צבא ואסטרטגיה

כרך 5 | גיליון 3 | דצמבר 2014

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 3 | דצמבר 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.

עורך ראשי: אלוף (מיל.) עמוס ידלין
עורך: ד"ר גבי סיבוני
חברי המערכת: תא"ל (מיל.) אודי דקל, ד"ר עודד ערן, פרופ' זכי שלום
מתאם כתב העת: דניאל כהן

ועדה מייעצת:

סונג'וי ג'ושי / מרכז אובזרבר למחקר, הודו
פטר ויגו ג'קובסון / הקולג' הדני המלכותי להגנה, דנמרק
רוט דיאמינט / אוניברסיטת טורקוואטו די טלה, ארגנטינה
מטין הפר / אוניברסיטת בילקנט, אנקרה, תורכיה
ג'יימס ג'. ווירץ / בית הספר הימי ללימודים מתקדמים, ארצות הברית
ריכרדו ישראל זיפר / האוניברסיטה האוטונומית של צ'ילה, צ'ילה
דניאל זירקר / אוניברסיטת וואיקאטו, ניו זילנד
ג'פרי ג'. לארסן / תאגיד יישומי מדע בינלאומי SAIC, ארצות הברית
ג'יימס לואיס / המרכז למחקר ללימודים אסטרטגיים CSIS, ארצות הברית
ג'ון נומיקוס / מרכז המחקר ללימודים אירופאים ואמריקניים, יוון
תיאו נית'לינג / אוניברסיטת המדינה החופשית, דרום אפריקה
גלן מ. סגל / סקוריטטם ויגילאתא, אירלנד
פרנק ג'. סילופו / אוניברסיטת ג'ורג' וושינגטון, ארצות הברית
סטפן ג'. סימבלה / אוניברסיטת פן סטייט, ארצות הברית
ט.ו. פאול / אוניברסיטת מקגיל, קנדה
מריה רחל פריר / אוניברסיטת קוימברה, פורטוגל
מרים דאן קאוולטי / המכון הפדרלי השוויצרי לטכנולוגיה, צירך, שוויץ
אפרים קארש / קינגס קולג', לונדון, בריטניה
קאי מיכאל קנקל / האוניברסיטה האפיפיורית הקתולית של ריו דה ז'נרו, ברזיל
ברונו תרטרס / קרן למחקר אסטרטגי, צרפת

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

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

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

© 2013 כל הזכויות שמורות

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

איום ארגוני הטרור במרחב הסייבר

גבי סיבוני, דניאל כהן, אביב רוטברט

מטרת מאמר זה היא לדון באיום הטרור במרחב הסייבר ולבחון את אמיתות התפיסות שהתגבשו בשנים האחרונות כלפי איום זה וכן לבחון מהן היכולות ששחקן לא מדינתי יכול להשיג והאם יכולות אלה עלולות להוות איום ממשי על ביטחונן הלאומי של מדינות. ניתוח האיומים העיקריים שבפניהם עומדת מדינה בראייה רב שנתית ולאור שינויים צפויים במאזן האסטרטגי שלה מחייב הצגת הגורמים המאיימים על המדינה, תוך זיהוי שורשי האיום וסיבותיו. לפיכך, מאמר זה ייבחן האם הטרור, שהשפעתו בדרך כלל טקטית יוכל לעשות (ואולי כבר עשה) את המעבר ליכולת של נשק סייבר בעל השפעות אסטרטגיות, נשק בעל נזק רחב היקף או לאורך זמן, מהסוג שמוריד מדינות על ברכיהן וגורם למערכות קריטיות לקרוס.

מילות מפתח: מרחב הסייבר, סייבר טרור, נשק קיברנטי, ארגוני טרור, שחקנים לא מדינתיים, סייבר פשע, מערכות מידע ארגוניות, מערכות ליבה מבצעיות, יכולת אכוונה מודיעינית, יכולת טכנולוגית.

מבוא

סרט הראינוע הראשון שהוצג בפני קהל נעשה על ידי האחים לומייר ב־1895. הסרט הראה רכבת נכנסת לתחנה, לכאורה לכיוון הצופים באולם. הצופים, שהיו משוכנעים שהרכבת מתקרבת אליהם, צרחו בבהלה וברחו מהבניין. בסרט הקולנוע הראשון שהוקרן אי פעם, נדמה היה לצופים שהם רואים מולם מציאות.[1]

ד"ר גבי סיבוני הינו חוקר בכיר וראש תכנית לוחמת סייבר במכון למחקרי ביטחון לאומי. דניאל כהן הינו עמית מחקר ומתאם תכנית לוחמת סייבר במכון למחקרי ביטחון לאומי. אביב רוטברט הינו מלגאי תכנית ניובאוור במכון למחקרי ביטחון לאומי ותלמיד לתואר שלישי בבית הספר למדעי המחשב באוניברסיטת תל־אביב.

המחברים מבקשים להודות לנעם ק. מהמטה הקיברנטי הלאומי, לדורון אברהם וקרן ח'טקביץ, מתמחים בתכנית לוחמת סייבר במכון למחקרי ביטחון לאומי, על סיועם בהכנת מאמר זה.

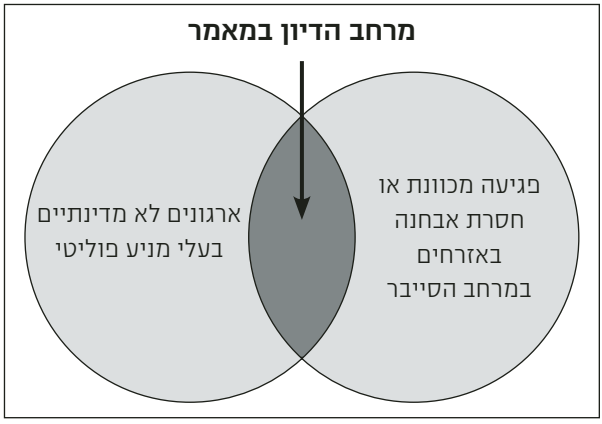
איום טרור הסייבר הוא נושא בו מתערבבים לעיתים המציאות והדמיון. אם נבחן את אחת התפיסות המרכזיות במרחב הסייבר – ההתמודדות עם איומי טרור – ניווכח כי רציונל התפיסה (שהחלה להתפתח לאחר אירועים מעצבים מתחילת שנות האלפיים, כגון "באג המילניום" ופיגועי 11 בספטמבר 2001) הוא שהעולם נראה כבשיאו של תהליך הנמצא מעֵבר לעידן המודרני והטכנולוגי – עידן הנעדר גבולות מגוננים, ובו מדינות חדירות למידע, לרעיונות, לאנשים ולחומרים; בקיצור, עולם פתוח. הטרור שנלקח בחשבון באיום הייחוס בעולם כזה הוא טרור מסוג חדש: איום, בו טרוריסט הנמצא במרתף נידח בקצה העולם הוא בעל פוטנציאל נזק המשנה לחלוטין את מאזן הכוחות על ידי יכולת חדירה למערכות ביטחוניות או כלכליות חשובות בכל מדינה ומדינה ברחבי העולם והשגת מידע רגיש מהן, כמו גם יכולת לגרום להרס של מערכות.[2]

האם המציאות של 11 בספטמבר 2001, בה ארגון טרור התכונן במשך כשנתיים לפיגוע, כולל הכשרת טייסים בקורס טיס, שלבסוף השתמשו בסכינים יפניות פשוטות לבצע מגה פיגוע, יכול לחזור על עצמו במרחב הסייבר? האם תרחיש, בו ארגון טרור ישלח קבוצת טרוריסטים כסטודנטים לקורסים רלוונטיים במדעי המחשב, יחמש אותם באמצעים טכנולוגיים נגישים לכל, ויבצע באמצעותם ובאמצעות היכולות שרחשו מגה פיגוע טרור במרחב הסייבר הוא מציאותי או דמיוני? כדי לתת מענה לשאלה זו יש לבחון, ראשית, מהן היכולות ששחקן לא מדינתי מסוגל להשיג והאם יכולות אלו עלולות להוות איום ממשי על ביטחונן הלאומי של מדינות. ניתוח האיומים העיקריים שבפניהם עומדת מדינה, בראייה רב־שנתית ולאור שינויים צפויים במאזן האסטרטגי שלה, מחייב הצגת הגורמים המאיימים על המדינה, תוך זיהוי שורשי האיום וסיבותיו.

אין עוררין על כך שגורמים לא מדינתיים, ארגוני טרור ועבריינים ממנפים את מרחב הסייבר למטרותיהם ומפיקים תועלת מתחום שבו כולם ניצבים באותה נקודת זינוק, תחום המאפשר גם לשחקנים יחידים קטנים להשפיע, ובאופן שאינו נמצא ביחס ישר לגודלם. אסימטריה זו מייצרת סביבה סכנות שונות, שבעבר לא משכו את תשומת הלב ואת האנרגיות של המעצמות. השאלה היא האם פעילותם של גורמים אלה במרחב הסייבר היא איום בעל פוטנציאל לנזק גדול ורחב היקף? ואם כן, מדוע הוא לא התממש עד כה?

מאמר זה יבחן האם התקפות של ארגוני טרור במרחב הסייבר, שהשפעתן עד היום היא בדרך כלל טקטית, יוכלו להשתדרג (ואולי כבר השתדרגו) לכלל יכולת להפעיל נשק סייבר בעל השפעות אסטרטגיות, נשק היכול לגרום נזק רחב היקף ו/או לאורך זמן, מהסוג ש"מוריד מדינות על ברכיהן" וגורם למערכות קריטיות לקרוס. מטרת מאמר זה היא לדון באיום הטרור במרחב הסייבר ולבחון את אמיתות התפיסות שהתגבשו בשנים האחרונות כלפי איום זה.

המאמר מתרכז בפעולות של ארגונים לא מדינתיים בעלי סדר יום ומטרות פוליטיות, גם אם אלה מופעלים או נתמכים לעיתים על ידי מדינות. זאת, כדי להבדיל בין אותם ארגונים לבין פעולות המבוצעות ישירות על ידי מדינות שאינן בתחום עיסוקו של מאמר זה, או על ידי ארגוני פשיעה או ארגונים אחרים בעלי מטרות שהן בעיקר בעלות אופי פלילי. לצורך המאמר, פעולת טרור של ארגון לא מדינתי במרחב הסייבר תוגדר כפעולה במרחב זה, שמטרתה לפגוע באופן מכוון או חסר אבחנה באזרחים. כך, לדוגמה, פעולה לשיבוש אתר אינטרנט של בנק מסחרי על ידי ארגון לא מדינתי, שלו מטרות פוליטיות, תוגדר כפעולת טרור במרחב הסייבר. לצורך המחשה ניתן להתבונן בתרשים הבא, המתאר את מרחב הדיון במאמר זה:



המתודולוגיה של המחקר

מספר אבני דרך נדרשו לצורך בחינת פעילותם של ארגוני הטרור במרחב הסייבר. הראשונה שבהן הייתה זיהוי המניעים לשימוש במרחב הסייבר במסגרת המאבק הפוליטי אותו מנהלים ארגוני הטרור. כך ניתן לזהות שני מניעים עיקריים לשימושים אלה: הראשון הינו השימוש במרחב הסייבר לצרכי תמיכה בפעילות הטרור, ובעיקר לצרכי גיוס כספים ופעילים, או לצורך הלבנת כספים לצרכי הפעילות; השני הינו השימוש בכלים במרחב הסייבר שיספקו את הפגיעה בפועל ביעדים שקבע לעצמו ארגון הטרור, וזאת לצד שימוש באמצעים אלימים אחרים. כאן נבחן שיתוף הפעולה שבין ארגונים לא מדינתיים לבין מדינות המפעילות אותם והתומכות בפעילות הטרור שלהם.

אבן הדרך השנייה של המחקר חייבה בחינה והבנת עומק של היכולות עליהן יכולים ארגוני הטרור להניח יד. זאת, מתוך הבנה שלא כל מפעיל מחשב, יהיה זה גאון טכנולוגי ככל שיהיה, יוכל לייצר פיגוע טרור אפקטיבי ומשמעותי, ותוך

בחינת ההנחה שפגיעה משמעותית במרחב הסייבר תמשיך להיות נחלתן של מדינות עתירות טכנולוגיה ומחייבת משאבים לא מבוטלים – הן מודיעיניים והן טכנולוגיים. עם הבנת סל היכולות הטכנולוגיות והמודיעיניות הרלוונטיות של ארגוני הטרור, נדרש היה לבחון האם זוהו פעולות של ארגונים כאלה בפועל. לבסוף, נעשה ניתוח של כלל הממצאים במטרה לגבש תובנות והמלצות מסכמות כחלק מהמענה.

ניתוח יכולות

מרחב הסייבר מסייע להעמקת ידע ורכישת יכולות. בנוסף, הטכנולוגיה מסייעת ליצירת רשת תקשורת אנונימית.[3] כמו כן, מרחב הסייבר משמש מצע להרחבת השותפים לפעילות טרור. לעומת גיוס פעילי טרור במרחב הפיזי, מרחב הסייבר מאפשר הגדלה משמעותית של מאתר המשתתפים בפעילות, גם אם במקרים רבים נעשה שימוש בשותפים "משוּטים", המופעלים על ידי ארגונים ומדינות באצטלה של פגיעה בממסד. תופעות כאלו ניתן היה לראות באירועי התקיפה של האקרים על יעדים ישראליים ב־7 באפריל 2013,[4] כאשר חלק מהפעילים במתקפה קיבלו הכוונה, באמצעות אתרי אינטרנט בכיסוי, באשר לשיטות הפעולה וליעדים לתקיפה. שימוש בתחושות אנטי־ממסדיות של צעירים, כמו גם בתחושות כלליות נגד המערב או מדינת ישראל, מאפשר הרחבה משמעותית של מאתר הפעילים וכן מייצר מסה משמעותית המאפשרת את פעולת טרור הסייבר. לדוגמה, נטען שבמבצע "עמוד ענן" נרשמו יותר ממאה מיליון מתקפות סייבר על אתרים ישראליים,[5] וכי פעילים לא מעטים הופעלו במהלך אותו מבצע ובהתקפות המשך שלו, באמצעות הכוונה שמאחוריה עמדו ככל הנראה איראן וגרורותיה.[6]

סל היכולות והאמצעים של ארגוני טרור במרחב הסייבר מוגבל מצד אחד בשל קשר הדוק ונגישות טכנולוגית, שהינה בדרך כלל נחלתן של מדינות בעלות יכולות טכנולוגיות מתקדמות ושל חברות בעלות יכולות טכנולוגיות משמעותיות, ומן הצד השני – נגיש לשוק החופשי המאפשר מסחר בכלי נשק קיברנטיים ובמידע בעל ערך לתקיפה. גורם מסייע בבניית יכולות אלו הוא מדינות התומכות בטרור, המעוניינות להשתמש במתווך (Proxy) כדי להסתיר את זהותן כיוזמות תקיפה על יעד מסוים. בנוסף, נדרש ארגון הטרור להכשרת מומחים ולצבירת ידע על שיטות איסוף מודיעין, שיטות תקיפה ואמצעים להסוואת כלי תקיפה, כדי לחמוק ממערכות הגנה ביעד.

המחקר מראה שעד עתה אין לארגוני הטרור את התשתית המדעית והטכנולוגית העצמאית לפיתוח כלי סייבר בעלי יכולות לגרום נזק משמעותי, וכי הם חסרים את היכולת לבצע איסוף מודיעין איכותי למבצעים (מל"ם). היכולות

של ארגוני הטרור לקיים פעילות פוגענית במרחב הסייבר ייבחנו, אפוא, תחת אילוצים אלה.

ככלל, יש להפריד בין שלושה מרחבי תקיפה בסיסיים: תקיפה של שער הארגון, בעיקר אתרי אינטרנט, וזאת באמצעות תקיפות, מניעת שירות או השחתה של אתרים; תקיפה של מערכות המידע הארגוניות;[7] ולבסוף, התקיפה המתוחכמת (והמורכבת) ביותר – תקיפת מערכות הליבה המבצעיות[8] של הארגון, הנוגעות לליבה התפעולית שלו, למשל מערכות בקרה תעשייתיות.[9] טרור הסייבר נגד מדינה ואזרחיה יכול להתבצע במספר רמות תחכום, כאשר בכל רמה נדרשות יכולות הן בהיבט הטכנולוגי והן בהיבטי ההשקעה בצד התוקף. הנזק שאפשר לגרום נמצא ביחס ישיר לרמת ההשקעה.

תקיפת שער הארגון

כאמור, ברמה הבסיסית ביותר ניתן לתקוף את שער הארגון, כלומר את אתר האינטרנט שלו, החשוף לציבור. הרמה הפשוטה ביותר של טרור קיברנטי מתאפיינת בהתקפות המונעות שירות, מפריעות לשגרת החיים, אך לא גורמות לנזק מהותי, בלתי הפיך או מתמשך. התקפות כאלו מכונות "התקפות מניעת שירות מבוזרות" (DDoS –Distributed Denial of Service), ומהותן היא גרימת עומס פניות אל מחשב או שירות אינטרנטי מסוים, באופן שחורג מסף היכולת שלו לספק מענה. בכך משיגים למעשה השבתה של השירות. פניות תמימות ואמיתיות לא ייענו, מכיוון שהשירות עמוס בהתמודדות שלו עם הפניות מצד התוקף.

התקפות DDoS אותן יבצע ארגון טרור[10] נדרשות להיות אפקטיביות ולהימשך פרק זמן סביר, כדי שמספר רב ככל האפשר של אנשים יבחינו במתקפה וייפגעו ממניעת השירות. יעדים מתאימים למתקפה כזו יכולים להיות, בין היתר, בנקים, שירותי סלולר, חברות טלוויזיה בכבלים ובלווין, ושירותי בורסה (מסחר וחדשות). לרשימה זאת ניתן להוסיף גם אפליקציות סלולריות נפוצות, ששיבוש הגישה אליהן יכול לגרום למטרד, דוגמת: WAZE, גישה לשירותי דואר אלקטרוני וליומן פגישות, וגם אפליקציות לשיחות על גבי רשת האינטרנט (Voice Over IP).

שיטה נוספת לתקיפת שער הארגון היא תקיפות על שרתי DNS – שרתים המשמשים לניתוב תעבורת האינטרנט. תקיפה כזו תביא לכך שאנשים המבקשים לגשת לאתר או לשירות מסוים יגיעו בפועל לאתר אחר, אליו התוקפים מעוניינים לנתב את התעבורה. תקיפה דומה אך פשוטה יותר יכולה להתבצע ברמת המחשב הבודד במקום ברמת שרת ה־DNS הכללי; כלומר, התקשורת ממחשב בודד תנותב לאתר של התוקף במקום לאתר האמתי אליו המשתמש מנסה לגלוש. הנזקים שתקיפות כאלו יכולות לגרום נעים מגניבת מידע, דרך מניעת שירות מלקוחות וכתוצאה מכך פגיעה עסקית בשירות שהותקף, ועד פגיעה תדמיתית בשירות:

התוקף יכול להפנות את התעבורה אל דף המכיל תעמולה ומסרים אותם הוא רוצה להציג לציבור.

שיטה פופולרית ויחסית פשוטה לפגיעה תדמיתית בשער הארגון היא השחתת אתר האינטרנט שלו. ההשחתה (Defacement) כוללת שתילת מסרים פוגעניים בעמוד הראשי, הכנסת תעמולה שהתוקפים מעוניינים להפיץ לקהל רחב ופגיעה תדמיתית (ואולי גם עסקית) בארגון, הנתפס כלא מוגן ולא מאובטח מפני תוקפים פוטנציאליים.

תקיפת מערכות המידע של הארגון

רמת הביניים במדרג הפגיעה במרחב הסייבר מכילה תקיפות של מערכות המידע והמחשוב של הארגון, דוגמת שרתים, מערכות מחשב, מאגרי נתונים, רשתות תקשורת ומכונות לעיבוד נתונים. התחכום הטכנולוגי הנדרש ברמה זו גבוה יותר מהנדרש לצורך תקיפת שער הארגון. רמה זו מחייבת השגה של נגישות למחשבי הארגון דרך עובדים בארגון או באמצעים אחרים. הנזק אותו ניתן לגרום בסביבה הווירטואלית כולל פגיעה בשירותים חשובים כמו בנקים, שירותי סלולר ודואר אלקטרוני.

קו ברור מפריד בין התקיפות המתוארות כאן ובין האיומים של הטרור הקיברנטי הפיזי: בדרך כלל לא ניתן לצפות בתקיפות אלו לנזק פיזי, אולם ההסתמכות על שירותים וירטואליים והנגישות אליהם עלולה בכל זאת לייצר פגיעה משמעותית. דוגמה לכך ניתן לראות בתקיפה באמצעות וירוס המחשבים Shamoon,[11] שפגע במחשבי חברת הנפט הסעודית ערמקו (Aramco) באוגוסט 2012. התקיפה, גם אם לא פגעה במערכות הליבה המבצעיות של החברה, הצליחה להשבית עשרות אלפי מחשבים ברשת הארגונית שלה, תוך גרימת נזק משמעותי באמצעות מחיקת מידע ממחשבי הארגון והאטת פעילותו לאורך זמן.[12]

תקיפת מערכות הליבה המבצעיות של הארגון

הרמה הגבוהה ביותר במדרג סיכון התקיפה הינה התקיפה של מערכות הליבה המבצעיות והתפעוליות של הארגון. לדוגמה, ניסיון פגיעה בתשתיות קריטיות פיזיות כמו תשתיות הולכת מים, חשמל, גז, דלק, מערכות בקרה על תחבורה ציבורית, או מערכות תשלומים בנקאיות. זאת, על ידי מניעת אספקת השירות החיוני לזמן מסוים, או במקרה החמור אף גרימה של נזק פיזי באמצעות פגיעה במערכות הפיקוד והבקרה של הארגון הנתקף.

מתקפה מוצלחת עלולה לגרום לשחרור חומרים מסוכנים לאוויר ולפגיעה פיזית באוכלוסייה גדולה. זוהי הנקודה בה פיגוע וירטואלי עלול לייצר נזק פיזי, וההשפעות עלולות להיות הרסניות. בעקבות חשיפת ה־Stuxnet עלתה המודעות

לצורך להגן על מערכות בקרה תעשייתיות, אך מכאן ועד יישום בפועל של פתרונות הגנה עדיין הדרך ארוכה. את הפער הזה יכולים לנצל גורמי טרור, למשל על ידי יצירת קבוצת מומחים מתחומי המחשוב ואוטומציה של תהליכים, לצורך יצירת וירוס המסוגל לפגוע במערכות אלו.[13]

דרך נוספת להשגת נשק קיברנטי־פיזי עשויה להתפתח מהשוק השחור של נשק הסייבר ומהתרחבותו גם לתחום של תשתיות פיזיות, וזאת בנוסף על הנשק הווירטואלי אותו הוא מציע כבר היום. יש לציין כי עד כתיבת שורות אלו, תרחיש זה טרם התממש בפועל, אך מכיוון שמדובר בנשק קיברנטי מורכב ויקר, ייתכן והמסחר בו מתנהל במחשכי האינטרנט באופן חשאי.[14] זוהי, כאמור, המדרגה הגבוהה ביותר של פיגוע סייבר, והעלויות והנזקים הנגרמים ממנו הם גבוהים בהתאמה, כפי שניתן ללמוד מהתולעת Stuxnet.[15]

פיתוח יכולות תקיפה, בין של מדינות ובין של ארגוני טרור, מחייב תמהיל מתעצם של יכולות לפעולה במרחב הסייבר בשלושה מרכיבים עיקריים: יכולות טכנולוגיות, יכולת הכוונה מודיעינית לקביעת היעדים (ייצור מטרות) ויכולת מבצעית.

יכולות טכנולוגיות

אופייה המבוזר של רשת האינטרנט מקל מאד על הסוחרים בנשק קיברנטי. ואכן, האקרים וסוחרים רבים מנצלים את היתרונות הללו ומציעים כלי סייבר ושירותי תקיפה במרחב הסייבר לכל דורש. כך התפתח שוק מגוון ומשוכלל מאד של סחר במוצרי סייבר למגוון מטרות, כאשר טווח המחירים נע בין דולרים בודדים לתקיפה פשוטה וחד־פעמית של מניעת שירות, לאלפי דולרים עבור שימוש בחולשות שאינן מוכרות ויכולות לאפשר לתוקף דילוג לתוך מערכת מחשב מוגנת ביותר. שוק זה צומח בזכות מרחב הסייבר, על גבי תשתיות של רשתות חברתיות ופורומים המאפשרים תקשורת אנונימית בין סוחרים לקונים.[16] תופעה מעניינת לה אנו עדים בתקופה האחרונה היא יציאתם של סוחרים אלה ממחשכי הרשת האפלה אל האור. ניתן למצוא אותם ברשת החברתית הפופולרית ביותר, "פייסבוק".[17] בבלוג של חברת אבטחת המידע RSA[18] מתוארת מציאות חדשה, שבה הסוחרים מציעים את מרכולתם לא רק כמוצר, אלא כשירות שלם הכולל התקנת שרתי פיקוד ובקרה, הדרכה על השימוש בכלים ואפילו הנחות ומבצעים ואפשרות לרכוש רק מודולים מסוימים מתוך כלי התקיפה, כדי להוזיל את המחיר. במצב זה של פריחת השוק נשאלת השאלה, האם וכיצד ארגוני טרור יכולים לעשות שימוש לתועלתם בכל הידע והכלים שהצטברו בשוק הפשיעה הקיברנטי?

כדי לענות על שאלה זו, נצטרך לבחון את הפער בין שפע הכלים והיכולות המוצעים כיום למכירה חופשית באינטרנט, לבין הצרכים של ארגוני טרור. השוק

של כלי התקיפה כיום מוכוון לארגוני פשיעה קיברנטית, ובעיקר לצרכי הונאות, גניבת כסף מחשבונות בנק תמימים והתחזות, תוך איסוף פרטים של כרטיסי אשראי, מספרי חשבון בנק, תעודות זיהוי וכתובות מגורים, סיסמאות כניסה לאתרים פיננסיים ועוד. כלים אלה לא מתאימים בהכרח לצרכי ארגון הטרור. עם זאת, ארגוני טרור רבים יכולים לכלול גם מרכיבים של ארגון פשיעה קיברנטי כדי לאסוף כסף למימון פעילות הטרור המרכזית שלהם. המטרה המרכזית של ארגוני הטרור – גרימת נזק משמעותי והפחדה – יכולה להתבצע במספר דרכים, בדרגות קושי וחומרה שונות. הכלים מעולם הפשיעה הקיברנטית יכולים לסייע רבות בתקיפות לשיבוש שירות (DDoS), או בגניבת כמויות גדולות של מידע רגיש מחברות שאינן מוגנות מספיק (למשל מידע על כרטיסי אשראי ממאגרי מידע לא מאובטחים) – דבר שיעורר, קרוב לוודאי, חרדה בציבור. יחד עם זאת, גרימת נזק למערכות הבקרה דורשת כברת דרך נוספת מצדם של הטרוריסטים, שכן משימתם מורכבת הרבה יותר מגניבת כרטיסי אשראי וכלי הפשיעה הקיברנטיים לא משרתים אותה. באשר לרמת הביניים שתוארה לעיל, הנוגעת לפגיעה במערכות המידע של הארגון, נראה כי קיימים בעולם הפשיעה כלים היכולים לסייע לטרור הסייבר. אמנם, נדרשת התאמה מסוימת של כלים אלה, כמו למשל התאמה מגניבת מידע למחיקת מידע, אולם מדובר בכברת דרך קטנה יותר, שמפתחי הווירוסים יסכימו, קרוב לוודאי, לבצע אותה עבור ארגוני טרור תמורת תשלום מתאים.

יכולת הכוונה מודיעינית

אחד המרכיבים המרכזיים בתהליך תכנון פיגוע קיברנטי הוא בחירת יעד או קבוצת יעדים שהפגיעה בהם תביא ליצירת האפקט הרצוי מבחינת ארגון הטרור. לצורך זה על גוף הטרור לרכז רשימת גופים המהווים פוטנציאל ליעדי פגיעה. כבר כיום קיימת טכנולוגיה חינמית שמספקת כלים המקלים על ביצוע משימה זו. למשל, באמצעות הרשתות החברתיות "פייסבוק" ו"לינקד־אין", ניתן לאתר מיהם העובדים באגפי המחשוב של חברות תשתית, חברות מזון ועוד. אם ניקח לדוגמה את חברת החשמל, מחקרים אקדמיים[19] מראים כי ניתן למפות ללא קושי רב את אגפי החברה, לאתר את העובדים במחלקות השונות ולברור את העובדים להם יש גישה למערכות המבצעיות של החברה.[20] אם עובדים אלה מודעים לחשיבותה של אבטחת המידע ולא ניתן בשל כך לתקוף אותם ישירות, אפשר לאתר בני משפחה וחברים שלהם באמצעות "פייסבוק" ולתקוף דרכם את היעד המבוקש. רשתות חברתיות מהוות מקור חשוב לריגול ואיסוף מידע עסקי ואישי על חברות וארגונים,[21] וארגוני טרור יכולים לעשות בקלות שימוש במידע המופץ בהן לתועלתם.

קיים גם צורך למפות את מערך המחשוב של הארגון המותקף, להבין אילו מחשבים מחוברים לרשת, אילו מערכות הפעלה ותוכנות הגנה מותקנות בהם, אילו הרשאות יש לכל מחשב, ודרך אילו מחשבים ניתן לשלוט במערכת הבקרה של הארגון. לדוגמה, אם ארגון טרור ירצה לשלוט על התפקוד של טורבינת ייצור חשמל, המשימה המוטלת עליו, אף על פי שהיא טכנית יותר וקשה יותר ממיפוי המבנה הארגוני של החברה, קלה היום במיוחד לאחר פרסום עבודתו של האקר "כובע לבן" שערך את "מפקד האינטרנט" הראשון בהיסטוריה.[22]

באמצעות רשת ענפה של רובוטים (תוכנות המושתלות על מחשבים וממתינות לפקודה ממרכז הפיקוד והבקרה איתו הן מתקשרות), ערך אותו האקר רשימה של 1.3 מיליארד כתובות IP הנמצאות בשימוש, ועל חלקן הוא פרסם גם נתונים טכניים, כמו סוג השערים הפתוחים, לאילו בקשות מגיבות הכתובות הללו ועוד. תוצאות המפקד מפורסמות באינטרנט באופן חופשי לכל דורש. עבור האקר בעל כוונות זדון, אלה לפעמים כל הנתונים הנדרשים כדי לבצע תקיפה ולהשתלט על מערכת מחשב שלמה של אדם פרטי או ארגון. כך ניתן למפות מבנה ארגוני של חברה, ואם הרשת שלה אינה מוגנת מספיק – גם לדלות מידע על המחשבים הנמצאים בשימוש עובדי החברה.

הגנה טובה ומודעות לאבטחת מידע יכולות להקשות מאד על האקרים וטרוריסטים לבצע את הפעולות שתוארו לעיל. ארגונים להם מערכות מבצעיות קריטיות מפעילים לרוב שתי רשתות מחשוב: האחת חיצונית, המקושרת לאינטרנט, והשנייה פנימית, המנותקת פיזית מהאינטרנט ומחוברת למערכות הבקרה התעשייתיות של הארגון. מִפקד האינטרנט אינו מכיל נתונים על רשתות פנימיות מבודלות, מכיוון שהן לא נגישות דרך האינטרנט. תקיפה של רשתות אלו דורשת מודיעין, משאבים ומאמץ גדול מאד, וספק אם קיימים ארגוני טרור המסוגלים לבצע תקיפות כאלו. כאן באה לעזרתם של ארגוני הטרור עבודת מחקר נוספת שנערכה על ידי חוקרים מאוניברסיטת ברלין,[23] המציגה על גבי מפה של "גוגל" (שמציעה לחוקרים, כחלק משירות המפות שלה, להציג ולשתף מידע גיאוגרפי שאספו) מספר רב של מערכות בקרה תעשייתיות (ICS) הפרוסות בכל העולם ומחוברות לרשת האינטרנט. המידע המוצג במפה לקוח מתוך מאגר מידע עצום הנגיש בחינם לכל דורש דרך האתר Shodan,[24] אשר הופך את חייו של האקר טרוריסט לקלים יותר. שירות זה נעזר במידע אותו אספה חברת "גוגל" לצורך שירותי המיפוי והפרסום מבוסס־המיקום שלה, והפכה אותו לנגיש לציבור. ייתכן שהאקרים שפרצו לאחרונה לרשתות ביתיות של מאות ישראלים עשו שימוש בשירותיו של אתר Shodan כדי לאסוף מודיעין לתקיפה, ואולי גם כדי להשיג כלים (תחמושת קיברנטית) לביצועה בפועל.[25]

יכולת מבצעית

לאחר איסוף המודיעין וייצור או רכישה של הכלים הטכנולוגיים לקראת התקיפה, על מתכנני הטרור הקיברנטי לעבור לפעילות אופרטיבית. זהו השלב של ביצוע התוכנית בפועל, המנוהל באמצעות וקטור תקיפה.[26] הכוונה במושג זה היא לשרשרת פעולות המתבצעות על ידי התוקפים, כאשר כל פעולה מהווה מדרגה אחת בדרך ליעד הסופי וכוללת, בדרך כלל, שליטה מלאה או חלקית על מערכת מחשב או על מערכת בקרה תעשייתית. בווקטור תקיפה לא ניתן לדלג על מדרגות, וכדי להתקדם למדרגה מסוימת, יש לוודא שכל השלבים שלפניה הסתיימו בהצלחה.

השלב הראשון בווקטור תקיפה הוא, בדרך כלל, יצירת נגישות ליעד. שיטה נפוצה מאד ומוצלחת ליישומו במרחב הסייבר מכונה Spoofing[27] או זיוף. יש דרכים שונות לעשות שימוש בשיטה זו, כאשר המשותף לכולן הוא זיוף הזהות של שולח הודעה כדי שנמען ההודעה יבטח בתוכן ולא יהסס לפתוח קישור בתוך ההודעה. למשל, קל מאד לשלוח דואר אלקטרוני לעובד בחברת החשמל, שהוזכרה לעיל, כאשר השולח המזייף משתמש בכתובת של עמית לעבודה, בן משפחה או אדם קרוב אחר. מטרת התוקף במקרה זה היא לגרום לנמען ההודעה לבטוח בתוכן ההודעה ולפתוח דבוקות המצורפות אליה, או להיכנס לכתובות אינטרנט המופיעות בתוכה.

זיוף דואר אלקטרוני הוא שיטת תקיפה הקיימת שנים רבות. בהתאם לכך גם פותחו אמצעי הגנה נגדה אלא שגם התוקפים צברו ניסיון. כיום ניתן להצביע על אירועים שבהם נשלח דואר אלקטרוני הנראה תמים לחלוטין, תפור לנמען ומכיל התייחסות אישית אליו, ובתוכו קיימים מסמכים הנוגעים ישירות לתחום עיסוקו. כתובת השולח במקרים אלה הייתה מזויפת והופיעה ככתובת של עמית לעבודה. ברגע שהנמען פתח את הדואר האלקטרוני, המחשב שלו נדבק בווירוס ללא ידיעתו.

שיטת הזיוף יכולה להועיל כאשר היעד הוא מחשב המחובר לרשת האינטרנט ויש אפשרות לשלוח אליו הודעות, אך במקרים מסוימים לא זה המצב. רשתות המוגנות ברמה גבוהה יהיו, בדרך כלל, מנותקות מהעולם החיצון באופן פיזי, כלומר לא יהיה קישור פיזי (גם לא אלחוטי) ביניהן ובין רשת בעלת רמת אבטחה נמוכה יותר. במקרה כזה יצטרך התוקף לנקוט צעד אחר או נוסף בווקטור התקיפה – הדבקת רשת היעד בווירוס באמצעות החדרתו על גבי מכשירים שפועלים גם ברשת הלא מוגנת וגם ברשת המוגנת. דוגמה לכך הם התקני Disk On Key, המשמשים כאחסון נייד ונוח של קבצים. כאשר התקפה כזו מצליחה, התוקף משיג גישה אל ציוד טכנולוגי השייך לקורבן (מחשב, מחשב כף יד, טלפון חכם), והשלב הראשון בווקטור התקיפה – יצירת נגישות ליעד – מסתיים. בתרחישים מסוימים הצעד הזה הוא החשוב והמשמעותי ביותר מבחינת התוקף. למשל, כאשר הושגה בדרך זו

נגישות לרשת מבצעית של חברה, ומטרתו של הטרוריסט היא לחבל באותה הרשת ולמחוק מתוכה מידע, האתגר העיקרי הוא להשיג גישה ליעד. פעולת המחיקה והחבלה קלות יותר, בהנחה שהווירוס שהושתל ברשת מופעל ברמת הרשאות מספיק גבוהה. אך בתרחישים מורכבים יותר, כאשר הטרוריסט מעוניין לגרום נזק משמעותי ולהשיג אפקט הפחדה גדול יותר, נדרשת השקעה לא מבוטלת בצעדים הבאים בווקטור התקיפה.

חברת "לוקהיד־מרטין", שהייתה קורבן להתקפת סייבר, מציעה מתודולוגיה לניתוח פעולות התקפיות במרחב הסייבר, אותה היא מכנה "שרשרת הקטל הקיברנטית".[28] על פי מתודולוגיה זו, מתקפת סייבר מורכבת בנויה משבע אבני דרך, המקבילות לפעולות של הכנת המבצע ויצירת וקטור התקיפה. הצעד הראשון הוא איסוף מודיעין על היעד. לאחר מכן יש לבחור את כלי הנשק הקיברנטי המתאים לתקיפה, ואז לשגר אותו אל היעד. הצעד הבא כולל ניצול חולשה אצל מחשב היעד, שתאפשר לשתול קובץ זדוני במערכת שלו, ולאחר מכן להתקין את הכלי באופן שיוכל לבצע פעולות בתוך המערכת. השלב הבא הוא יצירת תקשורת בין הכלי ובין שרתי הפיקוד והבקרה של התוקף, כדי שניתן יהיה להנחות את הכלי ולקבל ממנו דיווח על המתרחש במחשב הקורבן. השלב האחרון בשרשרת הקטל הוא ביצוע פעולות אקטיביות בתוך מחשב הקורבן, כמו מחיקה, התפשטות של הכלי, השתלטות על התקנים פיזיים הנגישים מהמחשב ועוד. המונח "שרשרת קטל קיברנטית" נבחר במטרה להדגיש כי כדי שהתוקף יצליח לבצע פיגוע קיברנטי, הוא צריך לצלוח את כל אבני הדרך מבלי להתגלות ומבלי שגישתו אל היעד תיחסם.

ארגון טרור המבקש לפגוע במערכות מבצעיות יצטרך לבצע את כל השלבים בשרשרת. אלו הן פעולות מתקדמות ומורכבות שארגוני טרור בדרך כלל לא ידעו לבצע בעצמם. אם היעד מוגן ברמה נמוכה מאד, לא תידרש יכולת טכנולוגית גבוהה מהתוקף כדי לייצר פגיעה או השחתה; אך ברוב המקרים יצטרכו הטרוריסטים לרכוש מוצרים או שירותים מהאקרים מומחים. במילים אחרות, הם יצטרכו לבצע "מיקור חוץ".

טרוריסטים ימצאו בשוק מוצרי הסייבר ההתקפיים יכולות נגישות ליעד שאינן בעלות רשת מבודלת. באותו שוק הם ימצאו גם מוצרי תקיפה, וניתן להניח שימצאו גם מוצרים לניהול מבצעים ברשת היעד (בדומה לממשק הניהול של הסוס הטרויאני SpyEye[29]). למרות כל זאת, טרם זוהו כלים זמינים ברשת המאפשרים תקיפה של המערכות המבצעיות של הארגון. הנגישות לכלים אלה אמנם אפשרית,[30] אך היא משימה הדורשת משאבי כוח אדם רב (מרגלים, פיזיקאים, מהנדסים), השקעה כספית (בפיתוח כלי תקיפה ובדיקתו בתנאי מעבדה על ציוד אמיתי) וזמן רב כדי לאתר חולשות ולבנות וקטור תקיפה מוצלח.

סוגי התקיפות במרחב הסייבר

ניתן לאפיין מספר סוגי תקיפה במרחב הסייבר, הן לפי רמת הנזק הצפויה והן לפי עוצמת ההשקעה המודיעינית, הטכנולוגית והמבצעית. ברוב המקרים קיימת הלימה בין שני המדדים. הסקירה להלן מציירת תמונה של יכולות ארגון שאינו מדינתי לפעול במרחב הסייבר.

תקיפה חובבנית

זוהי פעולה הנעשית באמצעות כלים המוכרים (ברוב המקרים) לחברות אבטחת המידע ומזוהים על ידי תוכנות ההגנה הסטנדרטיות. נגד כלים אלה פותחו הגנות ולפיכך הם עשויים להיות אפקטיביים רק מול מטרות שאינן מוגנות. שימוש בכלים כאלה נעשה, בדרך כלל, למטרות לימוד או משחק בלבד, מכיוון שרק במקרים נדירים הם יכולים לשמש לגניבת מידע בעל ערך או לחבלה במערכות מחשב מוגנות. אמנם, יש להם יכולות ריגול וחבלה, אך אלו הן ברמת תחכום נמוכה.

תקיפה קלה

זוהי תקיפה שלא מושקעים בה מאמצים רבים, ועיקר הפעילות בה היא חיפוש כלים מוכנים ברשת האינטרנט או רכישתם מידי חברות המתמחות בכך. תקיפות מסוג זה בדרך כלל לא יצליחו לפגוע בגופים בעלי מודעות לאבטחת מידע (גופים מדינתיים, צבאיים, תעשיות מתקדמות), אבל יוכלו לחדור למחשבים פרטיים ולגנוב מהם מידע ואף לחבל בהם. תקיפות אלו הינן ברוב המקרים חד־פעמיות (גניבת קובץ חשוב, מחיקת כונן), אך לעיתים יכולות להיות חלק מתקיפה ארוכה יותר, כמו למשל במקרה של גניבת ה־DNS (Domain Name System) של המחשב המאפשרת מעקב אחר הפעילות שלו ברשת האינטרנט.

הכלים בהם ייעשה שימוש בתקיפה קלה לא יכללו מודולים שונים של תוכנה, אלא רכיב קוד אחד שעלותו זולה, המבַצע את כל הפעולות של הכלי. רכיב קוד זה יהיה כתוב בצורה שלא מאפשרת לשנות או להרחיב בקלות את יכולותיו ויהיה מוכוון מטרה. חיפוש באינטרנט ורכישה בסכומים שלא עולים על כמה אלפי דולרים יוכלו לספק לכל דורש נשק סייבר בעל יכולות מצומצמות.

בקטגוריה זו של תקיפה נכלל גם השימוש ברשת סוכני תוכנה (בוֹטְנֶט) לתקיפות DDoS. יצירת הרשת היא פעולה מורכבת יותר, אך מרגע שנוצרה, היא יכולה לשמש למבצעי DDoS רבים. ניתן גם להשכיר אותה לשימוש לכל דורש לצורך מניעת שירות מאתרים שונים שאינם מוגנים ברמה גבוהה מפני תקיפה כזו.

תקיפה בינונית

זוהי תקיפה המסוגלת לגרום נזק משמעותי, או לבצע פעולות ריגול מתקדמות, אבל בעלות נמוכה יותר מאשר תקיפה חמורה (ראו להלן). בפעולה כזאת לא יהיה, בדרך כלל, שימוש בחולשות ייחודיות חדשות (כיוון שהן יקרות מאד), אלא בחולשות מוכרות או מוכרות חלקית, שיעד התקיפה עדיין אינו מוגן מפניהן. הפעולה לא תכלול מודוּלים יקרים למימוש ובדיקה, דוגמת אה שפותחו עבור "סטוקסנט". יחד עם זאת, פעולה כזאת, באמצעות מודוּלים לתקיפה של מערכות מחשב (מחיקה, שיבוש) ומודוּלים לריגול, יכולה להיות יעילה מאד במסגרת תקיפה בטווחי זמן קצרים למטרות הרס (כי לא ייעשה מאמץ להסתיר את ההרס; הדבר יקר מדי), או לריגול נגד קורבן שלא מאבטח את מערכותיו ברמה גבוהה.

העלות של תקיפה בינונית פחותה משמעותית מעלותה של תקיפה חמורה: פחות שנות אדם, ללא ציוד חומרה ייחודי ויקר להשגה וללא רכישה של חולשות חדשות ויקרות, אלא של חולשות זולות יותר המספיקות לצורך חדירה למערכות המחשוב של הקורבן, תוך ידיעה שהן עלולות להתגלות ולהיחסם בעתיד הלא רחוק. קטגוריית התקיפה הבינונית כוללת גם וירוסים המסוגלים להתפשט ברשת מחשבים (תולעים) ולהמתין לפקודה מהמפעיל שלהם. מודל תקיפה כזה שימושי במיוחד ליצירת רשת סוכני תוכנה רובוטיים, המשמשת למבצעי DDoS. כמו כן נכללת בקטגוריה זו תקיפת DDoS נגד אתרים מוגנים, הדורשת תחכום מצד התוקף והכרת מערכת ההגנה ביעד.

תקיפה חמורה

המדובר בפעולה שהושקעו בפיתוחה משאבים רבים של כוח אדם, מִחשוב וכסף, ואשר נבדקה באופן יסודי במעבדה קודם להפעלתה. פעולה כזאת מנצלת חולשות לא מוּכרוֹת (אשר יתנו למפעילי התקיפה טווח זמן רחב להפעלתה עד שיתגלו וייסגרו). בדרך כלל זו פעולה שתוּפסווה כדי להותיר עקבות מעטות. כלי התוכנה יכיל מספר מודוּלים, שחלקם עשויים להיות מיועדים לחבל במערכות תוכנה או חומרה ייעודיות שנמצאות אצל הקורבן (למשל "סטוקסנט"), ולא יפעלו בשום מקרה אחר, כדי להפחית אפשרות לזיהוי.

פעולת תקיפה חמורה עשויה להכיל מגוון רחב מאד של מודוּלים, בהתאם למטרה שאותה היא נועדה לתקוף, כגון מודוּלי ריגול – חיפוש קבצים או מידע ושליחתו למפעיל; ומודוּלי תקיפה והסוואת התקיפה – חבלה בצנטריפוגות תוך כדי הטעייה של מערכת הבקרה כדי שתדווח שהן תקינות. העלות של תקיפה כזו תהיה שנות אדם רבות, מִחשוב מתקדם ולפעמים גם מערכות חומרה וציוד בדיקה שנועד לדמות את הזירה בה יפעל הקוד המפַגע, למשל צנטריפוגות עם מערכות בקרה של חברת "סימנס" במקרה של "סטוקסנט".

הטבלה הבאה מסכמת את ההבדלים בין תקיפות הסייבר השונות, וזאת באמצעות רשימת קריטריונים המאפשרת להבחין באופן ברור בין סוגי נשק סייבר על פי מדרג יכולות. הפרמטרים מתחלקים למספר קטגוריות: הראשונה כוללת את מעטפת נשק הסייבר ואת היכולת שלו להגיע אל יעדו ולפעול בו באופן חופשי מבלי שייחסם. שני הפרמטרים הראשונים נכללים בקטגוריה זו. חשיבותם היא בכך שהם מאפשרים סביבת עבודה נוחה לתוקף, היודע שהוא יכול לחדור אל יעדיו ולבצע בהם פעולות בזמן ובאופן הנדרש, מבלי לחשוש מסגירת היכולת או מחשיפה של הנשק והסרתו. שלושת הפרמטרים הבאים מהווים קטגוריה שנייה, המתייחסת ליכולת הנשק הקיברנטי לבצע את פעילותו העיקרית ביעד, בין אם מדובר בגניבת מידע, הריסתו, פגיעה ושיבוש אלקטרוניים או פיזיים. כלי הנשק השונים בקטגוריה זו נבדלים על פי האלגוריתמים שהם מיישמים לטובת ריגול ביעד ועל פי יכולותיהם לשבש מערכות ממוחשבות ופיזיות. יכולת פגיעה פיזית תהווה מדרגה עליונה בקטגוריה זאת. הקטגוריה האחרונה מייצגת שני פרמטרים הקשורים להתנהלות הכלי בתוך רשת היעד, ומידת היכולת והחופש שהוא נותן למפעיליו לנהל את המבצע ביעד. יכולות גבוהות בקטגוריה זו נחשבות לכאלו שמאפשרות לעדכן את כלי הנשק על ידי שליחת מודולים מרחוק, שינוי הגדרות המשימה, שליחת פקודות לכלי והגדרת יעדים מודיעיניים חדשים עבורו. כמו כן, כלים מתוחכמים יידעו לנהל מבצע איסוף גדול ברשת היעד, על ידי התפשטות בין מחשבים שונים ואיסוף מרוכז ומתואם של מידע מתוכם.

ההבדלים בין תקיפות הסייבר

	תקיפה חמורה	תקיפה בינונית	תקיפה קלה	תקיפה חובבנית
יכולות חדירה למערכות	טובה מאד	טובה	טובה	נמוכה
יכולות הסוואת הפעילות	טובה מאד	טובה	בינונית	נמוכה
יכולות ריגול	טובה מאד	טובה מאד	טובה	בינונית
יכולות פגיעה במערכות מחשוב	טובה מאד	טובה מאד	טובה	נמוכה
יכולות פגיעה במערכות פיזיות המקושרות למערך המחשוב	טובה	נמוכה	נמוכה	נמוכה
יכולות התפשטות	טובה מאד	טובה	נמוכה	נמוכה
יכולות תקשורת מול שרת בקרה	טובה מאד	טובה	בינונית	נמוכה

ניתן ללמוד מהטבלה כי הקריטריונים המבדילים באופן משמעותי את יכולות התקיפה החמורה (המצויה בידי מדינות מעטות) משאר יכולות התקיפה בסייבר הם היכולת להתפשט ברשת, לקיים תקשורת מול שרת הבקרה ולפגוע במערכות פיזיות המקושרות למערכות המחשוב. אלו הן הפעולות הדורשות את התחכום הרב ביותר בייצור תקיפות סייבר. רק מדינות מעטות נגישות לידע וליכולת לייצר כלי נשק מסוג זה. העמודה "תקיפה קלה" בטבלה משקפת את מדרגת הכניסה הנמוכה למרחב הלחימה הקיברנטי. ניתן לראות כי גם כלי נשק קטנים המצויים בידי גורמים לא־מדינתיים מסוגלים לחדור למערכות מחשב בצורה טובה, לבצע ריגול ברמה טובה מאד, ואם הם מיועדים לכך – גם לחבל במערכות המחשב אליהן הם חדרו. מכיוון שיכולת ההסוואה שלהם היא בינונית, הם לא יוכלו לשהות במערכת המותקפת זמן רב כמו כלי נשק כבדים או בינוניים, ולכן יצטרכו להשיג את מטרותיהם בטווח זמן קצר.

פעילות במרחב הסייבר המיוחסת לארגוני טרור

פרק זה מפרט פעולות טרור במרחב הסייבר בהתאם לתיחום שפורַט לעיל, כלומר פעולות שמטרתן פגיעה מכוונת או חסרת אבחנה באזרחים, וזאת באמצעות פעולה במרחב הסייבר של ארגונים לא מדינתיים בעלי סדר יום ומטרות פוליטיות, גם אם אלה מופעלים או נתמכים לעיתים על ידי מדינות.

אחת ההתקפות המתועדות הראשונות של ארגון טרור נגד מערכות מחשוב מדינתיות התרחשה בסרי־לנקה על ידי לוחמי הגרילה "הנמרים הטמילים" ב־1998. שגרירויות של סרי־לנקה ברחבי העולם הוצפו במשך שבועיים בכ־800 הודעות דואר אלקטרוני ביום עם המסר: "אנחנו נמרי האינטרנט השחורים ואנחנו הולכים לשבש את מערכות התקשורת שלכם". יש הטוענים כי מסר זה השפיע על המקבלים אותו וזרע חשש ופחד בשגרירויות.[31] מספר שנים לאחר מכן, ב־3 במארס, 2003, כת יפנית בשם Aum Shinrikyo ("האמת העליונה") ערכה מתקפה קיברנטית מורכבת שכללה השגת מידע רגיש הנוגע למתקני גרעין ברוסיה, אוקראינה, יפן ומדינות נוספות, תוך ניסיון לתקוף את מערכות אבטחת המידע של המתקנים. המידע הוחרם וניסיון התקיפה נכשל לפני שהארגון הצליח לפעול.[32]

תקיפה באמצעות שליח התקיימה בינואר 2009 בישראל. באירוע זה התקיפו האקרים את תשתית האינטרנט של ישראל בתגובה למבצע "עופרת יצוקה" ברצועת עזה. התקיפה בוצעה על יותר מחמישה מיליון מחשבים. בישראל משערים שהיא נעשתה ממדינות שהיו חלק מברית המועצות לשעבר, בהוראה ובתשלום של גורמי חמאס וחזבאללה.[33] בינואר 2012, קבוצת האקרים פרו־פלסטיניים הקוראת לעצמה "Nightmare" הפילה למשך זמן קצר את אתר הבורסה לניירות ערך בתל אביב ואת אתר חברת "אל על" ושיבשה את פעילות אתר "הבנק הבינלאומי

הראשון". בהתייחסות לכך מסר דובר חמאס ברצועת עזה כי "החדירה לאתרים ישראליים פותחת מרחב חדש של התנגדות ומלחמה אלקטרונית חדשה נגד הכיבוש הישראלי".[34]

מלחמת האזרחים בסוריה הביאה לפעילות התקפית ערה מצד ארגון "הצבא הסורי האלקטרוני" (Syrian Electronic Army – SEA) – קבוצה אינטרנטית המורכבת מהאקרים תומכי משטר אסד, התוקפת את קבוצות האופוזיציה הסוריות תוך שימוש בטכניקות של מניעת שירותים ומידע או פריצה לאתרים ושינוי תוכנם. הקבוצה הצליחה להוציא לפועל פעולות שונות הפוגעות בעיקר באתרי האופוזיציה הסורית, כמו גם באתרי אינטרנט מערביים. פעילות אחרונה זו שלה מכוונת בעיקר כלפי אתרי מדיה, תרבות וחדשות ברשתות מערביות. הקבוצה הצליחה לפרוץ ליותר מ־120 אתרים, ביניהם *The Financial Times, The Telegraph, The Washington Post, Al Arabia*.[35] אחת התקיפות המשמעותיות והאפקטיביות הייתה באפריל 2013, בעת ש"הצבא הסורי האלקטרוני" פרץ לחשבון הטוויטר של *Associated Press* ושתל "ציוץ" מזויף, שבו נאמר שהבית הלבן הופצץ ושבאותה מתקפה נפצע נשיא ארצות הברית. המשמעות המיידית של הודעה זו הייתה צניחה חדה בשווקים הפיננסיים בארצות הברית ובמדד דאו ג'ונס למשך כמה דקות.[36] הארגון גם חשוד בניסיון חדירה למערכות שליטה ובקרה של מערכות מים. כך, למשל, ב־8 במאי 2013 פורסם בסוכנות ידיעות איראנית צילום מסך של מערכת ההשקיה של קיבוץ סער.[37]

במהלך מבצע "עמוד ענן" ברצועת עזה ב־2012 וכן בחודשים שלאחריו, ערכה קבוצת האקרים המכנה עצמה "OpIsrael" תקיפות[38] נגד אתרים ישראליים על רקע הסכסוך הישראלי־פלסטיני, בשיתוף עם "אנונימוס". בין היתר נפגעו אתר משרד ראש הממשלה, אתר משרד הביטחון, אתר משרד החינוך, אתר המשרד לאיכות הסביבה, אתר התעשייה הצבאית, אתר הלשכה המרכזית לסטטיסטיקה, אתר האגודה למלחמה בסרטן, האתר הרשמי של לשכת נשיא המדינה ועוד עשרות אתרים ישראליים קטנים. הקבוצה פרסמה כי הסיבות לתקיפה היו פגיעה בזכויות אדם של פלסטינים והפרת החוק הבין־לאומי על ידי ישראל.

באפריל 2013, קבוצת האקרים פרו־פלסטיניים, בשם "לוחמי הסייבר של עז א־דין אל קסאם" המזוהה עם הזרוע הצבאית של חמאס, לקחה אחריות להתקפה על אתר האינטרנט של חברת אמריקן אקספרס. אתר החברה ספג התקפת DDoS אינטנסיבית שנמשכה כשעתיים ושיבשה את האפשרות של לקוחות החברה להשתמש בשירותיו. בניגוד להתקפות DDoS טיפוסיות, כמו אלה שמבוצעות על ידי "אנונימוס" ומבוססות על רשת מחשבים שנפרצו ואוגדו לבוטנט הנשלט ע"י התוקף, ההתקפה של עז א־דין אל קסאם השתמשה בסקריפטים שהופעלו על גבי שרתי רשת פרוצים, יכולת המאפשרת גיוס רוחב פס גדול יותר לביצוע המתקפה.[39]

אירוע זה שייך למגמה הכוללת התעצמות יכולות הסייבר של חמאס, בין השאר, בשכלול המערכה המודיעינית האיסופית כנגד צה"ל, ואיום השתלטות עוינת על מכשירי סלולר של אנשי צבא וחשיפת סודות באמצעותם.[40]

תקיפות סייבר עצמאיות של ארגוני טרור

ניתוח התקפות ארגוני הטרור במרחב הסייבר מראה שסף הכניסה הנמוך למתקפות מסוימות והנגישות לכלי תקיפה קיברנטיים לא הובילו למעבַר של ארגוני הטרור לתקיפות בעלות פוטנציאל נזק גדול ומתמשך. ארגוני הטרור פעלו עד כה בעיקר בתקיפת שער הארגון. כלי התקיפה העיקרי היו מתקפות למניעת שירות והתקפות בסדר גודל של תקיפה חובבנית עד תקיפה בינונית. הסיבה העיקרית לכך היא שסל היכולות והאמצעים של ארגוני הטרור במרחב הסייבר הינו מוגבל, ועד עתה אין להם התשתית המדעית והטכנולוגית העצמאית לפיתוח כלי סייבר בעלי יכולות לגרום נזק משמעותי. בהתחשב בכך שארגוני הטרור חסרים את היכולת לבצע איסוף מודיעין איכותי למבצעים (מל"ם), הסבירות לביצוע תקיפת סייבר משמעותית שלהם נראית נמוכה .

כדי שארגון טרור יוכל לפעול עצמאית ולהוציא לפועל פיגוע משמעותי במרחב הסייבר, יידרשו מגוון יכולות, בהן: יכולות איסוף מודיעין מדויק על היעד, רשתות המחשבים והמערכות שלו; רכישה או פיתוח של כלי סייבר מתאימים; מציאת קצה חוט לחדירה לארגון; הסוואת כלי התקיפה תוך כדי השתלטות על המערכת; ולבסוף – ביצוע המתקפה בזמן ובמקום אשר יפתיעו וישיגו תוצאה משמעותית. נראה שפעולה עצמאית של ארגון טרור, ללא גורם מדינתי התומך בו, אינה דבר מובן מאליו. אולם, אין לגזור מכך גזרה שווה באשר לארגונים הנתמכים ואף מופעלים על ידי מדינות בעלות יכולות משמעותיות.

קיימת אפשרות לתקיפות של ארגוני טרור תוך שימוש במיקור חוץ. אם נבחן את ארגוני הפשע, ניווכח כי ארגונים אלה עשו קפיצת דרך משמעותית בשנים האחרונות. מעבדת קספרסקי (Kaspersky) חשפה לאחרונה קבוצה חדשה של תוקפים, ככל הנראה בהזמנת ארגוני פשע או בהזמנה של מדינה על רקע ריגול תעשייתי. מדובר בקבוצה של האקרים בשם Icefog, המתמקדת בפגיעה בשרשרת האספקה של הארגון בצורה ממוקדת (בשיטת "תקוֹף ובְרח"), בעיקר במגזרי תעשיות צבאיות ברחבי העולם.[41] התפתחות נוספת חלה בתפוצת קודים זדוניים, תוך שימוש של מעבדות פשע ברשת השחורה (DarkNet), שהגבירה את הנגישות לקודים קיימים למטרות תקיפה. ארגוני פשע עושים כבר כיום שימוש בקודים קיימים לתקיפת מערכות פיננסיות על ידי שכפולם והפיכתם לקודי מוטציה.[42]

האפשרות שארגוני טרור יעשו שימוש ויקנו שירותי תקיפה מהאקרים שכירי חרב, וכן יעשו שימוש עתידי בקודי מוטציה, על בסיס וריאציה של קודים קיימים

לתקיפת מטרות, היא ריאלית בעתיד הקרוב, ואין להתעלם ממנה בבניית איום הייחוס במרחב הסייבר לתקיפות שער הארגון ואפילו מערכות המידע שלו. לכן, ישנה סבירות גבוהה לכך שבשנים הקרובות תחול התקדמות ביכולות התקיפה הקיברנטית של ארגוני טרור, שיתבססו על רכישת יכולות מתקדמות יותר על ידיהם ותרגומן לתקיפות על מערכות המידע של ארגונים (ולא רק על שער הארגון).

יכולת לבצע מתקפה שתכלול חדירה למערכות המבצעיות ותפגע בהן היא מורכבת למדי. הצורך ביכולות מודיעין ויכולות החדרה ברמה גבוהה, שקיימות רק אצל מספר מדינות מצומצם, גורם לכך שפעולה התקפית תהיה מדינתית, ולכן לא נראתה עד היום התקפה מוצלחת של שחקן לא מדינתי על מערכות הליבה המבצעיות של ארגון כלשהו. אף שתקיפה כזו טרם זוהתה, ניתן לראות עלֶיה במגמת השיפור ביכולות הטכנולוגיות של שכירי החרב הפועלים במרחב הסייבר לצרכי פשיעה והונאה. מתוך כך ניתן להניח, שתמורת תגמול מתאים יסכימו גורמים טכנולוגיים פליליים לייצר כלים שיוכלו לבצע תקיפות על מערכות הליבה המבצעיות של תשתיות קריטיות ושל חברות מסחריות. גורמים אלה יוכלו להעמיד את מרכולתם גם לטובת ארגוני טרור.

המלצות להתמודדות ברמה הלאומית

מגוון האיומים במרחב הסייבר הוא רחב. ההגנות הבסיסיות מפני איומים אלה לא צריכות להבדיל בצורה מהותית בין מקורותיו של האיום. לכן, המחשבה כי ניתן ליצור הגנה ייעודית במרחב הסייבר דווקא מול איומים של גורמי טרור, נראית לא מעשית. אדרבא, תפיסת המענה לאיומים לפגוע במרחב הסייבר על ידי ארגוני טרור אינה צריכה ואף אינה יכולה להיות שונה מהותית מתפיסת המענה הכוללת לאיומים במרחב זה.

תפיסת ההגנה היסודית בפני איומי הסייבר צריכה להתבסס על מספר מרכיבי יסוד: מודיעין; מענה הגנתי רב־שכבתי; מענה התקפי; הסברה; מענה אזרחי.

מודיעין

מרכיב היסוד הראשון בהתגוננות מפני איומי הסייבר הוא המודיעין, ובמסגרתו איסוף מודיעין שיתבסס על הכְוונה לאור הערכות מצב. בהקשר זה קיימת חשיבות לזיהוי האיומים ולהכוונת גורמי האיסוף מול מידע הנוגע לגורמי טרור המבקשים לפעול במרחב הסייבר. כפי שנכתב לעיל, במקרים רבים עומדות מדינות מאחורי הפעילות של ארגוני טרור, ולכן מודיעין הנאסף בהקשר המדינתי יוכל לספק מידע גם בהקשר של ארגוני טרור המסונפים או מופעלים על ידי אותה מדינה.

תחום המודיעין מהווה נדבך חיוני מאין כמוהו בהתמודדות עם איומים במרחב הסייבר. היכולת לאסוף ולנתח מידע רב מאפשרת כיום לייצר מודיעין איכותי

הן ברמה המדינתית והן, במקרים לא מעטים, ברמת ארגונים ועסקים המנטרים באופן קבוע את רשתות המידע והתקשורת. זאת, כדי לאתר התנהגויות אנומליות העשויות להעיד על תקיפה העתידה להתרחש, או ללמד על פעילות חריגה ברשת המחשבים. בהקשר זה ראוי להדגיש, כי העובדה שמדינה דוגמת איראן תומכת, ולעיתים אף מפעילה, ארגוני טרור, מחייבת את ארגוני המודיעין במערב לנטר לא רק את מדינת היעד אלא גם את הארגונים המסונפים לה. בהקשר של איראן המדובר בחזבאללה, בחמאס, וב"הצבא הסורי האלקטרוני".

מענה הגנתי הכולל מספר שכבות

המדובר בהגנה היקפית ובהגנה על נכסים חיוניים, הכוללת יכולות שימור פעולה גם אחרי חדירה של קוד מפַגע וסיכול מקדים של גורמים פעילים, למשל על ידי חשיפה של מידע מודיעיני לרשויות החוק במדינות בהן מתבצעת הפעילות וביצוע פעילות סיכול באמצעות כלים משפטיים במדינות אחרות. כך יתכן שיבוש של היכולת להפעיל את הקוד המפגע קודם שזה הופץ.

מענה התקפי לאיומים

מרכיב זה בהתמודדות עם איומי הסייבר כולל שני רבדים: הרובד הראשון נוגע ליכולת לפעול התקפית באמצעות מהלומה מקדימה, במרחב הסייבר ולעיתים גם מחוצה לו, כנגד משאבי הסייבר בארגון טרור (תשתיות, מימון, אתרים ופעילים). הרובד השני נוגע ליכולת לבצע פעולת תגמול אחרי התקיפה ואחרי זיהוי מסַפק של הגורמים לתקיפה. מהלומה זו לא חייבת להיות מתוחמת רק למרחב הסייבר ויכולה אף לכלול מרכיבים פיזיים של ממש. בחלק מהמקרים נדרשת הסדרה חוקית של הפעילות ההתקפית, כדי לאפשר אפקטיביות של המענה. במקרים לא מעטים ניתן לזהות את שרשרת הפעולה כאשר מדינות (דוגמת איראן) מפעילות ארגונים לא מדינתיים (דוגמת חזבאללה ו"הצבא הסורי האלקטרוני"), כשכולם יחד מפעילים גורמים בעלי עניין ואף גורמים משוּטים ברשת לצורך הגדלת יכולות התקיפה. הצורך להפעיל מערכת רחבה של תוקפים מחייבת הכְוונה במספר הקשרים: הראשון שבהם נוגע לקביעת המטרות אותן יש לתקוף; השני נוגע לעיתוי התקיפות; והשלישי נוגע לכלים לביצוע ההתקפות. כל אלה מחייבים הקמה של אתרים ופורומים ייעודיים אליהם מופנה המידע. פעילות זו יוצרת נקודת תורפה, מאחר וניתן לפעול לשיבוש ולשיטוי וכך לייצר בלבול, תוך הקהיה של עוקץ התקיפה שתוכנן על ידי מובילי התקיפה.

פעילות הסברה

ניתן להניח שפעילות הסברה לא תהייה אפקטיבית מול הגרעין הקשה של הפעילים בהתקפות הסייבר. לפעילות המניעה ההסברתית שתי מטרות: הראשונה

היא הגדלת המודעות לאפשרות שתוקפים עלולים להיפגע כתוצאה מפעילות סיכול במדינה בה הם שוהים (למשל, חשיפה שלהם לגורמי האכיפה במדינה); השנייה היא החשיפה של העומדים מאחורי ההתארגנות. כאמור, במקרים רבים התוקפים המשוטים לא יודעים כלל שהם מופעלים על ידי מדינות וארגוני טרור. לפיכך, באמצעות פעולות כאלו יתכן וניתן יהיה לצמצם במידה מסוימת את היקף התופעה.

ארגון המענה האזרחי במרחב הסייבר

נקודות התורפה של מערכת הסייבר האזרחית בישראל מהוות פְּרצה הקוראת לגנב עבור ארגוני הטרור. ההגנות החלשות יחסית על מערכות אלו מאפשרות לארגוני הטרור לפעול באופן שאינו מסובך מול מטרות במרחב זה. מאחר ומערכת הסייבר האזרחית מייצרת חולשות מובנות, יש להסדיר את המענה האזרחי במרחב הסייבר, ויפה שעה אחת קודם. יש לציין, בהקשר זה, המלצה של המכון למחקרי ביטחון לאומי לממשלת ישראל להסדיר את ההגנה של מרחב הסייבר האזרחי באופן שיוכל לספק מענה הולם לאיומים.[43]

ארגוני הטרור טרם חצו את הרף המבצעי והטכנולוגי המאפשר להם לפעול באופן עצמאי מול ישראל ומדינות אחרות במערב בתחום לוחמת הסייבר. אולם, התפתחות שוק התקיפה הפלילי עלולה ליצור יכולות תקיפה משמעותיות. התפתחות זאת, לצד המשענת וההכוונה המודיעינית והמבצעית של מעצמות טכנולוגיות דוגמת איראן, יכולה לגרום לפעילות מסוכנת בתחום הסייבר גם מצדם של ארגוני טרור. לכן, ראוי יהיה לא לזלזל באיום זה. אף שטרם נצפתה פעילות משמעותית של ארגוני טרור בתחום הסייבר, התפתחות האיום בתחום זה מחייבת התארגנות מתאימה.

הערות

1 מיכל אביעד, **קולנוע תיעודי**, תל אביב, חידקל, 2007, עמ' 5.

2 ראו למשל: חיים פס ודן מרידור (עורכים), **הקרב של המאה ה־21: דמוקרטיה נלחמת בטרור**, **פורום עיון**, המכון הישראלי לדמוקרטיה, ירושלים, תשס"ז–2006, עמ' 25.

3 ראו למשל TOR – תוכנה המסייעת ליצירת אנונימיות ברשת. כל שכבה מוצפנת וכל תחנה במסלול מקלפת את השכבה שלה ומעבירה לתחנה הבאה. עיקרון זה נקרא "ניתוב בצָל" (The Onion Router – TOR), https://www.torproject.org/

4 Oded Yaron, "Hackers Plan Cyber Attack against Israeli Targets in April", *Haaretz*, March 14, 2013 http://www.haaretz.com/news/diplomacy-defense/hackers-plan-cyber-attack-against-israeli-targets-in-april.premium-1.509214 .

5 "שטייניץ: האיום הצבאי על ישראל הפך גם לאיום טרור סייבר", **גלובס**, 9 ביולי 2013, http://www.globes.co.il/news/article.aspx?did=100086069

6 ראו התבטאות של ראש הממשלה בנימין נתניהו בנושא זה: "נתניהו: גידול משמעותי במתקפות הסייבר מאיראן וגרורותיה", **גלובס**, 9 ביוני 2013,

http://www.globes.co.il/news/article.aspx?did=1000851092

7 הכוונה היא לכל מערכת המאחסנת, משנעת או מעבדת מידע ארגוני, בין אם היא מקושרת לרשת האינטרנט ובין אם לא, ובין אם היא מהווה חלק מליבת העשייה העסקית של הארגון ובין אם לא.

8 מערכת ליבה מבצעית של הארגון היא החומרה שעל גביה והתוכנה אשר באמצעותה מנוהלים תהליכי הליבה של הארגון (בין אם הוא ארגון ביטחוני או ארגון עסקי אזרחי). זו מערכת ששיבוש או הריסה שלה יכולים להפסיק את פעילות הארגון או חלקים ממנו, עד כדי גרימה של נזק פיזי במקרים מסוימים.

9 מערכת בקרה תעשייתית (ICS) היא כלי המשלב רכיבי תוכנה וחומרה ונועד לפקח על תהליך פיזי של ייצור תהליכי. המערכת כוללת חיישנים לניטור התהליך המבוקר ופקדים לשליטה על תהליך זה. המערכת עשויה לכלול גם חיבור לרשתות מחשבים אחרות של הארגון ולעיתים אף לרשת האינטרנט.

10 סוג התקפות זה נעשה גם על ידי אקטיביסטים ואנרכיסטים בצורה עצמאית, או בשליחות והכוונה של ארגוני טרור.

11 "Shamoon Virus Targets Energy Sector Infrastructure", *BBC News Technology*, August 17, 2012, http://www.bbc.co.uk/news/technology-19293797

12 באירוע זה הוחדר קוד זדוני למערכת המחשוב של ערמקו, וכתוצאה מכך הושבתו כ־30,000 מחשבים.

13 ראלף לנגר, הרצאה בנושא אבטחת מערכות בקרה תעשייתיות, ועידת הסייבר השנתית, המכון למחקרי ביטחון לאומי, 4 בספטמבר 2012, http://youtube/sBsMA6Epw78

14 "The Disturbing World of the Deep Web, Where Contract Killers and Drug Dealers Play their Trade on the Internet", *Daily Mail*, October 11, 2013, http://www.dailymail.co.uk/news/article-2454735/The-disturbing-world-Deep-Web-contract-killers-drug-dealers-ply-trade-internet.html .

15 Jesse Emspak, "Why We Won't Soon See another Stuxnet Attack", *Tech News Daily*, July 24, 2011, http://www.technewsdaily.com/7012-stuxnet-anniversary-look-ahead.html

16 Aditya K. Sood, Richard J. Enbody, "Crimeware-as-a-Service – A Survey of Commoditized Crimeware in the Underground Market", *International Journal of Critical Infrastructure Protection*, Volume 6, Issue 1, March 2013, http://www.sciencedirect.com/science/article/pii/S1874548213000036

17 עמוד ב"פייסבוק", בו מוצעים למכירה נשקי סייבר: https://www.facebook.com/groups/53807916899/

18 Limor Kessem, "Zeus FaaS Comes to a Social Network Near You", RSA, Speaking of Security, April 2013, http://blogs.rsa.com/zeus-faas-comes-to-a-social-network-near-you/

19 Michael Fire, Rami Puzis, Yuval Elovici, "Organization Mining Using Online Social Networks", http://arxiv.org/pdf/1303.3741v2.pdf

20 Aviad Elishar, Michael Fire, Dima Kagan, Yuval Elovici, "Homing Socialbots: Intrusion on a Specific Organization's Employee Using Socialbots", International Workshop on Social Network Analysis in Applications (SNAA), August 2013.

21 Fernando M. Pinguelo, Bradford W. Muller, Norris Mclaughlin, P.A. Marcus, "Is Social Media a Corporate Spy's Best Friend? How Social Media Use may Expose your Company to Cyber-Vulnerability", Bloomberg Law, http://about.bloomberglaw.com/practitioner-contributions/is-social-media-a-corporate-spys-best-friend/

22 Internet Census 2012, Carna Botnet, http://internetcensus2012.bitbucket.org/paper.html

23 מפת מערכות סקאדה בעולם: http://goo.gl/maps/nqnan

24 האתר Shodan, המכיל מידע שימושי להאקרים: http://www.shodanhq.com/

25 גילי כהן, "האקרים תקפו רשתות ביתיות של מאות ישראלים", **הארץ**, 11 בספטמבר 2013, http://www.haaretz.co.il/misc/2.444/.premium-1.2117098

26 וקטור תקיפה: http://searchsecurity.techtarget.com/definition/attack-vector

27 מתקפת זיוף: http://www.webopedia.com/TERM/S/spoof.html

28 Eric M. Hutchins, Michael J. Cloppert, Rohan M. Amin, "Intelligence-driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains", Leading Issues in Information Warfare & Security Research, 1 (2011), p. 80.

29 Doug Macdonald, "A Guide to SpyEye C&C Messages", Fortinet, February 15, 2011, http://blog.fortinet.com/a-guide-to-spyeye-cc-messages

30 Thomas Rid, "Cyber-Sabotage Is Easy", Foreign Policy, July 23, 2013. http://www.foreignpolicy.com/articles/2013/07/23/cyber_sabotage_is_easy_i_know_i_did_it?pa

31 Dorothy E. Denning, Cyberterrorism, Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Service, U.S House of Representatives, May 23, 2000, p. 269 http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

32 לכרונולוגיה של פעולות של Aum Shinrikyo ראו: http://cns.miis.edu/reports/pdfs/aum_chrn.pdf

33 Paul Everard, "NATO and Cyber Terrorism", in: Center of Excellence Against Terrorism, *Response to Cyber Terrorism*, Ankara, Turkey, 2008, pp.118-126, http://www.nato.int/docu/review/2013/Cyber/timeline/EN/

34 דניאל כהן ואביב רוטברט, "תפוצת נשק קיברנטי במרחב הסייבר", **צבא ואסטרטגיה**, כרך 5, גיליון 1, מאי 2013.

35 Dylan Love, "10 Reasons To Worry About The Syrian Electronic Army", Business Insider, May 22, 2013, http://www.businessinsider.com/syrian-electronic-army-2013-5?op=1#ixzz2h728aL8P

36 Peter Foster, "'Bogus' AP tweet about explosion at the White House wipes billions off US markets", The Telegraph, April 23, 2013, http://www.telegraph.co.uk/finance/markets/10013768/Bogus-AP-tweet-about-explosion-at-the-White-House-wipes-billions-off-US-markets.html

37 יניר מגנה ועודד ירון, "מומחה ישראלי אמר ש'הצבא הסורי האלקטרוני' תקף בישראל – והכחיש", **הארץ**, 25 במאי 2013, http://www.haaretz.co.il/news/politics/1.2029071

38 אמיר בוחבוט, "מתקפת סייבר: הופלו אתרי משרד ראש הממשלה, הביטחון והחינוך", **וואלה חדשות**, 7 באפריל 2013, http://news.walla.co.il/?w=/90/2630896

39 נמרוד צוק, "פיגוע סייבר: לוחמי עז א דין אל קסאם הולמים באמריקן אקספרס", **כלכליסט**, 2 באפריל 2013, http://www.calcalist.co.il/internet/articles/0,7340,L-3599061,00.html

40 לי ירון, "מחלקת ביטחון מתריעה: יכולות הסייבר של חמאס התעצמו", **במחנה**, 14 בנובמבר 2013, עמ' 19.

41 "Kaspersky Lab Exposes 'Icefog': a new Cyber-espionage Campaign Focusing on

Supply Chain Attacks, September 26, 2013
http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_exposes_Icefog_a_new_cyber-espionage_campaign_focusing_on_supply_chain_attacks

42 להרחבה בנושא קוד מוטציה ראו: כהן ורוטברט, "תפוצת נשק קיברנטי במרחב הסייבר", **צבא ואסטרטגיה**, כרך 5, גיליון 1, מאי 2013.

43 גבי סיבוני, "מענה לאומי להגנה אזרחית בסייבר", מסמך עמדה למקבלי החלטות, המכון למחקרי ביטחון לאומי, אפריל 2013, http://heb.inss.org.il/index.aspx?id=4354&articleid=5904

מודיעין 2.0 – גישה חדשה לעשיית מודיעין[1]

דודי סימן טוב ועופר ג'

המודיעין חווה בשנים האחרונות תמורות עמוקות, הן ביחסים בתוך המערכת המודיעינית עצמה והן ביחסים בינו ובין הסביבה המדינית והצבאית שאותה הוא משרת. שינויים אלה מתבטאים גם בפרקטיקה שבה עושים כיום מודיעין, וכן בתפיסות חדשות המופיעות בשיח המודיעיני ודוחקות את מקומן של תפיסות מסורתיות שעבר זמנן. השינויים במודיעין הם תוצאה מתבקשת של השינויים העמוקים המתחוללים במציאות האנושית ובאופי המלחמות במאה ה־21. במוקדם עומד השינוי העמוק באופי היריבים ובאופי המלחמות והשינוי העמוק הגלום במעבר מהעידן התעשייתי לעידן המידע הדיגיטלי. מאמר זה בוחן את התמורות שחלו בעשייה המודיעינית ומציג מספר בעיות אתן מתמודדת כיום קהילת המודיעין. הטענה המרכזית של המאמר היא כי ניתן לשפר באופן משמעותי את יכולות המודיעין ולהעבירו אל המאה ה־21, אם נאמץ גישה חדשה לעשיית מודיעין, השואבת מקור השראה ראשי מתופעת ה־WEB 2.0.

מילות מפתח: מודיעין, וב 2.0, מעגל המודיעין, יחסי איסוף־מחקר, ויקיפדיה, בלוגים, איסוף־מחקר

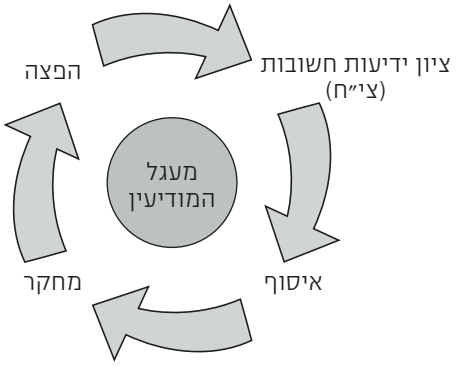
"מעגל המודיעין" כרעיון מסדר

"מעגל המודיעין" היווה רעיון מסדר מרכזי, לאורו הוקמו ופעלו הממסדים המודיעיניים לאחר מלחמת העולם השנייה. קדמה לו, במקרה הישראלי, פעולתם של יחידים, ללא ארגון וללא שיטה או היררכיה וללא אבחנה בין "איסוף" ובין

סא"ל עופר ג' הינו ראש ענף בחטיבת המחקר באגף המודיעין בצה"ל.
דודי סימנטוב הוא חוקר לשעבר במכון לחקר המודיעין של אגף המודיעין בצה"ל.

"מחקר". חיים הרצוג, שהיה ראש מחלקת המודיעין באג"ם וראש אמ"ן השלישי, הגדיר זאת כך: "בתקופה הראשונה היו התחלות פרימיטיביות... אימפריות קטנות עם גנרלים קטנים שקיימו קשר ישיר עם בן־גוריון – כל אחד רץ עם המודיעין שלו אליו... היו אנשים טובים, [אך] חסרה להם תשתית צבאית, קונספציה, גישה אנליטית, מחקר ושיטות עבודה – איסוף, מיון, ניתוח והפצה בצורה מדעית. זאת אומרת, הפיכת ידיעות למודיעין, שהוא מדע בעיני [בפני] עצמו. אנחנו הבאנו מהצבא [הבריטי] שיטות עבודה ובנינו את המודיעין הצבאי".[2]

התפיסה של "מעגל המודיעין" הגדירה מספר שלבים ברורים ומובחנים זה מזה, המרכיבים יחדיו את התהליך המודיעיני: איסוף ידיעות, עיבוד ידיעות (כלומר, מחקר) והפצת המודיעין המוגמר לצרכנים השונים. התהליך התבצע לאור הצי"ח (ציון ידיעות חיוניות), שאמור היה להינתן על ידי המפקד/הקברניט. מדובר בתהליך מעגלי החוזר על עצמו:[3]



מימוש רעיון "מעגל המודיעין" התבצע במסגרת הקמתו של הממסד המודיעיני הצבאי הישראלי – אגף המודיעין בצה"ל (אמ"ן). אז הופרד המפעל המודיעיני לשניים: גופי האיסוף וגופי המחקר. בין גופים אלה תיווך בהצלחה מרובה ענף איסוף (לימים מחלקת איסוף), שעלה בידיו לכוון ביד רמה את העבודה האיסופית. זו נעשתה לאור הצי"ח, שנוסח בקפידה וכלל מספר שאלות מצומצם. לגורמי המחקר לא נותר אלא לקבל "מן המוכן" את המידע שהגיע אליהם, כמעט ללא מעורבות בעבודת הכוונת האיסוף.

ההיגיון של "מעגל המודיעין" היה ארגון העשייה המודיעינית לפי כללים ברורים. המידור, שהיה עיקרון מוביל בו, נבע לא רק מטעמים ביטחוניים, אלא גם מטעמים תפיסתיים. הוא נועד להבטיח ש"כל אחד יעשה את העבודה שלו" ולא "יפריע" לעבודה של יתר מרכיבי המערכת או יוטה על ידם. לשם כך בדיוק נועד תפקידו של ענף איסוף, כגורם מתווך בין שני הצדדים.

עוד עיקרון שנבע מההיגיון המסדר של "מעגל המודיעין" היה זרימה חד־כיוונית של המידע: המחקר שולח לאיסוף את שאלות הצי"ח; האיסוף שולח חזרה למחקר את התשובות. לא היה מקום רב למעורבות של אחד מהצדדים בעולמו של השני. עיקרון מרכזי נוסף שעמד בבסיסו של "מעגל המודיעין" היה רעיון "שרשרת הערך". לפי עיקרון זה, ככל שנתקדם בתהליך, הערך של המוצר המודיעיני יהיה רב יותר: ממידע גולמי לידיעה מודיעינית מזוקקת, וממנה להערכת מודיעין המגולמת במסמך מחקרי.

לא היו ב"מעגל המודיעין" ולא נדרשו בו אזורים של שיח ומרחב משותפים לפיתוח ידע, משום שלכל אחד מהרכיבים במערכת היה תפקיד שונה ומובחן ממשנהו ומשום שהתפיסה הניחה כי כל רכיב יכול וצריך לבצע את עבודתו באופן עצמאי. הבידול בין רכיבי המערכת המודיעינית התחזק עוד יותר משנות השבעים של המאה העשרים, בעקבות הכישלון המודיעיני במלחמת יום הכיפורים ודוח ועדת אגרנט. האחרון הוביל, בין היתר, להנחלת רעיון הפלורליזם המודיעיני כעיקרון מכונן, שנועד "לוודא תפקוד יעיל של כל גורמי קהילת המודיעין לספק התרעה". ועדת אגרנט גם קבעה (בדוח המלא שלה) כי "יש לבצע שינויים נרחבים במבנה אמ"ן, שיתנו ביטוי לדעות שונות ונוגדות בקרב עובדי מחלקת מחקר".[4]

סדקים ב"מעגל המודיעין"

כבר בשנות השישים של המאה הקודמת החלו להופיע בקהילת המודיעין הישראלית זרמים שאתגרו את תקפותו של "מעגל המודיעין" כרעיון מסדר בלעדי של המפעל המודיעיני. כך, למשל, נוצר החל משנות השישים קשר ישיר בין גורמי ההאזנה לגורמים מבצעיים כמו חיל האוויר וחיל הים, שביטא הבנה כי לפחות מול איומים מסוימים נדרש ליצור "מעגלים קצרים" בין גורמי האיסוף לגורמי המחקר. דוגמה נוספת לקשר ישיר בין גורמים שונים בקהילת המודיעין היא מעורבות המחקר בסוגיות של פיתוח ותחקור מקורות יומינט (אנושיים). ואולם, היו אלה יוצאים מהכלל, ומרבית המפעל המודיעיני התנהלה בהתאם ל"חלוקת העבודה" שהוצגה קודם לכן.

בשנים האחרונות מוסכם על רבים בקרב אנשי המודיעין כי "מעגל המודיעין" אינו תקף יותר כרעיון מסדר בלעדי. יתר על כן, בשיח המודיעיני בארצות הברית אף מופיעים קולות הקוראים "להרוג את "מעגל המודיעין".[5] קולות אלה הופכים לרווחים יותר ויותר.

ניתן לפרוס קשת רחבה של גורמים וסיבות שהביאו לכך, אולם אם נמקד אותם לכדי גורמי היסוד המשפיעים ביותר, אפשר להצביע על שתי מהפכות בקנה מידה היסטורי שראשיתן בשלהי המאה העשרים: הראשונה היא המעבר מהעידן התעשייתי לעידן המידע הדיגיטלי, שבא לידי ביטוי בהופעת המרחב

הקיברנטי, ובתוך כך המצאת המחשב והאינטרנט ששינו את פני האנושות; השנייה היא המהפכה במישור הצבאי, אשר העבירה את המוקד מעימותים בין מדינות וצבאות להתמודדות עם מגוון הולך ומתרחב של עימותים בלתי קונבנציונליים, לא מדינתיים ובעלי אופי דינמי, היברידי ורשתי.

בכדי להתמודד עם האתגרים המשתנים בלחימה, הוקמו כבר בשנות השבעים צוותים משותפים לגופי המודיעין ולגורמים מבצעיים (כמו הצמ"אות בחיל האוויר – "צוותי מודיעין אופרטיביים"), אולם אלה היו בבחינת חריג במשך זמן רב. כיום, נוכח שכיחות העימותים עם יריבים אסימטריים הנוקטים דפוסי "היעלמות" והיטמעות באוכלוסיה, ש"חלון ההזדמנויות" לפעול מולם יכול להצטמצם לכדי דקות בלבד, ומול הצורך הגובר לצמצם פגיעה בבלתי מעורבים, הרעיון של חמ"ל המאגד בתוכו את כל הרכיבים הרלוונטיים של המערכת המודיעינית והמבצעית הפך לנחלת הכלל, וזאת כדי לאפשר לסגור מעגל מודיעיני ומבצעי בזמן אמת. צורת התארגנות זו מוכיחה שניתן לשבור חסמים ארגוניים, נוכח אתגרים מבצעיים דוחקים.

על בסיס אותו היגיון, אך למול אתגרים מודיעיניים בעל אופי תשתיתי וארוך טווח, התפתחה צורת התארגנות מודיעינית חדשה. במסגרתה מוקמים צוותי מודיעין משימתיים, המשלבים את כלל התפקידים והיכולות (מחקר ואיסוף לגווניו), במטרה להתמודד עם סוגיה מודיעינית "מקצה לקצה". כמו תאי התקיפה המשולבים, גם צורת התארגנות זו שוברת גבולות ארגוניים, אולם כיוון שמדובר בגופים הפועלים לאורך זמן ממושך ולא למול משימה מבצעית מיידית, האיום שהם מציבים על התרבות הארגונית הקלאסית, המקדשת את הבידול ואת המידור בין הגופים השונים, הינו עמוק יותר.

התפתחות נוספת שמאתגרת את תקפותו של "מעגל המודיעין" הייתה היווצרותו של יומן רשתי משותף לכל הגורמים, אשר בשעת לחימה מאפשר לכל השותפים לעדכן ולהתעדכן בזמן אמת. התועלת של יומן כזה ברורה: כלל הגורמים האיסופיים יודעים בדיוק רב ובאופן בלתי אמצעי (ללא מתווכים) מה הציו"ח ונותנים לו מענה מיידי, הם מבינים בזמן אמיתי את הבעיות שמטרידות את הגורם המחקרי או המבצעי, ותורמים לו ככל יכולתם. במקביל, איש המחקר זוכה לקבל את המידע הדרוש לו בזמן רלוונטי, תוך היחשפות חסרת תקדים למפעל האיסופי, ללא חסמים ומגבלות המאפיינים את עקרון "מעגל המודיעין". האיתגור לתפיסה של "מעגל המודיעין" אינו רק בהיבט של ביטול המידור, אלא גם בהיבט של שבירת עקרון "שרשרת הערך". היומן הרשתי מגלם הבנה, כי לפחות במצבים בהם הזמן דוחק, יש ערך מודיעיני רב יותר למידע איסופי שלא עבר את כל תהליך העיבוד והבקרה הסדור, אך מגיע בזמן אמת, על פני הידיעות המודיעיניות ה"קאנוניות", שקיבלו את "תו התקן" הרשמי של יחידת האיסוף כראויות להפצה.

הבאנו כאן דוגמאות לכלים ולצורות התארגנות שכבר קיימים בקהילת המודיעין הישראלית וזוכים להכרה כחלק אינטגרלי ומחויב המציאות של המפעל המודיעיני. אולם כלים וצורות התארגנות אלה עדיין לא מצויים בשימוש מספק, ועדיין קיימים חילוקי דעות באשר ליכולת להפוך אותם מ"אִיים" של מרחבים משותפים לנתח דומיננטי בתוך העשייה הכוללת.

כאמור, גורם יסוד האחראי לאיתגור של פרדיגמת "מעגל המודיעין" הוא עידן המידע. באופן קונקרטי יותר, ניתן לדבר על הופעת המרחב הקיברנטי. מרחב זה האיץ את השינוי המדובר בשני מובנים: הראשון מתמקד בהצפת המידע, בגיוונו ובהפיכתו לנגיש הן לגורמי המחקר והן לגורמי האיסוף; השני הוא הופעת דרכים וגישות חדשות לאופן שבו מתפתח ונשמר הידע. העברתו של מרכז הכובד בעולם המידע והידע של היום מהממסדים אל ההמון (ש"ויקיפדיה" מהווה ייצוג יפה שלו) והופעה של בלוגים ורשתות חברתיות, שכפי שנראה בהמשך הם חלק ממהפכת הווב 2.0, מהוות גורם מערער מרכזי על שיטת עשיית המודיעין המסורתית. הן מעלות את המתח בין האופן שבו מתפתח, זורם ונשמר המידע האזרחי ובין האופי המיושן שמציג "מעגל המודיעין". גישה חדשה זו לשיתוף במידע ולפיתוח הידע מחלחלת אל תוך קהילת המודיעין, במידה רבה בתיווכו של הדור הצעיר, המביא אל עולם המודיעין את תרבות שיתוף המידע ופיתוח הידע, אליה הוא נחשף בשעות הפנאי.

גם אופי המידע האיסופי בעידן הקיברנטי משתנה: הוא מתבסס יותר ויותר על מידע כתוב ועל מסדֵי נתונים ופחות על שיחות טלפון בשפות השגורות רק בקרב גורמי האיסוף. נוכח מורכבות והיקפי המידע הקיימים בעולם זה, האיסוף כבר אינו יכול להתמודד לבדו עם חומרי הגלם העומדים לרשותו, ונדרש קשר הרבה יותר עמוק ועשיר בין המחקר ובין האיסוף – בעיקר למידה ועשייה משותפות – כדי להתמודד עם האתגר ההולך וגדל. זאת ועוד, תחומים טכנולוגיים או כלכליים העולים בחומר המודיעיני מבליטים את יתרונו של החוקר המתמחה בהם ומחייבים את סיועו במיצויים. לנוכח ההיקפים העצומים של המידע, האיסוף "ילך לאיבוד" אם לא ייעזר במחקר כדי לבור את המוץ מהתבן.

כך הולך ומיטשטש הגבול החד בין האיסוף למחקר, ואט אט הופכים כל הרכיבים של המערכת המודיעינית לשותפים לאותה משימה. עם זאת, חשוב להדגיש הדגשה יתרה כי הגבולות בין מרכיבי המערכת המודיעינית אינם מוּסָרים לחלוטין; כל צד נדרש להמשיך לשמור על ייחודו המקצועי, כדי שיוכל להביא את הערך המוסף שלו לעשייה הכוללת. אולם על כל צד גם להקדיש זמן רב יותר להכרת "האחר" – שותפו למערכת המודיעינית: על המחקר להכיר טוב יותר את ההתלבטויות של האיסוף ואת יכולותיו, ועל האיסוף להכיר טוב יותר את התלבטויות החוקר ואת צרכיו.

עם הופעת המרחב הקיברנטי שולבו עד מהרה כלים חדשים ושיטות חדשות בעשיית המודיעין, אולם דומה ש"מעגל המודיעין" לא נשבר עדיין וממשיך להוות רעיון מסדר ראשי. כך, למשל, ידיעות וסקירות החלו לעבור במערכות ממוכנות כדואר אלקטרוני ("מיילים"), במקום הפצה בעותקים קשיחים שהייתה נהוגה קודם לכן. שיטה זו מאפשרת לקצר את זמני ההפצה, להרחיב את תפוצת המידע ולשפר את יכולת שמירתו ואחזורו בהמשך. אולם גם במצב זה, הרעיון של העברת המידע מצד אחד לשני באופן חד־כיווני נותר בעינו, ולא נוצר באופן טבעי מרחב משותף לשימור ולפיתוח ידע מודיעיני.

קושי מרכזי נוסף הוא יכולת החיבור בין מערכות המידע של ארגונים שונים. מצב זה נובע מכך שמערכות אלו נבנו כ"מעגל סגור", כמעט ללא כל צורך ליצור שילוביות וקישוריות ביניהן. התוצאה העגומה היא, שבעוד שהקישוריות בתוך יחידות ומערכים השתפרה, הקשר ביניהם עודנו מזערי או שאינו קיים כלל. ניסיון שנעשה להקים באמ"ן, לפני למעלה מעשור, "רשת מודיעינית" לא הוכתר בהצלחה רבה, והרשת נותרה משנית בלבד, אינה מהווה מרחב עבודה עיקרי ולא מתפתח בה ידע מודיעיני.

החל מראשית שנות האלפיים נעשה ניסיון ליישם באגף המודיעין בצה"ל כלים ושיטות של ניהול ופיתוח ידע, שכיום ניתן להגדירם, בדיעבד, כ־וב 1.0. המדובר בפורטלים ארגוניים ונושאיים, בפורומים שונים ובחדרי עבודה. יעדם של כלים ודפוסים חדשים אלה היה לנהל את הידע המודיעיני וליצור קהילות ידע מודיעיניות. ניסיונות אלה כשלו כמעט כולם: הפורטלים הרבים שנפתחו כפטריות אחר הגשם נסגרו אט־אט והפכו למצבות וירטואליות; הפורומים המודיעיניים וחדרי העבודה נותרו שוממים וקפואים, לא התפתח בהם ידע חדש ועד מהרה גם לא נשמר בהם מידע עדכני. הניסיון של אמ"ן לסגל לעצמו כלים חדשים לשימור וניהול הידע הארגוני כשל. הפער בין החזון המרשים של הפרויקט בשנותיו הראשונות – "יצירת קהילות מודיעיניות המייצרות מידע וידע" – לבין המציאות העגומה הינו גדול ונוקב.

דומה שבין הסיבות לכישלון זה נמצאת העובדה כי למהלך הטכנולוגי לא קדם שינוי תפיסתי: כאשר יחידה ומערך אינם חשים צורך לפעול באופן רשתי, על בסיס יום יומי, עם יחידות אחרות, קשה לצפות להתפתחות קהילות ידע שבמהותן הן חיבור בין גופים שונים. בנוסף לכך, לא נעשה ניסיון לתרגם ולפרש את הכלים החיצוניים לסביבה המודיעינית הייחודית והשונה כל כך.

הקושי והכישלון בשילוב מערכות מידע ויישומים אזרחיים מעולם ה־וב 1.0 בארגונים אינו נחלת קהילת המודיעין הישראלית בלבד. במאמר שמנתח את כישלון הפורטלים בארגונים, נטען כי בין הסיבות לכך ניתן למנות את ההתעלמות מהרשת החברתית בארגון ויצירת פלטפורמה לתקשורת חד־כיוונית, המחמיצה את

האפשרות שה"צרכנים", כלומר העובדים בארגון, יתרמו לפורטל תכנים משלהם; וכן את העובדה שרבים מהפורטלים הכושלים נבנו בצורה אחידה ולא אִפשרו למשתמשים ליצור לעצמם "דף בית" לפי רצונות וצרכים אישיים.[6]

ווב 2.0 – חידושים תרבותיים ותפיסתיים

ווב 2.0 (web 2.0) הוא תופעה טכנולוגית וחברתית־תרבותית המתייחסת לדור השני של מוצרים ושירותים באינטרנט. בעוד שהדור הראשון (ווב 1.0) התמקד באתרי אינטרנט שהתוכן בהם נוצר על ידי "מנהלי אתרים", וזרימת המידע בו הייתה חד־כיוונית (מהיצרן לצרכן), הדור השני מתייחס לאתרים כאל תשתית ליצירה משותפת של תכנים, הנשענים על שיתוף במידע ועל יצירה של הגולשים. המהפכה של תופעה זו הינה תרבותית יותר מאשר טכנולוגית, והגולש הפשוט הופך באחת מצרכן פסיבי של מידע לשותף ביצירתו. זאת ועוד, השליטה באתרים עברה מגופי תקשורת וממסדים לאזרחים עצמם, ונוצרה מעין "דמוקרטיה" בתחום המידע. אך טבעי היה שהשבועון *TIME* בחר בשנת 2006 בגולש האינטרנט לאיש השנה.[7]

ניתן להגדיר את ווב 2.0 כתשתית טכנולוגית לשיתוף ויצירה של תכנים על ידי הגולשים עצמם ובינם לבין עצמם באמצעות הרשת החברתית. ווב 2.0 מבטא את רעיון ה"יָצרכנים" (Prosumer, יצרן + צרכן), מושג שטבעו אלווין והיידי טופלר.[8] הוא מציג את עלייתו של גורם כלכלי חדש – צרכן המעורב בייצור השירות והמוצר שהוא צורך. ה־ווב 2.0 גם מבטא את הרעיון של "חוכמת ההמונים", באמצעות טכנולוגיה ותפיסה שיתופית, המובילים לכך שהתרומה של פרטים קטנים מסתכמת בסופו של דבר בפיתוח ידע בהיקפים ובאיכות שלא היו נוצרים בדרך אחרת. ביטוי מובהק לכך הוא מיזם ה"ויקיפדיה", שאינה "אנציקלופדיה מקוונת" גרידא, אלא מתבססת על הגולשים כיוצרי התכנים.

מושג נוסף הרלוונטי למהפכת ה־ווב 2.0 ומבטא את השינויים החברתיים העומדים מאחוריו הוא "דור ה־Y". הכוונה במושג זה היא לדור האחרון שנולד לתוך מהפכת האינטרנט וחווה את השינויים המהירים שהיא טומנת בחובה. מאפייניו של דור זה הם היותו בעל יכולת להסתגל לשינויים טכנולוגיים מהירים ויכולת לעבוד בקבוצה, לפזר קשב ולעשות שימוש נרחב ברשתות חברתיות כאמצעי ראשי ליצירת קשרים ולהעברת תכנים. בשונה מהדור הקודם, אשר מסתפק בדואר אלקטרוני להעברת מסרים כחלופה לדואר הרגיל, מבכר דור ה־Y את ה"פייסבוק" כתשתית להעברת מסרים בדרכים שונות.

ווב 2.0 מאופיין גם בחוויית משתמש עשירה ומגוונת – מחשבים ניידים, סמארטפונים, טאבלטים ועוד. זאת, לצד דרכים חדשות ומתחדשות להעברת מסרים – החל בבלוגים, המשך ב"טוויטר", שמאפשר צורה אחרת של קשר

המבוססת על "עוקבים", ועוד. לכל אלה מתווספת חוויה של גילוי מקרי ואקראי (Serendipity), אשר הרשת מאפשרת ומזמנת. לא אחת מקבל הגולש הצעה להכיר מישהו שעשוי לעניין אותו, מבלי שביקש להכירו, או הפְניה למאמר שעשוי להיות בעל ערך עבורו מבלי שחיפש אותו. הדבר שונה תכלית השינוי מגישת השאלה־תשובה שמגלם "מעגל המודיעין".

מודיעין 2.0

עיקרי התפיסה

כיצד יכולים מימוש ופירוש רלוונטיים של ווב 2.0 לתת מענה לבעיות שבהן לוקה המודיעין בעת הזו? יש להקדים ולומר כי אין מדובר בתרופת קסם וכי תפיסה זו אינה עומדת בפני עצמה; אולם אנו מציעים לבחון את החלתה על עולם המודיעין, תוך מתן פרשנות ראויה שתתאים אותה לטבעו השונה והמיוחד.

ההתאמה הראשונה שיש לעשות הינה ליישם את תפיסת ה־ווב 2.0 באופן שונה בשתי סביבות הפעולה השונות של המודיעין – הסביבה המודיעינית הפנימית והסביבה החיצונית שהמודיעין הוא שותף מרכזי בה. הסביבה המודיעינית כוללת שורה של קהילות ידע שונות. חלקן עוסקות ביריב מסוים (לדוגמה, חזבאללה או איראן), חלקן בגזרה מסוימת (לדוגמה, לבנון על גורמי הכוח השונים בה) וחלקן באיומי אמל"ח ובאיומים טכנולוגיים. בסביבה המודיעינית שותפים יחדיו גורמי המחקר והאיסוף באמ"ן ובקהילת המודיעין (כולל המוסד והשב"כ). לעומתה, הסביבה החיצונית כוללת שורה מגוונת וארוכה של גופי תכנון וביצוע בצה"ל, במערכת הביטחון ובמערכת המדינית (לדוגמה, המטה לביטחון לאומי ומשרדי ממשלה), ואפשר לכלול בה גם מכוני מחקר אזרחיים. בסביבה הפנימית, המודיעין עוסק בעיקר בהשגת מידע ובפיתוח ידע על "האחר", מתוך הבנת צרכיה של הסביבה החיצונית. בסביבה החיצונית, המודיעין מסייע לתהליכי העיצוב, התכנון והמימוש, באמצעות הבאת המידע שהשיג והידע שפיתח.

הרעיון המסדר העומד בלב תפיסת מודיעין 2.0 הוא המרחב המודיעיני הרשתי המשותף. כלומר, במקום חלוקה עבודה היררכית ומבודלת, אנו מציעים יצירת מרחב מודיעיני רשתי משותף וקהילות ידע מודיעיניות דינמיות ומתפתחות. מדובר במרחב משותף בכמה מישורים: מרחב משותף לגורמי המחקר ולגורמי האיסוף, העמלים יחד על פיתוח הידע על היריב; מרחב משותף בין יחידות המחקר השונות, שיפתחו את ההבנות שלהן על גבי תשתית אחת; ומרחב משותף לקהילת המודיעין ולקהילות שעושות שימוש במודיעין ("צרכנים" של המודיעין, קהילת ידע טכנולוגית המשרתת את המודיעין ועוד). האבחנה החדה בין יצרן לצרכן מיטשטשת במרחב המשותף החדש. כל הצדדים – המחקרי והאיסופי, המודיעיני וזה של המשתמש במודיעין – שותפים בקהילות ידע חדשות, שתכליתן אחת:

פיתוח ידע יישומי לטובת המעשה המדיני והצבאי. כל זאת, בלי שינסו להחליף אלה את אלה ותוך שהם שומרים על מקצועיות והתמחות דיסציפלינרית.

נדגיש כי הצגת מרחב רשתי משותף כיסוד חדש לעשיית מודיעין אינה סותרת היווצרות מרחבים פיזיים משותפים ליחידות המודיעין, בין שהם מוקמים אד־הוק לטובת מבצע (חפ"ק משותף, הכולל גורמי מחקר, איסוף ומבצעים) ובין שמדובר בהקמת חדר הפקה ומחקר משותף לגורמי המחקר והאיסוף, למילוי משימה ייעודית או אף לאורך זמן. במאמר זה איננו מתייחסים לאפשרות של מרחב פיזי משותף, שראוי לקדמה במקביל כמגמה משמעותית נוספת המשפיעה על המעשה המודיעיני.

הקריאה ליצירתו של מרחב מודיעיני משותף הולכת וקונה לה אחיזה בשיח העדכני. אולם נדמה, כי מהשיח הקיים חמקה העובדה שהמרחבים המשותפים, מעצם טבעם המטשטש את הגבולות בין השותפים השונים, ובעיקר בין הגופים המחקריים השונים לבין עצמם, מערערים על עקרון הפלורליזם. לדעתנו, העמדת עקרון הפלורליזם במבחן הזמן תוכיח כי הוא לא העלה תרומה של ממש לעשייה המודיעינית או למניעתן של טעויות והפתעות, וכי אדרבא, הוא תרם דווקא למגמה של בדלנות ותחרות לא בריאה בקהילת המודיעין הישראלית.[9] יתרה מכך, נוכח העומס והמורכבות של האתגרים הניצבים בפני המודיעין כיום, כמו גם מצוקת המשאבים הדוחקת, ומעל לכל – לנוכח המאפיינים המורכבים, ההיברידיים והרשתיים של רבים מהאיומים (שהג'האד העולמי מהווה דוגמה טובה להמחשתם), יש לדעתנו לדחוק הצידה את עקרון הפלורליזם ולהעדיף על פניו איחוד של המאמצים המודיעיניים.

גישת המודיעין הרשתי לא בהכרח תבטל את עקרון הפלורליזם, והיא אף עשויה להעניק לו פרשנות חדשה ויישום נכון ועמוק יותר. את המלצות ועדת אגרנט בדבר הצורך לאפשר ריבוי דעות ושקיפות במידע ניתן ליישם באמצעות מרחבים רשתיים משותפים. במרחבים אלה ישוקף כלל המידע המודיעיני ותינתן אפשרות טובה יותר לבטא ולהציג חילוקי דעות בקרב אנשי המודיעין בתוך אותו ארגון, או בקרב אנשי מודיעין מארגונים שונים, המייצגים נקודות מבט שונות. בכך תגביר הגישה המוצעת של מרחב ידע משותף את השיח המודיעיני ותאפשר ביתר קלות לתת במה לוויכוחים המודיעיניים ולעימותים בין תזות, עמדות ופרשנויות שונות, תוך חיסכון בעבודה הכפולה שמתבצעת כיום בין גורמי מחקר עמיתים.

רעיון מרכזי נוסף העומד בבסיס המרחב החדש הוא רעיון **השיח**, כלומר נכונות השותפים בקהילות הידע להשתתף ולשתף בתובנות שלהם. רעיון השיח מהווה, במידה רבה, חלופה למנגנון הצי"ח, שכבר שנים אינו ממלא את תפקידו. פלטפורמות השיח שמייצר ה־וב 2.0 עשויות לאפשר לאנשי המחקר והאיסוף לקיים דיונים אינטימיים סביב מושא עבודתם בזמן אמת או באופן מתמשך. כך,

איש מחקר שיקבל דיווח חדש מהאיסוף יוכל להתייחס אליו או לבקש מהאיסוף הבהרות לגביו בזמן כמעט אמיתי; איש האיסוף, מצידו, יוכל לדעת אם המידע שתרם לקהילה מסייע אם לאו, ולהוסיף מידע נוסף שלא היה יכול להציג במסגרות הרשמיות של הידיעות המודיעיניות ה"קאנוניות" שמופצות היום מיחידות האיסוף.

המעבר מצי"ח לשיח מהווה בסיס חשוב לבחינת ההצלחה של קהילת ידע. אם חבריה לא ירגישו בנוח להיחשף ולא יגיבו זה לדברי חברו, יהיה בכך סימן לכשל אפשרי באופן הבניית השיח באותו מרחב. על מובילי השיח יהיה מוטל אז לנקוט דרכים לפתרון הבעיה. תפקיד כזה, של "מוביל קהילת ידע", האחראי לקידום תהליכי פיתוח הידע, הינו תפקיד הכרחי בעולם הידע החדש.

מימוש תפיסת מודיעין 2.0 ייצור שינוי של ממש בתחום שימור הידע הארגוני ויצירת זיכרון ארגוני. במצב הנוכחי, ידע שאינו זוכה להיכנס למסמכים רשמיים אובד; רוב השיח הבלתי רשמי מתקיים על גבי דואר אלקטרוני, אולם הוא אינו נשמר באופן שיטתי, ונכס ארגוני פוטנציאלי זה פשוט נמחק ונעלם. כשאדם הממלא תפקיד מרכזי ורב־שנים בארגון – שבאופן טבעי מהווה מוקד ידע ארגוני – עוזב את תפקידו, הן הידע שבראשו והן חומרים שצבר ופיתח במחשב שלו נעלמים. אף שמדובר בנכסים ארגוניים מהמעלה הראשונה, הם אינם מוגדרים ככאלה, ואין כיום ניסיון או דרך לשמר אותם. בגישה החדשה שאנו מציעים, הדגש הרב שיושם על תהליכי השיח הפנימיים יאפשר למצות, לחשוף ולהנגיש את הידע הלא פורמלי השמור בראשם של אנשי המודיעין המהווים מוקד ידע: לאלה תוצע אפשרות לשתף אחרים בתובנות האישיות ובמאגרי המידע שאצרו במחשביהם האישיים, באופן שיטתי וקבוע וכחלק משגרת העשייה הארגונית.

כלים מרכזיים למימוש התפיסה

לאחר שבָּחַנו כמה היבטים תפיסתיים מרכזיים שיכולים לאפיין את תפיסת המודיעין 2.0, נפנה עתה להצגת כלים מרכזיים הקיימים בעולם ה־וב 2.0 ולבחינת ההסבה שניתן לעשות להם לעולם המודיעין.[10]

ניתן להקים במרחב המודיעיני המשותף "ויקיפדיה מודיעינית", אשר כל חברי קהילת המודיעין יהיו נגישים לה ושותפים לעדכונה. ב"ויקיפדיה" זו ניתן יהיה לעדכן ערכים מחקריים על היריב, אך גם ידע ארגוני הנוגע לתורות ולתפיסות הפעלה מודיעיניות, לתוכניות עבודה ולפרויקטים מודיעיניים שונים וכיוצא באלה. כמובן שנדרש יהיה לקבוע כללים לעדכון, ועליהם להיות שונים מאלה שבמרחב האזרחי, בו "חוכמת ההמון" מהווה את הבסיס לקיומה של ה"ויקיפדיה". במקרה המודיעיני, דווקא "חוכמת מומחים" (יחידים או קבוצות קטנות) היא המהווה את העוגן עליו צריכה להישען ה"ויקיפדיה המודיעינית". המומחים המעטים בכל תחום יכולים ללמוד אלה מאלה ולהציג את המידע והידע שברשותם על

גבי אותו ערך ב"ויקיפדיה", כך שיציג את התמונה המלאה ביותר האפשרית על מושא הכתיבה, במקום להתחרות זה בזה. בשונה מה"ויקיפדיה" האזרחית, עדכון ערכים ב"ויקיפדיה המודיעינית" לא יהיה בבחינת רשות או התנדבות, אלא יעוגן בנהלים ובמיסוד תפקידים חדשים בארגון ויהווה מחויבות מרכזית של העורכים המוסמכים לכך. עיקרון נוסף הרווח במרחב האינטרנט ולא נכון ליישמו בסביבה המודיעינית הוא רעיון האנונימיות, שכן בסביבה המודיעינית יש חשיבות רבה להכרת הגורם העומד מאחורי התובנה, כדי שניתן יהיה לחזור אליו בבקשה להבהרות או לעדכון אמירותיו.

חלקים מ"הוויקיפדיה המודיעינית" ישוקפו למרחב המשותף שבין עולם המודיעין ובין הצרכנים שמחוץ לו, אך שם לא תהיה לקוראים יכולת עדכון. כלומר, "הוויקיפדיה המודיעינית" תוכל להוות תשתית ידע גנרית וזמינה, אשר תשמש את חברי קהילת המודיעין בבואם להכין תוצרים מודיעיניים, והתוצרים המודיעיניים יוכלו להוות בתורם תשתית ידע שניתן לעדכן באמצעותה את הערכים ב"ויקיפדיה".

עדכון תוצרים תשתיתיים מוגמרים כערכים בתוך "הוויקיפדיה המודיעינית" גם יכול לתרום לרמת העדכון של הידע המודיעיני. כך, בשונה מהמצב כיום, בו סקירה מודיעינית מאבדת מהר מאד עדכניות של חלק מהמידע המצוי בה (אך לא באופן המחייב כתיבתה של סקירה מעדכנת), ב"ויקיפדיה המודיעינית" תוכל סקירה זו להיות עדכנית, כיוון שכל הראוי תיקון או עדכון יוכל להתבצע בזמן אמת.

בלוגים יהוו כלי מרכזי במרחב המשותף, שבו יוכלו חלק מהשותפים לכתוב את תובנותיהם האישיות באופן רציף ועיתי. עם זאת, בשונה מהמצב ברשת האזרחית, דומה שלא נכון כי כל אחד בקהילת המודיעין יהיה רשאי לפתוח בלוג, ללא שום הגבלה, הכְּוונה או בקרה. יתכן שיש להגביל, בשלב ראשון, את רשת הבלוגים של הארגון, כך שתכלול רק את מוקדי הידע בו ואת בכיריו. חלק מאנשי המודיעין הוותיקים מחזיקים בידע רב וייחודי, שלא יכול לקבל ביטוי בתוצרים הרשמיים הרגילים – "הגיגים" בסוגיות מתודולוגיות, הבחנות בנוגע לסוגיות מודיעיניות מתוך פרספקטיבה רבת־שנים, חוויות אישיות מאירועים מודיעיניים שהן בעלות ערך תורתי, ועוד. בדומה לכך, יש בכירים שהיו רוצים להעביר באופן תדיר ולא פורמלי את נקודת המבט שלהם על התהליכים המתקיימים בארגונים שעליהם הם אחראים, ולהניח כיוונים להמשך עשייה. בלוגים יכולים להוות פלטפורמה אידיאלית לאישים אלה להעלות את תובנותיהם על הכתב.

אחד הכיוונים החשובים והמבטיחים שיכול להציע עידן ה־וב 2.0 למודיעין הינו הקמתה של **רשת מודיעינית חברתית**,[11] שתהווה בעתיד חלופה מתקדמת למֵייל הארגוני. המֵייל הארגוני, שנכנס ככלי עבודה עיקרי בצה"ל ובאמ"ן בשנות האלפיים, נועד להעביר מסר בין אנשי הארגון. למרות שהוא לא נועד להיות

פלטפורמה טכנולוגית לפיתוח ידע, הוא הפך לכזה בעולם המודיעיני, בשל הצורך הרב באמצעי כזה והיעדר חלופה אחרת. שימוש במייל הארגוני לשיתוף ולפיתוח ידע כרוך בבעיות ובחוסרים רבים: מסיבות טכניות ומטעמי מידור לא ניתן להעבירו לכל הנמענים הרצויים; לא ניתן לקיים בו דיונים לאורך זמן (ה"חיות" של דיון במייל היא קצרה); המיילים מופיעים בתיבת הדואר (Inbox) של המשתמש כשהם אינם מסודרים הגיונית לפי סוגיות מודיעיניות, אלא כרשימה "שטוחה" ונטולת סדר (וזאת לצד "דואר זבל" רב); וחמור מכל, לא ניתן לשמור את המיילים באופן שיטתי, והידע המתפתח בהם אובד.

הטמעה רחבה של המדיה החברתית תסמן מהפכה של ממש בקישוריות ובחיבוריות שבין פרטי הארגון ותיצור קהילות ידע חיות ודינמיות, שתהוונה תשתיות חיונית לכל ארגון מודיעיני עתידי. כך, במקום לדעת על חברי הארגון את שמם, מספר הטלפון שלהם ותפקידם בלבד (המצב הנוכחי ברשתות ארגוניות שאינן "חברתיות"), הרשת החברתית תאפשר להכיר את הפרטים בארגון כמו שה"פייסבוק" מאפשר בבית. כל פרט בארגון יוכל להגדיר את העמיתים ("החברים") הרלוונטיים לו ולעקוב אחריהם ואחר תכנים חדשים שיעלו לרשת. יתרה מכך, הפרופיל של כל משתמש יכלול, באופן אוטומטי ובאמצעות הזנה ידנית, פירוט של תחומי המומחיות והעניין שלו (בין היתר, כנגזרת מהתפקידים השונים שביצע וההכשרות האקדמיות, הצבאיות והמודיעיניות שלו) ושל תוצרים רשמיים ותכנים לא רשמיים שפרסם. באמצעות למידה של קריטריונים אלה, תדע המערכת להציע לו תכנים או להציע לו להצטרף לדיונים מקוונים ולקהילות ידע מסוימות, שעשויים לעניין אותו ואשר הוא לבדו לא היה מגלה. באותה מידה, חברים אחרים ברשת יוכלו לאתר אותו משתמש ולהסתייע בו לפי אותם קריטריונים, בין אם בעקבות חיפוש יזום על ידם ובין אם באמצעות המערכת, שתדע "להציף" להם אותו ואת התכנים שלו.

שינוי מרכזי נוסף שטומן בחובו מודיעין 2.0 הוא היכולת, שאינה קיימת כיום, לערוך דיונים לא סינכרוניים – דיונים בסוגיה מסוימת שיכולים להתקיים לאורך זמן וללא רציפות. תרבות של דיונים שלא נדרש תזמון משותף כדי לקיימם הינה גישה שנכון לאמץ לא כחלופה למפגשים פיזיים, אלא כהשלמה הכרחית שתעניק להם ערך מוסף. כך יוכל איש השגרירות בארצות הברית או בהודו להשתתף בדיון שנוגע לארץ בה הוא משרת, וכך יוכלו חברי קהילת ידע מודיעינית, הממוקמים בשני קצוות של המדינה, להיפגש. באופן זה גם יוכל אדם לתרום לדיון שהתקיים לפני מספר חודשים, אם דיון זה עדיין רלוונטי. ניתן לפתח עניין זה ולהציע שקבוצות הדיון ברשת החברתית (קהילות הידע) יוגדרו באופן רשמי כתצורה הארגונית המובילה לקיומם של צמ"מים (צוותי משימה משולבים) מודיעיניים. אולם, בשונה

מבעבר כאשר הגדרת צמ"מ חייבה מפגש פיזי הרי העידן הנוכחי מזמן אפשרות לקיומו של צמ"מ רשתי.

סיכום

התחרות על הלמידה הופכת לשדה מאבק מרכזי בעידן הנוכחי. על ארגוני המודיעין להפוך לארגונים לומדים ומסתגלים במהירות רבה יותר לשינויים המתחוללים בסביבת הפעולה שלהם. באימוץ תפיסת ווב 2.0 לַמעשה המודיעיני, תוך פרשנות רלוונטית שלה לסביבה המודיעינית, טמונה מהפכה שעשויה לשנות מן היסוד את הזיקות בין גופי המודיעין לבין עצמם, ובינם לבין צרכניהם. הדבר יסייע להקנות לתהליכי העבודה את הרשתיות, הסינרגיה, הגמישות והמהירות, שחיוניות כדי להתמודד עם האתגרים הדינמיים ועם היריבים ההיברידיים של העידן הנוכחי.

קשיים ואתגרים לא פשוטים ניצבים בפני היכולת לממש את הגישה החדשה, בשל קשת נרחבת של סיבות: ראשית, גישה זו מנוגדת, לכאורה, למסורת המודיעינית של סודיות ומידור מזה, ושל תחרות ופלורליזם מזה. תרבות המתנהלת על בסיס הערך לפיו "ידע הוא כוח", ומתוך העיקרון שחשיפת מקורות ומידע צריכה להיות רק על בסיס צורך (On a need to know basis), תתקשה להשתנות באחת ולהתנהל על בסיס הערך לפיו "שיתוף הינו עוצמה" (On a need to share).[12]

קושי משמעותי נוסף, הנגזר מקודמו, הוא היעדר חיבוריות טכנולוגית בין ארגוני המודיעין לבין עצמם, קל וחומר בין גופי המודיעין לצרכניהם. המדובר במציאות של בידול רשתי הנגזרת ממסורת עמוקה של מידור, בידול ותחרות בין רכיבי קהילת המודיעין, ונובעת בין היתר מהיגיון שעיצב "מעגל המודיעין". אין מדובר בקישוריות של דואר אלקטרוני (אשר אף היא לא תמיד קיימת), אלא ביצירת מרחב רשתי משותף שיאפשר פיתוח ידע משותף ותשתית ידע שכולם שותפים לה.

קושי שלישי, המונע לעיתים מארגונים בכלל ומארגוני מודיעין בפרט לאמץ לחיקם את המדיה החברתית, נובע מהחשש של ארגונים מפני היווצרותו של מידע מסוג חדש. זאת, הן בשל חשש של ותיקים בארגון להתמודד עם הטכנולוגיה החדשה ועם התפיסה העומדת מאחוריה והן בשל החשש כי תִקשוּר באמצעות מדיה חברתית יסיט את הפרטים בארגון ממשימותיהם. בהקשר זה יש להדגיש כי יישום הרשת החברתית בעולם המודיעיני עלול ליצור מתח בין האופי הכאוטי המאפיין את השיטוט ברשת האזרחית לבין הצורך במיקוד ומשימתיות בעולם המודיעיני. האתגר הקיים כאן הוא להשתמש ברשת החברתית המודיעינית כך שתמצה את התועלות של מאפייניה הייחודיים, ובה בשעה תצליח להימנע מהבעייתיות שיוצרים מאפיינים אלה ביחס למשימתיות המודיעינית.

קושי משמעותי נוסף, עליו ניתן ללמוד מהניסיון האמריקאי,[13] הוא האפשרות שהכלים החדשים ליצירת קשר ולהעברת מסרים בין חברי קהילות המודיעין,

כמו גם הכלים לשימור ופיתוח הידע המודיעיני, יהיו כלים משניים נוספים מבין מערכות המידע של הארגון. בכך, לא רק שהכלים החדשים לא ישרתו את תהליך פיתוח הידע המודיעיני, אלא ייצרו כפילויות וימנעו את הפיכת הרשת המודיעינית החברתית למרחב המרכזי בו נשמר ומפותח הידע בארגון.

הדרך להתמודד עם אתגרים אלה מורכבת ממספר נדבכים. נראה כי הנדבך העיקרי הוא הצורך החיוני שהרשת החברתית המודיעינית תוגדר כסביבת העבודה הראשית־מבצעית של הארגון. באמצעות רשת זו תתקשר קהילת המודיעין טוב יותר בינה לבין עצמה ובינה לבין גופים חיצוניים שיוכלו להשתלב בה (במגבלות הנדרשות). כך, גרסה מודיעינית של "פייסבוק" תשמש, בין היתר, כמרחב העבודה של צוותים משימתיים; שימור ידע במערכת יהיה בתשתית "ויקי"; ותהליכי ההכנה והאישורים של התוצרים המודיעיניים ייעשו אף הם במרחב המשותף החדש.

המרחב הרשתי מבוסס ה־וב 2.0 צריך להיות מועיל ובעל ערך מוסף ברור בהיבטי ניהול המידע. לשם כך, יש לוודא שכל מקורות המידע, וכן נכסי הידע של הארגון, ירוכזו ויימצאו במרחב זה, תוך מתן אפשרויות מתקדמות יותר הן לשמירת המידע והידע והן לנגישות אליהם (אינטגרציה ומיזוג תכנים, שיתוף מסמכים וקבצים, קישור למערכות חיצוניות, גישה למאגרי מידע, שירותי אחזור חזקים). כבסיס לכך, נדרשת מהפכה אמיתית בתחום מערכות המידע והקישוריות בין הארגונים. יצירת מרחבים משותפים תתאפשר רק אם ייווצרו סטנדרטיזציה ותקנים בין המערכות השונות, כך שאלו יוכלו "לדבר" אחת עם רעותה.

מעבר לכך, ובדומה להבנה שהתפתחה בשיח האמריקאי, לא די בשילוב כלים טכנולוגיים חדשים אלא נדרש שינוי תרבותי ותפיסתי עמוק. שינוי זה צריך לבוא לידי ביטוי גם בהכשרות ובמיסוד מקצועות חדשים. בנוסף, נדרש עיסוק תורתי בתפיסת פיתוח הידע המודיעיני, שיוביל לעדכון של תהליכים ארגוניים מיושנים ולהפסקת דפוסים המעמיקים את הפירוד והתחרות בין הארגונים.

קיימות מספר הצעות בשיח האמריקאי הנוכחי כיצד לצאת מן המצר ו"לחלץ את העגלה המודיעינית התקועה". ראויה לציון ביניהן תפיסה שפיתחו אנשים מתוך סוכנות המודיעין הגיאוגרפי של ארצות הברית (NGA), הנקראת Living Intelligence. תפיסה זאת קוראת לשַנוֹת את התרבות ואת ההרגלים והדפוסים הישנים של עשיית מודיעין.[14]

החידוש בתפיסה זו הוא הקריאה לראות את **המדיה החברתית כסביבת העבודה הראשית של קהילת המודיעין**. במילים אחרות, הגישה מציבה בראש מעייניה את התוצר המודיעיני ומציעה להפוך את התוצרים המודיעיניים, את תהליכי הייצור שלהם ואת אופן ההצגה שלהם לרִשתיים ו"חברתיים". עוד קוראת התפיסה ליצירת תוצרים מודיעיניים משולבים, ובכך להקטין משמעותית את החפיפה והעבודה הכפולה בין ארגוני המודיעין.

מרכיב קריטי נוסף בהעלאת סיכויי הצלחתו של המהלך הינו **מודל פיקודי שונה** מהמודל הקלאסי־הירארכי, התופס הובלה של שינויים כתהליך שאמור להגיע בעיקר "מלמעלה". המודל החדש צריך לאפשר גם מקום ל"כאוס מנוהל", תוך אימוץ וחיבוק של הדור הצעיר המצטרף לקהילת המודיעין כמוביל השינוי. בני הדור הזה רגילים לתקשר ברשתות חברתיות טרם גיוסם ולחיות בסביבה משתפת. כל שנותר הוא לא לשנות את ההרגלים שלהם ולא לשרש אותם, אלא לחזקם, ולספק לצעירים אלה את הכלים להם הם רגילים לטובת שיתוף ופיתוח ידע. כל זאת, כמובן, תוך "דיאלוג" בין המודל הפיקודי הרשתי ובין המודל הקלאסי, כדי למצוא את שביל הזהב בין הצורך בחדשנות שתבוא מלמטה ובין "גידור" אזורי העשייה, בהם יש לשמור על העקרונות של מדרגי האחריות והסמכות בכל הנוגע לאישור תוצרים מודיעיניים.

החשש של ארגונים וממסדים לשלב מדיה חברתית כדרך לתקשר ולפתח ידע בארגונם הוא מובן, אך הוא עלול להוות חסם ראשי בפני יצירת קהילות מודיעיניות רשתיות וחוצות ארגונים. ניסיון להגביל את הדרכים בהן יוכלו פרטים בקהילה ליצור קשר, לא יצלח; הם פשוט יעשו זאת ברשתות החברתיות האזרחיות, ואילו הרשת המודיעינית תיוותר משנית ומנוונת. אימוץ של המדיה החברתית לחיק קהילת המודיעין יביא עימו את מהפכת המודיעין 2.0, ויחד איתה בשורה אמיתית למעשה המודיעיני.

הערות

1 המאמר נכתב והופץ באמ"ן במהלך שנת 2012. מאז, במסגרת תהליך עמוק של שינוי ארגוני ותפיסתי שמוביל ראש אמ"ן, מיושם חלק מרכזי מהרעיונות המובאים במאמר. ברצוננו להודות **לגור ע. וטל גוטמן** על תרומתם הרבה לתהליך הלמידה שבמסגרתו נכתב המאמר.

2 חיים הרצוג, כפי שהוא מצוטט אצל זהבה אוסטפלד, **צבא נולד**, משרד הביטחון־ההוצאה לאור, 1994, עמ' 333.

3 אמ"ן, **תהליך עבודת המודיעין**, 1956, ארכיון צה"ל. עותק של החוברת נמצא במכון לחקר המודיעין באמ"ן.

4 הדוח המלא של ועדת אגרנט לחקירת מלחמת יום הכיפורים, אתר ארכיון צה"ל, עמ' 160, 168, http://www.archives.mod.gov.il

5 Kristan J. Wheaton. "Let's Kill the Intelligence Cycle", http://sourcesandmethods.blogspot.com/2011/05/lets-kill-intelligence-cycle-original.html

6 שני אבנט, **User Experience – בלי חוויה אין משתמש, על העצמת פורטלי מידע באמצעות חוויית משתמש**, חברת Netwise. ראו המצגת בכתובת: http://api.ning.com/files/x6R-TdDcUc0aH8798ORM5OWlq3G5G-1lnmXkOaf1WI8dFFg7BwS1RyyeiOuO7tCvYtSUlTTqOn2M-kjH8EJ5cGbX6OI1A2rt/file.pdf

7 *Time Magazine*, December 25, 2006, http://www.time.com/time/magazine/article/0,9171,1570810,00.html

8 אלווין והיידי טופלר, **הגל השלישי**, עם עובד, תל אביב, 1984; אלווין והיידי טופלר, **עושר מהפכני**, עם עובד, תל אביב, 2008.

9 שמואל אבן ועמוס גרנית, **קהילת המודיעין הישראלית – לאן?**, המכון למחקרי ביטחון לאומי, מזכר 97, 2009, עמ' 49.

10 D. Calvin Andrus, "The Wiki and the Blog: Toward a Complex Adaptive Intelligence Community", *Studies in Intelligence*, 49, no. 3 (September 2005), pp. 63-70, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=755904.

11 רשת מודיעינית חברתית הוקמה באמ"ן בשנת 2011 ועושים בה שימוש אלפי אנשי מודיעין מיחידות האיסוף והמחקר, כמערכת עיקרית ליצירת מודיעין.

12 David Schroeder, "Efficacy and Adoption of Central Web 2.0 and Social Software Tools in U.S. Intelligence Community", American Public University System, March 2011.

13 שם, עמ' 2.

14 Chris Rasmussen, "Toward Living Intelligence", August 9, 2009, http://www.gov2expo.com/gov2expo2009/public/schedule/detail/10599; ראו גם את הסרטון ב"יו־טיוב" בכתובת: http://www.youtube.com/watch?v=XdQPuTVDOH4.

האם כוח הוא התשובה? "בּוֹקוֹ חראם", הכוח הצבאי המשותף והג׳יהאד העולמי

דניאל אג׳יגבה אגביבואה

במאמר זה אציע בחינה ביקורתית של הטרור הדתי שמשליט ארגון "בּוֹקוֹ חָרָאם" בצפון ניגריה, תוך התמקדות בשאלה מדוע קיים הארגון ומה טיב הקשר המתחזק בינו לבין הג׳יהאד העולמי. אציג את הערכתי לתגובתה של ממשלת ניגריה ל"בוקו חראם", המתאפיינת בכפייה מצד אחד ובפיוס מצד שני, תוך התייחסות ספציפית ל"כוח המשימה הצבאי המשותף" שהקימה. אציג את הפרובלמטיקה של הגישה הדוגלת בהרג ומתמקדת בפן הביטחוני בלבד של ההתמודדות עם הטרור הדתי ואטען שעל מדינות הנלחמות בטרור מחוץ לגבולותיהן ללמוד מהניסיון הניגרי של המלחמה ב"בוקו חראם", ולהסיק מכך כי "הכרזת מלחמה על הטרור" רק מזינה מעגל אכזרי של טרור נוסף ושל מלחמות שאין להן קץ.

מילות מפתח: בוקו חראם; טרור דתי; צפון ניגריה; ג׳האד עולמי; כוח משימה צבאי משולב; אל הרג.

מבוא

מאמר זה עוסק בטרור הדתי שמפעיל בימים אלה ארגון אסלאמי קיצוני בצפון־מזרח ניגריה. באופן רשמי, הארגון מכנה את עצמו "אנשים המחויבים לנבואות הנביא להפצת הג׳יהאד", אולם המקומיים הצמידו לו את השם "בוקו חראם", שפירושו בשפת ההאוסה "החינוך המערבי אינו חוקי". מאז הקמתו ב־2002 גבה הארגון יותר מ־10,000 קורבנות, והוא מטיל את אימתו על מיליונים מתושבי ניגריה.[1] היעד העליון שלו הוא להקים מדינה אסלאמית הנשלטת על פי חוקי

דניאל אג׳יגבה אגביבואה הוא חוקר בבית־הספר למחקר מדעי החברה, האוניברסיטה הלאומית של אוסטרליה.

השריעה.[2] למרבה הצער, כל ניסיון לשאת ולתת עמו, לרבות הצעה לחנינה לחבריו שהועלתה לאחרונה, כָּשַל, עקב חוסר אמון בשני הצדדים ובשל הנהגת הארגון המפולגת בין תאיו השונים.

במאמר זה אציע בחינה ביקורתית של בעיית "בוקו חראם" בצפון ניגריה, תוך התמקדות בשאלה מדוע קיים הארגון ומה טיב קשריו המתהדקים עם הג'יהאד העולמי, וזאת בהובלת קבוצות על־לאומיות דוגמת "אל־קאעדה" באזור המגרב ו"אל־שבאב" בסומליה. אציג הערכה לתגובות ממשלת ניגריה לאיום הביטחוני שמציב "בוקו חראם", הנעות בין פייסנות לכפייה, תוך התייחסות ספציפית ל"כוח המשימה הצבאי המשותף" שהוקם ולאסטרטגיה הכוחנית הנוכחית שלו נגד הארגון הג'יהאדיסטי. אציג את הפרובלמטיקה של הגישה הדוגלת בהרג לשם התמודדות עם טרור דתי, המונעת על ידי שיקולי ביטחון בלבד, ואטען שמדינות הנלחמות בטרור מחוץ לגבולותיהן צריכות להסיק מהניסיון הניגרי כי "הכרזת מלחמה על הטרור" רק מעודדת מעגל אכזרי של טרור נוסף ומלחמה שאין לה סוף.

מסגרת תיאורטית: התעמתות עם הטרור

אין הגדרה סטנדרטית לטרור, כפי שממחיש הממצא של אלכס שמיד (Schmid), לפיו יש כמאה שימושים שונים במונח זה.[3] יחד עם זאת, מרבית ההגדרות חולקות כמה מאפיינים משותפים: (א) טרור, לרבות אלימות ממניעים דתיים או פוליטיים, מכוון לעורר איום; (ב) טרור מכוון לעורר פחד בקהל רחב; (ג) טרור מושג בעיקר באמצעות שימוש בנשק אלים או פסיכולוגי.[4] במאמר זה, טרור יוגדר באופן שעולה בקנה אחד עם הנוסח באמנת אלג'יר משנת 1999, דהיינו מעשה אשר "מתוכנן או מיועד לעורר אימה, להפחיד, להכריח, לאלץ או לגרום לממשלה, לגוף, למוסד כלשהו או לציבור הרחב, או לכל פלח בתוכו, לעשות מעשה כלשהו או להימנע מעשייתו; לאמץ או לנטוש עמדה מסוימת; לפעול בהתאם לעקרונות מסוימים; לשבש שירות ציבורי כלשהו או אספקה של שירות חיוני כלשהו לציבור, או ליצור מצב חירום בציבור; או לעודד מרידה כללית במדינה".[5] מעשי טרור יכולים להתבצע על ידי מדינות, גורמים מדינתיים, גורמים שאינם מדינתיים, ארגונים או יחידים, וזאת בניסיון להשיג יעדים מסוימים או להשליט ערכים רצויים. הגדרה זו רלוונטית במיוחד בהקשר הניגרי, שם הממשלה נוטה לעשות שימוש בטרור נגד אזרחיה שלה.

לנוכח השאלה עד כמה המדינה מסוגלת להתמודד עם ארגוני טרור, ניתן לשלוף מתוך הספרות הקיימת שתי גישות מתחרות למלחמה בטרור: כפייה או פיוס. לב הוויכוח הוא השאלה האם המדינה צריכה להשליט מדיניות מחמירה שתכליתה להעניש טרוריסטים, וכך להרתיע מעשים כאלה בעתיד, או שמא עליה להתמקד בסיבות השורש ולהפחית את התמריצים לפנות לטרור.[6] במילים אחרות,

האם מדיניות של כפייה מרתיעה טרור, או שהיא יוצרת מעגל אכזרי של אלימות? שאלה זו, שאין עליה הסכמה רבה, עלתה ביתר שאת לאחר מתקפת הטרור של 11 בספטמבר 2001.[7]

גישת הכפייה כוללת שימוש בכוח פיזי מצד הממשלה, במטרה לפגוע או להרוג את הטרוריסטים או שולחיהם. שימוש כזה מתרחב לכדי טרור מדינתי, חיסולים, ירי טילים ופלישות. מדינות רבות תומכות בגישת הכפייה, והיא גם מאפיינת את מדיניות התגמול של ישראל ואת המערכה העולמית שמנהלת ארצות הברית נגד הטרור.[8] הלוגיקה שמאחורי גישת הכפייה היא ההנחה שפעולת תגמול תיצור תדמית לפיה סופם של טרוריסטים להיענש, וכך תניא אותם מפעולות דומות בעתיד. בהמשך לכך, מדינות שלא מגיבות בהפעלת כוח, או שנענות לתביעות של טרוריסטים, מואשמות כמציגות עמדה רכה מדי, המעודדת טרור.[9]

גישה פייסנית פירושה שעל המדינה להתייחס לסיבות המהותיות לטרור ובכך להפחית את הלגיטימיות של תביעות הטרוריסטים ואת דבקותם במטרה. מדינות עושות שימוש בפייסנות כדי לפתור משברים או כדי לסכל משברים עתידיים, באמצעות משא ומתן עם טרוריסטים.[10] דוגמאות לוויתורים הם רפורמה חברתית, שחרור אסירים או משא ומתן עם מדינה הנותנת חסות לטרור. המבקרים את גישת הפייסנות טוענים כלפיה שהיא מהווה כניעה לתביעות הטרור, למרות שהיא כוללת גם ניסיונות לשכנע ארגוני טרור ותומכיהם לנטוש את הטרור באמצעות הבטחה לשינויים.[11] המתנגדים לגישת הכפייה טוענים שלא רק שהיא נכשלת בהרתעת הטרור, אלא שהיא גם מגבירה את ההתנגדות לממשלה ומובילה למעגלים של אלימות. צפון אירלנד, ישראל וצ'צ'ניה ממחישות התנהגות מדינית שלא רק שכשלה בעצירת הטרור, אלא גם האריכה את משך האלימות.[12]

המתנגדים לגישה זו גם מפנים את תשומת הלב לאסטרטגיה ה"תוקפנית" שאפיינה את ממשל הנשיא בוש בארצות הברית, שלעתים קרובות מדי הייתה "בלתי מועילה והרסנית כלפי לעצמה",[13] כשהיא מסכנת שיתופי פעולה בין־לאומיים במלחמה בטרור ומספקת תחמושת למאמצי הגיוס של טרוריסטים במזרח התיכון ובמקומות נוספים.

אני טוען נגד "אסטרטגיית ההרג" המונעת משיקולי ביטחון בלבד ואביא דוגמאות לכך שהרג נוסף רק מגביר את הטרור. הרתעה אינה כלי טוב מול טרוריסטים המוכנים להקריב את חייהם. עוד אטען כי מדינות הנלחמות בטרור מחוץ לגבולותיהן, כמו ארצות הברית, בריטניה וצרפת, צריכות ללמוד מהניסיון הניגרי של מלחמה ב"בוקו חראם" ולהסיק מכך ש"הכרזת מלחמה על הטרור" רק מייצרת מעגל דמים אכזרי של טרור והתדרדרות לאלימות שאין לה סוף. הסתמכות על כוח קשה במלחמה בטרור מחמיצה את טבעו הדתי ומחמירה את האיום בצורה

ניכרת. במקום זאת, אני טוען לגישת אל־הרג, שמזהה את המוטיבציות והמחאות של ארגוני הטרור ומנסה להתמודד אתן.

גישת אל־הרג כוללת תפיסות של שלום (היעדר מלחמה או תנאים מעודדי מלחמה), אי־אלימות (פסיכולוגית, פיזית או מבנית), ו"הִימְסָה" (Ahimsa, בתרבות ההינדית –הימנעות מגרימת נזק במחשבה, במילים ובמעשים).[14] קיומה של תפיסת האל־הרג מקבל גיבוי על ידי התזה פורצת הדרך של גלן פייג' (Paige), שמראה בצורה משכנעת שפחות ממחצית האחוז מכל בני האדם הרגו אי פעם בני אדם אחרים.[15] פייג' מגדיר חברה ללא הרג כ"קהילה אנושית, מהקטנה ביותר ועד הגדולה ביותר, ממקומית ועד גלובלית, המאופיינת בכך שאינה הורגת בני אדם, אין בה איומים להריגה, אין בה נשק המיועד להרוג בני אדם, אין הצדקות להשתמש בנשק כזה, ואין תנאים חברתיים התלויים באיום להשתמש בכוח קטלני או בשימוש בו בפועל לצורך שימור מצב קיים או שינויו".[16] הנקודה המעניינת בטיעון של פייג' היא שמַבנים רחבים בחברה אינם זקוקים ליכולת הרג כתנאי חיוני לשינוי או לשימור. טענה זו קוראת תגר על האמונה ארוכת השנים שהרג הוא תכונה בלתי נמנעת ביחסי אנוש – אמונה שממשיכה להזין (בשגגה) את המלחמה העולמית בטרור.

האסלאם הקיצוני, שהמאמר הנוכחי מתמקד ישירות בו, הוא תוצר לוואי של מספר התפתחויות היסטוריות, לרבות ליקוי תפקודי של החברות המוסלמיות בתחום הכלכלי, המדיני והחברתי, שחוסם את התפתחותן. החסרונות בחברות אלה פתחו פתח לקיצוניים לנצל תחושה של השפלה תרבותית ולקרוא מחדש את ההיסטוריה המוסלמית דרך דוקטרינה שמאשימה ומתעבת את "המערב". כפי שאסביר בהמשך על פי המקרה של "בוקו חראם", חלק מהבעיה הוא שארגונים ג'יהאדיסטיים מוסיפים את המרכיב הדתי לתוך הקלחת הרותחת של התמרמרות על שחיתות, דיכוי, עוולות וחלוקה לא הוגנת של עושר וכוח, כפי שטוען דניאל בנג'מין, "במרבית המדינות המוסלמיות קיים זעם אמיתי כלפי השלטון והשחיתות, שהופך למוקד קובלנה מרכזי של ג'יהאדיסטים, המדברים על השליטים ה'בוגדים', וכך מתרגמים את הזעם לביטוי דתי".[17]

אסטרטגיה צבאית המונעת משיקולי ביטחון בלבד מעניקה בדרך כלל יתרונות נוספים לאסלאמיסטים קיצוניים. הם צוברים ניסיון בטקטיקות, ויוצרים רשתות חדשות של תמיכה וקשרים חברתיים עם קבוצות שונות, במטרה להניב שיתופי פעולה בעתיד. אסטרטגיה זו גם מעניקה להם הזדמנות לגייס עוד כספים ולרכוש נשק וציוד נוספים. יתרה מכך, השימוש בכוח צבאי כאסטרטגיה למלחמה בטרור אינו רצוי, עקב טבעו שאינו מבחין בין הנפגעים ויוצר לעיתים קרובות ניכור דווקא בקרב אותם יחידים בקהילה שלא היינו רוצים לראות בהקצנתם. זאת ועוד, פעולה צבאית כנגד יעדי טרור מסתיימת לא פעם במותם של אנשים חפים מפשע, גם אם ננקטו כל אמצעי הזהירות הנדרשים, כפי שמוכיחות התגובות הצבאיות הלא

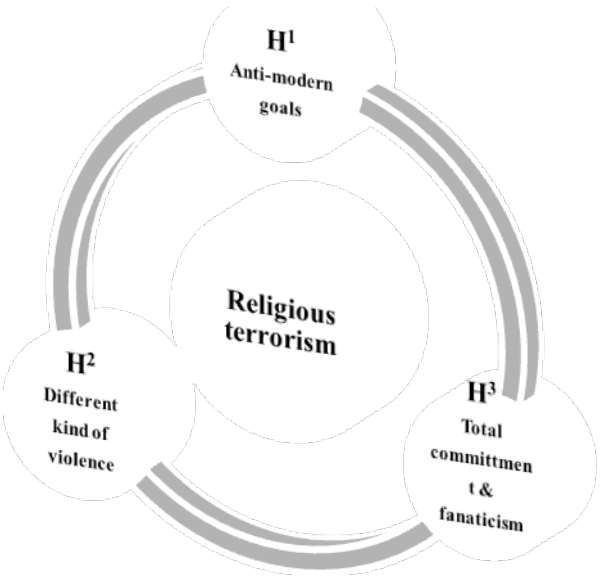
מתונות והתמוהות משהו לפעולות הטרור של "בוקו חראם" – תגובות שהביאו ליותר נזק לניגריה מאשר תועלת.

להבין את הטרור הדתי

לדֶבק שמחבר דת וטרור יש שורשים ארוכים במחקר המערבי. הרעיון של "טרור דתי" מקורו במאמר פרי עטו של דיוויד רפופורט,[18] שניתח את השימוש בטרור בשלוש הדתות המונותיאיסטיות. המאמר האקדמי נתן השראה לעבודות דומות רבות שביקשו להסביר "מדוע אלימות ודת צמחו שוב ובצורה כה דרמטית בנקודה מסוימת בהיסטוריה, ומדוע ניתן למצוא אותן פעמים כה רבות כרוכות זו בזו".[19] במילותיו של סקוט אפֶלבִי: "מדוע נדמה שדת זקוקה לאלימות, ואלימות זקוקה לדת?".[20] לפי אסכולה זו, הטרור הדתי התעלה מעל להיותו כותרת פשוטה, והפך למערך של מאפיינים תיאוריים ותביעות מהותיות שגורמים להגדרתו כ"סוג" ספציפי של אלימות פוליטית, השונה מהותית מצורות קודמות או אחרות של טרור.[21]

הטענה על טבעו המיוחד של הטרור הדתי נשענת על מספר השערות מרכזיות, ששלוש מהן מובאות בקצרה להלן (ראו תרשים 1).

תרשים 1: שלוש השערות על הטרור הדתי



השערה 1: טרוריסטים דתיים מחזיקים באמונות אנטי־מודרניות שעושות אידיאליזציה לעָבר ומבקשות להחזיר את החברה לימי קדם, ולכן יתנגדו בהכרח לדמוקרטיה ולקִדמה.

אודרי קרונין גורסת כי "דומה שכוחות ההיסטוריה דוחפים את הטרור הבין־לאומי בחזרה לזמן הרבה יותר קדום, המרַמז על התנהגות של טרוריסטים 'קדושים' [...] כפי שנראה בברור בארגון טרור דוגמת 'אל־קאעידה'".[22] מארק יורגנסמאייר מחזיק בדעה שטרור דתי חותר לעבר "אג'נדה פוליטית אנטי־מודרנית".[23] כמו כן נטען שטרוריסטים דתיים מחזיקים במטרות שהן מוחלטות, קשיחות, לא ריאליסטיות, מתרחקות מפרגמטיות פוליטית ועוינות משא ומתן.[24] במאמרו המצוין "מקורות הטרור החדש" קובע מתיו מורגן: "הטרוריסטים כיום לא מעוניינים לשבת לשולחן; הם רוצים להרוס את השולחן ואת כל מי שיושב סביבו".[25] דניאל ביימן מציין לגבי "אל־קאעידה": "בשל היקף מחאותיו, האג'נדה הרחבה שלו שמבקשת לפצות על השפלות, והשקפת העולם המורעלת שמאדירה את הג'יהאד כפתרון, פיוס אל־קאעידה יהיה קשה בתיאוריה ובלתי אפשרי במעשה".[26] השקפה זו נתמכת על ידי דניאל בנג'מין, שגורס כי שלא כמו מרבית ארגוני הטרור, "אל־קאעידה" "נמנע מלצבור הישגים ואינו מבקש להיות שותף למשא ומתן כלשהו. הוא מחפש להשיג את יעדיו המרכזיים, הכוללים הגדלת מספר המוסלמים, באמצעות אלימות".[27]

השערה 2: טרוריסטים דתיים מיישמים סוג אחר של אלימות בהשוואה לטרוריסטים חילוניים

הטענה היא שעבור טרוריסט דתי, "אלימות היא [...] פעולה מקודשת או חובה שמימית, שמתבצעת בתגובה ישירה לתביעה תיאולוגית כלשהי",[28] וזאת בניגוד לאמצעים טקטיים המשרתים יעד פוליטי. יתרה מכך, היו מי שהעלו את הסברה, שמִשום שטרוריסטים דתיים מחזיקים במטרות טרנסצנדנטליות, מעורבים במלחמה קוסמית ונעדרים ציבור בוחרים ממשי, הם אינם מוגבלים באלימות שלהם, ולכן מ־מצים עימות אלים מתוך נקודת מבט אפוקליפטית: "מה שהופך את האלימות הדתית לפרועה ואכזרית במיוחד הוא שהדוגלים בה גייסו דימויים דתיים של מאבק אלוהי ומלחמה קוסמית לשירות המאבקים הפוליטיים הגשמיים שלהם".[29] מסיבה זו, פעולות של טרור דתי הן לא רק טקטיקות במאבק פוליטי, אלא גם תזכורת לעימות רוחני הרבה יותר גדול. משום כך, טרוריסטים דתיים מכוונים למרב הקורבנות ומוכנים להשתמש אפילו בנשק להשמדה המונית,[30] כפי שמנסח זאת מגנוס רנסטרופ: הם "יחסית בלתי מרוסנים בשימוש הקטלני וחסר ההבחנה שהם עושים באלימות, [מכיוון שהם נעדרים] מגבלות מוסריות לשימוש באלימות".[31]

השערה 3: לטרוריסטים דתיים יש יכולת לעורר מחויבות טוטאלית ופנאטיות בקרב אנשיהם.

יש הטוענים כי טרוריסטים דתיים מאופיינים בכך שהם שמים בצד את הספק ומאמצים השקפת עולם לפיה "המטרה מקדשת את האמצעים". זאת, בניגוד לגישות ה"בוגרות" יותר כביכול של הארגונים החילוניים.[32] מארק יורגנסמאייר גורס כי "תופעות מטרידות אלו לָוו בטענות נמרצות לצידוק מוסרי ולאבסולוטיזם מתמשך, המאופיינות באינטנסיביות של הלהט האקטיביסטי הדתי".[33] היו מי שגרסו כי במקרים מסוימים, המוחלטות של נקודת המבט הדתית וההבטחות לעולם הבא הן הגורמים המניעים הראשיים בדחיפת צעירים מנוכרים וחסרי ביטחון, המגיעים משולי החברה, להצטרף לארגוני טרור דתיים כאמצעי של העצמה פסיכולוגית. עוד נטען, שצעירים מנוכרים ומחוסרי כוח הנוחים להשפעה נחשפים לשטיפת מוח ולהשפעה פסולה מצד גֻיָסים, מטיפים קיצוניים או חומרים באינטרנט.[34]

בהמשך המאמר אסתמך על שלוש ההשערות הנוגעות לטרור הדתי כדי להסביר את המערכה האלימה שמנהל "בוקו חראם" בניגריה.

טרור דתי: המקרה של "בוקו חראם"

"אנו חוזרים ומצהירים שאנו לוחמים בשם הג'יהאד (מלחמה דתית) בניגריה, ושהמאבק שלנו מתבסס על המסורת של הנביא הקדוש. לעולם לא נסכים לאף מערכת ממשלתית, למעט משטר האסלאם, משום שזו הדרך היחידה לשחרור המוסלמים [...] אנחנו לא מאמינים במערכת המשפט הניגרית ונילחם בכל מי שיסייע לממשלה בביצוע מעשים לא חוקיים".[35]

מוחמד יוסוף, שנולד ב־29 בינואר 1970 בכפר ג'רג'יר שבמדינת יוּבֶּה בניגריה, הקים את "בוקו חראם" בשנת 2002 במטרה לבסס את משטר השריעה במדינת בּוֹרנוֹ שבצפון ניגריה. יוסוף הקים מתחם דתי בעיר הולדתו, שכָּלל מסגד ובית ספר, אליו נרשמו תלמידים רבים ממשפחות עניות מכל רחבי ניגריה ואף מארצות שכנות. למעשה, למרכז היו מטרות פוליטיות נסתרות, ועד מהרה הוא החל לפעול גם כבסיס לגיוס ג'יהאדיסטים לעתיד שיילחמו נגד המדינה. "בוקו חראם" מצא תמיכה בקרב האוכלוסייה המנוכרת והענייה בצפון ניגריה, אשר רבים בה נמשכו לאופן שבו גינה הארגון את האליטות השולטות במדינה, אותן כינה מושחתות ובוגדות.[36] "בוקו חראם" הצליח למשוך אליו יותר מ־280,000 חברים מכל צפון ניגריה, וכן מניג'ר ומצ'אד, ושפתו הייתה ערבית בלבד.[37]

האידיאולוגיה של "בוקו חראם" נעוצה בסלָפיזם הרדיקלי – מיעוט קטן באסלאם שמקורו במאה התשיעית לספירה, ומאפייניו העיקריים התגבשו סביב הגותו של המלומד האסלאמי בן המאה ה־14 תקי אל־דין אחמד אבן תימייה

(מת בשנת 1328). המאפיין את הסלפיזם הוא קריאה למוסלמים לחזור לאסלאם הטהור של דור הנביא מוחמד ושני הדורות שאחריו. המוסלמים בתקופה קדומה זו נקראו "אל־סלף אל־סאלח" (האבות הקדושים), ומכאן השם סלפים. "בוקו חראם" מציג אידיאולוגיה מגובשת, ועבור חלק מהמוסלמים גם אותנטיות משכנעת, בשל השימוש שהוא עושה בטקסטים מוסלמיים קאנוניים. לדוגמה, ידוע כי חסידי "בוקו חראם" מושפעים מהביטוי בקוראן הקורא לפנאטיות ולמחויבות טוטאלית (ראו השערה 3): "כל מי שאינו מציית לדבריו של אללה נמנה על הפושעים".[38] חברי הארגון רואים זאת כחובתם וכמטרתם להיות מעורבים במאבק אלים נגד "אויבי האסלאם", הן בארצם והן מחוצה לה. הם רואים בהפלת הממשלות החילוניות פעולה מוצדקת, מכיוון שהשליטים שם נתפסים כמי שמסכימים או נוטים לדרכם של אויבי האסלאם.

"בוקו חראם", כפי שמעיד שמו, מתנגד נחרצות למה שהוא רואה כפלישה מערבית שהורסת את המסורת והערכים של הקהילות המוסלמיות בצפון ניגריה. המנהיג הראשון של הארגון, מוחמד יוסוף, אמר בראיון ל־BBC ב־2009: "השכלה בסגנון מערבי מכניסה נושאים הסותרים את האמונה שלנו באסלאם".[39] במקום אחר טען המנהיג הכריזמטי של הארגון: "אדמתנו הייתה מדינה מוסלמית לפני שהאדונים הקולוניאליסטיים הפכו אותה לאדמת כָּאפיר (כופרים). המשטר הנוכחי מנוגד לאמונה האסלאמית האמיתית".[40] לכן, "בוקו חראם" מציג עצמו בברור כארגון עם מטרות המתנגדות למודרניות, ומבקשות להחזיר את החברה לימי העבר הנתפסים כאידיאליים (ראו השערה 1).

"בוקו חראם" הפך לארגון אולטרה קיצוני ב־2009, בעקבות עימותים בינו לבין גופי הביטחון המקומיים במדינת בָּאוצ'י שבניגריה. כוחות הביטחון עסקו באכיפת חוק חדש שחִייב אופנועים בכל רחבי המדינה לחבוש קסדות. העימות האלים החל בתהלוכת לוויה של "בוקו חראם" במָיידוגוּרִי, לאחר שחברי הארגון האבלים לא קיימו את חוק חבישת הקסדה. אנשי ביטחון, שנמנו על כוח משימה מיוחד למלחמה בשוד שהורכב מאנשי משטרה וצבא, פתחו באש על משתתפי הלוויה והרגו 17 מהם. מוחמד יוסוף תבע עשיית צדק, אבל "הרשויות לא חקרו את השימוש המוגזם בכוח ולא התנצלו על הירי".[41] ב־21 ביולי 2009 פשטו כוחות הביטחון על מקום המסתור של הארגון בבאוצ'י והחרימו חומרים להכנת מטעני חבלה.

בעקבות הפעולה נגדו החליט "בוקו חראם" לעבור למתקפות נקמה. ב־26 ביולי העלו חברי הארגון באש תחנת משטרה בדוּנְגֶ־טָנְשִי שבפאתי באוצ'י. בפעולה נהרגו חמישה מחברי הארגון, וכמה מקציני המשטרה נפצעו קשה. בתגובה פשטו המשטרה והצבא על מסגד ובית בבאוצ'י, שם התכנסו חברי הארגון, והרגו עשרות מחבריו. המשטרה דיווחה כי 52 מחברי הארגון, וכן שני קציני משטרה וחייל,

נהרגו בתקרית האלימה. יוסוף נשבע להשיב מלחמה, כשהוא מצהיר שהוא מוכן להילחם עד מוות כדי לנקום את הרג חבריו. נאמן להבטחתו, הוא הוביל את אנשיו במתקפות מתואמות ברחבי מיידוגורי, כשהם תוקפים תחנות משטרה ובתים של קציני משטרה, לרבות כאלה שפרשו. כמו כן, הם הציתו כנסיות ופשטו על הכלא המרכזי, כשהם משחררים אסירים והורגים את הסוהרים.

בתגובה לכך הוקף ב־28 ביולי המתחם של יוסוף על ידי חיילי צבא ניגריה. רבים מאנשיו נאסרו ולפחות כמה עשרות מהם נהרגו כשהיו כבר בידי המשטרה.[42] ב־29 ביולי פשטו כוחות הביטחון שוב על מקום מסתור של הארגון בפאתי העיר והרגו לפחות 43 מאנשיו של יוסוף.

המהומות שכחו זמנית לאחר שכוחות הביטחון הניגריים לכדו והרגו את מוחמד יוסוף עצמו וכאלף מאנשיו. מותם של יוסוף ושל רבים מחברי "בוקו חראם" דחף את התנועה לשנות את המבנה שלה לכדי רשת של תאים מחתרתיים עם מנהיגות סמויה. מצב זה הפך כל פתרון צבאי של בעיית הטרור של "בוקו חראם" לאשליה.[43] התנועה הייתה רדומה כשנה, ואז הגיחה מחדש ב־2010 עם מתקפות מתוחכמות יותר, שלפי ההשערה נתמכו על ידי ארגוני ג'יהאד עולמי, כמו "אל־קאעידה" באזור המגרב, "אל־שבאב" בסומליה, "קרן אל־מונתדה" וארגון "החברה האסלאמית העולמית". הפנייה לאלימות מצד ממשלת ניגריה כדי לעצור את האיום של "בוקו חראם" הסתיימה, אפוא, בהקצנת הארגון ובדחיפת מנהיגיו לחבור עם תנועת הגי'האד העולמי כאסטרטגיה של הישרדות.

דרך הפעולה של "בוקו חראם" התאפיינה מאז בשימוש במחבלים מתאבדים וברוצחים על אופנועים, שהרגו שוטרים, פוליטיקאים, וכן כל מי שיצא נגדם, לרבות איש דת מוסלמי שמסר מידע על מקום הימצאותם לרשויות הביטחון. ב־2012 יצא "בוקו חראם" למספר מתקפות נגד קציני משטרה, כשהוא תובע לשחרר את כל האסירים חברי הארגון ולהעמיד לדין את האחראים להרג מנהיגו.[44] ביוני ובאוגוסט 2011 פוצצו טרוריסטים של הארגון את מטה משטרת ניגריה ומטה האו"ם בבירת ניגריה, אבוג'ה. במתקפות שביצע הארגון בעשרת החודשים הראשונים של שנת 2012 נהרגו מעל 900 איש – יותר ממספר הקורבנות בשנים 2010 ו־2011 גם יחד.[45]

ב־6 ביולי 2013 פשטה קבוצה של אנשים שנחשדו כחברי "בוקו חראם" על פנימייה במדינת יובה, בצפון־מזרח ניגריה, ושרפה למוות 29 תלמידים ומורה.[46] בעקבות הטבח הנוראי, פרסם המנהיג הנוכחי של הארגון, אבו באכֶּר שֶׁקָאוּ, סרטון וידאו בן 15 דקות ובו קריאה לבצע מתקפות דומות. תוך שהוא חוזר על עמדת הארגון המתנגדת לדמוקרטיה ולקִדמה (ראו השערה 1), הצהיר שקאו בסרטון באופן שאינו משתמע לשתי פנים: "הקוראן מלמד שעלינו להתרחק מדמוקרטיה, מהחוקה ומהחינוך המערבי". ואכן, במרחץ הדמים האחרון, שהיה במדינת בּוֹרנוֹ, רצחה קבוצה של אסלאמיסטים, כפי הנראה חברי "בוקו חראם", 44 מתפללים

במסגד. מקרים אלה מעידים על טיבה של האלימות חסרת ההבחנה שנוקטים חברי הארגון ועל היעדר כל מגבלה מוסרית מצדם (ראו השערה 2).

"בוקו חראם" והג'יהאד העולמי

אחת מהשאיפות המרכזיות של ארגון "בוקו חראם" היא להפוך לשחקן מרכזי בג'יהאד העולמי, שהמלחמה לקידומו מתנהלת בידי ארגוני טרור על־לאומיים, כמו "אל־קאעידה" על סניפיו במאלי ובכל אזור הסאהל, ו"אל־שבאב" הסומלי. האוכלוסייה המוסלמית באפריקה, הצומחת במהירות, הפכה ליעד לגיוס לארגוני הג'יהאד, וחלקים מהסאהל הפכו למקלט בטוח לגורמים הקיצוניים של אזור המגרב. לא יהיה זה מפתיע אם "בוקו חראם" יחליט לנצל אזורים מוכי סכסוכים אלה, ולהצטרף למוג'הדין (לוחמי הג'יהאד) בארצות ערב ובמדינות נוספות, כמו צ'צ'ניה ואפגניסטן. ידוע שחברי הארגון התאמנו ביחד עם ארגון "אל־שבאב" הסומלי, ואחרים מקרבם גם לחמו במאלי לצד ארגונים המסונפים ל"אל־קאעידה". יהיה זה אימון משמעותי על המשטר המצרי ועל ישראל אם הם גם יצטרפו לארגוני ג'יהאד בחצי האי סיני.

"בוקו חראם" גם הגביר את מאמצי התעמולה שלו שנועדו להפגין סולידריות עם "אל־קאעידה" וסניפיו. ביולי 2010 פרסם מנהיג הארגון, אבו באכר שקאו, הצהרה ברשת המהללת את "אל־קאעידה", והביע את תנחומיו לתא "אל־קאעידה" בעיראק על שאיבד את אבו איוב אל־מסרי ואבו עומר אל־בגדאדי, שניים מהפעילים המובילים של הארגון שם. בסרטון וידאו נוסף, שפורסם בנובמבר 2012, הביע שקאו תמיכה מלאה בג'יהאד באפגניסטן, בפקיסטן, בקשמיר, בצ'צ'ניה, בעיראק, בערב הסעודית, בתימן, בסומליה, באלג'יריה, בלוב ובמאלי. בסרטון, שאורכו 39 דקות, נראה שקאו כשהוא נואם בערבית, קורא ללוחמי הג'יהאד "אחים" ויוצר בכך את הרושם שהוא פונה למנהיגי "אל־קאעידה" ולמשפחת הג'יהאד הרחבה.[47]

באוגוסט 2011 טען גנרל קרטר הָאם, מפקד הכוחות האמריקאיים באפריקה (AFRICOM), כי "אל־קאעידה" ו"אל־שבאב" מממנים את "בוקו חראם", וכן ששני ארגוני הטרור הגי'האדי העולמי האלה מתאמנים ביחד עם "בוקו חראם" ומסתייעים בלוחמיו. הוא תיאר זאת כ"דבר המסוכן ביותר שיכול להתרחש, לא רק לאפריקנים, אלא גם לנו".[48] בנובמבר אותה שנה אמר סגן שר החוץ של אלג'יריה, עבד אל־קאדר מֶסאהל, כי "אין ספק שמתקיים תיאום בין 'בוקו חראם' לבין 'אל־קאעידה'", כשהוא מצטט דוחות מודיעין ומתייחס לשיטות פעולה משותפות.[49]

שינוי משמעותי ביעדים האידיאולוגיים והאסטרטגיים של "בוקו חראם" ניתן לראות בפיצוץ מכונית התופת בבניין האו"ם באבוג'ה על ידי מחבל מתאבד ב־2011. זו הייתה הפעם הראשונה שהארגון תקף מטרה שבמובהק אינה ניגרית, וזאת בעקבות מתקפות של "אל־קאעידה" על יעדים של האו"ם באלג'יריה ומתקפות של

"אל־שבאב" על מתקני האו"ם בסומליה.[50] ב־24 בנובמבר 2012 אישר דובר הארגון, אבו אל־קעקע, את החשד: "נכון שיש לנו קשרים עם אל־קאעידה. אנחנו עוזרים להם והם עוזרים לנו".[51] הארגון גם אישר את קשריו עם סומליה. בהצהרה שכנראה פורסמה מטעם הארגון: "בקרוב מאד נצא במלחמת ג'יהאד [...] אנחנו מבקשים להודיע לכל שהגי'האדיסטים שלנו הגיעו לניגריה מסומליה, שם קיבלו אימון אמיתי בלוחמה מהאחים שלנו, שהפכו את המדינה לבלתי ניתנת לשליטה [...] הפעם המתקפות שלנו יהיו חזקות ורחבות יותר מבעבר".[52] מאז הגביר הארגון את פיגועי ההתאבדות בניגריה, שמספרם הגיע לפחות ל־19 פיגועים ביעדים שונים, לרבות כנסיות, מסגדים, בתי בירה, מערכות עיתונים, פקידי ממשלה וכוחות הביטחון.[53]

ב־2012 הוסיף משרד החוץ האמריקאי את מנהיג "בוקו חראם", שקאו, לרשימת הטרוריסטים המבוקשים. לאחרונה הכריזה ארצות הברית על פרס בסך שבעה מיליון דולר עבור לכידתו, כשהיא מציבה אותו בכך בין מנהיגי הג'יהאד המבוקשים ביותר.[54] ארבעה מנהיגים נוספים של "אל־קאעידה" באפריקה נכללו גם הם ברשימת המבוקשים שתמורתם יינתן "פרס למען עשיית צדק". משרד החוץ האמריקאי ציין ש"בוקו חראם" וסניף "אל־קאעידה" בתימן ובערב הסעודית משתפים פעולה במטרה "לחזק את היכולת של 'בוקו חראם' להוציא לפועל מתקפות טרור".[55]

אם "בוקו חראם" יחליט להגביר את פעילותו העולמית מעבר לגבולות ניגריה, הוא יציב בכך איום ממשי על יעדים נוספים של הג'יהאד העולמי. כפי שהוזכר לעיל, חצי האי סיני ושדה הקרב בסוריה עשויים להפוך אז לסיבה לדאגה למדינות השכנות.

תגובת ניגריה

ג'פרי סיאול אמר פעם כי "דת היא לא הסיבה לסכסוך דתי, אבל עבור רבים היא מספקת את קו השבר שלפיו נחלקות הזהות הקבוצתית והתחרות על המשאבים".[56] בהקשר זה יש לראות את העובדה שהרוב המכריע של האוכלוסייה בניגריה חי בעוני (75 אחוזים מתושבי הצפון, בהשוואה ל־27 אחוזים מתושבי הדרום הנוצרי) – אחד הגורמים לתופעות ההתמרדות האלימה במקום, כמו של "בוקו חראם". על פי דוח עדכני של "Human Rights Watch" על צפון ניגריה, אבטלה, היעדר הזדמנויות כלכליות וחוסר שוויון בחלוקת העושר הם מקור לתסכול עמוק בחלקים של הצפון המוסלמי.[57] היקף הקיפוח היחסי בצפון ניגריה הוביל כמה חוקרים לטעון כי "ממדים דתיים של העימות הובנו בצורה שגויה כאילו הם המניע העיקרי לאלימות, בעוד שלמעשה, השורש לכך הוא שלילת זכויות אזרח וחוסר שוויון".[58]

אין להטיל ספק במיומנות שבה "בוקו חראם" ניצל את הנסיבות הקיימות של קיפוח יחסי ועוול פוליטי בצפון ניגריה כדי לקדם את חזונו להפוך את ניגריה

למדינה אסלאמית הפועלת לפי חוקי השריעה. לצד זאת, טענתי היא שיש לזהות את שורשי המפנה שעשה הארגון לעבר אלימות קיצונית באירוע של חיסול מנהיגו, מוחמד יוסוף, ללא משפט, וכן בפעולות המתמשכות של מאסרים שרירותיים, עינויים והרג של חברי הארגון בידי כוחות הביטחון הניגריים. עד 2009, "בוקו חראם" נתפס כארגון רדיקלי, אך לא כאולטרה־אלים.[59] חיסול מייסדו של "בוקו חראם" בעודו תחת חסות המשטרה הצית תגובה עזה בקרב חברי הארגון, שהפכו את יישוב החשבון עם המשטרה והצבא למטרתם העיקרית.[60] בסרטון וידאו שפורסם ביוני 2010, נשבע אבו באכר שקאו, מנהיג הארגון שהחליף את מוחמד יוסוף, לנקום את מותם של חבריו. בסרטון האופייני לסגנון של "אל־קאעידה" איים שקאו: "אל תחשבו שהג'יהאד נגמר, הוא רק התחיל".[61] אין זה, לפיכך, צירוף מקרים שבין ינואר לספטמבר 2012, לפחות 119 קציני משטרה ניגריים קיפחו את חייהם במתקפות שנחשדו כפעולות של "בוקו חראם" – כאמור, יותר מאשר בכל 2010 ו־2011 ביחד.[62]

כיצד הגיבה ממשלת ניגריה לפעולותיו של "בוקו חראם"? ניתן לזהות שתי גישות מרכזיות בתגובתה: פיוס וכפייה. הגישה הפייסנית, שהיא נדירה לממשלה הניגרית, כללה משא ומתן פוליטי עם כל המעורבים בעימות עם "בוקו חראם". גישת "הגֶזר" ברמת המדינה הייתה בהיקף קטן, ננקטה לעתים רחוקות מדי, ועירבה ניסיונות של הידברות והתקרבות לאנשי הארגון המורד. במסגרת ניסיון ראוי לציון שנעשה לאחרונה לשאת ולתת עם הארגון, הקים הנשיא ג'ונתן ועדת חנינה בת 26 חברים, שנועדה לקיים "דיאלוג ופתרון בדרכי שלום לאתגרי הביטחון בצפון". הוועדה, שכללה פקידי ממשלה לשעבר ובהווה, אנשי דת ופעילי זכויות אדם, קיבלה שלושה חודשים כדי לנסות ולשכנע את חברי הארגון להניח את נשקם בתמורה לחנינה מהמדינה ולהשתלבות בחברה.[63] ראש הארגון, שקאו, הגיב להפצרות של הממשלה הניגרית שיבקש חנינה באומרו שארגונו לא ביצע כל פשע, ולכן אין לו צורך בחנינה. שקאו טען שהממשלה הניגרית היא זו שביצעה פשעים נגד המוסלמים, ובמילותיו: "למרבה ההפתעה, הממשלה הניגרית מדברת על הענקת חנינה לנו. איזה פשע עשינו? להיפך, אנחנו אלה שצריכים להעניק לכם חנינה".[64] שקאו נשבע שלא לעצור את הג'יהאד של ארגונו להקמת מדינה אסלאמית בניגריה שתפעל תחת חוקי השריעה.[65]

פחות משבוע לאחר ש"בוקו חראם" דחה את הצעת החנינה של ממשלת ניגריה ונאמן לשבועתו ביצע הארגון שתי מתקפות אלימות בזו אחר זו בצפון המדינה. בראשונה הטילו אנשי הארגון מצור על העיר בָּאמָא שבמדינת בורנו, כשהם הורגים 55 בני אדם, רובם אנשי משטרה וביטחון, ומשחררים יותר ממאה אסירים מהכלא. כמה ימים לאחר מכן הרג הארגון 53 בני אדם והעלה באש 13 כפרים במרכז ניגריה.[66] לנוכח פרץ האלימות הקשה הכריז הנשיא ג'ונתן על מצב חירום

בשלוש מדינות הצפון – בורנו, אָדָמָאווָה ויוּבּה – שם היה הארגון פעיל ביותר, וזאת בניסיון להחזיר את הסדר על כנו ולהוציא את השליטה מידי הטרוריסטים.[67] לפי ג'ונתן, "אנו ניצבים לא רק בפני מיליטנטיות ופשיעה, אלא מול מרד מצד ארגוני הטרור, מה שמציב איום חמור ביותר על האחדות הלאומית ועל השלמות הטריטוריאלית שלנו".[68] הנשיא נשבע "לנקוט כל פעולה נדרשת [...] כדי לשים קץ למורדים ולטרוריסטים שחומקים מעונשם".[69] לשם כך, הקימה ממשלת ניגריה "כוח משימה צבאי משותף מיוחד" שזכה לשם "מִבצע להשבת הסדר", שהופקד על מרדף ולכידה של חברי הארגון ואיתור מקומות המסתור שלהם.

אין זו הפעם הראשונה שממשלת ניגריה מכריזה על מצב חירום כתוצאה ממתקפות "בוקו חראם". בעקבות שרשרת פיגועים שביצע הארגון בצפון ניגריה בסוף 2011, הכריז הנשיא ג'ונתן על מצב חירום שהִשעה זכויות חוקתיות ב־15 אזורים בארבע מדינות צפוניות. מצב החירום נכשל כישלון חרוץ במטרתו לעצור את גל האלימות באזור וכמוהו נכשלו תקנות הכפייה שפורסמו באפריל 2012, אשר העניקו לכוחות הביטחון סמכויות חירום לפעול לחיסול האיום של "בוקו חראם". למעשה, במהלך ששת החודשים של מצב החירום הוציא הארגון לפועל יותר מתקפות והרג יותר אנשים מאשר בשנים 2010 ו־2011 גם יחד.[70] ההעדפה שנתנה ממשלת ניגריה לפתרון הצבאי אינה מפתיעה, אם זוכרים את דבריו של איש מדע המדינה הניגרי המנוח, פרופ' קלוד אָקֶה: "המצב הפוסט־קולוניאלי בניגריה הפך יותר מדי פעמים לכלי לאלימות, מכיוון שהבסיס שלו בכוחות החברתיים נותר חלש מאד והוא נשען יותר מדי על כפיית הציות במקום על סמכות".[71]

בהיערכות הצבאית הגדולה ביותר בניגריה מאז מלחמת האזרחים של השנים 1967–1970, הורתה הממשלה הפדרלית להעביר כ־8,000 חיילים לאזור הצפון מוכה הטרור, כחלק ממתקפה צבאית נגד "בוקו חראם". עוצר הוטל על מיידוגורי, ו"כוח המשימה הצבאי המשותף" נעזר במתקפות אוויריות לתקיפת מעוזי הארגון. כמו כן הוטל מצור על הבסיס הוותיק של הארגון במיידוגורי במטרה לשקם את "השלמות הטריטוריאלית"[72] של ניגריה. עם זאת, פעמים רבות מדי הואשמו אנשי "כוח המשימה הצבאי המשותף" בהרג אנשים חפים מפשע בשם מיגור הטרור. לדוגמה, במדינת בורנו ביצעו אנשי הכוח הרג לא חוקי, מעצרים המוניים והפחדות של תושבי בורנו חסרי האונים.[73] פעולת אנשי הכוח לא הייתה מבוססת על מודיעין, ובסופו של דבר הוא פשוט כיתר אזורים וביצע חיפושים מבית לבית, כשלפרקים הוא ירה בצעירים שהתגוררו באותם בתים.[74] הפשיטות הפכו כה תכופות, עד שהורים ביקשו מבניהם לברוח כל אימת שהתרחשה מתקפת טרור. לאחר סדרת ראיונות מדגמיים עם תושבים במיידוגורי, דיווח ארגון Human Right Watch: "במהלך הפשיטות, חיילים שרפו בתים, חנויות ומכוניות, עצרו באקראיות גברים, ובחלק מהמקרים ירו בהם למוות בפתח החנות או הבית שלהם".[75]

בחילופי אש שאירעו לאחרונה בין חיילי "כוח המשימה הצבאי המשותף" ובין אנשי "בוקו חראם" בבָּגָה, ליד גבול ניגריה עם קמרון, נהרגו 187 בני אדם ו־77 נוספים נפצעו, אולם תושבי בָּגָה האשימו את חיילי הכוח ולא את אנשי הארגון בירי חסר הבחנה לעבר אזרחים ובהצתת אש במוקדים רבים בעיירת הדייגים ההיסטורית.[76]

רק לעתים נדירות העמידו הרשויות הניגריות למשפט חיילים על פשעים נגד אזרחים. אחת הבעיות של השימוש בצבא ובמשטרה בצפון ניגריה היא שמדובר בכוחות לאומיים ולא מקומיים. פירוש הדבר הוא שהחיילים הפועלים בצפון המדינה לא חולקים רקע תרבותי ואתני עם האוכלוסייה המקומית.

לאחרונה פרסם שר החוץ של ארצות הברית, ג'ון קרי, הצהרה חריפה: "אנו [...] מודאגים מאד מהאשמות מבוססות לפיהן כוחות הביטחון הניגריים מבַצעים הפרות בוטות של זכויות אדם, שבתורן רק מסלימות את האלימות ומזינות את הקיצונים".[77] יש לזכור, עם זאת, כי ארצות הברית עצמה אינה אמינה בצורה כזו המאפשרת לה להיות "מודאגת מאד" מהשימוש באלימות ומהפרות זכויות אדם בניגריה, וזאת לאור העובדה שהיא ממשיכה ליישם אסטרטגיה דומה ב"מלחמה העולמית בטרור" שהיא מנהלת במזרח התיכון ובאזורים נוספים.[78]

טענָתי היא שמדינות הנלחמות בטרור מחוץ לגבולותיהן, כמו ארצות הברית, בריטניה וצרפת, צריכות ללמוד מהניסיון הניגרי של המלחמה ב"בוקו חראם" ולהבין כי "הכרזת מלחמה על הטרור" היא מלחמה שאין לה סוף, מלחמה שרק מזינה מעגל אכזרי של טרור נוסף. גישה צבאית למלחמה בטרור, המונעת על ידי שיקולי ביטחון בלבד, לא רק שמתעלמת מתרבות ואורח חיים דמוקרטיים, אלא גם מקצינה עוד את ארגוני הטרור הדתיים ומחזקת את הנחישות הקולקטיבית של החברים בהם, שאינם צפויים להתפשר (שכן פשרה היא בגידה באמונותיהם). באופן דומה, איומים באלימות או במאסר כמעט שאינם מרתיעים, כפי שעולה מהצהרה של מנהיג "בוקו חראם": "מאז שפתחנו במלחמה מתמשכת זו, שהם קוראים לה מצב חירום [...] היו מקרים שחיילים שעמדו מולנו הסתובבו לאחור וברחו".[79] טענתו של שקאו כי ידו של ארגונו היא על העליונה עומדת בניגוד להצהרת ממשלת ניגריה, לפיה "כוח המשימה הצבאי המשותף" מנצח במלחמה בטרור.

בסיכומו של דבר, מדינות הנלחמות בטרור חייבות ללמוד כי להכרזת מלחמה עליו יש יכולת מוגבלת בלבד לגרום לשינוי ממשי, מכיוון שהיא "אף פעם לא תוכל להתמודד עם התנאים המביאים גורמים [דוגמת 'בוקו חראם'] לדחות את הסֵדר הקיים ולפתח עמדות קיצוניות, או לבחור להשתמש באלימות מלכתחילה".[80] המלחמה העולמית בטרור עתידה להשיג "ניצחון פירוס", שרק יערער עוד יותר את סמכות הממשל, יגביר את הגיוס לארגוני הג'יהאד הקיצוני ואת התפשטותם

באפריקה, וסופו שיגרום להם לצבור עוצמה רבה יותר, כפי שמלמד המקרה של "בוקו חראם".

מאז עצמאותה, חסרה ניגריה תפיסה בת־קיימא של אסטרטגיה למלחמה בטרור – דוקטרינה שתנחה את פעולות המדינה, תסייע לשבש את גיוס הטרוריסטים ותשנה את הסביבה שבה הם מתגוררים לְסביבה שבהדרגה לא תאפשר להם לפעול. מדיניות ניגרית אפקטיבית למלחמה בטרור אינה יכולה להסתפק באסטרטגיה של הרג המונעת משיקולי ביטחון בלבד, אלא עליה להטמיע את המלחמה בטרור באסטרטגיית ביטחון לאומי מקיפה, כזו שרואה את ההקשר הרחב שבו פועל האסלאם הרדיקלי וחותרת לשנות אותו בצורה מהותית ובלתי אלימה. במילים אחרות, ניגריה חייבת לנטוש את המדיניות הביטחונית שהופכת את המלחמה בטרור לפריזמה שדרכה נשפט ונקבע הכל.

אסטרטגיה ארוכת טווח, שתפחית את הסיכוי של חברות מוסלמיות להפוך לחממות לקיצונים ותחליש את המשיכה לג'יהאד, חייבת להשתמש בכוח באופן מצומצם ואחראי. עליה לכוון למתן מענה לצרכים אנושיים בסיסיים, בכך שתציע פיתוח, ביטחון וכיבוד זכויות אדם. העוני והאבטלה בצפון המוסלמי, לצד הגידול באוכלוסייה וחוסר היכולת של הממשלה להתמודד ביעילות עם גורמים לא מדינתיים, עלולים להפוך את הפרובינציות הצפוניות של ניגריה לקרקע פורייה לגיוס אנשים לארגוני ג'יהאד עולמיים כמו "אל־קאעידה" ו"אל־שבאב". לבסוף, כדי להתמודד טוב יותר עם הטרור המקומי של "בוקו חראם" ושאיפותיו הגלובליות, יש צורך באסטרטגיה מבוססת־מודיעין. בנוסף, יש צורך בשיתוף פעולה בין־לאומי רב יותר, שיאפשר זיהוי והצלבת מידע לאיתור מקורות המימון החיצוניים של "בוקו חראם", מקורות ההצטיידות שלו בנשק ואימוניו, שהם מרכיבים מכריעים ביכולותיו המבצעיות.

הערות

1 Daniel E. Agbiboa, "Living in Fear: Religious Identity, Relative Deprivation and the Boko Haram Terrorism", *African Security* 6, no. 2, 2013, pp. 153-170.

2 Human Rights Watch, "Spiralling Violence: Boko Haram Attacks and Security Forces Abuses in Nigeria", October 4, 2013, http://www.hrw.org/sites/default/files/reports/nigeria1012webwcover.pdf

3 Alex Schmid, *Political Terrorism: A Research Guide to Concepts, Theories, Data Bases and Literature*, Amsterdam: North-Holland, 1983, pp. 70-111.

4 R.F. Young, "Revolutionary Terrorism, Crime and Morality", *Social Theory and Practice* 4, no. 3, 1977, p. 288.

5 OAU 1999, cited in: Daniel E. Agbiboa, "(Sp)oiling Domestic Terrorism? Boko Haram and State Response", *Peace Review: A Journal of Social Justice* 25, no. 3, 2013, pp. 431-432.

6 Gregory D. Miller, "Confronting Terrorisms: Group Motivation and Successful State

Policies", *Terrorism and Political Violence* 19, 2007, pp. 332-333.

7 Human Rights Watch, "Spiralling Violence".

8 William O'Brien, "Israel's Counterterror Strategies, 1967-1987", *Middle East Review* 20, 1987, pp. 23-30; Reuben Miller, "Responding to Terrorism's Challenge: The Case of Israeli Reprisals", *Virginia Social Science Journal* 25, 1990, pp. 109-123.

9 שם.

10 Miller, "Responding to Terrorism's Challenge".

11 Daniel Benjamin, "Strategic Counterterrorism", *Foreign Policy at Brookings*, Policy Paper 7, October 2008, pp. 1-17.

12 Miller, "Confronting Terrorisms".

13 שם.

14 Ada Aharoni, "Nonkilling Global Society", in: Ada Aharoni (ed.), *Peace Building*, Oxford: UNESCO and Eolss Publishers, 2005.

15 Glenn D. Paige, *Nonkilling Global Political Science*, Honolulu, Hawaii: Center for Global Nonkilling, 2009, p. 1.

16 שם.

17 Benjamin, "Strategic Counterterrorism", p. 7.

18 David Rapoport, "Fear and Trembling: Terrorism in Three Religious Traditions", *American Political Science Review* 78, no. 3, 1984, pp. 658-677.

19 Mark Juergensmeyer, *Terror in the Mind of God: The Global Rise of Religious Violence*, California, Berkeley: University of California Press, 2003, p. 121.

20 Scott R. Appleby, *The Ambivalence of the Sacred: Religion, Violence and Reconciliation*, New York: Littlefield, 2001, p. 7.

21 Bruce Hoffman, *Inside Terrorism*, New York: Columbia University Press, 2006, pp. 88, 272.

22 Audrey Cronin, "Behind the Curve: Globalisation and International Terrorism", *International Security* 27, no. 3, 2003, p. 38.

23 Juergensmeyer, *Terror in the Mind of God*, p. 230.

24 Jeroen Gunning and Richard Jackson, "What's so 'Religious' about 'Religious Terrorism?'", *Critical Studies on Terrorism* 4, no. 3, 2011, pp. 369-388.

25 Matthew Morgan, "The Origins of the New Terrorism", *Parameters* 34, no. 1, 2004, pp. 30-31.

26 Daniel L. Byman, "Al-Qaeda as an Adversary: Do We Understand our Enemy?", *World Politics* 56, no. 1, 2003, p. 147.

27 Benjamin, "Strategic Counterterrorism", p. 2.

28 Hoffman, *Inside Terrorism*, p. 88.

29 Juergensmeyer, *Terror in the Mind of God*, pp. 149-150.

30 Gunning and Jackson, "What's so 'Religious' about 'Religious Terrorism?'".

31 Magnus Ranstorp, "Terrorism in the Name of Religion", *Journal of International Affairs* 50, no. 1, 1996, p. 54.

32 Gunning and Jackson, "What's so 'Religious' about 'Religious Terrorism?'".

33 Juergensmeyer, *Terror in the Mind of God*, p. 220.

34 Hoffman, *Inside Terrorism*, pp. 197-228, 288-290.

35 *Daily Trust*, April 25, 2011.

36 John Campbell and Asch Harwood, "Nigeria's Challenge", *The Atlantic*, June

24, 2011, http://www.theatlantic.com/international/archive/2011/06/nigeria-challenge/240961/.

37 Sani Umar, *The Discourses of Salafi Radicalism and Salafi Counter-Radicalism in Nigeria: A Case-Study of Boko Haram*, Evanston, IL: Northwestern University, 2011.

38 Alex Thurston, "Threat of Militancy in Nigeria", Commentary for Carnegie Endowment for International Peace, September 1, 2011, http://carnegieendowment.org/2011/09/01threat-of-militancy-in-nigeria/4yk8.

39 "Nigeria's 'Taliban' Enigma", *BBC News Africa*, July 31, 2009, http://news.bbc.co.uk/2/hi/8172270.stm.

40 "Nigeria: Boko Haram Sect Leader Ustaz Mohammed Vows Revenge", *Daily Trust*, July 27, 2009, http://www.nairaland.com/302352/islamists-yar-adua-want-total/6.

41 Human Rights Watch, "Spiraling Violence", p. 33.

42 שם.

43 Roland Marchal, "Boko Haram and the Resilience of Militant Islam in Northern Nigeria", NOREF Report, July 13, 2012, p. 3.

44 Daniel E. Agbiboa, "No Retreat, No Surrender: Understanding the Religious Terrorism of Boko Haram in Nigeria", *African Study Monograph* 34, no. 2, 2013, pp. 65-84.

45 Human Rights Watch, "Spiraling Violence".

46 נראה שהמתקפה הלא מוצדקת על ילדים היא חלק מהניסיון להחליש את הבסיס ההשכלתי של הצפון, לאור הבוז של הארגון כלפי השכלה מערבית. ראו:
Monica Mark, "Boko Haram Leader Calls for More School Attacks after Dorm Killings", *The Guardian*, July 15, 2013, http://www.guardian.co.uk/world/2013/jul/14/boko-haram-school-attacks-nigeria.

47 Bill Roggio, "Boko Haram Emir Praises Al-Qaeda", *The Long War Journal*, November 30, 2012.

48 "Boko Haram: Nigeria's growing new headache", *Strategic Comments*,Volume 17, Issue 9, December 2011, pp. 1-3.

49 שם, עמ' 2–3.

50 James J. Forest, *Confronting the Terrorism of Boko Haram in Nigeria*, Florida: The JSOU Press, 2012, p. 130.

51 Farouk Chothia, "Who are Nigeria's Boko Haram", *BBC News Africa,* August 26, 2011, http://www.bbc.co.uk/news/world-africa-13809501.

52 Katherine Zimmerman, "From Somalia to Nigeria: Jihad", *The Weekly Standard*, June 18, 2011, http://www.weeklystandard.com/keyword/somalia.

53 Bill Roggio, "Boko Haram Suicide Bombs Kill 11 at Nigerian Military Church", *The Long War Journal*, November 25, 2012, http://www.longwarjournal.org/archives/2012/11/boko_haram_suicide_b.php.

54 Bill Roggio, "US Offers Rewards for Boko Haram, African Al-Qaeda's Leaders", *The Long War Journal*, June 4, 2013, http://www.longwarjournal.org/archives/2013/06/us_offers_rewards_fo.php.

55 שם.

56 Jeffrey R. Seul, "Ours is the Ways of God: Religion, Identity and Intergroup Conflict", *Journal of Peace Research* 36, no. 5, 1999, p. 553.

57 Human Rights Watch, "Spiraling Violence".
58 Chris Kwaja, "Nigeria's Pernicious Drivers of Ethno-Religious Conflicts", *Africa Security Brief*, June 28, 2011, p. 1.
59 Freedom Onuoha, "Boko Haram: Nigeria's Extremist Islamic Sect", *Al Jazeera Center for Studies* 29, no. 2, 2012, p. 2.
60 Marchal, "Boko Haram and the Resilience of Militant Islam", p. 2.
61 שם.
62 שם.
63 שם.
64 Nick Chilles, "After Rejecting Nigeria's Amnesty Offer: Boko Haram Continues to Kill", *Atlanta Blackstar*, http://atlantablackstar.com/2013/04/23/after-rejecting-nigeria-amnesty-offer-boko-haram-continues-to-kill.
65 שם.
66 שם.
67 Agbiboa, "No Retreat, No Surrender".
68 שם, עמ' 65.
69 שם, עמ' 66.
70 Human Rights Watch, "Spiraling Violence".
71 Claude Ake C.F.,"The New World Order: A View From the South", Malthouse Press Limited",Lagos, 1992, p. 155.
72 Agbiboa, "No Retreat, No Surrender".
73 Human Rights Watch, "Spiraling Violence".
74 שם, עמ' 9.
75 שם, עמ' 60.
76 Chilles, "After Rejecting Nigeria's Amnesty Offer".
77 "Nigerian Forces Shell Fighter Camps", *Al Jazeera*, May 17, 2013, http://www.aljazeera.com/news.africa/2013/05/20135171163037848.html.
78 Benjamin, "Strategic Counterterrorism", p. 1.
79 "Boko Haram: We're Winning War against Nigerian Army", Press TV, July 25, 2013, http://www.presstv.com/detail/2013/05/29/305978/boko-haram-were-winning-war-in-nigeria/.
80 Human Rights Watch, "Spiraling Violence", p. 240.

מדיניות הכלה מחודשת ומתוחכמת – ניהול וצמצום מלחמות ועימותים אלימים בעולם

אנדראס הרברג־רות'

מאמר זה יציג את השערתי, לפיה מניעת איראן מהשגת נשק גרעיני היא דבר העומד בסתירה לפרשנות הפרטנית של המושג המסורתי "הכלה". לעומת זאת, מטרת העל הפוליטית של הקהילה הבינ־לאומית צריכה להיות מדיניות הכלה חדשה ומתוחכמת, שתדע לפעול נגד מלחמות גדולות ואלימות המונית, ובכלל זה נגד התפשטותו של נשק להשמדה המונית והסלמה של סכסוכים אלימים. חשוב לזכור שאסטרטגיית ההכלה יושמה בהצלחה נגד ברית המועצות והובילה לבסוף להתפרקותה. השאלה הנובעת מכך היא: כיצד ניתן להתאים את מדיניות ההכלה המסורתית לעולם הגלובלי של ימינו?

מילות מפתח: בלימה מחודשת, הכלה מסורתית, גלובליזציה, קלאוזביץ, תיאורית המלחמה הצודקת, אסטרטגיה, הסלמה של האלימות

נשיא ארצות הברית, ברק אובמה, טען זה מכבר כי מדיניות ההכלה המסורתית אינה הגיונית ככל שהדבר נוגע לאיראן. לדבריו, מדיניותו כלפי איראן נועדה למנוע ממנה לייצר נשק גרעיני ולא רק להכיל איראן גרעינית. למרות זאת, ארצות הברית נוקטת למעשה מדיניות הכלה מסורתית כלפי סין, המעצמה העולה והצוברת הגמוניה של מזרח אסיה. מהשימוע שנערך בסנט של ארצות הברית לצ'אק הייגל לקראת אישור מינויו לשר ההגנה התברר כי עדיין קיימת אי־בהירות סביב האסטרטגיה של הממשל האמריקאי בנושא זה, אם כי קרוב לוודאי יש הסברים לאי־בהירות זאת.[1]

אנדראס הרברג־רות' הוא מרצה בפקולטה למדעי החברה והתרבות באוניברסיטה למדעים יישומיים, פולדה, גרמניה.

גרסה מוקדמת של מאמר זה ראתה אור בפרסום הבא: *A New Containment-Policy: The Curbing of War and Violent Conflict in World Society*, S. Rajaratnam School of International Studies, Singapore, May 2, 2013.

מניעת נשק גרעיני מאיראן היא לא פחות מאשר מדיניות הכלה מחודשת ומתוחכמת: בלימת הפצתו של נשק להשמדה המונית, ובמיוחד של פצצות גרעיניות. רק על בסיס של מדיניות בלימה חדשה כזאת, המכוונת לבלום מלחמות גדולות ואלימות המונית, שהשפעתן על חברות דומה להשפעת מחלת הסרטן על הגוף האנושי, ניתן יהיה למנוע מאיראן השגת פצצה גרעינית. כפי שהראה השימוע שנעשה לצ'אק הייגל, לא ניתן למנוע מאיראן את זכויותיה כחברה באומות המאוחדות, אולם ניתן לטעון, כחלק ממדיניות ההכלה החדשה, שיש למנוע מכל מדינה נוספת להשיג נשק גרעיני.

מאמר זה יציג את השערתי, לפיה מניעת איראן מהשגת נשק גרעיני היא דבר העומד בסתירה לפרשנות הפרטנית של המושג המסורתי "הכלה". לעומת זאת, מטרת העל הפוליטית של הקהילה הבין־לאומית צריכה להיות מדיניות הכלה חדשה ומתוחכמת, שתדע לפעול נגד מלחמות גדולות ואלימות המונית, ובכלל זה נגד התפשטותו של נשק להשמדה המונית והסלמה של סכסוכים אלימים. חשוב לזכור שאסטרטגיית ההכלה יושמה בהצלחה נגד ברית המועצות והובילה לבסוף להתפרקותה. השאלה הנובעת מכך היא: כיצד ניתן להתאים את מדיניות ההכלה המסורתית לעולם הגלובלי של ימינו?

אנו עדים להסלמה כלל עולמית במלחמות ובאלימות, שכדי לעמוד נגדה יש ליצור הכלה מסוג חדש. כבר ב־1987 הדגיש זאת ג'ורג' קֶנאן: "מסיבות אלו מוטל עלינו לפתח תפיסה רחבה יותר של משמעות המושג הכלה [...] במילים אחרות – תפיסה הקשובה יותר לבעיות בנות זמננו מאשר זו שביטאתי בזמנו בביטחון כה רב [...] בדצמבר 1946".[2] שישים שנה חלפו מאז שג'ורג' קנאן ניסח את חזונו המקורי לגבי סוגיית ההכלה. למרות שהרעיון המקורי שלו עתיד היה להשתנות במהלך יישומו על ידי ממשלים אמריקאיים שונים, הוא הוטמע בפועל בתפיסה ובמדיניות הביטחון, כהשלמה חיונית למדניות ההכלה הצבאית.[3] רעיונות אלה עדיין תקפים, אך כפי שקנאן עצמו ציין, הצורך בפרשנות וביישום חדשים שלהם גדול מאי פעם, בייחוד בעקבות ההתפתחויות בעיראק ובאפגניסטן, אותן קנאן לא יכול היה לחזות, שהוכיחו כי השגת ניצחון מסורתי על היריב אינה ישימה בעולם הגלובלי של ימינו.[3] במקום אסטרטגיות אלה שזמנן עבר, אנו זקוקים לאסטרטגיה המתמקדת בהמרת הצלחות והישגים צבאיים בהסדר מדיני בר־קיימא.

מדיניות הכלה מחודשת זאת אינה רק אסטרטגיה כפולה. הרקע הפוליטי עליו נשענת התפיסה של הכלת מלחמות ואלימות בעולם של ימינו מורכב מחמש צלעות, שהן "הפנטגון לבלימת מלחמה ואלימות":

1. יכולת להרתיע ולרַפות את ידיו של כל יריב המבקש להילחם מלחמה בקנה מידה גדול, או לפנות לפעולה צבאית נקודתית כמוצא אחרון.

2. אפשרות להשתמש או לאיים[4] בכוח צבאי כדי להגביל ולבלום אלימות חריגה במיוחד ובקנה מידה גדול, שיש לה פוטנציאל להשמיד חברות שלמות.
3. מוכנות להתנגד לתופעות התורמות לאלימות, כמו עוני ודיכוי, במיוחד במרחב הכלכלי, וכן הכרה בפלורליזם של תרבויות וסגנונות חיים בחברה הכלל־עולמית.
4. מוטיבציה לפתח תרבות של ניהול סכסוכים אזרחיים (תפיסות שניתן לסכמן בעזרת הרעיון "המשושה האזרחי" של Dieter Senghaas, ממשל גלובלי ושלום דמוקרטי), בהתבסס על המסקנה לפיה פנייה לאמצעים צבאיים היא בלתי יעילה, וסופה למתוח עד הקצה את יכולות הצבא.
5. הגבלה על החזקה והפצה של נשק להשמדה המונית ומערכות השיגור שלו, וכן של נשק קל, וזאת מתוך הבנה שהפצת נשק מכל סוג שהוא היא הרסנית מטבעה לסדר החברתי.

הסלמת האלימות ומדיניות הכלה חדשה

דומה שבעקבות קריסת ברית המועצות לא ניתן היה לעצור את התפשטות הדמוקרטיה והשווקים החופשיים, עד שלפרקים נדמה שהמאה ה־21 צפויה להיות מאה של כלכלה, ולכן במידה רבה עידן של שלום. ציפיות אלו התבדו במהרה, לא רק בשל אירועי הטבח ורצח העם שנמשכו באפריקה שמדרום לסהרה, אלא גם בשל שובה של המלחמה לאירופה (בעיקר ביוגוסלביה לשעבר), מתקפת 11 בספטמבר 2001 בארצות הברית, ומלחמת עיראק על השלכותיה האלימות המתמשכות. נראה שהחל מאבק נגד הטוטליטריות החדשה בנוסח האסלאם, שהתפיסה הרווחת לגביה היא שלמלחמה ולאלימות יש בה תפקיד מרכזי. המלחמה והאלימות גם נתפסות כנעדרות גבולות יותר מאי פעם, הן במה שנוגע למרחב הפעולה שלהן – מתקפות טרור הן בעלות נוכחות פוטנציאלית קבועה – והן במה שנוגע למִשכן, שאין רואים את סופו. אפשר גם לדבר על ממד חדש של אלימות, הנוגע להיקפה ולאכזריותה, כפי שממחישה האלימות הקיצונית במלחמות האזרחים המתמשכות באפריקה. בנוסף, אנו ניצבים בפני סוגים חדשים לחלוטין של איומים, כמו החזקת נשק להשמדה המונית בידי ארגוני טרור או פיתוח פצצות אטום בידי מדינות "בעייתיות", כמו איראן וקוריאה הצפונית. הצמיחה הפוטנציאלית של סין כמעצמת־על חדשה ואולי של מעצמות "גדולות" חדשות, כמו הודו, עשויה להוביל למרוץ חימוש חדש, שההנחה היא שיהיה לו גם ממד גרעיני. בתודעתם של רבים, האלימות של ימינו יוצאת מכלל שליטה רציונלית – דימוי שהתקשורת לא היססה לאמץ, בייחוד ביחס לאפריקה שמדרום לסהרה.

מאז שנות התשעים של המאה העשרים טוענים כותבים שונים בעלי השפעה כי תאורית המלחמה של קלאוזביץ אינה ישימה עוד, הן ביחס לעימותים עכשוויים

והן באופן כללי. היו אף שטענו שהמשך השימוש בתיאוריה זאת כבסיס להבנת הלוחמה העכשווית וכמדריך לפעולה פוליטית יהיה מזיק ואפילו הרסני, לנוכח השינויים המהפכניים במלחמה ובאלימות ברחבי העולם. קלאוזביץ, כך נטען, עסק רק במלחמה בין מדינות המפעילות צבאות סדירים, בעוד שהעימותים כיום מערבים בעיקר גורמים שאינם מדינתיים. שתי הטענות מתעלמות הן מליבת התיאוריה של קלאוזביץ והן מהמאפיינים הייחודיים של "המלחמות החדשות". למעֵט חלק גדול של אפריקה וכמה סכסוכים ישנים מאד בשולי האימפריות לשעבר, מדינות וארגונים דתיים־פוליטיים היראכיים, דוגמת חזבאללה וחמאס, הם הרוב המכריע במלחמות גם כיום, גם אם לא היחידים. השאלה היא האם אנו עומדים, כפי שסבור קולין גריי, לפני מאה שנים נוספות של שפיכות דמים.[5]

המלחמות בעיראק ובאפגניסטן סיפקו את התובנה הנוראית, שבעולם הגלובלי של ימינו, ניצחון במערכה אינו בהכרח ניצחון במלחמה. על פי אמיל סימפסון, נקודת המוצא היא שניצחון צבאי במלחמה פירושו ניצחון ביחס לאויב, אלא שכיום ישנם קהלים שחשיבותם עולה בהדרגה על זו של האויב. הנרטיב עוסק במה שאותם קהלים חושבים לא פחות ממה שהצד הנלחם או האויב חושבים. אם הנרטיב האסטרטגי של שדה המערכה במאה ה־21 לא אמור להתמקד אך ורק בניצחון הצבאי, במה הוא אמור, אפוא, להתמקד?[6]

אני מבקש להציע שלושה נושאים שונים, אך קשורים זה בזה, להסברת הנושא: הלגיטימיות של השימוש בכוח; התנהלות המלחמה בפועל; הכרה הדדית של הקהילות הנלחמות בתום המלחמה זו בזו. קודם להסבר המפורט של הדברים, בכוונתי להבהיר את הרעיונות שבבסיסם. הצעתי נובעת בראש ובראשונה מהפרשנות שלי ל"שילוש" של קלאוזביץ, השונה למדי ממה שמכונה "מלחמה משולשת", שאינה רעיון של קלאוזביץ עצמו, אלא טיעון שהציגו הארי סאמרס, מרטין ואן קרפלד ומרי קלדור.[7] להשקפתי, כל מלחמה כוללת את שלושת המרכיבים הבאים: הכוח המופעל, המאבק או הלחימה של כוחות הצבא, והקהילה הלוחמת אליה משתייך הצבא. ניתן לייחס בקלות לשלושה היבטים פרשניים אלה שלי לקלאוזביץ את הלגיטימיות של השימוש בכוח, את אופן התנהלות המלחמה בפועל ואת ההכרה ההדדית של הכוחות הלוחמים בתום המלחמה.

הבסיס הרעיוני השני להבנת גישתי קשור למסורת של "מלחמה צודקת", אם כי בצורה שונה מכפי שהיא שולבה, למשל, ברעיון של "האחריות להגן". אנו נוהגים לעשות הבחנה במסורת של "מלחמה צודקת" בין jus in bello, jus ad bellum ו־jus post bellum. שלושה מונחים לטיניים אלה פירושם, בהתאמה, הזכות לצאת למלחמה צודקת, שמירת הזכויות והצדק במהלך המלחמה, והכוונת המלחמה לקראת שלום צודק בסיומה. השערתי היא שבעולם הגלובלי של ימינו, שלושת הנרטיבים האלה שלובים זה בזה. שתי המסורות האירופיות החשובות ביותר

להבנת משמעות המלחמה – הרעיון של "מלחמה צודקת" ושל "הזכות והצדק במהלך מלחמה" – תרמו להגבלה ניכרת של האלימות בתחילת המלחמה במקרה של "מלחמת מדינה במדינה".

על פי קארל שמיט, ההכרה באויב כשווה ערך וכבעל זכויות שוות הייתה התנאי המקדים להגבלת מלחמות בין מדינות יריבות באירופה לאחר האסון של מלחמת שלושים השנה. היו תקופות שבהן נעשה בשולי העולם האירופי שימוש בצורות לא מקובלות של כוח: במהלך מסעות הצלב של ימי הביניים ובמסעות הכיבוש הקולוניאלי במאות ה־16 עד ה־18, יריבים לא אירופיים היו יעד לא רק למלחמה, אלא גם להשמדה פיזית. בשני המקרים, הגישה האירופית הרגילה והמחייבת של שימוש בכוח, על פיה נהגו עד אז, הסתיימה באסונות.

הרעיון של "מלחמה צודקת", שתרם להגבלת המלחמה והאלימות לתקופות ארוכות בימי הביניים, הביא לבסוף לקרבות הדת של המאה ה־16 ולמלחמת שלושים השנה. השיטה האירופית של "מלחמת מדינה במדינה" ב"עידן ווסטפליה", שהתבססה על הזכות למלחמה בין יריבים שווי מעמד, ואשר במאות ה־18 וה־19 הובילה להגבלה משמעותית של האלימות המלחמתית, הביאה לאסון של שתי מלחמות העולם. לפיכך, לא ניתן לעשות אידיאליזציה של המודל האירופי של "מלחמת מדינה במדינה" רק על סמך האופן שבו הוא התממש במקור במאות ה־17 וה־18, שכן אותו מודל בדיוק (ביחד עם תיעוש המלחמה ואידיאולוגיות טוטליטריות ולאומניות חדשות) הביא, בסופו של דבר, לשתי מלחמות העולם. באותה מידה לא יהיה זה נכון לפסול את מסורת "המלחמה הצודקת" רק על סמך מלחמות הדת ומלחמת שלושים השנה. במקום זאת, ראוי לזכור את ההשפעות המרסנות והמגֵנות שהיו למסורת זו במהלך תקופות ארוכות של ימי הביניים.

הסתמכות על "מלחמה צודקת" אין פירושה עידוד אלימות צבאית, אלא דווקא מניעתה או לפחות סיוע להגבלתה. "מלחמה צודקת" מובנת רק אם היא מסווגת כמלחמה למטרות שלום. פירוש הדבר הוא שהאיום באלימות צבאית או מימושו יכולים להיות מוצדקים רק בצורה מותנית – כאמצעי למנוע, להגביל ולמתן אלימות. למרות הגדרה אידיאלית זו של "מלחמה צודקת", התעוררו שלוש בעיות מהותיות בהקשר זה במהלך ההיסטוריה: התפרצות אלימות בשל הרעיון שהמלחמה צודקת; הכתמת היריב כפושע; צמצום אפשרויות הפעולה הזמינות לכדי אמצעים אלימים בלבד, בשל הקשר המיידי בין מוסריות לפוליטיקה.

איני בטוח לחלוטין בהצעה שלהלן, ומדובר יותר בכל דבר אחר בהפרחת בלון ניסוי; אפילו הרעיון של שלום צודק לאחר מלחמה אינו נטול פגמים. לשם דוגמה, הנאצים חיפשו הרמוניה מושלמת בחברה הגרמנית, ולכן החריגו את כל מי שנראה להם כעלול לשבש את רעיון ההרמוניה המושלמת של האומה הגרמנית המאוחדת באמצעות יצירת גזע הומוגני. יתכן שביקורת זו על הרעיון של שלום

צודק לא משכנעת במבט ראשון, אבל היא חלק בלתי נפרד מכל אסטרטגיה, שבה יעדי המלחמה מקדשים את האמצעים.

אם רוצים להימנע מבעיה זו בכך שמתמקדים רק באחת משלוש התפיסות, יש לראות את בלימת המלחמה והאלימות כמטרת־על פוליטית, המוטמעת בפעולות השונות של קהילות לאומיות ובין־לאומיות. בלימת מלחמה ועימותים אלימים מבוססת על שימור איזון עדין בין שלוש המגמות.

בעשרים השנים האחרונות אנו עדים לתקוות שתלו ב"מהפכה בתחום הצבאי" (RMA) ולהופעה של מה שנראה כסוגים חדשים של לוחמה, שזכו לכינוי "המלחמות החדשות". "המהפכה בתחום הצבאי" מבטיחה להציג פתרונות טכנולוגיים מקיפים לעימותים. דומה שלוחמה ו"פעולות צבאיות שאינן מלחמות" נתפסות כלגיטימיות במקרה שהניצחון מושג בקלות. על פי ההשקפה הקלאסית, במקרה כזה העלויות יישארו נמוכות והאויב יוצג כמפר את חוקי הקהילה הבין־לאומית, כדיקטטור או כמחרחר מלחמה שתמיכת ההמונים אינה נתונה לו. כל שלוש התפיסות התגלו, בסופו של דבר, כשגויות לחלוטין באפגניסטן ובעיראק.

הבנה זו של מרחב הלחימה העכשווי קמה לתחייה לזמן קצר במערכה נגד לוב ובפרשנות שניתנה ל"אביב הערבי" על ידי המערב, הרגיל לראות קהילות כאילו היו מורכבות מאוסף של יחידים. זאת, בעוד שבמרבית חלקי העולם, החברה מורכבת מקהילה של קהילות. העימות הנוכחי בסוריה קובר פעם נוספת השקפת עולם טכנית זו של המערב.

בלימת מלחמה, עימות אלים או אלימות המונית אינה חייבת להיעשות רק בדרך של מלחמה מוגבלת; היא יכולה להיעשות גם על ידי קביעת הגבלות על הסלמת האלימות בעימותים קיימים. חשיבות הדבר תעלה ככל שיהיו יותר אפשרויות טכניות ללוחמה במאה ה־21. בניסוח מפורש יותר, מרחב הלחימה המתפתח של המאה ה־21 סובב סביב האתיקה והמוסריות של השימוש בכוח וסביב הלגיטימיות לכך. ככל שנפתח יותר הזדמנויות טכניות ללוחמה, שאלת מוסריות השימוש בהן תהיה מרכזית יותר. לדוגמה, הצבא האמריקאי שם דגש רב על פיתוח לוחמה רובוטית ועל לוחמה שניתן לנהל באמצעות אינטליגנציה מלאכותית. במבט ראשון התפתחות זו נראית גאונית, הודות לשמירה על חיי אדם שהיא מציעה. היא אכן גאונית כהגנה נגד פושעים וברבָּרים. אולם מה קורה אם היריב אינו פושע או ברברי, אלא בן אנוש? במקרה זה, הבעיה המוסרית ברורה: מה המשמעות של רובוט המצויד באינטליגנציה מלאכותית ההורג בן אדם? בעיה כזו מובילה לנושא השני, והוא המלחמה בפועל.

ניתן להיווכח בחשיבות ה־jus in bello במשבר הנוכחי בסוריה. השאלה היא מה הופך נשק להשמדה המונית לכה ייחודי בעיני לוחמים ואזרחים כאחד? אני סבור שאנו יכולים ללמוד מסוריה שֶמה שמייחד נשק זה הוא לא מספר הקורבנות,

אלא העובדה שהשימוש בו הוא לא הוגן ולא מוצדק. הרגש שמתעורר לנוכח התנהגות לא צודקת בעת מלחמה מוטבע עמוק בהיסטוריה של המלחמות ובתודעה האנושית גם יחד.

הרעיון של לוחמה אסימטרית צבר תאוצה בעשרים השנים האחרונות. הוא שימש לתיאור המלחמות החדשות, שלפי מוּנקלר ניתן לאפיין כ"אסימטריה של חולשה": הצד החלש בעימות יפנה ללוחמה אסימטרית רק בשל חולשתו ואי־יכולתו להילחם מלחמה רגילה.[8]

טרור, לוחמת גרילה או לחימה נגד אזרחים של האויב הם כולם דוגמאות טיפוסיות ללוחמה אסימטרית. אולם, יש סוג נוסף של לוחמה אסימטרית, שבה הצד החזק מנסה להתנהל במלחמה באופן שלא מותיר ליריבו סיכוי. ניסיון כזה להשיג יתרון אסימטרי עומד בלב הוויכוח על "המהפכה בתחום הצבאי". אני נדהם מכך שהחיבור המתבקש בין שני סוגים אלה של לוחמה אסימטרית לא זוכה, למיטב ידיעתי, לדיון פומבי ראוי. דומה שההשקפה השלטת היא שיש להביא את הצד השני למצב שבו אין לו כל סיכוי לנצח, וכך לגרום לו שלא לצאת למלחמה, ואם כבר יצא למלחמה – להפסיק אותה. אבל יש אפשרות נוספת לצד החלש, והיא לפנות גם הוא ללוחמה אסימטרית. הבעיה שעולה מִגישה כזו היא שככל שאתה צובר יתרון אסימטרי על יריבך, כתוצאה מעוצמתך הטכנית הנתפסת בעיני הצד השני כלא מוצדקת ולא הוגנת, כך הוא ידבק יותר בלוחמה אסימטרית, שהיא מפלטו של החלש, כמו טרור או לוחמת גרילה.

דברים אלה מביאים אותנו לאחרונה משלוש ההצעות שלי, והיא הכרה הדדית מצד הצדדים הלוחמים בסיום המלחמה, במטרה לגבש שלום צודק. קשה כמובן, אם לא בלתי אפשרי, להכיר בפושעים, בטרוריסטים, במחרחרי מלחמה, בסוחרי סמים, בקנאים דתיים, בפושעי מלחמה או בגנגסטרים ובריונים כלוחמים לגיטימיים ושווי מעמד. אלא שגורמים אלה החלו להתלבט בעשור האחרון של המאה העשרים. סכסוכים בין גורמים כאלה עדיין קיימים במרבית אזורי אפריקה שמדרום לסהרה ובשוליים של אימפריות לשעבר, אולם מרבית הסכסוכים בעולם של היום הם פוליטיים במהותם, כך שהאפיון דלעיל של הגורמים המעורבים בהם אינו חל עליהם בצורה גורפת. כאן אני תלמידו של קלאוזביץ, ומסכים לחלוטין עם ההנחה שלו: "הסלמת המלחמה תהיה אינסופית, אם ההתייחסות לאסטרטגיה תהיה שהיא 'אינה מושפעת מהערכה קודמת לגבי המצב הפוליטי העתיד להיווצר בעקבותיה'".[9]

מסקנתי היא, אפוא, שאנו זקוקים לאסטרטגיה מחודשת של הכלה, החייבת להיות שונה מזו של המלחמה הקרה, אם כי מבוססת על עקרונות דומים. בהשוואה למלחמה הקרה, אין עתה גורם בלעדי שיש לבלום אותו, כפי שהייתה ברית המועצות. גם בהנחה שצודקים אלה החוזים שסין תהפוך למעצמת־על חדשה תוך

עשרים שנה, אין זה הגיוני לפתח אסטרטגיית הכלה צבאית נגדה, שתהיה דומה לזו ששימשה נגד ברית המועצות בשנות החמישים והשישים של המאה הקודמת, שכן התנהלות כזו עשויה לעורר בדיוק אותם משברים ועימותים שהאסטרטגיה מבקשת למנוע.[10] הניסיון לבנות את הודו כמשקל נגד לסין, על ידי סיוע לשאיפות ההודיות ליכולת גרעינית, מסתכן בחתירה נגד המערכה הבין־לאומית להגבלת הפצתו של נשק גרעיני בעולם.

ההבדל השני הוא בכך שההתפתחויות הנוכחיות בסביבה האסטרטגית מגלמות נטיות סותרות: בין גלובליזציה ובין מאבקים על זהות, יתרונות מקומיים ואינטרסים[11]; בין מלחמות היי־טק לקרבות עם "סכינים וגרזנים" או מחבלים מתאבדים; בין לוחמה סימטרית ללוחמה אסימטרית; בין הפרטה של מלחמה ואלימות [12]לפוליטיזציה ולאידיאליזציה מחדש שלהן, וכן מלחמות על "הסֵדר העולמי"[13]; בין עיצוב מוקדי כוח אזוריים חדשים לדומיננטיות אימפריאלית־הגמונית של מעצמת־על יחידה; בין פשע בין־לאומי מאורגן למיסוד של קהילות ומוסדות גלובליים ואזוריים; בין הפרות גוברות של החוק הבין־לאומי וזכויות אדם מצד אחד להרחבתם מצד שני. אסטרטגיה שמטרתה תהיה התמודדות עם אחת ממגמות סותרות אלו בלבד, עשויה למצוא עצמה במצב בעייתי ביחס לאחרות. לפיכך, נחוץ להגיע לאיזון בין האפשרויות המתחרות.

ההבדל השלישי הוא שההכלה המסורתית נתפסה בעיקר כהרתעה צבאית של ברית המועצות, למרות שבניסוח המקורי של ג'ורג' קנאן היא הייתה שונה למדי מהסבר זה. ההנחה המרכזית שלנו היא שהכלה חדשה חייבת לשלב מצד אחד הכלה צבאית מסורתית, ומצד שני מרחב של הזדמנויות לשיתוף פעולה. הדבר חיוני לא רק ביחס לסין, אלא גם ביחס לאסלאם הפוליטי, וזאת כדי להפחית מהמשיכה שחשים מיליוני צעירים מוסלמים לתנועות אסלאמיות קיצוניות.

לצורך השגת היעד של ריסון המלחמה והאלימות בחברה הגלובלית נדרשת הגדלת מספר האזורים הלא צבאיים לכלל מה שמכונה בתפיסה של עמנואל קאנט "שלום דמוקרטי", וכן הכלה אקטיבית והגבלת התרחבותן של המלחמות והאלימות. אפשרות זו חייבת להיות מובנת מאליה, כדי שתהיה מוסכמת על עמים ומנהיגים פוליטיים שונים. חשוב לבדל רעיון זה מרעיונות מתחרים, ויש להתייחס אליו ככזה המתאים להתמודד עם התפתחויות עכשוויות. לבסוף, יש בכך, במידה מסוימת, ביטוי לְמה שהקהילה הבין־לאומית עושה בלאו הכי: "מדינות אחרות עושות שימוש באמצעים, כמו שיבוש זרימת הכספים ממוסד אחד למשנהו, הגבלת תנועה של טרוריסטים, חיסול מקומות המקלט שלהם, איתור ולכידה של המנהיגים שלהם או תקיעת טריז בין ארגוני הטרור לאוכלוסיות עליהן הם מתיימרים להגן".[14] האסטרטגיה שמדינות אלו נוקטות ממילא היא אסטרטגיית ההכלה!

השאלה נותרת כיצד להרתיע מאמינים קנאים, חברים ברשתות טרור או אנשים כמו נשיא אירן לשעבר, שעבורם הֶרס עצמי עשוי להיות אמצעי להחשת יעדים קיצוניים. כמובן שקשה מאד להרתיע את "המאמינים האדוקים" או את הגרעין הקשה של הטרוריסטים, אך זו רק סיבה נוספת מדוע הכלה אינה צריכה להצטמצם לאסטרטגיה של הרתעה. גם במקרים כאלה, המשימה האמיתית היא לפעול מדינית וצבאית באופן שיאפשר להפריד בין "המאמינים האדוקים" ובין "המאמינים", ובין אלה לבין "האוהדים". האסטרטגיה יכולה לכלול פעולות צבאיות ואיומים אמינים, אולם במקביל עליה להיות מבוססת על אסטרטגיה כפולה שתציע ברירה בין חלופות, מתוך הבנה שההצטמצמות לאמצעים צבאיים בלבד רק תעצים את ההתנגדות האלימה. גם "המאמינים האדוקים" יכולים למצוא עצמם נדרשים לבחור בין להמשיך להיות חלק מהסביבה הדתית והחברתית שלהם (או מוּקעים ממנה) ובין למתֵן שאיפות קיצוניות. באימוץ אסטרטגיה זו אין ערבוּת לכך שניתן יהיה למנוע כל מתקפת טרור. אבל זאת לא השאלה האמיתית; בהנחה שהמטרה של אסלאמיסטים קיצוניים היא לעורר תגובת יתר של המערב כדי להצית מלחמה כוללת בין המערב ובין האסלאם, אין ברירה אלא לנסות להפריד בינם לבין הסביבה הדתית, החברתית והפוליטית שלהם.

תפיסות מתחרות

מימושה של תפיסה זו ניתן להסבר באמצעות הדוגמה של דמוקרטיזציה. הגבלת המלחמה והאלימות מניחה את היסודות לדמוקרטיה. אם האסטרטגיה הנגדית היחידה להפצת אלימות הייתה דמוקרטיזציה כללית וחובקת עולם בצורת הטמעת בחירות דמוקרטיות – תנאי מקדים הכרחי אך לא מספיק לביסוס חברות דמוקרטיות אמיתיות – דמוקרטיזציה שתיושם במידת הצורך באמצעות כוח תוביל, כמעט בוודאות, לתוצאה הפוכה מהרצוי. הדבר ברור במיוחד באותם מקרים שבהם אין עדיין דמוקרטיות חוקתיות מפותחות אלא מדינות וחברות הנמצאות בתהליך התחלתי של שינוי. שלא כמו בדמוקרטיות מפותחות, במקרים כאלה נכון יותר לדבר על סתירה הגיונית לרעיון של שלום דמוקרטי.

אפשרי, לפיכך, שדרישה חד־צדדית לתהליכים דמוקרטיים מבלי לתת את הדעת לתנאים המקומיים, תתרום במקרים מסוימים ליצירת תנועות טוטליטריות. הניסיון ההיסטורי של מעבר מתהליכים דמוקרטיים לטוטליטריים מגולם בהתפתחויות שאירעו במהלך ולאחר מלחמת העולם הראשונה. בכמעט כל המדינות שהובסו באותה מלחמה היו בהתחלה תהליכי דמוקרטיזציה, לרבות מהפכות דמוקרטיות. למרות זאת, כמעט כולם הסתיימו בדיקטטורה. "הזכות להגדרה עצמית לאומית" עליה הכריז נשיא ארצות הברית וילסון, התפרשה במזרח אירופה ובבלקנים באופן לאומני יותר מאשר דמוקרטי, וגרה הדָרה של אוכלוסיות שלמות, ואפילו רצח

העם הראשון של המאה העשרים נגד הארמנים, שהחל עוד בזמן מלחמת העולם הראשונה.[15]

מה שמכונה "האביב הערבי" היה נראה במבט ראשון כהיפוך של מגמה זו, אולם האירועים האחרונים במצרים, בסוריה ובלוב דווקא מעצימים אותה, משום שכל שלוש המדינות מֻטלטלות בסוג של מלחמת אזרחים ונמצאות בדרכן להפוך ל"מדינות כושלות". ואכן, אין לשלול את האפשרות שתהליכי דמוקרטיזציה שקודמו מבחוץ יערבו שימוש באלימות, למרות שמבחינה היסטורית, אחרי מלחמת העולם השנייה התרחשו מספר תהליכי דמוקרטיזציה כתוצאה מתבוסות צבאיות הרסניות: בגרמניה וביפן, ומאוחר יותר בסרביה לאחר מלחמת קוסובו. מנקודת המבט של מניעת מלחמה ואלימות, יהיה זה הגיוני, במקרים מסוימים, לוותר על תהליכי דמוקרטיזציה לטובת התפרקות מנשק.

הגישה המרכזית המוצגת כאן, המנוגדת לתפיסות תיאורטיות אחרות של שלום, היא של תפיסות של "שלום דמוקרטי" ברוח קאנט, שהן חלק מתיאוריות שיווי המשקל, ותפיסות של הגמוניה ואימפריות, ששימשו להגבלת המלחמה והאלימות בחברה העולמית. הבעיה היא שאמצעים אלה הפכו לעתים קרובות למטרות בפני עצמן. לשיטתי, מניעת המלחמה והאלימות הופכת למטרת־על של הפעולה הפוליטית והקהילתית. כאשר יוצאים מנקודת המוצא של המטרה הפוליטית, יש אפשרות לקבוע איזה יעד ואיזו פעולה הם הנכונים ביותר.

מסגור מחדש של האידיאולוגיה והפוליטיקה של המלחמה

ניתן לראות את ההתפתחויות באפגניסטן כדוגמה למסגור מחדש של האידיאולוגיה והפוליטיקה של המלחמה והעימותים האלימים. לאחר הניצחון על הצבא הסובייטי, החלה בסוף שנות השמונים של המאה העשרים מלחמת אזרחים בין הצבא לשבטים באפגניסטן. העימות קיבל מסגרת אידיאולוגית חדשה, ואז תפס הטליבאן את השלטון. ניתן לראות שמלחמות אזרחים לא הופכות ל"פרטיות", עד אשר הקהילות הקטנות ביותר מחזיקות בקלצ'ניקובים. אלו קהילות שֶמה שמחזיק אותן ביחד היא האלימות, ושבהן הלחימה היא מטרה בפני עצמה.[16]

היו גם מספר מקרים שבהם מלחמות אזרחים הסתיימו במסגור מחדש של האידיאולוגיה והפוליטיקה. אפגניסטן היא דוגמה טובה לכך, משום שניתן להמחיש באמצעותה את האיכות החדשה של "הפרטת" המלחמה והאלימות, ובמקביל היא מראה בצורה ברורה את המסגור מחדש של האידיאולוגיה והפוליטיקה של הסכסוך, עם ניצחונו של הטליבאן ועלייתו לשלטון. הטענה ש"הפרטת" המלחמה באפגניסטן מוכיחה את האיכות החדשה של "המלחמות החדשות" מובילה לפרדוקס, אלא אם כן היא מוגבלת לתקופה של עד ניצחון הטליבאן ב־1996. לכן, מקרה זה אינו יכול לשמש דוגמה של השינוי הנובע מ"הפרטת" המלחמה;

למעשה, הוא מוכיח שהתפתחות האיכות החדשה, למרות שהייתה אמיתית, נמשכה פרק זמן מוגבל בלבד, עד שהחל שלב חדש ב־1996 – שלב של מלחמות על הסֵדר העולמי.

ניתן להוסיף על החלוקה לתקופות שאני מציע גם סיווג גיאוגרפי־היררכי של שני השלבים: "הפרטת" האלימות באזורים רבים של אפריקה שמדרום לסהרה ובאזורי עימותים מסורתיים כמו הבלקן והקווקז; התפתחות עימותים על רקע הסֵדר העולמי בין המערב לאסלאם הקיצוני, ובעתיד גם ביחסים עם סין ואולי עם רוסיה. עימותים בצורה של מלחמות בין מדינות מתפתחים לשני כיוונים חדשים ומקבילים: לעֵבר מלחמות "מופרטות" מצד אחד, ולעֵבר מלחמות בין מדינות־על – מלחמות על הסֵדר העולמי. הבחנה זו מהותית יותר מאשר הניסיון להבחין בין מלחמות "מופרטות" ו"חדשות" ובין מלחמות "מפוזרות" הנובעות מתהליך הגלובליזציה, ומאשר הניסיון להשתמש בכך כדרך לאתגר את הלגיטימיות של מערך התפיסות הראשון,[17] יציאה למלחמה לצורך קידום ערכים,[18] או כדרך לארגון העולם (בין אם סדר זה נתפס כאוניברסלי או כמקומי) שונה למדי מיציאה למלחמות "מופרטות" או "מפוזרות". שתי רמות אלו של מלחמות קשורות אחת עם השנייה וכן עם מלחמות בין מדינות, אך יש חשיבות להבחנה האנליטית ביניהן: מלחמות מתנהלות עדיין על ידי מדינות; עם זאת, במרבית המקרים הן עושות זאת לא מתוך שאיפה להשיג אינטרסים מוגדרים שלהן, אלא מסיבות הקשורות לסֵדר העולמי. דוגמה לכך היא השימוש ברעיונות כמו "אימפריה אמריקאית"[19] ו"הגמוניה אמריקאית."

תהליכים כמו רוויה תקשורתית, כלכלית וטכנולוגית בעולם מעצימים תנועה דואלית זו בצורה דרמטית, משום שפעמים רבות הם מקשרים מרחבי פעולה ישירות אחד עם השני. לדוגמה, במהלך מלחמת האזרחים בסומליה ניתן היה לראות קבוצות של לוחמים העושים שימוש במחשבים כדי לקנות ולמכור מניות בוול סטריט. הגורם הקובע, עם זאת, הוא התנועה הדואלית הנגדית – לעבר "הפרטה" של האלימות, ובמקביל לעבר מלחמות על סדר עולמי קיים ועתידי, שיכולות להיות גלובליות או אזוריות. גם אם לא ניתן לראות זאת במבט ראשון, בפועל הגלובליזציה אכן משנה את הסדר העולמי.[20]

מושג ההכלה והלוחמה בת זמננו

דוגמה נוספת ליתרון של הגישה שאני מציע, ניתן לראות באמצעות בחינת המצב הסופי הרצוי שאליו אמורה לשאוף המלחמה בטרור. השאלה היא האם עלינו "לשים את היד" על טרוריסטים ולחסל את כולם, כפי שהצהיר שר ההגנה לשעבר של ארצות הברית דונלנד רמספלד?[21] שאלה נוספת היא כיצד להילחם בארגונים שאין להם מבנה היררכי אלא מבנה רשתי.

היעד של המלחמה בטרור אינו צריך להיות השגת ניצחון, משום שאף אחד לא יכול להסביר איזה ניצחון ניתן להשיג במלחמה מסוג זה. יתרה מכך, כל ניסיון להשיג ניצחון מוחלט על הטרוריסטים רק יגביר את מספרם. בעיה נוספת היא לא כיצד אנו עצמנו תופסים את רעיון הניצחון, אלא באילו דרכים היריב שפעל מולנו בטכנולוגיה פחות מתקדמת מגדיר ניצחון ותבוסה. זוהי בעיה שהתשובה לה מחייבת ידע תרבותי והיסטורי הרבה יותר משהיא דורשת טכנולוגיה מתקדמת.[22] במקום אלה ניתן להצהיר שהיעד הוא "לבלום את הטרור", שהוא כמובן מצב שונה לחלוטין מאשר רגיעה. הגבלה מהותית של הסכנות שמציבים ארגוני הטרור יכולה להתבסס על שלושה היבטים: ראשית, מאבק בין רעיונות פוליטיים במטרה לזכות בתמיכתם של מיליוני צעירים; שנית, ניסיון לרסן חילופי מידע, תמיכה כספית ותקשורת בין הרשתות במטרה להשיג בידוד ברמה המקומית; ושלישית, אבל רק לצד שתי המשימות הקודמות, הריסה של מה שהישראלים מכנים תשתית הטרור. להבנתי, ניסיון להשיג ניצחון צבאי מסורתי על הטרור לא רק שייכשל, אלא אף עלול להוביל לחיזוק הטרור בעתיד הנראה לעין.

רעיון "מרכז הכובד" בלוחמה יכול לספק המחשה נוספת לדרך שבה תפיסתי יכולה להציע שינוי. קלאוזביץ מגדיר מלחמה כמעשה של אלימות שמטרתו לאלץ את האויב לעשות את רצוני. הגדרה זו מתאימה להבנתנו את המלחמה בין יריבים שווים, יריבים שבהם צד אחד אינו מעוניין להשמיד את השני, או את הישות הפוליטית, האתנית או המשפטית שמאחוריו. אבל בעימותים בין יריבים בעלי רקע אתני או תרבותי שונה, כפיית רצונו של צד אחד נתפסת לרוב כניסיון להשמיד את הזהות והקהילה של האחר. לכן, החלופה היחידה עבור חברות דמוקרטיות היא לראות במלחמה מעשה של אלימות, שבו, במקום לכפות את רצוננו על היריב, המטרה היא להביא אותו למצב שבו הוא לא יהיה מסוגל עוד לממש את רצונו באופן אלים ולהשתמש בכוחו כדי לאכוף את רצונו עלינו או על אחרים, ולהגביל את כוחו, כך שלא יוכל עוד לאיים עלינו או להילחם בנו כדי לאלץ אותנו לעשות את רצונו.

המטרה של הכלת מלחמה ואלימות היא, אפוא, להסיר מהיריב התוקפני את חופש הפעולה המוסרי והפיזי שלו, אולם מבלי לתקוף את מקור הכוח ואת הסדר החברתי שלו. המפתח ל"ניהול האלימות" הוא לשלוט בתחומים מבצעיים מסוימים, בטריטוריה, בתנועת המונים ובכוח צבאי, אבל גם במידע ובפעולות הומניטריות. אין לתפוס עוד את המשימה של "ניהול האלימות" כמכוונת נגד מרכז הכובד של היריב, אלא ככזו המכוונת נגד "השוליים" של שדה הכובד. במקום לאכוף את הרצון של צד אחד על השני עד לנקודה של שליטה בתודעתו, כפי שמנסחים זאת מומחי לוחמת המידע האסטרטגית,[23] הדרך היחידה לשים

קץ לעימות במאה ה־21 היא להכיל את הסלמת המלחמה והאלימות, ובמקביל לאפשר פעולה במסגרתן.

העמדה שהצגתי כאן מכוונת למדיניות עולמית שוחרת שלום ומתייחסת להגבלה הפרוגרסיבית של מלחמות ואלימות כאל תהליך מתמשך ואינסופי, וכיעד בפני עצמו. ההכלה הקבועה והמתמשכת של המלחמות והאלימות נחוצה כדי לשמור על קיומן ואפילו על שרידותן של מדינות, וכן על צלם האנוש של חברות מקומיות ושל החברה הכלל־עולמית.

הערות

1 See Tim Mark, "Chuck Hagel Stumbles on Iran Questioning," Politico, January 31, 2013, http://www.politico.com/story/2013/01/chuck-hagel-stumbles-on-iran-question-87001.html

2 George, F. Kennan, "Containment: 40 Years Later", in: Terry L. Deibel and John Lewis Gaddis (eds.), *Containment: Concept and Policy*, Washington: National Defense University Press, 1986, pp. 23-31.

3 Charles W. Kegley Jr ., "The New Containment Myth: Realism and the Anomaly of European Integration", *Ethics & International Affairs*, 1991, Vol. 5, pp. 99-115.

4 Nathan K. Finney, "Using the Threat of Violence to Contain Syria: An External Approach", *Infinity*, Vol. 3, Summer 2013, pp. 13-16.

5 Colin S. Gray, *Another Bloody Century. Future Warfare*, London: Weidenfeld & Nicholson, 2005, p. 9.

6 Emile Simpson, *War from the Ground Up*, London: Hurst Publishers, 2012.

7 Andreas Herberg-Rothe, *Clausewitz's Puzzle. The Political Theory of War*, Oxford: Oxford University Press, 2007; Andreas Herberg-Rothe, *The Evolving Battle Space of the Twenty-First Century*, Lecture in Nanyang University, Singapore, September 19, 2013.

8 Herfried Munkler, *The New Wars*, London: Polity Press, 2004.

9 Carl von Clausewitz, *On war*, translated and edited by Michael Howard and Peter Paret (Princeton, Princeton: University Press 1984), p. 78.

10 "US Denies New Containment Policy against China," *People's Daily Online*, November 24, 2005, http://english.people.com.cn/200511/24/eng20051124_223692.html

11 זיגמונט באומן כינה נטייה סותרת זו בשם "Glocalisation", שהוא שילוב בין המילים "Localisation" ו- "Globalisation":
Zygmunt Bauman, "Glokalisierung oder: Was für die einen Globalisierung, ist für die anderen Lokalisierung", *Das Argument* 217, 1996, pp. 653-664; Zygmunt Bauman, *Globalization*, London: Polity Press, 1998.

12 Munkler, *The New Wars*; Mary Kaldor, *New and Old Wars. Organized Violence in a Global Era*, Stanford: Stanford University Press, 1999.

13 הִצגתי את ההשערה שלאחר התפרקות אימפריה ושינוי הסדר העולמי, מופיעה תמיד נטייה להפרטת מלחמה ואלימות לרמה אחת מתחת למערכת שהתפרקה. הדבר קרה לאחר נפילת ברית המועצות והסדר הדו־קוטבי של המלחמה הקרה. להערכתי, בטווח הארוך החשיבות של הפוליטיקה והאידיאולוגיה דווקא תעלה. ראו: Andreas Herberg-

Rothe, "Privatized Wars and World Order Conflicts", *THEORIA* (South Africa), No. 110, August 2006, pp. 1-22.

14 Antulio Echevarria, *Fourth-Generation Warfare and other Myths*, Carlisle, 2005, pp. 5-6.

15 Dan Diner, *Das Jahrhundert Verstehen*, Frankfurt: Fischer, 2000.

16 דימוי זה מסמל את שיח "המלחמות החדשות" טוב יותר מכל דבר אחר, וכן הוא מסמל את המלחמה של תומס הובס, של כולם נגד כולם.

17 Sven Chojnacki, Wandel der Kriegsformen? – Ein kritischer Literaturbericht. In: *Leviathan*, 32:3, pp. 402-424.

18 Hans Joas, Kriege und Werte. Studien zur Gewaltgeschichte des 20. Jahrhunderts (Weilerswist:Velbert) 2000.

19 Michael Walzer, *Just and Unjust wars. A Moral Argument with Historical illustrations*. (New York: Basic books) 2000; Michael Walzer, "Die Politik der Rettung", In: *Berliner Debatte Initial* 6, 1995, pp. 47-54.

20 Antulio Echevarria, Globalization and the Clausewitzian Nature of War. In: The *European Legacy*, Vol. 8, No. 3, 2003, pp. 317-332.

21 Donald Rumsfeld, "You can only Defend by Finding Terrorists and Rooting them Out", Interview with Donald Rumsfeld, *The Daily Telegraph*, February 25, 2002.

22 Robert D. Kaplan, "The Story of a War", *Atlantic Monthly*, November 2003.

23 David Lonsdale, *The Nature of War in the Information Age. Clausewitzian Future*, London: Frank Cass, 2004, p. 208.

שילוב טכנולוגיות להגנת העורף מפני איומים בליסטיים וטילי שיוט

יוסי ארזי וגל פרל

מאמר זה דן בטיב המענה ההגנתי האקטיבי לאיום הרקטי על עורף מדינת ישראל. במלחמה כוללת צופה מערכת הביטחון כי העורף יותקף במשך כשלושים יום, ויספוג בכל יום כאלף טילים שיגרמו לאלפי נפגעים ולפגיעה בתשתיות ובאתרים אסטרטגיים. לישראל מערכת ההגנה האקטיבית, שלה חמש שכבות טילי יירוט. בשיתוף עם ארצות הברית פותחה מערכת הגנה מבוססת לייזר כימי בשם "נאוטילוס" שהנגזרת המיידית שלה היא מערכת ה־"סקייגארד". ב־2007 נבחרה מערכת "כיפת ברזל", שטיליה יקרים יותר, על פני "סקייגארד" משיקולים כלכליים ומבצעיים. רק מענה משולב, הכולל מערכות טילי הגנה מפני טילים ומערכות לייזר כימי, יהווה פתרון הגנתי אקטיבי מקיף לכלל האיומים, וללא קושי כלכלי משמעותי.

מילות מפתח: כיפת ברזל, הגנה אקטיבית, נשק תלול מסלול, מערכת סקייגארד, מבצע עמוד ענן

רקע

מבצע "עמוד ענן", שהתרחש בנובמבר 2012, חידד מחדש את העובדה כי האיום הרקטי על מדינת ישראל גבר. מול הפיחות המשמעותי באיום התמרון היבשתי מצד מדינות אויב שכנות נגד ישראל, העלה המבצע על סדר היום שוב, וביתר שאת, את קיומו של איום ממשי על מרכזי האוכלוסייה של המדינה.[1] אמר על

אל"מ (מיל.) יוסי ארזי שירת בחיל האוויר כטייס קרב וכראש מחלקת מערכות בלהק ציוד. כיום מנכ"ל עמותת "מגן לעורף".
גל פרל הוא עוזר מחקר בתכנית המאזן הצבאי במזרח התיכון של המכון למחקרי ביטחון לאומי (INSS). שימש כמתמחה בתכנית צבא ואסטרטגיה.

כך בשעתו רא"ל (מיל') גבי אשכנזי: "מי שמייצר יתרון בלחימה זה מי שמצליח להיערך ראשון לאיום הבא".[2]

מערכת הביטחון צופה כי במלחמה כוללת יותקף העורף במשך כשלושים יום, וזאת על ידי סוריה, חזבאללה וחמאס. הצפי הוא שעורף מדינת ישראל יספוג בכל יום כאלף טילים, רקטות וטילי שיוט למיניהם,[3] חלקם מונחי GPS, עם דיוק פגיעה של מטרים בודדים. אומדן הנזק במקרה כזה הוא של אלפי נפגעים, הרס תשתיות ופגיעה באתרים אסטרטגיים.

מדינת ישראל מפתחת ומיישמת מערכת הגנה מפני סוגים שונים של טילים ורקטות, שתפעל מרגע שיגורם. מערכת ההגנה מבוססת על חמש שכבות של טילי הגנה ("כיפת ברזל", "שרביט קסמים", "חץ" 2, "חץ" 3 ו"פטריוט"). הנחת העבודה היא כי משרד הביטחון ישלים את תהליכי הפיתוח של כלל מערכת ההגנה, כולל מערכות מכ"ם ותקשורת, וכי תהייה הצטיידות בטילי ההגנה למיניהם בכמות מספקת למספר ימי לחימה.

ממשלת ישראל החלה באמצע שנות התשעים של המאה הקודמת בשיתוף פעולה תעשייתי ומבצעי הדוק עם ארצות הברית לפיתוח מערכת הגנה מפני קטיושות, המבוססת על לייזר כימי רב עוצמה, שכונתה "נאוטילוס". ייעוד ה"נאוטילוס" היה הגנת קריית שמונה, ואף תוכנן להציבה שם לפני הנסיגה מלבנון במאי 2000. בשנים 2000–2004 נערכו 46 ניסויים להפעלת המערכת נגד איומים בליסטיים שונים, ובהם פצצות מרגמה, רקטות למיניהן ופגזי ארטילריה. כולם יורטו, ללא יוצא מהכלל. במקביל, הסתיים התכנון המלא של מערכת "סקייגארד" – הנגזרת המיידית מה"נאוטילוס" – והיא הייתה מוכנה לייצור. בתחילת 2007 המליצה ועדת נגל, שמונתה על ידי שר הביטחון לבחון את מערכת ההגנה על העורף, להעדיף את מערכת "כיפת ברזל" על פני "סקייגארד", בנימוק שיש יתרון מובהק בהיבטי עלות, כמו גם בהיבטים מבצעיים, לחלופת היירוט הקינטי על פני חלופת היירוט באמצעות לייזר. מאז הופסק המשך פיתוחה של מערכת "סקייגארד", ובכלל זה נפסקו הניסויים לבחינתה. יצוין כי בדוח מבקר המדינה 59א' (2008) נמתחה ביקורת על אופן גיבוש ההמלצה להעדיף את החלופה הקינטית והודגש, בין היתר, כי לא הוגדר צורך מבצעי התוחם את הפער המבצעי וההישג הנדרש ממערכת הגנה אקטיבית וכי הדבר גרם להרחבת איום הייחוס – מרקטת "קסאם" בלבד לכלל סוגי הירי תלול המסלול קצר הטווח.[4]

מאמר זה נועד להראות כי רק מענה משולב, הכולל מערכות טילי הגנה מפני טילים ורקטות, יחד עם מערכות לייזר כימי רב עוצמה, יביא למימוש פתרון הגנתי אקטיבי מקיף, שיענה לכל סוגי האיומים על העורף – מרכזי האוכלוסייה המשמעותיים והאתרים החיוניים. המאמר יצביע על כך שמענה משולב זה, שיאפשר הגנה במשך זמן לחימה ארוך ככל שיהיה, ניתן למימוש ללא קושי כלכלי

משמעותי ולעומת זאת, כי מערכת המתבססת על טילי הגנה בלבד אינה ישימה, הן מן הבחינה הכלכלית והן משום שאינה יכולה לספק הגנה בחלק מהמתארים המבצעיים.

מִתאר האיום לייחוס

תפיסת הביטחון של ישראל גורסת כי בעת מערכה עתידית, נוכח איום המוגדר כסכנה ברורה ומיידית, על מדינת ישראל, החסרה עומק אסטרטגי, לבצע פעולת מנע בהקדם, תוך שאיפה לקיצור משך הלחימה ככל האפשר. זאת, בשל כושר ספיגה נמוך הן מן הבחינה הכלכלית והן מבחינת הנפגעים בנפש. מכאן, שיש לחתור להכרעת האויב בשטחו הוא, באופן מהיר וברור, בכדי להימנע מניהול לחימה בקרבת האוכלוסייה האזרחית בישראל.[5]

צה"ל נערך למימוש תפיסה זו מן הבחינה ההתקפית באמצעות דוקטרינת לחימה הנשענת על שלושה מרכיבים: "הראשון – מהלומת אש הרסנית נגד נכסי הליבה; השני – תמרון מהיר לפגיעה באויב ושיתוק יכולות השיגור ממרחב התמרון; והשלישי – כושר עמידה ויכולת התגוננות בחזית האזרחית".[6] דוקטרינה זו מתבססת על ההנחה שכאשר יפרוץ עימות צבאי בסדר גודל דומה לזה של מלחמת לבנון השנייה או מבצע "עופרת יצוקה", הן מבחינת עצימותו והן מבחינת איום הירי של מאות רקטות וטילים ביממה, לא יהיה ברשות ישראל מרחב פעולה רב במובנים של זמן, מרחב ולגיטימציה להפעלת כוח, ולכן מוטב יהיה לפעול במהלומת אש ולהכות את האויב,בדומה לתקיפת מפקדות חזבאללה בביירות במלחמת לבנון השנייה, במטרה להשיג "אפקט דאחיה" ולהרתיע את האויב.[7] אמר על כך בשעתו רא"ל בני גנץ: "במציאות, כאשר נפגע באופן רציני ביכולת השיגור של האויב, וכאשר ההישגים שלנו על הקרקע יהיו ברורים והצד האחר יתחנן להפסקת אש, לא יהיה ספק מי המנצח ומי המנוצח".[8]

עצם השאיפה לקיצור משך הלחימה אינה מבטיחה כי משך המערכה אכן יהיה קצר.[9] בחינה של מלחמת לבנון השנייה, בה לחם צה"ל נגד חזבאללה לבדו במשך 34 ימים, תראה כי הארגון ירה במהלכה לעבר העורף הישראלי כ־4,000 רקטות מסוגים שונים (לקראת סופה שוגרו כ־250 רקטות ביום), ובכך שיתק את מהלך החיים התקין של תושבי צפון המדינה.[10] קיימת סבירות לא מבוטלת כי לחימה עתידית נגד סוריה, חזבאללה וחמאס תימשך הרבה יותר מיומיים־שלושה, ויתכן שתימשך אף שלושים ימים, כפי שצופה מערכת הביטחון.

האיום הרקטי על מדינת ישראל הולך ומתעצם מכל בחינה[11] – כמויות, טווחי הירי, גודל הראש הקרבי ודיוק הפגיעה. אזורי השיגור מתפרסים מטווח של מאות מטרים מהגבול (פצמ"רים) ועד 1,500 ק"מ ומעלה (טילי "שיהאב" מאיראן). זהו איום מתמשך ומתפתח, הן מבחינת החימוש, ההופך למדויק והרסני בהרבה, הן

מבחינת התרחבות האיום – בעבר היה האיום של נשק תלול מסלול רלוונטי לגבולה הצפוני של מדינת ישראל בלבד, ואילו היום הוא קיים גם מכיוון רצועת עזה ואף מחצי האי סיני ומאיראן – והן מבחינת כמות החימוש המצוי בידי האויב.[12]

על מדינת ישראל לנתח איום זה ולתכנן בהתאם לו את מערכות ההגנה שלה. בהיבט הכמותי, מדובר באיום של אלפים בודדים עד מאות אלפי טילים ורקטות, כולל פצצות מרגמה, לטווחים של עד מספר קילומטרים, המהווים את אחד האיומים העיקריים על יישובי "עוטף עזה"; ברקטות "קסאם" ו"גראד", המשוגרות לטווחים של שלושה עד כארבעים ק"מ; ברקטות לטווח בינוני־קצר מסוג "פג'ר", שהטווח שלהן הוא שישים עד תשעים ק"מ; ברקטות F110 ו־M600 המשוגרות לטווחים של 200 עד 300 ק"מ, עם ראשי נפץ של 200 ק"ג ומעלה ודיוק GPS; ובטילי "סקאד" לטווחים של 200 עד 700 ק"מ, בעלי ראשי נפץ של מאות קילוגרמים, העשויים לשאת רש"ק כימי או ביולוגי. ניתן להוסיף לקשת איומים זו את טילי "שיהאב" 3 ו־4 של איראן, להם פוטנציאל לשאת גם ראשי קרב גרעיניים, ואת טילי השיוט, שהמסוכן שבהם הוא P800 ("יאחונט") מתוצרת רוסיה, המצוי בידי סוריה. לטיל זה דיוק GPS והוא משייט בגובה של 10–15 מטרים ובמהירות של עד 2.5 מאך. לטילים אלה פוטנציאל הרס של כל המטרות האסטרטגיות במדינת ישראל, כבר בשלב הפתיחה של העימות.

הבסיס לתכנון מערכת ההגנה, כמוצע במאמר זה, הוא ההנחה של מערכת הביטחון כי יש לקבוע מודל כמותי לכל סוג איום שישוגר לעבר ישראל בכל אחד משלושים ימי הלחימה. זאת, אף שניתן להניח כי ככל שהלחימה תימשך, ירד קצב השיגורים נגד מדינת ישראל, כפי שאכן אירע במבצע "עופרת יצוקה": בתחילתו הגיב חמאס בירי מאות רקטות ביממה, אך זה פחת במהלך המבצע לכדי עשרות ביום, ולבסוף הגיע ל־13 רקטות.[13] הערכה גורסת כי בכל יום נתון ישוגרו לעבר מדינת ישראל מאות פצצות מרגמה, כ־800 רקטות קצרות טווח – מ"קסאם" 1 ועד "גראד" משופר – כמאה רקטות וטילים לטווח בינוני־קצר, ובהם רקטות "פג'ר" ו־F110 וכן טילי "זלזאל", כמאה טילים ורקטות לטווח בינוני ומעלה, ובהם רקטות M600, טילי "סקאד" וטילי "שיהאב" מאיראן, וכן כמה עשרות טילי שיוט.[14]

דרישות בסיסיות ממערכת הגנה מיטבית

מול קשת רחבה זו של איומים יש להציב מערכת שתוכל להתמודד באופן אופטימלי עם כמות רבה של איומי נשק תלול מסלול ורקטות מסוגים שונים, ולהשמידם לפני הגעתם לקרקע, ללא קשר למשך העימות הצבאי. מערכת אידיאלית תהיה מסוגלת ליירט תחת מגבלות מינימאליות ככל האפשר את מרב האיומים שביכולת האויב לשגר, כולל ירי במטחים, ולשמור על יכולתה זאת לאורך זמן, ככל שיידרש; עלות השמדת איום באמצעותה תהיה נמוכה ביותר, בכדי למנוע הגבלה כלכלית

על הפעלתה; ניתן יהיה להפעילה נגד כל סוגי האיומים הבליסטיים וטילי השיוט ובכל מזג אוויר; זמן התגובה מרגע שיגור האיום או מכניסתו למעטפת ההגנה ועד להשמדתו יהיה קצר ביותר, כדי לאפשר פעולה נגד איומים הנורים לטווחים קצרים במיוחד; ההצטיידות בסיום הלחימה, כהכנה לעימות הבא, לא תדרוש השקעות מסיביות, שכֵּן לא יתחייב פיתוח טכנולוגי כל אימת שאיום חדש מופיע בזירה.

מאמר זה יבחן ויעריך את הפתרונות השונים ושילובם, לאור יכולתם לעמוד בדרישות אלו.

מערכת טילי הגנה בלבד – יתרונות, חסרונות וישימות

היתרון המבצעי העיקרי של מערכת המבוססת על טילי הגנה בלבד הוא יכולתה לפעול בכל תנאי מזג אוויר (בהנחה שכך היא מתוכננת). יתרון נוסף הוא עצם הימצאותה בשלבי יישום שונים – השלמת פיתוח ("כיפת ברזל" ו"חץ" 2), פיתוח ראשוני ("שרביט קסמים" ו"חץ" 3) והצטיידות ("כיפת ברזל", "חץ" 2 ו"פטריוט") – המאפשרים הצטיידות מהירה יותר. החיסרון של מערכת כזו הוא שהופעת איום חדש מחייבת פיתוח של טיל הגנה חדש נגדו.

מערכת הגנה הנסמכת על טילי הגנה בלבד מוטעית מיסודה: לא ניתן לתקצב רכש טילי הגנה שיתחרה בכמות האיומים שבידי האויב, שכֵּן הוא דורש סכומי עתק שאין למדינת ישראל יכולת להקצותם, כפי שיוצג בהמשך. המסקנה היא כי ברשות צה"ל תהיה רק כמות קטנה יחסית של טילים נגד טילים, ההגנה תהיה חלקית בלבד, והיא תקטן ותפחת ככל שהלחימה תימשך.

ישנם חסרונות נוספים למערכת המבוססת על טילי הגנה בלבד, הנובעים מאי־עמידה בדרישות המבצעיות נוכח האיום. כך, למשל, למערכת "כיפת ברזל" אין יכולת להתמודד עם איומי רקטות "קסאם" למיניהן וטילי "גראד" רגילים ומשופרים, הנורים לטווחים קצרים של כשלושה עד כ־15 ק"מ.[15] הסיבה לכך היא זמן המעוף הקצר של האיום. כמו כן, אין למערכת "כיפת ברזל" יכולת להגן מפני פצצות מרגמה. המשמעות היא שההגנה על יישובים הקרובים לגבול, עד כדי 10–15 ק"מ ממנו, לוקה בחסר:[16] יותר ממיליון תושבים, המתגוררים לאורך גבולות המדינה, יישארו חשופים לירי טילים מבלי שתהיה הגנה טובה עליהם. בנוסף לכך, לטילי ההגנה לסוגיהם אין כנראה יכולת להתמודד עם טילי שיוט, בעיקר לא עם P800 הרוסי.

הגדלת דִיוּקן של הרקטות תביא לקריסת התפיסה של ירי סלקטיבי, כלומר אי־יירוט האיומים שיפלו בשטחים פתוחים יביא לצורך ליירט את כולם וישפיע השפעה חמורה מבחינה כלכלית. זאת ועוד, סיום הלחימה יחייב חידוש המלאי של כל טילי ההגנה שנורו במהלכה. הצטיידות זו תימשך שנים רבות ובעלות גבוהה מאד, שעד השלמתה תיוותר המדינה חשופה לאיום.

מצדדי מערכת "כיפת ברזל" גורסים, כפי שאמר אלוף פיקוד הצפון דאז, גדי איזנקוט, כי היא "צריכה להיות מופנית בראש ובראשונה לשימור היכולת ההתקפית של צה"ל ולא להגנת אזרחים" וכי עליה להגן על תשתיות חיוניות של המדינה, על בסיסי צה"ל ועל נקודות לריכוז כוחות; המהלך ההתקפי שיבצע צה"ל יביא, תוך כשלושה ימים, לצמצום משמעותי של הירי ולפגיעה כזו באויב, שתביא להפסקת הירי,[17] ומכאן שהמערכת אינה נדרשת להתמודד עם כמות רבה של רקטות.

לדברי תא"ל (מיל') דני גולד, ששימש כראש מחלקת המחקר והפיתוח במשרד הביטחון, המערכת הקיימת מהווה הוכחה לנכונות המדינה למגן את אזרחיה וקניינים, כמו גם לאפשר את המשך פעולת המשק בעת מלחמה.[18] בנוסף לכך, מערכת "כיפת ברזל" מאפשרת לדרג המדיני מרחב תמרון רחב יותר בעת מהלך צבאי.[19] זאת ועוד, מחקר שערך עוזי רובין, בעבר ראש מנהלת "חומה" במשרד הביטחון, מצביע על כך, שבניגוד למלחמת לבנון השנייה, במהלכה נדרש חזבאללה לירות 75 רקטות בממוצע כדי להרוג אדם אחד, מערכת "כיפת ברזל" שיפרה את היחס פי חמישה, עד כדי צורך של חזבאללה לירות 375 רקטות כדי להרוג אדם אחד.[20]

מכלול הגנה המבוסס על לייזר כימי רב־עוצמה – יתרונות, חסרונות וישימות

מערכות לייזר קרקעיות – "נאוטילוס" ו"סקייגארד"

מערכת "נאוטילוס" פותחה לצורך הגנה על קריית שמונה מפני הקטיושות שנורו אליה מלבנון החל משנות השבעים של המאה הקודמת. הפיתוח החל ביוני 1996 והסתיים ביוני 2000, עם ביצוע שני ניסויים מוצלחים שכללו השמדת רקטות בעת מעופן. מאז יוני 2000 ועד נובמבר 2004 בוצעו עשרות ניסויים במערכת, במהלכם היא יירטה את כל 46 האיומים ששוגרו נגדה: 31 קטיושות ורקטות אחרות, חמישה פגזי ארטילריה 152 מ"מ ועשר פצצות מרגמה, מהן שלוש שנורו כמטח.[21]

מערכת "סקייגארד" מהווה, כאמור, פיתוח ישיר של מערכת "נאוטילוס". התכנון ההנדסי המפורט שלה נעשה בשנים 2000–2005, והוצג בפני הצבא האמריקאי ונציגי משרד הביטחון באוגוסט 2005. השיפורים העיקריים במערכת "סקייגארד", בהשוואה ל"נאוטילוס",[22] הם הקטנת ממדי המערכת פי ארבעה והגדלת שטף האנרגיה על המטרה פי ארבעה עד פי חמישה. כתוצאה מכך גדל הטווח היעיל שלה לכעשרה ק"מ (15 ק"מ עם אופטיקה אדפטיבית). מנתון זה ניתן לגזור, כי באמצעות שימוש בשמונה מערכות "סקייגארד" בלבד ניתן להגן על כל מרחב יישובי "עוטף עזה", כי ב־26 מערכות כאלו ניתן להגן על כל אזור הצפון – מקריית שמונה ועד קו חיפה־עפולה־בית שאן – וכי סך כולל של שמונים מערכות כאלו יוכל להגן על כלל ארבעים מרכזי האוכלוסין הגדולים והאתרים האסטרטגיים

במדינת ישראל.[23] בנוסף לכך, החברה המפתחת את "סקייגארד" התחייבה בפני משרד הביטחון לעמוד בסטנדרטים צבאיים מלאים (זמינות, אמינות, תחזוקה ויבילות) ולספק, על בסיס השלמת התכנון ההנדסי,[24] מערכות "סקייגארד" החל מ־18 חודשים מקבלת החלטה, במחיר קבוע ותוך נכונות לשאת בקנסות פיגורים.

מערכת "סקייגארד" צורכת להפעלתה חמישה סוגים שונים של גזים (חנקן פלואורי, מימן, אתילן, הליום, חמצן) וכן דלק מטוסים סילוני. כולם סחירים בשוק החופשי, אינרטיים, לא רעילים ולא מתפוצצים (עלולה להיווצר שריפה במקרה של פגיעה ישירה בהם). תוצרי הלוואי לאחר השימוש בלייזר (ה"לְזירה") כוללים פחמן פלואורי וחומצה פלואורית (HF/DF) המסוכנים לבריאות. טווח הביטחון הנדרש מהם הוא מאה מטרים, וירד עד עשרים־שלושים מטרים, אם יותקן מסנן מיוחד במערכת. ליד כל יחידת "סקייגארד" קרקעית מוצבות שתי מכליות (בגודל מכלית רגילה לאספקת דלק), המכילות את הגזים והדלק הנדרשים לארבעים שניות של לזירה רצופה (מתאים להשמדת עשרים איומים בממוצע). זמן מיתוג ממכלית אחת לשנייה הוא מספר שניות וזמן החלפת מכלית ריקה במלאה הוא בן שתיים לשלוש דקות.

יתרונותיה של מערכת "סקייגארד" הקרקעית הם גם במושגי יסוד בתחום הירי. המושג "החטאה" אינו קיים במערכת, עקב הנעילה של קרן הלייזר על האנרגיה החוזרת מהמטרה. למעשה, יש למערכת "מחסנית אין סופית" וזמינה של דלקים וגזים הנדרשים לתפעולה, שניתן יהיה לספקם בדומה לתדלוק מטוסי חיל האוויר. המערכת תשמיד כל מטרה שתיכנס לטווח הכיסוי שלה (כ־10–15 ק"מ), כפי שהוכח בניסויים, ותהיה יעילה הן נגד פצצות מרגמה והן נגד מגוון סוגי הטילים והרקטות, כולל טילי "שיהאב" 4 הנורים לטווחים של עד כ־2,000 ק"מ, וגם תענה לאיום של טילי השיוט. הקצב הממוצע של השמדת מטרות על ידי המערכת הוא אחת לכשלוש שניות, כולל המעבר למטרה הבאה. כך יתאפשר להשמיד מטחים של טילים הנורים בו־זמנית. לדוגמה, נדרשות כ־38 שניות מרגע כניסתה של רקטת "גראד" משופרת, המשוגרת לטווח של ארבעים ק"מ, לטווח היעיל של "סקייגארד" (15 ק"מ) ועד לפגיעתה בקרקע. המערכת תוכל להשמיד מטח של כ־11 רקטות כאלו, שנורו בו־זמנית (שתי מערכות שיגנו על אותו אתר יוכלו להשמיד 22 איומים שנורו בו־זמנית).

מערכת "סקייגארד" פועלת במהירות האור, ולפיכך אין צורך בשדרוגה כאשר מופיעים איומים מתקדמים יותר. היא גם מאפשרת ליירט את המטרה מיד לאחר גילויה, ללא צורך בשערוך נקודת היירוט. מכאן שניתן להשמיד באמצעותה איומים תוך פחות מחמש שניות מרגע שיגורם או מרגע כניסתם לטווח היעיל שלה. זאת ועוד, עלות היירוט של המערכת נמוכה ביותר – כ־1,000–3,000 דולר[25] (מחיר הגזים והדלק המשמשים ליצירת קרן הלייזר משתנה בהתאם לטווח) – לעומת

עלות של מאות אלפי דולרים (שני טילי "כיפת ברזל" עבור מטרה אחת) ועד כמה מיליוני דולרים (עלותם של שני טילים כמו "שרביט קסמים" או "חץ", הדרושים לאותה פעולה). למערכת "סקייגארד" יש יכולת הגנה עצמית מפני כל איום בליסטי הנורה אליה, הטכנולוגיה שלה זמינה והיא הוכחה בעשרות ניסויים.

החיסרון העיקרי של מערכת "סקייגארד" הוא ירידה משמעותית בטווח היעיל של קרן הלייזר כאשר יש צורך לחדור עננות סמיכה וצפופה (מ־5/8 ומעלה). במצב זה יש צורך להסתמך על טילי ההגנה. גם אז תוכל מערכת "סקייגארד" ליירט איומים בליסטיים עם רדתם מתחת לבסיס הענן, כאשר קרן הלייזר "תמתין" להם בנקודה בה הם ייחשפו מחדש.

מערכת "סקייגארד" מוטסת

בתחילת שנות התשעים של המאה הקודמת החלה ארצות הברית לפתח מערכת לייזר רב עוצמה מוטסת, הנקראת ABL, שמותקנת במטוס "בואינג" 747. ייעודה הוגדר כהשמדת טילים בליסטיים בשלב ההאצה שלהם, בטווחים של מאות ק"מ מהמטוס המיירט. לאחר תהליך פיתוח ממושך בוצע בפברואר 2010 ניסוי ראשון במערכת, בו יורטו שני טילים בליסטיים לאחר שיגורם, בטווח קרוב למאה ק"מ ממטוס ה־ABL.[26] הייתה זו היסטוריה בהתהוותה. להצלחת הניסוי משמעות רבה: לראשונה בהיסטוריה הושמדו טילים בליסטיים מהאוויר, ובטווחים גדולים מאד. הניסוי הוכיח, אפוא, את ישימותה הטכנולוגית של המערכת.

היירוטים של המערכת המוטסת מתבצעים מעל העננים, מעל תופעות מזג האוויר. כל טיל שמשוגר לטווחים של כשלושים ק"מ ומעלה מגיע לגבהים העולים על 40,000 רגל, וככל שהטווח עולה – כך גדל גם הגובה אליו הוא מגיע. לכן, המערכת המוטסת תוכל להשמיד כל איום שמשוגר מטווחים שנעים החל משלושים ק"מ ועד לטווח המרבי ממנו מאוימת ישראל – כאלפיים ק"מ. זאת ועוד, כיוון שתחילת היירוט תהיה בטווחים גדולים מאד מהמטוס המיירט, תהיה לו אפשרות להשמיד גם ראשים מתפצלים, כאשר כל "פיצול" ייורט בנפרד.

בשנת 2003 הציעה חברת "נורתרופ־גרומן" למשרד הביטחון להתקין מערכת "סקייגארד" רגילה במטוס תובלה בינוני. כינויה של המערכת היה ARIEL. תצורה זו אפשרה להשמיד איומים בטווחים של כ־130 עד 150 ק"מ מהמטוס המיירט. מאמר זה מציע לבחון תצורה משופרת של מערכת "סקייגארד" מוטסת: הגדלת ההספק לשלושה מגוואט והגדלת קוטר האופטיקה ל־1.5 מטר, כפי שבוצע ב־ABL. ניתן להתקינה במטוס גדול, כמו "בואינג" 300–747, שיאפשר לשאת כמות גדולה של דלק וגזים לביצוע מספר רב של יירוטים. מספר מטוסים כאלה, שיטוסו "מסביב לשעון", יוכלו ליירט כל איום בליסטי, וזאת בשילוב עם שכבות ההגנה של טילים נגד טילים.

יכולותיה הצפויות של מערכת "אריאל" המשופרת, בדומה למערכת ABL, הן יירוט איומים בליסטיים שנמצאים בטווח של עד כ־400 ק"מ ממנה, ומעל גובה של כ־30,000 רגל. חישובים ראשוניים מראים שניתן להפיק כמאתיים ויותר לזירות, קרי העברה קבועה של אנרגיית לייזר אל המטרה כדי להשמידה, עד הגעה לצורך לתדלוק המטוס מחדש בגזים ובדלק הדרושים ללזירה. חישובים תרמיים מראים כי ניתן להניח זמן לְזירה נדרש של כחמש שניות להשמדת האיום של טילי "שיהאב" ו"סקאד" D, ועוד כשתי שניות למעבָר לאיום הבא. זמן הלזירה שיידרש עבור יתר האיומים, מ"סקאד" C ומטה, הוא כשלוש שניות, ועוד שתי שניות למעבָר לאיום הבא. זמני היירוט (ברוטו) יהיו שבע שניות וחמש שניות בהתאמה (יצוין, כי כל הנתונים וההנחות שהוצגו לעיל מחייבים בדיקת היתכנות מדוקדקת, שתכלול גם ניסויי טיסה). מערכת "אריאל" תוכל ליירט כל איום בליסטי שיֻיָרה לטווח העולה על כשלושים ק"מ ובמטחים צפופים, ככל שהאויב יוכל לייצר. יתר הרקטות הטקטיות, מ"גראד" רגיל ומַטה, שאינן עוברות גובה של 30,000 רגל בעת מעופן, ייורטו על ידי מערכות "סקייגארד" הקרקעיות וטילי "כיפת ברזל", בטווחים בהם הם יעילים.

הפעילות במערכת ה־ABL הופסקה בשנת 2011. לדבריו של רוברט גייטס, שר ההגנה לשעבר של ארצות הברית, הסיבה לכך הייתה שאין למערכת די הספק כדי לאפשר למטוס לפעול מחוץ לגבולותיה של איראן.[27] הגבלה זו אינה רלוונטית לישראל, משום שהמטוס יוכל לשהות באוויר מעל שטחה־שלה ויירט את האיומים בשלב החדירה שלהם, כשמרחקם הוא כ־400 ק"מ ומטה ממטרתם.[28]

מִתאר תקציבי

בניתוח המִתאר התקציבי של מערכת הגנה משולבת יש להניח את הנחות היסוד הבאות:

1. מִתאר הלחימה הוא כמפורט בפרק "מתאר האיום" לעיל.
2. מערכת הביטחון תמשיך ותשקיע במערכות טילי הגנה.

הערכת עלות ההצטיידות בטילי הגנה בלבד מתבססת על ההנחות הבאות: הכנת מלאי לארבעים ימי לחימה והצטיידות בטילים במקום אלה שנורו במהלכם של שלושים ימי הלחימה. כדי להגיע לסיכוי הצלחה סביר ליירוט איום יידרשו שני טילי הגנה. מחיר טיל "כיפת ברזל" הוא 100,000 דולר,[29] מחיר טיל "שרביט קסמים" הוא 1,250,000 דולר ומחיר טיל "חץ" 2 /3 הינו כ־3,000,000 דולר.

הערכת העלות הצפויה של אלמנט הלייזר המוטס והקרקעי במערכת המשולבת מתבססת על חמש מערכות "סקייגארד" מוטסות ושמונים מערכות "סקייגארד" קרקעיות. תשתיות המכ"ם והתקשורת עבור מערכות טילי ההגנה תתמוכנה גם במערכות הלייזר.

ההשקעה הנדרשת להצטיידות בטילי הגנה בלבד (ללא משגרים, ללא מערכות תומכות ותשתיות) היא כדלהלן: ליירוט 250 רקטות קצרות טווח בכל יום, העתידות ליפול בשטחים בנויים (מתוך 800 רקטות שישוגרו), יידרשו 500 טילי "כיפת ברזל", שעלותם תגיע עד שני מיליארד דולר להתכוננות לארבעים ימי לחימה; יירוטם של מאה טילים ורקטות לטווח בינוני יחייב שימוש במאתיים טילי "שרביט קסמים" בכל יום לחימה, בעלות שתסתכם בעשרה מיליארד דולר עבור הכנות לארבעים ימי לחימה; עלותם של מאתיים טילי "חץ" ו"פטריוט", ליירוט האיומים ארוכי הטווח בכל יום, תגיע עד 24 מיליארד דולר. בסה"כ יהיה צורך בכ־36 מיליארד דולר עבור הצטיידות במלאי לארבעים ימי לחימה. מחיר ה"לחיצות על ההדק" בלבד ביום לחימה אחד יהיה כ־900 מיליון דולר. מחיר ההצטיידות לאחר הלחימה במלאי שישלים את כמות הטילים שיירו במשך שלושים ימי הלחימה יגיע ל־27 מיליארד דולר (3/4 מהמחיר עבור ההצטיידות לארבעים ימים). העלות הכוללת של הכנת מלאי טילים לארבעים יום והצטיידות בהם מחדש לאחר שלושים ימי לחימה תגיע ל־63 מיליארד דולר. אלה סכומים שלא ניתן לעמוד בהם ויש להניח שלעולם לא יוקצו.

השקעה במערכות "סקייגארד" קרקעיות ומוטסות

מערכות לייזר קרקעיות

המִפרט שהגישה חברת "נורתרופ־גרומן" בשנת 2007 נוקב במחירים הבאים:

- 310 מיליון דולר עבור שלוש מערכות "סקייגארד" ראשונות.
- ארבעים עד חמישים מיליון דולר עבור מערכת בייצור (בהתאם לכמות שתוזמן).

המחיר כולל תקשורת וכן מכ"ם ייחודי לכל מערכת "סקייגארד", שמחירו כ־15 מיליון דולר. יש צורך במכ"ם אחד שיזין ארבע עד חמש מערכות, כך שניתן להניח מחיר של כשלושים מיליון דולר למערכת "סקייגארד" בייצור סדרתי. המחיר עבור 77 המערכות הנותרות יהיה כ־2.3 מיליארד דולר. בנוסף לכך יידרשו מאתיים מיליון דולר (הערכה) לתשתיות תדלוק ו־300 מיליון דולר (הערכה) לתשתיות מנהלתיות ותחזוקתיות ולחלפים. בסה"כ יידרשו, אפוא, כ־3.1 מיליארד דולר עבור שמונים מערכות "סקייגארד" קרקעיות, להגנה על ארבעים האתרים החיוניים במדינה ועל מרכזי האוכלוסין שלה.

מערכות לייזר מוטסות

שלב הפיתוח למערכות מוטסות ידרוש עד מאה מיליון דולר עבור "בואינג" 747 משומש (הערכה) וכ־250 מיליון דולר לבניית אב טיפוס של מערכת "סקייגארד"

מוטסת ראשונה (מבוסס על מכתבה של חברת "נורתרופ־גרומן", בו ננקב סכום של 177 מיליון דולר למערכת "סקייגארד" קרקעית ראשונה).

המערכת המוטסת פשוטה ליישום בהשוואה למערכת הקרקעית, עקב ביטול הצורך במרב יכולותיה של מערכת התת־לחץ הנדרשת לייצור קרן הלייזר (בגובה 40,000 רגל יש תת־לחץ באופן טבעי). על הוצאות אלו יתוספו כמאה מיליון דולר לצרכי תכנון וביצוע ההתקנה במטוס ומאה מיליון דולר נוספים לצרכי ניסויים. כמו כן, יידרשו כמאה מיליון דולר לתשתיות תחזוקה ותדלוק מערכות הלייזר על הקרקע ועוד כחמישים מיליון דולר להוצאות אחרות – סה"כ כ־700 מיליון דולר לשלב הפיתוח וייצור המטוס הראשון.

הצטיידות בארבע מערכות "סקייגארד" מוטסות נוספות תעלה כ־120 מיליון דולר למטוס עם התקנה ועוד חמישים מיליון דולר מחיר מערכת הלייזר (בהשוואה לשלושים מיליון דולר – מחירה של מערכת "סקייגארד" קרקעית) וכעשרים מיליון דולר לצרכי חלפים, תמיכה תחזוקתית והוצאות נוספות. מחיר מטוס אחד בהצטיידות יהיה לפיכך כ־190 מיליון דולר, ומחירם של ארבעת המטוסים הנוספים יהיה כ־760 מיליון דולר. מחיר ההצטיידות הכולל במערכות לייזר קרקעיות ומוטסות, כולל תמיכה תחזוקתית, מערכות עזר מבצעיות ועוד, צפוי שיגיע לכ־4.6 מיליארד דולר – השקעה שתיפרס על פני כשמונה שנים. זו השקעה שניתנת לביצוע מהבחינה הכלכלית.

עלות שלושים ימי לחימה עם מערכות "סקייגארד" בלבד

עלות יום לחימה אחד, שיכלול אלף "לזירות" להשמדת כל אלף האיומים, יגיע לשני מיליון דולר. עלות 72 שעות טיסה (שלושה מטוסים ברציפות, לפי 15,000 דולר לשעה) תהיה 11 מיליון דולר, ובסה"כ 13 מיליון דולר ליום. זאת, בהשוואה ל־900 מיליון דולר ליום שהם מחיר ההתגוננות (החלקית) עם מערכות טילי ההגנה. עלותם של שלושים ימי הלחימה עם מערכות "סקייגארד" תהיה כ־400 מיליון דולר, בהשוואה ל־63 מיליארד דולר – עלות טילי ההגנה בלבד.

טבלת השוואה – ביצועים ועלויות

מיירט / סוג איום, תכונות ועלויות	"כיפת ברזל"	"שרביט קסמים"	"חץ" 2	"חץ" 3	מערכת "סקייגארד" קרקעית	מערכת "סקייגארד" מוטסת
פצמ"רים	/	/	/	/	V[1]	/
טיל שיוט P800	/	/	/	/	V[1] מטח של 4–5 טילים	/
"קסאמים" ו"גראדים" 12–15 ק"מ	/	/	/	/	V[1]	/
"גראדים" לטווח 15–40 ק"מ	V	/	/	/	V[1] מטח של 10–12 טילים	V[1,2] מטח של 10–30 טילים
"פג'ר" 3, 5	V	אולי	/	/	V[1] מטח של 9–10 טילים	V[1,3] מטח של 15–23 טילים
"זלזאל", M600, F110	/	V	אולי	/	V[1] מטח של 4–5 טילים	V[1,3] מטח של 18–52 טילים
"סקאד" B, C	/	אולי	V	אולי	V[1] מטח של 2–3 טילים	V[3,4] מטח של 56–64 טילים
"סקאד" D, "שיהאב" 3, 4	/	/	/	V	V[1] מטח של 1–2 טילים	V[3,4] מטח של 15–33 טילים
עלות ירוט אחד (שני טילים)	200,000 דולר	2.5 מיליון דולר	6 מיליון דולר	6 מיליון דולר	עד 3,000 דולר	עד 5,000 דולר
עלות יום לחימה	50 מיליון דולר (250 ירוטים)	250 מיליון דולר (100 ירוטים)	300 מיליון דולר (50 ירוטים)	300 מיליון דולר (50 ירוטים)	2–3 מיליון דולר	2–3 מיליון דולר, כולל 72 שעות טיסה

1. השמדת איום כל שלוש שניות.
2. ירי לטווח מעל שלושים ק"מ.
3. ייורטו איומים מתחת לטווח של 400 ק"מ ומעל גובה של 30,000 רגל.
4. זמן "לזירה" (משוער) – שלוש־חמש שניות.

יעילותו של הפתרון המשולב

הפתרון המשולב מאפשר ליישם, הן מהבחינה המבצעית והן מהבחינה הכלכלית, מערכת הגנה כוללת, אפקטיבית ויעילה להגנת כל העורף. לפי המִתאר התקציבי,

תמורת השקעה של כ־4.6 מיליארד דולר במערכות הלייזר הקרקעיות והמוטסות ניתן לחסוך למעלה מ־55 מיליארד דולר מעלותם של טילי ההגנה בלבד, דבר ההופך את המערכת המשולבת לבת־יישום.

המערכת המשולבת תכלול כחמישה מטוסי לייזר רב עוצמה ("אריאל"), חמש שכבות הגנה של טילים נגד טילים ("כיפת ברזל", "שרביט קסמים", "חץ" 2, "חץ" 3 ו"פטריוט") בכמויות ובפריסה כפי שייקבעו על ידי מערכת הביטחון, ושמונים מערכות "סקייגארד" קרקעיות. אותן מערכות מכ"ם, תקשורת ושליטה, המיועדות לתמוך בטילי ההגנה, תתמוכנה גם במערכות הלייזר הקרקעיות והמוטסות.

שילוב זה עומד בכל הקריטריונים הנדרשים ממערכת הגנה אולטימטיבית אידיאלית. מערכת משולבת כזו תאפשר הגנה מפני פצצות מרגמה וטילי שיוט, הגנת היישובים הקרובים לגבול ומענה הגנתי כפול ברוב המקרים – על ידי מערכות הלייזר ועל ידי טילי ההגנה. מטעמי חיסכון, יש להעדיף תמיד את הפעלת מערכות הלייזר, בעוד שטילי ההגנה יהוו גיבוי למערכות הלייזר הקרקעיות במקרה של מזג אוויר גרוע ובעת הצורך להגן מפני מטחים צפופים במיוחד.

מבצע "עמוד ענן" כמקרה ייחודי – הגנה מפני כל האיומים המשוגרים מרצועת עזה

מבצע "עמוד ענן" הוא ייחודי, עקב היותו העימות הראשון בו הייתה למדינת ישראל מערכת הגנה אקטיבית – "כיפת ברזל" – שאף נעשה בה שימוש נרחב יחסית. המבצע החל, כפי שהמליץ הדרג הצבאי לדרג המדיני, כמהלך סדור ומתוכנן, שיעדיו היו חיזוק ההרתעה, פגיעה קשה במערך הרקטות של חמאס וארגוני הטרור האחרים ופגיעה כואבת בהם עצמם, והפסקת הירי הרקטי מרצועת עזה על מדינת ישראל.[30] מהלך הפתיחה של המבצע כלל את חיסול אחמד ג'עברי, מפקד הזרוע הצבאית של חמאס ברצועת עזה, בתקיפה מהאוויר, ותקיפה אווירית נוספת שיעדיה היו מחסנים ובורות שיגור שבהם היו רקטות "פג'ר" 5 לטווח של כ־75 ק"מ. ניכר כי צה"ל פעל לקיצור משך הלחימה. הדבר בא לידי ביטוי הן בחתירת הדרג המדיני להשגת מנגנון סיום למבצע[31] והן בהנחיית הרמטכ"ל, בני גנץ, "להמשיך ולתקוף בכל הכוח, להגביר את הקצב",[32] וזאת בהתאם לתפיסה כי יש להשיג את היעדים במהירות.

אין ספק שלמערכת "כיפת ברזל" הייתה תרומה משמעותית למורל של העורף בעת הלחימה. במהלך המבצע ירה חמאס 1,506 רקטות לעבר מדינת ישראל, אולם רק 479 מתוכן נורו לשטחים מאוכלסים. "כיפת ברזל" הצליחה ליירט 421 רקטות ולהשיג בכך שיעורי הצלחה של 84 אחוזים.[33]

אין כל ספק שככל שמערכת ההגנה תהיה יעילה יותר, המורל של העורף ויכולתו להמשיך ולהתמודד יהיו טובים באופן משמעותי. מבצע "עמוד ענן"

הוא הזדמנות נאותה לבחון את טיעוני מאמר זה בדבר המגבלות והחסרונות של השימוש במערכת המבוססת על טילי הגנה בלבד, לעומת היתרונות של שילוב שתי הטכנולוגיות – טילי הגנה ולייזר רב עוצמה – במערכת הגנה כוללת. בבחינה זו נתייחס לשתי נקודות עיקריות: אי־היכולת של מערכות טילי ההגנה להגן על היישובים הסמוכים לגבול ומחירם של טילי ההגנה (שהופך למגבלה על כמות הטילים בהם ניתן להצטייד).

שתי ממשלות הכירו במגבלותיה של מערכת "כיפת ברזל" להגן על אתרים הקרובים לגבול. ממשלת אולמרט החליטה בתחילת 2008 (לאחר שהובהרו לה מגבלותיה של המערכת) למגן את כל הבתים המרוחקים עד 4.5 ק"מ מהגבול (איום הייחוס אז היה "קסאם" 1 האיטי). ממשלת נתניהו החליטה במחצית השנייה של 2012 למגן את כל הבתים עד מרחק של שבעה ק"מ מהגבול. השר להגנת העורף, מתן וילנאי, אף הצהיר בנובמבר 2011 כי כל היישובים עד מרחק של 15 ק"מ מהגבול ימוגנו באופן מלא.[34]

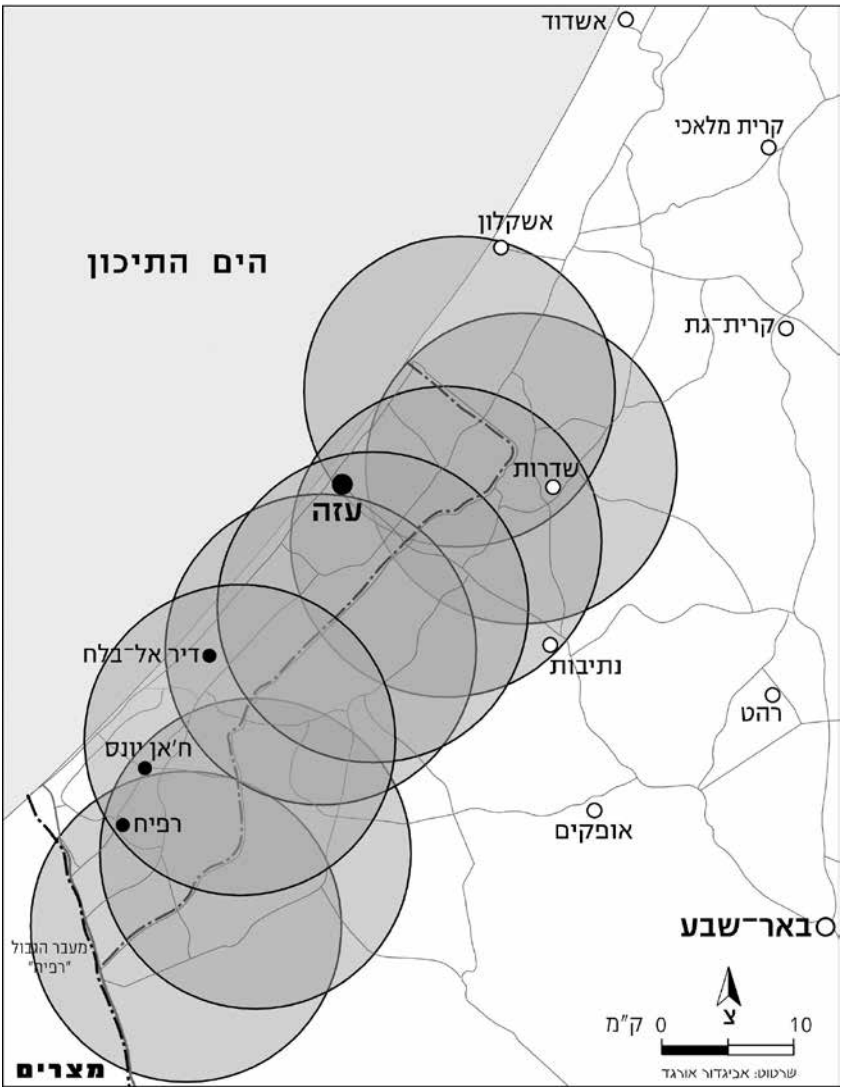
המציאות בעת מבצע "עמוד ענן" אכן הוכיחה את הצורך בהגדלת טווח המיגון: לא הייתה כל הגנה מעשית על העיר שדרות ויישובי "עוטף עזה" (למעט מקרים בודדים של יירוט רקטות באזור שדרות, ששוגרו ככל הנראה מחלקה הדרומי של רצועת עזה – טווח ירי מספיק גדול שאִפשר יירוטן באמצעות מערכת "כיפת ברזל"). מערכת "כיפת ברזל" הגנה על יישובים המרוחקים מהגבול, כמו באר שבע, אשדוד ואשקלון, אך גם זו לא הייתה הגנה מלאה, כפי שנראה בהמשך.

מבצע "עמוד ענן" הסתיים לפני ששוגרו כל טילי "טמיר" (טילי היירוט של "כיפת ברזל") שהיו ברשות צה"ל. קל לדמיין את אשר היה קורה אם המבצע היה נמשך עוד מספר ימים, כשצה"ל היה מגיע ל"תחתית החבית" בכל הקשור למלאי של טילי ההגנה. אין ספק שלקראת מצב זה, ממשלת ישראל ופיקוד צה"ל היו נאלצים לעמוד בפני מערכת לחצים משמעותית לסיים את המבצע לפני כלות כל הטילים, דבר שהיה משפיע על כל תוצאה של משא ומתן הקשור בסיום הלחימה. לחילופין, אם הלחימה לא הייתה נפסקת במועד, קל לדמיין את גודל האכזבה של האוכלוסייה ואת המכה המורלית שהייתה סופגת, וזאת בנוסף לפגיעות הפיזיות. יתר על כן, לא ניתן להתעלם מדוח מס רכוש, המציג את רשימת הנזקים שנגרמו בעת מבצע "עמוד ענן" בערים עליהן הגנה מערכת "כיפת ברזל", המסתכמים במאות פגיעות במבנים ובמכוניות. בנוסף לכך, דוח של משטרת ישראל מציין כי חבלני המרחב הדרומי טיפלו ב־109 נפילות של רקטות בתוך שטחים מיושבים. המסקנה משני נתונים אלה היא שההגנה אותה סיפקה מערכת "כיפת ברזל" לא הייתה מספקת.

נבחן עתה את שילובן של מערכות "סקייגארד" בהגנה מפני "האיום העזתי". לרצועת עזה אין עומק אסטרטגי. רוחבה כמעט לכל אורכה הוא כשבעה ק"מ

ורק בחלקה הדרומי מגיע הרוחב עד כ־13 ק"מ. שרטוט מס' 1 מציג את הכיסוי המבצעי של שמונה מערכות "סקייגארד" שיוצבו סביב רצועת עזה במרחק של כק"מ אחד מהגבול (מאחורי קפלי קרקע, למניעת ירי בכינון ישיר אליהן). למעט אזור מצומצם אחד, כל נקודות השיגור מכוסות על ידי מערכות "סקייגארד".

שרטוט מס' 1: הכיסוי המבצעי של שמונה מערכות "סקייגארד" סביב רצועת עזה



אין צורך בתהליכי שיערוך למערכת "סקייגארד". הווקטור אל המטרה מתקבל תוך שנייה אחת עד שתי שניות מרגע שיגור האיום, והמטרה תושמד תוך שתיים עד שלוש שניות נוספות, לרוב בעודה מעל שטח הרצועה, ואין זה משנה לאן תשוגר – לשדרות או לתל אביב. עקב הטווחים הקצרים, הירי על יישובי "עוטף עזה" הוא רובו ככולו שטוח מסלול. הגובה המרבי שאליו מגיע האיום (למעט "קסאם" 1) הוא כ־550 מטרים ("גראד" משופר הנורה לטווח של 15 ק"מ). גובה זה הוא מתחת לבסיס הענן האופייני, המתחיל בכ־700 מטרים ומעלה. המסקנה היא שגם בתנאי מזג אוויר קשים, מערכות "סקייגארד" יגנו על יישובי "עוטף עזה".

למעשה, מערכות הלייזר מקיפות את רצועת עזה במעין "חומת מגן" שתיירט כל איום שיֻיָרה ממנה לכל מטרה בישראל. איום זה כולל גם את רקטות "פג'ר", להן טווח של כשבעים ק"מ.

ההשקעה הנדרשת בהצבת שמונה מערכות "סקייגארד" מול רצועת עזה היא כ־500 מיליון דולר, ותחילת האספקה תהיה תוך כשנתיים. השילוב עם מערכות "כיפת ברזל" יכול להיות מיטבי: מערכות "כיפת ברזל" תוצבנה במקומות המרוחקים יחסית מהגבול, עליהם ביכולתן להגן, בעוד שהיירוט הראשוני נגד כל האיומים יתבצע עם מערכות "סקייגארד", שלהן יש, כאמור, "מחסנית אין סופית". כל מה ש"יסתנן" (אם בכלל) דרך מערכות "סקייגארד" יישאר לטיפולן של מערכות "כיפת ברזל". זהו שילוב שיאפשר הגנה ללא כל לחץ, בעיקר על מקבלי ההחלטות. אז גם יינתן אורך נשימה לממשלת ישראל לשקול כל החלטה, ביודעה שהעורף מוגן בצורה הטובה ביותר.

אי־הרלוונטיות של מערכות הגנה המבוססות על "לייזר מצב מוצק"

דחיית היישום של הלייזר הכימי ("נאוטילוס" ו"סקייגארד"), הזָמין והמוכח, בציפייה ללייזר על בסיס מצב מוצק, ולכאורה מתקדם יותר, אינה מעוגנת בשום מציאות טכנית.[35] ללייזר מצב מוצק יש מספר מגבלות מהותיות: ראשית, מגבלת הספק. ההספק הגבוה ביותר שהושג בטכנולוגיה זו – כמאה קילוואט בלבד, שהושג על ידי חברת "נורתרופ־גרומן" בפברואר 2009 באמצעות טכנולוגיית לוחיות – הינו כעשירית מהדרוש ליירוט טילים. הגעה להספק של מגוואט ומעלה תחייב פריצת דרך טכנולוגית, שאינה נראית בת־יישום; שנית, נצילות מערכת הלייזר על בסיס מצב מוצק גדולה אך במעט מעשרה אחוזים. לכן, ליצירת קרן בהספק הנדרש של מגוואט אחד לפחות, נדרש להשקיע כתשעה מגוואט הספק חשמלי, מתוכם כשמונה מגוואט יהפכו לחום, אותו יש לפזר בעת הלזירה – קרי שתיים עד שלוש שניות. אין בנמצא כל טכנולוגיית קירור המסוגלת לבצע זאת, ולכן אין סיכוי למימושה של המערכת בעתיד הנראה לעין; שלישית, למערכת כזו

יש רגישות יתר להשפעות מזג האוויר, הנובעות מאורך הגל הקצר שבו פועלים לייזרים אלה (כמיקרון אחד, לעומת 3.8 מיקרון של "נאוטילוס" ו"סקייגארד"). נִיחוּת הקרן בעת המעבר באטמוספרה יהיה גדול מאד בהשוואה למערכות לייזר על בסיס כימי. בנוסף, קיימת סכנת עיוורון מאוֹר מוחזר, הנובעת מאותו אורך גל. זאת ועוד, אין כל תחזית שתצביע על מועד להשלמת פיתוחה של מערכת כזאת, שתאפשר הגנה על ריכוזי אוכלוסייה ואתרים אסטרטגיים.

מכלול מגבלות זה מהווה מחסום טכנולוגי, המונע את יישומה של מערכת לייזר רבת עוצמה המבוססת על מצב מוצק.[36]

סיכום

לנשק הבליסטי ולטילי השיוט המדויקים יש פוטנציאל הרס של התשתיות החיוניות למדינת ישראל, והם מהווים איום על חייהם של אלפים רבים. מערכת המבוססת על טילי הגנה בלבד אינה ישימה, עקב ההוצאה הכספית הכרוכה בהצטיידות ונוכח אי־עמידתה בחלק מהיעדים המבצעיים הנדרשים להגנה בסיסית. למרות זאת, יש להמשיך בפעילות הנוכחית של הקמת חמש שכבות הגנה המבוססות על טילי הגנה, וזאת כדי להביא לשילובן של טכנולוגיות אלו עם מערכות הלייזר רב העוצמה.

השקעה של כ־4.6 מיליארד דולר בשמונים מערכות קרקעיות ובחמש מערכות מוטסות של "סקייגארד", שתימשך כשמונה שנים, תביא להקמת מערכת משולבת עם כל מרכיביה של מערכת טילי ההגנה. מערכת משולבת כזו תעמוד בכל הדרישות מ"מערכת אידיאלית": היא תגן מפני כל איום, בכל עת, בכל מזג אוויר ולמשך כל זמן שיידרש – והכל בעלות מזערית ותוך חיסכון משמעותי.

על ממשלת ישראל "לשוב אל שולחן השרטוט", להכיר ביתרונותיה של המערכת המשולבת ולפעול בהתאם – בעיקר מול שלטונות ארצות הברית – בכל הקשור להתנעה מחודשת של הפעילות במערכות "סקייגארד", שאם לא כן, עלולה מדינת ישראל להיאלץ להתמודד עם משבר חמור בעימותים העתידים לבוא.

הערות

1 עמוס הראל, "צ'יקו תמיר חושב שתוכנית גנץ עלולה להוביל לאסון", **הארץ**, 18 ביולי 2013.
2 עמיר רפפורט, "גולנצ'יק", **מעריב**, 28 בינואר 2004.
3 זאב קליין וחזי שטרנליכט, "מתן וילנאי: 'נותקף באלף טילים ליום'", **ישראל היום**, 3 ביוני 2011, http://www.israelhayom.co.il/site/newsletter_article.php?id=11489
4 משרד מבקר המדינה, **דו"ח שנתי 59א לשנת 2008**, מארס 2009, עמ' 13–20.
5 יהודה וגמן, "מדוע צה"ל מתקשה להצליח?", **מערכות**, 419, יוני 2008, עמ' 11.
6 גבריאל סיבוני, "מהאִנתִפאדה השנייה דרך מלחמת לבנון השנייה למבצע 'עופרת יצוקה'", **צבא ואסטרטגיה**, כרך 1, גיליון 1, אפריל 2009.
7 גיורא איילנד, "מבצע 'עמוד ענן' – היבטים אסטרטגיים", בתוך: שלמה ברום (עורך),

לאחר מבצע "עמוד ענן" (רצועת עזה, נובמבר 2012), מזכר 123, המכון למחקרי ביטחון לאומי, תל אביב, 2012, עמ' 12.

8 רן דגוני, "סגן הרמטכ"ל בני גנץ: 'במלחמת לבנון השלישית ננצח; כשנוציא את הסוסים מהאורווה, יכאב מאוד ללבנון'", **גלובס**, 2 ביוני 2010, http://www.globes.co.il/news/article.aspx?did=1000563836 .

9 גדי איזנקוט, "השתנות האיום? המענה בזירה הצפונית", **צבא ואסטרטגיה**, כרך 2, גיליון 1, יוני 2010, עמ' 20.

10 עפר שלח ויואב לימור, **שבויים בלבנון**, ידיעות ספרים, תל אביב, 2007, עמ' 221.

11 זאב קליין וחזי שטרנליכט, "מתן וילנאי: 'נותקף באלף טילים ליום'".

12 גדי איזנקוט, "השתנות האיום? המענה בזירה הצפונית".

13 עמוס הראל, "האלוף גנץ: 'אני מרוצה מיכולת ישראל כלפי איראן; אנחנו נמצאים במקום טוב – ונהיה במקום טוב יותר'", **הארץ**, 31 בדצמבר 2010, http://www.haaretz.co.il/news/politics/1.1238152.

14 המִתאר גובש באמצעות הסתמכות על כלל הירי נגד ישראל במלחמת לבנון השנייה ובמבצע "עופרת יצוקה".

15 מכתב עמותת "מגן לעורף" לשר הביטחון: "ביצועים צפויים של כיפת ברזל", 15 בדצמבר 2009.

16 יפתח שפיר, "'כיפת ברזל' – מלכת המערכה", בתוך: שלמה ברום (עורך), **לאחר מבצע "עמוד ענן"**, עמ' 36.

17 גדי איזנקוט, "מאפייניו של עימות אפשרי בזירה הצפונית ובעורף", הרצאה בסמינר לזכר חללי מלחמת לבנון השנייה, אוניברסיטת חיפה, 30 בנובמבר 2010, http://www.youtube.com/watch?v=l0xkjirjvCI

18 עוזי רובין, "מערכת ההגנה האקטיבית 'כיפת ברזל' בפעולה: הערכה ראשונית", *Perspectives* 151, מרכז בגין־סאדאת, אוניברסיטת בר אילן, 31 באוקטובר 2011.

19 נועם ברקן, "מושלים בכיפה", **ידיעות אחרונות**, 11 באפריל 2011.

20 יובל אזולאי, "מחיר הדמים: כמה רקטות נדרשות כדי להרוג ישראלי אחד?", **גלובס**, 27 באפריל 2012.

21 יצחק בן ישראל, ראיון ליועז הנדל, **מקור ראשון**, 29 בדצמבר 2006.

22 מצגת חברת "נורתרופ־גרומן" למשרד הביטחון, ינואר 2007.

23 מטעמי יתירות, הכוונה להציב שתי מערכות "סקייגארד" להגנת כל אתר. דבר זה יביא, בין השאר, להכפלת כמות האיומים שייורטו. אם קצב הגעת האיומים יהיה קטן מ־1.5 שניות בממוצע, כל האיומים יושמדו. ראו טבלת סיכום יכולות ועלויות במאמר זה.

24 Dr. Josef Shwartz, Northrop-Grumman, *Year 2008 Multinational BMD Conference*, Honolulu, September 2008.

25 יצחק בן ישראל, ראיון ליועז הנדל, **מקור ראשון**, 29 בדצמבר 2006.

26 "ABL's Successful Shootdown", *DT Defensetech*, February 12, 2010, http://defensetech.org/2010/02/12/abls-successful-shootdown/

27 Subrata Ghoshroy, "Coming not so soon to a theater near you: Laser weapons for missile defense", *Bulletin of the Atomic Scientists*, November 1, 2011, p. 35.

28 ראו טבלת ביצועים ועלויות מול האיומים השונים בהמשך המאמר.

29 יואב זיתון, "לפיד מקצץ בביטחון: חשש שמיגון טנקים ייפגע", **ynet**, 28 במארס 2013, http://www.ynet.co.il/articles/0,7340,L-4361962,00.html

30 עמוס ידלין, "סיכום", בתוך: שלמה ברום (עורך), **לאחר מבצע "עמוד ענן"**, עמ' 77.

31 בנג'מין ס' למבת', "מלחמת לבנון השנייה – הערכה מחודשת", **צבא ואסטרטגיה**, כרך 4,

גיליון 3, דצמבר 2012, עמ' 51.

32 אמיר בוחבוט וניר יהב, "גנץ: 'להמשיך ולתקוף בכל הכוח, להגביר את הקצב'", **וואלה!**, 17 בנובמבר 2012, http://news.walla.co.il/?w=/551/2587039

33 יפתח שפיר, "'כיפת ברזל' – מלכת המערכה", בתוך: שלמה ברום (עורך), **לאחר מבצע "עמוד ענן"**, עמ' 35.

34 זאב קליין וחזי שטרנליכט, "מתן וילנאי: 'נותקף באלף טילים ליום'".

35 מסמך עמותת "מגן לעורף": "מערכת הסקייגארד – האמצעי היחיד להגנת יישובי עוטף עזה מרקטות ופצצות מרגמה", 16 באוקטובר 2012.

36 D. L. Carroll, "Overview of High Energy Lasers: Past, Present and Future", 2011, *AIAA*, 2011-3101.

איומים ביטחוניים חדשים, שימוש חד־צדדי בכוח והסדר המשפטי הבין־לאומי

אפנו סופר אודומובו

איומים ביטחוניים חדשים על הקהילה הבין־לאומית הובילו להערכה מחודשת של הסדר המשפטי הבין־לאומי הקיים. אירועי 11 בספטמבר 2001 מסמנים את תחילת עידן הטרור, ובעקבותיו החשש שארגוני טרור יניחו את ידם על נשק להשמדה המונית ואף יעשו בו שימוש. המלחמה נגד הטרור הבין־לאומי והפצת הנשק להשמדה המונית הם סוג חדש של לוחמה, המעמיד את הקהילה הבין־לאומית בפני איומים ייחודיים ואתגרים ביטחוניים שלא הכירה עד כה. הכרזת המלחמה בטרור הכניסה מספר חידושים למסגרת המשפטית הבין־לאומית הקיימת, בין היתר חידושים הנוגעים לחוקים המסדירים את השימוש בכוח בין מדינות. למרות הדוקטרינות הנורמטיביות של jus ad bellum ("צדקת המלחמה") הנוגעות ל"הגנה עצמית" ול"צורך" בה, היו מקרים שהאילוצים הפוליטיים, ההומניטריים והאסטרטגיים לא הותירו ברירה למדינות אלא לפעול מחוץ לגבולות החוק.
המאמר מבקש למקם את התנאים העכשוויים לשימוש בכוח בהקשר ההיסטורי והמשפטי שלהם, ולבדוק באיזו מידה הם סוטים מהסדר המשפטי הבין־לאומי הקיים.

מילות מפתח: סדר משפטי בינלאומי; נשק להשמדה המונית; טרור; הגנה עצמית מקדימה; שימוש בכוח.

אפנו סופר אודומובו הינו עמית מחקר במכון הצרפתי לחקר אפריקה, (IFRA-Nigeria) ועוזר למתאם פרויקטים, Nigeria Watch/IFRA-Nigeria, אוניברסיטת איבאדן, ניגריה.

מבוא

הוויכוח סביב הנסיבות המצדיקות את השימוש בכוח על פי החוק הבין־לאומי מלווה מזה זמן רב את הזירה המשפטית והמדינית. הקמת האומות המאוחדות הביאה לשינוי המהותי ביותר שהתחולל במאה העשרים במשפט הבין־לאומי, בשל הוצאתו אל מחוץ לחוק של השימוש בכוח ביחסים בין־לאומיים. האיסור על השימוש בכוח מתבסס על אמנות, ובראשן מגילת האו"ם, לצד אמנות אזוריות, כמו האמנה הצפון אטלנטית (נאט"ו) והאמנה הבין־אמריקאית לסיוע הדדי. תנאי אמנות אלו משמשים כנורמת העל (jus cogens) הבסיסית ביותר במשפט הבין־לאומי העכשווי, הכוללת את הערך העיקרי של הביטחון הקולקטיבי.

בעיות ביטחון חדשות תפסו את המשפט הבין־לאומי העכשווי כשהוא לא מוכן להתמודד אתן. הקהילה הבין־לאומית הייתה עדה בשנים האחרונות לגל של איומי טרור, והבינה את הסכנה הגלומה בייצור ובהפצה של נשק להשמדה המונית. גם טִבעוֹ המשתנה של העימות החמוש חשף את הקהילה הבין־לאומית לאתגרי ביטחון חדשים: סכסוכים בין מדינות ואיומים שמציבים "מדינות כושלות" וגורמים לא מדינתיים חמושים התגלו כבעלי השפעה על החוק המסדיר את השימוש בכוח.

איומים ביטחוניים חדשים אלה הובילו לתביעה להעריך מחדש את הרלוונטיות של החוק הבין־לאומי הנוכחי. התפיסה בקרב חלק מחברי הקהילה הבין־לאומית היא שהחוקים הבין־לאומיים הקיימים הינם מיושנים באופן חסר תקנה לנוכח איומי הביטחון החדשים, ולכן יש להביא לשינוי רדיקלי בסדרי המשפט הבין־לאומי הקיים.

המאמר הנוכחי בוחן את השימוש בכוח על פי דיני המשפט הבין־לאומי המנהגי ואת והמסגרת המשפטית שהוגדרה בתום מלחמת העולם השנייה במטרה להגן על הקהילה הבין־לאומית מפני איומים על השלום והביטחון הבין־לאומיים. המאמר גם בוחן את היכולת של המסגרת המשפטית הנוכחית לתת מענה לאיומים שמנסחי מגילת האו"ם לא נתנו עליהם את הדעת. במיוחד בוחן המאמר את הרלוונטיות של הַסדר המשפטי הבין־לאומי הקיים לנוכח איומים ביטחוניים חדשים, ואת הנטייה הגוברת לאחרונה לפנות לשימוש בכוח באופן חד־צדדי ולא מאושר.

המאמר פותח בסקירת השימוש בכוח על פי החוק הבין־לאומי המנהגי; לאחר מכן הוא בוחן את השימוש בכוח על פי מגילת האו"ם; בחלק השלישי בודק המאמר את הסיכוי לסֵדר משפטי בין־לאומי חדש לנוכח עולם משתנה; בחלק הרביעי הוא בוחן את טבעו של הסדר המשפטי הבין־לאומי בעולם שלאחר פיגועי 11 בספטמבר 2001; החלק האחרון מוקדש לסיכום.

שימוש מוֹנע בכוח על פי המשפט הבין־לאומי המנהגי

ההתנהלות בעת מלחמה נתונה לפיקוח של קורפוס גדול של חוקים העוסקים במשפט הבין־לאומי ההומניטרי. קורפוס זה של חוקים התפתח במשך מאות שנים, כשהוא נשען על אמנות היסטוריות, ובמיוחד על אמנות האג וז'נבה.[1] בעוד שאמנות האג וז'נבה שויכו במקורן לדיני המלחמה (jus in bello), מוקד המשפט הבין־לאומי המנהגי היה בחוקים הקשורים ל"צדקת המלחמה"/חוקיות השימוש בכוח (jus ad bellum). החוקים המסדירים את השימוש בכוח, לצד עקרונות הומניטריים בסיסיים נוספים, סיפקו במשך זמן רב את המסגרת לארגון הפורמלי של היחסים הבין־לאומיים הרשמיים ולדו־קיום בין מדינות.

עד לעידן הנוכחי, המשפט הבין־לאומי המנהגי ראה בזכות לשימוש בכוח ובסמכות לצאת למלחמה תכונה מהותית של מדינות, וכתוצאה מכך זכות השמורה לכל מדינה. ניסח זאת צ'ני הייד (Cheney Hyde), מומחה ידוע במשפט הבין־לאומי: "תמיד נתונה למדינה הסמכות לנסות לתקן עוולות או להשיג יתרון פוליטי או כל יתרון אחר, לא רק באמצעות אכיפת כוחה אלא גם באמצעות פנייה ישירה למלחמה".[2] בהקשר זה, המשפט הבין־לאומי המנהגי הכיר גם הוא בהגנה עצמית כבסיס מוצדק לשימוש בכוח. לפיכך, הייד ממשיך וטוען כי: "פעולה של הגנה עצמית היא פעולת מגננה המכוונת כלפי התוקף או מי שמתכנן לתקוף. לא ניתן לכנות פעולה כלשהי בשם זה, מבלי שהגורם לה הוא מתקפה או חשש ממתקפה. כל עוד פעולות לשמירת הקיום העצמי שנוקטות מדינה הן פעולות הגנה עצמית בלבד, הן מותרות על פי דין משפט העמים ומוצדקות עקרונית, גם אם אפשר שהן מתנגשות עם... הזכויות של מדינות אחרות".[3]

המשפט הבין־לאומי המנהגי מכיר למעשה בשימוש בכוח כנגד הצד התוקפן כזכות המתבססת על תנאי ההגנה עצמית, אפילו אם התוקפן טרם תקף בפועל. הזכות המוכרת של מדינה לעשות שימוש בכוח למטרות הגנה עצמית כוללת באופן מסורתי שימוש בכוח כגורם מונע.

התקדים אותו נוהגים לצטט מדינות ומומחים למשפט בין־לאומי לתיאור הגנה עצמית מוֹנעת, הוא ניסוחו של מזכיר המדינה האמריקאי דאז, דניאל ובסטר, בדבר הזכות למתקפה מונעת. ובסטר ניסח זאת על רקע "פרשת קרוליין" המפורסמת: במהלך ההתקוממות של 1837 נגד השלטון הבריטי בקנדה הקולוניאלית, התעורר החשד שהספינה "קרוליין" נושאת אספקה למורדים בנֵייבי איילנד, שתקפו ספינות בריטיות בצד הקנדי של הנהר. כוחות בריטיים חצו את הגבול לתוך ארצות הברית, לכדו את הספינה, העלו אותה באש ושלחו את שרידיה לעבר מפלי הניאגרה. הממשלה הבריטית טענה שפעלה כהגנה עצמית, מכיוון שארצות הברית לא מנעה מהמורדים מלפעול בשטחה. ארצות הברית מחתה על כך, ובמהלך המגעים

הדיפלומטיים ניסח מזכיר המדינה, דניאל ובסטר, את שני התנאים החיוניים ללגיטימיות של שימוש מונע בכוח, בכפוף למשפט הבין־לאומי המנהגי.

אחת מהערותיו של דניאל ובסטר הייתה שפלישה לטריטוריה של מדינה אחרת יכולה להיות מוצדקת כאקט של הגנה עצמית רק באותם "מקרים שבהם הצורך באותה הגנה עצמית הוא מיידי, מכריע, ואינו מותיר ברירה וזמן לדיון".[4] בהערה נוספת ציין ובסטר שהכוח המשמש בנסיבות מעין אלו חייב להיות פרופורציונלי לאיום.[5] לכן, על פי המשפט הבין־לאומי המנהגי, המגבלות המנהגיות על השימוש בכוח מנע להגנה עצמית הן שהוא חייב להיות נחוץ ומידתי;[6] כדי שהמעשה יהיה נחוץ, יש להוכיח שכל אמצעי שאינו כוח חמוש (מאמצים דיפלומטיים, סנקציות כלכליות, אמברגו וכדומה) לא יהיה מספיק, או כשהוכח שהוא אינו מספיק.

השימוש בכוח על פי מגילת האו"ם

החוקים הקובעים את השימוש בכוח להגנה עצמית מונעת מוסדרים בכמה אמנות, הסכמים בין־לאומיים ומוסכמות, שבתוכם מגילת האו"ם היא המרכזית ביותר, בהיותה העיקרון המארגן של הַסדר המשפטי הבין־לאומי. האיסור על השימוש בכוח הוא עיקרון בסיסי של המשפט הבין־לאומי העכשווי, המעוגן במגילת האו"ם. המגילה יוצרת מערכת של ביטחון קולקטיבי, שבה מועצת הביטחון מוסמכת "לקבוע אם קיים איום כלשהו על השלום, הפרה של השלום או מעשה תוקפנות", וכן "להחליט שיינקטו אמצעים... לשמר את השלום והביטחון בעולם".[7] המגילה מחייבת את המדינות החברות "להסדיר את המחלוקות הבין־לאומיות ביניהן בדרכי שלום",[8] וכן "להימנע במהלך היחסים הבין־לאומיים ביניהן מאיום או משימוש בכוח כנגד השלמות הטריטוריאלית או העצמאות הפוליטית של מדינה אחרת, או מכל התנהגות שאינה עולה בקנה אחד עם המטרות של האומות המאוחדות".[9]

מגילת האו"ם הוציאה מבחינה נומינלית מחוץ לחוק את השימוש בכוח ביחסים בין־לאומיים. למרות זאת, היא מכירה בזכותן של מדינות להשתמש בכוח למטרת הגנה עצמית. סעיף 51 במגילת האו"ם קובע כי: "דבר במגילה הנוכחית לא יפגע בזכות הטבעית להגנה עצמית אינדיבידואלית או קולקטיבית, במקרה שמתרחשת התקפה חמושה נגד חברה באומות המאוחדות, עד לנקיטת האמצעים הדרושים מצד מועצת הביטחון לשמירת השלום והביטחון הבין־לאומיים".[10] הזכות המוכרת מכוח סעיף זה ידועה בשם "הזכות הטבעית" של כל מדינה להגנה עצמית. יחד עם זאת, הניסוח של סעיף 51 משקף תפיסה לפיה הפנייה להגנה עצמית נועדה להיות אמצעי זמני, המותר כאמור "עד לנקיטת האמצעים הדרושים מצד מועצת הביטחון לשמירת השלום והביטחון הבין־לאומיים".[11] למרבה הצער, תהליך קבלת

ההחלטות הקולקטיבי במועצת הביטחון הפך לחסר יעילות, כתוצאה מהצבעה המונעת על ידי שיקולים אסטרטגיים של החברות הקבועות בה.

זכות הווטו שבידי החברות הקבועות במועצת הביטחון היא אחד הגורמים המרכזיים שהפכו את המועצה למוגבלת למדי בהרשאת השימוש בכוח על פי סעיף 42 במגילה, אף שישנם חריגים לזכות זאת. כך, למשל, החלטה מספר 377 של העצרת הכללית של האו"ם משנת 1950, הידועה גם בשם "מתאחדים למען השלום" ("Uniting for Peace"), מסמיכה את העצרת הכללית לגבש המלצות לחברות האו"ם בדבר אמצעים קולקטיביים, לרבות שימוש בכוח, "היה ומועצת הביטחון, בשל היעדר תמימות דעים בקרב החברות הקבועות, לא תצליח להוציא לפועל את האחריות המרכזית שלה לשמירת השלום והביטחון הבין־לאומיים".[12]

פרשנות מילולית של נוסח סעיף 51 של מגילת האו"ם, העוסק בזכות להגנה עצמית, היא שהסעיף אינו מתיר את השימוש בכוח מנע מצד מדינות יחידות או קבוצת מדינות, אלא שומר את הזכות להתיר שימושים כאלה בכוח באופן בלעדי למועצת הביטחון. על פי פרשנות זו, אמצעי הגנה עצמית יהיו לגיטימיים רק לאחר שכבר החלה התקפה חמושה.[13] פירוש סעיף 51 באופן מילולי, כמוהו כ"להגן על זכותו של התוקפן להיות הראשון שתוקף".[14] חיוב מדינה הניצבת מול פוטנציאל למתקפה רדיולוגית, כימית, ביולוגית או גרעינית "להתיר לתוקפיה לשגר את המתקפה הראשונה ואולי המכרעת בקטלניותה",[15] יהיה בגידה בכוונותיה של מגילת האו"ם. מצב זה מצביע על כך שעמדתה של מגילת האו"ם בנוגע למצב שמגדיר שימוש מוצדק בכוח אינה עדכנית ואינה עולה בקנה אחד עם האיומים החדשים וטכנולוגיות הנשק המודרניות.

הן הפרשנות המילולית והן הפרשנות הנומינלית של סעיף 51 במגילת האו"ם נתונות למעשה במחלוקת. ליבת המחלוקת היא האם המשפט "אם מתרחשת מתקפה חמושה" שולל הגנה עצמית מונעת, כלומר, האם המשפט הבין־לאומי, כפי שהוא בא לידי ביטוי בסעיף 51 של המגילה, מעניק למדינות זכות מקדימה להגנה עצמית? בניסיון להימנע ממחלוקת זו סביב הפרשנות המילולית או הנומינלית, ישנם מומחים הטוענים כי סעיף 51 מכיר בזכות הטבעית של היחיד או הקולקטיב להגנה עצמית, כפי שהתפתחה במשפט הבין־לאומי המנהגי קודם לאימוץ מגילת האו"ם, ושומר עליה כפי שהייתה אז.[16]

המשפט הבין־לאומי העכשווי לא הבהיר מעולם בצורה משביעת רצון האם צורה כלשהי של הגנה מקדימה מותרת מכוח סעיף ההגנה העצמית (סעיף 51) של מגילת האו"ם. עם זאת, הן בתיאוריה והן במעשה, ישנה הסכמה כללית שמדינות אינן חייבות להמתין עד שיותקפו לפני שיגיבו בכוח, וזאת במקרים שיש עדות מכרעת למתקפה מתוכננת כזו.[17] עמדה זו זכתה לתמיכתו של אליהו רוט (Root), שר המלחמה האמריקאי (1899–1904), שהגדיר הגנה עצמית כ"זכות של כל מדינה

ריבונית להגן על עצמה באמצעות מניעת מצב עניינים שבו יהיה זה מאוחר מדי עבורה להגן על עצמה".[18] שלא כמו המשפט הבין־לאומי המנהגי, משטר מגילת האו"ם הנוגע למשפט הבין־לאומי הינו מוגבל, בשל היעדר הבהירות שבו בנוגע להגנה עצמית מקדימה.

נקודת תורפה זו יוצרת קושי לציית לסעיפי המגילה, שהוביל בעקבות זאת למקרים של שימוש לא מורשה וחד־צדדי בכוח מצד מדינות שעמדו בפני איומים ביטחוניים חדשים. כך, למשל, הפלישה לעיראק ב־2003 בהובלת ארצות הברית, עשתה שימוש בכוח צבאי ללא מתן אישור מפורש של מועצת הביטחון של האו"ם, ואף על פי כן ארצות הברית ובעלות בריתה הצדיקו את פעולתן והציגו אותה כלגיטימית בשל אי־הציות של עיראק להחלטה 1441 של מועצת הביטחון משנת 2001, אשר קבעה שעיראק ביצעה "הפרה חמורה" של מחויבויותיה להתפרק מנשק.[19] חלק מחברות מועצת הביטחון, כמו סין ורוסיה, "הביעו עמדה נחרצת, שהחלטה זו לא סיפקה הרשאה אוטומטית לשימוש בכוח, וכי זהו תפקידה של המועצה (ולא של מדינות בודדות) להחליט האם עיראק מפרה את תנאי החלטה 1441".[20] ואמנם, סעיפי מגילת האו"ם המסדירים את השימוש בכוח ניצבים בפני בעיה של ציות, לנוכח האיומים הביטחוניים המודרניים.

קידמה טכנולוגית ואיומים ביטחוניים בעידן המודרני

המהפכות הטכנולוגיות בתחום הצבאי במהלך חמישים השנים האחרונות שינו מן היסוד את טבעו של העימות החמוש בקצב מהיר מכפי שהמשפט הבין־לאומי העכשווי מצליח להדביק. כניסתם לזירה של נשק להשמדה המונית, טילים בליסטיים, האינטרנט ולוחמת המידע, הפחיתה את הזמן הנחוץ כדי להוציא לפועל מתקפות קטלניות והכפילה בעשרות מונים את עלויותיהן של אסטרטגיות הגנה. לפי ויליאם ברדפורד, פריצות הדרך "בהתפתחות הטכנולוגית, בהפצת נשק להשמדה המונית וכן בהקצנה ביחסים הבין־לאומיים בשל דיפלומטיה של כפייה, הגבירו את היקף האיומים על אוכלוסיות אזרחיות ואת המהירות שבה אויבים יכולים לתקוף, כך שקנֵה המידה של הספינה 'קרוליין' בקביעת איום 'ממשי', כפי שהיה בעידן שקדם לנשק להשמדה המונית, אינו יעיל עוד לריסון מדינות באופן שגם יבטיח את הישרדותן".[21] במילים אחרות, צמיחתם של איומים שקשה להגדירם והם קטלניים יותר באופיים בעקבות החיבור בין טרור לנשק להשמדה המונית, משנה את ההגבלות הקיימות בחוק הבין־לאומי על המושג איום "ממשי", משום שאיום של מתקפה גרעינית הוא תמיד ממשי.

ההתקדמות הביו־טכנולוגית הפכה את העשרת הגרעין לפשוטה יותר, וישנן כיום רשתות בלתי רשמיות המאפשרות העברת הטכנולוגיה הדרושה להמרת חומרים גרעיניים לנשק להשמדה המונית. כך, למשל, ב־2004 היו דיווחים על

העברה אסורה של טכנולוגיית נשק גרעיני לפקיסטן ולקוריאה הצפונית, ויתכן גם לאיראן וללוב, באמצעות רשת של המדען הפקיסטני עבדול קדיר ח'אן.[22] בנוסף לכך, שלא כמו גורמים מדינתיים, ארגונים חמושים לא מדינתיים יכולים להפעיל נשק להשמדה המונית מבלי לחשוש מתגובה גרעינית הרסנית. כך, ביוני 1990 שמה קבוצה של המורדים "הנמרים הטמילים" את ידה על מכלי כלורין ממפעל נייר, ושחררה את הגז במתקן שנמצא בשליטת כוחות הצבא של סרי לנקה.[23] אין ספק, אפוא, שהמשטר הבין־לאומי הנוכחי לפיקוח על השימוש בנשק גרעיני אינו מסוגל להתמודד עם איומים ביטחוניים ביו־טכנולוגיים וגרעיניים מודרניים.

החוק הבין־לאומי והשימוש בכוח בעידן שלאחר פיגועי 11 בספטמבר 2001

התגובה האמריקאית למתקפות הטרור של "אל־קאעידה" על מרכז הסחר העולמי והפנטגון ב־11 בספטמבר 2001 הייתה פנייה לכוח צבאי. ארצות הברית ובעלות בריתה יזמו פעולות צבאיות נגד מחנות האימונים של הטרוריסטים של "אל־קאעידה" ונגד מתקני הצבא של משטר הטליבאן באפגניסטן, כשהן מיישמות את זכותן הטבעית להגנה עצמית אינדיבידואלית וקולקטיבית.[24] למרות שהפלישה נתפסה בעולם כלגיטימית וכמתבססת על סעיף ההגנה העצמית במגילת האו"ם, לא התקבלה אף החלטה ספציפית של מועצת הביטחון המאשרת אותה. כתוצאה מכך, יצרה הפלישה תקדים משפטי שיש ביכולתו לערער על תנאי המשפט הבין־לאומי הקיים, המסדיר את השימוש בכוח בין מדינות.

אישים משפטיים בולטים ומומחים למשפט בין־לאומי[25] טוענים שהחוק המתייחס לשימוש בכוח עוסק בעיקר ביחסים מדיניים, וכי תחולתו אינה כוללת פעילות של ישויות שאינן מדינה. הבלבול שקיים במגילת האו"ם סביב מעמדם של גורמים לא מדינתיים ואחריותן של המדינות שבתחומן הם שוכנים, נוצל על ידי כמה מדינות כדי ליזום מתקפות צבאיות כנגד מדינות אחרות. הבעיה שנובעת מהתפתחות זו מתרכזת בעיקר בשאלה, האם המשפט הבין־לאומי העכשווי מכיר במתקפה שיוזם ארגון חמוש לא מדינתי כ"מתקפה חמושה" שסעיף 51 חל עליה, וכך מצדיק את השימוש בכוח נגד אותו ארגון ונגד כל מדינה שבה ממוקם הארגון.

ראוי לציין שמרבית האמצעים הכוחניים למלחמה בטרור שנקטה ארצות הברית נגד מדינות אחרות לאחר אירועי 11 בספטמבר נתקלו בהתנגדות מועטה באופן משמעותי מצד הקהילה הבין־לאומית. כך, מועצת הביטחון של האו"ם הביעה תמיכה פה אחד בהתערבות הצבאית שהובילה ארצות הברית כנגד משטר הטליבאן באפגניסטן. המועצה שבה ואישרה בהחלטות 1368 ו־1373 משנת 2001[26] את הזכות הטבעית של היחיד והקולקטיב להגנה עצמית נגד גורמים לא מדינתיים. אמנם, אין לראות בהיעדר גינוי לארצות הברית הסכמה לדוקטרינה

משפטית שמתירה את השימוש בכוח בנסיבות אלו, אך יש בכך עדות למגמה של סובלנות גוברת שלאחרונה הביאה להכרה בזכותן של מדינות להגנה עצמית נגד ארגונים חמושים לא מדינתיים.

סוגיית השימוש בכוח נשקלת גם בנסיבות שמעבר להגנה עצמית, ומתרחבת למקרים שעד עתה לא נכללו במשטר הקיים בחוק הבין־לאומי להסדרת השימוש בכוח. לדוגמה, ארצות הברית מרחיבה את החוק המסדיר את השימוש בכוח, שלב אחד מעֵבר לדוקטרינה של הגנה עצמית מונעת. דוקטרינת "המלחמה המונעת" של הנשיא בוש טענה לזכות להגנה עצמית "גם אם נותרה אי־ודאות באשר למועד ולמקום של התקפת האויב".[27] במילים אחרות, תומכי הדוקטרינה (במיוחד ארצות הברית) מצדיקים שימוש בכוח שאינו מבוסס בהכרח על איום ממשי במתקפה, אלא כזה המהווה חלק מאסטרטגיה של מניעת סיכון ארוך טווח. זה גם היה פחות או יותר הטיעון שהעלתה ארצות הברית לתקיפת עיראק ב־2003.[28]

כחלק מהמענה למתקפות של 11 בספטמבר, ארצות הברית דחפה להחלפת הסטנדרטים המיושנים להערכת חוקיותה של ההגנה העצמית בדוקטרינת בוש, המותאמת ליכולות וליעדים של האויבים בעידן הנוכחי. דוקטרינת בוש אותתה שארצות הברית ומדינות אחרות, כמו ישראל, לא ימתינו עוד להתממשות מלאה של האיום, אלא ינקטו פעולה מונעת בעת הצורך כדי להגן על אזרחיהן. דוקטרינת "המלחמה המונעת" של בוש היא "עמדה לוחמנית וטרנספורמטיבית מאד",[29] המותחת בברור את גבולות ההגנה העצמית המקדימה.

רעיון שקרוב מאוד ברוחו לדוקטרינת בוש הוא הרעיון של "איום ממשי ומיידי", המשמש בסיס למתקפות המל"טים האמריקאיים. "ספר לבן" סודי של משרד המשפטים האמריקאי מצדיק את חוקיות השימוש של ארצות הברית באמצעי קטלני זה במדינות זרות, נגד אזרח אמריקאי המוגדר כ"מנהיג מבצעי בכיר ב'אל־קאעידה' או בארגון המקושר אליו", כאשר אדם זה מציב "איום ממשי של מתקפה אלימה נגד ארצות הברית", ובמצב שבו לכידתו "אינה אפשרית", ובלבד ששימוש בכוח קטלני מעין זה "יתבצע באופן שעולה בקנה אחד עם עקרונות דיני המלחמה הישימים".[30] למרות שלא מדובר במסמך משפטי, "הספר הלבן" מצדיק את סמכות הממשל לפעול שלא במסגרת משפטית להריגת אזרחים המציבים איום ממשי של מתקפה אלימה נגד ארצות הברית.

מבחינה היסטורית, היו מספר מקרים של תוקפנות צבאית במסווה של הגנה עצמית מקדימה, לרבות פלישת יפן למנצ'וריה ב־1931 ופלישת גרמניה לפולין ב־1939. מדינות כמו סין, קוריאה הצפונית, פקיסטן וחברות בליגה הערבית עשויות לטעון לזכות משפטית זו כדי לתקוף את טייוואן, קוריאה הדרומית, הודו וישראל בהתאמה, כשהן מצדיקות את פעולותיהן כהגנה עצמית מקדימה במקום כתוקפנות, וזאת בנימוק של טבעם האלים הגיאו־פוליטי של האזורים בהם

מדובר. לדוגמה, בתגובה לפשיטת טרוריסטים צ'צ'נים על בית ספר בדרום רוסיה בספטמבר 2004, הציגה ממשלת רוסיה טיעון, לפיו השימוש שעשתה בכוח צבאי נגד הטרוריסטים היה כדי לחסל את הטרור באזור.[31]

אירועי הטרור של 11 בספטמבר תרמו ליצירת סדר עולמי חדש, המאופיין בשימוש בלתי מאושר וחד־צדדי בכוח ביחסים בין מדינות, כשהוא "מניע תהליך משמעותי של התרופפות המגבלות החוקיות על השימוש בכוח".[32] התמיכה החזקה מצד חברות הקהילה הבין־לאומית בשימוש שעושה ארצות הברית בכוח מחוץ לגבולותיה (למשל, נגד אפגניסטן), בשילוב חששות מוגברים מטרור בין־לאומי, חיזקו את זכותה של מועצת הביטחון של האו"ם להתיר את השימוש בכוח לצורך הגנה אינדיבידואלית או קולקטיבית. למרות ש"הפלישה המקורית לאפגניסטן באוקטובר 2001 בוצעה ללא אישור ספציפי של מועצת הביטחון, הנוסח של החלטות 1368 ו־1373 אִפשר לארצות הברית לטעון ללגיטימיות של פעולותיה. זוהי דוגמה ברורה לכך שהמשפט הבין־לאומי משתנה בתגובה לאיומים עכשוויים הניצבים בפני הקהילה הבין־לאומית.

המשפט הבין־לאומי בעולם משתנה: לעֵבר סֵדר משפטי חדש

החוקים הקיימים במשפט הבין־לאומי, המסדירים את ההתנהלות במלחמה, נוסחו בזמן שמלחמה הייתה בעיקר נחלתן של מדינות לאום. יתר על כן, מערכת האומות המאוחדות הוקמה כדי לפקח על יחסים בין מדינות, ובכלל זה על "הצהרת מלחמה בין מדינות".[33] אולם המצב הביטחוני הנוכחי בעולם הפך למורכב מבעבר, וכיום יש יותר מדינות וארגונים חמושים לא מדינתיים המסוגלים לגרום לנזק רב־ממדים, מעוניינים לייצר או לרכוש נשק להשמדה המונית, ולכן מאיימים על הביטחון האזורי והגלובלי. נשק כימי, ביולוגי, רדיולוגי וגרעיני, הנמצא בידיהם של ארגוני טרור, או בהישג ידם, יוצר כמה מאיומי הביטחון הגדולים ביותר של העידן המודרני. לכן, הבעיה היא "שבאקלים הביטחוני הנוכחי, הציפיות של האתמול הופכות לחוקים של היום".[34]

הסביבה הביטחונית המתפתחת מחייבת כללים חדשים להסדרת השימוש בכוח למטרות הגנה עצמית. התפתחויות חדשות בסביבה הבין־לאומית מצריכות ניסוח מחודש של דיני המלחמה ושל כלל המערכת המשפטית הבין־לאומית, באופן שישקף את טבעם המשתנה של האיומים הביטחוניים ויכלול את המציאות העכשווית במסגרת המשפטית הבין־לאומית. המשטר המשפטי הבין־לאומי מאותגר באופן קבוע לנוכח המצבים המשתנים תדיר, והחוק הבין־לאומי מתעדכן בהדרגה כדי להכיל שינויים אלה. ההתפתחויות החדשות כוללות, בין היתר, את עלייתם של ארגוני טרור בין־לאומיים, ריבוי של גורמים לא מדינתיים, כמו קרטלי

סמים, ארגוני מורדים או פיראטים המעורבים בעימותים חמושים, ומספר עולה של "מדינות כושלות", המאיימות על השלום והביטחון בעולם.

גורמים לא מדינתיים והמשפט הבין־לאומי

אין ספק שמערכת האו"ם נוצרה במטרה להסדיר את השימוש בכוח ואת היחסים בין מדינות לאום, ומגילת האו"ם לא מכירה בישויות שאינן מדינות כגורמים בזירה הבין־לאומית. למעשה, מגילת האו"ם מצדיקה הגנה עצמית רק נגד מדינות. כתוצאה מכך, הוגדר היעד – המדינה התוקפנית – והמטרה הייתה ברורה: להדוף את התוקפנות.[35] בניגוד לכך, איומים ביטחוניים עכשוויים הם מעורפלים, "משנים את ההגדרה של פגיעויות, איומים וסכנות, ומעניקים נראוּת אסטרטגית למגוון גורמים לא מדינתיים".[36] בסביבה הביטחונית הנוכחית, איומים שבעבר נבעו ממחלוקות בין מדינות, מתעוררים כיום מעימותים בין מדינות, שמאחוריהן גורמים לא מדינתיים הפועלים מחוץ לשטחן.

הטרור נחשב כיום לאחד מהאיומים הביטחוניים הגדולים ביותר על השלום והביטחון בעולם. העובדה שארגוני טרור הם גורמים לא מדינתיים וקשה לשייכם למדינה מסוימת מעלה את הצורך בביסוס דרכים חוקיות במשפט הבין־לאומי לקביעת אחריות המדינה שמתוך שטחה פועלים ארגוני טרור אלה. בהתאם לכך, הדוקטרינה של "אחריות מדינה למעשה עוולה בין־לאומי"[37] מספקת הבהרות משפטיות לאחריותן של "מדינות כושלות" ושל גורמים לא מדינתיים על פי החוק הבין־לאומי. חקיקה משנית של החלטות מועצת הביטחון של האו"ם ממלאת חלקית חלל משפטי זה, הודות לקביעתה שניתן להתייחס לטרוריסטים כאל סוכנים של הממשלה המארחת אותם.[38] למרות זאת, כללים אלה עדיין מותירים ללא מענה את השאלה האם מלחמה נגד המדינה שממנת את הטרור היא חוקית מכוח סעיף ההגנה העצמית של מגילת האו"ם.

החלל במגילת האו"ם בנוגע לגורמים לא מדינתיים מתייחס לרוב לגורמים שלא הוקמו על ידי מדינות ואינם נשלטים על ידן בדרך כלשהי. המצב הופך למורכב יותר כאשר גורמים אלה אינם בנויים בדרך המאפשרת כינון יחסים דיפלומטיים.[39] גורמים לא מדינתיים, כמו קרטלי סמים, פיראטים או ארגוני טרור, מקדמים מטרות בלתי חוקיות ומציבים איומים ביטחוניים לא רק על הטריטוריה שמתוכה הם פועלים, אלא גם על הקהילה הבין־לאומית הרחבה.[40] לדוגמה, התפתחויות שהיו לאחרונה בחופי סומליה הביאו להחלטת מועצת הביטחון 1816 משנת 2008,[41] המתארת את הפעילות הפיראטית כאיום על השלום והביטחון העולמיים. למרות שפיראטיות נחשבה עד כה למעשה פלילי בים הפתוח, ההחלטה היא אישור לכך שאיומים מצד גורמים לא מדינתיים יכולים להגיע לסדרי גודל המאיימים על כלל הקהילה הבין־לאומית.

"מדינות סוררות", "מדינות כושלות" והַסדר המשפטי הבין־לאומי

התפיסה של "מדינות סוררות" ו"מדינות כושלות" צמחה מתוך עולם המושגים של היחסים הבין־לאומיים. שני המצבים תויגו כאיומים על השלום והביטחון העולמיים, מכיוון שמדינות אלו נתפסות כפגיעות במיוחד לרשתות טרור. קיומן של "מדינות כושלות" מסבך עוד יותר את בעיית הזיהוי והפניית האשמה כלפי אותן מדינות שנותנות חסות לטרור. "מדינות סוררות" ו"מדינות כושלות" מציבות איום גדול על השלום והביטחון העולמיים, שכן הן משמשות קרקע פורייה לארגוני טרור ודומיהם, ויש סבירות גדולה שהן יעניקו חסות ומימון לפעילות טרור נגד מי שלתפיסתן הוא אויב.

החלטה 748 של מועצת הביטחון של האו"ם, משנת 1992, קבעה כי "לכל מדינה יש את החובה להימנע מלהסית, לסייע או להשתתף במעשי טרור כנגד מדינה אחרת, או מלהסכים לפעילות מאורגנת בשטחה המיועדת לביצוע מעשים כאלה, כאשר אותם מעשים מערבים איום או שימוש ממשי בכוח".[42] אולם, האם אפשר להטיל על "מדינה כושלת" את האחריות לפעולות של ארגוני טרור בשטחה? במילים אחרות, מהי חובתה של "מדינה כושלת" על פי החוק הבין־לאומי? לדוגמה, האם ניתן על פי החוק הבין־לאומי לתבוע מסומליה, שהיא מדינה אפריקאית כושלת, אחריות על חוסר יכולתה למנוע פעולה של ארגוני טרור המתבצרים באזורים שונים בה ופועלים מהם? האם חוסר יכולתה של ממשלת סומליה לעצור פעולות אלו פירושו הסכמה שלה להן? המגבלות המובְנות בתוך המסגרת המשפטית הבין־לאומית ביחס לישויות שאינן מדינות הופכות את מתן התשובה לשאלה זו במסגרת מגילת האו"ם לקשה, אם לא לבלתי אפשרית.

למרות שעקרונות הליבה של האו"ם בדבר אי־התערבות, כיבוד השלמות הטריטוריאלית של המדינות החברות ואיסור על שימוש חד־צדדי בכוח "הם אבן היסוד של הסֵדר הבין־לאומי",[43] לחוק הבין־לאומי יש תנאים נוספים,[44] המכירים בזכויות ובאחריות של "מדינות כושלות" ושל גורמים לא מדינתיים. המשפט הבין־לאומי ההומניטרי ודיני זכויות האדם מכירים ב"מדינות כושלות" ובגורמים לא מדינתיים כחברים במערכת המשפטית הבין־לאומית, על הזכויות והאחריות הנלוות לכך. הרעיון הקובע שכל הגורמים מחויבים למשפט הבין־לאומי ההומניטרי קיבל אישור של מועצת הביטחון של האו"ם בהתייחסותה לליבריה ולסומליה.[45] יחד עם זאת, דיני זכויות אדם עשויים להיות מושעים ב"מדינה כושלת", בהיעדר סמכות ממשלתית מוכרת.

על רקע זה ניתן לפקפק אם אפשר להטיל על "מדינה כושלת" את האחריות על הפרת התחייבויותיה הבין־לאומיות בתקופה שבה היא חווה קריסה והתפוררות. לכן, "אחריות המדינה על מעשי עוולה בין־לאומיים" מייחסת לישות לא מדינתית

התנהלות של מדינה טריטוריאלית רק אם ישות זו מיישמת "אלמנטים של סמכות ממשלתית בהיעדר סמכות רשמית, ובנסיבות של מימוש אלמנטים אלה של סמכות".[46] למרות שהדוקטרינה מספקת הבהרות משפטיות לבעיית הייחוס במקרה של "מדינה כושלת", היא ישימה רק כאשר יש מידה מסוימת של מִבנה מדינתי מתַפקד וסמכות ממשלתית.

התערבות הומניטרית חד־צדדית או קולקטיבית

חובתן של מדינות להגן על אוכלוסייה אזרחית במדינה אחרת, שבה הממשלה היא מקור לאיום הומניטרי על אזרחיה, מהווה אתגר לריבונות המדינה על פי המשפט הבין־לאומי.[47] כשמדובר בהתערבות הומניטרית חד־צדדית למטרת סיוע לאוכלוסייה, לנוכח הפרה בוטה של זכויות אדם, נוצר אתגר לא פשוט לריבונות המדינה על פי החוק הבין־לאומי המנהגי. לאור העובדה שהתערבות כזו גוררת לרוב עימותים חמושים בין המדינה המתערבת ובין המדינה שבשטחה מתרחשת ההתערבות, זהו גם אתגר ביטחוני נכבד. דומה שההתערבות הצבאית של נאט"ו בקוסובו ב־1999, מסיבות הומניטריות, סללה את הדרך לבסיס משפטי חדש ועוררה ויכוח סביב הצורך בדוקטרינה הומניטרית חדשה למלחמה. בעקבות זאת, נראה היה שהתבסס העיקרון, לפיו התערבויות צבאיות להשגת יעדים הומניטריים אינן מחייבות אישור מיוחד ממועצת הביטחון של האו"ם.[48]

על פי "הוועדה הבין־לאומית הבלתי תלויה לקוסובו",[49] ההתערבות הצבאית של נאט"ו הייתה "לא חוקית אבל לגיטימית", מכיוון שהתבצעה ללא אישור ספציפי ממועצת הביטחון, אולם הייתה מוצדקת על בסיס הומניטרי ומתוך הבנה שכל הערוצים הדיפלומטיים מוצו לפני הפעולה. ואף על פי כן, סעיף 2(7) של מגילת האו"ם מציין כי "דָבר מִמה שנאמר במגילה הנוכחית אין בו כדי להסמיך את האו"ם להתערב בנושאים שבמהותם הם חלק מתחום השיפוט של מדינה כלשהי, או כאלה שמחייבים את המדינות החברות לפעול להסדרתם על פי כללי המגילה הנוכחית"; כלומר, "אף מדינה או ארגון בין־לאומי אחר אינם רשאים לבחון את המתרחש בתוך מדינה אחרת, למעט במקרה של קבלת הסכמה מלאה לכך מצד המדינה הטריטוריאלית".[50]

ההתערבות האחרונה של נאט"ו הייתה בלוב, במטרה להגן על אזרחים מפני הפרות זכויות אדם מצד כוחות הצבא הנאמנים לשליט דאז, מועמר קדאפי. למרות שמועצת הביטחון קיבלה החלטה המאשרת את נקיטת "כל האמצעים הנחוצים להגנה על אזרחים שנתונים לאיום מתקפה",[51] ההתערבות חרגה מהאישור שניתן בהחלטה. חוקיות ההתערבות הצבאית בלוב עדיין מוטלת בספק, משום שנאט"ו יישם את החלטת מועצת הביטחון לא רק לשם הגנה על אזרחים, אלא גם "כדי להצדיק השגת תמיכה כללית במורדים וכדי לתקוף את הנכסים הצבאיים של

ממשלת לוב".[52] לנוכח המחלוקת סביב ההתערבות הצבאית של נאט"ו בלוב, מתעוררת השאלה אילו נסיבות יצדיקו התערבות חיצונית על פי החוק הבין־לאומי? במילים אחרות, באיזו נקודה הופך השימוש החד־צדדי בכוח למען מטרה הומניטרית לחוקי? מן הסתם, שאלות אלו קשות מאד למענֶה, בין היתר משום שבנפרד מהחוק הבין־לאומי ומדוקטרינת "האחריות להגן",[53] מתפתחים גם אינטרסים כלכליים, פוליטיים ואסטרטגיים כגורמים בעלי משקל להצדקת השימוש בכוח על רקע הומניטרי.

כל הפעולות הצבאיות של העת האחרונה "כופפו או הפרו את דיני המלחמה, כפי שהובנו עד עתה".[54] איומים ביטחוניים חדשים גרמו למעצמות העולם המובילות לראות בחוק הבין־לאומי גורם משני ביחס להפגנת עוצמתן הצבאית. מטבע הדברים, מדינות הנוטות לפקפק ביכולתו של המשפט הבין־לאומי להסדיר התנהגות בין מדינות או בין גורמים לא מדינתיים, אינן מוטרדות יתר על המידה מהנזק למערכת המשפטית הבין־לאומית. המגמה המצטיירת מהשפעתן המצטברת של התפתחויות אלו היא, שתנאי מגילת האו"ם המסדירים את השימוש בכוח אינם נתפסים עוד כחוק בין־לאומי מחייב,[55] וכיום קשה לקבוע מתי הדיפלומטיה מוצתה ומתי השימוש בכוח הופך לחיוני.

הערות מסכמות

למרות שהנטייה של מדינות לפנות לשימוש בכוח כצעד מניעתי הייתה קיימת עוד לפני 2001, הנטייה העכשווית של מדינות לפנות לשימוש מקדים בכוח מקורה בעיקר בחשש מהאיומים שמציב הטרור, ומהקטלניות של נשק להשמדה המונית, במיוחד לאור מתקפת הטרור של 11 בספטמבר 2001. האיומים מנשק להשמדה המונית מקושרים לא רק לשינויים בסביבה הבין־לאומית, אלא גם לתהליך הגלובליזציה הכלכלית, שפגע ביעילות המשטרים המסורתיים שלא דגלו בנשק זה. המשפט הבין־לאומי, כפי שהוטמע במגילת האו"ם, טרוד יותר בשימור השלום והביטחון ופחות בכללים החוקיים לשימוש בכוח. התנאים המשפטיים במגילה הנוגעים לשימוש בכוח הינם מעורפלים. לכן, כחלק מהצורך לתת מענה לאיומים החדשים, החוק הבין־לאומי מוצא עצמו פעמים רבות מתוקן על ידי פרקטיקה מדינתית המפרה את המסגרת המשפטית הבין־לאומית הנוכחית. למרות ששינויים אלה עדיין לא קיבלו מעמד של חוק בין־לאומי מחייב, והם עדיין ברמה של פרקטיקה מדינתית אינדיבידואלית, הם מציבים תקדים משפטי שמדינות אחרות צפויות להסתמך עליו בעתיד.

ואכן, הפרות של החוק הבין־לאומי מצד מדינות משמשות כתקדים משפטי, ויש להן יכולת לשנות בצורה עקיפה את החוק, במיוחד כאשר המדינה המפרה זוכה לתמיכה רחבה בפעולותיה. עם זאת, הקהילה הבין־לאומית חייבת לנקוט

משנה זהירות ולהבטיח שגם אם המטרה היא להתמודד עם אתגרי הביטחון החדשים, שינויים אלה לא יטו את הכף יותר מדי לצד השני ולא יהפכו, בסופו של דבר, לגורם שמפר את היציבות במארג העדין של היחסים הבין־לאומיים. למעט לצורך הגנה עצמית נוכח איומים ברורים ומפורשים, או כחלק מהחתירה ליעדים שהוכרו כלגיטימיים בקהילה הבין־לאומית הרחבה, השימוש בכוח מערער לרוב את הביטחון בסדר המשפטי הקיים ומגביר את הטינה כלפיו בקרב המדינות החלשות.

ללא רפורמות משמעותיות, שיהיה בהן מבט כולל וגמיש יותר על זכותה של מדינה להגנה עצמית נגד איומי טרור ונשק להשמדה המונית, המשפט הבין־לאומי, שמסדיר את השימוש בכוח, יהפוך לבלתי רלוונטי אל מול האיומים הביטחוניים המתעוררים. גם שינוי הדרגתי של קורפוס דיני המלחמה הנוכחי לא ייתן לכך מענה, מכיוון שכל המבנה המשפטי נתון בסכנת קריסה מִכּוֹבד משקלם של האיומים החדשים. בנוסף לכך, ההכרה בסדר משפטי חדש לא תמנע בהכרח עלייה של איומים חדשים על הקהילה הבין־לאומית. זאת ועוד, קשה לחזות את ההשפעה של סדר משפטי חדש על היציבות הבין־לאומית בעתיד. כדי שחוקי הסדר המשפטי החדש יהיו אפקטיביים ומחייבים, עליהם להבָּנות בתוכם מספיק גמישות עבור המדינות, כך שבעת הצורך יעלה בידן להפעיל כוח מבלי לערער או להרוס את האמינות והלגיטימיות של הסדר המשפטי הבין־לאומי.

הערות

1 Tomas Valasek, "New Threats, New Rules: Revisiting the Law of War", *World Policy Journal*, spring 2003, pp. 17-24.
2 Charles Cheney Hyde, "International Law Chiefly as Interpreted and Applied by the United States", *Congressional Research Service* (CRS), Vol. 3, 1945, p. 168.
3 Ibid., p. 234.
4 John Bassett, "Letter from Secretary of State Daniel Webster to Lord Ashburton of August 6, 1842", *A Digest of International Law*, Vol. 2, 1906, p. 412.
5 David Ackerman, "International Law and the Pre-emptive Use of Force against Iraq", *Congressional Research Service* (CRS), Library of Congress, 2003, p. 2.
6 I.C.J. Report, "Legality of the Threat of Use of Nuclear Weapons", *International Court of Justice Reports*, 1996, p. 14, paragraph 41.
7 The United Nations, *Charter of the United Nations*, San Francisco, 1945, Article 29.
8 שם. סעיף 2 (3).
9 שם. סעיף 2 (4).
10 שם. סעיף 51.
11 שם.
12 United Nations, GA/RES 377 (V) A, 1950, http://www.kentlaw.edu/faculty/bbrown/classes/IntlOrgSp07/CourseDocs/VUnitingforPeaceResolution.pdf
13 I.C.J. Report, "Legality of the Threat of Use of Nuclear Weapons", *International Court of Justice Reports*, 1996, p. 14, paragraph 41.

14 Humphrey Waldock, quoted in: Guy B. Roberts, "The Counterproliferation Self-Help Paradigm: A Legal Regime for Enforcing the Norm Prohibiting the Proliferation of Weapons of Mass Destruction", *Denver Journal of International Law and Policy*, 27, 1999, p. 483.

15 שם, עמ' 513.

16 Bruno Simma, *The Charter of the United Nations: A Commentary*, Oxford: Oxford University Press, 1994, p. 51.

17 Valasek, "New Threats, New Rules", p. 18.

18 Elihu Root, "The Real Monroe Doctrine", *American Journal of International Law*, Vol. 8, 1914.

19 United Nations, UN Doc. S/RES 1441, 2002, http://www.un.org/depts/unmovic/documents/1441/pdf

20 Justin Morris and Nicholas Wheeler, "The Security Council's Crisis of Legitimacy and the Use of Force", *International Politics*, Vol. 44, 2007, pp. 214-231.

21 William Bradford, "The Duty to Defend them: A Natural Law Justification for the Bush Doctrine of Preventive War", *Journal of National Security Law and Policy*, 2003, p. 15.

22 Michael Laufer, "A. Q. Khan Nuclear Chronology", *Proliferation Brief*, no. 8, 2005, http://carnegieendowment.org/2005/09/07/a,-q.-khan-nuclear-chronology/6jq

23 Jonathan Tucker, "The Future of Chemical Weapons", *The New Atlantis*, Fall 2009/ Winter 2010, pp. 3-29.

24 Dan Balz and Bob Woodward, "America's Chaotic Road to War", *The Washington Post*, January 27, 2002.

25 Michael Byers, "Terrorism, the Use of Force and International Law after 11 September", *International Relations*, Vol. 16, no. 2, 2002, pp. 155-170; Thomas Franck, "What Happens Now? The United Nations after Iraq", *American Journal of International Law*, Vol. 97, 2003; Antonio Cassese, "Terrorism is also Disrupting some Crucial Legal Categories of International Law", *European Journal of International Law*, Vol. 12, no. 2, 2001, pp. 993-1002; Michael Glennon, "How War Left the Law Behind", *The New York Times*, November 21, 2002.

26 United Nations, UN Doc. S/RES 1368, 1373, 2001, http://www.un.org/documents/scres.htm

27 Devika Hovell, "Chinks in the Armour: International Law, Terrorism and the Use of Force", *UNSW Law Journal*, Vol. 27, no. 2, 2004, pp. 398-427.

28 שם.

29 Franck, "What Happens Now?

30 United States, "Lawfulness of a Lethal Operation Directed Against a U.S. Citizen Who Is a Senior Operational Leader of Al-Qa'ida or An Associated Force", *Department of Justice White Paper*, http://users.polisci.wisc.edu/kmayer/408/020413DOJ White Paper.pdf

31 Nicholas Kralev, "Russia Vows Pre-emptive Terror Hits", *The Washington Post*, September 9, 2004.

32 Michael Byers, "Terrorism, the Use of Force and International Law after 11 September", p. 165.

33 Valasek, "New Threats, New Rules", p. 18.

34 שם, עמ' 19.
35 Cassese, "Terrorism is also Disrupting some Crucial Legal Categories of International Law".
36 David Kennedy, "International Symposium on the International Legal Order", *Leiden Journal of International Law*, Vol. 16, 2003, p. 841.
37 Responsibility of States for Internationally Wrongful Acts, UN Doc. A/56/10, 2001.
38 Valasek, "New Threats, New Rules", p. 18.
39 Cherif Bassiouni, "The New Wars and the Crisis of Compliance with the Law of Armed Conflict by Non-State Actors", *Journal of Criminal Law and Criminology*, Vol. 98, 2008, pp. 711-810.
40 Ian Brownlie, *Principles of Public International Law*, 6th Edition, New York: Oxford University Press, 2003, pp. 713-714.
41 United Nations, UN Doc. S/RES 1816, 2008, http://www.un.org/documents/scres.htm
42 United Nations, UN Doc. S/RES 748, 1992, http://www.un.org/documents/scres.htm
43 Morris and Wheeler, "The Security Council's Crisis of Legitimacy", p. 222.
44 United Nations, Universal Declaration of Human Rights, UN Doc. A/819, 1948; Responsibility of States for Internationally Wrongful Acts, UN Doc. A/56/10, 2001.
45 United Nations, UN Doc. S/RES 788, 1992 ;United Nations, UN Doc. S/RES 814, 1993.
46 Responsibility of States for Internationally Wrongful Acts, UN Doc. A/56/10, 2001, article 9.
47 Bradford, "The Duty to Defend Them"; Anthony Arend, "International Law and Rogue States: The Future of the Charter Framework", *New England Law Review*, 2002.
48 Valasek, "New Threats, New Rules", p. 21.
49 Independent International Commission on Kosovo, 2000, http://www.cfr.org/kosovo/independent-international-commission-kosovo-kosovo-report-executive-summary/p25962
50 Valasek, "New Threats, New Rules", p. 19.
51 United Nations, UN Doc. S/RES 1973, 2011, http://www.un.org/News/Press/docs/2011/sc10200.doc.htm
52 Ben Smith, Vaughne Miller and Arabella Lang, "Military Interventions: Some Comparisons", *Commons Library Standard Note*, August 29, 2013, http://www.parliament.uk/briefing-papers/sn06715/military-interventions-comparison
53 *The Responsibility to Protect*, Report of the International Commission on Intervention and State Sovereignty, 2001, Vol. II.
54 Valasek, "New Threats, New Rules", p. 18.
55 Michael Glennon, "Military Action against Terrorists under International Law. The Fog of War: Self-Defence, Inherence, and Incoherence in Article 51 of the United Nations Charter", *Harvard Journal of Law*, Vol. 25, 2002.

הגנת סייבר באמצעות אסטרטגיות של "צמצום מידע אסימטרי"[1]

גיא פיליפ גולדשטיין

"אם אתה יודע את האויב ויודע את עצמך, אל לך לחשוש
גם לא ממאה קרבות. אם אתה יודע את עצמך אך לא את
אויבך, אזי כל ניצחון שלך יִלָווה בתבוסה. אם אינך יודע
לא את האויב ולא את עצמך, תובס בכל קרב".
סאן צו, אמנות המלחמה[2]

מאמר זה מתמודד עם שתי בעיות מרכזיות בהגנת סייבר: סוגיית ייחוס התקיפה (מי התוקף) וסוגיית סף ההחלטה (האם הפגיעה מצדיקה מלחמה כוללת). המאמר פותח בתרחיש של משחק מלחמה, ומציע מסגרת אנליטית המבוססת על "מדריך טאלין" לשרטוט מקרים של מלחמה ואזורי משבר. בהמשך מציע המאמר דרכים להתמודד עם משברי סייבר, וזאת באמצעות שתי אסטרטגיות של "צמצום מידע אסימטרי": טיפול בסוגיית הסף בעזרת הבנה טובה יותר של ההשפעות הגלויות והמדומות על מדינות מרושתות הפועלות כמערכת המתגוננות מפני מתקפות סייבר, תוך התבססות על הרעיון של קולונל ג'ון וורדן; טיפול בבעיית הייחוס, המחייב מצוינות בשיטות הליבון וההבהרה, וכן חקירה כופה הזוכה בתמיכה בין־לאומית – בהשראת מושג הכפייה (compellence) של תומאס שלינג. השליטה הגוברת של העולם הדיגיטלי בחברות המודרניות עשויה להפוך אסטרטגיות אלו לחלק מאבני היסוד של דוקטרינה חדשה להשגת יציבות צבאית ופוליטית במאה ה־21.

מילות מפתח: נשק הסייבר; הגנת הסייבר; הרתעה; דוקטרינה; אכיפה; מדריך טאלין

גיא פיליפ גולדשטיין הוא סופר; מחבר רב המכר **בבל שעת אפס**, הוצאת שוקן, 2010.

מבוא – תרחיש אזורי

השעה 09:00 במדינה X. הכספומטים בבירת המדינה הפסיקו לעבוד. חלק מהלקוחות המקוונים של שלושה מהבנקים הגדולים במדינה לא מצליחים ליצור גישה לחשבונות הבנק שלהם. בחלק מהמקרים, נתוני החשבונות המקוונים נמחקו. טלפונים סלולריים כמעט שלא מתַפקדים. דומה שמדובר במתקפה מסוג חדש, שההשפעות שלה דומות למתקפות הסייבר של שנת 2007 באסטוניה, אולם מבחינה טכנית, הפעם הן לא נראות כמתקפות מפוזרות למניעת שירות: לא זוהתה כמות גדולה של כתובות IP המכבידות על השרתים. אין פתרונות מיידיים לתיקון התקלה ולא ברור כמה זמן היא תימשך. החרדה ברחובות מדינת X גואה במהירות. האם ניתן יהיה לשחזר את הנתונים? האם זהו גל ראשון המבשר על מתקפות נוספות?

מדינת X אינה לבדה. שבוע לאחר מכן, חברת אבטחת תוכנה ידועה ממדינה B זיהתה תוכנה זדונית חדשה: GlobalWorm. למרות שאופן פעולתה אינו ידוע ברגע הגילוי, נראה ש־GlobalWorm הדביקה מערכות רבות במדינות שונות. בהודעת התרעה שמוציאה חברת אבטחת התוכנה, היא מקשרת את המתקפה נגד מדינה X ל־GlobalWorm. מדינות נוספות שנפגעו מ־GlobalWorm חוות קשיים, וביניהן מדינות ידידות של מדינה X וגם אויבות שלה, אולם מדינה X חווה את ההשפעות החמורות ביותר.

מי אחראי למתקפות על מדינה X באמצעות GlobalWorm? מהו סוג האיום ש־GlobalWorm מציב בפני מדינה X? כיצד עליה להגיב? התשובה לשאלה השלישית תלויה בשתי השאלות הראשונות.

כאילו המצב לא סבוך דיו, מתברר שלחברת אבטחת התוכנה, שבידיה המידע הרב ביותר על GlobalWorm, יש קשרים הדוקים עם המערכת הצבאית של מדינה B, שאינה ידידה קרובה של מדינה X. כאשר המועצה לביטחון לאומי של מדינה X מתכנסת, השאלות מתלהטות: האם זו מכה נוספת מכיוונה של מדינה Y – האויב המוצהר של מדינה X? האין זה נכון שמדינה Y הגדילה את השקעותיה בנשק סייבר? או שמא המתקפה מגיעה ממדינה Z, שקשריה עם מדינה X התערערו בצורה דרמטית במהלך חמש השנים האחרונות?

ראש מדינת X מנסח את שלוש השאלות המרכזיות שעומדות על הפרק:

1. האם תוכלו להוכיח לי שמדינה Y ומדינה Z לא קשורות לעניין?
2. כמה זמן עומד לרשותי לפני שיהיה עליי להגיב?
3. כיצד אוכל להגיב אם איני יודע את התשובות לשאלה הראשונה והשנייה ?

ראש המודיעין של מדינה X מאשר כי בשלב זה אין אינדיקציה ברורה שמדינה Y או מדינה Z עומדות מאחורי המתקפות, למרות שלא ניתן לשלול זאת. במקביל, הוא לא שולל את האפשרות שמדובר במניפולציה של מדינה B.

המתקפות אמנם זעזעו את אוכלוסיית המדינה, אולם לא הסלימו במהלך שמונה השעות האחרונות. לא ניתן לומר כיצד האיום עתיד להתפתח – אם הוא בכלל ימשיך להתפתח. מה שברור הוא שחלה פגיעה בעוצמתה של מדינה X. ללא נקיטת צעדים כלשהם לבירור הנושא, לשיקום העוצמה ולתגמול על הפגיעה, מעמדה של מדינה X כמעצמת סייבר יאותגר, דבר שאין להקל בו ראש. הסברה המקובלת בעידן הנוכחי היא שפעולות מלחמתיות גדולות יתחילו במרחב הסייבר, כך שהשליטה במרחב זה היא מבחן לעוצמה הצבאית הכוללת.

שר החוץ של מדינה X מקבל את רשות הדיבור. לדבריו, למדינה A, אחת מהידידות הקרובות ביותר של מדינה X בזירה הבין־לאומית, אין אינדיקציה ברורה על מקור ההדבקה ב־GlobalWorm. עם זאת, מכיוון שמדינה A רואה בכך בעיה עולמית, היא לא תתיר למדינה X להגיב ללא הוכחה ודאית מיהו התוקף. מעבר לכך, מדינה A טוענת שהתגובה צריכה להיות מתואמת היטב, למקרה שהיא תביא לעוד פעולות תגמול בסייבר, שכן גם מדינה X וגם מדינה A אינן יודעות כיצד GlobalWorm עובד. המצב שונה מתרחישים שבהם מדינה X היא הצד התוקף. מדינה X אינה שולטת בנתונים וגם לא בסביבה, ומהלך שגוי שלה עלול להתגלות כמסוכן עבורה, ואולי אף עבור שאר המדינות. ניתן לדמיין אינספור מניפולציות, והלא ידוע רב על הידוע.

מצב זה של בלבול אסטרטגי הוא אולי מה שהתוקף כיוון אליו כשתכנן את המתקפה. מדינה X עדיין אינה יודעת על מה ועם מי מתנהל השיג והשיח. ההצעה הברורה היחידה מגיעה ממדינה B: באמצעות חברת אבטחת התוכנה שלה, היא מציעה מומחיות ייחודית ב־GlobalWorm. מן הסתם יהיה לכך מחיר. בנוסף, מדינה A ומדינה B הן מדינות מתחרות בזירה הבין־לאומית. מדינה A עשויה להתנגד לכך שמדינה B תגיש סיוע למדינה X. היחסים בין מדינה A למדינה X עלולים אז להיפגע.

בתרחיש שתואר לעיל לא ניתן להסתמך על תגובה בכלים קונבנציונאליים או אסטרטגיים. למעשה, מדינה X ניצבת בפני שיתוק אסטרטגי. תיאוריית ההרתעה המושלמת קובעת כי האסטרטגיה האופטימלית היא "תגובה בעוצמה זהה" (response in kind)[3]. אסטרטגיה כזו תוכיח שהצד המותקף מחזיק באיום אמין לגמול על התקפה עליו. במקרה המדובר, יהיה בכך איתות שמדינה X אינה מחפשת בהכרח להסלים את המצב. פול הות' (Huth) תיאר מצב זה כסגנון משא ומתן "קשוח אך גמיש".[4] תגובה הנמנעת מהסלמה חריפה, ובמקום זאת מציגה עמדה קשוחה, מאפשרת לרמוז על אופציות מבלי ליישם אותן: זוהי העֶמדה המועדפת ביותר על פוליטיקאים, כמו גם על אנשי המערכת הפיננסית. זהו מצב אופטימלי גם כשמדובר בתהליכי החלטה בתחום הסייבר. אולם במצב הנוכחי שבו נתונה מדינה X, "תגובה בעוצמה זהה" אינה אפשרית. ראשית, ישנו מכשול

מרכזי: מדינה X אינה יודעת כלפי מי להגיב ונתקלת למעשה בבעיית הייחוס.[5] אבל גם אם הייתה יודעת בוודאות מי התוקף, אזי עומד בפניה מכשול גדול נוסף: היא לא בהכרח יודעת כיצד להגיב.

הבה נניח לרגע שמדינה X הוכיחה שמדינה Y היא הצד התוקף. מכיוון שנפרצו כספומטים של בנקים, חשבונות בנק מקוונים וכמה רשתות סלולריות, מדינה X מבקשת להגיב בעוצמה זהה. הבה נניח עוד שמדינה Y לא הקשיחה מראש את אבטחת הסייבר סביב מה שהיא יודעת שיהיו יעדי התגובה של מדינה X. נותר עדיין ספק גדול באשר לשאלה האם מדינה X תהיה מסוגלת לגרום לפגיעה במדינה Y לפחות באותה רמה כמו זו שהיא עצמה ספגה. אם היא תנסה לגרום נזק דומה אך תיכשל בכך, אמינות האיום שלה תיפָגע עוד יותר; אם היא תגרום לנזק גדול מדי, היא עלולה לעורר השלכות לא צפויות ולהכניס את העימות לסחרור. במצב הנוכחי של היכולות הטכניות, קשה לחזות במדויק את ההשפעות של נשק הסייבר, וקושי זה גובר עוד כאשר מדובר בשימוש מאולתר בנשק זה במטרה להשיג תגמול מהיר.

מדינה X ניצבת בפני בעיה נוספת: סוגיית הסף.[6] אין לה פתרון בדרך של תגובה בעוצמה זהה, כלומר אין לה יכולת לאיים בצורה אמינה בתגמול. דוקטרינה הדוגלת ב"תגמול מאסיבי" בסייבר עשויה להיות נתונה לאותה ביקורת כמו זו של וויל קאופמן על החלטה NSC-162/2 של נשיא ארצות הברית אייזנהאואר משנת 1954,[7] בתוספת אזהרה שהמונח "מאסיבי" קשה להגדרה, אלא אם מדובר בפגיעה מאסיבית וודאית באזרחים. מנגד, היעדר תגמול פוגע בבירור בעקרון ה"תגובה בעוצמה זהה", ועשוי להזמין תקיפה נוספת.

בשלב זה אין אופציות תגמול טובות למדינה X. אם המתקפות הגיעו לסף נזק מסוים ומדינה X תחוש מאוימת ממצבה הגיאופוליטי המשתנה, היא עשויה לרצות לרמוז לשכנותיה שיהיו השלכות למתקפה עליה. היא גם עשויה לנסות להוציא לפועל "תגובה בעוצמה זהה" שאינה מושלמת, בכך שתשים את הדגש על האיום האמין והקביל ביותר שיש לה – איום שאינו בתחום הסייבר אלא בתחום הקינטי, כמו הפגנת כוח אווירית או קרקעית. אם הייחוס לא יהיה ודאי, יהיו לכך השלכות דיפלומטיות נגדיות שיחזרו כמו בומרנג במקרה שמתקפות הסייבר יימשכו, וסופן שיעלו את הסיכון לפגיעה באמינותה של מדינה X (לאור העובדה שחשפה את היכולות הקונבנציונאליות שלה). מצד שני, אם מתקפות הסייבר לא גבו מחיר גבוה מדי, ומקורן נותר מעורפל, אזי ייתכן שמדינה X תרצה להפיג את המתח ולהפחית את הסיכון, ואז תוכל לייחס את הקשיים שנוצרו לבעיות טכניות או לגורמים שאינם מדינתיים. מדינה X תוכל אז להסכים לקבל סיוע ממדינה B דרך חברת אבטחת התוכנה שלה. כמובן שיהיה לכך מחיר, כפי שכבר צוין קודם לכן.

אסטרטגיה ראשונה של "צמצום מידע אסימטרי": הבהרת שאלת הסף בעזרת תהליך ומסגרת להערכת מתקפות סייבר

מסגרת ההערכה

למדינה X יכולה להיות דרך פעולה טובה יותר. כדי לתכנן את התגובה הטובה ביותר, עליה להבין אילו סוגי מתקפות עומדים בפניה. במיוחד עליה לפתור שתי בעיות שכבר הוזכרו: ייחוס וסף. הייחוס חייב להיות מקושר בצורה ישירה יותר לסוגיית "ההכחשה הסבירה" (plausible deniability), שכן מה שמוטל בכף הן ההשלכות הפוליטיות והדיפלומטיות של היעדר ייחוס. הגדרת הסף היא בעיה מורכבת אפילו יותר: ישנו קושי מובנה בהגדרה של "סף פשוט וניתן לזיהוי" במתקפות סייבר.[8] פעולות המתקרבות אל הסף ניתן לחלק לשתיים: כאלו שיש להן השפעה ישירה על המדינה (כמו שיבוש של ענף תעשייה ואובדן חיים), והכנות צבאיות (כמו תזוזת צבא ופעולות איסוף מידע) הקודמות לפעולות אלו שיש להן השפעה ישירה.

האם הצבת מלכודות לוגיות ברשת האלקטרונית של היריב מהווה פעולת מלחמה? האם יש מקבילה בלוחמת סייבר לתזוזת צבאות וריכוזם על הגבול? לשאלות אלו אין מענה פשוט, במיוחד משום שהן מתייחסות לנושאים כמו סוגיית הסף לפעולת תגמול על פי "עקומת האמינות"[9].

"מדריך טאלין" הוא נקודת מוצא לתשובות לשאלות אלו, אולם נכון להיום אינו מציע מענה מוסמך להן.[10] מבחינה כללית והיסטורית, אלו הן סוגיות המצויות בליבת ההתנהלות האסטרטגית של מדינות, שנענות כל אחת לגופה מתוך ראיית המציאות, אולם מבלי שגובש להן מענה רשמי ומקיף. אסטרטגיית הסייבר מחייבת מאמץ נוסף להמשגת התשובה. למרות שיהיה בכך משום חריגה ממסגרתו של מאמר זה, ניתן לציין בו כמה מראי דרך ראשוניים.

נקודת המוצא, המוזכרת בספרות העוסקת בלימודי לוחמת הסייבר וכן ב"מדריך טאלין", היא ההשפעה הישירה.[11] זוהי גישה שצבאות רבים בעולם יכולים להבין, החל מחיל האוויר של ארצות הברית, שהוא עדיין חסיד של מבצעים מבוססי־תוצאה המקשרים בין פעולות, תוצאות ויעדים.[12] כפי שמודגש ב"מדריך טאלין", לגישה כזאת יש גם תקדימים משפטיים, במיוחד סביב המונח "היקף ותוצאות".[13] יחד עם זאת, נותרת בעינה השאלה אילו תוצאות פירושן חצייה קו אדום מבחינת הצד המתגונן? קל יותר להתחיל מִמה שנתפס כקביל או כנסבל, ולאחר מכן להבהיר מה לא יהיה קביל לעולם ויגרור תגובה צבאית אוטומטית, כאשר בין שני אלה שוכן השטח האפור של המשברים.

לדוגמה, ריגול הוא בגדר הנסבל (אם כי לא רשמית). הוא נהנה מסובלנות בין־לאומית, מכיוון שהוא "שלוחה של משטרים המקיימים פיקוח", דבר שמאפשר

שיתוף פעולה פונקציונלי.[14] דומה שחלק מסובלנות זו התפשט גם לכמה מ"יישומי הסייבר" של הריגול.[15]

מה שלא יהיה קביל לחלוטין ואף יצית תגובה צבאית אוטומטית, הוא מספר גבוה של קורבנות בקרב אוכלוסייה שאינה לוחמת. מקרה כזה יתורגם ככלל להפרה של דיני העימות החמוש בנוגע ל־*jus ad bellum* (צדקת המלחמה), כפי שנוסחו באמנת ז'נבה משנת 1949 ואושררו ב"מדריך טאלין".[16] מה שלא יהיה קביל לחלוטין מבחינה אסטרטגית, וייחשב כמלחמה, גם הוא ברור ממבט ראשון: הרס חלקי או מלא של מקומות מקלט (sanctuary). הדבר מתייחס גם לכל ניסיון משמעותי לפגוע בצורה הרסנית במוסדות המגנים על מקומות אלה. מכיוון שהמדינה מחזיקה במונופול על הפעלת אלימות בקנה מידה רחב,[17] פירוש הדבר הוא להגן הן על היכולת לממש אלימות בהיקף גדול והן על מרכז קבלת ההחלטות המפקח על השימוש באלימות. במונחים מעשיים, הגנה על מקום מקלט פירושו, בראש ובראשונה, הגנה על חיי האזרחים. מלחמה הופכת לבלתי נמנעת כאשר אומה סופגת אבידות כבדות.

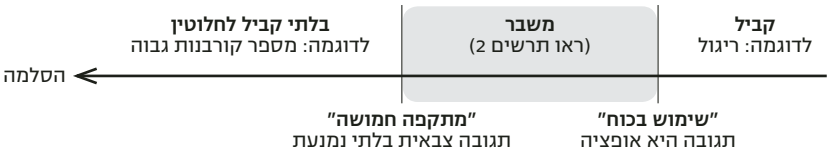
כשמדובר בהפעלת אלימות בקנה מידה גדול, ישנן כמה סוגי יכולות ומערכות שאין לפגוע בהן: בראש ובראשונה יכולת המכה השנייה של המדינה, אולם גם מערכות אחרות שכל תפקוד כושל שלהן עשוי לפגוע באופן משמעותי ביכולת להגן על מקומות המקלט. באלו נכללים מערכות התקשורת ברשת והחיישנים הספציפיים הדרושים להפעלת מערכות אלו, וכן מערכות תקשורת פנים־ממשלתיות החיוניות לראש המדינה ולצוותו לצורך פיקוד ושליטה ולשם תקשורת בין ראשי מדינות. תנאים אלה זכו להסכמת שתי המעצמות הגדולות במהלך המלחמה הקרה. ההסכם לאמצעים שיש לנקוט בעת תאונות (Accident Measures Agreement) וההסכם למודרניזציה של "הקו החם" (Hotline Modernization Agreement) משנת 1971 הגנו על תקשורת לוויינית החיונית להעברת מסרים בין ארצות הברית לברית המועצות בעתות משבר, כמו גם על מתקני התקשורת למערכות התרעה נגד טילים.[18]

ניסיונות לפעול נגד כוחות חירום ונגד אמצעים רפואיים שנועדו להגביל את מספר האבידות מהווים גם הם קו אדום. סוגיה זו זכתה להסכמתם של דיפלומטים רוסיים ואמריקאיים ב־2011 ונכללה גם ב"מדריך טאלין", וזאת במטרה להחיל את החוקים הקיימים של דיני העימות החמוש על ההתנהלות בתחום הסייבר.[19] המדובר באמצעים ובמערכות תקשורת לפיקוד ושליטה של כוחות חירום ורפואה, וכן לתקשורת עם ראש המדינה. חשוב לציין עוד שהגנה על מערכות התקשורת פירושה גם הגנה על נתונים מפני השחתה: אם לא ניתן להגן על הנתונים, המשמעות המעשית היא חבלה במערכות התקשורת המשמשות להעברת הוראות.

כאשר מדובר בהגנה כלכלית על מקום המקלט, יש לשאול את השאלה: באיזה שלב הופך הנזק הכלכלי לחמור כל כך, עד שמלחמה היא בלתי נמנעת? לפי ספרות מדע המדינה, קשיים כלכליים יכולים להביא לשינוי פוליטי: מיתון יכול להוביל להחלפת מפלגת השלטון במדינות דמוקרטיות,[20] ותקופות שפל יכולות להביא לשינוי משטר דרך עליית תנועות קיצוניות, כפי שאירע בתקופה שבין שתי מלחמות העולם.[21] אם תסיסה כלכלית כזו מקורה בחבלת סייבר, היא מהווה "פעולה כופה" שנועדה להרוס את שלמותה של המדינה.[22] תוצאה "פוליטית" זו עשויה להצטרף להגבלת משאבים שתוטל על צבאה של אותה מדינה כתוצאה מהקשיים הכלכליים. צמצום משמעותי במוכנות הצבאית הוא נקודת סף בפני עצמה. תרחישים אחרים עשויים להיות מניפולציה ישירה על מנגנוני הפיקוח הפוליטיים של המדינה (למשל, השחתה של מערכות הצבעה אלקטרוניות וסחיטה אלקטרונית המונית של נבחרי ציבור). אם רוב פוליטי יכול ליפול בעקבות חבלת סייבר, דינה של חבלה כזו הוא כדין ניסיון משמעותי לפגיעה בשלמות המדינה, ולכן כדין חציית קו אדום. אלו הן פעולות הפוגעות בצורה כה חמורה, עד שניתן לסווגן בקלות כ"בלתי קבילות לחלוטין". מתקפות שגורמות לתוצאות כאלו נחשבות ב"מדריך טאלין" ל"מתקפות חמושות".[23] בנקודת סף זאת, תגובה צבאית היא ודאית.

אם זהות התוקף ידועה, זהו חלק מ"שפת האלימות" המקובלת בין מדינות, וניתן להחיל עליה את כלליה של "שפה" זו. המדינות ייכנסו אז למשחק הסלמה – מתגובה קונבנציונלית ועד תגמול בעל פוטנציאל אסטרטגי. נשק הסייבר יהפוך אז לנשק נלווה לשאר מערכות הנשק,[24] אף שמדינות יכולות להגיב בעוצמה זהה עם נשק שאינו סייבר. הדבר יוסיף ממד של הבהרה ודגש לשיח זה. (ראו תרשים 1)

תרשים 1: מסגרת לקבלת החלטות בעלת סובלנות להשפעות



אם התוצאות ניתנות לזיהוי ומשפיעות על נכסים או על אוכלוסייה אזרחית, ואם זהות התוקף ידועה, אזי ניתן להגדיר את הפעולה כטרור. האקרים המאפשרים מתקפות כאלו, ללא ייחוס לאומי הניתן לזיהוי, פועלים כ"לוחמים בלתי חוקיים"[25] או כ"לוחמים חסרי זכויות".[26] הם אזרחים המעורבים ישירות בעימות חמוש, תוך הפרה של דיני המלחמה. מכיוון שלא ניתן לקשר אותם למדינה המחויבת לאמנת ז'נבה, ברגע שהמתקפה שלהם גורמת לנזק "בלתי קביל לחלוטין", הם מאיימים למעשה על כל המטרות האזרחיות. התגובה למתקפת טרור כזו חייבת להוביל

למאסר ההאקרים, או לכל הפחות להענשת המדינה המארחת אותם. זאת, בהתאם לתקדים המשפטי שנקבע בעקבות המתקפה על אפגניסטן לאחר אירועי 11 בספטמבר 2001, ובמיוחד לאור החלטות 1368 ו־1372 של מועצת הביטחון של האו"ם מ־2001.[27] כמו במקרה של טרור גרעיני הנעדר ייחוס, גם כאן, איסוף מודיעין הוא המפתח לפעולת תגמול.[28]

בין ה"קביל" ל"בלתי קביל לחלוטין" משתרע שטח אפור של משברים. הנזק במקרים הנכללים בשטח זה ברור דיו כדי שאותם מקרים יוגדרו כ"שימוש בכוח", אך עוצמתו אינה חמורה מספיק כדי להגדיר אותו בוודאות כ"מתקפה חמושה".[29] כפי שמציין בית המשפט הבין־לאומי לצדק, המצוטט ב"מדריך טאלין": "[...] לא כל שימוש בכוח עולה לדרגת מתקפה חמושה".[30] המשבר יכול להישאר נסתר מעיני הציבור – אופציית ברירת מחדל שנועדה למנוע התערבות ידיים רבות מדי בעולם חסר החוקים של מרחב הסייבר – אם כי הוא יהיה עדיין אמיתי. לאי־הוודאות במקרה זה יש סיבות רבות. התוצאות של מקרה "בלתי קביל לחלוטין" אולי טרם התממשו, אולם ניתן להתייחס אליהן כאל ודאיות: אם הבעיות בבנקאות המקוונת מתפשטות ונמשכות מספר שבועות, האם הדבר לא יוביל לפאניקה פיננסית? האם ההתאוששות תהיה פשוטה? כך גם לגבי מקרה של פריצת רֶשת החשמל, אף שביום השני לאירוע יהיה עדיין קשה לומר דברים ברורים.

לא רק שקשה להעריך את התוצאות הישירות, אלא שגם קשה להעריך מה המשמעות של פעולות צבאיות של האויב במרחב הסייבר, קרי של "תזוזת צבאות וירטואלית". זוהי נקודה קריטית, מכיוון שעל פי כללי המלחמה, כפי שנוסחו לראשונה על ידי סאן צו, ההפתעה היא המפתח לניצחון:[31] הלוחם הטוב יותר הוא זה שאינו יוצר דפוסים קבועים או תקדימים, ושצעדיו קשים לניבוי.

חובה להתמודד עם מצב זה של "שטח אפור" ולמפות אותו. ניתן להיעזר לצורך זה בקטגוריות ההסלמה שתיאר הרמן קאהן בספרו *On Escalation*.[32] מהי עוצמת המתקפה, מבחינת הסבירות שהיא תגיע לדרגה של "בלתי קבילה לחלוטין"? כמה מרכיבים שונים של המדינה כמערכת מותקפים? מהם ההתפתחות והקצב של המתקפה, במיוחד לאור העובדה שהאצה חדה בהם עלולה להיות סימן לפעולות צבאיות פיזיות העומדות על הפרק? הסיווג שמציע הרמן קאהן מאפשר לעשות הבחנה פשוטה בין:

1. מה שאינו קביל, אולם מבטא ריסון עצמי בהסלמה: המתקפה מוגבלת בעוצמתה ולא ניתן להגדירה כמאיימת על מי שאינם לוחמים. היא מוגבלת בהיקפה בכך שרק סוג אחד של מטרות מותקף; היא מוגבלת בממד הזמן שלה בכך שהתרחשה רק פעם אחת או פעמים ספורות בלבד, או שיש לה "תאריך תפוגה". מתקפות כאלו ניתן לסווג כמתקפות "מוגבלות".

2. מה שאינו קביל וניתן להגדירו כבעל פוטנציאל להסלמה: העוצמה או ההיקף של המתקפה נראים כנטולי ריסון עצמי ועלולים להסלים, או שיש חזרה והאצה שלהם לאורך זמן, ללא תאריך סיום ברור. מתקפות כאלו ניתן לסווג כמתקפות "מסלימות".

לדוגמה, אם GlobalWorm היה מכוון במודע לשנות את התפקוד של תוכנה או של ציוד ספציפיים בלבד, או אם התוכנה או הציוד שנפגעו מ־GlobalWorm היו רק לשימוש צבאי או לשימוש כפול, ולא הייתה זליגה למערכות נשק אחרות או לתשתית אזרחית, או אם השינוי שחל לא הוביל לנזק נלווה משמעותי בקרב כוח אדם אזרחי או בחיי אזרחים, או אם ל־GlobalWorm היה תאריך תפוגה ידוע (לדוגמה, כתוצאה מאישורים דיגיטליים שהגנו עליו ואשר נועדו לפוג במועד מסוים), אזי מתקפת GlobalWorm נגד מדינה X הייתה מוגדרת כמתקפה "מוגבלת". אולם נראה שאין זה כך במקרה של מדינה X: תוצאות המתקפה עליה אינן מוגבלות לציוד מסוים אלא הולכות ומסלימות, וכמו כן קשה לזהות מה יהיו ההשלכות המשניות שלה, למשל של היעדר פעילות בנקאית מקוונת במשך 48 שעות.

כדי לפשט את העניין, ניתן לצרף יחדיו תוצאות "מזוהות"[33] (שניתן לזהותן ולהבין היטב את כל ההשלכות המיידיות שלהן) אך "מסלימות", עם תוצאות שהן "קשות לזיהוי" (שלא ניתן להבין באופן מלא מה יהיו כל ההשלכות המיידיות שלהן). שני סוגי התוצאות מציגים סיכון גבוה להפתעה, לשיפוט שגוי ולהסלמה, כמפורט בתרשים 2.

תרשים 2 – מסגרת החלטות ל"משברים"

		אפיון התוצאות	
		מזוהות ומוגבלות	קשות לזיהוי / מזוהות ומסלימות
אפיון הזהות	ידוע	מִבצעים מיוחדים/ מכה מוגבלת. יריית אזהרה.	מתקפות נגד מערכות נשק טקטי. מתקפות בעצימות נמוכה נגד אזרחים.
	לא ידוע	מבצעים חשאיים. פעולת ריגול (שלא נחשפה).	מתקפת חבלה. טרור בעצימות נמוכה. פעולת איסוף מידע.

תהליך ההערכה

הקטגוריה של תוצאות "קשות לזיהוי" הינה בעייתית במיוחד. קשה להשיג דרגה מספיקה של חיזוי לתוצאות אלו: לא מדובר בנזקים "סבירים לחיזוי", אם להשתמש בביטוי שמופיע ב"מדריך טאלין";[34] לא די בהסתמכות על צפייה בתוצאות, מקיפה ככל שתהיה, תוך התמקדות במודיעין, או בניתוח צורת הפעולה של התוכנה הזדונית בסביבת התוכנה שלה; גם לא ניתן להגיע, בעזרת צעדים חיוניים אך בלתי מספקים אלה, להערכת ההשלכות על "מדינה הנתפסת כמערכת" – אם להשתמש במונחים של קולונל ג'ון וורדן.[35] הערכה כזו היא תוצאה של בניית מודלים, הדמיה וניתוח מערכות, כולל רכיבים חברתיים וכלכליים. המטרה של ניתוח כזה היא להעריך את הנזק הפוליטי הצפוי למדינה המותקפת. בהקשר הגנתי, הצעד הבא יוביל באופן טבעי לניתוח, באמצעות תהליך של הִנדוס לאחור, של "מבצעים מבוססי תוצאה". המטרה היא לא להשיג את הדיוק הדרוש לשימוש התקפי ב"מבצעים מבוססי תוצאה", שהיה קשה למדי להשגה עד היום, עם כלי התוכנה הנוכחיים;[36] המטרה היא להטמיע, כחלק מהשימוש ההגנתי, צורה של לוחמת סייבר שנקודת הסף שלה מוכרת מבחינה בין־לאומית ושתקשר את פעולות הסייבר עם יעדים רצויים ועם תוצאות ישירות. הדבר גם ישמש למתַן תוקף חוקי לכל סוגי התגובות, לרבות פעולות קינטיות או דיפלומטיות. או אז, הקטגוריה של "פשוט, בולט וניתן לזיהוי" תהפוך לקטגוריה של "מדויק ביותר".

כדי שאפשר יהיה לתת אמון בצורת לוחמה זו, חיוני שמעצמות הסייבר המובילות יצהירו עליה. השתתפות מדינות נוספות בגיבושה, על פי אותו הגיון מרכזי משותף, תבטיח שהיא גם תוכר על ידי גורמים רבים, ובאופן כזה גם תהפוך לשיטה הבולטת והמקובלת. כדי להיות גם אמינה, יהיה עליה לשקף את ההשפעה האמיתית שיש לה על עקומת האמינות של המדינה. לשם כך, יהיה צורך לפעול על פי המתווה של קולונל ג'ון וורדן ולפתח מסלול של מחקר והדמיות, שמטרתו להבין את מהותה של "המדינה המרושתת כמערכת". במסגרת זו ניתן יהיה לבחון ב"טווחי סייבר" וירטואליים לא רק את האינטרנט, אלא גם רכיבי משנה של המדינה.

ארגונים ומערכות תשתית שונים לוקחים כיום חלק בהפצת "נתוני ענק" (big data) – החל מפרויקטים של נתונים פתוחים במגזרים ציבוריים, דרך ממשקיAPI בתהליכים פנימיים של תאגידים ותעשיות,[37] וכלה בשימוש חברתי ופוליטי, כפי שהוא מתבטא ברשתות חברתיות. כל אלה מסייעים בפיתוח מודל בסיסי משופר ומדויק יותר של "המדינה המרושתת כמערכת". מודלים דינמיים אלה של מידע יכולים להיבדק אז מול הדמיות של מקרי אלימות. במקרה זה, הדייקנות פחות חשובה מאשר הערכות אמינות ומוסכמות. התפתחות זאת תהיה כרוכה במאמץ מתמשך, שכן מרחב הסייבר מתפתח ללא הרף.

הבנה של נקודת הסף אינה פותרת את הבעיה המרכזית השנייה בתחום המידע, והיא שאלת הייחוס. בעיה זו מחייבת מאמץ ייחודי המעֵבר מודיעין, כפייה ודיפלומטיה.

אסטרטגיה שנייה של "צמצום מידע אסימטרי": הבהרת שאלת הייחוס בעזרת "כפייה משותפת"

מכיוון שמרחב הסייבר נשען על שלושה יסודות – חומרה, תוכנה,[38] ו"תודעת רשת" (brainware) – על המודיעין לחקור ולפתח השערות לגבי כל אחד משלושת היסודות האלה. מערך הייחוס צריך להיות מורכב מאוסף של סימנים אופייניים שונים, כמו דפוסי תעבורת IP, סגנונות קידוד ושיטות פעולה. יש לכלול גם מודיעין אנושי "קלאסי" על ההאקרים עצמם ועל נותני החסות הפוליטיים שלהם. פעולות חקירה אלו צריכות להשתמש בשיטות העבודה הטובות ביותר בתחום ליבון הנתונים, תוך שימת דגש על שיטות דדוקטיביות המיושמות במודיעין, כפי שמציע יצחק בן־ישראל.[39] לפי אחת המתודולוגיות של עבודת המודיעין,[40] השערות ייחוס יכולות להיות מוצגות בקבוצות שונות (כגון, "השערה 1: מדינה Y היא התוקפת"; "השערה 2: מדינה Z היא התוקפת"). לאחר מכן ניתן להעמיד נתונים אמפיריים המפריכים כל השערה בכל קבוצה. צבירת נתונים מול השערת הייחוס תהיה השלב הראשון בניסיון לענות על השאלה איזו מדינה היא החשודה העיקרית בתקיפה.[41] הדבר יחייב לזהות מראש את המודלים הרבים של ההכנות הדרושות לפתיחה במתקפת סייבר מאסיבית על ידי מדינה כלשהי ולעשות הדמיה שלהם. מודלים אלה יכללו, כמובן, גם מאמצים נוספים להסתרה ולהקשחת ההגנה. במצב אידיאלי ניתן יהיה לערוך בשלב זה מבחני דדוקציה A/B, בצורה של ניסויים מבוקרים ב"נאשמים" אפשריים, כדי לאשר או להפריך השערות ייחוס. לדוגמה, ניתן לעשות שימוש באחת מהאסטרטגיות ששימשו את הדמות הבדיונית ג'ורג' סמיילי: הדמיה של השפעות בלתי צפויות של תוכנה זדונית עשויה לחשוף את מקורה האמיתי, וזאת בשל חוסר נוחות ומבוכה פתאומיים שהיא גורמת.[42] איתור חוסר נוחות כזה יכול לסייע לקביעת הייחוס.

חתירה אל האמת היא קריטית ליצירת הגנה וחיונית לשכנוע בעלות ברית שאין כוונה לתמרן אותן. אם מדינות אלו ישוכנעו בכנות הדברים, הן יוכלו להיות "עדי אופי" בפני דעת הקהל העולמית ולספק קונצנזוס דיפלומטי רחב יותר לאופציות התגמול. חתירה אל האמת גם תבטיח שהדרג הפוליטי של המדינה המתגוננת לא יטעה טעות חמורה בייחוס המתקפה, ושלממשלתה יהיה ביטחון מלא בהחלטותיה. בשלב זה תימצא הממשלה במקום נוח יותר לבחון אמצעים לא פומביים ולא מענישים, אם אלה הם אכן האמצעים הנדרשים. כמו בכל עבודת

ריגול נגדי, ייתכן שטוב יותר לשמור לזמן מה את האויב באשליה שתחבולותיו טרם נחשפו.

במרחב הסייבר, כמו בכל תחום מידע אחר דוגמת המודיעין ה"מסורתי",[43] אמת היא כוח. האמצעים והשיטות לביסוס אמת שלכאורה אינה ניתנת להפרכה הם המפתח לכוח, ולכן המפתח להשפעה. יבוא יום שזירת הדיפלומטיה בסייבר תֵדמה לזירת האינטרנט האזרחי הרגיל, שבו כמה ממנועי החיפוש הגדולים ביותר או ספקי תוכן (כמו ויקיפדיה) מתחרים על מקומם כבעלי הרלוונטיות הגבוהה ביותר. היכולת להפריד ולבודד את האות הנכון היא התכונה החשובה ביותר של כל מערכת מידע.

מן הסתם, קשה לשתף מספר רב של מדינות בנתונים ובטכניקות של קביעת הייחוס שצוינו לעיל, כפי שמקובל לרוב בשיתוף פעולה מודיעיני. בעולם ההופך בהדרגה לרב־קוטבי, אם לא תימצא דרך לטפל בהבהרת סוגיית הייחוס או לנהל אותה במשותף, הדבר עשוי להוביל לשיתוק יכולת ההגנה או לחילופין לירידה באמינות ההרתעה. ייתכן שניתן למצוא שיטה כזו באמצעות מבחן דדוקטיבי רחב היקף ופומבי, במיוחד לאור העובדה שדדוקציה היא שיטה מעולה להבהרת האמת בניתוחים מודיעיניים.[44]

ריצ'רד קלארק ורוברט נֶייק מדגישים בספרם *Cyberwar* את "עקרון ה־רֶסָנִיסְט": נטל החקירה צריך להיות מועבר מהחוקרים אל המדינה שממנה שוגרה המתקפה.[45] אם המדינה החשודה תסרב לשתף פעולה, היא תיחשב לאחראית. במקרה כזה, גוף בין־לאומי, שקלארק ונייק מכנים "צוות בין־לאומי לציות וזיהוי פלילי בסייבר", יהיה רשאי להציע סנקציות סייבר, החל מהשבתת ספקי שירותי אינטרנט מסוימים ועד חסימת אותה מדינה בפני מרחב הסייבר.[46] הישענות על גישה זו והרחבתה מאפשרות לטפל באופן ממשי בכמה מקרים של לוחמת סייבר, שהם בעלי פוטנציאל להיות חמורים במיוחד, ולשקם מחדש את הרתעת הסייבר. בנוסף לקביעת עצם הייחוס באמצעות "עקרון הארסניסט", גישה כזו יכולה לייחס מעשית את המתקפה לתוקף מסוים. במונחים דיפלומטיים, היא יכולה למנוע מהתוקף את השימוש ב"הכחשה סבירה". ביסוס הייחוס הוא חקירה מודיעינית לא פחות משהוא תהליך דיפלומטי, שבֵּן יש לפעול לשכנע בו מדינות נוספות.

אמינותה של האמת מושגת טוב יותר כאשר משקיפים (או בוחנים) חיצוניים מאשרים את השערת הייחוס. תהליך חברתי זה קיים מאז "כלל שני העדים" במשפטי בגידה בימי אנגליה האליזבתנית,[47] דרך הכלל של הופר בנוגע ל"עדות בו־זמנית",[48] ועד לשיטות הסטטיסטיקה המודרניות, שבהן עולה הביטחון בתחזיות ככל שגדֵל מספר התצפיות. מבחן ברמה הציבורית מחייב שמדינות ותושביהן יהפכו לתצפיתנים.

תהליך דיפלומטי יבטיח תיאום טוב יותר, ולכן יחזק את מצור הסייבר שיש להטיל כדי ללחוץ על מדינות חשודות. חוזק המצור חיוני כדי שהאיום יהיה אמין. אם ניתן יהיה להתגבר עליו, כפי שמעצמות המערב הצליחו לעשות במהלך משבר ברלין ב־1948 כנגד המצור שהטילה ברית המועצות על העיר, אזי המדינה המאיימת תיכשל במאמציה[49]. אם לא ניתן יהיה להתגבר על המצור, אזי המדינה המאוימת תיאלץ לבחור בין הסלמה ובין נסיגה, וכאשר הסיכון לעצמה יהיה גבוה מדי, יש סיכוי סביר שהיא תבחר לסגת, כפי שברית המועצות עשתה במהלך משבר הטילים בקובה ב־1962. בנוסף לכך, קידום תהליך הייחוס – תחילה עם ידידות קרובות ולאחר מכן עם קבוצה גדולה יותר של מדינות – יוביל ליצירת רצון טוב, להתקרבות וליתר הבנה כלפי המדינה המתגוננת. מצב זה נותן למדינה המתגוננת שוליים פוליטיים לתמרון, אם תבקש לפעול להטלת סנקציות דיפלומטיות, כלכליות או צבאיות נוספות מעבר למרחב הסייבר ולמצור הסייבר. הדבר יתרום לאמינות נוספת לְמה שביסודה היא אסטרטגיה כופה, או כפי שתיאר זאת שֶלינג: "איום המיועד להניע את האויב לפעולה כלשהי".[50] מדינות חשודות ייאלצו לשתף פעולה, אחרת הן ימשיכו לסבול לא רק ממצור הסייבר, אלא גם מבידוד. מדינות שיהיו מעוניינות להוכיח את רצונן הטוב יעדיפו לשתף פעולה ולו כביכול, ואולי אפילו יחלקו את המודיעין שלהן הנוגע לסוגיית הייחוס, כמחווה נוספת של רצון טוב. מדינות שלא ישתפו פעולה יַחשפו בכך את כוונותיהן האמיתיות.

קל יותר לכפות שיתוף פעולה אם המדינות המעורבות לא צריכות להתבזות. ניתן להשתמש באבטחת סייבר במודל לבריאות הציבור של רָטְרֵי והִילֵיי ובמטאפורה של צוותי החקירה של ארגון הבריאות העולמי (WHO) הפועלים בעת מגפות:[51] ממשלות אינן חייבות להיות מואשמות ישירות, שכן הן אינן האחראיות למגפה; במקרה שלנו האשמה מוסטת אל עבר התוכנה הזדונית או אל עבר ההאקרים הזדוניים שמאחוריה. ניתן לנצל את העובדה של היעדר ייחוס ברור של המתקפה למדינה מסוימת, כדי לאפשר לקואליציה של המדינות המתגוננות לבקש את שיתוף הפעולה של המדינות החשודות. כשם שאזורים שלמים מוכנסים להסגר בעת מגפות, כך יכולה להתבצע גם חסימת הסייבר. במצב זה, המחיר של אי־שיתוף פעולה יוטל על הצד התוקף, ומחיר זה יעלה ככל שמדינות אחרות ישתפו פעולה והמדינה התוקפת תידחק לבידוד הולך וגובר. מנגד, מחיר שיתוף הפעולה מצד המדינה התוקפת יהיה נמוך יותר, שכן הוא לא יהיה כרוך באובדן כבוד, גם אם הוא יכלול עדיין איום ממשי – עצם המחיר שהתוקפן אמור לשלם על ביצוע הפעולה: חשיפה ונטרול של יכולות התקיפה שלו (שרתים, קודים, האקרים) כאשר יחליט לבסוף לשתף פעולה. שיתוף פעולה מתמשך מצד המדינה התוקפת, והמודיעין הנוסף שיתלווה אליו, יסייעו לשמר מצב זה.

מדינות שהתחמקו משיתוף פעולה ייאלצו לחזור ולשתף פעולה, וההשקעה שלהן ביכולות ההתחמקות תרד לטמיון. עם זאת, שיתוף הפעולה שלהן לא יהיה כרוך בהכרח בנזק לעצמן בדעת הקהל – דבר ההופך את "החזרה לשיתוף פעולה" לאפשרות סבירה, ולפיכך לבעלת פוטנציאל להשגת יציבות. במצב כזה, המשימה הקשה של ייחוס פומבי ורשמי של המתקפה לגורם ספציפי – דבר המחייב רמת ודאות גבוהה מאד – הופכת למיותרת.

אסטרטגיות ותנאים לכפייה משותפת

כדי שאסטרטגיה זו תצליח, עליה למנף את המאמצים להגיע לייחוס המתקפה. איכות המודיעין היא קריטית למימושה של גישת כפייה זו. ראשי המדינות נמצאים בלב העימות האסטרטגי. דרך התנהלותם ואופן העברת המסרים המאיימים ישפיעו על אמינות פעולת התגמול שלהם. ראש המדינה המתגוננת, בסיוע קואליציה של מדינות ידידותיות, כמוהו כחוקר משטרה המטיח בפני החשודים: "תנו לנו גישה למידע, שתפו עמנו פעולה, או שנשאיר אתכם במעצר". מדובר במיקוח, בדיוק כפי שנעשה בעבודת המשטרה.[52] ככל שהמודיעין טוב יותר, כך תכנון החקירה והתהליך יהיו יעילים יותר: "המידע עשוי להיות מקור הכוח החשוב ביותר" בחקירות.[53] כשנעשה בו שימוש בתהליך החקירה, הוא ממחיש את ההתמצאות הרבה של החוקר. בכך הוא מבסס את אמינותו ואת העובדה שלא ניתן להוליך אותו שולל, והנחקר יהסס למסור לו מידע שגוי. במקביל, החוקר מוכיח שהוא יכול להיות בן־שיח בעל ידע. עסקת שיתוף פעולה תהיה, במקרה זה, עסקה יציבה.

במקרה שלנו, "החוקר" יכול ליזום מבחנים כדי לבדוק באמצעותם את תגובת המדינות החשודות. מבחנים כאלה יכולים לעשות הדמיה של תוצאות בלתי צפויות למדינה המתגוננת. המדינה המתגוננת, מצדה, יכולה לזרוע ספק במדינה התוקפת באמצעות מניפולציה נגדית, המשדרת למדינה התוקפת מסר, לפיו נשק הסייבר אינו כלי אמין ועלול לגרום להסלמה לא רצויה לתוקף.

המדינה המתגוננת יכולה לזכות ביתר קלות באהדה ובתמיכה חיצוניות ככל שהתוכנה הזדונית פוגעת באינטרסים פנימיים חיוניים שלה. הסולידריות שיפגינו כלפיה מדינות אחרות תעמיק ככל שמקורה של התוכנה הזדונית לא יהיה מזוהה, כך שכל מדינה עלולה להפוך ליעד למתקפה שלה. התהליך הדיפלומטי שילווה את הכפייה יסייע בהפניית המתקפה של התוקף כלפי עצמו, כפי שקורה בג'ודו. ככל שמתקפת הסייבר חמורה יותר, כך תתחזק הסולידריות בין המדינה המתגוננת ובין ידידותיה ויתהדק מצור הסייבר על המדינות החשודות. באופן כזה, היוזמה תעבור לידיו של המתגונן, והוא אף יוכל לשלוט בקצב ההסלמה.

אסטרטגיית כפייה זו לפתרון בעיית הייחוס היא בת־ביצוע, שכן מאחורי כל מתקפה מתוחכמת חייבת לעמוד מדינת לאום, ומאחורי כל מתקפה של גורמים

לא מדינתיים עומדת בהכרח מדינה מפותחת. לארגוני טרור הממוקמים ב"מדינות כושלות" אין כרגע יכולת טכנית ליזום מתקפות סייבר מתוחכמות ואסטרטגיות. לדוגמה, "סטקסנט" היה קוד שנכתב על ידי מהנדסי IT מוכשרים ביותר. הוא עשה שימוש באישורים דיגיטליים שנגנבו משתי חברות טיוואניות חוקיות,[54] ונבדק על מודל סייבר מלא, שכָּלל הדמיות של צנטריפוגות P-1.[55] כל אלה מחייבים מימון רב לגיוס ולשימור המומחים, גישה ממשית למאגר מומחים רב־תחומיים (במיוחד אם יש צורך במודלים של סייבר), וכן השקעה קבועה בהכשרה ובפיתוח, שכֵּן מרחב הסייבר משתדרג ללא הפסקה. אין גם לשכוח בהקשר זה את הצורך בשירותים חשאיים שיחדרו לתוכנות חסויות או ישיגו גישה אליהן. מדובר ביכולות שנכון להיום אינן מצויות באזורים לא מפותחים של העולם.

כאמור, מאחורי כל ארגון אד־הוק הפותח במתקפת סייבר מתוחכמת ניצבת מדינת חסות מפותחת ומתקדמת. מדינות מתקדמות תלויות יותר מתמיד במרחב הסייבר לצורך גישה לנתונים, פיתוחם ועיבודם. חלק גדול מהתקשורת העסקית ועיבוד הנתונים עובר ל"ענן", כלומר לשרתים הממוקמים לרוב במדינות זרות. לאור זאת, ההשפעה המשתקת שיש לחסימת הסייבר עשויה להיות חריפה במיוחד במדינות מפותחות.

אסטרטגיית הכפייה המשותפת תפעל אם בעלות בריתה של המדינה המתגוננת ייאלצו או יומרצו גם הן לפעול. יש ליצור תיאום מתמשך, הסכמה על נורמות ושיתוף תהליכים כתנאים מוקדמים לכך, עוד לפני פרוץ המשבר. רמות שיתוף הפעולה יהיו פועל יוצא של מעגלי הקִרבה בין המדינות משתפות הפעולה – מהידידות הקרובות ביותר ועד לרחוקות ביותר – כך שמרחב הסייבר ישקף את מערכת היחסים והסכמי שיתוף הפעולה הקיימים ביניהן זה מכבר.[56] בנוסף, כדי להוסיף אמינות לתהליך, ניתן להגביר את שיתוף הפעולה בתוך המעגלים ובין מעגלים סמוכים. התוויית הכיוון הצפוי חשובה כדי לגבש שיתוף פעולה בין־לאומי. חשובים עוד יותר הם הקשרים בין הצדדים, שצריכים לקבל תרגום מעשי בשטח. לדוגמה, מדינות ידידותיות יכולות לעשות שימוש בתוכנות הנמצאות בשימוש אצל מדינות ידידותיות אחרות. שימוש משותף באותה תוכנה או באותם תקנים יגביר את הסיכון של המדינה התוקפת להיתקל בתוצאות בלתי צפויות. שימוש כזה גם מעביר מסר חזק שהתקפה על מדינה מסוימת כמוה כהתקפה על כל ידידותיה. שימוש משותף באותה תוכנה במרחב הסייבר עשוי למלא תפקיד דומה לזה שמילא הכוח הצבאי האמריקאי בברלין במהלך המלחמה הקרה[57]: הוא ייצור מעורבות אוטומטית ולא יותיר ספק בכך שתהליך הכפייה מופעל במשותף בידי קואליציה של מדינות ידידות.

על המדינות המתגוננות לייצר יכולות סייבר עודפות כדי שיוכלו לספוג את המכה הראשונה. יכולות מִחשוב ותקשורת עודפות יפחיתו באופן זמני צווארי

בקבוק. ניתן לנטרל באופן חלקי מניפולציה סמנטית בעזרת שמירה של נתונים חיוניים במאגר נתונים "לכתיבה בלבד", וזאת כדי לאפשר שחזור "ערכי אמת" לפני מתקפה.

אמצעי הגנה הם לרוב בלתי מספיקים. כל עוד לא מתמודדים עם נחישותו של האויב ללמוד טכניקות מתקפה חדשות, הוא ימשיך ללמוד ולאמץ כאלו, כשהוא מחקה את דינמיקת האבולוציה של "המַלכּה האדומה" הקיימת בטבע.[58] ללא התמודדות כזו לא ניתן להשיג הרתעה. כדי להשיגה יש להתמודד ישירות עם רצון התוקף ללמוד שיטות תקיפה חדשות מבלי לחלוק אותן עם אחרים; כמו כן, יש לקבוע מחיר לאויב על שאיפותיו אלו. בכל מקרה, חיוני שתימצא בידי המותקף יכולת לספוג את המכה הראשונה. מודלים להרתעה קונבנציונלית יוצאים מתוך הנחה שחולשה של המותקף מזמינה מתקפות עליו.[59] במצב של חולשה, מכה ראשונה עלולה להיות כה קשה, עד שלמדינה המותקפת לא יהיה זמן לתגובה ראויה ולגיבוש קואליציה של ידידות.

המצב האידיאלי הוא שתהליך הייחוס ייקבע בעזרת צוות מפקחים בין־לאומי. דבר זה יבטיח את שמירת "הצל הארוך של העתיד":[60] במצב כזה, האמת תצא לאור, סוגיית הייחוס תובהר סופית והתוקף לא יוכל לברוח מאחריות.

לסיכום, ברגע שנקבע הייחוס וניתן לזהות ולהעריך את תוצאות התקיפה במסגרת עקומת האמינות של המדינה המתגוננת, האסימטריה פוסקת לפעול לטובת הצד התוקף. "שפת הפעולה הצבאית" שבה לפעול לטובת הצד המתגונן, שיכול אז לאיים בצורה אמינה בתגמול. לאחר זיהוי ראוי של תוצאות ההתקפה, המתגונן יכול ליזום תגובה הולמת אפילו בעזרת אמצעים שאינם סייבר – דיפלומטיים, כלכליים, קינטיים או אסטרטגיים. יכולת זו מעניקה משקל רב יותר לצד המתגונן, וכל האופציות הופכות אז לזמינות עבורו. איומים בתגובה שאינה בתחום הסייבר יכולים להיות עדיפים, אם יתברר שתגובה כזו היא בלתי פגיעה למתקפות סייבר. יכולת העמידה שלה תהפוך אותה אז לבת מימוש. חריגה מתגובה באמצעות סייבר בלבד מהווה איתות של הצד המתגונן כי ביכולתו לעבור למתקפות שיש להן תוצאות חומריות ממשיות. התוקף ייאלץ אז לבחור בין נסיגה להסלמה, וייקלע למצב קשה, במיוחד כאשר יעמוד מול כפייה רבתי. כאמור, כפי שהיה בעת משבר הטילים בקובה, במצב כזה התוקפן המבקש לחרוג מהסטטוס קוו יעדיף לסגת מאשר להסלים את המצב.

סיכום: לקראת דוקטרינה צבאית ומדינית חדשה לעידן הדיגיטלי

הצורך ליצור שוויון בתוצאות השימוש בנשק הסייבר ובנשק שאינו סייבר, והצורך להחליף את אמצעי התגמול מאמצעי סייבר לכאלה שאינם סייבר, מצביעים

על החשיבות הרבה שיש להגדרה מחודשת של הפעולות הנעשות במסגרת לוחמת הסייבר, יחסית לשאר מערכות הנשק. בהמשך לדברי אדוארד לוטוואק,[61] אסטרטגיית סייבר המתבססת על כוח אחד (one force) עשויה להיות בלתי יעילה, בדומה למה שלוטוואק מכנה בביטול "לא־אסטרטגיה", דהיינו, אסטרטגיה המבוססת על כוח אחד בלבד וטוענת לאוטונומיה אסטרטגית, כמו "אסטרטגיה ימית", "אסטרטגיה אווירית" ו"אסטרטגיה גרעינית".

מרכזי הכובד של אסטרטגיות הלחימה התפתחו תמיד בד בבד עם השינויים הטכנולוגיים באמצעי הלחימה. כך, מרכזי הכובד במלחמה הקרה היו שונים מאלה של מלחמת הבזק של גוּדֶריאן, או של וָאוּבָּאן ומבצרי הענק שלו; האסטרטג ג'וליאן קוֹרְבֶט קבע ששליטה ימית ניתן להשיג לא על ידי כיבוש שטחים ימיים – שאינם אפשריים בהחזקה – אלא על ידי הבטחת יכולת המעבר בימים.[62] ככל שהעימותים עוברים לעולם הדיגיטלי או אל ה"לוגוס" הדיגיטלי,[63] עתידים להתפתח מרכזי כובד חדשים.

ככל שהקריטיות של המרחב הסמנטי גבוהה יותר מאשר הבסיס הפיזי, פוחתת חשיבותם היחסית של קווי התקשורת המסורתיים: האינטרנט נבנה כדי שאפשר יהיה לשגר מידע גם בהיעדר תשתית פיזית. החשוב מכל הוא לוודא את נתוני האמת – מיהם התוקפים? מה הם תוקפים? – לדעת למי לייחס את המתקפה ולהכיר ולזהות את תוצאותיה. אלה הם מרכַזי כובד קוגניטיביים. במונחים אסטרטגיים, זוהי עליונותו של הידע: להפעיל פיקוח ולגונן על המדינה ועל מערכות המשנה שלה מפני מניפולציות במידע. במילים אחרות, האמת היא הגורם החשוב ביותר בעולם המידע.

חשיבות עולם המידע הדיגיטלי יחסית לשאר המרכיבים של "האומה המרושתת הפועלת כמערכת" עשויה לשנות עדיפויות אסטרטגיות. שינויים נוספים בתעשייה עשויים לשנות עוד את סדר העדיפויות החדש. ככל שהתוכנה ממשיכה "לאכול את העולם",[64] וחשיבותם של נתונים ושל יישומים מבוססי־נתונים עולה, כך שמירה על ה"לוגוס" הדיגיטלי עשויה להפוך לחשובה לא פחות מאשר שמירה על הנכסים הפיזיים. בחלק מהתחומים החיוניים זוהי המציאות כבר כיום: עושר נמדד ועובר ידיים באמצעות ביטים אלקטרוניים המייצגים ערכים כספיים. בעוד שעל פי הגדרתו של לוטוואק, לוחמת סייבר נחשבת ללא־אסטרטגיה, יש אפשרות – קטנה ורחוקה ככל שתהיה – שהאסטרטגיה של ה"לוגוס" הדיגיטלי תהפוך לאוטונומית, כלומר תייצג הן את המטרה והן את האמצעים. מערכות מידע, החל מהדנ"א ועד לשפה המדוברת, חיוניות לניהול כל אורגניזם, כך שעליונותו של ה"לוגוס" הדיגיטלי אינה אמורה להפתיע איש.

תהליך זה מסמן שינוי עמוק בתפקיד המדינה המגֵנה על האומה. המדינה חייבת לשמור על המונופול שיש לה להפעיל אלימות בקנה מידה גדול, אלימות

אותה ניתן להגדיר כהגנה על נכסים פיזיים מפני השחתה באמצעות כוח קינטי. יהיה עליה גם להגן על מהימנות הנתונים שמשמשים את המערכות האסטרטגיות האזרחיות והצבאיות, וברמה גבוהה יותר – לשמר את מהימנותו של המידע האסטרטגי עצמו, וזאת כדי לאפשר המשך המוּדעות למצב של "אומה הפועלת כמערכת". המדינה תהיה אז קו ההגנה האחרון של האמת.

כל האפשרויות האלו נידונו להתממש בשל התגברות יכולות המחשוב והאחסון של טכנולוגיות המידע. לשם דוגמה, כוח המחשוב של מחשבי העל המובילים עתיד להתחזק פי עשר בשלישית פלופס לפחות במהלך עשר השנים הבאות.[65] לאור העלייה בסדרי הגודל של עוצמת המחשוב, אין לשלול גם שינויים גדולים ביכולת ההדמיה והלמידה של המחשבים.[66] אפשר שהמגבלות הקיימות כיום בניתוחי "מבצעים מבוססי תוצאות" ו"מדינה הפועלת כמערכת" הן זמניות, כמו הקשיים שהיו בזמנם בתחום הבינה המלאכותית: הבינה המלאכותית הוגדרה במשך עשורים כשדה מחקר בעייתי,[67] אך כיום היא נחשבת לתחום מבטיח.[68] לאור זאת, היכולות המתפתחות של ניתוח והדמיה של "מבצעים מבוססי תוצאות" עשויות לגרום לשינויים גם בשיקולים של מעצמות גדולות.

עלייה ביכולת ההדמיה פירושה שיפור יכולת החיזוי: בדרך זו מתאפשר מבט ארוך טווח וצפוי יותר על המתרחש. ככל שהמידע על היכולת ה"אמיתית" של כל צד מדויק יותר, כך פוחת הסיכון למלחמה. גם זֶ'ארה[69] וגם אקסלרוד[70] מראים, כל אחד בנפרד, שככל שתהליך זה הולך ומתפתח, כך גובר הסיכוי לגיבוש אסטרטגיות שיתופיות (או אסטרטגיות של סטטוס קוו).[71] שימוש מוצלח באסטרטגיית כפייה משותפת יביא גם הוא בטווח הארוך להעדפת הסטטוס קוו: אם אין תועלת במעבר מצד לצד והכפייה המשותפת צפויה להביא להגברת שיתוף הפעולה, אזי אין טעם בתשלום הכרוך במעבר כזה, והדבר מעלה אוטומטית את ערכה היחסי של אופציית הסטטוס קוו (כלומר המשך שיתוף הפעולה). כפי שמניחה תיאוריית "ההרתעה המושלמת", העלייה בערכה של אופציית הסטטוס קוו יחסית לכל אסטרטגיה אחרת של מעבר מצד לצד, היא אחד הגורמים החשובים ביותר להשגת יציבות.[72]

על רקע דברים אלה ניתן להוסיף, כי הגישות העוסקות בהדמיות של "מדינה הפועלת כמערכת" ושל "כפייה משותפת" מצביעות על כך שכניסתה המואצת של הציביליזציה האנושית למעמקי ה"לוגוס" הדיגיטלי עשויה להפוך לגורם נוסף שיביא לשלום וליציבות. אסטרטגיות אלו של "צמצום מידע אסימטרי" יכולות לשמש כאבני בניין מרכזיות למסגרת דוקטרינרית חדשה לקבוצות חברתיות בעידן ה"לוגוס" הדיגיטלי. מסגרת דוקטרינרית זאת תמשיך לקדם שלום ויציבות, תוך שילוב הדוקטרינות העכשוויות של הרתעה קונבנציונלית והרתעה גרעינית. היא גם תכיר ביתרון של מערכות המידע הדיגיטליות בנושאים אזרחיים וצבאיים, ולבסוף תוביל להגדרה מדויקת יותר של מושג העימות.

הדוקטרינה של "השמדה הדדית מובטחת" הפכה את המלחמות בין מתחרים לעמיתים בזירה הבין־לאומית לתרגיל עקר ב"משחק־סכום־שלילי", וזאת במידה רבה בשל היכולות להנחית מכה שנייה. דוקטרינה של שיתוף פעולה דיגיטלי כפוי, המלווה בביטול כל יתרון אסימטרי בתחום המידע שיש למדינה הקוראת תגר, עשויה לסייע בבלימת הסלמתם של משברים בין־לאומיים ב"ציביליזציה הדיגיטלית" של המאה ה־21.

הערות

1 ניתן לראות מאמר זה כהשלמה לסוגיות אי־היציבות במרחב הסייבר שפורטו במאמר: Guy-Philippe Goldstein, "Cyber Weapons and International Stability", *Military and Strategic Affairs*, Vol. 5, No. 2, 2013, pp. 121-139.

2 Sun Tzu, *The Art of War*, (transl. Lionel Giles), 1910, Ch. 3, http://www.gutenberg.org/cache/epub/132/pg132.html

3 Frank C. Zagare, D. Marc Kilgour, *Perfect Deterrence*, Cambridge: Cambridge Studies in International Relations, 2000, pp. 296-301.

4 Paul K. Huth, *Extended Deterrence and the Prevention of War*, New Haven: Yale University Press, 1988, cited in: Zagare, Kilgour, *Perfect Deterrence*, pp. 296-301.

5 לפירוט נוסף של הסוגיה ראו לדוגמה: Goldstein, "Cyber Weapons and International Stability".

6 שם.

7 William W. Kaufmann, *The Requirements of Deterrence*, Princeton: Center of International Studies, Princeton University Press, 1954; Fred Kaplan, *The Wizards of Armageddon*, Stanford: Stanford University Press, 1983, pp. 193-200.

8 ראו דיון בנושא זה אצל: Goldstein, "Cyber Weapons and International Stability". גולדשטיין מפנה להגדרות של תומס שלינג ל"קו אדום":
Thomas C. Schelling, *Arms and Influence*, Yale University Press, 1966, p. 137.

9 ראו דיון אצל גולדשטיין, שם, המפנה לרעיון של "עקומת האמינות" בתוך:
Carey B. Joynt, Percey E. Corbett, *Theory and Reality in World Politics*, Pittsburgh: University of Pittsburgh Press, 1978, pp. 94-95.

10 Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, New York: Cambridge University Press, 2013, p. 88: "The international Group of Experts achieved no consensus as to whether non-destructive but severe cyber operations satisfy the intensity criterion"; Ibid. pp. 82-83, comments #14 and #15.

11 דוגמה לדיון על לוחמת סייבר בהקשר של "לוחמה מבוססת השפעה" ראו:
Amit Sharma, "Cyber Wars: A Paradigm Shift from Means to Ends", in: Christian Czosseck and Kenneth Geers (eds.), *The Virtual Battlefield: Perspective on Cyber Warfare*, Amsterdam: IOS Press, 2009.
"מדריך טאלין" מציין בצורה מפורשת עוד יותר כי "פעולת סייבר מהווה שימוש בכוח כאשר ניתן להשוות את ההיקף וההשפעה שלה לפעולה שאינה סייבר שעושה שימוש בכוח" (כלל מספר 11); ולאחר מכן: "מתקפת סייבר היא פעולת סייבר, בין אם לצרכי הגנה או התקפה, שיש סיכוי סביר שתגרום לפגיעה או למוות לאנשים, או לנזק או להרס של אובייקטים" (כלל מספר 30). הדיון מדגיש בהקשר זה כי: "אין לראות

'פעולות אלימות' כמוגבלות לפעולות של כוח קינטי. הדבר מוסדר היטב בדיני העימות החמוש. בהקשר זה יש לציין שמתקפות כימיות, ביולוגיות או רדיולוגיות חסרות בדרך כלל השפעה קינטית על המטרה, אולם יש הסכמה כוללת שהן מהוות מתקפות על פי החוק". מה שחשוב הוא ההשפעה הישירה על אוכלוסייה אזרחית או על רכוש, ואין זה משַנה באיזו דרך – קינטית או אחרת.

12 Col. Paul M. Carpenter and Col. William F. Andrews, "Effects-Based Operations – Combat proven", *Joint Force Quarterly* 52, 1st Quarter (2009), pp. 78-81.

13 קבוצת המומחים הבין־לאומיים של "מדריך טאלין" מציינת את הרעיון של "היקף ותוצאה", שהוצג בפסק הדין של בית הדין הבין־לאומי לצדק בעניין ניקרגואה: "Nicaragua judgement: Military and Paramilitary Activities in and against Nicaragua (Nicar. V. US), 1986 I.C.J.14 (27 June); Schmitt, *Tallinn Manual*, p. 45.

14 Christopher D. Baker, "Tolerance of International Espionage: A Functional Approach", *American University International Law Review*, Vol. 19, Issue 5 (2003), pp. 1091-1113.

15 "The lack of an international prohibition of espionage leaves decision makers with the usually acceptable liability of merely violating the target nation's domestic espionage law": Thomas C. Wingfield, "Legal Aspects of Offensive Information Operations in Space", *USAF Academy Journal of Legal Studies*, 121, 1999, p. 140; Martin C. Libicki, *Cyberdeterrence and Cyberwar*, Santa Monica: Rand Corporation, 2009, pp. 23-24.
הדיון על כלל 10 ("איסור על איום או שימוש בכוח") ב"מדריך טאלין" (מהדורת 2013) מציין: "[...] לא כל התערבות ב[מערכות] סייבר מפרה אוטומטית את החוק הבין־לאומי האוסר על התערבות [...] כפי שציין בית הדין בניקרגואה, 'התערבות' מנוגדת לחוק כאשר היא עושה שימוש בשיטות של כפייה. יוצא מכך שריגול סייבר וניצול של סייבר, הנעדרים מרכיב של כפייה, אינם מפרים כשלעצמם את עקרון אי־ההתערבות".

16 Schmitt (ed.), *Tallinn Manual*, Part I, Section 2: Self-Defence, and Rule 32, "Prohibition on attacking civilians".

17 Charles Tilly, "War Making and State Making as Organized Crime", in: Peter Evans, Dietrich Rueschemeyer and Theda Skocpol (eds.), *Bringing the State Back*, Cambridge: Cambridge University Press, 1985; Antonio Giustozzi, *The Art of Coercion: Armed Force in the Context of State Building*, CSRC Seminar, 2008.

18 Agreement on Measures to Reduce the Risk of Outbreak of Nuclear War Between the United States of America and the Union of Soviet Socialist Republics, http://www.state.gov/t/isn/4692.htm; Agreement Between the United States of America and the Union of Soviet Socialist Republics on Measures to Improve the USA-USSR Direct Communications Link, http://www.state.gov/t/isn/4787.htm, Cited in: Laura Grego, *A History of Anti-Satellite Programs*, UCS Global Security Programs, 2012.

19 Karl Frederick Rauscher, Andrey Korotkov, "Russia-US Bilateral on Critical Infrastructure Protection", in: *Working toward Rules for Governing Cyber Conflict*, East-West Institute, 2011; Schmitt, (ed.), *Tallinn Manual*, "3/The law of armed conflict generally" (in particular "Rule 20"), "4/Conduct of hostilities" (in particular "Rule 29 – Civilians" and Section 3: "Attacks against persons").

20 Michael S. Lewis-Beck, Mary Stegmaier, "Economic Determinants of Electoral Outcomes", *Annual Review of Political Science*, Vol. 3 (2000), pp. 183-219.

21 Alan de Bromhead, Barry Eichengreen and Kevin Hjortshøj O'Rourke, *Right Wing Political Extremism in the Great Depression*, Discussion Papers in Economic and Social History, Number 95, University of Oxford, 2012.

22 "מדריך טאלין" מגדיר כלא חוקית פעולת סייבר המנסה לפגוע בעצמאות הפוליטית של מדינה כלשהי (כלל 10).

23 "מדריך טאלין", כלל 11, עמ' 51.

24 Martin C. Libicki, "Cyberspace is not a Warfighting Domain", *I/S: A Journal of Law and Policy for the Information Society*, 8, no. 2 (2012), p. 330.

25 ראו "מקרה קווירין" מ־1942, העוסק במחבלים גרמניים, עם דגש מיוחד על מחבלים שלא ענדו סמלים לאומיים: "[...] מרגל שחוצה את הגבול בזמן מלחמה בצורה חשאית וללא מדים, מתוך כוונה לאסוף מידע צבאי ולהעבירו לאויב, או לוחם של האויב החוצה את הגבול באופן חשאי וללא מדים, במטרה לפגוע בחיים או ברכוש, הם דוגמאות ללוחמים שבאופן כללי אינם זכאים למעמד של אסירי מלחמה, אלא של מי שהפרו את דיני המלחמה, והם יועמדו למשפט וייענשו בבתי דין צבאיים". U.S. Supreme Court, EX PARTE QUIRIN, 317 U.S. 1 (1942). יש לציין שלוחמים בלתי חוקיים זכאים בכל זאת "ליחס הומאני, ובמקרה של משפט לא תימָנע מהם הזכות למשפט סדיר והוגן על פי האמנה הנוכחית": Geneva Convention Relative to the Protection of Civilian Persons in Time of War, August 12, 1949 (GCIV).

26 על "לוחמים חסרי זכויות" ראו "מדריך טאלין" 2013, עמ' 100, הערה 17.

27 Ben Smith, Arabella Torp, "The Legal Basis for the Invasion of Afghanistan", *House of Commons, International Affairs and Defence Section*, February 26, 2010, pp. 4-5.

28 Ashton B. Carter, Michael M. May, William J. Perry, *The Day After – Action in the 24 Hours following a Nuclear Blast in an American City*, Report based on Workshop, The Preventive Defense Project, Harvard and Stanford Universities, 2007, in particular: "6. Retaliation and Deterrence", pp.15-17.

29 כלל 11 ב"מדריך טאלין", 2013.

30 כלל 13, הערה 5 ב"מדריך טאלין" 2013, עמ' 55, המצטט את פסק דין ניקרגואה, פסקה 191.

31 "All warfare is based on deception", Sun Tzu, *The Art of War*, p. 66.

32 Herman Kahn, *On Escalation*, London: Pall Mall Press Ltd., 1965.

33 לזיהוי התוצאה יש לצרף ניתוח טכני של התוכנה הזדונית עצמה. דבר זה עשוי לארוך זמן רב. לדוגמה, הווירוס "סטקסנט" זוהה על ידי וירוס "בלוקדה" ביוני 2010, אך נותח לעומק רק בנובמבר 2010. ראו: Nicolas Falliere, Liam O. Murchu, Eric Chien, *W32. Stuxnet Dossier*, Symantec, 2010. מכאן הדרישה לחילופי התרעות מידע עדכניות, שיזרמו מכל מרכזי הפעילות האזרחיים והצבאיים לנקודת איסוף אחת בתחום הסייבר, שתהיה מסוגלת לפרש תקריות סייבר וליצור תמונה שלמה לשימושם של מוסדות הביטחון של המדינה.

34 ראו כלל 30, הערה 5, ב"מדריך טאלין" 2013, עמ' 106.

35 John A. Warden III, "The Enemy as a System", *Airpower Journal*, Vol. 9, Issue 1, 1995.

36 General James N. Mattis, USMC, "USJFCOM Commander's Guidance for Effects Based Operations", *Joint Force Quarterly,* No. 51, 2008; Paul M. Carpenter, William F. Andrews, "Effects-Based Operations Combat Proven", *Joint Force Quarterly*, No. 52, 2009: (ביקורת של קציני חיל האוויר האמריקאי על USJFCOM).

37 Robin Vasan, "Business Process API-ification: the LEGO promise fulfilled",

GigaOm, October 6, 2012, http://gigaom.com/2012/10/06/business-process-api-ification-the-lego-promise-fulfilled/; Mark Boyd, "Getting C-Level Buy-In: Demonstrating the Business Value of APIs", *ProgrammableWeb*, September 11, 2013, http://blog.programmableweb.com/2013/09/11/getting-c-level-buy-in-demonstrating-the-business-value-of-apis/

38 לדיון במרכיבים המרכזיים של מרחב הסייבר ראו: Goldstein, "Cyber Weapons and International Stability".

39 Isaac Ben-Israel, *Philosophie du renseignement*, Paris : Editions de l'Eclat, 2004.

40 שם.

41 דוגמה זו שואבת השראה ישירה מניתוח מלחמת יום הכיפורים, כפי שהובא ב: Ben-Israel, *Philosophie du renseignement*.

42 כדי לגלות את הזהות של "ג'רלד", החפרפרת שעבדה עבור ברית המועצות, שולח סמיילי הודעה לראש ה"סירקוס", המאלצת את "ג'רלד" לבקש פגישת חירום עם איש הקשר הסובייטי שלו בדירת מבטחים, שמיקומה היה ידוע זה מכבר לסמיילי. זה המבחן שאִפשר לסמיילי לפרוץ לדירת המבטחים ולזהות את "ג'רלד": John Le Carré, *Tinker Tailor Soldier Spy*, London: Hodder & Stoughton, 1974.

43 לדיון המשווה בין העולם "הדיגיטלי" המגדיר את מרחב הסייבר לבין עולם "המידע החסוי" שמגדיר את תחום המודיעין המסורתי ראו: Goldstein "Cyber Weapons and International Stability".

44 Ben-Israel, *Philosophie du renseignement*.

45 Richard Clarke and Robert K. Knake, *Cyberwar*, New York City: HarperCollins Publishers, 2010, pp. 249-254.

46 שם.

47 L. M. Hill, "The Two-Witness Rule in English Treason Trials: Some Comments on the Emergence of Procedural Law", *American Journal of Legal History*, 12, 1968, pp. 95-111.

48 Glenn Shafer, "the Combination of Evidence", *International Journal of Intelligent Systems*, Vol. I, 1986, pp. 155-179.

49 ראו ניתוח על פי תיאוריית המשחקים של משבר ברלין ב־1948 בתוך: Frank C. Zagare, *The Dynamics of Deterrence*, Chicago: University of Chicago Press, 1987, pp. 11-28.

50 Thomas C. Schelling, *the Strategy of Conflict*, Cambridge: Harvard University Press, 1963, p. 69.

51 Greg Rattray, Chris Evans, Jason Healey, "American Security in the Cyber Commons", in: Abraham M. Denmark and James Mulvenon (eds.), *The Future of American Power in a Multipolar World*, Washington D.C.: Center for a New American Security, 2010, pp. 151-172.

52 Daniel L. Shapiro, "Negotiation Theory and Practice: Exploring Ideas to Aid Information Eduction", in: Robert A. Fein, Paul Lehner, Bryan Vossekuil (eds.), *Educing Information*, Washington D.C.: Intelligence Science Board, National Defense Intelligence College Press, 2006, pp. 267-280.

53 M. P. Rowe, "Negotiation Theory and Educing Information: Practical Concepts and Tools", in: Fein, Lehner, Vossekuil (eds.), *Educing Information*, p. 295.

54 וירוס "סטקסנט" עשה שימוש באישורים דיגיטליים של החברות הטיוואניות Realtek ו־JMicron, שעברו מניפולציה. ראו: Falliere, Murchu, Chien, *W32. Stuxnet Dossier*.

55 David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks against Iran", *The New York Times*, June 1, 2012.

56 ניתן להתחיל, למשל, במדינות החברות ב"תוכנית לשיתוף פעולה טכני" (5 eyes" nations"), שיש להן היסטוריה של שיתוף פעולה צמוד בסוגיות קריטיות (למשל, בפעולות סייבר משותפות או בסוגיות לשיתוף מודיעיני), כמו המדינות המשתתפות בברית נגד אל־קאעדה. ראו:
Dana Priest, "Help from France Key in Covert Operations", *The Washington Post*, July 3, 2005.

57 Schelling, *Arms and Influence*, p. 47.

58 לניסוח ראשוני של הביולוגיה האבולוציונית ראו:
Leigh Van Valen, "A New Evolutionary Law", *Evolutionary Theory* 1 (1973), pp. 1-30; Rattray et al., *The Future of American Power in a Multipolar World*, Section "Adaptation and Counter-Adaptation", p. 154; Kevin Mandia, "Cyber Threats and ongoing Efforts to Protect the Nation", Permanent Select Committee on Intelligence, US House of Representatives, October 4, 2011.

59 Edward Rhodes, "Conventional Deterrence", *Comparative Strategy*, 19: 3 (2000), pp. 221-253, in particular pp. 222-223.

60 Robert Axelrod, *the Evolution of Cooperation*, New York City: Basic Books, 1984. ראו עמ' 13 להסבר על "צל העתיד" ועמ' 124 על "הגדלת צל העתיד" לקידום שיתוף פעולה.

61 Edward N. Luttwak, *Strategy – The Logic of War and Peace*, revised and enlarged edition, Cambridge: The Belknap Press of Harvard University Press, 2001, Chapter 11, "Nonstrategies", pp. 168-184.

62 Julian S. Corbett, *Some Principles of Maritime Strategy*, London: Longmans, Green & Co., 1911, p. 90: "Command of the Sea, therefore, means nothing but the control of maritime communications, whether for commercial or military purposes".

63 לדיון על "לוגוס" דיגיטלי ראו: Goldstein "Cyber Weapons and International Stability".

64 Marc Andreessen, "Why Software is Eating the World", *The Wall Street Journal*, August 20, 2011.

65 FLOPS – Floating Point Operations Per Second – יחידת מידה לעוצמתם של מחשבים. מחשב העל המהיר ביותר ב־2010 היה Cray Jaguar, שמהירותו הייתה 1.8 10^15 פלופס: top500.org, November 2009-2010. ביצועים מעבר לאקסא־פלופ אחד או 10^18 פלופס צפויים להיות מושגים עד שנת 2020: Agam Shah, "SGI, Intel Plan to Speed Supercomputers 500 Times by 2018", *Computerworld*, June 20, 2011.

66 יכולות של זטא־פלופ (10^21) עשויות לאפשר יצירת מודלים לחיזוי מדויק של מזג האוויר לתקופה של שבועיים מראש. ראו בעניין זה:
Erik P. DeBenedictis, "Reversible Logic for Supercomputing" *Proceedings of the 2nd Conference on Computing Frontiers*, Sandia National Laboratories, 2005, pp. 391-402.

67 חוקרים דיברו על "חורף של בינה מלאכותית" במהלך שתי תקופות לפחות: בין 1974 ל־1980 ובין 1987 ל־1993. ראו:
Jim Howe, "Artificial Intelligence at Edinburgh University: a Perspective", 1994; Stuart J. Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach*, (2nd ed.), Upper Saddle River, New Jersey: Prentice Hall, 2003, p. 24.

68 באמצע העשור הראשון של שנות האלפיים השתנתה הגישה כלפי הבינה המלאכותית והתחילו לדבר על "אביב" בתחום זה. ראו לדוגמה:
John Markoff, "Behind Artificial Intelligence, a Squadron of Bright Real People", *The New York Times*, October 14, 2005.

69 Zagare, *The Dynamics of Deterrence*, pp. 48-56.

70 Axelrod, *The Evolution of Cooperation*, p. 13 (דיון על "צל העתיד").

71 Goldstein, "Cyber Weapons and International Stability".

72 Zagare, Kilgour, *Perfect Deterrence*, pp. 293-296.

קול קורא להגשת מאמרים

כתב העת "צבא ואסטרטגיה" הינו כתב עת שפיט היוצא לאור שלוש פעמים בשנה בעברית ובאנגלית. עורך כתב העת הינו ד"ר גבי סיבוני העומד בראש תכנית צבא ואסטרטגיה ותכנית לוחמת סייבר במכון למחקרי בטחון לאומי.

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

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

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

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

להגשת הצעות ולפרטים נוספים ניתן לפנות אל:
דניאל כהן
מתאם כתב העת "צבא ואסטרטגיה"
danielc@inss.org.il