

סייבר, מודיעין וביטחון

כרך 1 | גיליון 2 | יוני 2017

אכיפת גבולות או חציית גבולות בסייבר: דילמת הריבונות

אלסנדרו גוארינו ואמיליו אזיילו

ארבעה עקרונות ועוד אחד: מודל חדש להגנת סייבר

מת'יו כהן, צ'אק פרייליך, גבי סיבוני

תגובה מידתית למתקפות סייבר

ז'רנו לימנל

התכסית האנושית ומודיעין תרבותי במבחן המלחמות העכשוויות

קובי מיכאל ועומר דוסטרי

"גישה שיתופית" ביחסי מודיעין-קברניט ברמה הלאומית: האם יש לה

תוחלת?

דודי סימן טוב ושי הרשקוביץ

ישראל והודו: הערכה השוואתית של האסטרטגיה הצבאית למאבק בטרור

וינאי קאורה

להבין את איום הסייבר בעזרת האנלוגיה של "טרור בליסטי"

דוד שטרנברג

INSS

המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES



אוניברסיטת תל אביב
TEL AVIV UNIVERSITY

סייבר, מודיעין וביטחון

כרך 1 | גיליון 2 | יוני 2017

תוכן

אכיפת גבולות או חציית גבולות בסייבר: דילמת הריבונות
אלסנדרו גוארינו ואמיליו אזיילו | 3

ארבעה עקרונות ועוד אחד: מודל חדש להגנת סייבר
מת'יו כהן, צ'אק פרייליך, גבי סיבוני | 19

תגובה מידתית למתקפות סייבר
ז'רנו לימנל | 35

התכסית האנושית ומודיעין תרבותי במבחן המלחמות העכשוויות
קובי מיכאל ועומר דוסטרי | 51

"גישה שיתופית" ביחסי מודיעין-קברניט ברמה הלאומית: האם יש לה תוחלת?
דודי סימן טוב ושי הרשקוביץ | 77

ישראל והודו: הערכה השוואתית של האסטרטגיה הצבאית למאבק בטרור
וינאי קאורה | 95

להבין את איום הסייבר בעזרת האנלוגיה של "שרור בליסטי"
דוד שטרנברג | 113

סייבר, מודיעין וביטחון

כתב העת **סייבר, מודיעין וביטחון** מיועד להעשיר, להפרות ולהעמיק את השיח הציבורי באשר לנושאים רלוונטיים. המאמרים המופיעים בכתב עת זה, הרואה אור שלוש פעמים בשנה, נכתבים על ידי חוקרי המרכז ואורחיו והדעות המובעות בהם הן של המחברים לבדם.

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

עורך ראשי: אלוף (מיל.) עמוס ידלין
עורך: ד"ר גבי סיבוני
מתאמת כתב העת: הדס קליין
עוזר מתאם: גל פרל פינקל

ועדה מייעצת:

סונג'י ג'ושי / מרכז אובזרבטור למחקר, הודו	סונג'י ג'ושי / מרכז אובזרבטור למחקר, הודו
פטר ויגו ג'קובסון / הקולג' הדני המלכותי להגנה, דנמרק	פטר ויגו ג'קובסון / הקולג' הדני המלכותי להגנה, דנמרק
רוס דיאמינס / אוניברסיטת טורקוואטו די שלה, ארגנטינה	רוס דיאמינס / אוניברסיטת טורקוואטו די שלה, ארגנטינה
ג'יימס ג'. ווירץ / בית הספר הימי ללימודים מתקדמים, ארצות הברית	ג'יימס ג'. ווירץ / בית הספר הימי ללימודים מתקדמים, ארצות הברית
ריקרדו ישראל זיפר / האוניברסיטה האוטונומית של צ'ילה, צ'ילה	ריקרדו ישראל זיפר / האוניברסיטה האוטונומית של צ'ילה, צ'ילה
דניאל זירקר / אוניברסיטת וואיקאטו, ניו זילנד	דניאל זירקר / אוניברסיטת וואיקאטו, ניו זילנד
ג'פרי ג'. לארסן / תאגיד יישומי מדע בינלאומי SAIC, ארצות הברית	ג'פרי ג'. לארסן / תאגיד יישומי מדע בינלאומי SAIC, ארצות הברית
ג'יימס לואיס / המרכז למחקר ללימודים אסטרטגיים CSIS, ארצות הברית	ג'יימס לואיס / המרכז למחקר ללימודים אסטרטגיים CSIS, ארצות הברית
ג'ון נומיקוס / מרכז המחקר ללימודים אירופאים ואמריקניים, יוון	ג'ון נומיקוס / מרכז המחקר ללימודים אירופאים ואמריקניים, יוון

תיאודור ניטלינג / אוניברסיטת המדינה החופשית, דרום אפריקה
גלן מ. סגל / סקורישטס ויגילאטא, אירלנד
פרנק ג'. סילופו / אוניברסיטת ג'ורג' וושינגטון, ארצות הברית
סטפן ג'. סימבלה / אוניברסיטת פן שטייט, ארצות הברית
ט.ו. פאול / אוניברסיטת מקגיל, קנדה
מריה רחל פרייר / אוניברסיטת קווימברה, פורטוגל
מרים דאן קאוולטי / המכון הפדרלי השוויצרי לשכנוע, ציריך, שווייץ
אפרים קארש / קינגס קולג', לונדון, בריטניה
קאי מיכאל קנצל / האוניברסיטה האפיפיורית הקתולית של ריו דה ז'נרו, בразיל
ברונו תרשרס / קרן למחקר אסטרטגי, צרפת

עיצוב גרפי: מיכל סמוֹקובץ 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 סייבר, מודיעין וביטחון מוצגים באתר המכון: www.inss.org.il

© 2017 כל הזכויות שמורות
(מודפס) ISSN 2519-6677 • (מקוון) ISSN 2519-6685

אכיפת גבולות או חציית גבולות בסייבר: דילמת הריבונות

אלסנדרו גוארינו ואמיליו אזיילו

התפיסה לגבי מרחב הסייבר התפתחה בהדרגה, מהגישות הליברטניות של שנות התשעים של המאה העשרים ועד המצב הנוכחי, שבו מדינות לאום מבקשות לבסס מחדש את ריבונותן במרחב זה. המאמר בוחן את התפתחות התפיסות לגבי מרחב הסייבר – מהתפיסות האוטופיות שהגיעו לשיאן במה שכוונה "הצהרת העצמאות של מרחב הסייבר", ועד לשימת הדגש על הממד הטכנולוגי ומהלכי החקיקה שממשלות נוקטות כיום כדי להגביר את השליטה על מרחב זה. המאמר מתייחס למאמצים שנעשים במערב ובמזרח כאחד לפתור את האתגרים המגוונים, מרובי ההיבטים והמתמסכים שמציב הסייבר. מאמצים אלה נעים מתמיכה במרחב סייבר פתוח ועד לרצון לנשר מקרוב את האיום הגלום בו ואת השחקנים המדינתיים והלא מדינתיים השונים הפועלים במסגרתו. המאמר מתמקד בקשיים הרגולטוריים והטכניים הכרוכים בקביעת גבולות למרחב הסייבר, לרבות ההשלכות שיש לכך על נושאי מדיניות, ומסביר כיצד שחקני סייבר חוצים גבולות באמצעות שימוש בטכניקות שונות, כגון קריפטוגרפיה ו"מקלטי נתונים". המסקנה העיקרית של המאמר היא ש"הבלקניזציה" של מרחב הסייבר אינה רק מציאות קיימת, אלא גם תהליך שקשה לראות כיצד הוא ישנה את כיוונו. הדבר מעלה את השאלה כיצד חברות פתוחות יכולות לאזן בין ריבונות ובין חופש הפרט במרחב הסייבר. ההצעה המועלית במאמר מסתמכת על דוגמאות שבהן הריבונות של מדינות הלאום הינה מוגבלת, והגבולות אינם רלוונטיים, כמו מערכת החוקים הבין-לאומית המסדירה את סוגיית המשאבים הגלובליים.

מילות מפתח: אבטחת סייבר, משילות באינטרנט, יחסים בין-לאומיים, לוחמת סייבר, עימות סייבר, סין, פרשיות

אלסנדרו גוארינו הוא יועץ אסטרטגי בחברת "StudioAG", חברת אבטחת מידע ואבטחת סייבר איטלקית. אמיליו אזיילו הוא מנתח מודיעין סייבר אסטרטגי, המיעץ לארגוני מודיעין צבאיים ואזרחיים של ממשלת ארצות הברית, כמו גם לחברות במגזר הפרטי המספקות מודיעין סייבר.

מבוא

ההתפשטות הכלל-עולמית של תשתית ייחודית להעברת מידע דיגיטלי במהלך העשור האחרון של המאה העשרים, הביאה לשינוי עמוק בכול היבט של החיים והחברה – מאינטראקציות חברתיות ועד לכלכלה הגלובלית. זמינות הגישה לאינטרנט נחשבת כזכות כמעט מובנת מאליה, לפחות במדינות המפותחות. אולם מרחב הסייבר אינו תופעה טבעית, אלא תופעה היסטורית ופוליטית, וככזו הוא נתון להשפעות של ישויות פוליטיות וחברתיות. מבין הישויות הפוליטיות השונות, חשיבות עליונה יש למדינות הלאום.

ממשלת ארצות הברית הייתה גורם מרכזי בפיתוח האינטרנט, מאז תחילתו כפרויקט מחקר בסוכנות לפרויקטים מתקדמים של משרד ההגנה האמריקאי (DARPA). הקהילה הבין-לאומית וחלק מהארגונים העל-לאומיים מגלים עניין בסוגיית הרגולציה והשימוש שנעשה באינטרנט. לאחרונה הכריז נאט"ו על מרחב הסייבר כמרחב לחימה אוטונומי. נאט"ו עשה זאת משיקולים פוליטיים ואסטרטגיים, תוך שהוא מאמץ עמדה שאינה בהכרח משותפת לכלל החוקרים את נושא הסייבר. מאז שהאינטרנט נפתח לשימושם של גופים מסחריים בשנות התשעים של המאה העשרים, רכשו לעצמם גורמים מהמגזר הפרטי (ממפעילי רשתות ועד ספקי שירות) מעמד בולט בוויכוח על הרגולציה שלו ועל השאלה האם מרחב סייבר חסר גבולות מציע יתרונות לחברות האינטרנט אך גם מציב אותן בהכרח על מסלול התנגשות עם מדינות ריבוניות? מצדו השני של הרצף נמצאים האזרחים הפשוטים (כגון מפעילים, יצרני תוכן, תושבים, מומחים, עיתונאים וכול משתמש שהוא), המבקשים לגבש תפיסה משלהם לגבי מרחב הסייבר כיום, ובכלל זה האם וכיצד יהיה נתון לשליטה ופיקוח בעתיד.

רקע היסטורי

לא ניתן להבין כהלכה את מרחב הסייבר מבלי להכיר היטב את הרקע ההיסטורי שלו. אין זה מפתיע שההיסטוריה הסייבר היא בעלת עשורים ספורים בלבד. הקצב המהיר של השינויים וההתפתחויות בעולם הסייבר הופך את המבט לאחור לא רק לאפשרי אלא גם לחיוני, במיוחד אם רוצים לבסס את הדיון בסייבר על קרקע יציבה. ההתפשטות הפתאומית והמהירה של האינטרנט הייתה תוצאה של שורת גורמים טכניים ופוליטיים שהתכנסו יחדיו. סביר להניח שאף אחד מהשחקנים המעורבים לא השכיל לצפות את העתיד להתרחש ולא העריך עד כמה מהפכנית תהיה המצאת האינטרנט. בתוך פרק זמן קצר הוא הפך מרשת צבאית ואקדמית בעיקרה, המחברת בין כמה עשרות אתרים ושימושית רק דרך ממשקים של שורות פקודה, למשאב כלל-עולמי הנגיש למיליוני בני אדם, המשתמשים בממשק "הצבע ולחץ" של דפדפן הרשת.

הטלקומוניקציה הקולית של שנות השבעים והשמונים של המאה העשרים שיקפה עולם אחר לחלוטין מאשר עולם רשתות הנתונים, המעבֵר חילופי נתונים ומסרים של מחשב למחשב. חברות הטלקומוניקציה (טלקום) שפעלו בשוק נהנו ממעמד דומיננטי, מונופוליסטי או כמעט מונופוליסטי, ומתזרים מזומנים שהתלווה לכך. אולם בארצות הברית, שבה קיימת מסורת חקיקה בתחום ההגבלים העסקיים עוד מהמאה ה־19, התרחש תהליך מתמשך של דה־רגולציה ועידוד התחרות, שכלל שבירת מונופולים וחברות. חברת AT&T היא דוגמה בולטת לכך. ההשפעה הישירה של תהליך זה הייתה דחיפה לחדשנות בתחום התשתיות.

הליברליזציה של שוק הטלקומוניקציה אפשרה במידה מסוימת לארצות הברית להרחיב את השפעתה גם לשאר העולם המפותח. מהלך מדיני חשוב נוסף הייתה ההחלטה של רשות התקשורת האמריקאית הפדרלית (FCC) לסווג מחדש "עיבוד נתונים" – קרי, תקשורת דיגיטלית בין מחשב למחשב – כשירות המעניק "ערך מוסף", וזאת בניגוד לשירותי הקול הבסיסיים.¹ התוצאה הייתה יצירת שוק פתוח ולא מפוקח של שירותים דיגיטליים, שנעדרו אפילו את מחסומי הסחר המקובלים.² שירותי מידע היו בעבר חלק זעיר מהכנסותיהן של חברות הטלקומוניקציה, דבר שהביא לכך ששוק זה נשאר גם עתה ללא פיקוח. סביר להניח שהדבר נבע, כאמור, מהעובדה ששירותי המידע נחשבו לתחום שההכנסות ממנו היו קטנות בהשוואה להכנסות משירותי הקול. בכול מקרה, מדיניות זו סללה את הדרך לרשת מידע דיגיטלית כלל עולמית.

לצד המדיניות הכללית, היו גם כמה היבטים טכניים שתרמו להתרחבות האינטרנט, ובכלל זה לאופן שבו תקשורת הנתונים מנוהלת ברשת. האינטרנט התבסס על טכנולוגיית מיתוג־מנות (packet-switching), המאפשרת לשני צמתים להחליף ביניהם מידע מבלי ליצור נתיב קבוע או אפילו ידוע מראש ביניהם. הנתונים מחולקים ל"מנות" קטנות המשודרות בנפרד, יתכן בנתיבים שונים ואף בסדר שונה מהמקורי. השלם נבנה מחדש ביעד על ידי תוכנת הרשת. תהליך זה היה שונה לחלוטין מטכנולוגיית "מיתוג המעגלים" של רשתות הטלפוניה, שבה מוגדר מעגל (או נתיב) ייעודי בכול פעם שנוצרת תקשורת בין שני צמתים. ארכיטקטורת מיתוג־מנות אפשרה ניהול מבוזר, משום שאת החלטות הניתוב בנוגע למנות הנתונים ניתן היה לעשות ברמה המקומית, ללא צורך במידע מפורט ברשת. לכך הצטרפה העובדה שפרוטוקולי התקשורת הספציפיים ששימשו באותו זמן (TCP/IP) היו סטנדרטיים וציבוריים – החלטה הנדסית שהתקבלה עשרות שנים קודם לצמיחה המהירה של האינטרנט ואפשרה הוספה של רשתות קיימות. למעשה, עד אז פירוש

1 Milton L. Mueller, *Network and States* (Cambridge: MIT Press, 2010).

2 שם.

המילה "אינטרנט" היה מילולי: חיבור בין־רשתי של שתי רשתות מחשבים או יותר (רק מאוחר יותר היא קיבלה את ה' היידוע והפכה להיות "האינטרנט"). תרומה טכנולוגית נוספת הייתה הבשלתה של תנועת התוכנה החופשית שאפשרה, בין היתר מסיבות כלכליות, את זמינותם של מרכיבים שסייעו להקמת מספר רב של חברות אינטרנט ושרתים. GNU/Linux ושרת הווב Apache הם שתי דוגמאות בולטות לכך. אין להמעיט גם בערך כניסתן של טכנולוגיות ה־xDSL, שהביאו לציבור חיבורי פס רחב יחסית.

מתח המשילות

הוויכוח בנושא הפיקוח על מרחב הסייבר נחלק לשתי עמדות מנוגדות. מצד אחד ניצבת ההשקפה הטוענת שמרחב זה הוא מעין ישות נפרדת לחלוטין מהעולם ה"פיזי", ישות שבה המידע זורם בחופשיות ואין חוק המחייב אותה. העמדה המנוגדת גורסת שכול מדינה אחראית לחלקה הריבוני באינטרנט הגלובלי ורשאית ליישם כל מנגנון משפטי כדי להבטיח את ביטחון הפעילות המקוונת החוצה את מרחבי הרשת שלה. עד היום לא הושגו הסכמה או פשרה לגבי עמדות מנוגדות אלו, והסטטוס קוו נותר על כנו, אם כי שאלת המשילות באינטרנט ממשיכה לעורר ויכוח עז.

על פי ההשקפה שלפיה מרחב הסייבר הוא ישות נפרדת מהעולם הפיזי, מדינות לאום אינן רוצות ואינן יכולות לפקח על כל המתרחש באינטרנט. פירוש הדבר הוא שמרחב הסייבר אינו כפוף לדיון, לריבונות או לגבולות "הרגילים". גישה זו זכתה לניסוח מוצלח אצל ג'ון פרי בארלו (Barlow), לפיו: "ממשלות העולם המתועש, אתן הענקיות היגעות [...], באתי ממרחב הסייבר, משכנה החדש של הַפִּינָה [...], מקום שבו אין לכן כל ריבונות"³. כתמיכה באמירה זו ניתן להוסיף כי התכונות הטכניות של האינטרנט – ביזור (הודות לפרוטוקולים של IP) וטבעו המתנייד בקלות של המידע – הן שמעניקות למערכת את עצמאותה מהעולם הפיזי ומהריבונות של מדינות הלאום. התשתית מאפשרת לידה וצמיחה של ארגוני רשת, המורכבים מחברי קבוצה ומקשרים בלתי תלויים לחלוטין במיקומים פיזיים, בסמכויות שיפוט או בגבולות. הארגון הפנימי של חברי הקבוצה בתוך אותם מבנים חברתיים – בין אם מדובר בארגוני חברה אזרחית, במועדונים המשקפים אינטרסים מיוחדים או ברשתות חברתיות – תלוי אך ורק בזרימת המידע.

עקרון היסוד של מה שניתן לכנות "ליברטיניות הסייבר" הוא שאין צורך בפיקוח ריבוני ובחוקים במרחב הקיברנטי. אלא שלמרבה הצער, עוצמתם של ארגונים

3 John Perry Barlow, "A Declaration of the Independence of Cyberspace", in *Crypto Anarchy, Cyberstates and Pirate Utopias*, ed. Peter Ludlow (Cambridge: MIT Press, 2001).

מרושתים יכולה לשמש גם להקמת ארגוני טרור ופשיעה, המנצלים את האנונימיות היחסית שהסייבר מאפשר. טבעם העל-לאומי של ארגונים אלה מאפשר לחבריהם לתפקד בצורה מלוכדת, למרות שהם פועלים במיקומים גיאוגרפיים נפרדים ותחת סמכויות שיפוט שונות.

ההשקפה השנייה נוגעת לריבונות המדינה במרחב הסייבר. השקפה זו גורסת כי לא רק שהרכיבים הטכנולוגיים של האינטרנט צריכים להיות כפופים לסמכות המדינה, אלא שגם המידע שנוצר, שנכנס אל המרחב הדיגיטלי הריבוני שלה או שחוצה אותו חייב להיות כפוף לה. הפוטנציאל ליצירה ולקיום של רשתות חברתיות על-לאומיות בקלות, בגמישות ובאופן אנונימי יחסית, נתפס כאיום הן על ריבונות המדינה והן על הביטחון הלאומי שלה.

תפיסה זו הלכה והתבססה מאז תחילת המאה ה-21, במיוחד נוכח העימות המתמשך עם רשתות הטרור המאורגן. אולם הטרור שפגע באירופה ובארצות הברית אינו המניע היחיד הניצב מאחורי העמדה הדוגלת בריבונות המדינה במרחב הסייבר. התנועות החברתיות שהובילו ל"מהפכות הצבעים" ול"אביב הערבי" הן אות לעשוי לקרות אם מידע ימשיך לזרום ללא פיקוח. יתרה מכך, למדינות לאום יש נטייה טבעית לשמר ולהרחיב את גבולות כוחן. הפוטנציאל של מרחב הסייבר כערוץ לתקשורת וללחימה הופך אותו, לפיכך, לשלוחה טבעית של עוצמת המדינה. ואכן, השליטה על תנועות פיננסיות, ואפילו מדיניות מטבע, הן מאפיינים של ריבונות הנמצאת תחת מתקפה.

מתנגדי תפיסת הריבונות רואים בה כלי המשמש משטרים אוטוריטריים כדי לתת תוקף חוקי לפיקוח ולשליטה על אזרחיהם. ואכן, מתנגדים ואופוזיציה פוליטית הפכו פעמים רבות ליעד למעקב פנימי צמוד, והאיום הקיומי של הטרור, כפי שהוא נתפס על ידי המערב, הפך למהות הקיום של המדינה המפקחת. זאת ועוד, מדינות אוטוקרטיות ופחות דמוקרטיות אינן נזקקות אפילו לנימוק זה כדי לקבוע את גבולות המותר והאסור.

המתח בין שתי ההשקפות השפיע על הוויכוח בנוגע ל"משילות באינטרנט" בשנות התשעים של המאה העשרים, ובמיוחד מאז תחילת המאה ה-21. מתח זה הוביל לשני מודלים של משילות: לפי המודל האחד, מרחב הסייבר נתפס כמשטר בין-לאומי נוסף שיש להסדירו באמצעות אמנות וארגונים בין-מדינתיים (איגוד הטלקומוניקציה הבין-לאומי – ITU – הוא דוגמה בולטת לכך). לפי המודל השני, יש לפעול למען יצירת רשת משילות (המונח הנוכחי של האיחוד האירופי לכך הוא "ריבוי בעלי עניין"). רשת משילות, שתוקם על ידי גורמים ממשלתיים ולא ממשלתיים גם יחד, נתפסת על ידי רבים כמודל המתאים ביותר לאינטרנט, והיא למעשה הדרך שמרחב הסייבר פועל לפיה כיום.⁴ החזון של מרחב הסייבר כמשאב

כלל עולמי הוא אטרקטיבי אך מטעה: הסייבר הינו תחום מלאכותי לחלוטין, ואין בו אף חלק שמתקיים מחוץ לריבונות כלשהי (אפילו כבלים תתי־מיים הם חלק ממערך שלם של רגולציות ואמנות, שמקורו עוד במאה ה־19).⁵

המתח בין שתי ההשקפות מודגש ביתר שאת נוכח העובדה שמודל של משילות רשתית כבר היה קיים כאשר מדינות החלו להבין את פוטנציאל מרחב הסייבר ולבסס מחדש את ריבונותן המסורתית. תאגיד האינטרנט להקצאת שמות ומספרים (ICANN) והניהול המבוזר של מערכת שמות המתחמים (DNS) הם דוגמאות מובהקות לכך. משילות מבוזרת הפכה את האינטרנט להצלחה הגדולה שהוא מהווה, וקשה לטעון לפיכך את ההיפך.

ההתפתחות האחרונה

מדינות לאום החלו להשיג שליטה על מרחב הסייבר מאז תחילת המאה ה־21. התפתחות זו התפשטה גם אל מחוץ למדינות המערב, שבהן האינטרנט ומרחב הסייבר נתפסים כנשלטים על ידי "הגמוניית הסייבר" של ארצות הברית. אף שההתנגדות ל"הגמוניית הסייבר" משמשת ככלי תעמולה בידי סין, הדבר לא מנע מארצות הברית ומבעלות בריתה הקרובות, ובמיוחד מסוכנויות הביטחון שלהן, מלהחזיק בגישה "ניאו קולוניאליסטית" מסוימת ביחס למרחב הסייבר. דוגמאות בולטות לכך הן פיתוח ופריסה של נשק סייבר, כמו תולעת "סטקסנט" והשפעתה; המתקפה של המודיעין הבריטי על חברת הטלקום הבלגית Belgacom; התביעה לתת תוקף כלל עולמי לדין האמריקאי בתחום הסייבר תוך התעלמות מסמכויות שיפוט אחרות; וצו בית המשפט שחייב את חברת "מייקרוסופט" לשחרר נתונים שאוחסנו באחד ממרכזי הנתונים שלה באירלנד.

כאשר בוחנים את הסוגיה מנקודת מבט זו, הפרקטיקות שנוקטות מדינות דמוקרטיות וליברליות אינן שונות בהרבה מאלו של המדינות הפחות דמוקרטיות. יתרה מכך, פרקטיקות אלו אף סותרות לעתים האחת את השנייה. לדוגמה, הניסיונות ליצור "שוק דיגיטלי יחיד" ללא גבולות בתוך האיחוד האירופי הולכים יד ביד עם יצירה ואכיפה של גבולות חיצוניים שנועדו למנוע הצפה אמיתית או מדומה מצד חברות שמחוץ לאיחוד האירופי, למשל לצורך התחמקות מתשלום מס.

אכיפת גבולות

את המדיניות והפעולות שנוקטות מדינות במטרה לבסס ולאכוף גבולות למרחב הסייבר ניתן לסווג באמצעות בחינת שני משתנים: המשתנה הראשון מתייחס לשאלה האם הפעולה היא "גלויה" או "סמויה" (covert/overt). השימוש במונח

Alessandro Guarino, "Cyberspace Does Not Exist", *Strange Loops*, January 15, 2015, <http://www.studioag.pro/en/2015/01/la-nuvola-non-esiste/>.

"סמוי" בהקשר זה הוא חופשי למדי וכולל שילוב של שתי המשמעויות – סמוי וסודי – כאשר סמוי, בניגוד לסודי, פירושו הסתרת המקור. המשתנה השני קשור לשאלה האם לכללי המדיניות יש אופי טכני או לא, ובמילים אחרות, האם הם טכניים או משפטיים/פוליטיים באופיים.

מדיניות של מאמצים לא טכניים גלויים תהיה ניסיון להחזיר את משילות האינטרנט לחיקה של המדינה, ישירות או באמצעות ארגונים בין-ממשלתיים. פעולות גלויות אחרות הן כאלו שנגזרות מטבעו הפיזי של מרחב הסייבר. כל התקני הרשת (שרתים, נתבים, תשתית הכבלים, תחנות לוויין) ממקמים בטריטוריה ריבונית של מדינת לאום וכפופים לחוקיה (או לדין הבין-לאומי במקרה של כבלים תתימיים חוצי אוקיינוס). אמנם, קשה לנטר ולשלוט בזרימת הנתונים, אך ניתן ליצור ולאכוף חוקים ותקנות להיבט הפיזי של "הענף".

פעולה פוליטית גלויה יכולה גם לאפשר פעולה טכנית גלויה, כשזו מגובה בהנמקה משפטית (לפחות כלפי המדינה הנוגעת בדבר). "חומת האש הגדולה" של סין היא דוגמה מצוינת לכך. החלטות מדיניות יצרו ארסנל שלם של אמצעים טכניים שנועדו לבסס מחדש את ריבונותה של סין על חלקה "הלאומי" במרחב הסייבר. מדובר באמצעים הנעים מביקורת וסינון מעמיקים של חבילות נתונים בנתבים ההיקפיים, דרך חסימה והחרמה של אתרי אינטרנט, ועד מניפולציה של ה-DNS בתוך סין – ואלו רק חלק מהדוגמאות. במילים אחרות, קל להשיג שליטה ברמה הפיזית, אולם קשה לעשות זאת ברמה גבוהה יותר, כמו עם פרוטוקול TCP/IP ועם ניתוב. בניגוד לכבל פיזי, טכנולוגיית מיתוג-מנות מקשה על השליטה בנתיב שהיא עוברת (למשל, אילו טריטוריות לאומיות היא חוצה).

הצד הסמוי של סיווג מטריציוני אידיאלי יכול ללול את הרמה הטכנית, שבה מדינות שונות נמצאות במרוץ למיליטריזציה של הרשתות הגלובליות, וזאת מתוך רצון להשיג את היתרון הווירטואלי שיאפשר להן לגנוב מידע בשיטה הקלאסית של ריגול ולהיות מוכנות ללוחמת סייבר עתידית. היערכות כזאת פירושה גם יכולת להגן על רשתות קריטיות של המדינה מפני חדירות. דוגמאות לאמצעים לא טכניים סמויים הן ניטור תוכן ברשתות חברתיות ואחרות, אותו מבצעות סוכנויות ביטחון ומודיעין. באופן כללי ניתן לומר כי ממשלות המחליטות על מדיניות סמויה, מאפשרות לסוכנויות הביטחון הפנימיות שלהן שליטה על זרימת המידע. דוגמה רלוונטית אחרת לאמצעים לא טכניים סמויים היא "שכנוע מוסרי" שמפעילות ממשלות על ספקי שירותי אינטרנט (ISP) ושאר מפעילי רשת, וזאת כדי להבטיח את שיתוף הפעולה שלהם לצורך שליטה על זרימת המידע (לדוגמה, באמצעות התקנת ציוד יירוט ממשלתי אצלם).⁶

חציית גבולות

ניתן לציין כמה מניעים לרצונן של מדינות להותיר את מרחב הסייבר ללא חסימות והפרעות, או לרצונן להגביל אותו באמצעות הגברת השליטה, הפיקוח והמעקב. באופן טבעי, מדינות עשויות לרצות לחצות גבולות כדי לקדם מסחר ותקשורת, או מנגד, כדי לגנוב סודות ולשבש מערכות. הסביבה החוקית (או היעדרה) היא אחת הדרכים המרכזיות של מדינה לשמר את הסטטוס קוו.

מדינות פועלות כיום במטרה להגדיר התנהגות מקובלת במרחב הסייבר. לדוגמה, בסיום מפגש G-20 שנערך ב־2015, הצהירו נציגים בכירים של המדינות החברות על התחייבות להימנע מריגול כלכלי בסייבר לצורך קידום אינטרסים מסחריים.⁷ למרות הכרזות חגיגיות אלו, ריגול בסייבר נותר אמצעי אטרקטיבי לגניבת מידע ולמעקב אחר יידיים ואויבים כאחד. סביר להניח שהתחייבות חברות ה־G-20 תביא לכך שמדינות יקפידו לערפל את פעילויותיהן בתחום הסייבר יותר משיחדלו מהן לחלוטין.

מכיוון שממשלות מבקשות לחזק את קשריהן הכלכליים האחת עם השנייה תוך שימוש בסייבר כאמצעי מסייע, גבולות הסייבר שמדינות כמו סין ורוסיה מעוניינות לחזק, הופכים קשים יותר ויותר להגדרה. מצב זה מותיר את המדינות בעמדה לא פשוטה, לפיה כל אחת מנסה להגן על חלקה באינטרנט, ובמקביל מנסה להרחיב את קשריה המדיניים והכלכליים עם שותפותיה הגלובליות.

טכנולוגיות מסייעות לחציית גבולות

אין הגדרה גלובלית מוסכמת למרחב הסייבר. משרד ההגנה של ארצות הברית מגדיר מרחב סייבר כ"תחום המאופיין בשימוש באמצעים אלקטרוניים ובספקטרום האלקטרומגנטי כדי לאחסן, לשנות ולהחליף נתונים דרך מערכות רשת ותשתיות פיזיות משויכות".⁸ כלומר, המינוח האמריקאי מתמקד בארכיטקטורת הרשת ובתהליכים המתרחשים במרחב הדיגיטלי. לעומת זאת, רוסיה מעדיפה להשתמש במונח "מרחב מידע", אותו היא מגדירה כ"ספרת הפעילות הקשורה לתצורה, יצירה, המרה, העברה, שימוש ואחסון של מידע, ואשר יש לה השפעה על תודעה חברתית ופרטנית, על תשתית המידע ועל המידע עצמו".⁹ גם סין רואה את מרחב

Emilio Iasiello, "G20 – No Commercial Hacking by Anyone", *Dead Drop*, January 14, 2016, <http://deaddrop.threatpool.com/g20-no-commercial-hacking-by-anyone/>.

US Department of Defense, *Joint Terminology for Cyberspace Operations – Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands, and the Directors of the Joint Staff Directorates* (November 2010).

Keir Giles and William Hagestad, "Divided by a Common Language: Cyber Definitions in Chinese, Russian and English" (Tallinn: Fifth International Conference on Cyber Conflict, 2013).

המידע כישות הוליסטית. ההגדרה הסינית היא כדלקמן: "הפונקציה המרכזית של מרחב המידע היא רכישה ועיבוד של נתונים על ידי אנשים [...] מקום חדש לתקשר עם אנשים ופעילויות. זהו שילוב של כל רשתות התקשורת, מסדי הנתונים והמידע בעולם, המעצב 'סביבה' עצומת ממדים, מקושרת הדדית, בעלת מאפייני אינטראקציה אתניים וגזעיים מגוונים, במרחב שהוא תלת-ממדי"¹⁰.

למרות ההבדלים ביניהן, כל שלוש ההגדרות מתייחסות להיבטים הרשתיים של תחום הסייבר, שהוא מעשה ידי אדם. סביבה כה מורכבת תכלול בהכרח, בין יתר נקודות התורפה שלה, שגיאות אנוש. אלה שעזרו לעצב את הרשת במהלך השנים התמקדו באתגרים הטכניים של העברת מידע במהירות ובאמינות, ולא צפו כי משתמשי האינטרנט עצמם יעשו שימוש באותה רשת כדי לתקוף האחד את השני. מתקפות ושימוש לרעה אינם חייבים להיות משוכללים כדי להצליח, אך ככול שהגורמים התוקפים או העוינים מיומנים יותר, כך הם מפגינים יכולת ליצור כלים ייחודיים, לנצל נקודות תורפה ולהסב נזקים, תוך שהם מצליחים להישאר סמויים מן העין. להלן כמה טכניקות באמצעותן מצליחים גורמים כאלה לחצות גבולות סייבר של מדינת לאום:

- **הצפנה:** הגורמים הפועלים מנצלים את ההצפנה לצורך הסוואת הנתונים שקצרו והגנבתם אל מחוץ לארגון (Exfiltration). בחלק מהמקרים, הם מסתירים את המידע בקבצים תמימים למראה (סֶטְגֶּנוֹגרִפִּיה). טקטיקות אחרות כוללות דחיסה (הקטנת גודל הקבצים מבלי להסיר מידע); הקבצה (Chunking – פירוק הנתונים לחלקים קטנים כך שיתערבבו טוב יותר בתעבורה הרגילה); ערפול (Obfuscation – הסוואת מאפיינים לקוד הקסדצימלי כדי למנוע את זיהוי הנתונים). הצפנת הנתונים מאפשרת לגורמים הפועלים להקשות על הארגון הנפגע בחשיפת סוג המידע שנגנב, וכך הם מונעים את עצם הפתיחה בחקירה בעקבות גילוי הפריצה ואת שיקום הנזקים, לא כל שכן את המאמצים לגלות מי עומד מאחורי המעשה.

- **רשת TOR (The Onion Routing):** למרות שישנו ויכוח האם תוכנת TOR היא אנונימית לחלוטין, היא נותרה דרך פופולרית בידי הגורמים הפועלים לבצע את תוכניותיהם. כוחה של רשת TOR נשען על העובדה שתיאורטית לא ניתן לדעת איזה מחשב ביקש את התעבורה, שכן המחשב יכול להיות יוזם הקשר או רק הצומת שפועל כממסר לצומת TOR אחר. לקוח TOR בוחר נתיב אקראי דרך צומתי TOR עד שהוא מגיע ליעד הסופי. בהקשר זה, TOR הוא כלי פופולרי למשתמשים המבקשים לעקוף את מגבלות ובקורות הצנזורה במדינה מסוימת, ובאותה מידה הוא משמש גורמים עוינים. תקרית מ־2014 המחשה כיצד רשת

10 אמיליו אזיילו, "האם נשק סייבר משפיע על כלים צבאיים?", **צבא ואסטרטגיה**, כרך 7, גיליון 1, מארס 2015, עמ' 24–25.

TOR מונפה לפעילות של ניצול רשתות: צומת TOR זדוני שימש לשיגור מתקפות ריגול בסייבר נגד ממשלות אירופיות.

- **העברות נתיקות (Pluggable Transports):** העברות נתיקות מסוות תעבורת TOR כך שתיראה כמו תעבורה משירותים נפוצים אחרים, דוגמת HTTPS או "סקיפ", או כמו תעבורה רגילה באמצעות שינוי זרם התעבורה ב־TOR בין ה"לקוח" ובין ה"גשר".
- **רשתות וירטואליות פרטיות (VPN) ושרתי "פרוקסי":** רשתות VPN ושרתי "פרוקסי" מגנים על המשתמש באמצעות הצפנת כל הפעילות אל המחשב ומתוכו. כל עוד המחשב מחובר לרשת וירטואלית פרטית, למפעילי הרשת אין גישה לתעבורה (למשל, לאתרים שהמשתמש ביקר בהם). באופן דומה, שרתי "פרוקסי" משמשים כדי לתווך בין הלקוח ובין השרת, ומונעים את הצורך בתקשורת ישירה בין שני הצדדים. הם מספקים רמה מסוימת של אבטחה משופרת בהגנה על זהות המחשב דרכו מתבצעת הגלישה.

מצוקת דיפלומטיית הסייבר

"הסביבה הדיפלומטית" של מרחב הסייבר ממשיכה להיות דינמית – מצב המזמין פעילות עוינת. המבוי הסתום בתחומים קריטיים של מרחב הסייבר הותיר את הממד המשפטי שלו במצב של חוסר ודאות: מדינות ממשיכות לחצות גבולות קיימים מבלי שיהיו לכך השלכות משפטיות כלשהן ברמה הבינלאומית. במקביל הן נאבקות להגיע להסכמות על הגדרות וסוגיות מפתח משפטיות, כגון טרמינולוגיה לאבטחה וללוחמת סייבר, בעודן נמנעות מלקבל על עצמן אחריות מדינית. הדבר דומה לשאלת הריבונות בתחום הסייבר. כך, למשל, סין ממשיכה לקדם את ריבונותה במרחב הסייבר כשלוחה של ריבונותה הטבעית – זכות המוקנית לה מתוקף מגילת האו"ם. ארצות הברית, ובמידה מסוימת גם בעלות בריתה, מאמינות כי האינטרנט, בהיותו פלטפורמה גלובלית של קישוריות הדדית, חייב להישאר פתוח לכול (חשוב לציין שבעוד שזו עמדתה הרשמית של ארצות הברית, קיימות עמדות אחרות בתוך הממשל האמריקאי הנוגעות לאסטרטגיות הסייבר, שלעתים אף סותרות האחת את השנייה).

משילות באינטרנט היא זירה למחלוקת מרכזית נוספת. נכון להיום, אין ארגון יחיד המשפיע על האופן שבו האינטרנט אמור להתרחב, על הטכנולוגיות שישמשו בו או על הכללים שישלטו ברשת הגלובלית. סין ורוסיה מעדיפות ארגון ממשלתי בין-לאומי, דוגמת ITU (שהינו חלק ממערך האו"ם), שיפקח על כלל הפעילות באינטרנט וינהל אותה. הודו ישרה קו עם עמדה זו באפריל 2016. לפחות מבחינה רשמית, ארצות הברית מעדיפה גישה של ריבוי מעורבים, שתכלול לא רק ממשלות

אלא גם את המגזר הפרטי, האקדמיה, החברה האזרחית והקהילה הטכנולוגית.¹¹ הוויכוח בין שתי העמדות חשוב, והצדדים ממשיכים לנסות ולגייס בעלי ברית לקידום עמדותיהם.

תחום משפטי שלישי שנותר לא מוגדר נוגע לשאלה מהו "נשק מידע". סין ורוסיה הציעו ב־2011 לאסור את השימוש בכול "נשק מידע" וטכנולוגיות הקשורות בו, ועשו זאת בנוסח ההצעה הראשונית לקוד האתי שהובא בפני העצרת הכללית של האו"ם. הגרסה החדשה של הקוד, משנת 2015, השמיטה איסור זה נוכח החשש שהכללתו עלולה להתפרש כרמז לכך ששימוש במידע עשוי לעודד אייציבות אזרחית, כפי שאכן קרה במהלך "האביב הערבי".

עמדתה המסורתית של ארצות הברית היא התנגדות להוצאת נשק סייבר התקפי אל מחוץ לחוק. הגורם במחלקת המדינה של ארצות הברית האחראי לנושא הסייבר סבור שאמנות צבאיות או דיפלומטיות קונבנציונליות אינן מתאימות למרחב הסייבר, ובמקום זאת מעדיף פיתוחן של "נורמות".¹² גישה זו מתנגשת עם תוצאותיו של מחקר שערכו מומחים משפטיים בהזמנת "מרכז המצוינות המשותף להגנת סייבר של נאט"ו".¹³

מציאת בסיס משפטי משותף היא משימה קשה להשגה אפילו בקרב מדינות "ידידותיות". כך, למשל, ישנם הבדלים מהותיים בין ארצות הברית ובין האיחוד האירופי בגישות המשפטיות כלפי מושג הפרטיות, דבר שהוביל לביטול הסכם "נמל מבטחים" (Safe Harbor) להעברת נתונים בין שני הצדדים. גם הסכם המסגרת החדש – "מגן פרטיות" (Privacy Shield) – נראה כבנוי על בסיס רעוע.

סביבה פוליטית

סביבות פוליטיות תורמות גם הן להתחמקות של מדינות מקביעת גבולות. ממשלות מסוימות יוצרות סביבה מתירנית המאפשרת לפעילויות מסחריות, פליליות או לכול פעילות עבריינית אחרת לעבור דרך המרחב שלהן. הדבר קורה בין אם ממשלות אלו מונעות במכוון חקיקה פנימית ובין אם הן בוחרות באכיפה סלקטיבית של החוק. סביבות פוליטיות אלו אינן תוצאה ישירה של משטרים או של שיטות ממשל מסוימות, אלא בעיקר של אינטרסים של ממשלות המאפשרות את קיומן של פעילויות אלו.

US Department of State Fact Sheet, "Internet Governance", August 2015, <https://www.state.gov/documents/organization/255010.pdf>. 11

Kenneth Corbin, "State Department Argues Against Cyber Arms Treaty", *CIO*, May 26, 2016, <http://www.cio.com/article/3075442/government/state-department-argues-against-cyber-arms-treaty.html>. 12

Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013). 13

לשם דוגמה, הסביבה הפוליטית ברוסיה מפגינה סובלנות כלפי פושעי סייבר ופצחנים (האקרים) לאומניים. על פי ארגון "עיתונאים ללא גבולות", רוסיה מנהלת מערך של מעקב ופיקוח הדוקים בשם SORM, כאשר SORM-1 מתמקד בירות תקשורת טלפונית, SORM-2 מתמקד בנתונים המועברים דרך האינטרנט, ואילו SORM-3 יודע ליירט כל סוג של תקשורת וכולל אחסון לטווח ארוך. ישנה ברוסיה גם אכיפה קבועה של צנזורה.¹⁴ כאשר מדובר במרחב הסייבר, דומה שפושעי הסייבר הרבים ברוסיה פועלים על פי שני כללים בסיסיים: רוסים לא פורצים לרוסים; אם המודיעין הרוסי מבקש עזרה, הם נענים.

הפצחנים הרוסים זכו לתשומת לב מאז מתקפות DDoS נגד אסטוניה ב־2007 ומעורבותם בעימות בגיאורגיה ב־2008. פצחנים לאומנים רוסים היו מעורבים במהלך תקריות אלו במתקפות סייבר בשם ההגנה על התרבות והלאומנות הרוסיות, כאשר חלק מהמתקפות הגיעו מהמרחב האינטרנטי הרוסי או חצו אותו. לאחרונה התרחשה פעילות דומה באוקראינה, שם מתנהל עימות בין אוקראינים לבדלנים רוסים, והמתקפות המקוונות מתקיימות ברמת תכיפות גבוהה.

שלא כמו רוסיה, הסביבה הפוליטית בארצות הברית אינה תומכת ואינה מגלה סלחנות כלפי פעילויות של גורמים לאומנים העוסקים בפיצוח בשם מה שהם קוראים אינטרסים אמריקאיים. עם זאת, העובדה שפצחן אמריקאי בשם "The Jester" מבצע מתקפות נגד טרוריסטים ושאר פעילויות "אקטיביסטיות", מבלי שייחקר או ייעצר על ידי רשויות החוק, מעלה את האפשרות שיש לו אישור לעשות כן. יותר מכך, הסביבה הפוליטית בארצות הברית היא כזו, שבה הרמות הגבוהות ביותר בממשל מעלימות עין ממעקבים מפוקפקים, שבמסגרתם נאספות כמויות ענק של נתונים לא רק ברחבי העולם, אלא גם בתוך ארצות הברית עצמה, וזאת מבלי ליידע את האזרחים או לקבל את אישורם. לאור זאת ניתן לומר שממשלת ארצות הברית חוצה את גבולותיה שלה ועושה שימוש ביכולות המעקב הטכנולוגיות החזקות שלה כדי ליירט ולאחסן מידע נגד מדינות יריבות, אך גם נגד מדינות ידידותיות, ואף נגד אזרחיה שלה.

סמכות חוקית

למרות שפושעי סייבר על-לאומיים משפיעים על כלל המדינות בעולם, ממשלות רבות עדיין לא הסדירו חקיקה מספקת בנושא זה, באופן שיאפשר חקירה והעמדה לדין על פשעים כאלה. גם במדינות שקיימת בהן חקיקה, עדיין לא הוכח שהיא מצליחה להרתיע מפני פעילות כזו. לדוגמה, בארצות הברית נחקקו כמה מהחוקים

"Russia: Control from the Top Down – FSB (The Federal Security Service of the Russian Federation)", *Reporters without Borders*, March 11, 2014, <https://12mars.rsf.org/2014-en/2014/03/11/russia-repression-from-the-top-down/>.

המחמירים ביותר לגבי פשעי סייבר בעולם, וקיימת יכולת אכיפה בתחום זה, שהולכת וגדלה, ואף על פי כן, ארצות הברית היא עדיין מהמדינות המובילות בפשעי סייבר. שיתוף הפעולה הבין-לאומי בין רשויות האכיפה הוא במקרה הטוב נקודתי. מציאות זו מחייבת את אנשי החוק שוב ושוב ל"משחקי תופסת" עם גורמי פשיעת הסייבר. אין חקיקה בין-לאומית מוסכמת בנושא פשיעת סייבר, למרות ש"האמנה לפשעי סייבר" של מועצת אירופה (האמנה הבין-לאומית הראשונה שמתייחסת לפשעים באינטרנט) עשתה מאמצים רבים לגייס מדינות לפעולה בתחום זה. מה שקורה לעתים הוא ששיתוף הפעולה בין המדינות נגד פשיעת סייבר הינו מוגבל, או שבעיות של סמכויות שיפוט מעכבות את התקדמות החקירות בתחום זה. המציאות היא שלא כל גופי האכיפה עשו את הצעדים הנדרשים כדי להגיע לרמה מתקדמת בלחימה בפשיעת הסייבר, ובמקרים מסוימים אף קורה שגוף אכיפה אחד מסרב לסייע לגוף אכיפה אחר.

נכון להיום, דומה שרק "האמנה לפשעי סייבר" מציעה מענה בצורת שיתוף פעולה נגד פשעי סייבר חוצי גבולות. זאת, במקום שניתן יהיה להסתמך על הסכמים משפטיים בילטרליים בין מדינות או על הסכמים פרטניים שיחולו על מקרים ספציפיים. הצדדים החתומים על "האמנה לפשעי סייבר" הסכימו לאמץ חוקים המוציאים סוגים מסוימים של פשעי סייבר אל מחוץ לחוק, ולנקוט פעולה משפטית נדרשת כדי להבטיח שיתוף פעולה באכיפתם. נכון למאוס 2016, 48 מדינות אשררו את האמנה, ואילו שש מדינות נוספות חתמו עליה, אך עדיין לא אשררו אותה. סין ורוסיה בולטות בהיעדרותן מרשימה זו.

סין כמשל

סין הציגה בשנת 2010 לראשונה את עמדותיה בנושא הריבונות באינטרנט, ועשתה זאת בנייר עמדה שכותרתו "האינטרנט בסין".¹⁵ המסר הסיני היה ברור: סין מעוניינת לבסס קווים ברורים של ריבונות במרחב הסייבר, כשם שהם קיימים ביבשה, בים ובאוויר. בהמשך לכך, בכנס האינטרנט העולמי של 2015 שנערך בעיר וו ג'ן, נפגשו פקידי ממשל ואנשי עסקים סיניים בכירים עם פקידי ממשל מקזחסטן, קירגיזסטן, פקיסטן ורוסיה, כדי לדון בסוגיות הקשורות לאינטרנט. בדברי הפתיחה שנשא נשיא סין, שי ג'ינפינג, הוא הדגיש את הצורך של כל הממשלות לכבד את זכויותיהן של המדינות השונות לפתח ריבונות בסייבר עבור אזרחי כל מדינה.¹⁶ מהלכים אלה היו ביטוי לרצונה של סין לשמור על מעמדה של המפלגה

Shannon Tiezzi, "China's Sovereign Internet", *Diplomat*, June 24, 2014, thediplomat.com/2014/06/chinas-sovereign-internet/.

"China Allows no Compromise on Cyberspace Sovereignty", *China Daily*, December 17, 2015, http://www.chinadaily.com.cn/world/2015wic/2015-12/17/content_22735756.htm.

הקומוניסטית הסינית, להגן על האינטרסים הטריטוריאליים של המדינה ולשמר את יציבותה. בעידן שבו האינטרנט מחבר בין כל מרכיבי החברה, סין רואה בריבונות על הסייבר מרכיב קריטי בריבונותה הלאומית.¹⁷ יתר על כן, סין רואה בריבונות על הסייבר לא רק אמצעי להבטיח טוב יותר את האינטרסים שלה, אלא גם כלי חשוב לעמידה נוכח פעולות שמטרתן להשיג הגמוניה בתחום הסייבר ולערער את ביטחונה הלאומי של הרפובליקה הסינית. כותבים סינים התייחסו בהקשר זה למה שהם כינו ניסיונות אמריקאיים לשלוט על האינטרנט הגלובלי – חשש שקיבל חיזוק בחשיפות של פטר סנוואדן ב־2013 על המעקבים שארצות הברית מבצעת באינטרנט בכול רחבי העולם. "החופש המוחלט" של מרחב הסייבר אותו מהללת ארצות הברית נתפס בסין כמצב המיטיב עם הביטחון הלאומי האמריקאי, בעודו פוגע בביטחון שאר העולם.

כדי לקדם את ריבונותה בתחום הסייבר, סין נשענת על מגילת האו"ם, בה היא מוצאת הצדקה להרחבת עקרון השוויון הריבוני גם למרחב הסייבר. סין משיגה בכך שתי מטרות: היא ממחישה את כוונתה לעשות שימוש בחוק הבין־לאומי כדי לתמוך בעמדתה; היא מממשת את רצונה לעורר סוגיות אלו בפורומים בין־לאומיים ובפני ממשלים שונים. מינוף הזווית המשפטית מעניק לגיטימיות להצעה הסינית, והשימוש בזירת האו"ם ממחיש את מחויבותה של סין לפעילות רב־צדדית. ואכן, בדצמבר 2015 נאבקה סין לכלול את המילה "רב־צדדי" ("multilateral") במסמך האו"ם העוסק בהנחיות לקווי המדיניות לאינטרנט בעתיד, והצליחה בכך. חשיבות התוספת הייתה בהצביעה על כך שממשלות, ולא ארגונים עסקיים או אזרחיים, הן שצריכות להיות האחראיות לניסוח הכללים בסוגיה זו. אמנם, מסמך האו"ם המדובר אינו מחייב את המדינות החברות בארגון, אך הוא מספק את האיזון הדרוש מול ההנחיות שנוסחו והתקבלו בעבר.

סין אינה פועלת לבדה, אלא מקדמת ריבונות בסייבר בפורומים בין־לאומיים שונים, כמו למשל במדינות BRICS (ברזיל, רוסיה, הודו, סין ודרום אפריקה), ב"ארגון שנחאי לשיתוף פעולה" וב"קבוצת מומחי הממשל של האו"ם". יש לציין, בהקשר זה, שסין פעלה לחיזוק ההגנה על האינטרסים הביטחוניים הלאומיים המרכזיים שלה באמצעות שורה של חוקים והצעות חוק. דוגמאות לכך הם:

- **חוק אבטחת הסייבר:** בנובמבר 2016 אישרה ממשלת סין את חוק אבטחת הסייבר שלה. החוק מתייחס לאבטחת מערכות מידע ואינטרנט מרכזיות ומחזק את כוחה של הממשלה לתעד ולסכל הפצה של מידע שנקבע כ"בלתי חוקי". שני נושאים מרכזיים בולטים בחוק זה: היכולת לנטר ולשלוט במידע; חובת

"Why Does Cyber Sovereignty Matter?", *China Daily*, December 16, 2015, 17
http://www.chinadaily.com.cn/business/tech/2015-12/16/content_22728202.htm.

הציות של ארגונים זרים לכללים. מבקרי החוק ציינו כי הוא מהווה ניסיון של ממשלת סין לחזק את שליטתה על החברה האזרחית במדינה, בעודה מטילה תביעות לא סבירות על עסקים זרים.¹⁸

- **החוק לניהול ארגונים לא ממשלתיים זרים:** כל ארגוני ה-NGO נדרשים לקבל אישור מגוף מפקח מיוחד כדי שיוכלו לפעול בסין. כמו כן, נאסר על ארגונים סיניים לבצע פעילויות בשם ארגון NGO בלתי מורשה או יחד אתו. למרות שהחוק אינו קשור ספציפית לסייבר, סביר להניח שארגונים לא ממשלתיים הרשומים כנדרש ברשויות הסיניות יחויבו לציית לכול כללי המדיניות המקובלים בנושא השימוש בטכנולוגיה, כפי שתקבע הממשלה הסינית בחקיקתה.
 - **חוק הביטחון הלאומי 2015:** החוק נועד לספק מסגרת חוקית לסוגיות הביטחון של סין לנוכח איומים מתעוררים. שיקולים ביטחוניים חופפים ממחישים את התפיסה הסינית, לפיה ביטחון לאומי הוא תהליך משולב מיסודו, שתוצאתו היא "מסלול ביטחון לאומי לפי מאפייניה של סין".¹⁹ עובדה משמעותית היא שהחוק אינו מוגבל לסין בגבולותיה הגיאוגרפיים, אלא כולל גם את מרחבי הקטבים, את החלל החיצון ואת מרחב הסייבר.
 - **החוק למלחמה בטרור 2015:** החוק, שהתקבל בדצמבר 2015, מאלץ חברות טכנולוגיה לסייע לממשלת סין בפענוח מידע ומעניק לרשויות הסיניות גישה לנתונים מוצפנים. החוק משלב אמצעים מינהליים, משפטיים וצבאיים כדי לתת מענה למאמצי המלחמה בטרור של סין, ומבטא תפיסה המשקפת את רצונה של בייג'ין לשלב את כל היבטי הביטחון תחת מטרייה אחת של חוק הביטחון הלאומי החדש. חוק הטרור הסיני מתכתב עם הנטייה העכשווית של סוכנויות הביטחון האמריקאיות להחליש את מערכות ההצפנה כדי לאפשר גישה ממשלתית אליהן.²⁰
- ניתן לראות מאמצים אלה של סין כניסיון להשיג גמישות רבה יותר לנוכח השפעות חיצוניות, ולהפחית מהחובות הכלכליות ו/או הדיפלומטיות הפוטנציאליות שארצות הברית מבקשת לכפות (כגון סנקציות בתחום הסייבר, סנקציות כלכליות, כתבי אישום וכדומה). בנוסף לכך, מהלכים אלה מחזקים את העמדה הסינית,

Bethany Allen-Ebrahimian, "The Chilling Effect of China's New Cybersecurity 18 Regime", *Foreign Policy*, July 10, 2015, <http://foreignpolicy.com/2015/07/10/china-new-cybersecurity-law-internet-security/>.

"China Focus: China Defines Overall National Security Outlook in Draft Law", 19 *Xinhuanet*, April 20, 2015, http://news.xinhuanet.com/english/2015-04/20/c_134166428.htm.

Joseph Lorenzo Hall, "Issue Brief: A Backdoor to Encryption for Government 20 Surveillance", *CDT*, March 3, 2016, <https://cdt.org/insight/issue-brief-a-backdoor-to-encryption-for-government-surveillance/>.

הגורסת כי ממשלות זכאיות לנהל בעצמן את ענייני הסייבר הפנימיים שלהן. ואכן, רבים מהחוקים הסייבריים שצוינו לעיל זוכים לביקורת על שהם מקדמים את האינטרסים הכלכליים של סין כמדינה ומחזקים את יכולת הבקרה של הממשלה, וזאת למרות התעקשותה של בייג'ין שהכול נעשה בהתאם לכללי מגילת האו"ם.

מסקנות

הוויכוח בין מדינות הלאום בנושא המשילות באינטרנט נותר סוגיה שנויה במחלוקת. כתוצאה מכך מתרחשת כיום תופעה המכונה "בלקניזציה" של מרחב הסייבר. תופעה זו מקבלת תנופה בשל השילוב בין אינטרסים של ביטחון לאומי, איומים ולוחמה כלכלית בעולם המערבי, ובין רצונן של מדינות לשלוט על דעת הקהל והשיח הפוליטי ולנטר אותם. אכיפת גבולות במרחב האינטרנט תוביל בסופו של דבר לאובדן הזדמנויות רבות במונחים של פיתוח כלכלי, זרימה חופשית של מידע וחופש מקוון. אמנם, נכון שהחזון הנאיבי־משהו של מרחב הסייבר, כפי שהתגלם ב"הצהרת העצמאות" של ברלו, לא התגשם, אולם גם כיום חיוני למצוא את האזון בין ריבונות לגלובליזציה ובין ביטחון לאומי לחופש.

מחובתן של דמוקרטיות ליברליות ושל ארצות הברית – בעלת ההגמוניה לכאורה – להוביל את המאמצים למציאת פתרון מוסכם בסוגיית הסייבר. לא יהיה זה מציאותי למזער את מעורבותן של ממשלות בתהליך זה, בדיוק כפי שאין זה מציאותי להטיל עליהן בלבד את משימת מציאת הפתרונות, דבר שעלול להוביל להתנערותן מאחריות. לאור זאת, הסכם רב־צדדי, שיתבסס על הצלחת הקווים המנחים לרגולציה של משאבים גלובליים – האיסור על פעילות צבאית בחלל, הבטחת חופש התנועה בימים הפתוחים ואיסור תביעות ריבוניות על אנטרקטיקה – יכול להשיג פתרון בר־קיימא. בניית משילות ארוכת טווח ברשת, שתאפשר הן למדינות לאום והן לצדדים שאינם מדינות לפעול יחדיו, נראית כדרך היחידה העשויה להניב תועלת הדדית לממשלות השונות. בדרך זו הן יוכלו ליהנות מיתרונות מרחב הסייבר מבלי לסכן את האינטרסים הביטחוניים שלהן.

ארבעה עקרונות ועוד אחד: מודל חדש להגנת סייבר

מת'יו כהן, צ'אק פרייליך, גבי סיבוני

כמו בכול האיומים המתעוררים, גם מרחב הסייבר מציב סכנות חדשות שלא קל לתת להן מענה. מאמר זה שוען כי איומי הסייבר אינם שונים במהותם מאיומים אסימטריים אחרים, ומציג מודל קונצפטואלי לפיתוח תגובה, תוך הסתמכות על העקרונות הקלאסיים של האסטרטגיה הצבאית: התרעה, הרתעה, התגוננות והכרעה, ולצד אלה את עקרון החוסן. המאמר מציע מודל למדיניות המתייחסת לכול אחד מהעקרונות הללו, באופן שיספר את הביטחון של מערכות סייבר לאומיות. המסגרת המוצעת תאפשר פיתוח אסטרטגיות ותוכניות מפורטות שיענו על הדרישות הספציפיות הנובעות מאיומי הסייבר, בין אם הם באים מצד מדינות ובין אם מצד שחקנים לא מדינתיים או מצד גורמים יחידים.

מילות מפתח: סייבר, התרעה, הרתעה, התגוננות, הכרעה, חוסן

מבוא

מרחב הסייבר הוא מקום מסוכן עבור מדינות. ב־2016 הודיעה קבוצה שכינתה עצמה "סוחרים הצללים" ("Shadow Brokers") כי גנבה בהצלחה קוד מסווג של תוכנות נזקה שהיו בשימוש של הסוכנות לביטחון הלאומי של ארצות הברית (NSA) – גוף המסווג כסודי ביותר. חלק מהקוד, שנועד לפעולות ריגול, זמין כעת להורדה באינטרנט, ואת חלקיו האחרים הציעו ה"סוחרים" למכור לכול מי שיהיה מוכן לשלם להם את המחיר הגבוה שדרשו.¹

Paul Szoldra, "New Snowden Documents Prove the Hacked NSA Files are Real", *Business Insider*, August 19, 2016, <http://www.businessinsider.com/snowden-confirm-hacked-nsa-files-2016-8>.

מת'יו כהן הוא דוקטורנט ומרצה במחלקה למדעי המדינה באוניברסיטת Northeastern בארצות הברית. ד"ר צ'ק פרייליך הוא עמית בכיר במרכז בלפר באוניברסיטת הרווארד, לשעבר סגן ראש המל"ל. ד"ר גבי סיבוני הוא חוקר בכיר וראש תוכנית צבא ואסטרטגיה ותוכנית ביטחון סייבר במכון למחקרי ביטחון לאומי.

ב־2015 הודיעה ארצות הברית כי פצחנים (האקרים) חדרו למערכות מחשב רגישות בבית הלבן, וציינה שהאירוע נחשב לאחת ממתקפות הסייבר המתוחכמות ביותר ששוגרו אי פעם נגד מערכות הממשל בארצות הברית. החשודה המתבקשת באירוע זה הייתה רוסיה.² באותה שנה שיגרה קוריאה הצפונית מתקפת סייבר נגד מתקן הגרעין של קוריאה הדרומית, אירוע שעורר חששות לגבי מידת הבטיחות של תחנות הכוח הגרעיניות של האחרונה.³ ב־2014 תקפו פצחנים את השרתים של חברת "סוני", פרסמו הודעות דוא"ל פרטיות ושלחו אימים חריפים נגד החברה ונגד כל בית קולנוע שיעז להקרין סרט סטירי על קוריאה הצפונית. ארצות הברית האשימה את פיונגיאנג במתקפה, וציינה כי תגיב עליה "באופן מידתי". זמן קצר לאחר מכן חווה שירות האינטרנט של קוריאה הצפונית שיבושים שנמשכו מספר ימים.⁴ אלו הן דוגמאות מעטות בלבד למתקפות סייבר מהשנים האחרונות. מאמר זה מבקש לטעון כי למרות שאיומי הסייבר הם בעלי מאפיינים שחלקם מאתגרים במיוחד, ניתן לגבש להם תגובה יעילה. לשם כך דרוש מודל קונצפטואלי שיהווה מסגרת לדיון על חומרתם של איומי הסייבר השונים, הטכנולוגיות שיש לפתח והמדיניות הממשלתית הנדרשת בעניין זה. המאמר מציע מודל קונצפטואלי כזה באמצעות הסתמכות על ארבעת העקרונות הקלאסיים של האסטרטגיה הצבאית – הרתעה, התרעה, התגוננות והכרעה – ולצדם המושג הידוע פחות – חוסן. בנוסף לכך מנתח המאמר כיצד ממשלות, צבאות וגופים פרטיים יכולים לפעול יחדיו בתוך המסגרת המוצעת כדי להתמודד עם איומים במרחב הסייבר. ארבעת העקרונות הקלאסיים שהוזכרו לעיל מוכרים ומיושמים על ידי ממשלות ברחבי העולם, אולם מוגדרים לעתים בצורה שונה על ידי שורה של חוקרים ומדיניות. לדוגמה, "האסטרטגיה הלאומית למאבק בטרור" של ארצות הברית משנת 2003 מיישמת מודל של ארבעה עקרונות שהיא מכנה בשם "הבסה, מניעה, צמצום והתגוננות" (Defeat, Deny, Diminish, Defend).⁵ לעומת זאת, ישראל מבססת את תפיסת הביטחון הלאומי שלה מזה עשרות שנים על מודל שלושת

2 Evan Perez and Shimon Prokupcz, "How the U.S. Thinks Russians Hacked the White House", *CNN*, April 8, 2015, <http://www.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/index.html>.

3 K. J. Kwon, "Smoking Gun: South Korea Uncovers Northern Rival's Hacking Codes", *CNN*, April 22, 2015, <http://www.cnn.com/2015/04/22/asia/koreas-cyber-hacking/index.html>.

4 Haroon Siddique, "North Korea Responds with Fury to US Sanctions over Sony Pictures Hack", *The Guardian*, January 5, 2015, <http://www.theguardian.com/world/2015/jan/04/north-korea-fury-us-sanctions-sony>.

5 "National Strategy for Combating Terrorism", US Department of State, February 2003, https://www.cia.gov/news-information/cia-the-war-on-terrorism/Counter_Terrorism_Strategy.pdf.

העקרונות – התרעה, הרתעה והכרעה⁶ – ומאוחר יותר הוסיפה עיקרון רביעי התופס גם עבור איומי הסייבר – התגוננות.⁷

שום מחקר לא החיל עד היום אסטרטגיה מקיפה של ארבעת העקרונות דלעיל על איומי הסייבר, אם כי היו מחקרים שעסקו בכול אחד מעקרונות אלה בנפרד. כל מחקר כזה העלה תובנות חשובות על מרחב הסייבר, אך ארבעת העקרונות, בשילוב מושג החוסן, כוללים מרכיבים בעלי קשר הדדי שעלולים להיעלם כאשר סוקרים אותם בנפרד. לפיכך, רק מסגרת אנליטית הוליסטית הבוחנת עקרונות אלה ביחד תוכל להגיע להבנה מלאה יותר של איום הסייבר, וזאת לא רק למטרות אקדמיות, אלא גם לצורך קביעת מדיניות.

הגדרת עולם הסייבר

מונחים רבים הנוגעים למרחב הסייבר חסרים הגדרות ברורות ומוסכמות. לצורך הטיעונים של מאמר זה, מתקפת סייבר תוגדר כשימוש פוגעני במרחב הסייבר, אשר משבש מחשבים, רשתות או טכנולוגיות אחרות, או מנצל אותם למטרות פוליטיות או פליליות מזיקות, הרסניות או משבשות.⁸ בדומה לצורות אחרות של לוחמה, גם מתקפות סייבר בעלות מניע פוליטי נועדו לספק יתרון אסטרטגי, דיפלומטי, כלכלי או צבאי על פני היריב, או לאלץ אותו לנקוט פעולה נגד רצונו.⁹ מתקפות סייבר יכולות להיות משוגרות על ידי מדינות, ארגונים שאינם מדינה או אנשים. הגנת סייבר כוללת את המאמצים שנועדו להבטיח את שמירת השליטה על ספקי שירותי האינטרנט (ISP) ועל התעבורה הנכנסת והיוצאת, וכן את היכולת לעצור מתקפות בעת התרחשותן.¹⁰ ריגול סייבר מתייחס לשימוש שעושות מדינה או סוכנויות לאומיות כמו ה-NSA (לעתים קרובות באמצעות תוכנות זדוניות או

6 Matthew S. Cohen, Chuck Freilich and Gabi Siboni, "Israel and Cyberspace: Unique Threat and Response", *International Studies Perspectives* 17 (2016): 307-321; Chuck D. Freilich, "Why Can't Israel Win Wars Anymore?", *Survival* 57, no. 2 (2015): 79-92.

7 "The IDF Strategy", IDF Chief of the General Staff, Israel Defense Forces, July 2016, <https://www.idfblog.com/s/Desktop/IDF%20Strategy.pdf>.

8 Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Rand Corporation: Project Air Force, 2009); Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to do About It* (New York: Harper Collins, 2012); Brandon Valeriano and Ryan C. Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System* (Oxford: Oxford University Press, 2015).

9 Jeffrey Carr ed., *Inside Cyber Warfare* (Cambridge: O'Reilly, 2012); Oona A. Hathaway and Rebecca Crootof, "The Law of Cyber-Attack", *California Law Review* 100, no. 4 (2011): 817-886; Valeriano and Maness, *Cyber War versus Cyber Realities*.

10 Chris C. Demchak, *Wars of Disruption and Resilience* (Athens: University of Georgia Press, 2011); Valeriano and Maness, *Cyber War versus Cyber Realities*.

פריצות, כגון spear-phishing) במטרה לגנוב או לאסוף מידע, או כדי לדעת מהי יכולת התוקפים לחדור לרשתות.¹¹

ארבעה עקרונות ועוד אחד

בחלק זה אנו מבקשים לטעון כי ניתן לטפל ביעילות באיומי סייבר על סמך העקרונות הבסיסיים של האסטרטגיה הצבאית ובאמצעות כמה התאמות שלהם. מדובר בהרתעה, התרעה, הכרעה והתגוננות, ובנוסף לכך במושג החוסן החדש יותר.

הרתעה

כדי להרתיע יריב, יש לזהות ולהכיר את "כתובת המען" שלו שנגדה ניתן לפעול. אחד האתגרים הקשים במיוחד בתחום הסייבר הוא הייחוס. ההרתעה במרחב הסייבר מסובכת גם בשל העובדה שלא תמיד ניתן לדעת מתי נגרם נזק, וייתכן מצב שבו המטרה אפילו לא תדע שהיא הותקפה.¹²

רמת הוודאות של הייחוס היא שתקבע את סוג התגובה שעל המדינה ליישם. רמה נמוכה יחסית של ודאות מספיקה כדי להפעיל דיפלומטיה "מאחורי הקלעים". במגעים דיפלומטיים כאלה, מדינה יכולה להאשים מדינה אחרת על שניסתה להתערב ולהשפיע על התנהגותה, גם אם אין לה הוכחה מוחלטת לכך. להאשמה פומבית נדרשת כבר רמה בינונית של ודאות, ולביצוע פעולה משפטית או צבאית תידרש רמת הוודאות הגבוהה ביותר.

במקרים של מתקפות סייבר הניתנות לייחוס, סוג השחקן (מדינה, ארגון טרור, ארגון לא מדינתי או גורם יחיד) ממלא תפקיד חשוב בקביעת אופייה של מדיניות ההרתעה. הרתעת גורמים מדינתיים מפני ביצוע מתקפות סייבר אינה שונה מהותית מהרתעתם מפני עימותים מסוגים אחרים. במקרה זה, המדינה המותקפת יכולה להגיב בכול קשת היכולות העומדות לרשותה – סייבר, דיפלומטיה, צבא או כלכלה. הרתעת ארגוני טרור מלבצע מתקפות סייבר דומה למניעת פיגועים פיזיים, וכוללת הפעלת מגוון רחב של פעולות תגמול אפשריות בסייבר ומחוץ לסייבר. מרבית ארגוני הטרור פועלים לכאורה בשם ערכים מסוימים, אם כי החשיבות שהם מייחסים לערכים אלה והמוכנות שלהם לסבול בגינם עשויות להיות שונות מאלו של מדינות. יכולת התגמול על מתקפות סייבר של ארגוני טרור הינה מוגבלת בשל אותם שיקולים החלים על ההחלטה לנקוט נגדם תגמול פיזי, לרבות שיקולי מרחק ופגיעות. הרתעת טרוריסטים היא אתגר מורכב בדיוק כמו בעולם הפיזי, ולכן גם קשה להרתיע ארגוני טרור מלתקוף במרחב הסייבר.

P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar* (New York: Oxford 11 University Press, 2014); Valeriano and Maness, *Cyber War versus Cyber Realities*.

Libicki, *Cyberdeterrence and Cyberwar*. 12

המספר הרב של ארגונים לא מדינתיים ושל תוקפים בודדים (פצחנים ואקטיביסטים) פוטנציאליים המפוזרים ברחבי העולם מהווה אתגר ליכולות הניטור והייחוס הנדרשות לצורך ההרתעה. עם זאת, יכולות הסייבר המתוכננות של המדינה עשויות להקשות על ארגון או אדם להסתיר את זהותו. "החדשות הטובות" בנוגע ליחידים ולארגונים לא מדינתיים הן שלרוב יש להם פחות משאבים כדי לשגר מתקפות סייבר משתקות נגד מדינות מפותחות. זאת ועוד, אחד המניעים העיקריים שלהם הוא לעתים קרובות עצם הפרסום, עובדה שמסייעת לייחס את הדברים לאותם יחידים וארגונים לא מדינתיים. גם פיתוח כלים טובים יותר לזיהוי פלילי – מאמץ שכבר נמצא בעיצומו – יעזור לקבוע מי שיגר את המתקפה.

התרעה

זיהוי מראש או התרעה מוקדמת של התקפות מתקרבות הם קריטיים במרחב הסייבר, כמו בעולם הפיזי. מניעת המתקפה היא אפשרית רק אם יש התרעה מוקדמת מספיקה. בדרך כלל גם קל יותר להתגונן מפני התקפה שלגביה יש התרעה. למדינות מעטות בלבד, לא כל שכן לגורמים לא מדינתיים, יש את היכולות הנדרשות כדי לנהל בהצלחה מתקפת סייבר גדולה נגד מדינה בעלת יכולות הגנה משוכללות. האתגר האמיתי של גילוי מתקפת סייבר טמון לא במספרם העצום של התוקפים הפוטנציאליים ברחבי העולם, אלא במספרם המוגבל למדי של המתוכננים שבהם. במצב זה, ההתמודדות עם המתקפה הופכת לאפשרית יותר.

המרכיב שמסבך את התמונה הוא התחזקות הקשרים ההדדיים בין הרשתות הממשלתיות, הצבאיות והפרטיות. רשתות של המגזר הפרטי יכולות כיום לשמש כשער כניסה לרשתות ממשלתיות וצבאיות מסוימות, ופירוש הדבר הוא שהמגזר הפרטי מהווה נקודת תורפה לפגיעויות. על רקע זה, מדינות מתמודדות עם הצורך לספק התרעה מוקדמת לא רק למערכות ממשלתיות ולתשתיות קריטיות, אלא גם לחברות ולארגונים מרכזיים. חלק מהמדינות כבר החלו להשקיע מאמצים מוגברים באיסוף מודיעין והגדילו את שיתוף המידע עם המגזר הפרטי, אך שיתוף מידע בין ממשלות לחברות פרטיות נותר עדיין, ככלל, אתגר משמעותי. הגברת מאמצים לשיתוף פעולה כזה עשויה לחייב, ככול הנראה, שינויים משפטיים, ארגוניים ופוליטיים בממשלות ובארגונים גם יחד.¹³

הטכנולוגיה היא מרכיב קריטי במערכות לאומיות שנועדו להתריע בפני איומי סייבר. מאמצי ההתרעה נגד מתקפות סייבר יקבלו חיזוק משמעותי על ידי הגברת

Aviram Zrahia, "A Multidisciplinary Analysis of Cyber Information Sharing", *Military and Strategic Affairs* 6, no. 3 (2014): 59-77.

איסוף המודיעין המסורתי על תוקפים פוטנציאליים, וזאת לצד המידע שנאסף עליהם באינטרנט.¹⁴

מספר גורמים פועלים לטובת הצד המתגונן. מתקיפים מבצעים לעתים קרובות "משימות סיור בסייבר" כדי להעריך את נקודות התורפה במערכות הצד המתגונן.¹⁵ ככול שמתקפת סייבר מתוכננת או מתמשכת היא גדולה יותר, כך קל יותר לייצר את התקשורת בין התוקפים וליישם פעולת הגנה. זאת ועוד, המספר הקטן של כבלי התקשורת הנושאים את תעבורת האינטרנט הופך את בעיית ההתרעה לפשוטה יותר עבור מדינות רבות.

התגוננות

התגוננות עוסקת במניעה ובצמצום של מתקפות על רשתות תשתית צבאיות, ממשלתיות וקריטיות, וכן על רשתות פרטיות, עסקיות ושל יחידים. שחקנים שונים מסוגלים לבצע סוגי מתקפות בעלות אופי שונה ודרגות חומרה מגוונות, ולכן מקור המתקפה קובע מהם האמצעים הטובים ביותר להתגונן מפניה. בדרך כלל קשה יותר להתגונן מפני התקפות מצד מדינות, בעוד שהיכולות הטכנולוגיות של ארגונים ואנשים שאינם מדינה הן פחות מתקדמות, וניתן לטפל בהן באמצעות פתרונות טכנולוגיים פשוטים יחסית.

הטכנולוגיה ממלאת תפקיד מרכזי במאמץ ההגנתי ומדינות שונות כבר החלו בבניית תוכניות שיסייעו בהגנה על רשתות ומערכות סייבר. פיתוח של טכנולוגיות המסוגלות להתמודד עם סוגים שונים של איומים הוא כמובן מטרה רצויה, אך אילוצי המשאבים מחייבים מדינות לתת עדיפות לאיומים הדחופים ביותר, שבהם הן יוכלו למקד את משאביהן. זהו תחום נוסף שבו ממשלות והמגזר הפרטי יכולים לפעול יחדיו. שיתוף פעולה כזה יגדיל את יכולתם של שני הצדדים לזהות את האיומים הגדולים וליצור כלים חדשים להגנה מפניהם. גם אם חברות אבטחת סייבר פרטיות יבחרו שלא לשתף פעולה עם ממשלות, אותן ממשלות יוכלו להפיק תועלת מעצם ההתבוננות מקרוב באיומים בהם עוסקות אותן חברות, כבסיס להערכת האיומים שהן יבצעו. ממשלות גם יכולות לשתף פעולה עם גורמים פרטיים כדי להבטיח שמערכות אבטחה ברשתות המתחברות למערכות ממשלתיות ישמרו על עדכניותן.¹⁶

Gabi Siboni and Ofer Assaf, *Guidelines for a National Cyber Strategy* (Tel Aviv: 14 Institute for National Security Studies, 2016).

Ned Moran, "A Cyber Early Warning Model", in *Inside Cyber Warfare*, ed. Jeffrey 15 Carr.

William J. Lynn, "Defending a New Domain", *Foreign Affairs*, October 2010, <https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain>; Milton L. Mueller, Andreas Schmidt and Brenden Kuerbis, "Internet Security and

הגנת סייבר לא יכולה להיעשות רק באינטרנט. נדרש מאמץ רב־שכבתי של איסוף מידע מודיעיני, שיבוש מתקפות ואבטחת רשתות, נקיטת צעדים משפטיים, גיבוש נורמות התנהגות חדשות ועידוד שיתוף פעולה אפקטיבי עם ממשלות זרות. נכון להיום, אין נורמות או חוקים בין־לאומיים ברורים לגבי התנהגות במרחב הסייבר,¹⁷ אף שאמנות, חוקים ונורמות יכולים להתגלות כיעילים להגבלת פעולות זדוניות של מדינות במרחב זה. כדי להשיג יעילות בהתגוננות מפני התקפות סייבר, על מדינות להסכים ביניהן מהם סוגי הפעילות הרלוונטיים, מה אחריות המדינה במסגרת ההסכמה ומה יהיה העונש על הפרתה. בנוסף, מדינות יצטרכו להקים גופים בין־לאומיים שיפקחו על הציות לאותן הסכמות.¹⁸

חשיבות רבה יש לשיתוף פעולה בין־לאומי. גידול במספר המדינות שישתפו פעולה ביניהן בנושא ביטחון הסייבר יביא תועלת למדינות רבות. שיתוף מודיעיני, הסכמים דו־צדדיים ורב־צדדיים ושיתוף פעולה משופר עם רשויות אכיפת החוק במדינות אחרות, יכולים לתרום רבות לתכנון אסטרטגיות הגנה.¹⁹ יהיה צורך בשיפור שיתוף הפעולה בין מדינות גם כדי להבטיח את אכיפת החוקים והנורמות החדשים.²⁰

הבסה

עקרון ההבסה בעולם הסייבר אין פירושו מניעה מוחלטת של כל התקפת סייבר. למעשה, הבסה מוחלטת היא נדירה למדי הן בעולם הפיזי והן בעולם הסייבר. לכן, יש לראות את הבסת היריב בסייבר כמפחיתה את ההיקף והחומרה של המתקפות

Networked Governance in International Relations", *International Studies Review* 15, no. 1 (2013): 86-104; Ido Naor, "ATMZombie: Banking Trojan in Israeli Waters", *SecureList*, February 29, 2016, <https://securelist.com/blog/research/73866/atmzombie-banking-trojan-in-israeli-waters/>; Teri Radichel, "Case Study: Critical Controls that could Have Prevented Target Breach", *SANS Institute*, 2014, <https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412>.

Abraham D. Sofaer, David Clark and Whitfield Diffie, "Cyber Security and International Agreements", *Proceedings of a Workshop on Deterring Cyber-Attacks: Informing Strategies and Developing Options for U.S. Policy* (Washington DC: National Academies Press, 2010), <http://www.nap.edu/catalog/12997.html>; Valeriano and Maness, *Cyber War versus Cyber Realities*.

Sofaer, Clark and Diffie, "Cyber Security and International Agreements".
 "International Public Private Partnership in Cyber Governance (Panel)", *CYFY, 2013 Report*, The India Conference on Cyber Security and Cyber Governance, Observer Research Foundation, <http://www.bic-trust.eu/files/2014/04/CYFY-2013-Report-WEB-version-15Apr14.pdf>.

Sofaer, Clark and Diffie, "Cyber Security and International Agreements".

לרמה המאפשרת לחברה לשמור על אורח חייה ולחזור במהירות לשגרה לאחר המתקפה (ראו בהמשך פירוט בסוגיה זו בפסקה על נושא החוסן).

כדי להשיג הבסה בעולם הסייבר, על המדינה להיות מסוגלת להוכיח ליריביה שביכולתה למנוע מתקפות סייבר גדולות; שהתקפות הסייבר שהיא לא הצליחה למנוע אינן משיגות את מטרתן, בין משום שהן לא גרמו נזק משמעותי ובין משום שהמדינה יודעת לחזור במהירות לשגרה; וכן שמתקפות סייבר ייתקלו בפעולת תגמול כזו או אחרת. כללית ניתן לקבוע כי השגת הבסה מחייבת מדינות להיות מסוגלות ליישם בהצלחה את כל אחד מארבעת העקרונות שנמנו עד כה, בתוספת עקרון החוסן.

מדינות צריכות לייחס למתקפות סייבר את אותה החשיבות שהן מייחסות למתקפות פיזיות, ובמידת הצורך להשתמש בשיטות ובאסטרטגיות דומות, כמו תגובה שאינה מגבילה עצמה לכלי סייבר אלא פונה גם ליכולות צבאיות.²¹ שיגור התקפות צבאיות נגד מדינות הוא מהלך ישיר וברור, אך כשמדובר בשחקן לא מדינתי, המהלך הרבה יותר מסובך ומחייב את יוזם ההתקפה הצבאית להשיג את אישורה של המדינה המארחת, שאם לא כן הוא מסתכן בהסלמה צבאית. בנוסף לכך, יש לקחת בחשבון כי התגובה הציבורית לתקיפה צבאית שתבוא כצעד תגובה למתקפת סייבר של גורם לא מדינתי, עשויה להיות שלילית.

אופיו הלא ממוקד של איום הסייבר גורם לכך שמדינות אינן יכולות לצפות למנוע את כל מתקפות הסייבר מכול גורם יחיד או ארגון לא מדינתי בכול רחבי העולם. מדינה יכולה להביס את היריב במרחב הסייבר על ידי מזעור הסיכוי להתקפה גדולה שיש בה כדי להסב שיבושים או נזקים נרחבים. אם היריב לא הצליח להוציא לפועל מתקפה גדולה, הוא למעשה הובס. במרבית המתקפות מצד יחידים וגורמים לא מדינתיים, התגובה ההולמת יותר היא ההגנה, שיש בה שימוש נכון יותר במשאבים, במיוחד כאשר הגורמים התוקפים לא מחזיקים ביכולות לגרימת נזקים חמורים.²² הגברת שיתוף הפעולה הבינלאומי יכולה לשפר את יכולתן של מדינות להכריע שחקנים כאלה באמצעות הטלת עונשים משפטיים ופליליים על התקפות חוצות גבולות.²³ בסופו של דבר, על מדינות להציב מטרות מציאותיות יותר בבואן להביס מדינות, ארגוני טרור וארגונים לא מדינתיים המשתמשים בנשק הסייבר.

Robert Hackett, "Let's Get Physical? United States Weighs Options When it Comes to Cyber Attacks", *Fortune*, May 12, 2015, <http://fortune.com/2015/05/12/rogers-cyber-attacks-us-response/>.

Herbert S. Lin, "Offensive Cyber Operations and the Use of Force", *Journal of National Security Law and Policy* 4, no. 63 (2010): 63-86.

Valeriano and Maness, *Cyber War versus Cyber Realities*. 23

חוסן

כאשר מתקפה מצליחה, מתעוררת השאלה כיצד יש לנהל את המערכת הפגועה ולהתאושש מהר ככול האפשר, כלומר כיצד יש לבנות מראש מערכות בעלות "חוסן". מערכות שונות יחייבו רמות שונות של חוסן. רשתות מסוימות צריכות לחזור במהירות לרמה מינימלית בלבד של תפקוד, בעוד שאחרות חייבות לחזור לרמת התפקוד המקורית שלהן בהקדם האפשרי.

תהליך הבנייה של מערכות בעלות חוסן במרחב הסייבר מתחיל בניסוח תרחישים בעלי סבירות גבוהה ועלות נמוכה, לצד תרחישים בעלי סבירות נמוכה אך עלות גבוהה. לאחר שלב גיבוש התרחישים, ניתן לבנות תוכניות וכלים להתמודדות עם האיום. דבר זה חייב להתבצע לפני שלב הכישלון בהתגוננות, ולכלול אמצעים טכנולוגיים, פיתוח משאבי אנוש, אימונים ותרגילים, וכן אמצעי יישום.²⁴ החוסן בהקשר של תחום הסייבר חייב לכלול גם תוכניות לשיקום מפגיעות פיזיות בעקבות מתקפות סייבר.

משאבים הינם מצרך מוגבל מטבעו, ופירוש הדבר שיש חשיבות קריטית לתעדוף המערכות הדורשות חוסן. לדוגמה, מערכות צבאיות ורשת החשמל חשובות למדינה הרבה יותר מאשר רשתות אחרות. ניתן לפתח מדדים כדי לקבוע אילו מערכות הן הקריטיות ביותר והיכן יש להשקיע משאבים טכנולוגיים.²⁵ ההשפעה של רשת או תשתית פגועות על המורל הציבורי ועל אמונת האזרחים ביכולת ממשלתם לספק מוצרים ציבוריים בסיסיים, היא שיקול מרכזי שיש להתחשב בו.

בניית החוסן גם דורשת עבודה צמודה עם המגזר הפרטי, מה גם וחברות פרטיות אחראיות פעמים רבות על תחזוקת מתקנים ורציפות פעילותם ועל טיפול באיומים. ממשלות צריכות לעבוד במשותף עם המגזר הפרטי, ובמקביל לפקח עליו, וזאת כדי להבטיח קיומן של תוכניות נאותות להתמודדות עם שירותים שנפגעו.²⁶ המציאות מלמדת שיש להתכונן לכשלים בלתי צפויים בהגנת הסייבר, וכי התוצאות של כשלים כאלה עלולות להיות קיצוניות. מערכת בעלת חוסן יכולה ליצור את ההבדל בין התאוששות מהירה יחסית ובין תוצאות חמורות. איסוף מודיעין על תוכניות האויב או על יכולותיו הכלליות הינו חיוני לצורך תכנון

Singer and Friedman, *Cybersecurity and Cyberwar*; Valeriano and Maness, *Cyber War versus Cyber Realities*.

שם. 25

Dana Pasquali, "3 Steps Towards Building Cyber Resilience into Critical Infrastructure", *Dark Reading*, August 2, 2016, <http://www.darkreading.com/vulnerabilities---threats/3-steps-towards-building-cyber-resilience-into-critical-infrastructure/a-d-id/1326464>; Jan Trobisch, *Challenges in Protection of US Critical Infrastructure in the Cyber Realm* (Fort Leavenworth, KS: School of Advanced Military Studies, United States Army Command and General Staff College, 2014), <https://www.hsdl.org/?abstract&did=791151>.

ההתאוששות.²⁷ מערכות בעלות חוסן מצמצמות את השפעת ההתקפה, ובכך מקטינות את התמורה שמקבל התוקף.²⁸ עובדה זו כשלעצמה מקטינה את הסבירות לעצם התרחשות ההתקפה מלכתחילה.

עם זאת, גם לחוסן יש מגבלות. בסופו של דבר, מתקפה יכולה להפיל גם את המערכת וגם את אמצעי התגובה המיועדים להתמודד עם הפגיעה. מדינות חייבות להיות מוכנות לאפשרות כזו ולפתח תוכניות נוספות שיאפשרו המשך פעילות גם ללא המערכת, אפילו לתקופה ממושכת. מצב כזה צפוי לגרום לכפילות מסוימת ולהביא לפיתוח תוכניות שאינן תלויות בטכנולוגיה.

השלכות על המדיניות

בחלק זה נבקש לדון בהמלצות מדיניות ספציפיות שנגזרות ממודל ארבעת העקרונות ועקרון החוסן. כדי להשיג הרתעה, על מדינות להבהיר ליריביהן מהן פעולות התגמול הצפויות ואיזה מחיר הם עשויים לשלם. הצגת עמדותיו וכוונותיו של המרתיע יכולה להיעשות באמצעות הצהרות פומביות ו/או בערוצים סודיים.²⁹ הקושי הוא בקביעת הייחוס, שכן לא תמיד ברור מי צריך להיות היעד להצגת עמדות וכוונות אלו, אולם ניתן להתגבר על כך ככול שיכולות הייחוס הולכות ומשתפרות. יכולות ייחוס משופרות ישכנעו את היעד להרתעה כי הוא עתיד לשלם מחיר, ובנוסף לכך יסייעו למדינות למקד את עצמן ביתר יעילות באויבים הרלוונטיים.

אופי הממשל במדינה שממנה מגיעה מתקפת הסייבר, ובמיוחד נכונותו של אותו ממשל לשתף פעולה עם התוקפים, הם שני גורמים חשובים ביכולת של הגורם המותקף להגיב. במקרה כזה פעולת תגמול בסייבר אינה אפשרית, אלא אם כן המדינה המותקפת מוכנה לפגוע בריבונות המדינה שאירחה את תוקפי הסייבר. לחילופין, מדינה עשויה להצליח ליצור הרתעה באמצעות פעולה מול גופי המודיעין ורשויות החוק של הממשלה המארחת את תוקפי הסייבר. במקרים מסוימים, עצם הסיכוי לנקיטת צעדים משפטיים חמורים עשוי ליצור הרתעה מספקת. דרך זאת הינה מוגבלת למדי בשימוש כיום, דבר המאפשר לארגונים וליחידים לבצע התקפות סייבר.

כאשר מקורן של התקפות הסייבר הוא במדינות שאינן משתפות פעולה בהתמודדות עם איום הסייבר או אינן יעילות בכך, היכולת להרתיע אותן באמצעים משפטיים תהיה כמובן מוגבלת יותר. שאלת ההרתעה תהיה במקרה כזה דומה

Demchak, *Wars of Disruption and Resilience*. 27

"The DoD Cyber Strategy", US Department of Defense, 2015, https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf. 28

29 שם.

יותר לפעולת תגמול על התקפה פיזית, ותתמקד ביכולות הסייבר של התוקף או ביכולות אחרות שראוי לתקוף, ובמידת ישימותה של דרך פעולה כזו.

כמו בעולם הפיזי, כך גם בעולם הסייבר הבעיה האמיתית בהרתעת גורמים לא מדינתיים היא מידת הנזק שהם גורמים, שהוא בדרך כלל מוגבל. זאת, בעוד שיכולת הספיגה של אותם גורמים עולה לא פעם על עוצמת התגמול שהמדינה המותקפת מוכנה להפעיל. הדבר נכון במיוחד לגבי הדמוקרטיות המערביות. כמובן שדמוקרטיות מסוגלות להביס איומים מצד גורמים לא מדינתיים, אולם המאמץ הנדרש מהן כדי לעשות זאת, ובכלל זה הפגיעה והמחיר בחיי אדם, נתפס בדרך כלל כגבוה מדי בהשוואה למידת האיום שאותם גורמים מציבים על האינטרסים של המדינה. דבר דומה נכון גם לגבי מתקפות סייבר. יחד עם זאת, אם גורם לא מדינתי יוציא לפועל מתקפת סייבר קיצונית, או שיתגלה מידע אמין על מתקפה קלה כזאת, אין ספק שהמדינה שתהיה נתונה למתקפה או לסכנה למתקפה כזאת תפגין מוכנות רבה יותר להפעיל אמצעי הרתעה חמורים.

כדי להשיג הרתעה, על מדינות להיות מסוגלות לקבוע ייחוס למתקפה. לשם כך, מדינות צריכות לעשות שימוש בכלים טכנולוגיים ומודיעיניים ולשפר אותם באופן מתמיד, כולל איסוף מידע על היכולות הטכנולוגיות של יריבים פוטנציאליים ועל יעדיהם.³⁰ זהו תחום שראוי שגופים פרטיים וממשלתיים ישקלו לשתף פעולה בו, וזאת נוכח העובדה שחברות פרטיות העוסקות בביטחון סייבר יכולות לזהות תוכנות זדוניות ולהציע תובנות לגבי מקורותיהן.³¹

קושי נוסף בהתמודדות עם התקפות סייבר הוא שניתן לנתב אותן באמצעות ספקי שירותי אינטרנט במדינות "צד שלישי". ממשלות יכולות לפעול יחד עם ספקי שירותי אינטרנט או הממשלות המארחות אותם, או להפעיל עליהם לחץ כדי שיעצרו את מתקפות הסייבר טרם התרחשותן.³² אם לא מושג שיתוף פעולה כזה, ניתן לשקול תגובה שתכלול פרסום וביוש (שיימינג) פומבי של אותם מדינה, ארגון או אדם העומדים מאחורי המתקפה. יתרון נוסף של מהלך כזה הוא האזהרה שהוא מספק לשירותי הביטחון בעולם לגבי התוקף, אשר מקטינה את יכולתו לבצע מתקפות נוספות.

המאמצים לשיפור ההרתעה על מתקפות סייבר צריכים להתבסס הן על אמצעים מותאמים במיוחד לאיסוף מודיעין סייבר והן על הגדלת נתח משאבי המודיעין האלקטרוני והאנושי הקיימים שכבר מושקעים בתחום זה. טכנולוגיית הסייבר

Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks", *Journal of Strategic Studies* 38, no. 1-2 (2015): 4-37.

Grant McCool, "Computer Spying Malware Uncovered with 'Stealth' Features: Symantec", *Reuters*, November 23, 2014, <http://www.reuters.com/article/us-symantec-malware-regin-idUSKCN0J70SH20141123>.

Clarke and Knake, *Cyber War*. 32

אמנם יוצרת בעיות התרעה חדשות, אך גם מספקת אפשרויות חדשות בתחום ההתרעה.³³ כך, למשל, אסטרטגיית הסייבר הלאומית של אוסטרליה מדגישה נקודה זו, כשהיא קוראת להתרעה משופרת באמצעות ניטור רציף באינטרנט בזמן אמת.³⁴ למרות שניתן לשגר בודיזמים מספר עצום של מתקפות סייבר ממקורות שונים, טכנולוגיות סייבר יכולות לזהות מספר גדול לא פחות של מתקפות ולפעול נגדן. אחת האפשרויות (המתאימה בעיקר נגד תוקפים לא מדינתיים ונגד תוקפים יחידים) היא להתחזות לאקטיביסטים וחברים ברשתות הסייבר, וזאת כדי לאסוף מודיעין ומידע על יכולות ואמצעים.³⁵

אחד הקשיים בגילוי מתקפות סייבר מצד מדינות או גורמים לא מדינתיים הוא שיגורן ממדינות ידידותיות, דבר המגביל את היכולת לעקוב אחריהן מבלי לפגוע בקשרים דיפלומטיים. הטכנולוגיה יכולה לסייע בכך, שכן היא מאפשרת גילוי מרחוק מבלי לפגוע בריבונותה של המדינה. מנגד, דווקא במצבים כאלה גובר הצורך בשיתוף פעולה בין-לאומי ובשיתוף מידע.

מדינות המעוניינות לחזק את יכולותיהן במונחים של התגוננות יכולות להתמקד בשיפור השימוש שהן עושות בטכנולוגיה. הגנה על עולם הסייבר מחייבת שיפור הטכנולוגיות הקיימות ויצירתן של טכנולוגיות חדשות. מנגנון ההגנה גם חייב להתאים למצב השורר ברגע נתון: בשלבים הראשונים של המתקפה, לפני שנגרם נזק ממשי או לפני שנפרצה מערכת כלשהי, ייתכן שיהיה די במאמצים לשבש או להטות את כיוון המתקפה. אם המערכת נפרצה או שנגרם נזק, על מנגנון ההגנה לנסות ולבלום את המתקפה, ובמקביל למנוע מהתוקף לדעת שהפריצה התגלתה ונבלמה בהצלחה.³⁶

הגנה על רשתות הן במגזר הממשלתי והן במגזר הפרטי תדרוש חקיקה ותקנות חדשות. ייתכן שגם יהיה צורך בהקמת סוכנויות ממשלתיות חדשות שיעסקו בניסוח הדרישות הספציפיות ויבטיחו את יישומם של מנגנוני ההגנה. פיקוד הסייבר האמריקאי ורשות הסייבר הלאומית בישראל הם דוגמאות לגופים מרכזיים האחראים לפקח על גיבושן ויישומן של אסטרטגיות התגוננות בסייבר, במקביל למאמצי שיתוף פעולה עם המגזר הפרטי.

“The National Strategy to Secure Cyberspace”, Department of Homeland Security, 33 February 2003, https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

“Australian Government Cyber Security Strategy”, Commonwealth of Australia, 34 2009, <http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf>.

“Impersonation”, Microsoft, <http://technet.microsoft.com/en-us/library/cc961980.aspx>. 35

Siboni and Assaf, *Guidelines for a National Cyber Strategy*. 36

ממשלות, חברות פרטיות ואנשי אקדמיה צריכים לשתף פעולה ביניהם כדי לפתח אסטרטגיות וכלים טכניים חדשים להגנה וכדי לשפר את הכלים הקיימים. ממשלות יכולות להציע תמריצים כספיים על פי הצורך לגופים פרטיים שיישעו בבניית הגנות איתנות.³⁷ צעדים פשוטים עשויים להתגלות כיעילים למדי, כמו למשל חיוב עובדים של סוכנויות ממשלתיות וגופים פרטיים המחזיקים לרשתות ממשלתיות להשתמש בסיסמאות חזקות המוחלפות באופן קבוע, כמו גם חיובם לעבור הכשרה כיצד לזהות ולמנוע איומי סייבר.³⁸

המתגוננים חייבים גם לשקול את שרשרת האספקה המשמשת לתכנון וייצור הציוד שבו הם מסתייעים. נכון להיום, חומרה, קושחה ותוכנה נוצרים ונבנים בכול העולם, עובדה המקשה לוודא שהמוצר אכן מאובטח. החברות והמדינות שבהן ציוד כזה מתוכנן ומיוצר עלולות לשלב בו קודים מוסתרים שיאפשרו פריצה למכשירים בבוא העת. על ממשלות לשקול פעילות משותפת עם חברות ומדינות זרות במטרה לפתח מערכת הסמכה שתבטיח שקיפות בתהליכי התכנון והייצור.³⁹ יחד עם זאת, תוכנית כזו יוצרת סיכון מסוים, משום שהיא עלולה להקשות על שמירת קניין רוחני, להעלות את מחיר הציוד בשל עלויות נוספות ואולי אף לדכא את קצב החדשנות.⁴⁰

גיבוש חוקים גלובליים, נורמות והסכמים בין-לאומיים יסייע לחיזוק הגנת הסייבר. נראה כי התמקדות בהגנה על תשתיות קריטיות ואזרחיות (לדוגמה, איסור התקפות על בתי חולים או חדירות למערכותיהם) היא בעלת הסיכוי הרב ביותר לגייס הסכמה.⁴¹ מדינות צריכות לנסות למלא תפקיד פעיל בניסוח חוקים ונורמות אלה, שכן ככול שמדינה תהיה מעורבת יותר, כך תגדל יכולתה להגן על האינטרסים שלה בעת עיצוב המערכת העתידית.⁴² הניסיון לגבש חוקים ונורמות הוא משימה לא יקרה, שעשויה לשפר את ביטחון הסייבר של מדינות בכול העולם. אם תצלח, יהיו בידינו אמצעים לחזק לא רק את ההתגוננות, אלא גם את ההתרעה, ההרתעה ויכולת ההבסה.⁴³

Radichel, "Case Study: Critical Controls that could Have Prevented Target Breach". 37
שם. 38

David Inserra and Steven Bucci, "Cyber Supply Chain Security: A Crucial Step 39
toward U.S. Security, Prosperity and Freedom in Cyberspace", *Heritage Foundation*,
March 6, 2014, <http://www.heritage.org/research/reports/2014/03/cyber-supply-chain-security-a-crucial-step-toward-us-security-prosperity-and-freedom-in-cyberspace>.

Sofaer, Clark and Diffie, "Cyber Security and International Agreements". 40
Clarke and Knake, *Cyber War*; Sofaer, Clark and Diffie, "Cyber Security and 41
International Agreements"; Valeriano and Maness, *Cyber War versus Cyber Realities*.

Siboni and Assaf, *Guidelines for a National Cyber Strategy*. 42

"International Public Private Partnership in Cyber Governance (Panel)". 43

למרות כל הנאמר לעיל, כוחם של הנורמות והחוקים הבין-לאומיים במרחב הסייבר הוא מוגבל. אופיו המבוזר של מרחב הסייבר יוצר קושי לדעת עד כמה יעילים יהיו החוק והנורמות הבין-לאומיים.⁴⁴ יתר על כן, מדינות עלולות לסרב לנסח הסכמים שישיעו לרעה על השימוש בסייבר, במיוחד כאשר הוא מועיל לאינטרסים הלאומיים שלהן, וזאת גם לאור העובדה שמדובר בתחום חדש שלא עבר תהליכי הרשאה מספיקים.⁴⁵ לבסוף, העובדה שקשה לדעת מתי מתקפה תתרחש, ובדיעבד למי לייחס אותה, מביאה מדינות להאמין שהן יכולות לפעול ללא חשש מפעולת תגמול.

מדינות יכולות לנקוט כמה צעדים כדי להגביר את יכולתן להביס תוקפים בסייבר. הן יכולות לנסות לבדוד מדינות תוקפניות ולהפנות נגדן כלים כגון סנקציות כלכליות או דיפלומטיות, מתוך כוונה לשכנע אותן שהמשך הפעולה ההתקפית יגבה מהן מחיר יקר מדי. הסיכוי להביס אויב במרחב הסייבר יגבר, אם מדינות יתמקדו בדרכים להרוס את יכולות הסייבר של אותו אויב. זאת, בשל התכנון המקיף והציוד היקר הדרושים כדי לאפשר לו שיגור מתקפות מתוחכמות.⁴⁶

בנוסף לצעדים משפטיים, מדינות יכולות לנקוט מהלכים שיצמצמו את האיום מצד תוקפים יחידים. בידוד של פצחנים יחידים מהקהילה שעליה הם נמנים ומסתמכים, בין אם באמצעות שיבוש הקשרים האינטרנטיים שלהם ובין אם בדרך של הפצת מידע שייסב להם נזק בתוך הקהילה שלהם, יכול לפגוע ביכולתם לתכנן או לשגר מתקפה.⁴⁷ בנוסף, מדינות יכולות לנסות לגייס פצחנים לשמש כמודיעים, או לחדור לרשתות של פצחנים על ידי שתילת סוכנים בהן. אסטרטגיות כאלו עשויות להועיל גם נגד חלק גדול מהגורמים הלא מדינתיים, שגם אצלם יש הסתמכות על קהילות דומות לצורך תמיכה. אמנם, אסטרטגיה זו יוצרת סיכון נוכח החוק הבין-לאומי (והמקומי), אך היעדר חקיקה בין-לאומית ברורה בשאלות הנוגעות ספציפית למרחב הסייבר מקטין סיכון זה.

כדי לשפר את החוסן בתחום הסייבר, מדינות צריכות לשאוף לגיוון ציוד הסייבר. חומרה ותוכנה לא אמורות להגיע ממקור אחד או מחברה אחת. ציוד מגוון יאפשר למדינות לבדוד מהר יותר את הבעיה, לעבור לציוד של חברה אחרת ולחדש את הפעילות, אם כי מערך כזה עלול להגדיל סיכונים בשרשרת האספקה.

Valeriano and Maness, *Cyber War versus Cyber Realities*. 44

Sofaer, Clark and Diffie, "Cyber Security and International Agreements" 45

Jonathan Silber, "Cyber Vandalism – Not Warfare", *Ynet*, January 26, 2012, <http://www.ynetnews.com/articles/0,7340,L-4181069,00.html>. 46

Scott D. Applegate, "The Principle of Maneuver in Cyber Operations", in *Fourth International Conference on Cyber Conflict*, ed. C. Czosseck, R. Ottis and K. Ziolkowski (Tallinn: NATO CCD COE, 2012), https://ccdcoe.org/publications/2012proceedings/3_3_Applegate_ThePrincipleOfManeuverInCyberOperations.pdf. 47

בעת תכנון רשתות, ניתן לכלול בהן תכונות שנועדו לשפר את החוסן ולתמוך בתהליך ההתאוששות. כדי לעזור בבניית חוסן של הרשתות הקריטיות ביותר, על מדינות לעצב ארכיטקטורת סייבר שתציע ערוצי גישה שונים למערכות הבקרה.⁴⁸ יש לכלול מראש מעקפים פיזיים כדי להבטיח דרכים נוספות להשתלטות מחדש על מערכות קריטיות. לדוגמה, ניתן לתכנן מערכת רכבות עם יכולת לעצור רכבת שנחטפה, באמצעות בקורות פיזיות שאינן תלויות במערכות הסייבר.

מסקנות

מתקפות סייבר אינן שונות במהותן מאיומים אחרים, וניתן להתמודד אתן באמצעות יישום ארבעת העקרונות הקלאסיים של האסטרטגיה הצבאית, בשילוב רעיון החוסן. ייתכן שעקרונות אלה לא יספקו מענה מלא, כשם שהם אינם נותנים מענה מלא לאיומים אסימטריים וקונבנציונליים אחרים, ובהחלט אפשר שיידרשו התאמות על פי האתגרים הספציפיים שמציבים איומי הסייבר. עם זאת, בתחומים שבהם הוכחה יעילותם של עקרונות אלה, אנו משוכנעים שנראה פיתוח של יכולות חדשות במהלך הזמן, כפי שקורה תמיד כאשר מתעוררים איומים חדשים.

מחקר ופיתוח הם נקודת המפתח במאמץ לגבש את היכולות החדשות על בסיס ארבעת העקרונות הקלאסיים והעיקרון הנוסף – החוסן. מדינות מתקדמות כבר הצליחו במידה רבה להבטיח שמנגנוני ההגנה שלהן יהיו טובים יותר מהיכולות ההתקפיות שבידי הגורמים הלא מדינתיים. עם זאת, אין ביטחון שכך יהיה גם בעתיד, במיוחד אם מדינות ייטו לא להתייחס ברצינות לאיומים.

מאמר זה הוא מאמץ מקיף ראשון ליישם את המודל של "ארבעה עקרונות ועוד אחד" על איומי הסייבר, במטרה להפוך אותו למסגרת מושגית שתוכל להנחות אסטרטגיות של מדינות בתחום הסייבר. הסתמכות על המודל הבסיסי תאפשר פיתוח של תוכניות מפורטות יותר, שיתנו מענה לדרשות הספציפיות שמעוררים האיומים השונים. המאמר גורס כי שיפור המודיעין, הקניית חוסן לארכיטקטורת הסייבר והידוק שיתוף הפעולה בין הממשלה ובין המגזר הפרטי, וכן בזירה הבין לאומית, הם האמצעים המרכזיים ליישום עקרונות אלה. נדרש מחקר שיסייע בקביעת דרכים נוספות שיאפשרו להתאים או להרחיב את המודל גם לעולם הסייבר.

תגובה מידתית למתקפות סייבר

ז'רנו לימנל

מחקרים שנעשו בשנים האחרונות מראים כי קיים שוני ניכר בין תגובות של ממשלות שונות למתקפות סייבר. למרות לחצים פוליטיים משמעותיים "לעשות משהו" נגד מתקפות כאלו, ניסיון העבר מצביע על כך שרוב התגובות התבססו על מדיניות אד הוק. מצב זה מלמד כי מרחב הסייבר הוא זירת עימות חדשה יחסית, במיוחד עבור קובעי המדיניות, ולכן יש להפנות אליה תשומת לב מיוחדת; כי התגובות למתקפות סייבר הן סוגיה שעדיין לא נחקרה בצורה משביעת רצון; וכי יש צורך במחקר נוסף כדי להבין כיצד על מדינות לאום להגיב בצורה הטובה ביותר לפעולות עוינות בסייבר ובאילו כלים עליהן להשתמש לצורך זה.

מאמר זה מצביע, באמצעות ניתוח מקיף, על כך שיש להתייחס למתקפות סייבר כסוגיה פוליטית. הוא מספק מסגרת כללית שעליה יכולים להתבסס קובעי המדיניות, המשלבת בין השפעת האירוע ובין המדיניות האפשרית כלפיו, ומפרט חמישה משתנים שעליהם לשקול כאשר הם באים להעריך מהי התגובה ההולמת למתקפת סייבר. המאמר מתווה את דרכי הפעולה השונות של "פוליטיקת הסייבר" אותן ניתן ליישם כתגובה למתקפות קיברנטיות, כאשר מסגרת התגובה אמורה להיות חלק בלתי נפרד מצעדי ההרתעה של המדינה בתחום הסייבר.

מילות מפתח: אבטחת סייבר, מתקפות סייבר, לוחמת סייבר, אסטרטגיית סייבר, פוליטיקה, פוליטיקת סייבר, תגובה, ביטחון, לוחמה היברידית

מבוא

באוקטובר 2016 יצאו המשרד לביטחון המולדת ומשרד המודיעין הלאומי של ארצות הברית בהכרזה מרעישת, לפיה ממשלת רוסיה עומדת מאחורי מתקפה על

פרופ' ז'רנו לימנל מלמד ביטחון סייבר באוניברסיטת אלשו שבפינלנד.

הדואר האלקטרוני של יחידים ומוסדות בארצות הברית, כולל ארגונים פוליטיים,¹ וקבעו כי "הגניבות והחשיפות שנעשו נועדו להפריע לתהליך הבחירות בארצות הברית".² האשמה זו היא יוצאת דופן בשני היבטים. ראשית, במעשה עצמו: הפריצה הייתה סחריר (ספין) פוליטי משמעותי שנוסף לפריצות קודמות, וניתן לראות בה ניסיון ברור להשפיע על הבחירות לנשיאות באמצעות ניצול מרחב הסייבר. הפריצה גם הייתה תזכורת לאופן שבו מתקפות סייבר יכולות לערער את תפיסת הריבונות, לזרוע בלבול בקרב האוכלוסייה האזרחית ולטשטש את הגבולות בין מלחמה לשלום; ההיבט השני קשור לשאלת הייחוס. למרות שייחוס מוחלט של מתקפת סייבר הוא דבר קשה להשגה, במקרה זה קהילת המודיעין האמריקאית הודיעה כי אין לה ספק שהפריצות אושרו ברמות הגבוהות ביותר של הממשל הרוסי.³ האשמה פומבית ופוליטית ישירה זו מעידה על רמה גבוהה של ודאות לגבי הייחוס. גורמים רוסיים רשמיים הגיבו על כך בביטול ופטרו את ההאשמות כ"שטויות" שנועדו להצית היסטוריה אנטי-רוסית.⁴

שני ההיבטים שלעיל מעוררים את השאלה החשובה והמעניינת יותר: מה תהיה התגובה של ארצות הברית לפריצות אלו? כפי שאמר הנשיא הקודם ברק אובמה, מרחב הסייבר הוא "ים לא מוכר", שבו "אין, למשל, פרוטוקולים קובעים בנושאים צבאיים או בסוגיות הנוגעות למערכות נשק, נושאים וסוגיות שבהם נצבר ניסיון בשאלה מה מקובל ומה לא מקובל".⁵ המועמדת לנשיאות, הילרי קלינטון, הבהירה מצדה כי "ארצות הברית תתייחס למתקפות סייבר בדיוק כמו לכול מתקפה אחרת".⁶

1 ביולי 2016 פרסם אתר "וויקיליקס" הודעות דוא"ל מביכות שנלקחו מחשבונות המפלגה הדמוקרטית של ארצות הברית. פצחנים השיגו גישה מלאה לרשת ששימשה את צוות מטה הבחירות של המפלגה, לרבות דוא"ל, מזכרים ומחקרים שהתייחסו למועמדים הדמוקרטיים לקונגרס.

2 *Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security*, October 7, 2016, <https://www.dhs.gov/node/23199>.

3 *Assessing Russian Activities and Intentions in Recent US Elections*, Intelligence Community Assessment, January 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

4 Dmitry Solovyov, "Moscow Says U.S. Cyber Attack Claims Fan 'Anti-Russian Hysteria'", *Reuters*, October 8, 2016, <http://www.reuters.com/article/us-usa-russia-cyber-ministry-idUSKCN1280DO>.

5 *Remarks by President Obama and President Xi Jinping of the People's Republic of China after Bilateral Meeting*, The White House, June 8, 2013, <https://www.whitehouse.gov/the-press-office/2013/06/08/remarks-president-obama-and-president-xi-jinping-peoples-republic-china/>.

6 Andrew Blake, "Hillary Clinton: U.S. Will Treat Cyberattacks 'Just Like any Other Attack'", *Washington Times*, October 7, 2016, <http://www.washingtontimes.com/>

רבים בארצות הברית ובעולם המערבי קראו לממשל האמריקאי לפעול ולהבהיר לרוסיה כי מתקפת סייבר נגד התהליך הדמוקרטי תיענה בתגובה הולמת. ואכן, הנשיא אובמה אישר כי ארצות הברית שוקלת "תגובה מידתית" והוסיף כי עומד לרשותה מגוון של אפשרויות זמינות.⁷ ארצות הברית גם הצהירה כי התגובה "תהיה בזמן שנבחר, ובנסיבות שבהן תושג ההשפעה הגדולה ביותר".⁸ יחד עם זאת, הנשיא לא הבהיר מהי המשמעות של "תגובה מידתית" מבחינת הפעולה הקונקרטית. יותר מאוחר מסר הנשיא אובמה כי ארצות הברית תטיל סנקציות על תשעה גופים ואישים רוסיים ותגרש 35 דיפלומטים של רוסיה כתגובה על הפרצה וניסיון ההתערבות בבחירות. אובמה גם אמר כי ארצות הברית "תמשיך לנקוט מגוון פעולות" במועד ובמקום שתבחר, שחלקן לא יפורסמו בפומבי.⁹ אין ספק כי מדובר במצב חדש עבור הממסד הביטחוני האמריקאי וקובעי המדיניות בארצות הברית.

ההתערבות בבחירות לנשיאות ארצות הברית ושקילת תגובה למתקפת הסייבר הן רק דוגמה אחת לנושא שהמאמר הנוכחי עוסק בו, והיא מעוררת מספר שאלות ובהן: מדוע חשוב לנסח מסגרת לתגובה פוליטית על מתקפות סייבר בעידן הנוכחי ומה צריך להילקח בחשבון כאשר מחליטים על תגובה מידתית למתקפות סייבר? ניסיון ההתערבות בבחירות בארצות הברית הוא גם תזכורת לצורך הדחוף בפיתוח נורמות בין-לאומיות שיצמצמו את האפשרות למתקפות ולפעולות עוינות בסייבר, בעולם ההולך ונעשה יותר ויותר דיגיטלי.

רקע תיאורטי

ביטחון מרחב הסייבר הוא חלק בלתי נפרד מהביטחון, המלחמה והפוליטיקה של ימינו. לכן, חשוב להבין כי אין לבדוד מתקפות ופעילויות אחרות במרחב הסייבר מההקשר הפוליטי, האסטרטגי והגיאופוליטי הרחב יותר. לדוגמה, מרכיב הסייבר

news/2016/sep/1/clinton-us-will-treat-cyberattacks-just-any-other-/.
7

Julie Davis and Gardiner Harris, "Obama Considers 'Proportional' Response to Russian Hacking in U.S. Election", *New York Times*, October 11, 2016, <http://www.nytimes.com/2016/10/12/us/politics/obama-russia-hack-election.html>.

David E. Sanger, "Biden Hints U.S. Response to Russia for Cyberattacks", *New York Times*, October 15, 2016, <http://www.nytimes.com/2016/10/16/us/politics/biden-hints-at-us-response-to-cyberattacks-blamed-on-russia.html>.
8

Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment, The White House, December 29, 2016, <https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity>.
9

היה חלק בלתי נפרד במלחמה המתמשכת באוקראינה, ונתפס כהמשכה של הפוליטיקה באמצעים אחרים.¹⁰

כל פעולה מורכבת לרוב מחמש רמות: רמת המדיניות והמטרות; רמת האסטרטגיה; רמת המבצעים (כולל מערכות צבאיות); רמת הטקטיקות; רמת הכלים והאמצעים.¹¹ כל הרמות הללו הן חשובות, אך אנשי מקצוע בתחום הביטחון, העוסקים בשאלת ביטחון הסייבר, מתמקדים לעתים קרובות רק בטקטיקות ובכלים, וגם זאת במיוחד מבחינה טכנולוגית.

מאמר זה עוסק בתחום הסייבר בעיקר מנקודת המבט הפוליטית, וזאת בשל החשיבות הגוברת שיש לדבר בעולם המקושר של היום ובפוליטיקה הבין-לאומית. לשם דוגמה, נאט"ו הכיר במרחב הסייבר כמרחב מבצעי שבו על הארגון להגן על עצמו ביעילות, כפי שהוא עושה באוויר, ביבשה ובים.¹² נאט"ו גם פעל כדי שניתן יהיה להסתייע בסעיף 5 באמנת הארגון בתגובה להתקפות סייבר – מהלך שהוא החלטה פוליטית.

ניתוח של מתקפות הסייבר שהתרחשו בשנים האחרונות מראה שהתגובות הרשמיות להן שונות זו מזו במידה רבה.¹³ יש לחץ פוליטי ניכר "לעשות משהו" נוכח מתקפות סייבר, אך הניסיון מלמד כי רוב התגובות מתבססות על מדיניות אד הוק. מכאן נובע שתחום הסייבר הוא זירת עימות חדשה יחסית, במיוחד עבור קובעי המדיניות, ולכן הוא זקוק לתשומת לב מיוחדת; שהתגובות על מתקפות סייבר הן עדיין במידה רבה תופעה שלא נבחנה מספיק; וכי יש צורך במחקר נוסף כדי להבין מהי התגובה הטובה ביותר שמדינות לאום צריכות לאמץ לנוכח התקפות סייבר, ומהם הכלים שכדאי להשתמש בהם לצורך זה.

ככול שפעולות סייבר התקפיות הופכות לנפוצות יותר, כך גובר האתגר שניצב מול קובעי המדיניות לפתח תגובות מידתיות להתקפות שהן בעלות אופי של שיבוש או הרס. עם זאת, לפני שמגיבים יש להתחשב במספר משתנים שינותחו בהמשך. בסוף המאמר מופיע תרשים המציג מסגרת כללית הקושרת בין ההשפעות של מתקפת הסייבר ובין אפשרויות התגובה המדיניות, הסיכונים, הזמן, הייחוס והמידתיות,

10 גישה זו, ברוח דבריו של קלאוזוביץ, הינה שנויה במחלוקת, אך מתארת כיצד פוליטיקה ומלחמה כרוכות זו בזו. ראו למשל: Mary Kaldor, "Inconclusive Wars: Is Clausewitz Still Relevant in these Global Times?", *Global Policy* 1, no. 3 (2010): 271-281.

11 Richard Bejtlich, "Strategic Defence in Cyberspace: Beyond Tools and Tactics", in *Cyber War in Perspective: Russian Aggression Against Ukraine*, ed. Kenneth Geers (Tallinn: NATO CCDCOE, 2015), pp. 159-170.

12 *Warsaw Summit Communiqué*, NATO, July 9, 2016, http://www.nato.int/cps/en/natohq/official_texts_133169.htm.

13 Sico Van der Meer, "Signaling as a Foreign Policy Instrument to Deter Cyber Aggression by State Actors", *Clingendael*, December 2015, https://www.clingendael.nl/sites/default/files/PB_Signalling_as_a_foreign_policy_instrument_SvdM.pdf.

ומשרטטת בהתאם לכך את המנופים השונים העומדים לרשות "פוליטיקת הסייבר", אותם ניתן ליישם בתגובה לאירועי סייבר מסלימים. מסגרת זו, המהווה ניתוח של "התוצאה הסופית" של פעולות התגובה, יכולה לשמש כבסיס להחלטה אצל קובעי המדיניות.

חשיבות הפוליטיקה בעולם הסייבר

בדיקת הגבולות

מתקפות של פצחנים (בין אם "ממשלתיים" ובין אם לאו) על המערכות הדיגיטליות שבהן תלויות מדינות לקבלת שירותים חיוניים, לשמירת השגשוג הכלכלי ולביטחון, הפכו בעשור האחרון למתוחכמות יותר ויותר. הפריצות למערכות אלו יצרו איום על תשתיות קריטיות, על קניין רוחני, על הפרטיות של המשתמשים, על מידע חשוב בתחום הביטחון הלאומי ועל נתוני כוח אדם. ההתקדמות הטכנולוגית והתלות הגוברת במרחב הסייבר הפכו את ביטחון הסייבר, כמו גם את הצורך בכללים ובגישות משותפים בסוגיה זו, לנושא מרכזי וחשוב. במקביל, המושגים של התקפה, הגנה, הרתעה, שיתוף פעולה בין-לאומי וריגול קיבלו משמעות חדשה. ההסתמכות המוגברת על התשתית הדיגיטלית ופגיעותה להתקפות סייבר הובילו ממשלות וגורמים לא מדינתיים לנצל את מרחב הסייבר כדי לתת ביטוי להבדלים הגיאופוליטיים ביניהם ולקדם את מטרותיהם הפוליטיות. משמעות הדבר היא גם התחזקות חשיבותה של "הלוחמה הלא קינטית".

זה זמן רב קיים צורך בדיונים ברמה הלאומית והבין-לאומית על התקפות סייבר והתגובה להן, אלא שדיונים כאלה לא התקיימו למרות ההכרה הרחבה לה זוכה החשיבות האסטרטגית של המרחב הדיגיטלי. נכון להיום, "כללי המשחק" הפוליטיים בסייבר עדיין מעטים, אף שהם הולכים ורבים מדי יום. זאת, כתוצאה ממעבר העולם לשימוש אסטרטגי גובר בנשק הסייבר ככלי להביא לשינוי התנהגותו של היריב.

מדינות ושחקנים לא מדינתיים כאחד בוחנים כיום את גבולות "שדה הקרב בסייבר", כאשר מספר פעולות הסייבר הנראות והבלתי נראות הולך וגובר, רמת התחכום שלהן עולה, ודרכים חדשות לנצל את מרחב הסייבר נסללות ומיושמות. בדצמבר 2015 היינו עדים להתקפה המאומתת הראשונה שנועדה להשבית רשת חשמל, אשר השפיעה על כ-225,000 אזרחים באוקראינה.¹⁴ יכולות הסייבר הולכות ומשתכללות, וכך גם הרצון והנכונות להשתמש בהן, ודומה שאין לנו מושג כיצד להתמודד עם המציאות החדשה.

¹⁴ "Analysis of the Cyber Attack on the Ukrainian Power Grid", E-ISAC, March 18, 2016, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

עליית פוליטיקת הסייבר

נושאים הקשורים לסייבר ולשימושיו חדרו בשנים האחרונות לרמה הגבוהה ביותר של הפוליטיקה. זאת, לעומת העבר, כאשר מרחב הסייבר נחשב בעיקר לסוגיה הקשורה לפוליטיקה ברמה נמוכה, שבמרכזה נושאי רקע ותהליכים. ביטחון הסייבר הפך כיום למוקד של התנגשות אינטרסים, הן מקומיים והן בין-לאומיים, ולזירה שבה מוקרנת עוצמתן של מדינות.¹⁵

חשוב להבין כי מרחב הסייבר הוא מרחב פוליטי, במיוחד לאחר שתובנה זו נזנחה ונשכחה לעתים קרובות. כאשר בוחנים את מרחב הסייבר מנקודת המבט של מדינת הלאום, מגלים שהשאלות המרכזיות של מרחב זה כיום הן פוליטיות מאוד. לפיכך, יש להתייחס לתחום הסייבר כאל זירה פוליטית בעיקרה, כפי שקורה ביחס לתחומים אחרים. כאשר קיימת מעורבות פוליטית, מתעוררות תמיד גם שאלות הקשורות לכוח. לדוגמה, בהקשר של מלחמה, כלי הסייבר דומה לעוצמתם של כוחות היבשה, הים או האוויר ומשמש כמוהם אמצעי להשגת מטרה פוליטית או לצבירת כוח. זוהי הסיבה להתגברות השימוש האסטרטגי במרחב הסייבר להשגת מטרות פוליטיות ויתרונות גיאואסטרטגיים.

התפתחותו של מרחב הסייבר והתלות העמוקה שלנו בו יוצרות זירה חדשה להתנהלות הפוליטית. יותר מכך, אפשר שאנו עדים להיווצרות צורה חדשה של פוליטיקה. מדובר בתהליך שזכה לכינוי "סייברזיצה",¹⁶ המתייחס לחדירתם של ממדים שונים של סייבר לכול תחומי הפוליטיקה. זו גם הסיבה לשימוש הנרחב הנעשה כיום במושג "פוליטיקת סייבר".¹⁷

פוליטיקת סייבר מתייחסת להתלכדות של שני סוגי תהליכים: התהליכים הנוגעים לפוליטיקה של קביעת "מי מקבל מה, מתי ואיך"; התהליכים העושים שימוש במרחב הסייבר, כלומר, זירה של אינטראקציות דיגיטליות. הפוליטיקה בזירה הפיזית ובזירת הסייבר גם יחד כרוכה בעימותים, במשא ומתן ובמיקוח על מנגנונים, ממוסדים או אחרים, מתוך מטרה לפתור באופן מוסמך מחלוקות סביב נושאי ליבה. לכן, ניתן לומר שכאשר מדינות שוקלות תגובות מידתיות למתקפות סייבר, הדבר הופך את פוליטיקת הסייבר למוחשית.

Jelle Van Haaster, "Assessing Cyber Power", in *8th International Conference on Cyber Conflict: Cyber Power*, eds. N. Pissaniadis, H. Rõigas and M. Veenendaal (Tallinn: NATO CCD COE, 2016), pp. 7-22.

Jan-Frederik Kremer and Benedikt Müller, eds., *Cyberspace and International Relations, Theory, Prospects and Challenges* (London: Springer, 2014) pp. xi-xvii.
Nazli Choucri, "Cyberpolitics in International Relations", in *Oxford Companion to Comparative Politics*, ed. Joel Krieger (New York: Oxford University Press, 2012), pp. 267-271.

פוליטיקת סייבר מיושמת בעיקר על ידי אנשי אקדמיה המעוניינים לנתח את השימוש שנעשה במרחב הסייבר לצורך פעילות פוליטית, ובכלל זה את היקפו ועומקו של שימוש זה. למרות שפוליטיקת הסייבר קיימת הן ברמה הלאומית והן ברמה הבין-לאומית, ונושאי הסייבר מצויים בלב מדיניות החוץ והביטחון של מדינות, פוליטיקת הסייבר ועולם הסייבר יצרו תנאים חדשים שאין להם תקדים. התכנים האמיתיים של פוליטיקת הסייבר ייחשפו בשנים הקרובות, וסביר להניח שאז נוכל לחזור להשתמש במושג "פוליטיקה" בלבד. זאת, מתוך הנחה שענייני הסייבר יהיו חלק בלתי נפרד מהפוליטיקה, שכן תחום הסייבר אינו שונה, בסופו של דבר, מהמסגרות המקובלות שלה.

נורמות סייבר גלובליות נמצאות עדיין בחיתוליהן

ב־2015 ניסתה קבוצה של מומחים באו"ם לפתח כללים בתחום המידע והטלקומוניקציה בהקשר של ביטחון בין-לאומי.¹⁸ הדוח שהם כתבו הרחיב באופן משמעותי את הדיון בסוגיה גם לנורמות, לכללים ולאמצעים לבניית אמון במרחב הסייבר. קבוצת המומחים המליצה כי מדינות ישתפו פעולה ביניהן כדי למנוע שימוש מזיק בסייבר, וקבעה כי עליהן למנוע שימוש ביודעין בטריטוריה שלהן לביצוע פעולות בין-לאומיות פוגעניות באמצעות טכנולוגיות מידע ותקשורת (ICT). אחת ההמלצות החשובות של הקבוצה גרסה שהמדינה אינה צריכה להוביל פעילות בתחום טכנולוגיות המידע והתקשורת שכוונתה לפגוע או לשבש בדרך אחרת את השימוש והתפעול של תשתיות קריטיות, או לתמוך ביודעין בפעילות כזו. דוח מומחי האו"ם הדגיש כי "הפיכת מרחב הסייבר ליציב ובטוח יכולה להתבצע רק באמצעות שיתוף פעולה בין-לאומי", וחייב את המדינות לנקוט אמצעים מתאימים כדי להגן על התשתיות הקריטיות שלהן. עם זאת, הדוח לא כלל הנחיות לתגובה, במיוחד על התקפות סייבר שנעשות בחסות מדינות. כמו כן נכתב בדוח כי העובדה שמקורה של מתקפת סייבר הוא בשטחה של מדינה מסוימת, או שמתקפה כזאת שוגרה מתשתית של טכנולוגיות מידע ותקשורת הנמצאות בתחומה, אינה מספיקה כדי לייחס אותה לאותה מדינה.¹⁹

למדינות שמורה זכות טבעית להגנה עצמית לפי סעיף 51 של מגילת האו"ם במצבים של איום ממשי עליהן. לפיכך, התנהגות המדינה במרחב הסייבר צריכה גם היא לעלות בקנה אחד עם הנאמר במגילת האו"ם. עם זאת, האתגר של קביעת הייחוס ושל הבנת היקף הנזק ממתקפה ברשת עלול לסבך את המצב. הזכות להגנה

¹⁸ "Developments in the Field of Information and Telecommunications in the Context of International Security", United Nations General Assembly, July 19, 2016, http://www.un.org/ga/search/view_doc.asp?symbol=A/71/172.

עצמית, ובכלל זה לשימוש בכוח, תחול אם מתקפת הסייבר תגיע לרמה של "התקפה חמושה", אך הדיון המשפטי על מה מהווה "התקפה חמושה" במרחב הסייבר נמצא רק בראשיתו. בכול מקרה, ניתן לשער כי פעולה עוינת בסייבר, אותה ניתן לייחס למדינה, יכולה להיחשב כהפרה של סעיף 2 (4) של מגילת האו"ם, וזאת בהתאם לאופייה ולתוצאותיה.²⁰ הדבר גם מעורר את השאלה הכללית כיצד יש להעריך את השפעתה של מתקפת סייבר, במיוחד כאשר לא נגרם בעקבותיה נזק פיזי. מתקפת סייבר לא צריכה לגרום בהכרח לנזק פיזי כדי להיחשב לחמורה. הרס פיזי זוכה להדגשה רבה, אולי בגלל המסורת הארוכה של עיסוק בביטחון פיזי, וגם משום שהשלכות פיזיות ברורות יותר לעין. לכן, דרך החשיבה הישנה היא שמתקפת סייבר "חמורה" צריכה לכלול הרס פיזי, כולל מוות ופגיעה בתשתיות קריטיות. עם זאת, ככול שאנו נעשים תלויים יותר ויותר בנתונים ובנכסים לא קינטיים, נשאלת השאלה האם יש להתייחס למניפולציה על רשומות בריאותיות או פיננסיות, למשל, באותה רמה של חמורה כמו להשלכות פיזיות.²¹ יתרה מכך, יש לשאול האם קיים הבדל בין מניפולציה על נתונים בנקאיים ובין מניפולציה על נתונים בריאותיים, כשהראשונה עלולה לגרום לשיבושים כלכליים חמורים, אך האחרונה עלולה לגרום במקרים קיצוניים למוות. התשובה לכך לא ברורה. כמו כן, לא ברור מה המשמעות בפועל של מתקפת סייבר "רחבת היקף". חשוב להבין שהתשובה לשאלה האם התקפת סייבר היא מעשה מלחמה או לא, היא במהותה החלטה פוליטית.

חמישה משתנים

בבואם לקבוע מהי התגובה הראויה למתקפת סייבר, על קובעי המדיניות לשקול את חמשת המשתנים הבאים, המהווים שאלות שיש להשיב עליהן לפני החלטה על תגובה.

מי עשה את זה?

ייחוס מתקפת סייבר לנותן החסות – השחקן המדינתי או הלא מדינתי שמאחורי ההתקפה – נותר אתגר משמעותי, שכן הוא מחייב אמצעים יעילים ויכולת לזהות את העומדים מאחורי ההתקפה. בעיית הייחוס מורכבת ביותר ולא תמיד ניתנת

²⁰ סעיף 2 (4) של מגילת האו"ם קובע: "במסגרת היחסים הבין-לאומיים שלהן, יימנעו כל המדינות החברות מאיום או משימוש בכוח נגד השלמות הטריטוריאלית או העצמאות המדינית של מדינה כלשהי, או מכול התנהגות אחרת שאינה עולה בקנה אחד עם מטרת האומות המאוחדות".

²¹ Jarno Limnéll and Charly Saloni-Pasternak, "Challenge for NATO – Cyber Article 5", Briefing Paper, Center for Asymmetric Threat Studies, Swedish Defense University, June 2016.

לפתרון. מרחב הסייבר מאפשר מידה רבה של אנונימיות, וניתן לנתב התקפות דרך שרתים בכול רחבי העולם כדי להסוות את מקורן. ייחוס שגוי של המתקפה עלול להוביל לתגובה שתהיה מכוונת אל יעד לא נכון. כאשר בוחנים את סוגיית התגובה המידתית, על קובעי המדיניות לדעת מה רמת הביטחון שבידם לגבי ייחוס המתקפה.²² לדוגמה, אם רמת הביטחון בייחוס היא נמוכה, מקבלי ההחלטות יהיו מוגבלים בבחירת התגובה שלהם, גם אם חומרת הפגיעה היא גבוהה. על מדינות לחשב את העלויות הכרוכות בייחוס שגוי של מתקפה ולשקול את העלויות הפוטנציאליות של הסלמה. לפיכך, מידת ודאות הייחוס משפיעה על הפעולה שתניקט.

היכולת לייחס מתקפה למקור מסוים חשובה לצורך שמירה על האמינות ולהבטחת הלגיטימיות מבית ומחוץ. האתגר נובע מכך שניתן לאסוף ראיות מספיקות לייחוס באמצעות מקורות מידע מודיעיניים חשאיים או דרך מדינות ידידותיות, אך לרוב המדינה אינה מעוניינת לחשוף את מקורות המודיעין הללו בפומבי. עם זאת, אם מדינה רוצה לבנות לגיטימציה בין-לאומית לפעולת התגמול שהיא נוקטת, חיוני שתפרסם הוכחה כלשהי לקביעת הייחוס.

לייחוס יש היבטים רבים, כולל טכניים, משפטיים ופוליטיים. זהו נושא רב-ממדי הדורש ניתוח של מקורות מידע רבים, כולל ממצאים פורנזיים, דוחות מודיעין אנושי, מודיעין אותות, היסטוריה וגיאורפוליטיקה. כפי שטוענים ריד וביוקנון, הייחוס הוא תרגיל של צמצום אי-הוודאות בשלוש רמות: הרמה הטקטית, שבה הייחוס הוא אמנות לא פחות ממדע; הרמה המבצעית, שבה הייחוס הוא תהליך מורכב ולא בעיה של שחור-לבן; הרמה האסטרטגית, שבה הייחוס הוא פונקציה של מה מונח על כפות המאזניים מבחינה פוליטית.²³ ייחוס מוצלח דורש מגוון של כישורים בכול הרמות, ניהול זהיר, עיתוי, מנהיגות, בדיקת יכולת העמידה בלחץ, תקשורת שקולה והכרה במגבלות ובאתגרים. אמנם, העניין הרב של מומחי הביטחון ברמות השונות של הייחוס הביא להגברת היכולת לייחס מתקפות, אך ההחלטה הסופית לגבי הייחוס לצורך נקיטת צעדי תגובה היא תמיד פוליטית.

מה ההשפעה?

על קובעי המדיניות להבין מה הייתה השפעת מתקפת הסייבר, שכן זו תקבע את סוג התגובה ורמתה. כמה מהשאלות שיש לשאול בהקשר זה הן: כמה מזיקה הייתה הפגיעה בביטחון הלאומי ובחברה? איזה סוג של שירותים נפגעו או הושפעו

Tobias Feakin, "Developing a Proportionate Response to a Cyber Incident", *Council on Foreign Relations*, August 2015, <http://www.cfr.org/cybersecurity/developing-proportionate-response-cyber-incident/p36927>.

Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks", *Journal of Strategic Studies* 38, no. 1-2 (2014): 4-37.

מהתקיפה? האם ההתקפה גרמה לאובדן משמעותי של אמון במוניטין של המדינה? הניתוח יכול לקחת שבועות, אם לא חודשים או שנים, עד שמומחי מחשבים יקבעו במדויק את היקף הנזק שנגרם לרשתות המחשב של הארגון שהותקף. כך, למשל, נדרשו לשלטונות ערב הסעודית כשבועיים כדי להבין את היקף הנזק שנגרם מההנוזקה Shamoon, אשר מחקה נתונים של 30,000 מחשבים בחברת "אראמקו" הסעודית. לעתים קורה שחברות או ארגונים ממשלתיים מבינים שנפרצו רק חודשים או שנים לאחר מעשה.

ברור שקל יותר להעריך השפעה פיזית של מתקפה. כאשר ההשפעות של מתקפת סייבר לא תמיד ברורות, קשה למקבלי ההחלטות לקבוע אם הפעולה העוינת היא ברמה של התקפה ואם נדרשת תגובה. יש דוגמאות רבות למתקפות סייבר שכשלו בהשגת המטרה, והפכו למטרד או לסוג של פעולת ריגול רגילה למדי.²⁴ חישוב מידתיות התגובה למתקפת סייבר הוא אתגר הנובע מרמת החשאיות של המתקפה ומהמהירות בה בוצעה. ככלל, קשה לקבוע את סדר הגודל של מתקפת סייבר ואת השלכותיה, מה גם והמידע הדרוש כדי להבין השלכות אלו יכול גם הוא להיות קשה להשגה. לדוגמה, מוסדות פיננסיים וחברות פרטיות עשויים לסרב לספק מידע על הנזק שנגרם להם בשל שיקולים של סודיות עסקית.²⁵

אילו כלים יכולים לשמש בתגובה?

כאשר בוחנים תגובה מידתית למתקפות סייבר, ההחלטה היא תמיד נגזרת של האפשרויות העומדות לרשות המדינה. נהוג לומר שלכול מדינה יש לפחות ארבעה כלים לתגובה: דיפלומטיה (כלומר, כלי מדיניות חוץ, כגון תקשורת דיפלומטית, אזהרות וסנקציות), כלי מידע, צבא וכלכלה.²⁶ על קובעי המדיניות לשקול את מלוא טווח התגובות העומד לרשותם, החל מנזיפה דיפלומטית שקטה ועד מתקפה צבאית. אין סיבה להניח שתגובה מידתית לפעולה עוינת בסייבר צריכה להיות מוגבלת רק למרחב הסייבר. אדרבא, אין להגביל את התגובה למרחב הסייבר בלבד ואין דבר המונע מהמדינה מלהשתמש באמצעים אחרים, אם כי כל אחד מאמצעים אלה נושא את הסיכונים הפוליטיים שלו. מערכת הביטחון האמריקאית אף הציעה שארצות הברית לא תשלול תגובה גרעינית במקרה של מתקפת סייבר קיצונית במיוחד.²⁷

James Stavridis, "How to Win the Cyberwar against Russia", *Foreign Policy*, 24 December 12, 2016, <http://foreignpolicy.com/2016/10/12/how-to-win-the-cyber-war-against-russia/>.

Marco Roscini, *Cyber Operations and the Use of Force in International Law* (New York: Oxford University Press, 2014).

Timothy Thomas, "Creating Cyber Strategists: Escaping the 'DIME' Mnemonic", 26 *Defence Studies* 14, no. 4 (2014): 370-393.

Task Force Report: Resilient Military Systems and the Advanced Cyber Threat, 27 Department of Defense, Defense Science Board, January 2013, <http://www.dtic>.

בדרך כלל מקובל שתגובות קינטיות מותרות רק כאשר להתקפה יש כוונות קטלניות ואם היא גרמה לסבל אנושי או לאובדן חיים, או הייתה הפרה מפורשת של זכויות אדם.²⁸ עם זאת, כשעוסקים בחברות שהדיגיטציה בהן הולכת וגוברת, מדובר בגישה צרה מדי, כפי שנטען בראשיתו של מאמר זה. בכול מקרה, נכון להיום, קשה להצדיק תגובה צבאית למתקפת סייבר, אם זו לא גרמה נזק פיזי במובן המקובל.²⁹

הסוגיה המרכזית בהקשר זה היא הצורך לשקול אילו אמצעי נגד (פיזיים, בסייבר או אחרים) יכולים לשמש כחלק מ"ארסנל התגובה" של מדינת הלאום ואילו מהם צריכים לשמש בכול אחד מהמקרים. זוהי שאלה של מינוף העוצמה הלאומית העומדת לרשות המדינה ונכונותה להשתמש בה. תגובה להתקפות סייבר עשויה להתבצע בצורה גלויה או בחשאי. אם נבחרו שיטות סייבר, קשה יהיה לפתח תגובה חשאית במהירות, אלא אם הממשלה כבר בנתה מראש יכולות נגד יעד מסוים. במקרה כזה, סביר להניח שיכולות אלו יסתמכו על ריגול סייבר קודם ועל לימוד נקודות התורפה של המטרה. מנגד, תגובה פחות חשאית תורמת להרתעה גם נגד מדינות אחרות.

לתגובות סייבר גלויות יש גם חסרונות: מדינות עשויות לאבד את היכולת לשגר תגובות סייבר דומות נגד מטרות אחרות בעתיד, והן גם חושפות את עצמן לתגובה נגדית. אם התגובה גלויה לציבור, היא צריכה להיות מלווה גם בנרטיב של צדק ולא של נקמה. מדינות יכולות גם לבחור להפקיד את פעולת התגובה בידי קבוצות פצחנים חיצוניות הפועלות כשלוחה שלהן (proxy). עם זאת, שימוש בדרך זו עשוי להגבילן בשליטה על התגובה ואולי אף לגרור אותן לפעולות מסלימות.

מהן הנחיות המדיניות?

על קובעי המדיניות לשקול את אסטרטגיית הביטחון הלאומי ואבטחת הסייבר הקיימות, המתוות את הקווים המנחים של המדיניות הכללית של המדינה בכול הנוגע לנכונותה הפוליטית לפעול ולמנף את כוחה. אם המדינה חברה בבריתות ובארגונים בין-לאומיים, יהיה עליה לשקול גם את הנחיות המדיניות של ישויות אלו בבואה לגבש את התגובה המידתית, אחרת ניתן יהיה להאשים אותה שאינה מקיימת את המדיניות המוסכמת המשותפת. כאמור, מרחב הסייבר אינו חסין בפני הנורמות המשפטיות המחייבות את אומות העולם להגיב באופן מידתי על התקפה.

mil/get-tr-doc/pdf?AD=ADA569975.

28 ראו למשל: Thomas Wester, "Just Cyberwar", Cyber Security Policy and Research Institute, The George Washington University, November 24, 2014.

29 Patrick Lin, Neil Rowe and Fritz Allhoff, "Is it Possible to Wage a Just Cyberwar?", *Atlantic*, June 5, 2012, <http://www.theatlantic.com/technology/archive/2012/06/is-it-possible-to-wage-a-justcyberwar/258106/>.

מתקפת סייבר יכולה לגרום לכך שקובעי המדיניות יחליטו על תגובת יתר. מספר מומחי סייבר העריכו כי הסכנה לתגובת יתר היא ממשית מאוד ולכן על מקבלי ההחלטות לשקול בזירות כל הסלמה אפשרית לפני שהם מגיבים. ליביצקי טוען בהקשר זה כי על מקבלי ההחלטות להבין מה מונח על כפות המאזניים, כלומר, מה הם מקווים להרוויח מתגובה בשיטה כזו או אחרת.³⁰

למומחי ביטחון סייבר עשוי גם להיות תמריץ להאדיר את איום מתקפות הסייבר, שבתורו יגביר את הסיכון לתגובת יתר. גם אם הלחץ הפוליטי בעקבות מתקפת סייבר הוא רב, דרושה זהירות פוליטית, ולפחות יש לעודד רמה מסוימת של איפוק. איפוק עצמי הוא מושג הרלוונטי למניעת הסלמה במצב, במיוחד אם נשקלת תגובה קינטית. ככלל, כדי להרתיע מפני הסלמה, על היריב להאמין שתוצאת ההסלמה תהיה הרבה יותר גרועה מזו של האיפוק. איפוק יכול לעתים להיות אמצעי חזק יותר לביטוי עוצמה לאומית.

עד כמה דחופה התגובה?

הזמן הוא נושא רלוונטי בפוליטיקה. הלחץ הפוליטי להגיב מתגבר במיוחד כאשר תוצאת מתקפת הסייבר נחשפת בפומבי וזהות התוקף מוכרזת רשמית. תגובה שאינה מהירה מספיק יכולה להביא לפגיעה במוניטין ובאמינות הפוליטית. יריבים פוליטיים עשויים גם הם להפעיל לחץ "לעשות משהו". רמת ודאות נמוכה של הייחוס עשויה לשמש כתירוץ לא לעשות דבר.

מסגרת לתגובה

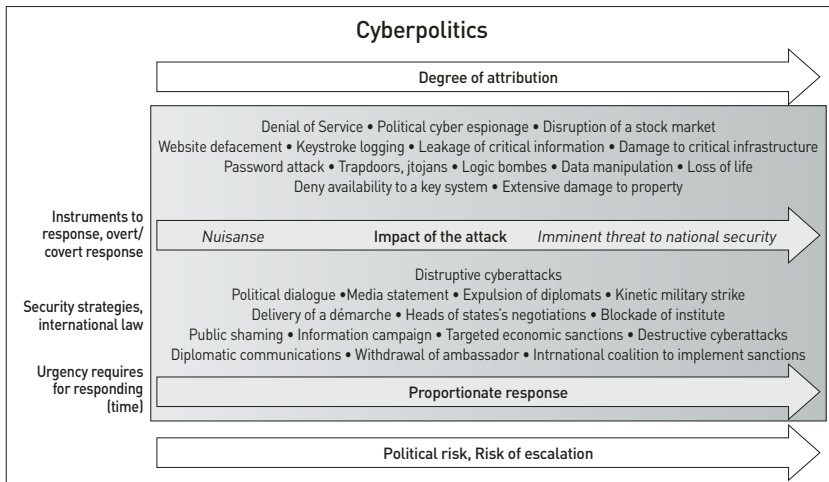
פעולות עוינות בסייבר מציבות ממשלות בפני תהליך מורכב של קבלת החלטות, החל מהבנת רמת הייחוס וחומרת הפגיעה ועד הערכת התגובה המידתית הראויה והסיכונים הכרוכים בנקיטת דרכי פעולה מסוימות. מקבלי ההחלטות גם חייבים להעריך את היכולות של הכלים הקינטיים והלא קינטיים שבידיהם, וזאת במצב של לחץ זמן ושל לחץ פוליטי גובר. פסיביות מול מתקפת סייבר עלולה לעודד יריבים להיות יותר אגרסיביים.

קובעי המדיניות צריכים להיות פרואקטיביים בקביעת אפשרויות התגובה המתאימות. פיתוח מסגרת תגובה למתקפות סייבר יאפשר לקובעי המדיניות לשקול פתרונות במהירות ולאמץ אופציות שכבר נותחו מבחינת יתרונות והשלכות אפשריות. זיהוי מראש של התגובה הראויה יכול לחסוך למדינה טעויות העלולות לסכן שלא במתכוון אינטרסים פוליטיים, כלכליים, מודיעיניים וצבאיים. למרות

Martin C. Libicki, "Cyberwar Fears Pose Dangers of Unnecessary Escalation", 30 *RAND Review*, Summer 2013, <http://www.rand.org/pubs/periodicals/rand-review/issues/2013/summer/cyberwar-fears-pose-dangers-of-unnecessary-escalation.html>.

שכול תגובה היא ספציפית למקרה (תלוית מצב), המסגרת תאפשר לקובעי המדיניות לשקול במהירות את האפשרויות העומדות לרשותם.

תרשים 1 מציג דוגמה כללית למסגרת שעל קובעי המדיניות לבנות כדי לקבוע את התגובות הפוטנציאליות לפעולה עוינת בסייבר עוד לפני שזו התרחשה. המסגרת נותנת למקבלי ההחלטות בסיס לביצוע הערכות לגבי המהלך שיש לנקוט בעת משבר. בעזרת שילוב של מידת הייחוס, השפעת האירוע, האפשרויות המדיניות, הסיכונים, אסטרטגיות הביטחון, הדין הבין-לאומי, הדחיפות והמידתיות, מתוארים המנופים השונים של פוליטיקת הסייבר שיש ליישם כתגובה לרמות ההסלמה וחומרת ההתקפה. מטרתה של המסגרת (שמוצגת כאן בהפשטה מכוונת) היא להמחיש את ההיבטים השונים שעל קובעי המדיניות לנתח בזיהור כאשר מדינה שוקלת מגוון אפשרויות ותגובות למתקפת סייבר, כולל החלטה לא לעשות דבר. על פי המסגרת, ככול שמתקפת הסייבר חמורה יותר, כך התגובה צריכה להיות חזקה יותר. המסגרת מדגימה את השפעתה וחומרתה של מתקפת סייבר, כאשר הפלת אתר נמצאת בקצה אחד של הסולם ואובדן חיים – בקצה השני. ממד זה מנותח כנגד רמת התגובה, שנעה מהצהרות לתקשורת ועד תגובה צבאית. אפשרויות התגובה יכולות להיות חשאיות לחלוטין ו/או גלויות לחלוטין, ולעשות שימוש בכלים שונים. קשת התגובות מציגה הן את הסיכונים הפוליטיים והמשפטיים הטבועים בכול החלטה והן את העלייה בסיכון במקביל לעלייה ברמת התגובה.



תרשים 1: מסגרת תגובה פוליטית

על פי Feakin, קובעי המדיניות צריכים להבין היטב את העלויות הכרוכות בכול תגובה.³¹ לכול תגובה תהיה השפעה על היחסים הדיפלומטיים, המוניטין, העוצמה והפעולות הצבאיות והמודיעיניות של המדינה. ההשלכות צריכות להיות ברורות לפני בחירת התגובה. הערכת האופציות מחייבת תשומות מצד גורמים ממשלתיים רלוונטיים, וכן מצד חברות פרטיות שפעילותן ועסקיהן עשויים להיות מושפעים מהתגובה.

אין לפרש את המסגרת כ"קווים אדומים" פוליטיים לתגובות מסוימות. שני ממדים צריכים להילקח בחשבון בעת קביעת "קווים אדומים" לגבי פעולות עוינות בסייבר: מצד אחד, "קו אדום" מזמין יריבים לפעול מתחת לו, מתוך מחשבה שהם ייהנו מחסינות או מסיכון פוליטי נמוך בביצוע פעולות מסוג זה. "קווים אדומים" גם יכולים לדחוף מדינה לפינה, כך שתאלץ להגיב כאשר הקו נחצה כדי לשמור על אמינותה. לפיכך, יש להניח שמדינות יעדיפו לא להיות ספציפיות מדי בעת שהן משתפות את הציבור בתגובותיהן האפשריות לחציית "קווים אדומים"; מצד שני, קביעת "קווים אדומים" היא מסר חזק של הרתעה ליריביה של מדינה, שמבהיר כי המדינה תגיב אם הגבול שנקבע ייחצה. מידה מסוימת של עמימות עשויה להיות הפתרון הטוב ביותר מבחינה פוליטית: המדינה מודיעה כי תהיה תגובה, אך אינה חושפת את פרטי התגובה מראש.

מסקנות

עולם הסייבר מעצב יותר ויותר את סביבת הביטחון העולמית ואת הדינמיקה של הכוח בין מדינות ושחקנים אחרים. במקביל, יכולות הסייבר הולכות ומשתכללות. העולם נכנס לעידן לא יציב ולא ודאי, ועושה זאת ללא מפת דרכים ברורה של עקרונות פוליטיים. מדינות המבקשות להגיב על פעולות עוינות בסייבר מנסות לנווט בגבולות המקובל והמידתי. כאשר מדינות מנסות לקבוע מהי הדרך המידתית להגיב לסוגים שונים של מתקפות ברשת, גובר הצורך שלהן בהבנה פוליטית ובמחויבות פוליטית. כשמדובר בביטחון סייבר, פעמים רבות מדי מושם דגש על הפרטים הטכניים, מבלי להבין את ההקשר הפוליטי. בסופו של דבר, ההחלטה אם התקפה ברשת היא מעשה מלחמה או משהו אחר היא קביעה פוליטית, בייחוד במקרים הנמצאים בתוך "השטח האפור" שבין התקפה שתוצאתה היא שיבוש בלבד ובין התקפה המנסה לשים קץ לעצם קיומה של מדינה.

נדרשות מומחיות פוליטית ובקיאיות בנושאי סייבר כדי לפעול כיום בתוך "סביבת ביטחון היברידי ובלתי צפויה". אין ספק שהחשיבות של פוליטיקת הסייבר תגדל בשנים הקרובות. יותר מכך, קובעי המדיניות יאלצו להמשיג מחדש

Feakin, "Developing a Proportionate Response to a Cyber Incident". 31

את המונחים "לוחמת סייבר" או "עימות סייבר" ולראות בהם צורה של "לוחמה היברידית" המתנהלת גם בימי שלום.

הפרוטוקולים המשמשים כיום למתן מענה לפעולות עוינות בסייבר אינם ברורים, ויש לפרש מצב זה כהיעדר עוצמה מספקת להתמודד עם מרחב זה. מאמר זה ביקש להציג מסגרת לתגובה פוליטית על מתקפות סייבר, שתשמש כנקודת מוצא לממשלות ולמקבלי החלטות לגיבוש דרכי פעולה ותגובות ספציפיות לכול מדינה. הלחץ הצפוי על ממשלות להגיב על התקפות סייבר מחייב את קובעי המדיניות לפתח מסגרת תגובה הולמת קודם להתרחשותן של פעולות עוינות או הרסניות במרחב הסייבר. המסגרת שהמאמר הציע מציגה את המשתנים העיקריים שיש לקחת בחשבון בעת גיבוש תגובה להתקפת סייבר. היא גם מעודדת ממשלות לפתח את מוכנותן ויכולותיהן כדי לגבש תשובות לשאלות המוצגות במסגרת המוצעת, וזאת לפני שיחליטו כיצד להגיב.

הכנת מסגרת לתגובה פוליטית אין פירושה שייעשה בה שימוש בדיוק באותה דרך. סיבה אחת לכך היא התפתחותן הרצופה של שיטות חדשות לניצול מרחב הסייבר. בפוליטיקה וגם בפוליטיקת הסייבר נשמרת תמיד גמישות, וזאת בהתאם לזהותם של מקבלי ההחלטות ולעמימות המצב. מאחר שלכול מדינה יש מאפיינים תרבותיים, פוליטיים וצבאיים משלה, כל מדינה צריכה לפתח מסגרת מדיניות מותאמת לה. מה שנכון למסגרת לאומית אחת, אינו נכון בהכרח למסגרת לאומית אחרת.

התכסית האנושית ומודיעין תרבותי במבחן המלחמות העכשוויות

קובי מיכאל ועומר דוסטרי

מאמר זה מבקש לתאר ולהגדיר את תפיסת התכסית האנושית, שהתפתחה בצבא האמריקאי לאור ניסיונו באפגניסטן ובעיראק. המאמר יעמוד על הסיבות שהובילו את הצבא האמריקאי לפתח תפיסה זאת; יתמקד בתשתית התיאורטית ובזיקות שבין התכסית האנושית לבין מודיעין תרבותי ואינטליגנציה תרבותית. כל אלה, לאור הניסיון האמריקאי והישראלי בזירות העימות השונות. הבנה מעמיקה של התרבות המקומית הפכה לתנאי הכרחי להבשחת הרלוונטיות של המשימה הצבאית. המודיעין התרבותי, כחיבור בין הידע התרבותי שנוצר באמצעות מערכת התכסית האנושית לבין המודיעין הנדרש לצורך ביצוע המשימה הצבאית, התברר כחיוני ביותר. ההכרה בחשיבות המודיעין התרבותי הובילה את הצבא האמריקאי לפתח את מערכת התכסית האנושית, המושתתת על צוותים מקצועיים של מדעני חברה המצוותים לכוחות ברמות השונות, שתפקידה הוא לתרום להבנת התרבות והחברה בזירות הלחימה. מפקדים ואנשי צוות שלקחו חלק בתוכנית הסכימו על התרומה של מערכת התכסית האנושית לרלוונטיות של המשימה הצבאית ולהצלחתה. אלא שלצד החשיבות שיוחסה למערכת זאת, הפעלתה עוררה גם ביקורת, הן במרחב הצבאי והן במרחב האקדמי. למרות ההתפתחויות המתודולוגיות המבצעיות והארגוניות של מערכת התכסית האנושית בהקשר האמריקאי, עדיין קיימים פערים, והתוצרים במקרים רבים אינם מספקים. גם בקרב גופי הביטחון והמודיעין בישראל קיימים פערי ידע בנושא זה ובהטמעתו בתורת הלחימה ובמתודולוגיה המודיעינית.

מילות מפתח: מודיעין, מודיעין תרבותי, תכסית אנושית, צבא, צה"ל, צבא ארצות הברית, תרבות, מתודולוגיה

ד"ר קובי מיכאל הוא חוקר בכיר במכון למחקרי ביטחון לאומי. עומר דוסטרי הוא מוסמך לתואר שני בתוכנית לדיפלומטיה מאוניברסיטת תל אביב ומתמחה במכון למחקרי ביטחון לאומי.

מבוא

המושג והתפיסה "תכסית אנושית" (Human Terrain) התפתחו בצבא האמריקאי החל משנת 2006, בעקבות קשיים אתם התמודדו כוחותיו בזירה העיראקית והאפגנית. התכסית האנושית מתייחסת ליסודות החברתיים, האתנוגרפיים, התרבותיים, הכלכליים והפוליטיים בזירה רוויית אוכלוסייה אזרחית, שבה פועל כוח צבאי ואשר המפתח להצלחתו הוא התמקדות באנשים.²

חשיבה צבאית ומודיעין, השמים דגש על מיצוי הכוח הצבאי, על יכולות האש ועל טכנולוגיות מודיקות לצורך פגיעה במטרות והשגת הכרעה צבאית, אינם מספיקים כדי להתמודד באופן יעיל עם מבצעים נגד התקוממות או מבצעים לשמירת שלום. במבצעים כאלה נתקל הכוח הלוחם באוכלוסייה אזרחית, שמאפייניה התרבותיים והפוליטיים שונים וזרים מאלה של המדינות מהן הוא מגיע.³ כוח המשימה ושולחיו נדרשים, לפיכך, למודיעין מסוג שונה, שיוכל לסייע בצמצום הפערים בהבנת המאפיינים התרבותיים הקיימים בינו ובין האוכלוסייה המקומית, פערים הפוגעים ברלוונטיות שלו.⁴

על החשיבות של הסוגיה התרבותית עמד גנרל רופרט סמית', שהגדיר את המלחמה בעת החדשה כ"מלחמה בקרב אנשים" (war amongst the people).⁵ מלחמה זו מתאפיינת לדבריו בטשטוש מובהק בין החזית האזרחית לחזית הצבאית, בפעילות צבאית אינטנסיבית בשטחים אורבניים צפופי אוכלוסין ובמעורבות גדלה ומשמעותית של שחקנים לא מדינתיים, בדמות ארגוני טרור וגרילה, הפועלים מתוך האוכלוסייה ובחסותה. מאפיינים אלה משפיעים על המודיעין הנדרש להבנת חשיבותם של האוכלוסייה האזרחית והמרחב האזרחי כמרחבי לחימה, כיעד ללחימה וככלי בלחימה. זאת, תוך שימת דגש על החלשת התמיכה בכוחות המורדים – טרור וגרילה – הגברת התמיכה בצבאות הלוחמים ומינוף השפעתם של מנהיגים וכוחות מקומיים לטובת קידום יעדי הלחימה. אלה, ולצדם ההכרח המוסרי

1 מושג זה הוזכר בעברית לראשונה במאמרו של אהד לסלוי, "התכסית האנושית כבסיס להפעלת הכוח: ההתמודדות עם הבדווים במערכה בנגב במלחמת העצמאות", בתוך: **בין הקטבים**, גיליון 1: ספר – עיון בהתהוות האתגר בגבולות (מרכז דדו לחשיבה צבאית בינתחומית והוצאת מערכות, פברואר 2014), עמ' 27–7.

2 Roberto González, "Human Terrain Past, Present and Future Applications", *Anthropology Today* 24, no. 1 (2008): 21–26.

3 Kobi Michael and David Kellen, "Cultural Intelligence for Peace Support Operations in the New Era of Warfare", In *The Transformation of the World of War and Peace Support Operations*, eds. Kobi Michael, David Kellen and Eyal Ben-Ari (Westport, Connecticut: Greenwood Publishing Group, 2009).

4 שם.

5 Rupert Smith, *The Utility of Force: The Art of War in the Modern World* (New York: Alfred A. Knopf, 2007).

והציווי המשפטי הבין-לאומי של הגנה על אוכלוסייה אזרחית, הובילו להפנמת ההבנה כי יש צורך בהעמקת הידע על האוכלוסיות האזרחיות באותם מרחבים. מאמר זה מתאר ומגדיר את תפיסת התכסית האנושית שהתפתחה בצבא האמריקאי ועומד על הסיבות שהובילו אותו לפתח תפיסה זאת. המאמר מתמקד בתשתית התיאורטית, בהגדרותיה ובמאפייניה, ובוחר את הזיקות בין התכסית האנושית ובין מודיעין תרבותי ואינטליגנציה תרבותית, וכן את מאפייני יישומה של התכסית האנושית בזירות העימותים של ארצות הברית וישראל. זאת, תוך הצגת הלקחים הבולטים מהניסיון המצטבר, שלדעתנו יכולים להיות רלוונטיים גם למאפיינים של אתגרי הלחימה שבפניהם ניצב צה"ל.

התכסית האנושית – רקע, מאפיינים והגדרות תיאורטיות

התכסית האנושית מוגדרת כ"אפיון תרבות, אנתרופולוגיה ואתנוגרפיה, הנוגע לאוכלוסייה האנושית ולפעולות גומלין בתוך אזור פעילות משותף". ניתוח התכסית האנושית הוא "התהליך שבאמצעותו ניתן להבין את המרחב האנושי והתפתחותו, והוא משלב בין גיאוגרפיה אנושית ובין מידע תרבותי".⁶

פרויקט מערכת התכסית האנושית הוא תוכנית צבאית אמריקאית המגייסת ומאמנת צוותי תכסית אנושית, הכוללים מומחים צבאיים לצד מומחים אזרחיים, ומציבה אותם ביחידות הצבא בזירות הלחימה.⁷ הפרויקט החל בשנת 2006, לאור קשיי הצבא האמריקאי בהתמודדות עם תנאי הזירות החדשות בעיראק ובאפגניסטן. בעקבות זאת אישר משרד ההגנה של ארצות הברית ומימן בשנת 2007 תמיכה מקצועית לכוחות הצבא האמריקאי שם, לצורך היכרות עם נושאים חברתיים ותרבותיים.⁸

מערכת התכסית האנושית בארצות הברית מנוהלת על ידי "פיקוד ההכשרה והתורה של צבא היבשה של ארצות הברית" (U.S. Army Training and Doctrine Command). צוותים של חמישה עד תשעה אזרחים ואנשי צבא מוצבים בחטיבות, באוגדות ובדרגי מטה ושטח, לצורך הכנתם להתמודדות עם אוכלוסייה אזרחית. הם עושים זאת על ידי מתן הדרכות קפדניות לפני הצבת אותם גורמים בשטח,

6 Joint Doctrine Note 4/13 – Culture and Human Terrain (Swindon, Wiltshire: Ministry of Defence, 2013), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/256043/20131008-JDN_4_13_Culture-U.pdf.

7 Montgomery McFate and Steve Fondacaro, "Reflections on the Human Terrain System during the First 4 Years", *FEATURES* 2, no. 4 (2011): 63-82, <https://www.ciaonet.org/attachments/19701/uploads>.

8 Christopher A. King, Robert Bienvenu and T. Howard Stone, "HTS Training and Regulatory Compliance for Conducting Ethically-Based Social Science Research", *Military Intelligence Professional Bulletin* 37, no. 4 (2011): 16-20, https://fas.org/irp/agency/army/mipb/2011_04.pdf.

וממשיכים במתן תמיכה מקצועית לאחר הצבתם שם, וזאת בעזרת מרכז תמיכה וניתוח ושימוש בטכנולוגיות לניתוח חברתי-תרבותי.⁹

צוותי התכסית האנושית מורכבים ממומחים בעלי רקע במדעי החברה ורקע מבצעי, הרוכשים ידע והבנה על האוכלוסיות המתגוררות בשטחי הלחימה, וזאת בעזרת ראיונות וקשרי גומלין שהם מקיימים עם יחידים מאותן אוכלוסיות.¹⁰ ניתוח מדעי-חברתי של האוכלוסייה המקומית מסייע להגביר את מודעותם של הכוחות הצבאיים בזירה למצב, לשפר תהליכי קבלת החלטות בתחום התרבותי, לחדד את התכליתיות המבצעית ולשמר ולחלוק ידע חברתי-תרבותי.¹¹

בין תכסית אנושית, אינטליגנציה תרבותית ומודיעין תרבותי מהי תרבות?

"תרבות" מוגדרת כמנהגים, מושגים, רעיונות והתנהגות חברתית, המשותפים לקבוצת אנשים ומכוונים את אמונתם והתנהגותם. אפיון תרבות מחייב מענה לשאלות כמו: כיצד אנשים מאורגנים? מהם האמונות והערכים שלהם? מהן הדרכים שבהן אנשים מתקשרים ביניהם ועם אחרים (חיצוניים לחברתם/תרבותם)? ככלל, אנשים אינם מתנהגים באופן אקראי, אלא בדרך שנראית גיונית לאנשים אחרים בקבוצתם. התנהגותם מקובלת ומובנת בתוך הקבוצה בזכות הרעיונות המשותפים שלה, המגדירים מהי התנהגות נורמלית.¹²

תרבות כוללת שכבות רב-משמעיות, המתבססות על שפה, חברה, כלכלה, דת, היסטוריה ותחומים אחרים. שכבות אלו באות לידי ביטוי במאפיינים מוחשיים המעצבים את הזהות התרבותית, כגון הופעה פיזית, ביגוד, ארכיטקטורה, מחוות, חוקים חברתיים, סגנון תקשורת ואמונות.¹³

אינטליגנציה תרבותית

בשפה האנגלית יש זהות מילולית בין "אינטליגנציה תרבותית" ובין "מודיעין תרבותי" (cultural intelligence), אלא שלמרות הקשר המהותי ביניהם, מדובר בשני מושגים שונים. האינטליגנציה התרבותית מתייחסת ל"יכולת קוגניטיבית

9 Yvette Clinton, Virginia Foran-Cain, Julia Voelker McQuaid, Catherine E. Norman and William H. Sims, *Congressionally Directed Assessment of the Human Terrain System* (CNA's Center for Naval Analysis, 2010), p. 15, <https://info.publicintelligence.net/CNA-HTS.pdf>.

10 King et al., "HTS Training and Regulatory Compliance", p. 16.

11 McFate and Fondacaro, "Reflections on the Human Terrain System", p. 63.

12 *Joint Doctrine Note 4/13 – Culture and Human Terrain*.

13 *Cultural intelligence and the United States military* (Washington, D.C.: Center for Advanced Defense Studies, 2006), [https://www.psa.ac.uk/sites/default/files/conference/papers/2015/Human%20Terrain%20System%20\(for%20PSA\).pdf](https://www.psa.ac.uk/sites/default/files/conference/papers/2015/Human%20Terrain%20System%20(for%20PSA).pdf).

ופסיכולוגית של יחידים או קבוצה להסתגל, לבחור ולעצב סביבה תרבותית שונה".¹⁴ אינקסון ותומס הגדירו אינטליגנציה תרבותית כ"יכולת, מיומנות וגמישות להבנה וללמידה של תרבות, עיצוב הדרגתי של האדם לגלות אהדה לתרבות [שונה משלו], והפיכת התנהגותו למכילת ונאותה יותר בקשרי הגומלין עם תרבויות אחרות".¹⁵ אינטליגנציה תרבותית היא אחד מהכלים החשובים ביותר לפיתוח מודעות תרבותית. לעומת זאת, מודיעין תרבותי מתייחס לתפקוד המבצעי הצבאי של איסוף וניתוח מידע על זירה ויריב, שפרשנותם מושפעת מהיבטים תרבותיים. אינטליגנציה תרבותית הינה דרישה הכרחית עבור מודיעין תרבותי, בשל הצורך להבין את ההקשר ואת ההבדלים בין צד אחד ובין יריבו, והיא חיונית עוד יותר בהקשר של "מלחמה בקרב אנשים".¹⁶

אינטליגנציה תרבותית מאפשרת את היכולת לעסוק במערכת התנהגויות הכוללת שפה, יכולות בין-אישיות ועוד. רכישת אינטליגנציה תרבותית אינה תהליך קבוע או מוגדר, אלא תהליך למידה מתמשך באמצעות חינוך וניסיון, המשולבים עם יכולתו של הפרט לקלוט צרכים של סביבות שונות. אלה מאפשרים לא רק לרכוש ידע על תרבויות אחרות, אלא גם לפתח את היכולת להבין תרבויות אלו. הבנת תרבויות אחרות מאפשרת לצפות צרכים ולעשות צעדים הכרחיים לקראתם, להכיר רמזים תרבותיים דקים וליצור תקשורת, לנהל משא ומתן ולמצוא פתרונות.¹⁷

מודיעין תרבותי

המודיעין התרבותי עוסק בארגון רציונלי של פוליטיקה מקומית, בהבנת קודים וצרכים תרבותיים ובסדר הפנימי של הרשתות החברתיות. מודיעין זה נועד לא רק לזהות איומים, אלא גם להבין הזדמנויות לקידום שינוי פוליטי. לכן, המודיעין התרבותי צריך להתבסס על הבנה רחבה של הממדים הפוליטיים והחברתיים של זירת העימות.¹⁸

ביחסים הבין-לאומיים, מודיעין תרבותי מוגדר כ"ניתוח של חברות, פוליטיקה, כלכלה ודמוגרפיה, המספק הבנה על אנשים או על היסטוריה, מוסדות, פסיכולוגיה, אמונות והתנהגויות של מדינות". סכסוכים מודרניים, כמו למשל בעיראק ובאפגניסטן, מחייבים את הצבא לשים דגש על האוכלוסיות המקומיות, המהוות את התחום

Michael and Kellen, "Cultural Intelligence for Peace Support Operations", p. 170. 14

David C. Thomas and Kerr Inkson, "Cultural Intelligence: People Skills for a Global Workplace", *Consulting to Management* 16, no.1 (2005): 5-9. 15

Michael and Kellen, "Cultural Intelligence for Peace Support Operations", p. 170. 16

Todd J. Clark, *Developing a Cultural Intelligence Capability* (Kansas: Fort Leavenworth, The Faculty of the U.S. Army Command and General Staff College, December 2008). 17

Michael and Kellen, "Cultural Intelligence for Peace Support Operations", p. 162. 18

המשמעותי במלחמה בטרור ובמלחמות הגלובליות.¹⁹ הפקת מודיעין תרבותי ברמה גבוהה מחייבת את גורמי האיסוף והמחקר להשתחרר מגישות אתנוצנטריות, המייחסות ערך או משמעות אוניברסלית לערכי החברות מהן הם מגיעים, ולגלות פתיחות ורגישות לתרבויות האחרות.

במאמר ביקורת שכתבה דינה רזק נגד הלך החשיבה האתנוצנטרי של סוכנויות ביון במערב לאורך העשורים האחרונים, היא מסבירה כי חוקרי מודיעין שם מתקשים עד היום להתייחס להרגלי תרבות מסוימים בקרב החברה הערבית-מוסלמית, כגון לתפקיד האסלאם בחברה, לשימוש הדומיננטי בטרוריקה, למוטיבציה פוליטית ולתפקיד המשמעותי של תחושת הכבוד.²⁰ לדבריה, האלטרנטיבה לידע תרבותי היא מצב שבו שולטים ערכים, דוקטרינות ואמונות אוניברסליים המושפעים מהמערב, לפיהם יש להתיישר ברמה הרעיונית והתפיסתית, כמו מושגים חד-ממדיים של "דמוקרטיה", "חופש" ו"רציונליות". לטענת רזק, הסכנה של אוניברסליזם מחזקת את הצורך והחשיבות שקהילות מודיעין יקדישו מאמצים נוספים ללימודי תרבות.²¹ החשיבות שבהבנת תרבותו של היריב על ידי סוכנויות המודיעין באה לידי ביטוי משמעותי יותר בזירה המודרנית של "מלחמה בקרב אנשים". בזירה זאת חלות מגבלות על הפעלת הכוח, ואיכות שיתוף הפעולה בין השחקנים הצבאיים ובין השחקנים האזרחיים (האוכלוסייה האזרחית, ארגונים לא ממשלתיים וארגונים בין-לאומיים) תלויה ומושפעת הדדית. מכיוון שכול השחקנים בזירה נחשבים למפיקי מודיעין, נדרשת שפה משותפת בין כולם, שתוביל לשיתוף פעולה פורה. מדובר, בין השאר, בארגונים לא מדינתיים, במשטרה ובמגזר הפרטי, האוספים ומפיקים מידע הנדרש למודיעין, אך עדיין לא שותפים מלאים בזירות העכשוויות.²² כוחות הצבא, הפועלים להשגת מטרותם, חייבים להבין את ההקשר הפוליטי והתרבותי ולהתאים את הדוקטרינה והאמצעים הצבאיים להקשר זה ולסביבה שבה הם פועלים. אחד הכלים החשובים ביותר לצורך זה הוא המודיעין. משום כך, האמצעים והשיטות של המודיעין חייבים להתאים להקשר הפוליטי בזירה ולאופי הדינמי שלה. גורמים שמפקדי הצבא רגילים לפעול מולם בזירה צבאית מסורתית, אינם דומים לאלה שמולם פועל הצבא בקרב אוכלוסייה אזרחית.²³

Clark, *Developing a Cultural Intelligence Capability*. 19

Dina Rezk, "Orientalism and Intelligence Analysis: Deconstructing Anglo-American Notions of the 'Arab'", *Intelligence and National Security* 31, no. 2 (2016): 226.

שם, עמ' 244-245.

Michael and Kellen, "Cultural Intelligence for Peace Support Operations", p. 162. 22

Kobi Michael, "Doing the Right Thing the Right Way: The Challenge of Military Mission Effectiveness in Peace Support Operations, in a 'War amongst the People' Theatre", in *Cultural Challenges in Military Operations*, eds. Cees M. Coops and Tibor Szvircsev Tresch (Rome: NATO Defense College, October 2007), pp. 254-263, <https://www.ciaonet.org/attachments/381/uploads>. 23

מומחי מודיעין נדרשים להבין את התרבות, השפה וסביבת הסכסוך, וכן שאיסוף מידע בסוג כזה של זירה מחייב מעורבות אינטנסיבית בקרב האוכלוסייה המקומית. מדובר בקבוצת אנשים שהיא בוזמנית גם הזירה (סביבת הפעולה הצבאית), גם המטרה (הן לצורך ערעור התמיכה בגורמי הטרור והגרילה הפועלים בחסותה ובתמיכתה, והן לצורך ביסוס הלגיטימציה והתנאים לשיתוף פעולה עם כוחות הצבא נגד גורמים אלה) וגם מקור חשוב למודיעין.²⁴

מורדים, ובכללם ארגוני טרור וגרילה מאזור מסוים, מבינים את התרבות המקומית טוב יותר מכול כוח לוחם זר. לכן, יש להם יתרון משמעותי על כוח הלחימה הזר בכול הנוגע להיטמעות בקרב האוכלוסייה ולפעילות בחסותה ובסיועה. כדי להבטיח שכוח המשימה הצבאי יצליח בהשגת תמיכתה של האוכלוסייה המקומית, עליו להבין אותה ואת תרבותה באופן שיאפשר להפעיל את מנגנוני ההתערבות ושיתופי הפעולה הנדרשים אתה לצורך החלשת כוחות הגרילה והטרור, לערער את בסיס התמיכה שלהם בקרב האוכלוסייה המקומית²⁵ ולעצב (בשיתוף עם גורמי הכוח וההשפעה בקרב האוכלוסייה המקומית) מבנה חברתי-פוליטי שיאפשר התמודדות עצמאית של אותה אוכלוסייה עם כוחות אלה לאורך זמן.

ערן זהר, המתייחס לתפקוד המודיעין הצבאי הישראלי לפני "האביב הערבי" ובמהלכו, טוען כי ניסיון של סוכנויות מודיעין, דוגמת אגף המודיעין בצה"ל, להבין את האויב, אינו יכול להצליח כל עוד חוקרי מודיעין אינם מבינים את התרבות והשפה הערבית: "העבודה הקשה והמתישה של לימוד האויב, והניסיון להבין את כוונותיו, אינם צריכים להידחק הצדה מפני האפשרות הקלה יותר של הגדרת רציונל האויב".²⁶ "לטענתו, 'סוכנות מודיעין מרוויחה מחוקרי מודיעין שצוברים הבנה מעמיקה ואינטימית של מדינת המטרה ומכירים את ההיסטוריה שלה, תרבותה ומסורותיה. כישורים אלה עשויים לסייע בחיזוי מהפכות".²⁷

הניסיון של ארצות הברית בעיראק ובאפגניסטן חשף את האופי הבעייתי של המפגשים התרבותיים בין כוחות משימה ובין אוכלוסיות מקומיות, כאשר כוחות המשימה האמריקאיים התקבלו על ידי המקומיים כזרים וכפולשים.²⁸ רוברט מיהארה אף טוען כי עצם הפלישה האמריקאית לאפגניסטן ולעיראק חשפה

24 שם.

25 *Insurgencies and Countering Insurgencies*, FM 3-24/MCWP 3-33.5. (Washington DC: Department of The Army, May 2014), http://www.marines.mil/Portals/59/MCWP%203-33.5_Part1.pdf.

26 Eran Zohar, "Israeli Military Intelligence's Understanding of the Security Environment in Light of the Arab Awakening", *Defence Studies*, 15 no. 3 (2015): 20.

27 שם, עמ' 26.

28 Richard Burchill, "Jihadist Insurgency and the Prospects for Peace and Security", *Small Wars & Insurgencies* 27, no. 5 (2016): 958-967.

חוסר הבנה של ממשל בוש את ההתפתחויות הפוליטיות בעולם ואת הנושא של "בניית מדינה" (state building) בשתי מדינות אלו. לדידו של מיהארה, המדיניות והאסטרטגיה האמריקאיות נבעו מנקודת מוצא, לפיה אידיאולוגיות דמוקרטיות וליברליות מתאימות לשינוי פני החברה במדינות שונות בעולם, ובכלל זה בעיראק ובאפגניסטן. אלא שמגזרים רבים בקרב החברה המקומית לא היו מעוניינים לקחת חלק בחזון של ממשל בוש ל"בניית מדינה", והתנגדו לערכים הדמוקרטיים והליברליים שהאמריקאים ביקשו לקדם.²⁹ גם ההצלחה המוגבלת של ארצות הברית בלחימה נגד התקוממות וטרור של האסלאם הקיצוני באפגניסטן ובעיראק, ולאחרונה גם נגד "המדינה האסלאמית" בעיראק ובסוריה, נובעת מחוסר ידע ומהיעדר הבנה של מערכת האמונות (בעיקר הדתיות) המניעה את הטרור האסלאמי (הג'יהאדיסטי-סלפי) ושל הסיבות להצלחתו לגייס פעילים, תמיכה מקומית ומשאבים.³⁰

היעדר בסיס דתי באידיאולוגיה הפוליטית המערבית המודרנית אינו מבטל את חשיבות הדת בתרבויות אחרות. אידיאולוגיה דתית היא, ככול הנראה, הגורם החשוב ביותר שבו המערב צריך להתמקד ככול שהדבר נוגע לתנועות התקוממות ג'יהאדיסטיות, ולפחות לנסות להבינו טוב יותר. לחימה נגד התקוממות אינה מסתיימת תמיד בתבוסה צבאית ברורה של המתקוממים ותומכיהם, אך יחד עם זאת, יש צורך להבטיח הישגים משמעותיים בלחימה כזאת, שיאפשרו רגיעה ומניעת התקפות עתידיות נוספות של המתקוממים.³¹

מאבק יעיל בהתקוממות ג'יהאדיסטית מחייב אמנם את המערב לגבש אסטרטגיה צבאית ולהפעיל כוח צבאי, אך בה בעת לכוון את המאמצים גם נגד האידיאולוגיה המניעה קבוצות טרור. לצד ההתמקדות בנושא האסטרטגי, חשוב להבין מי הם האנשים העוסקים בטרור האסלאמי ומה מושך אותם להצטרף למאבק האסלאמי. האתגר הניצב בפני המערב בעימותים מסוג זה הוא פיתוח היכולת "לכבוש" את הלבבות ואת התודעה של האוכלוסייה (hearts and minds).³² המאבק לכיבוש הלבבות והתודעה, בפרט של האוכלוסייה הצעירה, נתקל באתגר משמעותי מצד ארגוני טרור, כמו "המדינה האסלאמית", המנצלים את עידן האינטרנט והרשתות החברתיות לפעילות מודיעינית תרבותית. מטרתה של פעילות זו היא לא רק לגייס פעילים באמצעות דעת הקהל, אלא גם להפוך את הטרור לפופולרי, לנחשק ולדרך חיים שתהווה מודל לחיקוי.³³

Robert Mihara, "The Inutility of Force", *Infinity Journal* 5, no. 3 (2016). 29

Burchill, "Jihadist Insurgency and the Prospects for Peace and Security". 30

שם. 31

Smith, *The Utility of Force*. 32

Javier Lesaca, "On social media, ISIS uses modern cultural images to spread anti-modern values", *Brookings Institution*, September 24, 2015, <https://www.brookings.org>. 33

יתרה מזאת, חלק לא מבוטל מהתמונות וקטעי הווידאו ש"המדינה האסלאמית" משתמשת בהם כדי לפתות ולגרות את האוכלוסייה הצעירה בעולם הערבי והמוסלמי במטרה לתמוך בארגון או להצטרף אליו ולקחת חלק בפעילותו, לקוח ישירות מהתרבות המודרנית של המערב, המוכרת היטב לקהל הצעיר מסרטי קולנוע, ממשחקי מחשב ומקליפים פופולריים. באופן פרדוקסלי, ארגוני הטרור משתמשים בתרבות ובמיתוג המערביים המודרניים לקידום ערכים ותרבות המנוגדים לאלה של המערב.³⁴

הבנת התרבות של האוכלוסייה המקומית חשובה ותורמת משמעותית גם להתמודדות עם התקפות של "זאבים בודדים", כלומר עם פעולות טרור של יחידים שאינם קשורים או מזוהים באופן רשמי עם ארגון טרור זה או אחר או פעילים במסגרתו, אך לעתים משייכים עצמם לארגון כזה בסמוך לפיגוע, במהלכו או לאחריו. זאת, מתוך הזדהות עם רעיון שהוא מבטא ובמטרה להגביר את התהודה של מעשה ההקרה והשפעתו על דעת הקהל.³⁵

החלטת המפגע הבודד, שהושפע ממסרים ורעיונות קיצוניים, לצאת לפיגוע עצמאי מתקבלת בתהליך שבינו לבין עצמו, ולרוב בלוח זמנים קצר, דבר שמקשה מאוד על סיכול הפיגוע. ואולם, ניתן עדיין לאתר סימנים מעידים אצל בודדים או קבוצות קטנות לפני ביצוע פיגועים, כמו ביקור במדינות בהן פועל ארגון טרור, מעורבות בפעילות פלילית ומעצרים קודמים של המפגע, או נראות בולטת ברשתות החברתיות. "לצורך איתור הסימנים והרמזים, ועל מנת לנסות להיכנס לראשם של המפגעים הפוטנציאליים, לא די באמצעים טכנולוגיים, אלא יש גם צורך בהבנת הלכי הרוח, 'בתי הגידול', רקע סוציו-אקונומי וגורמים סביבתיים. אלה מחייבים הבנה תרבותית, שפתית ומנטלית".³⁶

הארגון הצבאי, כארגון היררכי ומשמעתי, מתנהל על פי עקרונות המבדלים אותו מארגונים אחרים, ובעיקר מארגונים אזרחיים. ההתבדלות מהחברה האזרחית בסביבה זרה ועוינת הופכת למכשול משמעותי בפני היכולת לפתח ולשכלל את המודיעין התרבותי. זה מחייב, כאמור, התערות בקרב האוכלוסייה ומגע קרוב אתה לצורך היכרות והבנה מעמיקה שלה. חובה להשיג יעדים אלה כדי שניתן יהיה להגיע ליעילות במילוי משימות הצבא, במיוחד בזירה מורכבת כמו זו של "מלחמה בין אנשים". סוג כזה של לחימה דורש פתיחות לאמצעים צבאיים אסטרטגיים

edu/blog/techtank/2015/09/24/on-social-media-isis-uses-modern-cultural-images-to-spread-anti-modern-values/

34 שם.

35 שלמה מופז, "אתגרי המודיעין בעידן הטרור", *Israel Defense*, 28 ביולי 2016.

36 שם.

שונים ומגוונים, וביניהם צורות ומקורות מגוונים של מודיעין, כמו מודיעין תרבותי, שחלקם נמצאים מחוץ למרחב הצבאי.³⁷

החיבור השבעי בין אינטליגנציה תרבותית למודיעין תרבותי

כוחות צבאיים הפועלים בזירת הלחימה המודרנית מתמודדים עם ארגוני טרור או גרילה הפועלים בתוך סביבה אזרחית ומשתמשים באזרחים כמגן אנושי. התפתחות מורכבת זו של צורת המלחמה מאלצת את כוחות הצבא המערביים להתאים את הדוקטרינות ואמצעי הפעולה שלהם לאתגרים החדשים, כדי להתמודד אתם בצורה תכליתית.³⁸

השינויים בזירת הלחימה ובפעילות הצבאית הגבירו את החשיבות שבהכרת תרבותה של האוכלוסייה המקומית אתה מתמודדים הצבאות השונים, ושל צרכיה, וזאת כאמצעי להצלחת המשימה הצבאית. את המענה לצורך זה אמורה לספק עבודת המודיעין. תנאי הכרחי ליכולת להגיע למודיעין מהימן ואיכותי שתורם להצלחת המשימה הוא שיפור, פיתוח והטמעת אינטליגנציה תרבותית בקרב הצבא, ובעיקר בקרב הכוחות בשטח, לצורך הפקת מודיעין תרבותי.

במצבים המתוחים והמורכבים המאפיינים את הלוחמה המודרנית, אינטליגנציה תרבותית הופכת לכישור הכרחי בקרב מפקדים וקצינים בכירים הפועלים בזירה. אינטליגנציה תרבותית, המאפשרת "יכולת להיות תכליתי בקשרי גומלין עם אנשים מתרבות שונה", הופכת לפלטפורמה הקוגניטיבית לקליטת מידע, להבנתו ולהתקשרות עם האוכלוסייה והמוסדות המקומיים, כמו גם עם ארגונים אזרחיים הפועלים בזירה המקומית.³⁹

אחד האתגרים התרבותיים הבולטים אתם נדרשו כוחות צבא מערביים להתמודד היה המפגש עם חברות ואוכלוסיות (מוסלמיות ברובן) במדינות ערביות-מוסלמיות ובמדינות מוסלמיות שאינן ערביות (לדוגמה, אפגניסטן). הדת והעדיות ממלאות תפקיד חשוב הרבה יותר בחברות מוסלמיות בעולם הערבי מאשר בעולם המערבי. העובדה שהעולם הערבי, בניגוד לעולם המערבי, לא עבר תהליך חילון וכי בדור האחרון אף גבר משקלה של הדת ברוב מדינות המזרח התיכון, מקשה מאוד על היכולת להעריך את התנהלותן של החברה והתרבות הערבית במונחים של "ריאל-פוליטיק" ועל פי ההיגיון המערבי.⁴⁰ תשתית ידע כתוצר של המודיעין התרבותי תאפשר יכולת גבוהה יותר בשקלול "הציווי הדתי והמוטיבציה שהוא מייצר, וגם

Michael and Kellen, "Cultural Intelligence for Peace Support Operations", pp. 37 262-263.

38 שם, עמ' 168.

Michael, "Doing the Right Thing the Right Way", pp. 259-260. 39

40 אפרים קם, "המזרח התיכון כאתגר מודיעיני", **עדכן אסטרטגי**, כרך 16, גיליון 4 (ינואר 2014), עמ' 83-93.

של המתח בין הציווי הדתי לאילוצי המציאות". בהיעדר מתודולוגיה מפותחת של מודיעין תרבותי ותשתית ידע מספקת ורלוונטית, אין במערב "הבנה מספקת לתפקיד הפוליטי והחברתי שממלאות הדת, העדתיות והשבטיות, המשפיעות על הסדר המדינתי ולעתים פוגעות בו". המערב מתקשה להתמודד עם אוכלוסיות ערביות ומוסלמיות, כפי שניתן להיווכח בהסתבכות האמריקאית בעיראק, שם ארצות הברית לא הבינה את תפקיד העדתיות במדינה הכבושה ואת הבסיס המדינתי הרעוע שנוצר בה עם כינונה.⁴¹

התפתחות תחום התכסית האנושית – הניסיון האמריקאי הצורך במערכת התכסית האנושית

מערכת התכסית האנושית בצבא ארצות הברית היא ביטוי רחב למבנה הארגוני ולתהליכי העבודה הדרושים לביצוע מחקר שטח אתנוגרפי ולפיתוח תשתית הידע המסייעת לכוחות צבאיים במבצעים ביטחוניים וביישוב סכסוכים או ניהולם. המחקר האתנוגרפי מתבצע על בסיס נתונים הנאספים בשטח על ידי צוותים קטנים, הכוללים אנשי מדעי החברה המתערים בקרב האוכלוסייה המקומית וחוקרים את מאפייניה. הם עושים זאת באמצעות ראיונות וסוגים שונים של קשרי גומלין עמה.⁴²

במהלך השנים בהן מופעלת מערכת התכסית האנושית בצבא האמריקאי הוצבו בה יותר מאלף אנשי צוות. העלות הכוללת של הפעלת המערכת הגיעה בשנים 2007–2014 לסכום של כ־750 מיליון דולר, מה שהפך אותה להשקעה הגדולה ביותר בפרויקט מתחום מדעי החברה בתולדותיו של הממשל הפדרלי.⁴³ הכוחות האמריקאיים שהתמודדו עם האוכלוסייה המקומית בעיראק ובאפגניסטן נדרשו להבין את מבנה הכוח בקרב אותה אוכלוסייה ולמפות את סוכני ההשפעה הפוטנציאליים בקהילה. בנוסף לכך, היה עליהם לרכוש את אמונה של האוכלוסייה המקומית ולהפחית בדרך זו את תמיכתה בארגוני המורדים, וכן לתת את המענה הנדרש לצורכי האוכלוסייה ולשפר את ביטחונה ורווחתה.⁴⁴

תחקירים שנכתבו בפנטגון בידי מפקדים שחזרו מהשטח הצביעו על קשיים ומגבלות בהפעלת הכוח, בהתמצאות במרחב ובהתמודדות עם הכוחות המורדים,

41 שם.

42 Richard M. Medina, "From Anthropology to Human Geography: Human Terrain and the Evolution of Operational Sociocultural Understanding", *Intelligence and National Security* 31, no. 2 (2014): 137-153.

43 Christopher Sims, "The Life and Death of the Human Terrain System", *Foreign Affairs*, February 4, 2016, <https://www.foreignaffairs.com/articles/afghanistan/2016-02-04/academics-foxholes>.

44 McFate and Fondacaro, "Reflections on the Human Terrain System", p. 65.

שנגרמו, בין היתר, כתוצאה מהיעדר ידע חברתי-תרבותי נדרש.⁴⁵ הצורך במערכת התכסית האנושית גבר במיוחד לאחר שמבצעי הלחימה המשמעותיים של ארצות הברית בעיראק הסתיימו במאי 2003, וייצוב המרחב האזרחי לאחר המלחמה הפך לאתגר מרכזי – מה שחייב תכנון מחדש של המבצעים וההיערכות הצבאית.⁴⁶

התכסית האנושית בצבא האמריקאי – מאפיינים ומבנה ארגוני
מערכת התכסית האנושית בצבא האמריקאי מאורגנת בשתי רמות עיקריות: הצוותים המוצבים בשטח וצוותים מקצועיים במטה בארצות הברית, המעניקים לצוותי השטח תמיכה מינהלית, אימונים, ניתוחים וטכנולוגיית מידע. צוותי התכסית בשטח ממלאים את תפקידם בארבע רמות:

- תמיכה במפקדי החטיבה.
 - תמיכה ברמת מפקדי אוגדה ומעלה.
 - תיאום המחקר והניתוח בין גורמי השטח לגורמי המטה בזירה ותמיכה מדעית-חברתית ברמת מטה הזירה.
 - ליווי מקצועי של מבצעים.
- מטה מערכת התכסית האנושית ממוקם, כאמור, בארצות הברית, ומורכב משמונה אגפים. אגפים אלה תומכים בדרגי השטח בהיבטים לוגיסטיים, מבצעיים, תורתיים-הדרכתיים ומחקריים.⁴⁷

המתח בין המודיעין הצבאי למערכת התכסית האנושית
עם סיום הקמתה ובנייתה של מערכת התכסית האנושית, התפתח דיון בתוך הצבא האמריקאי לגבי שאלת מיקומם ושילובם של צוותי התכסית האנושית במבנה הארגוני הצבאי. ההתלבטות הייתה בין מיקום הצוותים לצד התאים המודיעיניים, ובין מיקומם בתאי ההשפעה הלא קטלניים (הכוללים מבצעים פסיכולוגיים ויחידות אזרחיות). בסוף שנת 2008 הוחלט למקם את הצוותים בתאים הלא קטלניים.⁴⁸ ההחלטה לא לכלול אותם בתאים מודיעיניים לא טשטשה את תכליתה המודיעינית של מערכת התכסית האנושית. מידע תרבותי מסוים הנאסף, נקלט, מעובד ומנותח ביד צוותי התכסית האנושית, ויש בו כדי לתרום לביטחון היחידות והאוכלוסייה המקומית, נחשב כמודיעין צבאי לכול דבר ועניין.⁴⁹

King, et al., "HTS Training and Regulatory Compliance", p. 16. 45

McFate and Fondacaro, "Reflections on the Human Terrain System", p. 65. 46

Clinton et al., *Congressionally Directed Assessment of the Human Terrain System*, pp. 15-17. 47

Cristopher Sims, *The Human Terrain System: Operationally Relevant Social Science Research in Iraq and Afghanistan* (U.S. Army College – Strategic Studies Institute, 2015), pp. 239-240. 48

שם. 49

המתח בין המודיעין לבין מחקר התכסית האנושית גבר בעקבות טקטיקת הלוחמה נגד התקוממות בסביבה אזורית צפופה. טקטיקה זו, הנשענת על שיתוף פעולה עם האוכלוסייה המקומית בזירת הלחימה וגיוס תמיכתה בכוח המשימה ובמטרותיו, תוארה כ"חשובה להצלחה המבצעית לפחות כמו הלוחמה עצמה". הלחימה נגד התקוממות, המחייבת הבנה מעמיקה של האוכלוסייה ותרבותה, יצרה היפוך בהיררכיה של רמות המודיעין (אסטרטגי, מערכתי וטקטי). מידע שנאסף ברמה הטקטית לצורך ביצוע המשימה הצבאית בקרב האוכלוסייה האזורית הפך לחשוב יותר מהמודיעין ברמות הגבוהות יותר.⁵⁰ היפוך זה משקף את החשיבות של פיתוח מודיעין התכסית האנושית ברמה הטקטית לצורך הפקת מודיעין איכותי ברמה המערכתית ועיצוב אסטרטגיה כוללת ורלוונטית.

הזיקה המובהקת בין המודיעין לבין המחקר התרבותי הפכה את עבודתם של צוותי התכסית האנושית לתחום אפור – בין ערוץ המודיעין ובין ערוץ מידע חברתי-תרבותי. התכנון המבצעי והצורך לשמור על ביטחון כוחות הקואליציה ועל ביטחון האזרחים באזורי עימות חייב מודיעין איכותי הניזון מהבנה מעמיקה של התכסית האנושית.⁵¹ למעשה, ניתן להגדיר את חיבור המיומנות המקצועית בין המודיעין הצבאי ובין המחקר החברתי-תרבותי כ"מודיעין תרבותי".

התפתחות מערכת התכסית האנושית בצבא האמריקאי

לאחר בדיקה ראשונית של הרעיון בשנת 2006, הוקמו והוצבו חמישה צוותי תכסית אנושית לתמיכה בחטיבות הצבא האמריקאי באפגניסטן ובעיראק. בדוח ההערכה הראשוני על הצוות הראשון שהוצב בבסיס "סאלרנו" באפגניסטן בשנת 2007, ציינו מפקד החטיבה ואנשיו כי צוות התכסית האנושית שיפר משמעותית את יכולתם של הכוחות בשטח להבין את האוכלוסייה המקומית, וכי הדבר אפשר להם לתקשר בהצלחה רבה יותר אתה. התוצאה הייתה שעוד לפני שכול חמשת הצוותים הניסיוניים הוצבו בשטח, כבר דרש הצבא האמריקאי לשגר צוותים נוספים.⁵² בעקבות ההצלחה של הצוותים הראשונים (בתחילת שנת 2007), עברה מערכת התכסית האנושית משלב "הוכחת יכולת" (proof of concept), שבוצע על ידי קבליים חיצוניים, לשלב של "יכולת מתמשכת" המופעלת על ידי אזרחים עובדי ממשלה ומומחים המועסקים על ידי הצבא, במימון תקציב המדינה (משרד ההגנה).⁵³ המטה הכללי האמריקאי הפנים את משמעות הדרישות שבאו לידי ביטוי בדוחות על הצרכים המבצעיים (Operational Needs Statements) ובדוחות על הצרכים

50 שם, עמ' 240–241.

51 שם.

Clinton et al., *Congressionally Directed Assessment of the Human Terrain System*, 52 p. 15

King et al., "HTS Training and Regulatory Compliance", p. 16. 53

הדחופים (Joint Urgent Operational Needs Statements),⁵⁴ ופעל לתת את המענה באמצעות הקמתה של מערכת תכסית אנושית בכול דרגי הפיקוד בזירה – מרמת הגדוד ועד רמת האוגדה.⁵⁵

בתוך ארבע שנים מאז הוקמה הפכה מערכת התכסית האנושית הניסיונית מרעיון מופשט לתוכנית צבאית ממוסדת, שהורחבה מחמישה צוותים לשלושים, התקציב השנתי שלה גדל ל-150 מיליון דולר, והיא הייתה לארגון החולש על 530 אנשי מקצוע. במקביל פותחה תוכנת המיפוי של מערכת התכסית האנושית (MAP-HT Toolkit), שיושמה בעיראק ובאפגניסטן, וכן פותחה ויושמה תוכנית הדרכה ואימונים להכנת צוותי התכסית האנושית לקראת הצבתם בשטח.⁵⁶ מערכת התכסית האנושית הופעלה במוצב הטקטי הקדמי של "מבצעים ליצירת יציבות כפרית" (village stability operations), לצד הכוחות למבצעים מיוחדים (SOF – special operations forces), וזאת עד לרמה האסטרטגית. "אזרחים ואנשי צבא, ללא קשר לדרגתם או לתפקידם, הפיקו תועלת מהרמה הגבוהה של ההבנה, המודעות וההקשר שהציעה המסגרת של אנשי מדעי החברה". מאמציהם של אנשי צוות התכסית האנושית גבו מחיר בחיי אדם, כאשר ארבעה מחבריהם נהרגו במהלך פעילותם בשטח.⁵⁷

מערכת התכסית האנושית בצבא האמריקאי – מקרי בוחן עיראק

סכסוך בין היזידים ובין הממשל העיראקי והכוחות הכורדיים בעיראק איים להסלים את המצב באזור בשנת 2008. היזידים התגוררו בשטח עימות בין הכורדים ובין הממשל העיראקי. שטח זה חלש טופוגרפית על אזור של קידוחי נפט שהיה נתון במחלוקת ותחת מאבק כלכלי-פוליטי בין הממשל המרכזי בעיראק ובין הכורדים סביב משאבי הנפט ואופן הקצאתם.⁵⁸

ספרות מחקר בשפה האנגלית על התרבות היזידית הייתה מוגבלת ונדירה, בשל חשש של חוקרי מדעי החברה לעסוק בנושא זה בתקופת משטר הבעת' בעיראק. חשש זה עוד גבר לאחר נפילתו של משטר זה.⁵⁹ חוקרת מדעי החברה, ג'ניפר קלארק, היא שזיהתה והבינה את מאפייני הסכסוך שהתרחש באזור ואת

54 שם, עמ' 67.

Steve Chill, "One of the Eggs in the Joint Force Basket: HTS in Iraq/Afghanistan and Beyond", *Military Intelligence Professional Bulletin* 37, no.4 (2011): 11-15.

McFate and Fondacaro, "Reflections on the Human Terrain System", p. 64. 56
Myron Varouhakis, *Challenges and Implications of Human Terrain Analysis for Strategic Intelligence Thinking* (The Political Studies Association, Defence and Military Intelligence panel, 2015). 57

שם. 58

Sims, *The Human Terrain System*, pp. 278-280. 59

מורכבותו. התובנות שעלו מהמחקר החברתי-תרבותי שנערך בהובלתה באותו אזור, שבו לא הייתה נוכחות צבאית, הביאו להחלטה לחצוץ בין הצדדים הנצים באמצעות כוח צבאי של נחתים אמריקאים. כוח כזה אכן הוצב במקום ופעל להורדת רמת החיכוך בין האוכלוסיות ולצמצום האלימות.⁶⁰

אפגניסטן

חוקר מדעי החברה ממחוז פאקטיקה באפגניסטן חקר את המערכת החקלאית באזור. הוא הבין את מורכבותה של סוגיית המים באזור והמליץ לפיכך לצבא האמריקאי לקחת חלק בפיקוח על מערכת ההשקיה, שהיוותה מרכיב קריטי במערכת החקלאות המקומית.⁶¹ בעקבות מחקר זה החלה מחלקת המדינה של ארצות הברית בפרויקטים לניהול מים באפגניסטן במטרה לשפר את החקלאות, להעלות את רמת החיים ולהגדיל את התעסוקה של האוכלוסייה הגברית. אוכלוסייה זאת עלולה הייתה להצטרף למורדים אם המשבר במערכת החקלאית היה נמשך.⁶²

מסקנות מיישום מערכת התכסית האנושית בצבא האמריקאי

עשור של לחימה בעיראק ובאפגניסטן הביא מפקדים בצבא האמריקאי ואנשי צוותי תכסית אנושית להסכמה רחבה על היתרונות שיש למומחים חברתיים-תרבותיים, למידע חברתי-תרבותי ולניתוחו. מידע ומומחים אלה עוזרים להתכונן להתמודדות עם האוכלוסייה האזרחית ועם מבצעי לחימה, וכן לממשם ולהעריך את משמעויותיהם.⁶³ כך, למשל, מפקד חטיבה 56 שפעל בעיראק בשנת 2008 התבטא כלפי אנשי התכסית האנושית: "אם מישו היה אומר לי שהוא מתכוון לקחת ממני את צוות התכסית האנושית, מחלקה שלמה של חיל רגלים הייתה מתייצבת כדי לעצור אותו [...] צוות התכסית האנושית תרם בהחלט למשימות המבצעיות שלנו. הצלחנו להפוך מצבים מסוימים שבהם היינו פותרים בעיות באמצעים קטלניים, למצבים שבהם אנו משתמשים באמצעים לא קטלניים, וזאת על בסיס המידע של צוות התכסית האנושית".⁶⁴

למרות התרומה המוערכת של צוותי התכסית האנושית, לא היה בכך די. בדוח על הצרכים המבצעיים הדחופים בעיראק ובאפגניסטן (The Afghanistan and Iraq Joint Urgent Operational Needs Statement) הוצגו פערי היכולות המבצעיות: "ארצות הברית ממשיכה לפעול באפגניסטן כשהיא חסרה את המומחיות החברתית-

60 שם.

61 שם, עמ' 282.

62 שם.

63 Mark Bartholf, "The Requirement for Sociocultural Understanding in Full Spectrum Operations", *Military Intelligence Professional Bulletin* 37, no. 4 (2011): 4.

64 McFate and Fondacaro, "Reflections on the Human Terrain System", p. 64.

תרבותית הנוגעת לתושבים המקומיים, את ההבנה ואת הכלים המתקדמים לביצוע איסוף מעמיק, ויזואליזציה וניתוחים של המבצעים הרלוונטיים לגורמים החברתיים-תרבותיים בשדה הקרב.⁶⁵ הפיקוד בעיראק הצהיר ש"פרטי מידע של האוכלוסייה המקומית חיוניים בזירות בהן הכוחות האמריקאיים מגבירים את פעילות הלוחמה נגד מרידות ואת מבצעי שמירת היציבות. הכוחות האמריקאיים ממשיכים לפעול בעיראק ללא ידע עדכני באשר לכללי ההתנהגות בקרב האוכלוסייה המקומית, מה שמגביל מאוד את המודעות המצבית של המפקדים ויוצר סיכונים רבים יותר לכוח".⁶⁶

במאמר תגובה למאמר ביקורתי של כריסטופר סימס (Sims) בנוגע למערכת התכסית האנושית בצבא ארצות הברית,⁶⁷ הציג תומס מנקן (Mahnken) מספר המלצות למקבלי ההחלטות בממשל ובצבא האמריקאי, וזאת על בסיס הניסיון שנצבר בשימוש במערכת התכסית האנושית: ראשית, לגייס יותר מהגרים ודוברי שפות זרות; שנית, לחזק את המומחיות התרבותית והחברתית על ידי הגדלת מספר הקצינים המתמחים בתחומי מדעי החברה, וזאת בניגוד לדגש הרב שמושם כיום על טכנולוגיה, הנדסה ושאר תחומים בעלי רקע מתמטי; שלישית, לחייב צוערים וקדטים ללמוד שפות זרות במסגרת לימודיהם הצבאיים; רביעית, להציע למגויסים לשורות הצבא הזדמנויות נוספות ללימוד ועבודה ברחבי העולם, לצורך התערות בתרבויות שונות ורכישת מידע וידע חשובים עליהן.⁶⁸

ביקורת והתנגדויות

מערכת התכסית האנושית הייתה שנויה במחלוקת אצל מספר גורמים בצבא ובקהילת המודיעין של ארצות הברית, וכן בקרב האקדמיה. הפולמוס שהתקיים בתוך הצבא ובמרחב האקדמי והציבורי הוביל לסיקור תקשורתי משמעותי ולדיון ער סביב השימוש במדעי החברה לצורכי הביטחון הלאומי.⁶⁹

ביקורת במערכת הצבאית

הביקורת על פרויקט התכסית האנושית בתוך המערכת הצבאית נמתחה בעיקר על ידי דרגים זוטרים בצבא האמריקאי⁷⁰ ומספר חוקרי מדעי החברה שלקחו

65 שם.

66 שם.

67 Sims, "The Life and Death of the Human Terrain System".

68 Thomas G. Mahnken, "The Military and the Academy", *Foreign Affairs*, May 6, 2016.

69 McFate and Fondacaro, "Reflections on the Human Terrain System", p. 64.

70 Ben Connable, "How the Human Terrain System is Undermining Sustainable Military Cultural Competence", *Military Review* 89, no. 2 (2009): 57-64, https://www.wired.com/images_blogs/dangerroom/files/MilitaryReviewConnableApr09.pdf.

- חלק בפעילות המערכת. אלה טענו כי הצבא נכשל ביישום הפרויקט בשל "חוסר מקצועיות והיעדר ארגון ויכולת כללית מצד הצוות, הקבלנים ומנהלי [הפרויקט]"⁷¹. בעקבות הביקורת המקצועית, הציגו פיקולסקי, אורטון, לאמב ודייוויס מספר הבחנות ומסקנות בנוגע לתכנונה, פיתוחה ויישומה של מערכת התכסית האנושית:
- הפנטגון היה איטי בגיבוש תוכנית שנועדה לספק ידע חברתי-תרבותי למפקד כוחות היבשה. צוות התכסית האנושית הראשון הוצב יותר מחמש שנים לאחר תחילת מבצע "חופש מתמשך" (Enduring Freedom) נגד ארגון "אל-קאעדה" באפגניסטן, שהחל באוקטובר 2001.
 - מערכת התכסית האנושית שרדה רק מכיוון שלארגון חדש – "הסוכנות המשותפת למיגור איומים מאולתרים" (Joint Improvised-Threat Defeat Agency)⁷² – הייתה הגמישות להקצות משאבים לרעיונות חדשים ומבטיחים ולהגדיר את המשימה באופן רחב, לצורך השקת תוכנית עתירת כוח אדם במערכת המתמקדת בעיקר בטכנולוגיה חדשה.
 - "פיקוד ההכשרה והתורה של צבא היבשה של ארצות הברית" התקשה לעמוד בדרישות הגוברות לצוותי תכסית אנושית מצד המפקדים בשטח.
 - מערכת התכסית האנושית חסרה בסיס תיאורטי המגובה בניסיון בשטח, בו ניתן היה להשתמש כדי לעדכן את תוכנית ההכשרה ולהדריך מפקדים כיצד למצות את הפוטנציאל של צוותי התכסית האנושית.
 - מערכת התכסית האנושית שרדה בשל הערכת המפקדים את תרומתם של הצוותים שהפעילו אותה. הערכת המפקדים העידה על דלות הידע החברתי-תרבותי בקרב כוחות הצבא האמריקאי, כך שאפילו התרומה המוגבלת של מערכת התכסית האנושית התבררה כחיונית.⁷³
- סימס מוסיף על דברים אלה כי מערכת התכסית האנושית הייתה בסופו של דבר "קורבן של הצלחתה שלה". במקום להקים חמישה צוותים במהלך שנתיים, כפי שתוכנן מראש, הצבא האמריקאי הקים יותר מעשרים צוותים. כתוצאה מכך, "צוותים רבים נשלחו לשטח עם ציוד לא מספיק, ורק מספר קטן שלהם הצליח להשלים את משימותיו באופן סביר". כך, למשל, היו מקרים רבים שבהם אנשי האקדמיה לא הצליחו לערוך מחקר שיטתי ונאלצו להסתפק במצגות PowerPoint

Zenia Helbig, *Personal Perspective on the Human Terrain Systems Program*, The AAA's Annual Conference, 2007, https://www.wired.com/images_blogs/dangerroom/files/aaa_helbig_hts.pdf.

72 הכוונה במינוח זה היא לאיומים מסוג מטעני צד ודומיהם.

Christoper Lamb, James Douglas Orton, Michael Davis and Theodore Pikulsky, "The Way Ahead for Human Terrain Teams", *Joint Force Quarterly* 70, no. 3 (2013): 25-26, http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-70/JFQ-70_21-29_Lamb-et-al.pdf.

שטחיות. פערי התרבות (המתודולוגית) בין האקדמיה ובין הצבא גרמו, לדברי סימס, לשיבושים רבים בתקשורת ביניהם.⁷⁴ בנוסף, היו חוקרי מדעי החברה שקבלו על היעדר נגישות מספקת לאוכלוסיות המקומיות שהיו בטיפולם, וזאת בשל הצורך של הצבא לשמור על תוכניות ההיסעים שלו בצורה עמומה שלא תסגיר אותן. היו אנשי אקדמיה שהצליחו לעבד מידע לפני תחילת המשימה, אך הקצב המהיר של הפעולות הצבאיות הגביל את יכולתם להשפיע על התכנון.⁷⁵

ביקורת במרחב האקדמי

רבים במרחב האקדמי ראו את מערכת התכסית האנושית כבעייתית ומעורפלת מבחינה אתית ואקדמית, והיו מי שתיארו אותה כלא אקדמית ולא מודיעינית.⁷⁶ רוב הטענות נגד השימוש במידע התרבותי-חברתי בשעת מלחמה התמקדו בבעייתיות של שליטה על אוכלוסיות, לוחמה פסיכולוגית או סימון אנשים למטרות כליאה, התנקשויות ושיטות אלימות אחרות, תוך הסתייעות במתודולוגיות ובחוקרים מהאקדמיה. חלק מהמתנגדים השוו בין מערכת התכסית האנושית לבין מבצעים ופעולות שנויות במחלוקת שביצעה בעבר סוכנות הביון המרכזית (CIA) במזרח אסיה ובאמריקה הלטינית. בנוסף, אותם מבקרים טענו שישנן ראיות לכך שמערכת התכסית האנושית גרמה לתוצאות הרסניות בקרב האוכלוסייה המקומית, ובכללן מעשי אלימות, חלוקה מחדש של אוכלוסיות והרעלה חקלאית. זאת, אף על פי שאין ממצאים המצביעים על כך שהמערכת פעלה או תכננה לפעול בדרך זו.⁷⁷ האגודה האמריקאית לאנתרופולוגיה (AAA) הסתייגה משימוש באנתרופולוגים במערכת התכסית האנושית, בשל מה שהיא תפסה כמיליטריזציה של התחום המדעי/אקדמי ו"שימוש לא מקובל במומחיות אנתרופולוגית".⁷⁸ במרס 2010 שלחה האגודה עצומת מחאה לבית הנבחרים ולסנאט של ארצות הברית, בה נכללו ארבע טענות עיקריות נגד מערכת התכסית האנושית:

- אין הוכחה לכך שמערכת התכסית האנושית היא תכליתית.

74 Sims, "The Life and Death of the Human Terrain System"

75 שם.

76 *Final Report on The Army's Human Terrain System Proof of Concept Program* (AAA Commission on the Engagement of Anthropology with the US Security and Intelligence Communities, 2009).

77 Medina, "From Anthropology to Human Geography", pp. 142-143.
78 *American Anthropological Association's Executive Board Statement on the Human Terrain System Project* (American Anthropological Association, 2007).

- זוהי מערכת מסוכנת – שלושה אנשי מדעי החברה נהרגו בשטח (נכון לשנת 2009), אחרים התלוננו על הכשרה לקויה, ואילו אנשי צבא התלוננו שההגנה על צוותי התכסית האנושית מעמידה את חייהם של הלוחמים בסכנה.
- היא מבזבזת כספי ציבור.
- היא אינה אתית מבחינתם של אנתרופולוגים ואנשי מדעי החברה האחרים, מכיוון שהיא מפרה את תקני המחקר המדעי והפדרלי, לפיהם חלה חובה להסכמה של מושאי המחקר.⁷⁹

מערכת התכסית האנושית בצבא האמריקאי – מבט לעתיד

בשנת 2015 פורסמו דיווחים על סיומו לכאורה של פרויקט מערכת התכסית האנושית.⁸⁰ למרות זאת, הממשל האמריקאי אישר בתקציבו לשנת 2015 הקצאה לתוכנית ניסיונית של התכסית האנושית עבור הפיקוד הפסיפי של ארצות הברית, שאמורה הייתה להסתיים ב־30 בספטמבר 2016.⁸¹ יתרה מזאת, במאוס 2016 הצהיר פקיד בכיר במשרד ההגנה של ארצות הברית כי לא ברור מדוע הצבא האמריקאי טען שפרויקט התכסית האנושית הסתיים; לא רק שהפרויקט עודנו קיים, אלא שהצבא יוכל להרחיבו אם יוזרם אליו תקציב נוסף.⁸²

תפיסת התכסית האנושית והמודיעין התרבותי בהקשר הישראלי

ישראל עושה שימוש דומה לזה שעושה הצבא האמריקאי במערכת התכסית האנושית בהתמודדותה מול שחקנים דומים וזירות דומות במזרח התיכון – גורמי אסלאם קיצוני וארגוני טרור. ברם, לצד הדמיון, ישנם הבדלים משמעותיים בין שני הצדדים, שיש לתת עליהם את הדעת. ראשית, ארצות הברית נלחמת ביבשות מרוחקות מהיבשת האמריקאית, ואזרחיה כמעט ואינם מושפעים ממלחמות אלו בחיי היומיום שלהם. לעומת זאת, המאבק של ישראל הוא אינטנסיבי, נערך בזירות הנמצאות או בתוך מדינת ישראל עצמה או סביב גבולותיה, הינו מוחשי יותר, ונושא אופי קיומי-הישרדותי. החברה האזרחית הישראלית מעורבת במלחמות אלו ומושפעת מהן יחד עם כוחות הביטחון הישראליים, וזאת הרבה יותר מאשר מקביליהם בארצות הברית.

79 שם.

Tom Vanden Brook, "Army kills controversial social science program", *USA TODAY*, 80 June 29, 2015, <http://www.usatoday.com/story/news/nation/2015/06/29/human-terrain-system-afghanistan/29476409/>.

Roberto Gonzalez, "The Rise and Fall of the Human Terrain System", *Counterpunch*, 81 June 29, 2015, <http://www.counterpunch.org/2015/06/29/the-rise-and-fall-of-the-human-terrain-system/>.

Tom Vanden Brook, "725M\$ program Army 'killed' found alive, growing", *USA TODAY*, 82 March 9, 2016.

שנית, הטיפול של הסוכנויות והמוסדות האמריקאיים בנושא תרבות האויב שאתו מתמודדת ארצות הברית הוא תחום חדש יחסית. לעומת זאת, המוסדות והגופים בישראל העוסקים בהיבטים השונים של חיי היומיום של האוכלוסייה הערבית במדינה ובשטחי יהודה ושומרון ורצועת עזה הם ותיקים יותר, נמצאים במגע אינטנסיבי עם אוכלוסייה זאת וחשופים לתרבותה ומאפייניה לאורך עשרות שנים. אופי האתגרים הניצבים בפני ישראל, המנהלת אורח חיים מערבי, מחייב אותה, ככורח קיומי והישרדותי, להכיר לעומק את התרבויות השונות במרחב ואת דרכי חשיבתן. זאת, מתוך מטרה להבין טוב יותר עם מי היא מתמודדת מבחינה צבאית ומדינית ולהתארגן ביעילות כדי לתת מענה הולם לכך.

חשיבות הכרת התרבות ומאפייני האוכלוסייה המקומית על ידי צה"ל וכוחות הביטחון בישראל

במסמך "אסטרטגיית צה"ל", שפורסם באוקטובר 2015, צוין כי בין האתגרים העומדים לפתחו של הצבא נמצאים "ירידת איום הצבאות הסדירים המדינתיים ועליית האיום של ארגונים תת-מדינתיים, בלתי סדורים או סדורים למחצה, השואפים להפוך לישויות שלטוניות", וכן "פריסה והיטמעות האויב באזורים אזרחיים מיושבים".⁸³ אתגרים אלה, המעמידים את צה"ל בפני מצבים של לחימה בתוך מרחב מאוכלס בצפיפות, מחייבים אותו להכיר את התרבות של אותה אוכלוסייה, שממנה גם יוצאים ארגוני הטרור שאתם הוא מתמודד. היכרות שטחית ולא מספקת עם תרבות האויב עלולה לגרום לטעויות אסטרטגיות ומבצעיות. מתאם פעולות הממשלה בשטחים, אלוף יואב מרדכי, התייחס לשינוי באופי הלחימה בשדה הקרב. לדבריו:

האוכלוסייה היא היום מרכיב מרכזי בכול ניתוח של שטח בתפיסה הצה"לית. בעבר היו מנתחים את האויב ואת תוואי הקרקע. היום הבנת האוכלוסייה, ההיכרות, הכרת התשתית ואפשרויות הפינוי שלה הם משפיעים מרכזיים בכול מבצע. לפני מבצע אנחנו מבצעים מיפוי של אתרים רגישים [...] זה לא אומר שהוא לא יכול לפגוע במקום במידה והוא מרגיש מאוים. המרכיב של הסיוע האזרחי הוא בראש ובראשונה שיקול ערכי, כי אין לנו כוונה לפגוע באזרחים חפים מפשע, אך משימה נוספת היא לאפשר אורך נשימה כדי לאפשר לצבא לעמוד ביעדים המבצעיים.⁸⁴

83 אסטרטגיית צה"ל (תל אביב: צה"ל, לשכת הרמטכ"ל, אוגוסט 2015), http://www.idf.il/sip_storage/files/9/16919.pdf.

84 יפתח כרמלי, "המתפ"ש: האוכלוסייה האזרחית היא מרכיב מרכזי בניתוח השטח לפני מבצע", אתר צה"ל, 2 בדצמבר 2014, <http://www.idf.il/1133-21547-HE/IDFGDover.aspx>.

על חשיבותה וחיוניותה של הכרת השטח ותרבותה של האוכלוסייה המקומית על ידי הצבא עמד גם הרמטכ"ל, רביאלוף גדי איזנקוט, כשהסביר:

הנטייה הראשונית היא לטפל בהתרחשויות החדשות על ידי הכנסתן לתבניות המוכרות מן העבר. אך יש לדעת שמדובר במצב חדש, שכדי להתמודד אתו צריך להבין את זרמי העומק הפועלים בחברה הפלסטינית. צבאות וארגוני מודיעין מתמקדים בדרך כלל בשני קטבים: קוטב אחד כולל את מקבלי ההחלטות ומערכות הפיקוד של היריב, והקוטב השני את יכולותיו. זרמי עומק הפועלים אצל הצד השני הם נושא קשה להבנה, ודווקא הם המטרידים ביותר.⁸⁵

שינויים שהתרחשו בזירה הפלסטינית בשנים האחרונות חידדו עוד יותר את חשיבותו של הידע התרבותי, במיוחד של מבנה הכוח החברתי-פוליטי ומאפייני הזיקות בין קבוצות האוכלוסייה השונות. בבסיס השינויים עומדת חולשתה הפוליטית והמוסדית של הרשות הפלסטינית, שאינה מצליחה לנהל בהצלחה את השטחים שבידיה.⁸⁶ חולשה זו באה לידי ביטוי במאבקי כוח פנימיים, ובכללם אלימים, ובהתפתחות של מבני כוח אלטרנטיביים בעלי מאפיינים שונים וייחודיים לכול מרחב גיאוגרפי ו/או דמוגרפי בשטחי הרשות.⁸⁷

85 גדי איזנקוט, "אתגרי צה"ל 2015–2016", **צבא ואסטרטגיה**, כרך 8, גיליון 1 (יולי 2016), עמ' 5–16, <http://www.inss.org.il/uploadImages/systemFiles/ArmyStrategics8-1.01>, LtGenEizenkot.pdf.

86 להרחבה בנוגע לדפוס הכישלון המדינתי של הרש"פ ראו: קובי מיכאל ויואל גוז'נסקי, **המרצב הערבי בנתיב הכישלון המדינתי** (תל אביב: המכון למחקרי ביטחון לאומי, אוניברסיטת תל אביב, 2016), עמ' 111–122.

87 להרחבה בנושא זה ראו: פינחס ענברי, "הרשות הפלסטינית ממשיכה להתפורר", **המרכז הירושלמי לענייני ציבור ומדינה**, 26 ביוני 2016, <http://jcpa.org.il/2016/06/%D7%94%D7%90%D7%99%D7%A8%D7%A9%D7%95%D7%AA-%D7%94%D7%A4%D7%9C%D7%A1%D7%98%D7%99%D7%A0%D7%99%D7%AA-%D7%9E%D7%9E%D7%A9%D7%99%D7%9B%D7%94-%D7%9C%D7%94%D7%AA%D7%A4%D7%95%D7%A8%D7%A8/>

פינחס ענברי, "האם מתגבש כוח פוליטי פרו ירדני בהר חברון?", **המרכז הירושלמי לענייני ציבור ומדינה**, 1 ביוני 2016, <http://jcpa.org.il/2016/06/%D7%94%D7%90%D7%9D-%D7%9E%D7%AA%D7%92%D7%91%D7%A9-%D7%9B%D7%95%D7%97-%D7%A4%D7%95%D7%9C%D7%99%D7%98%D7%99-%D7%A4%D7%A8%D7%95-%D7%99%D7%A8%D7%93%D7%A0%D7%99-%D7%91%D7%94%D7%A8-%D7%97%D7%91%D7%A8%D7%95/>

פינחס ענברי, "מחנות הפליטים – איום גובר על יציבות הרשות הפלסטינית", **המרכז הירושלמי לענייני ציבור ומדינה**, 9 באוגוסט 2015, <http://jcpa.org.il/2015/08/%D7%9E%D7%97%D7%A0%D7%95%D7%AA-%D7%94%D7%A4%D7%9C%D7%99%D7%98%D7%99%D7%9D-%D7%90%D7%99%D7%95%D7%9D-%D7%92%D7%95%D7%91%D7%A8-%D7%A2%D7%9C-%D7%99%D7%A6%D7%99%D7%91%D7%95%D7%AA-%D7%94%D7%A8%D7%A9%D7%95/>

בנוסף לשינויים בחברה ובפוליטיקה הפלסטינית, אירועי "האביב הערבי" הביאו לשינויים גיאופוליטיים גם במדינות שונות במרחב המזרח התיכון. שינויים אלה יצרו מצב חדש לישראל, בו היא נאלצת להסתגל למציאות שבה רוב האיומים המופנים כלפיה לא באים ממדינות, אלא ממערכות וממחנות על-לאומיים ותת-לאומיים. איומים אלה נובעים מהפיצול, מהגיוון, מהמורכבות ומריבוי האינטרסים של השחקנים השונים באזור. מצב זה מחייב את המודיעין הישראלי להסתכל על המפה המזרח תיכונית באופן שונה מזה שהורגל אליו עד כה. יתרה מכך, על המודיעין הישראלי להיערך לשינויים נוספים שעשויים להתרחש, שכן המרחב דינמי ואינו יציב.⁸⁸

יעקב עמידור מדגיש כי השינויים המשמעותיים באזורנו מחייבים "ישיבה על המדוכה, חשיבה וניסיון להבין מה צריך לשנות על מנת להתמודד טוב יותר במצב החדש שנוצר". לדבריו, המסגרות הישנות, המדינות, האידיאולוגיות, הבריתות והכללים נעלמו, והמציאות החדשה מעוצבת, במידה רבה, על ידי תהליכים סוציולוגיים עמוקים, הנובעים מהתנהגותו של ההמון ולא מהחלטות של מנהיגות בישות היררכית. חלק ניכר מהאויבים אתם מתמודדת ישראל כבר אינם מדינות. נוסף לכך הקושי הנובע מהתפתחותה של טכנולוגיה חדשה: העולם החדש בנוי על האינטרנט והסייבר, כך שהתקשורת והמחשבים יוצרים עולם מודיעיני חדש עם הזדמנויות ואתגרים רבים.⁸⁹ לדברי עמידור, "התוצאה מבחינת המודיעין היא שחלק ניכר מהניסיון העצום שנצבר במערכת אינו רלוונטי. כך, למשל, יש חשיבות להבין היטב את המאבק בין השיעה לבין הסונה בתחילת התגבשותו של האסלאם, יותר מאשר את המאבק בין מצרים לבין סוריה לפני שלושים וארבעים שנה. תופעות חדשות מחייבות מבט אחר".⁹⁰

התפתחויות אלו משקפות את המציאות המורכבת בזירות עימות סמוכות מאוד לישראל ואת החשיבות של יצירת תשתית ידע רחבה ומבוססת על החברות הערביות, מבנה הכוח שלהן, התרבות הפוליטית והלכי הרוח בהן, וזאת לצורך הבטחת הרלוונטיות המבצעית.

בישראל פועלים שני גופים עיקריים הבאים במגע עם האוכלוסייה הפלסטינית ועם מוסדות הרשות הפלסטינית ומהווים מוקדי ידע בסוגיות הנוגעות אליהם: מפקדת מתאם פעולות הממשלה בשטחים (מתפ"ש) ושירות הביטחון הכללי (שב"כ).

88 יוסי קופרווסר, "מתאר האיומים הנוכחיים", **דיונים בביטחון לאומי**, גיליון 30 (אוגוסט 2016), עמ' 9-15, <http://besacenter.org/wp-content/uploads/2016/09/CSD30web.pdf>.

89 יעקב עמידור, "אתגרי המודיעין", **דיונים בביטחון לאומי**, גיליון 30 (אוגוסט 2016), עמ' 23-28, <http://besacenter.org/wp-content/uploads/2016/09/CSD30web.pdf>.

90 שם.

מתאם פעולות הממשלה בשטחים

מתפ"ש אחראי לתיאום פעילות משרדי הממשלה, צה"ל וגורמי הביטחון מול הפלסטינים, תוך יישום המדיניות הממשלתית בתחומים האזרחיים הנוגעים להם. בנוסף, עוסק מתפ"ש בקידום נושאים הומניטריים, פרויקטים תשתיתיים ופרויקטים כלכליים בגדה המערבית וברצועת עזה.⁹¹ תחת מתאם פעולות הממשלה בשטחים פועל מטה, הכולל ענפים העוסקים בכלכלה, בתשתיות, בארגונים בין-לאומיים ובקשרי חוץ, וכן משרד לפניות הציבור, לשכת דובר ומשרד היועץ לענייני פלסטינים. בית הספר לתיאום וקישור של היחידה עוסק בהכשרת הדור הבא של מפקדי התיאום והקישור ובהעברת קורסים בערבית ליחידות שונות במערכת הביטחון. ביהודה ושומרון פועל תחת פיקוד המתפ"ש המינהל האזרחי, שמרכז את הפעילות מול הפלסטינים ומול היישוב היהודי שם. למול רצועת עזה פועלת מינהלת תיאום וקישור, האחראית לתיאום האזרחי, הכלכלי והביטחוני עם הצד הפלסטיני.⁹²

קורס קציני המינהל האזרחי כולל הרצאות רבות על האסלאם, החברה הפלסטינית ויסודות הסכסוך, רכישת השפה הערבית והבנת תפקדיהם של שלל הארגונים הבין-לאומיים הפועלים במרחב. לאלה יש להוסיף הקניית הבנה מעמיקה בדיני המלחמה ובמשפט הבין-לאומי, שלא פעם מהווים בסיס לפעילות צה"ל בשטחים.⁹³ קציני המינהל האזרחי במחוזות השונים מקיימים קשרים ודיאלוגים רציפים עם גורמים רשמיים של הרש"פ ועם גורמים לא רשמיים מקרב האוכלוסייה הפלסטינית. ערוצי תקשורת עם גורמים לא רשמיים בחברה האזרחית הפלסטינית מסייעים לפיתוח תשתית הידע על האוכלוסייה המקומית, וההתנהלות בין הצדדים, במקביל למגעים עם גורמי שלטון פלסטיניים, מסייעת לשמר את התיאום ביניהם, להעמיקו ולהתאימו לשינויים ולהתפתחויות.⁹⁴

ראש המינהל האזרחי ביהודה ושומרון לשעבר, תא"ל דוד מנחם, התייחס לחשיבות הידע התרבותי ותרומתו לתכלית המבצעית של צה"ל בהקשר של מבצע "שובו אחים", שבו פעל הצבא ברחבי יהודה ושומרון במטרה לאתר שלושה נערים יהודים שנחטפו ואחר כך התברר שנרצחו בידי מחבלים פלסטינים. ההבנה שהעיר חברון נחשבת לאחד מהמעוזים הבולטים ביותר של תנועת חמאס ביהודה ושומרון

91 מתאם פעולות הממשלה בשטחים, **אתר צה"ל**, <http://www.cogat.idf.il/896-he/IDFG.aspx>.

92 שם.

93 אנשיל פפר, "צה"ל מנסה לשפר הטיפול בפלסטינים", **הארץ**, 5 בנובמבר 2010, <http://www.haaretz.co.il/news/politics/1.1228496>.

94 לירן אופק, "התיאום הביטחוני (עדיין) כאן", **שורטי, ביטחון בגובה העיניים**, המכון למחקרי ביטחון לאומי, 12 באוקטובר 2015, <http://heb.inss.org.il/index.aspx?id=5193&Blogid=10749>.

נבעה, לדברי מנחם, מכך ש" [...] האוכלוסייה הערבית בחברון יותר מסורתית, דתית ופחות ליברלית ממה שתמצא ברמאללה, למשל, והחיבור לתנועה איסלאמיסטית כמו החמאס הוא טבעי [...] זה לא אומר שתושבי חברון הם טרוריסטים, אבל המצע התרבותי-דיאולוגי יותר קרוב למה שהחמאס מציע".⁹⁵

ידע תרבותי זה הביא את צה"ל להחליט לא לפגוע בשגרת חייה של האוכלוסייה הפלסטינית באזורים אחרים ביהודה ושומרון במהלך המבצע הצבאי, ולהמשיך ולנפק אישורי עבודה שם. סגן ראש מינהלת התיאום והקישור בחברון, רס"ן משה טטור, הסביר כי אם אירוע בסדר גודל של מבצע "שובו אחים" היה מתרחש מספר שנים לפני כן, אופן הפעולה של צה"ל היה שונה.⁹⁶ את השינוי ניתן לייחס לתרומת הידע התרבותי שנבנה במהלך השנים.

שירות הביטחון הכללי

מוקד ידע תרבותי נוסף בישראל הוא שירות הביטחון הכללי. חלק מרכזי בהכשרת הרכזים בארגון מתחיל ב"אולפן" – בית הספר לשפות של השירות הקיים זה 45 שנים. במהלך הכשרתם רוכשים הרכזים מיומנות גבוהה בשפה הערבית ונחשפים לממדים שונים של ההקשר התרבותי, ובכלל זה הממד הדתי, של החברה הפלסטינית.⁹⁷ מטען הידע התרבותי של הרכזים מתפתח ומשתכלל עם הניסיון המבצעי שהם רוכשים בשטח, גם אם בשנים האחרונות מדובר ב"למידה מרחוק", בגין נגישות מוגבלת למרכזי האוכלוסייה הפלסטינית, בעיקר ברצועת עזה. במבצע "צוק איתן" התלוו רכזי שב"כ לקציני חטיבת הנח"ל במהלך כיבוש שטח בצפון הרצועה. קציני החטיבה התרשמו מאוד מרמת הבקיאיות שהפגינו הרכזים ושיבחו את היקף הידע שלהם ושליטתם בשטח, למרות שכף רגלם מעולם לא דרכה בבית חנון.⁹⁸

תרומה דומה ניתן לייחס לחוקרי שבויים, הנלווים אל הכוחות הלוחמים ואמונים על מיצוי מודיעין מחקירת שבויים בשטח, ומודיעין מעמיק ורחב יותר באמצעות חקירת שבויים המועברים למחנות שבויים בעורף. תהליכי ההכשרה המקצועית של חוקרי השבויים מקנים להם היכרות מעמיקה יחסית עם היבטים תרבותיים, ככלי נדרש להתמודדות עם נחקרים.

ראש השב"כ לשעבר, יעקב פרי, הסביר כי "אתה חייב היכרות מעמיקה עם השטח שעליו אתה אחראי. אתה צריך להיות פרופסור לתא השטח שלך, ואתה חייב להכיר את האוכלוסייה המגוונת שחיה בו מבחינה סוציאו-קונומית, כלכלית,

95 יפתח כרמלי, "שנה ל'שובו אחים': כך השפיע המבצע על האוכלוסייה הפלסטינית בחברון", אתר **צה"ל**, 6 בדצמבר 2015, <http://www.idf.il/1133-22312-HE/IDFGDover.aspx>.

96 שם.

97 אמיר בוחבוט, "חשיפה: עולמם הסודי של אנשי הצללים שנלחמים בטרור", **וואלה**, 24 באפריל 2015, <http://news.walla.co.il/item/2843137>.

98 שם.

פוליטית וחברתית. להכיר את החמולות והארגונים המשפיעים, את הרחובות ואת כל הפרטים שיעזרו לך לשלוט בשטח".⁹⁹

למרות העדויות להתפתחותה של מודעות לחשיבותו של הממד התרבותי בקרב הארגונים שתוארו לעיל, ממד זה עדיין אינו מפותח ומשפיע דיו בתהליכי עבודת המודיעין (איסוף, עיבוד והפצה) שלהם, בעיקר בהיבטים המקרו חברתיים. מהות המודיעין התרבותי טרם הוטמעה בתהליכי ההכשרה, בניין הכוח ותורת ההפעלה של המתפ"ש, המינהל האזרחי בשטחים והשב"כ, והיא גם לא תורגמה לשיתוף פעולה שגרתי, סדור ושיטתי עם חוקרים באקדמיה ולשילוב שלהם במערך המחקר המודיעיני ברמות השונות.

סיכום ומסקנות

מערכת התכסית האנושית בצבא האמריקאי נוצרה והתפתחה בשל האתגרים שהציבה הלחימה בזירות רוויות באוכלוסייה אזרחית. המעבר ממלחמה קלאסית למלחמה בטרור הג'יהאדיסטי, למבצעים נגד התקוממות ולמבצעים לשמירת שלום ביבשות ובמדינות אחרות, אילץ את הכוח הלוחם לשנות את דפוסי פעילותו. השינוי הוביל לצורך במודיעין איכותי על היריב הלא מדינתי, הפועל מתוך האוכלוסייה האזרחית ובחסותה.

הבנה מעמיקה של התרבות המקומית הפכה לתנאי הכרחי להבטחת הרלוונטיות של המשימה הצבאית. המודיעין התרבותי, כחיבור בין הידע התרבותי שנוצר באמצעות מערכת התכסית האנושית ובין המודיעין הנדרש לצורך ביצוע המשימה הצבאית, התברר כחיוני ביותר. כדי להבטיח איכויות גבוהות של מודיעין תרבותי, נדרשות מודעות ורגישות תרבותית, שהן ביטוי של אינטליגנציה תרבותית.

ההכרה בחשיבות המודיעין התרבותי הובילה את הצבא האמריקאי, הפועל בעשורים האחרונים בזירות מרוחקות (גיאוגרפית ותרבותית) ומורכבות כמו עיראק, אפגניסטן וסוריה, לפתח את מערכת התכסית האנושית. מערכת זו מושתתת על צוותים מקצועיים של אנשי מדעי החברה המצוותים לכוחות ברמות השונות, ותפקידה הוא לתרום להבנת התרבות והחברה בזירות הלחימה.

מפקדים ואנשי צוות שלקחו חלק בתוכנית התכסית האנושית הסכימו שהיא תורמת לרלוונטיות של המשימה הצבאית ולהצלחתה. אלא שלצד החשיבות שיוחסה למערכת זאת, הפעלתה עוררה גם ביקורת, הן במרחב הצבאי והן במרחב האקדמי. חרף הביקורות, ובניגוד לדיווחים על ביטול התוכנית, הודיע משרד ההגנה האמריקאי כי היא תימשך, וייתכן שאף יוקצו לה משאבים נוספים.

מאחר וסביר להניח שארצות הברית תמשיך להיות מעורבת במבצעים נגד התקוממות ונגד טרור במזרח התיכון, במיוחד לאחר עלייתה והתחזקותה של

"המדינה האסלאמית" והתחייבות הקואליציה המערבית בראשותה להשמדה, הצורך בהבנת החברה והתרבות בזירות הפעולה ימשיך להיות משמעותי. הבנה כזו יכולה להיות חשובה גם לצורך שימור הבריתות הקיימות של ארצות הברית ופיתוח יחסים מדיניים חדשים באסיה, באירופה, באפריקה ובדרום אמריקה. המודיעין התרבותי מתברר כתשומה הכרחית בעידן ה"מלחמות בקרב אנשים". למרות זאת, ולמרות ההתפתחויות המתודולוגיות, המבצעיות והארגוניות של מערכת התכסית האנושית בהקשר האמריקאי, עדיין קיימים בה פערים, והתוצרים שהיא מפקה הם, במקרים רבים, בלתי מספקים. גם בקרב גופי הביטחון והמודיעין בישראל קיימים פערי ידע בנושאים תרבותיים, והטמעתם בתורת הלחימה ובמתודולוגיה המודיעינית אינה מיטבית. לאור מאפייני הלחימה של צה"ל בסביבות רוויות אוכלוסין, מומלץ לפתח יכולות של איסוף ומחקר, לצד מתודולוגיות ותהליכי הכשרה בתחום הידע התרבותי בזירות השונות. זאת, תוך הסתייעות באנשי מדעי החברה ושילובם הן בתהליכים והן במסגרות הארגוניות. דבר זה יאפשר פיתוח ושיפור תשתית הידע על התרבויות השכנות.

"גישה שיתופית" ביחסי מודיעין-קברניט ברמה הלאומית: האם יש לה תוחלת?

דודי סימן טוב ושי הרשקוביץ

קיים ויכוח בשיח המודיעיני בשאלה איזו מידת קרבה צריכה להתקיים בין אנשי המודיעין ובין הקברניטים, ומה צריך להיות היחס בין שאיפתו של איש המודיעין להשפיע על תהליך קבלת ההחלטות ובין מחויבותו המקצועית הראשית ליצירת מודיעין המשקף, ככול האפשר, את המציאות. בהמשך לכך נוספו עוד שאלות: האם מחויבותו המקצועית הראשית של איש המודיעין היא רק לייצר מודיעין או גם להיות שותף פעיל בעיצוב מדיניות, והאם המודיעין האסטרטגי הינו תוצר של גורמי המחקר בקהילת המודיעין או שהינו תוצר של שיח שבו הקברניט משפיע ומושפע, ובסיומו נוצר ידע אסטרטגי חדש המאפשר גיבוש מדיניות לאומית?

טענתנו המרכזית במאמר זה היא שהדרך הנכונה לפתח ידע שישמש לגיבוש מדיניות ברובד האסטרטגי היא בצורה שיתופית – במפגש בין איש המודיעין ובין מקבל ההחלטות. אלא שהיעדר תנאים מתאימים בסביבה שבין המודיעין לקברניט מונע זאת במקרים רבים. לפיכך, יש להכיר במוגבלות היכולת של קהילת המודיעין והדרג המדיני לפעול בצורה שיתופית ולפתח מסגרת של מנגנונים ותהליכי למידה שיהפכו אותה לאפשרית, תוך מזדעות למגבלותיה ולמאפייני הסביבה האסטרטגית גם יחד.

המאמר יסקור את הגישות המרכזיות הנוגעות לממשק בין הקברניט ובין המודיעין – הגישות המסורתיות מול מה שאנו מכנים "הגישה השיתופית" – ויציע גישה הרואה בעבודת המודיעין ברמה הלאומית פרויקט משותף לאנשי מודיעין ולקברניטים. במקביל, יעמוד המאמר על המתחים והמכשולים העומדים בפני יישומה של גישה זאת ויציע דרכים אפשריות להסדרים.

מילות מפתח: מודיעין אסטרטגי, מודיעין לאומי, קהילת המודיעין, יחסי מודיעין-קברניט, מעגל המודיעין

דודי סימנטוב הוא חוקר בכיר במכון למחקרי ביטחון לאומי. ד"ר שי הרשקוביץ הוא מרצה למדע המדינה באוניברסיטת תל אביב.

מבוא

רבות נכתב על מערכת היחסים המורכבת בין קברניטים ומצביאים ובין אנשי המודיעין. כבר בעשור הרביעי של המאה העשרים, עם הקמת הממסדים המודיעיניים הלאומיים, החלו בארצות הברית ניסיונות חלוציים לקביעה והסדרה של התורה המודיעינית בהקשרה למרחב שבין הקברניט למודיעין. עיקר הוויכוח, אז כהיום, נסוב סביב השאלה באיזו מידת קרבה על אנשי המודיעין לעבוד עם הקברניטים, ומה היחס בין שאיפתו של איש המודיעין להשפיע על תהליך קבלת ההחלטות לבין מחויבותו המקצועית הראשית ליצירת מודיעין המשקף ככול האפשר את המציאות. בהמשך נוספו שאלות כמו: האם מחויבותו המקצועית הראשית של איש המודיעין היא רק לייצר מודיעין או שמא הוא אמור להיות שותף פעיל בעיצוב מדיניות, והאם המודיעין האסטרטגי הינו תוצר של גורמי המחקר בקהילת המודיעין או תוצר של שיח שבו הקברניט משפיע ומושפע, ובסיומו נוצר ידע אסטרטגי חדש המאפשר גיבוש מדיניות לאומית.¹

כבר מראשית ימי המודיעין כמוסד ממלכתי שנועד, בין השאר, לספק מודיעין אסטרטגי, נשאלו שאלות באשר למהותו ברמה האסטרטגית: מה מקומו בקבלה והוצאה לפועל של מדיניות?; האם הוא עומד בפני עצמו, כלומר מייצר תוצר המנותק לכאורה מעיצוב האסטרטגיה הלאומית, או האם הוא משמש, בלשונו של ראש אמ"ן לשעבר, יהושפט הרכבי, "עזר למדיניות?"² שאלות אלו נוגעות לשני ממדים: הראשון, האופן שבו גורמים מחוץ למערכת המודיעין תופסים את תפקידו ותפקודו של המודיעין; השני, האופן שבו המערכת המודיעינית תופסת את עצמה.

מהו מודיעין אסטרטגי?

עוד בטרם נצלול לסבך היחסים שבין ראשי קהילת המודיעין לקברניטים, מן הראוי לאפיין את המודיעין האסטרטגי כתפוקה המחקרית של גופי המודיעין וכתוצאה של השיח בין המודיעין ובין מקבלי ההחלטות. תפקידו של המודיעין האסטרטגי הוא לסייע לקברניטים בגיבוש תפיסות עולם, בעיצוב מדיניות ובקבלת החלטות בתחומי הביטחון הלאומי. עליו לספק הערכות כדי לסייע ולאפשר לקברניטים להבין את המציאות, לנהל סיכונים ולנצל הזדמנויות. על המודיעין גם לאתגר את המדיניות הנוכחית כאשר הוא מאתר פערים בהבנת הסיבה האסטרטגית,

1 דיון זה הוא הדהוד לפלוגתא רחבה יותר בתחומי לימודי החברה, והיא האם ניתן להפריד את הידע מן היודע, והאם אובייקטיביות ככול האמור לחקירת התנהגויות אנושיות היא דבר אפשרי. דיון מעניין בנושא זה ראו: Richard Bernstein, *Beyond Objectivism and Relativism* (Philadelphia: University of Pennsylvania Press, 1983), pp. 1-50.

2 דוד סימנטוב, שי הרשקוביץ, אמ"ן יוצא לאור (תל-אביב: מערכות, 2013), עמ' 52-53.

בשרטוט המגמות האסטרטגיות וביכולת להעריך את מקומו של המתבונן בסביבה האסטרטגית בעתיד.

שאלה מרכזית שתעמוד בלב מאמר זה נוגעת לנקודת המבט שצריכה להיות לראשי גופי המודיעין בבואם לספק מודיעין אסטרטגי: האם המודיעין, בבואו לספר על ה"אחר", יכול להיות אדיש וסגור ב"מגדל שן מודיעיני" כאשר הוא מתייחס למדיניות הקברניט לו הוא מדווח? האם מעורבות המודיעין במדיניות עלולה לעוות את עיניו ולהטות אותו ממתן מודיעין אסטרטגי רלוונטי, או שמא דווקא הניתוק עלול להביא לכך שהערכותיו יהיו בלתי רלוונטיות, משום שלא יעשו בהן שימוש? האם המודיעין האסטרטגי מתמקד בעשייה מודיעינית בלבד, או שתפקידו הוא לאפשר דיון ולהניע שיח, שבסופו מתגבשת המדיניות ומתקבלות החלטות ברמה הלאומית?

הגישות המסורתיות ליחסי קברניט-מודיעין

הגישה המסורתית גורסת כי על המודיעין להישאר מרוחק ככול הניתן ממקבלי ההחלטות ובלתי תלוי באינטרסים שלהם, אחרת הוא מסתכן בהפיכתו לגורם נוסף, אחד מיני רבים, בדיון על המדיניות, ובכך הוא חוטא פעמיים: ראשית, הוא עשוי להציג תמונה שאינה "אובייקטיבית" ולהטעות את קובעי המדיניות; שנית, הוא יאבד את סמכותו כגורם הראשי המייצג את "המציאות" בדיון האסטרטגי שמוביל מקבל ההחלטות. המייצגים המרכזיים של גישה זו, לפחות בראשיתה, היו ויליאם דונובן, אלן דאלאס ורוסקו הילנקוטר – שלושתם מאבות הביון האמריקאי.³ הם האמינו כי על המודיעין לשמור על ריחוק מסוים (אך לא להיות מנותק) מתהליך קבלת ההחלטות, לבצע מחקר והערכה בלתי תלויים ולהימנע משיפוט מודיעיני ה"תפור" לשיקולים האידיאולוגיים והפוליטיים של מקבל ההחלטות.⁴

גישה זו נתמכה גם על ידי שרמן קנט,⁵ לפחות בראשית דרכו האקדמית, כשכתב בשנת 1949 כי המודיעין ברמה הלאומית הוא גוף "שירותי" (Service Function), ועליו להימנע מהכתמת התוצר המודיעיני בשיפוט סובייקטיביים כתוצאה

3 דונובן כיהן כראש ה-OSS במלחמת העולם השנייה ונחשב לאב המייסד של ה-CIA. הילנקוטר כיהן כראש ה-CIA הראשון, בשנים 1947-1951. דאלאס כיהן כראש ה-CIA בשנים 1953-1961.

4 יש להניח כי הם הושפעו מהשיח הפוזיטיביסטי שרווח באותה עת בקרב אנשי אקדמיה אמריקאים שקידש את החקירה "המדעית" (קרי, האובייקטיבית) בתחום לימודי החברה. סקירה בנושא זה ראו: Peter Halfpenny, *Positivism and Sociology: Explaining Social Life* (London: Allen & Unwin, 1982).

5 שרמן קנט היה פרופסור להיסטוריה באוניברסיטת ייל, לפני שהצטרף במהלך מלחמת העולם השנייה לשירות בן 17 שנה ב-OSS וב-CIA. הוא עמד בראש גוף המחקר של ה-CIA ונחשב לתיאורטיקן הבולט ביותר בתחום המודיעין הלאומי וכמי שעיצב את קהילת הביון האמריקאית. השפעתו ניכרת עד היום בכתיבה על המודיעין ובפרקטיקה המודיעינית.

ממגע ישיר בין צרכן המידע ובין הידע. בכך טבע קנט את התפיסה הרואה באיש המודיעין יצרן ובקברניט צרכן – כלומר, שתי פונקציות נפרדות מהותית ותפקודית. לפי קנט, המודיעין מחויב להגיב לבקשות של מקבל ההחלטות, אך עליו לשמור על עצמאות ואובייקטיביות בתהליך המודיעיני.⁶ בתארו את היחסים בין היצרן והצרכן, עמד קנט על מספר ממדים בעייתיים: ראשית, אצל מקבלי ההחלטות קיימת ספקנות מובנית ביחס למוצר המודיעיני. הדבר נובע מכך שאנשי המודיעין נוטים לקבל אחריות מוגבלת על התוצר המודיעיני (בפרט בכול מה שקשור לתחזיות), מה שאינו תורם למקבלי ההחלטות לבטוח במודיעין שהם מקבלים. לכן סבר קנט כי המודיעין צריך לחדד את תפקידו כמתבונן מן החוץ על התופעה הנחקרת, ולעשות זאת בצורה אובייקטיבית, דבר שיאפשר לקברניט לקבל את ההחלטות הנכונות הנוגעות למדיניות הנחוצה. קרבה רבה מדי בין היצרן ובין הצרכן, טען קנט, תפר את האובייקטיביות של המודיעין, תפגע באמון (המוגבל ממילא) שרווח "הצרכן" ל"יצרן" המודיעין ותעקר את התכלית הבסיסית של המודיעין. כדי לשמור על רלוונטיות, על המודיעין לקיים בכול זאת מידה מסוימת של קרבה למקבל ההחלטות, אך עליו להישמר מלהיות קרוב מדי אליו, כדי לא לאבד את האובייקטיביות והיושרה המקצועית.⁷ היטיב לבטא גישה זאת דונובן שאמר: "המודיעין חייב להיות נפרד מהאנשים אותם הוא משרת, כדי שהחומרים אותם הוא משיג לא יעוותו על ידי השקפות העולם של האנשים המכוונים את הפעילות המודיעינית".⁸

שרמן קנט הציע, לפיכך, למשטר את המגע בין איש המודיעין ובין הקברניט, שכן בהיעדר ערוצי תקשורת ממוסדים, עלולים להיווצר פערי ציפיות בין הצדדים. הוא גם חשש שמקבל ההחלטות יטיל על המודיעין משימות בלתי אפשריות, מה שיגרור גישה אפולוגטית מצד אנשי המודיעין. לכן, יש לדעתו ליצור מנגנונים ולמסד תהליכי עבודה שיאפשרו לקברניט להכווין בצורה מסודרת את עבודת המודיעין. הָכוּונה כזאת תבנה את האמון בין שני הצדדים ותאפשר למודיעין להצליח בתפקידו.

קנט פיתח את תפיסת "מעגל המודיעין", שבה תיאר ממשק מזערי בין אנשי המודיעין ובין הדרג המדיני,⁹ כשרוב תהליך פיתוח הידע והחשיבה מתבצע בתוך ארבע אמותיה של המערכת המודיעינית. קנט מתאר תהליך לינארי בעל שישה שלבים: ראשית, הופעה או זיהוי של בעיה אסטרטגית – דבר הנובע מדירקטיבה

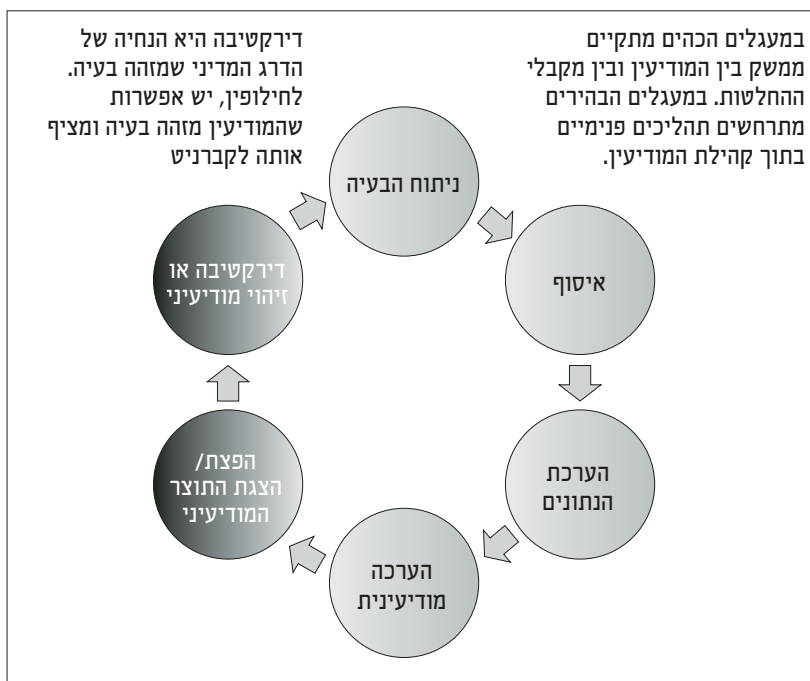
Sherman Kent, *Strategic Intelligence for American World Policy* (New Jersey: Princeton University Press, 1949), p. 200. 6

שם, עמ' 80. 7

William J. Donovan, *Vital Speeches*, XII/14, May 1946, p. 248. 8

Kent, *Strategic Intelligence for American World Policy*, pp. 159-164. 9

של הקברניט או כאשר המודיעין (באמצעות האיסוף) מזהה משהו היוצא מגדר הרגיל; שנית, שלב ניתוח הבעיה – שלב המתבצע בגופי המודיעין עצמם; שלישית, איסוף נתונים על הבעיה באמצעות הכוונת האיסוף – שלב המתבצע בקרב גופי המחקר המודיעיני; רביעית, הערכת הנתונים וביקורתם על ידי גורמי המחקר, תוך השוואה של החדש עם הידוע; חמישית, גיבוש היפותזה, כלומר ביצוע הערכה בהתבסס על המידע הנאסף; שישית, הצגה והפצה של התוצר המודיעיני לקברניט. בשלבים הראשון והאחרון מתקיים מפגש בין גורמי המודיעין ובין הקברניט. במרוצת השנים נעשו ניסיונות לשכלל את תפיסת "מעגל המודיעין". ניסיונות אלה הניחו בבסיסם את מלאכת ייצור הידע כפרויקט כמעט בלעדי של המודיעין, ובהתאם לכך ערכו התאמות ועדכונים. כך, לדוגמה, עמוס ג'ורדן וויליאם טיילור הוסיפו שני רכיבים לתפיסת המעגל הבסיסית של קנט – ניהול ותיאום. אלה עומדים בבסיסו של "מעגל המודיעין" כמעין גלגל שיניים שסביבו נסובים שאר ששת הרכיבים.¹⁰



תרשים 1: מעגל המודיעין על פי שרמן קנט

Amos Jordan, William Taylor, *American National Security: Policy and Process* 10 (Baltimore and London: Johns Hopkins University Press, 1981).

מאוחר יותר התפתחה הגישה הבתר־מסורתית, שאמנם נשענת על הגישה המסורתית, אך אינה רואה במודיעין את הרכיב היחיד, ואפילו לא בהכרח המשמעות ביותר, בתהליך קבלת ההחלטות. ג'ק זלוטניק טען בזכות הידוק הקשר בין איש המודיעין למקבל ההחלטות, על רקע העובדה שהראשון נאבק עם גורמים אחרים על הקשב של האחרון. לדעתו, צמצום המרחק בין איש המודיעין ובין מקבל ההחלטות יעניק בולטות לראשון, ויאפשר לו להבין טוב יותר את השפעת המודיעין על תהליך קבלת ההחלטות, מה שבתורו ישפר את עבודת המודיעין.¹¹

הגישה הבתר־מסורתית סבורה כי לצד תיאור המציאות, על המודיעין להציג בפני מקבל ההחלטות גם את ההשלכות העתידיות האפשריות של יישום המדיניות. במקביל היא מדגישה את הצורך בהבחנה ברורה בין יצרן המודיעין ובין צרכניו, במיוחד בכול האמור להיבטים מבניים. כך, לדוגמה, טען ג'ון הויזינגה כי אמנם יש צורך בקיום דיאלוג מתמשך בין השניים, מאחר והמודיעין הוא חלק אינהרנטי מתהליך קבלת ההחלטות, אך על המודיעין להציג תמונה אובייקטיבית ככול האפשר, שאינה כפופה לשיקוליו של הקברניט.¹²

מראשית ימיו של המודיעין הלאומי בישראל, הגישה המסורתית הייתה הדומיננטית בו. אנשי אקדמיה ומודיעין חזרו והדגישו את הצורך של המודיעין להישאר "טהור" ולשקף נאמנה את המציאות, מבלי להיות מוסט על ידי שיקוליו הפוליטיים של הקברניט.¹³ לשיטתם, המציאות, על אף מורכבותה, ניתנת לחשיפה באמצעות שכלול האיסוף, ועל כן, תפקידו של איש המודיעין ברמה הלאומית הוא להבין ולפרש את המציאות ולהנגיש פרשנות זו למקבל ההחלטות.¹⁴

כאמור, לא רק אנשי מודיעין החזיקו ומחזיקים בגישה זו. ניתן לזהותה גם בקרב חלק מהקברניטים. הסיטואציה הישראלית ייחודית בהקשר זה, מאחר ולעתים קרובות הקברניטים הישראליים היו בעלי ניסיון צבאי וביטחוני, כמו משה דיין, יצחק רבין, עזר ויצמן, אריאל שרון ואהוד ברק. חלקם העדיפו לעתים שהמודיעין יספק מידע גולמי, ימעט בפרשנות ולא יתערב בקבלת ההחלטות. אחרים מביניהם סברו כי מאחר והאחריות מוטלת על כתפיהם, מוטב שיעריכו את המודיעין בעצמם,

11 Jack Zlotnick, *National Intelligence* (Washington, D.C.: Industrial College of the Armed Forces, 1964); Jack Zlotnick, "Bayes, The Forum for Intelligence Analysis", *Studies in Intelligence* 16, no.2 (Spring 1972): 43-52.

12 ג'ון הויזינגה היה חבר במועצה לתכנון מדיניות במחלקת המדינה בין השנים 1964-1966, ולאחר מכן סגן מנהל המשרד להערכות לאומיות ב־CIA. דבריו המובאים לעיל מופיעים בעדותו בפני ועדת מרפי (The Murphy Commission) שעסקה בארגון הממשל האמריקאי לטיפול בענייני חוץ. ראו הדוח המלא של הוועדה: research.policyarchive.org/20213.pdf.

13 Uri Bar-Yosef, *Intelligence Intervention in the Politics of Democratic States: The United States, Israel and Britain* (Pennsylvania State University Press, 2004).

14 אל"מ י', "האחר שבתוכנו", **מערכות**, גיליון 434, עמ' 52-59.

ללא המסננת של אנשי המודיעין. זאת ועוד, סדרת כישלונות מודיעיניים כואבים החרותים בהיסטוריה הישראלית, וועדות החקירה שבאו בעקבותיהם, יצרו אצל מקבלי ההחלטות את ההכרה כי לא תמיד הם יוכלו להינקות מאחריות להחלטות שקיבלו, גם אם אלו התקבלו בהמלצת אנשי המודיעין. גם משום כך נוטים מקבלי ההחלטות להתייחס להערכות המודיעין בזירות, שלא לומר בחשדנות. תופעה נוספת שניתן להבחין בה בישראל היא הנטייה של חלק מהקברניטים לא לשתף את קהילת המודיעין ביוזמות מדיניות. דוגמאות לכך הן יוזמת השלום עם מצרים, תהליך אוסלו, הנסיגה מלבנון וההתנתקות מרצועת עזה. אפשר שהסיבה לכך היא מידור חמור ורצון להשאיר את מעגל שותפי הסוד קטן ככול הניתן כדי למנוע הדלפות, אולם ייתכן שהדבר מבטא חוסר רצון של קברניטים לראות בקהילת המודיעין שותפה לקבלת ההחלטות ולגיבוש האסטרטגיה.

הבעייתיות בגישה המסורתית

הגישה המסורתית רואה בידע בכלל ובידע המודיעיני בפרט דבר "אמיתי" אם הוא מהווה ייצוג מדויק של המציאות, ו"נכון" אם הוא מתאר נאמנה את מצב העניינים כמות שהוא "באמת". עניין זה מתייחס לייצוגים מצומצמים ולייצוגים רחבים, לייצוגים פיזיקליים מוחשיים ולייצוגים מופשטים, והוא מהווה הרחבה של המושג "ידיעה עובדתית" גם לתחומים תודעתיים ומופשטים יותר. טענה מרכזית בביקורת על הגישה המסורתית היא שבניגוד לסביבה הטקטית, שבה הידע הוא אוניברסלי, בסביבה האסטרטגית לא ניתן לנתק את הידע מהידע, ובכלל זה מזווית ההסתכלות ומהאינטרסים שלו.

כדי להמחיש זאת, נתבונן בבעיה מודיעינית מהעולם הטקטי לעומת בעיה מודיעינית מהעולם האסטרטגי. שאלה טקטית עשויה להיות מיקומה של מחלקת טנקים בנקודה מסוימת. התשובה לשאלה זו היא חדה, מוחלטת ונשענת על בסיס עובדתי: האם המחלקה נמצאת בנקודה הספציפית או לא. התשובה אינה נתונה לפרשנות המתבונן, משום שכול מתבונן, בלי קשר לזהותו, יוכל לראות את מחלקת הטנקים באמצעות תצלומי לוויין. לפיכך, מדובר בידע אוניברסלי.

שאלה ברובד האסטרטגי עשויה להיות: "האם משטר היריב יציב?" התשובה לכך היא פרשנית ותלויה, בין השאר, בכוונתו של שואל השאלה, באינטרסים שלו, בנקודת מבטו ובמדיניותו: האם כוונתו היא ליציבות פוליטית, כלכלית או חברתית? האם כוונתו היא ליציבות/אי-יציבות במשמעות של החלפת המנהיג או כלל המערכת השלטונית? איזה היבט ביציבות המשטר של היריב רלוונטי עבור השואל, מעצם היותו גורם המשנה את מצב העניינים האסטרטגי? האם שואל השאלה הוא ראש המדינה (לדוגמה, נשיא סוריה אסד או נשיא מצרים א-סיסי), שמבחינתו יציבות היא עניין הישרדותי, או גורם חיצוני (למשל, ישראל או ארצות

הברית), שמבחינתנו יציבות עשויה להיות קשורה לקיום הסכמי שלום או ליציבות באזור שלם (לדוגמה, במזרח תיכון)?

להבדיל מהימצאות או אי-הימצאות של טנקים במקום מסוים, יציבות כשאלה אסטרטגית תלויה, כאמור, בנקודת המבט של המתבונן ובפרשנות שהוא מעניק לה. אם ניקח את שיטת המשטר הישראלית כדוגמה, היא נתפסת על ידי ישראלים רבים כיציבה, גם אם אורך החיים הממוצע של ממשלות ישראל עומד על מעט יותר משנתיים. לעומת זאת, מתבונן זר עשוי לראות את המערכת הישראלית כסובלת מחוסר יציבות כרוני, דבר שהופך השקעה בה למסוכנת.

בעיה נוספת העולה מהגישה המסורתית נוגעת לתפיסת "מעגל המודיעין" שתוארה לעיל. המושג "איסוף" (של ידיעות מודיעיניות) בגישה זו מהווה מטאפורה לליקוט עובדות המונחות אי שם באופן בלתי תלוי, כאשר משימתו של איש המודיעין היא ללקטן. מתוך אותה נקודת מבט, המושג "עיבוד" מבטא את הרעיון שלפיו איש המודיעין מחבר את פיסות המידע לתמונה רחבה ושלמה של המציאות "האמיתית". לפי הגישה המסורתית, העשייה המודיעינית שקולה לפאזל ואין בה כמעט מקום לפרשנות סובייקטיבית, למעט הערכה המהווה השלמה לאזורים החסרים בפאזל. לפיכך, הפרקטיקה של עשיית המודיעין הלאומי, המאפיינת את היחסים בין איש המודיעין לדרג המדיני, היא של הפרדה וחד-צדדיות. איש המודיעין נדרש להציג את הערכתו בדרך כלל בראשית הדיון, או להעביר את מסקנותיו בצורה של סקירה כתובה. כלומר, הערכה מחקרית של היריב מקדימה את הדיון בגיבוש מדיניות כלפיו. לפי תפיסה זאת, בסביבה המודיעינית האסטרטגית, ההערכה המודיעינית מקדימה את המעשה המדיני, בדיוק כפי שקורה בשדה הקרב, שבו הידיעה המודיעינית מקדימה את הפעולה.

הגישה השיתופית

המגע ההדוק בין אנשי המודיעין ובין מקבלי ההחלטות האמריקאים במהלך שנות השישים של המאה העשרים, וסדרת כישלונות מודיעיניים במהלך שנות השבעים, הביאו לשינוי בגישות המטיפות להפרדה ברורה וקשיחה בין המודיעין למקבל ההחלטות. כישלונות מודיעיניים סביב מלחמת וייטנאם, הדלפות לעיתונות על מבצעי מודיעין רגישים וגילויים כי ה־CIA מבצע מבצעים ללא אישור וידוע הדרג המדיני, הביאו להקמת ועדות חקירה שבחנו מחדש את עבודת שירותי הביון האמריקאיים ולגיבוש גישה חדשה בעבודת המודיעין, שלצורך מאמר זה נכנה אותה "הגישה השיתופית".¹⁵ ההכרה בקיומם של אזורי פעילות נסתרים של

15 מבין הוועדות הבולטות נציין את דוח שלזינגר מ־1971, את ועדת רוקפלר שפרסמה את ממצאיה ביוני 1975 ואת ועדת צ'רץ' שהקים הסנאט ופרסמה את דוחותיה באפריל 1976. מעניין לציין כי ועדת חקירה נוספת, שפעלה שלושה עשורים לאחר מכן (ועדת אספן-בראון

שירותי הביון האמריקאיים, ללא ידיעת הדרג המדיני, הביאה את חברי הוועדות להמליץ לא רק על מיסוד הפיקוח, אלא גם על הקמת מנגנונים להידוק הקשר בין המודיעין לקברניטים. לפי גישתם, יש לפתח ערוץ הידברות ישיר ואישי, לעתים בלתי פורמלי, בין אנשי המודיעין ובין צרכניו. זאת, מכיוון שהיחסים בין שני הגורמים הם סימביוטיים במהותם, ולכן חייבים להתקיים ביניהם קשרי עבודה קרובים שיוסדרו באמצעות מכניזמים ארגוניים ויוודאו העברת מידע ומשוב באופן דרכיוני.

מעניין לציין כי אחד התומכים המרכזיים בגישה השיתופית, פרופסור ווילמור קנדל מאוניברסיטת ייל, פרסם כבר בשנת 1949, שנים רבות לפני שגישה זאת הפכה לפופולרית, מאמר שכותרתו "The Function of Intelligence", בו התפלמס עם הטענות שעלו בספרו של שרמן קנט.¹⁶ לפי קנדל, תפקיד המודיעין הוא לסייע למקבל החלטות להשפיע על המציאות ולעצב אותה. לכן, הוא לא ראה פסול ביחסים קרובים בין השניים ואף טען כי אלה הכרחיים ורצויים. כמו קנט, גם קנדל האמין שמקבל החלטות חייב להיות זה שמנחה את איש המודיעין, אך בניגוד לקנט, הוא המשיך וטען כי המודיעין עוזר למקבלי החלטות להשפיע על המציאות, בכך שהוא מבאר עבורם כיצד המתרחש בעולם משפיע ועשוי להשפיע על הביטחון הלאומי. לכן, איש המודיעין אינו יכול לבדל עצמו מנקודת המבט שלו-עצמו, שכן היא מהווה חלק בלתי נפרד מתפקידו.

רוג'ר הילסמן,¹⁷ אחד ממעצבי תורת המודיעין האמריקאית, צידד בגישה שהביע קנדל וגרס כי יש לעודד את המודיעין לבחון כיצד הערכותיו משפיעות על מרחב האפשרויות המונח בפני מקבל החלטות. הילסמן טען כי לא ייתכן שאנשי מודיעין יהיו מנותקים ממי שעבורו הם מייצרים את התוצר שלהם. לדבריו, אנשי מודיעין עובדים עבור מקבלי החלטות ומשרתים את מטרותם על ידי כך שהם מספקים להם את הרקע הנחוץ להערכת מצבים ולקבלת החלטות.¹⁸ זאת,

בשנת 1996), הגיעה למסקנות זהות פחות או יותר לאלו של ועדת צ'רץ' בכול האמור לצורך בהידוק הקשר בין מקבל החלטות ובין איש המודיעין.

Wilmoore Kendall, "The Function of Intelligence", *World Politics* 1, no. 6 (1949): 16 452-453.

17 הילסמן היה פרופסור למדע המדינה, שהתגייס לצבא האמריקאי במלחמת העולם השנייה, ומשם המשיך לתחום המודיעין הלאומי. בתפקידו האחרון כיהן כראש המחקר של מחלקת המדינה של ארצות הברית.

18 Roger Hilsman, *Strategic Intelligence and National Decisions* (Glencoe: Free Press, 1966); Roger Hilsman, "On Intelligence", *Armed Forces and Society* 8, (Fall 1981): 129-143; Roger Hilsman, *The Cuban Missile Crisis: The Struggle Over Policy* (Westport: Praeger, 1996).

בניגוד למצב ההפוך, אותו היטיב לתאר רוברט ג'רוויס: "קל לשמור על מודיעין טהור כשהוא לא רלוונטי".¹⁹

גם ויליאם ברנדס סבר כי תוצר המודיעין חייב להיות בר שימוש עבור מקבל ההחלטות, ולכן על קהילת המודיעין להבין היטב מהו הצורך שלו. כדי להבין זאת, על איש המודיעין להימצא בקרבה למקבל ההחלטות. לדברי ברנדס, הצורך של מקבל ההחלטות הוא בבחינת אלומת האור המכוונה את מאמצי האיסוף והמחקר, כשלצדה קיימת מערכת של היזון חוזר ממקבל ההחלטות על תוצרי המודיעין שהגיעו אליו.²⁰

אימוץ גישה זו על ידי ראשי קהילת המודיעין האמריקאית ניתן לראות בדברים שנשא רוברט גייטס בשנת 1992, זמן קצר לאחר מינויו לתפקיד מנהל המודיעין הלאומי של ארצות הברית (DCI – Director of Central Intelligence). גייטס הדגיש את הדיאלוג הפתוח שחייב להתקיים בין המודיעין ובין הקברניט, בפרט לאור העובדה שאף צד מהמעורבים בדיון האסטרטגי אינו חסין מטעויות: "לאף אחד אין מונופול על האמת; כולנו לומדים דברים חדשים מדי יום... חייב להתקיים דיאלוג, על כל משתתף להיות פתוח לרעיונות חדשים, ודעות אלטרנטיביות (ובלבד שהן) מבוססות היטב חייבות לקבל ביטוי".²¹

גייטס טען כי האינטראקציה בין אנשי המודיעין למקבלי ההחלטות היא מפגש שבו שני הצדדים מקיימים שיח ויוצרים יחדיו ידע, ולא אירוע חד-צדדי ולינארי שבו רק המודיעין מעביר מידע לקברניט:

הצורך להביא את מקבל ההחלטות לקרוא את תוצרי המודיעין שלנו – אל לו לסכן את האובייקטיביות שלנו ואין בכך כדי לרמז שעלינו לעדן את הערכותינו. ההפך הוא הנכון. המשמעות היא שעלינו לייצר דיון כן ומאוזן בסוגיה. אם אנו יודעים שמקבל ההחלטות מחזיק בדעה מסוימת על נושא מסוים, דעה השונה מהערכתנו, אל לנו להתרחק מגישתנו, אלא דווקא להתייחס אל נקודות החזקה והחולשה שלה, לעגן אותה בעובדות ולהסביר כיצד הגענו אליה.²²

בניגוד לפופולריות שלה זוכה הגישה המסורתית בישראל, הגישה השיתופית זוכה לאהדה פחותה, וניכר כי מרבית המצדדים בה שייכים דווקא לצד של אנשי המודיעין. אותם גורמים נוטים לעמעם את הממד הפרוצדורלי הפורמלי המסדיר שיתופיות כזו ומדגישים את האמון בין שני הצדדים כמפתח לשותפות ואת רעיון

Robert Jervis, "What's Wrong with the Intelligence Process?", *International Journal of Intelligence and Counterintelligence* 1, no.1 (Spring 1986): 39.

William J. Brands, "Intelligence and Foreign Policy: Dilemmas of a Democracy", *Foreign Affairs* 47 (1969): 288.

Robert Gates, "Guarding Against Politicization", *Studies in Intelligence* 36, no. 5 (1992): 8.

שם. 22

האחריות המשותפת.²³ גם מפקדים בכירים בקהילת המודיעין הישראלית בעת האחרונה, כמו רח"ט מחקר באמ"ן לשעבר, איתי ברון, מדגישים כי תפקידם של אנשי המודיעין אינו מסתכם בבירור המציאות והצגתה לקברניט. לדעת ברון, אנשי המודיעין צריכים להיות מעורבים גם בתהליכים של עיצוב מדיניות ברמות השונות.²⁴ בעדות של ראש אמ"ן לשעבר, אלוף אביב כוכבי, בפני מבקר המדינה שחקר את מערכת "צוק איתן" בעזה 2014, הוא הדגיש כי המפקדים הצבאיים והקברניטים המדיניים לא צריכים להיות מאזינים פאסיביים להערכת המודיעין. בראייתו, עליהם לקחת חלק בתהליך של חיכוך עם המודיעין ולהיות שותפים בניתוח המידע ובפרשנות שלו. מנקודת מבטו כראש אמ"ן, הוא ציין כי השיח עם הקברניטים מעשיר את הערכת המודיעין והדגיש כי גופי ההערכה, גם אם הם מתבססים על מקורות טובים, צריכים להיות חשופים לביקורת.²⁵

בין המצדדים הבולטים בגישה השיתופית ניתן לציין את ראש אמ"ן לשעבר, משה יעלון, שמילא גם תפקידי פיקוד מרכזיים בצה"ל (מפקד פיקוד המרכז ורמטכ"ל) ובממשלה. יעלון ציין, בראיון שנערך עמו לאחרונה, כי תהליכי למידה וחשיבה משותפים בין הדרג המדיני לדרג המודיעיני חיוניים בכדי לפתח אסטרטגיה הולמת וכי הוא עצמו נקט פרקטיקה משתפת, שבה השיח התנהל לא באופן היררכי וללא "טקס", וזאת הן במסגרת תפקידיו בצבא והן כשכיהן כשר הביטחון. יעלון ציין כי יחד עם זאת, לא תמיד יכול הדרג המדיני לחשוף את כוונותיו לדרג הצבאי-אסטרטגי בכלל ולדרג המודיעיני בפרט, והוא זכאי לשמור על עמימות אסטרטגית. במקרים כאלה נדרש הדרג המודיעיני המקצועי לפתח יכולות לפענח את כוונותיו של הדרג המדיני ואת הדירקטיבה שלו, כדי שיוכל להפנות את מאמצעי המודיעין באופן שיסייע לו בגיבוש אסטרטגיה הולמת.²⁶

גישתנו התיאורטית לדפוס היחסים הרצוי בין איש המודיעין ובין מקבל ההחלטות יוצאת מנקודת מוצא שאנו מכנים, כאמור, "גישה שיתופית". גישה זו נשענת על הנחת יסוד שאינה רואה בידע המודיעיני התייחסות למציאות אובייקטיבית בלתי תלויה במתבונן. כפועל יוצא מכך, איננו רואים בפרויקט המודיעיני "מוסד לבירור המציאות",²⁷ המנותק מהמתבונן. בעינינו, מטרותיו של המתבונן המודיעיני, עולם ערכיו, האינטרסים האסטרטגיים שלו, ואף עצם בחירתו להתבונן במושא מחקר מסוים ולא באחר – כולם מהווים מסגרת חיונית לאופן בו המציאות מפורשת על ידיו. לכן, אנו יוצאים נגד התפיסה הרואה בפיתוח ידע על סביבה או על יריבים

23 גרשון הכהן, מה לאומי בביטחון הלאומי (תל-אביב: מערכות, 2014).

24 איתי ברון, המחקר המודיעיני (רמת השרון: המרכז למורשת המודיעין, 2015), עמ' 42.

25 מבקר המדינה, מבצע צוק איתן, 28 בפברואר 2017, עמ' 75.

26 ראיון שקיים דודי סימן טוב עם משה יעלון, המכון למחקרי ביטחון לאומי, 6 באוקטובר 2016.

27 יצחק בן ישראל, הפילוסופיה של המודיעין (תל-אביב: מערכות, 1999).

פרויקט בלעדי של המודיעין, ואיננו רואים בתוצר המודיעיני מהלך אחרון בתהליך המודיעיני, קרי "תוצר" המונח על שולחנו של "הצרכן", אלא נקודת פתיחה לשיח ולפיתוח ידע משותף.

גישתנו מדגישה שלושה ממדים בתפקידו ובתפקודו של המודיעין ברמה הלאומית: ראשית, הסתלקות מראיית המודיעין כנועד לברר את המציאות באמצעות "גילוי" האמת, פשוט מאחר וזו אינה קיימת ברמות האסטרטגיות; שנית, נטישת אמת המידה כאילו טיב הערכת המודיעין ברמה האסטרטגית נבחן לאור יכולתו לשקף את המציאות "האובייקטיבית", והערכתו על סמך מידת הרלוונטיות שלו לקבלת ההחלטות; שלישית, הדגשת הצורך בשותפות בין הקברניט לאיש המודיעין בפיתוח הידע, וכן ביצירת תנאים לשיח פתוח הנחוץ לפיתוח ידע ברמה הלאומית, כדי לגבש מדיניות ולהוציאה אל הפועל.

מעובדות לפרשנויות

כאמור, הידע הנדרש לעיצוב אסטרטגיה מוצלחת הוא ידע מופשט, שמומשג בהקשר קונקרטי ומבטא רעיון ופרשנות ולא ידיעה ממשית. בניגוד לידיעה המודיעינית בסביבה הטקטית, המודיעין ברמה הלאומית מפותח על ידי איש המודיעין עצמו ואינו מתקבל כידיעה מודיעינית. האתגר העומד בפני המודיעין לפי גישה זו שונה בתכלית מתפקידו בגישה הקודמת: לא השגת ידיעה עובדתית, אלא מתן פרשנות והמשגה לתופעות שמתרחשות אצל היריב, כבסיס לשיח מפרה עם הקברניט, כדי שזה ישמש מצע לגיבוש מדיניות. במרבית המקרים, המשגה זאת אינה מצויה בצד השני, ומהווה פרשנות סובייקטיבית שלנו את היריב. זאת ועוד, לא ניתן לבחון אותה בשיפוט "נכון" או "לא נכון", משום שהיא מבטאת תפיסה אפשרית בלבד, שבאה לשרת גיבוש מדיניות קונקרטית ולא מדיניות אוניברסלית.²⁸

מן הראוי להדגיש, כי המעבר של המודיעין מעובדות לפרשנויות אין משמעו שהוא נוטש את המישור העובדתי: הפרשנות בסביבה האסטרטגית נשענת על עובדות ברמה הטקטית. במעבר מאובייקטיביות לרלוונטיות, על המודיעין להיזהר מוויתור על היושרה המקצועית של מי שמתבונן בעובדות ואף נהנה בגין כך מיתרון על פני שותפים אחרים לדיון האסטרטגי. בהקשר זה, המודיעין נהנה מיתרון כפול: הוא בעל גישה ייחודית, ולעתים בלעדית, לרמה העובדתית; הוא בין הבודדים סביב שולחן הדיונים המורגל בתהליכי פיתוח ידע, הנחוצים כל כך לקבלת החלטות.

Thomas L. Hughes, *The Fate of Facts in a World of Men: Foreign Policy and Intelligence-Making*, Headline Series 233, December 1976, p. 5; Richard Betts, "Policy-Makers and Intelligence Analysis: Love, Hate or Indifference?", *Intelligence and National Security* 3, no. 1 (1988): 184-185.

מאובייקטיביות לרלוונטיות

למרות שלעתים נשמעות גישות המדגישות את הרלוונטיות על חשבון האובייקטיביות, ואף שוללות מלכתחילה את היכולת להגיע לאובייקטיביות, הדעה הרווחת בקרב ראשי המחקר בקהילת המודיעין הישראלית, כמו זו האמריקאית, מצדדת בשאיפה להשיג אובייקטיביות, או למצער לתמרן בינה ובין הרלוונטיות. כך, לדוגמה, באתר ה־CIA מודגש הצורך במחקר אובייקטיבי: "אנשי מינהלת המחקר (של ה־CIA) מסייעים לספק הערכת מודיעין רלוונטית, מדויקת ואובייקטיבית המבוססת על כל מקורות המודיעין, ובכול הנוגע לכלל היבטי הבטחון הלאומי ומדיניות החוץ; הערכה זו מסופקת לנשיא, לקבינט ולבכירי מקבלי ההחלטות בממשלה האמריקאית".²⁹

כפי שצינו, השאיפה לאובייקטיביות של הידיעה המודיעינית היא לדעתנו עניין עקר, שכן ידיעה וידע לעולם יהיו יחסיים ותלויים במתבונן. לפיכך, אנו מבקשים להסתלק מהעיקרון הבוחן את טיבו ותפקודו של המודיעין בהקשר של רעיון האובייקטיביות ולהחליפו בעקרון הרלוונטיות שלו לתהליך קבלת ההחלטות. עקרון הרלוונטיות, כאמת מידה לבחינת המודיעין מול מקבלי החלטות ברמה הלאומית, הוצג יפה על ידי ג'וש קרבל ואנתוני אולקוט.³⁰ השניים טענו כי נדרשת "סינתזה בין המודיעין למקבלי ההחלטות", במסגרתה יחדל המודיעין להיות ספק של מידע בלבד ויתחיל להיות ספק של ידע ורעיונות. הדבר מחייב שינוי כפול: ראשית, על מקבלי ההחלטות "לתת אמון ולחשוף את מדיניותם בפני המודיעין", וכן "לשאול שאלות על יותר מאשר נתונים";³¹ שנית, על אנשי המודיעין להיות מעורבים בגיבוש המלצות ולהתגבר על רתיעתם מכך, המונעת שילוב של השלכות פעילות כוחותינו בהערכותיהם. לשיטתם של קרבל ואולקוט, בתנאים אלה של שיח ושיתוף, לא ניתן יהיה יותר לדבר על הצלחות במדיניות או על כישלונות מודיעיניים, משום שהם יהיו שזורים אלה באלה. שינוי נוסף נובע מהצורך בלימוד המדיניות ובהתאמת הערכות המודיעין לצרכים הנובעים ממדיניות זו, ובלשונם של קרבל ואולקוט: "המודיעין ידרש לתת מה שצריך ולא מה שיש. איש המודיעין החדש צריך ללמוד לקבל יעדים פוליטיים ואסטרטגיים כלגיטימיים וראויים".³² פיתוח דפוס כזה של מודיעין, המשולב בעיצוב המדיניות, עלול לגרום למצב של מתח בינו ובין מקבלי ההחלטות. לפי קרבל ואולקוט, במקרים בהם איש מודיעין

29 כפי שמובא באתר סוכנות הביון המרכזית (CIA), <https://www.cia.gov/offices-of-cia/intelligence-analysis/index.html>

30 Josh Kerbel and Anthony Olcott, "Synthesizing with Clients, not Analyzing for Customers", *Studies in Intelligence* 54, no. 4 (2010): 11-27.

31 שם.

32 שם.

אינו מזדהה עם המדיניות המוצעת, עליו להתפטר, הגם שקיימת סכנה שבהיעדר מתח בין שני הצדדים, המודיעין יהפוך לכלי בידי המדינאי³³ (כפי שנטען נגד קביעות המודיעין במערב בהתייחסו לעיראק בשנת 2003).³⁴ לדעת קרבל ואולקוט, ההישג המרכזי של גישה זו, מעבר להפיכת המודיעין לרלוונטי, הוא שלמקבלי ההחלטות, אם ירצו בכך, יהיה שותף שעמו הם יוכלו "להתלבט, לשאול שאלות ולגבש מדיניות הולמת".³⁵

מדיכוסומיית יצרן/צרכן לשותפות

הקברניט נדרש לשותף כדי שיוכל, יחד עם המודיעין וגורמים נוספים, לעמוד על מגבלות ותורפות השחקנים בסביבה האסטרטגית ולעצב לאורן מדיניות או אסטרטגיה מוצלחת. מלאכת גיבוש האסטרטגיה היא אפוא מלאכה משותפת בהובלת הקברניט, שלמודיעין חלק ייחודי בה (אם כי לא בלעדי), משום שהוא זה שאמור להביא לדיון הבנות ופרשנויות על הסביבה האסטרטגית. עם זאת, הידע אותו מביא המודיעין אינו עומד בפני עצמו (כמתואר ב"מעגל המודיעין" של קנט), אלא מתקיימים תהליכים משותפים של פיתוח ידע וגיבוש הבנות. העמדת התובנות המודיעיניות על הסביבה כנושא בפני עצמו, מבלי לשקף הבנות על המתבונן, יוצרת חסך משמעותי.

נוכח הנאמר לעיל, גיבוש מערכת הבנות אסטרטגיות מול זירה או יריב חייב להתבצע במשולב על ידי אנשי מודיעין וקברניטים. אנו מבקשים אפוא להיפרד מהדיכוסומיה המסורתית, המבחינה בין יצרני המודיעין לצרכניו, ולהתייחס אליהם, לפחות ברמה התיאורטית, כאל שותפים, גם אם לא שווים. איננו מציעים להיפרד מתפיסת "מעגל המודיעין" של קנט במלואה, אולם בראיתנו, השלב הראשון והאחרון שלה צריכים להתבצע תוך ממשק קרוב ואינטראקטיבי בין המודיעין ובין הקברניט, אשר הופך את דפוס היחסים לדו-צדדי.

הטבלה הבאה מסכמת את ההבחנה בין הגישה המסורתית ובין הגישה השיתופית האקטיבית בה אנו אווזים.

33 יהושפט הרכבי, **המודיעין כמוסד ממלכתי** (תל-אביב: מערכות, 2015), עמ' 71. יהושפט הרכבי, שהיה ראש אמ"ן ובהמשך שימש יועץ אסטרטגי לשר הביטחון ויועץ למודיעין לראש ממשלה, כינה תופעה זו "חייטות מודיעינית".

34 Paul R. Pillar, "Intelligence, Policy and the War in Iraq", *Foreign Affairs* (March-April 2006).

35 Kerbel and Olcott, "Synthesizing with Clients".

תרשים 2: השוואה בין הגישה המסורתית ובין הגישה השיתופית³⁶

הגישה המסורתית	הגישה השיתופית
מה אתה רוצה לדעת?	מה אתה רוצה להשיג?
ממוקדת איומים	ממוקדת הזדמנויות
מתייחסת לעבר	מתייחסת לעתיד
נוטה להיות טקטית	חייבת להיות אסטרטגית
תוצר	תהליך, שיח
מחפשת השוואות ואנלוגיות	מנסה לאתר את הייחודי
מתעניינת באובייקטים	מתעניינת בהקשר ובזיקות
תגובתית	יוזמת, פרו־אקטיבית
מופנמת	מוחצנת
נוטה להתמקד במה שהשתבש	מאפשרת לבחון (גם) מה הצליח
מתגמלת שנינות – מערכות גדולות, עוד כוח אדם, התמחויות, תוכניות רחבות	מתגמלת דמיון – גמישה, מסתגלת, פחות היררכית, יותר רשתית
איסוף	קוגניציה – הבנה

הבעייתיות ביישום הגישה השיתופית

דומה שהגישה השיתופית היא פרקטיקה מקובלת בממשק שבין אנשי מודיעין ובין מצביאים אנשי צבא, כמו, למשל, קמ"ן פיקוד שהוא חלק אינטגרלי מקבוצת הלמידה אותה מוביל מפקד הפיקוד. עם זאת, לאורך השנים ניכרים קשיים של ממש ביישום הגישה השיתופית ברובד הלאומי, קרי בממשק שבין אנשי המודיעין ובין הדרג המדיני. אנו מעריכים כי הסיבה לכך טמונה במאפיינים התנהגותיים ומבניים, הן מצד הקברניט והן מצד איש המודיעין, ובמתחים האופייניים לסביבה הלאומית. בסביבה האסטרטגית קיים מתח בסיסי בין נקודת המבט של אנשי המודיעין, שחלקם מעוניינים לתאר את העתיד, ובין נקודת המבט של הקברניט, שכוונתו היא לעצב את העתיד.³⁷ קברניטים סבורים לעתים קרובות שאנשי מודיעין נוטים להרחיב את תחומי אי-הוודאות בעולם שבו הקברניטים פועלים, במקום לצמצמם. הקברניטים זקוקים לפתרונות, ואילו הערכת המודיעין מציפה להם בעיקר אתגרים, וכמעט שלא מניחה לפתחם פתרונות. זאת ועוד, אנשי מודיעין נוטים להערים סייגים על הערכותיהם ולשרטט מגוון תרחישים המתוארים לעתים קרובות בצורה עמומה. קברניטים מעוניינים לעתים תכופות שהמודיעין יספק להם תחזיות, אך

36 טבלה זו מבוססת על טבלה המופיעה במאמר של קרבל ואולקוט, שם, עמ' 23.

37 Hans Heymann, "Intelligence and Policy Relationships", in *Intelligence Policy and Processes*, eds. Alfred C. Maurer, Marion D. Tunstall and James M. Keagle, (Boulder: Westview Press, 1985), pp. 57-66.

קציני מודיעין שידבקו במעמד של נביאים לא יוכלו להיות שותפים נאמנים של הקברניטים במלוא מובן המילה.

חסם מרכזי נוסף העומד בפני יישום התפיסה השיתופית נובע מכך שהקברניט אינו מעוניין בדרך כלל לשתף את קהילת המודיעין בשיקוליו ובכוונותיו הכמוסות: הוא חושש מהדלפות, לעתים אינו רוצה שיאתגרו אותו, מעדיף לקדם תפיסת עולם מסוימת ואינו מעוניין שגורם מקצועי יטיל בה ספק. בעיה אחרת נוגעת להיעדר שפה משותפת בין הקברניט ובין איש המודיעין, כאשר מבחינת הקברניטים, שפתם של אנשי המודיעין אינה ברורה, או למצער אינה מבטאת את רמות הוודאויות הנחוצות להם כדי לנהל סיכונים.

יתרה מכך, לא תמיד קיים קשר ישיר בין הערכת המודיעין ובין קבלת ההחלטות. לעתים ההחלטות, במיוחד המשמעותיות שבהן, מתקבלות במנותק מהערכת המודיעין, והגורם המרכזי המביא לקבלתן אינו נוגע להבנות שמשקף המודיעין ביחס לסביבה ולשחקניה, אלא משקף שיקולים אחרים הנובעים מנקודת המבט של הקברניט. זאת ועוד, לעתים מתקבלות החלטות במהופך מהערכת המודיעין, שכן השוני בנקודות המבט של איש המודיעין ושל הקברניט עשוי להביא לפרשנויות שונות, שלא לומר מנוגדות, של המציאות.

סוג אחר של בעיות נובע מהעובדה שמקבל ההחלטות ניזון מקשת רחבה של מקורות מידע על הסביבה האסטרטגית, שמרביתם אינם מודיעיניים. דבר זה נכון בעיקר בעת הנוכחית, שבה כל אחד יכול להיות נגיש לים המידע, לפרשנויות ולתובנות שונות, וכאשר לקברניט יש מקורות משלו. קברניט יכול לשאול את עצמו, לעתים בצדק, מה הערך המוסף של קהילת המודיעין על פני פרשנויות חלופיות, הזמינות לו באופן ישיר, וייתכן שהן דומות יותר לתפיסת עולמו.

בנוסף, לעתים קרובות יש לקברניט יתרון על המודיעין בהבנת המערכת האסטרטגית, במיוחד כאשר מדובר בקברניט בעל ניסיון וקשרים אישיים עם קברניטים בעולם. הקברניט מגלה בדרך כלל הבנה עמוקה של האופן בו מתנהלת המערכת הבין-לאומית, והדבר עלול לגרום לכך שלא יראה בקהילת המודיעין שותפה, במיוחד אם זו מדגישה היבטים של איומים צבאיים ושמה דגש פחות על הזדמנויות מדיניות. עניין אחרון שעלול להקשות על השותפות בין הקברניט למודיעין הוא אופי סדר היום המדיני של קברניט שמעוניין בידע על חברות אזרחיות, כלכלה ותרבות. זאת, בניגוד לנקודת המבט של המודיעין ששמה, כאמור, דגש על איומים צבאיים. פער זה עלול להקשות על הקברניט לראות במודיעין שותף, גם אם הוא רוצה בכך. עד כה תיארונו בעיקר את הקשיים והחסמים הגורמים לקברניט לא לראות במודיעין שותף. בה בשעה, קיימים חסמים גם אצל אנשי המודיעין, העלולים למנוע מהם לראות את עצמם שותפים לקברניט. חסמים אלה נובעים, למשל, מאחזתה העמוקה של הגישה המסורתית בקרב קהילת המודיעין ומאופיים של

התוצרים המודיעיניים. במקרים רבים, אלה אינם מעודדים שיח, אלא מבקשים לתאר "שורות תחתונות", וגם אז הן מנוסחות לא פעם בצורה מעורפלת. השילוב של חסמים דו־כיווניים אלה, ובעיקר היעדר הכרה משותפת לשני הצדדים כי בגישה השיתופית טמונה הזדמנות של ממש לשיח אסטרטגי פתוח בין המודיעין לקברניט, הופכים את יישומה של גישה זאת למהלך קשה מאוד לביצוע.

סיכום

מגבלות לא פשוטות עומדות בפני מימוש הרעיון של סינתזה בין המודיעין ובין מקבלי ההחלטות: אי־רצון של מקבלי ההחלטות להיחשף ו/או להתחייב למדיניות, חשש מהדלפות ומסורת בירוקרטית ותפיסתית. עקרונות דוגמתיים של יחסי יצרן־צרכן, שהינם עדיין דומיננטיים למדי בשיח המודיעיני הלאומי, וכן החתירה לאובייקטיביות (מדומה), מהווים גם הם חסמים משמעותיים.

השינוי בדפוס היחסים בין המודיעין ובין הקברניט מצוי בחיתוליו. נראה כי הרעיון של יחסי שיתוף בין שני הצדדים הוא הכיוון הנכון שלאורו יש לעצב יחסים אלה, במטרה לתת מענה מיטבי לאתגרי השעה בפניהם ניצבים מעצבי המדיניות ואנשי המודיעין כאחד. התנאי המקדמי ליצירת שינוי כזה הוא "הרצון להשתנות" כפי שהיטיבו להגדירו בפשטות קרבל ואולקוט.³⁸

בכדי לממש את תפיסת השיתופיות בין הקברניט ובין המודיעין, ראוי להכיר אותה ולראות את הפוטנציאל החדש הטמון בה. ייתכן שהיא אינה מתאימה לכול הקברניטים, אולם אלה שלהם היא מתאימה נדרשים למאמץ משמעותי בכדי ליישמה. בהנחה שגורמי המודיעין מעוניינים לעודד שיח פתוח עם הקברניטים, הם נדרשים להביא בפניהם תוצרים שאינם מתיימרים "לחזות את העתיד" ברמות האסטרטגיות, משום שתחזית כזו רק תיצור מרחק בינם ובין הקברניט. תוצרים המשרטטים מרחבי אפשרויות ומאפשרים לקברניט לנהל סיכונים מעלים את הסיכוי שהוא יראה באנשי המודיעין שותפים.

מצדו של הקברניט, אם הוא מעוניין לשנות את דפוס יחסיו עם אנשי המודיעין, עליו ליצור תנאים לשיח פתוח עמם, ולאפשר להם להשמיע דעות שונות ומאתגרות. הקברניט נדרש ליצור יחסי אמון עם המודיעין ולשתף אותו, ככול הניתן, בתוכניותיו ובהתלבטותיו. איש המודיעין מצדו צריך להשיב על מתן אמון זה בכך שישמור על סודות הקברניט באופן דיסקרטי וימנע מהדלפתם.

השותפות בין המודיעין לקברניט ברמה האסטרטגית אינה דבר מובן מאליה, ונדרש לעשות מאמץ רב בשני הצדדים כדי ליישמה. יחד עם זאת, יש בשותפות כזאת פוטנציאל לשיח מסוג חדש, שיתרום הן לגיבוש אסטרטגיה טובה יותר והן לניצול טוב יותר של קהילת המודיעין.

ישראל והודו: הערכה השוואתית של האסטרטגיה הצבאית למאבק בטרור

וינאי קאורה

ראש ממשלת הודו, נרנדרה מודי, השווה את תגובת ארצו לטרור הפקיסטני שבא לידי ביטוי במתקפה על כוחות הודיים באוּרִי, בחלק של קשמיר שנמצא בשליטת הודו, בספטמבר 2016, לפעולות התגמול והמנע שמבצעת ישראל מעבר לגבולותיה. אמירתו פתחה פתח לדיון מעמיק סביב השאלה האם נכון להודו לאמץ את האסטרטגיה הצבאית הישראלית. ההיסטוריה, התרבות הפוליטית והשיח על ביטחון לאומי שמאפיינים מדינה משפיעים מאוד על קובעי המדיניות ועל הציבור שמאחוריהם. לאור זאת, מאמר זה מבקש לטעון כי ההבדלים המהותיים בתפיסה האסטרטגית, בעמדה הדיפלומטית ובטקטיקות הצבאיות בין הודו לישראל יוצרים שוני בין שתי המדינות בגישות ובסדרי העדיפויות שמכתיבים את תגובתן לטרור. בנסיבות השונות שבהן פועלים הישראלים וההודים, אימוץ האסטרטגיות הישראליות למאבק בטרור יהיה מהלך בעייתי מאוד עבור הודו.

מילות מפתח: הודו, ישראל, ערבים, טרור, התקוממות, צבא־מדינה, צה"ל, צבא הודו, קשמיר, פלסטינים, ביטחון סייבר, גבולות

מבוא

ישראל הפכה למודל לחיקוי בקרב החוגים האסטרטגיים וחוגי האקדמיה בהודו מאז שראש ממשלת הודו השווה בין צבאות שתי המדינות. בדברים שנשא באירוע פומבי במדינת הימאצ'אל פראדש, באוקטובר 2016, השווה נרנדרה מודי בין הפעולה הממוקדת שביצע צבא הודו חודש קודם לכן בחלק של קשמיר שבשליטת פקיסטן, נגד טרוריסטים שחצו את קו השליטה (LoC) וערכו מתקפה על כוחות הודיים, ובין המדיניות הישראלית הדוגלת בפעולות צבאיות ממוקדות ובחיסולים.

ד"ר וינאי קאורה הוא פרופסור חבר במחלקה לעניינים בין־לאומיים ולימודי ביטחון ומתאם המרכז ללימודי שלום וסכסוכים באוניברסיטת סרדאר פאטל לענייני משטרה, ביטחון ומשפט פלילי, ג'דפור, רג'סטאן, הודו.

לדבריו, "גבורת הצבא ההודי היא נושא לשיחה ברחבי המדינה בימים אלה. בעבר שמענו כיצד ישראל פועלת בדרך זו. האומה היהודית רואה כיום שצבא הודו הוא בעל יכולות שאינן נופלות מאלו של כל צבא אחר".¹

נותר עדיין לראות אם ההשוואה שעשה מודי בדבריו אלה נועדה לאוזני תומכיו הפוליטיים, או שהעידה על שינוי בתפיסה האסטרטגית של הודו. אולם סימונה של ישראל כאדיאל של פעילות צבאית ממקם את הדברים בתוך הנרטיב הרחב יותר של האסטרטגיה הצבאית ההודית. דבריו של ראש הממשלה וההד שיעוררו מעלים כמה שאלות: האם להודו יש מבנה מוסדי ומנגנונים שניתן להשוות לסטנדרטים הישראליים? אם לא, האם הודו צריכה לשאוף לחקות אותם סטנדרטים?

החלטת עצרת האו"ם משנת 1947 לחלק את מה שהיה המנדט הבריטי על פלסטין לשתי מדינות – אחת יהודית והשנייה ערבית – הינה גורם מרכזי באי היציבות ובנפיצות הטבועים במזרח התיכון. למעשה, סוגיית פלסטין הייתה הראשונה שהעצרת הכללית של האו"ם נדרשה לפסוק בעניינה. לאחר שדחו את תוכנית החלוקה, הכריזו הערבים מלחמה על מדינת ישראל מיד עם הקמתה. המלחמה ב־1948 לא הצליחה להביא לפתרון הסכסוך, ומדינות ערב עברו למלחמת התשה נגד ישראל. שתי נקודות ציון היו למלחמה זאת – מערכת סיני ב־1956 ומלחמת ששת הימים ב־1967. ב־1956 הלאים נשיא מצרים נאצר את תעלת סואץ, מהלך שהוביל לפרוץ המלחמה באוקטובר 1956, שבה ניסתה ישראל לנצל לטובתה את הכעס הבריטי והצרפתי על הצעד הפתאומי והבלתי צפוי של נאצר.

המלחמה ב־1967 הייתה תוצאה של מאמץ משותף מצד רבות ממדינות ערב לחסל את המדינה היהודית, מאמץ שסוכל בזכות מתקפת מנע ישראלית מוצלחת. מלחמת ששת הימים שינתה באופן יסודי את החזות הטריטוריאלית, האסטרטגית והפסיכולוגית של המזרח התיכון, לאחר שישאל כבשה שטחים מסוריה, ירדן ומצרים. בעקבות אותה מלחמה השתנתה מטרות הערבים מחיסול המדינה היהודית לשחרור השטחים הכבושים.

במלחמת יום הכיפורים, ב־1973, יצאו מצרים וסוריה למתקפת פתע כדי לשוב ולהשתלט על השטחים שאיבדו. תחילה ספג הצבא הישראלי אבדות כבדות, אולם עד מהרה התהפכה המגמה והוא הדף את המצרים והסורים בחזרה אל מעבר לקווי הגבול המקוריים.

ב־1982 פלשה ישראל ללבנון במטרה לשים קץ לירי הארטילרי עליה מצד הארגון לשחרור פלסטין (אש"ף). למרות מהלך זה ומהלכים נוספים, כמו הסכמי השלום שחתמה ישראל עם מצרים (1979) ועם ירדן (1994) ותהליך השלום עם אש"ף (1993), הסכסוך הישראלי-ערבי נותר רחוק מפתרון. זאת ועוד, מאז סוף שנות

1 PTI, "PM Lauds Indian Army", *Hindu*, October 19, 2016.

השמונים של המאה העשרים התמודדה ישראל עם שתי התקוממויות עממיות ("אינתיפאדות") של הפלסטינים בגדה המערבית וברצועת עזה.

על רקע כל אלה, צה"ל צריך להיות ערוך לא רק למלחמה גדולה בין מדינות (כמו סוריה או איראן), אלא גם למאבק בטרור ולפעולות שנועדו לדכא התקוממויות. זאת, כשברקע מנהל ארגון חזבאללה – מיליציה לבנונית-שיעית קיצונית שזוכה לגיבוי מאיראן – פעולות גרילה נגד חיילים ואזרחים ישראלים לאורך גבול ישראל-לבנון, שב-2006 הביאו לפרוץ מלחמה בין שתי המדינות. את המתקפה שהובילה ישראל נגד חזבאללה בלבנון ב-2006 ניתן להגדיר כמקרה של אכיפת חוק וסדר מחוץ לגבולותיה.

התפיסה האסטרטגית

ביטחון, הישרדות וריבונות הם עיקרי התפיסה האסטרטגית של ישראל. אסטרטגים ישראלים פועלים על בסיס התחושה שהמדינה סובלת מפגיעות גיאוגרפיות. תפיסה אסטרטגית זאת הושפעה רבות מהיעדר עומק טריטוריאלי לישראל. ואכן, קשה לשכוח את השטח הקטן והצר שבו נלחמה ישראל ב-1948 (ירושלים לא נכללה בשטח של המדינה עד שהעיר חולקה בין ישראל לירדן בעקבות הפסקת האש של 1949). הניצחון הישראלי ב-1967 היה קו פרשת מים, שכן הוא הביא עמו את כיבוש הגדה המערבית, מזרח ירושלים, רמת הגולן, רצועת עזה וחצי האי סיני. אלה העניקו לישראל עומק אסטרטגי גדול לאין שיעור משהיה לה בעת הקמתה.² ניתן לטעון שאותו מחסור ראשוני בעומק טריטוריאלי מכתוב מאז את הצורך של ישראל לנהל את מלחמותיה מעבר לגבולותיה.

האיום הקיומי הוא זה שדחף גם לפיתוחה של תוכנית הגרעין הישראלית, כמו גם ההערכה שבמקרה של תבוסה צבאית במלחמה קונבנציונלית, האופציה הגרעינית תבוא לעזרתה. נשק גרעיני נחשב למדיניות הביטוח במקרה שישראל תעמוד מול מצב חירום מדיני וצבאי קיצוני, כגון אובדן היתרון הצבאי הקונבנציונלי או השגת נשק גרעיני על ידי מדינה ערבית. תוכנית הגרעין של ישראל מגלמת את העדפתה למקסם עוצמה וחופש פעולה.³ תפיסת ישראל את תוכנית הגרעין האיראנית כאיום קיומי צריכה להתפרש בהקשר זה.

מוראות השואה יצקו משמעות חדשה לציונות והותירו צלקות עמוקות על מדינת ישראל. השואה הייתה מאירועי רצח עם הגדולים בהיסטוריה המודרנית, והצורך בביטחון הפך למרכיב מהותי בדנ"א הישראלי. הדגש החזק המושם על

Greg Cashman and Leonard C. Robinson, *An Introduction to the Causes of War: 2*
Patterns of Interstate Conflict from World War I to Iraq (Plymouth: Rowman and
Littlefield, 2007).

Efraim Inbar, *Israel's National Security Issues and Challenges since the Yom Kippur 3*
War (New York: Routledge, 2008).

המחיר החריג שהעם היהודי שילם על מימוש זכותו הלאומית נובע מהשואה, שמשמשת הן כמקור והן כהצדקה לדוקטרינת הביטחון ההתקפית של ישראל. מכוח דוקטרינה זו הפציצו מטוסים ישראלים את הכור הגרעיני "אוסירק" שבעיראק ביוני 1981, וכן (על פי הפרסומים) את אתר הכור הגרעיני הסורי בספטמבר 2007. ההצדקה למלחמת לבנון של 1982 התבססה גם היא על לקחים מהשואה, כפי שנתפסו בעיניה של המנהיגות הישראלית אז.⁴

התכנון האסטרטגי של ישראל מיישם שלושה יעדים מרכזיים: הבטחת קיומה של המדינה; הגנה על שלמותה הטריטוריאלית; שמירה על יתרון מול אויביה מבחינת עוצמה. ישראל אכן קידמה משמעותית את עוצמתה היחסית כאשר הצליחה להרחיק מדינות ערביות מרכזיות מלחבור לקואליציות המבקשות לתקוף אותה. בנוסף, ישראל עמדה כמה וכמה פעמים בהצלחה במבחן המלחמה.

התפיסה האסטרטגית של הודו עוצבה גם היא על ידי גורמים גיאוגרפיים והיסטוריים, לצד המציאות הגיאופוליטית אתה היא התמודדה בתקופות שונות. מאז קבלת עצמאותה בשנת 1947, ועד סוף המאה העשרים, הגיבה הודו למצב הגיאופוליטי הגלובלי והאזורי בהתאם לתפיסות הביטחון שלה. השיח הביטחוני של הודו במהלך תקופה זו הושפע בעיקר מהמלחמה הקרה – עידן שבו איומים קיצוניים בדינמיקה של עולם דו־קוטבי היו המקור המרכזי לערעור הביטחון. בניגוד לכך, הנשק הגרעיני נתפס בהודו כמספק ערבות ביטחונית. עם זאת, המדיניות האסטרטגית של הודו לא מוסדה, ומנהיגים פוליטיים כריזמטיים, ובעיקר ג'והרלל נהרו ובתו אינדירה גנדי, היו אלה שקבעו את החזון האסטרטגי של המדינה. קץ המלחמה הקרה, והניסויים הגרעיניים של הודו ב־1998, שינו דרמטית הן את תפיסת הביטחון שלה והן את נקודת מבטה האסטרטגית.⁵

התפיסה האסטרטגית הנוכחית של הודו מעוצבת על פי אתגרים ושאיפות שרבים מהם ייחודיים למדי. הודו נמנית על המדינות הגדולות בעולם, הן מבחינה דמוגרפית והן מבחינה גיאוגרפית, והבסיס התעשייתי והטכנולוגי שלה הינו אדיר ממדים. בהיותה מדינת גרעין מוצהרת עם יכולות מרשימות בחלל, הודו משחקת בהכרח תפקיד חשוב, הן בזירה האזורית והן בזירה הבין־לאומית. הודו היא המנהיגה הטבעית של אזור דרום אסיה, שכן היא שולטת על כמעט שלושה רבעים מהטריטוריה והאוכלוסייה בו. גבולותיה, הכוללים יבשה וים, נהרות והרים, הם ארוכים וחדירים, ועובדה זו מקשה מאוד על ניהול יחסיה של הודו עם שכנותיה, בעיקר משום שהגבולות אתן לא נקבעו ולא סומנו באופן מלא.

4 Guy Ben-Porat and others, *Israel Since 1980* (New York: Cambridge University Press, 2008).

5 C. Raja Mohan, *Crossing the Rubicon: The Shaping of India's New Foreign Policy* (New Delhi: Viking, 2003).

הודו מצויה בסכסוך מתמשך עם שכנתה הקטנה ביותר, פקיסטן. שורש המחלוקת היה ונותר חבל קשמיר, שפקיסטן תובעת את זכותה עליו מנימוקים דתיים. מאז 1947 לחמו הודו ופקיסטן שלוש מלחמות גדולות ואחת קטנה יותר. בנוסף לכך, הודו נלחמת בטרור בכמה מאזורי המדינה, ובקשמיר היא מנהלת מלחמה אסימטרית. כניסת הנשק הגרעיני לארסנל של שתי היריבות העלתה את המחיר הפוטנציאלי של כל עימות ביניהן. במקביל, הודו ופקיסטן מעורבות בשיחות שלום מתסכלות, מקוטעות ובלתי יעילות, שנועדו להסדיר את המחלוקות ביניהן סביב הגבולות. יחסי הודו עם סין הם מקור נוסף של יריבות באזור.

האתגרים שכוחות חיצוניים כמו פקיסטן וסין מעמידים בפני הודו אולי אינם קיומיים, אך עדיין מאיימים. כל עוד הודו לא תגיע להבנות עם פקיסטן, לא ניתן להשיג שלום ויציבות בדרום אסיה. גם להתגברות חוסר היציבות והיעדר הביטחון באפגניסטן יש השלכות מרחיקות לכת על הודו. שיתוף פעולה בין-לאומי אפקטיבי בנושאי טרור הוא עדיין אתגר מרכזי עבורה. לעלייתם של שחקנים לא מדינתיים אלימים הפועלים נגד הודו הייתה השפעה חמורה על ביטחונה הלאומי. בנוסף לכך, האיומים הפנימיים, המוצאים ביטוי באלימות חברתית וקהילתית, הינם קשים ומעוררי דאגה.

סקטיקות צבאיות

המצב הביטחוני בישראל אינו יציב: היא מוקפת בישויות מדינתיות ולא מדינתיות, אתן היא נלחמת מאז הקמתה ב־1948. עימותים אלה כללו את מלחמת העצמאות ב־1948, מלחמת סיני ב־1956, מלחמת ששת הימים ב־1967, מלחמת ההתשה מול מצרים בשנים 1968–1970, מלחמת יום הכיפורים ב־1973, מלחמת לבנון הראשונה ב־1982, האינתיפאדה הראשונה בשנים 1987–1993, האינתיפאדה השנייה ("אינתיפאדת אל־אקצא") בשנים 2000–2005, מלחמת לבנון השנייה ב־2006, והמלחמה האחרונה ברצועת עזה ב־2014 המכונה גם מבצע "צוק איתן". איראן, שאינה חולקת גבול עם ישראל, התבטאה גם היא בתוקפנות גלויה כלפיה. בכול הנוגע ליריבים לא מדינתיים, ישראל עומדת בפני איומים מצד חמאס ברצועת עזה ופת"ח בגדה המערבית, וכן מצד חזבאללה, הממשיך להוות איום מכיוון לבנון. העדיפות הראשונה של צה"ל היא להגן על ריבונותה של ישראל ועל שלמותה הטריטוריאלית. ישראל הגיבה לאיומים מצד אויביה באמצעות בניית צבא שנושען על העיקרון של איכות על פני כמות. היא משקיעה רבות בנשק מתקדם, מגייסת את כוחותיה המזוינים לשירות חובה, ומאמנת כוח מילואים המורכב מחלק משמעותי מאוכלוסיית המדינה. התכונה הבולטת ביותר של הצבא הישראלי, המבדלת אותו ממרבית הצבאות הלאומיים האחרים, היא השפעתו העצומה על המבנה החברתי של המדינה.

יש שני ממדים למבצעים הצבאיים של ישראל. הראשון הוא פעולה חשאית שנועדה לסכל מתקפות טרור ולהרתיע מפני ביצוע התקפות על אזרחים ישראלים; השני הוא שורה של מלחמות ומבצעים צבאיים גלויים. כאמור, ישראל מנהלת עימותים צבאיים ישירים מזה עשרות שנים. ביצועי צה"ל נגד אויבים מבחוץ, דוגמת מצרים וסוריה, היו מרשימים במיוחד. השמדת חיל האוויר המצרי עם פתיחתה של מלחמת ששת הימים ב-1967 הייתה מהלך מזהיר שהיטה את הכף לרעת הערבים. היכולת של ישראל לספוג את ההלם של מתקפת יום הכיפורים ב-1973, ואף להפוך את הקערה על פיה באמצעות מתקפות נגד בסיני ומעבר לתעלת סואץ וכן ברמת הגולן, מעידה על כושר צבאי רב.

אחרי שנים של התאמה לאתגרים שהציבו האינתיפאדות, הפך צה"ל לפשיר מאוד לתת מענה גם למה שהוא מכנה "עימותים בעצימות נמוכה". יחד עם זאת, ישראל מצאה עצמה מתקשה להילחם במה שהאסטרטגים שלה מכנים "עימותים בעצימות גבוהה", כמו זה שהיה בלבנון ב-2006. הניסיון הישראלי בלבנון מוכיח שקרב אינטנסיבי נובע לא בהכרח מסדר הגודל של היריב, אלא מאתגרי האיכות שמציבים יריבים היברידיים. הניסיון הביא את ישראל לכוון מחדש חלקים גדולים מההכשרה הצבאית לעבר תחום העימותים בעצימות גבוהה, ובהצלחה רבה מבעבר.⁶ הודו כיוונה את האסטרטגיה הצבאית שלה בראש ובראשונה לניהול מלחמות בין מדינות בעזרת ארסנל נשק קונבנציונלי וגרעיני גם יחד. יריבתה העיקרית פקיסטן מיקדה את האסטרטגיה הצבאית שלה באופן בלעדי בניהול מלחמה נגד הודו. המדיניות ההודית מורכבת יותר, שכן היא מתמקדת במלחמות בין מדינות, אך תוך שימת דגש על הכלה של התקוממויות מקומיות ומלחמות בקנה מידה קטן בגבולות. הניסיון האחרון של הצבא ההודי בקשמיר אינו מספק עדות של ממש לכך שהוא זנח את אסטרטגיית העימות בין מדינות.⁷ הדבר אף מוצא ביטוי בדבריו של ראג'ש רג'ופאלן, שכתב כי "הצבא ההודי הצליח להתאים עצמו למאבק בהתקוממות רק עד גבול מסוים, והמגבלה העיקרית שלו היא ההטיה החזקה הקיימת בדוקטרינה שלו לכיוון מלחמה קונבנציונלית".⁸

העימות והמחלוקת שאופפות את דוקטרינת המלחמה של הודו, המכונה "Cold Start", הן תזכורת ברורה לכך שהודו ניצבת מול פערים ענקיים בין שאיפותיה הבאות לידי ביטוי בדוקטרינה, ובין יכולותיה בפועל. דוקטרינת "Cold Start"

David E. Johnson and others, eds., *Preparing and Training for the Full Spectrum of Military Challenges: Insights from the Experiences of China, France, the United Kingdom, India and Israel* (Santa Monica: RAND, 2009), pp. xx, xxvi.

Norrin M. Ripsman and T. V. Paul, *Globalization and the National Security State* (New York: Oxford University Press, 2010), p. 126.

Rajesh Rajagopalan, *Fighting Like a Guerrilla: The Indian Army and Counterinsurgency* (New Delhi: Routledge, 2008), p. 29.

שמה דגש על גיוס מהיר ויעדים טריטוריאליים מוגבלים, ונועדה ביסודה לתקוף ולהשמיד כוחות של צבא פקיסטן ב"מכות עונשין", כפעולות תגמול על מתקפות טרור נגד הודו. כל זאת, מבלי להגיע להסלמה קונבנציונלית או גרעינית רחבה יותר. הרמטכ"ל החדש של צבא הודו, הגנרל בפיין קאוןאט, התייחס לקיומה של דוקטרינה זו בראיון שנתן לאחרונה,⁹ אך אחרים בהודו אמרו כי "אין עדיין כל הוכחה לכך שלהודו יש את היכולות הדרושות כדי ליישם מהלך שדומה במשהו ל"Cold Start"¹⁰.

הערכה השוואתית

הודים רבים ציינו בהזדמנויות שונות שכאשר מדובר בבעיות הקשורות לפעולות צבאיות, הודו יכולה להתייחס לישראל כמודל. שתי המדינות מתמודדות עם סביבות אסטרטגיות המחייבות קיומם של צבאות שיהיו ערוכים לעמוד מול שילוב של איומים פנימיים עם איומים חיצוניים. איומים כאלה תובעים קיומם של צבאות מאומנים, מאורגנים ומצוידים לפעולות בעצימות נמוכה וקונבנציונלית גם יחד. התאמת הצבאות לעימות בעצימות נמוכה או למלחמות בקנה מידה קטן הייתה תהליך הדרגתי, שכן דינמיקות ארגוניות מושכות להעדיף התכונות למלחמה קונבנציונלית. למרות זאת, שני הצבאות עשו מאמץ בכמה תחומים להסתגל למצב החדש, עם רמות שונות של הצלחה.

העובדה שישראל חייבת להכין את צבאה למגוון של איומים, הופכת אותה למקור הטוב ביותר להשוואה עבור הודו. כפי שהצבא ההודי למד מהניסיון בקשמיר ובצפון-מזרח הודו, גורמים לא מדינתיים אלימים, למרות היותם מתויגים כאיומים בעצימות נמוכה, עלולים להיות קשים מאוד להתמודדות. בנוסף לאיומים בעצימות נמוכה, צבא הודו חייב להיות מוכן להתמודד עם יריבים מדינתיים החמושים בנשק גרעיני. לכן, הניסיון העדכני של ישראל בהתמודדות עם ההתקוממות בשטחים הפלסטיניים ועם מיליציות חמושות היטב בלבנון, במקביל לשמירת רמת המוכנות לפעולות נגד איראן וסוריה, יכולים לשמש כמודל יעיל לצבא ההודי.

ברמת המאקרו, צבא הודו יכול ללמוד מהשיטות הישראליות לשמירה על ביטחון האזרחים. אולם כאשר הדברים אמורים בסוגיות ספציפיות, הניסיון הישראלי עשוי להיות לא רלוונטי במה שנוגע לחיזוק הסביבה הביטחונית של הודו. להלן הגורמים שכדאי לזכור בעת שעורכים השוואה בין הפעולות והמבצעים של שני הצבאות.

General Bipin Rawat, interview by Sandeep Unnithan, "We Will Go Across Again", *India Today*, January 16, 2017.

Vipin Narang and Walter C. Ladwig III, "Taking 'Cold Start' Out of the Freezer?", *Hindu*, January 11, 2017.

אסטרטגיה התקפית מול אסטרטגיה הגנתית

התנהגות הצבא הישראלי מונעת בחלקה משיקולים הקשורים בעימותים צבאיים ארוכים, ובחלקה משיקולי המגבלות הדמוגרפיות והגיאוגרפיות של ישראל. כתוצאה מכך, צה"ל פיתח דוקטרינה צבאית הדוגלת בלחימה מחוץ לגבולותיה של מדינת ישראל. במילים אחרות, ההגנה הלאומית של ישראל היא התקפית, כאשר מתקפות מנע הן גורם מרכזי באסטרטגיה הצבאית שלה. בניגוד לכך, גישתה הצבאית של הודו היא בעיקר הגנתית. למרות שתוכניותיה הצבאיות כללו פעולות התקפיות נגד פקיסטן, היה קשה להוציא תוכניות אלו לפועל. אפילו כאשר הייתה עדות מספקת לכך שפיגועי הטרור נגד הפרלמנט ההודי ב-2001, במומביי ב-2008 ובבסיס האווירי בפטנקוט ב-2016 נהגו ותוכננו על ידי טרוריסטים מפקיסטן, ממשלת הודו לא נקטה פעולות עונשין נגדה.

שטחה של ישראל ואוכלוסייתה מהווים פחות מאחוז אחד מאלה של הודו. ישראל ניהלה מלחמות עם כל שכנותיה, ויחסיה אתן היו מתוחים עקב סכסוכים טריטוריאליים. זאת ועוד, ישראל לא רק חסרה עומק אסטרטגי, אלא גם חווה תחושת אמת של חוסר ביטחון גיאופוליטי. סיבות אלו חשובות מספיק כדי לגרום לה לשאוף שקו ההגנה שלה יהיה מעבר לגבולותיה, ובכלל זה מעבר לים או בתוך טריטוריות זרות. לעומת זאת, להודו יש עומק אסטרטגי מספיק נגד יריבותיה. לאחר המתקפות הכיורוגיות האחרונות של הצבא ההודי לאורך קו השליטה, אמר ראש הממשלה מודי כי "הודו לא תקפה אף אחד. אין לה כל רצון להשתלט על שטח כלשהו".¹¹

מנהיגים ישראלים נוטים להזהיר בפומבי את שכנותיה של ישראל מפני פעולה צבאית – איום שלעיתים קרובות מגובה בפעולות של ממש. האמינות לגבי נחישותה של ישראל להשתמש בכוחה הצבאי גדלה במידה ניכרת לאחר שמנחם בגין עלה לשלטון ב-1977. יש לשער שהדימוי הניצי שלו בעולם הגביר את ההרתעה הישראלית. בגין הראה מוכנות רבה יותר מקודמיו להשתמש בכוח כדי להשיג מטרות פוליטיות מעבר לגבולות ישראל.¹² ראש הממשלה הנוכחי, נתניהו, שהיה מבקר קולני של העמדות ה"יוניות" של קודמיו, נהנה גם הוא ממוניטין של מפעיל יד קשה, במיוחד נגד חמאס וחזבאללה. לעומת זאת, ראש ממשלת הודו, מודי, עדיין לא רכש דימוי ניצי, על אף מה שנראה כתפיסה נוקשה ועמדה פומבית אגרסיבית שלו. מודי גם טרם הציג את המקבילה ל"דוקטרינת בגין", הגורסת שישראל תפעל נגד כל איום על קיומה.

¹¹ "India has Never Attacked or Been Hungry for Territory, only Fought for Others: 11 PM Modi", *Indian Express*, October 3, 2016.

¹² Inbar, *Israel's National Security Issues and Challenges since the Yom Kippur War*, 12 p. 16.

מערכת היחסים בין הצבא למדינה

מערכת יחסים סימביוטית קיימת בין אזרחי ישראל לצה"ל, כאשר הצבא מתפקד ככוח מאחד של כלל החברה הישראלית. תמימות דעים כמעט מלאה שוררת בקרב החוקרים, לפיה צה"ל ממלא תפקיד מרכזי, אם לא דומיננטי, בעיצוב המדיניות הביטחונית של ישראל. על אף שהצבא הישראלי כפוף על פי חוק למנהיגות הפוליטית של המדינה, הוא שותף שווה מעמד בתהליך הביטחוני ובקבלת החלטות גם בנושאי חוץ. ייחודה של מערכת היחסים האזרחית-צבאית הישראלית מתבטא בכך שהצבא, "המעורב עמוקות בתהליך המדיני, משפיע הן על הדרג המדיני והן על הציבור, בזכות ידיעותיו וטיעונו המשכנעים, ועדיין מציית לדרג המדיני".¹³ התפיסה של "אומה מגויסת" או "צבא העם" מקורה במדיניות הגיוס הכמעט גורפת של ישראל, אשר גובשה ויושמה בשל הנחיתות המספרית שלה ביחס לשכנותיה הערביות. מדיניות זו מטפחת קשר חזק בין החברה לצבא. במהלך שירות החובה לומדים כל הישראלים לחיות יחד ולחלוק מטרה משותפת של הגנה על מולדתם. גם לאחר חזרתם לחיים האזרחיים, הם ממשיכים להישאר "חיילים בחופשה של 11 חודשים בשנה", כפי שאמר פעם יגאל ידין, הרמטכ"ל השני של ישראל.¹⁴ אחד החוקרים ציין באופן ביקורתי כי "ישראל היא לא מדינה שיש לה צבא, אלא דוגמה מובילה לחברה מונעת צבאית, המגייסת לעצמה דימוי של מדינה".¹⁵ בשל הדומיננטיות של הממסד הצבאי בישראל, קשה לעשות הבחנה מוחלטת בין מנהיגים אזרחיים לצבאיים. מפקדים צבאיים, בין שפרשו מצה"ל ובין שנמצאים בשירות פעיל, ממשיכים להשפיע על היבטים שונים בפוליטיקה, בחברה, בכלכלה ובתרבות בישראל. עם סיום הקריירה הצבאית שלהם, מפקדים כאלה פונים לעתים קרובות לקריירה שנייה במגזר האזרחי. אין זה מקרה שישחק רבין, אהוד ברק ואריאל שרון, כולם מפקדי צבא בכירים בעברם, טיפסו עד לראשות הממשלה. באופן פרדוקסלי, העליונות של הממסד הביטחוני הישראלי הקלה פעמים רבות על גנרלים בצבא ובכירים בשירותים החשאיים של ישראל לקרוא תגר על המדיניות הנוקשה והקשה של כמה ראשי ממשלה. ראש הממשלה נתניהו נוהג להמעיט בחשיבות עמדותיהם של ראשי מערכת הביטחון שהפגינו ביקורת כלפי מספר מרכיבים במדיניותו, ומינויו של אביגדור ליברמן לשר הביטחון במאי 2016 נתפס כמהלך של ראש הממשלה נגד מערכת זאת. ליברמן הנוקשה ידוע בביקורת

Kobi Michael, "The Dilemma behind the Classical Dilemma of Civil-Military Relations: The 'Discourse Space' Model and the Israeli Case during the Oslo Process", *Armed Forces and Society* 33, no. 4 (2007): 518-546.

Ahron Bregman, *Israel's Wars: A History since 1947* (New York: Routledge, 2000), pp. 46-47.

David Theo Goldberg, *The Threat of Race: Reflections on Racial Neoliberalism* (Victoria: Wiley-Blackwell, 2009), p. 137.

החריפה שלו על התנהגות הצבא הישראלי, וכמי שקרא תמיד לצעדים תקיפים נגד הפלסטינים.¹⁶

מאז מינויו של משה דיין לשר הביטחון ב־1967, מונו לשרי ביטחון בישראל פוליטיקאים בעלי רקע ביטחוני משמעותי. החריגים לכך היו מנחם בגין (1980–1981), עמיר פרץ (2006–2007), וכיום אביגדור ליברמן. עם זאת, אין לראות במינויו של ליברמן, שעשוי להיות תופעה זמנית בלבד, אות לסיום תפקידו הדומיננטי של הממסד הצבאי בתהליך המדיני בישראל.

לעומת ישראל, המסגרת האזרחית-צבאית של הודו מוטה במידה רבה לטובת ההנהגה האזרחית. הצבא ההודי נרתע מלהשתתף בתהליך המדיני ומבודד מהחברה האזרחית. הביורוקרטיה האזרחית של הודו שולטת כמעט לחלוטין בתהליכים הביטחוניים ובתפקידים הבכירים במנגנוני הביטחון הלאומי, והמנהיגות הצבאית ההודית אינה חושפת בדרך כלל את חילוקי הדעות שלה עם המנהיגות האזרחית בפני התקשורת והציבור.

קווי המתאר של הממשק צבא-מדינה בהודו העצמאית נוצרו בתקופת כהונתו של ראש הממשלה נהרו, כאשר שר ההגנה השנוי במחלוקת שלו, קרישנה מנון, יזם כמה שינויים ארגוניים שהצבא התנגד להם בתוקף. טיפולה של המנהיגות הפוליטית ההודית בתכנון המבצעי של המלחמה הכושלת עם סין ב־1962 הוביל למסקנה שיש להשאיר את הנושאים המבצעיים לשיקול דעתו של הצבא. מאז התקבעה מסורת, לפיה הנחיות מבצעיות כלליות מגיעות מההנהגה הפוליטית, ואילו תכנון הפעולות בפועל נותר בידי ההנהגה הצבאית.¹⁷ כך, למשל, הצבא ההודי המשיך להשתמש בזכות הווטו שלו בסוגיות מבצעיות, כגון בשאלת הנסיגה מקרחון סיאצ'ן ובכוונה לבטל את חוק הסמכויות המיוחדות של הכוחות המזוינים (AFSPA) באזורים מסוימים השנויים במחלוקת.

מפקדי צבא בדימוס מונו אמנם כשגרירים וכמושלי מדינות בהודו, אך שלא כמו בישראל, כניסתם לפוליטיקה היא נדירה, וכשהם עושים זאת, הם לא ממלאים תפקיד משמעותי בה. מפקד הצבא לשעבר, גנרל סינג, נבחר לפרלמנט ב־2014. הייתה זו הפעם השנייה בלבד שמפקד צבא בדימוס נכנס לפרלמנט מאז מינויו של גנרל שנקר רויצ'ודהרי. יתר על כן, גנרל סינג מכהן כיום בתפקיד שר זוטרי בממשלה ולא כשר במשרד הביטחון.

Isabel Kershner, "Naming of Israeli Defense Minister Augments Netanyahu's Alliance", *New York Times*, May 25, 2016.

Harsh V. Pant, "Indian Strategic Culture: The Debate and its Consequences", in *Handbook of India's International Relations*, ed. David Scott (London: Routledge, 2011).

יש כיום בהודו דרישות גוברות לתת לצבא תפקיד בולט בקבלת החלטות הקשורות בביטחון הלאומי. אלה המצדדים במתן תפקיד רחב יותר לצבא ההודי מותחים ביקורת חריפה על יחסי צבא-מדינה בהודו ועל היעדר יוזמה לרפורמה בתהליכי הרכש הצבאי. בהקשר זה גם נטען כי הדמוקרטיה ההודית הצליחה ליצור מערכת המאפשרת פיקוח אזרחי חזק על הצבא, אך שיטה זו השפיעה לרעה על איכות קבלת ההחלטות האסטרטגיות במדינה.¹⁸

הסביבה הדיפלומטית

ישראל ויריבותיה במזרח התיכון מחליפות ביניהן מסרים רק לעתים רחוקות, שכן לישראל יחסים דיפלומטיים רק עם שתיים משכנותיה – ירדן ומצרים. לישראל אין יחסים דיפלומטיים עם סוריה, ערב הסעודית, איחוד האמירויות הערביות, קטר, עיראק או מעצמות אזוריות מרכזיות אחרות, כולל כמובן איראן, ויחסיה עם מדינות אלו מאופיינים בעוינות ארוכת שנים. כך, למשל, ישראל איימה לא פעם בתקיפה אווירית על איראן – איום שמבטא בברור את החיפוש הבלתי פוסק שלה אחר ביטחון. לעומת זאת, הודו שמרה תמיד על קשרים דיפלומטיים רשמיים עם יריבותיה – פקיסטן וסין – ואפילו במהלך עימותים צבאיים לא גירשה את שגריריהן. גם בעקבות מלחמת הודו-סין ב-1962, הודו צמצמה את נוכחותה הדיפלומטית בבייג'ין אך לא ניתקה את קשריה עם סין. ההנהגה ההודית חייבת להתחשב בתמונה הכוללת של מדיניות החוץ של המדינה לפני שהיא מחליטה על פעולת ענישה נגד ישויות מדינתיות או לא מדינתיות הפועלות בגבולותיה.

ישראל היא המדינה בעלת היכולת הגרעינית החשובה ביותר במזרח התיכון ההפכף. האסטרטגים הצבאיים הישראלים מודעים לכך שהפשיטות של ישראל מעבר לגבול או מתקפות המנע של צה"ל בשטחים הפלסטיניים, בלבנון או בסוריה, לא יגררו תגובה צבאית חזקה יותר או התקפה גרעינית עליה. הנזק המרבי שיכול להיגרם לישראל הוא ממתקפות גרילה וירי רקטות של חזבאללה וחמאס. אסימטריה כזו מעניקה לצה"ל שסתום ביטחון משמעותי. בניגוד לכך, להודו יש שתי שכנות גרעיניות, ולפיכך אין זה אפשרי או רצוי לה להעתיק את שיטות הפעולה הפרובוקטיביות של ישראל כלפי שכנותיה.

למדיניותה של הודו כלפי שכנותיה יש השפעה רבה על מצבה הפנימי, במיוחד במחוזות הסמוכים לגבולות: מתחים אקראיים בסרי לנקה פוגעים במדינת טמיל נאדו שבדרום הודו, שיש לה קשרים אתניים קרובים עם הטמילים של סרי לנקה. שיקולים פוליטיים בטמיל נאדו השפיעו על המדיניות של הודו כלפי הסכסוך האתני בסרי לנקה, כפי שניתן לראות מהתערבותה הצבאית שם. מצב זה נכון

18 Stephen P. Cohen and Sunil Dasgupta, *Arming Without Aiming: India's Military Modernization* (Washington, DC: Brookings Institution, 2010).

גם לגבי מדיניותה של הודו בבנגלדש, שבה ניתן לזהות בברור השפעה מקומית חזקה של בנגל המערבית. אפילו מדיניותה של הודו כלפי פקיסטן אינה עומדת בפני עצמה, אלא מושפעת מהתפתחויות פוליטיות בקשמיר. מדיניותה של הודו כלפי שכנותיה מעוצבת, אפוא, בעיקר על ידי הדינמיקה הפוליטית הפנימית ולא על ידי שיקולים של מדיניות החוץ. בניגוד לכך, מדיניות החוץ של ישראל לא מוגבלת על ידי שיקולים דומים.

עוצמה צבאית יחסית

ישראל ממשיכה להיות בעלת יתרון מכריע על שכנותיה הערביות מבחינת איכות כלי הנשק וכוח האדם שלה. מלבד הנשק המתוחכם, לישראל יתרונות פסיכולוגיים ואסטרטגיים מובהקים על פני יריביה. לעומת זאת, להודו יש אמנם יתרון צבאי מסוים על פקיסטן, אך לא יתרונות אסטרטגיים ופסיכולוגיים מכריעים. יתר על כן, להודו אין שום יתרון על פני סין. אף על פי שהודו חיזקה את יכולותיה ההתקפיות והיא רוכשת יכולות הקרנת עוצמה חדשות, אין לה מתקני ייצור ביטחוניים מקומיים אמינים.

הצבא הישראלי תיקן את רוב הליקויים שנחשפו במלחמת 1973, ולאחר מכן הצליח להשיג כמה הישגים ראויים לציון. הפעולה המיוחדת המפורסמת ביותר שלו בוצעה ביולי 1976, כאשר סיירת מטכ"ל חילצה את הנוסעים הישראלים שהוחזקו כבני ערובה בשדה התעופה אנטבה שבאוגנדה, לאחר שמטוסם נחטף בידי מחבלים פלסטינים. השמדת הכור הגרעיני העיראקי ביוני 1981 היא דוגמה נוספת למבצע ישראלי מיוחד שהושלם בהצלחה. על אף הגינויים בזירה הבין-לאומית, מכת המנע על הכור נטרלה למעשה את תוכנית הנשק הגרעיני של סדאם חוסיין. הצלחות חוזרות ונשנות אלו אישרו את עליונותה הצבאית של ישראל מעבר לגבולותיה. לעומת אלו, "התקיפות הכירורגיות" שהודו ביצעה לאחרונה לאורך קו השליטה שלה בקשמיר הן מההישגים הבולטים הבודדים של הצבא ההודי מעבר לגבולות המדינה. צבא הודו ממשיך לגייס יכולות הגנה להגברת ההרתעה, אך ההנהגה המדינית ההודית לא הצליחה עד כה להפגין את הרצון הפוליטי הנחוץ כדי להתגבר על השיתוק המדיני בתחום הביטחון. "סנונית אחת אינה משרת את בוא האביב", ולצבא ההודי יידרש עוד זמן כדי לפתח יכולות מבצעיות מעבר לגבול.

אף דיון על עוצמתו של הצבא הישראלי לא יהיה שלם מבלי להתייחס לתפקיד שממלאת בו ארצות הברית. ישראל רואה בארצות הברית את התומכת ובעלת הברית העיקרית שלה, וארצות הברית מצדה רואה בישראל שותפה אזורית חיונית. האינטרסים המשותפים לשתי המדינות גדולים בהרבה מההבדלים ביניהן. כתוצאה מכך, ארצות הברית מספקת לישראל את הנשק העדכני ביותר שלה,

ואילו ישראל מגייסת את יכולתה לחדשנות במדע ובטכנולוגיה לשם ייצור אמצעי לחימה חדשים. במהלך העשורים האחרונים הפכה ישראל ליצואנית מובילה של ציוד ביטחוני והתברגה לצמרת עשרת יצואני הנשק המובילים בשוק העולמי. מגמות אלו מסבירות היטב את הסיבות לעוצמתו של צה"ל. בהשוואה לכך, להודו אין גישה לציוד הצבאי המשוכלל ביותר ולא תמיכה דיפלומטית ממעצמת העל המובילה בעולם, שהיא קריטית בכול פעולה צבאית.

מנגנונים משפטיים למאבק בטרור

ארגוני המשרטה, המודיעין והצבא תורמים כולם למאמצי המאבק בטרור של הודו. המקבילה ההודית למשרד לביטחון הפנים בישראל הוא משרד הפנים, שמפקח על המשרטה הלאומית, על מודיעין הפנים ועל הכוחות הצבאיים למחצה. החקיקה העיקרית העוסקת בטרור בהודו הוא החוק למניעת פעולות בלתי חוקיות (Unlawful Activities Prevention Act – UAPA). לצד זאת קיימים בכמה מחוזות בהודו, כגון מְהָרָשְטְרָה וקֶרְנָטָקָה, חוקים המשמשים להעמדה לדין של חשודים בטרור. החוק ההודי הראשון למניעת טרור (TADA – Terrorist and Disruptive Prevention of Terrorism) פג בשנת 1995¹⁹, והחוק למניעת טרור (Activities Act – POTA) שהחליף אותו בוטל ב-2004, לאחר טענות על שימוש לרעה באופן היישום שלו. בהמשך הוכנס תיקון לחוק הנוכחי המשמש למניעת טרור (UAPA). החוקים ההודיים השונים נגד טרור לא הצליחו לספק את התוצאות הרצויות. היו גם טענות על כך שחוקים אלה נוסחו כך שייגנו או לחילופין יפגעו בקהילות או בקבוצות דתיות מסוימות. "ועדת הרפורמות האדמיניסטרטיביות" (ARC) השנייה של הודו קבעה בדוח שלה מ-2008 כי "יש צורך לגבש מסגרת משפטית מקיפה ויעילה לטיפול בכול היבטי הטרור. החוק צריך לכלול אמצעים נאותים שימנעו שימוש לרעה בו".²⁰

אחד הליקויים העיקריים בגישה המוסדית של הודו למאבק בטרור הוא הפער העמוק בין האופן שבו הממשלה הפדרלית תופסת את הנושא ובין האופן בו עושים זאת ממשלי המדינות. זו הסיבה שההצעה להקים את "המרכז הלאומי ללוחמה

"The Terrorist and Disruptive Activities (Prevention) Act, 1987", *South Asia Terrorism Portal*, <http://www.satp.org/satporgtp/countries/india/document/actandordinances/TADA.HTM#7A>.

"Dealing with Terrorism: Legal Framework", Government of India, Second Administrative Reforms Commission, ch. 4, in *Combating Terrorism, Protecting by Righteousness, Report no. 8*, http://arc.gov.in/8threport/ARC_8thReport_Ch4.pdf.

בטרור" לא זכתה להצלחה. כמה מממשלות המדינות בהודו הטילו וטו על הקמת המרכז, בטענה שהוא יערער את המבנה הפדרלי של החוקה ההודית.²¹ מזה זמן רב מורגש צורך להוציא את תפקידי ביטחון הפנים ממשרד הפנים ההודי ולהעבירם למשרד נפרד, כמו המשרד לביטחון הפנים בישראל או המשרד לביטחון המולדת בארצות הברית, אך אף מהלך לא ננקט בכיוון זה עד כה. "הסוכנות הלאומית לחקירות", שהוקמה לאחר הפיגועים במומביי ב-2008, סובלת גם היא ממחסור בסמכויות.

למרות שגם הודו וגם ישראל הן דמוקרטיות פרלמנטריות, אופי המערכות השלטוניות שלהן שונה. בניגוד להודו הפדרלית, כל ישראל מהווה מדינה אחת. עובדה זו מעניקה לה יתרונות מסוימים שאין להודו הפדרלית. ממשלת ישראל אינה כפופה לרשות מבצעת נוספת בעלת סמכויות חוקתיות ליצור מנגנונים חקיקתיים ומוסדיים לטיפול בביטחון וביטחון, כולל על ידי מאבק בטרור.

ביוני 2016 חוקקה ישראל חוק חדש שהרחיב את כוחה של המדינה להילחם בטרור ואת ההגדרות מהם ארגוני טרור ופעולות טרור.²² החוק הישראלי החדש נגד טרור הוא קיבוץ של רוב הוראות החוק הקיימות, בנוסף להחלפה של מספר תקנות הגנה מימי המנדט הבריטי. אף כי החוק החדש נועד לחזק את הממסד הביטחוני והמשפטי במאבקם בטרור, יישומו בפועל צפוי להיתקל בקשיים, במיוחד בכול הנוגע ל"איונים והבלמים הדרושים כדי להגן מפני הפרות בלתי סבירות של זכויות אדם של יחידים".²³

ביטחון סייבר

ישראל פיתחה מומחיות עולמית בתחום ביטחון הסייבר, כחלק מהמאבק בטרור ובאיומים מתעוררים אחרים. מאחר שמוסדות הממשל והצבא בישראל נמצאים תחת מתקפה מתמדת של טרור סייבר ופצחנים (האקרים) ג'האדיסטים, יצרו גופי המשטרה וסוכנויות המודיעין שלה ארכיטקטורה תקשורתית איתנה ומאובטחת, עם יכולות הגנה והתקפה בתחום ביטחון הסייבר. בצדק נאמר כי בישראל "מהפכת

Gurmeet Kanwal, "India's Counter Terrorism Policies are Mired in Systemic Weaknesses", Institute of Defence Studies and Analyses, May 14, 2012, http://www.idsa.in/idsacomments/IndiasCounterTerrorismPoliciesareMiredinSystemicWeaknesses_gkanwal_140512.

Jonathan Lis, "Knesset Passes Sweeping Anti-Terrorism Law", *Haaretz*, June 15, 2016, <http://www.haaretz.com/israel-news/1.725225>.

"The Counter Terrorism Law 5775-2015", State of Israel, Ministry of Justice, The Legal Counseling and Legislation Department (International Law), http://www.justice.gov.il/Units/InternationalAgreements/HumanRightsAndForeignRelations/Faq/CounterTerrorismLaw5775-2015_BackgroundDescriptionJune2016.pdf.

הסייבר היא המהפכה השלישית, אחרי החקלאות והתעשייה.²⁴ מדינות אחרות מאמצות את הגישה הישראלית במדיניות הסייבר הלאומית שלהן. לעומת זאת, הודו צריכה עדיין לפתח מנגנונים שיוכלו לתרגם את הניסיון הבינלאומי בתחום ביטחון הסייבר לדוקטרינה מתאימה לה. סוכנויות הביטחון והצבא של הודו חסרות תרבות של התמחות, ומומחי סייבר או מומחי לוחמת המידע ההודים אינם ממשיכים לעבוד בתחום ההתמחות שלהם לאחר תקופת שירותם המוגבלת בזמן. מפקדי הצבא והכוחות הצבאיים למחצה ממשיכים לפעול על פי התפיסה הכוללת לגבי תפקידיהם של קצינים, וגם כאשר קצינים מפתחים מידה מסוימת של התמחות בתחום הסייבר, מעברם לתפקידם הבא מקבל לרוב עדיפות על פני הישארותם בתפקידם הנוכחי ופיתוח מומחיות בו.²⁵

יכולות הסייבר של הודו מפגרות משמעותית אחרי השחקנים הגלובליים. "הפיקוח הרופף על החומרה שבה משתמשים גולשי האינטרנט ההודיים, וכן על המידע המועבר באמצעותם, [גורם לכך ש] מערך הביטחון הלאומי של הודו ניצב בפני משימה קשה כשהוא בא להתמודד עם מרחב הסייבר".²⁶ חוק טכנולוגיית המידע (IT) שנחקק בשנת 2000 נחשב כבר מזמן למיושן וזקוק לתיקון מקיף. מספר סוכנויות מופקדות על ניהול הרמות השונות של ביטחון הסייבר בהודו. סוגיות כמו חפיפת סמכויות בין ארגונים שונים, כפילות במאמצים או כשלים בתיאום פעולות במרחב הסייבר בין בעלי עניין שונים עדיין לא זכו לטיפול הולם.²⁷ אף שב-2013 גובשה מדיניות ביטחון סייבר לאומית בהודו וב-2014 מונה מתאם לאומי לביטחון סייבר, מערכת ביטחון הסייבר במדינה לא התקדמה מאז באופן משמעותי.²⁸ הודו מדורגת במקומות ה-96 וה-105 במהירות ההורדה וברוחב הפס הממוצע בהתאמה,²⁹ והיא נמצאת עדיין עשר שנים לפחות מאחורי ישראל ומדינות מפותחות אחרות בתחום ביטחון הסייבר.

John Reed, "Israel Cyber-Security Expertise Lures Growing Share of Investment", 24 *Financial Times*, January 12, 2016, <https://www.ft.com/content/dfa5c916-b90e-11e5-b151-8e15c9a029fb>.

Vivek Chadha, *Even If It Ain't Broke Yet, Do Fix It: Enhancing Effectiveness Through Military Change* (New Delhi: Pentagon Press, 2016), p. 129.

Arun Mohan Sukumar, "Upgrading India's Cyber Security Architecture", *Hindu*, 26 March 9, 2016.

Arun Mohan Sukumar and Col. R. K. Sharma, "The Cyber Command: Upgrading India's National Security Architecture", ORF Special Report 9 (New Delhi: Observer Research Foundation, March 2016).

Subimal Bhattacharjee, "Too Casual an Approach to Cyber Security", *Business Line*, 28 October 3, 2016.

Chittaranjan Tembhekar, "Demon in the Details: India has Low Cyber Security, Bandwidth", *Times of India*, December 22, 2016, <http://timesofindia.indiatimes>.

כפי שקורה בעולם כולו, מרחב הסייבר סיפק לארגונים אסלאמיסטיים וג'יהאדיסטיים בקשמיר פלטפורמה פסיכולוגית שבאמצעותה הם הצליחו להעביר מסרי תעמולה, אינדוקטרינציה וגיוס לקהלים הולכים וגדלים. השימוש הגובר באינטרנט ובטלפונים חכמים הוסיף דלק למדורה.³⁰ דוגמה מהזמן האחרון יכולה להסביר את הליקוי הרציני שיש להודו בהתמודדות עם חזית הסייבר: הדרכים שבהן השתמשו גורמי הביטחון והמודיעין של הודו בעת המהומות והאלימות שפרצו בקשמיר בעקבות חיסול מחבל ב־8 ביולי 2016, הוכיחו שיש עוד מקום רב לשיפור. במקום לפעול ביעילות נגד מתקפות הסייבר ששיגרו פעילים מקומיים ורשתות סייבר ג'יהאדיסטיות פקיסטניות, הגיבה ממשלת הודו בסגירת רשתות הטלפונים הסלולריים והקישוריות לאינטרנט בקשמיר. בכך היא שללה מגורמי הביטחון שלה עצמה גישה לרמזים חיוניים, למגמות ולמידע רלוונטיים במרחב הסייבר.

מניתוח פלטפורמות של רשתות חברתיות, כגון טוויטר, פייסבוק וווטסאפ, בשבוע שבין 8 ל־14 ביולי 2016, עולה כי מתוך מדגם של 126,000 תגובות, 45 אחוזים הגיעו ממיקומים גיאוגרפיים "לא ידועים", ארבעים אחוזים הגיעו ממיקומים בהודו, וכשמונה אחוזים הגיעו מפקיסטן.³¹ נתונים אלה לא מפתיעים, שכן כל עוד ממשלת הודו לא תפתח יכולות מתוחכמות לאיסוף מידע, ימשיכו פעילים מיליטנטיים לנצל פלטפורמות שונות של רשתות חברתיות כדי להסית לטרור.

מסקנות

מאמר זה בחן את התפיסה האסטרטגית של ישראל, תוך סקירה היסטורית קצרה של התמודדות צה"ל עם הסכסוך הערבי־ישראלי, וכן בחן את הנסיבות השונות שבהן פועלים הצבא הישראלי והצבא ההודי. מבחינת הישראלים, העימות האסימטרית עם הפלסטינים נסוב סביב ההכרה בזכותם לחיות במדינה יהודית ללא איום חיצוני. אותם פלסטינים הדוגלים בהתנגדות באמצעי טרור אלימים, כולל פיגועי התאבדות והתקפות טילים, כדרך להתגבר על חוסר הסימטריה, מקבעים עוד יותר את מנטליות המצור של ישראל.

המאמר השווה בין האסטרטגיות של הצבא ההודי ושל צה"ל, וזאת במטרה להראות את ההבדלים באופן שבו שני הצבאות מגיבים לטרור ולצורות אחרות

com/city/mumbai/demon-in-the-details-india-has-low-cyber-security-bandwidth/articleshow/56112036.cms.

Justin Rowlett, "How Smartphones are Shaping Kashmir's Insurgency", *BBC*, July 30 12, 2016, <http://www.bbc.com/news/world-asia-india-36771838>.

Himanshi Dhawan, "Pakistan May be Waging Proxy War in Cyberspace Too", *Times of India*, July 19, 2016, <http://timesofindia.indiatimes.com/india/Pakistan-may-be-waging-proxy-war-in-cyberspace-too/articleshow/53273657.cms>.

של לוחמה אסימטרית. חשוב להכיר בכך שתגובות צבאיות ללוחמה אסימטרית כרוכות בקשיים מוסריים, משפטיים ואסטרטגיים. ישראל מגיבה על מעשי טרור באופן יזום והתקפי, בעוד שהודו מעדיפה להישאר מתגוננת ותגובתית. פיגועי הטרור בהודו מתרחשים בשגרה מדאיגה, ובנסיבות הגיאורפוליטיות הנוכחיות לא נראה שיש תקווה רבה לצמצם את איום הטרור הג'יהאדיסטי שם. בכול פעם שמתרחש פיגוע בהודו, מתעוררת זעקה להגיב בפעולת תגמול נגד המבצעים, אולם גישתה של הודו למלחמה בטרור נותרה, כאמור, הגנתית ובלתי יצירתית בעליל. אם הודו לא תשכיל להתגבר על האתגרים האסטרטגיים והגיאורפוליטיים שתוארו לעיל, צבאה יתקשה להתמודד עם הטרור בדרך שעושה זאת ישראל. יש צורך דחוף בגיבוש אמצעי מנע הודיים חדשים נגד התקפות טרור. למרות פעולות התגמול שצבא הודו ביצע לאחר הפיגוע באורי שבקשמיר, קשה לקבוע בוודאות שגישה תקיפה זו תמשיך להינקט על ידו גם להבא.

להבין את איום הסייבר בעזרת האנלוגיה של "טרור בליסטי"

דוד שטרנברג

"אנו לא מבינים ולא מפנימים עד כמה אנו חשופים [לאיומים בעולם הסייבר]... בעיני, הדבר דומה לטילים... הייתי שם כשהחלו לשגר טילים בשנות השמונים. הם היו אז כלי נשק קטנים ולא מדויקים ולא נראו כאיום רציני. אבל כיום, כמעט שלוש שנים מאוחר יותר, עשויה להיות לטילים יכולת לפגוע אפילו בצלחת שעל גג בניין המטכ"ל. הדבר נכון גם לגבי תחום הסייבר. בעודנו עסוקים בהגנה על סודות הליבה, על מערכות ההגנה ועל התשתית הלאומית שלנו, אנו עשויים למצוא את עצמנו סופגים נזק רב במגזר האזרחי."

תא"ל איתי ברון¹

איומי סייבר הם תופעה חדשה, מתפתחת ומורכבת. אחת הדרכים המרכזיות לסייע למקבלי ההחלטות להתמודד עם הקושי שהיא יוצרת היא על ידי שימוש באנלוגיות כתבניות פסיכולוגיות מפשטות. אנלוגיה שימושית כזו היא הטרור, ובמיוחד "טרור בליסטי", כפי שהוא נחוץ במקרה הישראלי. כאשר נשענים על אנלוגיה זאת, ניתן להפיק ממנה שלוש תובנות: הראשונה היא כי יש מקום לשוב ולבחון הנחות יסוד מרכזיות על עתיד ביטחון הסייבר; השנייה היא האפשרות לאמץ מהמאבק בטרור אסטרטגיה היברידית לעולם הסייבר, הבנויה משישה רכיבים – הגנה, מעקב, הרתעה, הכרעה, מניעה ודיפלומטיה; השלישית, שנגזרת מאותה אנלוגיה, נוגעת להתארגנות אל מול האתגר ומדגישה את הצורך ליצור גם בעולם הסייבר תצורות מבצעיות גמישות חדשות, לצד רשת גופי שיתוף פעולה בין-לאומיים (ובעתיד אפשר שילוב בין השניים).

מילות מפתח: איום סייבר, טרור, בליסטיקה, אנלוגיה, מטאפורה, ישראל

Yoav Limor, "Attacks in the Golan Heights are a Matter of Time", *Israel Hayom*, 1 January 16, 2005, http://www.israelhayom.com/site/newsletter_article.php?id=22837.

דוד שטרנברג הוא בוגר בית הספר על שם קנדי באוניברסיטת הרווארד. מאמר זה הוא גרסה מקוצרת של מחקר שנכתב במסגרת זו.

להבין תופעה חדשה בעזרת אנלוגיות ומטאפורות²

מחקר היחסים הבין-לאומיים מתייחס בהרחבה לשימוש באנלוגיות ככלי לקבלת החלטות.³ הספרות בנושא זה מתבססת על חקירה של אירועים היסטוריים, המשמשים להפקת לקחים אותם ניתן ליישם על נושאים עכשוויים. יחד עם זאת, אנלוגיות ומטאפורות ניתן לאמץ וליישם לא רק על אירועים היסטוריים, אלא גם על רעיונות, נושאים, אנשים, מנגנונים ומצבים.

השימוש באנלוגיות ומטאפורות תורם היבטים פסיכולוגיים חשובים לקבלת החלטות. אנלוגיות ומטאפורות משמשות כמבני ידע לצורך עיבוד המידע והבנתו, וכן לשם השלמת נתונים חסרים.⁴ תיאוריות בלשניות ופילוסופיות מדגישות את תפקידן של האנלוגיות והמטאפורות גם כאמצעי המשמש יחידים וקבוצות להבנת תופעות מורכבות ובלתי מוחשיות, ובסופו של דבר לגזור מכך פעילויות.⁵ ועדיין, ישנן סכנות בשימוש באנלוגיות ומטאפורות. האנלוגיה כמנגנון פסיכולוגי יכולה להוביל את מקבל ההחלטות לצורות עיבוד חשיבתיות פשוטות ונגישות יחסית, אך לא דווקא נכונות. כמו כן, היא יוצרת הטיית "מסגור" שיש בה כדי להשפיע על הגישה והאופן שבהם מקבלי החלטות יתפסו את הבעיה.⁶

מדוע הנושא רלוונטי לסייבר?

זירת הסייבר היא עולם מורכב המתפתח במהירות. זוהי זירה קשה להבנה ולהמשגה בשל אופייה עתיר הטכנולוגיה, ההשפעה הרבה שיש לה על חיי היומיום, ריבוי הרכיבים המקושרים ביניהם, הדיסציפלינות השונות שמעורבות בה וקצב ההתפתחות המהיר שלה. פער דורות בין מקבלי ההחלטות, שפעמים רבות הם "חסרי אוריינות טכנולוגית", לבין אנשי המקצוע המומחים, רק מחריף מתחים אלה. אנלוגיות ומטאפורות יכולות לפשט את המכשול האינהרנטי הקיים בין שני הצדדים ולסייע בהכוונת אלה שהם בעלי ידע כללי.

2 אנלוגיות מוגדרות במאמר זה כהשוואה בין שתי ישויות שונות המבוססות על היבטים דומים, בעוד שמטאפורות הן השלכה של מאפיינים מישות אחת על השנייה. לצורך המחשה, "איטי כמו צב" היא אנלוגיה ואילו "שאגת האדם" היא מטאפורה.

3 Yuen Foong Khong, *Analogies at War: Korea, Munich, Dien Bien Phu and the Vietnam Decisions of 1965* (Princeton: Princeton University Press, 1992); Sean Lawson, "Putting the 'War' in Cyberwar: Metaphor, Analogy and Cybersecurity Discourse in the United States", *First Monday* 17, no. 7 (2012), <http://firstmonday.org/ojs/index.php/fm/article/view/3848/3270#p2>.

4 Khong, *Analogies at War*.

5 George Lakoff and Mark Johnson, *Metaphors We Live By* (Chicago: University of Chicago, 1980).

6 Daniel Kahneman and Amos Tversky, "Prospect Theory: An Analysis of Decision under Risk," *Econometrica*, 47, no. 2 (1979): 263-291.

כאשר בוחנים את שיח הסייבר העכשווי בארצות הברית, קשה שלא להתרשם מריבוי האנלוגיות המשמשות בתחום זה. ככול הנראה, יש בכך ביטוי לאתגר שהנושא טומן בחובו ולצמא להיאחז בעוגנים מוכרים בסוגיה קשה לתפיסה מבחינה אינטלקטואלית. האנלוגיות מגוונות בסוגן ובהיקפן, אולם הן מציעות פתרונות חלקיים בלבד. חלקן מציגות אירועים, ואחרות – קטגוריות של לוחמה, סוגי נשק או תהליכים היסטוריים.⁷ רשימה קצרה שלהן כוללת את אירועי פרל הרבור ו־11 בספטמבר 2001, הוריקן קתרין, "המלחמה הקרה", "דוקטרינת מונרו", "פרויקט מנהטן", דיני הים, "מלחמת בזק" (בליצקריג), "יוזמת ההגנה האסטרטגית", פרוץ מלחמת העולם הראשונה, בלקניזציה, עוצמה אווירית, לוחמה כלכלית, לוחמה ביולוגית, מערכת החיסון, הרתעה גרעינית באמצעות "הרס הדדי מובטח" (MAD), מלחמת צוללות, תופעת הפיראטיות, "מלחמות חדשנות", "התקוממות", וכן הלאה.⁸ יש הטוענים כי החלת המשגה צבאית על מרחב הסייבר אינה יעילה, שכן היא מחזקת את רעיון ה"איום" וזורעת תבהלה קבוצתית הפוגעת ביכולת לפתור בעיות באופן קולקטיבי. מטאפורות ידועות בשדה הסייבר, דוגמת "מרחב הסייבר" (cyberspace) או "ביולוגיה", לוקות גם הן בחסר. כך, הגדרות צרות כגון "מרחב הסייבר" מחמיצות את טבעו של עולם הסייבר, המשולב במרחב האמיתי, ואת הדינמיקה הבלתי ליניארית שלו. זאת ועוד, מטאפורות ביולוגיות, המתייחסות למתודולוגיות הקשורות לבריאות הציבור, למגיפות, למערכת החיסון ולרעיונות של "הסתגלות" או "הוליסטיות", מתעלמות מהמקור של הבעיה: מרחב הסייבר הוא יצירה אנושית, המשרתת רציונל חברתי-פוליטי ומתקיימת ברמה הסמנטית.⁹ הכתיבה בנושא זה בישראל פחות מפותחת מאשר בארצות הברית. עם זאת, כאשר בוחנים את השיח הציבורי בישראל, יש שימוש ברור באנלוגיות. לדוגמה, ישנם חוקרי אקדמיה המשתמשים במטאפורות מהעולם הביולוגי ("קוד מוטציה") או באנלוגיות מההיסטוריה של המלחמות, כגון התייחסות למתקפות סייבר כאנלוגיה להכנסת כטמ"מים (כלי טיס מופעלים מרחוק) לשדה הקרב.¹⁰ חלק מהחוקרים מתייחסים לעליית הזירה האווירית כדי לתאר את תחום הסייבר

Emily O. Goldman and John Arquilla, eds., *Cyber Analogies* (Monterey: Naval Postgraduate School, 2014).

Robert Axelrod, "A Repertory of Cyber Analogies", in *Cyber Analogies*, eds. Emily O. Goldman and John Arquilla.

David J. Betz and Tim Stevens, "Analogical Reasoning and Cyber Security", *Security Dialogue* 44, no. 2 (2013): 147-164.

Brent Rowe, Michael Halpern: ראו לדוגמה: "Is a Public Health Framework the Cure for Cyber Security?", and Tony Lentz, *Crosstalk* (Nov/Dec 2012): 30-38.

Gabi Siboni, ed., *Cyberspace and National Security: Selected Articles* (Tel Aviv: Institute for National Security Studies, 2013).

החדש,¹¹ ואילו אחרים מעדיפים אנלוגיה של "ונדליזם" במקום מלחמה.¹² גורמים רשמיים בממשלת ישראל המבקשים להסביר את הנושא לציבור משתמשים גם הם באנלוגיות, למשל מעולם הבריאות או מתחום הבטיחות בדרכים.¹³

האנלוגיה של "טרור בליסטי"

מאמר זה עושה שימוש במונח "טרור בליסטי" כדי לתאר את הטקטיקות של המתקפות שמבצעים ארגוני טרור, ובכלל זה ירי ארטילרי של פצצות מרגמה, של רקטות קצרות טווח וארוכות טווח, של רקטות מונחות ושל טילים (כולל, למשל, טילי קרקע-קרקע, ים-יבשה, נגד טנקים, טילי שיט, טילי כתף), וכן כטמ"מים. כאמור לעיל, נעשה שימוש בקשת רחבה של אנלוגיות כדי להבין את האתגר שמציב עולם הסייבר, ומאמר זה בוחן האם האנלוגיה של הטרור מתאימה לתיאור מתקפות סייבר. כדי להימנע מהשוואות כלליות, מתמקד המאמר במיוחד במקרה של אתגר "הטרור הבליסטי" שארגוני הטרור העמידו בפני ישראל במהלך שני העשורים האחרונים.

נוישטט ומאי הציעו בעבודתם הידועה *Thinking in Time* כי שימוש באנלוגיות ייעשה על ידי הבחנה ברורה בין הדומה ובין השונה,¹⁴ שכן בדרך זו מקבלי ההחלטות יהיו מודעים לנקודות החוזק והחולשה של אותן אנלוגיות. מאמר זה יעשה שימוש בפרקטיקה פשוטה ואינטואיטיבית זו כדי להשוות בין ירי טילים מצד ארגוני טרור על ישראל לאיום הסייבר, תוך הצבעה על קווי הדמיון והשוני ביניהם, ובסייגים הרלוונטיים.

החלת האנלוגיה של טרור בליסטי על איומי סייבר –

קווי הדמיון

מאפייני הנשק

המאפיינים של סוגי הנשק הבליסטי הם הסיבה המרכזית לכך שארגוני הטרור אימצו את הטרור הבליסטי כטקטיקה מובילה. מדובר בנשק פשוט ולא יקר: הוא בעל יכולת חדירה עמוקה לשטח האויב, וניתן להפעילו במקביל ובמרווחי זמן

Shmuel Even and David Siman-Tov, *Cyber Warfare: Concepts and Strategic Trends* 11 (Tel Aviv: Institute for National Security Studies, 2012).

Jonathan Silber, "Cyber Vandalism – Not Warfare", *Ynet*, January 26, 2012, <http://www.ynetnews.com/articles/0,7340,L-4181069,00.html>. 12

Hadas Geifman, "Dr. Eviatar Matania: 'Cyber Security is Likened to Hand Washing to Maintain Health – Important, But Not Enough'", *People and Computers*, June 26, 2012, <http://www.pc.co.il/it-news/89919/> 4, (in Hebrew). 13

Richard E. Neustadt and Ernest R. May, *Thinking in Time: The Uses of History for Decision Makers* (New York: Free Press, 1986). 14

קצרים (נדרשות דקות ספורות מרגע ההחלטה ועד הירי בפועל). זאת ועוד, קשה להתגונן מפני סוג זה של נשק, וקשה לאתרו בשל החתימה המזערית שלו ופריסתו הרחבה. במובן זה, לנשק הסייבר יש תכונות דומות: הוא מופעל במקביל ופעולתו מיידית, לרוב הוא קל לבנייה ולשימוש, אינו יקר (בעיקר מחייב ניצול חולשות ומודיעין) ויכול בקלות לחדור דרך "נקודות עיוורות ורכות" של היריב, במיוחד בתחום האזרחי והפרטי, אולם גם במטרות צבאיות.

היבטים של ייחוס מתקפות סייבר

מרחב הסייבר מעורר קושי מרכזי במה שנוגע לייחוסו לגורם כלשהו (בעיקר בזמן אמיתי). זאת, עקב הטשטוש בין זהויות אמת ובין כתובת ה-IP הניתנת לזיהוי.¹⁵ מצב זה מחליש את הבסיס לפעולת תגמול והרתעה, שכן תגובה שגויה עשויה להיות בלתי מדויקת ולהוביל להסתבכות, למבוכה ולנזקים שונים.

כאשר מחילים את אנלוגיית הטרור הבליסטי ברמת רזולוציה של אירוע ירי ספציפי (ולא מערכה רצופה), מופיעות שתי בעיות ייחוס דומות: הראשונה נוגעת למצב של תקרית ירי בודדת המתרחשת בין סבבים של עימות בקנה מידה גדול. במקרה זה הדילמה היא האם היריב העיקרי הוא שאחראי לירי או שמדובר בצד שלישי. זוהי בעיה מודיעינית מרכזית הקשורה לשאלה של עוצמת ההרתעה; הבעיה השנייה היא במקרה של אירוע ירי מסוים המתרחש במהלך עימות אינטנסיבי. כאן השאלה היא האם ניתן לזהות ולהפליל אתר מסוים כאחראי לשיגור. שאלה זו חשובה עקב אופי הסביבה האזרחית שבתוכה פועל ארגון הטרור. המספר הגבוה של שיגורים, האחסון והירי הנעשים מאתרים אזרחיים וממתקנים הומניטריים, הפעולה המבוזרת מבחינת פיקוד ושליטה, והתכונות של ניידות והסוואה, כל אלה תורמים לקושי בזיהוי. אין מדובר בזיהוי של אחראי-העל, אלא באדם או במקום ספציפיים הנושאים באחריות, שנגדם יש לפעול. הצורך בתגובה הולמת למקרה הספציפי מכתיבה את הצורך בייחוס ברור.

15 כמו בכול התחומים הטכנולוגיים, גם סוגיה זו משתנה במהירות. יש הטוענים כי בעיית הייחוס אינה רק טכנולוגית, אלא משתנה בהתאם לסדר הגודל של המטרה (הייחוס למטרות בעלות ערך גבוה לרוב אינו שגוי), וכן כי ייחוס הוא "אמנות": תהליך רב היבטים שמשלב הוכחות טכנולוגיות עם חשיבה מבצעית ואסטרטגית. כמו בחיים האמיתיים, התהליך אינו בינארי (נפתר/לא נפתר) ואינו מבוסס ראיות בלבד. בסייבר, כמו בתחומים אחרים, ייחוס מתבסס לא רק על ראיות פורנזיות, אלא גם על טווח רחב של מקורות מודיעין. יחד עם זאת, ייחוס בסייבר יכול לסטות מאנלוגיית הטרור הבליסטי מבחינת זמן, משאבים ותחכום היריב. עוד בנושא הייחוס ראו: Jon R. Lindsay, "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack", *Journal of Cybersecurity* 1 no. 1 (2015): 53-67; Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks", *Journal of Strategic Studies* 38 no. 1-2 (2015): 4-37.

תפקידם של גורמים לא מדינתיים ושל מדינות חסות

בלוחמת סייבר קיימת הבחנה בין פעולות סייבר שמבצעות מדינות או ממשלות לבין כאלו שמוצאות לפועל על ידי גורמים לא מדינתיים. יחד עם זאת, גורמים לא מדינתיים משמשים לעתים כזרוע או כהסוואה של מערכת לאומית, כך שהמדינה תוכל להכחיש מעורבות או להימנע מחציית הקו המהווה עילה למלחמה. תופעה דומה קיימת בשדה הטרור הבליסטי. הן מדינות (איראן לדוגמה) והן גורמים לא מדינתיים (למשל חזבאללה) השתמשו בעבר בארגונים קטנים כאמצעי עקיף לפעולה נגד ישראל.¹⁶ בשני המקרים, גורמים לא מדינתיים עשויים לרכוש יכולות משמעותיות בדומה למדינות, או להסוות עצמם כמדינות. כפי שהוסבר לעיל, פירוש הדבר הוא סבירות גבוהה יותר לתקריות שמטרתן לעורר עימות, וסיבוב נוסף ביכולת לשלוט במצב ולמנוע הסלמה.

ערבוב של תשתיות אזרחיות וצבאיות

ייחוס שגוי עלול לגרום לטעות בזיהוי התוקף. הדוגמה הקלאסית בתחום הסייבר היא מתקפת בוטנט שעושה שימוש בתשתית שנתפסה והוכנה מראש במטרה לשגר ממנה את המתקפה. ההשלכה המרכזית של התקפה על מחשב שנקלע להשתלטות "תמימה" היא יצירת נזק משני. כאשר תשתיות צבאיות ואזרחיות מעורבות זו בזו, הדבר יוצר בעיה מהותית. מצב דומה שורר כאשר מתקיים ירי רקטות מצד ארגוני טרור הפועלים משכונות אזרחיות. הצד השני אך הדומה בין מתקפות סייבר ובין הטרור הבליסטי הוא המטרה המשותפת של שניהם – הסבת נזק לתשתיות אזרחיות קריטיות, ובדרך זו שיבוש השגרה האזרחית. הן רקטות מונחות שנוורות על תחנת כוח והן נטרול תחנת כוח באמצעות מתקפת סייבר נועדו לעורר אימה באוכלוסייה ולזרוע חוסר ודאות, יותר מאשר לפגוע במאמץ המלחמתי הכללי.

מרכיבים של דינמיקת הסלמה

סכנת ההסלמה גדולה יותר במתקפות סייבר, משום שאלו אינן מחייבות תנועה של כוחות ואמל"ח, הן זולות, קלות למימוש ומיידיות, ובמקרים מסוימים ברגע ששוגרו הן יודעות להתפשט במרחב.¹⁷ כמה ממרכיבים אלה נכונים גם לטרור בליסטי: כאשר מנהלים מתקפה ומתקפת נגד יש מעט מאוד זמן לקבלת החלטות. בדומה לכך, טעויות במתקפת נגד או גרימת נזק משני גבוה, דבר שהוא אופייני למלחמת טילים, יכולות להתרחש גם בעקבות שיגור מתקפת סייבר כלפי יעדים

16 Eyal Zisser, "The Return of Hezbollah", *Middle East Quarterly* (Fall 2002): 3-11. 17 מת'יו ס' כהן, 'צ'אק ד' פרייליך, גבי סיבוני, "ארבעה עקרונות ועוד אחד: מודל חדש להגנת סייבר" (ראו מאמר בגיליון זה).

בעלי רגישות אזרחית. מהלך כזה עלול לעורר הסלמה מהירה, עקב פעולת תגמול ותגובת נקמה נגדית לפעולת התגמול. המאפיין של חתימה נמוכה שהוזכר לעיל מוסיף לערפל הקרב ולקושי להגיע לייחוס נכון.

ניתן לטעון שהשוני בקנה המידה ובקצב בין שני המקרים של טרור בליסטי ושל מתקפת סייבר הוא זה היוצר את ההבדל המהותי ביניהם: במקרה של הסייבר אין קווים אדומים ברורים או תפיסה ברורה האם יש מתקפה שהיא "חשובה יותר" או "אגרסיבית יותר" מהאחרת, כך שהשליטה על רמת ההסלמה הופכת לקשה ביותר. בניגוד לכך, בהקשר הבליסטי ניתן ליישם אמות מידה ברורות יחסית. אפשר גם לומר שבמקרה של מתקפה בליסטית ישראל יכולה להמתין עם תגובתה יום או יומיים, ולא להיגרר להסלמה הנובעת מדינמיקה של "הגנה אקטיבית". עם זאת, דומה שלמרות הקצב השונה בין מתקפות בליסטיות למתקפות סייבר, אותו עיקרון נשמר בשתייהן: אתגרים קבועים ניצבים בפני פעולות תגמול על מתקפות בליסטיות, ובאותה מידה תקריות סייבר אינן מסתיימות בהכרח בהסלמה מהירה.

גיוון הנשק

מאגר נשק הסייבר מתפרס על פני רצף הנמדד לפי מידת תחכומו. בקצה האחד נמצאות נזקות (malware) נפוצות, שמרבית מערכות האבטחה יודעות לנטרל בזכות חתימתן המוכרת. בצד השני של הרצף נמצאים האמצעים המשוכללים יותר, היודעים לנצל חולשות ברגע התגלותן ("מתקפת אפס ימים"), לדלג בין רשתות, להסוות עצמם ולפגוע בתשתית חיונית ספציפית. בעולם הטילים קיים רצף אחר אך דומה: בקצה האחד שלו נמצאים טילים לטווח קצר או פצצות מרגמה (למרות שהניסיון מלמד שגם הם מסוכנים וקטלניים), ואילו בצד השני מצויים כלים ארוכי טווח מדויקים, כטמ"מים התקפיים, טילי שיוט וטילי חוף-ים, היודעים לתמרן בצורה שונה ומבטאים את ההתקדמות בכול הנוגע לטווחים, לדיוק ולקטלניות, וכך מחייבים חשיבה אסטרטגית ומבצעית שונה.

בעיית הרב־קוטביות

למרות שכוחות חיזוניים, דוגמת איראן, רוסיה או קוריאה הצפונית, תרמו להפצת טכנולוגיות הטילים, נראה שהלחץ שהפעילה ישראל על נתיבי האספקה הביא לשינוי בתהליך זה. הלחץ הישראלי האיץ את הפיתוח של מחרטות וסדנאות הנשענות על יכולות מקומיות לייצור נשק – כפי שניתן לראות בשנים האחרונות ברצועת עזה. ההתרחבות של התעשייה המבוזרת, הנתמכת על ידי העברת ידע יותר מאשר על ידי העברת חומרים וציוד, מתפתחת לכדי איום מגוון ורב־מוקדי, בעיקר בצורה של מערכות טילים לטווחים קצרים שאינן זקוקות למוקדי אספקה.

במקביל, עולם הסייבר חולק את אותו מבנה של ריבוי שחקנים המנהלים בעצמם את המחקר והפיתוח, או לפחות את הייצור והשכלול של מערכת הנשק.

תהליך הלמידה

אחד מקווי הדמיון המרכזיים בין מתקפות סייבר ומתקפות בליסטיות הוא דינמיקת הלמידה. שלא כמו אנלוגיות מהעולם הביולוגי, מדובר בהתמודדות עם יריבים תבוניים שהאתגר שלהם הוא העברת טכנולוגיות ("טכנולוגיה טרנספורמטיבית")¹⁸, וזאת בשל הקושי להבין אותה מבחינה אסטרטגית. בשני המצבים, החיכוך המבצעי המתמשך מקדם את ההבנה, את אוצר המילים ואת התפיסות. בהקשר זה ניתן לציין כי אפילו התנסויות ייחודיות, דוגמת השימוש בוורוס "סטקסנט" (מתקפה על תשתית), ב"להבה" או ב-"Heartbleed", הן "טרנספורמטיביות" ומהוות חלק מרצף של למידה.

גם הטרור הבליסטי נגד ישראל רשם התקדמות שהתבססה על למידה ממשברים (כגון מלחמת לבנון השנייה), אם כי במונחים מעשיים מדובר בתהליך למידה שהיה ממושך יותר. בהקשר זה יש לציין כי המונח המשמש בעגה הצבאית להגדרת התפתחויות בשדה הטרור הוא "תחרות למידה".¹⁹ גם במקרה הבליסטי יש מתח מובנה בלימוד והמשגת התופעה בין השקפותיהם של אנשי האקדמיה ובין האנשים בשטח,²⁰ בדיוק כפי שקורה במרחב הסייבר.²¹

החלת אנלוגיית הטרור הבליסטי על איומי הסייבר –

קווי השוני

כחלק מההיצמדות למסגרת של נוישטט ומאי, ומתוך מודעות לכשלים קודמים, חשוב גם לעמוד על ההבדלים המרכזיים בין טרור בליסטי ובין איומי סייבר. להלן פירוט ההבדלים.

חוקי הפיזיקה מול חוקי הסייבר

כאמור, כאשר בוחנים את המאפיינים המשותפים לשני סוגי הנשק – טרור בליסטי ומתקפות סייבר – כדאי לזכור גם את ההבדלים ביניהם. מן העבר האחד ישנם טילים בעלי מאפיינים הנענים לחוקים פיזיקליים מוכרים וצפויים; מן העבר השני

Joseph S. Nye Jr., "Nuclear Lessons for Cyber Security", *Strategic Studies Quarterly* 18 (Winter 2011): 19-38.

Brian A. Jackson, "Organizational Learning and Terrorist Groups", RAND Working Paper (2004): 27.

20 יוסי בידץ ודימה אדמסקי, "התפתחות הגישה הישראלית להרתעה – דיון ביקורתי בהיבטיה התאורטיים והפרקטיים", **עשתונות**, גיליון 8, אוקטובר 2014.

Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft", *International Security* 38, no. 2 (2013): 7-40.

נמצאות מתקפות סייבר, שהן נשק בעל פוטנציאל לטווח אינסופי ויכולת לשהות במערכת במשך שנים מבלי להתגלות, וכן לרכוש מאפיינים בלתי צפויים וחדשים (למשל, כאשר היריב מגלה לפתע פגיעות מהותית שלא הייתה ידועה בעבר). דבר דומה ניתן לטעון לא רק על סוג הנשק אלא גם על הסביבה. ירי טילים, כמו גם שרשרת האספקה שלהם ופריסת המשגרים, מתנהלים בתוך מרחבים פיזיים ותחת תנאים מסוימים. הצדדים הלוחמים משתמשים בתנאים אלה כדי לאשר הישגים של היריב או להתכחש להם. לדוגמה, קיים קשר הגיוני בין טווח הטילים לבין אתרי השיגור. כדי לטווח מטרות רגישות, ארגוני הטרור חייבים לקרב את הנשק לעמדות חדשות. רק הגדלת טווח הטילים משנה משוואה זאת. זה היה ההיגיון מאחורי החלטה 1701 של מועצת הביטחון של האו"ם בתום מלחמת לבנון השנייה.²²

בניגוד לטרור הבליסטי, למרחב הסייבר יש יכולת לעבור עיצוב מחדש. דוגמה אחת לאפשרות כזו היא הוויכוח המתמשך בנוגע לשינוי הארכיטקטורה של האינטרנט ושאלת המשילות באינטרנט. הוויכוח על עקרון ה"קצה לקצה" ממחיש באופן מעשי את היכולת הפוטנציאלית להגדיר מחדש את שדה הקרב של הסייבר.

ממדי האתגר

טרור בליסטי הוא מאבק המוגבל על ידי טווח וריבונות. ישראל מתמודדת עם מספר אזורים וגורמים, בעיקר לבנון, רצועת עזה, חצי האי סיני, סוריה ואיראן. לאזורים ולגורמים אלה יש שורה של מאפיינים, כגון טופוגרפיה, גבולות, דרכים ונמלים, וכן התפלגות אתנו-דמוגרפית. גם האויבים, או לפחות האויב המרכזי, ידועים. לכן, במובן מסוים מדובר במערכת בעלת גבולות, היררכיות, קישורים ומתחים, אותה ניתן לחקור וללמוד לאורך זמן. פני השטח, היכולות והכוונות נלמדים על סמך עימותי עבר ואיסוף מודיעיני.

לעומת זאת, למתקפות סייבר יש טווח בלתי מוגבל. התוקפים יכולים להימצא במיקומים מרוחקים, להשתייך למספר גורמים, להיות בעלי סדרי גודל שונים, זהות ישנה או חדשה (כולל זהות היברידית במקרה של שיתופי פעולה), ומונעים מאינטרסים שונים. אלה יוצרים הבדל כבר מלכתחילה בכול הנוגע לשאלת הייחוס, כפי שנדונה לעיל. במקרה של טרור בליסטי, מספר האפשרויות צר יותר ושאלת הייחוס נבחנת ברזולוציה שונה.²³

22 ההחלטה (מ'11 באוגוסט 2006) קבעה כי לא תורשה נוכחות של כוחות חמושים (במשתמע, חזבאללה) מדרום לנהר הליטאני, למעט יוניפי"ל וצבא לבנון. הרעיון היה למנוע פריסה של טילים קצרי טווח באזור זה.

23 כאשר שוקלים את ההשתייכויות, הגדלים, הזהויות והאינטרסים השונים של ארגוני הטרור על רקע האנלוגיה הכללית של טרור, ההבדלים מוגבלים יותר.

הקשר העימות

תופעת הטרור הבליסטי נחווה בעיקר במהלך עימותים גדולים (כגון בלבנון) או בסבבים חוזרים של לחימה (כמו מול רצועת עזה ובחצי האי סיני). כחריג מכך ניתן להביא את ירי הטילים המתמשך ("טפטופים") נגד היישובים בדרום ישראל (כמו שדרות) מאז שנת 2002 ועד 2014 (ואף מעבר לכך בעצימות נמוכה יותר), כדפוס פעילות מתמשך ולא כאירוע חד-פעמי. איומי הסייבר נתפסים גם הם דרך פריזמה של משבר או אירוע מרכזי. יחד עם זאת, הם רבים יותר במספרם ובתדירותם, ומטבעם אינם בעלי דפוס של שיא ושפל. התוצאה היא שהדינמיקה של הטרור הבליסטי רגישה מאוד להקשר של העימות הספציפי, בניגוד לאיומי הסייבר. במילים אחרות, במקרה של הסייבר לא קיים "זמן שלום" לעומת "זמן מלחמה", משום שפעילות הסייבר מתקיימת באופן קבוע ובדרגות שונות של הטרדה.

הגנת "החוליה החלשה" ומתקפה "מדורגת"

מרחב הסייבר מתאפיין בכך שהוא מתקשה להגן על החוליה החלשה ביותר. גם אם ההגנה חזקה ומשוכללת במרבית הרמות, מספיקה פירצה לא מזוהה אחת כדי לאפשר את קריסת המערכת כולה. כמובן שאפשר לפתח ארכיטקטורות שנלחמות בשבריריות זו באמצעות הכנסת גורמים אנושיים או אנלוגיים לשידור, פישוטם או פירוקם.²⁴ עם זאת, אלה אינם משקפים את המגמות העכשוויות, שמאופיינות בתלות הדדית מוגברת ובשילוביות. תכונה ייחודית זו מובילה גם לטקטיקות מתקפה שונות, כגון מתקפה "מדורגת" (cascade-based), המנצלת תהליך של "למידה באמצעות חיכוך" כדי לגלות את נקודות התורפה.

בטרור בליסטי המצב שונה: מערכות ההגנה פועלות לפי פרמטרים סטטיסטיים וניהול סיכונים, בעוד שמאגר הטילים נבנה על תכנון ארוך טווח ועל הזדמנויות. עם זאת, יריבים עשויים לנסות לאתר במהלך עימותים נקודות "רכות" ביכולות ההגנה או ההתקפה של הצד השני. גילוי של נקודת תורפה ספציפית, גם אם אינה חלק בלתי נפרד מתפקוד כלל המערכת (כמו בסייבר), עלול להביא לשינויים דרמטיים במצב האסטרטגי. לדוגמה, ירי של כמה טילים מרצועת עזה לעבר שדה התעופה הבין-לאומי של ישראל במהלך מבצע "צוק איתן" גרם לרשויות בארצות הברית להוציא צו שאסר באופן זמני על נחיתות של מטוסים אמריקאיים בנמל התעופה בן-גוריון. חברות תעופה זרות הזדרזו ללכת בעקבות ארצות הברית. לעצירת הטיסות בפועל הייתה, למשך פרק זמן קצר, השפעה אסטרטגית²⁵

Richard Danzig, *Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies* (Washington DC: Center for a New American Security, 2014).

25 דבר דומה ניתן לטעון לגבי תקרית אפשרית של פגיעה המונית בגן ילדים או פגיעה באתר סמלי כלשהו, באופן שעשוי לשנות לחלוטין את הדינמיקה של העימות המזוין.

תפוצת נשק

השוואה בין תהליך תפוצת הנשק של טרור בליסטי ושל לוחמת סייבר מדגישה שתי סוגיות: הראשונה היא העברת ידע פיזי לעומת העברת ידע אלקטרוני. נשק הסייבר אינו מאופיין בחומר או במטען מסוימים, אלא בנוי מביטים (bits), בתים (bytes) ונוסחאות לוגיות. הקטלניות או היעילות של נשק זה מקושרות ישירות לתכונות אחרות שהוא נושא, בעיקר המיקוד המודיעיני (כלומר, הכרת נקודות הכניסה לרשת או למערכת), נקודות התורפה שהוא מנצל, היכולת להתגבר על מערכות אבטחה והחתמה הנמוכה. לאור זאת, אפשר לייצר כלי נשק כאלה כמעט בכול הנסיבות. לעומת זאת, טילים, למרות שגם עבורם נדרש ידע מסוים (כמו כיצד לייצר מנוע טיל מתפקד או מערכת הנחיה לטווח מסוים), עדיין מחייבים העברה פיזית של חלקים וחומרים דרך גבולות או נמלים.

הבעיה השנייה היא הדרך הייחודית של תפוצת הנשק: נשק הסייבר יכול לשמש פעם אחת בלבד והופך לחסר תועלת ברגע שהוא משאיר חתימה ומזוהה.²⁶ תפוצתו נובעת לעתים מתהליך של למידה ואימוץ שימוש אחר מאשר השימוש המקורי שלו. לדוגמה, ברגע שקוד כמו "סטקסנט" או "להבה" מופץ בעולם, הוא הופך אוטומטית לבסיס לבניית גרסאות חדשות של אותה טכנולוגיה, ותפוצת הנשק מתבצעת למעשה באמצעות תהליכי הנדסה לאחור. בניגוד לתכונות ייחודיות אלו, טרור בליסטי נשען רבות, לפחות עד לאחרונה, על הפצת טילים ורקטות באמצעות ספקים שונים, בעיקר איראן.

תפקיד המגזר הפרטי־אזרחי בתחום הסייבר

בניגוד לנשק בליסטי, נשק סייבר הוא "כפול־שימוש" (דואלי), הן מבחינת אופיו (טכנולוגיות רלוונטיות) והן מבחינת התפיסה. חברות פרטיות ומגזרים אזרחיים ממלאים תפקיד חשוב הן במתקפות סייבר והן באבטחת סייבר: הם אינם רק מטרות למתקפה, אלא גם גורמים התורמים להגנה, להערכת האיום ואף לתקיפה. בנוסף לכך, לנשק הסייבר יש השפעה כלכלית גדולה לא רק כתוצאה מההרס הפיזי (כפי שקורה במתקפות טילים), אלא גם כתוצאה של מגוון פעולות אחרות, כמו גניבה של פיתוחים טכנולוגיים.

לסיכום, טרור בליסטי חולק קווי דמיון רבים עם אתגר הסייבר, אולם במקביל ישנם גם הבדלים משמעותיים ביניהם. ניתוח קווי הדמיון והשוני מעלה תמונה מורכבת. יחד עם זאת, דומה שיש בסיס טוב להשוואה בין השניים. כנקודת מוצא, חשוב לא להתייחס להבדלים בקצב, בקנה המידה ובטווח, שכן סביר להניח שאלה לא יהיו בני השוואה גם בכול אנלוגיה אחרת. במקום זאת, מוצע להסתכל על מודל הטרור הבליסטי דרך משקפיים של דינמיקות, תהליכי למידה, התפתחות

איומים ויחסים. כאשר משקללים את כל אלה, קווי הדמיון בין הטרור הבליסטי לאתגר הסייבר מתחזקים במידה ניכרת.

הרחבת אנלוגיית הטרור

החלה של האנלוגיה הספציפית של "טרור בליסטי" על מתקפות סייבר מאפשרת לטעון שגם "טרור" באופן כללי יכול להיות אנלוגיה למתקפות סייבר. המאמר הנוכחי לא עוסק בביסוס טענה זו, אולם דומה שכאשר בוחנים את הדילמות המשותפות העומדות בפני מקבלי החלטות העוסקים הן במתקפות טרור והן במתקפות סייבר, יש בסיס לטענה זו.²⁷ המדובר, בין היתר, בדילמות הבאות:

- **בעיית ההגדרה:** אין הסכמה לגבי הגדרה אוניברסלית לתופעת הטרור, כמו גם לאיומי הסייבר.
- **אתגרים מודיעיניים:** בשני המקרים המודיעין חיוני לזיהוי, לתגמול, להפללה ולקביעת מטרות, אולם נאלץ להיאבק עם שורה של מתחים רב-ממדיים, חוצי גבולות וחוצי גופים.
- **שאלת ההרתעה:** שאלה זו מתעוררת כחלק מהתמודדות עם ארגונים חשאיים, מבוזרים, לא היררכיים ובעלי נכסים מוגבלים.
- **משקלן של טקטיקות התקפיות:** המאבק בטרור יצר מערך של טקטיקות התקפיות, המכוונות לפגוע הן ביכולת והן במוטיבציה של ארגוני הטרור. מרחב הסייבר מעלה גם הוא שאלות בנוגע לצורך, לעיתוי ולקריטריונים של מתקפות יזומות.
- **סוגיות חקיקה:** שאלות הנוגעות לקיומה של חקיקה ראשית ייחודית,²⁸ למידת האחידות וההתאמה של החקיקה הבין-לאומית,²⁹ להגדרה של מתקפה וליישום חוקים העוסקים בסיוע (תמיכה, הכשרה ומימון) לארגוני טרור קיימות גם כשדנים במתקפות סייבר.
- **הממד הציבורי והממד התקשורתי:** בשני המקרים – של טרור ושל סייבר – הכיסוי בתקשורת ההמונים מעצים את הפעולות או מנצל אותן להעברת מסרים לקהלי יעד. מצב זה מעלה שורה של דילמות בנוגע למדיניות המידע, למדיניות החינוך, לצנזור התקשורת ולסוגיות של אתיקה.

Boaz Ganor, *The Counter-Terrorism Puzzle: A Guide for Decision Makers* (New 27 Brunswick NJ: Transaction, 2007).

28 זהו עיקרון המשתקף במקרה האמריקאי, דוגמת "חוק הפטריוט". החקיקה הישראלית נגד טרור לא בנויה על מקור חקיקה ראשי שעוסק ישירות בנושא, אלא נשענת על חקיקת חירום. תקנות החירום מעניקות לממשלה גמישות וכוח רבים לפעול נגד טרור, אולם הן גם נתקלות בביקורת רבה ונתונות לוויכוח.

29 Jack Goldsmith, "Cybersecurity Treaties: A Skeptical View", in *Future Challenges in National Security and Law*, ed. Peter Berkowitz (Stanford: Hoover Institution, Stanford University, 2011).

- **הצורך החיוני בשיתוף פעולה בין-לאומי:** הארכיטקטורה הדומה של הבעיה בשני התחומים – רשת בין-לאומית שמעורבים בה נותני חסות מדינתיים, ישויות הפועלות בתוך מדינות המעניקות חסות והגנה, ארגוני "שליח" (proxy) או ארגוני חזית – יצרה את הצורך במסד של נורמות וחוקים בין-לאומיים משותפים, וכן במסגרות עבודה מבצעיות ובשיתוף מודיעיני.

תובנות מרכזיות

אימוץ האנלוגיה של טרור בליסטי מאפשר לגזור ממנה שלוש תובנות מרכזיות: הראשונה נוגעת להנחות היסוד של עתיד אבטחת הסייבר; השנייה מתייחסת למרכיבים של המאבק באיום; השלישית עוסקת ברמה הארגונית ובצורך לגבש תצורות מבצעיות גמישות חדשות, וכן גופי שיתוף פעולה בין-לאומיים. נוישטט ומאי הציגו את השאלה "האם אנלוגיה מסוימת ממשיכה להתאים גם כאשר בוחנים מצב חדש?". בחינה מחודשת של חיבורם *Thinking in Time* מאפשרת לקבוע כי אין די בכך שאנלוגיה תהיה "מתאימה", אלא שעליה גם ללמד אותנו דבר מה בנוגע להנחות היסוד ולאי-הבהירות שנלוות לתיאור הסוגיה האסטרטגית. ניתוחם של מורן וסולק³⁰ מאפשר להשתמש באנלוגיית הטרור הבליסטי כדי לחקור ולבחון חמש הנחות, או שאלות יסוד, לגבי אבטחת הסייבר. ההנחות הן: • "למדינות יש יכולת לשמור על עליונות במרחב האינטרנטי". כאשר בוחנים את אנלוגיית הטרור הבליסטי במקרה הישראלי, אין ספק שישראל שומרת על עליונות במרחב האווירי שלה לפחות מאז שנות השמונים של המאה העשרים. למרות זאת, הטרור הבליסטי, שנתפס תחילה כלא מתוחכם, הפך עד מהרה לגורם אסטרטגי היוצר איזון חלקי עם עליונות ישראלית זו, או למצער מאתגר אותה. • "מדינות לאום הן איום חמור יותר מאשר גורמים לא מדינתיים". בעולם הבליסטי, הנחה זו תלויה כמובן בסוגיית ההתחמשות (קונבנציונלית או לא קונבנציונלית). נכון להיום, מדובר בעיקר בהבחנה בין יכולות של מדינה ובין יכולות של גורם לא מדינתי. עם זאת, כשמוציאים את הנשק הלא קונבנציונלי מהתמונה, ומניחים כי הן כוח הירי והן הדיוק, הקטלניות והטווח (המכסה את כלל שטח ישראל) של אלה הנמנים על מחנה הקיצונים (איראן, סוריה, חזבאללה וחמאס) הפכו למרכיבים בני השוואה, אזי דומה שגם גורמים לא מדינתיים מחזיקים ברשותם כוח משמעותי. לכן, כמו בהנחה הראשונה, גם הנחה זו צריכה לעבור עדכון.

David Sulek and Ned Moran, "What Analogies Can Tell Us about the Future of 30
Cybersecurity", *The Virtual Battlefield: Perspectives on Cyber Warfare* no. 3 (2009):
118-131.

- "עד כמה חמור האיום?". סוגיה זו עוררה ויכוח גדול בזירה האקדמית והציבורית הדנה בסייבר. הספקנים (ויימן, ליביצקי, גרצקה, מנקו, ריד ואחרים)³¹ רואים הגזמה באיום הסייבר ומפקפקים ביכולת שלו לגרום נזק רציני וקבוע למדינות, כזה שיגרור עלויות צבאיות ונזק פוליטי. המחנה השני (קאר, קלארק, קלו ואחרים), המשקף את הלך הרוח בקרב אנשי המקצוע, גורס שהאיום שמציבות מתקפות הסייבר הוא אמיתי, מתחזק ומהיר יותר מאשר אמצעי ההגנה מפניו ותורות ההתגוננות שפותחו נגדו.³² לדעתם, מתקפות סייבר התגלו כמשמעותיות בתחום הצבאי (כגון בעימותים עם רוסיה באסטרונגיה ובגיאורגיה) והמחישו היטב את הפוטנציאל לקריסה מאסיבית של תשתיות (כמו במקרה של "סטקסנט"). לעומת זאת, במקרה של טרור בליסטי, למרות שהוא מביא לאובדן רכוש וחיי אדם ולמרות הפוטנציאל שלו לגרום אבדות גדולות הרבה יותר, אי אפשר שלא לתהות האם לא מדובר בפגיעה מוגבלת בהרבה ביחס לציפיות ולהשקעה בהתגוננות, והאם תהליך קבלת ההחלטות התבסס על הנחת "הגרוע מכול".³³ בהתאם לכך, היו שקראו לשים את הדגש במאבק בטרור הבליסטי על פתרונות התקפיים במקום על התגוננות.³⁴ עם זאת, ובמבט לאחור, מרבית השיח רואה בהחלטה של ישראל להשקיע במערכת הגנה רב-שכבתית הצלחה מוכחת. האנלוגיה הישראלית מחזקת אפוא את ההערכה שמרחב הסייבר מהווה איום ממשי ההולך וגדל.
- "האם הדור הבא של הטכנולוגיות והיישומים האינטרנטיים יהיה בטוח יותר?". שאלה זו עוסקת ברמות הפגיעות של תשתיות מתפתחות, וזאת בשונה מעולם הבליסטיקה. עם זאת, ניתן לטעון שהשילוב בין נשק וטקטיקות ובין המציאות הפוליטית-כלכלית המתפתחת עשוי להציג דור חדש לחלוטין של איומים. כדי להמחיש זאת בהקשר של הטרור הבליסטי, ניתן לציין כמה נושאים המעוררים חשש: הסכנה לאסדות הגז ליד אשקלון (השולטות בשמונים אחוזים מאספקת האנרגיה של ישראל) ולהובלה הימית בנמל אשדוד (המכסה שישים אחוזים מהייבוא למדינה) – שני אתרים הפגיעים לטילי חוף-ים, לכטמ"מים או לטילי שיוט; מסילת הרכבת לשדרות, החשופה לטילים נגד טנקים; הסכנה לפעילות האווירית האזרחית בעתיד (נמל התעופה בן-גוריון ושדה התעופה העתידי בתמנע).

31 ראו לדוגמה: Martin C. Libicki, "Cyberattacks Are a Nuisance, Not Terrorism", *Rand Blog*, February 20, 2015, <http://www.rand.org/blog/2015/02/cyberattacks-are-a- nuisance-not-terrorism.html>.

32 כהן, פרייליך, סיבוגי, "ארבעה עקרונות ועוד אחד: מודל חדש להגנת סייבר".

33 יצחק רביד, "על הנחת החמור ביותר", *מערכות* 351 (1997), עמ' 2–12.

34 Avi Kober, "Iron Dome: Has the Euphoria Been Justified?", *BESA Center Perspectives Paper* no. 199, February 25, 2013, <http://besacenter.org/perspectives-papers/iron-dome-has-the-euphoria-been-justified/>.

• "האם יש מספיק רצון פוליטי לשיתוף פעולה דיפלומטי בין-לאומי?". כאמור, היכולת לקבוע מסגרות משפטיות נורמטיביות נראית חלשה. מקרה הטרור הבליסטי ממחיש זאת דרך כישלון יישומה של החלטת מועצת הביטחון 1701. דומה שגם אימוץ מהלכים הדרגתיים וחלקיים נכשל. חלוקת האיום למקטעים שונים, כפי שנעשה במאמצים הדיפלומטיים שהושקעו בסוגיית הטילים הזעירים קרקע-אוויר (טזק"א – MANPADS), במזכר ההבנות הבילטרלי בין ישראל לארצות הברית בנושא מניעת הברחות נשק לחמאס (מינואר 2009), בהחלטה 1747 של מועצת הביטחון של האו"ם (ממארס 2007) האוסרת על יצוא והעברה של נשק מאיראן, או בהסכמי הפסקת אש, התגלתה כהישג זמני, לא מספק או בלתי ניתן לאכיפה. זאת, עקב אינטרסים ועדיפויות מנוגדים (סין ורוסיה בולמות פעילות במועצת הביטחון של האו"ם), אזורים שאין בהם שליטה ריבונית (לוב, לבנון, סיני) ומדינות סוררות. הלכה האפשרי שניתן להפיק מניסיון הטרור הבליסטי הוא שיש להשקיע הון פוליטי, בעיקר בשיתופי פעולה המתבססים על תפיסות זהות, וכן בפעולות חד-צדדיות למניעה ולהרתעה.

מאסטרטגיית "ארבעת ה-D" לאסטרטגיית "ששת ה-D"

"האסטרטגיה הלאומית למאבק בטרור", עליה הכריזה ממשלת ארצות הברית בפברואר 2003, כללה "ארבעה D" להתמודדות עם אתגר הביטחון הגדול של המילניום החדש. ארבעת היסודות היו Defeat – הבסה של ארגוני הטרור; Deny – מניעת חסות, תמיכה ומקלט מטרוריסטים; Diminish – צמצום התנאים המעודדים טרור, משמשים קרקע פורייה לרעיונות ומובילים אנשים לאמץ טרור; Defend – התגוננות מפני מתקפות טרור.

כהן, פרייליך וסיבוני מציעים ארבעה D שונים, ובוחנים את התאמתם לסוגיית איומי הסייבר.³⁵ הם משאירים את יסודות ההבסה וההתגוננות, אך מדגישים שני עקרונות אחרים: גילוי (Detection) והרתעה (Deterrence). במובן מסוים, ארבעת ה-D האלה הם חלק מהעקרונות של פרדיגמת הביטחון של ישראל. הניסיון בפועל של ישראל מול הטרור הבליסטי התאפיין בעקרונות הבאים: אִפְחוּת (mitigation) – פגיעה במשגרים ובמתקנים; מניעה – עצירת אספקת נשק; התגוננות – מערכת הגנה רב-שכבתית; הרתעה מפני ביצוע פעולות בעתיד; דיפלומטיה – הבנות והסכמות. כאשר בוחנים את שלוש אסטרטגיות המאבק – האסטרטגיה הלאומית למאבק בטרור של ארצות הברית, ארבעת ה-D של כהן, פרייליך וסיבוני, והאמצעים שנוקטת ישראל נגד טרור בליסטי – ברור למדי שיש ביניהן חפיפה וכי הן חולקות עקרונות דומים. לדוגמה, היעד של "הבסה" (defeat) בשתי המסגרות של ארבעת ה-D, מקביל ליעד "אפחות" (mitigation) באסטרטגיה של ישראל נגד הטרור הבליסטי,

35 כהן, פרייליך, סיבוני, "ארבעה עקרונות ועוד אחד: מודל חדש להגנת סייבר".

במובן זה שמדובר בגישה התקפית שמטרתה פגיעה ביכולות האויב ובמורל שלו. דבר דומה ניתן לומר על היעד "מניעה" (prevention) באסטרטגיה הישראלית נגד הטרור הבליסטי, שדומה לרעיון ה"מניעה" (Deny) בארבעת ה־D של ארצות הברית, קרי פגיעה בחימוש ובתמיכה הלוגיסטית. דוגמה נוספת היא המרכיב "גילוי" (Detection) שמציעים כהן, פרייליך וסיבוני, המגולם בתוך המרכיבים של "התגוננות", "מניעה" ו"אפחות" באסטרטגיה של ישראל, שכן שלושתם לא יבואו לידי מימוש ללא "גילוי" האיום תחילה.

כהן, פרייליך וסיבוני מדגימים היטב ובפירוט כיצד מרכיבים אלה משתקפים גם בתחום הסייבר. יתר על כן, ארבעת ה־D אותם הם מחילים על מתקפות סייבר, יכולים להיות מוחלים גם על אנלוגיית הטרור הבליסטי. לעומת זאת, אסטרטגיית המאבק בטרור הבליסטי כוללת שני מרכיבים בלבד הישימים לניתוח עולם הסייבר – "דיפלומטיה" ו"שלילה" (או "מניעה"). בדרך זו מתקבלת אסטרטגיה של "שישה D" ללחימה במתקפות סייבר (Defeat, Deny, Diminish, Defend, Diplomacy, Detection).

באשר למרכיב "דיפלומטיה", התייחסתי לעיל לקושי לבסס פתרונות משפטיים נורמטיביים במרחב הסייבר. עם זאת, ראוי לבחון אפשרויות ליצירת פתרונות נורמטיביים כלליים במרחב זה אצל מדינות החולקות תפיסות דומות, ובהמשך הזמן לעודד מדינות אחרות לאמץ נורמות אלו (בדומה למודל "קבוצת ספקיות הגרעין" שגובש לצורך בקרת ייצוא). שיתוף פעולה רב־צדדי בין מדינות החולקות תפיסות דומות נראה ככלי פעולה סביר ואף חיוני במציאות המשפטית המורכבת של ימינו. שיתוף פעולה כזה יכלול לא רק שיתוף בתחום המבצעי (כגון אכיפה) והמודיעיני (שיתוף מידע), אלא גם מחקר ופיתוח טכנולוגיים משותפים, וכך ישפר את יכולות הגילוי והניטור. שיתוף הפעולה הישראלי-אמריקאי בפיתוח מערכות הגנה אווירית, והצעת פתרונות אלה לשותפים נוספים, יכולים גם הם לשמש כמודל לתחום הסייבר.

באשר ל"שלילה" (המקבילה ל"מניעה"), ניתן להניח שהמרכיבים של סיוע, תמיכה ומימון היריב חלשים יותר בעולם של איומי הסייבר יחסית לזירת הטרור הבליסטי, וכי לאור זאת הם פחות פגיעים. במילים אחרות, כאשר שרשרת האספקה קצרה וצרה יותר והמערכת הסביבתית כולה פחות גלויה לעין, היריב פחות חשוף להתערבות. עם זאת, מרכיבים אחרים המצויים בידי היריב, כגון ידע, מודיעין ויכולת הסוואה, הם בעלי משמעות וניתנים לגילוי וחשיפה. דוגמה לכך בתחום הטרור הבליסטי היא תפיסתם או סיכולם של משלוחי נשק מאיראן לארגוני טרור פלסטיניים בשנים 2001, 2009 ו־2014.

סוגיה מרכזית הנמצאת על הפרק, בנוסף להכרת האסטרטגיות השונות, היא סדר העדיפויות של כל אחת מאסטרטגיות אלו. בדוגמה של הטרור הבליסטי,

ברור כי האמצעי הבולט ביותר הוא השילוב של "מניעה" ו"הגנה". פגיעה ישירה במאגרי המשגרים והטילים, השפעה באמצעות הדרך הדיפלומטית ויצירת הרתעה לא השיגו את אותן תוצאות כמו צעדי המניעה שהובילו לתפיסה ולסיכול העברות נשק בקנה מידה גדול (כמובן, לצד אמצעי ההגנה של "כיפת ברזל").

אם לשפוט את הדברים על פי כהן, פרייליך וסיבוני, נראה כי לא כך המצב בתחום הסייבר, שבו לכול האסטרטגיות שנוסו יש מגבלות משמעותיות, ודומה שאין אסטרטגיה אחת דומיננטית. אמנם, האסטרטגיות של "הגנה" ו"גילוי" מפותחות יותר מאחרות, וישראל אף מדגישה את יכולותיה בתחומים אלה,³⁶ אך המספר הגדול של מתקפות סייבר (יותר ממיליון במבצע "עופרת יצוקה" בלבד) יוצר אתגר גדול.³⁷ במילים אחרות, בניגוד לניסיון שהצטבר בלחימה בטרור הבליסטי, המסקנה המרכזית שעולה מעולם הסייבר היא שנדרשת אסטרטגיה היברידית במקום אסטרטגיה מובילה אחת.

ההיבט הארגוני

השאלה כיצד לארגן פעולת נגד בסייבר מתבססת בהכרח על המורכבות והדינמיקה של האיום. הניסיון שהצטבר ממבצעי המאבק בטרור מצביע על החשיבות שיש להקמתם ולשילובם של הגופים הנכונים במאמץ הלאומי.³⁸ בהקשר זה, יש לטפל תחילה בהקמתו של ארגון אסטרטגי חדש ברמה הלאומית, שיתמודד עם האתגר. כאשר בוחנים את אנלוגיית הטרור, נראה כי חקר מקרים קודמים, כגון הלמידה הארגונית בעידן שלאחר 11 בספטמבר 2001 והקמת "המרכז הלאומי למאבק בטרור" (NCTC), לצד פרקטיקות צבאיות שנעשה בהן שימוש במרחב הסייבר, עשויים לסייע בהקמת ארגונים לאומיים חדשים לצורך מאבק זה. עיקרון דומה שהביא להקמתו של ארגון חדש להתמודדות עם בעיית הסייבר ניתן למצוא, לדוגמה, ב־2009, כאשר הצבא האמריקאי הקים פיקוד משנה לסייבר.³⁹ גם צה"ל החל לאחרונה לבחון מהלך דומה.⁴⁰ בפברואר 2015 החליטה ממשלת ישראל לפעול

Yonah Jeremy Bob, "Rule of Law: Obama, Israel and Cyber Warfare", *Jerusalem Post*, March 22, 2013, <http://www.jpost.com/Features/Front-Lines/The-cyber-party-over-307367>.

David Shamah, "Hackers Threaten 'Israhell' Cyber-Attack over Gaza", *Times of Israel*, July 9, 2014, <http://www.timesofisrael.com/hackers-threaten-israhell-cyber-attack-over-gaza>.

Bruce Hoffman and Jennifer Taw, *A Strategic Framework for Countering Terrorism and Insurgency* (Santa Monica: RAND Corporation, 1992).

היו כאלה, לרבות אדמירל (מיל') ג'יימס סטברדיס (המפקד העליון של נאט"ו לשעבר), שקראו להקמת זרוע סייבר חדשה בכוחות הביטחון.

"Election Results and the Defense Establishment", *Israel Defense*, March 19, 2015, <http://www.israeldefense.co.il/en/content/election-results-and-defense-establishment>.

להאחדת כוחות ואמצעים על ידי הקמת רשות סייבר לאומית. גוף זה אמור לקבל לידיו אחריות מבצעית ולהצטרף למטה הסייבר הלאומי שכבר קיים.

מבט מקרוב על הרמה הארגונית מצביע על כמה סוגיות: בזירת הטרור, לא ברור אם "המרכז הלאומי למאבק בטרור" מבצע את המצופה ממנו, וגם הקשרים בינו לבין שאר גופי המודיעין הלאומיים בארצות הברית, כגון ה-CIA, אינם ברורים דיים.⁴¹ גם בזירת הסייבר יש חוסר בהירות בכול מה שנוגע לפעילות מול קהילת המודיעין, אף מעבר לחוסר הבהירות הקיים בזירת הטרור. המודיעין אינו רק גורם מסייע למתקפה אלא, כפי שמוכיח הטרור הבליסטי, משולב בצד ההתקפי ובצד ההגנתי גם יחד, בשל העובדה שהגבולות בין איסוף מודיעין (ניצול הסייבר) ובין המבצעים הינם כיום מעורפלים.⁴²

הניסיון הישראלי מחדד את הדילמה, משום שמערכת הביטחון של ישראל קטנה יותר בממדיה מזו של ארצות הברית ונשלטת על ידי שלושה גופים חזקים. גופים אלה לא רק נהנים מעוצמה פוליטית,⁴³ אלא גם יצרו אפשרות ליחסי עבודה סימביוטיים בעת הצורך ולחלוקת עבודה הכוללת רוטציה בפקוד בהתאם להקשר.⁴⁴ כאשר מסתכלים על זירת הטרור הבליסטי, ניתן להיווכח בלקח שהפיק צה"ל, המוצא את ביטויו בקבלת אחריות מלאה על המאבק בזירה זו.⁴⁵ אין זה מפתיע שמתחים סביב שאלת הסמכויות בתחום הסייבר צצים ועולים כבר כיום.⁴⁶

Richard A. Best, *The National Counterterrorism Center (NCTC) Responsibilities and Potential Congressional Concerns* (Washington DC, Congressional Research Service, 2011).

42 דוגמה לכך ניתן לראות בארצות הברית, שם קהילות המודיעין והמבצעים תלויות מאוד האחת בשנייה, עובדה המומחשת, בין השאר, בכך שפיקוד הסייבר וה-NSA חולקים אותו מפקד. הסיבה לסימביוזה זו נובעת מהבעיה להגדיר גבולות ברורים בין המבצעים, איסוף המידע המודיעיני והמידע הסיכולי, ובין יוזמות ותגובות התקפיות, הגנתיות ושל הגנה פעילה.

43 שניים מהם כפופים ישירות לראש הממשלה, וכך מצמצמים את הסמכות של כל גוף מקביל אחר.

44 ישראל אכן הקימה גוף מתמחה לתיאום בתחום הטרור – "המטה ללוחמה בטרור", שהוקם ב-1996, בזמן גל פיגועי ההתאבדות. אולם גוף זה אינו כולל יכולות מודיעין, מבצעים ותכנון בפועל, שנותרו בלעדית בידי זרועות הביטחון הקיימות, ובראשן שירות הביטחון הכללי (שב"כ). למידע נוסף על המבנה והמשמעות של קהילת המודיעין בישראל ראו: שמואל אבן ועמוס גרניט, **קהילת המודיעין הישראלית – לאן?** (תל אביב: המכון למחקרי ביטחון לאומי, 2009); Yosef Kuperwasser, *Lessons from Israel's Intelligence Reforms*, Analysis Paper, no. 14 (Washington DC: Brookings Institute, 2007).

45 צה"ל פיתח זרוע משולבת חזקה מול הרשויות האזרחיות בדמות פיקוד העורף, לתיאום סוגיות של הגנה אזרחית. ניסיון להפעיל גוף מקביל במסגרת משרד ממשלתי חדש, "המשרד להגנת העורף", כשל עקב מאבקים פוליטיים פנימיים בממשלה.

46 לדוגמה, מאבק שהתעורר בין השב"כ ובין מטה הסייבר הלאומי סביב שאלת האחריות להגנה על רשתות ציבוריות ואזרחיות קריטיות.

השאלה שעומדת על הפרק בסופו של דבר היא מדוע לא להפוך את ארגוני המודיעין הקיימים לכאלה שיוכלו להתמודד עם אתגר הסייבר, במקום להקים ארגונים חדשים.⁴⁷ אחת הדרכים לעשות זאת היא באמצעות התארגנות חדשה ברמה המבצעית. במילים אחרות, הדגש צריך להיות מושם לא על הסוגיה של אחדות הפיקוד, אלא על פלטפורמות שמאפשרות פעילות גמישה. בהמשך לקו מחשבה זה, ההגדרה של "כוחות מיוחדים" בהקשר של איומי טרור יכולה להיות מיושמת גם בעולם הסייבר. אחת האפשרויות יכולה להתבסס על אנלוגיית הטרור הבליסטי, שהביאה את צה"ל להקים "מרכזי אש" משולבים.⁴⁸ מבנה ארגוני זה פותח כדי לרכז את כל הכלים הדרושים לגילוי משגרי הטילים, והוא משלב יכולות שונות שנועדו להשיג גמישות וזריזות ברמה הטקטית.⁴⁹

פלטפורמות משותפות כאלו אינן צריכות להיות מוגבלות לרמה המקומית בלבד, אלא ניתן להרחיבן לרמה הבין-לאומית. בדומה למאבק בטרור, גם אסטרטגיה לשיתוף פעולה בין-לאומי בסייבר אינה נעדרת בעיות הקשורות לאינטרסים, חוקים ושיקולים פוליטיים. עם זאת, ממשלת ישראל מכירה בחשיבות פיתוחו של תחום זה. כך, למשל, ישראל ושותפים בין-לאומיים השקיעו מאמצים במחקר ובפיתוח,⁵⁰ והתחזק שיתוף הפעולה הבין-לאומי בין גופי CERT באמצעות שימוש בכלים מיוחדים לשיתוף מידע, ללמידה משותפת ולמבצעים.⁵¹ עם זאת, יש עדיין מקום לשפר ולהרחיב משמעותית מגמה זאת.

גורמים בכירים לשעבר במערכת הביטחון של ישראל רמזו כי שיתוף הפעולה בין ישראל לארצות הברית בתחום הסייבר אינו מיטבי, וכי יש צורך ליצור "מנגנון משותף לשילוב יכולות טכנולוגיות ומודיעיניות". אותם גורמים ציינו כי "שותפות מבצעית בין ישראל לארצות הברית קיימת כבר עשרות שנים, אבל יש רמות שונות

47 אביאם סלע, "הקמת רשות הסייבר הלאומית – טעות", *Israel Defense*, 17 בפברואר 2015, <http://www.israeldefense.co.il/he/content/>, 2015.

48 "Employing any OrBat on the Ground or in the Air", *Israel Defense*, June 2, 2015, <http://www.israeldefense.co.il/en/content/employing-any-orbat-ground-or-air>.

49 זאת, בשונה מ"צוות החירום לאירועי מחשב" (CERT), המתמקד בענפי התשתית המרכזיים ומגיב למתקפות מחשבים ברמה הלאומית. פורמט קרוב יותר לרעיון של "כוחות מיוחדים" הם "צוותי ההתערבות" שהקים אגף התקשוב/C4I של צה"ל. ראו: "Ready for any Scenario: Military or Civil", *Israel Defense*, February 24, 2014, <http://www.israeldefense.co.il/en/content/ready-any-scenario-military-or-civil>.

50 "Israel's New National Cyber Operations Center", *Israel Defense*, November 13, 2014, <http://www.israeldefense.co.il/en/content/israel%E2%80%99s-new-national-cyber-operations-center>.

51 "IAI: Cyber R&D Center in Singapore", *Israel Defense*, February 13, 2014, <http://www.israeldefense.co.il/en/content/iai-cyber-rd-center-singapore>.

של שיתוף פעולה בתחומים השונים", וכי "המודל הטוב ביותר הוא שיתוף הפעולה בתחום הגנת הטילים, שהוליד את פיתוח ה'חץ', 'כיפת ברזל' ו'שרביט קסמים'".⁵² אחד המודלים האפשריים לפעול על פיו הוא שיתוף הפעולה הבין-לאומי בתחום הפיננסים המתקיים כחלק מהמאבק בהלבנת הון ובמימון הטרור. זאת, באמצעות רשת של ארגונים בין-לאומיים, דוגמת ארגון Financial Action Task Force (FATF)⁵³ ברמה הגלובלית, וארגון Financial Crimes Enforcement Network (FinCEN) ברמה הלאומית.⁵⁴ אנלוגיה זו היא נושא ראוי למחקר עתידי. עקב המאפיינים המיוחדים של בעיית ביטחון הסייבר, לא יהיה זה מרחיק לכת לקבוע כי שתי ההמלצות האחרונות של פיתוח שיתופי פעולה בין-לאומיים וטקטיים עשויות בשלב מסוים להתכנס יחדיו: המורכבות, קנה המידה והשונות של האתגרים עשויים להביא לכך ששיתוף הפעולה העתידי יתפתח ויהפוך מתחום שעניינו חילופי מידע בלבד לפעולות משולבות ומשותפות, ואולי אף יכלול הקמת "כוחות משימה משותפים" או חילופי נציגים בפקודים מבצעיים וביחידות, שיפעלו כקציני שיתוף פעולה.

סיכום

אנלוגיות הן כלי עזר חיוני להתמודדות עם אתגרים חדשים. האיומים במרחב הסייבר הם עצומי ממדים, אינטנסיביים מבחינה טכנולוגית ומתפתחים במהירות, ומטבעם הם זקוקים לאנלוגיות ומטאפורות. הטרור הינו תופעה הדומה לאיומי הסייבר מבחינת קנה המידה, הצורה וההשפעה ההרסנית שלו על שגרת החיים, והוא גם זירה שבה מדינות שונות צברו ניסיון רב ומומחיות. מאמר זה ביקש לערוך השוואה בין איום הסייבר ובין איום הטרור, באופן פחות אינטואיטיבי ויותר אנליטי. בהתאם לכך חודדה רזולוציית ההשוואה מ"טרור" בכלל ל"טרור בליסטי", והוגבלה להקשר הישראלי. המסקנה שהתקבלה היא שניתן ללמוד רבות מהאנלוגיה, וזאת מבלי להתעלם מהבעיות שבה, כגון שאלות של מהירות, היקף וחוסר האפשרות לחזות את האירועים.

52 רן דוגני, "ידלין: בלוחמת סייבר, מדינה צריכה לתקוף, לא רק להתגונן", **גלובס**, 29 באפריל 2015, <http://www.globes.co.il/news/article.aspx?did=1001031543>.

53 FATF הוא ארגון בין-ממשלתי שהוקם בשנת 1989 ביזמת מדינות ה-G7 כדי לגבש מדיניות למאבק בהלבנת הון. בשנת 2001 התרחב ייעודו גם לתחום המאבק במימון הטרור. הארגון מנטר את התקדמותן של מדינות ביישום המלצותיו באמצעות שימוש בסקירות של עמיתים (הערכות הדדיות) בין המדינות החברות. מזכירות FATF שוכנת במטה ארגון ה-OECD בפריז. לפרטים נוספים ראו: www.fatf-gafi.org/.

54 FinCEN הוא גוף השייך למשרד האוצר האמריקאי, ותפקידו הוא לאסוף ולנתח מידע בנוגע לעסקאות פיננסיות, במטרה להיאבק בהלבנת הון מקומית ובין-לאומית, במימון טרור ובפשעים פיננסיים אחרים. למידע נוסף ראו: www.fincen.gov/.

המאמר ניתח שלוש הצעות מרכזיות: הראשונה – בחינה מחדש של הנחות יסוד הנוגעות לעתיד אבטחת הסייבר; השנייה – האפשרות לאמץ את מסגרת "ששת ה־D" מהמאבק בטרור לעולם הסייבר; השלישית, ברמה הארגונית – הצורך בתצורות מבצעיות גמישות חדשות ובגופי שיתוף פעולה בין־לאומיים (ובעתיד שילוב בין השניים).

המסגרת המוצעת במאמר משאירה מקום למחקר נוסף של הסוגיות, כאשר החשובות שבהן אמורות להתייחס לעצם יישום ההצעות שלעיל. לדוגמה, כיצד ניתן לתרגם רעיונות כמו "מניעה" לטקטיקות של לחימה באיום הסייבר, או האם גוף ביטחוני יטפל במאמצים הלאומיים לאבטחת הסייבר טוב יותר מאשר גוף אזרחי? התייחסות מרכזית נוספת אמורה להתמקד בשאלות: כיצד להרכיב יחידות וכוחות חדשים, מה יהיו המרכיבים של יחידות אלו וכיצד יוקצו תחומי האחריות והמשאבים ביניהם? שאלות אלו ממחישות את הנקודה המרכזית של המאמר, והיא שהאנלוגיה בין איומי הסייבר ובין איומי הטרור צריכה לשמש לא רק לקביעת מדיניות מסוימת, אלא גם כדי לפתוח את הדלת לשיח עשיר ורלוונטי שישפיע על תפיסות ויעלה רעיונות חדשים לפעולה.

לבסוף, השאלה שהוצגה על ידי הקצין הישראלי הבכיר שצוטט בפתח המאמר עדיין נותרת בעינה. במבט לאחור, קל לראות כיצד התפתח האיום הבליסטי, על שיטותיו, מרכיביו והדינמיקה שלו. החשיבה המבצעית סביב איום הסייבר נמצאת רק בראשיתה, במיוחד בכול מה שנוגע לאיום מצד גורמים לא מדינתיים. לכן, קשה לדמיין את אופיו המדויק של איום זה, והשאלות לגבי הצורות שילבש וכיצד למנוע את התפתחותו הן סוגיות מפתח להמשך עיסוק בעתיד.

סייבר, מודיעין וביטחון

קול קורא להגשת מאמרים לכתב העת

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

ייבחנו מאמרים הנוגעים לתחומים הבאים:

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

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

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

להגשת מאמרים ולפרטים נוספים ניתן לפנות לח"מ.

בברכה

הדס קליין, מתאמת כתב העת: **סייבר, מודיעין וביטחון**

hadask@inss.org.il



המכון למחקרי ביטחון לאומי – תוכנית ביטחון וסייבר

רח' חיים לבנון 40, ת"ד 39950, רמת אביב, תל אביב 61398 | טל': 03-6400400 | פקס: 03-7447588