# צבא ואסטרטגיה

כרך 5 | גיליון 1 | מאי 2013



INSS
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 5 | גיליון 1 | מאי 2013**

# 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 61398.

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)

# שקיפות משפטית כאסטרטגיית ביטחון לאומי

**יוני אשפר**

נקיטת יוזמה נחשבת לעיקרון מועיל בזירות שונות המרכיבות את תפיסת הביטחון הלאומי של ישראל– הזירה הצבאית, הזירה המדינית והזירה התקשורתית. העצה המקובלת בכולן היא לא להיגרר אחר האירועים, ולעולם לא לתת לירִיב לעצב את המערכה. יוצאת דופן, כך נדמה, היא הזירה המשפטית. למרות שההכרה בחשיבותה עלתה מאוד, החשיבה עליה מוגבלת למישור הגנתי ותגובתי, דהיינו: כיצד לספק לדרג המדיני והמבצעי ייעוץ מקצועי והגנה מפני עתירות, תביעות וועדות חקירה, והליכים משפטיים אחרים בישראל ובחו"ל. זוהי משימה חשובה, אך האם בזאת מסתכמת יכולתו של החוק לתרום לביטחון? כיצד יכולה להיראות אסטרטגיה משפטית מקיפה יותר, פרואקטיבית ויוזמת יותר? איזו תועלת, אם בכלל, יכולה לצמוח ממנה, ובאיזה מחיר? על השאלות הללו אשאף להשיב במאמר זה, באמצעות סקירה של קמפיין משפטי־ציבורי חסר־תקדים בצורתו ובהיקפו, שהוביל ממשל אובמה לאורך כהונתו הראשונה.

הקמפיין המדובר לא כלל מודעות בעיתונים או סרטוני פרסומת ויראליים ברשתות חברתיות. המסר הועבר על ידי סדרה של נאומים שנשאו הגורמים המשפטיים הבכירים ביותר של הממשל. הם יצאו זה אחר זה, חלקם יותר מפעם אחת, כדי לפרוס בפני הציבור בצורה בהירה ומפורטת את ה"חזון המשפטי" שבמסגרתו שומר הממשל על הביטחון הלאומי, ומנהל את המלחמה נגד ארגון אל־קאעדה וספיחיו ברחבי העולם.

מאמר זה לא יציע ניתוח משפטי של תוכן הנאומים, או יתיימר לאמץ צד בוויכוח הנמשך בין הממשל למבקריו על עמדותיו המשפטיות בנושאי צבא וביטחון. הנחת היסוד של סדרת הנאומים הייתה שוויכוח כזה הוא בלתי־נמנע, ואף חיוני בכל מדינה דמוקרטית. הבעיה היא שכשהוא מחריף, בעיקר בעתות מלחמה, עלול ויכוח זה לשקף את המתח בין ביטחון לבין ערכים כבחירה בלתי־נמנעת בין

יוני אשפר הוא מנהל המחלקה הציבורית בארגון "גישה". מאמר זה מייצג את עמדותיו הפרטיות בלבד.

השניים. את ה"בחירה הכוזבת" הזאת זיהה אובמה כמכשול, והחליט לפעול כדי לבטל אותה. לשם כך, הוא לא חולל מהפכה בעמדות המשפטיות של הממשל, אלא הגדיר מחדש את המסגרת הרעיונית שבתוכה מתנהל הוויכוח עליהן. בהמשך אנסה לנתח את המסגרת הזאת, ולהסביר מדוע היא הוכיחה את עצמה כאמצעי יעיל הן לחיזוק הביטחון והן לחיזוקם של החוק ושל הערכים שהוא מייצג. לסיכום יוצעו לקחים וכיווני חשיבה ופעולה רלוונטיים לישראל.

## ביטול "הבחירה הכוזבת"

"מאז ה־11 בספטמבר", אמר המועמד אובמה בינואר 2008, "הממשל הנוכחי [של הנשיא בוש] הציב בחירה כוזבת בין החירויות שאנחנו מוקירים לבין הביטחון שאנחנו דורשים". הוא התריע על כך ש'רוח המפקד' שנשבה מהבית הלבן במהלך שמונה שנים הביאה את אמריקה למשבר לגיטימיות פנימי ובינלאומי, שפגע קשות במעמדה והקשה על יכולתה להיאבק בטרור ביעילות. חודשים ספורים אחרי שנבחר פרס הנשיא אובמה את האלטרנטיבה שלו בנאום[1] שנשא בארכיון הלאומי ב־21 במאי 2009.

בבסיס ה"אני מאמין" שהוא פירט באריכות עמדה הקביעה שאחריותו העליונה כנשיא לשמור על ביטחונו של העם האמריקאי אינה עומדת בסתירה למחויבותו לשמור על הערכים הדמוקרטיים ועל ערכי מוסר אוניברסליים, כפי שהם מוגדרים בחוקה ובחוק האמריקאי והבינלאומי. מה שדרוש אינו איזון בין ביטחון לערכים, אלא נחישות לא להתפשר על אף אחד מהשניים, מתוך הבנה שבטווח הארוך הם מחזקים זה את זה וחיוניים זה לזה. הוא הדגיש ששמירה על עקרונות אינה מותרות, וציות לחוק אינו מעמסה. אלה הם "נכסי הביטחון הלאומי הטובים ביותר שלנו", במיוחד במלחמה נגד אויב חמקמק שאינו מחויב לאותם חוקים וערכים.

אובמה נתן מספר דוגמאות לאופן שבו נאמנות אמיצה לערכים מתורגמת לתועלת ביטחונית. ככל שארצות הברית שומרת על דימוי ערכי חיובי, הסביר, היא נהנית משיתוף פעולה הדוק יותר עם בעלות־בריתה, ומגייסת בקלות רבה יותר בעלות־ברית חדשות. במצב זה קל לה יותר לקדם את האינטרסים שלה במסגרת מוסדות בינלאומיים. לתעמולה הנגדית כלפיה קשה יותר להתסיס את דעת הקהל, ולאויביה קשה יותר לגייס לוחמים ולרתום תמיכה עממית החיונית למאבקם. פעולותיה הצבאיות עומדות בקלות רבה יותר בביקורת של בתי המשפט והקונגרס, ומעוררות פחות התנגדות ומחאה מבית ומחוץ. הנשיא התייחס גם לאופן שבו הכרזתו החד־משמעית על הפסקת השימוש בעינויים לא רק מסירה כתם מוסרי, אלא גם מעודדת לוחמי אויב להסגיר את עצמם, מאפשרת למדינות ידידותיות להסגיר שבויים לכוחות האמריקאים לצורך חקירה ומשפרת, בסופו של דבר, את איכות המודיעין שנצבר.

חציו השני של הנאום הוקדש לתחום נוסף שבו ביקש אובמה להיבדל מקודמו – שקיפות. העימות מול אויב כמו אל־קאעדה מעורר באופן מובן שאלות אתיות מורכבות. הדרך שהוא הציע להתמודד איתן היא להסביר כל מה שניתן להסביר, ולהשקיע זמן ומשאבים כדי לשכנע את האמריקאים לתת אמון בתהליכי קבלת ההחלטות, ובמנגנונים המפקחים על הפעולות שננקטות למען ביטחונם. למטרה זו כלל הנשיא בנאומו הבטחה לעולם לא להסתיר את האמת רק משום שאינה נוחה, ותמיד לשתף את הציבור בשיקולים שעמדו מאחורי החלטתו לפרסם או לא לפרסם מידע כלשהו. שמירה על סודיות בצורה שקופה יותר מעוררת פחות חשדות ותיאוריות קונספירציה מהסוג שאפיינו את תקופת ממשל בוש, שבה "הרגישו האמריקאים לעיתים קרובות שחלק מהסיפור הוסתר מהם שלא לצורך". הדברים האלה מהדהדים את נאומו של הנשיא, ג'ון פ. קנדי, על חופש עיתונות משנת 1961, שבו דיבר על כך ש"הסכנות שנובעות מהסתרה מופרזת וחסרת בסיס של עובדות משמעותיות עולות בהרבה על הסכנות שמונים כדי להצדיק אותה".[2]

לשני הנושאים המרכזיים בנאום – חוקיות ושקיפות – ייחס אובמה תפקיד כפול: הן משמשות כמנגנוני בקרה הכרחיים על בעלי כוח וסמכות אבל גם כמקורות ללגיטימציה, החיונית לא פחות עבורם. לתפיסתו, כל עוד התפיסה בציבור היא שחוקיות ושקיפות מנוגדות לביטחון, המדינה תישאר במצב שבו הדמוקרטיה שלה שברירית ומרחב הפעולה שלה מוגבל. כך הוא תיאר זאת:

> אנו רואים איך לאחרונה הוויכוח כיסה על האמת ושלח אנשים לקצוות מנוגדים ומוחלטים. מצדו האחד של הספקטרום עומדים אלה שמתעלמים מהאתגרים שמציב הטרור, ושכמעט אף פעם לא יציבו את הביטחון הלאומי מעל לשקיפות. ובצד השני של הספקטרום עומדים אלה שמאמצים עמדה שאפשר לנסח בשתי מילים: 'הכול הולך'. לפי הטיעונים שלהם, המטרה של לוחמה בטרור מצדיקה את כל האמצעים, ולנשיא צריכה להיות סמכות גורפת לעשות כל מה שהוא רוצה – בתנאי שזה נשיא שאיתו הם מסכימים...אבל שני הצדדים טועים. העם האמריקאי [...] יודע שאנו לא צריכים להקריב את ביטחוננו בשביל ערכינו, ולא את ערכינו בשביל ביטחוננו, כל עוד אנו ניגשים לשאלות מורכבות בכנות, בזהירות, ועם מנה של הגיון בריא.

אולם, אם היו לנשיא הטרי ציפיות שבנאום אחד הוא יצליח "למסגר מחדש את הוויכוח", נכונה לו אכזבה. מימין ראו בהצהרותיו אישור לטענות בדבר היחס ה"חלבי" שלו למלחמה בטרור, והתגובה מצד ארגוני זכויות אדם הייתה צוננת לא פחות. העיתונאי דניאל קליידמן תיאר בספרו פגישה שקיים אובמה עם הדמויות המרכזיות בקהילת זכויות האדם האמריקאית יום לפני הנאום, ובה הוא פרס בפניהם את עיקרי משנתו. לפי הדיווח, האירוע הסתיים בטונים צורמים. המשתתפים, שהוזמנו לצפות בנשיא נואם למחרת, בחרו לא להגיע.[3]

## "הנאומים הקאנוניים"

גם בנאום הזכייה שלו בפרס נובל, בדצמבר 2009, חזר אובמה והדגיש את התועלת שבציות לחוק בזמן מלחמה, אבל השינוי התפיסתי שהוא ניסה לקדם התחיל להיות מורגש רק כאשר לנאומיו שלו נוספו בהדרגה נאומים של דמויות בולטות נוספות מהצוות המשפטי של הממשל. כולם השתמשו בנאומי הנשיא כנקודת מוצא וציטטו אותם בהרחבה, אבל כל דובר הרחיב והעמיק את הדיון בסוגיות הערכיות והמשפטיות שנוגעות לתחום האחריות שלו, או שהיו בכותרות באותו הזמן.

הראשון ביניהם היה הארולד קו (Harold Koh), היועץ המשפטי של מחלקת המדינה, לשעבר דיקן הפקולטה למשפטים של אוניברסיטת ייל, ודמות ותיקה ומכובדת בתחום זכויות האדם. הנאום[4] המפורט שהוא נשא במרס 2010 בכנס השנתי של ה־American Society of International Law, שהוא אחד הפורומים החשובים ביותר בקרב מומחי המשפט הבינלאומי בעולם, נועד לצקת תוכן משפטי נוסף לתוך המסגרת שהגדיר כבר הנשיא. טיעונו המרכזי היה שהממשל מחויב ללא סייג לחוק הבינלאומי בכל הפעולות שהוא נוקט במאבק בטרור. באותה תקופה התברר שאובמה הגביר בצורה דרמטית את השימוש ב"הריגות ממוקדות" (targeted killings – המכונות בישראל "סיכולים ממוקדים") באמצעות כלי־טיס בלתי־מאוישים, גם מחוץ לשדה הקרב "החם" של אפגניסטן – דבר שעורר ביקורת הולכת וגוברת. קו רתם את סמכותו המקצועית והמוסרית לטענה שהפעולות הללו אינן מנוגדות למשפט הבינלאומי, ומבחינות משפטיות מסוימות הן אפילו עדיפות על אמצעים אחרים.

מנאומו של קו ואילך ניתן לזהות תבנית קבועה. בכל פעם שהתעורר ויכוח משפטי או ציבורי סביב פעולות הממשל וזרועות הביטחון, יצא גורם בכיר והציג בפומבי את ה"קייס" המשפטי של הממשל. קמפיין הנאומים יצר עבור משפטני הממשל פלטפורמה שאפשרה להם להגיב לביקורת באופן ישיר, בשפה פשוטה ובתוך הֶקשר של מסגרת משפטית רחבה ושל מהלך ציבורי ממושך. ברוח זו, חודשים ספורים אחרי נאומו של קו הסביר דייויד קריס (David Kris), עוזרו של התובע הכללי אריק הולדר (Eric Holder), בנאום[5] במכון ברוקינגס את עמדת הממשל בעוד נושא שנוי במחלוקת – העמדה לדין של זרים הנאשמים בטרור בבתי המשפט הפדרליים. אחרי הריגתו של בן־לאדן פרסם קו פוסט בבלוג משפטי מוביל, שבו הסביר מדוע הפעולה הייתה חוקית.

לא רק יועצים משפטיים לקחו חלק בקמפיין הציבורי המתהווה. כדי לבטל את הטענה שקיים שקלול תמורות (trade-off) בין ביטחון לערכים לא היה די במשפטנים מכובדים ש"ידברו ביטחון". נדרשו גם אנשי ביטחון מוערכים שישכנעו כי החוק אינו נטל אלא נכס ביטחוני. ג'ון ברנן (John Brennan), יועצו של הנשיא לביטחון לאומי וללוחמה בטרור, היה האיש המושלם למשימה. עם קריירה ארוכה

ב־CIA מאחוריו, ועם הופעה תואמת שכאילו נלקחה מסרט הוליוודי, הפך ברנן לאחד מנושאי המסר המרכזיים. בספטמבר 2011 הוא נשא נאום[6] בבית הספר למשפטים של אוניברסיטת הרווארד, שכותרתו מסכמת את תוכנו: "מחזקים את ביטחוננו באמצעות נאמנות לערכינו ולחוקינו". זמן קצר לאחר מכן חזר המיקרופון לידי המשפטנים, כאשר היועץ המשפטי של משרד הביטחון, ג'ה ג'ונסון (Jeh C. Johnson), נשא שני נאומים בהפרש של ארבעה חודשים בלבד זה מזה – באוקטובר 2011[7] ובפברואר 2012.[8]

ג'ונסון סקר את מאמצי הממשל ואת הצלחותיו בשכלול המסגרת המשפטית כך שתיתן כלים להתמודדות עם איומים מהסוג שמציבים ארגוני טרור, ובמקביל תשמור על ההפרדה הנדרשת בין מערכת המשפט הצבאית לבין מערכת המשפט האזרחית. הוא התייחס לנושאים רגישים כמו מעצרים צבאיים ממושכים והחוקיות של הריגה ממוקדת ללא משפט של אזרחים אמריקאים שהצטרפו לאל־קאעדה. בנאום השני, כשהוא מתייחס לשמועות על חילוקי דעות חריפים בינו לבין הרולד קו, אישר ג'ונסון שמתקיימים ויכוחים בין היועצים השונים והציע לראות בהם הוכחה למורכבות האתגר המשפטי, ולרצינות שבה מנסים להתמודד איתו. אם במכוון ואם לאו, מכל הנאומים מתקבל הרושם שהעמדות המשפטיות כלפי חלק מהסוגיות המורכבות ביותר, גם כשהן מגובשות ומוסכמות, נולדו בלא־מעט ייסורים והתחבטויות.

הבא בתור ברשימת הנואמים היה התובע הכללי אריק הולדר – כנראה המקורב ביותר לאובמה באופן אישי מקרב כלל הדוברים. במרס 2012 הוא נשא נאום[9] בבית הספר למשפטים של אוניברסיטת נורת'ווסטרן, שבו התייחס בין השאר לביקורת על תוכנית ההאזנות שמפעיל הממשל, וחידד כמה מהעמדות המשפטיות שהשמיעו קודמיו. הפתעת הסדרה הגיעה כחודש אחרי כן, כאשר גם ה־CIA הצטרף ל'מתקפת השקיפות המשפטית'."[10] סטיבן פרסטון (Stephen W. Preston), היועץ המשפטי של סוכנות הביון המרכזית, טען בנאום[11] פומבי ומפורט באופן לא־טיפוסי לסוכנות החשאית, שגם פעולותיה כפופות לאותם עקרונות ערכיים ולחוק האמריקאי והבינלאומי.

בסוף אפריל של אותה שנה, בעקבות ביקורת ציבורית על תוכנית ההריגות הממוקדות, שלח הנשיא את ברנן לנאום[12] שוב. ברנן התמקד הפעם בניסיון לשכנע שהתוכנית פועלת תחת מערך של סטנדרטים ונהלים קפדניים, ובפיקוחו הישיר של הנשיא, כדי להבטיח את החוקיות של כל פעולה ולצמצם תקלות וטעויות למינימום. "מעולם", הוא הצהיר, "לא היה הממשל האמריקאי כה גלוי בנוגע למדיניות הלוחמה בטרור שלו וההצדקות המשפטיות שלה".

בשלב זה, פרשנים לא יכלו להתעלם עוד מסדרת ה"נאומים הקאנוניים"[13] שהחלה בנאום הנשיא ונמשכה בנאומי היועצים המשפטיים הבכירים של מחלקת

המדינה, משרד הביטחון, משרד המשפטים, ה־CIA וכמובן, נאום "מר ביטחון", ברנן. למעטים היה ספק שמדובר במהלך שתואם בצורה הדוקה על ידי הבית הלבן. לפי תיאור אחד,[14] מי שהייתה שותפה לניסוח הטיוטות ולתיאום המסרים היא אברייל היינס (Avril Haines), היועצת המשפטית של המועצה לביטחון לאומי.

הנאום[15] הבא נישא בספטמבר 2012 על ידי הרולד קו, וסיפק תשובות לשאלות בנושא שלא כוסה על ידי הנאומים הקודמים – לוחמת סייבר. בנאומו פירט קו כיצד רואה הממשל את תקפותו של המשפט ההומניטרי הבינלאומי גם בשדה הלחימה הווירטואלי. תקיפת סייבר, הוא טען, יכולה להיחשב כתקיפה צבאית שמפעילה את זכות ההגנה העצמית. כמו כן, כל פעילות צבאית בתחום זה כפופה לעקרונות דיני הלחימה של המשפט הבינלאומי.

קו התייחס גם לשאלה, מדוע כדאי לארצות־הברית להתחייב מיוזמתה למגבלות חוקיות בתחום חדש שאינו מכוסה על ידי "החוקים הישנים". "המשפט הבינלאומי", השיב, " לא רק מגביל אותנו, הוא מספק לנו את החופש ואת הכוח לעשות דברים שלא היינו יכולים לעשות לעולם ללא הלגיטימיות של החוק. אם נצליח לקדם תרבות של שמירה על החוק, אנחנו נקטוף את הפירות שלה. אם נרוויח מוניטין של שומרי חוק, הפעולות שנעשה יזכו ליותר לגיטימציה ברחבי העולם בזכות נאמנותן לשלטון החוק".

האחרון בסדרה עד כתיבת מאמר זה היה נאום[16] נוסף של ג'ה ג'ונסון, שזכה לתשומת לב תקשורתית רבה יחסית בארצות־הברית ומחוצה לה. ייתכן שאחת הסיבות לכך הייתה שהפרקליט הבכיר של הפנטגון בחר לשאת אותו באוקספורד, בריטניה, אבל סביר יותר שתוכן הנאום הוא האחראי העיקרי לעניין שהוא עורר. ג'ונסון בחר להקדיש את הנאום האחרון שלו בתפקיד לאחת מנקודות התורפה העיקריות של המסגרת המשפטית, שהוא ושאר הנואמים טרחו לנסח ולהציג לפני הציבור.

לפי אותה מסגרת, חלק ניכר מהסמכויות שמפעילה ארצות־הברית במלחמתה נגד אל־קאעדה נובע מהעובדה שהיא נמצאת במצב מלחמה עם הארגון וספיחיו בעולם מאז 2001, בעקבות ההתקפה של האחד־עשר בספטמבר. טיעון זה עורר ביקורת על כך שלמעשה מדובר במסגרת משפטית של מלחמה שאינה מוגבלת במרחב ובזמן. כך היא עלולה להפוך את המצב החריג של מלחמה, עם הסמכויות ששמורות לו כמו הריגה ללא משפט, העמדה לדין בבתי משפט צבאיים ומעצר ללא הגבלת זמן, למצב הנורמלי החדש. כדי להפיג את החשש הזה ניסה ג'ונסון לשכנע את שומעיו שבעיני הממשל, למלחמה עם אל־קאעדה יש סוף. השאלה היא רק, איך נדע שהוא הגיע.

ארצות־הברית, הוא הסביר, נמצאת במלחמה לא־קונוונציונלית, נגד אויב לא־קונוונציונלי, ולכן גם אין לצפות שהיא תסתיים בצורה קונוונציונלית כמו הסכם

שביתת נשק או כניעה. עם זאת, אין לראות בה מלחמה תמידית. לטענת ג'ונסון, אם ארגון אל־קאעדה ימשיך להיחלש, ושורותיו ימשיכו להתדלדל, כפי שקורה בשנים האחרונות, תגיע בהכרח נקודת מפנה (tipping point) שבה יסתיים מצב הלחימה, ואיתו גם הסמכויות הרלוונטיות שהוא מעניק לממשל.

## על המשפט הבינלאומי

אחד המכשולים המרכזיים שעמדו בפני הטמעה מוצלחת של המסרים היה היחס השלילי שטופח בזמן ממשל בוש כלפי המשפט הבינלאומי והמוסדות המזוהים איתו. הממשל החדש קידם קו שונה שלפיו החוק הוא בבסיסו טוב ונחוץ, אבל נדרשת פרשנות מעודכנת שלו.

רבים מהנואמים הדגישו שכל פעולה הננקטת על ידי כוחות הביטחון בעימות עם אל־קאעדה נשקלת מול ארבעת עקרונות היסוד של דיני המלחמה: 1) נחיצות – מדובר בפעולה הכרחית מבחינה ביטחונית, 2) הבחנה – נעשה מאמץ להבחין בין לוחמים לאזרחים שאינם מעורבים בלחימה, 3) מידתיות – כל נזק שבכל זאת נגרם לאזרחים הוא מידתי ביחס לתועלת הצבאית של הפעולה, ו־4) אנושיות – הימנעות מגרימת סבל מיותר ושמירה על כבוד האדם באשר הוא אדם. כשהם מוצגים כך, בפשטות, נראים דיני הלחימה (המכונים גם המשפט ההומניטרי הבינלאומי) כמערכת נורמטיבית שקל להסכים עליה. קל גם להסכים כי שמירה עליה במהלך סכסוכים א־סימטריים היא אתגר מורכב. זוהי נקודת פתיחה משופרת לוויכוח על הפרשנות הנכונה לחוק, כך שימלא את ייעודו המקורי גם בעימותים של המאה ה־21.

גם ביחס למוסדות משפטיים בינלאומיים הועבר מסר דומה: הם חשובים, אבל טעונים שיפור. הרולד קו התייחס בנאומו בהרחבה לבית הדין הפלילי הבינלאומי (ICC) ולמועצת זכויות האדם של האו"ם (Human Rights Council). בין שני המוסדות האלה לבין ארצות־הברית עומדים סלעי מחלוקת משמעותיים – הגדרת הפשע של תוקפנות (the crime of aggression) והיחס הבלתי מאוזן כלפי ישראל, בהתאמה – אבל, ציין קו, הממשל הנוכחי, בניגוד לקודמו, החליט לפעול לתיקון הפגמים באמצעות שיתוף פעולה בונה.

תמצית המסר לציבור הייתה שהחוק הבינלאומי והמוסדות שמזוהים איתו אינם עומדים באופן מובנה בסתירה לאינטרסים של ארצות־הברית. אדרבה, יש בהם פוטנציאל חיובי שניתן לממש בעזרת גילוי יוזמה ומנהיגות.

## מבחן התוצאה

האם סדרת הנאומים הצליחה למסגר מחדש את הוויכוח? ואם כן, האם היו לדבר השלכות חיוביות על הביטחון, על ערכים ועל החוק? עדיין מוקדם להעריך באופן ודאי, אבל יש די סימנים לכך שהתשובה לשתי השאלות האלה יכולה להיות 'כן'.

לכל הפחות, אפשר לומר שהוויכוח על מדיניות הממשל במאבק בטרור התמתן בצורה משמעותית בהשוואה לתקופת בוש. בדרכו לניצחון נוסף בבחירות קיבל הנשיא ציונים גבוהים מהציבור, ואף מיריביו הפוליטיים, בכל הנוגע לביטחון לאומי ולמאבק בטרור. במקביל, הביקורת על הרקורד המשפטי והמוסרי של ממשלו מצד הקונגרס, התקשורת וארגוני זכויות אדם נשארה מצומצמת לאורך מרבית שנות הכהונה הראשונה. משפטן אחד שמילא תפקיד בכיר בממשל בוש הודה[17] שאובמה הצליח יותר מקודמו בתפקיד בהשגת אישורים למדיניות שלו מבתי המשפט ובשיתוף פעולה של בעלות־ברית. ג'ון ברינג'ר, שהיה היועץ המשפטי של מחלקת המדינה בתקופת כהונתה של קונדליזה רייס, הביע[18] הערכה רבה לצוות המשפטי של אובמה על הדרך הארוכה שעשו בהסברת החוקיות של כל הפעולות הנעשות בשם הביטחון הלאומי. פרשנים נוספים תיארו את המצב שהושג לקראת סוף הכהונה הראשונה של אובמה כ"יציבות של הארכיטקטורה המשפטית"[19] של הממשל בנושאי ביטחון. יש מי שאף דיברו[20] במונחים של קונצנזוס רחב וחוצה מפלגות על המסגרת המשפטית של לוחמה בטרור – מציאות שקשה היה לדמיין עד הזמן האחרון.

הניתוחים הללו מעניינים במיוחד לאור העובדה שרוב בקרב אותם פרשנים טוען שמבחינת העמדות המשפטיות הטהורות, חלה בין ממשל בוש השני לבין ממשל אובמה יותר המשכיות מאשר שינוי[21]. לפיהם, ממשל אובמה הצליח לגייס לגיטימציה רבה יותר מבית ומחוץ עבור עמדות משפטיות ואמצעים צבאיים שאינם שונים מאוד מאלה של קודמו. עובדת היותו נשיא דמוקרטי ללא ספק סייעה בכך, אך קרוב לוודאי שהאסטרטגיה המשפטית שלו והקמפיין הציבורי ש"שיווק" אותה תרמו תרומה משמעותית. את הלגיטימציה הזאת תרגם הממשל להרחבת הפעילות הצבאית שמכוונת כלפי אל־קאעדה ולהעמקת הבריתות באזורים שונים בעולם. דווח[22] כי במסמכים שנתפסו בביתו של בן־לאדן לאחר הריגתו התלונן מנהיג הארגון על דעיכת המותג "אל־קאעדה", בין השאר בשל שינויים ברטוריקה שבקעה מוושינגטון מאז בחירתו של אובמה.

הדעות חצויות יותר בשאלת הצלחתו של אובמה לקדם את הערכים שעליהם דיבר. יש הטוענים שקמפיין הנאומים סייע להרדים את הקולות הביקורתיים בציבור, בבתי המשפט, בקונגרס ובקהילה הבינלאומית. הם מסתכלים בדאגה על הלגיטימיות שממנה נהנות היום פעולות שבעבר עוררו ביקורת עזה, כמו תוכניות האזנה נרחבות שאישר הממשל, או המשך הכליאה בכלא גואנטנמו, במקרים

מסוימים – ללא העמדה לדין וללא קציבת זמן. בנוסף, ההחלטה של הממשל לא לחשוף מסמכים שמתארים מקרים קשים של עינויים מתקופת בוש ולא להעמיד לדין איש מהמעורבים עוררה את החשש שאובמה ממשיך במסורת של חסינות בפני החוק.

חששות אלה קיבלו חיזוק נוסף כאשר זמן קצר לאחר בחירתו לכהונה נוספת, בימים האחרונים של שנת 2012, אישר הנשיא שני חוקים שנויים במחלוקת: אחד (FISA) שמאריך את תוקף הסמכויות שהוענקו לסוכנות לביטחון לאומי להאזין ולצותת לאזרחי ארצות־הברית, והשני (NDAA) שחוסם באופן כמעט מוחלט את הסיכויים לקדם את סגירת כלא גואנטנמו.

אין ספק שהביקורות הנוקבות ביותר כלפי העמדות המשפטיות של ממשל אובמה עוסקות בחיסולים הממוקדים מן האוויר במדינות שאיתן ארצות־הברית אינה נמצאת מבחינה חוקית במצב של מלחמה, כמו פקיסטן, תימן וסומליה. מארי אוקונל (Mary O'Connell), פרופסור למשפטים מאוניברסיטת נוטרה דאם, שהובילה את ההתנגדות למבצעים כאלה מאז שהחל בהם ממשל בוש ב־2002, ממשיכה גם כיום לעמוד בחודם של חיצי הביקורת, אבל היא כבר אינה קול יחיד. בחוגים אקדמיים, בקרב ארגוני זכויות אדם ובתקשורת הולכות ומתרבות טענות על פער גדול בין המילים היפות שנאמרו בנאומים לבין היישום שלהן בשטח.[23] גם מחוץ לארצות־הברית, שם הייתה לקמפיין המשפטי תהודה מוגבלת, גוברת אי־הנחת בדעת הקהל כלפי ההריגות הממוקדות, וכבר הועלתה התהייה שמא תהפוך סוגיה זו להיות "הגואנטנמו של אובמה".[24] גם ההתחייבות ל"נקודת מפנה" עתידית כלשהי שתסיים את המלחמה לא הרגיעה את הביקורות הללו.[25]

עם זאת, ייתכן שהציפיות לשינוי קיצוני יותר היו מוגזמות. כפי שהסבירו כמה מהנואמים, כל ממשל חייב לשמור על מידה רבה של המשכיות עם העמדות המשפטיות של קודמו. אובמה, למרות שהיה מוגבל גם על ידי רוב רפובליקאי בקונגרס, הצליח ליישם שורה מרשימה של רפורמות, למגר נורמות פסולות כמו עינויים ולהגדיר סטנדרטים חדשים של שקיפות בענייני ביטחון לאומי.

סדרת הנאומים לא שלהבה את הציבור הרחב, אבל היא הותירה רושם חיובי על קהלים בעלי השפעה בעולם המשפט, באקדמיה, בתקשורת ובמוסדות בינלאומיים. לאלה, בתורם, הייתה השפעה ניכרת על השיח הציבורי. הצגתן של עמדות משפטיות סבוכות באופן פשוט ונגיש לציבור סיפקה לגיטימציה לא רק לפעולות הממשל, אלא גם למערכת המשפט ולחוק האמריקאי והבינלאומי בפני עצמם.

בשנת 2013 צפויה אסטרטגיה זו לעמוד במבחן רב־משמעות בזירה הבינלאומית. בחודש ינואר הכריז חוקר מיוחד של נציבות זכויות האדם של האו"ם, בן אמרסון (Emmerson), על פתיחת חקירה מקיפה שתבחן את החוקיות של הריגות ממוקדות מהאוויר. יהיה זה מעניין לראות, האם העובדה שיועצי

הקדנציה הראשונה של אובמה הקדימו והציגו באופן יזום מערך טיעונים סדור ומנומק תסייע להרכב של הקדנציה השנייה להתמודד טוב יותר עם אתגר משפטי, תקשורתי ודיפלומטי מסוג זה.

גם התלהטות המחלוקת סביב סוג אחד של פעילות צבאית לא תפחית בהכרח מההשלכות העמוקות וארוכות־הטווח של מדיניות אובמה. בהנהגתו גובשה והוטמעה פילוסופיה פוליטית שמגדילה בצורה משמעותית את מידת הכפיפות של סמכויות הנשיא בענייני ביטחון לאומי לחוק האמריקאי והבינלאומי.[26] בעזרת אנשי ונשות צוותו הוא הדגים מודל שבו הממשל כבול יותר לחוק, ובאותו הזמן חופשי יותר לפעול בגבולות החוק; חשוף יותר לביקורת עניינית ולגיטימית אך מוגן יותר מפני ביקורת עוינת.

הוויכוח סביב מדיניות הלוחמה בטרור של ארצות־הברית נמשך, כאמור, אבל הוא השתנה. אפשר לומר שאובמה החליף את "הבחירה הכוזבת" בין ביטחון לערכים בבחירה אחרת, אמיתית, בין שתי אפשרויות. באפשרות הראשונה (שהוא ייחס לממשל שקדם לו), מדיניות הביטחון הלאומי נעשית מבלי להיצמד לחוק וללא שקיפות, אך היא מוגבלת על ידי לגיטימציה מצומצמת מבית ומחוץ. באפשרות השנייה, זו שאובמה הציע, המדיניות מוגבלת על ידי פיקוח הדוק של החוק ועל ידי סטנדרטים גבוהים של שקיפות, אך נהנית מלגיטימציה רחבה. בשתי האפשרויות קיימת סכנה של שימוש מוגזם ולא מוסרי בכוח, ובשתיהן טמון פוטנציאל להגבלות מופרזות עליו. לכן תמיד יישמר תפקיד חשוב לביקורת ציבורית, שיפוטית ופרלמנטרית. עם זאת, אובמה ושאר הנואמים ניסו, ובמידה רבה הצליחו לשכנע שהאפשרות השנייה, האפשרות שלהם, היא הדרך היחידה שבה ניתן לשמור על ביטחון ועל ערכים מבלי להתפשר על אף אחד מהם.

## לקחים לישראל

למקבלי ההחלטות בישראל יש כמה סיבות טובות לחשוב היטב לפני שהם מאמצים אסטרטגיה משפטית־ציבורית זהה לזו שתוארה כאן. ישראל היא מדינה קטנה, האיומים על ביטחונה רבים וקרובים, מרחב הטעות שלה מצומצם והרגישות שלה לאובדן חיילים ולשבויים היא גבוהה. אין לה יכולת או יומרה "להנהיג את העולם החופשי" או לעמוד בראש קואליציות גדולות. היא חשופה הרבה יותר מארצות־הברית למהלכים מדיניים ומשפטיים במוסדות בינלאומיים, ובחלקם אין לה כיום סיבה לצפות ליחס הוגן. המשפט הבינלאומי נתפס על ידי רבים כאן כנשק שמופעל בצורה צינית ובלתי־הוגנת על ידי גורמים עוינים לישראל, במטרה להכפיש ולהחליש אותה. נוסף לכל אלה, המציאות המשפטית הסבוכה מעבר לקו הירוק ושאלות חוקתיות מהותיות שממתינות להכרעות פוליטיות עשויות לחסום גם שאיפה כנה להציג חזון משפטי שלם, קוהרנטי ומשכנע.

למרות כל זאת, כדאי לשים לב לכמה נקודות דמיון. כמו ממשל בוש בזמנו, גם ממשלת ישראל סובלת ממשבר לגיטימציה חריף שמגביל את יכולת התמרון המדינית והצבאית שלה. גם בישראל, הרוח הנושבת מהדרגים המדיניים והצבאיים היא שבסוג העימותים שבהם נתונה ישראל צריך לפעמים לבחור בין ביטחון לבין החוק (או לשנות את החוק). לישראל, בדומה לארצות־הברית, יש יסודות ערכיים שמהווים מצפן מוסרי. אלה נטועים עמוק בדת היהודית, בערכים האוניברסליים של ההשכלה ובתפקיד ההיסטורי ששמור לסיפור היהודי בהתפתחותם של המשפט הבינלאומי ושל המודעות לזכויות אדם אחרי מלחמת העולם השנייה.

את העמדות המשפטיות של ישראל במרבית הסוגיות הקשורות לביטחון ניתן למצוא מפוזרות כחלקי פאזל בתשובות לעתירות, בפסיקות של בג"ץ, בפרוטוקולים של עדויות בפני ועדות, בכתבות בתקשורת ובסיכומים של פאנלים אקדמיים. כאשר ממשלה ממנה ועדה לחיבור חוות דעת משפטית מקיפה יותר – כמו במקרים של הוועדות בראשות עו"ד טליה ששון, השופט בדימוס יעקב טירקל והשופט בדימוס אדמונד לוי – היא מעניקה לה מנדט צר, ולא תמיד מאמצת את מסקנותיה. עמימות משפטית נראית לא רק כברירה המועדפת משיקולים ביטחוניים ומדיניים, אלא גם ככורח פוליטי.

ההתייחסות למשפט הבינלאומי באמירות המושמעות על ידי גורמים במערכת הממשלתית ואף במערכת הביטחון נעה, לעיתים קרובות, בין זלזול לבין ראייתו כבעיה שאין ברירה אלא להתחשב בה.[27] פרופ' אייל בנבנישתי כתב לאחרונה[28] מעל במה זו על הסכנה בהתבטאויות כאלה:

> ...אמירות של דוברים שונים בצה"ל או המייעצים לצה"ל, המביעים זלזול במשפט הבין־לאומי, יכולות להשפיע על החלטות של בית הדין הבין־לאומי בעתיד...האמירות האלה עלולות לסכן את חופש הפעולה של צה"ל ולצמצם אותו בלחימה בעתיד. בשל אמירות כאלה עלול להיווצר רושם שישראל ממעיטה בחשיבותו של המשפט הבין־לאומי מתוך התפיסה שאינו רלוונטי ואינו מוסרי.

באותו פרסום תיארה גם אל"מ (מיל.) פנינה שרביט ברוך[29] כיצד היחס הפומבי למשפט הבינלאומי בזירה הציבורית מונע הפקת לגיטימציה מהמאמץ בזירה המשפטית:

> ...מקוממות האמירות, המושמעות על־ידי גורמים שונים במערכת הביטחון, חלקם בכירים, שלפיהן "הכללים [של המשפט הבינלאומי – י.א.] אינם מתאימים וצריך לגבש כללים חדשים". ראשית, לדעתי, הקביעה הזאת אינה נכונה. בנוסף, אמירות כאלה עלולות ליצור רושם שישראל אכן התעלמה מדיני הלחימה ולא החילה עליה את "הכללים הלא מתאימים". כך אנו מוצאים את עצמנו במצב שבו מצד אחד אנחנו פועלים לפי הכללים גם כאשר המשמעות היא הטלת מגבלות על עצמנו, ומצד אחר מואשמים בהתעלמות מהם, בין היתר על בסיס האמירות האלה.

אלה המלצות חשובות, ואם לשפוט על פי התנהלות הגורמים הרשמיים במהלך מבצע "עמוד ענן", נראה שהן הופנמו, לפחות באופן חלקי. בהחלטת הממשלה מיום תחילת המבצע נכתב במפורש כי "ישראל תפעל כמיטב היכולת כדי למנוע פגיעה באזרחים תוך כיבוד הצרכים ההומניטריים של האוכלוסייה, והכול בהתאם לכללי המשפט הבינלאומי". כמו כן, הופיעו מספר דיווחים בתקשורת על התפקיד המרכזי שמילא היועץ המשפטי לממשלה באישור פעולות הצבא. שר המשפטים, יעקב נאמן, אמר בראיון לגלי צה"ל: "מדינת ישראל מקפידה לפעול כחוק... צה"ל עושה את כל מה שדרוש כדי לשמור על כל כללי המשפט הבינלאומי. למרות שהצד השני מפר את כל הכללים, פוגע באזרחים, אנחנו נשמור על כל כללי המשפט הבינלאומי".[30]

כל אלה משקפים תהליך מבורך של הפקת לקחים מהעימותים הצבאיים של השנים האחרונות. עם זאת, במרבית הדוגמאות הללו, עדיין מדובר בגישה שנשארת מוגבלת לאמירות כלליות ולמזעור נזקים. תועלת רבה יותר עשויה לצמוח מגיבוש העמדות המשפטיות לכדי חזון שניתן להציג לפני הציבור, ולהסביר כיצד הוא מספק מענה לאתגריה הביטחוניים של ישראל במסגרת מחויבות בלתי־מתפשרת לחוק הישראלי והבינלאומי.

תארו לעצמכם מציאות שבה הטיעון המשפטי שמצדיק פעולה או מדיניות בעלת אופי ביטחוני מוסבר במלואו לציבור לפני הצגתו בבית המשפט; קודם שמוגשת העתירה ולא בתשובה אליה; על ידי גורם משפטי בכיר ולא פרקליט אנונימי; ישירות לאזרחי ישראל ולא בפני ועדות כאלה או אחרות; בשפה פשוטה ולא פתלתלה; וכחלק ממסגרת משפטית רחבה וסדורה ולא כמענה לאתגר נקודתי. תארו לעצמכם את הפרקליט הצבאי הראשי מתאר בנאום פומבי את תהליך קבלת ההחלטות לפני אישור תקיפה מן האוויר או הצבת מחסום, או את היועץ המשפטי לשב"כ מסביר לסטודנטים למשפטים מהם הקריטריונים לאישור מעצר מנהלי, ומהו מנגנון הפיקוח על ההחלטות האלה. דמיינו סרטון ביו־טיוב של נאום היועץ המשפטי של משרד החוץ על המסגרת המשפטית שבתוכה נקבעת מדיניות ישראל בגדה המערבית וכלפי רצועת עזה. תארו לכם את מסיבת העיתונאים שבה מודיע שר הביטחון על החלטתו לקבוע נקודת איזון חדשה בין הצורך להסתיר מידע מבצעי מהאויב לבין הצורך לחשוף לעיני הציבור עד כמה שניתן את הסטנדרטים שלפיהם פועלים בשמו ולמען ביטחונו. ולסיום, תארו לכם שאת כל המהלך המשפטי־ציבורי מוביל ומתאם משרד ראש הממשלה. האם יוזמה כזאת תפגע בביטחונה של ישראל או תחזק אותו?

אין ספק ששינוי כזה דורש מנהיגות ומאמץ משותף של משרדי ממשלה שונים. אולי אין זה מקרה שהקמפיין שתואר כאן הובל על ידי ממשל אמריקאי שבו הנשיא הוא פרופסור למשפט חוקתי,[31] והוא מוקף במשפטנים. בכהונתו הראשונה היו

יועץ הנשיא לביטחון לאומי, סגן הנשיא, היועץ לביטחון לאומי של סגן הנשיא, מזכירת המדינה, שר הביטחון והשר לביטחון המולדת – כולם עורכי דין בהכשרתם.

עם זאת, אם בסיוע מלמעלה או בלעדיו, הכוח לקדם מסגור מחדש של הוויכוח הציבורי נמצא בידיהם של כל מי שנוטלים בו חלק. בידי אנשי צבא ומומחים לביטחון הכוח לבסס את המודעות לכך שציות לחוקים ושמירה על הערכים הם נכסים אסטרטגיים מהמעלה הראשונה. הם יכולים גם לתרום לעיצוב נורמות משופרות של שקיפות במערכות הביטחוניות. ליועצים משפטיים הכוח לדחוף לפרסום הטיעונים המשפטיים של המדינה באופן יזום, מסודר ונגיש, גם, או בעיקר כלפי נושאים השנויים במחלוקת. לארגוני זכויות אדם הכוח להוכיח שמחויבות בלתי־מתפשרת לחוק ולערכים יכולה ללכת יד ביד עם התייחסות רצינית לדאגות ביטחוניות ולמורכבויות המבצעיות והאתיות של עימותים אסימטריים. למכוני מחקר ולמוסדות אקדמיים הכוח לחזק את הזיקה בין מחקרי ביטחון לאומי למחקר בנושאי משפט וזכויות אדם. עבור רוב מכריע מקרב כל אלה מדובר במתן ביטוי לאמת שבה הוא כבר מאמין: בטווח הארוך, אי־אפשר לשמור על ביטחון ללא ערכים, ואי־אפשר לשמור על ערכים ללא ביטחון.

## הערות

1 Barack Obama, "Remarks by the President on National Security", National Archive, Washington D.C., May 21, 2009. http://www.whitehouse.gov/the-press-office/remarks-president-national-security-5-21-09

2 The President and the Press: Address before the American Newspaper Publishers Association, April 27, 1961.

3 Daniel Klaidman, *Kill or Capture: The War on Terror and the Soul of the Obama Administration*, (Boston and New York : Houghton Mifflin Harcourt, 2012).

4 Harold H. Koh, "The Obama Administration and International Law", Annual Meeting of the American Society of International Law, Washington D.C., March 25, 2010. http://www.state.gov/s/l/releases/remarks/139119.htm

5 David Kris, "Law Enforcement as a Counterterrorism Tool", Brookings Institution, Washington D.C., June 11, 2010. http://www.brookings.edu/events/2010/06/11-law-enforcement

6 John O. Brennan, "Strengthening our Security by Adhering to our Values and Laws", Harvard Law School, Cambridge, Massachusetts, September 16, 2011. http://www.whitehouse.gov/the-press-office/2011/09/16/remarks-john-o-brennan-strengthening-our-security-adhering-our-values-an

7 Jeh C. Johnson, "Is More Detainee Legislation Needed?", The Heritage Foundation, Washington D.C., October 18, 2011. http://www.heritage.org/events/2011/10/jeh-johnson

8 Jeh C. Johnson, "National Security Law, Lawyers and Lawyering in the Obama Administration", Yale Law School, New Haven, Connecticut, February 22, 2012. http://www.cfr.org/national-security-and-defense/jeh-johnsons-speech-national-security-law-lawyers-lawyering-obama-administration/p27448

9 Eric Holder, "Attorney General Eric Holder Speaks at Northwestern University School of Law", Northwestern University, Chicago, March 5, 2012. http://www.justice.gov/iso/opa/ag/speeches/2012/ag-speech-1203051.html

10 הביטוי לקוח ממאמרו של ג'ון בלינג'ר:
John B. Bellinger, "More on the Obama Administration's National Security Speeches", *Lawfare Blog*, April 20, 2012.

11 Stephen Preston, "CIA and the Rule of Law", Harvard Law School, Cambridge, Massachusetts, April 10, 2012. http://www.cfr.org/rule-of-law/cia-general-counsel-stephen-prestons-remarks-rule-law-april-2012/p27912

12 John O. Brennan, "The Ethics and Efficacy of the President's Counterterrorism Strategy", Woodrow Wilson International Center for Scholars, Washington, D.C., April 30, 2012. http://www.wilsoncenter.org/event/the-efficacy-and-ethics-us-counterterrorism-strategy

13 זה הכינוי שהוענק להם בבלוג המשפטי Lawfare. ראו למשל:
Kenneth Anderson, "What should the Administration Say? The Canonical National Security Law Speeches of the Obama Administration Senior Officials and General Counsels", *Lawfare Blog*, April 19, 2012.

14 ראו הערה 10.

15 Harold H. Koh, "International Law in Cyberspace", U.S. Cyber Command Inter-Agency Legal Conference, Fort Meade, Maryland, September 18, 2012. http://www.state.gov/s/l/releases/remarks/197924.htm

16 Jeh C. Johnson, "The Conflict Against Al Qaeda and its Affiliates: How Will It End?", Oxford University, November 30, 2012. http://www.lawfareblog.com/2012/11/jeh-johnson-speech-at-the-oxford-union

17 Jack Goldsmith, "Obama's weak spots on counterterrorism are open to Romney", *The Washington Post*, April 27, 2012.

18 ר' הערה 10.

19 Robert Chesney, "Beyond the Battlefield, Beyond Al Qaeda: The Destabilizing Legal Architecture of Counterterrorism", *Michigan Law Review* (Forthcoming), Downloaded from SSRN, September 2012.

20 Ritika Singh and Benjamin Wittes, "Two Parties, One Policy: Washington's new Consensus on Terrorism", *Commonweal Magazine*, September 14, 2012.

21 John B. Bellinger, "More Continuity Than Change", *The New York Times*, February 14, 2010.

22 David Ignatius, "The bin Laden plot to kill President Obama", *The Washington Post*, March 16, 2012.

23 ראו לדוגמה בנוגע להריגות הממוקדות מהאוויר:
Micah Zenco, "The Seven Deadly Sins of John Brennan: What Obama's high priest of targeted killings doesn't want you to know", *Foreign Policy*, September 18, 2012.
Anthony Romero, Executive Director of American Civil Liberties Union, "When the President Orders a Killing", Letters to the Editor, *The New York Times*, May 31, 2012.

24 John B. Bellinger, "Will drone strikes become Obama's Guantanamo?", *The Washington Post*, October 3, 2011.

25 Glenn Greenwald, "The 'war on terror' – by design – can never end", *The Guardian*,

January 4, 2013.

26 Trevor Morrison, "Obama v. Bush on Counterterrorism Policy", *Lawfare Blog*, November 11, 2012.

27 כדוגמה חיובית להתייחסות למשפט בדרגים המקצועיים, ראוי לציין את הדברים שאמר תת־אלוף (מיל.) אביחי מנדלבליט כשהיה הפרקליט הצבאי, בראיון לעמוס הראל שפורסם ב"**הארץ**" ב־18 בספטמבר 2009. בין השאר הוא אמר: "...אבל הכלל היה ברור בכל הדרגים ובכל הרמות: אנחנו פועלים לפי עקרונות המשפט הבינלאומי לאורך כל הדרך"; "מלחמה א־סימטרית אינה כזאת רק במובן שלצד אחד יש פחות נשק ולשני יותר, אלא שהאחד (חמאס) רואה עצמו משוחרר מכללי המשפט הבינלאומי והשני (ישראל) כבול אליהם"; "מטרתנו היא לנצח במלחמה, אבל בהתאם למגבלות החוק. זה עניין מקצועי, חלק מהמקצוע הצבאי"; "ההנחיה לצבא היא לפעול לפי דיני העימות המזוין, המבחן קשור לפרופורציונליות וגם להבחנה בין לוחמים לאזרחים. צריך שהיתרון הצבאי שאתה מפיק מכל תקיפה יעלה על הנזק האגבי שעלול להיגרם. כך ירדו ההנחיות לשטח".

28 אייל בנבנישתי, "השפעת אתגרי הלחימה על דיני הלחימה", **צבא ואסטרטגיה**, כרך 4, גיליון 1, מאי 2012, עמ' 31–35.

29 פנינה שרביט ברוך, "דילמות משפטיות בלחימה בעימותים אסימטריים", **צבא ואסטרטגיה**, כרך 4, גיליון 1, מאי 2012, עמ' 37–45.

30 צה"ל שב וקורא לתושבי עזה להתרחק מאזורי פעילות של חמאס, טל לב־רם, גלי צה"ל, 20 בנובמבר 2012.

31 על הקשר בין הרקע האקדמי של אובמה והמדיניות שלו בנושאי ביטחון, ראו: David Luban, "What Would Augustine Do? The President, Drones, and Just War Theory", *Boston Review*, June 6, 2012.

# השפעת התפתחות טכנולוגיית הלוחמה הקיברנטית על שינויים בבניין הכוח בישראל

**גיל ברעם**

בעשור האחרון חלו ההתפתחויות מהירות בתחומי המחשוב וטכנולוגיות המידע, שהובילו לשינויים מרחיקי לכת כמעט בכל תחומי החיים, ביניהם גם בתחום הצבאי־ביטחוני. בתחום זה התרחשו שינויים רבים במאפייני הלחימה ובבניין הכוח של צבאות, בין היתר בשל התפתחויות שחלו בדפוסי המחשבה האסטרטגית ובגיבוש הדוקטרינות הצבאיות שהותאמו למציאות המשתנה. ניסיונות שנעשו לבחון את השלכות המעבר לעידן המידע על העיסוק הביטחוני הובילו בשנות התשעים של המאה ה־20 להתפתחותו של רעיון "המהפכה בעניינים צבאיים". הרעיון נולד בעקבות ההמצאות הטכנולוגיות החדישות, שהובילו לעליית מדרגה בזמינות המודיעין ובאיכותו, בקצב זרימת המידע וביכולות הדיוק של כלי הנשק. בשנים הבאות, ובייחוד עם הכניסה למאה ה־21, התפתחו טכנולוגיות מתקדמות בתחום הלוחמה הקיברנטית, שהובילו לשינוי איכותי במאפייני שדה הקרב ובדפוסי פעילותם של הצבאות המודרניים.

הטכנולוגיה הקיברנטית המשמשת לצורכי לחימה משפיעה על דפוסי הלחימה כך שמדינה המחזיקה בה נהנית מעליונות בשדה הקרב, ממודיעין איכותי ומקיף, מיכולת תקיפה מדויקת ומהירה, מיכולות הגנה על תשתיות קריטיות, מיכולות שליטה ובקרה גבוהות ועוד. יכולות אלה תורמות לעוצמתה של המדינה ומחזקות את ביטחונה הלאומי. טכנולוגיית הלוחמה הקיברנטית טומנת בחובה פוטנציאל ליתרונות עצומים, לצד סיכונים חדשים ובלתי־מוכרים. לאור חדשנותו הרבה של תחום זה, הבנת טיבו והשלכותיו עודם מצויים בראשית הדרך.

בשנים האחרונות הגבירו מדינות רבות, ובראשן ארצות־הברית וישראל, את קצב פעילותן בזירה הקיברנטית. פעילות זו מהווה עבורן מקור עוצמה, אך

גיל ברעם היא תלמידה לתואר שני בתוכנית ללימודי ביטחון באוניברסיטת תל אביב, עמיתת מחקר בסדנת יובל נאמן למדע טכנולוגיה וביטחון.

גם חושפת את "הבטן הרכה". זאת משום שהתשתיות החיוניות לתפקודה של כל מדינה הפכו תלויות במחשבים. אופן ההתמודדות הרצוי עם האיום הנשקף כתוצאה מהתפתחות טכנולוגיית הלוחמה הקיברנטית הוא תחום עיסוק מרכזי שעמו מתמודדת מדינת ישראל בשנים האחרונות.[1]

האינטרס הלאומי של ישראל מתרכז בשמירה על ביטחונה מפני אלה המעוניינים לפגוע בה ומערערים על עצם קיומה. אינטרס זה, וכן מיקומה הגיאו־פוליטי של ישראל, מחייבים אותה ליצור עליונות בתחום הקיברנטי כחלק בלתי־נפרד מיכולתה להגן על עצמה מפני פגיעות קונוונציונליות וקיברנטיות, וכיכולת התקפית הרתעתית בזירת המזרח התיכון ומעבר לו.

ישראל נחשבת למובילה בעולם מבחינת יכולת התמודדותה עם תקיפות קיברנטיות: בדו"ח מקיף שבחן את מידת מוכנותן של 23 מדינות בתחום הקיברנטי קיבלה ישראל את הציון הגבוה ביותר – ארבעה כוכבים וחצי מתוך חמישה. מהדו"ח עלה כי ישראל נתונה בכל דקה תחת כאלף מתקפות קיברנטיות. נתון זה הרשים במיוחד את מחברי הדו"ח, ששיבחו את מערכות ההגנה הישראליות וציינו שישראל ערוכה היטב להתמודדות עם מתקפה קיברנטית נגדה.[2]

פיתוח יכולות הפעולה של ישראל בזירת הלוחמה הקיברנטית הוא מרכיב מרכזי בשמירה על חוסנה הלאומי. הכלכלה, התעשייה, הביטחון, החינוך והשמירה על קיומה כחברה דמוקרטית, פתוחה ומבוססת ידע תלויים, ברובם, ביכולתה להגן על רשתות המחשבים החיוניות שלה מפני פגיעה שעלולה להוביל לשיבוש אורח החיים התקין במדינה. ההישענות הגוברת על מערכות מחשב בארץ ובעולם הביאה עמה אתגרים חדשים, המצריכים מענה מיידי ברמה הלאומית.[3]

מטרת המאמר היא להציג את מקומה של טכנולוגיית הלוחמה הקיברנטית בתפיסת הביטחון הישראלית, ולבחון את ההיערכות שבוצעה בישראל במטרה להתמודד עם האיום הקיברנטי באמצעות בחינת שלושה תחומים מרכזיים: גיבוש אסטרטגיה סדורה להתמודדות עם האיום הנשקף כתוצאה מהתפתחות טכנולוגיית הלוחמה הקיברנטית; הקצאת משאבים ותקציבים; יצירת שינויים בבניין הכוח. ההנחה היא כי באמצעות בחינת הפרסומים הממשלתיים אפשר יהיה ללמוד על מידת חשיבות הנושא עבור מקבלי ההחלטות, ומכאן על המשאבים המוקצים להתמודדות איתו. כל זאת, מתוך כוונה להציג את המצב בישראל ולנסות להצביע על הפערים הקיימים בתחום.

המאמר מתבסס על ספרות עדכנית בנושא ועל מידע פומבי בלתי־מסווג הכולל קטעי עיתונות, הצהרות לתקשורת, מסמכי ממשל וראיונות עם אישים מרכזיים בתחום. יש לציין כי בישראל קטן מספרם של הפרסומים הרשמיים על אודות דרכי ההתמודדות עם האיום הקיברנטי, ובפרט ביחס ליכולותיה ההתקפיות בתחום.

על כן, סביר להניח שלאור אופייה הביטחוני של ישראל, מידע רב על פעולות המבוצעות בנושא ותקציבים המוקצים לתחום נותר חסוי.

ביצוע המחקר לווה במספר קשיים: כיוון שמדובר בתחום מחקר חדש יחסית, עדיין לא קיים מספיק ידע היסטורי בנושא השפעתה של התפתחות טכנולוגיית הלוחמה הקיברנטית על יצירת שינויים באסטרטגיות הקיימות ועל בניין הכוח. עם זאת, כיוון שמדובר בתחום בעל חשיבות רבה רצוי להתחיל להתעמק בו חרף פערי הידע הקיימים.

חשוב לציין כי המחקר מתמקד בתחום הלוחמה הקיברנטית, המורכב מהיערכותה של המדינה בתחומי ההגנה וההתקפה, ואינו עוסק בתחום השימוש במחשבים לצרכי תקשורת או ניהול לחימה. משום שהמחשבים משמשים כיום לביצוע פעולות רבות בתחומי התקשורת והלחימה, מדובר בתחום נרחב מאוד, החורג מהיקפו של מאמר זה.

## מקומה של טכנולוגיית הלוחמה הקיברנטית בתפיסת הביטחון הישראלית

השינויים הרבים שחלו בתחום טכנולוגיות הלוחמה הקיברנטיות מאתגרים את התפיסות הביטחוניות הקיימות, ומחייבים בחינה מחודשת של מושגי היסוד. נוצר מצב שבו יש חשיבות ראשונה במעלה להגנה על התשתיות החיוניות של המדינה בתחומי האנרגיה, המים, המחשוב, התקשורת, התחבורה והכלכלה – הן במגזר האזרחי והן במגזר הביטחוני. על כן, יש לערוך את ההתאמות הנדרשות בתפיסת הביטחון על מנת שתוכל לספק מענה לאיומים החדשים.[4]

באפריל 2006 הוגשה לשר הביטחון דאז, עמיר פרץ, הצעה לתפיסת ביטחון מעודכנת. ההצעה הוכנה על ידי ועדה בראשות דן מרידור, שבין חבריה היו ראש המועצה לביטחון לאומי, ראש השב"כ, הממונה על הביטחון במערכת הביטחון ונוספים. מדו"ח הוועדה עלה שישראל נמצאת בעידן של שינויים אסטרטגיים גדולים ומהירים, ביניהם שינויים טכנולוגיים מרחיקי לכת.[5] בין היתר, המליצה הוועדה להוסיף את ההגנה כרכיב נוסף לשלושת הרכיבים המסורתיים (הרתעה, התרעה והכרעה),[6] ובפרט המליצה על הצטיידות בכלי־טיס בלתי־מאוישים ועל יצירת הגנה על מערכות המחשב הלאומיות מפני חדירת גורמים עוינים.[7]

בעקבות דיוני הוועדה עלתה האפשרות לצרף מונח יסוד רביעי ל"משולש הביטחון", והוא "התגוננות" או "הגנה".[8] ישראל אכן השקיעה חלק ניכר מתקציבה וממאמצי הביטחון שלה בהתגוננות פסיבית. רעיון ה"הגנה" הורחב, ונכללו בו, נוסף לכלי ההתגוננות הפסיביים, גם כלים התקפיים נקודתיים שמטרתם לסכל ירי תלול־מסלול או פיגועי טרור שמתחת לרף ההסלמה הרחבה.[9]

בתחום הלוחמה הקיברנטית קיימת חשיבות עליונה להגנה, כיוון שבאמצעות הגנה יעילה אפשר לוודא שמערכותיה החיוניות של המדינה ימשיכו לתפקד. נוסף על כך, יכולות קיברנטיות מתקדמות מאפשרות למדינה הגנה יעילה על התשתיות הקריטיות שלה וכך מספקות מענה לצורך בהגנה אקטיבית, כפי שהוצג בדו"ח ועדת מרידור.

במשך זמן רב נהוג היה לכנות את תחום ההגנה על מערכות ממוחשבות "אבטחת מידע", לפי התפיסה שהדבר המרכזי שעליו יש להגן הוא מידע רגיש (מידע מסווג או עסקי). עם השנים התפתחה גישה זו והקיפה איומים נוספים מלבד פגיעה במידע – מניעת שירות, השבתת תהליכים חיוניים מבוססי מחשב ועוד. ברמה הלאומית התרחב מושג ההגנה על מערכות ממוחשבות, ואפשר לכנותו "הגנה קיברנטית".[10] מאז פרסום הדו"ח חלה עלייה ניכרת בשימוש בטכנולוגיה קיברנטית לצורכי לחימה שונים בשדה הקרב. על כן, ראוי לבחון את מקומה של טכנולוגיית הלוחמה הקיברנטית בתהליכי עדכון תפיסת הביטחון של ישראל.

במבט היסטורי על מלחמות ישראל אפשר לראות שחשיבות הטכנולוגיה עלתה ממלחמה למלחמה, והשתכללה עם השנים. בין ישראל לבין מדינות ערב קיימים הבדלים בסיסיים, וכן קיימת א־סימטריה כמותית ברורה. אם שוקלים את הפערים הכמותיים הגדולים, בולט יתרונה היחסי של ישראל בהסטת המלחמה למישור הטכנולוגי: לישראל קל יותר להתמודד עם העולם הערבי בקרבות אוויר מתוחכמים או בביצוע פעולות קיברנטיות (על פי פרסומים זרים) מאשר בזריקת אבנים או בהתמודדות של חייל מול חייל. ככל ששדה הקרב רווי בטכנולוגיות מתקדמות, הולכים ומצטמצמים הפערים הכמותיים, וגדל ערכן של איכויות מערכות הנשק ושל כוח האדם. בצה"ל היטיבו לזהות את הפוטנציאל הרב הטמון במחשבים, וכבר משנות התשעים החל השימוש בלוחמת מחשבים (computer warfare) על סוגיה השונים.[11]

ההתמודדות עם האיום הנשקף כתוצאה מהתפתחות טכנולוגיית הלחימה הקיברנטית הולמת את תפיסת הביטחון הישראלית: מדובר בתחום המופעל ביכולות "כחול־לבן", שמסתמך על כושר הפיתוח וההמצאה "היהודי", בשילוב טכנולוגיות עולמיות. התחום מוכר היטב לישראלים הצעירים במדינה, שהוגדרה לאחרונה כ"מדינת סטארט־אפ"[12] ומתבסס על העיקרון של חשיבות האיכות על פני הכמות.

אפשר לראות ש"שלוש הרגליים" המקוריות של תפיסת הביטחון הישראלית המסורתית רלוונטיות עבור ההתמודדות עם האיום הקיברנטי:

1. הרתעה – יכולות קיברנטיות מתקדמות יאפשרו לישראל ליצור הרתעה מול אויביה. כדוגמה אפשר לראות את אירוע וירוס "סטקסנט" המיוחס לארצות־הברית ולישראל, שנתפס כעליית מדרגה בכל הנוגע ליכולות התקיפה

הקיברנטיות של מדינות ולעוצמת השפעתן, זכה לתהודה רחבת־היקף בתקשורת העולמית ותרם לחיזוק ההרתעה הישראלית.[13]

2. התרעה – היכולות הקיברנטיות מאפשרות לישראל לאסוף מידע רב על אויביה ובמקביל, למנוע מהם גישה למאגרי המידע שלה. כך תוכל המדינה להתריע באופן יעיל על כוונותיהם נגדה.
3. הכרעה – ישראל היא מהמדינות המובילות בעולם מבחינת יכולותיה הקיברנטיות. יכולות אלה מאפשרות לה להשיג יתרון בקרב, באמצעות שימוש בכלים קיברנטיים מתקדמים, ולהכריעו לטובתה. חשוב לציין כי מושג ההכרעה בתחום הקיברנטי, כמו למושג ההרתעה, הם מושגים חמקמקים שמשמעותם בהקשר הקיברנטי טרם מוצתה עד תום. עם זאת, כיום ברור כי עליונות קיברנטית בשילוב עם יכולות קינטיות מתקדמות עשויה להוביל להכרעת קרבות.

מקום המדינה ועד היום מושתתת תפיסת הביטחון על עקרון חשיבות האיכות על פני הכמות. טכנולוגיית הלחימה הקיברנטית עונה על עיקרון זה: באמצעות כלים קיברנטיים, שאינם דורשים הפעלת כוח פיזי רב אלא הכשרת כוח אדם מיומן, מתאפשרות פעולות המסייעות להגברת יכולת ההרתעה של ישראל ומקנות לה יוקרה רבה בזירה הבינלאומית.

לסיכום, נראה שאפשר לשלב את יכולות הלחימה הקיברנטית בתפיסת הביטחון הישראלית באופן פשוט יחסית, אם אכן זו תעודכן בקרוב. זאת משום שיכולות אלה עונות על שלושת העקרונות הבסיסיים שעליהם בנויה תפיסת הביטחון. כמו כן, פיתוח יכולות לחימה קיברנטיות עצמאיות וכלי לוחמה קיברנטיים מממשים בבירור את עקרון האיכות על פני הכמות: כל שנדרש הוא כוח אדם מיומן ברמה גבוהה לפיתוח מערכות המאפשרות ביצוע פעולות ביעדים רחוקים, מבלי לסכן חיי אדם ומבלי להזדקק למשאבים רבים.

## גיבוש אסטרטגיה סדורה לתחום הקיברנטי

האיום הקיברנטי הוא פועל יוצא של תפקידן הקריטי של מערכות המחשב בתשתיות הלאומיות ובחיי היום־יום. מרחב וירטואלי זה נוצר מהתפתחות מבוזרת של מערכות ומגזרים שונים, כחלק מהתפתחות כלכלית וטכנולוגית מואצת, ללא הקשרים ביטחוניים מובהקים. כשעלה בשנים האחרונות הצורך לעסוק בהיבטים הביטחוניים של התחום הקיברנטי, נשאלה השאלה – מיהו "בעל הבית" והאחראי לביטחון בו?[14]

אבטחת מידע והגנה על תשתיות ממוחשבות אינם נושאים חדשים בישראל. ישראל הייתה מהמדינות הראשונות בעולם שהכירו בחשיבות ההגנה על מערכות ממוחשבות חיוניות. כבר בשנת 1996 קיבלה הממשלה החלטות באשר לדרך

ההתגוננות הרצויה מפני איומים קיברנטיים.[15] בשנת 1997 הוקם פרויקט תהיל"ה (תשתית הממשלה לעידן האינטרנט), שמטרתו להגן על חיבור משרדי הממשלה לאינטרנט ולספק שירותי גלישה מאובטחים למשרדי הממשלה.[16] בהמשך, בשנת 1998 חוקק "החוק להסדרת הביטחון בגופים ציבוריים", שעסק בהגדרת מערכות ממוחשבות חיוניות ובאבטחתן.[17]

## ההחלטה על הקמת הרשות הממלכתית לאבטחת מידע

בישראל אין פרסום מוסדר של המדיניות הציבורית בתחום ההתמודדות עם האיום הקיברנטי, ומרבית המידע הקיים נסמך על פרסומים בתקשורת ומחקרים אקדמיים. עם זאת, מספר החלטות רשמיות שפורסמו שופכות אור על המצב: בפברואר 2002 התקבלה בוועדת השרים לענייני ביטחון לאומי ההחלטה בנושא "אחריות להגנה על מערכות ממוחשבות במדינת ישראל" (החלטה ב/84), שעיצבה את מתווה ההגנה על התשתיות הממוחשבות הקריטיות במדינה. ההחלטה משמשת בסיס להפעלת המענה הישראלי לאיום הקיברנטי על תשתיות מחשב לאומיות חיוניות. בהחלטה נקבעה הקמתם של שני גופים ייעודיים: האחד – ועדת היגוי עליונה שתבחן באופן שוטף את זהות הגופים הציבוריים והפרטיים החיוניים לתפקודה של מדינת ישראל; השני – יחידה ממלכתית להגנה על המערכות הממוחשבות.

ואכן, בהמשך להחלטת ועדת השרים הוקמה כבר באותה שנה ועדת היגוי בראשות ראש המועצה לביטחון לאומי, שמטרתה הייתה לגבש מכלול צעדים להגנה על מערכות המחשב החיוניות של המדינה. בוועדה נקבעו עקרונות תפיסת ההגנה, איומי הייחוס והגופים שיחויבו בצעדי הגנה.[18] כמו כן, היא פעלה כצוות היגוי המנחה את היחידה הממלכתית לאבטחת תשתיות ממוחשבות בשירות הביטחון הכללי (שב"כ).

באותה השנה הוקמה "הרשות הממלכתית לאבטחת מידע", הפועלת במסגרת חוק השב"כ. הרשות מנחה את הגופים שהוגדרו כחיוניים בנושאי ביטחון המחשוב והגנה על הרשתות, ומפקחת על ביצוע הנחיות אבטחת המידע והגנתו. כמו כן, היא מוסמכת לנקוט סנקציות נגד גופים המפרים את הנחיותיה. יש לציין כי גופי הביטחון השונים פועלים להגנה על תשתיותיהם הקריטיות באופן עצמאי, ללא הנחיה רשמית של הרשות לאבטחת מידע.[19]

## ההחלטה על הקמת המטה הקיברנטי הלאומי

בנובמבר 2010 הטיל ראש הממשלה על יושב ראש המועצה הלאומית למחקר ולפיתוח, אלוף במיל' פרופסור יצחק בן ישראל, להציג תוכנית עבודה למיזם לאומי להתמודדות עם האיום הקיברנטי.[20] בין המלצותיו של צוות המיזם היו: המלצה 1 א' – הקמת מטה קיברנטי לאומי להגנה, שייעודו קידום הגנת המרחב

הקיברנטי בישראל. המלצה 1 ב' – הרחבת סמכויות שב"כ כגוף הביצוע לטיפול במרחב האזרחי.[21]

המסמך המרכזי בנושא הוא החלטת הממשלה מיום ה־7 באוגוסט 2011 בנושא "קידום היכולת הלאומית במרחב הקיברנטי".[22] החלטה זו היא תולדה של פעילות צוות המיזם. בהחלטה נקבעה הקמת המטה הקיברנטי הלאומי, ונקבע כי מטרתו היא "קידום היכולת הלאומית במרחב הקיברנטי ושיפור ההתמודדות עם האתגרים הנוכחיים והעתידיים במרחב הקיברנטי". אחד מתפקידיו של ראש המטה הוא "להמליץ לראש הממשלה ולממשלה על מדיניות קיברנטית לאומית, להנחות את הגורמים הרלבנטיים אודות המדיניות עליה הוחלט... ליישם את המדיניות ולבקר את יישומה".[23] ההחלטה על הקמת המטה, שפורסמה בפומבי, הייתה התקדמות משמעותית באופן טיפולה של הממשלה בנושא האיום הקיברנטי, והיוותה נקודת מפנה בתחום.

בעוד גופי הממשל, זרועות הצבא וגופי מערכת הביטחון מוגנים על פי חוק, מרבית המגזר העסקי והאזרחים מהשורה נותרו ללא הגנה מספקת בתחום. המגזר העסקי אינו נתון לפיקוח רשמי ואינו כפוף לגוף לאומי כלשהו, האחראי לבדוק את יכולות ההתמודדות עם פגיעה במערכות המחשב החיוניות שלו בשעת חירום. זוהי נקודת תורפה משמעותית של ישראל, שכלכלתה תלויה בכושר הייצור והייצוא של המגזר העסקי והתעשייתי.[24]

מקבלי ההחלטות בישראל צופים שבמלחמה הבאה ייעשה שימוש באמצעי לוחמה קיברנטיים, ואף על פי כן, אין כיום גוף רשמי בישראל שאחראי ישירות על הגנת המגזר העסקי. נכון הוא שרשות לאומית אינה יכולה להחליף את המנהלים האחראיים על עסקיהם, אך מאחר שחלק מהארגונים הפרטיים במשק מספקים שירותים החיוניים להמשך החיים התקינים בעורף, יש מקום להתערבות ממשלתית בהנחיות, בתקנות ובבקרה.[25]

עם הקמת המטה הקיברנטי הלאומי אמר ד"ר אביתר מתניה, ראש המטה, כי לתפיסתו קיימים חמישה היבטים שבהם על המדינה להתערב בהקשר הקיברנטי:

1. יצירת נקודת מבט כלל־מערכתית ברמה הלאומית: ההגנה הקיברנטית מחייבת בחינה רב־מערכתית, מאחר שקיימת תלות הדוקה בין המערכות הציבוריות למערכות הפרטיות והעסקיות.
2. "איגום" משאבים, פעולות ומידע: משמעות האיגום היא איחוד משאבים ממקורות שונים לגוף מתַכלל אחד, במטרה להתמודד בצורה טובה יותר עם האיומים הנשקפים לישראל.
3. יצירת שיתוף פעולה בינלאומי: על ישראל להוביל את נושא שיתוף הפעולה באופן יזום, וליצור שיתופי פעולה עם בעלות־ברית ברחבי העולם.

4. יצירת הסדרה לתחום הקיברנטי: ביצוע הסדרה תקינה, רישוי והסמכה, וכינון שיטה שבה ארגונים ופרטים יהיו מסוגלים להגן על עצמם על פי סטנדרטים מוגדרים וברורים.[26]
5. קידום תהליכים על ידי המדינה: כפי שפעלה המדינה בשנות השישים לקידום תחום התעופה בארץ, באמצעות הקמת הפקולטה לאווירונאוטיקה בטכניון, כך היא צריכה לספק כלים ומנופים על מנת לתמרץ פיתוחים אקדמיים ותעשייתיים בתחום הקיברנטי.[27]

לדברי מתניה, מטרת המטה הקיברנטי הלאומי היא תכנון כלל העשייה בתחום ההגנה הקיברנטית: חיזוק האבטחה בארגונים באמצעות יצירת הסדרה חוצת ענפים המותאמת למאגרי המידע, וכן הסדרה ענפית לכל תחום ותחום. נדבך נוסף הוא בניית תוכניות לאומיות, שיתוף פעולה ושיתוף המידע, במיוחד בקשר שבין המערכת הביטחונית והמערכת האזרחית.[28]

מהות פעילות המטה נוגעת להסדרה, לתִכלול ולקידום הפעילות הכלל־ממשלתית בתחום הקיברנטי בראייה רחבה, אזרחית וביטחונית כאחד. המטה פועל ברוח החלטת הממשלה, יחד עם הגופים הרלוונטיים, לגיבוש מדיניות הגנה ובניית תפיסת הגנה לאומית, וליצירת שיתופי פעולה בין כלל הגופים הפועלים בתחום. זאת לצד גיבוש תוכניות כוללות ובניית מנגנונים לטיפוח ההון האנושי בתחום הקיברנטי; פיתוח תשתיות טכנולוגיות ומחקריות באקדמיה ובתעשייה; קידום שיתופי פעולה בין המגזר הפרטי־עסקי, המגזר הממשלתי, התעשייה, האקדמיה ומערכת הביטחון; קידום המודעות הציבורית לאיום הקיברנטי ועוד.[29]

מהאמור לעיל אפשר לראות שישראל היטיבה לזהות את האיום הנשקף לתשתיותיה הלאומיות, ופעלה להקמת מערך הגנה ברמה הלאומית. שתי נקודות ציון מרכזיות הן: הקמת הרשות הממלכתית לאבטחת מידע (רא"מ) בשנת 2002; החלטת הממשלה מאוגוסט 2011 על "קידום היכולת הלאומית במרחב הקיברנטי" והקמת המטה הקיברנטי הלאומי. עם זאת, הממשל הישראלי טרם הפיץ לציבור אסטרטגיה מוסדרת ואחידה בנושא.

ישראל היא מהמדינות המובילות בעולם ביכולותיה הקיברנטיות, אולם, כנהוג בישראל, אין לכך ביטוי הולם בכל הנוגע לקביעת אסטרטגיה סדורה ולפרסום ברור של דרך הפעולה הרשמית בתחום. נראה כי בישראל טרם גובשה אסטרטגיה בתחום,[30] וכי עיקר המידע מגיע מהצהרות לעיתונות ומכתבות בתקשורת, ולא ממידע ממשלתי רשמי. אמנם קיימת החלטת ממשלה רשמית בנושא, אולם טרם פורסמה אסטרטגיה סדורה.

## הקצאת תקציבים

בחלק זה ייבחנו התקציבים והמשאבים שהוקצו להתמודדות עם האיום הנשקף כתוצאה מהתפתחות טכנולוגיית הלוחמה הקיברנטית, מתוך הנחה שבחינת התקציבים תאפשר להקיש על מידת חשיבותו של הנושא עבור מקבלי ההחלטות בישראל.

המועצה הלאומית למחקר ופיתוח (המולמו"פ) יזמה בשנת 2007 ומימנה מחקר בנושא "מדדים למדע, לטכנולוגיה ולחדשנות בישראל", בשיתוף הלשכה המרכזית לסטטיסטיקה. מטרת המחקר הייתה לבחון את התקציבים המוקצים לנושאי מדע וטכנולוגיה בישראל. מהמחקר עלה שבעשור האחרון הוצאו בישראל מדֵי שנה כ־30 מיליארד ש"ח למחקר ופיתוח (מו"פ) אזרחי. בחינת האחוז מהתוצר הלאומי הגולמי המושקע במחקר ופיתוח הראתה שישראל מדורגת במקום הראשון בעולם – 4.3% בשנת 2009, לעומת 1.8% בממוצע במדינות הארגון לשיתוף פעולה כלכלי ולפיתוח (OECD). מרבית המימון בישראל, כ־79%, מגיע מהמגזר העסקי. הממשלה מממנת באופן ישיר כ־5 מיליארד ש"ח מהמו"פ האזרחי, נוסף על הכספים המוקצים למימון המו"פ בתחום הביטחוני.[31]

מהנתונים אפשר ללמוד שמדינת ישראל והמגזר העסקי שלה משקיעים סכומים לא־מבוטלים במחקר ופיתוח בתחום הטכנולוגי. לכך אפשר לצרף את התקציבים השונים שחולקו בשנה האחרונה למחקר ופיתוח בנושאים יישומיים ותיאורטיים בתחום הקיברנטי.[32] מצירוף הנתונים ניתן להניח שהתחום הקיברנטי מקבל תקצוב למטרות מחקר ופיתוח, מתוך הכרה בחשיבותו הגוברת לביטחון המדינה. התקצוב המדויק אינו מתפרסם ברבים.

אחת ההוצאות העיקריות בהצעת תקציב המדינה לשנים 2011–2012 יועדה ל"אשכול הביטחון והסדר הציבורי". מתוך הוצאה זו מוקצים כספים לגופי מערכת הביטחון השונים, האחראים על הטיפול בתחום הקיברנטי. סך התקציב שהופנה למימון האשכול עמד על סכום כולל של 61.8 מיליארד ש"ח בשנת 2011, וסכום כולל של 63.4 מיליארד ש"ח בשנת 2012. מתוך הסכומים האמורים, ההוצאות שהופנו לפעילות משרד הביטחון היו הגבוהות ביותר, ושיעורן עמד על כ־18% מסך ההוצאה התקציבית.[33] ניתן להניח שמשרד הביטחון משקיע סכומים לא־מבוטלים גם בפיתוח תחום הלוחמה הקיברנטית בגופים המצויים באחריותו.

המלצה נוספת של צוות המיזם הקיברנטי הייתה לייסד תוכנית מו"פ לאומית לבניית יכולות קיברנטיות, בשיתוף עם מערכת הביטחון, עם האקדמיה ועם התעשייה. התוכנית כללה המלצות להכוונת המשאבים הלאומיים הקיימים והוספת משאבים במידת הצורך. כל זאת במטרה להציב את ישראל בחמישייה המובילה של מדינות העולם מבחינת יכולותיה הקיברנטיות עד שנת 2015.[34] בהקשר זה חשוב לציין כי לא מדובר בהכרח רק בפיתוח יכולות צבאיות־ביטחוניות,

אולם סביר להניח כי לפחות חלק מהתקציב יוקצה לפיתוח ביטחוני בתחום הקיברנטי.

## תקציב המטה הקיברנטי

בהחלטת הממשלה מאוגוסט 2011 שבה הוחלט על הקמת המטה הקיברנטי הלאומי, הוחלט להקצות למטה תקציב שיועבר למשרד ראש הממשלה ממקורות משרד האוצר.[35] התקציב המלא שהוקצה לפעולות המטה אינו מפורט בהחלטה, מלבד סכום קטן (כ־4.5 מיליון ש"ח) שהוקצה עבור "הקמת ותפעול המטה" לשנת 2011.

תקציב המטה הקיברנטי כיום הוא 2.5 מיליארד ש"ח לחמש השנים הבאות, כ־500 מיליון ש"ח בשנה. 100 מיליון מתוכם יוקצו כסכום ייעודי מתקציב המדינה עבור המטה הקיברנטי, ו־400 מיליון יינתנו לאחר תהליך "איגום" כספים ממקורות שונים.[36] לדבריו של רס"ן טל, ראש תחום בכיר במטה הקיברנטי, ראש הממשלה רואה בתחום הקיברנטי נושא בעל חשיבות עליונה ופועל רבות לקידומו. קיימת נכונות לפיתוח התחום והתקציבים ניתנים בהתאם. חשיבות האיום הקיברנטי צוברת תאוצה, ואף נבנתה תוכנית ארוכת־טווח שתבטיח את תקציביו.[37]

בישיבת ועדת הכספים מחודש מאי 2012 הוקצו באופן מפורש תקציבים להמשך קידום פעילותו של המטה, מעבר לסכומים שכבר הוקצו.[38] בקשת המטה, כפי שהובאה לאישור הוועדה, כללה כ־12 מיליון ש"ח למימון שני נושאים מרכזיים: הראשון – תקציב תפעול המטה, שכלל תשלום משכורות לעובדי המטה ויצירת תשתיות ממוחשבות ותשתיות אבטחה פיזיות עבור גופים מסווגים הנדרשים לתשתיות מסוג זה. השני – תחילת מימוש תקציב פעילותו השוטפת של המטה.[39]

מתוך הכרה בחשיבות הקשר בין האקדמיה, התעשייה והמטה הקיברנטי הוקצו על ידי המטה, בשיתוף משרד המדע, כ־50 מיליון ש"ח לשלוש שנים עבור מלגות ומחקרים בתחומי עיסוק שונים של תחום העיסוק הקיברנטי, במטרה למצב את ישראל כמובילה בעולם בתחום.[40] נוסף לכך, הכריזו המדען הראשי והמטה הקיברנטי על הקצאת 80 מיליון ש"ח עבור תוכנית קידמ"ה,[41] שמטרתה פיתוח המו"פ והיזמות בנושא ה־Cyber Security.[42] גם במקרה זה, סביר להניח שחלק מהמלגות יוקצו לתחומים הנוגעים ללוחמה הקיברנטית.

לנוכח מיעוט הפרסומים העוסקים בנושא התקציב, קשה לאמוד מהי ההשקעה הממשלתית המדויקת בהתמודדות עם האיום הקיברנטי בישראל. עם זאת, מהנתונים שהוצגו לעיל אפשר לראות שהאיום הנשקף כתוצאה מהתפתחות טכנולוגיית הלוחמה הקיברנטית לא נעלם מעיניהם של מקבלי ההחלטות במדינה, וכי הנושא זוכה למשאבים לא־מבוטלים.

החל משנת 2011 החלו להתפרסם בפומבי הקצאות תקציבים לתחום הקיברנטי. ניתן להניח במידה רבה של ודאות, שלאור העובדה שהטיפול בתחום הקיברנטי הובל בעשור האחרון על ידי מערכת הביטחון במעטה סודיות, תקציבים שונים שהוקצו לתחום זה אינם מפורסמים בגלוי. עם זאת, לאחר קבלת ההחלטה הרשמית על הקמת המטה הקיברנטי הלאומי באוגוסט 2011, החל להתפרסם בגלוי מידע על התקציבים המופנים להתעצמות ולנושאי מחקר ופיתוח בתחום.

## שינויים בבניין הכוח

טכנולוגיית הלוחמה הקיברנטית יצרה שינוי במערכות הנשק של זירת הלחימה המודרנית, והפכה אותן למדויקות וליעילות יותר. בעקבות השינויים הרבים שחלו בסביבתה החיצונית של ישראל, גברו אתגרי הביטחון שמולם היא ניצבת, וגדלה מידת חשיבותו של המודיעין בתפיסת הביטחון הישראלית. כיום ניצבת ישראל בחזית הטכנולוגיה ומתמודדת עם האיומים הנשקפים לה, בסיוע כלים טכנולוגיים קיברנטיים המשולבים בכל זירות הלחימה.[43]

להתפתחויות מסוג זה הייתה השפעה לא־מבוטלת על עקרונות המלחמה ועל שינויים שחלו במבנה צבאות, ובכלל זה במבנה צה"ל. בבואו לבחון את מקומה של הטכנולוגיה לאורך מלחמות ישראל, טען פרופ' בן ישראל כי ככל ששדה הקרב מתקדם יותר מבחינה טכנולוגית, כך הגמישות והיכולת לאלתר ולשנות (changeability) תופסות חלק גדול יותר בלחימה המודרנית. למשל, מלחמת יום־הכיפורים הדגימה היטב שלא די לבנות מערכות לוחמה אלקטרונית נגד האיומים המוכרים של האויב, אלא יש צורך לבנותן כך שיוכלו להתמודד עם השינויים שיעשה האויב בפרמטרים האלקטרוניים של מערכותיו תוך כדי הלחימה.[44]

להלן ייבחנו השינויים המרכזיים שחלו בגופים הממשלתיים ובגופי מערכת הביטחון בישראל, לאור ההכרה הגוברת בסיכונים הנשקפים מהתפתחות האיום הקיברנטי ומכניסתה של הטכנולוגיה הקיברנטית לשדה הקרב.

## המטה הקיברנטי הלאומי

באוגוסט 2011 הכריז ראש הממשלה על הקמת "המטה הקיברנטי הלאומי", שייעודו העיקרי הוא הרחבת יכולות ההגנה על מערכות התשתית החיוניות למדינה מפני התקפות טרור קיברנטי, העלולות להיגרם הן על ידי מדינות זרות והן על ידי גורמי טרור.[45] המטה, הפועל כשנה וחצי ומצוי בשלבי צמיחה, מורכב כיום מארבעה אגפים: האגף הביטחוני; האגף האזרחי; אגף המודיעין והערכת מצב; האגף לארגון ולמדיניות. נוסף לכך הוקם חדר מצב בירושלים, הפעיל 24 שעות ביממה שבעה ימים בשבוע, ומצוי בקשר רציף עם הגופים הביטחוניים העוסקים בתחום. חדר המצב מאפשר ראייה כוללת של סך האיומים ואפשרויות ההתמודדות,

כך שבשעת ביצוע תקיפה קיברנטית על גוף אחד, אפשר יהיה לדעת בזמן אמת על אילו גופים נוספים יש להגן.

שלושת הנושאים המרכזיים שעליהם אמון המטה הקיברנטי הם:

**הראשון** – גיבוש תפיסת ההגנה הרשמית של ישראל, זאת באמצעות שיתוף פעולה בין כלל הגופים האמונים על תחום ההגנה. נוסחה תפיסה הפועלת בשתי רמות: רמת האבטחה הכללית במשק ורמת האבטחה המדינתית.

**השני** – פיתוח התשתית וקידום המובילות הלאומית של ישראל בתחום הקיברנטי. בין היתר, באמצעות הרחבת ההון האנושי וקידום נושא המלגות למחקרים בתחום הקיברנטי.

**השלישי** – הובלת תהליכים לאומיים בתחום הקיברנטי, כמו יצירת הסדרה בשוק האבטחה; יצירת תשתית אבטחה מדינתית באמצעות חקיקה וביצוע תרגילי חירום; חיזוק קשרי החוץ עם מדינות שונות בעולם ועוד.[46]

ההחלטה על הקמת המטה הייתה צעד חשוב בהתמודדותה של ישראל עם האתגר הקיברנטי, אולם יש להבטיח כי המטה יפעל על פי אסטרטגיה לאומית שתגובש בהקדם. לנוכח פיגורה של ישראל בקביעת אסטרטגיה פומבית סדורה, יש חשיבות רבה לכך שהמטה יקבל סמכויות רחבות־היקף. רק כך אפשר יהיה להתחיל לצמצם את הפער שנוצר ברמה הלאומית בניהול האסטרטגי המקיף של כלל הגופים האזרחיים והצבאיים הפועלים בתחום הקיברנטי.[47]

## הרשות הממלכתית לאבטחת מידע

הגוף הוותיק ביותר העוסק בנושא אבטחת המידע על היבטיו השונים הוא "הרשות הממלכתית לאבטחת מידע" בשב"כ. רשות זו צמחה מתוך יחידה שטיפלה במשך עשרות שנים בתחום אבטחת המידע הקלאסית, עד שקיבלה בשנת 2002 את האחריות על הנחיית כל גופי התשתיות הלאומיות האזרחיים להתגוננות מפני מתקפות סייבר אפשריות.

השב"כ קיבל סמכות על פי חוק להנחות גופים כגון חברת חשמל, מקורות, רכבת ישראל וחברות הגז. תחומי ההנחיה כוללים הוראות כמו כיצד למנוע השתלטות עוינת מרחוק, שעלולה לגרום פגיעה קשה במערכות קריטיות בלחיצת מקש, וכדומה. בשנים האחרונות התרחבה רשימת הגופים המונחים על ידי הרשות, מתוך הכרה לאומית באיום הקיברנטי הגובר.[48]

צפריר כץ, שכיהן עד לאחרונה כראש אגף הטכנולוגיה בשב"כ, העניק הצצה נדירה אל הנעשה בתחום הטכנולוגי בשב"כ ואמר כי כ־20% מאנשי השירות הם אנשים טכנולוגיים. השירות שינה את פניו לעומת שנות השמונים של המאה הקודמת, אז לא היה מוטה לכיוון הטכנולוגיה. היה צורך לפתח צורות העסקה

למספר שנים עבור אנשים צעירים. לתפיסתו, מדובר במהפכה הנמשכת לאורך כל העשור האחרון.[49]

## צה"ל

בשנת 2009 הגדיר הרמטכ"ל דאז, רב־אלוף גבי אשכנזי, את המרחב הקיברנטי "כמרחב לחימה אסטרטגי ואופרטיבי עבור מדינת ישראל". בהמשך לכך הוקם "מטה הסייבר הצה"לי", שנועד לשמש מטה מטכ"לי לתיאום ולהכוונה של פעולות הצבא בתחום הקיברנטי. המטה הוקם ביחידה 8200 באגף המודיעין של צה"ל.[50]

בחיל התקשוב הוקמה מחלקת הגנה בסייבר, שפעילותה מסווגת ברובה. המחלקה מאפשרת לקיים פעילויות מבצעיות ביבשה, באוויר ובים, בעידן שבו הצבא נשען יותר מתמיד על טכנולוגיית מחשבים. המחלקה פועלת בשיתוף פעולה עם מרבית היחידות המובחרות של צה"ל, בעודה מפעילה אמצעים טכנולוגיים מתקדמים מגוונים על מנת לנטרל את התקיפות הקיברנטיות של האויב.[51]

במטרה להגן על מערכות המחשוב של צה"ל, פיתח חיל התקשוב תוכנית הכשרה המכונה "מסלול הגנת הסייבר". במאי 2012 הסתיים המחזור הראשון של קורס "מגן בסייבר" של החיל. לאחר מספר חודשי לימוד אינטנסיביים הוכשרו החיילים לבצע פעולות הגנה במרחב הממוחשב, על רקע המציאות הטכנולוגית המתפתחת.[52]

## משרד הביטחון

בינואר 2012 פורסם כי משרד הביטחון עומד להקים מנהלת מיוחדת ללוחמה קיברנטית, שתרכז את כלל פעולות גופי הביטחון והתעשיות הביטחוניות העוסקים בפיתוח מערכות מתקדמות בתחום. במהלך שנת 2012 הוקמו מטות מיוחדים לעיסוק בלוחמה קיברנטית בתעשיות הביטחוניות המרכזיות, דוגמת אלביט מערכות, רפא"ל והתעשייה האווירית; גם התעשייה הצבאית שוקלת להיכנס לתחום[53]. טרם הוחלט מי יעמוד בראש המִנהלת החדשה, ואולם לדברי גורמים ביטחוניים, עצם ההחלטה להקים מנהלת חדשה "תיקח את העיסוק בתחום למקום חדש".[54]

## הרשות למשפט וטכנולוגיה

בספטמבר 2006 הוקמה הרשות למשפט ולטכנולוגיה (רמו"ט) במשרד המשפטים. תפקידה הוא להגן על המידע האישי בישראל. יעדי רמו"ט הם חיזוק ההגנה על מידע אישי; הסדרת השימוש בחתימות אלקטרוניות ופיקוח עליו; הגברת האכיפה על עבירות פגיעה בפרטיות, בכלל זה עבירות המבוצעות במרחב הקיברנטי.[55] רמו"ט משמשת גם מרכז ידע בממשלה לחקיקה ולפרויקטים בעלי היבטים

טכנולוגיים, כגון ממשל זמין.[56] בימים אלה מטפלת הרשות בחקירת פרטי האירוע שבו פורסם באינטרנט מידע אישי רב, לרבות נתונים של כרטיסי אשראי, על ידי מי שהזדהו כהאקרים סעודיים.[57]

## "ממשל זמין" – e-gov.il (תהיל"ה)

מערך "ממשל זמין" הוקם באגף החשב הכללי במשרד האוצר בשנת 1997 כיחידת תהיל"ה. מטרת פעילותו היא לאפשר לאזרחים לבצע מגוון פעולות רחב מול משרדי הממשלה ורשויות המדינה באמצעות האינטרנט, במקביל לשמירה על אבטחת המידע המועבר ועל פרטיות המשתמש. המערך מפעיל משאבים רבים לשמירת הפרטיות, החל בצוות מומחי אבטחת מידע וכלה בשימוש בטכנולוגיות אבטחה מהמובילות בעולם.[58]

## סיכום

ישראל היטיבה לזהות את מאפייניו של האיום הנשקף כתוצאה מהתפתחות טכנולוגיית הלוחמה הקיברנטית, החלה לפעול ליצירת השינויים הנדרשים ונראה כי קיימת זיקה הדוקה בין אופן הטיפול באיום הקיברנטי לבין ביטחונה הלאומי של המדינה. אופן הטיפול מתרכז בשלושה נושאים: **הראשון** – ארגונים ביטחוניים, צה"ל, קהילת המודיעין והתעשייה הביטחונית, שבמצב הקיים פועלים להגן על מערכותיהם באופן עצמאי, ואינם מונחים על ידי השב"כ. **השני** – התשתיות הלאומיות הקריטיות שאפשר לתקוף אותן תקיפה קיברנטית, ומונחות על ידי הרשות לאבטחת מידע. **השלישי** – המגזר הפרטי, שבו פועלות חברות אזרחיות החשופות למתקפות קיברנטיות. שכבה זו מטופלת בחלקה על ידי רמו"ט, ובחלקה הגדול אינה מטופלת כלל.[59]

המלחמה הקיברנטית מתחוללת במלוא עוזה, וישראל היא שחקנית ראשית בה.[60] ניתן לבחון את העובדות היבשות ולהתרשם: הוקם מטה קיברנטי לאומי במשרד ראש הממשלה; מענקים בגובה מיליוני שקלים יוענקו בכל אחת מהשנים הבאות למחקרים ולפעילויות חינוך בתחום הקיברנטי; בצבא חולקה האחריות בתחום הקיברנטי בין אגף המודיעין (התקפה) ואגף התקשוב (הגנה); והרשות הממלכתית לאבטחת מידע צפויה להרחיב את פעילותה.[61] נראה שהטיפול בתחום הקיברנטי צובר תאוצה במספר היבטים מרכזיים: החל להתפרסם בגלוי מידע על אודות העיסוק הממשלתי באיום הקיברנטי, הוקצו תקציבים ייעודיים למחקרים בתחום ונעשה ניסיון לתקצב את פעילות המטה הקיברנטי הלאומי באופן שוטף. במקביל, גופים שונים הוקמו ו/או התפתחו מאוד במטרה להתמודד באופן מיטבי עם האיום הקיברנטי הגובר.

השינויים הטכנולוגיים המהירים שהתרחשו בשנים האחרונות השפיעו על סדר העדיפויות של מקבלי ההחלטות במדינה בדרכים שונות, ביניהן פרסום החלטות ממשלה רשמיות והקמת גופים ייעודיים להתמודדות עם האיום הקיברנטי. אף שבמבט ראשון נראה שישראל מתקדמת מאוד בדרך התמודדותה עם האיום הקיברנטי הגובר, עדיין יש מקום לנקיטת פעולות נוספות המגדירות בצורה ברורה יותר מהי המדיניות הרצויה לטיפול כולל בנושא.

## הערות

1 דברי פרופ' יצחק בן ישראל ונוספים, מתוך: פרוטוקול מס' 95 – ישיבת וועדת המדע והטכנולוגיה: "לוחמה קיברנטית – הערכות מדינת ישראל למתקפות על רשתות מחשבים ותקשורת". יום שני, ב' תמוז תשע"א, (4 ביולי 2011), שעה 11:00. http://www.knesset.gov.il/protocols/data/html/mada/2011-07-04.html

2 לפי דו"ח של צוות חשיבה בינלאומי בנושא ביטחון – SDA (Security & Defense. Agenda) שנעשה בשיתוף חברת אבטחת המידע מקא'פי (McAfee) שהתפרסם בפברואר 2012: Cyber-security: The vexed question of global rules. An Independent report on cyber-preparedness around the world. With the support of *McAfee*. SDA, Belgium. בדו"ח זה קיבלה ארצות־הברית ציון של ארבעה כוכבים. http://www.mcafee.com/hk/resources/reports/rp-sda-cyber-security.pdf
ראו גם: אהוד קינן, "דו"ח: ישראל מוכנה יותר מארה"ב למתקפה מקוונת". YNET, 31 בינואר, 2012. http://www.ynet.co.il/articles/0,7340,L-4183126,00.html

3 נייר מטה לדיון הוועדה העליונה למדע וטכנולוגיה בנושא: **המיזם הקיברנטי הלאומי.** הצעה להקמת תוכנית לאומית לבניית יכולות קיברנטיות בשילוב היבטי מו"פ, כלכלה, אקדמיה, תעשייה וצורכי הביטחון הלאומי. תל אביב, נובמבר 2012, עמ' 18.

4 שמואל אבן ודוד סימן טוב, **לוחמה במרחב הקיברנטי: מושגים, מגמות ומשמעויות לישראל**, המכון למחקרי ביטחון לאומי, מזכר 109, (תל אביב: המכון למחקרי ביטחון לאומי, 2011).

5 זאב שיף, "דו"ח ועדת מרידור: חשש שמדינות מזרח־תיכוניות יצטיידו בגרעין בעקבות איראן", **הארץ**, 24 באפריל, 2006. http://www.haaretz.co.il/misc/1.1100503

6 שי שבתאי, "תפיסת הביטחון של ישראל – עדכון מונחי יסוד", **עדכן אסטרטגי**, כרך 13, גיליון 2, (אוגוסט 2010), עמ' 8–10.

7 אמיר בוחבוט, "משנים את תפיסת הביטחון", **NRG מעריב**, 24 באפריל, 2006. http:// www.nrg.co.il/online/1/ART1/076/915.html

8 ההצעה לא אושרה באופן רשמי בממשלה, בשל חילוקי דעות בין קברניטים. עם זאת, מרכיב ההגנה הפך לחלק מתפיסת הביטחון של ישראל באופן בלתי־רשמי.

9 "תפיסת הביטחון של ישראל – עדכון מונחי יסוד". עמ' 8–10.

10 רמי אפרתי וליאור יפה, "כך בונים הגנה קיברנטית לאומית", **Israel Defense**, 11 באוגוסט, 2012. http://www.israeldefense.co.il/?CategoryID=512&ArticleID=2960

11 יצחק בן ישראל . "לקחים טכנולוגיים", **מערכות**, גיליון מספר 332, (1993). עמ' 13.

12 עמוס ידלין, "הממד החדש של הלחימה – סייבר". **מבט מל"מ**, (ינואר 2010). עמ' 4. http://www.intelligence.org.il/KotarPort.aspx#http://malam.barebone.kotar.co.il/KotarApp/Viewer.aspx?nBookID=94837032&sSelectedTab=tdBookInfo%231.undefined.3.fitwidth

13 סוכנות הידיעות "רויטרס", "סטוקסנט שפגע באיראן – רק אחד מ־5 וירוסים", YNET, 29 בנובמבר, 2011. http://www.ynet.co.il/articles/0,7340,L-4168852,00.html

14 "כך בונים הגנה קיברנטית לאומית".

15 ליאור טבנסקי, "הגנה על תשתיות קריטיות מפני איום קיברנטי", **צבא ואסטרטגיה**, כרך 3, גיליון 2, (נובמבר 2011). , ע' 72.
החלטות לדוגמה: החלטת ממשלה 1886 בק/9 מ־20 במרס 1997: הקמת ועדת היגוי לנושאי מחשוב בכל משרד ממשלתי; החלטת ממשלה 3582 בק/77 מ־16 במרס 1998: אחריות לנושא אבטחת מידע במשרדי הממשלה; החוק להסדרת הביטחון בגופים הציבוריים 1998.

16 לפירוט נוסף על תהיל"ה ראו פרק אחרון במאמר זה העוסק בנושא בניין הכוח.

17 "כך בונים הגנה קיברנטית לאומית".

18 "הגנה על מערכות משובצות מחשב".
http://www.nsc.gov.il/NSCWeb/Templates/CounterTerrorismActivities.aspx.

19 "הגנה על תשתיות קריטיות מפני איום קיברנטי", עמ' 72–73.

20 בנובמבר 2010 הנחה ראש הממשלה על הקמת צוות מיוחד, שיעסוק בגיבוש תוכנית לאומית להצבת ישראל בין חמש המדינות המובילות בתחום הקיברנטי. העבודה בנושא, שכותנתה "המיזם הקיברנטי הלאומי", הובלה על ידי הוועדה העליונה למדע וטכנולוגיה, בראשות פרופ' בן ישראל. הצוות כלל נציגים מהגופים המרכזיים העוסקים בתחום הקיברנטי בישראל והורכב ממספר תת־צוותים שבחנו את המרכיבים החיוניים להתמודדותה של ישראל עם האיום הקיברנטי, וניתחו את התועלות הלאומיות בהיבטי הכלכלה, האקדמיה והביטחון הלאומי.

21 "המיזם הקיברנטי הלאומי", בתוך: **המועצה הלאומית למחקר ולפיתוח, דו"ח לשנים 2010–2011.** עמ' 10–17.
http://knesset.gov.il/committees/heb/material/data/mada2012-10-15.pdf

22 ההחלטה התקבלה בעקבות עבודת מטה מקיפה שבוצעה על ידי צוות לאומי בראשות יו"ר המועצה הלאומית למחקר ופיתוח , פרופסור יצחק בן ישראל.

23 "קידום היכולת הלאומית במרחב הקיברנטי". החלטת ממשלה מספר 3611 מיום 7 באוגוסט 2011.
http://www.pmo.gov.il/Secretary/GovDecisions/2011/Pages/des3611.aspx

24 "כך בונים הגנה קיברנטית לאומית".

25 יהודה קונפורטס, "דרושה: "כיפת ברזל" לסייבר שתגן על העורף", **אנשים ומחשבים,** 1 בפברואר 2012. http://www.pc.co.il/?p=79406

26 יוסי הטוני, "ד"ר אביתר מתניה: המרחב הקיברנטי מחייב התייחסות עסקית ולאומית־מדינתית; המסע לא קל", מתוך כנס CyberSec שהתקיים בפברואר 2012. **אנשים ומחשבים**, 12 בפברואר 2012. http://www.pc.co.il/?p=80025

27 שם.

28 דברי ד"ר אביתר מתניה, **כנס הסייבר הבינלאומי השני**, אוניברסיטת תל אביב, ב־9 ביוני 2012.

29 "כך בונים הגנה קיברנטית לאומית".

30 פרט לפרסום החלטת הממשלה על אודות הקמת המטה הקיברנטי הלאומי.

31 "מדיניות מו"פ לאומית כמערכת כלים שלובים", מסמך מסכם. מדברי פרופ' יצחק בן ישראל, כנס הרצלייה השנתי 2011. http://www.herzliyaconference.org/_Uploads/dbsAttachedFiles/OriSlonim2.pdf

32 "קול קורא למלגות בתחום: הגנת הסייבר ומחשוב מתקדם".
http://exactsci-info.tau.ac.il/exact_sciences/site/temp/cybersco.pdf

33 **תקציב המדינה – הצעה לשנות הכספים, 2011–2012 עיקרי התקציב ותוכנית תקציב רב־שנתית**. ירושלים, 2010. http://www.mof.gov.il/BudgetSite/StateBudget/Budget2011_2012/Lists/20112012/Attachments/1/Budget2011_2012.pdf

34 נייר מטה לדיון הוועדה העליונה למדע וטכנולוגיה בנושא: **המיזם הקיברנטי הלאומי.** הצעה להקמת תוכנית לאומית לבניית יכולות קיברנטיות בשילוב היבטי מו"פ, כלכלה, אקדמיה, תעשייה וצורכי הביטחון הלאומי. תל אביב, נובמבר 2012. ע' 20

35 "קידום היכולת הלאומית במרחב הקיברנטי", החלטת ממשלה מספר 3611, מיום 7 באוגוסט 2011. http://www.pm.gov.il/PMO/Secretarial/Decisions/2011/08/des3611.htm

36 מתוך ראיון עם פרופ' יצחק בן ישראל בנושא המיזם הקיברנטי. התקיים בתאריך 5 באוגוסט 2012, באוניברסיטת תל אביב.

37 מתוך ראיון עם רס"ן טל, ראש תחום בכיר במטה הקיברנטי. התקיים בתאריך 23 באוגוסט 2012, במטה הקיברנטי, רמת אביב. תוכנית התקצוב המוזכרת טרם פורסמה בפומבי.

38 שם.

39 **שינויים בתקציב לשנת 2012**, פרוטוקול מס' 1069, ישיבת ועדת הכספים. יום שני, א' באייר התשע"ב (1 במאי 2012), שעה 12:30. www.knesset.gov.il/protocols/data/rtf/ksafim/2012-05-01-02.rtf

40 "התקציב ותוכניות העבודה של מטה הסייבר הלאומי אושרו על ידי ראש הממשלה נתניהו". 6 ביוני 2012. http://www.pmo.gov.il/MediaCenter/Spokesman/Pages/spokecyber060612.aspx

41 ב־13 נובמבר 2012 הודיע ראש מטה הסייבר הלאומי על השקת תוכנית קידמ"ה – קידום מו"פ הגנת הסייבר. התוכנית היא פרי שיתוף פעולה בין המטה לבין המדען הראשי במשרד התמ"ת, שמטרתו לקדם את המו"פ והיזמות בתחום ה־Cyber-Security במטרה לשמר את הפוטנציאל התחרותי של התעשייה הישראלית בתחום זה בשוק העולמי, ואף להעצימו.

42 חוזר המדען הראשי: "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
ראו גם: "שמונים מליון ש"ח לקידום הסייבר", **IsraelDefenseTech**, 30 בדצמבר 2012, http://www.israeldefense.co.il/?CategoryID=760&ArticleID=3796

43 שמואל אבן ועמוס גרנית, "**קהילת המודיעין הישראלית – לאן? ניתוח, מגמות והמלצות**". מזכר מספר 97, תל אביב: המכון למחקרי ביטחון לאומי. מרס 2009. עמ' 64.

44 "יצחק בן ישראל, "לקחים טכנולוגיים", **מערכות**, גיליון מספר 332, (1993). עמ' 10.

45 כפי שפורט בהרחבה בפרק העוסק בקביעת האסטרטגיה.

46 מתוך ראיון עם רס"ן טל, ראש תחום בכיר במטה הקיברנטי. התקיים בתאריך 23 באוגוסט 2012 במטה הקיברנטי, רמת אביב.

47 מתוך דברי ראש הממשלה, מר בנימין נתניהו, **כנס הסייבר הבינלאומי הראשון**, אוניברסיטת תל אביב, 9 ביוני 2011.

48 עמיר רפפורט, "מתקפת סייבר על תשתיות לאומיות". **Israel Defense**, 8 בדצמבר 2011. http://www.israeldefense.co.il/?CategoryID=536&ArticleID=1421

49 עמיר רפפורט, "להגיב מהר כדי להיות רלוונטי", **Israel Defense**, 3 באפריל 2012, http://www.israeldefense.co.il/?CategoryID=512&ArticleID=2153

50 אמיר אורן, "זירת הלחימה החדשה של צה"ל נמצאת ברשתות המחשבים", **הארץ**, 1

בינואר 2010. http://www.haaretz.co.il/misc/1.1182490

51 "מקצועות המחשב מסלול מגן בסייבר", אתר חיל הקשר והתקשוב. http://www.tikshuv.idf.il/site/General.aspx?catId=60698&docId=76101

52 הדס דובדבני, "הסתיים קורס הסייבר הראשון בצה"ל. המטרה: שלושה מחזורים בשנה". אתר צה"ל. 3 במאי 2012. http://www.mako.co.il/pzm-soldiers/Article-595ec4bc4611731006.htm&sCh=3d385dd2dd5d4110&pid=1093150966

53 "חשיפה: מנהלת סייבר חדשה", **Israel Defense**, 12 בינואר 2012. http://www.israeldefense.co.il/?CategoryID=512&ArticleID=1657 – לא נמצאו פרסומים נוספים לגבי המִנהלת במשרד הביטחון, סביר להניח שמטעמי סיווג. ראו גם: "מתקפת סייבר על תשתיות לאומיות".

54 עמיר רפפורט, "חשיפה: תרגיל הגנת סייבר לאומי", **Israel Defense**, 19 בינואר, 2012. http://www.israeldefense.co.il/?CategoryID=512&ArticleID=1706

55 מתוך ראיון עם עו"ד יורם הכהן, ראש הרשות למשפט ולטכנולוגיה דאז, התקיים ב־5 בספטמבר 2012 בקריית הממשלה, תל אביב.

56 אתר הרשות למשפט, טכנולוגיה ומידע (רמו"ט) http://www.justice.gov.il/MOJHeb/ILITA/

57 הודעה לעיתונות בשם הרשות למשפט טכנולוגיה ומידע, משרד המשפטים, לשכת הדובר. http://www.justice.gov.il/NR/rdonlyres/4C39E414-E501-48C2-9C53-8EB533FD8B7D/32913/dover5.pdf

58 "אודות מערך ממשל זמין", http://e.gov.il/AboutUs/Pages/AboutUs.aspx

59 יוסי הטוני, "אל"מ (מיל') ד"ר גבי סיבוני: "יש שכבה שלמה של ארגונים שלא מוגנים מפני מתקפות סייבר", מתוך: כנס CyberSec 2012 המכון למחקרי ביטחון לאומי, ב־12 בפברואר 2012. **אנשים ומחשבים**, 15 בפברואר 2012. http://www.pc.co.il/?p=80466

60 אירועי ה־"סטקסנט", ה־"פליים" ונוספים, אשר על פי פרסומים זרים בוצעו על ידי ישראל.

61 "מתקפת סייבר על מתקני תשתית לאומית".

# כישלון שיטות הגנת הסייבר הקלאסיות – מה הלאה?

**אמיר אורבוך, גבי סיבוני**

## מבוא

שיטות ההגנה הקלאסיות הנהוגות בעולם בעשרות השנים האחרונות אינן מצליחות לעצור התקפות פוגעניות (malware) מודרניות העושות שימוש בפרצות אבטחה שאינן מוּכרות (ולכן אין להן עדיין תיקון), שנקראות חולשות יום־אפס (zero-day vulnerabilities). דוגמאות להתקפות אלה על מחשבים ועל רשתות תקשורת של ארגונים עסקיים ושל ספקי תשתיות ושירותים חיוניים וקריטיים הן וירוסים, תולעים, דלת אחורית, סוסים טרויאניים – כלי ניהול/גישה מרחוק (RATs). שיטות ההגנה הקלאסיות, הכוללות אמצעי תוכנה וחומרה והמתבססות על חומות אש (FireWall), חתימות וחוקים (rules), תוכנות אנטי־וירוס, סינון תוכן, מערכות איתור חדירה (IDS) ודומיהם נכשלות לחלוטין בהגנה מפני איומים לא־מוּכרים, דוגמת איומים המבוססים על חולשות יום־אפס ואיומים חדשים. איומים מתוחכמים וחמקניים אלה מתחזים להיות מידע ונתונים אמינים וחוקיים במערכת, ולכן מערכות ההגנה הקלאסיות אינן מספקות את המענה ההגנתי הדרוש. מערכות ההגנה המקובלות כיום מגֻנות מפני התקפות מוּכרות על סמך חתימות ידועות וניתוח לאחור של התקפות, על מנת לייצר באופן היוריסטי,[1] אבל הן חסרות תועלת מול ההתקפות המתרבות והולכות שאינן מוכרות, וחסרות כל חתימה. לפתרון בעיה זו דרושים חשיבה ופתרונות אחרים. מאמר זה מציע גישת הגנה עדכנית, שבבסיסה ניתוח מידע רגיש שעליו יש להגן, למטרת זיהוי התנהגויות אנומליות.[2] המידע המנותח כולל את פעילות התקשורת הארגונית (datasilos) כמקור להבנת התנהגות לא־רגילה (אנומליות), המעידה ברוב המקרים על קיום פוגענים במערכת.

פרופ׳ אמיר אורבוך הנו חבר סגל בית הספר למדעי המחשב באוניברסיטת תל־אביב וחוקר במסגרת תוכנית ניובאוור ללוחמת סייבר במכון למחקרי בטחון לאומי.
ד״ר גבי סיבוני הוא ראש תוכנית צבא ואסטרטגיה וראש תוכנית לוחמת סייבר במכון למחקרי בטחון לאומי.
מאמר זה נכתב בסיועו של אביב רוטברט, תלמיד לתואר שלישי, מלגאי בתוכנית ניובאוור במכון למחקרי בטחון לאומי.

המאמר מציע להתבסס על הנתונים שעליהם יש להגן כמקור ידע לפיתוח מערכת ההגנה. ניתוח אנליטי של נתונים מסיביים (BIG-DATA Analytics) יאפשר זיהוי פוגענים כאלה תוך בניית מודל המאפשר אמינות גבוהה של זיהוי ומזעור התרעות השווא (false positive), המהוות אתגר לכל מערכת הגנה.

## התפתחות האיומים והמגבלות של שיטות ההגנה המסורתיות

התקפות הסייבר הראשונות על מחשבים התבססו על וירוסים או תולעים המשכפלים עצמם ומתפשטים במהירות. אולם טכנולוגיית האנטי־וירוס נכשלה לחלוטין ונמצאה לא יעילה באיתור סוסים טרויאניים, שהתנהגותם שונה לחלוטין משל וירוסים. באופן מסורתי, מערכות ההגנה התפתחו כדי להגן מפני וירוסים מוכרים, מאחר שקיים קושי מהותי לזהות וירוסים אלה על פי התנהגותם ולא על פי מאפייני הזיהוי שלהם (חתימה). כך ניתן היה לייצר בסיסי מידע עם חתימות של וירוסים, ולהשוות קבצים ותקשורת המגיעים למחשבים מול חתימות אלה. גישה זו חייבה את יצרני תוכנות הגנה לעקוב באופן מתמשך אחר התפתחות הוירוסים כדי לייצר חתימה שלהם, ועל ידי כך להפיץ עדכונים ללקוחות כדי לאפשר להם לעדכן במהירות האפשרית את המערכות שבהן מותקנות תוכנות ההגנה שמתבססות על חתימות אלה. ההתפתחות הנרחבת בפיתוח וירוסים ופוגענים שונים וגידול עצום במספרם גרמה וגורמת לתהליך בלתי־אפשרי, המחייב השקעה של משאבים רבים בעדכון מתמשך של מאגרי נתוני החתימות של תוכנות אנטי־וירוס.

ניתן לחלק את סיכוני מתקפות סייבר באופן גס למשפחות הבאות: נוזקות, רוגלות, תולעים וסוסים טרויאניים (הפותחים 'דלתות אחוריות'[3]). חלוקה המתייחסת יותר למושא התקיפה כוללת: התקפות מתמשכות מתקדמות (Advanced Persistent Threats or APTs), שהחלו במתקפות סייבר של מדינות נגד רשתות צבאיות וארגוני ממשלה, ובשנים האחרונות התפתחו לתקיפה בעוצמה מדינתית של רשת ארגונית או תשתית קריטית אזרחית, ותקיפות של מערכות בקרה תעשייתיות המופעלות על ידי מחשבים (SCADA), כגון סטקסנט (Stuxnet). כך, מערכות של תשתיות חיוניות הנשלטות באמצעות מערכות בקרה תעשייתיות שבהן שולט פרוטוקול ה־SCADA חשופות לפגיעה העלולה להשבית את השירות החיוני, או אף לגרום נזק פיזי. נוסף לאלה – מתקפות על מערכות אלחוטיות ותחנות שידור ניידות, שימוש ברשתות חברתיות לצורכי הפצת רוגלות, נוזקות, ותקיפה של שירותי אחסון ומחשוב בענן.

מרחב התקיפה בסייבר ניתן לחלוקה הכוללת שני סוגי תקיפות שמנצלות חולשות רבות, כולל חולשות של יום־אפס:

**תקיפות כלליות (Broadcast Attacks)** – תקיפות המנסות לפגוע במחשבים ללא כל אבחנה. במסגרת תקיפות אלה ניתן למצוא גם הדבקה רחבה של סוכני תוכנה על מנת ליצור רשת שלמה של מחשבים שבויים (Botnet), וזאת כדי לגרום למחשבים אלה להפעיל מאוחר יותר פקודות עצמאיות, או למשוך פקודות מתוך שרת שליטה. כאמור לעיל, בדרך כלל, כשמידע על איומים חדשים מגיע לחברות האנטי־וירוס מזהים את חתימתם או חוקרים אותם באופן היוריסטי, וכך, באמצעות עדכונים שוטפים, ניתן להגן על המחשבים מפני תקיפות אלה. לאור קהל המטרה הנרחב, סביר להניח שהמידע על איומים כאלה יגיע במהרה לחברות הרלוונטיות ויוכנס לגרסאות עתידיות של מוצריהן. בחלק מהמקרים, מטרת תקיפה מסוג זה היא להגיע לכמות גדולה של מחשבים, למשל: עובדים (במקרה של התקפה על רשת ארגונית) או לקוחות (במקרה של התקפה על מוסד פיננסי, ניסיון לגנוב כרטיסי אשראי שבהם נעשה שימוש באינטרנט וכו'). לאחר הדבקת המחשב מותקן בו סוס טרויאני, המאפשר גניבת מידע או גישה מרחוק. תקיפות כאלה כוללות קוד זדוני מסוגים שונים, ואף קודים המשתַנים מהדבקה להדבקה, כדי להקשות את הגילוי באמצעות חתימה (וירוס רב־צורתי – Polymorphic Viruses). עדיין לא קיימת הגנה מלאה, משום שמפתחי סוסים טרויאניים בוחנים בצורה עקבית האם תוכנות האנטי־וירוס כבר זיהו את הקוד המפַגע וייצרו את החתימה או את קבוצת החוקים ההיוריסטיים המיירטת אותו. ברוב המקרים, אם מערכות הגילוי מצליחות לזהות את הקוד המפַגע, המפתחים מבצעים שינויים בדרך ההדבקה או ההפעלה שלו, כדי למנוע את הגילוי. לפיכך, קיימים סוסים טרויאניים רבים המצליחים להתחמק באופן עקבי מגילוי על ידי תוכנות ההגנה מובילות.

**תקיפות ממוקדות (Targeted Attacks)** – תקיפות אלה מתוכנתות במיוחד לצורך ספציפי ומנצלות חולשות שאינן מוכרות במערכות ההפעלה או בתוכנות מוכרות ונפוצות, תוך איתור עצמאי של חולשות חדשות. מטבע הדברים, הרוב המכריע של תוכנות האנטי־וירוס מבוסס על הגנת חתימה, הן אינן מסוגלות לזהות ולמנוע תקיפות מסוג זה, וקהל המטרה המצומצם מאפשר לתקיפות כאלה לחמוק "מתחת למכ"ם" של יצרני האנטי־וירוס. ראוי לציין שעולם האיומים מתפתח בצורה מהירה לכיוון של מתקפות ממוקדות על יעדים איכותיים.

תעבורת הנתונים ברשת תקשורת מודרנית היא רבה מאוד, בשל הצורך לספק שירותים רבים לתחנות קצה מסוגים שונים, ביניהן: מחשבים אישיים, תחנות עבודה, שרתים, מתגים וציוד תקשורת, ועוד יחידות רבות ומגוונות. באלה עושים שימוש משתמשים רבים, שברובם הגדול אינם בעלי גישת אבטחה כלשהי. כתוצאה מתופעה זו, התקפות APT מתמקדות לא רק במכונות אלא גם באנשים, לדוגמה: דרך השימוש ברשתות חברתיות. כך למשל, ההתקפה על חברת RSA שכוונה

לאנשים בארגון, והצליחה לחדור למערכות מאובטחות ביותר.[4] בשנים האחרונות אנו עדים לעלייה דרמטית בהיקף של התקפות חדשות מתוחכמות ולא מתועדות, בעלות אופי חמקני. הדבר מתבטא הן בקבוצת התקיפות הכלליות והן באלה הממוקדות. התקפות אלה מתגברות על כל ההגנות הקלאסיות והתקניות של החברות המובילות את תחום ההגנה כיום. מאחורי פיתוח אמצעי התקיפה עומדות השקעות בקנה־מידה גדול של מדינות ושל ארגוני פשיעה, כשהיקף הנזקים הוא רחב מאוד.[5] למעשה, קיימת עלייה עצומה בכמות הפוגענים המצליחים לחדור את כל מערכות ההגנה הקיימות, והמתגברים על כל ההגנות הקלאסיות המתבססות על חתימות וחוקים. העלייה הינה במאות אחוזים משנת 2011 עד ימים אלה.[6]

מערכות ההגנה הקיימות כיום מתבססות בעיקר על מניעה וסיכול של איומים מוכרים, תוך שימוש בחתימות ובחוקים ידועים מראש. מערכות אלה אינן יכולות לגלות מתקפות יום־אפס שאין להן חתימה ידועה ברגע נתון. כך גם מתקשות המערכות הללו לזהות סוסים טרויאניים ודלתות אחוריות, כשלהתקפות מתוחכמות וחמקניות רבות אין חתימות ידועות. הם חודרים כמעט לכל מערכת מחשוב משום שהם נראים כנתונים וקודים חוקיים ואינם נראים פוגעניים. תקיפות מצליחות לחדור לרשתות הארגוניות ולמחשבי הקצה למרות כל מערכות ההגנה, בשל העובדה כי ההופעה וההתנהגות הראשונית של הפוגענים נראית חוקית ותקינה. נוסף לכך, רוב המערכות המבצעיות כיום בנויות לטיפול בסוג מסוים של התקפה, ואין להן יכולת לטפל במגוון גדול של התקפות שונות בעלות מוטציות וגרורות.

אחת הדרכים לאתר תקיפות שאינן מוכרות ושאינן חתומות באמצעות תוכנות ההגנה המקובלות היא על ידי זיהוי התנהגות א־נורמלית של קודים שוהים במערכות הארגוניות, השונה מההתנהגות נורמלית של מרבית הנתונים. התנהגות שונה זו תסגיר את הקודים הזדוניים. בגישה זו, התנהגות לא־רגילה של רכיב תוכנה המנסה לבצע פעילות שאינה מורשית יכולה להוות בסיס אפשרי לזיהוי ולמניעת מתקפות. יצרני תוכנות ההגנה בעולם מבינים את האתגר ופועלים כדי לספק יכולות זיהוי כאלה. אולם, כאן טמון האתגר המשמעותי ביותר – הקושי לספק כלי אמין שלא יפיק התרעות שווא ושלא יפגע בצורה משמעותית בחוויית המשתמש. התרעות השווא הנן אחד האתגרים המשמעותיים ביותר של מערכות הגנה. התרעת שווא נוצרת כאשר המערכת מתריעה על קוד חוקי שהתנהגותו נורמלית, ומגדירה אותו כקוד זדוני או כחשוד ככזה. עומס רב מדי של התרעות שווא כאלה פוגע בצורה מהותית ביכולת העבודה במערכות המחשוב, ועלול לגרום למשתמשים לאבד את האמון במערכת ההגנה. אתגר שני הוא המענה לקוד זדוני החומק ממערכת ההגנה. תופעה זו קרויה false negative – כאשר מתקבלת תוצאה הנראית שלילית, אך למעשה היא חיובית. (בדומה לנשא נגיף של מחלה

חמורה, המקבל תוצאות בדיקת מעבדה שליליות באשר לנוכחות הנגיף בגופו). שני אתגרים אלה הנם ליבת העיסוק בתחום מערכות ההגנה בכלל, ובתחום השימוש בניתוח התנהגות אנומלית של קוד זדוני במערכות מידע בפרט.

## זיהוי אנומליות כגישה למענה אופרטיבי

מאמר זה יתרכז בדיון על הגנה המבוססת על איתור אנומליות ברשתות תקשורת, ברבדיה השונים. הבעיה רחבה יותר וכוללת את הצורך בזיהוי אנומליות של קודים זדוניים שהוחדרו בנקודות תורפה בתוכנות וביישומים (applications). גישת הגנה זו אינה נדונה במאמר זה, אלא אם כן, הקוד הזדוני נחשף בתקשורת הארגונית. למרות האמור לעיל, ניתן להניח שחלק מהרעיונות המוזכרים מתאימים גם למציאת אנומליות בתוכנות וביישומים.

אנומליות שהוצעו לראשונה בשנת 1987[7] הן סטיות מההתנהגות המצופה, שהיא ההתנהגות הנורמלית. ההנחה הבסיסית עבור כל מערכת למציאת אנומליות היא שלנתונים זדוניים (malicious) יש מאפיינים שאינם קיימים בהתנהגות הנורמלית שאופיינה בזמן הלמידה. מאז פותחו תיאוריות ומתודולוגיות נוספות המתבססות על גישות של למידת מכונה (Machine Learning) ועל תורת האינפורמציה[8] כגון רשתות עצביות,[9] מכונת וקטורים תומכים (support vector machine),[10] אלגוריתמים גנטיים[11] ועוד רבים אחרים. כמו כן קיימות גישות רבות העושות שימוש בכריית נתונים לשם מציאת קוד זדוני.[12] סקירה כללית על איתור אנומליות מובאת במאמרם של Chandola & Banerjee[13], וכן מובא מחקר על שיטות לאיתור קוד זדוני.[14]

אחת הגישות לאיתור התקפות על נתונים מרשתות תקשורת נעשית באמצעות ניטור (monitoring) האנומליות של הפעילות הרשתית, על ידי מציאת הסטייה מפרופיל נורמלי שנלמד מנתונים שפירים (תקינים, לא־פוגעניים). מתודולוגיה זו מתבססת על כלים שנלקחו ממחקרים על למידת מכונה,[15] אנליזה מתמטית וסטוכַסטית[16], סטטיסטיקה, כריית נתונים, תורת הגרפים, תורת האינפורמציה, גיאומטריה, תורת ההסתברות ותהליכים אקראיים, ועוד. כלים של למידת מכונה וכריית נתונים בשילוב המתודולוגיות שהוזכרו משמשים בהצלחה בתחומים רבים אחרים כמו מערכות להמלצת מוצרים של Amazon,[17] Netflix,[18] זיהוי תווים אופטי,[19,20] תרגום של שפה טבעית,[21] זיהוי דוא"ל זבל (spam).[22] למידת מכונה עוסקת בפיתוח אלגוריתמים שיאפשרו למחשב ללמוד על סמך דוגמאות. קיימת למידה מונחית של נתונים ידועים מראש (supervised), שבה יודעים מראש את המשמעויות הנכונות של הפרמטרים, כלומר, לנתונים יש תוויות סיווג (labeled); בלמידה בלתי־מונחית (unsupervised) מטרת האלגוריתמים היא למצוא ייצוג

פשוט של הנתונים, ללא תוויות סיווג. למידה מונחית מוגבלת יותר מבחינת תכולת הנתונים הנלמדים, אבל מצד שני, התוצאות אמינות יותר ולכן היא עדיפה.

הלמידה הראשונית נעשית על קבוצת נתונים "בריאה", שניתן להניח שאין בה פוגענים כלשהם. קבוצה זו נקראת קבוצת הלימוד (training set). רצוי בדרך כלל ששיטת הלמידה תדע לאבחן האם חלק מקבוצת הלימוד כולל פוגענים עד אחוז מסוים מסך־כל הנתונים. ברור שאם רוב קבוצת הלימוד מכיל פוגענים, אזי הם יילָמדו ויזוהו כנתונים נורמליים. כחלק מתהליך הסינון מופעל לעיתים תהליך הנקרא 'הסרת חריג החשוד כחריג' (outlier removal), שמוציא מקבוצת הלימוד נתונים הנראים כרעשים או זיהום.

קבוצת הלימוד מנותחת על ידי מגוון שיטות מתמטיות קיימות, לצד שיטות חדשניות. באמצעות תהליך זה ניתן לאתר את המאפיינים הנורמליים של הנתונים הנבחנים. למידה מסוג זה נקראת One Class. לעומתה קיימת שיטה שבה המאפיינים נלמדים על ידי השוואת קבוצת לימוד המכילה נתונים נקיים ולא־נקיים (לדוגמה: דוא"ל עם או בלי ספאם), הנקראת Binary Class. קבוצת הלימוד נגזרת מתוך מסת הנתונים הנצברת והנשמרת בארגון יחד עם נתונים חדשים הנשמרים באופן שוטף. למטרה זו פותחו שיטות ללמידת הנתונים המאפיינים את ההתנהגות הנורמלית. הבנת הגיאומטריה[21] של הנתונים הנלמדים היא אחת משיטות הניתוח, אולם קיימות שיטות נוספות. לדוגמה: בתהליך המתואר להלן מתואר מבנה כללי אפשרי של אלגוריתמים המופעלים והמעבדים את קבוצת הלימוד, במטרה למצוא את המאפיינים של ההתנהגות הנורמלית (התקינה):

1. פירוק כל יחידת נתונים בסיסית של תקשורת או אירוע למאפיינים (features, parameters).
2. כימות היחסים בין המאפיינים. קיימות מספר שיטות לאפיון היחסים הללו. שיטת גרעין (kernel Method)[23] היא אחת מהמתודולוגיות הנפוצות שבעזרתה מגדירים יחסים בין המאפיינים. בדרך כלל נעשה שימוש בפונקציות מרחק מתמטיות להגדרת היחסים הללו. אלה הם יחסי קִרבה וריחוק שמגוון תכונות מקיימות ביניהן. לאחר שלב זה נשמרים היחסים שבין נתוני התקשורת או האירועים.
3. הורדת ממד (dimension) הנתונים. בדרך כלל ממד הנתונים גבוה והוא נקבע לפי כמות המאפיינים שמרכיבים יחידת תקשורת בסיסית או יחידת אירוע בסיסית. לכן מורידים את ממד הנתונים[22] (לדוגמה, מעשרה מימדים לשניים) תוך שימור היחסים והקוהרנטיות בין המאפיינים שאותרו בשלב הקודם. הדבר דומה לפעולת דגימה שבה בוחרים בצורה מושכלת רק חלק קטן מהנתונים המקוריים, שמייצגים אותם בצורה נאמנה. נדרשת חדשנות מתמטית, אלגוריתמית וחישובית כדי לעבד נתונים מממד גבוה שיתאימו למחשב ושייצגו בצורה טובה

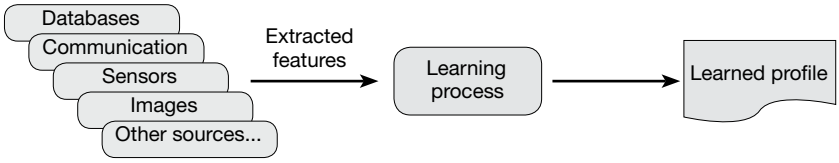
ומהימנה את נתוני המקור. הדגימה שמטרתה לצמצם את נפח הנתונים יכולה להיות אקראית, וניתן להוכיח שהיא משמרת את הקוהרנטיות של הנתונים. לשם כך יש שיטות מתמטיות רבות. אחת השיטות לייעול החישובים כדי לבנות מייצג קומפקטי של נתונים רבי־ממדים היא בניית מילונים (dictionaries),[24] שגורמים להאצה בחישובים תוך שימור היחסים והתכונות שאותרו לפני הורדת הממד. שיטות אחרות להאצת החישובים מאפשרות דילול (sparsification) של הנתונים[24,25] מטרת הגישות הללו היא אפיון הפרופיל הנורמלי של הנתונים מתוך קבוצת הלימוד, תוך התגברות על הבעיות החישוביות הכבדות בעיבוד קבוצת הלימוד. פעולת הלמידה היא בדרך כלל כבדה מבחינה חישובית. פעולה זו נעשית ברקע (offline) ואינה נדרשת לפעול בזמן אמת. שיטות נפוצות הנן: PCE,[25] LLE,[26] ISOMAP,[27] ועוד.

השיטות שתוארו לעיל מאפשרות לעבד ביעילות את קבוצת הלימוד שהיא "כבדה" ואף עלולה להיות בלתי־אפשרית מבחינה חישובית. מטרת עיבוד קבוצת הלימוד היא לאפיין את ההתנהגות הרגילה (הנורמלית) של נתוני הלימוד על סמך הבחינה של קבוצת הלימוד ועל בסיס היחסים שהוגדרו בין המאפיינים של הנתונים והאירועים של קבוצת הלימוד, בהנחה שהלמידה והמסקנות ממנה ישקפו את ההתנהגות הנורמלית של כל הנתונים החדשים העתידיים, שלא היו חלק מקבוצת הלימוד. ככל שנפח הנתונים של קבוצת הלימוד גדול יותר והמאפיינים רבים ומגוונים יותר, מאפייני ההתנהגות הנורמלית שהוסקו מקבוצת הלימוד יהיו אמינים יותר. אבל אז הסיבוכיות החישובית עולה, ולכן צריך להשקיע מאמץ רב בייצור אלגוריתמים שהם יעילים מבחינה חישובית ויכולים לטפל בנפחי נתונים גדולים.

התהליך המתואר מפרט מודל למידה אפשרי המייצר אפיון של ההתנהגות הנורמלית של הנתונים העתידיים בעזרת הפרופיל הנורמלי של קבוצת הלימוד. מכאן ואילך בודקים את המאפיינים של כל נתון חדש שמגיע או של אירוע חדש. מעבדים את המאפיינים הללו כדי לראות האם הם סוטים מהפרופיל הנורמלי שנלמד ונקבע בזמן הלימוד (אנומליה). הסטיות מהפרופיל הנורמלי צריכות לאתר את המתקפות המאופיינות כמתקפות יום־אפס. בשיטה שתוארה עד כה לא משתמשים בחתימות אלא במציאת סטיות התנהגותיות מהפרופיל הנורמלי שנוצר מעיבוד קבוצת הלימוד.

תרשים 1 הוא תיאור של תהליך הלמידה שתואר לעיל. התרשים מראה גם את מגוון המקורות שמהם נשאב המידע לצורכי הלימוד הראשוני.

**תרשים1: תהליך הלמידה**




השיטות הללו ונגזרותיהן למציאת פוגענים על ידי ניטור ההתנהגות של הנתונים ניתנות להפעלה בשני אופנים שונים, המשלימים זה את זה באופן השימוש בהם, כשהמשותף הוא למידה ברקע (offline) של נתוני התקשורת מהפרוטוקול שדרכו מגיעים הנתונים לארגון (כמו למשל: port 443 (HTTPS), UDP port 53 (DNS) ,TCP port 80 (HTTP), TCP שהם גם פרוטוקלי web), ובניית הפרופיל שמתאר את ההתנהגות הנורמלית של נתוני הפרוטוקול המסוים שאותו יש לבדוק, על פי קבוצת הלימוד.[28]

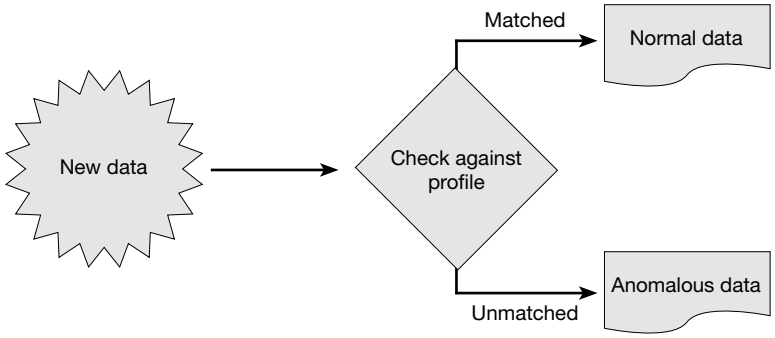
1. **הפעלה בזמן אמת** – האלגוריתם למציאת אנומליות בנתוני תקשורת (ממומש בתוכנה או בחומרה) ממוקם בכניסה לארגון, אחרי שעבר את כלי ההגנה הרגילים של IDS, IPS FireWalls (חתימות וחוקים אֶפשרו לו להיכנס), ואז הוא בודק כל יחידת תקשורת – האם התנהגותה מתאימה לפרופיל הנורמלי שנלמד מקבוצת הלימוד. אם הוא התגלה כאנומליה, דרכו לתוך הארגון נחסמת. היות שלא משתמשים בחתימות, הניתוח של מהות האנומליה ייעשה אוטומטית או ידנית.
2. **הפעלה ברקע** – מציאת פוגענים ברקע. נתוני התקשורת שנכנסו לארגון דרך כל מערכות ההגנה נראים כנתונים חוקיים ומתחילים לפעול לאחר מכן, כמו רשת מרגלים שנטמעים בסביבה ומתחילים לפעול בזמנים עתידיים. לצורך כך יש לעבד לוגים ואירועים שהתרחשו בעבר ומתרחשים כעת. כדי לעבד מידע של לוגים שנשמרו וחדשים שמגיעים משתמשים כיום בטכנולוגיית Security Information and Event Management (SIEM). SIEM היא מערכת ניטור אבטחת מידע נפוצה ברשתות ארגוניות, ומשמשת כמקום מרכזי לשמירה ולפענוח של לוגים ואירועים של נתוני התקשורת. SIEM היא הארכיון של כל נתוני התקשורת והאירועים, ובעזרתה אפשר לבצע ניתוחים "משפטיים" (forensic) למציאת אנומליות.

ניתן להפעיל את השיטות למציאת אנומליות שתוארו במאמר על הנתונים ש־SIEM אספה. אפשר להפעיל גם כלי כריית נתונים אחרים על נתוני ה־SIEM. ל־SIEM יש שתי פונקציות (מרכיבים) עבור ניהול הביטחון: Security information management (SIM) ו־Security event management (SEM). בשיטה שעושה

שימוש בנתונים של SIEM צריך להפעיל בהתמדה את המתודולוגיה למציאת אנומליות כדי לאתר את פעולתם של הפוגענים, כאשר יפעלו במועד עתידי כלשהו.

תרשים 2 מתאר תהליכים לבדיקת המידע לאור תוצאות ניתוח הלמידה.

**תרשים 2: תהליך הזיהוי**




## שימוש ב BIG-DATA למציאת אנומליות – הנתונים והאירועים מכתיבים את אופן הזיהוי

הרעיון המרכזי בבסיס מציאת האנומליות כפי שתואר לעיל הוא אפיון ההתנהגות של הנתונים בקבוצת הלימוד, והסקה מהם על התנהגות הנתונים שלא השתתפו בקבוצת הלימוד, כלומר, אפיון הנתונים החדשים שיגיעו. במילים אחרות, הנתונים מכתיבים את העיבוד, והדבר מתבטא באלגוריתמים שמכוונים ללמוד את הנתונים כפי שהם ולהסתגל אליהם. זאת בניגוד לכל ההגנות מפני פוגענים הקיימות כיום, שאין להן שום קשר להתנהגות הנתונים, אלא הן מחפשות דפוסים (patterns) של פוגענים ידועים זה כבר. במקרה של נתוני תקשורת, מנתחים את הנתונים מכל יחידת אינפורמציה של הפרוטוקול שאותו מנטרים. מוצאים את היחסים ביניהם על סמך שיטות גרעין ומשכנים אותם באופן לא־לינארי במרחבים עם ממד נמוך יותר. כך מורידים את ממד הנתונים שבדרך כלל הוא גבוה, והדבר מאפשר למצוא אנומליות באופן יעיל.

הנתונים שבהם נחפש אנומליות הם נתונים שמכונים כיום BIG-DATA. אלה נתונים בהיקף עצום הנאספים מכלל מקורות המידע הזמינים ברשת הארגונית. בארגונים רבים הם נשמרים על ידי מתודולוגיית SIEM. לפי אריק שמידט, מנהלה־לשעבר של גוגל, כמות נתונים של חמישה אקסה־בייט (Exabyte) [29] נוצרו משחר הציוויליזציה ועד שנת 2003. לטענתו של שמידט, כמות זו נוצרת עתה כל יומיים.

להלן מספר דוגמאות ליצירה של BIG-DATA: הבורסה של ניו יורק (NYSE) מייצרת מדי יום 1TB של נתונים, Facebook מייצר כל יום 20TB של נתונים דחוסים והמאיץ ב־CERN שבשווייץ מייצר מדי יום 40TB של נתונים. לפי דוח שפורסם[30], נפח הנתונים גדֵל פי שניים מדֵי שנה, ולפחות מחצית מן העסקים שומרים את הנתונים במשך שלוש שנים לפחות, לצרכים אנליטיים. חלקם מחויבים לפי חוק לשמור נתונים אלה במשך מספר שנים. מקורות חדשים בכמויות עצומות צצים כל הזמן בעסקים שונים כמו שירותים (utilities). חלק ניכר (80%) מנתונים אלה אינם מובְנים (unstructured), ולכן אינם ניתנים לשימוש יעיל בארגון. BIG-DATA הפך מקור לכריית מידע המאפשר לאתר פוגענים. לחברות רבות וידועות יש BIG-DATA יומיומי, כמו Facebook, Google, Amazon, LiveJournal, Wikipedia וזו רשימה חלקית מאוד. BIG-DATA נשמר כיום גם בענן. כמות הנתונים שנאגרת בכל ארגון היא עצומה ואף גדֵלה עם הזמן. כדי לטפל בנפחי נתונים גדולים (data silos) פותחו כלים לעיבוד BIG DATA שאינם קשורים לכריית נתונים או למציאת אנומליות כגון Hadoop[31], MapReduce[32] ו־Memcached[33,34] – מסדי נתונים מקביליים[35] עצומים שמאפשרים לבצע שאילתות מהירות עליהם. בנוסף מפתחים "צינורות" תקשורת רבים (חברת Mellanox) להעברה מהירה של כמויות הנתונים הללו. מאמץ רב מושקע בפיתוח כלים מתקדמים לעיבוד יעיל של BIG-DATA. לכן, הוא יכול להיות מקור למציאת קשת נרחבת של אנומליות התנהגותיות מתוחכמות של פוגענים שונים.

## סיכום

כדי לעבד BIG-DATA ולאתר פוגענים "איכותיים" ביעילות, יש לשלב בין כל השיטות שהוזכרו לעיל. הוזכרו כלים שרובם לא־לינאריים, המצמצמים את הנפח של BIG-DATA שהוא רב־ממדי בלי לפגוע בקוהרנטיות של הנתונים, תוך הקפדה על יעילותם של האלגוריתמים, כדי לטפל בנפחי נתונים עצומים. צירוף השיטות שהזכרנו במאמר זה הוא: ביצוע למידה מתוך קבוצה קטנה של נתונים, הפעלת שיטת גרעין על הנתונים שקובעת את היחסים (המרחקים) בין נקודת הדגימה, הורדת ממד הנתונים על ידי דגימה בדידה או אקראית של הנתונים. הדבר מדלל את הנתונים וכך מקבלים "שיכון" יעיל של BIG-DATA רב־ממדי במרחב עם ממד נמוך יותר משמעותית, ובו מבצעים את זיהוי האנומליות. בניית מילונים והפעלה של אלגוריתמים חכמים ויעילים, יחד עם כלים לעיבוד BIG-DATA – כל אלה פותחים אפשרויות רבות למציאת פוגענים בכל ארגון, על ידי אפיון ההתנהגות הנורמלית ואיתור סטיות ממנה.

הגישה המוצעת היא שילוב בין אנליזה של BIG-DATA בעלת יעילות חישובית גבוהה וכלים מתקדמים למציאת אנומליות שהן הפוגענים של מתקפות יום־אפס

שאין להם עדיין חתימות ודפוסי התנהגות ידועים. המתודולוגיה שנדונה כאן חייבת למצוא "סיכה" באוקיינוס של נתונים.[36] נקודת המוצא היא שהאלגוריתמים המוצעים מתאימים את עצמם ומסתגלים לנתונים עצמם. הנתונים הם שמכתיבים את אופן פעולת האלגוריתמים. המתודולוגיה המוצעת במאמר משלבת הבנת מבנה הנתונים על ידי למידה מתוך קבוצה קטנה, והסקת מסקנות לגבי ההתנהגות העתידית של הנתונים שלא השתתפו בקבוצת הלימוד. מתודולוגיה זו מסוגלת לאתר פוגענים שפעילותם מיידית, וכאלה שנכנסו לארגון ופועלים מאוחר יותר כמו סוסים טרויאניים.

## הערות

1 באופן היוריסטי הנו באמצעות חוקים המסייעים לגילוי הקוד המפַגע.

2 התנהגות אנומלית של קוד תוכנה או מידע הנה התנהגות לא־רגילה (לא־אופיינית), המעלה חשד לקיומו של פוגען במערכת.

3 פרצת אבטחה המאפשרת גישה למחשב ללא צורך באימות זהות. יכולה לנבוע משגיאת תכנות, מפרצה מכוונת בקוד מקור או כתוצאה מהתקנת תוכנה ייעודית (כגון סוס טרויאני).

4 Gabi Siboni and Y. R., "What Lies behind Chinese Cyber Warfare", *Military and Strategic Affairs*, Volume 4, No. 2, (September 2012), pp. 43-56.

5 Symantec, "Internet Security Threat Report 2011" *Trends, Vol. 17*, April 2012.

6 *FireEye Advanced Threat Report - 1H*, 2012. http://www2.fireeye.com/advanced-threat-report-1h2012.html

7 D.E., Denning, "An Intrusion-Detection Model, IEEE Trans*", Software Eng.,* Vol. SE-13 (2), 1987, pp. 222-232.

8 W. Lee and D. Xiang, "Information-Theoretic Measures for Anomaly Detection", in *Proc. IEEE Symposium on Security and Privacy*, 2001.

9 Z. Zhang, J. Li, C. Manikopoulos, J. Jorgenson, and J. Ucles," HIDE: a Hierarchical Network Intrusion Detection System Using Statistical Preprocessing and Neural Network Classification", in *Proc. IEEE Workshop on Information Assurance and Security*, 2001.

10 W. Hu, Y. Liao, and V. R. Vemuri, "Robust Anomaly Detection Using Support Vector Machines", in *Proc. International Conference on Machine Learning*, 2003.

11 C. Sinclair, L. Pierce, and S. Matzner, "An Application of Machine Learning to Network Intrusion Detection", in *Proc. Computer Security Applications Conference*, 1999.

12 M. A. Siddiqui, *Data mining methods for malware detection*, PhD Dissertation, University of Central Florida, 2008.

13 V. Chandola, A. Banerjee, V. Kumar, "Anomaly detection: A survey", *ACM Computing Surveys (CSUR)*, 41(3), article 15, 2009.

14 N. Idika, A.P. Mathur, *A survey of malware detection techniques*, Dept. of Computer Science, Purdue University, 2007.

15 R. Sommer and V. Paxson, "Outside the Closed World: On Using Machine Learning For Network Intrusion Detection", *Proc. IEEE Symposium on Security and Privacy*, May 2010.

16 תהליכים סטוכסטיים הם תהליכים שבהתפתחות שלהם במשך הזמן מעורבת מידה מסוימת של אקראיות בכל רגע נתון.

17 G. Linden, B. Smith, and J. York, "Amazon.com Recommendations: Item-to-Item Collaborative Filtering", *IEEE Internet Computing*, vol. 7, no. 1, pp. 76–80, 2003.

18 J. Bennett, S. Lanning, and N. Netflix, "The Netflix Prize", in *Proc. KDD Cup and Workshop*, 2007.

19 L. Vincent, Google Book Search: "Document Understanding on a Massive Scale", 2007.

20 R. Smith, "An Overview of the Tesseract OCR Engine", in *Proc. International Conference on Document Analysis and Recognition*, 2007.

21 F.J. Och and H. Ney, "The Alignment Template Approach to Statistical Machine Translation", *Comput. Linguist.*, vol. 30, no. 4, pp. 417–449, 2004.

22 P. Graham, "A Plan for Spam", in *Hackers & Painters*, O'Reilly, 2004.

23 B. Scholkopf and A. J. Smola, *Learning with Kernels: Support Vector Machines, regularization, Optimization, and Beyond*, The MIT Press, 2002.

24 M. Elad, "Sparse Redundant Representations", From *Theory to Applications*, Springer, 2010.

25 I.T. Jolliffe, *Principal Component Analysis*, Springer, New York, 1986.

26 S.T. Rowels, L.K. Saul, "Nonlinear dimensionality reduction by locally linear embedding", *Science*, Vol. 290 no. 5500 pp. 2323-2326, (2000).

27 J.B. Tenenbaum, V. de Silva and J.C. Langford, "A global geometric framework for nonlinear dimensionality reduction", *Science*, Vol. 290 no. 5500 pp. 2319-2323, (2000).

28 גישה זו מאפשרת גם בקרת ביצועים, ניתוח התנהגות משתמשים, ניתוח יחסי אדם־מכונה ובקרת תהליכים.

29 Exabyte = billion billion bytes

30 http://techcrunch.com/2010/08/04/schmidt-data/

31 http://hadoop.apache.org

32 J. Dean and S. Ghemawat. *MapReduce: Simplified Data Processing on Large Clusters*, *OSDI*, 2004.

33 L. Gavish, *New Caching policies for MEMCACHED*, M.Sc Thesis, Tel Aviv University, 2012.

34 B. Fitzpatrick. "Distributed caching with memcached", *Linux Journal*, 2004, http://hadapt.com/

35 M. Baker, D. Turnbull, G. Kaszuba, "Finding Needles in Haystacks (the Size of Countries)" *Blackhat*, Amsterdam, Netherlands, March 14-16, 2012.

# תפוצת נשק קיברנטי במרחב הסייבר

## דניאל כהן ואביב רוטברט

### מבוא

מרחב הסייבר הינו תופעה שעיקרה ניצול השדה האלקטרומגנטי לצרכים אנושיים באמצעות טכנולוגיה. במאמר זה ייטען כי טכנולוגיה זו היא סוג של נשק. ההגדרה המילונית המסורתית לנשק היא "שם כולל לכלים שהאדם משתמש בהם כדי להכריע את האויב".[1] "נשק קיברנטי" הוא, לפיכך, נשק המאפשר פגיעה שמטרתה להכריע את האויב באמצעות פגיעה במערכות המקושרות למרחב הקיברנטי. נשק קיברנטי ניתן להפעלה כנשק אל־הרג, וכולל את היכולת לגרום הרס רב ופגיעה קשה בתפקוד, בלי להחריב תשתיות פיזיות או לקטול חיי אדם. הסביבה האסטרטגית־קיברנטית כוללת שימוש בנשק קיברנטי לפעולות חדירה למערכות האויב לצורך ריגול, לוחמה פסיכולוגית, הרתעה, נזק למערכות תקשוב או ליעדים פיזיים.

יש להבחין בין יכולת התקפית רחבה וממושכת על יעדים אסטרטגיים ובעלי יכולת הגנה גבוהה, לבין התקפה שעלולה לגרום נזקים מקומיים או זמניים. יכולת תקיפה מהסוג הראשון שמורה לעת עתה בידי מספר מצומצם של מדינות, ונדרשים לה משאבים גדולים. לעומת זאת, ליכולת מהסוג השני נדרשת עלות נמוכה, ולכן כבר כיום ניתן לראות סימנים לייצור נשק המוני אשר זמין גם בשוק החופשי, ונמצא בשימוש של ארגוני טרור ופשע.

לוחמה קיברנטית הופכת להיות אחד מדפוסי הפעולה ההתקפיים בשימושן של מדינות המבקשות להגן על האינטרסים שלהן מפני מדינות או ארגונים עוינים. יעידו על כך התקפות הסייבר האחרונות שהתפרסמו בתקשורת, כגון המתקפה המיוחסת לאיראן על חברות נפט במפרץ הפרסי ועל בנקים אמריקאיים, ומנגד, התקפות המיוחסות לארצות־הברית ולישראל נגד מתקני הגרעין של איראן.[2] למציאות זו מספר סיבות, וביניהן: היכולת לבצע מתקפה ממוקדת, יכולתו של

דניאל כהן הוא מתאם תכניות לוחמת סייבר וצבא ואסטרטגיה במכון למחקרי ביטחון לאומי
אביב רוטברט הוא תלמיד לתואר שלישי, מלגאי בתכנית ניובאוור במכון למחקרי ביטחון לאומי

התוקף להסוות את עצמו והיכולת של הקורבן להסתיר את אירוע התקיפה, ובכך להימנע מההכרח לתקוף חזרה. מרחב הסייבר מאפשר למדינות בעלות משאבים ויכולות טכנולוגיות גבוהות להשתמש בארסנל נשק לצורכי תקיפות סייבר. מנגד, מדינות חסרות משאבים יכולות גם הן להצטייד בנשק התקפי ולפעול במרחב הסייבר, אם כי בהיקף מצומצם ובעל פוטנציאל נזק מועט יותר.

תופעה ייחודית במרחב הסייבר שאינה נמצאת במרחבי לחימה אחרים היא היכולת הגבוהה להתגונן מפני וירוסים או קוד זדוני[3] אחר, כאשר נעשה בו כבר שימוש בעבר והוא התגלה על ידי גופי אבטחה.[4] לכאורה, נשק סייבר עשוי להיות חד־פעמי ולהפוך חסר תועלת ברגע שזוהה ונחתם.[5]

אך האם כל שנות־האדם שהושקעו בפיתוח קודים זדוניים מתוחכמים יורדות לטמיון ברגע אחד, כאשר ההתקפה מתגלה ונחתמת?

מאמר זה ינסה להראות כי לא כך הם פני הדברים. עם התגברות התקיפות במרחב הסייבר, יגברו תפוצת הכלים ויכולות הסייבר בעולם. אחת הסיבות העיקריות לכך היא שניתן לעשות שימוש בנשק סייבר, כדוגמת קוד זדוני ששימש לתקיפה אחת, גם בתקיפות אחרות, וזאת לאחר הסבתו. בהשאלה מעולם הביולוגיה, קוד זה יכונה "קוד מוטציה". הוא בעל מאפיינים פונקציונליים דומים (עד כדי זהות מוחלטת) לקוד האב שממנו הוא נוצר. ההבדל בין קוד האב לקוד המוטציה הוא סינטַקטי (מִבני) בלבד ולא סמנטי, במטרה לחמוק מהרדאר של תוכנות לזיהוי פוגענים.

מכך ניתן להסיק כי נפילת קוד זדוני לידי יריב בעל מוטיבציה ויכולת נותנת לצד המותקף נשק שב"חימוש" מתאים, תוך ביצוע פעולות מורכבות כגון הנדסה לאחור (Reverse Engineering),[6] יכול להיות מנוצל לשימוש רב־פעמי. כמו כן, שימוש יעיל יכול להיעשות על ידי תוקף שמכיר את הנשק ויכול לשנות אותו על פי צרכיו לביצוע מתקפות נוספות.

אנו מצויים בעיצומה של מלחמת סייבר שקטה, שפרטים מעטים מאוד ממנה דולפים לתקשורת, אך העמימות אינה יכולה להישמר לנצח. נתבונן לדוגמה בהתפתחות של תחום כלי־הטיס הבלתי־מאוישים (כטב"ם). בימיו הראשונים היה התחום עטוף במעטה חשאיות. היכולת להפעיל כלי־טיס בלתי־מאויש למטרת ריגול ובהמשך לתקיפה הייתה נתונה בידיהן של מדינות מעטות, ואלו עשו שימוש מחושב וזהיר בטכנולוגיה, על מנת שלא לחשוף אותה לעיני היריב. עם התגברות השימוש בכלים בלתי־מאוישים נפרצה חומת העמימות, וכיום ניתן למצוא תיאורים מפורטים בתקשורת על המדינות שעושות שימוש בכלי־טיס אלה, על המטרות שהיו נתונות לתקיפות מן הסוג הזה, על היכולות והמגבלות של כלים כאלה, ועוד. גם ארגוני הטרור למדו היטב את כלי הנשק החדש־ישן שהופעל נגדם בהצלחה על ידי מדינות, ופיתחו דרכים להתגונן מפניו. תוצאה נוספת של השימוש הנרחב

בכטב"מים והחשיפה התקשורתית שבאה בעקבותיו היא פתיחה של מרוץ חימוש, שגרם למדינות רבות לנסות להיכנס ל"מועדון היוקרתי" של אלה המחזיקים בנשק זה לצורכי ריגול ותקיפה.[7] גם מדינות תומכות טרור נכנסו למרוץ,[8] וארגוני טרור הפועלים בחסותן של מדינות אלו נהנו גם הם מ"פירות ההשקעה": איראן השיגה יכולת הפעלת כלי־טיס בלתי־מאוישים, ולא עבר זמן רב עד שיכולת זו מצאה את דרכה אל ארגוני הטרור חמאס וחזבאללה.

היכולת לבצע מתקפה במרחב הסייבר לשיבוש מערכות בקרה תעשייתיות ויצירת הרס פיזי (כפי שנעשה בהחדרת וירוס 'סטקסנט' ויצירת נזק למערכות הסַרְפָּזוֹת בפּוּרים גרעיניים באיראן) היא יכולת שיש כיום, על פי ההערכות, למספר מצומצם של מדינות, ומדינות רבות נוספות חותרות להשגתה. בכך יש למעשה תהליך התחמשות בנשק לחימה מסוג חדש, המאפשר פגיעה והרס ממרחק רב.

יכולת לבצע מתקפה שתפגע בתהליך התעשייתי אינה מורכבת מדַי, וגורמי בקרה והנדסה יכולים לבצעה. לעומת זאת, כדי להבין ולנתח לעומק את התהליך התעשייתי במטרה המותקפת, יש צורך ביכולות מודיעין ויכולות החדרה ברמה מדינתית גבוהה.

גם שחקנים לא־מדינתיים במרחב הסייבר, ובראשם ארגוני פשע וטרור, עלולים לעשות שימוש או שכבר עשו שימוש בעבר בווריאציות של קודים זדוניים קיימים והסבתם לצורכי הארגון. כך קרה במקרה ב־2012, כאשר ארגוני פשע השתמשו בווירוסים קיימים ומוכרים בשם Zeus ו־SpyEye, שבהם ערכו שינויים משלהם, והצליחו בעזרתם למשוך כ־78 מיליון דולר מבנקים ברחבי העולם.[9] ככל שתגבר הנגישות לקודים קיימים, במקביל להגברת היכולת של יחידים או ארגונים קטנים לבצע הסבות, כך תתפשט תפוצת הקודים הזדוניים למטרות תקיפה בעולם הפיננסי, למטרת השגת רווחים כלכליים לארגוני פשיעה, ואף תתפשט בקרב ארגוני טרור לשם השגת מטרות חברתיות, אידאולוגיות ופוליטיות, על ידי הפחדה ושיבוש שגרת החיים האזרחית.

## יכולות השחקנים במרחב הסייבר

המעבר מהעידן התעשייתי לעידן המידע הפיק תוצר חדש בדמות מרחב הסייבר (או המרחב הקיברנטי). התפתחותו של עידן המידע קשורה לצמיחת טכנולוגיות תקשורת, בקרה ומחשוב. לצמיחה זו ישנן משמעויות חברתיות וכלכליות עמוקות. לשנת 2008 יש משמעות סמלית בכך שלראשונה חצה מספר המחשבים הביתיים את רף המיליארד (רובם מחשבים המחוברים לאינטרנט), ובאותה שנה דווח כי מספר האנשים בעולם שיש ברשותם טלפונים סלולריים עלה על מספר האנשים שאין להם מכשיר סלולרי. כל מחשב או טלפון כזה יכול לשמש דלת כניסה למרחב הסייבר ונשק לתוקף פוטנציאלי[10] (או להוות בעצמו מטרה לתקיפה).

ההתפתחויות הטכנולוגיות המהירות בעידן המידע יוצרות במרחב הסייבר מאפיינים ותכונות ייחודיות, המאפשרים הפעלה מהירה נגד יריבים המצויים הרחק מתחומי התוקף. התפתחויות אלה עשויות לשנות גם את פניו של שדה הקרב המודרני, והן יוצרות זירות לחימה שבהן השחקן הלא־מדינתי הוא למעשה שחקן מרכזי, המפעיל (יותר מבעבר) את השפעתו על מדיניות ממשלות ומוסדות בינלאומיים. הלחימה בקוסובו בשנים 1996–1999 מאופיינת כמלחמה הראשונה במרחב האינטרנטי. שחקנים מדינתיים ולא־מדינתיים השתמשו ברשת להפצת מידע, להפצת תעמולה וליצירת דמוניזציה ליריבים. האקרים השתמשו ברשת בעת הלחימה ככלי לחימה הן נגד יוגוסלוויה והן נגד נאט"ו, על ידי הפרעה למערכות מחשוב ממשלתיות והשתלטות על אתרים ממשלתיים. יחידים ואקטיביסטים השתמשו ברשת להפצת מסרים מתוך אזור הלחימה.[11]

דוגמה נוספת ניתן למצוא בלחימה באסטוניה. החל מאפריל 2007 ובמשך שלושה שבועות, הותקפה אסטוניה בסוג מתקפות המכונה "מניעת שירות מבוזרת" (DDoS - Distributed Denial of Service). גל המתקפות כלל פגיעה באתרי מוסדות שלטון, בבנקים ובמערכות עיתונים. ההתקפה החלה לאחר עימות עם רוסיה סביב הפגנות המיעוט הרוסי באסטוניה, ולכן רמזו גורמים באסטוניה ונאט"ו על מעורבות מדינתית רוסית בביצוע המתקפות.[12]

למרחב הסייבר יש משמעויות נרחבות בכל הקשור להפעלת כוח צבאי, פעילות חבלנית, פעילות פשע מאורגן, ריגול ומודיעין. בכל הקשור להפעלת כוח, תקיפת מחשבים אינה זקוקה לבסיס מדינתי, והיא יכולה להיעשות גם על ידי ארגונים ואף יחידים. נוסף לכך, התקיפה יכולה להתנהל גם בין מדינות ידידותיות, בתחרות להשיג מודיעין דיפלומטי וכלכלי.

מאפיין ייחודי של מרחב הלוחמה הקיברנטי, שאינו מצוי בשום מרחב לוחמה אחר, הוא היכולת ההדדית של התוקף והקורבן להסתיר בצורה מושלמת כמעט את דבר המתקפה. מעצם טבעו של המרחב הקיברנטי, התוקף יכול לבצע את הפעולה ההתקפית ממרחק גיאוגרפי רב מאוד מהמטרה שלו, ולהשתמש בטכניקות הסוואה שימנעו באופן מוחלט כמעט את חשיפתו. הקורבן, מן הצד השני, יכול תמיד לטעון שהנזק שנגרם למערכות שלו נובע מתקלה בחומרה או בתוכנה, ובכך להימנע מפגיעה תדמיתית ומהכורח להגיב או לאיים בתגובה כלפי מבצע ההתקפה.

תוצאה ישירה של מאפיין ההסתרה במרחב הקיברנטי היא חשיפה מועטה מאוד בתקשורת של מקרי תקיפות. אך מהמעט שכן מתפרסם בעיתונות ניתן ללמוד על גידול בהיקף ובתחכום של המתקפות הקיברנטיות. כל המעצמות כבר מעורבות בצורה זו או אחרת בלוחמת סייבר,[13] ומדינות רבות נוספות משקיעות בפיתוח התקפות והגנות על המרחב הקיברנטי. לוחמת הסייבר משתלבת באופן מושלם במלחמה הקרה שמתרחשת בין ה"מזרח" ל"מערב", כיוון שהיא מאפשרת

לאיים על היריב או לפגוע בו מבלי להכריח אותו להגיב. מתקפה קיברנטית שלא פורסמה ושום גורם לא קיבל עליה אחריות היא מתקפה שהקורבן אינו מרגיש מחויב להגיב עליה, אבל עדיין מבין היטב את הרמז שנשלח לעברו מכיוון התוקף. זוהי מהותה של מלחמה קרה.

בצד ההגנתי, עם התרחבות השימוש בנשק הסייבר, נוצרת מודעות רבה יותר לסכנות הטמונות בנשק זה ולפוטנציאל ההרס שביכולתו להסב מבחינה ביטחונית, כלכלית ותדמיתית. מודעות זו מביאה להשקעה של משאבים רבים בפיתוח מערכות תוכנה מוגנות ומאובטחות יותר, ובאבטחת מתקנים ותשתיות קריטיות במדינות שונות. כמו בכל מאבק בין תוקפים למגִנים, גם בתחום הסייבר הייתה ידם של התוקפים על העליונה כאשר החל להתפתח מרחב הלחימה הקיברנטי. אך כעת נראה שהפער הולך ומצטמצם, ככל שיותר ויותר גופים פועלים לאבטח את תשתיות התקשוב שלהם.

אחד ממאפייני מרחב הסייבר הוא הקושי לזהות את התוקף. בניגוד לתקיפת מטוסי הצי המלכותי היפני בפרל הרבור (1941) שהביאה להכרזת מלחמה אמריקאית רשמית על יפן, תקיפת סייבר גדולה כגון התקיפה על חברת ארמקו באוגוסט 2012[14] נמצאת כיום בוויכוח בקרב מומחי אבטחה לגבי זהות התוקף, למרות הפניית אצבע מאשימה לגורם מדינתי (איראן). מאפייני מרחב הסייבר גם מקשים את ההבחנה בין פגיעה מכוונת לתקלה ואת האפשרות לייחס פעולה לגורם מסוים (attribution), ולכן גם מקשים על המותקפים להגיב על תקיפה. יש הטוענים כי מאפייני המרחב הקיברנטי כיום מקנים יתרון לתוקף לעומת המגן.[15]

חמש קבוצות עיקריות משתמשות כיום, או שיש להן פוטנציאל לשימוש בעתיד, בכלי תקיפה קיברנטיים.[16]

מדינות – מדינות מפתחות יכולות התקפיות והגנתיות כחלק מיכולות הפעלת הכוח שלהן. הערכות סבירות הן שכארבעים מדינות מצטיידות ביכולות לוחמת סייבר או השיגו אותן כבר, לרבות היכולת לבצע מתקפות סייבר. רוב התוכניות הלאומיות הן חשאיות, ואין הסכמה בשאלה עד כמה החוק הבינלאומי הקיים, שתקֵף לעימות מזוין, אמור לחול על מצב ההתקפה החדש.[17]

עידן המידע מאופיין בפעילות מדינתית גוברת בתחומי כלכלה, תשתיות אזרחיות, ביטחון לאומי, ביטחון אזרחי, תקשורת בין־ארגונית, חינוך, ניהול מוסדות שלטון ועוד. בהתאם, מדינות ברחבי העולם מגדילות את השקעתן בתחום ההגנה על מערכות ממוחשבות – השקעה המתבטאת במשאבים המוקצים לנושא, ובפיתוח של טכנולוגיות ותפיסות הגנה ייעודיות.[18] במקביל, שירותי ביטחון ומודיעין מאמצים כלים של המרחב הקיברנטי להשגת מטרתם. טכנולוגיות המידע גם מעניקות לשירותי ביון מדינתיים מגוון רחב של אמצעים ודרכים לביצוע המשימה. למדינות יש יכולת לבצע כניסה גם למערכות מחשב סגורות על ידי

החדרת סוכן או הפעלת סוכן, ועל ידי התערבות במערכת האספקה והחדרת רכיבים "נגועים" למטרה היריבה.

מאפייני מרחב הסייבר המקשים את זיהוי התוקף יכולים לאפשר למדינה תוקפת יתרון בהפעלת שליח (Proxy), שיבצע או יקבל אחריות על תקיפת מדינה או חברה עסקית במדינה יריבה.

במרחב הסייבר המדינתי נחשפו במהלך 2012 שלוש תוכנות קוד זדוני חדשות: פליים, גאוס ומיני־פליים. פליים מהווה דוגמה של תוכנה זדונית מורכבת שהתקיימה לאורך זמן מבלי להיחשף, תוך איסוף נתונים ומידע.

פליים היא תוכנה גדולה במונחים של וירוסים (20 מגה־בייט), שבדרך כלל מסתמכים על היותם קטנים כדי לחמוק מזיהוי. התוכנה כוללת מאפיינים של סוס טרויאני, והיא אפשרה למפעיליה לפתוח "דלתות אחוריות" במערכות מחשבים כדי לאסוף מידע ולהעביר אותו לשרתים מרוחקים ברחבי העולם. בנוסף, התוכנה מסוגלת להקליט אודיו באמצעות המיקרופונים המותקנים במחשבים, לצלם צילומי מסך ולהתחבר למכשירי בלוטות' באזור התקיפה.

סוג כזה של התקפה שעקב מורכבותו מיוחס לתוקף מדינתי משפיע לא רק על מוסדות ממשלתיים, אלא גם על עסקים ותשתיות של חברות עסקיות הנמצאות בקשרים עסקיים עם גופים ממשלתיים.[19]

ארגוני פשע – מונָעים בעיקר מאינטרסים פליליים ועסקיים; ארגוני פשע מאורגן משתמשים בהאקרים, ובעיקר במפעילי רשתות שבויות למטרות רווח: גניבת זהות, הונאה, דואר זבל, פורנוגרפיה, הסוואת פעילות פלילית, הלבנות הון וכיוצא באלה. כשמונים אחוזים מהפשע באינטרנט מבוצע על ידי ארגוני פשע.[20]

נשיא האינטרפול, קהו בון הואי, טען כי הבנקים בארצות־הברית מאבדים מדי שנה 900 מיליון דולר כתוצאה מפשעי מחשב.[21] במהלך הרבעון הראשון של 2012 דווח כי ארגוני פשע יצרו וריאציות בווירוסים קיימים ומוכרים בשם Zeus־ו־SpyEye, לטובת מתקפה על בנקים באירופה ובאמריקה. ההתקפה זוהתה לראשונה באיטליה, שבה הותאם הקוד בצורה ממוקדת לבנקים השונים. לאחר מכן זוהתה תקיפה בעלת מאפיינים דומים בבנקים גרמניים והולנדיים. בהמשך התפשטו התקיפות לאמריקה הלטינית ולארצות־הברית. התוקפים הצליחו לגנוב לפחות 78 מיליון דולר בהעברות מחשבונות של כשישים מוסדות פיננסיים.[22]

הערכות של אנליסטים בכירים הן שהאקרים מצליחים לגנוב כמיליארד דולר בשנה ממוסדות פיננסיים. יש המעריכים כי שלוש מכנופיות הפשע הגדולות הפועלות בתחום מצליחות לגנוב באמצעות מערכות מחשוב כמאה מיליון דולר בשנה, בעוד שבגניבה קונוונציונלית מבנקים אמריקאיים נגנבו על פי ה־FBI בשנת 2010 רק 43 מיליון דולר.[23]

חברות עסקיות – פועלות בעיקר בתחום ההגנתי, כיוון שהיקף ההתקפות במרחב הקיברנטי בהקשרים עסקיים הולך וגדל במידה ניכרת, אולם חלק מהן עלולות לפנות (או שכבר פנו) לאפיק של התקפה על חברות מתחרות לצורך ריגול עסקי. כמו כן, חברות עסקיות מתמודדות בהגנה במרחב הסייבר מול אתגרים טכנולוגיים כגון הגנה על תשלום מקוון, אבטחת שידורי וידיאו בזמן אמת, אבטחת אפליקציות לטלפון חכם ואתגרים נוספים רבים.

ארגוני טרור – יתרונות הגלומים בשימוש במרחב הסייבר מנוצלים על ידי גורמים חבלניים על מנת להעביר מסרים מוצפנים, לגייס תומכים, לרכוש מטרות, לאסוף מודיעין, להסוות פעילות וכדומה.

משיקולי עלות/תועלת, ארגוני טרור אף משתמשים במרחב הסייבר לביצוע התקפות קיברנטיות. התקפות אלה תורמות להשפעה על דעת הקהל לשם העברת מסרים פוליטיים, ועד ביצוע דמוריליזציה והפחדה על מנת לשבש את שגרת החיים של האזרח. ארגוני טרור ממקדים את הפעילות הקיברנטית ההתקפית נגד סמלי שלטון כגון אתרי מוסדות ממשלתיים ותקשורתיים.

אחת ההתקפות הראשונות המתועדות של ארגון טרור נגד מערכות מחשוב מדינתיות התרחשה בסרי־לנקה על ידי לוחמי הגרילה "הנמרים הטמיליים" ב־1998. שגרירויות של סרי־לנקה ברחבי העולם הוצפו במשך שבועיים בכ־800 הודעות דוא"ל ביום עם המסר "אנחנו נמרי האינטרנט השחורים ואנחנו הולכים לשבש את מערכות התקשורת שלכם".[24] יש הטוענים כי מסר זה השפיע וזרע חשש ופחד בשגרירויות.[25]

בישראל, בינואר 2012, קבוצת האקרים פרו־פלסטיניים הקוראת לעצמה "Nightmare" הפילה למשך זמן קצר את אתרי הבורסה לניירות ערך בתל־אביב וחברת התעופה הלאומית אל על, ושיבשה את פעילות אתר הבנק הבינלאומי. בהתייחסות לכך מסר דובר חמאס ברצועת עזה כי "החדירה לאתרים ישראלים פותחת מרחב חדש של התנגדות ומלחמה אלקטרונית חדשה נגד הכיבוש הישראלי".[26]

גורמים "אנרכיסטיים" – מתנגדים למערכת הממסדית הקיימת מעוניינים לחבל בה מבפנים או מבחוץ ויבקשו לתקוף את מערכת המחשוב, שהיא כיום הבסיס לניהולה, בכוונה לשבש ואף להרוס את הסדר החברתי ואת מרקם החיים במדינה. למשל, קבוצות אקטיביסטים או יחידים התוקפים אתרי אינטרנט כדי להשתיל בהם מסר פוליטי, או פועלים לשבירת מנגנוני צנזורה וחשיפת סודות.

בנובמבר 2012, בזמן מבצע "עמוד ענן" בעזה, הודיעו גורמים בממשלת ישראל על מאה מיליון ניסיונות לתקיפות סייבר מקוונות נגד שירותי האינטרנט הממשלתיים בישראל.[27] ארגון "אנונימוס" המייצג קונספט תיאורטי של קהילת האקרים אקטיביסטים קיבל אחריות על הפלת אתרים ישראליים והדלפת מספרי

כרטיסי אשראי של אזרחים ישראליים בזמן העימות. "אנונימוס" אף פרסם רשימה של יותר מ־650 אתרים ישראליים, שלטענתו נפגעו או הופלו כתוצאה מהתקפות האקטיביסטים.[28]

בכיר בממשל האמריקאי דיבר על כך ש"כמה תריסרי מתכנתים מוכשרים יכולים לגרום נזק רב".[29] עם זאת, יש להבחין בין יכולת התקפית על יעדים אסטרטגיים של אויב בעל יכולות הגנה מתקדמות לבין יכולת לגרום נזקים מקומיים טקטיים. ההצטיידות בכלי נשק קיברנטיים בקרב השחקנים השונים נעשית בהתאם ליכולות ולמגבלות השחקנים להקים כוח קיברנטי בעל יכולות התקפיות, והיא מושפעת גם מהאינטרסים ומהצרכים של כל שחקן ושחקן.

שימוש בנשק קיברנטי לתקיפת יעדים אסטרטגיים במרחב הפיזי והסייבר מצריך יכולת השמורה, לפי שעה, למספר מצומצם של מדינות בעלות יכולות ומשאבים טכנולוגיים ברמה גבוהה. לעומת זאת, ישנה "מדרגת כניסה נמוכה" וכלי נשק קיברנטיים בעלי יכולת פגיעה עם נזקים טקטיים. יכולת ייצור המוני של כלי נשק קיברנטיים כאלה היא מהירה ובעלות נמוכה יחסית, חלקם אף זמינים בשוק החופשי. מדינות מנצלות את מרחב הסייבר כדי להשיג יתרון ולקדם את האינטרסים שלהן באמצעות איסוף מידע, השגת כושר פגיעה ביכולותיו של מי שנתפס כאויב, ועוד. גם שחקנים לא־מדינתיים כגון ארגוני טרור ופשיעה ממנפים את מרחב הסייבר למטרותיהם, ומפיקים תועלת במרחב המתיר גם לשחקנים קטנים להשפיע באופן שאינו יחסי לגודלם.

מטבלה 1 ניתן ללמוד כי השחקן המדינתי מסוגל להשיג יכולות תקיפה בכל הקטגוריות. למדינות יש צרכים מגוונים (ריגול, פגיעה בתעשיות של מדינת אויב) וגורמים מרסנים (הימנעות מפגיעה בחפים מפשע ויצירת נזק סביבתי רב, אשר יובילו לפיתוח נשק סייבר לתקיפה קיברנטית במקום לתקיפה פיזית, או נשק לתקיפה פסיכולוגית, כמו התרעה לפני הפצצה, שתאפשר להימנע מפגיעה באזרחים). שאר השחקנים במרחב הסייבר הם בעלי אינטרסים וצרכים ממוקדים יותר: לארגוני טרור יש יכולות ומשאבים מצומצמים יותר, והם מונָעים על ידי אינטרס של השגת מטרות פוליטיות ואידאולוגיות באמצעות פגיעה במערכות פיזיות (עדיין לא נרשם אירוע כזה), ריגול או לוחמה פסיכולוגית; ארגונים עסקיים, לעומת זאת, יהיו מעוניינים בעיקר בריגול עסקי, ולעיתים גם בשיבוש הפעילות של המתחרים; ארגוני פשע מעוניינים בעיקר בהשגת נכסים וכסף במרמה, ולכן יתמקדו בתקיפת מערכות קיברנטיות ובריגול שיתמוך בפעילות כזו (איסוף כרטיסי אשראי ופרטים מזהים לצורך תקיפה).

## טבלה 1: סל יכולות הנשק הקיברנטי של השחקנים השונים במרחב הסייבר

| | שימוש בנשק קיברנטי לתקיפת המרחב | שימוש בנשק קיברנטי לריגול | מניעת שירות ולוחמה פסיכולוגית |
|---|---|---|---|
| **המדינה** | | | |
| בשל המשאבים הרבים העומדים לרשות המדינה, יכולת התקיפה שלה היא הגבוהה ביותר. | המשאבים הרבים העומדים לרשות המדינה מאפשרים לה לתקוף מטרות מורכבות ומוגנות היטב. | המדינות המובילות בתחום הריגול הקיברנטי הן גם אלו שמשקיעות את המשאבים הרבים ביותר בפיתוח יכולות ריגול מתוחכמות. | יכולת זו היא פשוטה יחסית, ומדינה עלולה להשתמש בה בעת עימות עם מדינה אחרת בכדי לגרום לה נזק. |
| **ארגוני טרור** | | | |
| בדרך כלל, ארגוני טרור אינם מחזיקים ביכולת קיברנטית לתקיפה. | ארגוני טרור לרוב אינם מחזיקים ביכולת לתקוף מטרות מורכבות. | ארגוני טרור לרוב אינם מחזיקים ביכולת לבצע ריגול קיברנטי. | ארגוני טרור לרוב אינם מחזיקים ביכולת לבצע מתקפות מניעת שירות. |
| **ארגוני פשיעה** | | | |
| ארגוני פשיעה מחזיקים ביכולת לתקוף מטרות מורכבות, אך לרוב הם אינם עושים זאת. | ארגוני פשיעה מחזיקים ביכולת לתקוף מטרות מורכבות, אך לרוב הם אינם עושים זאת. | ארגוני פשיעה מחזיקים ביכולת לבצע ריגול קיברנטי, אך לרוב הם אינם עושים זאת. | ארגוני פשיעה מחזיקים ביכולת לבצע מתקפות מניעת שירות, אך לרוב הם אינם עושים זאת. |
| **חברות פרטיות** | | | |
| חברות פרטיות מחזיקות ביכולת לתקוף מטרות מורכבות, אך לרוב הן אינן עושות זאת. | חברות פרטיות מחזיקות ביכולת לתקוף מטרות מורכבות, אך לרוב הן אינן עושות זאת. | חברות פרטיות מחזיקות ביכולת לבצע ריגול קיברנטי, אך לרוב הן אינן עושות זאת. | חברות פרטיות מחזיקות ביכולת לבצע מתקפות מניעת שירות, אך לרוב הן אינן עושות זאת. |
| **יחידים** | | | |
| יחידים מחזיקים ביכולת לתקוף מטרות מורכבות, אך לרוב הם אינם עושים זאת. | יחידים מחזיקים ביכולת לתקוף מטרות מורכבות, אך לרוב הם אינם עושים זאת. | יחידים מחזיקים ביכולת לבצע ריגול קיברנטי, אך לרוב הם אינם עושים זאת. | יחידים מחזיקים ביכולת לבצע מתקפות מניעת שירות, אך לרוב הם אינם עושים זאת. |

## איום השימוש הרב־פעמי בנשק קיברנטי

כל מתקפת סייבר חדשה שמתגלה מקרבת את הפיכתו של נשק הסייבר לנחלת הכלל. עם התגברות השימוש בכלים ללוחמת סייבר, לא מן הנמנע שנשק קיברנטי מתוחכם ובעל יכולת לביצוע נזק אסטרטגי יהפוך לחזון נפרץ, וגרסאות שלו ימצאו את דרכן לידיהן של מדינות תומכות טרור וארגוני טרור.[30] כדוגמה, אפשר להתבונן על המתקפה על אתרי הגרעין האיראניים באמצעות וירוס סטקסנט (stuxnet). ההתקפה פעלה במשך שנים באופן חשאי, אך ברגע שהתגלתה היא הביאה למחקר ולניתוח מעמיקים ביותר של קוד הוירוס, ולניסיון להבין את כל ההיבטים שאִפשרו את הצלחתו. תוצאות הניתוח יכולות לשמש באופן מיידי לפיתוח של וירוסים חדשים בעלי עקרונות פעולה דומים לאלה של סטקסנט. הסוד נחשף, הנשק התפשט. מבחינה תיאורטית, הימצאות וניתוח קוד זדוני בידי חברות ומומחי אבטחה עשויה לחשוף את הוירוס כלפי חוץ לגורמים שונים, החל ממדינות ועד ארגוני טרור. הנשק הקיברנטי לא יישאר לעד נחלתם של מעטים.

קיימת סברה שלפיה הנשק הקיברנטי הינו חד־פעמי, והדבר יהווה גורם מרסן בשימוש בו וגורם מאט בפיתוח של כלי לוחמת סייבר חדשים, בשל הצורך לחדש כל העת והימנעות משימוש בכלי נשק שהתגלה כבר ונחתם על ידי תוכנות ההגנה. סברה זו לא הוכיחה את עצמה, ומהתבוננות בשטח ניתן להבחין שדווקא ההפך הוא הנכון – הווה אומר, קיים שימוש חוזר נרחב בכלי לוחמת סייבר שעוברים שינויים על מנת לאפשר להם לחמוק מהרדאר של תוכנות ההגנה. הצלחתה של מתקפת סייבר תלויה בניצול מוצלח של חולשה[31] במערכת המותקפת. חולשה יכולה להתבטא ברכיב תוכנה שבכתיבתו לא הובאו בחשבון שיקולי אבטחה מספיקים של קוד, ברכיב חומרה שניתן לחדור אליו ולגרום לו לבצע פעולות הרסניות או בפרוטוקול תקשורת לא מאובטח. על מנת שמערכת תיחשב מאובטחת, כל ההיבטים שצוינו צריכים להיבדק ולהיות מאובטחים בנפרד. מספיקה פרצה קטנה באחד מהם על מנת לאפשר חדירה והשתלטות על המערכת כולה. לדוגמה, אתר אינטרנט המחזיק מידע רגיש ומאובטח ברמה גבוהה מאוד, כך שאינו פגיע להתקפות רשת כמו Sql Injection, XSS ואחרות. אבל נניח שעל אותו שרת שבו מאוחסן האתר המאובטח נמצא אתר נוסף, חסר חשיבות ולא מאובטח בכלל. ניתן לתקוף את האתר הנוסף ודרכו להגיע אל המחשב המאחסן את האתרים שהם מטרה. ברגע שמשתלטים על המחשב, כל מערכות ההגנה של האתר המאובטח כבר אינן רלוונטיות והוא נפרץ.

נשק קיברנטי שהתגלה ונחתם אמנם נחסם לשימוש בצורתו המקורית, אך מכאן ועד לחסימה הרמטית והפיכת כל הקוד שפותח ללא־רלוונטי – המרחק עדיין רב. ראשית, כל כלי תקיפה מורכב ממספר מודולים (רכיבי תוכנה). בין היתר, ניתן למנות את המודול האחראי להסוואת הכלי במערכת המותקפת, מודולים שונים

לאיסוף מידע, מודול לאחסון המידע ומודול לשליחת המידע אל שרתי הפיקוד והבקרה של הכלי. אם סוס טרויאני התגלה ונחתם, ניתן לעשות שימוש חוזר בחלק מן המודולים שלו, כאשר אלה משולבים בתוך קוד של סוס טרויאני אחר. שילוב כזה ייצור כלי תקיפה חדש שעשוי לחמוק מתחת לרדאר של מערכות אנטי־וירוס. דרך אחרת לשימוש חוזר בקוד זדוני היא על ידי הסוואתו בשיטות המוכרות מעולם התוכנה כעֵרפול (obfuscation)[32] ואריזה (packing).[33] אלה יכולות לעיתים לשנות את הקוד הזדוני באופן שהוא לא יתגלה על ידי תוכנת הגנה. לבסוף, גם אם לא יתאפשר שימוש בקוד שהתגלה, ניתן לפתח קוד מוטציה המבוסס על רעיונות ואופני פעולה דומים ומנצל את אותן החולשות כמו הקוד המקורי.

טענה זו נתמכת על ידי השימוש בווריאציות השונות של הווירוס פליים שהתפרסם לאחרונה בתקשורת. גם לאחר שהתגלה הווירוס המקורי, נגזרות שונות שלו המשיכו לתקוף מחשבי יעד ללא הפרעה, עד שהתגלו גם הן.[34] גם הווירוס סטקסנט, שנחשב למתוחכם ביותר שהתגלה עד כה, פתח דלת לרבים שיבואו אחריו ויחקו את שיטות הפעולה שלו.[35] למעשה, ניתן לומר בסבירות גבוהה כי פליים[36] וסטקסנט יחדיו ממחישים באופן הברור ביותר את יכולת השימוש החוזר בקוד זדוני, כיוון שהם חולקים קוד רחב במשותף. אף על פי שהם נועדו למטרות שונות לחלוטין (ריגול ופגיעה במערכות בקרה תעשייתיות, בהתאמה) קיימות מספר פונקציות ששניהם צריכים למלא: חדירה למערך המחשבים של הארגון, הסוואת קיומו של הכלי, ניתוח הרשת הארגונית והתפשטות בתוכה על מנת למצוא מחשבי יעד ערכיים. את הפונקציות הללו ניתן לממש בשני כלי הנשק באמצעות אותו קוד, שנכתב ונבדק פעם אחת בלבד. היתרונות ביכולת השימוש באותו הקוד עבור שני כלים שונים הם עצומים, כיוון שתהליך ייצור נשק סייבר הוא ארוך ויקר. תהליך מציאת החולשות הוא מורכב מאוד, ודורש לעיתים מאות שעות עבודה של אנשים מיומנים. זהו תהליך שאינו מבטיח תוצאה בסופו, אף אם הושקעו בו מאמצים רבים. יתרה מכך, גם כאשר נמצאה חולשה, על מנת לנצל[37] אותה ולחדור דרכה למערכת מחשב יש להשקיע עוד עבודה רבה כדי לחבר את הקוד המתאים, ולבנות את הקבצים שיוכלו לעשות שימוש בחולשה. ייתכן גם שלא תימצא דרך לנצל את החולשה מפאת המורכבות שלה, ואז יהיה צורך להתחיל במחקר נוסף למציאת חולשה אחרת, קלה יותר לניצול. לכן, כאשר יצרן נשק סייבר מפתח יכולת חדירה למערכת הוא ישאף לנצל אותה בכמה תרחישים שונים ובכלים שונים, כדי למקסם את הרווח מההשקעה שלו. מנגד, ככל שיהיה שימוש רב יותר ומגוון יותר ביכולת סודית מסוימת, יגברו הסיכויים שהיא תיחשף ותיחסם לשימוש. עובדה זו מהווה גורם מרסן בשיקוליו של יצרן נשק סייבר לגבי התפשטות הכלים ושימוש ביכולת בתרחישים נוספים.

לכאורה היה צפוי כעת כי לאחר שהתוכנות הזדוניות התגלו ודבר החולשות והניצול שלהן התפרסם ברבים, התוכנות שבהן התגלו החולשות יעודכנו מייד (למשל מערכת ההפעלה windows), והעדכון יופץ לכל מחשב שבו מותקנת מערכת כזו, וכך בעצם יהפכו כל המחשבים לחסינים מפני קוד זדוני המנצל את החולשות המדוברות. אך לא כך הדבר. תהליך ההגנה על מערכות מפני קוד זדוני שהתגלה כולל ארבעה שלבים עיקריים: גילוי החולשה שבה השתמש הקוד, סגירת הפִּרצה במערכת, הפצת טלאי אבטחה לכלל משתמשי התוכנה והתקנתו על המחשבים. השלב של סגירת הפרצה שדרכה חדר קוד זדוני למערכת הוא מורכב, כיוון שלאחר תיקון הפִּרצה על התוכניתנים לוודא גם שתפקוד המערכת לא נפגע בעקבות השינוי שנעשה. יש צורך לבחון בזהירות את השפעות התיקון ולהריץ תרחישי בדיקה שונים כדי לוודא תקינות. בהתאם למורכבות המערכת, התהליך עשוי להימשך שבועות עד חודשים רבים.

יתרה מזאת, גם לאחר שפותח והופץ עדכון אבטחה (טלאי), אנשים רבים אינם מעדכנים באופן אוטומטי את המחשבים שלהם, ובמיוחד נכון הדבר בחברות אשר להן רשת תקשורת פנימית המנותקת מרשת האינטרנט. במקרה כזה, מחשבי הרשת הפנימית יעודכנו רק כאשר אחראי האבטחה יעביר באופן יזום את עדכון התוכנה מהאינטרנט אל תוך הרשת הפנימית. שתי סיבות אלו מביאות לכך שניתן לנצל חולשות גם זמן רב אחרי שהן התגלו ופורסמו.

תופעה מעניינת הקשורה בעדכוני האבטחה מזכירה את התופעה הידועה בשם "מלכוד 22". כאשר חברת מייקרוסופט, למשל, נתקלת בבעיית אבטחה במערכת ההפעלה שלה, היא מפתחת עדכון אבטחה ומעוניינת להפיץ אותו לכל המשתמשים החשופים לבעיית האבטחה. אבל ברגע שהעדכון מופץ, גם האקרים וכותבי קוד זדוני נעשים מודעים לקיומו, ויכולים לנתח אותו ולהבין איזו בעיית אבטחה הוא פותר – ובהתאם לזאת לכתוב קוד זדוני שמנצל את חור האבטחה שמייקרוסופט עצמה חשפה בפניהם. מובן שהקוד הזדוני יוכל לפעול רק במערכות שלא הותקן בהן עדכון האבטחה, אך למרבה הפלא יש לא מעט כאלה, גם של משתמשים פרטיים שאינם טורחים לעדכן את המחשב שלהם באופן תדיר, ובמיוחד בחברות שבהן נדרשת פעולה יזומה של אנשי המחשוב כדי לעדכן את מערך המחשבים בחברה. מצב זה יוצר חלון זמן של כמה ימים או יותר, שבו האקרים יכולים לנצל את פרצות האבטחה לפני שייסגרו. זוהי דוגמה לשימוש חוזר בקוד זדוני שמתאפשר באמצעות ניצול לרעה של תהליך הפצת עדכוני האבטחה. בדרך כלל, חברת מייקרוסופט מפיצה עדכוני אבטחה לתוכנות שלה ביום שלישי השני בכל חודש, ויום זה זכה לכינוי "Patch Tuesday"[38]. בהתאם לזאת, יום רביעי שלאחר מכן מכונה "Exploit Wednesday", כיוון שביום זה מנתחים האקרים את

עדכוני האבטחה ומתחילים לנצל אותם כדי לחדור למחשבים שעדיין לא הספיקו להתעדכן.

היכולת ליצור נשק סייבר חדש המבוסס על נשק קיים או על חולשה שפורסמה איננה תמיד מיידית ופשוטה. ההאקרים שמנצלים את עדכוני האבטחה של מייקרוסופט כדי לגלות את קיומן של חולשות במערכת ההפעלה "חלונות" צריכים להשקיע זמן בניתוח הטלאי, ובהשוואת הקבצים שהוא מתקן לקבצים המקוריים לפני התיקון (כדי לזהות היכן בדיוק התבצע התיקון, כיוון ששם נמצאת החולשה). לבסוף הם גם צריכים למצוא דרך לנצל את החולשה. תהליך זה עשוי להימשך בין ימים לשבועות, כתלות במורכבות הטלאי ובנחישות של ההאקר. לעומת זאת, ניתוח מעמיק של כלי מתוחכם כמו פליים ידרוש זמן רב יותר, וכוח אדם מקצועי ומיומן יותר. בדרך כלל, ניתוח כזה נעשה על ידי מדינות או חברות אבטחה ולא על ידי אנשים פרטיים. לדוגמה, נשק הסייבר מיני־פליים (MiniFlame[39]) שנותח באופן מעמיק על ידי חברת קספרסקי. ניתוח זה, שארך מספר חודשים ודרש משאבי כוח־אדם רבים, בוצע על מנת לפתח הגנה מפני הכלי ולהפיץ אותו בקרב לקוחות החברה. אבל תוצרי הניתוח יכולים לשמש בסיס לקוד מוטציה, העושה שימוש בטכניקות דומות ולעיתים אף בחלק מהקוד של הנשק המקורי. אם תוצרים אלה ידלפו מחברת קספרסקי לגורמים המפתחים נשק סייבר, לא יהיה זה מפתיע לגלות כלים חדשים החולקים קוד משותף עם המיני־פליים אך מופעלים על ידי תוקפים אחרים, נגד מטרות אחרות (ייתכן שאף נגד היוצר הראשוני של הנשק – אפקט הבומרנג).

בשנים האחרונות חווה העולם מגמת עלייה בתקיפות סייבר הדורשות יכולת התקפית רחבה וממושכת, ונגד יעדים אסטרטגיים ובעלי יכולת הגנה גבוהה. יכולת זו קיימת כיום רק במספר מועט של מדינות, אך לא מן הנמנע שמגמת העלייה לא תיעצר ומדינות נוספות ישיגו יכולות כאלו, גם לצורכי הגנה וגם להתקפה. מגמה זו תקפה גם לשוק עבריינות הסייבר העולמי.[40] ברוסיה, לדוגמה, ישנם סימנים המעידים על כך שגורמי פשע מאורגן החלו להצטרף "באמצעות שיתוף נתונים וכלים" כדי להגדיל את רווחיהם.[41] דו"ח של מעבדת קפרסקי לסיכום שנת 2012 חשף כי היקף ההתקפות של קודים זדוניים ברשת האינטרנט בקרב לקוחות החברה כמעט הכפיל את עצמו במהלך שנת 2012 לעומת 2011 (מ־946,393,693 התקפות ב־2011 ל־1,595,587,670 ב־2012). התקפות אלה כוללות התקפות רשת ב־202 מדינות. ארגוני פשע השתמשו ב־6,537,320 דומיינים ייחודיים ככלים לביצוע התקפות פיננסיות – כשני מיליון וחצי יותר משנת 2011.[42]

## סיכום

מדינות ושחקנים לא־מדינתיים רבים מצויים במרוץ חימוש חשאי במרחב הסייבר. מפת האינטרסים של השחקנים השונים מעידה על כך שהתקפות מסוגים שונים במרחב זה דורשות מגורמים מדינתיים להיות ערוכים למגוון התקפות אפשריות. במקביל, תכונות ומאפייני שדה הקרב הקיברנטי מציבים בפני התוקף דילמות הנובעות מהיותו של הנשק הקיברנטי רב־פעמי, ולכן עצם השימוש בו חושף את יכולותיו בפני הקורבן, שיכול מצדו לעשות בו שימוש חוזר, כולל נגד התוקף עצמו (אפקט הבומרנג). כלי נשק בעלי יכולת הרס אסטרטגי (כגון סטקסנט) עלולים ליפול (או נפלו) בידי מדינות תומכות טרור וארגוני טרור ופשע, וישמשו בסיס לתקיפות סייבר. פיתוח עצמאי של כלי תקיפה קיברנטיים או רכישתם בשוק השחור עלולים להקנות לגורמים אלה יכולת ליצור נזק רב, אף אם כלים שהושגו באופן כזה אינם מגיעים לרמת תחכום של נשק קיברנטי המיוצר על ידי מדינות מתקדמות.

קיימת בעייתיות בהימצאות נשק קיברנטי בידי גורמים פרטיים, וכתוצאה מכך, תפוצה בלתי־מבוקרת שלו. לדוגמה, חוקר אבטחת מידע בכיר טען שקוד הסטקסנט נמצא ברשותו ואף הציע לשתף אותו עם אחרים.[43] במועד אחר טען מומחה שניתח את הסטקסנט כי קוד זה שקול לכלי נשק רב־עוצמה, אך כאשר נשאל מדוע אינו משמיד את העותק שברשותו – העדיף לא להשיב. מלבד דיון בשאלות אתיות ומוסריות, אנו סבורים כי יש מקום לביצוע הסדרה תוך־מדינתית ובינלאומית בנושא, אשר תקבע מנגנוני ויסות ואכיפה נגד תפוצת קוד זדוני. יש לשקול להגביל, ובמקרים מסוימים אף לאסור את ההחזקה בקודי מחשב זדוניים, מחשש שיגיעו לידיים הלא־נכונות שיעשו בהם שימוש לרעה. בעניין זה, ניתן אולי ללמוד מהמלחמה שמתנהלת נגד הפצת קניין רוחני שיש עליו זכויות יוצרים, כמו סרטים ומוזיקה.

כיום, ארסנל כלי הנשק הקיברנטיים בעלי יכולת פגיעה טקטית מצמצם את פער ההצטיידות בין מדינות לבין שחקנים לא־מדינתיים. לעומת זאת, מתרחב הפער בין מדינות בעלות ארסנל יכולות תקיפה נגד יעדים אסטרטגיים, לבין מדינות ושחקנים שאין ביכולתם להגיע לסף הכניסה הגבוה. לא מן הנמנע שמדינות ושחקנים נוספים יחתרו להשגת יכולת של נשק קיברנטי בעל כושר פגיעה פיזית, ומגמת העלייה הדרמטית באיומים במרחב הסייבר מחייבת כיווני פעולה להתמודדות עם איומים אלה. לכן קיים צורך חשוב להעלות לדיון את תפיסת כלי הנשק הקיברנטיים כנשק רב־פעמי שניתן לנצלו לתקיפות נוספות.

## הערות

1 ראו: **מילון אבן שושן המרְכז: מחודש ומעודכן לשנות האלפים**, הוצאת ליאור שרף, 2004.

2 Mark Ambinder, "Did America's Cyber Attack on Iran Make Us More Vulnerable?" *The Atlantic***,** June 5, 2012. http://www.theatlantic.com/national/archive/2012/06/did-americas-cyber-attack-on-iran-make-us-more-vulnerable/258120/

3 קוד מחשב שנכתב במטרה לבצע פעולה על מערכת מחשוב, לרוב בעלת אופי של גניבת מידע או שיבוש תהליכים במערכת, ואשר מורץ ללא ידיעת בעל המערכת או אישורו.

4 לדוגמה: כאשר מתגלה תוכנה זדונית על ידי חברת אנטי־וירוס, נוצרת חתימה אלקטרונית של אותו הווירוס ונשלחת לכל הלקוחות של החברה. באופן כזה, כאשר לקוח אחר יותקף על ידי אותו הווירוס, תוכנת האנטי־וירוס תזהה את ההתקפה על פי החתימה שנשלחה אליה, ותחסום אותה ביעילות.

5 שמואל אבן ודוד סימן־טוב, **לוחמה במרחב הקיברנטי**, מזכר 109, תל אביב: המכון למחקרי ביטחון לאומי (מאי 2012), עמ' 41. http://www.inss.org.il/upload/(FILE)1306930376.pdf

6 תהליך של גילוי עקרונות טכנולוגיים והנדסיים של מוצר דרך ניתוח המבנה שלו ואופן פעולתו. לרוב, תהליך זה כולל פירוק המוצר למרכיבים וניתוח פרטני של דרך פעולתם של המרכיבים.

7 Drone Wars UK, "Mapping Drone Proliferation: UAVs in 76 Countries", *Global Research*, September 18, 2012, http://www.globalresearch.ca/mapping-drone-proliferation-uavs-in-76-countries/5305191

8 William Troop, "Got Drones? The Problem With UAV Proliferation", *The World*, March 26, 2012, http://www.theworld.org/2012/03/drones-proliferation/

9 Dave Marcus and Ryan Sherstobitoff, "Disserting operation High Roller", *McAfee & Guardian Analytics*, 2012. http://www.mcafee.com/us/resources/reports/rp-operation-high-roller.pdf

10 Martin C. Libicki, *Cyber deterrence and cyber war*, Rand, Project Air Force, 2009. http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf

11 Dorothy E. Denning, Activism, "Hacktivism and Cyberterrorism, in Networks and Netwars, The future of terror, crime, and militancy",in *The Future of Terror, Crime, and Militancy*, Edited by John Arquilla and David Ronfeld, Rand Cooparation, 2001, 240. http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf

12 Ian Trainor, "Russia accused of unleashing cyberwar to disable Estonia", *The Gaurdian*, 17 May, 2007.

13 שמואל אבן ודוד סימן־טוב, **לוחמה במרחב הקיברנטי**, עמ' 63.

14 באירוע זה הוחדר ב־15 באוגוסט 2012 קוד זדוני למערכת המחשוב של אראמקו, חברת נפט סעודית בבעלות ממשלתית, ועל פי הדיווחים הוצאו כ־30,000 מחשבים מכלל שימוש.

15 יצחק בן ישראל, ליאור טבנסקי, "מבט בינתחומי על אתגרי הביטחון בעידן המידע", **צבא ואסטרטגיה**, כרך 3, גיליון 3 (דצמבר 2011), עמ' 25.

16 יורם שוייצר, גבי סיבוני ועינב יוגב, "המרחב הקיברנטי וארגוני טרור", **צבא ואסטרטגיה**,

כרך 2, גיליון 3 (דצמבר 2011), עמ' 34.

17 James A. Lewis and Katrina Timlin, "Cybersecurity and Cyberwarfare," *UNIDIR Resources,* 2001. www.unidir.org/pdf/ouvrages/pdf-1-92-9045-011-J-en.pdf

18 רמי אפרתי וליאור יפה, "כך בונים הגנה קיברנטית לאומית", *Israel Defense*, 11 באוגוסט, 2012.
http://www.israeldefense.co.il/?CategoryID=512&ArticleID=2960

19 כגון תקיפות הנערכות נגד מטרות אזרחיות, בהן תשתיות לאומיות בעלות חשיבות קריטית, חברות המהוות חוליות בשרשרת הנגישות לאותן המטרות וחברות שתקיפתן משרתת צורך כלכלי.

20 אלי סניור, "האינטרפול: 1,000 התקפות סייבר בדקה בארץ", YNET, 8 במאי, 2012.
http://www.ynet.co.il/articles/0,7340,L-4226242,00.html

21 שם.

22 דו"ח של חברות Guardian ו־McAfee
Dave Marcus and Ryan Sherstobitoff, *Dissecting operation High Roller*, McAfee & Guardian Analytics, 2012.
http://www.guardiananalytics.com/researchandresources/researchstudies_resources/Dissecting_Operation_High_Roller_Research_Report.pdf

23 Greg Farrell and Michael A. Riley, "Hackers take $1 billion a year as Banks blame their clients", Bloomberg, 5 August, 2011.
http://www.bloomberg.com/news/2011-08-04/hackers-take-1-billion-a-year-from-company-accounts-banks-won-t-indemnify.html

24 Dorothy E. Denning, *Cyber terrorism*, Testimony before the Special oversight on Terrorism, Committee on Armed Service, U.S House of Representatives, May 23, 2000.
http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

25 Dorothy E. Denning, Activism, Hacktivism and Cyber terrorism, 269.

26 גיא גרימלנד ואחרים, "מתקפת סייבר", *TheMarker*, 16 בינואר, 2012.
http://www.themarker.com/markets/1.1618274

27 אור הירשאוגה ונתי טוקר, "קרבות הסייבר נגד ישראל: 100 מיליון תקיפות, ללא הישגים משמעותיים", *TheMarker*, 22 בנובמבר, 2012.
http://technation.themarker.com/hitech/1.1871058

28 John D. Sutter, *Anonymos declares cyber war on Israel*, *CNN*, 19 November, 2012.
http://edition.cnn.com/2012/11/19/tech/web/cyber-attack-israel-anonymous/index.html?hpt=hp_c1

29 שמואל אבן ודוד סימן־טוב, **לוחמה במרחב הקיברנטי**, עמ' 23.

30 למשל תוכנית הסייבר של ארגון חזבאללה:
Ward Carroll, "Hezbollah's Cyber Warfare Program", *DEFENSETECH*, June 2, 2008,
http://defensetech.org/2008/06/02/hezbollahs-cyber-warfare-program/

31 חולשה היא תכונה של רכיב תוכנה / חומרה / פרוטוקול המאפשרת לעשות שימוש ברכיב זה שלא למטרה שעבורה נועד, באופן שיעניק יתרון למנצל תכונה זו. היתרון יכול להתקבל באחת או יותר מהדרכים הבאות: השתלטות על מערכת, שיבוש מערכת, השגת מידע מתוך המערכת.

32 ערפול קוד הוא טכניקה מעולם התוכנה שלוקחת קוד מחשב קיים המיועד לביצוע משימה מסוימת, ומשנה אותו באופן שהפונקציונליות שלו לא תיפגע, אך התוצר יהיה

מספיק שונה מהמקור, באופן שתוכנות אנטי־וירוס לא יוכלו לזהות את התוצר כווירוס. תוכנות אנטי־וירוס המבוססות על זיהוי חתימות בקוד (חתימה בהקשר זה היא מקטע קוד שנועד לבצע פעולה מסוימת, שניתן לייחס אותה בסבירות גבוהה לתוכנה זדונית) יתקשו לזהות כווירוס קוד שעבר ערפול מוצלח, כיוון שכל החתימות המוכרות להן לא יופיעו בתוצר של תהליך הערפול.

33 אריזת קוד הינה סוג מתוחכם של ערפול קוד. בתהליך האריזה, קוד מחשב זדוני עובר שינוי צורה קיצוני כך שהוא כבר כלל לא נראה כמו קוד ריצה, אלא יותר כמו קובץ טקסט תמים. שיטה זו מונעת כמעט לחלוטין את היכולת של תוכנות אנטי־וירוס לגלות את הקוד הזדוני לפני שהוא מתחיל לבצע את פעולתו (למשל, בזמן החדירה של הווירוס למחשב, הוא לא יתגלה). קוד ארוז פועל על ידי תוכנת עזר תמימה, שכאשר היא מתחילה לרוץ היא קוראת את קובץ הטקסט שבו מסתתר הקוד הזדוני, מתרגמת את הטקסט לפקודות ריצה ובעצם הופכת בעצמה להיות וירוס. ניתן לדמות זאת לווירוס מתחום הביולוגיה, המשתלט על תא חי ומנצל את כל המנגנונים של התא לצרכיו.

34 רננה אשוח, "Kaspersky חושפת את miniFlame – קוד זדוני שתוכנן לפעולות ריגול", *YedaTech*, 15 באוקטובר, 2012.
http://www.yedatech.co.il/yt/news.jhtml?value=19827

35 למאמר על ממשיכי הדרך של סטקסנט:
Steven Cherry, "Sons of Stuxnet", *IEEE*, December 14, 2011, http://spectrum.ieee.org/podcast/telecom/security/sons-of-stuxnet

36 על אודות פליים:
Aleks, "The Flame: Questions and Answers", *SECURELIST*, May 28, 2012, http://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers

37 ניצול חולשה (Exploit) הינו קוד מחשב או קובץ שנועד לנצל פגיעות או חולשה של מערכת מסוימת באופן שיעניק לכותב ה־Exploit יכולת חדירה או שיבוש של המערכת המותקפת. לדוגמה: תוכנה להצגת תמונות על מסך המחשב, שמכילה חולשה מסוימת המאפשרת להריץ קוד על המחשב המותקף. ניצול חולשה כזאת עשוי לבוא בצורת קובץ תמונה המכיל קוד שאותו מעוניין התוקף להריץ על המחשב המותקף. קובץ תמונה כזה צריך, כמובן, לא רק להכיל את הקוד אלא גם לדעת לנצל את החולשה, או את נקודת התורפה של התוכנה להצגת התמונות.

38 המילה Patch מתארת עדכון או טלאי אבטחה שמולבש על המערכת.

39 Global Research and Analysis Team, Kaspersky Labs, "miniFlame aka SPE: Elvis and his friends", *SECURELIST*, October 15, 2012.
http://www.securelist.com/en/analysis/204792247/miniFlame_aka_SPE_Elvis_and_his_friends

40 שוק זה הוערך ב־2011 בלמעלה מ־12.5 מיליארד דולר, כאשר הנתח של רוסיה בעוגה הוא כ־2.3 מיליארד דולר (קרוב לכפול מערכו המוחלט בהשוואה לשנה הקודמת).
להרחבה: http://group-ib.com/images/media/Group-IB_Report_2011_ENG.pdf

41 צ'ילופו, קרדאש וס. סלמואירגי, "תוכנית להרתעת סייבר: בניית יציבות באמצעות כוח", **צבא ואסטרטגיה**, כרך 4, גיליון 3, (דצמבר 2012), עמ' 5 .

42 Denis Maselnnikov and Yuri Namestinkov, "Kaspersky Security Bulletin 2012. The overall statistics for 2012", *SECURELIST*, December 2012.
http://www.securelist.com/en/analysis/204792255/Kaspersky_Security_Bulletin_2012_The_overall_statistics_for_2012

43 כותבי מאמר זה נכחו באופן אישי בפגישה עם איש חברת אבטחת המידע בנובמבר 2012.

# לקחים מהפעלת "כיפת ברזל"

**יפתח ש. שפיר**

ישראל נתונה למתקפות שיגורי רקטות זה שנים רבות.[1] זכורות במיוחד תקופות ההפגזות על יישובי אצבע הגליל בשנות השבעים, מלחמת לבנון השנייה ב־2006, עת ספגה ישראל מעל 4000 רקטות תוך חודש אחד, והירי המתמשך מרצועת עזה בעשור האחרון.

במהלך השנים פיתחה מדינת ישראל דוקטרינת הגנה נגד תקיפות "ירי תלול־מסלול" שיֵרי הרקטות הוא אחד מגילוייו. דוקטרינה זו מתבססת על שכבות הגנה – החל בהגנה פסיבית, הגנה אקטיבית של יירוט רקטות וטילים על ידי מערכות "כיפת ברזל", "שרביט קסמים" (בפיתוח), חץ־2 ו־חץ־3 (בפיתוח), וכלה בתקיפת המשגרים בבסיסיהם.

מאמר זה מתמקד במערכת "כיפת ברזל" שנכנסה לשירות מבצעי בראשית שנת 2011, והציגה את יכולתה תוך חדשים ספורים מפריסתה. במאמר זה אנסה לבחון את לקחי פריסת המערכת, ולהעריך מחדש את ההחלטה על הצטיידות במערכת, וכן לבחון השלכות עתידיות מפריסת מערכת זו ומערכות נוספות הצפויות להיכנס לשירות בקרוב.

מאמר זה נכתב בחודש אוגוסט 2012, בעקבות כמה סבבי הסלמה בירי רקטות מרצועת עזה. בעקבות מבצע "עמוד ענן" שוכתב המאמר ועודכן.

## רקע

מערכת "כיפת ברזל" היא מערכת ליירוט רקטות ופגזי ארטילריה (בעלי טווח של עד 70 ק"מ).[2] המערכת פותחה על ידי רפאל (בשיתוף אלת"א – המייצרת את מכ"ם המערכת, ועם אמפרסט (mPrest) – האחראית על תוכנת השליטה והבקרה). המערכת מבוססת על יירוט הרקטות באמצעות טיל מיירט (טמי"ר) ייחודי. סוללת "כיפת ברזל" כוללת מערכת מכ"ם, מרכז שליטה ושלושה משגרי טילי טמ"יר, הנושאים 20 מיירטים כל אחד. אחד מיתרונותיה החשובים של המערכת הוא

יפתח שפיר הוא חוקר בכיר וראש פרויקט המאזן הצבאי במזרח התיכון, במכון למחקרי ביטחון לאומי

יכולתה לזהות את נקודת הפגיעה הצפויה של הרקטה המאיימת, להעריך האם היא תיפול באזור מיושב או לא, ולהחליט על העסקתה או אי־העסקתה בהתאם לכך. כך נחסכת העסקה מיותרת של רקטות שייפלו באזורים פתוחים, וממילא לא יגרמו נזק.

פיתוח המערכת החל עוד בשנת 2005, ביוזמתו של ראש היחידה למחקר ופיתוח במשרד הביטחון (מו"פ), תא"ל ד"ר דני גולד, אולם קיבל דחיפה בעקבות מלחמת לבנון השנייה בקיץ 2006. בשנת 2007 הוחלט במשרד הביטחון על הצטיידות במערכת ועל פיתוחה בקצב מואץ. ירי הרקטות מעזה במהלך מבצע "עופרת יצוקה" זירז עוד יותר את פריסת המערכת. כך בוצעו הניסויים הסופיים במערכת בסוף שנת 2010, ובראשית שנת 2011 נמסרה הסוללה הראשונה לידי חיל האוויר. בסוף חודש מרס הורה הרמטכ"ל, בהנחיית שר הביטחון, על פריסת המערכות להגנת אזרחים. ב־28 במרס נפרסה סוללה ראשונה באזור באר־שבע, ושבוע לאחר מכן נפרסה סוללה שנייה להגנת אשקלון. ב־7 באפריל 2011 יורטה הרקטה הראשונה על ידי "כיפת ברזל" – רקטה שנורתה מרצועת עזה לכיוון אשקלון.

סדר הכוחות של "כיפת ברזל" עומד על חמש סוללות. סוללה שלישית הצטרפה למערך בחודש יוני 2011 והסוללה הרביעית – במרס 2012, ואילו הסוללה החמישית, שתוכננה במקור להצטרף למערך בראשית 2013, הוחשה במהלך מבצע "עמוד ענן" ונפרסה להגן על אזור גוש דן.[3] עד סוף 2013 צפויות להיות בסדר הכוחות תשע סוללות,[4] ובסך־הכול מתוכננת כיום רכישה של 13 סוללות.[5] כבר במהלך "עמוד ענן" החליטה ועדת השרים לענייני הצטיידות להקצות עוד 750 מליון ש"ח להרחבת ההצטיידות ב"כיפת ברזל".[6] קליטתן של הסוללות מחייבת גיוס והכשרה של מספר רב של לוחמים, הן למערך הסדיר והן למערכי המילואים.

## ירי מבצעי

כאמור לעיל, יירוט מבצעי ראשון על ידי "כיפת ברזל" התקיים באפריל 2011. כעבור שנה, באפריל 2012, כבר הגיעה המערכת ל־93 יירוטים באירועים שונים.[7] שני סבבי ההסלמה החמורים ביותר היו בחודש אוגוסט 2011 בעקבות פיגוע הירי ליד אילת, עת שוגרו לעבר ישראל במשך שישה ימים 145 רקטות ו־46 פצצות מרגמה, ובחודש מרס 2012, כאשר במשך שלושה ימים נורו על ישראל 173 רקטות "גראד" ו"קסאם" ו־37 פצצות מרגמה, בעקבות חיסולו של פעיל ועדת ההתנגדות, זוהיר אל־קייסי.[8]

בסבב ההסלמה באוגוסט 2011 נגרמו, על אף הצלחות היירוט של "כיפת ברזל", לא מעט נזקים לרכוש ונפגעים בנפש, כולל 19 פצועים והרוג אחד (בבאר־שבע). בחודש מרס 2012 נפצעו ארבעה בני־אדם כתוצאה מֵרֵי הרקטות. לגבי סבב זה

פורסמו גם נתונים המאפשרים להעריך את אפקטיביות "כיפת ברזל" בלחימה אמיתית: המערכת יירטה בהצלחה 56 רקטות, מתוך 73 רקטות שהועסקו. (פירושו של דבר ש־100 מן הרקטות שנורו כוונו לעבר שטחים פתוחים, שם לא גרמו נזק). זהו שיעור הצלחה של 76.7% – שיעור מכובד לכל הדעות.[9]

הצלחתה הבולטת ביותר של "כיפת ברזל" הייתה במהלך מבצע "עמוד ענן" – בין ה־14 ל־22 בנובמבר 2012. המבצע החל בשעות אחר הצהרים של ה־14 בנובמבר, בחיסולו של בכיר חמאס, אחמד ג'עברי. עד הפסקת האש בשעות הערב של ה־21 בנובמבר נורו על ישראל 1506 רקטות. מתוכן נפלו 875 רקטות בשטחים פתוחים, ועל כן לא הועסקו על ידי "כיפת ברזל". עוד 152 שיגורים הוגדרו כשיגורים כושלים (והכוונה כנראה לרקטות שנפלו בשטח רצועת עזה עצמה). "כיפת ברזל" יירטה 421 רקטות, ו־58 רקטות נפלו בשטחים בנויים וגרמו נזקים. משיגורי הרקטות נהרגו חמישה ישראלים ונפצעו 240. על פי הודעת דובר צה"ל, השיגה "כיפת ברזל" שיעור הצלחה של 84%.[10]

מבצע "עמוד ענן" הוכיח את יכולתה של המערכת, שזכתה בצדק רב לשבחים, אך הלקחים מן המבצע מורכבים יותר. במבצע הוכחה גם חשיבותה העצומה של ההגנה הפסיבית: ההתרעה המוקדמת לתושבים באמצעות אזעקות והמיגון הפסיבי. אחת הדוגמאות הבולטות הייתה מקרה הפגיעה בבנין מגורים בראשון־לציון, כאשר רקטה הרסה דירה, אך הדיירים שישבו במרחב המוגן יצאו ללא פגע. תוצאות המבצע הוכיחו גם שלא תיתכן הגנה של מאה אחוזים.

## ביקורת

פריסת מערכת "כיפת ברזל" זכתה, לצד השבחים, גם לביקורת לא־מעטה מכיוונים שונים ומסיבות שונות. נטענו טענות חריפות כלפי מערכת הביטחון, הן בשל הבחירה במערכת "כיפת ברזל" על פני מערכות אחרות, שלדברי המבקרים עדיפות עליה, הן בשל הפצת הבטחות הגנה שלדברי המבקרים אינן מציאותיות, ונגד ההשקעה הגדולה במערכת.[11] להלן תוצג הביקורת על מערכת "כיפת ברזל" במספר רמות של ניתוח – טכנית־טקטית, מבצעית, ומדינית.

### ביקורת טכנית–טקטית

ראשית – יש לומר שמבחינה טכנולוגית השיגה המערכת הצלחה יוצאת דופן וייחודית. "כיפת ברזל" היא מערכת ייחודית, ואין כמוה בשום מקום בעולם. קיימת רק מערכת נשק מבצעית נוספת בעולם המיועדת ליירט רקטות קצרות־טווח ופצצות מרגמה: מערכת "סנטוריון" של צבא ארצות־הברית (מערכת זו מבוססת על מערכת התותח הימי "פאלאנקס" (Phalanx). היא מיירטת רקטות ופצצות מרגמה בטווחים קצרים באמצעות תותח מהיר בקוטר 20 מ"מ. ה"סנטוריון"

שימש להגנה על כוחות צבא ארצות־הברית ועל מתקנים אמריקאיים בעיראק – בפרט ב"אזור הירוק" בבגדאד – אזור מבוצר ששימש כמרכז השליטה של פעילות ארצות־הברית בעיראק, שהיה נתון לתקיפות חוזרות ונשנות.

מערכות אחרות מוצעות או נמצאות בפיתוח במקומות שונים בעולם. המוּכרת ביותר בארץ היא מערכת "סקייגארד" (Skyguard), המוצעת על ידי חברת נות'רופ גראמן (Northrop Grumman Corporation). המערכת מבוססת על מערכת הלייזר הטקטי "נאוטילוס" שפותחה בישראל בשנות התשעים. לטענת תומכיה פיתוחה הושלם – אך היא לא נרכשה ואינה מבצעית בשום מקום בעולם.[12]

בין הטיעונים נגד "כיפת ברזל" אפשר למנות ארבעה טיעונים ברמה הטכנולוגית: א. אי־יכולתה להתמודד עם איומים בעלי טווחים קצרים במיוחד. טווח המינימום של המערכת לא פורסם, אך לדברי המבקרים היא אינה יכולה ליירט רקטות או פגזים שטווחם קצר מ־5–7 ק"מ, וממילא אינה מסוגלת ליירט פצצות מרגמה. במהלך פיתוח המערכת פורסם כי היא תגן על יישובי 'עוטף עזה', ובין האיומים הוזכרו גם פצצות מרגמה, שטווחן בדרך כלל אינו עולה על קילומטרים ספורים. יש לציין כי הבטחות כאלה הושמעו בדרך כלל מצד גורמים פוליטיים, ולא על ידי מתכנני המערכת. מבקרים אלה טוענים שהיה על מערכת הביטחון להעדיף רכישת מערכות קיימות – "סקייגארד" או "סנטוריון" – או לשלב מערכות אלו לצד "כיפת ברזל" על מנת לכסות את הטווחים הקצרים יותר.[13]

ב. כפועל יוצא מזמן התגובה של המערכת היא תתקשה, לדברי המבקרים, להתמודד גם עם רקטות שיירו במסלולים שטוחים בטווחים גדולים עוד יותר – עד 18–16 ק"מ, לדברי המבקרים.

ג. מחיר היירוט גבוה. מחירו של מיירט "טמי"ר" הוא כ־40–50 אלף דולר. יתרה מזו, בחלק מן היירוטים נורים שני מיירטים לעבר מטרה אחת, מה שמייקר עוד יותר את היירוט. הדבר יגביל מאוד את יכולתה של מדינת ישראל להצטייד במיירטים לעימות ממושך.[14]

ד. למערכת יש "נקודת רוויה" – היא מסוגלת להעסיק מספר מסוים (שכמובן אינו מפורסם) של מטרות בעת ובעונה אחת – ולא יותר. רקטות נוספות שיירו במסגרת מטח צפוף כזה יוכלו לחדור ולפגוע.

אין בכוונת כותב שורות אלו להיכנס לדיון טכנולוגי. יֵאמר רק שלכל מערכת מהמערכות שהוזכרו (כמו לכל מערכת טכנולוגית) יש מגבלות. בסופו של דבר, הדיון חייב לשקלל את כל ההיבטים – לא רק את ההיבט הטכנולוגי.

**ביקורת מבצעית**

מבצע "עמוד ענן" וכן סבבי ההסלמה שקדמו לו הוכיחו ש"כיפת ברזל", על אף הצלחותיה, אינה מעניקה הגנה מלאה. רקטות חדרו את ההגנה, נגרמו נזקים לרכוש ונפגעים בנפש.

אולם האירועים המחישו גם שהבעיה האמיתית לא הייתה הנזק הפיזי שהרקטות גרמו – נזק שהיה בסופו של חשבון זניח, וגם לא האובדן בנפש – מצער ככל שיהיה, אלא העובדה שבכל אחד מן האירועים, כמיליון מתושבי מדינת ישראל נאלצו לשבת במקלטים, בתי ספר ומוסדות חינוך אחרים נסגרו בהוראות פיקוד העורף, ועל כן עובדים רבים לא התייצבו במקומות עבודתם – שכן הורים נאלצו להישאר בבית עם ילדיהם.

נוסף לנזק הכלכלי נגרם גם נזק למורל התושבים, שחשו חסרי ישע לנוכח התקיפות. הצד השני של אותה מטבע התבטא בעצרת ניצחון שקיים הג'יהאד האסלאמי בעזה בחודש מרס האחרון. מבחינת הג'יהאד האסלאמי, עצם הניצחון היה תחושה זו של הציבור הישראלי.[15] מצב זה חזר ונשנה בסיומו של "עמוד ענן". שוב חזרה הדגשת העובדה שעבור חמאס – הניצחון היה בעצם יכולתו לפגוע באוכלוסייה האזרחית בישראל, ולהתמיד בכך על אף התקפות חיל האוויר. מסיבה זו – הפגיעה ב"גוש דן" הייתה עבורו הישג נכבד.[16]

חשוב לציין כי הבעיה אינה ייחודית ל"כיפת ברזל". זוהי בעיה המאפיינת כל מערכת נשק הגנתית. גם אם היו לישראל 12 או 20 סוללות "כיפת ברזל" וגם אם הייתה מערכת נשק היפותטית טובה בהרבה מ"כיפת ברזל" כפי שהיא כיום – המצב העקרוני לא היה משתנה. בכל מקרה של התקפת רקטות על ישראל עדיין היה צורך להפעיל את הצופרים, פיקוד העורף עדיין היה צריך להוציא התרעות והנחיות לתושבים להיכנס למרחבים המוגנים, והנזק הכלכלי, כמו גם הנזק המורלי, היו נגרמים באותה מידה.

מכאן עולות שתי שאלות קשות:

ראשית – כמה סוללות "כיפת ברזל" צריכה מדינת ישראל? עִקבת ההגנה של סוללת "כיפת ברזל", לדברי מפתחיה, היא כ־100 קמ"ר, ולדברי מתנגדיה – הרבה פחות. שטח זה אינו גדול.[17] כדי להגן על אוכלוסיית כל היישובים בארץ במצב של מלחמה עם לבנון – יהיה צורך בעשרות רבות של סוללות. מאחר שמספר הסוללות שיירכשו חייב להיות מוגבל (וכך גם מספר המיירטים), תעלה בכל חריפותה השאלה "על מי להגן, ועל מי לא להגן?"

שנית – ושאלה זו נובעת ישירות מן השאלה הקודמת – האם יש בכלל טעם להגן על אוכלוסייה אזרחית? אם בידינו מערכת הגנה כה יקרה, האם לא עדיף להגן על מתקנים אסטרטגיים, ששרידותם חשובה לתפקודה התקין של המדינה? שאלה זו מתחדדת עוד יותר כאשר בוחנים את הצטיידות האויב, ובפרט – של חזבאללה.

מערכות הטילים שבידיו משתפרות – לא רק בטווחים וביכולת לכסות שטחים גדולים יותר ויותר של מדינת ישראל – אלא בעיקר בדיוק.[18] כל עוד הנשק שבידיו הוא נשק בעל פיזור סטטיסטי – אין טעם להשתמש בו נגד מתקנים אסטרטגיים, שכן הסיכוי לגרום להם נזק נמוך. עדיף לו להשתמש במערכות הטילים כנשק טרור נגד אוכלוסייה אזרחית. אולם כאשר הנשק מדויק יותר (וגם יקר יותר, ועל כן מצוי בכמויות קטנות יותר), התועלת המרבית ממנו תושג דווקא על ידי הפנייתו לעבר מטרות כאלה. על המתגונן, לפיכך, להפנות את משאביו להגנת אותם מתקנים – ולא להגנת האוכלוסייה.

ממערכת שיקולים זו עולה כי ההשקעה במערכות הגנה אקטיבית על אוכלוסייה אזרחית היא השקעה מיותרת. ניתן אמנם להקטין את הנזק לרכוש ולנפש במידה מסוימת, אך לא ניתן להגן על כל האוכלוסייה – אפילו לא על חלקה הגדול. חמור מכך הוא שכלל לא ניתן למנוע את הנזק האמיתי של התקפות הרקטות – הנזק לכלכלת המדינה וליכולת התפקוד התקין. אם כבר הושקע הכסף בפיתוח מערכת הגנה נגד רקטות – עדיף להשתמש בה כדי להגן על מתקנים אסטרטגיים ולא על אוכלוסייה.

לאור שיקולים אלה, ההשקעה ב"כיפת ברזל" נראית לכאורה מיותרת לחלוטין. אולם אין זה השיקול היחידי.

## הרתעה

טיעון חשוב בהחלטה על פריסת מערכות הגנה בכלל, ו"כיפת ברזל" בפרט הוא תרומתן להרתעה הישראלית. שני טיעונים עיקריים עולים בדיון מסוג זה:

ראשית, הטיעון שהגיונו הוא שהצלחת היירוטים תבהיר לאויב ששיגורי הרקטות שלו הם חסרי תוחלת, ובסופו של דבר יתייאש מהפעלתן. גם אם נתעלם לרגע מכך שטיעון כזה הוא אנטי־תזה לכל תיאוריית הרתעה קלאסית, (שעל פיה הרתעה מושגת על ידי איום בעונש, ולא על ידי מניעת הצלחה)[19] – קשה להבין את הטיעון, ועוד יותר קשה להעריך את תקפותו על סמך הניסיון שהצטבר. ברמה העקרונית – כישלון בהפעלת נשק התקפי עלול להביא אמנם לייאוש מניסיון נוסף להפעילו, אך עשוי גם לעודד מציאת פתרונות שיאפשרו להתגבר על ההגנה שפיתוח היריב.

בפועל, מצד אחד ניכר שארגוני הטרור בעזה אינם מתעלמים מהשפעת "כיפת ברזל" על הצלחותיהם, גם כשהם עצמם מציגים את האירועים כהצלחה, ואת הצלחת "כיפת ברזל" כחסרת משמעות.[20]

מאידך גיסא, אפשר למצוא רמזים למאמצי הצד השני למצוא פתרונות אפילו בדיווחים של אנשי "כיפת ברזל" עצמם, המדווחים על שינויים בנוהלי ההפעלה של הרקטות על ידי ארגוני הטרור בעזה. נראה ששינויים אלה נועדו לנסות להתגבר

על ההגנה (כנראה – ניסיונות לשגר מטחים צפופים על מנת לנסות להתגבר על ההגנה).[21]

שנית, קיים הטיעון שעלה אחרי הצלחת "כיפת ברזל" בסבבים האחרונים – המערכת העניקה חופש פעולה למקבלי ההחלטות.[22] ההיגיון המשתמע מטיעון זה הוא שלולא הצלחת "כיפת ברזל" היה נגרם לישראל נזק חמור בהרבה, ומקבלי ההחלטות היו מוצאים את עצמם נאלצים ליזום מבצע התקפי דוגמת "עופרת יצוקה". כעת, עם הצלחת המערכת, יש למקבלי ההחלטות רמת חופש גבוהה יותר להחליט האם לתקוף או לא, ומתי. טיעון זה בלט במיוחד בפרשנויות שפורסמו סביב מבצע "עמוד ענן", שהסתיים, כידוע, ללא פעולה קרקעית. טיעון זה הושמע, כמובן, מפי אלה שסברו שתקיפה קרקעית בעזה אינה רצויה.

לטיעון זה גם צד הפוך, שגם הוא עלה בדיונים, במהלך "עמוד ענן" ובמהלך סבבי ההסלמה שקדמו לו: הטיעון של תומכי הפעולה הקרקעית, הטוענים ש"כיפת ברזל" הפכה ל'עלה התאנה' של מקבלי ההחלטות, שמלכתחילה לא רצו במבצע קרקעי.[23]

הטיעון על שני צדדיו בעייתי. גם בעבר ספגה ישראל התקפות רקטות וטילים. בעבר, בהעדר כל אופציית הגנה, השתמשה ישראל בעיקר בהשמעת איומים הרתעתיים כלפי האויב. עם זאת, מעולם לא חשו מנהיגי ישראל שאין להם דרגת חופש להחליט האם לתקוף את האויב או לא, ומתי.[24] הטיעון שללא מערכת נשק זו או אחרת יימָנע ממקבלי החלטות שיקול הדעת דומה להבעת אי־אמון ביכולתם של מקבלי החלטות לשקול ולהחליט החלטות מושכלות.

## החלטות פוליטיות

הרמה השלישית של הניתוח היא נקודת המבט של מקבלי ההחלטות בדרג הפוליטי. כאן נכנסים שיקולים שונים לחלוטין.

**ראשית**, שיקול תרומת המערכת למורל האוכלוסייה האזרחית, בפרט באזורי פריפריה, שממילא מרגישים לא פעם מוזנחים על ידי הממשלה. רמז לכך ניתן לקבל מתוך קטעי וידאו שהועלו על ידי אזרחים לאתר "יוטיוב", הן במהלך סבבי ההסלמה במרס וביוני, והן במהלך "עמוד ענן". בקטעים אלה אפשר לראות את נקודת המבט של האזרחים. הרבה לא ניתן לראות בקטעים אלה: נקודה זוהרת בשמים מתנגשת בנקודה אחרת, ברק של פיצוץ קטן במרחק. אבל ברקע אפשר לשמוע את צהלות התושבים שצפו ביירוט המוצלח. הדבר בא לידי ביטוי ביתר תוקף בכותרות העיתונים במהלך מבצע "עמוד ענן".[25]

המשמעות היא אדירה. "כיפת ברזל" לא רק תרמה למורל האוכלוסייה. היא תרמה תרומה חשובה לחוסן האוכלוסייה האזרחית בכלל. היא הוכיחה להם שצה"ל עושה הכול על מנת להגן עליהם.

**שנית**, מנקודת מבטו של מקבל ההחלטות הפוליטי, ברגע שקיימת אפשרות טכנית כלשהי להגן על הציבור מפני תקיפות הרקטות – הוא יתקשה להחליט נגד רכישת מערכת כזו. מנהיג פוליטי במדינה דמוקרטית יתקשה מאוד לעמוד בפני קהל בוחריו ולומר לו "הטכנולוגיה קיימת, אבל החלטתי לא לרכוש אותה". יהיו נימוקיו כבדי־משקל ככל שיהיו, סיכוייו של מנהיג כזה להצליח להיבחר פעם נוספת יתדרדרו. הציבור יתקשה לקבל החלטה כזו.

הדרגים המבצעיים של צה"ל למדו זאת בדרך הקשה. כל עוד מערכת "כיפת ברזל" הייתה בשלבי פיתוח, לא הייתה בעיה להכריז שמפתחים מערכת להגנת האזרחים, אולם ברגע שהמערכת הראשונה נמסרה לצה"ל הופעל השיקול המבצעי, וצה"ל הגיע למסקנה (הסבירה והמתקבלת ביותר על הדעת, כפי שהוצג לעיל) שהתועלת המרבית ממערכת כזו תהיה בהגנה על מתקנים אסטרטגיים חשובים, כמו בסיסי צה"ל, וההפעלה המיטבית שלה תהיה כאשר המערכת תמוקם בבסיס צבאי, ותצא ממנו לפי הצורך המבצעי. ההחלטה עוררה תגובות מיידיות ומחאות חריפות בקרב הציבור, בפרט, כמובן, באזורים שהיו נתונים לאיום הנשק הרקֶטי. מהר מאוד נאלץ הדרג המדיני להורות לצה"ל לפרוס את המערכות להגנת יישובים אזרחיים.

**שלישית**, קיים היבט הבסיס הטכנולוגי והתעשייתי של ישראל. תפיסת הביטחון של ישראל ראתה תמיד בתעשייה הביטחונית מרכיב חשוב ביותר בביטחון ישראל. כדי לשמר בסיס זה, התעשייה צריכה לקבל הזמנות ממערכת הביטחון על מנת לשמר את יכולתה לייצר, ועל מנת לתמוך במכירות מערכות נשק בחו"ל. אולם מעבֶר למכירת מוצרים, חשוב לתעשייה לקבל אתגרים טכנולוגיים. בעבר היו אתגרים אלה בפרויקטים גדולים דוגמת מטוס ה"לביא", מערכת ה"חץ" ומערכות רבות נוספות. אתגרים אלה הם המנוע הדוחף את התעשייה לרמות טכנולוגיות גבוהות, והם שהביאו אותה למעמדה הנוכחי כאחת המובילות בעולם. בהיבט זה, גם פרויקטים שלא התממשו בסופו של דבר, כמו פרויקט מטוס ה"לביא", תרמו תרומה גדולה לאין שיעור להתקדמות התעשייה. (שיקול זה גם עמד, ככל הנראה, בהחלטת מערכת הביטחון להעדיף את מערכת "כיפת ברזל" על פני מערכות מתחרות מתוצרת חוץ).

**שיקול רביעי** – מערכת היחסים ההדוקה של ישראל עם ארצות־הברית. מערכת יחסים זו היא אחד מעמודי התווך של ביטחון ישראל. בתוך מערכת זו מהווה שיתוף הפעולה בנושאי הגנת טילים מרכיב מפתח, משום חשיבותה הגדולה של הגנת הטילים באסטרטגיה של ארצות־הברית. כך ניתן להבין את שיתוף הפעולה בפיתוח ובייצור מערכת ה"חץ" ומערכת "שרביט קסמים", ואת ההקצאות המיוחדות שהקצה ממשל אובמה – במסגרת בקשת התקציב שלו מן

הקונגרס – למענקים לישראל לרכש סוללות "כיפת ברזל" נוספות (הקצאות שהן מעבר לסיוע הביטחוני הכולל).

## שאלות פתוחות

"כיפת ברזל" לא עמדה עדיין במבחנים קשים מאוד. שאלה פתוחה היא, מה תהיה תרומתה האמיתית במקרה של התקפת רקטות מסיבית מלבנון. בקיץ 2006 ספגה ישראל מטח של 4000 רקטות במשך חודש ימים. כיום, מאגרי הנשק של חזבאללה גדולים בהרבה, ומוערכים ב־40,000–50,000 רקטות. מִתאר לחימה אפשרי עשוי לכלול ירי של כמה אלפי רקטות מדֵי יום.

להגנה במתאר כזה יש כמה היבטים.

**ראשית** – על מה להגן ועל מה לא להגן. במקרה זה, השאלה שנשאלה לעיל תצוף בכל חומרתה: 'האם "כיפת ברזל" צריכה להיפרס בפריסה חלקית על מנת להגן על אוכלוסייה אזרחית – חלק מן האוכלוסייה, כמובן – רק כדי לתרום למורל, או שמא לרכז את הסוללות הקיימות להגנה על אותם מתקנים ששרידותם תהיה חיונית לתפקודה של המדינה?'

**שנית** – קיימת שאלת יכולתה של המערכת להיות אפקטיבית, גם באזורים המוגנים. גם אם יוחלט להגן במתאר כזה על יישובים אזרחיים מסוימים (ודאי לא על כולם), האם המערכת תהיה אפקטיבית? האם יכולתה להקטין את הנזקים תהיה כזו שתורגש בכלל במתאר כה חמור? ואם התשובה היא שלילית, מה תהיה תגובת הציבור על הנזק שיספוג, והאם היא תאבד את תרומתה למורל האוכלוסייה ולחוסנה?

**שלישית** – השאלה שתישאר תמיד פתוחה לדיון פוליטי מסוג אחד היא "עד כמה". ההחלטה להצטייד במערכות כמו "כיפת ברזל" הייתה החלטה אחת. החלטות מסוג אחר לגמרי הן "כמה סוללות לרכוש? "על מה להגן?" "האם נמגן את עצמנו לדעת?"

באוגוסט 2012 פרסם דובר צה"ל שרבים מאוד ממגויסי השנה ליחידות הקרביות הביעו את רצונם להגיע ליחידות "כיפת ברזל". הדבר ממחיש את חומרת הבעיה, שכן השקעת משאבים בהתגוננות היא בהכרח על חשבון משאבים ליכולת התקפית. גם אם יימצא פתרון בהיבט הכספי, ויימָצאו תקציבים נוספים להתגוננות – מאגרי כוח האדם של מדינת ישראל נותרים כפי שהם. כשכותב שורות אלה היה על סף גיוס, ה"להיטים" בקרב המתגייסים היו קורסי טיס, הצנחנים והסיירות. השינוי הוא עמוק ויסודי. אם בעבר ביססה ישראל את ביטחונה על יכולתה ההתקפית, כיום, יותר ויותר ממשאביה ומכוחה מוקדש להתגוננות.

## סיכום

ישראל היא המדינה הראשונה בעולם שפורסת מערכת מבצעית נגד רקטות להגנה על אוכלוסייתה האזרחית. אולם מדינות מעטות מאוד בעולם סבלו תקיפות על אוכלוסייתן האזרחית במשך תקופה ממושכת כל כך, וברמת חומרה כזו. לפיכך, אין זה פלא שישראל השקיעה משאבים כה רבים בחיפוש אחר פתרונות לבעיה.

הפתרון שנבחר לא נבחר בלי מחלוקות. מתנגדי הפרויקט הצביעו על כמה מפגמיה של המערכת. אחדים מפגמים אלה טבועים בכל מערכת, אחרים הם ייחודיים למערכת, שככל מערכת סובלת מפגמים טכניים כאלה או אחרים. מתנגדים אחרים מצביעים גם על העלות הגבוהה של המערכת, וטוענים שיש פתרונות טכנולוגיים אחרים ועדיפים.

הניתוח דלעיל מראה שקבלת החלטות היא תהליך מורכב המביא בחשבון סוגי שיקולים שונים, שהשיקול המבצעי הוא רק אחד מהם. שיקולים חברתיים, פוליטיים ואף בינלאומיים אינם חשובים פחות, ואולי אף חשובים יותר. לנוכח מגוון שיקולים אלה, ההחלטה להצטייד במערכות הגנה נגד רקטות נראית החלטה נבונה.

השיקולים המכריעים בקבלת ההחלטה היו, לדעתי, השיקולים המדיניים והפוליטיים. אותם שיקולים אדישים להבדלים הטכניים בין המערכות השונות. לפיכך, אני סבור שכל ויכוח בשאלת החלופות הטכניות – "כיפת ברזל" או כל מערכת אפשרית אחרת – הוא ויכוח עקר לחלוטין.

ההחלטה הקשה יותר חייבת להיות ההחלטה להגביל את מידת ההשקעה ביכולת הגנתית, כדי לא לפגוע ביכולת ההתקפית של צה"ל. החלטה זו מחייבת דיון מעמיק ביחסים בין הגנה והתקפה בכלל. מערכת "כיפת ברזל" היא רק קצה הקרחון של דיון מקיף זה, שהיקפו חורג בהרבה מתחום מאמר זה.

## הערות

1 שימוש ראשון במשגרי רקטות כנגד ישראל היה ב־16 בספטמבר 1968, כאשר 8 רקטות בקוטר 130 מ"מ נורו מכיוון ירדן לעבר בית־שאן. (סופר 'דבר': "לראשונה הפעילו החבלנים נשק כבד בעת ההפגזה בבית שאן" **דבר**, 18 בספטמבר, 1968. ראו bit.ly/U2cTmq Jpress.org.il

2 הנתון מאתר www.rafael.co.il.

3 יעל לבנת ויפתח כרמלי,"חיל האוויר פרס סוללה חמישית של כיפת ברזל", **דובר צה"ל**, 17 בנובמבר 2012. ראו http://bit.ly/11wfOdD

4 הודעת שר הביטחון ברק, כפי שפורסמה על ידי דובר צה"ל ב־21 באוגוסט, 2012. ראו bit.ly/11bICrC

5 ידיעת Janes Defense Weekly מה־2 בספטמבר 2009. זה גם מספר הסוללות שאושר על ידי ועדת החוץ והביטחון בפברואר 2011 (ידיעת UPI מה־11 בפברואר 2011). על מספר זה חזר השר ברק בדבריו לתקשורת במהלך "עמוד ענן" (**הארץ** – עדכונים שוטפים במהלך "עמוד ענן" – 18 בנובמבר, 2012, 15:38).

6 מתן חצרוני, "כיפת ברזל תשודרג ב־750 מ' ש"ח". חדשות ערוץ 2 באינטרנט, 20 בנובמבר, 2012.

7 יעל לבנת, "שנה ליירוט הראשון של כיפת ברזל: ההצלחה בזכות הלוחמים" אתר דובר צה"ל, 5 באפריל 2012. ראו http://bit.ly/Yo4uRS

8 הנתונים הם מן הדוחות החודשיים באתר השב"כ www.shabak.gov.il

9 יעל ליבנת, שם.

10 מערכת אתר צה"ל, "סיכום מבצע עמוד ענן" 21 בנובמבר 2012. ראו http://bit.ly/10QRIKf. לפי חשבוני – 479 רקטות כוונו לאזורים בנויים (421 שיורטו ועוד 58 שפגעו). יירוט 421 מ־479 מהווה שיעור הצלחה של 87.8%. זהו שיעור ההצלחה של המערכת ולא של המיירט היחיד. על אף שבמספר קטעי וידאו שפורסמו נראים המיירטים יוצאים בזוגות – לא ניתן להסיק מכך שלעבר כל רקטה משוגרים שני מיירטים.

11 הביקורת העקרונית נגד מערכות הגנת טילים נשענת במידה רבה על הביקורת הרבה שזוכות לה מערכות הגנת הטילים האסטרטגית של ארצות־הברית. בארץ בלט בכך ד"ר ראובן פדהצור, (שהסתמך בעבודתו על עבודותיו של Ted Postol מ־MIT). פדהצור פרסם מתחילת שנות התשעים מאמרים רבים נגד פיתוח ה"חץ". בהמשך גם ביקר באופן דומה את הניסיונות לפתח מערכת הגנה נגד רקטות: בסוף שנות התשעים הייתה זו מערכת "נאוטילוס", ובהמשך – "כיפת ברזל". (ראו ראובן פדהצור, **מערכת החץ וההגנה האקטיבית נגד טילים בליסטיים – אתגרים ושאלות**, המרכז למחקרים אסטרטגיים ע"ש יפה, מזכר מס' 42, אוקטובר 1993. בנושא "כיפת ברזל" ראו: ראובן פדהצור, "כיפת ברזל חסרת אונים מול הקסאם" **הארץ**, 21 בפברואר, 2008. בין המבקרים את המערכת משיקולים טכנולוגיים בולטים התומכים במערכת הלייזר "סקייגארד", שהקימו לצורך העניין את עמותת "מגן לעורף". באתר האינטרנט של העמותה חומר רב בנושא. ראו http://www.magenlaoref.org.il ביקורת מסוג שלישי היא זו שהופיעה בדוחות מבקר המדינה שעסקה בצד הנְהָלי והכספי של תהליך קבלת ההחלטות על פיתוח המערכת.

12 ראו: "מענה לטענות משהב"ט באתר עמותת "מגן לעורף". http://bit.ly/WBLjib בחיפוש באתר החברה – northropgrumman.com כבר לא ניתן למצוא אזכור למערכת. (אם כי Google עדיין זוכר את דף המידע עליה).

13 אתר מגן לעורף http://bit.ly/TD1JFS. כאמור לעיל – אין נתונים רשמיים על טווח המינימום של "כיפת ברזל".

14 שם.

15 ראו: עמוס הראל, אבי ישראלי, "לקחי ההסלמה בדרום – כיפת ברזל העניקה לדרג המדיני הישג חשוב אך מוגבל", **הארץ**, 14 במרס 2012. בעברית – http://bit.ly/ACM5rZ; באנגלית – Israel's wake up call אתר **הארץ** מה־16 במרס 2012, http://bit.ly/whWYrn

16 דניאל סיריוטי, "חמאס הכריז על יום חג", **ישראל היום**, 22 בנובמבר, 2012. http://bit.ly/U9t6pX

17 חישוב פשוט יראה כי זה שטחו של מעגל שרדיוסו כ־5.6 ק"מ. יודגש, אגב, שעקבת הגנה של מערכות טילים – נגד מטוסים או נגד רקטות – אינה דווקא בצורת עיגול, נתון זה ניתן לצורכי המחשה בלבד.

18 רויטרס, אֵי פי, "נסראללה: באמצעות טילים מדויקים נוכל לפגוע במאות אלפי ישראלים", **הארץ**, 17 באוגוסט 2012, http://bit.ly/NJY202

19 יודגש שעל פי תיאוריית ההרתעה הקלאסית – נשק הגנתי אינו מרתיע. תיאוריה זו מניחה שהרתעה מושגת על ידי איום בנשק השמדה המונית – איום שמימושו אינו יכול להיות קביל על ידי הצד המורתע. אף על פי כן, הועלה השימוש במושג ההרתעה לעתים קרובות גם בדיונים על נשק הגנתי (כך בארץ בנושא ה"חץ" או "כיפת ברזל",

וכך בקשר למערכות הגנת טילים בעולם. הדיון התיאורטי בהרתעה באמצעות נשק קונוונציונלי ממילא מורכב בהרבה מן הדיון בהרתעה ה"קלאסית". ראו לדוגמה Stephen L. Quackenbush, "National Missile Defense and Deterrence", *Political Research Quarterly,* Vol. 59, No. 4 (December, 2006), pp. 533-541.

20 ראו: מאמר לא חתום "המלחמה על התודעה: הגם שסבב הלחימה האחרון ברצועה הסתיים במאזן שלילי בראייתם של ארגוני הטרור, הוא מוצג על ידם כ"ניצחון"." אתר מרכז המידע למודיעין וטרור על שם מאיר עמית, 22 במרס 2012. http://www.terrorism-info.org.il/he/article/17770

21 אחת הדוגמאות המרתקות הייתה מספר קטעי וידאו שהועלו לרשת במהלך "עמוד ענן", ומראים יירוט מספר גדול של רקטות בו־זמנית מעל שמי באר־שבע. אירוע זה מצביע, להערכתי, על ניסיונם של ארגוני המחבלים להביס את המערכת על ידי שיגור מספר גדול של רקטות בו־זמנית. מאידך גיסא, קטעים אלה מצביעים גם על יכולתה של מערכת "כיפת ברזל". ראו לדוגמה: שי מלול, "אזעקה בבאר שבע ו־12 יירוטים מוצלחים" http://www.youtube.com/watch?v=8kAyqbKwd1o. בקטע האמור אפשר לספור לפחות 14 מיירטי "כיפת ברזל" (רקטות הגראד אינן נראות). ניתן גם לספור פיצוצי פגיעה, אולם לא ניתן לדעת אילו מהם אכן יירוטים ואילו – השמדה עצמית של המיירטים.

22 הטיעון מועלה על ידי עוזי רובין. ראו: Uzi Rubin, "Iron Dome vx. Grad – a dress rehearsal for an all out war", *BESA* Center Perspectives, Papers No. 173, July 2012. http://bit.ly/Q1OZMx

23 כדוגמה למאמר התומך בתקיפה קרקעית, ראו Yori Yanover, "The Morally Reprehensible 'Iron Dome' – Hamas's Best Friend", *The Jewish Press* 19/11/2012http://bit.ly/XwD1Oy" כדוגמה למאמר מתנגד, ראו: ארי שביט, "לרדת מעמוד ענן" **הארץ**, 19 בנובמבר 2012, http://bit.ly/ZZNm48

24 כך היה בתקופות הקשות של מלחמת ההתשה. ראו למשל: סופר דבר בטבריה, "בעקבות הפגזת הקטיושות השניה נגד קרית שמונה – אזהרות חמורות ללבנון מפי ראש הממשלה ושר הבטחון", **דבר**, 12 במאי 1970.

25 ראו למשל: אנשיל פפר, "המושלים בכיפה" מאחורי הקלעים של "כיפת ברזל", **הארץ**, 23 בנובמבר, 2012. http://bit.ly/10oK9v5. ביטוי נוסף לתחושת הציבור אפשר היה לראות ברשתות החברתיות. ל"כיפת ברזל" הוקמו דפי פייסבוק (כיפת ברזל, Iron dome count) שזכו לאלפי "אוהבים" (לייקים). ביטוי מעניין להאדרת "כיפת ברזל" היו כתבות ששיבחו את החלטותיו של עמיר פרץ בתקופת כהונתו כשר ביטחון. ראו למשל: מוטי בסוק, "מי היה הראשון לזהות? כך נולדה כיפת ברזל", **הארץ**, **דה מרקר**, 19 בנובמבר, 2012. bit.ly/Xr2jxy

# כיצד לקבוע את הנורמות הראויות של הלחימה במצבים חדשים?

## סוגיה ביחסים בין "מוסר לחימה" לבין "דיני לחימה"[1]

**אסא כשר, עמוס ידלין**

דוקטרינה אתית של לחימה בטרור היא מערכת עקרונות המבטאים תפיסה סדורה בדבר הדרכים הראויות לניהול הלחימה בטרור. דוקטרינה כזו מתווכת בין הערכים המופשטים בסגנון "רוח צה"ל", האמורים להדריך את ההתנהגות של אנשי הצבא בכל הנסיבות של פעילותם, לבין הנהלים, הוראות הפתיחה באש והפקודות, האמורים להדריך את ההתנהגות של אנשי הצבא בנסיבות של לחימה מסוג מסוים, בזמן מסוים, במקום מסוים.

הדוקטרינה האתית שברקע מאמר זה וברקע המאמרים שהתפרסמו בגיליון הקודם של בטאון זה היא הדוקטרינה האתית של הלחימה בטרור, שפותחה בהקשר של המלחמה בין ישראל לבין ארגוני הטרור הפלסטיניים בעשור הראשון של מאה זו. פיתוחה נעשה על ידי מחברי מאמר זה בעזרת צוות שפעל במכללה לביטחון לאומי, בהשתתפות מומחים ללחימה בטרור ואנשי אתיקה ומשפט מצה"ל ומהאקדמיה. הדוקטרינה הוצגה בפורומים ממלכתיים שונים ולאחר מכן פורסמה בבטאונים מקצועיים.[2] למרות שמסמך הדוקטרינה לא אומץ באופן רשמי כתורת לחימה של צה"ל, שלושת הרמטכ"לים של תקופת הלחימה בטרור וקצינים רבים אחרים הביעו בהזדמנויות שונות תמיכה בעקרונותיה, והיא נתפסה בעיני רבים בתור הדוקטרינה הישראלית.

תיאורים תקשורתיים לא־מדויקים של הדוקטרינה עוררו תגובות מכל הסוגים, ביניהן תגובות של התנגדות לעיקרון זה או אחר שיוחס לנו כמחברי הדוקטרינה. תגובות כאלה באות לידי ביטוי גם במאמרים שהתפרסמו בגיליון הקודם. במאמר

אסא כשר הוא פרופסור לפילוסופיה באוניברסיטת תל-אביב, זוכה פרס ישראל אלוף (מיל.) עמוס ידלין הוא ראש המכון למחקרי ביטחון לאומי

הנוכחי ובמאמר המשך שיפורסם בהקדם נבהיר כמה היבטים של הדוקטרינה האתית של הלחימה בטרור, כפי שהצגנו אותה במאמרינו, נגיב על טענות אחדות שהועלו נגדה ונצביע על מספר עדכונים שלה, בעיקר בזיקה למצבים חדשים של לחימה בטרור בזירה הישראלית ובזירות של תימן, אפגניסטן, פקיסטן וסומליה, בין השאר.

## 1. דיון בדוקטרינה: הנחות רקע

בראשית הדברים, נבהיר את הגישה הכללית שלנו לדיון בדוקטרינה האתית של הלחימה בטרור.

"מעשיות": דוקטרינה של לחימה אמורה להוות בסיס להדרכה מעשית של מפקדים וחיילים בדבר פעילות הלחימה שלהם, במתכונת של נוהל, של הוראות פתיחה באש או של פקודה. לפיכך, יש לנו עניין רק בדיון המוביל למסקנות מעשיות, לכאן או לכאן, בדבר הפתרונות האפשריים והראויים של הבעיות המבצעיות המתעוררות בעת הצורך להגן על אזרחי המדינה ועל ריבונותה.

"אחריות": דיון בדוקטרינה אתית מנקודת מבט שתכליתה היא ביקורתית עלול להסתכם בהצבעה על היבטים לא־רצויים של מצבים העתידים להיגרם, אם יפעלו החיילים על פי הדוקטרינה. לנו יש עניין רק בדיון שתכליתו היא להוביל לשיפורים, כלומר, לתיקון הדוקטרינה או להחלפתה באחרת, כך שפעולה על פי הדוקטרינה החדשה תגרום להופעתם של פחות מצבים שיש להם היבטים לא־רצויים.

"אוניברסליות": הדוקטרינה האתית של הלחימה בטרור התגבשה במהלך השנים של הלחימה הישראלית בטרור הפלסטיני, כאשר אחד מאמצעי ההתגוננות המרכזיים הוא "הסיכול הממוקד". הדוקטרינה היתה אמורה לעמוד במבחן הזמן בכך שתוכל להוביל להתנהגות ראויה גם במצבים, במקומות ובזמנים אחרים. יש לנו עניין בדוקטרינה כללית שתדריך לא רק מבצעים של "סיכול ממוקד" במצבים מוכרים, אלא גם מבצעים של "סיכול ממוקד" במצבים חדשים, כדוגמת המבצע של ארצות־הברית בתימן, שהיה כרוך בהריגת אזרח ארצות־הברית כנזק אגבי,[3] או במבצעים מסוגים חדשים, כדוגמת המבצע של ארצות־הברית בפקיסטן, שבו נהרג בן־לאדן.[4]

"זהירות": בהקשרים של דיון מקצועי או אקדמי בדוקטרינה כלשהי, ההנחה המובנת מאליה היא שהמשתתפים בדיון למדו היטב את הדוקטרינה, כפי שהוצגה, ויש להם בסיס עובדתי מובהק בדבר תוכנה של הדוקטרינה, עקרונותיה והנימוקים שביסודה. ככל שהמדובר בדוקטרינה האתית שברקע מאמר זה, אין לנו מנוס מהצגת הדרישה הזאת להכרת הדוקטרינה, מפני שלעתים קרובות היא לא כובדה כראוי.

## 2. הדוקטרינה האתית והדין הבינלאומי: הקדמה

נקודת המוצא של הדוקטרינה האתית של הלחימה בטרור אינה הדין הבינלאומי. ההבדל בינינו לבין המומחים לדין בינלאומי אינו מקרי ובוודאי שאינו שרירותי. טעמי ההבדל הזה הם יסודיים וחשובים.

ראשית, **הטעם המוסרי**: בעינינו, ערכו של הדין הבינלאומי אינו בעצם קיומו אלא בתרומה שלו לשיפור המוסרי של העולם, בתחומי היציאה למלחמה והתנהלות הלחימה. כל נורמה של הדין הבינלאומי עומדת להערכה מוסרית. בהערכה כזאת, ייתכן שהנורמה תיחשב מוצלחת וייתכן שלא תיחשב כזאת. נקודת המוצא שלנו היא מוסרית.

שנית, **הטעם החוקתי**: הדין הבינלאומי מצטייר בעיני רבים כמערכת נורמות המחייבת את החייל הישראלי במישרין, מעין מערכת מקבילה למערכת הדין הישראלי, המחייבת אותו בהיותו אזרח המדינה וחייל צה"ל. אנחנו רואים את החייל הישראלי (כפי שהדין הישראלי רואה אותו) כפוף אך ורק לדין הישראלי, המחייב אותו, בין השאר, להישמע להוראות הדין הבינלאומי ככל שהמדינה קיבלה אותו על עצמה, או רואה אותו כמחייב אותה ואת הפועלים מטעמה. לפני שנורמה של הדין הבינלאומי מגיעה אל החייל, עליה לעבור במבחני התוקף שיש לה על פי דיני המדינה.[5]

שלישית, **הטעם ההיסטורי**: הדין הבינלאומי ההסכמי נוצר בהתפתחות היסטורית מורכבת על רקע תפיסות מסוימות בדבר טיבה של הלחימה ובדבר מגבלות שסביר להטיל עליה, מנקודת המבט של המנהיגים והיועצים הצבאיים שלהם. התפיסות הללו היו יפות לשעתן, ככל שהמדובר היה בעימות הקלאסי בין מדינה למדינה, במתכונת הקלאסית של עימות בין צבא אחד לצבא אחר. המגבלות שהוטלו על התפיסות הללו היו גם הן יפות לשעתן, ככל שהיה מקום להניח שבדרך כלל ישמרו הצדדים הלוחמים על הנורמות המגבילות אותם.[6] המגבלות עצמן היו מעשיות ואפילו פשוטות: ההבחנה בין הלוחמים לבין הלא־לוחמים, לדוגמה, נעשית במתכונת הפשוטה של הבחנה בין הלובשים מדים מסוימים לבין מי שאינם לובשים מדים כלשהם. ההנחות הללו עמדו ביסוד הנכונות של המנהיגים לקבל את הנורמות שבהסכמים הבינלאומיים.

כל התפיסות הללו אינן הולמות את עולם הלחימה בטרור. אין טעם בהנחה בדבר האופי המסורתי של הלחימה, אין שחר להנחה בדבר הקיום המעשי של הדדיות השמירה על הנורמות המגבילות את הלחימה, ומובן מאליו שאין דרך מעשית לקיים את המגבלות באמצעים מעשיים ופשוטים, כדוגמת ההבחנה בין לובשי מדים לבין זולתם. השינויים הללו במצב הדברים מעיבים על הנכונות לנהוג על פי ההסכמים הבינלאומיים, ואין ספק שיש מקום להרהר בתוקפם לגבי המצבים החדשים.

רביעית, **הטעם הרטורי**: טענות בדבר הפרות של הדין הבינלאומי נעשו אמצעי תעמולתי בדוק נגד המדינות הלוחמות בטרור, במיוחד נגד ישראל, גם אם הבסיס העובדתי שלהן קלוש ואפילו אם הן כוזבות. את האפקט התעמולתי של טענות כאלה יוצרת או מעצימה התקשורת, לפחות בחלקה, בעיקר באירופה ובישראל עצמה. האפקט התעמולתי הכולל מוצג על ידי התקשורת עצמה כמה שיוצר יחס שלילי ב"דעת הקהל הבינלאומית".

הביטוי "דעת הקהל הבינלאומית" הוא בעייתי. ייתכן שהוא משקף דעה הרווחת בחוגים מסוימים, שהם בעלי חשיבות משנית או שולית כשלעצמם, אבל בעלי נוכחות רבה בתקשורת משום שהיא חפצה ביקרם. איננו שוללים את הצורך של המדינה להיאבק גם בחזית זו, אולם אין מקום לתת חשיבות מכרעת לשאלה, האם מעשה מסוים יצטייר באמצעי תקשורת מוכרים כבסיס לטענות בדבר הפרות כביכול של הדין הבינלאומי. שיקולי התדמית אינם קודמים לשיקולי ההגנה העצמית, המוסר והאתיקה הצבאית.

כאן עלינו להדגיש, כי החשיבות שאנחנו מייחסים להבדל בין נקודת המוצא שלנו לבין נקודת המוצא של "חסידי" הדין הבינלאומי אינה בגדר "זלזול במשפט הבינלאומי", כדבריו של איל בנבנישתי, נגד "דוברים שונים בצה"ל או המייעצים לצה"ל".[7] כדי להבין מהו "זלזול" בעיני בנבנישתי, אפשר להיעזר בתיאור הסכנה שהוא מזהה כאן: "בשל אמירות כאלה עלול להיווצר רושם שישראל ממעיטה בחשיבותו של המשפט הבין־לאומי מתוך התפיסה שאינו רלוונטי ואינו מוסרי".[8] לטעמו של בנבנישתי, אסור לישראל להיות בעלת התפיסה שנורמות שבהסכמים הבינלאומיים אינן רלוונטיות לתחומים חדשים, כדוגמת הלחימה בטרור או הלחימה ברשת. לטענתו, הרלוונטיות של הדין הבינלאומי לכל מצב חייבת להיות עיקרון יציב של המדינה. יתר על כן, גם אסור לישראל להיות בעלת התפיסה שנורמות שבהסכמים הבינלאומיים אינן מוסריות ואינן הולמות את העקרונות המוסריים שביסוד המשטר הדמוקרטי שלה, כדוגמת עקרון השמירה על כבוד האדם. המוסריות של הדין הבינלאומי חייבת להיות עיקרון דוגמטי של המדינה.

אנחנו דוחים את המגבלות שמטיל בנבנישתי על התפיסה של המדינה הדמוקרטית ביחס לרלוונטיות או למוסריות של נורמות שבדין הבינלאומי. מדינה רשאית להיות בעלת תפיסה ביקורתית ביחס לרלוונטיות או למוסריות של היבט זה או אחר של הדין הבינלאומי: מדינה רשאית שלא להצטרף להסכם בינלאומי, רשאית להצטרף תוך הסתייגות מחלקים שלו, וגם להגיע למסקנה שיש בו חלקים שאינם רלוונטיים, המחייבים השלמה משמעותית, וגם חלקים בלתי־מוסריים, המחייבים שינוי משמעותי. הדוקטרינה האתית של הלחימה בטרור היא בעיקרה הצעה של השלמה.[9]

חשוב מאוד להבין כי השלמה משמעותית של הדין הבינלאומי אינה הקלה בכללים המחייבים חיילים ומפקדים. אדרבה, כפי שנראה להלן, בדוגמאות משמעותיות אחדות, ההשלמה שאנחנו מציעים בדוקטרינה שלנו מחייבת לעתים החמרה בכללים, כלומר תוספת כללים הדורשים יותר ריסון ומגבלות על הפעלת הכוח הצבאי מכפי שדורשים הכללים הקיימים.

## 3. הדין הבינלאומי: ניווט בערפל

הדיון בדין הבינלאומי, תוכנו, מידת חשיבותו בכלל ומידת חשיבותו מנקודת מבט ישראלית נערך בעת ובעונה אחת ברמות שונות, החל ברמה מופשטת מאוד וכלה ברמה קונקרטית מאוד. מייד נדון בהן בקצרה, אולם כבר בראשית הדברים נצביע על הערפול המאפיין את הטענות הנשמעות במקומותינו ובמקומות אחרים. על פי רוב, קשה לדעת לאיזו רמה מכוונים דבריו של אדם הטוען בדבר חשיבותו של הדין הבינלאומי – האם כוונתו לרמה מופשטת, שבה אנו מזדהים בהחלט עם דבריו, או שמא כוונתו לרמה קונקרטית, שבה יש מקום לגישה ביקורתית או אף להסתייגות מהותית. הערפול המהותי הזה ניכר בליבת דבריהם של איל בנבנישתי ופנינה שרביט־ברוך, ואף בשולי דבריו של אביחי מנדלבליט, ומוביל אותם למסקנות מוטעות, כפי שנראה להלן.

אלה הן הרמות השונות:

1. רוח הדין הבינלאומי
2. המערכת הבינלאומית של מוסדות, אמנות ומנהגים
3. דוקטרינות המתבטאות באמנות בינלאומיות
4. פרשנויות של אמנות בינלאומיות
5. תפיסות של המנהגים המחייבים
6. יישומים בדבר פעילות מסוימת, מראש ובדיעבד

(1) **רוח הדין הבינלאומי מקובלת עלינו בתור רוח ראויה.** אפשר להציג אותה כעקרון החובה לצמצם ככל האפשר את נזקי המלחמה, באמצעות הסדרים מסוימים המטילים מגבלות על עצם היציאה למלחמה צודקת, ומגבלות על הפעילות הראויה במהלך הלחימה. עיקרון זה מתבטא במסורת הארוכה של "תורת המלחמה הצודקת", על עקרונותיה הידועים, כדוגמת הדרישה שהיציאה למלחמה תהיה האמצעי האחרון לפתרון סכסוך מדיני, הדרישה להבחנה נאותה בין לוחמים למי שאינם לוחמים ודרישת המידתיות.[10] עם זאת, אלה הן דרישות מופשטות וארוכה היא הדרך בינן לבין נהלים, הוראות פתיחה באש ופקודות במצבים קונקרטיים.

**רוח הדין הבינלאומי היא בעלת אופי מוסרי.** לפיכך, כל מדינה דמוקרטית אמורה לבטא אותה בהליכותיה, כיוון שגם היא עומדת על עקרונות מוסריים

בדבר השמירה על כבוד האדם באשר הוא אדם. מדינת ישראל, בהיותה מדינה דמוקרטית, מחויבת גם היא לשמור על רוח הדין הבינלאומי. **על כך אין מחלוקת.**

(2) המערכת הבינלאומית כוללת מוסדות כדוגמת ארגון האו"ם ובמרכזו מועצת הביטחון, אמנות בינלאומיות שמדינות מקבלות על עצמן לקיים אותן על יסוד שיקולים שונים, כגון אמנות שונות של לחימה בטרור, ומנהגים המסוגלים להפוך ברבות הימים למנהג העולם, שיש לו מעמד מחייב. המערכת הבינלאומית הזאת אמורה לממש בהליכותיה את רוח הדין הבינלאומי, ובתור שכזו היא בעלת חשיבות מוסרית.

עם זאת, המערכת הבינלאומית מתנהלת על ידי מדינות ואלה פועלות, כל אחת ואחת מהן, על פי השיקולים של עצמה. לפיכך, המערכת הבינלאומית היא מערכת פוליטית שרבות מהליכותיה מאפשרות לה לפעול באופן בלתי־מוסרי באצטלה של רדיפת השלום והצדק.

נזכיר כאן רק שתי דוגמאות מן הזמן האחרון. דוגמה ראשונה: בית הדין הפלילי הבינלאומי (ICC) רשאי לדון במעשיה של מדינה שאינה חתומה על האמנה המכוננת אותו רק אם מועצת הביטחון פנתה אליו שיעשה זאת. המדינות בעלות זכות הווטו במועצת הביטחון לא יאפשרו פניות כאלה כשמדובר בבעלות־בריתן: רוסיה וסין כשמדובר בסוריה, ארצות־הברית כשמדובר בבחריין ובתימן, וגם בישראל. דוגמה שנייה: הפורום הגלובלי ללחימה בטרור (GCTF) שהוקם ביוזמת ארצות־הברית כולל 29 מדינות ואת האיחוד האירופי, אבל אינו כולל את ישראל,[11] ככל הנראה בגלל התנגדות של טורקיה, שמכהנת כיו"ר הפורום יחד עם ארצות־הברית. המערכת הבינלאומית, ככל שהיא נוהגת לממש את רוח הדין הבינלאומי, עושה זאת באופן סלקטיבי שהוא מטבעו לא הוגן.[12]

התבונה המדינית מחייבת יחס זהיר אל המערכת הבינלאומית, הזדהות עם מטרותיה לקידום השלום והשמירה על כבוד האדם בהתאם לרוח הדין הבינלאומי, אבל גם שיקול דעת מתמיד בדבר המידה והמתכונת של שיתוף פעולה עם מוסדות, הצטרפות לאמנות והסכמה למנהגים. דומה שזהו הקו הכללי המסורתי של ישראל, ואנחנו מניחים שגם הוא מקובל על כולנו.

(3) הכללים המופיעים באמנות בינלאומיות, כגון סעיפי אמנת האג בדבר מלחמה ביבשה (1907), מבטאים דוקטרינות בדבר המלחמה, שהן תפיסות כלליות ומורכבות בדבר היבטים מסוימים של המלחמה. לדוגמה, סעיפי פרק אחד באמנה[13] הם תפיסה כזו בדבר האפיון של צד לוחם במלחמה: המדובר לא רק בצבא, אלא גם בגופים מעין־צבאיים הממלאים אחר תנאים מסוימים, כגון פיקוד אחראי ונשיאת נשק בגלוי. הכללים הללו מבטאים את רוח הדין הבינלאומי (במסורת תורת המלחמה הצודקת) באופן המקל את המעבר מן העקרונות המופשטים שלו אל הרמה הקונקרטית של נהלים, הוראות פתיחה באש ופקודות. ככל שהתפיסות

המתבטאות בכללים עוזרות לממש הלכה למעשה את רוח הדין הבינלאומי, הן מועילות ובעלות ערך מוסרי.

עם זאת, התפיסות הללו אינן פשוטות ואינן תמימות, משום שהן מבוססות על הנחות עובדתיות שיכולות להיות לא־נכונות, ונובעות מהן מסקנות מעשיות שיכולות להיות לא־ראויות. לדוגמה, הנחה עובדתית לא־נכונה היא ההנחה שניתן להבחין בין הלוחמים לבין זולתם באמצעות "סימן היכר קבוע שאפשר להבחין בו מרחוק".[14] בנסיבות המלחמה בטרור הנחה זו אינה נכונה, כידוע. לדוגמה, מסקנה מעשית של הכללים היא כי כל חייל בצבא של צד לוחם אחד, שיצא למלחמה צודקת של הגנה עצמית מובהקת, הוא מטרה לגיטימית לפגיעה קטלנית של הצד הלוחם שמנגד, שיצא למלחמה תוקפנית לא־צודקת. זוהי מסקנה המוסיפה לעורר התנגדות מוסרית חריפה ומשכנעת.[15]

מהו היחס הראוי לדוקטרינה המתבטאת בכללים של אמנה בינלאומית, לנוכח האפשרות שהיא מבוססת על הנחות עובדתיות לא־נכונות או נובעות ממנה מסקנות מעשיות לא־ראויות? במישור העיוני התשובה פשוטה, כמקובל לגבי כל דוקטרינה כזו, בתחום כלשהו של החיים: ראוי לפתח דוקטרינה נוספת המבוססת על הנחות עובדתיות נכונות ושהמסקנות המעשיות הנובעות ממנה ראויות, או לפחות קרובות יותר אל הראוי, שגם היא בגדר מימוש של רוח הדין הבינלאומי במסגרת המערכת הבינלאומית. כך יש להבין את הדוקטרינה האתית של הלחימה בטרור, כפי שהוצגה בעבודותינו, במישור העיוני.

במישור המעשי התשובה מסובכת הרבה יותר. במישור זה ניתן לשאול מהי המדיניות הרצויה ביותר ביחס לדוקטרינה הבעייתית, כשהיא נראית מעוגנת ברוח הדין הבינלאומי, מקובלת במסגרת המערכת הבינלאומית ומתבטאת באמנה בינלאומית מחייבת? לשאלה זו אין תשובה גורפת, מפני שעל כף המאזניים האחת נמצאות המסקנות המעשיות הלא־ראויות של הדוקטרינה הנתונה, אולם על כף המאזניים השנייה נמצאות ההשלכות הלא־רצויות של התנערות מאחד המרכיבים המקובלים של המערכת הבינלאומית ומאמנה בינלאומית מחייבת. לא תמיד כף אחת של המאזניים מכריעה את חברתה.

לדעתנו, ניתן לפעול באופן שלא ייצור מראית־עין בלתי־רצויה של התנערות כזו. אם הדוקטרינה הנתונה מבוססת על הנחה עובדתית שאינה נכונה בנסיבות מסוג מסוים, כדוגמת הלחימה בטרור בתצורתו הנוכחית, עדיין ניתן לקיים אותה בנסיבות מסוג אחר, שבהן אותה הנחה עובדתית היא נכונה, כדוגמת העימות הצבאי החזיתי בין שני צבאות. כך אפשר להציע דוקטרינה נוספת ולפעול על פיה כל עוד הנחותיה נכונות. בצורה זו מתקיימות זו בצד זו שתי דוקטרינות, המעוגנות ברוח הדין הבינלאומי במסגרת המערכת הבינלאומית, וכל אחת מהן מופעלת בתנאים שונים, בהתאם להנחות העובדתיות שביסודה. במתכונת זו

אין התנערות לא רצויה במישור הבינלאומי, ואין שימוש בדוקטרינה שההנחות שביסודה אינן נכונות. כך יש להבין את הדוקטרינה האתית של הלחימה בטרור, כפי שהצענו אותה, במישור המעשי.

האם הגישה הזאת מקובלת על כולנו, במפורש או במובלע? נראה זאת מייד, לאחר שנדון ברמה הבאה – רמת הפרשנויות.

(4) האפשרות להדריך את ההתנהגות של הלוחמים על יסוד פרשנות של הדין הבינלאומי מקובלת על המשתתפים בדיון.

מנדלבליט כותב כי "יש לשמר את הכללים הקיימים המסורתיים של דיני הלחימה ולישמם בקפידה תוך כדי מתן **פרשנות מתאימה** לאתגרי הלחימה האסימטרית". הוא אינו מסביר מהי "פרשנות מתאימה", איך קובעים אותה ומי אמור לעשות זאת, אולם אנחנו נגיע מייד לשאלות הללו וגם נשיב עליהן.[16] בנבנישתי כותב כי "המשפט ודיני הלחימה בעיקרם לא השתנו, אבל הם נדרשים **להתאים את עצמם** למציאות של הפעלת שליטה".[17]

שרביט־ברוך כוללת בדבריה משפט דומה, אבל היא מוסיפה דוגמאות שיאירו את עינינו. "...בנושא הלחימה בעימותים אסימטריים יש עקרונות וכללים קיימים, **ויש ליישם אותם באופן המביא בחשבון את המציאות המיוחדת** של עימות מן הסוג הזה".[18] מושג הפרשנות אינו מופיע בדבריה של שרביט־ברוך, אבל הדעת נותנת שאין הבדל בין פרשנות של הכללים לבין יישום שלהם, "המביא בחשבון" היבטים מיוחדים של מצב הלחימה הנתון.

להדגמת טענתה מביאה שרביט־ברוך כמה דוגמאות חשובות. אחת מהן היא כללי הלחימה האווירית: "כאשר החלה הלחימה האווירית לא היו כללים לגביה".[19] עם הזמן, מדינות שנקטו בלחימה אווירית גרמו לכך ש"**התגבשו הכללים הרלוונטיים. הכללים האלה מבוססים על העקרונות והכללים של דיני הלחימה שכבר היו קיימים לגבי לחימה ביבשה ובים, תוך עשיית ההתאמות הנדרשות**".[20] דוגמה נוספת שהיא מביאה היא מתחום לוחמת הסייבר: "גם בעניין הזה מתבססים **הכללים החדשים על אלה הקיימים תוך עשיית [ה]התאמות הנדרשות**".[21] מייד נראה מה עולה מן הדוגמאות הללו לעניין הדוקטרינה האתית שלפנינו, אולם קודם לכן נזכיר דוגמה נוספת שמביאה שרביט־ברוך מתוך התחום של הלחימה בטרור, שהוא תחום הדוקטרינה שלנו.

"במלחמה הקלסית הייתה[22] קיימת הבחנה חדה יחסית בין חיילים לבין אזרחים. החיילים נחשבו למטרה לגיטימית... ואזרחים (כלומר, מי שאינם חיילים) לא נחשבו למטרה לגיטימית. ואולם מתעוררת השאלה: כיצד לנהוג כאשר בצד של האויב אין חיילים אלא אזרחים חמושים, ברמות שונות של ארגון, שאינם נלחמים בהכרח כל הזמן ושקשה להבחין ביניהם לבין שאר האוכלוסיה".[23] כאן מוסיפה שרביט־ברוך כמה נקודות מאירות עיניים: "...כיוועצים המשפטיים של צה"ל,

סברנו כי אין זה נכון לראות בכל חברי הארגונים המזויינים [של האויב] אזרחים המעורבים במעשי האיבה, אלא נכון יותר להגדיר את מי שנמנה עם הכוחות הלוחמים של האויב ושיש לו תפקידים מקבילים לאלה של חיילים בצבא, כלוחם שאין לו חסינות מתקיפה כל עוד הוא משתייך לכוחות אלה".[24]

כאן ראוי שנקרא לילד בשמו: מה ש"היועצים המשפטיים" כדוגמת שרביט־ברוך הגישו לצה"ל היה דוקטרינה חדשה בדבר הלחימה בטרור, ברוח הדין הבינלאומי הנתון.

תחת הכותרת "פרשנות מתאימה [של הכללים הקיימים המסורתיים]", כלשונו של מנדלבליט, לא באה שום פרשנות. תחת הכותרת של "יישום [עקרונות וכללים קיימים] באופן המביא בחשבון את המציאות המיוחדת", כלשונה של שרביט־ברוך, לא בא שום יישום של עקרונות וכללים קיימים. תחת שתי הכותרות הללו מופיעה דוקטרינה חדשה בדבר הלחימה בטרור, ברוח הדין הבינלאומי הנתון, שעניינו המקורי הוא המלחמה הקלאסית. לאמיתו של דבר, הדוגמאות של שרביט־ברוך מראות כי מדובר **בכללים חדשים** המוגדרים **ברוח הכללים הקיימים**. מגדיל לעשות בנבנישתי, המתאר את השינוי האמור להתחולל בעקבות השימוש הרווח בטכנולוגיות מתוחכמות המאפשרות פגיעות מדויקות: "מבחינת המשפט יש כאן מעבר מהתחום של המשפט הפרטי, כמו אכיפה של חוזה בין שני צדדים, לתחום של משפט ציבורי, המפקח על מקבלי ההחלטות, על הרגולטורים, על השולטים, על המנהלים, היכולים להחליט במי הם פוגעים..., מתי הם פוגעים, כיצד הם פוגעים ואיזה נזק אגבי הם גורמים".[25] מדובר, אפוא, בכללים חדשים, במסגרת תפיסה משפטית כוללת שיכולה להיות שונה מקודמתה.

במלים אחרות, לא רק אנחנו, בדוקטרינה האתית שלנו, מציעים כללים חדשים ברוח הדין הבינלאומי המוכר, העומד על תורת הלחימה הצודקת, אלא בדיוק כך עושים גם אנשי הדין הבינלאומי המותחים עלינו ביקורת על כך שאנחנו עושים זאת. אין הבדל עקרוני או מעשי בין היחס שלהם אל הדין הבינלאומי הנתון לבין היחס שלנו אליו: כולנו מוסיפים עליו כללים חדשים. מהו, אפוא, ההבדל בין גישתם לבין גישתנו?

שני הבדלים מצאנו בין גישתנו לבין הגישה של אנשי הדין הבינלאומי שהוזכרו לעיל. ההבדל הראשון הוא רטורי. הם מעוניינים להציג את ההתנהלות של מדינת ישראל, ובמיוחד של צה"ל, כשמירה על הכללים הקיימים של הדין הבינלאומי. הצגה כזו באה לסתור, מראש ובדיעבד, כל טענה עוינת המאשימה את מדינת ישראל ובמיוחד את צה"ל בהפרת הכללים הקיימים של הדין הבינלאומי. הדוקטרינה האתית שלנו מנוסחת בלשון אחרת: מדינת ישראל וצה"ל פועלים **ברוח הכללים** הקיימים של הדין הבינלאומי, בהתאם לדוקטרינות חדשות, שהן בגדר **תוספות לכללים הקיימים וברוחם**. לאמיתו של דבר, לא רק אנחנו נוהגים כך, אלא גם מדינות

אחרות הלוחמות בטרור עושות זאת. שרביט־ברוך עצמה מעידה על "התפיסה המקובלת בצבא ארצות־הברית ועל כוחות נאט"ו", שלפיה "המשתתפים בכוחות המזויינים של כל צד לעימות, גם צד לא מדינתי, אינם אזרחים אלא מקבילים לחיילי הצבא מבחינת יישום עקרון ההבחנה".[26] לאמיתו של דבר, אין מנוס מהנהגת כללים חדשים במסגרת הדוקטרינות החדשות, ברוח הדין הבינלאומי. להלן נציג ביתר פירוט דוגמאות חשובות של כללים חדשים המוצעים ברוח הדין הבינלאומי, כדוגמת כללים הדורשים מזעור הנזק האגבי, מעבר לכללים המקובלים הדורשים מידתיות. בשלב זה נסתפק בדוגמה פשוטה ביותר. במהלך הדיון שבעקבותיו נכתבו המאמרים שלפנינו, בתגובה על טענתנו שלא רק סגל רפואי אלא גם סגל של קציני בריאות הנפש (קב"נים) ראוי ליחס מיוחד, ברוח אמנת ז'נבה הראשונה הקובעת את המעמד המיוחד של סגל רפואי,[27] העיד נציג בכיר של "הצלב האדום" כי הקב"נים נחשבים לסגל רפואי הזכאי ליחס מיוחד. ההכרה בקב"נים בתור זכאים ליחס מיוחד אינה "פרשנות" של המונח "סגל רפואי", גם לא "יישום" של ביטוי זה לטיפול של הקב"נים. זהו כלל חדש בדין הבינלאומי, המבטא תפיסה בדבר מקומו של הקב"ן בצד הרופא, האחות, החובש (וכן קצין הדת, המוגן באותו סעיף), שהיא ברוח הדין הבינלאומי בדבר הסגל הרפואי, אבל מרחיבה אותו על ידי תוספת כלל חדש. הרחבה מעשית של קבוצת בני־אדם בעלי מעמד מסוים היא בגדר תוספת כלל חדש, גם אם מדובר במה שנראה כהרחבה טבעית.

ייתכן שהרטוריקה של "שמירה על הכללים הקיימים", תוך "פרשנות" או "יישום" שלהם, בהתאם לנסיבות המיוחדות של המלחמה בטרור היא בעלת יתרונות במישור ההסברה, אולם ראוי שלא להניח לנורמות של הסברה, יחסי ציבור, תקשורת או לוחמה פסיכולוגית לחלחל אל תוך ההבנה המקצועית של הפעילות הנדרשת. הרטוריקה הזאת אינה יכולה ואין זה מן הראוי שתוכל להסתיר את העובדה שמדובר בפיתוח דוקטרינות חדשות.

יתר על כן, הרטוריקה הגורפת של "שמירה על הכללים הקיימים", באופן מלא ומוחלט, מכרסמת בהחלטה החשובה של מדינת ישראל שלא לאשרר את הפרוטוקול המשלים הראשון (AP1) משנת 1977, שנועד להשליט כללים מקובלים להתנהלות במלחמה קלאסית גם על העימות של מדינה עם לוחמי גרילה, המטשטשים את ההבדל בינם לבין הלא־לוחמים שבסביבתם. ישראל לא היתה היחידה שנמנעה מאשרור הפרוטוקול הזה: ארצות־הברית לא אשררה אותו ואילו אוסטרליה, בריטניה, גרמניה, צרפת, קנדה ומדינות נוספות הוסיפו לאשרור הסתייגויות, שלפיהן מדינות אלה אינן מקבלות עליהן חלק מן הכללים החדשים.

"הצלב האדום" (ICRC) מנסה להפוך את כללי הפרוטוקול המשלים למחייבים את כל המדינות, בין אם אשררו אותו ובין אם לאו, בין אם במלואו ובין אם בחלקו. הוא עושה זאת במסמך משנת 2005,[28] הטוען שכללי הפרוטוקול המשלים הם

הדין הבינלאומי המנהגי, דהיינו, מערכת הכללים שהמדינות פועלות לפיהם הלכה למעשה. זוהי טענה שנויה במחלוקת[29] וודאי שמדינת ישראל אינה מקבלת אותה, בהיותה מדינה שלא אשררה את הפרוטוקול עצמו. טענות גורפות בדבר "שמירה על הכללים הקיימים", עלולות להתפרש כטענות גורפות בדבר מחויבות לשמור גם על מה שמדינת ישראל החליטה שהיא אינה מקבלת על עצמה. זוהי סכנה הנשקפת מן הרטוריקה של אנשי הדין הבינלאומי, הדוחפים למעשה את מדינת ישראל אל פינה מדינית וצבאית שהיא החליטה שאינה רוצה להיות בה. סכנה כזו אינה נשקפת מן הדרך שבה אנחנו מציגים אל־נכון את הדוקטרינה האתית.

כאן ראוי להעיר על תפיסת ההתנהלות הראויה של המדינה במישור שבו "מתפתח המשפט הבין־לאומי". שרביט־ברוך סבורה ש"הציפייה הזאת", דהיינו – "לכנס את נציגי כל מדינות העולם ולהסכים על אמנה חדשה שתיתן יותר חופש פעולה לצבאות בעימותים אסימטריים", היא "מנותקת לחלוטין מן המציאות הבין־לאומית".[30] ראשית, לא ברור מדוע סבורה שרביט־ברוך שתכלית ההסכמה הבינלאומית היא "יותר חופש פעולה לצבאות בעימותים אסימטריים". התכלית היא הסכמה לדוקטרינה חדשה, שתטיל מגבלות ברוח הדין הבינלאומי (במסורת תורת המלחמה הצודקת), באופן המתאים לטבעו של העימות עם הטרוריסטים. דוקטרינה כזו אינה אמורה להיבחן במתן חופש פעולה בהשוואה לדוקטרינה בדבר הלחימה הקלאסית. ייתכן שיהיו בה מגבלות חדשות, כשם שיהיו בה אולי היתרים חדשים. יתר על כן, לא ברור מדוע סבורה שרביט־ברוך שאין טעם בשום הסכמה בינלאומית, אם לא שותפות לה "כל מדינות העולם". אם נשמיט את הדרישה הרטורית בדבר "כל מדינות העולם" ונסתפק במדינות הדמוקרטיות המעורבות במלחמה בטרור, אין שום דבר "במציאות הבין־לאומית" שיש בו יסוד להניח שהסכמת העולם הדמוקרטי לדוקטרינה של לחימה בטרור ברוח הדין הבינלאומי היא "מנותקת לחלוטין מן המציאות".[31]

בשולי דבריה מזכירה שרביט־ברוך עוד ערוץ של התפתחות: "בדרך של גיבוש פרקטיקה והתאמות של הכללים למציאות המשתנה".[32] ביחס לאפשרות של "התאמות של הכללים", כבר ראינו לעיל שהמדובר ברטוריקה של הגנה המטשטשת את העובדה שלאמיתו של דבר מדובר בהנהגת דוקטרינות חדשות לגבי "המציאות המשתנה". יתר על כן, גם "גיבוש פרקטיקה" אינו אלא גיבוש דוקטרינה חדשה להדרכת הפרקטיקה. ככל שהמשפט הבינלאומי מתפתח במישור המנהגי, מובן מאליו שבידינו לגבש דוקטרינות חדשות ולנהוג על פיהן, ברוח הדין הבינלאומי (במסורת תורת המלחמה הצודקת), ובה בעת – ללמוד מן הדוקטרינות החדשות של מדינות דמוקרטיות אחרות הנלחמות גם הן בטרוריסטים, במאמץ מתמיד לגבש את הפרקטיקה של העולם הדמוקרטי במלחמתו בטרוריסטים. הדוקטרינה האתית שלנו נועדה להוות תרומה למאמץ הזה לפיתוח הדין הבינלאומי המנהגי.

הבדל נוסף בין הגישה של אנשי הדין הבינלאומי לבין הגישה שלנו הוא בכך שהגישה שלהם היא תוצר של פעילות מקצועית בתחום הדין הבינלאומי, שעה שהגישה שלנו היא תוצר של פעילות מקצועית בתחומי הפיקוד והאתיקה. השימוש ברטוריקה של "פרשנות" ו"יישום" נועד להשאיר את מלאכת הפיתוח של דוקטרינות חדשות בידי אנשי הדין הבינלאומי. לדעתנו, זו אינה מלאכה משפטית, ממש כשם שמלאכת העיצוב של הערכים והעקרונות האמורים להדריך את ההתנהלות במדינה, בארגון, במקצוע או בתאגיד עסקי אינה מופקדת בידי היועצים המשפטיים של כל אחד מן הגופים הללו. ערכי המדינה ועקרונותיה נקבעים בכנסת; ערכי האוניברסיטה אינם נקבעים על ידי היועץ המשפטי שלה, אלא על ידי ההנהגה האקדמית שלה; ערכי הרפואה גובשו בעולמם של הרופאים, בעזרת אנשי האתיקה הרפואית; ערכי חברת בנייה ייקבעו על ידי אנשיה המומחים בסוגיות הזהות שלה, בעזרת יועצים כאלה ואחרים. במקומותינו נהוג, במידה רבה ומופרזת, לטשטש את הגבולות בין עולם המשפט לבין עולם האתיקה,[33] אולם אסור להניח לטשטוש הזה ליצור את הרושם שהמשפטנים הם המופקדים על פיתוח הדוקטרינות החדשות. גם החובה לפתח דוקטרינות חדשות ברוח הדין הבינלאומי הקיים אינה מחייבת את הפקדת המלאכה בידי משפטנים: רוח הדין הבינלאומי היא תורת המלחמה הצודקת, שהיא מערכת עקרונות מסורתית המוסיפה להיות נושא לדיונים בפילוסופיה, במדע המדינה, בהיסטוריה, בתיאולוגיה וגם במשפט.

אין, אפוא, הבדל בין גישתנו לבין הגישה של בנבנישתי, מנדלבליט ושרביט־ברוך, ככל שמדובר בתיאור מדויק של הפעילות המתבקשת בנסיבות הנוכחיות. "צה"ל, כמו כל צבא של מדינת חוק במערב", טוען מנדלבליט, "מחויב להקפיד על עמידה בדרישות של דיני הלחימה".[34] מהן "הדרישות" הללו? אנחנו קוראים לילד הזה בשמו: אלה הן דרישות לפעול ברוח הדין הבינלאומי המוכר, במתכונת של כללים חדשים הנוספים עליו, ברוחו. זה מה שכולנו יודעים שצריך לעשות. זה מה שכולנו עושים. "הכללים הקיימים של דיני הלחימה הם המערכת הנכונה והמתאימה גם כאשר עוסקים בעימותים אסימטריים", טוענת שרביט־ברוך.[35] מהם "הכללים הקיימים" הללו? אם הכוונה לעקרונות המופשטים של רוח הדין הבינלאומי (במסורת תורת הלחימה הצודקת), כי אז אין מחלוקת בינינו, אולם אם הכוונה היא לכללים המתבטאים בסעיפי אמנות ז'נבה, לדוגמה, כי אז שרביט־ברוך עצמה אינה פועלת בהתאם לטענתה, שהרי היא מפתחת כללים חדשים, תחת הכותרת המטעה של "יישום" הכללים הקיימים, כאילו "יישום" כלל בדבר "סגל רפואי" מאפשר לכלול בו גם סגל קב"נים שאינו רפואי, כאילו "יישום" כלל בדבר מידתיות מאפשר לדרוש הרבה יותר, כדוגמת מזעור הנזק האגבי, וכיוצא בזה. ניסוח אחראי של הפרקטיקה הנהוגה בהדרכה הערכית והנורמטיבית של הלוחמים מוציא אותנו מן הערפל, ומביא אותנו להכרה הצלולה בדבר החובה

לפתח דוקטרינות חדשות, על יסוד התפיסות הערכיות של המדינה בכלל ושל צה"ל (והשב"כ) בפרט.

## 4. סימון החטאות

העמדה הביקורתית המתנסחת במונחי "שמירת הכללים של הדין הבינלאומי כמות שהם" היא נכונה, ככל שמדובר בעקרונות של רוח הדין הבינלאומי ותורת הלחימה הצודקת, ואינה נכונה, ככל שמדובר בכללים המפורטים יותר האמורים להדריך את המפקדים והחיילים. הרטוריקה של "שמירת הכללים כמות שהם", ללא כל הודאה שלאמיתו של דבר מתבצעת גם פעילות משמעותית של הנהגת תפיסות חדשות וכללים חדשים, יוצרת אצל המשתמשים בה רצון לתאר את עמדתם במונחים המבדילים אותה מכל מה שמתבטא בדוקטרינה האתית שלנו. לפיכך, אנחנו מוצאים את עצמנו נוכח גל של תיאורי סרק, המייחסים לנו עמדות שמעולם לא היו לנו וגם לא השתמעו מדברינו.[36]

נביא כאן כמה דוגמאות לתיאורי הסרק הללו, ונבהיר את עמדתנו בסוגיות הכרוכות בהם.

שרביט־ברוך מעוניינת להציג עמדה מרכזית: "לדעתי, הכללים הקיימים של דיני הלחימה הם המערכת הנכונה והמתאימה".[37] ההגנה על עמדה זו כרוכה, לדעתה, בהתנגדות לטיעונים משני סוגים, המנוגדים זה לזה. "הטיעון הראשון הוא כי הכללים הקיימים אינם מתאימים לעימות מן הסוג [הנוכחי] משום שהם מאפשרים שימוש מוגזם בכוח העלול לפגוע באוכלוסייה אזרחית... במקומות שבהם אין מדינה מאורגנת המסוגלת להגן על אזרחיה, אלא קיימים גורמים לא מדינתיים שאינם מציבים בראש סדר העדיפויות את טובת האוכלוסייה שלהם, בשל העדר רצון או חוסר יכולת, מוטלת על הצד השני חובת זהירות רבה יותר כלפי האוכלוסייה הזאת".[38] לפי הטיעון מן הסוג השני, "בלחימה באזורים מאוכלסים מול גורמים לא מדינתיים, בעיקר כאשר אלה אינם מכבדים את דיני הלחימה ואינם מבחינים את עצמם מן האוכלוסייה האזרחית, יש להטיל פחות מגבלות על השימוש בכוח... לפי הגישה הזאת הכללים הקיימים אינם מתאימים, ויש להתעלם מהם או לפחות להגמיש את המגבלות המפורטות בהם, שאם לא כן אחד הצדדים נלחם כשידיו כבולות".[39] כיוון ששרביט־ברוך אינה מצטטת או מציינת מראי מקום, אנחנו נאלצים לשאול היכן נמצאים הטיעונים שלנו בתמונה שלה, בין הטיעונים מן הסוג הראשון או בין הטיעונים מן הסוג השני?

אם מפיגים את הערפל המהותי שמביאה שרביט־ברוך לדיון ברטוריקה של "הכללים הקיימים... המערכת הנכונה והמתאימה", מתגלה תמונה מעניינת: ככל שמדובר ברוח הדין הבינלאומי (או בעקרונות של מסורת תורת המלחמה הצודקת), אין הבדל בין העמדה של שרביט־ברוך לבין עמדתנו, וכבר הרחבנו על

כך את הדיבור לעיל. אולם מרגע שעוברים אל הדוקטרינות שיש להשתמש בהן בעימות מן הסוג הנוכחי, הדוקטרינה שלנו אינה מן הסוג הראשון של שרביט־ברוך וגם אינה מן הסוג השני.

הדוקטרינה שלנו אינה מן הסוג הראשון, בין השאר, מפני שאנחנו מייחסים חשיבות מכרעת לשאלת השליטה האפקטיבית בשטח שבו נערכת הלחימה. המדינה נושאת באחריות לגורלו של כל אדם הנמצא בשטח שיש לה בו שליטה אפקטיבית ואינה נושאת באחריות מקבילה, ועל אחת כמה וכמה – "חובת זהירות רבה יותר", לגבי בני־אדם הנמצאים בשטח שאין לה בו שליטה אפקטיבית. דרך אגב, זוהי דוגמה משמעותית נוספת לכך שהדוקטרינה האתית שלנו מחמירה יותר מכללים מקובלים של הדין הבינלאומי.

הדוקטרינה שלנו אינה מן הסוג השני, בין השאר, מפני שהיא אינה כרוכה בטענה שיש "להתעלם" מן "הכללים הקיימים", או "להגמיש את המגבלות המפורטות בהם". כאשר אנחנו טוענים שהדוקטרינה של הדין הבינלאומי במתכונת המוכרת אינה מתאימה לעימות הנוכחי, איננו מתעלמים מן הכללים, משום שאנחנו מעוניינים בהחלט לשמור על רוחם, ולפתח דוקטרינה "אחות" המתאימה לעימות הנוכחי ונשענת על אותם עקרונות של רוח הדין הבינלאומי (במסורת תורת המלחמה הצודקת). גיבוש הדוקטרינה שלנו לא נועד "להגמיש את הכללים", אלא להגדיר כללים אחרים, מקבילים, המתאימים לעימות הנוכחי. הכללים בדוקטרינה שלנו מגבילים לא פעם את הפעלת הכוח יותר מן ההיתרים הגורפים של הדין הבינלאומי. כך, לדוגמה, ברוח עקרון ההבחנה, שהוא ברוח הדין הבינלאומי, ובמקביל לכלל ההבחנה הגסה בין לוחמים ללא־לוחמים במלחמה הקלאסית, הגדרנו כלל של הבחנה מדורגת על פי רמת הסיכון של התרומה לפעילות הטרור. יתר על כן, שעה שעקרון המידתיות, שגם הוא ברוח הדין הבינלאומי, דורש שהתועלת הצבאית הנגרמת מפעולה העלולה לגרום נזק אגבי תצדיק את הנזק הזה, ובלשון אחרת, שלא יהיה שימוש מופרז בכוח צבאי, הרי הדוקטרינה שלנו מחייבת מאמץ למזעור הנזק. מאמץ כזה מחייב, בין השאר, בדיקה מתמדת של האפשרות להשתמש באמצעי לחימה מתוחכמים.[40] כיוון שגם נזק שאינו מזערי יכול להיות מידתי ולא מופרז, גם כאן הכללים של הדוקטרינה שלנו מגבילים את הפעלת הכוח יותר מן הכללים המוכרים של הדין הבינלאומי.[41]

השוואה חשובה של הדוקטרינה שלנו עם כללים של הדין הבינלאומי עולה מפסק הדין בבג"ץ הסיכולים הממוקדים.[42] למרות שנשיא בית המשפט העליון (בדימוס), אהרן ברק, דן בתקינות של פעולה מן הסוג של סיכול ממוקד על יסוד הדין הבינלאומי המנהגי והדין הישראלי, הוא מגיע למסקנות דומות מאוד למסקנות העולות מהדוקטרינה האתית שלנו בשאלת ההבחנה בין המותר והאסור בפעולות צבאיות מסוג זה. שני הבדלים מתגלים בהשוואה בין הטיעון המשפטי לבין הטיעון

האתי. ראשית, נורמה של הדין הבינלאומי המנהגי דורשת שלאחר מעשה תיערך בדיקה עצמאית של הפעולה. איננו רואים את עצמנו בין החסידים הנלהבים של מיסוד גישה של חשדנות ואף אי־אמון ביחס לכל פעולה צבאית, אולם הדוקטרינה האתית שלנו אינה סותרת את הנורמה הזאת בדבר בדיקה מקצועית ועצמאית בדיעבד. לעתיד לבוא נכלול אותה בהצגת הדוקטרינה. שנית, פסק הדין קובע, כי מוטב לעצור, לחקור ולשפוט טרוריסט מאשר להורגו, ככל האפשר (סעיף 40 בדברי הנשיא (בדימוס) ברק). כך עולה גם מן הדוקטרינה האתית שלנו. בהקשר זה פסק הדין עוסק במפורש ב"תנאים של תפיסה לוחמתית ב[ה] הצבא שולט באיזור בו נעשית הפעולה", כך שמעצר, חקירה ומשפט הן "אפשרויות הניתנות לעתים למימוש". פסק הדין פוטר את הצבא מן החובה לממש אפשרות כזו, כאשר הנזק האגבי הצפוי ממנה רב מן הנזק האגבי הצפוי מהריגת הטרוריסט בסיכול ממוקד (שם). כאן נפרדות מסקנות פסק הדין ממסקנותינו. לשיטתנו, אין זה מן הראוי לפעול באופן היוצר סכנה ממשית לנזק אגבי, כאשר מדובר בשטח בתפיסה לוחמתית שיש בו שליטה אפקטיבית, היות שבשטח כזה הצבא אחראי להגנה על כל אדם שאינו משתתף בפעולות האיבה. ההצדקה שיש לצבא מבחינה אתית ומשפטית להטיל הגבלות על אדם כזה אינה כוללת הצדקה להורגו כתוצאה מהריגת טרוריסט.[43] לגישתנו, אין הצדקה לגרימת נזק אגבי כלשהו בשטח שהוא בשליטה אפקטיבית של הצבא.

מתוך כל הדוגמאות הרבות של הפער בין הטיעונים ששרביט־ברוך עוסקת בהם לבין הדוקטרינה שלנו, נזכיר כאן רק עוד דוגמה אחת:[44] "נקודה נוספת שמעלים המצדדים בטיעון [מן הסוג השני] היא שאין מקום לכיבוד הכללים על־ידי צד אחד לעימות כאשר הצד השני אינו מכבד אותם".[45] טענה זו אינה מקובלת עלינו, וככל שהיא מופנית נגדנו היא מגלמת אי־הבנה חשובה של דברינו.

עקרון ההדדיות של השמירה על כללי הדין הבינלאומי הוא בעל חשיבות בשני מישורים. ראשית, זוהי שאלה בעלת חשיבות צבאית, מדינית, אתית ומוסרית: האם הפרת הכללים על ידי צד אחד משנה את "מפת המותר והאסור" לצד השני, הסובל מן ההפרה? לדוגמה, אם צד אחד מפר את הכללים, משתמש בהרחבה בנשק כימי וזוכה בשל כך ביתרון צבאי משמעותי, האם הצד השני אמור להמשיך לשמור על הכללים כמות שהם, אפילו אם נשקפת לו בכך סכנה של מפלה צבאית? תשובה חיובית לשאלה זו נחשבת לא־סבירה ואף בלתי־נסבלת, להלכה ולמעשה, על ידי רבים וטובים.[46]

הדרישה הגורפת הזאת היא מחידושיו של הפרוטוקול המשלים האמור, משנת 1977, והיא אינה מקובלת עלינו (וגם לא על מדינות אחרות, ביניהן ארצות־הברית). מצד שני, היתר גורף לכל הפרה אפשרית של הכללים, לאחר שהאויב הפר אותם או חלק מהם, גם הוא אינו סביר ואף בלתי־נסבל. המטרה היסודית ביותר – לצמצם

ככל האפשר את נזקי המלחמה מבלי לוותר על החתירה המתמדת לניצחון – אינה מתבטלת אף פעם. השאלה היא, אפוא, באיזו מידה ובאילו תנאים משתנה "מפת האסור והמותר", לנוכח הפרת הכללים בידי האויב. הדוקטרינה שלנו יוצאת מן ההנחה שהאויב הטרוריסטי מפר את הכללים ברמה של רוח הדין הבינלאומי (ועקרונות תורת המלחמה הצודקת), ועם זאת, מובן שאין בה שמץ של היתר גורף להתעלמות מן הכללים, ברמה הזאת.

שנית, במישור שאין מרבים לעסוק בו, למרבה הצער, עקרון ההדדיות ממלא תפקיד בשיח ההצדקה שבין המדינה לבין לוחמיה.[47] מדינה דמוקרטית חייבת בכבוד האדם של אזרחיה, בכלל זה – לוחמיה. כיוון שהשמירה על כבוד האדם כוללת גם את השמירה על חייו, המדינה הדמוקרטית חייבת ללוחמיה הצדקה מכרעת לכל החלטה שלה להכניס אותם למצבים מסוכנים. מובן שאין מדובר בהצדקה הניתנת לחייל תחת אש, אלא להצדקה שהמדינה מגבשת לעצמה מראש, הניתנת לחיילים בזמן המתאים. ההצדקה של ציות לכללי הדין הבינלאומי עומדת על ההחלטה של המדינה לקבל על עצמה לנהוג על פי הכללים הללו. החייל רשאי לשאול את המדינה מדוע היא מטילה עליו חובה לנהוג לפי כללים אלה, גם אם בכך היא מחלישה את כוחו הצבאי. תשובת המדינה תכלול, בין השאר, את התבונה המדינית המתבטאת בכך שהמדינה קיבלה על עצמה לנהוג על פני כללים אלה. חלק מן התבונה המדינית מתבטא במימוש הצפוי של עקרון ההדדיות: מוטב לנו להגביל את עצמנו, באופן מסוים, כדי שבמקביל גם הצד השני יגביל את עצמו, באותו אופן או לפחות באופן דומה. מה קורה להצדקה הזאת במונחי "התבונה המדינית", כאשר ברור לחייל שעקרון ההדדיות אינו מתממש בחזית אף פעם?

כאן אין למדינה מנוס משינוי יסודי בהצדקה של מעשיה, לא עוד במונחי "התבונה המדינית" שביסוד עקרון ההדדיות, אלא במונחי מה שכולנו רואים בתור "הערכים הבסיסיים של המדינה".[48] העיקרון הראשון בדוקטרינה שלנו קובע לא רק את חובת המדינה להגן על אזרחיה, אלא גם את חובתה לעשות זאת תוך שמירה מתמדת על כבוד האדם, באשר הוא אדם. גם בנקודה זו מתפרצים מבקרינו אל דלת פתוחה לרווחה.

לסיכום, רוח הדין הבינלאומי היא בעינינו מצפן חשוב לעזרה בגיבוש האתיקה הצבאית של הלחימה בטרור. עם זאת, כללי הדין הבינלאומי כמות שהם מחייבים השלמות בדמות דוקטרינות חדשות, מן הסוג של הדוקטרינה האתית שלנו בדבר הלחימה בטרור. המדינות הדמוקרטיות, ומדינת ישראל ביניהן, אמורות להיות מצוידות בדוקטרינות שידריכו אותן כראוי כשהן מוצאות את עצמן בעימות מסוכן עם אויב, לא רק במלחמות המוכרות מן העבר, אלא גם במלחמות החדשות יותר, שבהן האויב אינו מדינה אלא ארגון מקומי או רשת ארגונים גלובלית, או שבהן האויב נוקט פעולות טרור באופן מכוון ומתמשך, או שבהן העימות מתנהל

במרחב הסייבר. דוקטרינות כאלה לא יהיו בגדר פרשנויות של הדין הבינלאומי הקיים, אלא בגדר תוספות משמעותיות, ברוח הדין הבינלאומי המוכר והמקובל.

## הערות

1 אנחנו מודים לפרופ׳ יפה זילברשץ על הערות מועילות לטיוטה של מאמר זה, ולקורא אנונימי מטעם בטאון זה על הערות חשובות לנוסח קודם של המאמר.

2 Asa Kasher and Amos Yadlin, "Military Ethics of Fighting Terror: An Israeli Perspective", *Journal of Military Ethics* 4:1 (2005) 3-32, 60-70; Asa Kasher and Amos Yadlin, "Assassination and Preventive Killing", *SAIS Review* 25:1 (2005) 41-57. וכן: עמוס ידלין ואסא כשר, "האתיקה הצבאית של הלחימה בטרור: עקרונות ונימוקים", **מאזני משפט** גיליון 6 (2007) 387–419 [תרגום לעברית של המאמר הראשון באנגלית]; אסא כשר, **"**מבצע "עופרת יצוקה" ותורת המלחמה הצודקת", **תכלת,** גיליון 35 (2009) 29–55; Asa Kasher, "Operation "Cast Lead" and the Ethics of Just War", *Azure* 37 (2009) 43-75 [תרגום לאנגלית של המאמר הקודם].

3 http://www.nytimes.com/2011/10/01/world/middleeast. הטרוריסט היה אנואר אל־עוולאקי ולצידו נהרג גם סמיר חאן, שהיה עורך עיתון של אל־קאעדה, אבל לא היה ברשימת המיועדים להיפגע בפעולת סיכול ממוקד. ההחלטה של מדינה דמוקרטית להתיר הריגת אזרח שלה בתור נזק אגבי של פעילות נגד טרוריסט מובהק ומסוכן היא החלטה בעייתית מסוג חדש. היא בעייתית, מפני שחובת המדינה לאזרחיה היא בדרך כלל להגן עליהם, ובוודאי לא לפגוע בהם. היא החלטה מסוג חדש, מפני שעד כה לא ניתן היתר כזה. פעולות "הסיכול הממוקד" שביצעה ישראל נגד טרוריסטים פלסטיניים גרמו נזקים אגביים, אבל לא בין אזרחי ישראל. בבעיה זו נדון במאמר ההמשך של מאמר זה.

4 Peter L. Bergen, *Manhunt: The Ten-Year Search for Bin Laden – from 9/11 to Abbottabed*, Crown, 2012. ההחלטה להתיר את הריגתו של בן־לאדן, אלא אם כן "הוא נכנע מעצמו באופן בולט", היא בעייתית. מצד אחד, ניתן היה לתפוס אותו בחיים גם אם לא נכנע מעצמו באופן בולט, אלא קפא למשך השניות הראשונות של ההיתקלות בלוחמי הקומנדו הימי של ארצות־הברית. מצד שני, הוא ראש ארגון מעין־צבאי הנלחם בארצות־הברית, ואולי בתור שכזה מותר להורגו כדי להימנע גם מסכנה הנשקפת ממנו בשעת מעשה בהסתברות נמוכה. בבעיה זו נדון במאמר ההמשך של מאמר זה.

5 בהקשר זה ניתן להעלות שאלה בדבר הנורמות הבסיסיות ביותר של הדין הבינלאומי (jus cogens), אלה שמקובלות על קהילת מדינות העולם כנורמות מחייבות שאין להסתייג מהן, כדוגמת האיסור על עינויים (במשמעות מסוימת של ביטוי זה). האם נורמות כאלה מחייבות את החיילים במישרין, או שגם הן מחייבות את החייל, מפני שמדינתו מודה בכך שהן מחייבות אותה ואת הפועלים מטעמה? גם בסוגיה זו נעסוק במאמר ההמשך של מאמר זה, שבו נטען כי גם נורמות בסיסיות כאלה מחייבות את החייל בעקיפין, בתיווך של מדינתו, ולא במישרין.

6 זוהי הנחה חשובה שראוי לדון בהרחבה במסקנות המוסריות והמדיניות העולות ממנה. כאן נזכיר כי יש נורמות, כדוגמת החובה לנהוג בשבויי מלחמה באופן סביר, שנשמרו בהיקפים מרשימים, כשם שיש נורמות, כדוגמת החובה להימנע מפגיעה מכוונת באוכלוסיה אזרחית, שהופרו באופן בולט, כמו ההפצצות של לונדון, מצד אחד, ושל הירושימה ונגאסאקי, מצד שני.

7 איל בנבנישתי, "השפעת אתגרי הלחימה על דיני הלחימה", **צבא ואסטרטגיה,** כרך 4 (1), מאי 2012, עמ׳ 35.

8 שם.

9 אם בנבנישתי סבור שרושם העולה מדברינו בעניין הדוקטרינה האתית יוצר סכנה ממשית, אולי מוטב היה שיתאמץ להראות שהרושם הזה מוטעה. עוד נוסיף, כי מי שקרא את עבודותינו ולא הסתפק ברשמים עיתונאיים בדבר תוכנן, לא ראה בהן "זלזול" מן הסוג שבנבנישתי מייחס לנו. ועוד נשוב לכך בסעיף הבא.

10 ספרו של מייקל וולצר, **מלחמות צודקות ולא־צודקות**, עם עובד, תל־אביב 1984, הוא הצגה מפורטת וחשובה של תורה זו. המהדורות של ספר זה באנגלית מתעדכנות מדי פעם, במתכונת של הוספת הקדמה העוסקת בקצרה במלחמות נוספות. המהדורה הרביעית של הספר הופיעה בשנת 2006.

11 ראו באתר מחלקת המדינה של ארצות־הברית:
http://www.state.gov/r/pa/prs/ps/2011/09/172010.htm

12 במהלך 2012 עלתה אפשרות מעשית שסודן תהיה חברה במועצת האו"ם לזכויות האדם, כאחת מנציגות אפריקה, אבל היא ויתרה על המינוי. נגד נשיא סודן, עומר חסן אל־בשיר, הוציא בית הדין הפלילי הבינלאומי בהאג שני צווי מעצר בשנת 2009 בגין פשעי מלחמה ופשעים נגד האנושות, ובשנת 2010 בגין ג'נוסייד. מדינה יכולה להיות חברה במועצת האו"ם לזכויות האדם כשהנשיא שלה מבוקש על ידי בית הדין הפלילי הבינלאומי בגין ג'נוסייד, פשעים נגד האנושות ופשעי מלחמה. איזו רמת אמון ראוי לגלות ביחס למערכת בינלאומית המאפשרת צירוף כזה?

13 נספח לאמנה, תקנות בדבר דיניה ומנהגיה של המלחמה ביבשה, חלק 1, פרק 1, סעיפים 1–3.

14 שם, סעיף 1, תנאי ב'. הנטייה לשחרר מחובת ההזדהות באמצעות מדים, כדי להקל על "לוחמי חופש" או הנלחמים "למען הגדרה עצמית", היא ראיה לזרמים הפוליטיים הפועלים במעמקי ההתפתחות של הדין הבינלאומי, אבל לא נאריך בזה כאן.

15 לדוגמה: Jeff McMahan, *Killing in War* (Clarendon Press, Oxford, 2009).

16 אביחי מנדלבליט, "לוחמת משפט – החזית המשפטית של ישראל", **צבא ואסטרטגיה**, כרך 4 (1), מאי 2012, עמ' 50–51, ההדגשה – שלנו.

17 איל בנבנישתי, "השפעת אתגרי הלחימה על דיני הלחימה", **צבא ואסטרטגיה**, כרך 4 (1), מאי 2012.

18 פנינה שרביט־ברוך, "דילמות משפטיות בלחימה בעימותים אסימטריים", **צבא ואסטרטגיה**, כרך (1), מאי 2012, עמ' 32, ההדגשה שלנו. התמונה של "המשפט ודיני הלחימה" כמי שמתאימים את עצמם היא בעייתית ועוד נשוב לכך להלן.

19 שם, עמ' 39, ההדגשות – שלנו.

20 שם, ההדגשות – שלנו.

21 שם, ההדגשות – שלנו.

22 לא ברור מדוע שרביט־ברוך מדברת כאן ובהמשך בלשון עבר, "היתה" ולא "ישנה", לדוגמה. הדעת נותנת, כי גם היא סבורה כמונו שדיני המלחמה הקלאסית בעינם עומדים.

23 שם.

24 שם, עמ' 39–40.

25 שם, עמ' 32.

26 שם, עמ' 40.

27 פרק 4, סעיף 24.

28 Customary International Humanitarian Law,
http://www.icrc.org/eng/war-and-law/treaties-customary-law/customary-law/index.jsp

29 ראו לדוגמה: Jeremy Rabkin, "Lawfare", *Jewish Review of Books* 3, no. 2 (2012):

pp. 29-32.

30 שם, עמ' 45.

31 ואולי לא מיותר להזכיר כי גם נוכח הקושי להגיע להסכמה בינלאומית כללית, לא סר הטעם לנסות לגבש הסכמה כזו. דוגמה חשובה מתוך "המציאות הבין־לאומית" היא המשך המאמצים הנערכים באו"ם לגבש הגדרה אוניברסלית של טרור, במסגרת אמנה בינלאומית כוללת למלחמה בו.

32 שם, עמ' 45.

33 בעניין זה, ראו: אסא כשר, "אתיקה מקצועית", בתוך: אסא כשר (עורך), **מבואות לאתיקה א**, הוצאת מאגנס והמרכז לאתיקה, ירושלים 2009, עמ' 1–20, וכן יצחק זמיר, "אתיקה ומשפט", בתוך: אסא כשר (עורך), **מבואות לאתיקה, א**, הוצאת מאגנס והמרכז לאתיקה, ירושלים 2009, עמ' 21–33.

34 שם, עמ' 48.

35 שם, עמ' 38.

36 תופעה מוזרה המתלווה אל הגל הזה של תיאורי סרק היא העדר כל הפניה סדורה אל הנאמר במאמרים שלנו. לשווא יחפש הקורא במאמרים הביקורתיים שלפנינו מראה מקום של טענה כלשהי המיוחסת לנו. האם ייתכן שהמבקרים יצרו לעצמם תמונה של דעותינו על פי כתבות עיתונאיות כאלה ואחרות, מבלי לקרוא את המאמרים שלנו עצמם? ראו בעניין זה את דרישת "הזהירות" שהצגנו בסעיף 1.

37 שם, עמ' 38.

38 שם, עמ' 37.

39 שם, עמ' 37–38.

40 בנקודה זו עולים דבריו של בנבנישתי בקנה אחד עם הדוקטרינה שלנו, כשהוא מציג את הטכנולוגיה בתור מוקד המאפיין את הלחימה הנוכחית (שם, עמוד 31 ואילך).

41 בסעיף 44 לדברי נשיא בית המשפט העליון (בדימוס) ברק בפסק הדין שלו בבג"ץ הסיכולים הממוקדים (769/02) נדון רק "המובן הצר" של מידתיות, כלומר היחס "בין המטרה הצבאית לבין הנזק האזרחי", למרות שמוזכר קיומם של מרכיבים אחרים של מידתיות בדין הבינלאומי. הדוקטרינה האתית שלנו כוללת מרכיבים מעבר לאותו "מובן צר", כפי שראינו זה עתה.

42 בג"ץ 769/02. פסק הדין ניתן ב־14 בדצמבר 2006, שנים לאחר פרסום הדוקטרינה האתית שלנו. מאמר אחד שלנו שבו היא מוצגת מוזכר בפסק־הדין.

43 במקום אחר בפסק הדין מצוטט סעיף 27 מאמנת ז'נבה הרביעית, המחייב להגן על כבוד האדם הנמצא בשטח שבתפיסה לוחמתית ואינו משתתף במעשי האיבה, במגבלות של "אמצעי פיקוח וביטחון" (סעיף 23 בפסק הדין של הנשיא (בדימוס) ברק).

44 דוגמה חשובה נוספת היא היחס לסביבה האזרחית הלא־מסוכנת של הטרוריסטים. נעסוק בה במאמר ההמשך.

45 שם, עמוד 44.

46 דיון מאיר־עיניים באפשרויות "התגמול הלוחמתי", ראו:
Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* (second edition, Cambridge University Press, Cambridge, 2010) pp. 253-260.

47 Asa Kasher, "The Principle of Distinction", *Journal of Military Ethics* 6, No. 2 (2007): pp. 152-167.

48 שרביט־ברוך, שם, עמ' 44.

# 'דילמת דוקו':
# הנחת העמימות והשאיפה חסרת התוחלת למלחמת סייבר סטרילית

**מת'יו קרוסטון**

הוויכוח סביב החלה או אי־החלה של הדין הבינלאומי בכל הנוגע למלחמת סייבר וסביב הצורך באמנת סייבר בינלאומית עשוי להתגלות כבלתי־רלוונטי. שני המחנות, התומכים והמתנגדים, מתווכחים האם יש צורך להחיל את דיני הלחימה, גם על תחום הסייבר, במקרה של מלחמת סייבר. במנותק מהדעה האם חוקי הלחימה חלים אם לאו, או האם יש לקדם אמנת סייבר בינלאומית, או שמא אמנה כזו תהיה חסרת משמעות, יש צורך אחד שנותר על כנו: השאיפה לחוקים שיפקחו על התנהלות מלחמת סייבר. אולם כל הצדדים מחמיצים את העובדה שמבנה תחום הסייבר מונע אסטרטגיה ש"תופסת טרמפ" על נורמות קונוונציונליות של מלחמה. נורמות אלה אפקטיביות בשל היכולת להבחין בין המגזר האזרחי למגזר הצבאי. לא ניתן ליישם הבחנה כזו בתחום הסייבר, בהיותו מאופיין במיזוג המשתתפים, המתקנים והיעדים לכדי ישות אחת, המשלבת באופן חסר־תקנה בין מוסדות אזרחיים לצבאיים. הסבר חשוב זה חסר ביחס לשאלה, מדוע מאמץ כלל־עולמי לשפר ולהבהיר נורמות סייבר נותר בלתי־מאוזן ובלתי־הולם.

וכך נוצרת 'דילמת דוקו': כל עוד המוקד הוא גיבוש יעדים לגיטימיים והצבת מגבלות על פעולה מורשית, ארצות־הברית ובעלות־בריתה חושפות את עצמן לפגיעויות, ובמקביל משקיעות מאמץ עקר שאינו מוביל לבקרת סייבר משופרת. בדיוק כמו הווירוס דוקו (Duqu) שכיכב בדיון הכלל־עולמי ב־2011, מתקפות הסייבר כיום יכולות להתבצע לצורך איסוף מידע **או** כפוטנציאל למתקפה פיזית; הן יכולות להיות יוזמה ממשלתית אך להתבצע דרך נכסים מסחריים חשובים; הן יכולת לכוון ליעדים מדיניים/צבאיים **ובמקביל** להסתייע בחדירה למערכות אזרחיות. יצירת כללי סייבר בדומה לנורמות קונוונציונליות היא לפיכך חסרת תוחלת, שכן כללים אלה אינם ניתנים לאכיפה (כפי שיידון בהמשך). משום כך

ד"ר מת'יו קרוסטון (Matthew Crosston), אוניברסיטת Bellevue, ארצות־הברית

המאמצים הנוכחיים פשוט כובלים את ידי המדינות שומרות החוק. המסקנה היא שיש להקדיש מאמץ רב יותר ליצירת אסטרטגיה מונעת, שמקבלת את בעיית העמימות האזרחית/צבאית כמציאות קיימת. הנטייה של חוקרים וקובעי מדיניות לחתור ללוחמת סייבר 'סטרילית' באמצעות הגבלת הנזק שייגרם על ידי סיווג ברור של המטרה, פירושה שאסטרטגיית הסייבר סובלת מהיעדר כוח הרתעה אמיתי. בקצרה, מומחים להגנת סייבר רק מעצימים את הדילמה.

## חוסר ההשפעה של הדין הבינלאומי

כפי שציין מכון המחקר East-West ב־2011, "קיים צורך דחוף לשיתוף פעולה בינלאומי בסוגיות אסטרטגיות אלה. אם ניכשל במשימה זו, האיום על היציבות הכלל־עולמית יהיה כאיומה של פצצה גרעינית".[1] נורמות בינלאומיות שגובשו באמנות האג וז'נבה הציבו קווי הגנה ברורים לאוכלוסיות אזרחיות בזמן שהמדינות מעורבות במלחמה. כבוד לחיי אזרחים והגנה עליהם נתפסים כיום כמקודשים, ללא קשר לצורה שבה מנוהלת המלחמה, ומכאן הציפייה שמרחב הסייבר יהיה כפוף לפיקוחן של הנורמות הקונוונציונליות.

היו שכינו סוגיה זו אחד מהקרבות הגיאופוליטיים החשובים שמתנהלים כיום, והרחיקו עד כדי האמירה שזהו ה'גראונד זירו' של הדיפלומטיה העולמית, של עבודת הביטחון הלאומי ושל המודיעין.[2] אכן, האופטימיים ביותר רוצים לראות הסכמים מרצון שמטילים מגבלות על פיתוח יכולות הסייבר, ולכאורה משפרים את ההתנהגות במרחב הסייבר. עם זאת, יש מי שהכירו בכך שקיימות סכנות פוטנציאליות בניסיון להגיע להישג כזה. סטיוארט בייקר (Stewart Baker), לשעבר יועץ כללי בסוכנות הביטחון הלאומי האמריקנית (NSA) ועוזר שר לענייני מדיניות במשרד לביטחון המולדת (DHS) בממשל הנשיא ג'ורג' וו. בוש, ניסח את החשש המובן מאליו: ארצות־הברית ובעלות־בריתה יצייתו לכללים, ובו־בזמן, אף לא אחד מיריביה יעשה כן.[3]

אולם הבעיה עלולה להיות אפילו קשה יותר מאשר אי־ציות לחוק: מרבית הרשתות הצבאיות שיכולות ליזום או לבצע מתקפת סייבר עובדות עם אינספור רשתות אזרחיות ותלויות בהן. נוסף לכך, רבים מהגורמים שהם חלק מהתכנון, היוזמה והפריסה של מתקפות סייבר אינם בהכרח גורמים צבאיים רשמיים, אלא עובדים אזרחיים של סוכנויות ממשלתיות. במילים אחרות, עולם לוחמת הסייבר אינו עולם של סיווג ברור אלא של עמימות מכוונת. למעשה, מגמות עתידיות מצביעות על כך שמיזוג זה רק יעמיק ויתחזק עם הזמן.

'הנחת עמימות' זו זכתה עד כה להתעלמות יחסית במהלך הוויכוחים השונים שהתקיימו סביב נושא הסייבר. במקום זאת, ויכוחים אלה התמקדו בשאלה עד כמה משוחררים או נוקשים, רשמיים או לא־רשמיים, בינלאומיים או מקומיים אמורים

להיות אותם קודים של מגבלות. רבים מהקודים המוצעים נועדו להגביל התנהלות בסייבר כך שתושג הגנה על בנקים, אנרגיה ורשתות אחרות של תשתית קריטית, 'למעט כאשר מדינות מעורבות במלחמה'.[4] בעיית העמימות, לעומת זאת, גורמת מבוכה למדינות: כיצד ניתן למתוח קו מפריד בין אזרחים לבין הצבא? הדילמה הגדולה ביותר, אפוא, היא לא הצלחה בזיהוי האחראי למתקפה (ייחוס נכון), אלא העמימות המובנית והמכוונת שמאפיינת את התשתית הקריטית המשמשת לפיתוח יכולות הסייבר של המדינה.

רבים מדיוני הסייבר העכשוויים לוקים באופן שבו הם מבקשים להקיש במשתמע מהלוחמה הקונוונציונלית ללוחמת הסייבר, ולראות במתקפות סייבר שוות־ערך למתקפות חמושות. אך כדי לעשות זאת, הדיון צריך לפנות להגדרות ולפרמטרים המשפטיים: מתי לוחמת סייבר עונה להגדרה של שימוש בכוח חמוש או מהלך רשמי של מלחמה? אילו פעולות ייחשבו כפשעי מלחמה? מה מידת הנזק המצדיקה תגובת נקם?[5] שאלות אלה קשות הרבה יותר למענה בזירת הסייבר בשל הסיוט הלוגיסטי שיוצרת הנחת העמימות. עובדה זו אינה מודגשת במחקרים ואינה זוכה למענה באסטרטגיה.

במקום זאת, מרבית השאלות עוסקות בהשוואה של מידת סכנת החיים, הערכות הנזק ובעיית הייחוס שהוזכרה לעיל. במידה מסוימת, כל הבעיות הללו נותרות בצל בעיית העמימות הצבאית/אזרחית. חוסר היכולת ליצור הפרדה זו פירושו שיכולת ההרס יכולה להיות קטלנית יותר, משום שהיא יכולה להתרחב מעבר לנפגעים צבאיים, הנזק יכול להיות הרסני יותר אם יקיף יותר מאשר מתקנים צבאיים, והייחוס עשוי אף להיות לא־רלוונטי כלל: השאלה **מי** עומד מאחורי המתקפה אינה הפתרון לבעיה, כל עוד ה**איך** שמאחורי ה**מי** משולב באופן שלא ניתן להפרדה לכדי ישות אחת של המגזר הממשלתי, הצבאי והאזרחי. במילים אחרות, רבים מניחים שההבנה **מי ומי** במלחמת סייבר תפתור את מרבית הבעיות המשפטיות, אך הנחת העמימות מציבה אזהרה: בסייבר, **מי** אף פעם אינו מובחן בקלות מ**איך** או חשוב יותר ממנו.

## התסכול שבהצבת תנאים

חלק מהקושי להחיל את הדין הבינלאומי ביעילות על מרחב הסייבר קשור בכישלון נושן לתרגם מונחים ופרמטרים חיוניים לדבר שישפיע על התחום. ההתקדמות לפתרון בעיה זו הייתה מוגבלת ביותר, ואכן, די בהצצה חטופה בספרות של העשור האחרון על מנת להיווכח שמלחמת סייבר אינה חופפת בדיוק למסגרות המשפטיות הקיימות בנוגע למלחמה ולשימוש בכוח.[6] למרות מציאות זו, נעשו ניסיונות נמרצים להתגבר ביעילות על קשיים טרמינולוגיים ודוקטרינריים אלה,

ולהחיל אותם על זירת הסייבר. מאמר זה טוען שניתן לייחס את חוסר ההצלחה למיזוג הצבאי/אזרחי הטבוע בהנחת העמימות.

השאיפה לתנאים, לפרמטרים, להגדרות, לחוקים ולהסכמים מפורשים מבוססת בעיקר על החשש שכישלון ליצור מצבים מפורשים כאלה יותיר את מלחמת הסייבר מחוץ לגבולות המלחמה הקונוונציונלית. המסקנות נחשבות חמורות: תשתית אזרחית קריטית תהיה יעד, כמו גם צרכים בסיסיים כגון חקלאות, מזון, מים, מערכת הבריאות הציבורית, שירותי חירום, טלקומוניקציה, אנרגיה, בנקאות ופיננסים וכן הלאה. עם זאת, הנחת העמימות מבהירה את חוסר התכלית של היעד: מרבית יכולות הסייבר של מדינה, אם לא כולן, מנצלות תשתית אזרחית קריטית שמספקת גם פונקציות אזרחיות חשובות רבות, ותלויות בה. עד היום לא יצרה שום מדינה יכולות סייבר שהן נפרדות ומובחנות במלואן מרשתות ומתשתיות אזרחיות. במילים אחרות, פגיעה ביעדים "צבאיים" פירושה, למעשה, פגיעה ביעדים אזרחיים. נראה שהספרות המחקרית העכשווית עוקפת עובדה זו, וכתוצאה מכך עוסקת בחידה מדומה: ניסיון לכפות תשובה מדויקת תיאורטית על מציאות עם עמימות אמפירית. הוכחה נוספת להתעלמות זו היא הדרישה שחוקי מלחמת הסייבר **יאסרו** למעשה על פגיעה ביעדים שהם תשתית אזרחית טהורה – דרישה המציינת שגורמי סייבר חייבים לנסות לכבד את אמנות ז'נבה בדיוק כמו גורמים קונוונציונליים.[7] אולם במלחמת סייבר, תשתית אזרחית טהורה היא קטגוריה הדומה לפחיתת תשואה. לנוכח ההעצמה וההעמקה של המיזוג הצבאי והאזרחי, תשתית אזרחית טהורה תתגלה יותר כמיתוס מאשר כמציאות.

הכישלון לתת מענה למציאות מבנית זו דומה להדגשת יתר של הגורם הפועל (agency). ג'יימס לואיס (James Lewis) מהמרכז ללימודים אסטרטגיים ובינלאומיים (CSIS) מדגיש כיצד יכולה מדינה להפחית את הסיכונים לכל הצדדים באמצעות אכיפת סטנדרטים משותפים, בדומה למעבר מ'המערב הפרוע' לשלטון החוק.[8] יוג'ין ספאפורד (Eugene Spafford) מסכים עמו, כשהוא מציין כי אבטחת סייבר היא תהליך, לא טלאי, המחייב השקעה מתמדת לטווח הארוך לצד תיקון מהיר, שכן בלעדיו מדינות ימצאו עצמן מיישמות מאוחר מדי את הפתרונות לבעיות.[9] השניים נמנים עם השמות המכובדים והמבריקים ביותר בתחום חקר הסייבר. האזהרות שלהם אינן בלתי־רלוונטיות, אך הדגש על המדינה כסוכן פעולה, ובמקביל הפשל להכיר בהשפעה ובחשיבות של מבנה הסייבר הטבוע, מותירים פער רגיש בחשיבה האסטרטגית בנושא הסייבר. ההכרה בכך היא מכרעת, שכן מדינות מעמיקות במכוון את העמימות לצורכי יתרון אסטרטגי ויעילות כלכלית. לכן, האסטרטגיה אינה אמורה להתמקד בשאלה כיצד לאכוף הפרדה אזרחית/צבאית, אלא עליה לקבל את הנחת העמימות כמציאות לוגיסטית שיש להסתמך עליה.

כדי לקבל אישור אמפירי על חוסר התועלת בניסיון לתת מענה לבעיות אלה, אין צורך להרחיק מעבר לצבא ארצות־הברית במהלך שש השנים האחרונות: גנרל אלכסנדר (Alexander) ממפקדת הסייבר האמריקנית ציין שהושגה התקדמות, אך הסיכונים עדיין צומחים במהירות;[10] סגן־אדמירל מייקל רוג'רס (Michael Rogers), מפקד מפקדת הסייבר של הצי האמריקני, הודה בפני הקונגרס שלא הושג כל הסכם בין המפקדות השונות שיסדיר את דיני לוחמת הסייבר, אך הוא מקווה לראות התפתחויות חיוביות 'בשלב כלשהו בטווח הקרוב';[11] ואפילו הפנטגון הפיק דוח סייבר, שבסופו של דבר טען כי דיני הלחימה אכן חלים על מרחב הסייבר כשם שהם חלים על לוחמה מסורתית, אולם הודה שהמונחים הבסיסיים של 'פעולת מלחמה' ו'שימוש בכוח' עדיין **לוקים בהגדרתם** בתחום הסייבר.[12]

## מלחמות מרות והליכה על חבל דק: דיון צבאי על פרמטרים של סייבר

בדיוק כמו חוקרים, קובעי מדיניות ודיפלומטים, גם הצבא מחויב בקביעות לגבש כללים נוקשים של התנהלות בסייבר, בדומה לכללי מלחמה קונוונציונלית.[13] כבר שנים אחדות תלוי ועומד תיקון לכללים הקיימים להתנהלות בעולם הסייבר.[14] נראה כי בעוד הצבא קיווה שקהילות החוקרים והדיפלומטים יוכלו לסייע, קהילות אלה עצמן קיוו לראות את הצבא מתווה את הדרך. חוסר הבהירות לגבי הנשיאה באחריות הוא עדות לבלבול הנוצר כל עוד הנחת העמימות הנוגעת למיזוג הצבאי/אזרחי אינה מטופלת.

גנרל אלכסנדר הצהיר כי בעת ניהול דיונים על כללי העימות בפעולות סייבר, ניסתה ארצות־הברית לעשות את הדבר הנכון.[15] אולם דיונים אלה נעו בין עמדות שרובן ככולן התעלמו מהעמימות המבנית העיקרית של תחום הסייבר. כתוצאה מכך, הצבא בזבז שש שנים בהבטחות להתקדמות שעתידה הייתה להגיע ולא התגשמה. אפילו הדוח הרשמי של הפנטגון תואר כ'חומק' מסדרה של שאלות מהותיות ובסיסיות חשובות, לרבות הצורך להגדיר מונחים כה בסיסיים כמו 'מלחמה', 'כוחות', ו'תגובה הולמת'.[16] נקודה זו מוזכרת לא על מנת ללעוג לצבא: לנוכח חוסר האונים של כל הצדדים הנוגעים בדבר בטיפול בהנחת העמימות, לצבא לא היה סיכוי רב להתקדם באופן מהותי במשימתו, ולהגדיר במדויק את הפרמטרים של פעולת סייבר.

כיצד, למשל, ניתן לצפות מ־USCYBERCOM לחבר את כל הנקודות, ולהיות הפוסק המתאים המכריע איזה אירוע הוא ראוי לפעולה, כאשר הוא עצמו מודה בקושי שיש לו אפילו לנסח מי בדיוק מרכיב את קבוצת לוחמי הסייבר שפועלת ומגִנה על רשתות הבית?[17] אם הסוגיות הנדונות לא היו כה חמורות ולא כל כך

מרחיקות לכת בנוגע לעתיד לוחמת הסייבר, זה היה כמעט משעשע. רק לאחרונה נראה היה שגופי הצבא הרלוונטיים מתחילים להפנים את הבעיות שנדונות כאן:

> למרות שננקטו כמה צעדים ראשונים ראויים לציון בהקמת מערך בינלאומי של נורמות סייבר – כפי שניכר בגופים דוגמת Convention on Cybercrime – כל מסגרת כלל־עולמית המפקחת על פעולות תגובה צבאית במרחב הסייבר צפויה לממש זאת בקצב איטי. אחרי הכול, כיצד ניתן להסב את כללי המלחמה, המבוססים על נוכחות פיזית של לוחמים וכלי נשק וטריטוריות ריבוניות, לעולם שבו ניתן לשגר באלפיות השנייה 'חיילים' ממספר רב של מדינות?[18]

הציטוט שלעיל תוחם לפחות את הדיון סביב אי־ההתאמה המובנית בין האופן שבו צפויה להתנהל מלחמה במרחב הסייבר, לבין האופן שבו התנהלו המלחמות בעבר. אולם עדיין, ציטוט זה מדגיש גורם פעולה על פני מבנה, ועוסק בהקמת מערך בינלאומי של נורמות סייבר, בעיקר על מנת לסמן רשמית את החלוקה בין נכסים צבאיים לאזרחיים, וכדי למתן פעולה שכבר מתבצעת. גישה זו יכולה להסביר מדוע מסמכי אסטרטגיה רשמיים מסיימים את דרכם כאוסף של אמירות שטחיות על האופן שבו ארצות־הברית מתכוונת להגן על עצמה. ראו לדוגמה את אסטרטגיית משרד ההגנה האמריקני לפעולה במרחב הסייבר, שפורסמה במחצית שנת 2011 :

> יוזמה אסטרטגית 1: יש להתייחס למרחב הסייבר כאל תחום מבצעי שיש לארגן, לאמן ולצייד, כך שמשרד ההגנה האמריקני יוכל לנצל את פוטנציאל מרחב הסייבר במלואו.
>
> יוזמה אסטרטגית 2: יש להפעיל תפיסות חדשות לתפעול הגנה, במטרה להגן על רשתות ומערכות מקומיות.
>
> יוזמה אסטרטגית 3: יש לחבור לשותפים נוספים במחלקות ובסוכנויות ממשלתיות וכן במגזר הפרטי, על מנת לבנות אסטרטגיית אבטחת סייבר כלל־ממשלתית.
>
> יוזמה אסטרטגית 4: יש לכונן קשרים איתנים עם בעלות־ברית של ארצות־הברית ועם שותפים בינלאומיים, על מנת לחזק אבטחת סייבר משותפת.
>
> יוזמה אסטרטגית 5: יש למנף את כושר ההמצאה של המדינה באמצעות כוח אדם ייחודי לסייבר וחדשנות טכנולוגית מהירה.

יש לנצל בצורה מלאה; להפעיל תפיסות חדשות; לחבור לשותפים; לכונן קשרים איתנים; למנף כושר המצאה – כל אלה סיסמאות נפלאות, אולם שום סיסמה אינה מלווה בחשיבה אסטרטגית חדשה ומפורשת שתוכל לגבש את היוזמות האמורות. כל ניסיון לאמץ אסטרטגיה קונוונציונלית חלקית ולאחר מכן לדחוק אליה את תחום הסייבר היה ויישאר פרויקט הנושא פירות דלים בלבד.

## התמודדות עם העמימות: חשיבה אסטרטגית על המיזוג האזרחי/צבאי בסייבר

הצורך בגישה אסטרטגית חדשה מומחש בצורה הטובה ביותר בטיעונים של שניים מההוגים האסטרטגיים המכובדים ביותר, האחד צבאי והשני משפטי, שבמקרה גם מייצגים שתי עמדות מנוגדות בוויכוח הסייבר בנוגע לדיני לחימה (LOAC). שני הצדדים מתעלמים מהבעיה של מיזוג מבני צבאי/אזרחי בסייבר. דנלאפ (Dunlap) אמנם מסכים לצורך בשיפור, אך מאמין שעיקרי דיני הלחימה מספיקים על מנת לתת מענה לסוגיות החשובות ביותר של מלחמת סייבר.[19] נראה שבעיית ההבחנה בין מטרות צבאיות לגיטימיות לבין מטרות אזרחיות אינה מטרידה את דנלאפ כשהוא דן בהשפעה של החלת דיני הלחימה:

> דיני הלחימה מתירים 'פגיעות מקריות' באזרחים ובאובייקטים אזרחיים, כל עוד 'לא מדובר בהיקף רחב ביחס ליתרון הצבאי הישיר והממשי הצפוי'. בקביעה מהן פגיעות מקריות, נדרשים אסטרטגים של סייבר להביא בחשבון פגיעות שניתן להעריך במידה סבירה כי ייגרמו ישירות מהמתקפה. הערכה של השפעות 'מהדהדות' מדרגה שנייה או שלישית עשויה להיות שיקול מדיני נבון, אולם לא נראה שדיני הלחימה מחייבים כרגע ניתוח מתקדם מעין זה.[20]

הבחנה זו שעושה דנלאפ חשובה למדי לנוכח האקלים האינטלקטואלי הנוכחי: הוא הכניס לוויכוח את השימוש החיוני למדי בריאליזם, בכך שהוא מזכיר לאנשים שדיני הלחימה מעולם לא היו אסטרטגיה נטולת פגמים, שהגנה בצורה מושלמת על אזרחים ועל אובייקטים אזרחיים. אולם הבעיה שעולה מדבריו היא שחששותיו בנוגע להבחנה בין הצבאי לאזרחי מוטעים.

טיעונים אלה, שתומכים בדיני הלחימה, נבנו ביעילות סביב העובדה שמלחמת סייבר אינה אמורה להיות מושלמת בכל הקשור להגנה על אזרחים, כיוון שגם דיני הלחימה אינם עומדים בכך. אך טיעונים אלה מתייחסים כאל נתון לכך שמתווה כזה **אפשרי** בדרך כלל. אין זה סביר שמלחמת הסייבר תצליח בעתיד ליצור יכולת כזו, כיוון שהוכח זה כבר עד כמה הפונקציות הקריטיות, הנכסים, ספקי השירותים ושרשרות האספקה מסתמכים כולם בצורה ניכרת על רשתות ותעבורה אזרחיות.[21] בשל כך, אסטרטגיה חדשה צריכה להיות כזו שמונעת את השימוש בנשק סייבר בכללותו, משום שבעצם הפעלתו טמונה סבירות גבוהה לכך שייגרמו **בפועל** סיכון, נזק או אבדות לאזרחים. 'סטריליזציה' של השפעת נשק סייבר שכבר נעשה בו שימוש – באמצעות ניסיון לחייב בחירת מטרות – לא תצלח.

מחנה המתנגדים לדיני הלחימה שוגה באותה שגיאה כשהוא דן בשאלה, מדוע דיני הלחימה אינם יכולים להבהיר את מלחמת הסייבר:

> דיני הלחימה נועדו להבטיח שהצדדים בעימות יראו כמטרות את הלוחמים ולא את האזרחים, ואם אזרחים הופכים למטרות, עליהם להבטיח שגורמים כאלה

> יאבדו את מעמדם המוגן. כדי לקבוע האם מתקפות סייבר מבחינות כהלכה בין יעדים צבאיים לאזרחיים, נדרשת הבנה של ההבחנה.[22]

המחנה המתנגד נכשל בכך שהוא מאמין כי הבחנה כזו אפשרית בסייבר. הוא אינו רואה את ההשפעה האסטרטגית של הנחת העמימות, ובמקום זאת מתמקד בליקויים של דיני הלחימה ושאר הסכמים ונורמות עכשוויים. בקצרה, ההנחה שלו היא 'צרו חוקים טובים יותר ועולם הסייבר יציית להם'. אי לכך, מחנה זה רחוק אפילו יותר ממציאות הסייבר. בעיקרון, המחנה המתנגד נוקט גישה ליברלית יותר ביחס לעימות, משום שהיעד הסופי שלו הוא יצירת אווירה של אמון שיכולה למזער רמות גבוהות של אלימות ובגידה.[23] גישה זו מנוגדת למבנה הנוכחי והעתידי של מלחמת הסייבר אפילו יותר מזו של המחנה השני. שני המחנות מאמינים ביכולת לנטר, לפקח ולהגביל את מלחמת הסייבר לאחר תחילתה, כפי שנעשה לרוב במלחמה קונוונציונלית. זוהי תקוות שווא. הדרך הטובה ביותר להשיג יכולת לנטר, לפקח ולהגביל פעולת סייבר היא באמצעות אסטרטגיה שתחדיר פחד מראש, ולפיכך תגרום זהירות והיסוס. אסטרטגיות סייבר נוכחיות שמכוונות לאמון, להבחנה בין מטרות ולמזעור השפעה על מי שאינם לוחמים פשוט מתעלמות ללא הסבר מהאופן שבו מלחמת הסייבר מאורגנת, נבנית ומבוצעת.

הגישה הליברלית שולטת גם בקהילה המשפטית, ונשענת עליה רבות לצורך חשיבה אסטרטגית שנועדה לשלב פרויקטים משפטיים בתחום הסייבר:

> [פתרון אפקטיבי לאתגר הכלל־עולמי של מתקפות סייבר] לא יושג בידי מדינות יחידות הפועלות לבדן. הוא מחייב שיתוף פעולה כלל־עולמי. לפיכך פירטנו את מרכיבי המפתח של אמנת סייבר, כלומר, קיבצנו חוקים להגדרות ברורות של לוחמת סייבר ומתקפת סייבר, והצגנו קווים מנחים לשיתוף פעולה בינלאומי לאיסוף הוכחות ולתביעות פליליות – אשר יספקו פתרון מקיף וארוך־טווח לאיום הגובר של מתקפות סייבר.[24]

הסקירה שלעיל מציגה צד נוסף המתמקד במיתון הסיכונים ובהגבלת הנזק בתחום הסייבר **לאחר מעשה**. ללא קשר לעמדה פילוסופית, סדר־יום פוליטי או תבונה תיאורטית, דומה שכל צד שבוחן את בעיית הפרמטרים וההגדרות בתחום הסייבר שולל שיקולים של אסטרטגיה מונעת, המבוססת על הרתעה ועל שכנוע להימנע מפעולה. גנרל אלכסנדר, ראש מפקדת הסייבר האמריקנית, ציין את הצורך לסלול את נתיבי הדרך שבה יוכלו או לא יוכלו ממשלות ללכת, וכי סלילת הנתיבים היא השלב החיוני הראשון במתן מענה לאתגר של מתקפות סייבר.[25] המשותף לכל המחנות שנבחנו כאן הוא הנטייה לשלם מס־שפתיים לאסטרטגיה, ולאחר מכן להתמקד באופן בלעדי ב**פעולות לאחר מעשה** כדי להשיג התקדמות. אם ההתמקדות תמשיך להיות על פעולת הסוכן ולא על ליקוי מבני, ההתקדמות לא רק תואט, היא לא תתקיים.

ישנם ניצני התחלה בספרות, המעידים על ניסיון ראשוני להגדיר שינוי תודעתי זה ואת חשיבותו האסטרטגית. הם מתמקדים באופן שבו יש לפעול כדי שהיעד של מעצמות גדולות לא יהיה תקוות השווא לפתח מערכת הגנה מושלמת של הרתעת סייבר, אלא היכולת להחדיר בהדרגה הרתעה המבוססת על פחד הדדי מאיום של מתקפה. מעמדה של ארצות־הברית טוב יותר הודות להתרחבותה למדיניות פתוחה ושקופה, שחותרת ליצור הרתעה המבוססת על יעילות יכולות מתקפת הסייבר שלה.[26] נעשה גם ניסיון ראשוני, אם כי בקנה־מידה קטן אף יותר, להגדיר כיצד פועל כוח סייבר מרתיע למניעה, או כיצד נראית אסטרטגיה כזו. השאיפה היא שאסטרטגיית סייבר גלויה כזו תיצור אמינות לנשק וירטואלי ככזה שמפעיל השפעה משבשת מתגלגלת כה חזקה, עד כדי שלילת השימוש בו. המפתח יהיה בביסוס חשש סביר אצל היריב.

עקב הגילויים האחרונים על תולעת 'סטקסנט' ועל יעילות הווירוסים 'דוקו' **(Duqu)** ו'פליים' **(Flame)** – שסביר מאוד להניח כי התקדמו מעבר ליכולות סטקסנט – נשק סייבר צובר במהירות מוניטין של הפחדה, ולפיכך הרתעה באמצעות אסטרטגיית סייבר גלויה כבר אינה פנטזיה בלבד. זהו טיעון מאזן חשוב לפיתוח אסטרטגיה מקיפה ומלאה, שתאפשר עוצמת סייבר אמריקנית גלויה וסמויה גם יחד.[27] העיקרון הוא לגרום ליריב להאמין מתוך אינטרס עצמי רציונלי שהתנהגות טובה תימנע פגיעה מסיבית, והתנהגות רעה תגרור השלכות חמורות. באופן מעט אירוני, אפשר לומר שהמפתח לפיתוח אסטרטגיית סייבר גלויה של הרתעה מונעת כרוך בהסתמכות על אסטרטגיות ריאליסטיות של האסכולה הישנה, תוך התרחקות מהנורמות הריאליסטיות של אותה אסכולה ישנה ביחס ללוחמה קונוונציונלית. ספרות חדשה זו משפיעה על הנחת העמימות, משום שניתן לטעון כי שינוי תודעתי ואסטרטגי זה הוא ההתמודדות המפורשת ביותר עם 'דילמת דוקו': הדרך היחידה 'להתגבר' על העמימות היא להימנע מכניסה למצב עימות שמחייב להתמודד איתה. במילים אחרות, מציאות הסייבר הנוכחית, כמו גם העתיד הנראה לעין, הופכים אסטרטגיות שמסתמכות על פעולה **לאחר מעשה** לנחותות מטבען, בהשוואה לאסטרטגיות מונעות.

## חשיבותה של 'דילמת דוקו'

הניתוח המוצג מצביע על ליקויים במאמצים הנוכחיים לגבש הגדרות ופרמטרים ברורים לפיקוח על כללי מלחמת הסייבר. הדגש שהושם כאן על קשיים מבניים – כלומר, המיזוג הטבוע בין המגזר הצבאי לאזרחי בסייבר – מציג את ההשלכות החמורות הצפויות כתוצאה מאסטרטגיות שאינן מתמקדות במאמץ לעצור מראש פעולת סייבר. רק לאחרונה מתחילים להופיע ניתוחים משפטיים בודדים, שמציפים בעיות אלה:

> אין זה סביר שמדינה כמו ארצות־הברית תוכל לנקוט אמצעי הגנה נגד השפעתן של מתקפות על מטרות צבאיות באמצעות הפרדה בין יעדים צבאיים לבין אזרחים ואובייקטים אזרחיים במרחב הסייבר. זאת בשל התלות ההדדית הקיימת בין מערכות אמריקניות ממשלתיות ואזרחיות, כחלק מההסתמכות הממשלית המלאה־כמעט על חברות אזרחיות לצורכי אספקה, תמיכה ותחזוקה של יכולות הסייבר שלה... אומדנים של החלוקה היחסית עתידים להוכיח שקיים סיכון במיוחד במרחב הסייבר, בעוד התוצאות קשות יותר לחיזוי מאשר בעולם האמיתי: למתקפות פיזיות יש לפחות יתרון של התבססות על כללי הפיזיקה והכימיה. לדוגמה, כיוון שרדיוס הפיצוץ של פצצת חצי־טון הוא נתון ידוע, ניתן לדעת מראש ובוודאות מה יימצא מחוץ לרדיוס הפיצוץ ומה ייכלל בו. גבולות השגיאה ומתקפות הסייבר הרבה יותר רחבים ופחות מוכרים...[מרבית הדוחות אינם מסבירים באיזה אופן] ניתן לכונן שותפויות ציבוריות־פרטיות אלה כך שיוכלו ליישם בצורה סבירה סוגיות של דיני לחימה, [והם] אינם נותנים מענה לשימוש הצפוי בהגנות אקטיביות מצד המגזר הפרטי.[28]

כפי שהודגם לעיל, סוגיה מבנית זו היא יותר מאשר סמנטיקה בלבד, היא כוללת הכול: מי מעורב במלחמת סייבר, מה ניתן להרוס במלחמה כזו, מי יכול להיחשב קורבן בעת מלחמת סייבר, ואפילו את השאלות הפילוסופיות והאתיות שיש לשאול על מלחמת הסייבר עצמה. 'דילמת דוקו' היא הפצרה להתרחק מיעדים בלתי־ניתנים להשגה ומחלומות אידאליסטיים, שמקורם בתקווה חסרת־שחר ליצור מלחמת סייבר סטרילית, בדומה להגבלות שנכפו על מלחמה קונוונציונלית. מלחמת סייבר לעולם לא תוכל להפוך לסטרילית באופן זה. משום כך, החשיבה האסטרטגית העכשווית ביחס לתחום הסייבר צריכה להכיר בכך שיש להפנות משקל רב יותר ל"הנחת העמימות", מאשר לבעיית הייחוס המוכרת.

## הערות

1 Tom Leithauser, "Rules of War Should Apply to Cyber Conflict", *Cybersecurity Policy Report,* February 14, 2011.

2 Tom Gjelten,"Shadow Wars: Debating Cyber Disarmament", *World Affairs, 173;4,* November/December, 2010.

3 .Ibid

4 Aliya Sternstein, "Experts Recommend an International Code of Conduct for Cyberwar", *National Journal,* June 10, 2011.

5 Andrew Liaropoulos, "War and Ethics in Cyberspace: Cyber-conflict and Just War Theory", *European Conference on Information Warfare and Security, 177-XI,* (Reading, UK), July 2010.

6 Anatolin-Jenkins, Vida CDR, "Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?", *Naval Law Review*, *51:132,* 2005.

7 Don Tennant, "The Fog of (CYBER) War", *Computerworld, 43;16,* April 27, 2009.

8 James Fallows, "Cyber Warriors", *The Atlantic Monthly, 305;2,* March 2010.

9 Ibid.

10 John Curran, "Updated Rules for Cyber Conflict Coming Soon, Defense Officials

Say", *Cybersecurity Policy Report,* March 26, 2012.
11 Lolita Baldor, "Cyber Warriors", *Army Times,* August 6, 2012.
12 Gorman, Siobhan and Julian Barnes, "Rules for Laws of War: US Decides Cyber Strike Can Trigger Attack", *The Australian,* January 1, 2011.
13 Anonymous, "Military Ponders Cyber War Rules", *Los Angeles Times,* April 7, 2008.
14 Ellen Nakashima, "Pentagon Seeks to Engage Rules of Engagement in Cyber War", *The Herald,* August 10, 2012.
15 Ibid.
16 Ellen Nakashima, "Pentagon: Cyber Offense Part of Strategy", *The Washington Post,* November 16 2011.
17 Wesley Andrues, "What US Cyber Command Must Do", *Joint Forces Quarterly, Issue 59, 4th quarter,* 2010.
18 Ibid.
19 Charles Dunlap, "Perspectives for Cyber Strategists on Law for Cyberwar", *Strategic Studies Quarterly,* Spring 2011.
20 Ibid.
21 Erik Mudrinich, "Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem", *Air Force Law Review, 68,* 2012.
22 Michael Gervais, "Cyber Attacks and the Laws of War", *Journal of Law and Cyber Warfare, 30;2*, 2012.
23 Ibid.
24 Hathaway, Oona, et al, "The Law of Cyber-Attack", *California Law Review,* 2012.
25 Ibid.
26 Matthew Crosston, "World Gone Cyber M.A.D: How Mutually Assured Debilitation is the Best Hope for Cyber-deterrence", *Strategic Studies Quarterly,* Vol. 5, No. 1, Spring 2011.
27 Matthew Crosston, "Virtual Patriots and a New American Cyber Strategy: Breaking the Zero-sum Game", *Strategic Studies Quarterly*, Vol. 6, No. 4, Winter 2012.
28 Hannah Lobel, "Cyber War Inc: The Law of War Implications of the Private Sector's Role in Cyber Conflict", *Texas International Journal of Law, 47;3,* Summer 2012.

## 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.

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 ביטחונית / 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 4,500 מילים.

המבקשים להציע מאמר מתבקשים לשלוח לח"מ תקציר של כ־200 מילים. לכותבים שהצעותיהם יאושרו ישלחו הוראות מפורטות לכתיבה בכתב העת.

להגשת הצעות ולפרטים נוספים ניתן לפנות לח"מ.

בברכה

דניאל כהן
מתאם כתב העת "צבא ואסטרטגיה"
danielc@inss.org.il