "צוק איתן" יותר מאשר במלחמת לבנון השנייה, וגם שניים מבוגרי המכינות הכלליות (שנפלו בלחימה) היו בוגרי מכינות אליטיסטיות (מיצר ומנהיגות בגליל). עם זאת, בידוד ההתיישבות העובדת הוותיקה בתוך המעמד הבינוני הוותיק מראה על ירידה של

שישים אחוזים במשקלה בהשוואה בין שתי המלחמות. נתון זה מזים את התחושה שרווחה בציבור, לפיה היה ייצוג ניכר של התנועה הקיבוצית בין הקורבנות ב"צוק איתן". גם בתוך תנועה זו, החללים שבלטו היו מקֶרב אלה שהיגרו לקיבוצים ולא בני משפחות ותיקות. יתר על כן, המיפוי הראה עלייה בין שתי המלחמות של כ־25 אחוזים בייצוג הפריפריה החברתית (כולל יוצאי אתיופיה), ועלייה של כחמישים אחוזים בקרב הדתיים, הגם שהיו אלה בעיקר דתיים מיישובים בתחומי הקו הירוק ולא מתנחלים (כשם שגם מרבית בוגרי המכינות הדתיות שנפלו היו תושבי יישובים בתחומי הקו הירוק).

למרות ששיעור הנפגעים מקרב קבוצות המעמד הבינוני החילוני היה דומה במלחמת לבנון השנייה ובמבצע "צוק איתן", המספר המוחלט הנמוך של החללים מקבוצות אלו ב"צוק איתן" – 34 ביחס ל־63 במלחמת לבנון השנייה – הִקשה עוד יותר על יצירת מסה קריטית להנעת מחאה, שכאמור, היה לה מלכתחילה פוטנציאל נמוך לאור יעדי המבצע. גם השיעור הנמוך של החללים מקרב חיילי המילואים (15 אחוזים במבצע "צוק איתן" בהשוואה ל־45 אחוזים במלחמת לבנון השנייה) הקטין את התשתית להצמחת מחאה, שהרי במחאות העבר מילאו חיילי המילואים תפקיד מפתח.

הפוטנציאל למחאה יכול היה להתגבר ככל שהיא הייתה ממוקדת באירועים של מוות הנראה כניתן למניעה, דוגמת מיגונם של החיילים במצבים שונים (הבולט ביותר בהקשר זה היה אירוע הפגיעה בנגמ"ש לא ממוגן של חטיבת "גולני" בקרב בשג'אעיה), אבל, כאמור לעיל, המספר הנמוך של חללים מקבוצות מבוססות הִקשה על הצמחת מחאה כזאת. בה בעת, הצטיירות הקורבן כאפקטיבי הקטינה את הסיכוי להצמחת מחאה משורות המשפחות השכולות הדתיות, ששיעורן היחסי עלה, באמור, בכחמישים אחוזים בין מלחמת לבנון השנייה למבצע "צוק איתן". במלחמת לבנון השנייה המשפחות השכולות הדתיות בלטו בייזום מחאה על רקע אכזבתן מתפקוד הצבא והממשלה.

היגד רביעי – הרגישות לחללים מושפעת מאופיו של מודל הגיוס

מודל גיוס החובה בישראל עובר בעשור האחרון שינוי, המעצב אותו כמודל הבנוי יותר ויותר על יסודות בררניים (מודל סלקטיבי). מודל גיוס בררני הוא מודל של גיוס חובה, החָל פורמלית על כל האוכלוסייה, אך גם פוטר מחובת הגיוס שיעור גבוה יחסית שלה, אם על בסיס קבוצתי (כמו הפטור לחרדים או לערבים) ואם על בסיס אישי, כמאפיין את דפוס המיקוח האישי בין מגויסים מקבוצות מבוססות ובין הצבא.[35] הבררנות חלה לא רק על עצם הגיוס לצבא, אלא במיוחד על ההצבה ליחידות קרביות – הצבה שבהדרגה נושאת אופי של שירות התנדבותי בפועל.[36]

ככל שמודל גיוס החובה נחלש, נחלשת גם הרגישות לחללים מצד המשפחות, לרבות המבוססות, ורשתותיהן החברתיות. המוות הצבאי נתפס בהדרגה כנובע מבחירתו האישית והמודעת של הפרט ולא מציווי מדינתי. לכן, קטן הסיכוי כי תחושת האובדן תתועל לטענות כלפי המדינה, שאחריותה למוות הצבאי נתפסת כנחלשת חלקית.[37] ב"צוק איתן" אף בלטה התופעה של הצגת החללים כחדורי מוטיבציה גבוהה לשרת בצבא: הנופלים לא תוארו כמי שהלכו ליחידות הקרביות מתוך חובה או צו, אלא ככאלה שעשו זאת מרצון, והתקשורת פיארה את גבורתם האישית במנותק משאלת המחיר ששילמו.[38] תחושה כזאת מגבילה את יכולת ההורים להתנגד למוות הצבאי ומעצימה את קבלתו. לכך יש להוסיף את המאמץ האפקטיבי שעשו צה"ל ומערכת החינוך בעשור האחרון להתמודד עם שחיקת המוטיבציה להקרבה, בעיקר אצל הקבוצות המבוססות. כניסת הצבא לבתי הספר, "קמפיין המשתמטים" והתחזקות מפעל המכינות הקדם־צבאיות החילוניות/מעורבות ועוד, הם הביטויים לכך.

היגד חמישי – מספר החללים משפיע אך לא מכריע

ויכוח נטוש בין החוקרים בארצות הברית סביב השאלה עד כמה מספר החללים מהווה גורם מכריע ביצירת תפנית בדעת הקהל נגד ההקרבה הצבאית.[39] טענתי היא שהמספר אינו מכריע. לשם השוואה, מלחמת ההתשה בתעלת סואץ (1969–1970), שהתנהלה הרחק מריכוזי האוכלוסייה של ישראל ובה נפלו כ־600 חיילים בתוך פחות משנתיים, כמעט שלא עוררה מחאה. בניגוד לה, מלחמת ההתשה הלבנונית (1982–1985), שהתנהלה קילומטרים ספורים מהקהילות האזרחיות בגליל, ובה נהרגו חיילים במספר דומה, עוררה מחאה. מהלכים צבאיים שבעבר זכו להסכמה נעשו לשנויים במחלוקת, לא בגלל שינוי אובייקטיבי במטרות המלחמה ובסיכון שהן נועדו לסלק, אלא בשל יכולתן של הקבוצות המבוססות (בעיקר) לנתק את עצמן מכבלי החשיבה הצבאית ולבחון את קורבנן בעיניים ביקורתיות.

אם נידרש לגורם זה בהשוואה בין מלחמת לבנון השנייה למבצע "צוק איתן", ניווכח שוב לראות שהמספר אינו משפיע. אמנם, מספר החללים במלחמת לבנון השנייה עמד על 119, וב"צוק איתן" על 65, אבל הפרש זה בלבד לא יכול להסביר את גל המחאה של הורים שכולים במקרה הראשון מול שתיקה והשלמה במקרה השני. לפנינו שני מצבים קוטביים ולא רצף. המסקנה היא שהגורמים האחרים שהוצגו במאמר זה מילאו תפקיד מכריע בהסבר המחאה או היעדרה.

סיכום

הנסיבות המצטברות יצרו את ההבדל במחאות בין מלחמת לבנון השנייה לבין מבצע "צוק איתן". על פניו, אותם הגורמים שהביאו להתפרצות מחאה המוגנת

מרגישות לחללים לאחר מלחמת לבנון השנייה היו אמורים לחולל מחאה גם לאחר מבצע "צוק איתן": מטרות מלחמה עמומות ונזילות, דשדוש בביצוע, כישלון למנוע ירי על העורף, הפתעה מיכולות היריב, ובעיקר מחדלים מבצעיים שהסתיימו במותם של חיילים. אך הנסיבות השונות של שתי המלחמות הביאו לכך שמשפחות החללים ב"צוק איתן" קראו את המציאות בצורה שמרנית ולא ביקורתית. הנסיבות האלה הגבירו את סיכוייה של ההנהגה להצדיק את המוות הצבאי, בעוד שהחלישו את הפוטנציאל לרגישות מצמיחת מחאה: המאמץ הצבאי הצטייר כקצר, אינטנסיבי ואפקטיבי, שיעור ההקרבה של הקבוצות המבוססות היה לא גבוה ומודל הגיוס לבש צורה התנדבותית.

יחסה של החברה בישראל לקורבנות צבאיים הוא אפוא מורכב. רמת הרגישות הינה גבוהה מכפי שהייתה במלחמות שקדמו לקו פרשת המים של מלחמת לבנון הראשונה, והפוטנציאל להצמחתה של התנגדות למלחמה, הנובעת מרגישות זו, נותר גבוה. קביעה זו נכונה בין אם קבוצות חברתיות מגלות רגישות בפועל ובין אם ראשי המדינה והצבא מאמינים בקיומה של רגישות כזאת, אפילו מעֵבר לפוטנציאל האמיתי שלה. נסיבות ספציפיות מכריעות האם רגישות זו תתפרץ או תיוותר רדומה. המסקנה כי "קורי העכביש" הפכו לעבותות וכי ארונות המתים מעוררים אדישות, נראית לפיכך גורפת מדי.

הערות

1 Gabi Siboni, "Operations Cast Lead, Pillar of Defense and Protective Edge: A comparative review," in *The Lessons of Operation Protective Edge*, eds. Anat Kurz and Shlomo Brom (Tel-Aviv: Institute for National Security Studies, 2014), p. 30.

2 ירדן סקופ, "מרצים באוניברסיטת ת"א: 'מנסים להטיל עלינו אלם'", **הארץ**, 26 באוגוסט 2014.

3 ציפי ישראלי ואלישבע רוסמן, "'בזכותם': התייחסות התקשורת לשאלת מחיר הנפגעים במבצע 'צוק איתן'", **צבא ואסטרטגיה**, כרך 7, גיליון 2, 2015, עמ' 27–45.

4 שוברים שתיקה, **ככה נלחמנו בעזה 2014** (2015), http://www.shovrimshtika.org/tzuk.

5 הוועדה לבדיקת אירועי המערכה בלבנון, **דין וחשבון סופי** (ירושלים: משרד ראש הממשלה, 2008), עמ' 106.

6 Christopher Gelpi, Peter D. Feaver, Jason Reifler, *Paying the Human Costs of War: American Public Opinion and Casualties in Military Conflicts* (Princeton NJ: Princeton University Press, 2009).

7 Udi Lebel, "Postmortem Politics: Competitive Models of Bereavement for Fallen Soldiers in Israeli Society," *Journal of Modern Jewish Studies*, 5, No. 2 (2006), pp. 163-181.

8 יגיל לוי, **מי שולט על הצבא? בין פיקוח על הצבא לשליטה בצבאיות** (ירושלים: מאגנס, 2010), עמ' 134–144.

9 הוועדה לבדיקת אירועי המערכה בלבנון, **דין וחשבון סופי**, עמ' 252.

10 מיטל עירן־יונה ובתיה בן־הדור, "על הרגישות לנפגעים: מבט השוואתי ומקומי, תפיסות מפקדים ומשמעויות לצה"ל", בתוך: **היבטים סוציולוגיים ופסיכולוגיים**

של פעולת הצבא בתווך האזרחי, מיטל עירן־יונה, עורכת (תל אביב: המרכז למדעי ההתנהגות, צה"ל, הוצאת במחנה, 2013), עמ' 126–142.

11 Yagil Levy, *Israel's Death Hierarchy: Casualty Aversion in a Militarized Democracy* (New York: New York University Press, 2012), pp. 127-145.

12 ראו לדוגמה: Martin Shaw, "Risk-transfer Militarism, Small Massacres and the Historic Legitimacy of War," *International Relations*, 16, No. 3 (2002), pp. 343-360.

13 Hugh Smith, "What Costs will Democracies Bear? A Review of Popular Theories of Casualty Aversion. *Armed Forces & Society*, 31, No. 4 (2005), pp. 487-512.

14 Edward N. Luttwak, "Toward Post-Heroic Warfare," *Foreign Affairs*, 74, No. 3 (1995).

15 Gelpi, Feaver, Reifler, *Paying the Human Costs of War*.

16 ראו לדוגמה:
Douglas L. Kriner, Francis X. Shen, *The Casualty Gap: The Causes and Consequences of American Wartime Inequalities* (New York: Oxford University Press, 2010); Yagil Levy, "How Military Recruitment Affects Collective Action and its Outcomes," *International Studies Quarterly*, 57, No. 1 (2013), pp. 28-40; Joseph Paul Vasquez, "Shouldering the Soldiering: Democracy, Conscription and Military Casualties," *Journal of Conflict Resolution*, 49, No. 6 (2005), pp. 849-873.

17 John E. Mueller, *War, Presidents and Public Opinion* (New York: Wiley, 1973).

18 לוי, **מי שולט על הצבא**, עמ' 151–153.

19 עמוס הראל, "שבוע למבצע, ישראל מנווטת אל היציאה", **הארץ**, 15 ביולי 2014.

20 Assaf Sharon, "Failure in Gaza," *The New York Review of Books*, September 25, 2014.

21 אפרים יער ותמר הרמן, **מדד השלום אוגוסט 2014**,
http://www.idi.org.il/media/3676236/Peace_Index_August_-2014-Heb.pdf;
Yehuda Ben Meir, "Operation Protective Edge: A Public Opinion Roller Coaster," in *The Lessons of Operation Protective Edge*, eds. Anat Kurz and Shlomo Brom (Tel-Aviv: Institute for National Security Studies, 2014), pp. 131-132.

22 ישראלי ורוסמן, "'בזכותם'", עמ' 36.

23 אודי סגל, "נציגי צה"ל לחברי הקבינט: 'מחיר כיבוש רצועת עזה – מאות חיילי צה"ל הרוגים'", חדשות ערוץ 2, 5 באוגוסט 2014.

24 אפרים יער ותמר הרמן, **מדד השלום יולי 2006**,
http://www.peaceindex.org/indexYears.aspx?num=2; אפרים יער ותמר הרמן, **מדד השלום ספטמבר 2014**,
http://www.idi.org.il/media/3714875/Peace_Index_September_-2014-Heb.pdf

25 William A. Boettcher, Michael D. Cobb, "Echoes of Vietnam? Casualty Framing and Public Perceptions of Success and Failure in Iraq," *Journal of Conflict Resolution*, 50, No. 6 (2006), pp. 831-854.

26 רביב דרוקר, "התקשורת ומבצע 'צוק איתן'", http://drucker10.net/?p=2310

27 Michael W. Reisman, "The Lessons of Qana," *Yale Journal of International Law,* 22, No. 2 (1997), pp. 395-396.

28 יער והרמן, **מדד השלום אוגוסט 2014**.

29 עמוס הראל, "מאזן הרווח וההפסד של נתניהו ושל מוחמד דף", **הארץ**, 24 ביולי 2015.

30 Yagil Levy, "How Israel Shifted Risk from Soldiers to Gazan Civilians," *The Washington Post* – Monkey Cage, August 18, 2015.

31 Bruce W.Jentleson, Rebecca L. Britton, "Still Pretty Prudent: Post-Cold War American Public Opinion on the Use of Military Force," *Journal of Conflict Resolution*, 42, No. 4 (1998), pp. 395-417.

32 הראל, "שבוע למבצע, ישראל מנווטת אל היציאה".

33 Levy, *Israel's Death Hierarchy*, pp. 37-125.

34 המיפוי מתבסס על בחינת מוצאם החברתי של החללים בהתאם לסיפורי חייהם וסיפורי המשפחות, כפי שהתפרסמו לאחר מותם בעיתונות האלקטרונית.

35 יגיל לוי, "'צבא העם' נגד גיוס חובה", **משפט וצבא**, 21 (א), עמ' 309–340.

36 עמוס הראל, **תדע כל אם עברייה: קווים לדמותו של צה"ל החדש** (אור יהודה: כנרת, זמורה־ביתן, 2013), עמ' 44–45.

37 להשוואה ראו:
Yagil Levy, "How Military Recruitment Affects Collective Action and its Outcomes," *International Studies Quarterly*, 57, No. 1 (2013), pp. 28-40.

38 ישראלי ורוסמן, "'בזכותם'", עמ' 39.

39 ראו לדוגמה:
Christopher Gelpi, "How many Casualties will Americans Tolerate? Misdiagnosis," *Foreign Affairs*, 85, No. 1 (2006), pp. 139-144.

בקרת נשק על הגרעין האסטרטגי של סין: איך להימנע מ"מלכודת תוקידידס"

סטיבן ג' סימבלה

"מלכודת תוקידידס" עוסקת בנטייתן של אומות מתפתחות בהיסטוריה לאתגר גופים הגמוניים מקובלים או כוחות מובילים אחרים להשגת מעמד בינלאומי, מה שמוביל לעיתים למלחמה. כוחה הצבאי והכלכלי המתגבר של סין במאה ה־21 מאתגר את המנהיגות הן האמריקאית והן הרוסית בנושאי ביטחון בינלאומי, לרבות בתחומי הבקרה על נשק גרעיני ואי־ההפצה. עם זאת, צמצום מאגרי הנשק האסטרטגיים המשיך להתבצע במסגרת דו־צדדית של משא ומתן אמריקאי־רוסי. על אף קיום קשיים הניכרים לעין, יש לכלול את סין בתהליך הצמצום של נשק גרעיני האמריקאי־רוסי, שכן סין מהווה מעצמה גרעינית עולה והיא נעה אל מעבר לסף המינימום שלה להרתעה מימי המלחמה הקרה.

מילות מפתח: הרתעה, בקרת נשק, סין, נשק גרעיני, הגנות טילים, מלכודת תוקידידס, START, מודרניזציה

מבוא

"מלכודת תוקידידס" מתייחסת לנטייה ההיסטורית, לפיה אתגרים שמציבות מעצמות עולות מול הגמוניה של מעצמות־על קיימות עלולים להתגלגל לכדי מלחמה. השאלה אם ארצות הברית וסין יכולות להימנע מ"מלכודת תוקידידס" נוגעת לסוגיות רבות,[1] שאחת מהן היא בקרת נשק גרעיני. ארצות הברית ורוסיה ישגו אם ימשיכו לראות בשיחות להגבלת הנשק הגרעיני האסטרטגי דיאלוג שאמור להתנהל רק בין שתיהן. המודרניזציה הצבאית הנוכחית והעתידית של סין מזכה גם אותה במקום סביב שולחן הדיונים על נשק גרעיני, לצד רוסיה וארצות הברית. בין שאר הסיבות לכך ניתן לציין את העובדה שסין ממשיכה לשפר את יכולותיהם של

סטיבן ג' סימבלה הוא פרופסור למדע המדינה בקמפוס פן סטייט ברנדווין, פנסילבניה, ארצות הברית.

הצוללות הגרעיניות שלה (SSBN) ושל הטילים הבליסטיים המשוגרים מצוללות (SLBM). בנוסף לכך, צי צוללות הקרב הגרעיניות של סין משתלב באסטרטגיה השאפתנית שלה ל"מניעת גישה ובלימת חדירה" (Anti-Access/Area Denial – A2/AD), שנועדה להרתיע התערבות צבאית אמריקאית שמקורה באינטרסים של בעלות בריתה של ארצות הברית באסיה, בניגוד לרצונה של סין.[2]

הדיפלומטיה הסינית מסייעת למנהיגי סין על ידי שהיא יוצרת עבורם מרחב תמרון נוסף בין הדרך שבה רוסיה תופסת את האינטרסים שלה ובין הדרך שארצות הברית תופסת את האינטרסים שלה. יחד עם זאת, סין עשויה לחוש חוסר מחויבות לשקיפות במה שנוגע לבקרת נשק, אף שדבר זה הוא חיוני כדי להפוך אותה לשותפה מרכזית במשטר בקרת הנשק הגרעיני המולטילטרלי.

אין פירוש הדבר שכוחה הצבאי והכלכלי העולה של סין, ביחד עם השפעתה הפוליטית באסיה ובעולם כולו, יביאו בהכרח למלחמה בינה ובין ארצות הברית. למעשה, עוצמתה הגרעינית המתפתחת של סין עשויה ליצור מצב של הרתעה הדדית במזרח אסיה, שבו האופציה של מלחמה כוללת או מלחמה גרעינית לא תיתפס כיתרון או אפילו כצעד מתקבל על הדעת. במקום זאת, התחרות בין סין לארצות הברית יכולה ללבוש צורה של יריבות כלכלית הנתמכת על ידי כוח צבאי ותבונה דיפלומטית. יציבות שתנבע מהרתעה גרעינית מחייבת שרוסיה, ארצות הברית וסין יהיו חלק מכל משטר בקרת נשק גרעיני באסיה.

סין כגורם מאזן

המומחה הרוסי לבקרת נשק, אלכסיי ארבטוב, מציין כי המדיניות "הזהירה ומרובת הווקטורים" של בייג'ין "אפשרה לה לתפוס את התפקיד שמסורתית היה התפקיד שאליו שאפה רוסיה – הגורם המאזן בין מזרח למערב. למעשה, מדיניות ה'אירואסייתיות' החדשה של רוסיה הפכה אותה בעצם להיות אותו 'מזרח'".[3] עם זאת, היעדים הצבאיים והפוליטיים של סין באסיה ובעולם שונים מאלה של ארצות הברית ורוסיה. הם משקפים את תפיסתה לגבי האינטרסים שלה והתפקיד שהיא מייעדת לעצמה בסדר העולמי המתגבש.[4]

כניסתה של סין למשוואת ההרתעה הגרעינית בין רוסיה לארצות הברית יוצרת אתגרים כבדי משקל, וזאת מכמה סיבות. ראשית, המודרניזציה הצבאית של סין עתידה לשנות את יחסי הכוחות באסיה, לרבות יחסי הכוחות הגרעיניים והבליסטיים. המודרניזציה הצבאית של סין נשענת לא רק על התרבות הצבאית שלה, אלא גם על ניתוח של ניסיון המערב וניסיונם של גורמים אחרים, כפי שמסביר דייוויד לאי (Lai): "אופי הלחימה הסיני שם דגש רב על השימוש באסטרטגיה, בתחבולות ובהטעיה. עם זאת, הסינים מבינים שגישתם זאת לא תהיה יעילה ללא גיבוי של כוח צבאי חזק. אסטרטגיית העל של סין היא להקדיש את שלושים

השנים הבאות כדי להשלים את משימת המודרניזציה, ואז להפוך למעצמת־על בכל המובנים".[5]

כוח הטילים האסטרטגיים של סין – "כוח הארטילריה השני של צבא שחרור העם" (PLASAF) – הוא בין אלה הצפויים ליהנות מהמודרניזציה הצבאית. כוח זה נקט צעדים משמעותיים במהלך תקופת שלטונו של הו ג'ינטאו, שהחלה ב־2002 עם התמנותו למזכיר הכללי של המפלגה הקומוניסטית הסינית ולנשיא סין. המשימה המרכזית של כוח הטילים האסטרטגיים של סין מתוארת בפרסומים הרשמיים כ"הרתעה כפולה, מבצעיות כפולה", כלומר אחריות להרתעה גרעינית ולמתקפת נגד גרעינית, לצד הרתעה קונבנציונלית ומתקפות קונבנציונליות ממוקדות.[6] הפרסומים הצבאיים הרשמיים של סין מציינים מספר משימות שאמורות להתבצע על ידי "כוח הארטילריה השני של צבא שחרור העם" בעיתות שלום או במצבי משבר ומלחמה. משימות אלו כוללות מניעת מלחמה, בקרת הסלמה, שימוש בהרתעה גרעינית כדי "לחסום" פעולות קונבנציונליות, וכן אילוץ האויב לצייתנות באמצעות פעולות הרתעה אסטרטגיות.[7]

למודרניזציה הצבאית של סין ולמשימות של הכוחות הגרעיניים והבליסטיים שלה יש השלכות חשובות על מדיניותה של ארצות הברית. ראשית, החשיבה הסינית הנוגעת להרתעה ולהגנה באמצעות נשק גרעיני מאופיינת בניואנסים שונים. למרות הישגי המודרניזציה של הצבא הסיני עד כה, מנהיגי המדינה מודעים לכך שסין עדיין רחוקה מלהיות בעלת עוצמה שווה ליכולות האסטרטגיות הגרעיניות של ארצות הברית או של רוסיה. יחד עם זאת, ייתכן שסין כלל אינה שואפת להגיע לשוויון אסטרטגי גרעיני עם מעצמות הגרעין המובילות כדי למנוע מלחמה באמצעות הרתעה גרעינית ואמצעים דומים; ייתכן שסין מעדיפה לראות בנשק הגרעיני אופציה אחת בלבד מבין מגוון אפשרויות שהייתה רוצה שיעמדו לרשותה כדי להרתיע או להשיב מלחמה, או גורם התומך בדיפלומטיה ובפעולות קונבנציונליות בעת הצורך. שוויון גרעיני אסטרטגי, שניתן למדוד אותו לפי אינדיקטורים כמותיים של עוצמה יחסית, עשוי להתגלות כפחות חשוב לסין מאשר שימוש איכותני בגרעין ובאמצעים אחרים, כחלק מאסטרטגיות צבאיות־דיפלומטיות רחבות יותר.[8]

שנית, סין מרחיבה את "תיק" המוכנות הצבאית שלה לא רק בפלטפורמות ובנשק, אלא גם בתחומֵי הפיקוד, הבקרה, התקשורת, המחשבים, המודיעין, המעקב ואיסוף המידע (C4ISR), וכן בטכנולוגיית מידע. האסטרטגים הצבאיים של סין, שעקבו אחר ההצלחה האמריקאית במבצע "סופה במדבר" בעיראק ב־1991, הגיעו למסקנה שמחשוב הלוחמה הוא הבסיס להרתעה עתידית וליכולת לממש פעולות הגנה.[9] ה"תיק" הסיני ההולך וגדל ביכולות חכמות ובפלטפורמות מודרניות כולל, בנוסף לפריטים שכבר הוזכרו, גם מטוסי חמקן, לוחמה נגד לוויינים,

צוללות שקטות, מוקשי טורפדו ימיים מסוג "ברילאנט", טילי שיוט משופרים, וכן פוטנציאל לשבש את פעילותם של שווקים פיננסיים. פול בראקן (Bracken) מציין כי ההשפעה המשולבת של ההתפתחות הצבאית הסינית היא הפיכתו של צבא סין למהיר תגובה יותר, כלומר לגמיש ומסתגל במהירות.[10]

החשיבות שסין מייחסת למהירות ולגמישות התגובה של הכוח, יותר מאשר לעוצמתו, מחזקת את התפיסה המסורתית הקיימת בחשיבה הצבאית הסינית מאז כתב סון טסו בשבח הניצחון ללא מלחמה, ואם המלחמה היא בלתי נמנעת – בזכות הצורך להיות הראשון שתוקף ומנחית את מכת המחץ. היא גם עולה בקנה אחד עם העמדה שדוגלת בתקיפת האסטרטגיה של האויב ובעלי הברית שלו, תוך שימוש מרבי בהטעיה, וכל זאת בהתבסס על מודיעין והערכות איכותיים. השילוב של פלטפורמות משופרות, פיקוד ושליטה ולוחמת מידע אמור להניב אופציות שיאפשרו שימוש סלקטיבי במתקפות של אש מדויקת ובמתקפות סייבר נגד מטרות הנמצאות בעדיפות גבוהה, וימנעו הרג מסיבי ומתקפות עקרות על מעוזי האויב.

היבט שלישי של המודרניזציה הצבאית של סין והשלכותיה על יכולת ההרתעה הגרעינית ובקרת הנשק באסיה הוא סוגיית בקרת ההסלמה. השיפור ביכולות של סין בכל הנוגע להרתעה גרעינית ולמלחמה קונבנציונלית מגביר את הביטחון של מנהיגי המדינה ביכולתם לנהל אסטרטגיית A2/AD נגד ארצות הברית, או נגד כל מעצמה אחרת שתחתור לבלום את ההתפשטות הסינית באסיה. במקרה של ארצות הברית, ביטחון זה עשוי להתגלות כשגוי, שכן התכנון והפריסה של כוחות ארצות הברית באסיה הם חלק מ"ציר" צבאי־אסטרטגי שהיא שותפה לו. לצורך זה גם מפתחת ארצות הברית דוקטרינה ובונה כוחות סיוע שיוכלו להפעיל אמצעי נגד בקרבות ים־אוויר, וכל זאת מול אסטרטגיית מניעת הגישה הסינית.[11]

ממד נוסף של בעיית בקרת ההסלמה מתייחס לשאלה של ניהול משבר גרעיני בין סין חזקה לשכנותיה באסיה או בינה למדינות אחרות. אסיה נתפסה בעידן המלחמה הקרה כמנותקת מהשאלה הגרעינית, מכיוון שתשומת הלב של מקבלי ההחלטות בארצות הברית ונאט"ו הייתה נתונה למרוץ החימוש האמריקאי־סובייטי. העולם של המאה ה־21 שונה מאוד. חרף התקריות האחרונות באוקראינה, אירופה היא אזור שקט יחסית בהשוואה למזרח התיכון או לדרום אסיה ומזרחה, בעוד שאסיה שלאחר המלחמה הקרה היא מקום מושבן של חמש מדינות גרעיניות: רוסיה, סין, הודו, פקיסטן וקוריאה הצפונית. שימוש ראשון בנשק גרעיני בעקבות מה שיתחיל כמלחמה קונבנציונלית, למשל בין הודו לפקיסטן או בין סין להודו, אינו מצב בלתי אפשרי. במקביל, קוריאה הצפונית ממשיכה להציב איום קבוע בשני התחומים: היא עלולה לפתוח במלחמה קונבנציונלית בחצי האי הקוריאני; או שמשטרו של קים ג׳ונג און עלול לקרוס ולהותיר אחריו חוסר בהירות לגבי הפיקוד והשליטה על כוחות הצבא, לרבות הנשק והתשתית הגרעינית.[12]

הקושי לשמור מדינות גרעיניות מתחת לסף השימוש הראשון בנשק גרעיני, או למנוע הסלמה לאחר מכן, היה מסובך דיו עוד בימי המלחמה הקרה. חוסר הוודאות ביחס לבקרת ההסלמה במקרה של מלחמה אזורית באסיה בימינו רק הולך ומתעצם. גם כיום ישנה אפשרות של תקרית גרעינית בין סין לארצות הברית בים, או להתנגשות סביב טיוואן שתסלים לכדי עימות קונבנציונלי שיתדרדר בעקבות אי־הבנה מדינית לכלל הכנסת כוחות גרעיניים לכוננות כאמצעי של הרתעה. חשוב להבין שכוחות סיניים ואמריקאיים לא יצטרכו לשגר נשק גרעיני בפועל כדי ליצור את המודעות ליכולת השימוש בו; הנשק הגרעיני יהיה מעורב בעימות כבר מראשיתו גם ללא שימוש בו, כשהוא מתפקד כתזכורת רקע מתמדת לכך ששתי המדינות עלולות למצוא עצמן מסובכות בתהליך של הסלמה שאף אחת מהן לא כיוונה אליו מלכתחילה.

בנקודה זו יש מקום להערת הבהרה חשובה: קובעי מדיניות ואסטרטגיה נוהגים לדבר על נשק גרעיני כעל אמצעי שמאז ומתמיד הביא להרגעת ההסלמה במקום להחמרתה. עמדה תיאורטית זו יכולה להיות תקפה בתנאי שלום רגילים. אולם ברגע שפורץ משבר, ובמיוחד אם מתחוללת תקרית ירי, הפן השני של הסכנה הגרעינית צפוי לצוץ. תחושת הרגיעה, שמתבססת על ההנחה ששימוש ראשון בנשק גרעיני אינו סביר, עשויה להתחלף בתחושה שהדבר סביר מאוד. מייקל ס' צ'ייס (Chase) התריע כי הערכה שגויה בעיצומו של משבר היא "אפשרות מטרידה במיוחד", שמתחזקת בעקבות חוסר הוודאות בנוגע למסרים שהצדדים מעבירים ביניהם, ו/או נוכח מנהיגים החשים ביטחון מופרז ביכולתם לשלוט בהסלמה.[13]

מתודולוגיה וניתוח

ההקשר

עמדתה הגיאו־אסטרטגית של סין ותהליך המודרניזציה של הצבא הסיני אינם משתלבים בקלות במודלים הקיימים של עימות גרעיני. השתתפותה של סין בהתפתחויות העתידיות במשטר בקרת הנשק הגרעיני האסטרטגי תחייב את המתכננים הצבאיים שלה לגבש את הערכותיהם לגבי התוצאות של מלחמה גרעינית, הגם שמלחמה גרעינית בין סין לרוסיה או בין סין לארצות הברית היא מאוד לא סבירה. יחד עם זאת, הצבא הסיני, כמו הרוסי והאמריקאי, ייאלץ להתכונן למלחמות הלא סבירות, כשם שהוא מתכונן למלחמות הסבירות. בנוסף לכך, גם שאלת המאזן הגרעיני היא רלוונטית, משום שסין מעדיפה לשמור על יכולת מכה שנייה מול ארצות הברית או רוסיה, ללא קשר לקצב המודרניזציה של צבאותיהן. הוויכוח הפנימי בסין לגבי מידת המודרניזציה של הכוח הגרעיני שלה כולל, ללא ספק, טיעונים ושאלות כמו "מתי זה מספיק", במיוחד כשמדובר במשימה הבסיסית של הבטחת יכולות לפעולת תגמול בכל מצב.

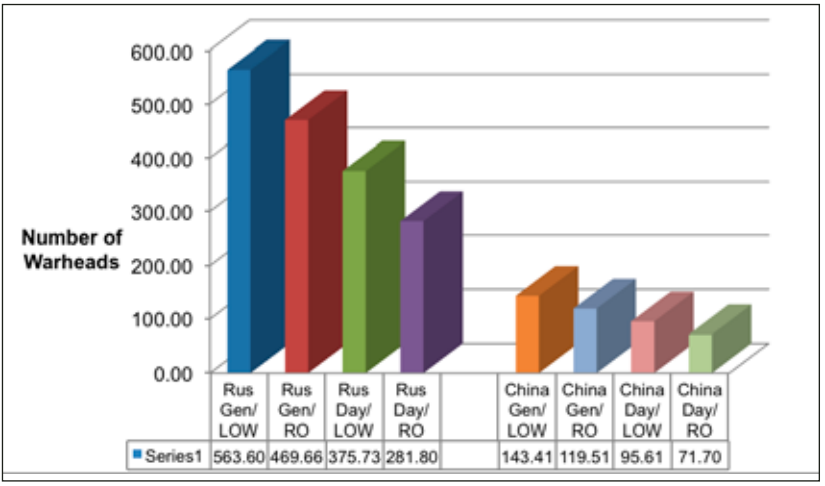
הדיון שבהמשך יציג תחזית לגבי כוחות הגרעין האסטרטגי של סין, רוסיה וארצות הברית בסביבות שנת 2020. קיימת אי־ודאות רבה בנוגע לסין בנושא זה, בהשוואה לארצות הברית ולרוסיה, משום ששתי האחרונות מחויבות לאמנת START החדשה בכל הנוגע לרמות של היערכות כוחותיהן הגרעיניים החל משנת 2018. בנוסף לכך קיימות דרישותיה של סין לגבי יכולות תצפית, התרעה מוקדמת, פיקוד ושליטה וקביעת מטרות, ההופכות למסובכות יותר בשל דרישות דומות של גורמים שונים באסיה וברחבי העולם. גם נאט"ו ורוסיה עומדות בפני בעיות אזוריות, אולם לנאט"ו ולרוסיה יש עשרות שנות ניסיון (כולל הניסיון של ברית המועצות לשעבר) בהערכת היכולת הגרעינית והכוונות של הצד השני, כמו גם במשא ומתן להשגת הסכמים צבאיים.

אסימטריה נוספת במשולש זה היא שרוסיה וסין יכולות, כל אחת, לגרום נזק "אסטרטגי" לשנייה, לרבות מתקפות על יעדים צבאיים ואזרחיים, וזאת מבלי לעשות שימוש בנשק ובמשגרים בעלי טווח בין־יבשתי. זו היא אחת הסיבות לכך שנשיא רוסיה, ולדימיר פוטין, העלה את הרעיון של יציאת רוסיה מהאמנה למניעת תפוצה של נשק גרעיני לטווח בינוני (INF). ארצות הברית ורוסיה הן היחידות שהתחייבו להימנע מנשק זה, בעוד שסין ויריבות אפשריות נוספות חופשיות לבנות ולפרוס אותו.[14] חשש נוסף הוא שסין מגלה פחות שקיפות לגבי יכולותיה הגרעיניות לעומת ארצות הברית ורוסיה – עמדה שמנקודת מבט סינית, יש כמה וכמה סיבות טובות לנהוג על פיה.[15]

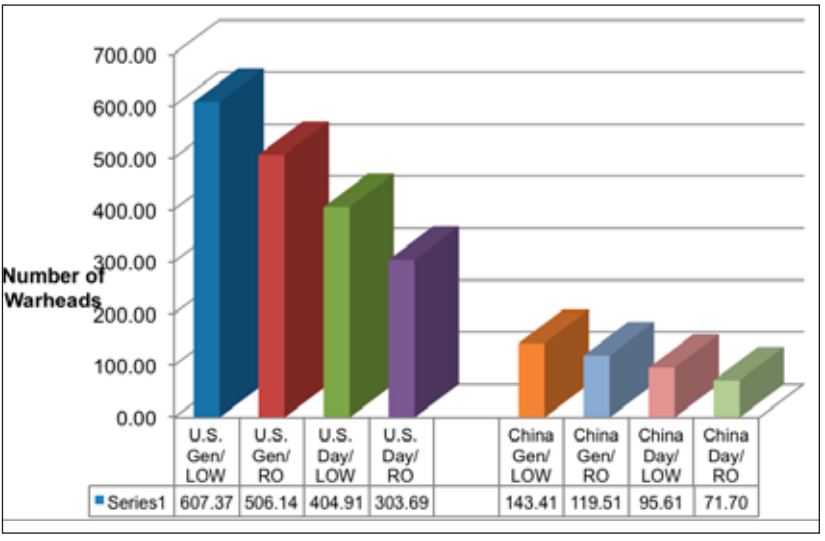
ניתוח

הניתוח שלהלן נועד להציג מבנה אנליטי של תחרות תלת־צדדית עם נשק גרעיני אסטרטגי. ההיפותזה שנבנתה לצורך זה היא: (1) כוחות הגרעין האסטרטגי של ארצות הברית ורוסיה מצייתים לאמנת START החדשה; (2) כוחות הגרעין הסיניים הצפויים הם משוערים בלבד, אך השערה זו עולה בקנה אחד עם מחקרים של מומחים ושל גופי הממשל האמריקאי.[16]

תרשים 1 מסכם את התוצאות של חילופי אש גרעיניים בין רוסיה לסין, בהתבסס על ההנחות שלנו לגבי עוצמתן הגרעינית הצפויה בשנת 2020. בתרשים 2 מוצג מידע דומה לגבי מלחמה גרעינית בין ארצות הברית לסין. בשני המקרים המספרים של ראשי נפץ גרעיניים שישרדו ויהיו זמינים לפעולת תגמול בכל מדינה מסוכמים לפי כל אחד מארבעת המצבים של דוקטרינת ה"כוננות ושיגור": (1) "קבלת התרעה" (Gen) ו"שיגור במצב של אזהרה" (LOW); (2) "קבלת התרעה" ו"שרידות בעקבות מתקפה" (RO), ולאחר מכן פעולת תגמול; (3) "התרעה יומיומית" (Day) ו"שיגור במצב של אזהרה"; (4) "התרעה יומיומית" ו"שרידות בעקבות מתקפה".



תרשים 1: רוסיה־סין: ראשי נפץ גרעיניים זמינים לפעולת תגמול – הערכת רמות פריסה לשנת 2020



תרשים 2: ארצות הברית־סין: ראשי נפץ גרעיניים זמינים לפעולת תגמול – הערכת כוחות לשנת 2020

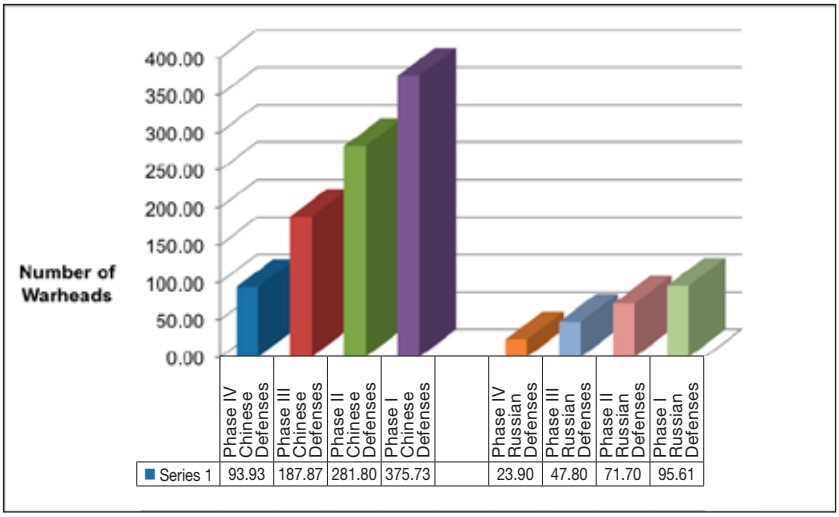
הסיכומים בתרשימים 1 ו־2 הם לצורכי המחשה בלבד ומבוססים על השערות, אולם למרות זאת ניתן ללמוד מהם רבות. חוסר העניין לכאורה של סין בהגעה לשוויון צבאי־אסטרטגי מול רוסיה או ארצות הברית מסתמן כהחלטה שקולה. למרות

שכוח הגרעין החזוי של סין לטווחים בין־יבשתיים בתקופת טרום המלחמה הוא קטן בהשוואה לכוחותיהן של רוסיה וארצות הברית, הוא אינו זניח. לנוכח הפריסה אמריקאית והרוסית, הכפופה לאמנת START החדשה או לאמנות אחרות, סין תהיה מסוגלת להבטיח "סף הרתעה", ואפילו יותר מכך, עד תום העשור הנוכחי. חשיבות מיוחדת יש לשיפורים בכוח הצוללות הנושאות טילים בליסטיים ובטילים הניידים שלה, בכל הנוגע לשרידותם במצב של מתקפת פתע. מנקודת מבטה של סין, טילים ניידים המשוגרים מהיבשה מחזקים את שרידות הכוח ומפחיתים את התמריץ לשגרם במצב של אזהרה או כמתקפת מנע, ובכך הם מחזקים את כושר ההרתעה הסיני ואת יכולתה של סין לייצב את המשבר.

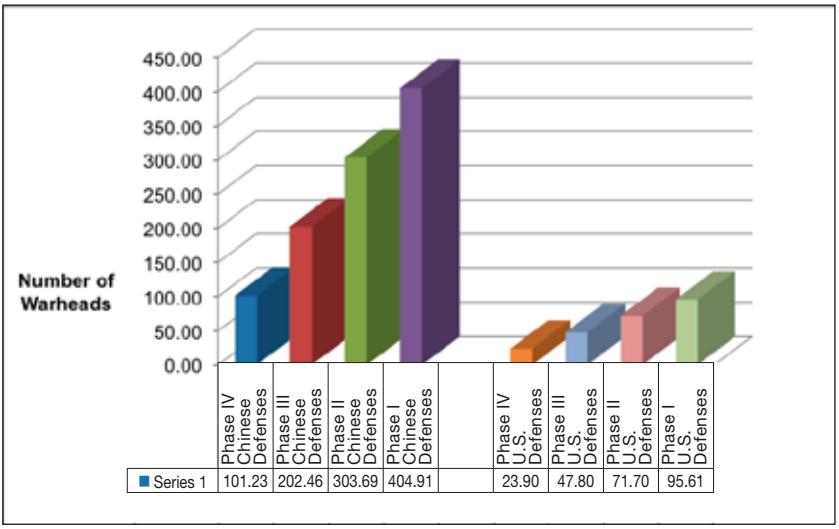
אחת הסוגיות שגרמה למבוי סתום מנקודת מבטה של רוסיה בעידן שלאחר אמנת START החדשה, היא התוכנית של נאט"ו לפרוס מערכות הגנת מפני טילים באירופה, המכונה European Phased Adaptive Approach. גם סין מודאגת מההשפעה שתהיה להצבת מערכת הגנת טילים כזאת על ההרתעה הגרעינית שלה. לפיכך, ניתחנו שוב את התוצאות שסוכמו בתרשימים 1 ו־2, הפעם לפי חישוב מספר ראשי הנפץ הגרעיניים של כל מדינה שישרדו ויהיו זמינים לפעולת תגמול, מול היכולת המשולבת של הגנת טילים והגנה אווירית של הצד השני. מכיוון שהמספרים המדויקים והיכולות העתידיות של הגנות טילים והגנות אוויריות אינם ידועים בוודאות, גיבשנו רצף אפשרי של יכולות הגנה אווירית והגנת טילים באופן הבא: בשלב I, הגנות אוויר וטילים מיירטות לפחות עשרים אחוזים מראשי הנפץ הגרעיניים הזמינים למכה שנייה; בשלב II הן מיירטות לפחות ארבעים אחוזים; בשלב III – לפחות שישים אחוזים; בשלב IV – לפחות שמונים אחוזים.

תרשימים 3 ו־4 מסכמים את תוצאות ההתקפה־הגנה במקרה של עימות בין רוסיה לסין (תרשים 3) ובמקרה של עימות בין ארצות הברית לסין (תרשים 4).

תוצאות הסימולציות המסוכמות בתרשימים 3 ו־4 מעניינות בכמה מישורים. ראשית, אפילו לאחר פריסת הגנות של כל שלוש המדינות, ארצות הברית ורוסיה שומרות על יתרון גרעיני יחסי על פני סין – אם מסתכלים על המספרים היבשים של ראשי נפץ גרעיני ומַשגרים ששרדו מתקפה וזמינים למכה שנייה; שנית, ולעומת זאת, גם ארצות הברית וגם רוסיה לא יצליחו לפרוק את סין מנשקה במהלך מתקפת מנע גרעינית, מבלי לספוג פעולת תגמול בממדים חסרי תקדים וכאלה שלא יוכלו להשלים עימם; שלישית, ההגנות האקטיביות של סין יתוגברו בהגנות פסיביות לצורכי פעולת תגמול, לרבות במערכות של מנהרות לאחסון ושינוע טילים ניידים המשוגרים מהיבשה.[17]



תרשים 3: רוסיה־סין: ראשי נפץ גרעיניים זמינים לפעולת תגמול, לעומת הגנות – הערכה לפריסה בשנת 2020



תרשים 4: ארצות הברית־סין: ראשי נפץ גרעיניים זמינים לפעולת תגמול, לעומת הגנות – הערכת כוחות לשנת 2020

מסקנות

התעצמות כוחה הכלכלי של סין, שאיפותיה הפוליטיות והמודרניזציה שעוברים הכוחות הגרעיניים והקונבנציונליים שלה מלמדים שהגיעה העת לכלול אותה במשטר בקרת הנשק הגרעיני של אסיה. עירובה בהגבלות המולטילטרליות על נשק גרעיני ו/או בשיחות לצמצום תפוצתו הוא, קרוב לוודאי, תנאי הכרחי אך לא מספיק להימנעות של ארצות הברית וסין מ"מלכודת תוקידידס". מה שנדרש כדי למנוע הפצה נוספת של נשק גרעיני באסיה הוא הימנעות מ"מלכודת תוקידידס משולשת", בצורת מרוץ גרעיני בין ארצות הברית, רוסיה וסין. כדי להשיג מטרה זו, על ארצות הברית ורוסיה לראות בסין שותפה מרכזית כאשר יחליטו להתקדם לעבר צמצום נוסף של הנשק הגרעיני בעידן שלאחר אמנת START החדשה.

המודרניזציה שעובר הצבא הסיני והיכולת הכלכלית של סין יוצרים עבורה פוטנציאל לפרוס כבר במהלך העשור הנוכחי, או בתחילת העשור הבא, כוחות הרתעה מעֵבר למינימום הדרוש כדי להבטיח פעולת תגמול בממדים בלתי נסבלים בתגובה לכל מתקפה על סין. זאת, במיוחד אם לוקחים בחשבון את הטילים הסיניים שהם בעלי טווח שהוא פחות מבין־יבשתי. הטילים והמטוסים לטווחים משתנים שבידי סין יכולים לזרוע הרס בשטחה של רוסיה ובמטרות באסיה שהן בעלות זיקה לארצות הברית, לרבות בעלות בריתה ובסיסים שלה באזור.

יחד עם זאת, אין זה מעשי לצפות שסין תפעל למודרניזציה גרעינית בלתי מוגבלת של כוחותיה כחלק מחתירה לשוויון או אף לעליונות גרעינית על ארצות הברית או על רוסיה. זהו תרחיש לא סביר, ומנקודת מבטה של סין גם חסר טעם. ייתכן אפוא שהגיעה העת, מנקודת מבט צבאית ודיפלומטית רחבה יותר, לדיאלוג תלת־צדדי על צמצומו והגבלתו של הנשק הגרעיני האסטרטגי, במקום לדיאלוג דו־צדדי בסוגיה זאת.

נספח: הערות על מתודולוגיה

ברצוני להביע בזאת הכרת תודה לד"ר ג'יימס ט' טריטן (Tritten), אשר במהלך 44 שנות הקריירה שלו בצי האמריקאי שירת כפרופסור וכראש המחלקה למחקרי ביטחון לאומי בבית הספר ללימודים מתקדמים של הצי (Naval Postgraduate School). במסגרת תפקידו זה פיתח ד"ר טריטן מודל של עימות גרעיני, המבוסס על גיליון נתונים. גיליון זה אימצתי ושיניתי, המרתי לגיליון אקסל ועדכנתי את מסד הנתונים, כך שישקף שינויים בכוחות האמריקאיים והסובייטיים (ולאחר מכן הרוסיים). פלט לדוגמה של גיליון כזה מובא להלן, עם נתונים לפי מדינות.

המודל מסייע לחוקרים באמצעות נוסחאות חישוב והמרת החישובים לגרפים. על החוקרים לציין את הערכים עבור מבנה הכוח, את מספרי הכוחות והנשק שנפרסו, את מאפייני הביצוע המוערכים של הנשק, וכן פרמטרים נוספים. ד"ר טריטן אינו אחראי לאף אחד מהניתוחים או הטיעונים המופיעים במחקר זה.

גיליון נתונים להמחשה לפי המודל של טריטן

מספר כולל של ראשי נפץ	ראשי נפץ שנפרסו	משגרים	כוחות רוסיים
0	1	0	SS-11/3
0	1	0	SS-13/2
300	10	30	SS-18
0	4	0	RS-24 silo
120	6	20	SS-19/3
60	1	60	SS-27 silo
480		110	סיכום ביניים של כוחות נייחים ביבשה
340	4	85	RS-24 ניידים
27	1	27	SS-27 ניידים
367		112	סיכום ביניים לניידים ביבשה
847		222	סיכום ביניים ליבשה
0	1	0	SS-N-6/3
0	1	0	SS-N-8/2
256	4	64	Delta IV - SS-N-23
256	4	64	Borei-Bulava
0	4	0	Delta III - SS-N-18
512		128	סיכום ביניים ימי
63	1	63	Bear H6
0	16	0	Bear H 16
13	1	13	Tu-160 Blackjack

כוחות רוסיים	משגרים	ראשי נפץ שנפרסו	מספר כולל של ראשי נפץ
סיכום ביניים אווירי	76		76
סה"כ כוחות רוסיים	426		1435
כוחות אמריקאיים			
Minuteman II	0	1	0
Minuteman III	0	1	0
Minuteman IIIA	400	1	400
Peacekeeper/MX	0	10	0
סיכום ביניים ליבשה	400		400
Trident C-4	0	4	0
Trident D-5/W-76	0	4	0
Trident D-5/W-88	240	4.5	1080
סיכום ביניים ימי	240		1080
B-52G gravity	0	0	0
B-52G gravity	0	0	0
ALCM		0	0
B-52H ALCM	32	1	32
B-2	16	1	16
סיכום ביניים אווירי	48		48
סה"כ כוחות אמריקאיים	688		1528

נתוני הטבלה הקודמת מוכפלים במערך של 17 פרמטרים כדי להפיק מתארי סיכום

מתארי סיכום	מספרים
סה"כ ראשי נפץ רוסיים המיועדים לשיגור	438.75
ראשי נפץ רוסיים רזרביים	175.90
סה"כ ראשי נפץ אמריקאיים המיועדים לשיגור	583.69
ראשי נפץ אמריקאיים רזרביים	252.34

הערות

1 להערכות בנוגע לרעיון זה, כולל הפניות רלוונטיות ליחסי ארצות הברית־סין, ראו: Graham Allison, "Just How Likely Is Another World War?," *The Atlantic*, July 2014, http://www.theatlantic.com/international/archive/2014/07/just-how-likely-is-another-world-war/375320/; James R. Holmes, "Beware the 'Thucydides Trap' Trap: Why the U.S. and China aren't necessarily Athens and Sparta or Britain and Germany before WWI," *The Diplomat*, June 13, 2013, http://thediplomat.com/2013/06/beware-the-thucydides-trap-trap/html

2 Jeremy Page, "Deep Threat: China's Submarines add Nuclear-Strike Capability, Altering Strategic Balance," *The Wall Street Journal*, October 27, 2014, http://online.wsj.com/articles/chinas-submarine-fleet-adds-nuclear-strike-capability-altering-strategic-balance-undersea-1414164738

3 Alexei Arbatov, "Engaging China in Nuclear Arms Control," Carnegie Moscow Center, October 9, 2014, http://carnegie.ru/publications/?fa=56886

4 ראו לדוגמה: Captain Bernard D. Cole, U.S. Navy (Retired), "Island Chains and Naval Classics," *Proceedings of the U.S. Naval Institute*, November 2014, pp. 68-73.

5 David Lai, "The Agony of Learning: The PLA's Transformation in Military Affairs," in: *Learning by Doing: The PLA Trains at Home and Abroad*, eds. Roy Kamphausen, David Lai, Travis Tanner (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, November 2012), pp. 337-384, p. 369.

6 Michael S. Chase, "Second Artillery in the Hu Jintao Era: Doctrine and Capabilities" in: *Assessing the People's Liberation Army in the Hu Jintao Era*, eds. Roy Kamphausen, David Lai, Travis Tanner (Carlisle, PA: Strategic Studies Institute, April 2014), pp. 301-353.

7 שם. עמ' 309.

8 *Hearing on Developments in China's Cyber and Nuclear Capabilities before the U.S.-China Economic and Security Review Commission*, March 26, 2012 (Testimony of Dr. Mark B. Schneider, Senior Analyst, National Institute of Public Policy), http://www.uscc.gov/Hearings/hearing-developments-china%E2%80%99s-cyber-and-nuclear-capabilities

9 Timothy L. Thomas, *Three Faces of the Cyber Dragon: Cyber Peace Activist, Spook, Attacker* (Fort Leavenworth, KS: Foreign Military Studies Office, 2012), pp. 39-66; Chase, "Second Artillery in the Hu Jintao Era," p. 331.

10 Paul Bracken, *The Second Nuclear Age: Strategy, Danger and the New World Politics* (New York: Henry Holt/Times Books, 2012), p. 206.

11 Jan Van Tol, Mark Gunzinger, Andrew Krepinevich, Jim Thomas, *AirSea Battle: A Point-of-Departure Operational Concept* (Washington DC: Center for Strategic and Budgetary Assessments, 2010), http://www.csbaonline.org/publications/2010/05/airsea-battle-concept/

12 Kang Seung-woo, "NK could Play Nuclear Option," *Korea Times*, August 12, 2014.

13 Chase, "Second Artillery in the Hu Jintao Era," p. 340.

14 Michael R. Gordon, "U.S. Says Russia Tested Cruise Missile, Violating Treaty," *The New York Times*, July 28, 2014.

15 *Hearing on Developments in China's Cyber and Nuclear Capabilities*, p. 2.

16 ראו לדוגמה: Hans M. Kristensen, Robert S. Norris, Matthew G. McKinzie, *Chinese Nuclear Forces and U.S. Nuclear War Planning* (Washington, D.C.: Federation of American Scientists and Natural Resources Defense Council, November 2006), pp. 35-46, כולל הפניות למסמכים רלוונטיים של משרד ההגנה ו־CIA; *Hearing on Developments in China's Cyber and Nuclear Capabilities*; לגבי כוחות ארצות הברית ורוסיה, ראו: Jon B. Wolfsthal, Jeffrey Lewis, Marc Quint, *The Trillion Dollar Triad: U.S. Strategic Modernization Over the Next Thirty Years* (Monterey, CA: James Martin Center for Nonproliferation Studies, January 2014); Mark B. Schneider, "The State of Russia's Strategic Forces," *Defense Dossier* 12 (October 2014), pp. 13-18; Hans M. Kristensen and Robert S. Norris, "US Nuclear Forces 2014," *Bulletin of the Atomic Scientists*, No. 1 (2014), pp. 85-93; Hans M. Kristensen, "Trimming Nuclear Excess: Options for Further Reductions of U.S. and Russian Nuclear Forces," Special Report No. 5 (Washington, D.C.: Federation of American Scientists, December 2012), http://fas.org/_docs/2012TrimmingNuclearExcess.pdf; Arms Control Association, "U.S. Strategic Nuclear Forces Under New START," July 2013, http://www.armscontrol.org/factsheets/USStratNukeForceNewSTART; Arms Control Association, "Russian Strategic Nuclear Forces Under New START," http://www.armscontrol.org/factsheets/RussiaStratNukeForceNewSTART; Joseph Cirincione, "Strategic Turn: New U.S. and Russian Views on Nuclear Weapons," New America Foundation, June 29, 2011; Pavel Podvig, "New START Treaty in numbers," Russian strategic nuclear forces (blog), April 9, 2010, http://russianforces.org/blog/2010/03/new_start_treaty_in_numbers.shtml

17 Arbatov, "Engaging China in Nuclear Arms Control"; Office of the Secretary of Defense, *Annual Report to Congress, Military and Security Developments Involving the People's Republic of China 2014* (Washington, DC: US Department of Defense, 2014 and 2013), p. 29.

היומינט בעידן הקיברנטי: משחקים בשני עולמות

אבי טל ודודי סימן טוב

עידן הסייבר מחולל שינוים עצומים בעולמות המודיעיניים והאיסופיים. מאמר זה דן בשאלות האם יש מקום למקצוע היומינט בעולם שבו הסייבר מהווה מרחב איסוף ופעולה מרכזי? באם יש מקום ליומינט, אילו משימות מוטלות עליו והאם נוצרות הזדמנויות לשיטות פעולה חדשות בעידן הסייבר? המאמר בוחן את מהות הדיסציפלינה היומינטית בעידן זה, ובתוך כך את האתגרים שמציב הסייבר בפני דיסציפלינה זו. בנוסף לכך הוא דן בתרומה הפוטנציאלית של היומינט בעידן הקיברנטי ומעלה את השאלה האם מדובר בדיסציפלינה מודיעינית־איסופית חדשה.
החלק הראשון במאמר מציג את היומינט עד לעידן הסייבר. חלקו השני דן ביומינט בעידן הקיברנטי, תוך שימת דגש על ההזדמנויות, הסיכונים והשינויים שחלו בו, ומציג הצעה לתפיסה חדשה באשר למקצוע היומינט בעידן הקיברנטי.

מילות מפתח: יומינט, מודיעין, איסוף מודיעיני, סייבר, קהילת המודיעין, יומינט קיברנטי, אוואטר.

מבוא

הסייבר הפך את העולם לכפר גלובלי. הוא מנגיש בו עמיתים ויריבים, אויבים וידידים, תוך גישור על גבולות ושפות. בסייבר עובר מידע גלוי וגם מסווג ומוצפן, והוא גם הפלטפורמה המרכזית לבקרה ולשליטה על מערכות וכלים. פלטפורמה זו מייצרת איומים של מתקפות קיברנטיות, שלעיתים יכולות להיות להן גם תוצאות קינטיות. הרשתות החברתיות, הבלוגוספירה והמדיה החדשה הפכו לבמה המרכזית

דודי סימן־טוב הינו חוקר של תחום המודיעין במכון למחקרי ביטחון לאומי, אבי טל הוא בכיר לשעבר במגזר הערבי בשב"כ

של ההמונים לשיח ולפעולה בכל תחומי החיים.[1] הרשתות החברתיות גם הפכו לפלטפורמה מרכזית להתארגנויות שונות, דוגמת "האביב הערבי", וכן להסתה, כמו זו שהובילה לגל הסכינאות העכשווי ברחבי ישראל. כמעט לכל אחד יש כיום דף בית אישי באינטרנט, וכמעט כולם נותנים בו במה לעמדותיהם ולרצונותיהם בנושאים אישיים ומקצועיים. המידע הגלוי עצום ורב ונמצא בעלייה מתמדת; לצידו קיימים אזורים קיברנטיים הקשים לחדירה.[2]

עידן הסייבר מחולל שינוים עצומים בעולמות המודיעיניים והאיסופיים. אלה מעוררים שאלות כגון: האם יש מקום ליומינט בעולם שבו הסייבר מהווה מרחב איסוף ופעולה מרכזי? ואם יש מקום כזה, האם נוצרות הזדמנויות לשיטות פעולה חדשות? מטרת המאמר היא לבחון מהם מאפייני היומינט בעידן הקיברנטי, תוך שימת דגש על השינויים שחלו בתפיסות ובשיטות ההפעלה שלו בהשוואה למקצוע היומינט הקלאסי. החלק הראשון במאמר מציג את היומינט עד לעידן הסייבר. חלקו השני דן ביומינט בעידן הקיברנטי, מדגיש את ההזדמנויות, הסיכונים והשינויים שחלו בו ומציג הצעה לתפיסה חדשה באשר למקצוע היומינט בעידן הסייבר.

היומינט הקלאסי

משחר ההיסטוריה ועד תחילת המאה העשרים התבססו גורמי המודיעין באופן בלעדי על מידע ממקורות אנוש. סון טסו, מצביא סיני מהמאה השישית לפני הספירה, כתב בספרו "אמנות המלחמה" על המרגלים וחשיבותם במלחמה.[3] יש הרואים במקצוע היומינט – המודיעין האנושי (Human Intelligence) – הקלאסי הוא אמנות משום שהוא דורש מהאדם העוסק בו יכולת תקשורת בין־אישית גבוהה, ידע כללי רחב, רב־גוניות ויכולת לשחק תפקידים שונים, לצד היכרות עם התחום הפסיכולוגי־פילוסופי של ההתנהגות האנושית, יכולת השפעה ושכנוע, וכמובן הנעה לפעולה.

קיימים שלושה שלבי מפתח במקצוע היומינט: הראשון הוא אתירה ובחירה, קרי איתור ובחירת האנשים הנדרשים לגיוס על בסיס כישורים אישיים וייעודיים, מניעים (קיימים ופוטנציאליים) ונגישות (לגיוס ולהפעלה); השלב השני הוא מִבצע הגיוס, שיכול להתבצע בשיטות שונות ומגוונות – גיוס מתוכנן, גיוס ישיר, גיוס עקיף באמצעות סייען ובכיסוי, גיוס מזדמן וגיוס מתנדבים;[4] השלב השלישי הוא הפעלה ומִבצעים. פגישה פיזית חשאית היא בעלת חשיבות רבה ליצירת אמון וזיקה אישית עם הסוכן ולהיבטים המבצעיים הקשורים בהפעלתו (מבחן אומץ, מתן אמצעים, הדרכות והכשרות ייעודיות ועוד).

היומינט הקלאסי היה בתחילת דרכו פעילות אנושית פשוטה.[5] הגיוס וההפעלה התבססו בעיקר על פגישות פיזיות, בשל היעדר כמעט מוחלט של נגישות מרחוק. תהליך האתירה נעשה על בסיס מודיעין מצומצם וחסר יחסית, ולכן

המאתרים ויכולת הבחירה האיכותית היו מוגבלים. בעולם פיזי זה, ככל שמִבצע הגיוס וההפעלה חייבו פעולה בכיסוי מול המגויס והסביבה, היה צורך בהתאמה מלאה של מערך ההפעלה למגויס ולסביבתו, וזאת בהתאם לסיפורי הכיסוי. אלה היו חייבים לעמוד במבחן הפיזי: דמות המפעיל, השחקנים המסייעים, ובכללם האבטחה, המקום, התפאורה, השפה ועוד. מצב זה יצר סיכונים רבים לביטחון המִבצע, למפעילים וגם לסוכן. ציוד הסוכן באמצעים לפעולה חשאית הגביר את הסיכון והיווה חותמת מפלילה.

מעמדו של המודיעין האנושי בקהילות המודיעין במערב נמצא בדעיכה משנות השבעים של המאה העשרים ואילך.[6] הסיבות לכך היו ההתפתחויות הטכנולוגיות ומעבר מסיבי של המין האנושי והצבאות לשימוש במרחב האלקטרומגנטי. אלה הביאו לעלייתו של האיסוף הטכנולוגי, לעלייה בתרומת המודיעין הגיאו־מרחבי באמצעות לוויינים וסייבר, וכן לעלייה עצומה בכמות המידע הגלוי (אוסינט).

מסקנות ועדות החקירה שחקרו את הפיגועים במגדלים התאומים בארצות הברית ב־11 בספטמבר 2001 ואת כישלון המודיעין האמריקאי בעיראק, היוו נקודת מפנה בקהילת המודיעין האמריקאית. מסקנות אלו הצביעו על היעדר מידע מדויק על ארגון "אל־קאעדה", מהסוג האינטימי שמערך היומינט אמור לספק. בעקבות זאת החל ניסיון להחזיר את היומינט למרכז העשייה המודיעינית בארצות הברית. דוגמה לתרומה אפקטיבית של היומינט לאיסוף המודיעיני האמריקאי ניתן למצוא במצוד אחר מנהיג "אל־קאעדה", אוסמה בן לאדן, כאשר ה־CIA גייס רופא פקיסטני שנתן חיסון מזויף לבן לאדן, ובאותה הזדמנות הפיק ממנו את הדנ"א שלו.

היומינט בעידן הקיברנטי

בשיח על האיסוף המודיעיני בעידן הקיברנטי קיימת גישה, לפיה לא נכון להתבסס על הסייבר כמקור איסופי כמעט בלעדי. לפי גישה זו, אין תחליף ליומינט כדי להבין את תמונת המודיעין השלמה, במיוחד כשמדובר בארגונים דוגמת דאע"ש וחמאס, שחתימתם בסייבר נמוכה, והסתמכות על מודיעין טכנולוגי בלבד כדי להגיע למידע מדויק עליהם הינה חסרה ובעייתית.[7] בהמשך לכך, קיימת גישה הגורסת כי דווקא בעידן הנוכחי, כאשר מתבררת מידת החדירה האיסופית לכלל תחומי החיים, מדינות וארגונים שואפים להפחית את רמת החתימה המודיעינית שלהם ולפעול באמצעות שליחים ופגישות עבודה.

בדיון התיאורטי על היומינט בעידן הקיברנטי יש המציעים להרחיב את מושג היומינט ולהוסיף לו את המושג "הנדסה חברתית" שבמסגרתו יוצרים זהות בדויה לשם גיוס מקורות אנושיים על מנת להשפיע עליהם לפעול באופן הרצוי. קיימות הצעה לבצע מיזוג בין היומינט ובין תחום ההנדסה החברתית, אולם נראה שמהלך כזה עלול להחמיץ את היתרונות הקיימים של דיסציפלינת היומינט ולתעל אותה

לתחום אחד בלבד שהוא תחום אבטחת המידע. וכך להחמיץ את הפוטנציאל הגלום בתחום היומינט הקיברנטי ההתקפי.

התפתחות היומינט הקיברנטי החלה באמצע העשור הקודם, על ידי הכוונת סוכנים לעשות שימוש בכלים קיברנטיים, ובראשם האינטרנט, כלומר הפניית הסוכנים לפורומים ברשת, שם הם יפעלו בשמם או בשם בדוי. השלב הבא היה יצירת דמויות מדומיינות, שמאחוריהן עמד צוות שהורכב ממספר אנשים מדיסציפלינות שונות. אלה הפנו את הדמויות המדומיינות לפורומים שונים, שבהם הן פעלו בזהות בדויה, ושם הן גם חדרו לאזורים שאין סבירות שסוכנים קיימים יפעלו בתוכם. שלב זה היה פועל יוצא של ההתפתחות הטכנולוגית המואצת של השנים האחרונות, שאפשרה יצירת דמויות באופן טכנולוגי וללא הגבלה. בהקשר הישראלי, שיטה זו יכולה לאפשר מעבר מפעילות של פיקוח וניטור של "טרור הסכינים" – סוג הפעילות הנהוגה כיום, שהאפקטיביות שלה מוטלת בספק – לפעילות אקטיבית ופרו אקטיבית שמטרתה להביא לצמצום ההסתה שמובילה לסוג זה של פיגועים וכן להשפיע על דעת הקהל.

לכאורה, קיימת סתירה פנימית בין מקצוע היומינט הקלאסי של הפעלת סוכנים ובין היומינט המבוסס על הפעלת סוכנים דרך הסייבר. היומינט הקלאסי כולל פגישות אישיות ליצירת אמון וזיקה אישית, היכרות קרובה, אינטימית וארוכת שנים ויצירת יחסי מרות הדומים ליחסי עובד־מעביד וכוללים מתן תגמולים חומריים ולא חומריים. כל זאת, יחד עם תוכנית לפיתוח ההפעלה בראייה ארוכת טווח, בדיקות מהימנות, הכשרות, ציוד באמצעים ועוד. לעומת זאת, היומינט הקיברנטי מתבסס על יחסים שאינם בהכרח קבועים, המחויבות והנאמנות הן ברמה נמוכה יותר, והקשרים בין המפעיל למקורותיו אינם עמוקים ואינם מתבססים על חיבור אנושי בלתי אמצעי.

ביומינט הקלאסי מתקיים מגע אנושי אינטימי, המאפשר שפה בלתי אמצעית ורגשית, שיוצרת חיבור וקירבה החורגים מעֵבר למפגש האינטרסים. ההפעלה ביומינט הקיברנטי מבוססת על אינטרסים מצטלבים. כתוצאה מכך, רמת המחויבות ביומינט הקלאסי גבוהה יותר, והסוכן אף עשוי לבצע מהלכים שיסכנו אותו; לעומת זאת, בהפעלה הקיברנטית רמת הסיכון לסוכן נמוכה הרבה יותר. זאת ועוד, המפגש הפיזי הבלתי אמצעי עם סוכנים מהווה מרכיב חשוב, ולעיתים קריטי, ליצירת הזיקה האישית, שהיא בעלת חשיבות רבה כמעט בכל היבט הפעלתי ומבצעי. המגע הפיזי, האכילה והשתייה המשותפות יוצרים חיבור מיוחד התורם לתחושת המוטיבציה של הסוכן. הסייבר, מצידו, מאפשר לקיים מפגש וירטואלי ברמה הקרובה למפגש פיזי, אך לא מפגש פיזי של ממש, שכל הנדרש במסגרתו הוא לבצע אותו במינימום סיכונים וחתימות מפלילות.

בעידן היומינט הקיברנטי, המאתרים לגיוס הינם מגוונים וכמעט בלתי מוגבלים. ניתן לקבל במהירות מודיעין הדרוש לאתירה, יכולת הבחירה היא מרובה, ואיתה גם הנגישות. זאת ועוד, הסייבר מאפשר לבצע את שלבי הגיוס וההפעלה בסיכון קטן יחסית וכמעט ללא עלות וללא מאמץ, באמצעות התחזות או אנונימיות, ובכלל זה פגישות במולטימדיה. ניתן גם להקים קשר עם יחידים וקבוצות ו/או להשתייך אליהם בלי סיכונים פיזיים. הדבר מאפשר פריצת גבולות ומשפר משמעותית את היכולת של אנשי היומינט להגיע לקהלי יעד רחוקים וקשים לגיוס. הסייבר גם תורם לאנשי החקירות על ידי פעולות לבדיקת מהימנותם של סוכנים וחקירתם של חשודים. כך, למשל, בחינת מהימנות של נחקר יכולה לעשות שימוש בנתונים שהוא שיתף בפייסבוק. דומה שסוגיית המקורות האנונימיים שזהותם אינה ידועה למפעיל הינה פחות משמעותית כאשר המידע נועד למחקר ולהבנת זרמי עומק חברתיים; לעומת זאת, שאלה זו מקבלת משמעות אקוטית כאשר המידע נדרש לפעולה סיכולית או אחרת, העלולה לסכן חיי אדם.

עידן הסייבר מאפשר להיעלם באוקיינוס הגדול של המידע ובתוך משחקי הזהויות והתפקידים, ובכך הוא מאפשר להגביר בצורה משמעותית את התקשורת הבטוחה עם הסוכנים. היכולות להעביר מידע בסייבר הן מגוונות, וניתן לעשות זאת במהירות ובנפחים גדולים. כתוצאה מכך, הסייבר משפר את אפשרויות התקשורת עם סוכנים וסייענים, ובכלל זה העברה מהירה של מידע בנפחים גדולים. בעבר, סוכנים היו צריכים למלא תיקים, מזוודות או ארגזים בחומר ולהעבירם למפעיליהם, תוך סיכון גבוה לשני הצדדים. כיום, די בשימוש בהחסן נייד כדי לאפשר לסוכנים להעביר כמויות גדולות של מידע במולטימדיה ובאיכות גבוהה אף יותר. בכך מצמצם הסייבר את הצורך במפגשים פנים אל פנים ומקטין את הסיכון לשני הצדדים. יחד עם זאת, לפעילות מודיעינית אקטיבית בסייבר יש חתימה, שעלולה להוות איום בטווח הקרוב או הרחוק. במקביל, קיימים סיכונים עקיפים בסייבר, המתגברים והולכים ככל שגוברות פעילויות של פיקוח, ניטור וגילוי.

היומינט הקיברנטי יכול לחדור למרחב הקיברנטי בו עושה היריב שימוש, כמו פורומים פתוחים או סגורים, ולהשתלב בהם בצורה פסיבית (לאיסוף מידע) או אקטיבית. ההשפעה האקטיבית של הסוכנים הקיברנטיים יכולה לבוא לידי ביטוי בגיוס סוכנים של היריב לטובת איסוף מידע, בהכוונה של סוכנים פיזיים לפעול בעולם הפיזי, או בהשפעה של סוכנים קיברנטיים על דעת הקהל (למשל, יצירת דעת קהל נגדית בתחום הדה־לגיטימציה של ישראל בפורומים רלוונטיים). כיוון נוסף שניתן לעשות בו שימוש בעולם הקיברנטי הוא יצירת שמועות שקריות על אדם שמעוניינים לפגוע בו – מעין "סיכול קיברנטי" (shaming). בנוסף, הפוטנציאל של יומינט קיברנטי מאפשר לסוכן הקיברנטי להיות מוביל טכנולוגי של פורום באינטרנט, ובכך להשפיע באופן רב יותר על המתרחש בו.

הפוטנציאל של יומינט קיברנטי להשפיע ולעצב את המרחב הקיברנטי של היריב הוא רב, ונובע מהאופי האזרחי הפתוח של עידן הסייבר. חשוב להדגיש בהקשר זה כי ארגוני מודיעין רבים פועלים כבר כיום בעולם הקיברנטי, וכי ניתן לאתר דמויות קיברנטיות של ארגונים אלה. הדבר מאפשר ליצור שיתופי פעולה וסינרגיה הדדית עם ארגוני מודיעין זרים בעלי אינטרסים משותפים. במקביל, יש לקחת בחשבון שגורמים עוינים או יריבים יעשו שימוש מניפולטיבי במרחב הקיברנטי וינסו להחדיר באמצעותו "סוכנים קיברנטיים כפולים" ולהזין גופי מודיעין במידע כוזב.

בעולם האזרחי המוביל את הסייבר פותחה דמות ה"אוואטר" (AVATAR), שהינה ייצוג של משתמש בסייבר באמצעות אייקון גרפי בדמות או בדמויות מדומיינות, כמו שחקן בהצגה או בסרט קולנוע. אייקון זה מאפשר לעשות שימוש במספר בלתי מוגבל של זהויות וליצור מצג וכיסויים כמעט לכל תרחיש שייבחר, וזאת בהיקפים גדולים, במהירות וללא צורך במבצעים מורכבים ועתירי משאבים.

המודיעין האמריקאי הזהיר מפני השימוש ב"אוואטרים" לצורכי טרור, דוגמת "אוואטר" של אוסאמה בן לאדן לגיוס המוני של טרוריסטים.[8] רוברט אוהארו, כתב ה"וושינגטון פוסט", המדבר על הפיכתו של שדה הקרב של המרגלים לווירטואלי, נותן כדוגמה "אוואטר" של איש עסקים בעולם המשחקים, ומציין כי אנשי מודיעין מצביעים על הפוטנציאל של "אוואטר" זה לשמש לצורכי טרור ופשיעה.[9]

יש מקום מרכזי להפעלת "אוואטרים" מסוגים ובהיקפים שונים ביומינט הקיברנטי, ובכלל זה להשתמש ב"אוואטרים המפותחים בחברות אזרחיות, כמו סוכן "אוואטר" לבדיקת אמת,[10] מכשיר לבדיקת אמת על בסיס קול[11] ואפליקציות של פוליגרף,[12] לצורכי סיוע בחקירות ובבדיקות מהימנות.

כיווני פעולה לבחינה בקהילות המודיעין

תחום היומינט הקיברנטי משלב בין המאפיינים ההפעלתיים של מודיעין אנושי ובין עולם הסייבר. שילוב זה מזַמן הזדמנויות חדשות ופורץ גבולות, שעולם היומינט המסורתי תחם לעצמו. מוקדם לדעת האם מדובר בדיסציפלינה חדשה, אך יש בשילוב זה מאפיינים חדשים של תפיסה ופעולה המחייבים סינרגיה חדשה בין הסביבה החשאית ובין הסביבה האזרחית־מסחרית. בכך טמון פוטנציאל גדול, הן להשגת מודיעין מקהלים חדשים, בזמנים קצרים יותר ובהיקפים רחבים יותר, והן להשפעה ברשתות החברתיות ובמרחב הסייבר של היריב.

היומינט בעידן הקיברנטי חווה שינוי מהותי, ובראשו כניסה של תת־מקצוע חדש, שהוגדר במאמר זה כיומינט קיברנטי. הסיבה להגדרתו ככזה היא, שלצד הזדקקותו לעקרונות הדומים לעקרונות יומינטיים מסורתיים לצורך הפעלה בתווך הקיברנטי, נוצר כאן מקצוע בעל מאפיינים חדשים, אשר אינו מחייב מגע ישיר עם

המקורות. הבנה זו מחייבת התארגנות בכלל ההיבטים של בניין הכוח המודיעיני, בדגש על תחום הכשרת כוח האדם המודיעיני, אשר לצד רגישות אנושית צריך לסגל לעצמו גם רגישות חברתית.

במאמר זה הצגנו את עקרונות מקצוע היומינט מהתקופה שקדמה לעידן הקיברנטי, כמקצוע מודיעיני־איסופי קלאסי. בהמשך הצגנו את ההתפתחות שחלה במקצוע זה בעידן הסייבר, בדגש על השונות והחדשנות שקיימות בעידן הנוכחי. בחַנו את שאלת הסתירה, לכאורה, שקיימת בין שתי הפנים של מקצוע היומינט – הקלאסי והקיברנטי – והצבענו על שורה של הבדלים ביניהם:

א. ביומינט הקלאסי נדרשים קירבה ומפגש בלתי אמצעי עם המקור. לעומת זאת, ביומינט הקיברנטי ניתן להפעיל מקורות בלי לדעת מה זהותם (עד גבול מסוים).

ב. ביומינט הקלאסי יש מגבלה על היכולת לעבור גבולות. לעומת זאת, ביומינט הקיברנטי ניתן לפרוץ גבולות ולהפעיל מקורות גם בעולמות רחוקים.

ג. היומינט הקלאסי מתמקד באיסוף מידע. ביומינט הקיברנטי ניתן גם להשפיע על דעת הקהל של היריב (באמצעות לוחמה פסיכולוגית).

ד. ביומינט הקלאסי המאתרים הם מוגבלים ויש קושי להשיג מידע על המועמדים לגיוס. לעומת זאת, ביומינט הקיברנטי המאתרים כמעט בלתי מוגבלים ומרבית האנשים מנדבים מידע וחושפים את עצמם מרצונם החופשי.

ה. ההפעלה ביומינט הקלאסי כרוכה בסיכון רב למפעיל ולמופעל. לעומת זאת, הפעלה קיברנטית היא לכאורה בטוחה יותר ואינה כרוכה בסיכון (זאת, למרות שגם הפעלה קיברנטית מותירה חתימות).

ו. בהפעלה הקלאסית המרחב הפיזי של היריב הינו נתון. לעומת זאת, בהפעלה קיברנטית ניתן להשפיע ולעצב את המרחב הקיברנטי של היריב.

ז. היומינט הקלאסי התבסס על מקורות אנושיים ועל מפעילים אנושיים. לעומת זאת, היומינט הקיברנטי מתבסס, לצד ההפעלה האנושית, גם על דמויות מדומיינות בשני הצדדים ועל מכונות היוצרות דמויות המוניות.

בעידן הסייבר התחזקה השילוביות בין הדיסציפלינות האיסופיות. הסייבר והסיגינט מספקים מודיעין ליומינט לצורכי אתירה וגיוס, לנגישות והפעלה ולהזדמנויות מבצעיות, וזאת לצד מטריה מפקחת ומאבטחת לפעילותו. היומינט מספק לסיגינט ולסייבר קצות חוט ו/או מודיעין המאפשר להם ליירט ולנטר באמצעותו מודיעין, וכן נגישות לאפיקי מידע ולמאגרי מידע וציוד קצה שאינם מחוברים לרשת, וכל זאת באמצעות סוכנים מזן חדש.

חשוב שהדיסציפלינה היומינטית בקהילת המודיעין תעקוב אחרי הנעשה בתעשיות ובחברות האזרחיות המובילות את המחקר והפיתוח בתחום הקיברנטי, וגם חודרות לעולם ההפעלה בסייבר,[13] ותתאים את מקצוע היומינט לאתגרי המציאות החדשה. בנוסף, חיוני שקהילת המודיעין תקיים שיח רציף עם התעשיות

והחברות האזרחיות העוסקות בתחום זה. שיח כזה יגדיל באופן משמעותי את יכולות ההתמודדות היומינטיות עם האתגרים שבפתח, משום שלפי הבנתנו קיימות טכנולוגיות ויכולות יומינט משמעותיות שנוצרו במגזר הפרטי, שהמערכת הביטחונית יכולה וצריכה ללמוד מהן, במקום לנסות לפתח את כלל הכלים והשיטות אצלה בבית.

הערות

1 Andrew Shapiro, "Is the Net Democratic? Yes – and No," Berkman Center for Internet and Society at Harvard University, http://cyber.law.harvard.edu/shapiroworld.html

2 Amit Steinhart, "The future is behind us? The human factor in cyber intelligence: Interplay between Cyber-HUMINT, Hackers and Social Engineering," Cyber Guard, 2014, http://diplomacy.bg/archives/1190?lang=en

3 Sun Tzu, The Art of War, Translated by Lionel Giles, XIII: The Use of Spies, The Internet Classic Archives, 1994-2009, http://classics.mit.edu/Tzu/artwar.html

4 מתנדבים מהווים סיכון/הזדמנות, כי טיבם אינו ידוע וכוונותיהם לא נבדקו. אלה יכולים להיות נוכלים ושרלטנים, כאלה הפועלים ממניעים אמיתיים ומגוונים, או כאלה שהם שליחי היריב המתכוונים לחדור לשורותינו כסוכנים כפולים. הם יכולים להפוך לסוכנים הטובים ביותר, ובאותה מידה יכולים להעביר אותנו אל עברי פי פחת. מאמר של החוקרת קתרין ל' הרביג, שפורסם על ידי משרד ההגנה של ארצות הברית, מנתח את השינויים בשיטות הריגול בארצות הברית בשנים 1947–2007: K.L. Herbig, "Changes in Espionage by Americans: 1947-2007," March 2008, https://www.fas.org/sgp/library/changes.pdf

5 יהושפט הרכבי, **המודיעין כמוסד ממלכתי, הספר הגנוז**, הוצאת מערכות, 2015, עמ' 173.

6 Julien Babanoury, "Where does Humint fit in with 21st Century Intelligence Community," September 8, 2014, http://www.secuinsight.fr/2014/03/03/where-does-humint-fit-in-with-the-21st-century-intelligence-community-by-julien-babanoury-ceis/

7 גבי סיבוני, "מודיעין זה לא רק סייבר", **הארץ**, 1 ביולי 2014.

8 Sara Malm, "A threat for the digital age – an avatar Osama Bin Laden: U.S. intelligence warned terrorists could create virtual jihadist to 'preach and issue fatwas for hundreds of years," MailOnline, January 9, 2014, http://www.dailymail.co.uk/news/article-2536440/A-threat-digital-age-avatar-Osama-bin-Laden-U-S-intelligence-warned-terrorists-create-virtual-jihadist-preach-issue-fatwas-hundreds-years.html; David Kravets, "US intel: Bin Laden avatar could recruit terrorists for hundreds of years," Wired, January 9, 2014, http://www.wired.co.uk/news/archive/2014-01/09/osama-bin-laden-avatar

9 Robert O'Harrow Jr., "Spies' Battleground Turns Virtual," *The Washington Post*, February 6, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/02/05/AR2008020503144.html

10 **AVATAR** – Automated Virtual Agent for Truth Assessments in Real-Time, University of Arizona, 2015, http://borders.arizona.edu/cms/projects/avatar-automated-virtual-agent-truth-assessments-real-time

11 Amir Liberman, The LVA (Layered Voice Analysis) Technology, nemesysco, http://www.nemesysco.com/technology-lvavoiceanalysis.html

12 Android apk Polygraph Lie Detector version 1.0 Free Download, 2014, http://appdownload.m5f.net/apk/com.ciberdroix.polygraph.html

13 למשל, חברת מודיעין סייבר ישראלית המפעילה "אוואטרים": https://www.sensecy.com

קול קורא להגשת מאמרים

כתב העת "צבא ואסטרטגיה" 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 לוחמת סייבר במכון למחקרי בטחון לאומי.

פניה זו הינה קול קורא לכתיבה של מאמרים ומחקרים שיפורסמו במסגרת כתב העת. ייבחנו מאמרים הנוגעים לתחומים הבאים:

- חשיבה צבאית ואסטרטגית אוניברסאלית וישראלית;
- למידה מצבאות ולחימה של אחרים;
- בניין כוח צבאי על מרכיביו: המשאב האנושי, אמצעי לחימה, תורה, ארגון, אימונים ופיקוד;
- תקציב הביטחון;
- מודיעין;
- היבטים אתיים, מוסריים ומשפטיים של הלחימה;
- הפעלת הכוח הצבאי בדגש על זירות הפעולה של מדינת ישראל או זירות של צבאות זרים מהן ניתן ללמוד בצה"ל;
- ממשקי צבא דרג מדיני ותהליכי קבלת החלטות;
- טכנולוגיה בטחונית / צבאית;
- לוחמת סייבר והגנה על תשתיות חיוניות;

ניתן לעיין במאמרים דומים שנכתבו בגיליונות הקודמים של כתב העת, באתר האינטרנט של המכון: http://www.inss.org.il/

ייבחנו מאמרים עם הערות שוליים ומראי מקום בהיקף של עד 5,000 מילים.

להגשת הצעות ולפרטים נוספים ניתן לפנות אל:
הדס קליין
מתאם כתב העת "צבא ואסטרטגיה"
hadask@inss.org.il