צבא ואסטרטגיה

כרך 4 | גיליון 3 | דצמבר 2012

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

צבא ואסטרטגיה

כרך 4 | גיליון 3 | דצמבר 2012

צבא ואסטרטגיה

כתב העת **צבא ואסטרטגיה** מיועד להעשיר, להפרות ולהעמיק את השיח הציבורי באשר למרכיב הצבאי של הביטחון הלאומי בישראל.

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

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

כתובת
המכון למחקרי ביטחון לאומי
רח' חיים לבנון 40, ת"ד 39950, תל־אביב 61398
טל' 03-6400400, פקס' 03-7447590
דוא"ל: info@inss.org.il

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

ISSN 1565-8880

תוכנית להרתעת סייבר: בניית יציבות באמצעות כוח

פרנק ג'. צ'ילופו, שרון ל. קרדאש וג'ורג' ס. סלמואירגי

במובנים רבים, אין ספק שהרתעה בעולם הסייבר היא נושא מורכב הרבה יותר מאשר ההרתעה במלחמה הקרה. טבעו של מרחב הסייבר הוא הגורם לכך. גם התיאוריות המתוחכמות ביותר של ההרתעה הגרעינית יתגלו כבלתי־מספקות בהתמודדות עם מורכבותו של תחום זה, שהוא מעשה ידי אדם, ואשר מקיף מספר אינסופי כמעט של יכולות, גורמים ומניעים המשתנים בהתמדה.[1]

איומי סייבר מציבים בעיה אמיתית וגוברת, ועד היום, מאמציה של ארצות־הברית לתת להם מענה הולם משתרכים מאחור. אמנם, היכולת להתגונן מפני התקפה או פלישה חייבת להישמר, אך ארצות־הברית, ככל מדינה אחרת, תפיק תועלת רבה אם תצליח מלכתחילה להרתיע את אויביה מפעולה – לפחות ככל שהדבר נוגע לפעולות מהסוג החמור ביותר, דוגמת לוחמת סייבר. ברור לחלוטין שלא ניתן להרתיע את כל סוגי ההתנהגות העוינת, אך חשוב לזהות סדרי עדיפויות בנושא זה, ולקבוע מהי הדרך הטובה ביותר להתמודד עם האיומים המובילים. חרף דיונים נמרצים, גיבוש פתרון מקיף ואחיד נותר חמקני. אחת הסיבות לכך הוא טיבה המורכב והמקיף של הרתעת סייבר, המחייב פתרון מקיף ומגובש הכולל בעלי עניין במגזר הציבורי והפרטי גם יחד.

על מנת לסייע בהבניית הדיון ובקידום המטרה, אנו מציעים מסגרת עבודה שבוחנת את הסוגיה בצורה ביקורתית, ומבקשת להניא, להרתיע ולהכניע גורמים עוינים מדינתיים ולא־מדינתיים גם יחד. הצבת האיומים הפוטנציאליים בתבנית רעיונית זו מסייעת להבהיר מהם מקורות הסכנה, ומשמשת נקודת פתיחה לזיהוי האחראים ולשיוכם לפעולות עוינות שמתבצעות נגד מדינה כלשהי או נגד בעלות־בריתה. הדבר יאפשר לשחקנים הרלוונטיים, שהפכו מטרה לגורמים עוינים, להמשיך

פרנק ג'. צ'ילופו הוא ראש המכון למדיניות להגנת המולדת (HSPI) ומנהל משותף של מרכז הסייבר לביטחון לאומי וכלכלי (CCNES) באוניברסיטת ג'ורג' וושינגטון. שרון ל. קרדאש היא מנהלת משותפת של ה־HSPI וחברה ב־CCNES, ג'ורג' ס. סלמואירגי הוא עורך דין ויועץ ל־HSPI בוושינגטון.

בפעולות ובדיונים הנחוצים על מנת להתוות ולהוציא לפועל אמצעי תגובה יעילים וראויים. יתרון נוסף של תבנית זו הוא סיוע בזיהוי תחומים ששיתוף פעולה בין הישויות המושפעות/המהוות יעד לפגיעה עשוי להועיל להם, או אפילו נדרש עבורם. לסיכום, מסגרת עבודה זו מספקת נקודת פתיחה לחקר הדרכים להרתעת גורמים עוינים, ובאופן זה מציעה נקודת מבט רעיונית בעלת ערך לארצות־הברית ולבעלות־בריתה גם יחד. פירוט מגוון הגורמים ופעילותם הפוטנציאלית שיובאו להלן אינו מתיימר להיות ממצה. נכון יותר יהיה לראות בו תמונת מצב או מעין טיוטה, שנועדה לתת מושג כללי במונחים של מי, מה, כיצד, מדוע וכדומה, וזאת כהקדמה לדיון מעמיק יותר על האסטרטגיה והמדיניות בתחום הרתעת סייבר.

גורמים מדינתיים

צבאות זרים עשויים להיות מעורבים ב"מתקפה על רשתות מחשב" או ב"ניצול רשתות מחשב" (CNA/CNE) כדי להגביל, לפגוע או להרוס יכולות של מדינה אחרת על מנת לקדם סדר־יום פוליטי. צבאות זרים משלבים יותר ויותר יכולות CNA/CNE במאמץ המלחמתי, בתכנון הצבאי ובדוקטרינה שלהם.[2] למאמצים כאלה יש יישומים קונבנציונליים בשדה הקרב (כלומר, שיפור במערכות נשק ופלטפורמות ו/או שיבוש מערכות אלה אצל אחרים) לצד יישומים בלתי־קונבנציונליים, ככל שמרחב הסייבר מותח את שדה הקרב וכולל בתוכו רכיבים חברתיים ואזרחיים. הפעילות במרחב הסייבר עשויה לכלול הכנות מודיעיניות של שדה הקרב, במטרה למפות תשתיות חיוניות של מי שנתפס כאויב.[3]

שירותי ביון ושירותי ביטחון: ניצול לרעה (Exploit) עשוי לכלול ריגול תעשייתי, כלכלי, צבאי ופוליטי, גניבת מידע מממשלה אחרת או על אודותיה, וכן גניבת קניין רוחני, טכנולוגיה, סודות מסחריים ועוד, שנמצאים בידי תאגידים פרטיים או אוניברסיטאות. שירותי ביון של מדינות רבות מעורבים בריגול תעשייתי בתמיכת חברות פרטיות.[4] מטרת־העל של פעילויות המתבצעות במסגרת זו היא השאיפה להשפיע על החלטות ועל מאזן הכוחות (האזורי והבינלאומי). כאן בולט שילוב של מודיעין טכני ואנושי, וכן איום מצד גורמים מבית ("insider").[5]

היבטים משולבים: ניתן לשלב רכיבים שונים ביכולתה של מדינה על מנת להשיג שלם הגדול מסכום חלקיו. בריתות (בין מדינות) יכולות להתגבש למטרה דומה. פעילות משותפת בהקשר זה עשויה לכלול איסוף מידע, שיתוף ממצאים שהשיג אחד הצדדים וביצוע משותף של מבצעים בשטח (מתקפות). מדינות יכולות גם לחפש ולגייס עזרה של גורמים לא־מדינתיים, כגון פצחנים (האקרים) להשכרה, שאינם חשים מחויבים או מוגבלים לנאמנות כלשהי.

גורמים לא־מדינתיים

ארגוני טרור לא־מדינתיים עלולים לבצע פעולות CNA/CNE כדי לקדם סדר־יום פוליטי מסוים. הם מייחסים חשיבות מרובה לאינטרנט (לצורכי גיוס, הדרכה, גיוס כספים, תכנון מבצעים וכדומה).[6] הצלחת מאמציהן של ארצות־הברית ובעלות־בריתה במלחמה בטרור בעולם הממשי עלולה להוביל ארגונים כמו אל־קאעדה ודומיו לחדור לעולם הסייבר באופן מעמיק יותר. אל־קאעדה אף עשוי לנסות להפיק לקחים מתוך פעילותם של ארגון "אנונימוס" ו"האקטיביסטים" (האקרים־אקטיביסטים) אחרים (או אפילו לחקות אותם), שעושים שימוש במרחב הסייבר על מנת למשוך תשומת לב למטרה שבה הם תומכים.

ארגוני פשע לא־מדינתיים מבצעים גניבת קניין רוחני, גניבת זהות וכן הונאות שונות, ומוּנָעים לרוב מתאוות בצע. הטכניקות והכלים הייחודיים לסייבר יכולים להניב תגמולים כספיים נכבדים. שוק עבריינות הסייבר העולמי הוערך ביותר מ־12.5 מיליארד דולר ב־2011,[7] אף על פי שהאומדנים משתנים (תוקף מתודולוגיות החישוב והאמינות של חלק מהמקורות נתון לוויכוח, וקשה להשיג הוכחה אמפירית).

היבטים משולבים: ניתן לצפות לבריתות מטעמי נוחות בין גורמים לא־מדינתיים (ארגוני טרור וארגוני פשע, ואפילו בין יחידים), במטרה לגשר על פערי יכולת כדי להשיג השפעה גדולה יותר. הסדרים דומים של נוחות הדדית אפשריים גם בין מדינה לבין ישויות שאינן מדינה (טרוריסטים, פושעים, האקרים יחידים). גורמים לא־מדינתיים יכולים להרחיב את היכולות והמיומנויות של המדינה, או לפעול כשלוחה שלה למטרות שונות. הסדרים כאלה הופכים את אתגר ייחוס האחריות (מי אחראי) למורכב עוד יותר, ומאפשרים למדינה ליהנות מיכולת הכחשה אמינה (plausible deniability).

השוואה בין הרתעת הסייבר להרתעה בתחום הגרעין[8] מעלה נקודות דמיון ושוני גם יחד.[9] מרחב הסייבר תובע במיוחד התמקדות בשחקנים ולא רק ביכולות/בנשק. לכן חיוני לסווג שחקנים אלה בהתאם להיקף, לעוצמה ולאופי האיום שהם נושאים. רק לאחר בחינה מדוקדקת שלהם נוכל לזהות את החשובים ביותר, ולהתמקד בהם באופן שמתעמת ומנטרל את הכוונות והיכולות הספציפיות שלהם.

הגנה והתקפה הן שני מרכיבים מכריעים בעמדה ובאסטרטגיה הרב־שכבתית האיתנה של ארצות־הברית, שנועדה להבטיח ביטחון לאומי. הרתעה יכולה לספק שכבת הגנה נוספת, באמצעות מניעת מהלכי פתיחה מצד בעלי אינטרסים עוינים כלפי ארצות־הברית. לכן, כדי לשמר ואף לקדם את הביטחון הלאומי/ביטחון המולדת, חשוב לשקול היטב, לפתח ולשמר לאורך זמן בתוך מערכת (טכנולוגית והגנתית/ביטחונית) מהירת צמיחה את היכולות האמריקאיות הנחוצות לתמיכה במדינה באופן אמין ויעיל, שיקנו לה מוכנות ויכולת להניא, להרתיע ולהכניע את

יריבה. אולם למרות מאמצים מרוכזים המכוונים למטרות אלה ולמערכות הגנה, אין לראות בגישה זו תחליף לבנייה ולאחזקת אמצעי שיקום משמעותיים נוספים, שמטרתם לאפשר התאוששות מהירה. אכן, יכולת התאוששות ושיקום כשלעצמה עשויה להיות הרתעה רבת־עוצמה. ברוח חוכמתו של סון צו (Sun Tzu), עצם היכולת להשתקם לאחר מכה, לצד מוכנות ברורה להגיב למתקפת סייבר, יפעלו לחיזוק מאמצי ההרתעה האמריקאית, ולכן ימנעו קרבות ושפיכות־דמים: "זכייה במאה ניצחונות במאה קרבות אינה שיא המיומנות. הכנעת האויב ללא קרב היא המיומנות בשיאה".[10]

קווי מתאר לאיום הסייבר

ארצות־הברית והאינטרסים שלה מצויים תחת איום סייבר יומיומי מגורמים מדינתיים ולא־מדינתיים גם יחד. המטרות האמריקאיות הפוטנציאליות רבות ומגוונות, ומתרחבות למגזרים חיוניים כמו מים, אנרגיה, כספים וטלקומוניקציה.[11] על פי דיווחי העיתונות המצטטים דובר של המִנהל הלאומי לביטחון גרעיני בארצות־הברית (NNSA) – "הארגון לביטחון גרעיני [של ארצות־הברית] חווה עד עשרה מיליון 'אירועי...ביטחון משמעותיים' בכל יום".[12] על פי חישובים של המשרד לביטחון המולדת של ארצות־הברית, מתגלות עשרות אלפי חדירות סייבר (ניסיונות ובפועל) בכל שנה, ועשרות מתקפות על מערכות תשתית חיוניות – כאשר מאז 2010 ועד 2012 חלה בהן עלייה בסדרי גודל.[13] טווח נושאי תפקידים בכירים בעבר ובהווה שהתריעו על כך הוא מרשים, וכולל את עוזר הנשיא לענייני ביטחון המולדת ומלחמה בטרור, ג'ון א. ברנן (John O. Brennan);[14] מנהל הסוכנות לביטחון לאומי וראש מטה הסייבר האמריקאי, גנרל קית' אלכסנדר (Keith Alexander); השר לשעבר לביטחון המולדת, מייקל צ'רטוף (Michael Chertoff); המתאם הלאומי לשעבר לענייני ביטחון ומלחמה בטרור ויועץ מיוחד לנשיא בנושא אבטחת סייבר, ריצ'רד קלארק (Richard Clarke); יו"ר ועדת הסנאט לביטחון המולדת, הסנטור ג'וזף ליברמן (Joseph Lieberman);[15] הנציג הבכיר בוועדת הסנאט לשירותים מזוינים, הסנטור ג'ון מקיין (John McCain), וראש ה־FBI רוברט מולר (Robert Mueller), שלאחרונה אף צפה שאיום הסייבר יחליף בעתיד את הטרור כאיום הראשי על המדינה.[16]

אחד הפרשנים תיאר זאת בבהירות רבה, כשאמר "מרגלים זרים ופשע מאורגן נמצאים כמעט בתוך כל רשת של חברה אמריקאית. בקרב היועצים הבכירים ביותר של הממשל בנושא אבטחת סייבר שוררת הסכמה רחבה, כי עברייני סייבר או טרוריסטים הפועלים בתחום הסייבר מסוגלים להשבית את התשתית החיונית במדינה בתחום הפיננסי ובתחום האנרגיה והתקשורת".[17] יחד עם זאת, נוסף לספיגת הפסדים כספיים שמוערכים על ידי הרשות הלאומית לריגול נגדי ופקידים

אמריקאיים נוספים במיליארדים, כתוצאה מניצול רשתות מחשב לגניבת קניין רוחני רב־ערך דרך פרצת אבטחה,[18] המדינה ניצבת נוכח מכה מאיימת יותר, עקב היותה מטרה למאמצי היריב לעסוק במה שמהווה המקבילה הסייברית להשגת מודיעין של שדה הקרב, דוגמת ניסיון מצד סין למפות תשתיות אמריקאיות חיוניות לאספקת מים ואנרגיה – שאותו הם עלולים למנף בהמשך כדי להניא, להתריע ולהכניע פעולה מצד ארצות־הברית.[19]

תעשיות חיוניות במדינות אחרות כבר חוו מתקפות סייבר. החברה הסעודית 'ארמקו' (Aramco) (חברה בבעלות המדינה ו"מפיקת הנפט הגדולה בעולם") סבלה מווירוס ממקור חיצוני שהדביק כ־30,000 מהמחשבים שלה באוגוסט 2012.[20] זמן קצר לאחר מכן, חברת RasGas מקטר ("המפיקה השנייה בגודלה בעולם של גז טבעי נוזלי") נפגעה אף היא.[21] דיווחי העיתונות מציינים כי "החברה הצרפתית Areva לתחנות כוח גרעיניות הייתה היעד למתקפת הסייבר בספטמבר [2011]".[22] והמגמה נמשכת.

מדינות מחזיקות ביכולות משתנות ברמה ובתחכום, ועשרות מהן מרחיבות את יכולת הסייבר שלהן, לרבות ארצות־הברית ובעלות־בריתה (ישראל היא שחקנית ראשית במרחב זה). אל מול ארצות־הברית, סין היא מקור מרכזי של "איום מתמיד ומתקדם", למרות שטביעות אצבע של המדינה הנותנת חסות אינן ניכרות תמיד על העכבר או על מסך המחשב. ייחוס האחריות קשה אף יותר כאשר נוצר שיהוי משמעותי בין האירוע לבין הדיווח או הבקשה לסיוע מצד הקורבן.[23] אולם עדות לכוונותיה של סין קיימת מזה כעשור: בשנת 1999 פרסמו שני קולונלים בצבא הסיני ספר תחת הכותרת "*Unrestricted Warfar*" ("לוחמה בלתי־מרוסנת"), שהדגיש אמצעים חלופיים להבסת יריב, שאינם פעולה צבאית ישירה ובעלת אופי מסורתי.[24]

גם רוסיה היא יריבה נחושה ומתוחכמת במרחב הסייבר. בעימות של 2008 בין רוסיה לגיאורגיה, תקפה רוסיה את רשת התקשורת הגיאורגית והרסה אותה. כפי שציין השגריר, דיויד סמית': "רוסיה שילבה פעולות סייבר בדוקטרינה הצבאית שלה", אם כי "בלא הצלחה מלאה... המתקפה המשולבת של רוסיה על גיאורגיה ב־2008 – מתקפה צבאית ומתקפת סייבר – הייתה המבחן המעשי הראשון של דוקטרינה זו... [ו]עלינו להניח שהצבא הרוסי למד מהלקחים שהופקו".[25] ב־2007, בנקים וממשל באסטוניה וכן גופים נוספים היו גם הם יעד ל"התקפות מניעת שירות (DDOS) נרחבות, מפוזרות וממושכות... רבות מהן – מקורן ברוסיה".[26] ממקום מושבם ברוסיה הצליחו האקרים ועבריינים להטביע את חותמם. מרחב הסייבר התגלה כמכרה זהב לעבריינים, שחדרו לעומקו ככל שההזדמנויות להרוויח בו המשיכו להכפיל את עצמן. ערך שוק עבריינות הסייבר העולמי הוערך ב־2011 בלמעלה מ־12.5 מיליארד דולר, כאשר הנתח של רוסיה בעוגה הוא כ־2.3 מיליארד

דולר (קרוב לכפול מערכו המוחלט בהשוואה לשנה הקודמת). כמו כן, ישנם סימנים לכך שגורמי פשע מאורגן במדינה החלו להצטרף "באמצעות שיתוף נתונים וכלים" כדי להגדיל את רווחיהם.[27]

הפוטנציאל לשיתוף פעולה בין ובקרב גורמים בעלי מניעים שונים לחלוטין מעורר חשש רציני. לדוגמה, מדינות שאין להן יכולות משלהן אך מבקשות להזיק לארצות־הברית או לבעלות־בריתה עשויות להצטרף, או פשוט לקנות/לשכור את השירותים והמיומנויות של עבריינים והאקרים, שיסייעו להן לתכנן ולבצע מתקפות סייבר. קל לאתר ערכות קוד בסגנון 'עשה זאת בעצמך' לניצול נקודות תורפה ידועות, ואפילו תולעת Conficker (שגרסאות שלה עדיין אורבות ומסוגלות ליצור בוטנט [botnet] מכ־1.7 מיליון מחשבים) נשכרה לשימוש.[28] לפיכך, היעדר גישה לתשתית או היעדר גיבוי ממעצמה אינם מכשול. גורמים שלוחים (פרוקסי) בעלי יכולות סייבר זמינים גם הם. קיים יריד חימוש לנשק סייבר. יריבים אינם זקוקים ליכולות, אלא רק לכוונה ולמזומנים.[29] זוהי תחזית מצמררת, אם זוכרים שארגון אל־קאעדה קרא למוג'אהידין ברשת לתקוף את ממשלת ארצות־הברית ותשתיות אמריקאיות חיוניות. סגן־אדמירל סמואל קוקס ממטה הסייבר ציין שפעילי ארגון אל־קאעדה מחפשים באופן פעיל אחר אמצעים לתקיפת רשתות אמריקאיות – יכולת שבאפשרותם לרכוש מהאקרים עבריינים.[30] כמו כן, בלי קשר לאופן השגתן, ליכולות סייבר יש פוטנציאל לשמש כמכפיל כוח במתקפה קונבנציונלית.

מוקדי דאגה אחרים הבולטים בהקשר זה כוללים את צפון־קוריאה ואיראן. את חוסר היכולת הקיימת, לפי שעה, משלימות שתי מדינות אלה בריבוי כוונות. איראן משקיעה משאבים נכבדים בהרחבה ובהעמקה של יכולות לוחמת הסייבר שלה.[31] היא גם מסתמכת זה מכבר על שלוחים כגון חזבאללה, שמתרבר עתה בארגון עמית בשם "סייבר חזבאללה" המיועד לפגוע במי שנתפס כאויב. גורמי אכיפת חוק מציינים כי היעדים והמטרות של "סייבר חזבאללה" כוללים הדרכה וגיוס אקטיביסטים בסייבר שהם תומכי משטר (כלומר, תומכי הממשל באיראן). אלה מצְדם מלמדים אחרים את הטקטיקות של לוחמת הסייבר. חזבאללה ממהר לנצל לרעה כלי מדיה חברתית דוגמת פייסבוק, כדי להשיג מודיעין ומידע, דבר שמייצר הזדמנויות נוספות לאיסוף עוד נתונים, במקביל לזיהוי יעדים פוטנציאליים חדשים ולפיתוח שיטות מותאמות ואמצעי גישה.[32]

נוסף לאלה, גורמים מתוך 'משמרות המהפכה' האיראניים עשו ניסיונות גלויים למשוך אליהם האקרים.[33] יש עדות לכך שבמוקד מאמצי הסייבר של 'משמרות המהפכה' פועלת קבוצת ההאקרים הפוליטית/עבריינית האיראנית "אשיאן" (Ashiyane).[34] משטרת הבאסיג', שמקבלת תשלום על ביצוע פעולות סייבר בשם המשטר, מספקת את מרבית כוח האדם לפעולת הסייבר של איראן.[35] במקרה של עימות במפרץ הפרסי, תוכל איראן לשלב שיטות ממוחשבות ואלקטרוניות

למתקפת רשת כדי לפגוע במערכות מכ"ם של ארצות־הברית ובעלות־בריתה, ולהקשות עליהן לבצע פעולות הגנה והתקפה גם יחד.[36] כחלק ממשימתו של ארגון חזבאללה עצמו להשיג הרתעה, הצהיר בגלוי מנהיגו, חסן נסראללה, שלא תהיה כל הבחנה בין ישראל לבין ארצות־הברית מבחינת פעולות נקם, אם תתקוף ישראל את איראן כדי לעכב את התקדמותה לעבר יכולת גרעינית: "אם ישראל תתקיף את איראן, אמריקה תישא באחריות".[37]

לסיכום, מדינות מנצלות לרעה את מרחב הסייבר כדי להשיג יתרון ולקדם את האינטרסים שלהן באמצעות איסוף מידע והשגת כושר פגיעה ביכולותיו של מי שנתפס כאויב. גם גורמים לא־מדינתיים, ארגוני טרור ועבריינים ממנפים את מרחב הסייבר למטרותיהם, ומפיקים תועלת מתחום שבו כולם ניצבים באותה נקודת זינוק, המתיר גם לשחקנים יחידים קטנים יותר להשפיע באופן שאינו יחסי לגודלם. אסימטריה זו מייצרת סביבה זרועת סכנות שונות, שבעבר לא משכו את תשומת הלב והאנרגיות של המעצמות. לפיכך, המעצמות חוששות מתרחישים מסוימים דוגמת אלה שצוינו לעיל, בשל יכולתם לערער באופן משמעותי ואף לחסל לחלוטין את האמון והביטחון במערכת (אמריקאית או אחרת).

איום זה אינו ייחודי לארצות־הברית. לוחמה אסימטרית היא כמובן אחת מהתכונות המאפיינות את ניסיונה של ישראל בשדה הקרב הממשי והווירטואלי גם יחד.[38] יש להביא בחשבון גם נפגעים ידועים פחות (לכאורה) של המאבק הסייברי. בהמשך לכך, הנה תיאור של הרשות הלאומית לריגול נגדי (Office of the National Counterintelligence Executive – הגוף האמריקאי שמרכז את המלחמה בטרור – בדוח לשנת 2011 שהגיש לקונגרס:

> המשרד הפדרלי הגרמני להגנה על החוקה (BfV – Federal Office for the Protection of the Constitution) מעריך שחברות גרמניות הפסידו בין 28 ל־71 מיליארד דולר ובין 30 ל־70 אלף מקומות עבודה בכל שנה בעקבות ריגול כלכלי של גורמים זרים. כמעט 70 אחוזים מכל המקרים מערבים גורמי פנים (insiders).
>
> דרום־קוריאה מדווחת שהעלויות כתוצאה מריגול כלכלי של גורמים זרים ב־2008 עמדו על 82 מיליארד דולר, לאחר שכבר הגיעו ל־26 מיליארד דולר ב־2004. הדרום־קוריאנים מדווחים ש־60 אחוזים מהקורבנות הם עסקים קטנים ובינוניים, וכי מקורו של מחצית מהריגול הכלכלי הוא בסין.
>
> משרד הכלכלה, המסחר והתעשייה היפני ערך סקר בקרב 625 חברות יצרניות בשלהי 2007, ומצא כי יותר מ־35 אחוזים מהחברות המשתתפות דיווחו על אופן כלשהו של הפסד טכנולוגי. יותר מ־60 אחוזים מדליפות אלה היו קשורות לסין.[39]

הדברים שאמר הסנטור הצרפתי, ז'אן־מארי בוקל (Jean-Marie Bockel) – שתועדו ב'דוח מידע' של ועדת הסנאט הצרפתית לענייני חוץ, הגנה והכוחות המזוינים – מטרידים במידה דומה:

> בצרפת, רשויות מנהליות, חברות ומפעילי שירותים חיוניים (אנרגיה, תחבורה, בריאות וכד') נופלים קורבן מדי יום למיליוני מתקפות סייבר... המקור למתקפות סייבר אלה יכול להיות האקרים של מחשבים, קבוצות אקטיביסטיות, ארגוני פשע וכן חברות מתחרות, או אפילו מדינות אחרות. האצבע המאשימה מופנית לרוב כלפי סין או רוסיה, אם כי קשה מאוד לזהות במדויק את היוצרים שמאחורי כל מתקפה.[40]

וכך גם ההערכה שמספק ג'ונתן אוונס (Jonathan Evans), העומד בראש שירותי הביטחון בבריטניה:

> אסטרטגיית הביטחון הלאומי של בריטניה ממקמת בצורה ברורה את אבטחת הסייבר לצד הטרור, כאחד מארבעת אתגרי המפתח שניצבים בפני בריטניה. נקודות תורפה באינטרנט מנוצלות לרעה בצורה אגרסיבית לא רק על ידי עבריינים אלא גם על ידי מדינות, וההיקף הוא מדהים: מדובר בתהליכים בקנה־מידה תעשייתי המערבים אלפי אנשים, שעומדים מאחורי ריגול סייבר במימון מדינות ופשע סייבר מאורגן... חברה שעמה עבדנו, מהגדולות בלונדון, מעריכה שסבלה הפסדי הכנסות בסך 800 מיליון ליש"ט כתוצאה ממתקפת סייבר מצד מדינה, ולא רק כתוצאה מאובדן קניין רוחני, אלא גם בשל פגיעה ביתרון המסחרי שלה בעת ניהול משא־ומתן על כריתת הסכמים. אלה לא יישארו הקורבן התאגידי היחידי שסובל מבעיה זו. [41]

אוונס הוסיף ואמר את הדברים הבאים:

> עד כה, ארגוני טרור קיימים לא הציבו איום משמעותי בערוץ זה, אולם הם מודעים לפוטנציאל הקיים בניצול נקודות תורפה בסייבר כדי לתקוף תשתית חיונית, ואני צופה שהם ירכשו יכולות נוספות כדי לעשות זאת בעתיד.[42]

השאלה הנדרשת היא, לפיכך, מה צריך לעשות.

הרתעת סייבר ותגובה רב־ממדית

על רקע העדויות הרבות והמטרידות על יכולות הסייבר ועל כוונות עוינות מצד גורמים מדינתיים ולא־מדינתיים כאחד, חייבת ארצות־הברית להתוות ולגבש בקפידה מסלול התקדמות להתמודדות עוצמתית עם העובדות ועם המציאות המדאיגה המאפיינות את מרחב הסייבר כיום (ואשר לא סביר שייעלמו בקרוב). תהא זו נחמת שווא לחשוב שארצות־הברית או בעלות־בריתה יוכלו לפתור את הבעיה בעזרת 'חומות אש' (firewalls) בלבד. במקום זאת, על ארצות־הברית לנסח, להבהיר וליישם אסטרטגיה להרתעת סייבר, שתסייע בתמיכה ובחיזוק אבטחת הסייבר וההגנה על תשתיות חיוניות.

בתחומים מסוימים כבר מתקיים דיון נמרץ אך ראשוני בנושא זה, אולם בשל טבעו המורכב, חוצה המגזרים והרב־תחומי של האתגר, לא גובשה עד כה תגובה אסטרטגית משולבת. האיומים מתפתחים מדי יום ומוסיפים עוד נדבך של מורכבות, ולמרות הקצב והעוצמה של זרם האיומים, המגזרים השונים אינם משתפים ביניהם

בדרך כלל את המידע על האמצעים והכלים המשמשים את גורמי האיום, ואינם מפרסמים אותו. בעיקרון, שתיקה זו אינה חסרת הגיון, שכן הממשלה מבקשת להגן על חומר מסווג והתעשייה מעוניינת להגן על מידע קנייני. אולם בפועל, שתיקה כזו "תוקעת מקלות בגלגלים" שאמורים להניע תגובה ומאמצי מניעה.

על רקע דברים אלה, אין ספק שהיקף המשימה מעורר אימה, אולם ארצות־הברית צפויה להפיק תועלת מרובה מפיתוח ומיישום אסטרטגיה להרתעת סייבר, וממדיניות השואפת להניא, להרתיע ולהכניע – הן כגישה כללית והן באופן שמותאם במיוחד לגורם/יריב מסוים. עמדה כללית יציבה, כלומר, צעדי אבטחה בסיסיים (הגנה, היגיינה, טכנולוגיה), יכולה להוות 80 אחוזים מהפתרון ולנטרל את מרבית האיומים לפני שהם מתממשים במלואם. בכך ניתן יהיה לשחרר משאבים (אנושיים, כספיים וטכנולוגיים), שיוכלו להתמקד באופן תלוי־הקשר בשאר התחומים שמרכיבים את הבעיות והאיומים הקשים ביותר מבחינת רמת התחכום והנחישות. כדי להפוך המלצות אלה למעשיות, יש להתוות קווים ברורים. ראוי לשמור על הגמישות של תגובת ארצות־הברית באמצעות שמירה על מידת עמימות מסוימת באשר לאמצעים שברשותה, כל עוד הפרמטרים מובהרים היטב באמצעות הצבת סימני דרך ייעודיים או קווים אדומים נבחרים, שחצייתם לא תעבור בשתיקה.[43]

על מנת לייצר הרתעה אפקטיבית מול יחיד או ישות, ובכך למנוע מהם מלהשיג את מטרתם – ומוטב למנוע מהם לפעול מלכתחילה – הכרחי להבין באופן מוחלט מה בדיוק מנסה הצד היוזם להשיג. (הרעיון מבוסס על הנושא/העיקרון של האסטרטג הנודע, מיאמוטו מוסאשי (Miyamoto Musashi): "דע את אויבך, דע את חרבו"[44]). הבנה בסיסית זו מהווה את הצעד הראשון בדרך להניא את היריב מפעולה או להכניעו, ויישומה כרוך בבחינה יסודית של המצב מנקודת מבטו של הצד האחר. אמנם, כל מקורות האיום שצוינו לעיל עוסקים בריגול ובניצול של מידע ומערכות דרך אמצעי סייבר, אולם יש לזכור שלגורמים שונים יש יעדים שונים ומובחנים. למרות שהם עושים שימוש באמצעים וירטואליים ובמדיום וירטואלי, כל אחד מגורמים אלה שואף להשיג תוצאות מסוימות בעולם האמיתי, ובהתאם לכך יכוון את מעשיו.

מה חייבת ארצות־הברית לעשות כדי לשכנע גורמים מדינתיים להימנע מהפעלת שירותי המודיעין והצבא שלהם לצורך ניצול רשתות מחשב או לשם מתקפה על רשתות מחשב, בשם מטרות־על כלשהן? תגובת הסייבר של ארצות־הברית צריכה להיות תוצאה של אסטרטגיית הרתעה רחבה יותר ביחס לגורם נתון. במילים אחרות, הרתעת הסייבר תהיה תואמת ומשלימה לאסטרטגיית הרתעה אמריקאית מקיפה יותר. מדינות אחרות צריכות להבין ולהעריך את העובדה שארצות־הברית מסוגלת להטיל עונש מידתי אם תותקף במרחב הסייבר, וכי

התגובה האמריקאית עשויה בסופו של דבר להיות 'סייברית' או צבאית, כאשר כל האפשרויות מונחות על השולחן. לגבי תגובת סייבר, יש להפגין את יכולת ההתקפה באופן שלא יותיר ספק באשר להשלכות שיהיו לחציית קו אדום של ארצות־הברית. עם זאת, הפגנת היכולת חייבת להתבצע תוך הכרה מלאה בעובדה שניתן יהיה ללמוד ולשנות כל כלי, טכניקה, טקטיקה או הליך שייושמו, ולהשתמש בהם כדי לנקום בארצות־הברית ובבעלות־בריתה. התגובה בהקשר זה תלויה ביכולת לייחס את המתקפה לגורם ספציפי אחד או יותר (כוחות זרים).

מבחינת המודיעין, יש לזכור שמאז ומתמיד עסקו מדינות בגניבת סודות. אמנם הריגול הפך דיגיטלי, אך ממשלות זרות משתמשות באמצעי סייבר למטרה המקורית: להשיג מידע שיכול לשמש לעיצוב ולחידוד קבלת החלטות, ולשם כך הן מנסות להתאים את 'המקצוע העתיק בעולם' השני למאה ה־21. במילים אחרות, מדינות משתמשות באמצעי סייבר (דוגמת האקרים רוסיים וסיניים העובדים בשירות ממשלותיהם) כדי להגביר את יכולתן לאסוף מידע בעל ערך עבור קובעי המדיניות שלהן. השאלה היא, איזה מידע מעוניינים גורמים אלה להשיג, ומדוע? המידה שבה הממשלה שעל הכוונת (ארצות־הברית או בעלת־בריתה) תהיה מסוגלת להגן טוב יותר על המערכות שלה ולהתאים להן פעולות הרתעה תלויה ביכולתם של המומחים להרתעת סייבר להציג תובנות, ולנסח תשובות ברורות לשאלה זו.

ריגול תעשייתי הוא תת־קבוצה בסוג זה של פעילות המתקיימת בחסות מדינה. הכוונה היא להגביר את השגשוג הכלכלי או את יישומם של שיקולים עסקיים במדינה מסוימת. למרות שפעולת הריגול מוכוונת על ידי המדינה, הנהנים ממנה עשויים להיות גורמים פרטיים או פרטיים־למחצה. מצד אחר, מנקודת מבטו של יעד הריגול, ההשלכות של גניבת סודות מסחריים עלולות להיות מעמיקות ולהתרחב מעבר לאובדן הכלכלי, עד כדי פגיעה במעמדה של המדינה בעולם. על פי הערכתו של רוברט בראיינט (Robert "Bear" Bryant) מהרשות הלאומית האמריקאית לריגול נגדי, ריגול סייבר הוא "איום שקט על הכלכלה שלנו עם תוצאות ניכרות ביותר... סודות מסחריים שפותחו במשך אלפי שעות עבודה על ידי המוחות המבריקים ביותר שלנו נגנבים בשבריר שנייה, ומועברים למתחרים שלנו".[45] החדשנות והפריון של ארצות־הברית עלולים גם הם לסבול כתוצאה מכך, עם השלכות פוטנציאליות משניות נוספות על צמיחה ופיתוח עתידיים. אם מידע צבאי נחשף ונגנב, עלולות להיות לכך גם השלכות על הביטחון הלאומי. אין צורך בדמיון רב כדי לשער מה יכול לעשות גורם עוין עם טכנולוגיה אמריקאית גנובה בעלת פוטנציאל ליישום צבאי.[46]

בדומה למדינות, גם ארגוני טרור על־לאומיים מבקשים להשיג יתרון אסימטרי שאותו יוכלו למנף, בניסיון להנחיל את סדר־היום הפוליטי שלהם. עם זאת, בדרך

כלל מחזיקים ארגונים כאלה משאבים פחותים מאלה של מדינה, ומשתדלים להימנע ממעורבות בתהליך הפוליטי ולהעדיף שימוש באלימות להשגת מטרותיהם. מנקודת מבט זו, לא יהיה זה מאמץ גדול מדי עבורם להשיג תמורה נוספת להשקעתם, באמצעות שימוש באמצעים דיגיטליים כמכפיל כוח של פעולה צבאית. ככל שניתן יהיה ללמוד פרטים נוספים על הסייבר הטקטי ועל המטרות והשאיפות הפוליטיות והאסטרטגיות של ארגונים אלה, כך יתקבל חומר גלם מועיל יותר לעיצוב הרתעת סייבר שתמנע מהם לפעול.

ארגוני הטרור והפשע עשויים גם להתאחד וליצור איום משולב המתבסס על ברית מטעמי נוחות, שבה כל צד נשען על המיומנויות והנכסים של הצד השני כדי לקדם את מטרותיו בהתאם. בניגוד לארגוני הפשע שמקור הכנסתם העיקרי הוא הפשע בלבד, רווח כשלעצמו אינו המניע של ארגוני טרור. הבדל מהותי זה מהווה למעשה פתח שניתן לנצלו באמצעות תצוגה וביצוע מקצועיים של אסטרטגיית הרתעת סייבר מותאמת.

יש לזכור שהרתעה היא תת־קבוצה של הכנעה, שמטרתה לגרום לירי להימנע מפעולה על ידי כך שהיא גורמת לו להאמין שהסבירות להצלחתו קלושה, או שהנזק מהתגובה יהיה גדול ממה שיהיה מוכן לשאת.[47] בעבר נדרש שהרתעה תכלול "שלושה רכיבים גלויים: ייחוס, איתות ואמינות".[48] בהקשר הנוכחי, הרתעה מגלמת הנחה מוקדמת על כך שהקווים האדומים הכלליים של ארצות־הברית הובהרו ליריביה וכן לבעלות־בריתה, שהיא אותתה כי חציית גבולות אלה לא תעבור בשתיקה, וכי היא יכולה ומוכנה להטיל את ההשלכות של כל הפרה כזו על מי שחוצה אותם. התגובה האמריקאית הצפויה צריכה להיות מאיימת דיה על מנת להניא את הגורם המאיים הפוטנציאלי מביצוע הפעולה מלכתחילה.

כאשר ארצות־הברית מגדירה קווים אדומים במרחב הסייבר, עליה לפעול במחשבה תחילה ובזהירות ניכרת, ולזכור שפעילויות שמתקרבות לקווים אלה אך אינן חוצות אותם יגררו עונש מופחת, כפועל יוצא של הגדרת הגבולות. יש להעריך בהתאם פעילויות שאינן מבוצעות למטרה חיובית, כגון מאמצים למפות את התשתית החיונית בארצות־הברית. שום טובה לא תצמח מכך שלמדינה אחרת או לגורם לא־מדינתי זר יהיה ידע מפורט על מערכות אלה.

הייחוס הוא מכריע בביסוס ההרתעה. חשוב שניתן יהיה לדעת מי פעל, על מנת להטיל עליו את ההשלכות. עם זאת, קשה לאתר את "המקלדת המעשנת" במרחב הסייבר, שכן מרחב זה נוצר כך שיאפשר הכחשה אמינה. סדרי הגודל והמשמעות של אתגר הייחוס בהקשר של תגובה למתקפת סייבר זכו להדגשה מצד אנליסטים בכירים,[49] אם כי יש גם דעות מנוגדות.[50] אם נתעלם לרגע מהקושי לעשות זאת, היכולת לקשר בין הפעולה לבין הגורם לה תאפשר לצד המותקף להגיב. היכולת להגיב באותה מטבע מעלה את מספר האפשרויות שהצד המותקף יוכל להסתמך

עליהן בדיעבד, לרבות האפשרות להגיב בעוצמה רבה יותר מזו שהצד המותקף ספג. ראוי אפוא להשקיע זמן ומשאבים במאמץ מרוכז שתכליתו לפתח יכולת ייחוס משופרת, באמצעות טכנולוגיות ואמצעים אחרים.

היריבים חייבים גם הם להבין ולהעריך שארצות־הברית ערוכה ומוכנה להשתמש במלוא הכוח שברשותה – במגוון, בהיקף ובעומק – על מנת לאכוף כללים אלה. כדי לשדר מסר זה בצורה משכנעת ולהביא לכך שהוא יגיע ליעדו ולאוזניהם של בעלי הכוונות העוינות, חייב להתקיים מצג פומבי של היכולות באופן שיבהיר את המסר לאשורו, מבלי לחשוף יותר מדי ולאבד את היתרון בשל כך. למשל, עליו למנוע אפשרות שהאויב יוכל לבצע "הנדסה הפוכה" (או לחקות בדרך אחרת), ולהשתמש באותם אמצעים ושיטות של ארצות־הברית שהוצגו בפומבי, שמא יהיה זה "גול עצמי". היבט ה"מצג" של התרגיל הופך מתעתע אף יותר כאשר זוכרים שהחוקים השולטים בלוחמת הסייבר עדיין בשלבי התפתחות, ולכן אינם חד־משמעיים במידה מסוימת. נקיטת זהירות ותשומת לב נדרשים, אם כך, גם ברמה המשנית.

אף על פי שארצות־הברית נדרשת להפגין את ארגז הכלים שלה, המצויד בכל הנדרש כדי להילחם בגורמים עוינים בעת הצורך, עד היום לא הייתה הפגנה פומבית חד־משמעית כזו של עליונות סייבר, שארצות־הברית טענה באופן יזום והחלטי לבעלות עליה. על רקע זה, האם עליה לשקול ביצוע מקביל דיגיטלי של ניסוי גרעיני חי? יש להפנות שאלה זו לקובעי המדיניות, למומחים ולאנשי הטכנולוגיה האמריקאיים, המבקשים להגדיר את מסלול ההתקדמות ולפתח דוקטרינה ואסטרטגיה עבור מרחב הסייבר. האירוניה היא שאם תרגיל כזה יתבצע בזהירות (ההולמת את גודלו), הוא יוכל לפעול ביעילות להרתעת גורמים עוינים, כך שאין להוציא מכלל אפשרות שהוא יתרום למניעת מלחמה.

בניית יציבות באמצעות עוצמה

נהוג לומר שההגנה הטובה ביותר היא ההתקפה. על פי דיווחים ממקורות גלויים, ארצות־הברית מפתחת כללים למעורבות בכל הקשור למתקפות סייבר, ומשרד ההגנה חותר לחיזוק ארסנל נשק הסייבר שברשותו[51] (אם כי מתקפת סייבר עשויה להביא לתגובה צבאית או לתגובת סייבר). כפי שציין סגן יו"ר המטות המשולבים לשעבר, הגנרל ג'יימס אי. קרטרייט (James E. Cartwright), מאמצים והשקעה מהסוג שתואר כאן יסייעו להתאים מחדש את יחס ההגנה מול ההתקפה – שעד לאחרונה עמד על 90% מול 10% לערך לטובת ההגנה[52] – ויחזקו ויבנו אמון ביכולתה של ארצות־הברית להרתיע ביעילות פעולה עוינת במרחב הסייבר.

עם זאת, קהילת ביטחון הסייבר בארצות־הברית, כמו המקבילות לה אצל בעלות־בריתה, טרם השלימה את התהליך. עוד ארוכה הדרך עבור קהילה זו, בייחוד

בארצות־הברית, עד שתגיע לרמת המיומנות והבשלות שמציגות כיום הקהילות העוסקות במלחמה בטרור בארצות־הברית.[53] סנכרון סעיפים 10 ו־50 בחוק האמריקאי ששילב יחדיו פונקציות מודיעין וצבא מהווה פריצת דרך משמעותית בעידן שלאחר פיגועי ה־11 בספטמבר, שהביאה לשיפור ניכר במצבה הכולל של ארצות־הברית במלחמה בטרור. היא יכולה למנף הישג זה באמצעות התאמה והחלה של תפיסה דומה גם על הסייבר. עליה לחתור לכך תוך התייחסות לשני אתגרים (שעדיין יש לעמוד בהם): הסדרת החוקים העוסקים במעורבות וחתירה לעמדה יוזמת יותר.[54]

כדי להתקדם בחוכמה במרחב הסייבר, חייבות ארצות־הברית ובעלות־בריתה להפגין מנהיגות ולהציג חזון, לצד תוכנית פעולה מבוססת. זמן רב מדי הניעו התקריות את האסטרטגיה, למעשה, זוהי טקטיקה במסווה של אסטרטגיה. ארצות־הברית מחזיקה במספר יכולות ייחודיות, אך אלה לא ינוצלו במלואן עד שתגובש מסגרת אסטרטגית רחבה יותר שבתוכה ניתן יהיה לשבצן. בהמשך למסגרת הרעיונית שהוצגה כאן, עולים עקרונות מפתח מסוימים שיכולים לשמש בסיס לפיתוח וליישום אסטרטגיה, יכולת ועמדה להרתעת סייבר יעילה. עקרונות אלה מהווים את ראשיתה של תוכנית להרתעת סייבר, כדלקמן:

כיול במטרה לממש את החזון. בהקשר זה, יכולת תומכת באמינות. יש לשקול בזהירות את הכיול הקיים ולכוונו כנדרש, בהתאם להשקעות ולמאמצים המשקפים את היחס בין הגנה להתקפה – שחוסר איזון בו עלול להשפיע לרעה על הביטחון הלאומי. בהיותו דרישה מקדימה לאכיפת ההשלכות, כיול (או כיול מחדש) מתקיים בד בבד עם הרצון הפוליטי לפעול לאכיפת סנקציות בבוא העת.

התחלה ובנייה מעמדת כוח. כדי להרתיע ולהניא יריבים בהצלחה, נדרשת יכולת לשכנע אויבים פוטנציאליים שהמחיר של פעולה עוינת מצדם יעלה על התועלת שהם מייחסים לה. פיתוח של יכולת מכת פתיחה ואיתות נכון על קיומה הם, לפיכך, בסיסיים.

שימת הדגש על מהירות, הפתעה ויכולת תמרון. במרחב הסייבר, כל ננו־שנייה קובעת. לכן, היעד הוא להגיב בזמן אמת ככל האפשר. בעוד אין לפקפק בעיקרון שלכל חציית קו אדום יהיו השלכות, יש ערך לשמירה על מידה של עמימות באשר לטיבן המדויק של השלכות אלה, ועל ידי כך יישאר אותו גורם במצב של אי־ודאות תמידי. גמישות ובהירות נראות סותרות לכאורה, אך למעשה הן מייצרות אסטרטגיה שקולה.

אין להותיר אף אחד מאחור. יכולת של מכת פתיחה בלבד תותיר את המדינה פגיעה ובלתי־מוכנה לתגובה באותה מטבע, אם היריב מסוגל לכך. כמו בשלב המלחמה הקרה של עידן הגרעין, יידרשו תכנון מראש וזהירות בהפעלת יכולת מכה שנייה באופן שיבטיח הגנה על הכוח. שימור העליונות המדעית והטכנולוגית

הוא גורם מכריע, שכן ניתן להגיע לפתרונות טכניים לנוכח האתגרים המטרידים במרחב הסייבר.

דע את האויב. הביטוי אולי ישן ושחוק, אך הוא עדיין תקף. כדי להביס אויב פוטנציאלי נדרשת הבנה מעמיקה של מטרותיו ושאיפותיו הספציפיות. תובנה מעין זו תאפשר לבנות את האסטרטגיה והטקטיקה לאותו מקרה תוך התאמת הרכיבים ליריב הספציפי, ובכך למקסם את פוטנציאל הסיכול. הכלל שתקף כאן הוא מה שמכונה "לולאת OODA": התבונן, התכוונן, החלט ופעל (observe, orient, decide, and act).

הובלה שמהווה דוגמה. ברעיון של הרתעת סייבר איתנה טמונה הנחת המוצא, שהישות המנסה להרתיע מחוסנת מפני מה שהיא מנסה לעולל לאחרים (שכן תמיד קיימת האפשרות לאפקט בומרנג). כל דרך אחרת כמוה כקפיצה מהמטוס ללא מצנח. לכן, המסקנה המכרעת היא שעל ממשלת ארצות־הברית לשאוף תחילה לפתרון בעיותיה שלה, כדי להתמודד עם האיום. יתרה מכך, על הממשלה ליזום את הצעדים הדרושים להקלת שיתוף המידע, כך שעובדות חיוניות יגיעו לידי כל גורמי המפתח האחראיים להגנה על נכסים ומשאבים לאומיים, לרבות אלה שבבעלות המגזר הפרטי ובתפעולו (תשתית חיונית).

שותפים להצלחה. אין מרכיב יחיד בממשלה, גם לא הממשלה כגוף אחד, שיוכל להתמודד לבדו במרחב הסייבר. חיוני לכונן שותפויות אמת בתוך המגזרים השונים וביניהם. בתוך הממשל לדוגמה, סנכרון זהיר ושילוב של פונקציות מודיעין וצבא (סעיפי החוק 10 ו־50) למטרות הרתעת סייבר עשוי להתגלות כבעל ערך רב, כפי שהיה בהקשר של מלחמה בטרור. החשיבות של התגוננות מראש מתרחבת מעבר למגזר הציבורי, לעבר רשתות ומערכות חיוניות שמצויות בידיים פרטיות. בהתאם לכך, על המגזר הפרטי להתחייב לנקוט את הצעדים הדרושים לחיזוק הביטחון הלאומי. כדי להבטיח עמידה בסף זה, הרשויות הפדרליות צריכות להושיט יד למגזר הפרטי, בגישה שתשלב תמריצים חיוביים ושליליים להשגת התוצאה המבוקשת, בשיטת "המקל והגזר".

חשיבה ופעולה במושגים בינלאומיים. אתגרים חוצי־גבולות מחייבים פתרונות חוצי־גבולות, ומרחב הסייבר הוא חסר גבולות מטבעו. שותפים נאמנים ברמה הבינלאומית יכולים וצריכים לספק ערך רב בהקשר זה. יש להודות שאינטרסים לאומיים עלולים לפגוע ביכולת לשתף נתונים ומידע רגיש. יחד עם זאת, ההימנעות ממינוף יחסים בילטרליים ובריתות מרכזיות תהיה "גול עצמי", החל מהסכם שיתוף המודיעין "Five Eyes"(בין אוסטרליה, קנדה, ניו־זילנד, ארצות־הברית ובריטניה), דרך ברית נאט"ו ועד האיחוד האירופי, וכן שותפות אסטרטגיות נוספות כמו באזור המזרח התיכון ואסיה, הכוללות את ישראל, סינגפור, הודו ויפן.

עם מנהיגות מעוררת השראה בלוחמת הסייבר ברמה של דמויות המופת הצבאיות, בילי מיטשל (Billy Mitchell), ביל דונובן (Bill Donovan) או ג'ורג' פטון (George Patton) – שהיטיבו להבין את השימושים האסטרטגיים והטקטיים של חידושי טכנולוגיה ונשק – ארצות־הברית יכולה לעצב ולהוציא לפועל אסטרטגיית הרתעת סייבר רבת־עוצמה שמישירה מבט אל אויביה כשהיא מוכנה כיאות, בשאיפה שהאירועים שנכונו לה יישארו כרוכים בבייטים וביטים בלבד, במקום בכדורים, בפצצות ובשפיכות־דמים.

הערות

1 Eric Sterner, "Deterrence in Cyberspace: Yes, No, Maybe," in *Returning to Fundamentals: Deterrence and U.S. National Security in the 21st Century* (Washington, DC: George C. Marshall Institute, 2011), p. 27.

2 Bryan Krekel, Patton Adams, and George Bakos, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*, Prepared for the U.S.-China Economic and Security Review Commission by Northrop Grumman Corporation, March 7, 2012, p. 54, http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf.

3 Siobhan Gorman, "Electricity Grid in U.S. Penetrated By Spies," *Wall Street Journal*, April 8, 2009, http://online.wsj.com/article/SB123914805204099085.html; and Mark Clayton, "Exclusive: Potential China Link to Cyberattacks on Gas Pipeline Companies," *Christian Science Monitor*, May 10, 2012, http://www.csmonitor.com/USA/2012/0510/Exclusive-potential-China-link-to-cyberattacks-on-gas-pipeline-companies.

4 Office of the National Counterintelligence Executive (NCIX), *Foreign Spies Stealing US Economic Secrets in Cyber Space: Report to Congress on Foreign Economic Collection and Industrial Espionage 2009-2011* (October 2011), p. 4, http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf;

5 שם.

6 Eben Kaplan, *Terrorists and the Internet*, Council on Foreign Relations, January 8, 2009, http://www.cfr.org/terrorism-and-technology/terrorists-internet/p10005; and Special Report by the Homeland Security Policy Institute (HSPI) and the University of Virginia's Critical Incident Analysis Group (CIAG), *NETworked Radicalization: A Counter-Strategy* (Washington, DC: May 2007).

7 Group IB, *State and Trends of the Russian Digital Crime Market 2011*, p. 6, http://group-ib.com/images/media/Group-IB_Report_2011_ENG.pdf.

8 ראו:
Thomas C. Schelling's classic text, *Arms and Influence* (New Haven: Yale University Press, 1966).

9 ראו לדוגמה:
Martin C. Libicki, *Cyberdeterrence and Cyberwar* (RAND Corporation, 2009).

10 Sun Tzu, *The Art of War*, translated by Samuel B. Griffith (New York: Oxford University Press, 1963).

11 Ellen Messmer, "DHS: America's Water and Power Utilities under Daily Cyber-Attack," *Network World*, April 4, 2012, http://www.networkworld.com/news/2012/040412-dhs-cyberattack-257946.html?t51hb&hpg1=mp.

12 Jason Koebler, "U.S. Nukes Face up to 10 Million Cyber Attacks Daily," *US News & World Report*, March 20, 2012, http://www.usnews.com/news/articles/2012/03/20/us-nukes-face-up-to-10-million-cyber-attacks-daily.

13 Joe Lieberman, "Cyber Networks Sitting Ducks for Attacks" *Hartford* Courant, April 8, 2012, http://articles.courant.com/2012-04-08/news/hc-op-lieberman-cyber-security-biggest-national-th-20120408_1_cyber-attack-cyber-networks-cyber-threats

14 John O. Brennan, "Time to Protect against Dangers of Cyberattack," *Washington Post*, April 15, 2012, http://www.washingtonpost.com/opinions/time-to-protect-against- dangers-of-cyberattack/2012/04/15/gIQAdJP8JT_story.html.

15 Lieberman, "Cyber Networks Sitting Ducks for Attacks."

16 Jason Ryan, "FBI Director Says Cyberthreat will Surpass Threat from Terrorists," January 31, 2012, http://abcnews.go.com/blogs/politics/2012/01/fbi-director-says-cyberthreat-will-surpass-threat-from-terrorists/.

17 "המציאות היא שהתשתיות שלנו עוברות קולוניזציה", אמר טום קלרמן, לשעבר הממונה מטעם הנשיא אובמה על המועצה לאבטחת הסייבר. ראו: David Goldman, "Cybersecurity Bills Aim to Prevent 'Digital Pearl Harbor,'" April 23, 2012, http://money.cnn.com/2012/04/23/technology/cybersecurity-bills/?source=cnn_bin.

18 "בכיר במודיעין שתידרך עיתונאים בנושא האנונימיות ציין כמה מקרים שבהם ניתנו אומדנים כחלק מתביעות נגד ריגול כלכלי במהלך שש השנים האחרונות: מחקר של Dow Chemical על הדברת חרקים בשווי של 100 מיליון דולר, נוסחאות כימיות של DuPont בשווי של 400 מיליון דולר, נתונים קנייניים של מוטורולה בשווי 600 מיליון דולר, נוסחאות צבע של Valspar בשווי של 20 מיליון דולר". ראו :
Ellen Nakashima, "In a World of Cybertheft, U.S. names China, Russia as Main Culprits," *Washington Post*, November 3, 2011, http://www.washingtonpost.com/world/national-security/us-cyber-espionage-report-names-china-and-russia-as-main-culprits/2011/11/02/gIQAF5fRiM_story.html.

19 Nick Hopkins, "Militarisation of Cyberspace: How the Global Power Struggle Moved Online," *The Guardian*, April 16, 2012, http://m.guardian.co.uk/technology/2012/apr/16/militarisation-of-cyberspace-power-struggle?cat=technology&type=article; and Nick Hopkins, "US and China Engage in Cyber War Games," *The Guardian*, April 16, 2012, http://m.guardian.co.uk/technology/2012/apr/16/us-china-cyber-war-games?cat=technology&type=article.

20 Reuters, "Saudi Oil Producer's Computers Restored After Virus Attack" *New York Times*, August 26, 2012, http://www.nytimes.com/2012/08/27/technology/saudi-oil-producers-computers-restored-after-cyber-attack.html?_r=1.

21 Elinor Mills, "Virus Knocks out Computers at Qatari Gas Firm RasGas," *CNET News*, August 30, 2012, http://news.cnet.com/8301-1009_3-57503641-83/virus-knocks-out-computers-at-qatari-gas-firm-rasgas/.

22 Christopher Brook, "Report: French Nuclear Company Areva Hit by Virus" *ThreatPost*, October 31, 2011, http://threatpost.com/en_us/blogs/report-french-nuclear-company-areva-hit-virus-103111.

23 מייקל מק'קול (McCaul), יו"ר ועדת המשנה לנושאי ביקורת, חקירה וניהול של ועדת בית הנבחרים לביטחון המולדת, אמר: "איסוף המידע האגרסיבי ביותר על הכלכלה והטכנולוגיה של ארצות־הברית נעשה מצד סין...יכולות לוחמת הסייבר של סין ומבצעי הריגול שהיא מפעילה הם הנפוצים ביותר מבין הגורמים המדינתיים. סין יצרה קבוצות האקרים אזרחיות המעורבות בריגול סייבר, והקימה יחידות צבאיות ללוחמת סייבר". ראו:
.NCIX, *Foreign Spies Stealing US Economic Secrets in Cyberspace*, p. 5;
ראו גם:
Cindy Saine, "Experts Warn of Increased US Cyber Security Threat" *VOA News*, April 24, 2012, http://www.voanews.com/english/news/usa/Experts-Warn-of-Increased-US-Cyber-Security-Threat-148786975.html.

24 Qiao Liang and Wang Xiangsui, published by China's People's Liberation Army, Beijing.

25 David J. Smith, "How Russia Harnesses Cyberwarfare," *American Foreign Policy Council Defense Dossier* (August 2012), http://www.afpc.org/files/august2012.pdf.

26 Jason Healey and Leendert van Bochoven, "NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow" *Atlantic Council Issue Brief* (2011) p. 2, http://www.acus.org/files/publication_pdfs/403/022712_ACUS_NATOSmarter_IBM.pdf.

27 Group IB, *State and Trends of the Russian Digital Crime Market 2011*, p. 6, http://group-ib.com/images/media/Group-IB_Report_2011_ENG.pdf;
ראו גם:
http://group-ib.com/images/media/Group-IB_Cybercrime_Inforgraph_ENG.jpg (איור).

28 Frank J. Cilluffo, "The Iranian Cyber Threat to the United States," Testimony Before the House of Representatives Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence, and Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies, April 26, 2012, p. 4, http://www.gwumc.edu/hspi/policy/Iran%20Cyber%20Testimony%204.26.12%20Frank%20Cilluffo.pdf; and Conficker Working Group, *Conficker Working Group: Lessons Learned*, http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf.

29 Cilluffo, Testimony Before the House of Representatives, p. 4.

30 Jack Clohurty, "Virtual Terrorism: Al Qaeda Video Calls for 'Electronic Jihad'" *ABC News*, May 22, 2012, http://abcnews.go.com/Politics/cyber-terrorism-al-qaeda-video-calls-electronic-jihad/story?id=16407875#.UEieyEQrOlg.

31 Yaakov Katz, "Iran Embarks on $1b. Cyber-Warfare Program," *Jerusalem Post*, December 18, 2011, http://www.jpost.com/Defense/Article.aspx?id=249864.

32 Cilluffo, Testimony Before the House of Representatives, p. 6.

33 Golnaz Esfandiari, "Iran Says it Welcomes Hackers Who Work for Islamic Republic," Radio Free Europe, March 7, 2011, http://www.rferl.org/content/iran_says_it_welcomes_hackers_who_work_for_islamic_republic/2330495.html

34 Iftach Ian Amit, "Cyber [Crime/War]," paper presented at DEFCON 18 conference, July 31, 2010.

35 "The Role of the Basij in Iranian Cyber Operations," *Internet Haganah*, March 24, 2011, http://internet-haganah.com/harchives/007223.html.

36 Michael Puttre, "Iran Bolsters Naval, EW Power," *Journal of Electronic Defense* 25, no. 4 (2002): p. 24; Robert Karniol, "Ukraine Sells Kolchuga to Iran," *Jane's Defense Weekly* 43, no. 39 (September 27, 2006), p. 6; Stephen Trimble, "Avtobaza: Iran's Weapon in Alleged RQ-170 Affair?" *The DEW Line*, December 5, 2011, http://www.flightglobal.com/blogs/the-dewline/2011/12/avtobaza-irans-weapon-in-rq-17.html.

37 Reuters, "Nasrallah: Iran could Strike US Bases if Attacked," *Jerusalem Post*, September 3, 2012, http://www.jpost.com/IranianThreat/News/Article.aspx?id=283706.

38 Ilan Evyatar, "Falling into the Trap, Over and Over Again," *Jerusalem Post*, November 17, 2010, http://www.jpost.com/Features/InThespotlight/Article.aspx?id=195767; Dan Harel, "Asymmetrical Warfare in the Gaza Strip: A Test Case," *Military and Strategic Affairs* 4, no. 1 (2012): pp. 17-24, http://www.inss.org.il/upload/(FILE)1339053338.pdf; Yolande Knell, "New Cyber Attack Hits Israeli Stock Exchange and Airline," *BBC* News, January 16, 2012, http://www.bbc.co.uk/news/world-16577184; and Joshua Mitnick, "Israel's Businesses Losing the Cyber War," *Wall Street Journal*, July 25, 2012, http://online.wsj.com/article/SB10000872396390443477104577549262451192148.html.

39 NCIX, *Foreign Spies Stealing US Economic Secrets in Cyberspace*, p. 19.

40 Jean-Marie Bockel, Senator for Haut-Rhin, "Cyber Defence an International Issue, a National Priority," *Information report no. 681 – Committee on Foreign Affairs, Defence and Armed* Forces, July 18, 2012, http://www.senat.fr/rap/r11-681/r11-681-syn-en.pdf.

41 נאום בהרצאה השנתית על ביטחון והגנה ע"ש לורד מאיור, שנערכת בעיר לונדון, https://www.mi5.gov.uk/home/about-us/who-we-are/staff-and-management/director-general/speeches-by-the-director-general/the-olympics-and-beyond.html.

42 ראו:
Tom Whitehead, "Cyber Crime a Global Threat, MI5 Head Warns," *The Telegraph*, June 26, 2012, http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/9354373/Cyber-crime-a-global-threat-MI5-head-warns.html.

43 Cilluffo, *Testimony Before the House of Representatives*, pp. 7-8.
ראו גם:
Frank J. Cilluffo, "The U.S. Response to Cybersecurity Threats," *American Foreign Policy Council (AFPC) Defense Dossier* (August 2012), http://www.afpc.org/files/august2012.pdf; and Martin C. Libicki, "The Strategic Uses of Ambiguity in Cyberspace" *Military and Strategic Affairs* 3, no. 3 (2011): pp. 3-10, http://www.inss.org.il/upload/(FILE)1333532281.pdf.

44 *The Book of Five Rings.*

45 Nakashima, "In a world of cybertheft, U.S. names China, Russia as main culprits" [citing NCIX Bryant].

46 שם.

47 W. W. Kaufmann, "The Requirements of Deterrence," in W. W. Kaufman, ed., *Military Policy and National Security* (Princeton: Princeton University Press, 1956); Peter Marquez, "Space Deterrence: The Pret-a-Porter Suit for the Naked Emperor," in *Returning to Fundamentals*, pp. 9-10. אילוץ מבקש להשפיע על היריב לפעול

או להימנע מפעולה באמצעות איום, או בפועל, לגבות מחיר מהיריב כדי להגביל את אפשרויותיו ו/או את חישובי העלות־תועלת שלו כך שהיריב מחליט כי העלות של פעולתו המשוערת אינה מצדיקה את התועלת שתופק ממנה.
Marquez, "Space Deterrence" at p. 10, citing G. Schaub, Jr., "Deterrence, Compellence and Prospect Theory" *Political Psychology* 25, no. 3 (2004), pp. 389-411.

48 Marquez, "Space Deterrence," p. 10.

49 לדוגמה, ראו:
Yasmin Tadjdeh, "U.S. Military Overestimates Value of Offensive Weapons Cyberweapons, Expert Says," *National Defense*, September 13, 2012, citing Martin Libicki, senior management scientist at RAND Corp, http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=887.

50 F. Hare, "The Significance of Attribution to Cyberspace Coercion: A Political Perspective." Paper presented at the *Cyber Conflict (CYCON), 2012 4th International Conference* on June 5-8, 2012.

51 Federal News Radio, "DoD Hammering out Rules of Cyberspace," October 21, 2011, http://www.federalnewsradio.com/?nid=398&sid=2602063; and Ellen Nakashima, "Pentagon to Fast-track Cyber Weapons Acquisition," *Washington Post*, April 9, 2012, http://www.washingtonpost.com/world/national-security/pentagon-to-fast-track-cyberweapons-acquisition/2012/04/09/gIQAuwb76S_print.html.

52 Lolita C. Baldor, "Pentagon to Publish Strategy for Cyberspace War," *Navy Times,* July 14, 2011, http://www.navytimes.com/news/2011/07/ap-pentagon-publish-strategy-cyberspace-war-071411/;
ראו גם:
"A Conversation on Cyber Strategy with General James E. Cartwright," *Homeland Security Policy Institute (HSPI) Capstone Series on Cyber Strategy*, May 14, 2012, http://www.gwumc.edu/hspi/events/cartwrightCS501.cfm.

53 Frank Cilluffo and Andrew Robinson, "Analysis: While Congress Dithers, Cyber Threats Grow Greater," *Nextgov*, July 24, 2012, http://www.nextgov.com/cybersecurity/2012/07/while-congress-dithers-cyber-threats-grow-greater/56968/.

54 Cilluffo, *AFPC Defense Dossier*.

על מלחמה גרעינית: הרתעה, הסלמה ובקרה

סטיבן ג' סימבלה

מבוא

במהלך המלחמה הקרה, ובייחוד בשנות השמונים של המאה ה־20, הושקעו מאמצים ניכרים בקרב הקהילה האקדמית ובחוגים של קובעי מדיניות בחקר השאלה, כיצד עלולה להסתיים מלחמה גרעינית.[1] ארסנל הנשק הגדול שהחזיקו הן ארצות־הברית והן ברית־המועצות, מגמות שרווחו בחשיבה הצבאית בשתי המעצמות וכן הספקות והחששות סביב מדיניותן – כל אלה מנעו את פתרון השאלה לפני תום עידן המלחמה הקרה. השאלה כיצד לנהל מלחמה גרעינית באמצעות כלים של קביעת מדיניות ואסטרטגיה עקבית זכתה להתייחסות מועטה בפולמוס על תפקיד הנשק הגרעיני, על הרצף בין שתי אסכולות מנוגדות – "הרתעה בלבד" ו"שימוש בפועל".

יש לפתוח עתה מחדש את העיסוק בסוגיית סיומה של מלחמה גרעינית, עקב השינוי שחל באופיו של האיום הגרעיני – אין מדובר עוד בכמות הטילים, אלא בעצם זהותו של המחזיק נשק גרעיני והמטרה שלשמה הוא מייעד את השימוש בנשק זה. ההיבטים הטכנולוגיים והפוליטיים של מערכת השיקולים הרלוונטית לפרוץ מלחמה גרעינית ולסיומה שונים במובהק מאלה של ימי המלחמה הקרה. תהיה זו טרגדיה גדולה אם ביום שאחרי השימוש הראשון בנשק גרעיני בזמן מלחמה מאז נגסאקי, ארצות־הברית ומעצמות אחרות יתגלו כמי שלא הקדישו חשיבה מעמיקה לשאלה כיצד לקטוע עימות גרעיני בעודו באיבו. בניגוד ל'מלחמת גוג ומגוג' ההיפותטית בין ארצות־הברית לברית־המועצות במאה הקודמת, שכלל לא התממשה, במאה הנוכחית עלולות להתרחש מלחמות גרעיניות, אמנם לא בהיקף כלל עולמי, אך אף על פי כן הרסניות ביותר. לחלק מעימותים אלה יש פוטנציאל להתפשט למלחמה נרחבת – לדוגמה, בין הודו לפקיסטן – שעלולה לכלול מדינות גרעיניות נוספות באזור האגן המזרחי של אסיה. פקיסטן עשויה

סטיבן ג' סימבלה הוא פרופסור למדעי המדינה באוניברסיטה של מדינת פנסילבניה

לזכות בתמיכתה של סין, והודו – בזו של רוסיה ו/או ארצות־הברית, תחילה באמצעים של הרחבת ההרתעה אך לאחר מכן באמצעות מתקפות ממשיות, קונבנציונליות או גרעיניות. כמו כן, למרות שהסבירות של מתקפה גרעינית מכוונת מצד ארצות־הברית או נאט"ו כלפי רוסיה, או להיפך, היא מן הסתם נמוכה מאוד עד אפסית, אין לשלול את האפשרות שתפרוץ מלחמה גרעינית לא־מכוונת, או שתחול הסלמה עד כדי שימוש לראשונה בגרעין באירופה, וזאת על פי הדוקטרינה הצבאית המוצהרת של רוסיה ותוכניות המגירה של נאט"ו.[2]

מטרתו של מחקר זה אינה בניית תרחישים ספציפיים של סיום מלחמות, או בחינת נושאים חשובים כמו אסטרטגיות משא־ומתן או פיקוח ובקרה על הפסקות אש במלחמה גרעינית. במוקד המחקר עומד מבט רחב יותר, שעיקרו ההקשר הצבאי־מדיני של ניהול משברי גרעין ופעולות צבאיות פוסט־משבריות, לרבות בקרת הסלמה וסיום המלחמה. ליתר דיוק, ההתמודדות עם חוסר יכולתן של מדינות להביא לסיום מלחמה גרעינית מחייבת תחילה את הסכמתם של אסטרטגים צבאיים וקובעי מדיניות על כך שסיומה של מלחמה גרעינית הוא בר־השגה ושיש לשאוף אליו. קיימים מכשולים ניכרים בדרך להסכמה זו, בראשם התנגדות אינטלקטואלית של רבים, המתבססת על ההנחה שיכולת ההרתעה נפגעת מן הנכונות להיערך היטב לקראת כישלון אפשרי של זו.

הרתעה: עד כמה היא אמינה?

השימוש בנשק גרעיני מצד מדינה כלשהי נגד מדינה אחרת לראשונה מאז 1945 עתיד להביא לשינוי טקטוני בתחזיותיהם של קובעי מדיניות ואסטרטגים צבאיים ברחבי העולם. הטאבו הגרעיני שלכאורה ריסן את ידיהם של מקבלי ההחלטות בתחום ניהול המשברים בתקופת המלחמה הקרה, ועד סוף המאה ה־20, יתנפץ לרסיסים. במקומו יישארו חוסר ודאות והציפייה המתבקשת לכך ששימוש ראשוני יגרור אחריו מתקפת תגובה והסלמה נוספת. מובן שמדינה גרעינית יכולה לבחור לתקוף או לגרור לעימות גם מדינה לא־גרעינית, בעיקר תוך שימוש בנשק קונבנציונלי, אך כאשר צִלו של כוחה הגרעיני משמש לה מכפיל כוח. ניסיון התגרות מעין זה עלול לגרור גינוי מצד הקהילה הבינלאומית ותגובות מבעלות־בריתה של המדינה המותקפת, לרבות מצד מדינות בעלות נשק גרעיני. העימותים שאינם ניתנים לחיזוי המתגלעים מעת לעת בין צפון־קוריאה לדרום־קוריאה, כולל הטבעת ספינת המלחמה הדרום־קוריאנית במרס 2010, מהווים דוגמה להתגרויות באמצעים מדיניים ושימוש בכוח צבאי קונבנציונלי, שנתמך בהרתעה המשתמעת מיכולתה הגרעינית המוגבלת של צפון־קוריאה.

מקובל לחשוב כי היתכנותה של מלחמה גרעינית קשורה באופן ניכר – אם כי קשה לאמוד אותו במדויק – למספר המדינות שברשותן נשק גרעיני, ולמידת

הידידותיות או העוינות שמאפיינת את היחסים בין מדינות אלה. לרוע המזל, מספרן הגובר של המדינות המצטרפות למועדון בעלות הארסנל הגרעיני מעיב על השלום במאה ה־21. בעקבות הצהרתה הרשמית של צפון־קוריאה על כך שהיא מחזיקה ביכולת לייצור נשק גרעיני, נערכה סדרת מגעים בינלאומיים ספורדיים במעמד ששת הצדדים (ארצות־הברית, רוסיה, סין, יפן, דרום־קוריאה וצפון־קוריאה), שמטרתם הייתה קידום משא־ומתן על הקפאה, ולאחר מכן פירוק תוכנית הגרעין הצבאית של המדינה. מאמצים אלה התגלו כמתסכלים במיוחד עבור אותן מדינות שנשאו ונתנו עמה, וחוסר הבהירות לגבי כוונותיה של צפון־קוריאה רק התגבר עם מותו של מנהיג־העל, קים־ג'ונג־איל, בינואר 2012 והעברת שרביט השלטון לבנו, קים ג'ונג־און, שאישיותו ודמותו הפוליטית לוטות בערפל.

לצד כניסתה של צפון־קוריאה למועדון הגרעין, גם איראן נחשדת כבעלת כוונות רציניות לממש את מעגל הדלק הגרעיני שלה בצורת נשק. ארצות־הברית ומדינות מובילות באיחוד האירופי, לרבות בריטניה, צרפת וגרמניה, הפעילו לחץ כלכלי ודיפלומטי על איראן מאז 2004, בניסיון לשכנע את טהראן שלא לחצות הלכה למעשה את סף היכולת לייצור נשק גרעיני, או להתייצב על רף שיוסכם מראש. בנוסף, נערכו שיחות בין איראן לבין מדינות ה־P5 (החברות הקבועות במועצת הביטחון של האו"ם: ארצות־הברית, רוסיה, בריטניה צרפת וסין) וכן גרמניה, במטרה ליצור מחויבות דיפלומטית מתמשכת – לצד הפעלת לחץ על איראן מצד הסוכנות הבינלאומית לאנרגיה אטומית (סבא"א) והאיחוד האירופי – להפגין יתר שקיפות בנושא שאיפותיה בתחום הגרעין והתשתית שהיא בונה לשם כך. חלק מהבעיה שניצבה בפני מדינות ה־P5+1 הייתה לקבוע בדיוק "עם מי" הן מדברות, כלומר עם אילו גורמים מקומיים הן מנהלות משא־ומתן: נראה היה שבקרב האליטות הצבאיות והפוליטיות באיראן, ובכללן משמרות המהפכה והמנהיגות הדתית במדינה, הפגינו גורמים שונים עמדות נחרצות וגמישות לסירוגין, שיצרו קליידוסקופ משתנה של כוונות ונקודות מוצא למשא־ומתן. תרשים 1 מסכם את הערכות המומחים להסתברות של דרכי פעולה שונות, שאותן עלולה איראן לנקוט על מנת להשיג חומר נפץ גרעיני.

נכון לנובמבר 2012, לא צלחו מנופי השכנוע הדיפלומטיים ולא תמריצים שונים, כלכליים ומדיניים, שהופעלו על איראן או על צפון־קוריאה, במטרה לגרום להן לנטוש את תוכניות הגרעין שלהן.[3] במקרה זה, היה על המעצמות והארגונים הבינלאומיים להחליט אילו צעדים נוספים באפשרותם לנקוט, למעט הכרזת מלחמה. אפשרות אחת הייתה להניח את סוגיית ההתגרענות של איראן או צפון־קוריאה לפתחה של מועצת הביטחון של האו"ם. במקרה כזה הייתה סין צפויה למנוע כל סנקציה משמעותית כלפי צפון־קוריאה. סיכויים גבוהים יותר נודעו למהלכים רב־צדדיים (שיכללו את ארצות־הברית ואירופה) או בינלאומיים

תרשים 1. רמות הסבירות לכך שאיראן תשיג חומר נפץ גרעיני, בדרכי פעולה שונות

שיטה	סיכוי ב־2013	סיכוי ב־2014–2015
זינוק חד באתרי הצנטריפוגות המוצהרים לאורניום מועשר בדרגה גבוהה (HEU) בעזרת אורניום מועשר בדרגה נמוכה (LEU) המצוי בפיקוח		
(א) נתנז	נמוך	נמוך
(ב) פורדו	נמוך עד בינוני	נמוך עד בינוני
זינוק חד באתר צנטריפוגות סודי ולא מוצהר העושה שימוש במלאי אורניום מועשר בדרגה נמוכה המצוי בפיקוח	נמוך עד בינוני	בינוני
ייצור אורניום מועשר בדרגה גבוהה בכפוף לפיקוח במתקני צנטריפוגות מוצהרים	נמוך	בינוני
תוכנית צנטריפוגות חשאית הפועלת במקביל	נמוך	בינוני
ייצור חשאי של אורניום מועשר בדרגה גבוהה באתרים מוצהרים ובפיקוח	נמוך	נמוך
כור באראכ ומתקן עיבוד חשאי ולא מוצהר (הכור צפוי להיות מבצעי ב־2014)	–	נמוך
העשרה בלייזר להפקת אורניום מועשר בדרגה גבוהה	נמוך	נמוך
השגת חומר בקיע באמצעים בלתי–חוקיים לשימוש בנשק גרעיני	נמוך	נמוך
פרישה כחוק מהאמנה למניעת תפוצת נשק גרעיני (NPT) וייצור נשק לאחר מכן	נמוך	נמוך עד בינוני

מקורות:

David Albright, Paul Brannan, Andrea Stricker, Christina Walrond and Houston Wood, "Preventing Iran from Getting Nuclear Weapons: Constraining its Future Nuclear Options," Institute for Science and International Security, March 5, 2012, http://www.isis-online.org/uploads/isis-reports/documents/USIP_Template_5March2012-1.pdf, cited in Anthony H. Cordesman and Alexander Wilner, *Iran and the Gulf Military Balance – II: The Missile and Nuclear Dimensions*, Working Draft, Major Revision 5 (Washington, D.C.: Center for Strategic and International Studies, July 16, 2012), p. 40, www.csis.org/burke/reports. See also David E. Sanger and William J. Broad, "Iran Said to Nearly Finish Nuclear Enrichment Plant," *New York Times*, October 25, 2012,
http://www.nytimes.com/2012/10/26/world/middleeast/iran-said-to-complete-nuclear-enrichment-plant.html?_r=0

(מצד מועצת הביטחון) כלפי איראן. סדרה של החלטות שקיבל האו"ם מאז 2006 הגבירו את הלחץ על איראן לציית לפקחים הבינלאומיים על בקרת נשק, להגביל את המסחר שלה בחומרים ובציוד הקשורים לשימוש צבאי או גרעיני, להקפיא את פעילות ההעשרה והעיבוד מחדש (של אורניום) ולהגביל את פעילות משמרות המהפכה וכן את זו של גורמים אחרים החשודים כמעורבים בפעילויות האסורות בחוק. בינואר 2012 החליטו מדינות האיחוד האירופי על הטלת אמברגו נפט על איראן, החל מיולי של אותה שנה, ועל הקפאת נכסי הבנק האיראני המרכזי. במרס 2012, בנקים איראניים שהפרו את הסנקציות שהטיל האו"ם נותקו ממערכת SWIFT – מערכת גלובלית לתיאום עסקאות פיננסיות בינלאומיות. מספר מדינות הטילו סנקציות בילטרליות על איראן, בייחוד ארצות־הברית, שהטילה אמברגו כלכלי כמעט מוחלט ואיסור על מכירת נשק, לרבות סנקציות על מוסדות פיננסיים איראניים ועל חברות המנהלות עסקים עם המדינה.[4]

למרות סנקציות אלה ואחרות, צעידתה של איראן על סִפה של יכולת ייצור נשק גרעיני נראית בלתי־נמנעת, אלא אם כן תחול פריצת דרך חסרת־תקדים במאמצים הדיפלומטיים או הצבאיים. מחקר מטעם המכון למדע וביטחון בינלאומי ציין כי:

> "אם איראן אינה מוכנה להגיע לפשרות לקראת משא־ומתן על פתרון לטווח ארוך, החלופה היחידה שתיוותר היא אסטרטגיה של הצבת קשיים ומגבלות בפני מאמציה של איראן להשיג יכולות של נשק גרעיני ואת הנשק עצמו. תישמר החשיבות של הגעה להסכמה באשר לצעדים שינקטו בטווח הקצר, כגון הצבת תקרות לרמות העשרה ופריסת צנטריפוגות. אולם כיוון הפעולה העיקרי יכתיב ריכוז המאמץ בעיכובה, סיכולה והסטתה מן המסלול של החתירה האיראנית ליכולות גרעיניות".[5]

בעיית ההכלה של תפוצת נשק בקרב מדינות וארגונים סוררים היא למעשה כפולה. מצדה האחד היא עוסקת בגישה שיש לנקוט כלפי מדינות נוספות המשיגות יכולות גרעיניות. צדה השני הוא החשש הממשי שמדינות גרעין סוררות עלולות להעביר טכנולוגיות גרעין וידע בתחום לגורמים שאינם מדינתיים, לרבות ארגוני טרור. ידוע לדוגמה, שעוד לפני פיגועי ה־11 בספטמבר ניסה ארגון אל־קאעדה להשיג חומר גרעיני מועשר ברמת שימוש כנשק. באופן אירוני, ארצות־הברית ומדינות ששטחיהן נרחבים באופן יחסי הפכו פגיעות יותר לסוגים מסוימים של מתקפות בנשק להשמדה המונית, כולל נשק כימי, ביולוגי, רדיולוגי או גרעיני, כיוון שלמדינות גדולות יש יעדים רבים יותר להגן עליהם, וכן תשתית אזרחית הפזורה על פני שטחים נרחבים יותר.

יהיו אופטימיסטים שיטענו לגבי ההשלכות האפשריות של המשך תפוצתו של נשק גרעיני בקרב מדינות שונות, כי ההרתעה תפעל בעתיד כשם שעבדה כביכול במהלך המלחמה הקרה. ראייה זו את מצב הדברים מתבססת על כך שבדיעבד חלפה המלחמה הקרה מבלי שיפרוץ, במכוון או בשגגה, עימות גרעיני בין ארצות־

הברית־המועצות – דבר שהיה מוביל לאסון בקנה־מידה עולמי. מי שחיו בשנות המלחמה הקרה, על נקודות המשבר הרבות שהיו בה, ובייחוד משבר הטילים בקובה, לא ראו בהכרח את הצלחתה של ההרתעה כדבר מובן אליו. יתרה מכך, גם אם ההרתעה במלחמה הקרה הייתה מובטחת, כפי שמניחים האופטימיסטים, הרי הרתעת ארגוני טרור וגורמים לא־מדינתיים אחרים מהיגררות להרפתקנות גרעינית היא כבר משימה שונה לחלוטין.

מאמר זה אינו עוסק בהרתעת גורמים לא־מדינתיים, בהנחה ש"הרתעה" במובנה הרחב ביותר לא עוסקת במניעת מתקפות טרור, כלל ועיקר.[6] די באתגר שמציבה השגת הרתעה כלפי מדינות סוררות או אחרות בפני קובעי המדיניות והאסטרטגים במערב. פקידי ממשל ואחרים החוששים מהתנהגותם של אותם גורמים סוררים מסכימים על כך שעל פי רוב, גורמים אלה מצויים מחוץ לתחום ההשפעה של אסטרטגיית הרתעה רציונלית. למצער, גורמים אלה עלולים שלא להיכנע בפני הפעלת מרות צבאית מצד ארצות־הברית או בפני כל מודל מערבי של הרתעה רציונלית.

ההיגיון של מודל ההרתעה האמריקאי מדגיש את שיקולי העלות־תועלת של חלופות שונות. מקבלי ההחלטות בוחרים בחלופה שעלותה הצפויה היא הנמוכה ביותר ובעלת התועלת הפוטנציאלית הגבוהה ביותר, בהשוואה לשאר החלופות הקיימות. לפיכך, תיאוריית ההרתעה מהווה היבט אחד של תיאוריית הבחירה הציבורית, ובשל כך היא תקפה רק בתוך מסגרת התייחסות מצומצמת או "רציונליות מוגבלת". במסגרת זו, הנחת היסוד היא כי לכל אחד מהצדדים הנְצים יש מידע מדויק על מטרותיו של האחר, על החלופות העומדות לרשותו ועל משקלם של היתרונות והחסרונות שהוא מייחס לאפשרויות השונות.

נקודות התורפה של מודל ניתוח זה – בבואנו ליישמו בעולם האמיתי של ניהול משברי גרעין – הן כבדות־משקל והרות־גורל.[7] הדבר אינו נובע בהכרח מכך שתיאוריית ההרתעה נוטה להיות מופשטת יותר, בהשוואה לגישות אחרות לניהול משברים. האתגר מצוי בהחלת הלוגיקה המופשטת על רבבות מצבים שונים ונפרדים. ישנה חשיבות לנסיבות הספציפיות של כל משבר בהבנת אופן התדרדרותו לכדי מלחמה. משעה שנכשלה לכאורה ההרתעה ופורצת מלחמה, מהלך הקרבות משפיע על החלופות הנותרות לקובעי המדיניות ולמנהיגים השואפים לעצור את המלחמה מוקדם ככל האפשר.

תהיה זו טעות להניח שכישלון ההרתעה מביא בהכרח למלחמה. ייתכן שאחד הצדדים היה נחוש בדעתו לתקוף ויהי מה. לפיכך, כדי לקבוע האם ומתי אויב פוטנציאלי עלול לתקוף, ידיעת המניעים ודרכי החשיבה שלו חשובה לא פחות מהכרת יכולותיו. בדברי הימים ידוע על מלחמות רבות שהחלו בהנחות מסוימות ביחס לכוונות האויב ויכולותיו, אשר הופרכו בהמשך במבחן הקרב. לא אחת פתח

הצד התוקף במלחמה נגד מדינה שכוחה הצבאי רב משלו. במרבית המקרים הללו הטיל התוקף ספק בנחישותו של הצד המתגונן. במקרים אחרים כשלו מדינות באופן הדדי בהבנתן את נטייתו של הצד השני למלחמה, משום שלא הבינו לאשורם היבטים חיוניים בתרבות האסטרטגית, בסדר הקדימויות של התכנון הצבאי או ב"אמנות המלחמה" שלו. יש הרואים במלחמות שעליהן הכריזו מנהיגים ששגו בהבנת אחד או יותר מגורמים אלה מלחמות שפרצו "בטעות" או "שלא בכוונה" (לרוב מדובר בחוקרי מדע המדינה המעדיפים מושגים כאלה, ופחות בהיסטוריונים הנוטים להפגין יותר ספקנות).

במהלך המלחמה הקרה הייתה ההרתעה מצויה בסכנה מתמדת של מתיחת גבולותיה יתר על המידה, לפחות במסגרת השיח האקדמי האמריקאי וניתוחי מדיניות ציבורית. מבחינתם של אנליסטים וקובעי מדיניות מסוימים היא שימשה מעין "קמע" שבא על חשבון הסתמכות על נתונים ממשיים וחשיבה מעמיקה. היו גם מי שראו לעיתים בהרתעה תחליף למדיניות במקום לאסטרטגיה צבאית (בעיות שונות, אם כי קשורות). 'תיאוריית הדומינו' ששימשה את ארצות־הברית כדי להצדיק את ההסלמה הצבאית בוויטנאם היא דוגמה אחת להרתעה (ותאומתה, האמינות) שנמתחה מעבר לקווי השבר הגיאוגרפיים והרעיוניים, אשר הפרידו בין מלחמה באירופה לבין המלחמה באסיה.

מוקדם מדי להצהיר שמדינות השואפות להשיג נשק גרעיני, ובכלל זה גם מדינות סוררות, מצויות "מעבר לתחום ההרתעה" במובן של הרתעה קיומית. אך יחד עם זאת, אין ספק שההרתעה תפעל במאה ה־21 באופן אחר בהשוואה לעידן המלחמה הקרה. אחת הסיבות לכך קשורה לתפוצתו של נשק גרעיני. במהלך המלחמה הקרה, אחזקתו של נשק גרעיני היוותה סימן היכר של המעצמות שלרוב היו מרוצות מהסטטוס־קוו הגיאופוליטי. מצד אחר, מדינות בעלות שאיפות גרעיניות או כאלו שכבר תהיה להן היכולת הזו עלולות לנקוט בעתיד מדיניות בינלאומית שתקרא תיגר על הסדר הקיים. למעשה, עצם המונחים מדינה "סוררת" (rogue) או "מדינה מדאיגה" (state of concern) מצביעים על כך: הסורר נתפס ככזה רק בעיניהם של אלה המבקשים לשמר את המערכת הקיימת על ערכיה. אלה המבקשים לשנות סדרי עולם עלולים לראות בהם גיבורים. במאה ה־18 נחשבו המהפכנים הצרפתיים והאמריקאיים סוררים מול הסדר הקיים: כיום, המדינות שקמו בעקבות פעולותיהם הן חלק מסדר זה.

שאלה נוספת שעולה בנוגע להרתעה היא האם ביכולתה להשפיע על ראשי מדינה, מנהיגים צבאיים או ארגוני טרור בעלי מניעים אפוקליפטיים, או בלתי־רציונליים בכל צורה אחרת. כאן מתבקשת, כמובן, השאלה: מהו מניע רציונלי?[8] די בכך אם נאמר שמה שנחשב במדינה מסוימת כרציונליות עלול להיתפס במדינה אחרת כאי־רציונליות – אך אין מדובר כאן בהבחנה קלינית. מנהיגים בעלי נטיות

קליניות עשויים בכל זאת לקבל בדעה צלולה החלטות בשם המדינות שלהם בעיתות משבר, ואכן כך היה בפעמים רבות. רציונליות עניינה ראיית הקשר הלוגי בין מטרות ובין האמצעים להשגתן: האם דרך הפעולה שנוקטת המדינה במצב נתון מבטיחה את הצלחתה או מצמצמת את סיכוייה להיכשל?

במשבר בין שתי מדינות גרעין, הקושי נובע מכך ששני הצדדים תלויים באופן הדדי במערכת קבלת ההחלטות או "ברציונליות" שלהם. כל צד נוקט סדרת צעדים – שעשויים להיתפס כהגיוניים יותר או פחות – בתגובה לאלה שנקט יריבו. תלות הדדית זו של צעדים ומניעים היא שהופכת משברים גרעיניים ואחרים לקשים כל כך לניהול.[9] אפשר לדמיין משחק שחמט דו־ממדי כשהשחקנים מכוסי עיניים, וכל צד מוגבל למספר מצומצם של טעויות (לדוגמה, שני מהלכים שגויים), בטרם יתפוצץ הלוח לרסיסים, ועמו השחקנים עצמם. דוגמה זו אינה כה מופרכת: נשיא ארצות־הברית, ג'ון פ. קנדי, מנהיג ברית המועצות דאז, ניקיטה חרושצ'וב, שיחקו משחק דומה במהלך משבר הטילים בקובה.

עקרונות בבקרת הסלמה

תיאוריות של בקרת הסלמה כוללות כמה הצעות מפתח בסוגיית סיומה של מלחמה גרעינית. כולן שנויות במחלוקת, אך כל אחת מהן אפשרית בפני עצמה. ראשית, אפילו מלחמה גרעינית, הרסנית ככל שתהיה, כרוכה במטרות פוליטיות, לפחות בתחילתה. שנית, ניתן להניח שחרף ההבדלים התרבותיים והלאומיים ביניהם, מדינות ומנהיגיהן יכירו בכמה "כללי משחק" בנוגע לאופיין של מלחמות גרעיניות והדרך לסיימן. שלישית, למרות המגבלות הנגזרות מאילוצי הזמן ומאופיו של תהליך התכנון הצבאי ביחס לאפשרות להביא לסיום המלחמה באמצעים של בקרת הסלמה, אין מניעה בפועל להצליח בכך.[10] ביחס להקשר המקובל של נושא זה בראי המלחמה הקרה, טען פול בראקן (Bracken) כי: "ההנחה של עמידות בפני סדי הזמן והתכנון נשענת על הוודאות שבזמן משבר גרעיני, מנהיגה של כל מדינה ייקח את המושכות לידיו וידלג מעל משוכות בירוקרטיות, כגון עיכובים וזניחת אחריות".[11]

אפשרות הבאתה של מלחמה גרעינית, שכבר החלה, לכלל סיום, מרמזת על כך שהרתעה ישימה באותה מידה הן לצורך הגבלת מלחמה והן למניעתה. מלחמה גרעינית היא תוצאתו של כישלון הרתעה שהתרחש. עם זאת, מצב גרוע יותר הוא עימות שבו חילופי האש בין הצדדים הנצים נמשכים עד שהם מכלים את מאגרי התחמושת שלהם, או עד חורבנן של כל הערים הגדולות. הושבת הצדדים סביב שולחן המשא־ומתן לאחר ההלם של מערכה גרעינית לא תהיה משימה קלה. למעט במקרים שבהם החלה המלחמה באופן לא־מכוון, כתוצאה משיגור בטעות או במקרה שקצין צבא חרג מסמכותו, למשל, יעמדו על הפרק מחלוקות סביב סוגיות

מדיניות מרכזיות. נוסף על כך, זעמם של אלה ששרדו במלחמה, לנוכח תוצאותיה של מתקפה גרעינית, צפוי להציב אתגר מנהיגותי לממשלותיהם. תביעות הנקם של השורדים או דרישתם להנחתת מכת תגובה עלולות לגבור על מאמציהם של מנהיגים להגיע להפסקת אש או להסכמי כניעה.

לסיומה של מלחמה גרעינית, כמו בכל מלחמה, יש היבטים טקטיים־צבאיים לצד היבטים אסטרטגיים־פוליטיים.[12] מטבע הדברים נודעת, כמובן, חשיבות למצב הטקטי בשדה הקרב. לאחר שבוצעו מתקפות הגרעין הראשונות, בכל צד עשויים להימצא כוחות ששרדו. הכוחות השורדים הם נכסי מיקוח שיכולים לשמש לצורכי משא־ומתן על הפסקת אש או הסכם שלום. גם כוחות מועטים בלבד בכל צד יכולים לאיים בגרימת הרס חברתי רחב־היקף לצד השני, ומנהיגיו עשויים להעדיף להידבר במקום להמשיך במלחמה. יחד עם זאת, בכאוס השורר בעקבות מלחמה גרעינית, גם כשמדובר במלחמה אזורית "קטנה" במונחים של המלחמה הקרה, עלולים מנהיגים ויועציהם הצבאיים שלא לקבל מידע אמין על מצב כוחות האויב ומערכות השליטה והבקרה שלו.

מערכות שליטה ובקרה מציגות חריגה בפני מתכננים העשויים לרצות להשאיר פתח לאפשרות של יצירת הרתעה במהלך המלחמה, ואף להביא לסיומה. מחד גיסא, במונחי החשיבה הצבאית המסורתית שמבוססת על ניסיון בלוחמה קונבנציונלית, יהיה זה אך הגיוני להתקיף את מערכות השליטה והבקרה ואת מערכות התקשורת. זוהי דרך יעילה להרוס את התיאום והלכידות הצבאית של היריב. תקיפת "מערכת העצבים המרכזית" ו"המוח" של האויב, כפי שנעשה במהלך מבצע "סופה במדבר", מהווה מכפיל כוח חשוב שיכול להביא לניצחון במלחמה בפרק זמן סביר, ולמנוע אבדות בנפש לשני הצדדים גם יחד.

אולם במלחמה גרעינית, הרס מערכות השליטה והבקרה של האויב, צבאיות ומדיניות כאחת, יוביל כמעט בוודאות להחמרתה של בעיית סיום המלחמה, בשתי רמות. ברמה הטקטית – הרס מערכות בקרה צבאיות יגרום נתק בין הכוחות האמונים על פעולת תגמול גרעינית לבין המפקדים שלהם. במקרה כזה, ברירת המחדל היא להמשיך בירי ובלחימה, אלא אם כן תתקבל הנחיה ישירה לחדול מכך. אך הפקודה לנצור את האש עלולה כלל לא להגיע למפקדים הרלוונטיים בשטח המופקדים על אחזקת הנשק הגרעיני, ולא לאלה המורשים לאשר את שיגורו (ייתכן שאלה יהיו אותם אנשים, אך לא בהכרח). לפיכך, הגורמים ה"מנותקים" בשרשרת הפיקוד הצבאית הגרעינית עלולים שלא לשמוע, או לסרב לשמוע, את הפקודה המורה על הפסקת אש.[13]

הרס שדרת הפיקוד המדינית של היריב עלול לשתק את ההנהגה האזרחית שלו ולהפוך לבלתי־אפשרית את הבטחתה של שליטה יציבה בכוחות המזוינים בידי הנשיא, ראש הממשלה או חברי קבינט אחרים.[14] חִשבו לדוגמה על התקפה

אירנית על ישראל, או של פקיסטן על הודו, "המצליחה" לפגוע בלב המנהיגות הפוליטית בצד המותקף. השליטה בפועל בכוחות המזוינים של המדינות המותקפות תועבר כמעט בוודאות ישירות לצבא ולזרועות הביטחון האחרות. במקרה כזה יהיו המנהיגים הפוליטיים ששרדו – בתל־אביב או בהודו – שבויים, גם אם באופן זמני בלבד, ברצף של תרחישים משתנים תדיר ונתונים למרותם של צווים צבאיים. זמן רב למדי צפוי לחלוף, ודרושה לפחות מראית־עין של הפסקת אש זמנית, בטרם ניתן יהיה לבסס מחדש יחסי עבודה קרובים ל"נורמליים" בין ראשי המדינה לכוחות הצבא.

קשה להעריך את יכולת קיומן של מערכות שליטה ובקרה בלחציה של מתקפה גרעינית, או באמצעות נשק להשמדה המונית מסוג אחר, בשל היעדר מידע אמין מן הרשומות הציבוריות. ניתן להניח, לדוגמה, שלכל מדינה או ממשלה יש הסדרים רשמיים וכתובים להאצלת סמכויות מדיניות ולהעברת השליטה על כוחות הצבא בעתות משבר ומלחמה – לכל תרחיש של עימות קונבנציונלי או גרעיני, במידת הצורך. עם זאת ייתכן שהדבר אינו נכון במקרים של מדינות השואפות ליכולת גרעינית, ומדינות שהגיעו ליכולת זו לא מכבר. גם אם קיימים פרוטוקולים כתובים, הדבר אינו מבטיח היצמדות אליהם עם פרוץ המלחמה, או את מידת התאמתם למציאות שתשרור במקרה כזה. כמו כן, האצלת סמכויות מדיניות והעברת אחריות על השליטה והבקרה על כוחות הצבא עשויות לסתור זו את זו בדרכים משמעותיות. קיים גם חוסר ודאות באשר לאופן שבו מערכות שליטה ובקרה צבאיות יפעלו בזמן משבר גרעיני או מלחמה, תחת מתקפת סייבר מבצעית או אסטרטגית. לדוגמה, מתקפות סייבר המקדימות או המלוות מתקפות ממשיות עלולות להקשות יותר את ניהולם של מבצעים צבאיים ואת ההערכה המדויקת של כוונות האויב, ועקב כך לחבל במגעים לסיום המלחמה.[15]

החוק האמריקאי לשמירת רציפות שלטונית ("Presidential Succession Act") וחקיקות שונות נוספות, כמו גם תכתיבים מכוח החוקה במדינה, מבהירים את ההליכים בשגרה ובחירום לפתרון השאלה "מי הממונה?" במקרה שהנשיא נהרג, או שנבצר ממנו לתפקד. שרשרת הפיקוד הצבאי, למרות שתחילתה במרכז הנשיאותי, אינה זהה לזו המדינית. בזמן מלחמה עוברת שרשרת הפיקוד הצבאי מהנשיא לשר ההגנה, ומשם לגורמים המנהליים או המרחביים המפקדים על ניהול המערכה (דרך קציני המטה הכללי). שיטה זו מבטיחה שגם אם מוקד קבלת ההחלטות הפוליטי משותק בעקבות מתקפת פתע, הפיקוד הצבאי המוסמך להורות על מכת תגובה יוכל לעשות זאת במועד. הסדרי שליטה ובקרה אלה פותחו דרך ניסוי וטעייה במהלך השנים הארוכות של המלחמה הקרה. מטרתם הייתה ועודנה מתן פתרון לדרישה שטבועה בה סתירה פנימית, שהכוחות לא יבצעו "לעולם"

ירי ללא הרשאה נאותה, ומנגד, יגיבו "תמיד" מיידית כאשר עליהם לבצע משימות המחייבות הרשאה.[16]

בשנותיו הראשונות של עידן הגרעין, קובעי מדיניות ומנהיגים צבאיים בארצות־הברית עשו מאמצים להגדיר כללים לפיקוח על נשק גרעיני בעתות שלום, ולניהול כוחות גרעין במהלך משבר ומלחמה. ממשל טרומן הפקיד תחילה את הנשק האטומי בידי סוכנות אזרחית. ניתן היה לשחרר את הנשק לצבא אך ורק מכוח צו נשיאותי. כיוון שהסדר זה הפך לבלתי־מעשי בעידן הטילים, נדרשו מערכות שיאפשרו העברת הנשק לידי הצבא בד בבד עם אחזקתו במיקום מאובטח, ומניעת האפשרות של שימוש לא־מורשה או שגוי בו. נוסף לכך, נדרש ניסוח פרוטוקולים מותאמים לסוגי הנשק השונים, על פי פלטפורמות השיגור שלהם – מן הים, מן האוויר או מהיבשה: כלי־טיס יכול להגיח לנקודת אל־כשל ("Fali Safe") ולהמתין לפקודת אישור לפני שימשיך בתקיפה. שיגור טילים, לעומת זאת, אינו ניתן לביטול: עצם שיגורם הוא החלטה שאין להשיבה לאחור על מלחמה.

בקרת הסלמה: אתגרים חדשים

אין זה מעניינו כאן לתאר בפרוטרוט את מהלכיהם של צבאות ארצות־הברית וברית־המועצות בזמן המלחמה הקרה, ובכלל זה את אופי הפעילות של מערכות השליטה והבקרה שלהם. עסקנו די בנושא זה כדי להדגיש את העובדה שרק כעבור זמן רב, וכתוצאה ממידה רבה של ניסוי וטעייה מצד מפעילים ואנליסטים, התבססו מערכות אלה כאמינות נגד פעולות חתרניות או שגויות, וכנתונות לפקודות מורשות. הלקחים שהופקו על ידי ארצות־הברית ורוסיה שלאחר המלחמה הקרה בנושא זה לא בהכרח הועברו לדורות הבאים של המדינות בעלות היכולת הגרעינית. אין זה ברור באיזו מידה חלק ממדינות הגרעין בהווה, וודאי העתידיות, מקבלות את הרעיון של הרתעה המבוססת על יכולת מכה שנייה, בניגוד למכה מקדימה. חלוקת התפקידים בדרגים הגבוהים ביותר של הפיקוד הצבאי והמדיני בנושא הזנקת כוחות הצבא או הפעלתם בזמן משבר או מלחמה אינה ברורה אף היא, ובייחוד ביחס למדינות כמו פקיסטן וצפון־קוריאה. טיבה של האצלת הסמכויות במדינות כגון הודו, פקיסטן, ישראל או צפון־קוריאה – באשר להפקדת נשק גרעיני בידי המפקדים בשטח ומתן ההרשאה לעשות בו שימוש – הינה בגדר סוד שמור ביותר.

משעה שנעשה שימוש בנשק גרעיני בדרום־מזרח אסיה, בצפון־מזרח אסיה או במזרח התיכון, האם מנהיגי המדינות באזור יהיו מסוגלים לנהל בקרה רציפה על החלטות הנוגעות להפעלת כוחות הצבא, הצבת מטרות לפעולה ונצירת האש? מדינות המחזיקות במאגרי נשק קטנים, בייחוד כאלו שאינן עמידות בפני מכה ראשונית, עלולות לפעול לפי הגיון של "להשתמש בהם או לאבד אותם",

ולנצל תוך זמן קצר את מלוא הארסנל הקיים שלהן. מצד אחר, אפילו מדינות קטנות עשויות לרצות לשמור על עתודות כדי להימנע במהלך המלחמה ממצב של סחטנות באמצעים גרעיניים בשלב שלאחר המתקפה. כוחות שיוריים ששרדו בהיקף מצומצם, למשל טילים טקטיים או כלי־טיס עם יכולת גרעינית בטווח מוגבל, עשויים להוות את ההבדל בין כניעה ללא תנאי לבין משא־ומתן לשלום. לפיכך, להבטחת הישרדותו של כוח גרעיני שיורי יש שני היבטים: כחלק מן האיום המוחשי של הסלמה נוספת, או במסגרת קיום שיחות להשגת רגיעה ולסיום העימות. מלחמה בין מדינות המחזיקות בנשק גרעיני הנמשכת עד אשר כל הצדדים הלוחמים מנצלים עד תום את ארסנל הנשק הגרעיני שברשותם תהיה כישלון פוליטי, ללא קשר להישגיה הצבאיים. מלחמה כזו מנוגדת לחלוטין למשנתו של קלאוזביץ' (Clausewitz, מחבר "עקרונות המלחמה"), והופכת את המערכה הגרעינית ואת ההשמדה ההמונית למטרות פסאודו־פוליטיות בפני עצמן.

תנאי מקדים לפתיחה במשא־ומתן לאחר חציית סף היכולת לייצור נשק גרעיני על ידי מדינה הוא שלמנהיגים בשני הצדדים תהיה שליטה איתנה על כוחות הגרעין שלהם – כך במקרה של הודו ופקיסטן, או לגבי ישראל ואיראן. לשם כך, יהיה על המנהיגים לשרוד במתקפות הראשונות, לקיים ערוץ תקשורת עם כוחות הגרעין שלהם ולאכוף ריסון בהפעלת האש ואף את נצירתה. אפשר שצעדים אלה להחשת המשא־ומתן לא יהיו אפשריים. קיימת סכנה של הפרת פקודה מצד קציני צבא שביכולתם להורות על הפעלת נשק גרעיני, אשר נכחו במו עיניהם בהרס חסר־התקדים במדינתם, ועלולים להתנגד להפסקת האש ולתבוע נקמה והשמדה מוחלטת של האויב. משהואצלה הסמכות לשיגור גרעיני מידי מנהיגי המדינה וקציני הצבא הבכירים אל הדרגים בשטח, הסגת הכוחות לאחור ו"החזרת השד לבקבוק" תחייב את מפקדי המערכה לדבוק במחויבות המקצועית שלהם ולפעול בהתאם לשרשרת הפיקוד הצבאי – ולא על פי הרצונות והמניעים האישיים שלהם. יהיו שיוכלו לעשות זאת, ויהיו כאלה שלא.

בעיה זו לא נפתרה לחלוטין גם בקרב מדינות גרעין "בשלות" יותר. בשנות התשעים נמצאה רוסיה במצוקה כלכלית קשה. ככל שדעכה המערכת הכלכלית במדינה, נזקקו כוחות הצבא הקונבנציונליים שלה נואשות לכסף ונאלצו להצר משמעותית את צעדיהם בנושאים מבצעיים. כתוצאה מכך הפכה רוסיה תלויה בעיקר בנשק הגרעיני שלה, ובייחוד בנשק לטווח ארוך, לצורכי הרתעה מפני מתקפה קונבנציונלית או גרעינית רחבת־היקף בשטחה הריבוני. מעמדה של רוסיה בשנות התשעים היה דומה לזה של נאט"ו במהלך המלחמה הקרה: נחיתות משוערת של כוחותיה הקונבנציונליים והישענות מוצהרת, בשל כך, על נשק גרעיני לצורך שידור עוצמה. בנוסף, לאחר נפילת ברית־המועצות התדרדר המצב של מערכות הבקרה וההתרעה נגד טילים שלה, לרבות רשתות הלוויין והמכ"ם

הקרקעי. מערך הנשק הגרעיני במדינה ומכוני המחקר המדעי בתחום נפגעו אף הם מהסחרור שעברה המערכת הכלכלית. ארצות־הברית גיבשה תוכניות סיוע צבאי לרוסיה בשנות התשעים, על מנת לשפר את יכולתה לטפל בנשק הגרעיני ובחומר המועשר, לרבות ניהול רישום מלאי מדויק, אחסון בטוח ופירוק.

מצב זה מהווה תפנית אירונית באירועים בהשוואה לימי המלחמה הקרה: ממשלת ארצות־הברית היא עתה "משקיעה" מרכזית בביטחון ובאבטחה של הגרעין ברוסיה. אך החשש בוושינגטון אינו עוד מהאפשרות למתקפה גרעינית מכוונת מצד רוסיה, אלא מאובדן שליטה צבאית או מדינית ברוסיה, אשר יותיר נשק ומשגרים גרעיניים בידי מפקדי צבא אזוריים, שעלולים להתגלות כבלתי־אמינים. נושא זה הוא כמעט בגדר טאבו בקרב חוגים דיפלומטיים רשמיים, אך ראוי לציין שעניין התפרקותה של רוסיה והיווצרות ישויות אזוריות מרובות מהווה מושא להשערות רבות בקרב הרוסים עצמם. על פי סקרי דעת קהל המבוצעים מעת לעת על ידי כלי התקשורת ברוסיה וחברות סקרים בנושא זה, כשליש מאזרחי רוסיה נוטים שלא להקל ראש באפשרות של התפרקות רוסיה הפוסט־סובייטית. השאלה במקרה כזה היא האם הפיצול יתרחש בצורה הדרגתית ותוך הסכמה פוליטית, או שמא יהיה כרוך במלחמת אזרחים.

הממשל הנוכחי, בהנהגת הנשיא ולדימיר פוטין, הבהיר את כוונתו להתנגד לכל תהליך של התפרקות אזורית או לכל חלוקה אחרת של רוסיה. התנגדותו הנחושה של פוטין להתקוממות ולטרור הצ'צ'ני, והלאו ("נייט") המוחלט שלו בתשובה לדרישה לעצמאות או לקיום אוטונומיה פוליטית באותו אזור שבמחלוקת היו עקביים ונחרצים: לא יתרחש כל ניתוק מרוסיה בדרך של התנגדות מזוינת. המדיניות האמריקאית תומכת בהישארותה של רוסיה מאוחדת, שכן התפרקות רבתי תערער את היציבות במרכז תת־היבשת האירו־אסיאתית ותכה גלים במערבה, במזרחה ובדרומה. החשש המיידי שעולה מפירוק המשטר ברוסיה הוא מן ההשלכות שיהיו לכך על יכולת השליטה והבקרה על הנשק הגרעיני שלה ועל פלטפורמות השיגור שלה.

ארצות־הברית ובעלות־בריתה כבר היו במצב זה בעבר. מייד עם שוך הסערה של התפרקות ברית־המועצות, הצטרפו לפתע המדינות הפוסט־סובייטיות אוקראינה, בלרוס וקזחסטן למועדון מדינות הגרעין העולמיות. גורלם של מאגרי הנשק הגרעיני של מדינות אלו הופקר, ואחדים מבכירי הממשל בהן שאפו "לשחק על הקלף הגרעיני" על מנת להשיג סיוע כלכלי או כדי לזכות ביוקרה הזמנית הכרוכה בו. המדיניות האמריקאית תמכה בביסוסה של רוסיה כיורשת המתבקשת והחוקית של ברית־המועצות, למטרת שליטה בנשק גרעיני ובכוחות הצבא. אחרת, פיזור הנשק הגרעיני בין המדינות הפוסט־סובייטיות עלול היה להוביל לכאוס, כולל הפצה לא־מורשית של נשק גרעיני וחומר מועשר לידי ארגוני טרור. לאחר "סחר

מכר" פוליטי ניכר בתחילת שנות התשעים בין ארצות־הברית, רוסיה ושלוש מדינות הגרעין החדשות, הושג הסכם שלפיו "יוחזרו" האמצעים הגרעיניים של אוקראינה, בלרוס וקזחסטן לרוסיה (כמחליפתה של ברית־המועצות), או שיפורקו.

לדבריהם של פקידי ממשל רוסיים, הנשק הגרעיני שמחזיקה המדינה בתצורות של טילים בין־יבשתיים או של מפציצים ארוכי־טווח נתון לאחסון ובקרה מאובטחים בעתות שלום.[17] המקרה הקרוב ביותר למשבר גרעיני התרחש בינואר 1995, כאשר שוגר טיל נורווגי למטרות מחקר מדעי, וזוהה בטעות על ידי מערכות ההתרעה של רוסיה כטיל בליסטי ששוגר מצוללת אמריקאית. מערך הגרעין הרוסי נכנס לפעולה. לראשונה מאז תום עידן המלחמה הקרה, נשיא רוסיה, בוריס ילצין, יחד עם שר ההגנה שלו וראש המטה הכללי, עשו שימוש ב"כפתור האדום" – אותה מזוודה שנושאים עמם ראש המדינה והיועצים הצבאיים הקרובים לו לכל מקום. הרוסים עקבו אחר נתיב מעופו של הטיל והגיעו לבסוף למסקנה שמסלולו פונה לכיוון הים, הרחק משטח המדינה.[18] לאחר מכן התברר כי שיגור הטיל מדגם Black Brant שהקפיץ את הרוסים היה תוצאה של תסבוכת דיפלומטית. ממשלת נורווגיה הודיעה למשרד החוץ הרוסי חודשים מראש על שיגור הטיל המתוכנן ועל יעדו – איסוף נתונים מדעיים על 'הזוהר הצפוני', אך התכתובות בנושא אבדו בסבך הבירוקרטיה הרוסית, ומעולם לא הגיעו לשולחנם של האחראים הרלוונטיים בכוחות הצבא ובמשרד ההגנה במדינה.

מטרת הסקירה שלעיל בנוגע לחששות ממדינות גרעין ותיקות אינה הפניית אצבע כלפי רוסיה, אלא אזהרה מפני קבלתה כמובנת מאליה של ההנחה כי מדינות גרעיניות חדשות או "סוררות" יגלו נטייה רבה יותר לפתוח במלחמה ולהימנע מסיומה בלא־פחות מאשר חורבן כולל, יותר מאשר מדינות המחזיקות ביכולת גרעינית מזה זמן רב. מובן שהארסנל הגדול והמגוון יותר שבידי המעצמות הגדולות נותן להן אפשרויות רבות יותר לשלוט בעימות וליצור הרתעה במהלך מלחמה, לעומת יכולתן של מדינות קטנות יותר. אך גם כשמדובר בהיקפים מצומצמים יותר של הכוח, איכותו ומאפייניו המבצעיים מהווים גורם משפיע על היכולת לשמר שליטה צבאית ומדינית במהלך מלחמה גרעינית.

אף על פי כן, קבלת ההחלטה האם להמשיך במלחמה או לסיימה מושפעת במידה רבה מאוד ממניעיהם ומאישיותם של המנהיגים, ומתנודות בדעת־הקהל של ציבור אזרחיה של המדינה המותקפת. משתנה נוסף בכל מדינה המעורבת במלחמה גרעינית יהיה תהליך תכנון המדיניות המתקיים בה: אופן חלוקת הכוח והשררה הפוליטיים בין בעלי התפקידים הרשמיים ובין דמויות מפתח אחרות בממשל. יש לנו מושג מסוים על תהליך קבלת ההחלטות בנושאי ביטחון לאומי בארצות־הברית, בבריטניה, בצרפת, בסין וברוסיה, שכן המערכות הפוליטיות במדינות אלו היו למושאי מחקר של רבים, הן מבית והן מחוץ.

אולם אילו שינויי כוחות יתרחשו עם תחילתה של מלחמה בהודו, בפקיסטן בצפון־קוריאה או באיראן? צפון־קוריאה אטומה כמעט לחלוטין בפני גורמי מודיעין זרים. הממשל בפקיסטן נתון במצור מצד ג'יהאדיסטים שהשפעתם מושרשת גם בתוך הצבא ובזרועות המודיעין במדינה. המשטר בטהראן נקרע בין אייטולות הדוגלים בשימור המסורת ועיניהם יוקדות משנאה כלפי ארצות־הברית וישראל, לבין מודרניסטים המבכרים התמקדות בפיתוח כלכלי ובשינוי חברתי הדרגתי. הודו היא הדמוקרטיה הגדולה בעולם ובין היציבות ביותר, אך בתנאי לחץ של מתקפה גרעינית עלול לחול מפנה חד ביחסים בין הצבא לממשלה, בהשוואה למתרחש בזמן שלום. בל נשכח כי במהלך המלחמה הקרה נרצחה ראש ממשלת הודו, אינדירה גנדי, בידי כמה ממאבטחיה האישיים.

על רקע דברים אלה, לאיזו תגובה נוכל לצפות מנשיא אמריקאי לאחר מתקפה גרעינית על אדמת ארצות־הברית מצד מדינה כלשהי, בין אם סוררת ובין אם לאו? ההיסטוריה האמריקאית אינה מבטיחה כי חמומי המוח ירוסנו, וכי הממשלה תנקוט צעדים מדודים במטרה להשיג "ניצחון" בעימות תוך גרימת הרס מזערי, או להגיע לשולחן המשא־ומתן במטרה להשיג הסכם שלום. אופן התנהלותה של ארצות־הברית לאחר פיגועי ה־11 בספטמבר היה מאלף: לא רק ארגוני טרור באשר הם, אלא גם משטרים שסייעו להם הפכו מטרה לתגובה אמריקאית. ארגון אל־קאעדה ראוי אמנם להוקעה הציבורית שזכה לה, אך אין זה עיקרו של דבר. האמריקאים ומנהיגיהם אינם מורגלים, לא מבחינת מזגם ולא מבחינת הכשרתם, להנחיל לאויביהם מכות צבאיות במינון מדוד. התגובה הסבירה למתקפה גרעינית על אדמת ארצות־הברית, גם מצד ארגוני טרור, תהיה דרישה ציבורית להסדר שלום שיבטיח את השפלת האויב.

סיכום

סיומה של מלחמה גרעינית היווה סוגיה שנויה במחלוקת בעידן המלחמה הקרה, ומסיבות שונות ימשיך להיות כך. אין לצפות שמוראותיה של מלחמה גרעינית יהיו על סדר־יומם של מרבית המנהיגים והעמים, למעט הפחד מטרור גרעיני השורר עתה בכל מקום לאחר אירועי ה־11 בספטמבר. אך מלבד העיסוק בטרור, מדינות עדיין מחזיקות באחריות לשמירה על הסדר העולמי, והחתירה לשלום אינה נפסקת משפרצה מלחמה. מנהיגים פוליטיים ואסטרטגים צבאיים במדינות המחזיקות ביכולת גרעינית ובמדינות מובילות אחרות חייבים לחשוב היטב על 'היום שאחרי', טרם כישלון ההרתעה.[19] אין להתיר למכונת המלחמה הגרעינית לפעול במצב של "טייס אוטומטי".

הדוגמאות שלעיל אינן מהוות תשקיף, אלא תבנית שתסייע בבחינת מספר היבטים של בעיית סיומו של עימות גרעיני. נעשה שימוש במקריהם של ארצות־

הברית ושל רוסיה, משום שאנו יודעים קצת יותר על האופן שבו הפעילו מדינות אלה את כוחות הגרעין שלהן בזמני שלום ובעתות משבר, וכיוון שהן התחייבו לפיקוח על תשתיות ועל מהלכים מבצעיים של מערכי הגרעין שברשותן עד שנת 2018. כמו כן, מגוון פלטפורמות השיגור שמחזיקות ארצות־הברית ורוסיה, גם אם בהיקף מצומצם במקרים מסוימים, מאפשר הסקת מסקנות ביחס למדינות גרעין קטנות יותר, ולגבי כאלה השואפות ליכולת גרעינית.

במדינות שהן דמוקרטיות באופן סמלי בלבד, או פחות מכך, הפיקוח על תפוצת נשק גרעיני ומניעתה הופכים קשים יותר בשל חוסר הוודאות לגבי היחסים בין ראשי המדינה לבין מפקדי הצבא באותן מדינות. כאשר ישיגו איראן או מצרים נשק גרעיני, כיצד תתבצע בהן האצלת הסמכות למתן הרשאה על הפעלה גרעינית לצורכי הרתעה או מלחמה, וכיצד ייעשה הדבר בצפון־קוריאה ובפקיסטן, המחזיקות כבר עתה ביכולות גרעיניות? חוסר הבהירות בנושאים אלה אינו מרגיע, ודיקטטורות נוטות להיראות יציבות מבחוץ, אך הן שבירות מבפנים ברגע שמשבר דיפלומטי גולש לכדי מלחמה. נוסף לכך, אסטרטגיות עתידיות של הרתעה וסיום מלחמה יהיו חייבות להביא בחשבון את החיבור האפשרי בין נשק להשמדה המונית, לרבות נשק גרעיני, לבין אסטרטגיות של לוחמת סייבר. ניתן לצפות כי בעתיד יכללו עימותים בין מדינות גם שימוש באמצעים של לוחמת סייבר במידה מסוימת, וכך גם התחומים של ניהול משברי גרעין, בקרת הסלמה וסיום לוחמה.[20]

הערות

1 ראו לדוגמה:
Stephen J. Cimbala, ed., *Strategic War Termination* (New York: Praeger Publishers, 1986); Paul K. Davis, "A New Analytic Technique for the Study of Deterrence, Escalation Control and War Termination," in Stephen J. Cimbala, ed., *Artificial Intelligence and National Security* (Lexington, Mass.: Lexington Books, 1986), pp. 35-60; and George H. Quester, "War Termination and Nuclear Targeting Strategy," ch. 14, in Desmond Ball and Jeffrey Richelson, eds., *Strategic Nuclear Targeting* (Ithaca, NY: Cornell University Press, 1986), pp. 285-305.
לדיון בנושא בפרספקטיבה של לאחר המלחמה הקרה, ראו מאמרים ב:
Stephen J. Cimbala and Sidney R. Waldman, eds., *Controlling and Ending Conflict: Issues before and after the Cold War* (Westport, Ct.: Greenwood Press, 1992).

2 "The Military Doctrine of the Russian Federation," www.Kremlin.ru, February 5, 2010, in *Johnson's Russia Lis*t 2010 - #35, February 19, 2010, davidjohnson@starpower.net. ראו גם: Nikolai Sokov, "The New, 2010 Russian Military Doctrine: The Nuclear Angle," Center for Nonproliferation Studies, Monterey Institute of International Studies, February 5, 2010, http://cns.miis.edu/stories/100205_russian_nuclear_doctrine.htm, and Jacob W. Kipp, "Russia's Nuclear Posture and the Threat that Dare Not Speak its Name," ch. 10, in Stephen J. Blank, ed., *Russian Nuclear Weapons: Past, Present, and Future* (Carlisle, Pa.: Strategic Studies Institute, U.S. Army War College, 2011), pp. 459-503.

3 המקרים של צפון־קוריאה ואיראן עשויים לחייב טיפול שונה מנקודת מבט של הרתעה ומניעת תפוצה, כיוון שצפון־קוריאה היא מדינה שהוכרזה כמחזיקה בנשק גרעיני, ואיראן לכאורה רק שואפת אליו. ראו:
Amitai Etzioni, *Security First: For a Muscular, Moral Foreign Policy* (New Haven, Yale University Press, 2007), pp. 241-42.

4 להיסטוריה של תוכנית הגרעין האיראנית, כולל רשימה מתועדת של הפרות איראן את הסכם הפיקוח מול הסוכנות הבינלאומית לאנרגיה אטומית, ראו:
Iran Watch, "Iran's Nuclear Program, " updated March 2012, http://www.iranwatch.org/wmd/wmd-nuclearessay-footnotes.htm. Downloaded August 13, 2012. See also: "Sanctions against Iran," *Wikipedia*, http://en.wikipedia.org/wiki/Sanctions_against_Iran.

5 David Albright, Paul Brannan, Andrea Stricker, Christina Walrond and Houston Wood, "Preventing Iran from Getting Nuclear Weapons: Constraining its Future Nuclear Options," Institute for Science and International Security, March 5, 2012, p. 45, http://www.isis-online.org/uploads/isis-reports/documents/USIP_Template_5March2012-1.pdf. Albright, et. al., also outline elements of a five stage framework agreement between the P-5+1 and Iran, pp. 42-44.

6 לדיון מפורט על טרור גרעיני, ראו:
Brian Michael Jenkins, *Will Terrorists Go Nuclear*? (New York: Prometheus Books, 2008); Etzioni, *Security First*:, esp. pp. 218-43; and Graham Allison, *Nuclear Terrorism: The Ultimate Preventable Catastrophe* (New York: Times Books – Henry Holt, 2004).
לדיון בנושא הטרור הגרעיני מנקודות מבט נוספות, ראו:
Morten Bremer Maerli, Annette Schaper, and Frank Barnaby, "The Characteristics of Nuclear Terrorist Weapons," pp. 209-222; Matthew Bunn and Anthony Wier, "The Seven Myths of Nuclear Terrorism," pp. 223-35, and John Mueller, "The Atomic Terrorist?" pp. 236-54, all in James J.F. Forest and Russell D. Howard, eds., *Weapons of Mass Destruction and Terrorism*, 2nd Edition (New York: McGraw-Hill, 2012).

7 לסקירות ביקורת נקודתיות על תיאוריית ההרתעה כפי שיושמה בסוגיות שלאחר המלחמה הקרה, ראו:
Colin S. Gray, *The Second Nuclear Age* (Boulder, Colo.: Lynne Rienner Publishers, 1999), esp. pp. 88-93; and Keith B. Payne, *Deterrence in the Second Nuclear Age* (Lexington, Ky: University Press of Kentucky, 1996. See also Patrick M. Morgan, *Deterrence Now* (Cambridge: Cambridge University Press, 2003), pp. 238-84.

8 בנושא רציונליות והרתעה, ראו:
Morgan, *Deterrence Now*, pp. 42-79.

9 עבודתו של Thomas Schelling בנושא זה כפי שיושמה על הרתעה גרעינית הייתה מקורית ופורצת דרך, כפי שנראה ב:
ראו גם: *Arms and Influence* (New Haven: Yale University Press, 1967).
Lawrence Freedman, *The Evolution of Nuclear Strategy*, 3rd ed. (New York: Palgrave-Macmillan, 2003), esp. pp. 171-84.

10 Paul Bracken, "War Termination," ch. 6 in Ashton B. Carter, John D. Steinbruner, and Charles A. Zraket, eds, *Managing Nuclear Operations* (Washington, D.C.: Brookings Institution, 1987), pp. 197-214.

11 שם, עמ' 201

12 Bracken, "Delegation of Nuclear Command Authority," ch. 10 in *Managing Nuclear Operations*, pp. 352-72, esp. pp. 355ff.,

מציע הבחנה דומה אם כי מעט שונה בין בקרה "פרובינציאלית" ל"פוליטית". בקרה פרובינציאלית כוללת בקרה טקטית ואסטרטגית של הכוחות המזוינים; בקרה פוליטית עוסקת באסטרטגיית־על, שהיא למעשה מדיניות.

13 היבטים שונים של סוגיה זו נידונים ב:
Bracken, *The Command and Control of Nuclear Forces* (New Haven, Ct.: Yale University Press, 1983).

14 בחינת בעיה זו ואחרות הקשורות בה מופיעה ב:
Albert Wohlstetter and Richard Brody, "Continuing Control as a Requirement for Deterring," Ch. 5 in Carter, Steinbruner, and Zraket, eds, *Managing Nuclear Operations*, pp. 142-96. See also Bracken, "Delegation of Nuclear Command Authority," p. 359.
כפי ש־Bracken מציין, האצלת סמכות ומתן הרשאה לפעולה גרעינית מצדם של מנהיגי מדינה לאחרים לא תתרחש אלא בנסיבות המאיימות ביותר – שהן בדיוק אלה שבהן עלולה להתרחש מלחמה גרעינית (שם, עמ' 356).

15 Robert A. Miller, Daniel T. Kuehl and Irving Lachow, "Cyber War: Issues in Attack and Defense," *Joint Force Quarterly* 61, no. 2 (2011) pp. 18-23, esp. p. 21.
בנושא בקרת הסלמה של פעולות תשתית ומידע "I2Os" (information and infrastructure operations). See also: U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (Washington, D.C.: U.S. Department of Defense, July 2011), http://www.defense.gov/news/d20110714cyber.pdf, downloaded August 14, 2012, and The White House, *International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World* (Washington, D.C.: The White House, May 2011), http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. פרשנות ביחס למסמכים אלה ובנושאים הקשורים בהם, ראו ב: Rosemary M. Carter, Brent Frick and Roy C. Undersander, "Offensive Cyber for the Joint Force Commander," *Joint Force Quarterly* 66, no. 3 (2012): pp. 22-27.

16 השקפה זו מורחבת ב:
Peter Douglas Feaver, *Guarding the Guardians: Civilian Control of Nuclear Weapons in the United States* (Ithaca, NY: Cornell University Press, 1992), pp. 12-28.
ראו גם באותו כרך את הערותיו על בקרה אזרחית לאחר ההחלטה להשתמש בנשק גרעיני, עמ' 55–66.

17 חומר המועשר לרמת שימוש כנשק וחומרים גרעיניים אחרים, לרבות מאגרים גדולים של אורניום ופלוטוניום, הם עניין נפרד. מומחים למניעת תפוצת הנשק בארצות־הברית ובמדינות נוספות עודם מודאגים מדליפה של חומרים גרעיניים או רדיולוגיים ממערך הגרעין של רוסיה או ממקורות אחרים. נושא זה כשלעצמו חשוב, אך מהווה עניין נפרד אף הוא. לעיסוק בתרחישים ספציפיים ובדיונים סביב ניסיונה של רוסיה בתחום זה לאחר המלחמה הקרה, בשנות התשעים, ראו:
Andrew and Leslie Cockburn, *One Point Safe* (New York: Doubleday, 1997),

18 שם, עמ' 240–244.

19 טיעון מצוין עלה בזכות נקודה זו ב:
George H. Quester, *Nuclear First Strike: Consequences of a Broken Taboo,* (Baltimore, Md.: Johns Hopkins University Press, 2006), esp. pp. 24-52 and 90-126.

20 להערכה של לוחמת סייבר בהקשר האסטרטגי, ראו:
Colin S. Gray, "Making Strategic Sense of Cyberpower: Why the Sky is Not Falling," paper, Wokingham, Berkshire, UK, September, 2012, esp. pp. 7-9.

מלחמת לבנון השנייה – הערכה מחודשת

בנג'מין ס' למבת'

מבצע "שינוי כיוון" (שם הקוד שניתן למלחמה בין ישראל לחזבאללה בלבנון ב־2006, על פי אגף המבצעים של צה"ל) הסתיים ללא הכרעה ברורה. למעשה, מבין כל טבילות האש הרבות שעבר צה"ל מאז 1948, הייתה זו הפעם הראשונה שבה עימות אזורי גדול הסתיים ללא ניצחון צבאי ברור לישראל. ההתנהלות והתוצאות של המבצע לא נבעו מכשל נקודתי מסוים, אלא "מצרוף נסיבות כולל", כניסוחם של שני פרשנים ישראלים הבקיאים בתחום זה.[1] ספציפית, המבצע לא שיקף כישלון של חיל האוויר הישראלי לממש את מלוא הפוטנציאל של יכולותיו (שהן ניכרות אך לא בלתי מוגבלות), כפי שרבים מהמבקרים נטו לטעון בשלב מסוים.[2] במקום זאת, יש לראות את תוצאות המבצע כפועל יוצא של ליקוי מקיף בבחירת האסטרטגיה, ובעיקר של חוסר העקביות בין היעדים המוצהרים ובין האמצעים הזמינים והרצון לחתור להשגתם. כמו כן תרמה לכך העובדה שממשלת ישראל הציבה מלכתחילה בסדר העדיפויות של המבצע את ההימנעות מנפגעים כיעד גבוה יותר מהיעד של השלמת המשימה.[3]

ככל שהעימות התמשך גבר התסכול בישראל מכך שבאף שלב במשך 34 ימי המבצע לא הצליחו כוחות צה"ל לעצור את מטר הקטיושות היומי שחזבאללה ירה לעבר ריכוזי אוכלוסייה אזרחית בצפון המדינה. למעשה, רק ההסכם ההדדי להפסקת אש שם קץ למטרד הרסני זה. מעבר לכך, תוצאות המלחמה לא הניבו את מה שראש הממשלה אהוד אולמרט הבטיח לאזרחי ישראל בראשית המבצע, דהיינו החזרה ללא תנאי של שני חיילי צה"ל שחזבאללה חטף ב־12 ביולי 2006 – הפעולה שהביאה ליציאה למבצע – וחיסול מוחלט של נוכחות צבאית פעילה של

ד"ר בנג'מין ס' לאמבת' הוא עמית בכיר במכון המחקר Center for Strategic and Budgetary Assessments בוושינגטון, ארצות הברית. מאמר זה מבוסס ברובו על ספרו:
Air Operations in Israel's War against Hezbollah: Learning from Lebanon and Getting It Right in Gaza, Santa Monica, CA: RAND Corporation, 2011, http://www.rand.org/pubs/monographs/MG835.html.

חזבאללה בדרום לבנון.[4] חוסר ההכרעה הצבאית השפיע לרעה על תדמיתה של ישראל כבלתי ניתנת להכנעה בעיני העולם הערבי והמערב; הוא גם הציף כשלים רבים בדרגים הגבוהים ביותר של ממשלת ישראל בכל הקשור להצבת יעדים וניהול ציפיות, הן בפן האזרחי והן בפן הצבאי.[5]

למרות ההסכמה הכללית על היעדר הכרעה, תהיה זו טעות להסיק מכך, כפי שהציע גורם אמריקאי כשנה לאחר תום המלחמה, כי תוצאות המלחמה היו "כמו לומר שהניתוח הצליח אבל החולה מת".[6] כנגד זאת, רמטכ"ל צה"ל במלחמת לבנון השנייה, רב־אלוף דן חלוץ, איש חיל האוויר ומי שפיקד על התכנון והביצוע של המלחמה, גילה נימה אופטימית יותר. בעדות שמסר בפני ועדת וינוגרד, שמונתה לבדוק את אירועי המלחמה, טען חלוץ כי "מה שהושג או לא הושג [במהלך המבצע] חייב יהיה להישפט בפרספקטיבה של זמן".[7] ראש הממשלה דאז, אהוד אולמרט, אמר בעדותו בפני הוועדה בנימה דומה, כי "התוצאות [של המלחמה] ישתפרו ככל שהזמן יעבור".[8] כיום, עם התפזרות עשן הקרב של אוגוסט 2006, אכן השתנתה בהדרגה תפישת המבצע, ועמה הדעה הרווחת בישראל, והתקרבה יותר להערכות המקצועיות והאופטימיות שהושמעו בזמנן. למעשה, כבר בתחילת 2008 החל ויכוח חדש לצבור תאוצה סביב השאלה "האם באמת הפסדנו במלחמה, או אולי לא".[9]

מדוע המלחמה אינה הפסד מוחלט מבחינת ישראל

מזכ"ל חזבאללה, חסן נסראללה, יכול היה לטעון בקלות עם סיום המבצע כי הוא "ניצח" בו, פשוט מעצם העובדה ששרד. יחד עם זאת, לא ניתן להתכחש לעובדה שכתוצאה ממתקפת צה"ל ספג ארגונו מכה קשה ושילם מחיר כבד על הפרובוקציה שיזם ב־12 ביולי 2006, שהייתה כאמור העילה למלחמה. צה"ל הרג כמעט 700 מלוחמיו המנוסים ביותר של חזבאללה ופצע יותר מ־1,000.[10] בנוסף, חלק ניכר מתשתית הארגון בלבנון הפך לגל הריסות או לפחות ניזוק משמעותית, כתוצאה מהפצצות אוויריות ומהפגזות ארטילריות מסיביות ורציפות של צה"ל.[11]

בין ההישגים החשובים ביותר של צה"ל במבצע היה השמדת מרבית טילי "זלזאל" לטווח ארוך והרקטות לטווח בינוני שבידי חזבאללה במהלך הלילה הראשון למבצע, וזאת הודות למתקפת פתע מתוכננת ומתורגלת היטב של חיל האוויר – מהמפתיעות שהיו בתולדות הלוחמה האווירית. בנוסף לכך, מוקד הבקרה והשליטה של נסראללה ברובע דחייה בביירות נהרס לחלוטין, גם הוא בתקיפות מדויקות של חיל האוויר.[12] זאת ועוד, משגרי רקטה רבי־קנים הותקפו שוב ושוב והושמדו בידי חיל האוויר בתוך דקות ספורות בלבד מרגע שצוותי השיגור שלהם ירו את המטח הראשון על צפון ישראל. לשיעור ההצלחה המרשים של חיל האוויר במתקפות ממוקדות ומתוזמנות אלו עשויה להיות השפעה בולמת על כל שימוש עתידי במשגרים מסוג זה מצד חזבאללה. סביר להניח שלוחמי הארגון יטו להיצמד

למשגרים חד־קניים, היורים פעם אחת בלבד לפני שהם מנוידים אל מחוץ לטווח הסכנה ונטענים מחדש.[13]

בנוסף לכך, למרות הצהרותיו החוזרות של נסראללה כי זכה ב"ניצחון גדול" במלחמת לבנון השנייה, פוטנציאל האיום של חזבאללה ירד בצורה משמעותית כתוצאה מהמתקפה המפתיעה והמסיבית של צה"ל. בהקשר זה ציין בצדק אלוף (מיל') יצחק בן ישראל, כי מבצע "שינוי כיוון" "הפך על פיה את התחושה שישראל אינה מוכנה להילחם עם מי שמנופף בחרב מעל ראשי אזרחיה", וכי "ההרס של רובע בעיר בירה ערבית, גם אם היה קשור ישירות למטה הראשי של חזבאללה בלבנון, קבע תקדים שיגרום לאויבי ישראל לחשוב פעמיים בעתיד".[14]

חשיבותו של המבצע הייתה גם בהתנסות המאלפת שהקנה לצה"ל, שכן הוא אִפשר לחשוף את טיבו האמיתי של חזבאללה כאויב, את נקודות החוזק והחולשה שלו, כיצד הוא נלחם ומה מידת ההרס של הרקטות והטילים נגד טנקים תוצרת איראן שבידיו. יתר על כן, בחירתה של ישראל בתגובה עוצמתית ויכולתה להפגין חוסן מתמשך הוכיחו את נחישותה להתמודד עם חזבאללה תוך הפעלת אמצעים לא פרופורציונליים בעליל, גם בתרחיש עתידי שיחייב הפעלת עוצמה כזו. ההיסטוריון הצבאי הישראלי מרטין ואן קרפלד ציין בהקשר זה, כי "אם מישהו היה צופה ימים ספורים לפני המלחמה שבתגובה לתפיסת שניים מחייליה ישראל תצא במתקפה אווירית על כל לבנון, תשנע שלוש חטיבות אל מעבר לגבול ותתמיד בהפעלת הלחץ למשך יותר מחודש ימים, בעוד היא סופגת אלפי טילים וסובלת יותר ממאה אבידות בנפש, היו מסתכלים עליו כעל מי שיצא מדעתו". לדברי ואן קרפלד, לאור תגובה מסיבית זו והמסר המרומז שדומות לה יתרחשו בעתיד אם ישראל תעמוד בפני הצורך להגיב על התגרות דומה, "לנסראללה יש סיבה טובה לחשוב פעמיים לפני שייצא להרפתקה נוספת מסוג זה".[15]

לסיכום, ניתן לקבוע כי 34 הימים של מתקפת הנגד של צה"ל על חזבאללה לא היו בדיוק מפלה גדולה לישראל כפי שרבים סברו תחילה. יותר נכון לחשוב על המציאות האסטרטגית שנוצרה ב"יום שאחרי", מלחמת לבנון השנייה, הן לחזבאללה והן לישראל: מאז השבועות הראשונים לבחירתו של נסראללה כמזכ"ל חזבאללה ב־1992, ירה הארגון באופן תדיר רקטות קצרות טווח על צפון ישראל, כשהוא חש חסין מפני תגובה, והתמיד בכך עד תחילת מבצע "שינוי כיוון"; מאז שהמבצע הסתיים, אף טיל לא נורה מלבנון לישראל, למעט תקרית שבה שוגרו שלושה טילים בעת מבצע "עופרת יצוקה" שערך צה"ל נגד ארגון חמאס ברצועת עזה בדצמבר 2008–ינואר 2009. למרות שעד לאותה עת חזבאללה כבר הספיק לצבור במחסני הנשק המשוקמים שלו טילים קצרי טווח בכמות גדולה מזו שהייתה ברשותו במלחמת לבנון השנייה (כ־40,000 טילים), הזדרזו מנהיגיו להתנער מכל

אחריות לשיגורים אלה.[16] מאז שורר שקט באזור הגבול הלבנוני – אינדיקציה לכך שההרתעה של ישראל כלפי חזבאללה נותרה איתנה.

השינוי בשיקולי נסראללה

מציאות חדשה ויציבה זו בגבול הצפוני של ישראל מלמדת שהמוטיבציה וההתנהלות של נסראללה לאחר מבצע "שינוי כיוון" הושפעו מהמכה המשמעותית שצה"ל גרם לארגונו. אין ספק שהלקח מאירועי המלחמה ב־2006 הופנם אצלו בהצלחה והרתיע אותו מלשגר רקטות לעבר צפון ישראל. לקח זה אף התחזק בעקבות פעולת הגמול הדומה שנקטה ישראל מול החמאס שנתיים מאוחר יותר. יתרה מכך, לאור הידיעה הברורה שהוא מהווה מטרה לצה"ל, נסראללה, וכן בכירי הארגון, נאלצו לעבור לפקד מתוך בונקרים, ולמעט חריגות ספורות נמנעו מלהופיע בציבור במהלך השנים שחלפו מאז הסתיימה מלחמת לבנון השנייה.

על רקע זה יש לראות את דבריו של מקור בכיר המקורב לראש הממשלה לשעבר אהוד אולמרט, בהתייחסו ל"מצעד הניצחון" שנסראללה ביים בביירות באמצע ספטמבר 2006, כחודש לאחר סיום הלוחמה: "נסראללה לא נראה טוב. הוא נראה בדיוק כמו מישהו שבילה את זמנו בבונקר, הרחק מהשמש, מאז 12 ביולי". מקור זה הוסיף וציין שערב אירוע ההמונים המבוים של מזכ"ל חזבאללה התנהל ויכוח בקרב הממסד הביטחוני הישראלי אם לנצל את ההזדמנות ולנסות ללכוד אותו גם במחיר הפוטנציאלי של גרימת מאות הרוגים בקרב האזרחים הלבנונים שהקיפו אותו. בסופו של דבר החליטה הממשלה שלא לצאת למבצע חיסול, לאחר שראשיה הגיעו למסקנה שהתקפה מעין זו, שעתידה הייתה להביא למותם של לבנונים רבים חפים מפשע, תגרום לישראל יותר נזק מאשר תועלת. עם זאת, הוסיף המקור הישראלי: "האיש [נסראללה] יבלה עוד שנים רבות בבונקר. הוא חשוב כמת".[17] לפני המלחמה ב־2006 נהג נסראללה ליטול חלק ביותר מתריסר אירועי ציבור המוניים מדי חודש. עבור מי שהשפעתו כמנהיג כריזמטי תלויה רבות בחשיפה תכופה לציבור, העובדה שהוא נאלץ לפקד ממקום מסתור מהווה פגיעה משמעותית באפקטיביות של השפעתו.

נוסף לכך, ישראל נהנית כתוצאה מהמבצע ממצב משופר באופן משמעותי בדרום לבנון. ב־11 באוגוסט 2006, בעוד נמשכת הספירה לאחור לקראת מתקפה יבשתית של צה"ל שתסלים את המבצע, אישרה מועצת הביטחון של האו"ם פה אחד את החלטה 1701, שקראה לעצירת הקרבות והורתה על פריסת 15,000 חיילים זרים באזור הלחימה כדי לסייע לצבא לבנון לקחת לידיו את השליטה על דרום לבנון. ההחלטה, שאושרה זמן קצר לאחר מכן על ידי ממשלות לבנון וישראל, התירה לאו"ם גם לנקוט את "כל הפעולות הנחוצות" כדי להבטיח שהאזורים שבהם יפטרלו כוחותיו "לא ינוצלו לפעילויות עוינות מכל סוג שהוא".[18] כמו כן

קראה ההחלטה לפירוק חזבאללה מנשקו בדרום לבנון ולהקמת כוח או"ם זמני שם (כוח יוניפי"ל). כדי לסייע באכיפת ההסדר באזור העימות, החל צבא לבנון לפרוס את כוחותיו בדרום המדינה כבר ב־17 באוגוסט 2006.

ממשלת לבנון, ויוניפי"ל בעקבותיה, נסוגו בסופו של דבר מהמחויבות לפרק את חזבאללה מנשקו, עליה הצהירו בתחילה, והנוכחות של חיילי צבא לבנון בדרום המדינה לא תרמה דבר להפחתת פוטנציאל הלוחמה המאיים והמתמשך מצד הארגון כלפי צפון ישראל. עם זאת, ולמרות האכזבות הצפויות הללו, נותרת בעינה העובדה החד־משמעית כי נסראללה נענש קשות על ידי התגובה הבלתי צפויה של צה"ל לחטיפת שני החיילים הישראלים ב־12 ביולי, ועשה מאז כל מאמץ לשמר את אזור הגבול רגוע כדי למנוע תגובת נגד לא פרופורציונלית נוספת מצד ישראל – כפי שחזה מפקד בכיר בצה"ל בחלוף שבוע אחד בלבד מתום המבצע: "זהו שינוי עצום שהמבצע אחראי לו".[19] פרשן אחר ציין שנה לאחר מכן, כי "החודשים האחרונים היו השקטים ביותר בגבול הצפוני מאז מבצע שלום הגליל ביוני 1982", והוסיף כי "מיקוד הוויכוח הציבורי [אך ורק] בכישלון מלחמת לבנון השנייה, תוך התעלמות גורפת מהישגיה, עלול לפגוע ביכולת צה"ל ללמוד מהניסיון ולהפיק את הלקחים הנכונים".[20]

קצין מודיעין ישראלי לשעבר שהתייחס להתפתחויות חיוביות שמבצע "שינוי כיוון" הביא לישראל, קבע כי למרות שמלחמת לבנון השנייה נכשלה בחיסול האיום פוטנציאלי של חזבאללה לטווח הארוך וביצירת שינוי משמעותי במצבה של ישראל מול הארגון, היא הניבה ארבעה הישגים חיוביים ייחודיים: ראשית, היא סיפקה תובנות מדויקות על יכולות הלוחמה המתקדמות ביותר של חזבאללה; שנית, היא סייעה להפחית את החששות בדבר הפעולות שעלולות לנקוט שלוחות איראניות (דוגמת חזבאללה) נגד אינטרסים מערביים; שלישית, היא אפשרה לישראל להבין מה עליה לעשות כדי להתכונן לעימות הבא עם חזבאללה; ורביעית, היא נתנה לפוליטיקאים בישראל תמריץ לשקול מחדש את התועלת שבמדיניות הדוגלת ב"שטחים תמורת שלום", כפי שגובשה כלפי רצועת עזה וחלקים מהגדה המערבית בשנת 2005.[21]

במבט לאחור, ניתן גם לשאול האם לא שגה נסראללה בצורה מהותית בקריאת ישראל כאשר תכנן את מהלך החטיפה, תוך המעטה כה חמורה בעוצמה הצפויה של תגובת צה"ל. כבר במהלך מתקפת הנגד של ישראל אמר סגן מפקד הזרוע הפוליטית של חזבאללה, מחמוד קומאטי, לעיתונאים מערביים, כי הופתע מעוצמת התגובה הישראלית וכי מנהיגי הארגון צפו רק "פעולת תגמול רגילה ומצומצמת" מצד צה"ל, כגון פשיטות קומנדו או מתקפות אוויריות מוגבלות.[22] זמן קצר לאחר כניסת הפסקת האש לתוקף הודה נסראללה עצמו בגילוי לב שלא היה מורה על לכידת חיילי צה"ל לו היה צופה מראש את תגובת ישראל: "אתה

שואל אותי אם הייתי יודע ב־11 ביולי... שהמבצע יוביל למלחמה כזו, אם הייתי עושה זאת? אני אומר שלא, לחלוטין לא".[23] לקראת סוף השבוע השני למבצע, ועל רקע התעצמות תגובת צה"ל, הציג בעל הטור האמריקאי תומאס פרידמן הערכה שיצאה נגד ההנחה השגורה כי נסראללה הוא מהמנהיגים הערבים היותר "מבריקים" ו"אסטרטגיים", כאשר כתב: "לאחר שהעשן יפוג, נסראללה ייזכר כמנהיג הערבי הנמהר ביותר מאז גמאל עבד אל־נאצר המצרי, ששיקול דעתו השגוי הוביל למלחמת ששת הימים".[24]

הערכתו של פרידמן מתחזקת נוכח העובדה שההשקעה ארוכת הטווח של איראן בחזבאללה ירדה לטמיון בעקבות ההתגרות היהירה שיזם נסראללה ב־2006. ניתן להשוות את צעדיה של איראן לחמש את חזבאללה בטילים מכל הסוגים לפריסת הטילים הבליסטיים לטווח בינוני של ברית המועצות בקובה, אשר הגיעה לשיאה במשבר הטילים ב־1962. צה"ל נקט למעשה אמצעים דומים לאלה שאותם נקטה ארצות הברית בהתמודדות שלה עם האתגר הצבאי הסובייטי בקובה. גורם ישראלי הבקיא בנושא זה ציין כי איראן ציידה את חזבאללה במלאי טילים מתוך תפישה שהארגון ישמש כמעין "נושאת מטוסים" איראנית המוצבת סמוך לגבול עם ישראל, שתיצור יכולת ש"הייתה אמורה להישאר נסתרת עד לרגע האמת, דהיינו עימות צבאי בין ישראל או ארצות הברית לבין איראן סביב תוכנית הגרעין של איראן. חשיפתה בטרם עת של המכה הקשה שהארגון התכוון להנחית [על ישראל] גרמה לנזק אסטרטגי לחזבאללה ולספקית שלו איראן, שאי אפשר להתעלם ממנו".[25]

כאילו כדי לאמת קביעה זו, בא הדיווח לפיו המועצה לביטחון לאומי של איראן גיבשה מסמך פנימי, זמן קצר לאחר תום הלחימה, המביע זעם רב על חזבאללה על ש"בזבז את ההשקעה הצבאית החשובה ביותר של איראן בלבנון, רק בגלל העימות שיצר עם ישראל סביב שני חיילים חטופים".[26] תגובה מעין זו מצד הגורמים השליטים באיראן אינה מפתיעה, בהתחשב בכך שפעילות צה"ל במהלך 34 ימי הלחימה מחקה למעשה חלק ניכר מארבעה עד שישה מיליארד הדולרים שהשקיעה איראן בבניית הזרוע הצבאית של חזבאללה וחייבו את איראן להוצאות חירום יקרות לשיקום התשתית הצבאית ומלאי הנשק של הארגון.

ישראל מול לוח שחמט חדש

תפקידו של חזבאללה כזרוע צבאית קדמית של איראן הודגש באופן דרמטי הרבה יותר בעקבות ההתנסות המבצעית במלחמת לבנון השנייה. הוא חידד עוד יותר את ההערכה בצה"ל, שכבר קודם לכן הייתה קיימת, בדבר רצינות האיום האיראני, ואִפשר למפקדיו להבין טוב יותר גם את האיום שמציב ארגון חמאס. בנוסף לכך, תדמיתו של חזבאללה כמגן האינטרס הלבנוני נסדקה קשות בעקבות ההשלכות

יקרות הערך שהיו לפרובוקציה של נסראללה על הכלכלה והתשתית האזרחית בלבנון. למנהיג הארגון יש כיום הבנות חדשות של תפישת העולם הישראלית ושל הדברים שהוא יוכל או לא יוכל לעשות בעתיד. היקף ועומק התגובה הישראלית המחישו לחזבאללה שישראל מוכנה לשלם מחיר גבוה כדי להגיב באופן הולם על התגרויות נגדה בעתיד ועל כל ניסיון לבחון את נחישותה.

מבצע "שינוי כיוון" הצביע על בעיות רציניות של מוכנות בכוחות היבשה של צה"ל ועל ליקויים חמורים בקשר שבין חיל האוויר לכוחות היבשה, ובכלל זה מתן סיוע אווירי צמוד לחיילים הנלחמים על הקרקע. שני מוקדי בעיות אלה תוקנו מאז, כפי שניתן היה לראות מביצועיו המאוחרים יותר של צה"ל מול חמאס במבצע "עופרת יצוקה" בדצמבר 2008–ינואר 2009.[27]

ברמה האסטרטגית, מלחמת לבנון השנייה הצביעה בפני ישראל על מציאות מתפתחת, שבה אויב שאינו מדינה, דוגמת חזבאללה, שיש לו יכולות וחימוש מתוחכמים יחסית, מהווה הרבה יותר מאשר מטרד שולי לביטחונה של המדינה. למעשה, ההפך הוא הנכון; עם חשיפת יכולתו של חזבאללה לסכן מספר גדול של אזרחי ישראל הנמצאים בטווח הטילים שלו, הפכה התנועה האסלאמית הקיצונית למה שאחד מהחוקרים בישראל היטיב לתאר: "איום אסטרטגי מהמעלה הראשונה".[28] שני חוקרים אוסטרלים טענו מאוחר יותר, כי תפוצת נשק טרור זול אך אפקטיבי כל כך באזור מערערת באופן כמעט מיידי את "החשיבות ההיסטורית שיש לכוח האווירי ככלי העיקרי במדיניות ההגנה של ישראל".[29] בהמשך לכך, היטיב לתאר החוקר הביטחוני האמריקאי אנדרו קרפינביץ' את מלחמת לבנון השנייה, כשהשווה אותה לאותה "קנרית במכרה הפחם", וזאת על שום האופן שבו חשפה כיצד "עימות חדש ולא רגיל, מסוג קטלני יותר... בתנאים של טכנולוגיה מתקדמת" הוכיח את הקושי ההולך וגובר להגן על מתקני צבא מרכזיים, על תשתיות כלכליות ועל עורף אזרחי המאוכלס בצפיפות כנגד אויבים היברידיים דוגמת חזבאללה וחמאס – אויבים החמושים במה שקרפינביץ' מכנה יכולות רמט"א (רקטות, מרגמות, טילים וארטילריה).[30]

הזיכרון הטרי ממלחמת לבנון השנייה אִפשר לצה"ל להגיע למסקנה הברורה כי התקפות שהן "מנגד בלבד" (standoff only) אינן יכולות להציע מענה הולם לאתגר החדש. צה"ל הפנים זאת כבר בסבב הלחימה הראשון שלאחר מלחמת לבנון השנייה – ברצועת עזה. בסבב זה יושמה ההבנה שהדרך היחידה להתמודד בצורה נכונה עם איומי רמט"א היא ב"תפיסת השליטה על אזורי השיגור של האויב... וכך למדה ישראל שוב לסמוך על כוח תמרון גדול ועל העיקרון של ניהול הקרב על אדמת האויב".[31] הסבר נוסף לכך שצה"ל תפקד במבצע "עופרת יצוקה" בעזה טוב יותר מאשר במלחמת לבנון השנייה היה שהפעם הן מפקדיו והן ממשלת אולמרט

היו מוכנים לספוג אבידות בנפש של חיילים במידת הצורך – אבידות שמספרן היה בסופו של דבר נמוך מהצפוי.

בהתייחסו לכל האמור לעיל, אמר אחד הפרשנים הישראליים כי "ישראל כמעט צריכה להודות לחזבאללה על קריאת ההשכמה".[32] חלק גדול מאותה קריאת השכמה היה ההבנה שבמלחמה מול חזבאללה, צה"ל נלחם למעשה בשלוחה קדמית של איראן. בהקשר זה קבע פרשן ישראלי אחר: "מאגר ענק וכמעט אין־סופי של קטיושות צמח מתחת לאפנו. מזלה הגדול של מדינת ישראל היה שהמלחמה התרחשה עכשיו ולא מאוחר יותר". אותו פרשן הוסיף: "נסראללה איבד את היכולת להרתיע אותנו. הוא הזהיר שמה שיקרה בביירות יקרה בתל אביב, ולפני שאפילו סיים לדבר הרסנו עוד עשרה בתים בביירות. הוא מבין שאיננו חוששים ממנו עוד... הוא זה שנמצא במלחמת קיום".[33]

לאור התבוסה הגדולה שהנחילה מתקפת צה"ל במלחמת לבנון השנייה הן לחזבאללה כארגון טרור והן לאינטרסים האסטרטגיים של איראן (וזאת מבלי לציין את השקט הרצוף שהושג בגבול הצפוני של ישראל מאז שהפסקת האש נכנסה לתוקף באוגוסט 2006), ניתן לומר בביטחון מלא על מבצע "שינוי כיוון" את מה שהסופר האמריקאי מארק טוויין אמר לכאורה פעם על אופרה של וגנר: "זה לא גרוע כמו שזה נשמע". במבט לאחור, שלושת היעדים האסטרטגיים הראשיים שהרמטכ"ל חלוץ הגדיר לצה"ל – הפסקת התקפות הטרור של חזבאללה לתוך ישראל מתוך אדמת לבנון הריבונית, הטלת האחריות על השליטה באזור הדרום על ממשלת לבנון, הסבת נזק משמעותי לתשתיות הצבאיות של חזבאללה – כולם הושגו בסופו של דבר.[34] הפן השלילי העיקרי היחיד, כפי שהודה בכנות תא"ל איתי ברון בניתוח המבצע בדיעבד, הוא ש"אנו [צה"ל וממשלת אולמרט] נכשלנו בהגנה על האוכלוסייה האזרחית בישראל ולא הצלחנו בקיצור משך המלחמה".[35]

ההערכה היא, כי הודות לתרומות הכספיות ולתמיכה הטכנית הרצופה מאיראן ומסוריה, חזבאללה וחמאס ביחד מחזיקים כיום מלאי של יותר מ־70,000 רקטות קצרות טווח.[36] יתר על כן, על פי מידע שהגיע למודיעין הישראלי ולאחר מכן דלף לעיתונות מנשיא המדינה שמעון פרס, סוריה ציידה את חזבאללה גם בטילי סקאד B, שעל פי הטווח ויכולת נשיאת חומר הנפץ שלהם יכולים לפגוע בכל עיר בישראל עם ראש נפץ של 900 ק"ג.[37] אם הדבר נכון, העברת הסקאדים לנסראללה תהפוך את ארגונו לישות הלא־מדינית הראשונה שתחזיק בנשק קרקע־קרקע קטלני כל כך (הגם שאינו מונחה ואינו מדויק).

מנקודת המבט השלילית, חזבאללה ספג מנה גדושה של תבוסות פוליטיות. כך, לדוגמה, ב־14 ביולי 2009 נהרס בפיצוץ עז מאגר תחמושת מרכזי של הארגון בכפר חירבּת סאלם שבדרום לבנון. באוקטובר אותה שנה התפוצץ בנסיבות מעורפלות בונקר תחמושת סודי נוסף של חזבאללה בדרום לבנון. שני האירועים גרמו למבוכה

ממשית לארגון בכך שחשפו שהוא מפר את החלטה 1701 של מועצת הביטחון, האוסרת על אגירת נשק מדרום לנהר הליטני. כאילו כדי להוסיף לפגיעה בתדמית הציבורית של הארגון, לוחמי חזבאללה, בסיוע ובעידוד של חיילי צבא לבנון, מנעו מפקחים זרים לבחון את אתר התקרית השנייה, וכך חשפו את חוסר הנייטרליות של צבא לבנון ואת העובדה שהוא מספק סיוע ותמיכה פעילים לחזבאללה.[38]

יותר משנה קודם לכן, ב־12 בפברואר 2008, חוסל מפקד הזרוע הצבאית של חזבאללה והמקורב ביותר לנסראללה, עימאד מורנייה, בפיצוץ מסתורי של כלי הרכב שלו בדמשק. בין יתר הפעולות שמורנייה נחשד בביצוען היו התכנון והפיקוח על החטיפה בגבול ישראל־לבנון ב־12 ביולי 2006, שהביאה לפרוץ מלחמת לבנון השנייה.[39] בהלוויה שנערכה בביירות ביום שלאחר מכן למי שהיה אחד מהמוחות המרכזיים של ארגון הטרור, האשים נסראללה את ישראל על שהתנקשה בחייו של יד ימינו ונשבע שפעולת גמול של חזבאללה בוא תבוא.[40] עד היום נסראללה לא מימש את הבטחתו לנקמה על מכה אנושה זו שהונחתה על הזרוע הלוחמת של ארגונו.[41]

זאת ועוד, מאז תום מתקפת צה"ל על דרום לבנון ב־2006, חזבאללה הפך למעין כולא ברק הסופג את אי־שביעות הרצון ההולכת וגוברת מצד האוכלוסייה הלבנונית על היותו הגורם העיקרי לפעולת הגמול של ישראל, שהסבה נזק כה גדול לתשתית האזרחית של לבנון ולכלכלתה. מסיבה זו, נסראללה מעריך שהוא אינו יכול להרשות לעצמו להיתפש בעיני העם הלבנוני כגורם לפעולת גמול כואבת נוספת מצד ישראל נגד לבנון. אם חזבאללה ירצה לבצע בעתיד פעולה אלימה נגד ישראל, שתהיה חמורה דייה כדי לעורר תגובה קשה מצדו של צה"ל אף יותר מזו של קיץ 2006, הוא יסכן בכך את האינטרסים שלו עצמו, על ידי שיצטייר כפוגע במדינת לבנון המארחת אותו.

העימות השני של ישראל ברצועת עזה – מבט לעתיד

ישראל הצהירה שהמעקב המודיעיני שלה אחר חזבאללה השתפר באופן משמעותי בהשוואה למצב שלפני מלחמת לבנון השנייה, ופיקוד הצפון של צה"ל הביע ביטחון רב שהתוצאה העמומה של מבצע "שינוי כיוון" ב־2006 לא תחזור על עצמה במקרה של עימות נוסף עם חזבאללה. לדברי אחד מהקצינים הבכירים של צה"ל ב־2009: "חזבאללה יותר ממוזמן לנסות. קבלת הפנים שאנו מכינים לו [הפעם] היא כזו שהוא יזכור אותה להרבה זמן".[42] בנוסף, המנהיגות הנוכחית של ישראל הבהירה בצורה ברורה, שמכיוון שחזבאללה הפך לשותף רשמי לממשלת לבנון, כל פעולה התקפית בעתיד מצדו תיחשב לפעולה שנוקטת ממשלת לבנון, ולפיכך ישראל רואה כיעדים לגיטימיים להתקפה של צה"ל מטרות כלכליות ותשתיות של המדינה.

יתרה מזו, בימים אלה, שבהם מממניו של חזבאללה בטהראן ניצבים בפני בעיות משלהם נוכח התסיסה בחזית הפנימית, נסראללה אינו יכול (לפחות לא לעת עתה) להסתמך על תמיכה אוטומטית של איראן במקרה של התקפה נוספת מצד ישראל על הנכסים החשובים ביותר שלו בלבנון. עיתונאי ופרשן ביטחוני ישראלי ניסח זאת כך: "למרות העובדה שחזבאללה חזק כיום במידה משמעותית במונחים צבאיים טהורים מאשר בעבר [ב־2006], מעמדו הפוליטי והאוטונומיה שלו ירדו בצורה ניכרת. ברור שנסראללה זהיר, והוא ישקול את האופציות בזהירות רבה לפני שיבחר בדרך פעולה שעלולה להביא למלחמה כוללת עם ישראל".[43]

העובדה שישראל ספגה שתי מלחמות טילים בזו אחר זו בטווח של פחות משלוש שנים וניצבת בפני איום תמידי של אתגרים דומים ואף גרועים יותר, שעתידים להגיע הן מחזבאללה והן מחמאס, המריצה אותה להשקיע מאמצים רבים במחקר ופיתוח של מערכת הגנה פעילה נגד טילים. השאיפה הייתה להכניס לשימוש מבצעי מערכת שתתמודד עם טילי גראד, קטיושות, קסאם ושאר הטילים קצרי הטווח שאיימו על האוכלוסייה האזרחית במהלך מלחמת לבנון השנייה ובחודשים שקדמו למבצע "עופרת יצוקה". לצד המערכות להגנה אזורית "חץ־2" ו"חץ־3", המיועדות לאיומים בליסטיים ארוכי טווח, ולמערכת היירוט "קלע דוד" שנועדה להשמיד טילי שיוט נמוכים ואיטיים יותר, החל צה"ל ב־2010 לפרוס את מערכת "כיפת ברזל" להגנה מקומית, הנותנת מענה לרקטות קצרות טווח מהסוג שחזבאללה וחמאס נוטים לשגר במספרים גדולים.

עד סוף שנת 2012 הוצבו משגרי הטילים הניידים של "כיפת ברזל" בעיקר סביב ערים ומתקנים ישראליים הסמוכים לרצועת עזה, שכן חמאס היה המקור היחיד לירי תדיר של רקטות לתוך אזורים מיושבים בישראל לאחר תום מבצע "עופרת יצוקה". אולם בבוא העת ייפרסו 13 סוללות "כיפת ברזל" באתרים בעלי חשיבות אסטרטגית בכל רחבי המדינה. השאיפה היא לערער במידה רבה ככל האפשר את טקטיקת ההתקפה המועדפת על חזבאללה וחמאס – ירי תלול מסלול של רקטות קצרות טווח לתוך ריכוזי אוכלוסייה בישראל, במטרה להטיל אימה. מערכת "כיפת ברזל", שתמומן בחלקה על ידי ארצות הברית ותכלול מכ"ם אמריקאי מתקדם וטכנולוגיות נוספות, לא הוכחה כיעילה נגד מרגמות, ואף נשמעו קולות שהביעו חשש מכך שקבוצות טרור קיצוניות כמו חזבאללה וחמאס ינסו לעקוף אותה באמצעות ירי מטחים כבדים של רקטות זולות, וכך יאלצו את צה"ל להוציא סדר גודל של 50,000 דולר על יירוט. עם זאת, כפי שדובר צה"ל הגיב בנושא זה, "הנושא הוא מעבר לעלויות. [מערכת 'כיפת ברזל'] עתידה לספק לנו מענה".[44]

בתחילת שנת 2012, נראה מענה זה קרוב מתמיד, לאור ההצלחה של מערכת "כיפת ברזל" בניסויי יירוט של טילי קסאם וקטיושות ארוכות טווח – נשק שידוע כנמצא במאגר של חזבאללה וחמאס בכמות של אלפי יחידות. בניסויים

מוצלחים אלה עשתה המערכת שימוש במכ"ם שמזהה את הטיל המגיע ומשגר אליו טיל קינטי המיירט אותו. המכ"ם גם הצליח לזהות מתי טיל עתיד ליפול בשטח פתוח, וכך לחסוך שיגור של טיל מיירט על מטרה שאינה מהווה איום.[45] החיסול הממוקד שביצע חיל האוויר בחבר בכיר בארגון הטרור הפלסטיני "ועדות ההתנגדות העממית" במארס 2012 עודד את חידוש מטחי הירי של טילי קסאם מתוך רצועת עזה, כאשר עד לסוף אותו חודש נורו כ־250 מהם על דרום ישראל. מערכת "כיפת ברזל", שכבר הפכה אז למבצעית, יירטה בהצלחה כמעט תשעים אחוזים מהטילים שאיימו לנחות בשטח מיושב.[46]

מפגן ביצועים מעודד זה של מערכת "כיפת ברזל" בטבילת האש הראשונה שלה קיבל אישור מקיף ומוחלט כשמונה חודשים לאחר מכן במבצע "עמוד ענן" בנובמבר 2012, שכלל מתקפה אווירית בת שמונה ימים של צה"ל על חמאס ברצועת עזה. מתקפה זו החלה בתגובה לירי הרקטות על דרום ישראל בחודשים שקדמו לה, שהסלים בהדרגה, ככל הנראה לאור העידוד ששאבו מנהיגי חמאס ממה שנתפש בעיניהם כהתפתחות חיובית מבחינתם של "האביב הערבי" במצרים ובמקומות אחרים בעולם האסלאמי.[47] במכת פתיחה מפתיעה ומדויקת, שהתאפשרה הודות למודיעין מבצעי בזמן אמת, הצליח חיל האוויר לחסל את מפקד הזרוע הצבאית של חמאס, אחמד אל־ג'עברי, בשעה שנע ברכב נוסע. במהלך שמונת ימי המבצע השמיד חיל האוויר בשיטתיות אתרים לאחסון טילים שבידי חמאס, וכן מתקני פיקוד ובקרה ונכסים צבאיים חיוניים אחרים בכל רחבי רצועת עזה.

בניגוד גמור לניסיונה הקודם בלבנון ב־2006 וברצועת עזה ב־2008–2009, הפעם הקפידה ממשלת ישראל על כך שיעדים מדיניים, לצד מאמצים דיפלומטיים להשגתם, הם שיכתיבו את הפעילות הקרבית של צה"ל. ממשלת נתניהו התייחסה למתקפה על חמאס כאל משא ומתן מזוין יותר מאשר כאל מלחמה כוללת וחתרה ביודעין להפסקת אש מוסכמת, תוך הסתייעות משמעותית בנשיא מצרים הנבחר מוחמד מורסי. המטרה הייתה הפסקה ארוכת טווח של הירי מצד חמאס על ישראל, וזאת בתמורה להקלות הדרגתיות במצור על רצועת עזה – מצור שתכליתו למנוע הזרמת משלוחי נשק סודיים לחמאס מאיראן ומסוריה דרך חצי האי סיני. ממשלת ישראל חתרה להפסקת אש למן הרגע הראשון, מתוך מודעות מלאה לכך שכדי להשיג את יעדיה המדיניים היא תאלץ לשלם מחיר של הימנעות מפעולה צבאית קרקעית מקיפה ומכריעה נגד חמאס. צדק שר הביטחון אהוד ברק, שאמר על רקע התקדמות המגעים להפסקת אש: "חמאס לא ייעלם, אבל הזיכרון של חוויה זו יישאר חקוק אצלו לזמן רב, וזה מה שישקם את ההרתעה".[48]

פרץ האלימות האחרון בין ישראל לחמאס והתגובה המוצלחת של צה"ל הצביעו על שני יתרונות נלווים נוספים שהצטברו מאז מבצע "שינוי כיוון". ראשית, חזבאללה צפה בהתפתחויות מהצד בעניין רב, כשהוא עֵד לשמונה הימים

שבהם ניחתו מכות על חמאס ולכך שמערכת "כיפת ברזל" הצילה חיי ישראלים רבים ומנעה נזק משמעותי שהיה עלול להיגרם משיגור הרקטות של חמאס עד לכניסת הפסקת האש לתוקף.[49] הוא נמנע במתכוון מכל ניסיון לפתוח חזית שנייה מול ישראל בגבולה הצפוני ולא הצטרף לירי הטילים של חמאס. ריסון זה מלמד שההרתעה הישראלית מול חזבאללה לא רק שנותרה ללא פגע, אלא אף גברה הודות לביצועים המרשימים של "כיפת ברזל". אמנם, זמן קצר לאחר תום העימות בין ישראל לחמאס הזהיר נסראללה בהפגנתיות שלוחמיו ישגרו את "אלפי" הטילים שבידיהם על תל אביב וירושלים במקרה של מלחמה עתידית בין ישראל לחזבאללה, אולם כהוכחה לכך שמעשים חזקים ממילים, ארגונו דאג שלא לנקוט אף פרובוקציה ממשית נגד ישראל שעלולה הייתה להביא לנקמה מאסיבית נוספת מצד צה"ל על נכסיו בכל רחבי לבנון. יתרה מכך, וכפי שהיה מאז מלחמת לבנון השנייה, נסראללה נשא את הצהרתו המאיימת אך הריקה מתוכן לא בציבור, אלא באמצעות וידאו ממקום מסתורו.[50]

לאחר יותר משישה עשורים של פעילות צבאית, הליקויים שנחשפו בביצועי צה"ל בלבנון ב־2006 הביאו, אולי בפעם הראשונה, לתהליך הפקת לקחים משמעותי בקרב ראשי הצבא. לתהליך זה הייתה השפעה חיובית וברורה על ההתנהלות והתוצאות של המלחמה הראשונה של צה"ל ברצועת עזה שנתיים לאחר מלחמת לבנון השנייה, ודומה שתוצאותיו הגיעו לשיא בסבב השני המוצלח של צה"ל מול חמאס בנובמבר 2012. זאת, למרות ששנתיים קודם לכן קבע מומחה ישראלי כי התרבות הצבאית בישראל צריכה להטמיע "מערכות פורמאליות להפקת לקחים מהמבצעים שלה" וכי המסקנות המוסקות בצה"ל מניסיונות הלחימה הקודמים נוטות להתמקד בהיבטים צרים של טקטיקה וטכניקה.[51]

לאחר המבצע הבעייתי בלבנון ב־2006, ותחת מעורבותו האישית של רב־אלוף דן חלוץ, צה"ל השקיע מאמץ אמיתי ונחוש בן שישה חודשים לנתח ולהבין את כשלי "שינוי כיוון", תוך שילוב כל שלוש זרועותיו. מאמץ זה הוביל לשיפורים משמעותיים בשילוב בין כוחות היבשה ובין חיל האוויר ובתכנונים מבצעיים משותפים, דבר שבתורו הביא ליכולת המשופרת שהפגינה ישראל במבצעים "עופרת יצוקה" ו"עמוד ענן".[52] כל אחת מהתפתחויות אלו הייתה תוצאה טבעית וישירה של ביצועי צה"ל מול חזבאללה ב־2006. במבט על שש השנים שעברו מאז, ניתן לראות בהן תרומה נוספת לרווח שמצבה הביטחוני של ישראל השיג מהניסיון של מלחמת לבנון השנייה.

בהצהרתו המסכמת בפני ועדת וינוגרד, בינואר 2007, אמר הרמטכ"ל דאז דן חלוץ משפט שהיטיב לתמצת את נקודת המבט המעודדת הזו:

> כאשר אני שופט את התוצאות [של המבצע] לאור היעדים, וכאשר אני מסתכל על התוצאה הצבאית, לפיה יצרנו מצב צבאי משופר שבו חזבאללה נחלש

> וממשלת לבנון הפנימה שעליה ליישם את אחריותה בכל שטחי לבנון... אני סבור כי... נקודת הפתיחה כיום טובה לאין ערוך בהשוואה למה שהיה לפני פרוץ המלחמה. אני לא יכול לומר כמה זמן זה יימשך, אך מה שכן אוכל לומר הוא שכבר עכשיו זו התקופה הארוכה ביותר אי־פעם שבה המצב הנוכחי נשמר לאורך הגבול... מנקודת מבט צבאית, [חזבאללה] ספג מכה שכמוה מעולם לא חווה.[53]

דומה שהערכה אופטימית זו זכתה לפחות עד עתה לשפע של הוכחות, לאור התנהגותו הזהירה של חזבאללה במהלך השנים שחלפו.

הערות

1 Amos Harel and Avi Issacharoff, *34 Days: Israel, Hezbollah and the War in Lebanon*, New York: Palgrave Macmillan, 2008, p. ix.

2 Benjamin S. Lambeth, "An Airpower Failure? Hardly!," *Aviation Week and Space Technology*, October 10, 2011, p. 70.

3 ביחס לטענה השנייה: בעדות בפני הכנסת בתום השבוע הראשון ללחימה, דיווח רמטכ"ל צה"ל שחזבאללה חותר למשוך את ישראל למלחמת התשה מדממת, ולמרות שלצה"ל יש תוכניות מיידיות למתקפת נגד קרקעית, הוא עדיין אינו מוכן ליישם אותן בשל ודאות גבוהה למספר נפגעים רב שיהיה לכוחות צה"ל בכל מהלך כזה. ראו: Abraham Rabinovich, "Hezbollah Trained for Six Years, Dug Deep Bunkers," *The Washington Times*, July 21, 2006.

4 שני יעדים שאפתניים אלה, שהאמצעים להשגתם כלל לא היו בידי חיילי צה"ל, הוכרזו על ידי אולמרט ביום השישי למבצע בנאום לכנסת, שניתן היה להבין ממנו שלא קדם לו דיון אסטרטגי מעמיק. יש לציין שמטרות אלו לא נמנו על יעדי המבצע הצנועים יותר שהמטה הכללי של צה"ל קבע באופן רשמי לכוחות בתחילת מבצע "שינוי כיוון", Harel and Issacharoff, *34 Days: Israel, Hezbollah, and the War in Lebanon*, pp. 107-108.

5 פירוט מלא של טיעון זה ראו: Lambeth, *Air Operations in Israel's War against Hezbolla*.

6 William M. Arkin, *Divining Victory: Airpower in the 2006 Israel-Hezbollah War*, Maxwell AFB, Ala.: Air University Press, 2007, p. 147.

7 "Testimony by Lieutenant General Dan Haloutz, IDF Chief of Staff, to the Winograd Commission Investigating the Second Lebanon War," unpublished English translation from the Hebrew, Jerusalem, January 28, 2007.

8 שם. מלחמת לבנון הראשונה, שהתחילה ב־1982 והגיעה לסופה עם נסיגתה המלאה של ישראל מלבנון בשנת 2000, גרמה לכמעט 600 חיילים ישראליים הרוגים במהלך 18 שנים. התפישה הרווחת בקרב חיילי צה"ל היא שהייתה זו "וייטנאם הישראלית".

9 ראיון עם תא"ל איתי ברון, בעת היותו מפקד מרכז דדו לחשיבה צבאית בין־תחומית, גלילות, 26 במארס 2008.

10 Dan Haloutz, *At Eye Level*, Yediot Books, Tel Aviv, 2010. (לפי תרגום לאנגלית שלא פורסם).

11 Eyal Zisser, "Nasrallah's Defeat in the 2006 War: Assessing Hezbollah's Influence," *Middle East Quarterly*, 16, no. 1 (2009), pp. 27-35.

12 Lambeth, *Air Operations in Israel's War against Hezbollah*, pp. 29-36. בנאום פומבי נדיר שנשא נסראללה ממקום מסתורו ב־18 ביולי 2012 והועבר בווידאו, במסגרת חגיגות יום השנה השישי למה שכינה "הניצחון האלוהי" על ישראל, הוא

התייחס במיוחד למכה המקדימה שהנחית חיל האוויר על מאגר הטילים הסודי של חזבאללה. נסראללה הכחיש שהפעולה הצליחה וטען שארגונו "ידע שישראל יודעת היכן ממוקמים הטילים", ולכן הצליח מבעוד מועד "לשנות את מיקומם מבלי שישראל תדע מכך" – כאילו די בלומר זאת כדי להפוך את הדברים לנכונים! מצוטט מתוך: "Sayyed Hassan Nasrallah, *Now Lebanon*," http://www.nowlebanon.com/NewsArchiveDetails.aspx?ID=420450

13 Amir Kulick, "The Next War with Hizbollah," *Strategic Assessment*, 10, no. 3 (2007), pp. 41-50.

14 Isaac Ben-Israel, *The First Israel-Hizbollah Missile War*, Program for Security Studies, College of Policy and Government, Tel Aviv University, Tel Aviv, May 2007, p. 19. (לפי תרגום מעברית שלא פורסם)

15 Martin Van Creveld, "Israel's Lebanese War: A Preliminary Assessment," *Journal of the Royal United Services Institution*, October 2006, p. 43.

16 Ronen Manelis, "Between Lebanon and Gaza: Hizbollah in Operation Cast Lead," *Military and Strategic Affairs*, 1, no. 1 (2009); pp. 43-50.

7 Ben Caspit and Jackie Hugi, "Speech of the Panicked Mice," *Maariv*, September 25, 2006.

18 Colum Lynch and Robin Wright, "Peace Resolution for Lebanon Unanimously Approved at UN," *The Washington Post*, August 12, 2006.

19 Steven Erlanger, "Israel Committed to Block Arms and Kill Nasrallah," *The New York Times*, August 20, 2006.

20 Gabriel Siboni, "From Gaza to Lebanon and Back," *Strategic Assessment*, 10, no. 1 (2007); pp. 66-69.

21 Guermantes E. Lailari, "The Information Operations War between Israel and Hizballah during the Summer of 2006," in James J. F. Forest (ed.), *Influence Warfare: How Terrorists and Governments Fight to Shape Perceptions in a War of Ideas*, Westport, Conn.: Praeger Security International, 2009, p. 322.

22 Greg Myre and Helene Cooper, "Israel to Occupy Area of Lebanon as Security Zone," *The New York Times*, July 26, 2006.

23 "Hezbollah Chief Revisits Raid," *The Washington Post*, August 28, 2006.

24 Thomas L. Friedman, "Not So Smart," *The New York Times*, July 19, 2006.

25 Ben-Israel, *The First Israel-Hezbollah Missile War*.

26 Jim Storr, "Reflections on the War in Lebanon," *Journal of the Royal United Services Institution*, April 2007, p. 71.

27 Benjamin S. Lambeth, "Forging Jointness under Fire: Air-Ground Integration in Israel's 2006 War against Hezbollah," *Joint Force Quarterly*, 66, no. 3 (2012), pp. 48-53.

28 Ron Tira, "Shifting Tectonic Plates: Basic Assumptions on the Peace Process Revisited," *Strategic Assessment*, 12, no. 1 (2009), pp. 91-107, especially pp. 100, 102.

29 Sanu Kainikara and Russell Parkin, *Pathways to Victory: Observations from the 2006 Israel-Hezbollah Conflict*, Canberra: Royal Australian Air Force, Air Power Development Centre, October 2007, p. 17.

30 Andrew F. Krepinevich Jr., "The Pentagon's Wasting Assets: The Eroding Foundations of American Power," *Foreign Affairs*, July/August 2009, p. 24.

31 Tira, "Shifting Tectonic Plates," p. 102.

32 Roni Bart, "The Second Lebanon War: The Plus Column," *Strategic Assessment*, 9, no. 3 (2006), pp. 16-17.

33 Ben Caspit, "First, Let's Win," *Maariv*, August 11, 2006.

34 Gabriel Siboni, "From the Second Intifada through the Second Lebanon War to Operation Cast Lead: Puzzle Pieces of a Single Campaign," *Military and Strategic Affairs*, 1, no. 1 (2009), pp. 25-33, especially pp. 28-29.

35 Itai Brun, "The Second Lebanon War as a 'Wake-Up Call': A Strategic Perspective and Major Lessons Learned," Glilot, Israel: Dado Center for Interdisciplinary Military Studies, undated briefing charts.

36 Michael Oren, "Time Is Short for Iran Diplomacy," *The Wall Street Journal*, August 7, 2012.

37 Bret Stephens, "Plotting the Next Mideast War," *The Wall Street Journal*, April 10, 2010.

38 Ronen Bergman, "Israel's Secret War on Hezbollah," *The Wall Street Journal*, October 10, 2009.

39 Ibid.

40 *Al Manar television* (Beirut), February 13, 2009.

41 יש הסבורים שהמתקפה של המחבל המתאבד איש חזבאללה, שהרגה חמישה תיירים ישראלים בבורגס שבבולגריה ב־18 ביולי 2012, הייתה פעולת גמול על הרג מורנייה. אולם הסבר סביר יותר לאותה תקרית הוא שהייתה זו פעולת גמול ישירה על הרג מדעני גרעין איראנים. איראן, הגורם המממן והמפעיל המרכזי שמאחורי חזבאללה, הטילה את האשמה לכך על סוכנים ישראלים. ראו:
Nicholas Kulish and Eric Schmitt, "Hezbollah Is Blamed for Attack on Israeli Tourists in Bulgaria," *The New York Times*, July 19, 2012.

42 Bergman, "Israel's Secret War on Hezbollah".

43 Ibid.

44 Howard Schneider, "Israel Finds Strength in its Missile Defenses," *The Washington Post*, September 19, 2009.

45 Yaakov Katz, "Iron Dome Successfully Intercepts Kassam, Katyusha Barrages," *The Jerusalem Post*, July 15, 2010.

46 Sheera Frenkel, "Israel Sees New Advantage in Iron Dome Anti-Missile System," *McClatchey*, March 26, 2012.

47 לאחר השקט היחסי בעקבות סיומו המוצלח של מבצע "עופרת יצוקה", היו בשנת 2010 365 מקרים של ירי מרגמות ורקטות מרצועת עזה לדרום ישראל; 680 ב־2011; ו־800 לאורך מרבית שנת 2012, מתוכם 171 בחודש אוקטובר 2012 בלבד (Peter Beinart, "Israel's Fatal Game," *Newsweek*, November 26, 2012). על תגובת חיל האוויר לפרובוקציות אלו אמר אל"ם (מיל') גבי סיבוני: "חייבים לשמר את ההרתעה. זו הייתה רק שאלה של זמן עד שהרגע יגיע". ראו: Isabel Kershner and Fares Akram, "Ferocious Israeli Assault Kills a Leader of Hamas," *The New York Times*, November 15, 2012.

48 Nidal al-Mughrabi and Jeffrey Heller, "Israel, Gaza Ceasefire Agreed to, Hamas Official says, Israel Denies," *Reuters*, November 20, 2012.

49 חמאס שיגר לכל אורך שמונת ימי המבצע 1,506 רקטות לשטח ישראל מרצועת עזה. מבין אלו שזוהו כעתידות לפגוע באזורים מאוכלסים, מערכת "כיפת ברזל" ירטה 421 רקטות. רק 58 רקטות נחתו באזורים עירוניים. בכך הגיע שיעור ההצלחה של המערכת

לכמעט תשעים אחוזים. בסך הכל נהרגו חמישה ישראלים מירי רקטות. ראו:
"IDF Newsletter: IDF Ends Operation Pillar of Defense," newsletter@idfblog.com, November 21, 2012.

50 Bassem Mroue, "Hezbollah Chief Says Rockets Would Hit Tel Aviv in War," *The Washington Post*, November 26, 2012.

51 Dima Adamsky, *The Culture of Military Innovation: The Impact of Cultural Factors in the Revolution in Military Affairs in Russia, the U.S. and Israel*, Stanford, CA: Stanford University Press, 2010, p. 124.

52 להערכה כיצד מאמץ מרוכז זה השתלם בתכנון ובביצוע שצה"ל הפגין במבצע "עופרת יצוקה", ראו:
Benjamin S. Lambeth, "Israel's War in Gaza: A Paradigm of Effective Military Learning and Adaptation," *International Security*, 37, no. 2 (2012), pp. 81-118.

53 "עדותו של רב־אלוף דן חלוץ, רמטכ"ל צה"ל, בפני ועדת וינוגרד לחקירת אירועי מלחמת לבנון השנייה", ע"מ 75.
http://www.news1.co.il/uploadFiles/343868434429169.pdf

להגנת וירוס הסטקסנט

ג'יימס א. לואיס

גילויים חדשים על הווירוסים 'סטקסנט' (Stuxnet) ו'פליים' (Flame) עוררו שוב מקהלה של אזהרות דחופות מפני סכנות מלחמת סייבר והצורך בפעולה. אך השאלה המטרידה יותר שעולה בעקבות חשיפת הווירוסים היא – אם לוחמת סייבר היא נושא כה קריטי – מדוע אנשים כה רבים מחזיקים במידע כה שגוי לגביה? הדעה ש"'סטקסנט' או 'פליים' הגבירו את הסיכון מעידה על הבנה לקויה של מידת הסיכון שכבר קיימת במרחב הסייבר, של התדירות הגבוהה של פעולות סייבר זדוניות[1] שכבר מתקיימות בחסותן של מדינות ושל הצמיחה המהירה ביכולות הלוחמה של מדינות רבות. לכן, נכון יותר לראות את 'סטקסנט' ו'פליים' כפרק נוסף בתחרות המתמשכת בין ארצות־הברית, איראן ורוסיה.

האמונה ש'סטקסנט' מגביר את הסיכון לארצות־הברית או לבעלות־בריתה מתבססת על מספר הנחות מוצא שגויות. תפיסות הטוענות למכות נגד, נזק נלווה או פתיחת 'תיבת פנדורה' אינן מתקבלות על הדעת לאור היקף הפיתוח והשימוש בטכניקות מתקפת סייבר במהלך שלושת העשורים האחרונים. 'סטקסנט' לא חשף יכולת לוחמה חדשה שאחרים יזדרזו להעתיק. מתקפת סייבר היא יכולת מודיעינית וצבאית מוכרת שנמצאת בשימוש במשך שנים רבות. ההערכה היא שכארבעים מדינות מצטיידות ביכולות לוחמת סייבר או השיגו אותן כבר,[2] לרבות היכולת לשגר מתקפות סייבר. רוב התוכניות הלאומיות אפופות סודיות, ואין הסכמה בשאלה עד כמה החוק הבינלאומי הקיים, שתקף לעימות מזוין, אמור לחול על מצב ההתקפה החדש. עם זאת, כל צבא מתקדם כבר מצויד ביכולת לוחמת סייבר, ומדינות רבות אחרות שואפות להשיגה.

ההאשמה כלפי תפקידה של ארצות־הברית ב'סטקסנט' לא הייתה הפתעה מיוחדת. רוב המדינות כבר הגיעו למסקנה שארצות־הברית הייתה אחראית לכך, ולא נדהמו להיווכח שתוכנה הופכת לכלי התקפי ולאמצעי כפייה. השימוש

ג'יימס א. לואיס הוא חוקר בכיר ומנהל של תכנית למדיניות טכנולוגית ומדיניות ציבורית במרכז ללימודים אסטרטגיים ובינלאומיים – Center for Strategic and International Studies (CSIS).

בטכניקות סייבר ככלי מודיעין החל בשנות השמונים. מתקפת סייבר מצד צבאות החלה בשנות התשעים.[3] פיתוח טכניקות סייבר התקפיות הואץ בשנות האלפיים, כאשר התרחבה זמינותן של רשתות גלובליות מהירות, והאינטרנט הפך מכלי עזר לתשתית מרכזית לפעילות כלכלית וממשלתית. בין אם מדובר בלוחמה שהיא "מוכוונת רשת" או לוחמה ב"תנאי מידוע" (informatized conditions – כפי שסין מגדירה זאת), מתקפת סייבר אינה חדשה למתכננים צבאיים.

מריגול למתקפה

למרות ש'סטקסנט' ו'פליים' התקבלו בהתלהבות כמבשרי עידן מלחמת הסייבר, גישה זו שגויה בכמה מישורים. מתקפת סייבר אינה דבר חדש, ולמרות שחבלה עשויה לערב שימוש בכוח, לא כל פעולת חבלה שקולה לפעולת מלחמה. ההתייחסות ל'סטקסנט' ו'פליים' כאל לוחמת סייבר מנציחה את ההנמקה האנלוגית השגויה והמוגזמת שדבקה בחקירת תחום אבטחת סייבר מראשית ימיה. יש לראות ב"מתקפת" סייבר ארסנל חדש של כלים לכפייה, לריגול ולמתקפה, יותר מאשר קטגוריית עימות ייחודית וחסרת־תקדים.

הקו המפריד בין ריגול למתקפה במרחב הסייבר הוא דק מאוד. יכולות החדירה לרשת והשליטה בה, שנדרשות לשם ריגול, עלולות לשמש לשיבוש שירותים חיוניים. יריב שמצליח להשיג גישה מבוקרת לרשת יכול גם לפגוע ואולי אף להרוס. אפשר לראות במתקפת סייבר סוג של "חימוש" ("weaponization") של מודיעין האותות (SIGINT) – המרת איסוף מידע פסיבי בשיבוש אקטיבי. פירוש הדבר הוא – אם למקם את המונח "פירוק נשק קיברנטי" בהקשרו הנכון – שאיסור על מתקפת סייבר יחייב גם איסור על ריגול – פעילות ששום מדינה לא תסכים לזנוח.

'פליים' היה רק אחד מבין תוכניות רבות לאיסוף מודיעין שנמצאות באינטרנט. כיום ידוע על כתריסר תוכניות דוגמת 'פליים' ששימשו לריגול סייבר. הטכנולוגיה שינתה את האופן שבו מדינות מרגלות זו אחר זו, וריגול סייבר הפך למרכיב מרכזי בתוכניות לאומיות לאיסוף מידע. האינטרנט יצר את מה שקציני מודיעין מכנים "תור הזהב" של הריגול.

"תור הזהב" הזה נכנס כבר לעשור השלישי שלו. בתחילת שנות השמונים השתמשו שירותי הביון הרוסיים בהאקרים (פצחנים) ממערב־גרמניה כדי לחדור לצבא ארצות־הברית, לחקור רשתות ולשאוב מידע. שירותי הביטחון הסיניים ניהלו מערכות ארוכות ומוצלחות נגד הרשתות של ארצות־הברית ובעלות־בריתה, והיו מעורבים בריגול תעשייתי נרחב בחסות המדינה. אם 'סטקסנט' הצביע לכיוון ארצות־הברית וישראל כמדינות שעשויות להפיק את הרווח הגדול ביותר משיבוש מאמצי הגרעין של איראן, ניתן לשאול איזו מדינה עשויה להרוויח מהשקעת משאבים עצומים במעקב אחר פעילי זכויות אדם בטיבט. ב־15 השנים האחרונות,

תוכניות איסוף רבות כמו 'פליים' הפכו ציבוריות. יש להניח שקיימות תוכניות נוספות המוסתרות טוב יותר. לצורכי ריגול, טכניקות סייבר הן במידה רבה הרחבה של יכולות מודיעין אותות מסורתיות, ומבחינתה של סין, מדובר בהרחבה של גישה מבוזרת העושה שימוש בסוכנים אזרחיים רבים, כפי שניתן לראות בתוכניותיה של סין לאיסוף מידע אנושי.

הן סין והן רוסיה משתמשות באקספלויטים (קודי מקור של פקודות תוכנה משבשות) בסייבר בדרכים שונות מאשר פעילויות הסייבר של שירותי המערב, מבחינת החשיבות והפוטנציאל שלהן לגרימת חוסר יציבות. שתי המדינות מסתמכות על גורמים שלוחים (פרוקסי) – פצחנים (האקרים) פרטיים הפועלים על פי הכוונת המדינה למטרות ממשלתיות. גורמים אלה מספקים דרגה קלושה למדי של יכולת הכחשה (במקרה שמשקיף רציני כלשהו אכן מאמין שסין ורוסיה אינן שולטות ברשתות שלהן), לצד חזית קדמית של תוקפים שיכולים לגונן על פעולות המדינה, ואם נדרש, גם "יקריבו" אותם על מנת לפייס מדינות אחרות. השלוחים הרוסיים התמקדו בפשעים פיננסיים, והסינים התמקדו בריגול תעשייתי. שתי המדינות מספקות רמה מסוימת של הדרכה ותמיכה לשלוחים שלהן, ומתעקשות רק על כלל מרכזי אחד – שלא יפעלו נגד יעדים מבית. כל עוד כלל זה נשמר, ובמקביל השלוחים מבצעים את המשימות שהמדינה מעבירה להם, הם חופשיים לפעול נגד מטרות בארצות אחרות. פצחנים רוסיים היו אחראיים לאקספלויטים נגד אסטוניה וגאורגיה (בגאורגיה היה תיאום מדויק עם תוכניות הצבא הרוסי), ואילו הסינים היו אחראיים לשאיבת נתונים מיעדים צבאיים וכלכליים רבים, בארצות־הברית ובמדינות אחרות.[4]

לעומת זאת, ארצות־הברית ובעלות־בריתה אינן עושות שימוש בשלוחים מטעמן לצורך מעורבות בפשעים פיננסיים בחסות המדינה, וארצות־הברית אינה מעורבת בריגול תעשייתי. הדוקטרינה האמריקנית לשימוש בטכניקות סייבר כהרחבה של אמצעי כפייה מסורתיים דוגלת בגישה שונה, אם כי בהחלט לא חסרת־תקדים.

מתקפת סייבר ותהליך ההתחמשות (Weaponization) של מודיעין האותות

יכולות כמו אלה של 'סטקסנט' משקפות שנים של פיתוח וניסויים בניצול רשתות דיגיטליות להשגת כוח צבאי. וירוס 'סטקסנט' צויד ביכולות הרס מתקדמות משום שתוכנן להשפיע על מערכות בקרה תעשייתיות – מחשבים ייעודיים המפעילים מכונות – אך למעשה הוא היה רק הרחבה ושיפור של טכניקות מתקפת תוכנה קיימות. היכולת להשתמש בתוכנה לשיבוש מערכות בקרה תעשייתיות ולגרום הרס פיזי הומחשה כבר בניסוי שנערך במעבדה הלאומית של איידהו (ארצות־

הברית) ב־2005. ההערכה היא שחמש מדינות מחזיקות ביכולת זו – ארצות־הברית, בריטניה, ישראל, רוסיה וסין, ומדינות רבות נוספות מנסות להשיג אותה. בהקשר זה ארצות־הברית יכולה להיחשב "ראשונה בין שוות", אך יש לה שותפים למעמד זה (או כמעט שותפים) בתחום מתקפת סייבר. 'סטקסנט' עשוי להיחשב ל"נשק" המתקדם ביותר מסוג זה (חותמת איכות אמריקנית נוספת), אך בשום אופן לא מדובר ביכולת ייחודית.

מתקפת סייבר היא אופציה נוספת הזמינה למתכננים צבאיים. במקרה של 'סטקסנט' למשל, המתכננים יכלו לשקול את היתרונות והחסרונות של מתקפת סייבר מול מתקפה אווירית, צוות מבצעי מיוחד, חבלנים או טילים. תורות הלחימה הקיימות הורחבו והותאמו למצב התקיפה החדש. מדינות יצרו יכולות מתקפת סייבר ופיתחו דוקטרינות ואסטרטגיות לשימושן. דוקטרינות לאומיות אלה אינן זהות בכל המדינות. אנו נמצאים בתקופת התנסות, שבה המדינות מעריכות יכולת צבאית חדשה זו וחוקרות מהי הדרך הטובה ביותר לנצל אותה. נוסף לשימוש שעשתה רוסיה ב"מתקפת" סייבר באסטוניה ובגאורגיה, והשימוש לכאורה שעשתה ישראל בסוריה, ראינו כיצד רוסיה וסין אוספות מידע לצורך מתקפות על תשתיות אמריקניות חיוניות (על פי ראש הסוכנות האמריקנית לביטחון לאומי),[5] ומשתמשות באיראן נגד ישראל ומדינות המפרץ. ארצות־הברית השתמשה במתקפות סייבר בשנות התשעים במהלך העימות עם סרביה, ונגד ההגנה האווירית של עיראק בין מלחמות המפרץ.

ארצות־הברית, רוסיה, סין ומדינות נוספות, כוללות בדוקטרינה שלהן לגבי שימוש צבאי במתקפת סייבר גם מתקפה על תשתיות חיוניות. הדוקטרינה הגלויה רומזת על כך שכל מדינה מקבלת החלטות על השימוש במתקפת סייבר באופן עקבי לתכנון השימוש שלה בסוגים אחרים של נשק ארוך־טווח – כגון שקלול יתרונות התקיפה, הסיכון בהסלמה והפוטנציאל לנזק נלווה. ניתן לראות בדוקטרינה האמריקנית כמה קוים מקבילים לחשיבה על הפצצה אסטרטגית ולשימוש בהפצצה אווירית להפחתת הנכונות והיכולת של האויב להתנגד, במקביל להימנעות מעימות ממושך עם כוחות צבאיים. הדוקטרינה הרוסית שמה דגש רב יותר על הפרת היציבות הפוליטית ועל שיבוש מערכות פיקוד צבאיות באמצעות טכניקות סייבר, בדומה לדוקטרינה הסובייטית שדגלה במכות פתיחה חזקות נגד נאט"ו באמצעות תקיפת תשתית חיונית. הדוקטרינה הסינית עמומה יותר, אך הדיון הציבורי מתמקד במתקפות על תשתיות במטרה לשבש יכולת אמריקנית להתערב במשברים אזוריים.[6]

כאשר בוחנים מתקפת סייבר בהקשר של קבלת החלטות צבאיות (בהנחה ששחקנים מדינתיים ושחקנים לא־מדינתיים חולקים לרוב תהליכי תכנון צבאי דומים), עולות ההשלכות של השימוש בה. הסבירות שמדינות ישגרו לעבר ארצות־

הברית או בעלות־בריתה מתקפת סייבר שתגרום נזק פיזי לא גברה בעקבות חשיפת 'סטקסנט', ובאותה מידה, אין סיכוי שמדינות אלה יפסיקו את השימוש בטכניקות סייבר לצורכי ריגול וכפייה פוליטית. הסיבה שאיננו עדים למתקפות שיכולות לגרום לארצות־הברית ולבעלות־בריתה נזק פיזי, הרס או נפגעים (בניגוד לריגול או לפשע) מצד המדינות שמחזיקות ביכולת כזו היא שמדינות אלה מעריכות שהסיכון לתגובה אלימה גבוה מדי. זו גם הסיבה שמונעת מהן לשגר מטוסים או טילים נגד ארצות־הברית. עם זאת, החוק והנוהג הבינלאומי אינם מצדיקים שימוש בכוח כתגובה לריגול ולפשע, וכך נעשה הסיכון לתגובה אלימה כזו נמוך וסביר.

הימנעות זו מתקיפה עשויה להשתנות ככל שמדינות אחרות, עם דרגת סובלנות אחרת כלפי סיכון, דוגמת איראן, ישיגו יכולות מתקדמות למתקפת סייבר, או כאשר גורמים שמעריכים באופן מופרז את יכולתם להישאר סמויים ישיגו יכולות מתקדמות. מה שאיננו יודעים הוא עד כמה התקדמו שחקנים לא־מדינתיים ביכולתם לפתח טכניקות הרסניות דומות. העובדה היחידה שאין עליה מחלוקת היא שעד היום לא ראינו שחקנים לא־מדינתיים המעורבים במתקפות כאלה. דבר זה עשוי לשקף היעדר מניע או יכולת, ולא ניתן להעריך באיזו מהירות עשויים גורמים אלה להשיג יכולת לבצע מתקפות דוגמת 'סטקסנט'.

לזכותם של מתכנני 'סטקסנט' ייאמר, שהוא נכתב בזהירות מספקת על מנת למנוע נזק נלווה. ייתכן שתוקפים אחרים לא יהיו כה זהירים, אך אין קשר בין עובדה זו לבין יכולת הגישה לקוד 'סטקסנט'. יריבים פוטנציאליים ממשיכים להתמודד עם אותם שיקולי בעד ונגד בהחלטתם האם להשתמש בכוח נגד ארצות־הברית, והם ימשיכו להירתע מהתגובה האפשרית של צבא ארצות־הברית לנוכח כל המשאבים הצבאיים שעומדים לרשותו מעבר למתקפת סייבר. אפשר שגורמים אלה יישענו על 'סטקסנט' כחלק מהצדקה ציבורית למתקפה, אך יהיה זה תירוץ בלבד ולא חלק מקבלת ההחלטות שלהם. הסיכוי שמדינות ישגרו מתקפת סייבר נגד ארצות־הברית או בעלות־בריתה בעקבות חשיפת 'סטאקסנט' אינו גבוה יותר מאשר הסיכוי שקדם לחשיפתו.

לאופן השימוש של צבאות בפוטנציאל של מתקפת סייבר יש השלכות המסבירות מדוע 'סטקסנט' ו'פליים' לא שינו באמת את מהלך העניינים. כמו לכל נשק, גם למתקפת סייבר יש מאפיינים משלה. מתקפות סייבר יכולות להיות מהירות וחשאיות ולהוות סיכון פוליטי מופחת בחלק מהתרחישים. החיסרון שלהן הוא תוצאה הרסנית פחות. מתכנן המתקפה ישקול היבטים אלה, ויעריך את הסבירות שמתקפת הסייבר תשיג את האפקט המבוקש ב"עלות" הנמוכה ביותר בהשוואה לאפשרויות מתקפה אחרות. בחלק מהתרחישים עדיפה מתקפת סייבר. החלופות ל'סטקסנט' כללו צוותי חבלה, התקפות אוויריות, ירי טילים או אפילו כיבוש שטח בידי כוחות קונבנציונליים. די ברשימה קצרה זו – שכל האפשרויות

בה כרוכות בסיכון רב יותר לאבידות, לאלימות ולהסלמה – כדי להראות מדוע מתקפת סייבר הייתה עדיפה.

יש מדינות שכבר עושות שימוש סדיר במתקפות סייבר בדרכים שמשרתות את צורכיהן. לאחרות יש יכולת להוציא לפועל מתקפה דוגמת 'סטקסנט', אך האסטרטגיה שלהן שמה דגש על יעדים אחרים, ועד היום לא היה להן עניין בגרימת נזק פיזי. רוסיה וסין הציגו יכולות מתקדמות, וביכולתן לשגר מתקפות דוגמת 'סטקסנט' אילו היה הדבר נתפס בעיניהן כמועיל. העובדה שהעימות בתחום סייבר נותר ברובו נסתר מעיני הציבור לפני 'סטקסנט', אין פירושה שהוא לא התקיים.

הנחה שגויה נוספת היא ש'סטקסנט' היה אירוע דוגמת הירושימה, בכך שהתיר את הרסן מכוח צבאי הרסני חדש וחסר־שליטה. אלא שכאן אין איש כאופנהיימר שידקלם בעקבות 'סטקסנט': "עתה הפכתי אני לכוח המוות, משמיד העולמות".[7] למרות הרצון המפתה לכאורה להשוות בין מתקפת הסייבר לנשק גרעיני, השוואה זו מופרכת מיסודה. גם לנשק גרעיני בקנה־מידה קטן ביותר יש כוח הרס עצום, אך למתקפות סייבר אין. הן מהוות נשק תמיכה, היעיל בעיצוב שדה הקרב לטובת המשתמש בו, אך השפעתן אינה כמו של הרס המוני או קטלני, ואין בכוחן להוות איום קיומי על מדינות. לכל היותר, ניתן להשוות מתקפת סייבר לטילים שמאפשרים מכה מהירה למרחק רב, עם מרכיב גדול יותר של סודיות (אולי), לצד תוצאה הרסנית פחות. יכולת הרס מוגבלת זו – אין פירושה שניתן לקדם בברכה שיבוש שנגרם מבהלה פיננסית מלאכותית או מהפסקת חשמל שנמשכת שבועות ארוכים, אך עלינו להימנע גם מהגזמה בהשפעה המיוחסת למתקפת סייבר.[8] 'סטקסנט' הפנה את תשומת הלב לפגיעותה של התוכנה המודרנית, אך הכוח ההרסני של מתקפת סייבר אינו קרוב כלל לזה של נשק גרעיני, או אפילו לזה של מתקפה בנשק קינטי.

התחרות האזורית

קוד 'סטקסנט' זמין עתה לציבור, ויש החוששים שיהיו מי שישתמשו בו שוב, אולם יש בכך התעלמות מאחת המגבלות העיקריות של מתקפת סייבר – בדרך כלל מדובר באקספלויט חד־פעמי. ברגע שהמתקפה חושפת שגיאות תֵכנות חדשות ("zero days") או אחרות במערכות ההפעלה או במערכות בקרה תעשייתית, הן לרוב מתוקנות. קוד 'סטקסנט' שנגיש לציבור היה חלק מאקספלויט גדול ומורכב יותר, שכלל מגוון טכניקות ריגול. הקוד היה רק חלק מהאקספלויט, ואינו מספיק כשלעצמו. אם 'סטקסנט' ישוגר שוב הוא לא יפעל. ההוכחה הטובה ביותר לכך היא שבעוד מערכות רבות ברחבי העולם נדבקו בווירוס, רק אחת ניזוקה – באיראן.

איראן עלולה לגלות רצון לנקום על 'סטקסנט', אך אין זה חדש לאיראנים שארצות־הברית ומדינות אחרות מעורבות במבצעים חשאיים שמיועדים לעכב

את תוכניתם הבלתי־חוקית לפיתוח נשק גרעיני, ובאותה מידה, האיראנים מעולם לא הסתירו את תמיכתם באלימות נגד ארצות־הברית או ישראל. איראן אחראית למותם של אנשי סגל אמריקניים בביירות, במפרץ הפרסי ובעיראק. 'סטקסנט' הוא פרק נוסף בעימות שמתקיים בחשאי ומתלקח מדי פעם בין ארצות־הברית לבין איראן, כבר למעלה משלושים שנה.

איראן לא היססה גם להביע איומים, ולא הסתירה את רצונה לפתח ולהשתמש בטכניקות מתקפת סייבר. רטוריקה ארסית מצד מנהיגי איראן נגד ישראל עשויה להיות התרברבות גרידא שנועדה לקהל הביתי, אך אין בכך כדי להצדיק אותה. למדינות יש אחריות על אמירות פומביות של מנהיגיהן. לנוכח האיומים שנשמעו, ועל רקע ההפרות החוזרות של המחויבות הבינלאומית ביחס לנשק גרעיני, יהיה זה תמוה לומר שפעולה סמויה הכרוכה בשימוש בתוכנה נגד תוכנית הגרעין האיראנית אינה ראויה, מה גם שלא נגרמו פגיעות בנפש או נזק נלווה.[9]

המסקנה שארצות־הברית הייתה מעורבת ב'סטקסנט' גם היא אינה מפתיעה. לארצות־הברית היסטוריה של נקיטת פעולות חשאיות נגד משטרים אגרסיביים ובלתי־דמוקרטיים. היכולת פותחה במלחמת העולם השנייה (בחסות הבריטים), ושוכללה והורחבה במהלך המלחמה הקרה. אולם ארצות־הברית מעולם לא השתמשה בכוח חשאי נגד מדינה דמוקרטית או נגד מדינה שאינה מהווה כל איום על השלום הבינלאומי. ניתן להטיל ספק ביכולתה של ארצות־הברית לזהות איומים על השלום, ואכן נעשו טעויות רבות בעבר, אך איראן אינה אחת מהן. במקרים רבים עדיפה פעולה חשאית על פני תגובות צבאיות אחרות, שכן היא מפחיתה את הסיכון לעימות ישיר או להרחבת הסכסוך. פעולה חשאית היא שביל הזהב בין הסכמה שבשתיקה לבין מלחמה גלויה, היא כלי לגיטימי נוסף להגנתה של מדינה, גם אם יש מי שיתנגדו לכך.

ארצות־הברית מצדיקה התערבויות אלה בכך שהיא מובילה קואליציה של מדינות המגֵנות על הדמוקרטיה – תפקיד שהוטל עליה בעקבות מלחמת העולם השנייה והמלחמה הקרה. תפקיד זה היה מקובל באופן כללי על הקהילה הדמוקרטית בין השנים 1941 ל־1990. גם אם איננו מקבלים את הטענה שארצות־הברית עדיין עומדת בראש קואליציה של מדינות להגנה על הדמוקרטיה, סיבה טובה המצדיקה נקיטת אמצעים אקטיביים כתגובה היא התנהגותה של איראן, המאיימת על ביטחונה של ארצות־הברית ועל שלום העולם.

היתרונות של 'סטקסנט' הם רבים, והצער היחידי שעלינו לחוש הוא שהתגלה מוקדם מדי. שיגור 'סטקסנט' הציב סיכון פוליטי נמוך הרבה יותר מאשר התקפות אוויריות. לא היה נזק נלווה, ולא שידור טלוויזיוני של בניינים עולים באש ואזרחים מבוהלים. לא הופל טייס ולא הוצעד ברחובות טהראן בדרך למתקן העינויים. הפיכת הקוד לנשק מלחמה עלתה הרבה פחות מאשר מטוס F16 אחד.

ההקשר הפוליטי החסר

הדגש שהושם על מלחמת סייבר בדיון הציבורי על 'סטקסנט' ו'פליים', הביא לכך ששאלות חשובות נותרו ללא התייחסות. כאשר אנו רואים שהיריב "חושף במקרה" פעולה חשאית ומורכבת, ובייחוד אם הדבר קורה יותר מפעם אחת, עלינו לשקול הסברים שאינם צירוף מקרים גרידא. ההשערה שכדאי להתעמק בה היא החיבור האפשרי בין חשיפת הווירוסים הללו לבין רוסיה. הגילויים בנוגע לוירוס 'פליים' שירתו סדר־יום פוליטי רוסי רחב יותר, שעניינו משילות אינטרנט (internet governance) ואבטחת סייבר. הצבת 'סטקסנט' ו'פליים' בהקשר של ריגול ופעולה פוליטית חשאית עשויה לספק הסבר טוב יותר מאשר ההתמקדות בלוחמה, בייחוד כאשר האופן שבו פורסם המידע על 'פליים' עולה בקנה אחד עם מניפולציה פוליטית שנועדה לזכות בתמיכה במפגשים רב־צדדיים בנושא משילות אינטרנט, שעתידים היו להתקיים במהלך 2012. רוסיה ומדינות אחרות רוצות שאיגוד הטלקומוניקציה הבינלאומי (ITU) ישחק תפקיד גדול יותר באבטחת סייבר ובמשילות אינטרנט. תפקיד גדול יותר של ה־ITU יחתור תחת כל מה שנתפס כ"הגמוניה" אמריקנית במרחב הסייבר, ואולי אף יפחית את הסיכון לרוסיה, כתוצאה מהגישה הבלתי־מוגבלת למידע שהאינטרנט מציע. רוסיה עשויה אף לחתור ל"הכפשת" השימוש במתקפות סייבר ולהשיג תמיכה רחבה באמנה האוסרת שימוש בנשק דוגמת 'סטקסנט', כחלק ממאמציה לערער תחום שנתפס כיתרון של הצבא האמריקני. מדובר בתכסיס ידוע ביחסים בינלאומיים – הצעת מגבלות המכרסמות ביכולתו של היריב יותר מאשר בזו של המציע (בדומה למאמצים בשנות השמונים לתמרן את פירוק הנשק הגרעיני באירופה כדי להפחית מיכולותיהן של מדינות נאט"ו יותר מאלה של החברות בברית ורשה).

בכל הקשור לנושא זה קיימים קישורים בלתי־שגרתיים: מנכ"ל החברה שחשפה את 'פליים' היה דובר לא־רשמי של ממשלת רוסיה בוועידת הסייבר בלונדון ב־2011. בנובמבר 2011 הכריזו החברה שלו ו־ITU על הקמת שותפות לקידום אבטחת סייבר גלובלית.[10] החברה טוענת שחשפה את 'פליים' לאחר ש־ITU ביקשה ממנה – בקשה שהייתה חסרת־תקדים כשלעצמה – לבחון פריצות נתונים במזרח־התיכון, ועל בסיס זה הכריזה ITU על אזהרה גלובלית של אבטחת סייבר, שגם היא הייתה חסרת־תקדים.[11] ייתכן שהדברים הם בדיוק כפי שהם, אולם השערה חלופית שלא ניתן לדחות אותה על הסף, היא שמדובר בתמרון פוליטי גדול יותר שתכננו הרוסים, על מנת להשפיע על השקפתן של מדינות מפתח. השימוש בגורם שלוח (פרוקסי) לפרסום מידע מזיק על היריב הוא טכניקת ביון מוכרת, ורוסיה נשענת באופן ניכר על גורמים שלוחים בשיטות ריגול הסייבר שלה. מצבים חריגים אלה מרמזים ומצביעים על השערות חלופיות, שהסבירה ביותר היא ששירותים

מערביים יצרו את 'פליים' כדי לרגל אחר איראן, וכי רוסיה ניצלה את החשיפה למטרות פוליטיות.

בשנים האחרונות החלו רוסיה וסין (לעתים דרך 'ארגון שנגחאי לשיתוף פעולה') לפתח אסטרטגיה בינלאומית שתיצור אינטרנט המותאם יותר לאינטרסים שלהן. הן מאמינות שהשליטה הדומיננטית של המערב במידע היא חלק מאסטרטגיה גדולה יותר של הגמוניה, ולא רק תהליך שצמח מתוך כישלון המדינה להחזיק בלעדית במדיה. בעוד הן יכולות לדכא את האזרחים שלהן, הן אינן יכולות לדכא מקורות מידע זרים. רוסיה וסין השקיעו רבות בצְנזור טכנולוגיות, אך גם ביקשו הסכמה בינלאומית להגדרת מידע כנשק שחובה לפקח עליו. האינטרנט יוצר לחצים פוליטיים שלא קל למשטרים רודניים לשלוט בהם, והוא יכול להוות איום עליהם (באיזה היקף – זוהי שאלה אחרת). מאמצים נרחבים אלה להגביל את הגישה למידע ולהחליש את ארצות־הברית הם ההקשר הפוליטי של 'פליים'.

באותו זמן לערך ש'פליים' ו'סטקסנט' משכו תשומת לב כה רבה, תוכנת ריגול נוספת הצליחה לחמוק בשקט. שירות פרוקסי פופולרי (שמאפשר למשתמשי אינטרנט לחמוק מפיקוח ממשלתי) נפגע כך שכל אדם שהוריד את תוכנת הפרוקסי הוריד גם תוכנה זדונית שסיפקה את שם המשתמש ואת שם המחשב, ותיעדה את כל הקשות המקלדת. התוכנה הזדונית Simurgh פגעה באלפי אנשים. החוקרים שאיתרו אותה – אנשי Munk Schoolשבאוניברסיטת טורונטו – מאמינים שהיא נועדה למתנגדי משטר איראניים וסוריים.[12] התוכנה הזדונית יצרה סיכון גבוה הרבה יותר מאשר 'פליים', אך לא זכתה להתייחסות כה מרעישה, וה־ITU לא הוציא אזהרה גלובלית בעקבותיו. הסבר אפשרי לחריגות זו הוא ש'פליים' מתאים לסדר־יום פוליטי רחב יותר מאשר Simurgh.

הקשר בין 'פליים' לבין משא־ומתן בינלאומי על אבטחת הסייבר (ומשילות אינטרנט), מספק רקע חשוב למאמצים הרב־צדדיים להפוך את מרחב הסייבר לבטוח יותר. אחד ההיבטים שלא זכו לתשומת לב בפרשנות הציבורית בנושא לאחרונה הוא שהסיכון החדש ממתקפת סייבר הפך לחלק מסדר־היום הבינלאומי בתחום האבטחה כבר לפני שנים אחדות, כאשר החלו לצוץ הסיכונים הביטחוניים והצבאיים מקישוריות גלובלית במהירות גבוהה. מרחב הסייבר, שכמעט אינו נשלט או מאובטח, הפך עתה מקור לחוסר יציבות בינלאומית. מדינות חוששות מהסלמה שתהפוך בהיסח הדעת לעימות קינטי (צבאי) נרחב יותר מאשר מההשפעה המעשית של מתקפת סייבר, בהתחשב בפוטנציאל המוגבל לנזק שהיא נושאת. דיאלוג רציני בנוגע לאפשרויות הפחתת הסיכון מתקיים לפחות מאז שרוסיה הפעילה טכניקות סייבר נגד אסטוניה ב־2007. ה"מתקפות" נגד אסטוניה ב־2007 היוו סכנה רבה יותר ליציבות הבינלאומית מאשר 'סטקסנט', שכן הן איימו לעורר עימות מזוין בין מדינות נאט"ו לבין רוסיה.

כתוצאה מכך, מתקיימים דיונים בפורומים רשמיים רבים בשאלה כיצד להפחית את הסיכון ולהגביר את היציבות, ביניהם קבוצת מומחי הממשל מטעם האו"ם (UN's Group of Government Experts), הארגון למען יציבות ושיתוף פעולה באירופה (Organization for Stability and Cooperation in Europe), הפורום האזורי של אסיה (Asian Regional Forum) וועידת לונדון (London Conference Process). ארגון מדינות אמריקה (Organization of American States) ערך מפגשים בנושא אבטחת סייבר. ארצות־הברית, רוסיה וסין מעורבות בדיאלוגים בנושא, וארצות־הברית משתתפת בדיונים דומים עם בעלות־בריתה הקרובות. תיאורם של 'סטקסנט' ו'פליים' כסכנה חמורה חדשה הוא אמצעי רטורי להשגת יתרון במשא־ומתן, יותר מאשר ניתוח רציני של מצב הביטחון הבינלאומי.

מסקנות

צבאות שמצטיינים בקדמה טכנולוגית יצרו טכניקות סייבר, ויעשו בהן שימוש כדי לקדם את האינטרסים שלהם. גם אם אין מדובר ב"לוחמה", בכל זאת קיים עימות. אם 'סטקסנט' ו'פליים' מהווים סיכון כלשהו, הסיכון הוא שחוסר ידע צבאי ורקע הולם למשא־ומתן על אבטחת סייבר, לצד מה שנראה כאמונות טפלות בנוגע למתקפת סייבר – הם אלה שיסכלו את המאמצים להפוך את מרחב הסייבר לבטוח ויציב יותר. 'סטקסנט' ו'פליים' לא היו אפוקליפטיים. למעשה הם אינם חדשים במיוחד, וודאי שאינם מבשרי עידן חדש של לוחמה. הטכנולוגיה מעצבת מחדש את הלוחמה מאז המהפכה התעשייתית. אולי הדבר אינו לרוחנו, אך נדיר שמדינות וארגונים חמושים ינטשו יכולת חדשה. מדינות עשויות לדחות נשק להשמדה המונית, אך למעט זאת הכל קביל, ומתקפת סייבר אינה יוצאת מכלל זה. מדינות ימשיכו לנהוג כפי שתמיד נהגו, ופשוט ינצלו טכנולוגיות חדשות להשגת מטרותיהן.

הערות

1 ניתן להגדיר פעולת סייבר זדונית כתוכנה שנשלחת באמצעות רשתות דיגיטליות להשגת גישה לא־חוקית למחשבי היעד, ומבצעת פקודות ללא הרשאת הבעלים.

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

3 ספרו של קליפורד סטול (Clifford Stoll): *The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage* (New York: Doubleday, 1989) מספק פרטים על ריגול סייבר סובייטי בשנות השמונים. אמנם התקיים דיון ציבורי מועט בלבד על מתקפות סייבר מצד ארה"ב נגד סרביה בשנות התשעים, אך פקידים אמריקניים סיפקו פרטים בראיונות.

4 US Cyber Consequences Unit, "Overview by the US CCU of the cyber campaign against Georgia," August 2009, http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf.

5 The Guardian, "Militarisation of Cyberspace: How the Global Power Struggle Moved Online," April 2012, http://www.guardian.co.uk/technology/2012/apr/16/militarisation-of-cyberspace-power-struggle

6 ראו לדוגמה:
Steve DeWeese, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, Northrop Grumman, October 2009.

7 רוברט אופנהיימר, המדען שעמד בראש פרויקט פיתוח פצצת האטום, ציטט משפט זה מתוך ה"בהגאוואד גיטה" (Bhagavad Gita), בעקבות הניסוי המוצלח הראשון.

8 תרחישי "סייבר־בדומה־לגרעין" כרוכים בשרשרת ארוכה של הנחות מפוקפקות על ההשפעה הפוליטית של מתקפה ועמידות המטרה. לדיון מפורט, ראו:
James Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats," CSIS, December 2002, http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf.

9 ראו לדוגמה:
Robert Wright, "How Obama's Cyberweapons Could Boomerang," *The Atlantic*, June 2012; Misha Glenny, "We will Rue Stuxnet's Cavalier Deployment," *Financial Times*, June 2012, http://www.ft.com/cms/s/0/6b674600-afc7-11e1-a025-00144feabdc0.html#axzz25KCLvt33;
או:
Jason Healy, "Stuxnets are not in the US National Interest: An Arsonist Calling for Better Fire Codes," Atlantic Council June 2012.
שימו לב שהאירוע שעורר זעקה זו לא היה המתקפה עצמה אלא סיפור חדשותי על המתקפה, שממחיש את תפקידה של המדיה בדיונים אלה. רעש תקשורתי אינו מדד טוב לסיכון ממשי.

10 "ITU Teams Up with Kaspersky Lab for ITU Telecom World 2012," http://www.kaspersky.com/about/news/business/2012/ITU_Teams_Up_with_Kaspersky_Lab_for_ITU_Telecom_World_2012.

11 Kaspersky Lab and ITU Research Reveals New Advanced Cyber Threat," http://www.kaspersky.com/about/news/virus/2012/Kaspersky_Lab_and_ITU_Research_Reveals_New_Advanced_Cyber_Threat/.

12 Munk School of Global Affairs, "Iranian Anti-Censorship Software 'Simurgh' Circulated with Malicious Backdoor," May 2012, https://citizenlab.org/2012/05/iranian-anti-censorship-software-simurgh-circulated-with-malicious-backdoor-2/.

לוחמת הסייבר של איראן

גבי סיבוני וסמי קרוננפלד

מבוא

בשנים האחרונות גוברת ההבנה בקרב הציבור ומקבלי ההחלטות במדינות שונות, שמרחב הסייבר מחייב התייחסות מתאימה כאל מרחב לחימה של ממש – מרחב המספק כר נרחב ונקודות תורפה רבות לפעולה של תוקפים החפצים לשבש מערכות מידע, ואף לפגוע פגיעה פיזית במערכים של תשתית חיונית, המבוקרים על ידי מערכות בקרה תעשייתיות. כתוצאה מכך, עולה היקף ההשקעות ומתעצמים תהליכי בניין הכוח של מדינות רבות בתחום יכולות פעולה (הגנה, איסוף מודיעין ויכולות התקפיות) במרחב הסייבר בקצב גובר והולך. משנפגעה איראן על ידי מתקפת Stuxnet – שניתן להגדירה כאחת מהתקפות הסייבר ההרסניות ביותר – היא פועלת במרץ רב לשיפור ההגנה במרחב הסייבר מצד אחד, ומצד שני – לבניית יכולות איסוף מודיעין ויכולות התקפיות במרחב הסייבר.

מטרות ההגנה של איראן במרחב הסייבר כפולות. הראשונה – הרצון למנוע הישנות מתקפה דוגמת מתקפת Stuxnet וחדירות למחשבים אירניים לצורכי איסוף מודיעין, כגון הווירוסים 'דוקו' ו־Flame. בהקשר זה, מטרות הפעילות האיראנית דומות לאלה של מדינות רבות בעולם, המבקשות להגן על תשתיות חיוניות שלהן. המטרה השנייה נוגעת לרצון לשמור על שרידות המשטר האיראני על ידי מעקב וחסימה של מידע ושירותים מהציבור האיראני. במקרים רבים, הכלים להשגת שתי המטרות דומים. לדוגמה: הניסיון האיראני ליצור רשת תקשורת מבודלת באיראן, או הניתוק של שרותי 'גוגל' במדינה.[1]

עם זאת נמצאת איראן בתהליך רחב של בניין כוח גם בהקשר ההתקפי, מתוך ההבנה שבכל עימות עתידי, השימוש במרחב הסייבר הוא בעל חשיבות מכרעת להשגת היעדים מול אויבי המדינה. מטבע הדברים, קיים קושי רב באיסוף מידע גלוי באשר ליכולות הסייבר האיראניות, ובייחוד ביחס ליכולות ההתקפיות של

ד"ר גבי סיבוני הוא ראש התכניות "צבא ואסטרטגיה" ו"לוחמת סייבר" במכון למחקרי ביטחון לאומי.
סמי קרוננפלד הוא מתמחה בתכנית "לוחמת סייבר" במכון למחקרי ביטחון לאמי.

המדינה. אורו של הזרקור על פעילות הסייבר של איראן הועצם לאחרונה, עקב חשד שאיראן הייתה מעורבת במספר אירועי סייבר חמורים, ביניהם גניבה של הרשאות אבטחה באינטרנט, תקיפת הרשת הארגונית של חברת הנפט הסעודית ולבסוף – חדירה למחשבי בנקים מרכזיים בארצות־הברית. מאמר זה מבקש להציג תמונה עדכנית ביחס למספר מרכיבים בתהליך הפיתוח של איראן בתחום הסייבר. חלקו הראשון הינו ניתוח של האסטרטגיה האיראנית במרחב הסייבר. החלק השני מפרט את המענה הארגוני והאופרטיבי של איראן לאסטרטגיה שגובשה. חלק זה בוחן שלושה מרכיבים: תשתיות ההכשרה ופיתוח כוח האדם הטכנולוגי בתחום הסייבר, תהליכי התעצמות טכנולוגיים ותהליכי בניין הכוח הכוללים בתחום הסייבר. לבסוף נבחנות מספר פעולות סייבר המיוחסות לאיראן, תוך ניסיון לגבש תובנות באשר לדרך שבה מוליכה איראן את פעילותה בסייבר, בשילוב ניסיון לבחון את ההשלכות על מדינת ישראל ועל מדינות אחרות במערב.

האסטרטגיה האיראנית במרחב הסייבר

תפקידן של רשתות התקשורת והמידע בהתנעת המהומות שפרצו לאחר הבחירות לנשיאות איראן ביוני 2009 ושל אירועי 'האביב הערבי', יחד עם מתקפות הסייבר באיראן, העניקו לזירה זו מקום מרכזי בתפיסת הביטחון הכוללת של המשטר האיראני. עדות לחשיבות הנושא בעיני מקבלי ההחלטות באיראן ניתן למצוא בהתייחסותו הישירה של המנהיג העליון, ח'אמנאי, להזדמנויות ולסכנות הטמונות במרחב הקיברנטי, בעת הכרזתו על הקמת "מועצת סייבר עליונה" במרס 2012 – שתורכב מבכירי השלטון, ותפעל לתכנון וליישום אסטרטגיית פעולה אחידה ומוכללת לזירת הסייבר.[2] מועצה זו אמנם החלה את עבודתה לאחרונה, אך עם זאת, ניתוח הפעילות האיראנית במרחב הסייבר בשנים האחרונות מצביע על קיומה של אסטרטגיית סייבר איראנית בעלת מטרות ויעדים ברורים.

שני נדבכי יסוד עומדים בבסיס תפיסת הפעולה של איראן במרחב הסייבר. הראשון נוגע לפיתוח יכולות הגנה מפני מתקפות של מדינות וגורמים עוינים, לצד פיתוח יכולות שיאפשרו לפעול מול מתנגדי המשטר מבית. הנדבך השני נוגע לפיתוח יכולות התקפיות שיאפשרו לאיראן להילחם במה שנתפס בעיניה כעליונות ושליטה אמריקאית ביכולות ובתשתיות האינטרנט הגלובליות.

בכל הקשור לתפיסת ההגנה, פועלת איראן להגשמת שתי מטרות מרכזיות בזירת הסייבר.[3] ראשית, היא מבקשת ליצור מעטפת טכנולוגית יעילה ומתקדמת, שתגן על תשתיות חיוניות ועל מידע רגיש מפני מתקפות סייבר כדוגמת מתקפת Stuxnet, שפגעה בתוכנית העשרת האורניום האיראנית והשביתה יותר מאלף צנטריפוגות במתקן ההעשרה בנתנז.[4] שנית, איראן מבקשת לבלום ולסכל פעילות סייבר של גורמי אופוזיציה ומתנגדי משטר, שעבורם מהווה מרחב הסייבר

פלטפורמה מרכזית לתקשורת, להפצת מידע ולארגון פעולות נגד המשטר. נוסף לכך, המשטר מבקש למנוע חדירה דרך מרחב הסייבר של רעיונות מערביים ושל מידע הנוגד את האינטרסים שלו, ובכך לבלום תהליכים של "מהפכה רכה" שתפגע באחיזתו במדינה וביציבותו. בהקשר לפיתוח היכולות ההגנתיות, יש לציין גם את הידיעות על התוכנית האיראנית לייצר רשת תקשורת עצמאית ומבודלת[5] – אשר לעיתים מוכחשות על ידי גורמים רשמיים איראניים,[6] אולם ככל שנוקף הזמן, נראה כי יש ממש בידיעות אלה.[7]

בהקשר למרכיב ההתקפי, אסטרטגיית הסייבר האיראנית רואה זירה זו בראש ובראשונה כזירה מרכזית במסגרת דוקטרינת הלוחמה הא־סימטרית, המהווה עיקרון מרכזי בתפיסת הפעלת הכוח האיראנית. לוחמת סייבר, בדומה לטקטיקות א־סימטריות מובהקות יותר כגון טרור ולוחמת גרילה, נתפסת בעיני איראן ככלי יעיל ואפקטיבי המאפשר לפגוע באופן משמעותי בעורפו של אויב בעל עליונות צבאית וגאו־אסטרטגית. מומחים בנושא מעריכים כי במקרה של הסלמת העימות בסוגיית הגרעין בין איראן לבין המערב, תחתור איראן להוציא לפועל מתקפת סייבר נגד תשתיות מרכזיות כגון תשתיות אנרגיה, מוסדות כלכליים, מערכות תחבורה ועוד, בתוך שטחה של ארצות־הברית.[8] מאמר מערכת שפורסם בעיתון האיראני Kayhan (המזוהה עם ח'אמנאי) ביולי 2011 אף רמז לכוונה איראנית זו, באומרו כי על ארצות־הברית להיזהר מפני תקיפה של שחקן "בלתי־נודע במקום כלשהו בעולם" על תשתיותיה החיוניות ביותר.[9]

נוסף לרמה הצבאית־אסטרטגית, המשטר האיראני ותומכיו משתמשים בלוחמה התקפית במרחב הסייבר גם כדי לפגוע בפעילות הסייבר של מדינות מערביות ושל מתנגדי משטר באיראן. קבוצות פצחנים (האקרים) איראניות, שלרוב אינן שייכות באופן רשמי לממסד אך הן קשורות אליו, יוזמות באופן קבוע מתקפות סייבר שונות כדוגמת הפלת אתרי אינטרנט, החדרת תוכן פרו־איראני, גניבת מידע, הונאות אשראי, פגיעה בספקי שרות וניתוב מחדש של תנועת רשת.[10] ערוץ פעולה נוסף שניתן לייחס אותו לפן ההתקפי של אסטרטגיית הסייבר האיראנית הוא התעמולה. המשטר האיראני מבין את חשיבותו של מרחב הסייבר בעיצוב התפיסות והשקפות העולם של קהלים רחבים בתוך איראן ומחוץ לה, ומשקיע רבות ביצירת מערך תעמולה גדול ופעיל, המאדיר את המשטר ופוגע ביריביו. על מנת לממש מטרות אסטרטגיות אלו משקיעה איראן משאבים לא־מבוטלים ביצירת מארג צפוף, מיומן ורב־שכבתי של יכולות סיכול, שליטה, ניטור ותקיפה במרחב הסייבר.

המענה הארגוני והאופרטיבי

כדי לממש את מטרותיה האסטרטגיות במרחב הסייבר, החלה איראן לפעול בנחישות לחיזוק יכולות הסייבר העומדות לרשותה. על פי דיווחים, החליטה איראן להשקיע כמיליארד דולר בפיתוח טכנולוגיות וברכישתן, וכן בגיוס ובהכשרת מומחים, שיקדמו ויחזקו את יכולותיה ההגנתיות וההתקפיות בזירת הסייבר.[11] מספר מרכיבים שלובים בתהליכי בניית המענה האופרטיבי והארגוני בתחום הסייבר: הראשון שבהם נוגע לבניית תשתית הכשרה ופיתוח של כוח אדם במכוני המחקר ובאקדמיה, השני נוגע למאמץ פיתוח טכנולוגי רחב־היקף והשלישי – לתהליכי בניין הכוח הכוללים פיתוח דוקטרינה והקמה של ארגונים, והסדרת סמכויות פעולה למימוש דוקטרינה זו.

הכשרה ופיתוח כוח אדם

תשתיות ההכשרה והפיתוח הטכנולוגי של מערך הסייבר האיראני ממוקמות בראש ובראשונה באוניברסיטאות ובמכונים הטכנולוגיים הפרוסים ברחבי המדינה. באיראן רשת ענפה של מוסדות להשכלה גבוהה ולמחקר אקדמי, העוסקים במחקר ובהכשרה בתחומי טכנולוגיות המידע, הנדסת מחשבים ותקשורת.[12] בין המוסדות המובילים בתחום זה ראוי להזכיר את האוניברסיטה הטכנולוגית שריף (Sharif University of Technology) מוסד הממוקם בטהראן ומציע תארים מתקדמים בהנדסת מחשבים, בהנדסת אלקטרוניקה ובמתמטיקה.[13] באוניברסיטה זו פועלים שני מכוני מחקר המתמקדים בטכנולוגיות תקשורת ומידע: Advanced Information and Communication Technology Center[14] ו־Advanced Communication Research Institute.[15] מוסד נוסף הראוי לאזכור בכל הקשור לתחום ביטחון המידע הוא האוניברסיטה הטכנולוגית אמיר כביר (Amirkabir University of Technology). באוניברסיטה זו, הממוקמת גם היא בטהראן, מחלקה למתמטיקה ומדעי המחשב ומחלקה להנדסת מחשבים וטכנולוגיית המידע. נראה כי במוסד זה מתמקדים בנושא אבטחת המידע, כאשר המחלקה להנדסת מחשבים מציעה מספר קורסים מתקדמים בביטחון מידע,[16] ומפעילה מעבדה מחקרית המתמחה בביטחון מידע[17] ומעבדה לניתוח מערכות מאובטחות.[18]

פרט למחקר ולהכשרה במוסדות האקדמיים, הממשל האיראני משקיע כספים רבים בקידום ובתמיכה בחברות טכנולוגיה העוסקות בטכנולוגיות מידע ותקשורת מחשבים. ההשקעה האיראנית מתבצעת הן באופן ישיר על ידי גופים ממשלתיים כגון משרד המדע, והן דרך מימון והקמת חממות לתמיכה בחברות טכנולוגיה שהשלטון מעוניין בהן.[19] גוף ממשלתי מרכזי בכל הקשור לטכנולוגיות מידע הוא המכון Iran Telecommunications Research Center, המתמחה במחקר טכנולוגיות מידע ותקשורת, והינו הזרוע המחקרית והמקצועית של משרד המידע והתקשורת.

המכון מפעיל ומכשיר צוותי מחקר מתקדמים בתחומים שונים, ובכללם אבטחת מידע.[20] גוף ממשלתי נוסף המקדם מחקר בתחום טכנולוגיות המידע הוא הלשכה לשיתוף פעולה טכנולוגי (TCO-Technology Cooperation Office). גוף זה משתייך למשרד הנשיא ומטרתו המוצהרת היא לשפר את שיתוף הפעולה הטכנולוגי עם מדינות אחרות. הארגון מנחה ויוזם פרויקטים מחקריים בתחומים רבים, ביניהם טכנולוגיות מידע.[21] הוא סומן על ידי האיחוד האירופי וגורמים אחרים במערב כמעורב בתוכנית הגרעין.[22]

נוסף להשקעות ישירות מצד גופים ממשלתיים, הממשל האיראני מפעיל גם חממות טכנולוגיות שבהן מתבצע מחקר בתחום אבטחת המידע. בין מרכזי טכנולוגיה אלה ניתן למצוא את הגן הטכנולוגי Paradis Technology Park המכונה "עמק הסיליקון האיראני". הוא הוקם בשנת 2001 ביוזמת משרד הנשיא וה־TCO, ופועלות בו למעלה מארבעים חברות העוסקות בטכנולוגיות תקשורת ומידע.[23] חממה טכנולוגית נוספת היא Guilan Science and Technology Park, המהווה מרכז לתמיכה בחברות בתחילת דרכן, וב־v רשומות מספר חברות העוסקות בתחומי אבטחת מידע.[24]

התעצמות טכנולוגית

פרט לפיתוח ולהכשרת מערך סייבר חזק, פעלה איראן גם במישור הטכנולוגי על מנת לקדם את מטרותיה האסטרטגיות בזירת הסייבר. תחום אחד שבו השקיעה איראן רבות הוא השליטה במרחב הסייבר הפנים־מדינתי ובתנועות המידע שבו. הממשל האיראני רכש ופיתח בשנים האחרונות מערכות טכנולוגיות מתקדמות, המאפשרות לעקוב ולנטר את תנועות המידע ברשתות המחשבים והסלולר במדינה. Telecommunication Co. of Iran – חברת הטלקומוניקציה הגדולה באיראן הנמצאת בשליטה ממשלתית – רכשה מחברת ZTE Corp הסינית מערכת מעקב המסוגלת לנטר מידע בקווי טלפון, ברשתות מחשב ובקווי סלולר. מערכת זו נקנתה כחלק מעסקה כוללת בין שתי החברות, המוערכת בכ־130 מיליון דולר. העסקה כללה מוצרים ממערכת ZMXT, המתוארת על ידי החברה הסינית כמערכת ניטור משולבת (Integrated monitoring system). המוצרים שנרכשו על ידי איראן מאפשרים ניטור שֶמע, הודעות טקסט וגלישת אינטרנט.[25]

נוסף לניטור ולמעקב, המשטר האיראני פועל גם לפיתוח טכנולוגיות חסימה וסינון של אתרים. כיוון שהסנקציות מונעות מאיראן רכישה של מסנני מידע מערביים, יזם הממשל פרויקט פנים־איראני של פיתוח טכנולוגיות סינון וחסימה. חברת Amnafzar – חברה לטכנולוגיות מידע בעלת קשרים עם המשטר – פיתחה טכנולוגיית סינון מידע המכונה SEPAR. מערכת זו מתעדכנת באופן קבוע ומשנה תכופות את אסטרטגיית הסינון שלה, כדי להתמודד עם ניסיונות עקיפה.[26] בעזרת

טכנולוגיה זו הצליח המשטר להגביל באופן ניכר את זרימת המידע אל המדינה ובתוכה. מחקר של OpenNet Initiative (יוזמה משותפת של מספר מוסדות, ביניהם האוניברסיטאות הרווארד וטורונטו) שהתפרסם במרס 2009 מצא שאיראן היא אחת המדינות המובילות בעולם בסינון ובחסימת אתרים, לצד מדינות כגון סין, צפון־קוריאה, סוריה ומיאנמר.[27]

טכנולוגיות אלו מעניקות לאיראן שליטה הדוקה יחסית במרחב הסייבר המדינתי, אך עם זאת, שאיפת המשטר היא שליטה מוחלטת במידע, ברעיונות ובגישה למרחב הסייבר האיראני. על מנת להשיג שליטה כזו פתחה איראן בפרויקט הקמת רשת אינטרנט לאומית עצמאית, הנבדלת מהרשת העולמית. לשיטתה של איראן, הקמת הרשת הלאומית המכונה Halal תאפשר למשטר שליטה מלאה בתכנים שאליהם נחשף הציבור, תפגע קשות במתנגדי המשטר, אשר חלק גדול מפעילותם מתבצע ברשת, ותקטין משמעותית את האפשרות לחדירת וירוסים ויישום מתקפות סייבר אחרות על תשתיות איראניות. פרויקט הרשת הלאומית החל לקרום עור וגידים בשנת 2009, כאשר הרשויות האיראניות הורו לחברות במדינה להעביר את פעילותן הרשתית לשרתים ולמרכזי מידע בתוך המדינה. במהלך 2012 דווח כי איראן מפתחת שירות דואר אלקטרוני פנימי, מערכת הפעלה עצמאית, מנוע חיפוש וכלים נוספים המיועדים לשימוש ברשת החדשה.[28] באוגוסט האחרון הצהיר שר התקשורת האיראני, רזה טגיפור (Reza Taghipour), כי איראן תתנתק מהרשת העולמית בתוך 18 חודשים.[29] אך עם זאת, מומחים במערב קובעים כי המשטר באיראן יתקשה להתנתק באופן מלא מהרשת החיצונית.[30]

איראן מבקשת ליישם את אסטרטגיית בידול הרשתות גם במגזר הביטחוני, ולהקים רשת תקשורת מודיעינית לאומית שתהיה מנותקת מהרשת הגלובלית.[31] סנונית ראשונה של מאמץ זה היא Basir – רשת פנים־ארגונית של 'משמרות המהפכה' שנחשפה במרס 2012. ידיעות על הרשת מתארות אותה כמעין רשת סלולר סגורה, שייתכן כי היא מופעלת על ידי תחנות ממסר ייעודיות. הרשת אמורה לספק לארגון קווי תקשורת מוצפנים ויעילים, גם בתרחיש של מתקפת סייבר כוללת על תשתיות התקשורת והמידע במדינה. לא ברור האם מדובר גם ברשת מידע, או רק ברשת קולית.[32]

בניין הכוח

באשר לתהליכי בניין הכוח בתחום הסייבר – מערך ההכשרה והפיתוח הנרחב העומד לרשותה של איראן אִפשר לרפובליקה האסלאמית להקים מערך סייבר נרחב בעל יכולות מגוונות, הגנתיות והתקפיות כאחת. בעשור האחרון החלה איראן במהלך אסטרטגי של הרחבת מערך הסייבר הלאומי, כאשר סוכנויות וגופי סייבר הוקמו כמעט תחת כל סוכנות ממשלתית רלוונטית. מטרתה של איראן היא

ליצור מערך ארגוני סייבר הירכי ומגוון עם אסטרטגיית פעולה ברורה, הקצאת משאבים מתוכננת, חלוקת תחומי אחריות ויכולות שימור והפצה של ידע ומידע.

גולת הכותרת של תהליך התעצמות הסייבר האיראני היא, כפי שהוזכר לעיל, הקמתה של "המועצה העליונה למרחב הסייבר". מועצה זו הוקמה במרס 2012 בהוראת המנהיג העליון, ח'אמנאי, והיא הסמכות הבכירה במדינה בכל הקשור למרחב הסייבר.[33] בתפקיד ראש המועצה מכהן נשיא איראן, ובין היתר, חברים בה בכירים כדוגמת מפקד 'משמרות המהפכה', ראש המג'לס, שרי המדע, התקשורת והתרבות, מפקד המשטרה ונשיא ארגון התעמולה האסלאמית. בסמכות המועצה לקבוע את מדיניות הסייבר הלאומית, והנחיותיה מחייבות את כלל הגופים האיראניים הפועלים בתחום. בחסות המועצה מתוכנן לקום "מרכז סייבר לאומי" אשר יתכלל את כלל פעילות הסייבר האיראנית, ירכז ויפיץ מידע והנחיות ויפקח על מילוי הוראות המועצה על ידי כלל הגופים הרלוונטיים.

מערך הסייבר האיראני מורכב ממספר רב של ארגוני סייבר הפועלים בתחומים שונים ומשתייכים באופן רשמי לגופי ממסד. ארגון מרכזי אחד בעל אוריינטציה הגנתית בעיקרה הוא "מפקדת הגנת סייבר", שפועלת במסגרת "ארגון ההגנה הפסיבית של איראן", המשויך למטה הכללי של הכוחות המזוינים.[34] לצד אנשי צבא, חברים בארגון סייבר זה גם נציגי משרדים ממשלתיים כגון משרד התקשורת, ההגנה, המודיעין והתעשייה, ומטרתו המרכזית היא לפתח דוקטרינת הגנה מקיפה למוסדות ולתשתיות המדינה נגד איומי סייבר.[35] הגוף הינו הגנתי בעיקרו, ונכון להיום לא נראה כי הארגון עסק בפעילות סייבר התקפית. גוף סייבר נוסף בעל אופי הגנתי הוא מרכז אבטחת המידע המכונה MAHER , שהוקם ופועל במסגרת המשרד לתקשורת וטכנולוגיות מידע. המרכז אחראי בראש ובראשונה על הפעלה של צוותי תגובה מהירה (Computer Security Incident Response Teams), במקרה של אירועי חירום ומתקפות סייבר. נוסף לכך, המרכז מכשיר כוח אדם מיומן, מפתח דרכי פעולה לטיפול במשברי סייבר ומהווה מרכז לאגירה ולהפצה של ידע בתחום אבטחת המידע. באחריות המרכז להגן על כלל אתרי האינטרנט הממשלתיים, כמו גם על אתרי חברות פרטיות הפועלות באופן רשמי ורשומות במשרד התקשורת. צוותי המרכז הם אלה שהופעלו על מנת לבלום ולסכל את פעולותיהם של הווירוסים Flame ו־Stuxnet שתקפו באיראן.[36]

ארגוני סייבר נוספים הפועלים באיראן מתמקדים באכיפה ובשליטה על פעילות סייבר פנים־איראנית הנוגדת את האינטרסים של המשטר. ביולי 2009 הוקמה על ידי "המועצה הגבוהה למהפכה תרבותית" הכפופה למנהיג העליון "ועדה לזיהוי אתרים בלתי־מאושרים". בוועדה זו חברים, בין השאר, התובע הכללי, מפקד המשטרה, הממונה על כלי התקשורת הממשלתיים ושרי ממשלה שונים (מודיעין, תקשורת, תרבות, מדע ועוד). באחריות הוועדה לאתר אתרי

אינטרנט שתוכנם ופעילותם אינם עולים בקנה אחד עם דרישות המשטר ורצונותיו, ובסמכותה להורות על חסימת גישה לאתרים אלה.[37] בשנת 2011 הוקמה יחידת הסייבר המשטרתית FETA.[38] משימתה העיקרית של יחידה זו היא התמודדות עם פשעי אינטרנט: הונאה, גניבת מידע, איומים וכדומה, אך באחריותה לפעול גם נגד עבריינות פוליטית וביטחונית במרחב הסייבר – משימה המהווה בפועל את עיקר פעילותה.[39] כמו כן אחראית FETA גם על ניטור, מעקב ושליטה במשתמשי האינטרנט באיראן, תוך דגש על משתמשי "אינטרנט קפה" הפרוסים ברחבי המדינה, ומאפשרים גלישה אנונימית במידה מסוימת.[40]

בכל הקשור ליכולות ההתקפיות של מערך הסייבר האיראני, התמונה שקופה וברורה במידה פחותה. באופן טבעי, 'משמרות המהפכה' הם השחקן המרכזי בכל הקשור להקמה ולהפעלה של מערך סייבר התקפי. מומחי סייבר במערב קובעים כי יכולות הסייבר של 'משמרות המהפכה' מציבות את איראן בין המדינות המתקדמות בעולם בתחום לוחמת הסייבר.[41] ניתוח של מכון המחקר Defense Tech מ־2008[42] העריך כי מערך הסייבר של 'משמרות המהפכה' מעסיק כ־2,400 אנשי צוות, ולרשותו תקציב של 76 מיליון דולר (נכון לאותה תקופה). בין יכולות לוחמת הסייבר שאותן מייחס המכון למשמרות המהפכה ניתן למצוא: פיתוח תוכנות מחשב נגועות על ידי השתלה של קוד זדוני בתוכנות מחשב מזויפות; פיתוח יכולות חסימה לרשתות תקשורת מחשבים ורשתות Wi-Fi; פיתוח קודי מחשב זדוניים (וירוסים ותולעי מחשב) המסוגלים להפיץ עצמם ברשתות ולפגוע במחשבי יעד; כלים לחדירה למחשבים ולרשתות כדי לאסוף מודיעין ולהעבירו לשרתים מרוחקים; פיתוח של 'כלים שוהים' המותקנים במחשבי היעד ומופעלים בצורה מושהית, או לפי פקודה משרתי שליטה.

נוסף ליכולות לוחמת המידע, 'משמרות המהפכה' פועלים גם ליצירת מערך לוחמה אלקטרונית שיכול לחסום מערכות מכ"ם ותקשורת. הארגון משקיע רבות ברכישת מערכות לוחמה אלקטרונית,[43] אשר בשילוב עם יכולות לוחמת סייבר יהוו כלי אפקטיבי לפגיעה במערכות האלקטרוניות של ארצות־הברית ושל בעלות־בריתה בשעת עימות צבאי.[44] על פי הצהרות של 'משמרות המהפכה', עוצמתה של איראן בתחום לוחמת הסייבר באה לידי ביטוי בלכידת מטוס הריגול הבלתי־מאויש של ארצות־הברית בדצמבר 2011.[45]

פרט ליחידות לוחמת הסייבר האורגניות, ישנן עדויות גם לקשרים בין 'משמרות המהפכה' לבין קבוצות פצחנים איראניות, הפועלות נגד אויבי המשטר בתוך איראן וברחבי העולם. השימוש ב"מיקור חוץ" מאפשר למשמרות המהפכה ולאיראן לשמור על ריחוק ולהתכחש להאשמות בדבר מעורבותה של איראן בלוחמה ובפשעי סייבר. קבוצת פצחנים איראנית אחת – שמומחים סבורים כי היא קשורה למשמרות המהפכה – היא Ashiyane Digital Security Team.[46] חברי קבוצה

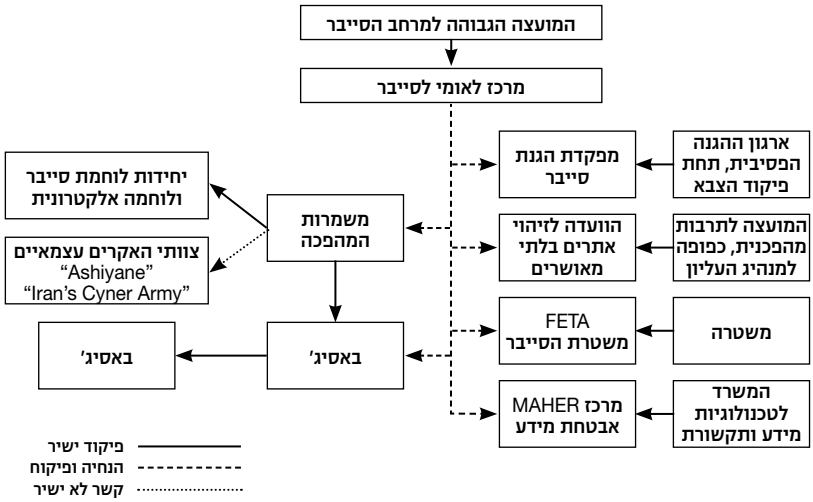
זו מוּנָעים על ידי תפיסות אידאולוגיות התומכות במשטר האיראני ובמהפכה, ומכוונים את התקפותיהם נגד אויבי המשטר. קבוצת Ashiyane מאמנת פצחנים ומקנה להם יכולות גבוהות,[47] אשר מנוצלות לאחר מכן הן לפעילות פוליטית הכוללת החדרה של תעמולה פרו־איראנית לאתרים מערביים וישראליים והפלתם, והן לפשעי סייבר (הונאות אשראי, גניבת זהות ופריצה למאגרי מידע ולמוסדות פיננסיים). נוסף לכך מקיימת הקבוצה פורום בשם War Games, שבו היא עורכת תחרויות פריצה בין פצחנים, כאשר בין המטרות ניתן למצוא גם חברות תשתיות אמריקאיות.[48]

קבוצת פצחנים נוספת הנתפסת כבעלת קשרים למשמרות המהפכה היא Iran's Cyber Army.[49] הארגון מורכב מפצחנים ומומחי מחשבים הפועלים בזהות בדויה, ומכריזים על עצמם כשייכים לארגון. פעולותיו העיקריות של צבא הסייבר האיראני כוללות: פריצה והחדרת תוכן פרו־איראני לאתרים מערביים, השתלטות על תעבורת מידע ותיעולה מחדש, פריצה לחברות ביטחון מידע מערביות ופגיעה באתרים של מתנגדי המשטר.

גם ארגון הבסיג' הכפוף למשמרות המהפכה נעשה פעיל בזירת הסייבר עם הקמתה בשנת 2010 של "מועצת הסייבר של הבסיג'". פעילות הבסיג' מתמקדת בראש ובראשונה ביצירת תעמולה פרו־איראנית במרחב הסייבר. הבסיג' מגייס ומדריך אלפי אירנים בכתיבת תוכן, ולאחר מכן מפעיל כיתות מחשבים מאורגנות, שמתוכן מופעלים עשרות אלפי בלוגים התומכים במשטר, וכן מעלים הפעילים תגובות וחומרים התומכים בשלטון ברשתות חברתיות, בפורומים ובאתרים מרכזיים באיראן ומחוצה לה.[50] עם זאת, הבסיג' מבקש לפתח גם יכולות סייבר מתקדמות יותר, ומשתמש במדריכים מתוך יחידות הסייבר של 'משמרות המהפכה' על מנת להכשיר פצחנים בעלי יכולות תקיפה גבוהות.[51]

אם כן, ניתן לראות כי בשנים האחרונות הקימה איראן מערך סייבר נרחב המקיף תחומי פעילות רבים, ולרשותו עומדות יכולות מגוונות. התרשים הארגוני שלהלן מתאר את המבנה ההיררכי של מערך הסייבר במדינה, כפי שהוא עולה מתוך הניתוח לעיל:

ניתן לראות התקדמות משמעותית בפיתוח תחום הסייבר באיראן. בתחום ההגנתי פועלת איראן במלוא המרץ לייצר יכולות הגנה ובידול, כדי להתמודד עם ניסיונות חדירה לרשתות ולתשתיות חיוניות במדינה. קשה לספק תמונה אמינה בהקשר לפיתוח היכולות ההתקפיות בתחום הסייבר. החלק הבא במאמר בוחן מספר פעולות כאלה.



פעולות סייבר המיוחסות לאיראן

בדצמבר 2011 הובילה חשיפה של תוכנית תחקירים של רשת הטלוויזיה Univision לחקירה אמריקאית בדבר מעורבותם של גורמים איראניים רשמיים במזימת סייבר נגד ארצות־הברית. תחקירני הרשת, שהצליחו להסתנן לתוך קבוצת פצחנים מקסיקנית שפעלה נגד מטרות אמריקאיות, צילמו בסתר פגישה בין נציגי הקבוצה לבין שגריר איראן במקסיקו. בפגישה שנערכה בשגרירות, ביקשו הראשונים לבדוק את האפשרות לקבלת תמיכה ומימון מממשלת איראן לטובת ביצוע מתקפות סייבר נגד מטרות אמריקאיות, ביניהן הפנטגון, ה־CIA, ה־FBI ומתקני גרעין בתחומי ארצות־הברית. בצילומים נראה השגריר האיראני במקסיקו דאז, מוחמד חסן גהאדרי, מציג שאלות ואף מציע דרכי פעולה אפשריות נוספות. השגריר הדגיש שאיראן מבקשת להשיג מידע מודיעיני לגבי האפשרות של תקיפה אמריקאית נגדה, ובסוף השיחה ביקש לשמור על קשר והבטיח להעביר ההצעה לממונים עליו.[52] ניתן להניח שניסיון זה לא היה יחידי, וכי איראן פועלת לגייס בעולם גורמים שיוכלו לשרת את מטרותיה ההתקפיות במרחב הסייבר.

קביעה ודאית של זהות תוקפים במרחב הסייבר היא פעולה מורכבת המחייבת הקצאה של משאבים רבים ושיתוף פעולה בין־לאומי. לכן, קשה לקבוע בוודאות מי עומד מאחורי פעולות רבות במרחב הסייבר. למרות זאת, במקרים רבים ובאמצעות תבחינים נסיבתיים ניתן לקבוע ברמה גבוהה של ודאות מיהו העומד מאחורי הפעילות. במסגרת מאמר זה נבחנו שלוש פעולות. הראשונה – תקיפה של שתי חברות אבטחה למטרת גניבה של הרשאות אבטחה באינטרנט, השנייה

נוגעת לתקיפת מוסדות פיננסיים גדולים בארצות־הברית והאחרונה הינה תקיפת חברת הנפט הסעודית Aramco.

מתקפה על החברות DigiNotar ו־Comodo

במהלך שנת 2011 בוצעו שתי מתקפות על חברות המספקות הרשאות SSL.[53] הראשונה על חברת Comodo מארצות־הברית והשנייה על חברת DigiNotar מהולנד. חברת האבטחה האמריקאית Comodo הותקפה במהלך חודש מרס 2011. נגנבו מספר הרשאות, ביניהן הרשאות לתחומים (domain) של שרותי דואר אינטרנטיים דוגמת Google, אולם אלה בוטלו בטרם נעשה בהן שימוש על ידי הגורם התוקף. למעשה, גורם המקבל אישור לתחום mail.google.com, יכול לגנוב סיסמאות של Gmail ו"לחטוף" חשבונות של משתמשים. כך גם מי שמקבל אישור מזויף לתחום Microsoft.com יוכל להתקין תוכנות זדוניות במחשבי הקורבנות. מדיווח של החברה על האירוע עולים הממצאים הבאים:[54]

1. בתקיפה זו לא היו מאפיינים של עבריינות סייבר.
2. התוקפים היו מאורגנים וידעו במדויק ומראש את מבוקשם – דבר המצביע על מעורבותו של ארגון מדינתי בתקיפה.
3. מקור המתקפה היה בעיקר איראן (לפי זיהוי כתובת IP).
4. אתר האינטרנט שבו נבדקו ההרשאות הגנובות מוקם באיראן, והוּרד מהרשת מייד לאחר גילוי המתקפה על ידי חברת Comodo.

תקיפת חברת Comodo לא הצליחה להשיג את מטרתה. ההתקפה זוהתה וטופלה בטרם נעשה שימוש בהרשאות הגנובות. שונה היה המצב בחברת DigiNotar ההולנדית. מאגרי החברה שהייתה הרשות המרכזית בהולנד להרשאות SSL הותקפו בחודשים יוני עד אוגוסט 2011. במהלך התקיפה, שקיבלה את הכינוי "טוליפ שחור", נגנבו תעודות המשמשות לאימות אתרים, כולל תעודה המשמשת לאימות שם התחום google.com, המאפשרת לתוקף התחזות וניתוב מחדש של שרתי Gmail.[55]

ניתוח שהזמינה חברת DigiNotar (שעקב אירוע זה פשטה את הרגל וחדלה להתקיים) הראה שנגנבו וזויפו 531 תעודות, וכי עיקר השימוש בהרשאות הגנובות היה לצורכי חדירה לחשבונות דוא"ל של משתמשים, בעיקר באיראן. הניתוח הראה שהתקיפה אפשרה חדירה ליותר מ־300,000 מחשבים, רובם המכריע באיראן (מעל 99%).[56] קשה לקבוע בוודאות את מקור התקיפה, אולם לדעת מומחים, מקורה באיראן והיא נועדה, ככל הנראה, לצורכי בטחון פנים במדינה,[57] בעיקר בשל הסיבות הבאות: יעדי המתקפה וההיקף הנרחב של משתמשים שהותקפו, וכן הודעות שהושארו באתר החברה שהצביעו על מעורבות של איראנים בפעולה.

מתקפה על מוסדות פיננסיים בארצות־הברית

דיווח שהופץ בארצות־הברית בחודש ספטמבר 2012 מעלה כי סמוך למועד זה הותקפו מספר מוסדות פיננסיים בארצות־הברית, ביניהם אתרים השייכים לבנק אוף אמריקה (Bank of America), לבנק מורגן צ'ייס ולבנק סיטיגרופ. להערכת גורמים בארצות־הברית, התקפות הסייבר נגד מוסדות פיננסיים אמריקאיים לא נערכו על ידי פצחנים אקראיים, אלא מומנו ככל הנראה על ידי איראן, והן בוצעו בתגובה לסנקציות שהוטלו על המדינה על ידי ארצות־הברית.[58]

בעקבות זאת, מרכז לניתוח ולשיתוף מידע פיננסי בארצות־הברית [59] פרסם התראה לבנקים בארצות־הברית בעניין תקיפות סייבר שמטרתן גניבת זהויות באמצעות דואר אלקטרוני, סוסים טרויאניים וכלים זדוניים המסוכלים לקלוט הקשות מקלדת – כל זאת כדי לחלץ שמות של משתמשים, עובדים וסיסמאות. אף שגם בנקים גדולים הותקפו, רוב הקורבנות של תקיפות אלה היו עסקים קטנים ובינוניים, בנקים קטנים וחברות אשראי. קבוצה הקרויה "לוחמי הסייבר של עז א־דין אל קאסם" הודיעה שהיא תקפה את בנק אוף אמריקה (BofA) ואת הבורסה של ניו־יורק בתגובה לסרט שפגע בנביא מוחמד, שהתפרסם בתחילת ספטמבר 2012. התקפות אלה, כפי שתוארו בהתראה, מצביעות על כך שהתוקפים הצליחו להשיג מידע רב וגישה לרשתות הבנקים לפחות במספר מקרים, וכן הצליחו להשיג אישורי כניסה מעובדי בנק ולעקוף את מנגנוני ההגנה.[60]

מתקפה על חברת Aramco

במהלך אוגוסט 2012, כנראה תוך סיוע פנימי של גורם בעל נגישות גבוהה למחשבי החברה, הותקפו כ־30,000 מחשבים של חברת Aramco הסעודית ומחשבי חברת הגז ResGas מקטר ההתקפה בוצעה באמצעות וירוס מחשב הידוע בשם Shamoon. לדעת מומחים, זוהי אחת ההתקפות ההרסניות ביותר שבוצעה נגד חברה אחת. וירוס המחשב התפשט דרך שרתי מחשבי החברה ופגע במידע שנשמר בהם. מומחי החברה טוענים שהנזק היה מוגבל למחשבים משרדיים, ולא השפיע על המערכות התפעוליות ומערכות הבקרה.[61]

חברת סינמטק זיהתה את הווירוס לראשונה בחודש אוגוסט 2012. בניתוח שערכו גורמים בחברה ובחברות אבטחה נוספות עלו כמה ממצאים:[62]

1. הווירוס Shamoon נועד לתקוף מחשבים במערכת המחשוב הארגוני (IT) ולא מחשבי מערכות בקרה. וירוס זה אינו שייך לקטגוריה של כלי לוחמת סייבר מתוחכמים דוגמת Stuxnet, שתקף את תוכנית הגרעין של איראן בשנת 2010.
2. מטרת התקיפה של הווירוס לא הייתה ריגול או איסוף מידע, כי אם השמדה מוחלטת של נתונים ופגיעה במחשבי היעד.

3. כותבי הקוד המפַגע אינם נראים כשייכים לעילית התחום (כמו כותבי קוד Stuxnet או Flame). קיימים ממצאים המראים שהגורמים העומדים מאחורי כתיבת הקוד אינם מתכנתים בעלי פרופיל מקצועי גבוה במיוחד, והושארו בו שגיאות קידוד רבות. אולם הם היו מיומנים דיים לייצר קוד הרסני במיוחד.
4. הווירוס הוחדר למחשבי החברה באמצעות משתף פעולה מתוך החברה, שהייתה לו גישה ישירה למערכת. נראה שהוא השתמש בהתקן USB על מנת להחדיר את הווירוס לתוכה.
5. כותבי הקוד עשו שימוש בחלק מתמונת דגל אמריקאי שרוף כדי להסתיר את תוכן הקבצים במחשבים הנגועים – פעולה המראה על שיוך פוליטי או דתי־אסלאמי מסוים של כותבי הקוד.
6. בקוד של מנגנון המחיקה של ה־Shamoon הטמיעו מפתחי הווירוס את השם Wiper. כינוי דומה מופיע בקוד הווירוס Flame, שתקף את מחשבי חברת הנפט האיראנית. הקבלה זו מעלה את החשד כי המתקפה על Aramco היא פעולת תגמול איראנית, בתגובה למתקפת Flame.

קבוצה בשם 'חרב הצדק' (The Cutting Sword of Justice), קיבלה אחריות לתקיפה וטענה שהיא כוּונה נגד מקור ההכנסה העיקרי של ערב־הסעודית, שהואשמה בביצוע פשעים במדינות כגון סוריה ובחריין. עוד טענה הקבוצה, שווירוס המחשב אִפשר להם גישה לסודות רבים. אולם נכון לכתיבת שורות אלה, טרם פורסם כל מידע רלוונטי בנושא. דיווחים על התקפות דומות על חברות נפט וגז באזור המפרץ העלו את החשד שתקיפות אלה היו חלק ממהלך רחב של מדינה. בדברים שאמר לאחרונה שר ההגנה האמריקאי, ליאון פאנטה, הוא רמז על מעורבות איראנית בתקיפה. בכיר לשעבר בממשל האמריקאי היה גלוי יותר, כשאמר שהממשל מאמין כי איראן עומדת מאחורי המתקפות במפרץ.[63]

ניתוח שערך מומחה האבטחה ג'פרי קאר (Jeffrey Carr)[64] מארצות־הברית מעלה מספר טיעונים הקושרים את איראן למתקפה זו. איראן היא המדינה היחידה שיש לה נגישות לקוד המקור Wiper, שממנו נוצר ככל הנראה הווירוס Shamoon. לפי הדיווח של חברת קספרסקי,[65] הקוד Wiper ששימש לתקיפת משרד האנרגיה האיראני באפריל 2012 שימש גם את יוצרי Shamoon. לאיראן מוטיבציה גבוהה לתקוף את חברת הנפט הסעודית בשל הסנקציות המחריפות על איראן בתחום האנרגיה. כמו כן, נבדק חשד לקשר של ארגון חזבאללה לתקיפה. מספר עובדים לבנוניים של חברת Aramco נעצרו ונחקרו בהקשר זה.

תובנות מסכמות

פיתוח יכולות הסייבר של איראן צריך להטריד את ישראל, וכמובן גם את ארצות־הברית, כמו גם מדינות נוספות במערב. בעקבות התעוזה בניסיון החיסול של

שגריר ערב־הסעודית בארצות־הברית, מציעים מומחים בארצות־הברית לא לזלזל בכוונות וביכולות האיראניות להעיז ולתקוף תשתיות חיוניות בארצות־הברית. כמו שאר העולם, ניתן להניח שגם איראן – שהייתה קורבן לאחת ממתקפות הסייבר ההרסניות ביותר – למדה היטב את לקחי תקיפת Stuxnet, והיא מבינה את הפוטנציאל ההרסני הגלום בפיתוח כלי תקיפה שיוכלו לפגוע במערכות בקרה תעשייתיות, ובכך לגרום נזק פיזי.

פיתוח האסטרטגיה האיראנית ותהליכי בניין הכוח שבאו בעקבותיה מצביעים על התארגנות שיטתית בניסיון להוות שחקן משמעותי בתחום לוחמת הסייבר. מומחים מדווחים על התקדמות מתמדת ביכולות ובמבצעי הסייבר של איראן. ראוי לשים לב לדברי אחד מהם, שאמר לאחר דיווח על מתקפת סייבר על מוסדות בנקאיים בארצות־הברית המיוחסת לאיראן: "[תוכנית הסייבר של איראן] דומה לתוכנית הגרעין, היא אינה מתוחכמת במיוחד אבל מתקדמת מדי שנה."[66] אין לזלזל ביכולות הטכנולוגיות של איראן. התשתית המדעית במדינה מפותחת ומאגר ההון האנושי רב. לכן, ניתן להעריך שתוך תקופה לא־ארוכה תוכל איראן להוות גורם משמעותי ברמה עולמית בתחום זה. הערכה זו מקבלת חיזוק מהמתקפה על מחשבי חברת Aramco, שבעקבותיה אמר ג'יימס לואיס (James A. Lewis), מומחה לביטחון סייבר, שאיראן הייתה מהירה יותר בפיתוח יכולות התקפיות, ונועזת יותר בהפעלה שלהן משניתן היה לצפות.[67] בדרך כלל, הפעילות שנחשפת הינה קצה הקרחון של פעילות בלתי־גלויה נוספת. מצד שני, שכלול ההגנה של איראן מחייב את הגורמים בעלי העניין להתארגן לפעולה בסביבה של רשתות מבודדות, או אף רשת תקשורת איראנית מבודדת מרשת האינטרנט. אף כי האתגר בהקמה של רשת כזו ובבידודה המוחלט הוא עצום, הרי ניתן לאתר דרכי פעולה גם בסביבה כזו. תפיסת הגנה זו תהווה אתגר לא־מבוטל לגורמים בעלי עניין בביצוע מהלכים במרחב הסייבר באיראן.

מתוך הפעולות המיוחסות לאיראן שתוארו לעיל, ניתן להפיק מספר תובנות. הניסיון האיראני להשיג הרשאות SSL מצביע על פעילות מול קבוצות גדולות של אזרחים יותר מאשר כלפי יעדים ממוקדים כמו מדינות או חברות וארגונים. ככל הנראה, הדבר נוגע לצורכי זיהוי ומעקב על גורמים פנימיים באיראן. עם זאת, הניסיון הנצבר בפעילות מסוג זה יאפשר פעילויות גם מול יעדים ממוקדים יותר דוגמת ארגונים ומדינות. ראוי לציין שאף כי הפעילות שנחשפה מצביעה על ארגון ושיטתיות, נדמה שאיראן טרם חצתה את הרף הטכנולוגי והארגוני כדי להוות גורם בעל תחכום רב. אולם, המוטיבציה האיראנית יחד עם תהליכי בניין הכוח והיכולות הטכנולוגיות במדינה יאפשרו לה לצעוד לכיוון זה במהירות רבה.

תקיפת חברת Aramco מעלה תובנות נוספות. הראשונה נוגעת לעובדה שההגנה המקובלת מפני איומים המגיעים דרך רשת האינטרנט אינה מספקת. רוב

המומחים מקבלים את ההנחה שהחברה לא חסכה השקעות בהגנה מפני איומים המועברים דרך רשת האינטרנט. הווירוס ההרסני לא התגלה על ידי מערכות ההגנה, והוחדר כנראה על ידי גורם פנימי בחברה, שהיה בעל הרשאה מתאימה. מערכות ההגנה הקיימות והסטנדרטיות אינן בנויות לספק הגנה מפני איומים ממוקדים (APT) וקוד זדוני בלתי־מוכר (zero date ואחרים). לכן גובר הצורך בפיתוח כלים שיוכלו לספק הגנות טובות יותר מפני איומים כאלה. אחד הכיוונים המתפתח הוא כלים שיתבססו על זיהוי, חסימה ונטרול של התנהגות אנומלית ובלתי־רצויה במחשבים מותקפים. כלים כאלה יוכלו לנטרל איומים גם אחרי שהקוד הזדוני הצליח לחדור למחשב היעד. התובנה השנייה נוגעת למטרות התקיפה, שנועדה בעיקר להשמיד מידע באופן גורף וללא אבחנה בעשרות אלפי המחשבים של חברת הנפט הסעודית, ופחות (אם בכלל) לאסוף מידע. אם פעילות מודיעין במרחב הסייבר יכולה להיחשב לגיטימית בחלק מהמקרים, הרי תקיפה רחבת־היקף כזו על ידי איראן על מטרה אזרחית מסמנת כי איראן עוברת לפעולות תגמול. הדבר צריך להטריד את הממונים על ההגנה במדינות רבות. דבריו של שר ההגנה האמריקאי, ליאון פאנטה, על הצורך לבוא חשבון עם הגורמים העומדים מאחורי תקיפה זו ממחישים זאת.[68] אולם, מה שיקבע יהיה מבחן המעשה ולא מבחן המילים.

כמי שנפגעה מהתקפת הסייבר ההרסנית ביותר עד כה, ניתן להעריך שאיראן מבינה היטב את הפוטנציאל הגלום בתחום זה, וכי היא תפעל לפתח יכולות כאלה משל עצמה בעתיד. לנוכח זאת, תהליכי בניין הכוח השיטתיים שפורטו לעיל יובילו את איראן תוך זמן לא רב להיות שחקן משמעותי בשדה הקרב הקיברנטי ולתקיפה של תשתיות חיוניות במדינות העוינות את איראן, כגון ארצות־הברית וישראל, תוך יצירת בידול מרבי במקרה של חשיפה וגילוי הפעילות. איראן מפעילה קהילות של פצחנים "אזרחיים" תוך ניסיון ליצור בידול בין אלה לבין הממשל והארגונים האיראניים. גישה זו דומה למתרחש במקומות נוספים בעולם, דוגמת סין ורוסיה, והיא מאפשרת למדינות להתנער מאחריות ולגלגל את המעשה לפתחם של אזרחים. כך יימשך הקושי הרב בשיוך פעולות הסייבר ההתקפיות למדינה האיראנית.

מיקוד פעילות הסייבר של איראן בישראל ובמדינות מערביות אחרות מחייב התארגנות הגנתית ייעודית. נדרשת תפיסה עדכנית בכל הקשור להגנות במרחב הסייבר. התחכום של התוקפים מחייב, לצד הגנות גנריות, גם פעילות הגנה המבוססת על מודיעין. לפיכך ולנוכח תהליכי ההתפתחות של איראן, חייבת מדינת ישראל להציב את תחום הסייבר האיראני במקום גבוה בסדר־העדיפות המודיעיני ובפעילות המסכלת. הדבר נועד לאתר ולסכל בעוד מועד התארגנויות לפעולות התקפיות. בדומה לתוכנית הגרעין האיראנית, האתגר אינו רק של מדינת ישראל, אלא של מדינות נוספות רבות במערב, כמו גם מדינות המפרץ, ותעיד על

כך ההתקפה על מחשבי חברת Aramco. לכן, יש ליזום שיתוף פעולה בין־מדינתי רחב ככל האפשר בתחום המודיעין והסיכול של פעולות סייבר איראניות.

לצד זאת, על מדינת ישראל להמשיך לבנות מענה הגנתי אפקטיבי. מענה זה צריך להתמקד בשלוש שכבות הסייבר הרלוונטיות במדינה: הראשונה – שכבת ארגוני הביטחון הנדרשים לבחון באופן קבוע את החשיפה ליכולות הסייבר של איראן, ולוודא שהם אינם מצליחים לפעול ולפגוע ביכולות חיוניות של מערכת הביטחון. השכבה השנייה נוגעת למערך התשתיות החיוניות במדינה, המונחות על ידי הרשות לאבטחת מידע מתוקף החלטת ממשלה. גם כאן, האתגר מחייב פעילות מתמדת בייחוד בכל הקשור להבנת תמונת האיום, לשיתוף מידע בין גורמים שונים ולהתאמת המענה לאיום זה. לבסוף, אין לזלזל ביכולות האיראניות לנסות לפגוע בעסקים ובתעשייה שאינם מונחים על ידי רשויות המדינה. עסקים ותעשייה במגזר הפרטי פועלים ברוב המקרים בעיקר להגנת נכסי המידע שלהם, וקשה לדרוש מהם להתגונן מפני האפשרות שיותקפו במרחב הסייבר על ידי מדינה זרה כמו איראן. לכן, החשיבות המכרעת של המטה הקיברנטי הלאומי שהוקם לאחרונה כגורם המתכלל ומי שיכול לקדם תהליכי אסדרה ושיתוף מידע ומודיעין בהתאם למפת האיומים המתפתחת.

הערות

1 Art Keller, "The Great Persian Firewall, Should we care that Iran just turned off Google?", *Foreign Policy*, September 28, 2012, http://www.foreignpolicy.com/articles/2012/09/28/Iran_firewall_google?page=full

2 הצהרתו של ח'מאנאי בעת ההכרזה על הקמת המועצה באתרו הרשמי: http://farsi.khamenei.ir/message-content?id=19225

3 Ilan Berman, *The Iranian Cyber Threat to the U.S. Homeland*, Statement before the U.S. House of Representatives Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies and Subcommittee on Counterterrorism and Intelligence, April 26, 2012, pp 1-3, http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20-%20Berman.pdf

4 CBS News, *Iran Confirms Stuxnet Worm Halted Centrifuges*, 29 November 29, 2010, http://www.cbsnews.com/stories/2010/11/29/world/main7100197.shtml

5 Kevin McCaney, *Iran building a private, isolated Internet, but can it shut out the world?* CGN, April 10, 2012, http://gcn.com/articles/2012/04/10/iran-building-separate-isolated-internet.aspx

6 Agence France Presse, *Iran denies has plan to cut Internet access*, AFP, 10 April 2012, http://www.google.com/hostednews/afp/article/ALeqM5h4e57x6CYbsavza1PeDuQP7Bf9Vg

7 Amir Taheri, *Iran will launch its national internet next week but not for the reasons you might think*, September 20, 2012, http://www.opednews.com/articles/Iran-will-launch-its-natio-by-Amir-Taheri-120919-83.html

8 Brian Ross, *What Will Happen to the US If Israel Attacks Iran?* ABC News, 5 March 2012, http://abcnews.go.com/Blotter/israel-attacks-iran-gas-prices-cyberwar-terror-threat/story?id=15848522

9 Ilan Berman, p 4.

10 Reza Marashi, *The Islamic Republic's Emerging Cyber War*, National Iranian American Council, April 30, 2011, http://www.niacouncil.org/site/News2?page=NewsArticle&id=7318

11 Yaakov Katz, Iran embarks on $1b. cyber-warfare program, *The Jerusalem Post*, 18 December 18, 2011, http://www.jpost.com/Defense/Article.aspx?id=249864

12 Patterson, J.P & M.N. Smith, *Developing a Reliable Methodology for Assessing the Computer Network Operations Threat of Iran*, Master's Thesis, Monterey, CA: Naval Postgraduate School, 2005, pp. 17-22, http://www.fas.org/irp/eprint/cno-iran.pdf

13 אתר אוניברסיטת שריף: http://www.sharif.ir/web/en

14 אתר המכון: http://www.aictc.com/web/content/main

15 אתר המכון: http://acri.sharif.ir/en/Default.asp

16 פירוט הקורסים המתקדמים: http://ceit.aut.ac.ir/autcms/courses/courseOfferingView.htm?level=M.Sc&depurl=computer-engineering&lang=en&cid=70317

17 אתר המעבדה לביטחון מידע: http://ceit.aut.ac.ir/autcms/labs/verticalPagesAjax/labHome.htm?id=3350532&depurl=computer-engineering&lang=en&cid=147776

18 אתר המעבדה למערכות מאובטחות: http://ceit.aut.ac.ir/autcms/labs/verticalPagesAjax/labHome.htm?id=3369580&depurl=computer-engineering&lang=en&cid=147732

19 Patterson, J.P & M.N. Smith, pp. 29-35.

20 פעילות המכון בתחום אבטחת המידע: http://www.itrc.ac.ir/itrc-secure-en.php

21 התייחסות להשקעה בטכנולוגיות מידע באתר של TCO: http://citc.ir/newpages/page27.aspx?lang=Fa

22 The Wisconsin project on nuclear arms control, *Iran Watch*, January 3, 2011, http://www.iranwatch.org/suspect/records/technology-cooperation-office.htm

23 רשימת החברות ב־Paradis Technology Park: http://www.techpark.ir/?/content/142

24 אתר Guilan Science Park: http://www.gstp.ir/modules.php?name=Content&pa=sho&pid=16

25 Steve Stecklow, "Chinese firm helps iran spy on citizens," Reuters, March 22, 2012, http://graphics.thomsonreuters.com/12/03/IranChina.pdf

26 Reza Marashi, 2011, עלון מידע המציג את טכנולוגית ה־SEPAR ומצביע על הקשר בין המשטר לבין פיתוחה: http://www.iranascience.com/1-home/newsletters/21-Web%20Filters.pdf

27 OpenNet Initiative, Country Study: *Internet Filtering in Iran 2004-2005*, 16 June 2009, http://opennet.net/research/profiles/iran

28 Kevin McCaney, "Iran building a private, isolated Internet, but can it shut out the world?" ,GCN ,10 April 2012, http://gcn.com/articles/2012/04/10/iran-building-separate-isolated-internet.aspx

29 Robert Tait, "Iranian state goes offline to dodge cyber-attacks," *The Telegraph*, 5 August 2012, http://www.telegraph.co.uk/news/worldnews/middleeast/iran/9453905/Iranian-state-

goes-offline-to-dodge-cyber-attacks.html

30 Cyrus Farivar, "Security researcher unearths plans for Iran's halal Internet," *Ars Technica*, 17 April 2012, http://arstechnica.com/tech-policy/2012/04/iran-publishes-request-for-information-for-halal-internet-project/

31 Robert Tait, 2012.

32 Ali Akbar Dareini and Brian Murphy, "Iran Internet Control: Tehran Tightens Grip On Web," The Huffington Post, 16 April 2012, http://www.huffingtonpost.com/2012/04/16/iran-internet-control_n_1429092.html?ref=world

33 Emily Alpert and Ramin Mostaghim, "Iran's supreme leader calls for new Internet oversight council," *Los Angeles Times*, 7 March 2012, http://latimesblogs.latimes.com/world_now/2012/03/iran-internet-council-khamenei.html

34 *Structure of Iran's Cyber Warfare*, BBC Persian, p. 1. http://nligf.nl/upload/pdf/Structure_of_Irans_Cyber_Operations.pdf

35 "Iran is formulating strategic cyber defense plan: official," *Tehran Times*,15 June 2012, http://tehrantimes.com/politics/98761-iran-is-formulating-strategic-cyber-defense-plan-official

36 מבנה המרכז ותפקידיו מפורטים באתרו הרשמי: http://www.certcc.ir/index.php?newlang=eng

37 "Structure of Iran's Cyber Warfare," BBC Persian, pp. 4-5.

38 "Iran to crack down on web censor-beating software," *Hürriyet Daily News*, 22 September 2012, http://www.hurriyetdailynews.com/iran-to-crack-down-on-web-censor-beating-software.aspx?pageID=238&nID=22789&NewsCatID=374

39 Structure of Iran's Cyber Warfare, p. 4.

40 בינואר 2012 חוקק המשטר מערכת חוקים לשם מעקב וניטור הגולשים מתוך האינטרנט קפה ברחבי המדינה. חוקים אלו מאפשרים ל־FETA ליצור "ספר משתמשים" של כלל הגולשים הארעיים במדינה ולנטר פעילות נגד המשטר במרחב הסייבר. Farnaz Fassihi, "Iran Mounts New Web Crackdown," *The wall Street Journal*, 6 January 2012, http://online.wsj.com/article/SB10001424052970203513604577142713916386248.html

41 lIan Berman, p. 4.

42 Kevin Coleman, "Iranian Cyber Warfare Threat Assessment," *Defense Tech*, 23 September 2008, http://defensetech.org/2008/09/23/iranian-cyber-warfare-threat-assessment

43 Stephen Trimble, "Avtobaza: Iran's weapon in alleged RQ-170 affair?" *The DEW Line*, 5 December 2011, http://www.flightglobal.com/blogs/the-dewline/2011/12/avtobaza-irans-weapon-in-rq-17.html

44 Frank J. Cilluffo, *The Iranian Cyber Threat to the United States*. A Statement before the U.S. House of Representatives Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence and Subcommittee on Cyber security, Infrastructure Protection and Security Technologies, 26 April 2012, p. 5. http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20-%20Cilluffo.pdf

45 Scott Peterson, "Iran's cyber prowess: Could it really have cracked drone," *The Christian Science Monitor*, 24 April 2012, http://www.csmonitor.com/World/Middle-East/2012/0424/Iran-s-cyber-prowess-Could-it-really-have-cracked-drone-codes

46 Frank J. Cilluffo, p. 5.

47 Patterson, J.P & M.N. Smith, pp. 44-49.

48 Iftach Ian Amit, *Cyber [Crime|War],* Linking State Governed Cyber Warfare with Online Criminal Groups, paper presented at DEFCON 18 conference, 31 July 2010, http://www.defcon.org/images/defcon-18/dc-18-presentations/Amit/DEFCON-18-Amit-Cyber-Crime-WP.pdf

49 Khashayar Nouri, *Cyber Wars in Iran*, Institute for War & Peace Reporting, 23 July 2010, http://iwpr.net/report-news/cyber-wars-iran

50 Golnaz Esfandiari, "Basij Members Trained To Conquer Virtual World," Payvand Iran News, 21 August 2010, http://www.payvand.com/news/10/aug/1206.html

51 Jeffrey Carr, "Iran's Paramilitary Militia Is Recruiting Hackers," *Forbes*,12 January 2011, http://www.forbes.com/sites/jeffreycarr/2011/01/12/irans-paramilitary-militia-is-recruiting-hackers/

52 Bob Beauprez, "Iranian Cyber-Attack Plot against U.S. Exposed in Mexico," Townhall, 13 December 2011, http://finance.townhall.com/columnists/bobbeauprez/2011/12/13/iranian_cyberattack_plot_against_us_exposed_in_mexico/page/full/

53 SSl - Secure Socket Layer הנו פרוטוקול לתקשורת מאובטחת באינטרנט, המוודא שהשרת שאליו מתחבר הלקוח הנו השרת הנכון, תוך הצפנת המידע בין דפדפן הלקוח לבין השרת. ניתן לרכוש מפתחות SSL מספקים מורשים. גניבת מפתחות מאפשרת לגורם (שיש לו שליטה על תשתית הרשת) להסיט גולשים לאתרים מזויפים המתחזים להיות אתרים חוקיים, וכך לקבל גישה למידע חסוי של המשתמש.

54 דיווח החברה מה־13 במארס 2011, http://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html

55 Eva Galperin, Seth Schoen and Peter Eckersley, *A Post Mortem on the Iranian DigiNotar Attack*, Electronic Frontier Foundation, 13 September 2011, https://www.eff.org/deeplinks/2011/09/post-mortem-iranian-diginotar-attack

56 Fox-It, Interim Report, *DigiNotar Certificate Authority breach "Operation Black Tulip"*, 5 September 2011.

57 Toby Sterling, "Iran Involvement Suspected In DigiNotar Security Firm Hacking," HuffPost Tech, 5 September 2011, http://www.huffingtonpost.com/2011/09/05/iran-diginotar-hack_n_949517.html

58 Gerry Smith, "Cyber Attacks Against US Banks Sponsored By Iran, Lieberman Says," The Huffington Post, 9 September 2012, http://www.huffingtonpost.com/2012/09/21/cyber-attacks-banks-iran-lieberman_n_1904846.html

59 זהו ארגון שמטרתו לנתח ולשתף מידע בין הגורמים הפיננסיים לגבי איומים על שירותים פיננסיים חיוניים בארצות־הברית. (Financial Services Information Sharing and Analysis Center FS-ISAC)

60 Jaikumar Vijayan, "U.S. banks on high alert against cyberattacks," *Computerworld*, 20 September 2012, http://www.computerworld.com/s/article/print/9231515/U.S._banks_on_high_alert_against_cyberattacks

61 Jim Finkle, "Exclusive: Insiders suspected in Saudi cyber-attack," Reuters, 7 September 2012, http://in.reuters.com/article/2012/09/07/net-us-saudi-aramco-hack-idINBRE8860CR20120907

62 Kelly Jackson Higgins, "Shamoon Code 'Amateur' But Effective," Dark Reading, 11

September 2012, http://www.darkreading.com/advanced-threats/167901091/security/attacks-breaches/240007179/shamoon-code-amateur-but-effective.html

וגם Nicole Perlroth, "Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," *New York Times*, 23 October 2012, http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?_r=1&adxnnl=1&pagewanted=all&adxnnlx=1351084069-1i53F0BCczNEGcP8ut3n4A&

63 Associated Press, "Panetta hints Iran behind Gulf cyberattacks," CBS News,12 October 2012, http://www.cbsnews.com/8301-202_162-57531088/panetta-hints-iran-behind-gulf-cyberattacks

64 Jeffrey Carr, "Who's Responsible for the Saudi Aramco Network Attack?" Blogspot, 27 August 2012, http://jeffreycarr.blogspot.co.uk/2012/08/whos-responsible-for-saudi-aramco.html

65 Global Research & Analysis Team, "Shamoon the Wiper - Copycats at Work," Kaspersky Lab Expert, Securelist, 16 August 2012, https://www.securelist.com/en/blog?print_mode=1&weblogid=208193786

66 "Iranian hackers attacked three largest U.S. banks as part of cyber campaign: sources," National post from Reuters, 21 September 2012, http://news.nationalpost.com/2012/09/21/iranian-hackers-attacked-three-largest-u-s-banks-as-part-of-cyber-campaign-sources

67 Nicole Perlroth, 23 October 2012.

68 Associated Press, 12 October 2012.

התעצמות הצי ההודי – מבט מערבה

יובל צור, תמיר מגל ונדב קדם

הקדמה

הודו היא מדינה המתפתחת במהירות,[1] היא נהנית מצמיחה כלכלית מרשימה, כוחה בזירה הבינלאומית עולה לאורך השנים והוא צפוי להמשיך לעלות.[2] במקביל להתפתחות העוצמה ההודית, הולכת ומתגבשת בהודו זהות מעצמתית. לאורך השנים מתחזקת התפיסה בהודו כי האינטרסים הלאומיים שלה מגיעים הרחק מעבר לגבולותיה הריבוניים. מכאן נובעת גישתה להגנה על האינטרסים הלאומיים שלה באמצעות דיפלומטיה ימית, ובהקשר זה, הקרנת עוצמה ימית באזורי העניין. במילים אחרות, הודו מעוניינת לפתח את יכולותיה על מנת למנוע פגיעה באינטרסים חיוניים שלה, על ידי הפגנת נוכחות והשגת שליטה ימית לפרק זמן ממושך, הרחק מגבולותיה הטריטוריאליים.

במאמר זה נסקור את עלייתה ההדרגתית של הודו לכדי מעצמה ואת התפתחות העניין שלה ב"שכונתה המורחבת",[3] תוך התמקדות בחלק המערבי של אותה "שכונה". עיקר האזור המדובר כולל בראש ובראשונה את המרחב הימי שממערב להודו, עד מצר הורמוז בצפון ומפרץ עדן/קרן־אפריקה בדרום. כמו כן, אזור זה כולל בתוכו את המפרץ הפרסי ואת אזור הים האדום וחופי מזרח־אפריקה. המאמר יסביר מושגים כגון: הקרנת העוצמה, עוצמה ימית וצי מים כחולים, תוך סקירת התפתחותו של הצי ההודי ופוטנציאל השימוש בו במרחב ממערב להודו. לבסוף, נבחן את הפוטנציאל המתפתח עבור ישראל לאור מגמות אלו.

תא"ל (מיל') יובל צור שימש כרמ"ט וסגן מפקד חיל הים. לאחר שחרורו מצה"ל שימש כסגן ראש הוועדה לאנרגיה אטומית. בימים אלו הוא שוקד על הקמתה וניהולה של הקתדרה לחקר אסטרטגיה ימית באוניברסיטת חיפה.
נדב קדם הוא דוקטורנט למדעי המדינה באוניברסיטת חיפה. נדב היה מלגאי בתכנית ניובאוור לתלמידי מחקר בשנים 2010 – 2012 במכון למחקרי ביטחון לאומי.
תמיר מגל הינו עוזר מחקר במכון למחקרי ביטחון לאומי.

הודו כמעצמה עולה

מאז קבלת עצמאותה ראתה הודו את עצמה כשחקנית מפתח בזירה הבינלאומית, ופעלה באופן עצמאי ואף מתגרה כלפי ארצות־הברית וברית־המועצות. עם זאת, עוצמתה הכלכלית והצבאית לא עלו בקנה אחד עם שאיפותיה הגלובליות. סיום המלחמה הקרה הביא לשינוי מהותי בסביבה הגיאו־פוליטית והאסטרטגית של הודו: ברית־המועצות, משענתה החשובה, קרסה; יריבתה האזורית הגדולה, סין, כבר הניחה את היסודות להתעצמותה; הדרך לשיפור היחסים עם ארצות־הברית נפתחה, וכלכלתה של הודו עברה רפורמות מקיפות מבית והחלה לצמוח בקצב מרשים. מרחב האפשרויות של הודו התרחב לאור עוצמתה הכלכלית הגדלה, נוצרו אפשרויות לפיתוח אזורי השפעה לנוכח נפילת ברית־המועצות והמגבלות של היכולת האמריקנית לבסס נוכחות בכל אזורי החיכוך על פני הגלובוס.

יתרה מכך, התפתחות הכלכלה ההודית חייבה להגביר את אספקת חומרי הגלם והסחורות המוגמרות. לפיכך, הודו – הענייה במשאבי טבע ובעלת תשתית תעשייתית מוגבלת – החלה לגלות עניין בנתיבי הקשר והסחר הבינלאומיים (S.L.O.C)[4] לשם הבטחת אספקתם של משאבים אלה. לבסוף, עלייתה של סין, "יריבתה הטבעית" של הודו, הובילה לחשיבה אסטרטגית מחודשת המביאה בחשבון את הצורך בהגברת העוצמה ההודית. כלומר, חשוב להודו (ולא בלתי־אפשרי) לדחוק את רגליה של סין באזורים בעלי חשיבות עבורה.

חשוב להדגיש כי סין מייחסת חשיבות רבה לנתיבי "מחרוזת הפנינים" [5] – נתיבי קשר ימיים מרכזיים המשתרעים מסין עד מזרח־אפריקה – והיא משקיעה מאמצים מרובים בהבטחת השפעתה באזורים אלה. נתיבי "מחרוזת הפנינים" מקיפים את הודו ומהווים חלק מאסטרטגיה לביסוס מעמדה של סין באזור האוקיינוס ההודי. מטבע הדברים, אסטרטגיה זו מעוררת חששות בהודו מדחיקת רגליה באזורים אלה.

יש להדגיש כי השינויים שעוברת הודו הם איטיים וארוכי־טווח. התוצר המקומי הגולמי (תמ"ג) ההודי עודנו נמוך משמעותית (במונחי שערי חליפין) מן התמ"ג הגרמני, הבריטי או הצרפתי (מדינות קטנות מהודו בשיעור ניכר). הבסיס התעשייתי של הודו עודנו מצומצם, התשתיות ההודיות לוקות בחסר והאתגרים הפנימיים שמולם ניצבת הודו הם הרקוליאניים בממדיהם. במידה רבה, יעדי הביטחון הלאומי והאסטרטגיות הנגזרות מכך בעידן שלאחר המלחמה הקרה עודם מתפתחים ומתעצבים.

למרות זאת, ניתן להבחין בתהליך עקבי ומתמשך של פיתוח זהותה של הודו כמעצמה אזורית חשובה, בעלת עניין באזורי השפעה שאינם בהכרח סמוכים לגבולותיה. תהליך זה נמשך תחת קואליציות פוליטיות שולטות שונות, ונראה שכיוונו הכללי אינו שנוי במחלוקת בקרב הציבור ומקבלי ההחלטות ההודיים.

הגדרת איזור ההשפעה והסברת חשיבותו

מזכיר ההגנה ההודי[6] לשעבר, שקהאר דוט (Shekhar Dutt), הגדיר ב־2007 את אזור ההשפעה שהודו שואפת אליו, באופן הבא:[7]

> "... עקב גודלה של המדינה ותפקידה בקרב האומות, תחומי העניין הביטחוני שלנו אינם מוגבלים לשכונה המיידית [immediate neighborhood]... אזור העניין הביטחוני של הודו משתרע מעבר להגדרה הגיאוגרפית המקובלת ביחס לדרום־אסיה... סביבת הביטחון של הודו משתרעת מן המפרץ הפרסי עד מצר מלאקה [Strait of Malacca] דרך האוקיינוס ההודי, ובכלל זה אזור מרכז־אסיה בצפון־מערב האוקיינוס ההודי, סין בצפון־מזרח האוקיינוס ההודי ודרום־מזרח אסיה".

מעבר להגדרה מוסכמת זו, יש אף גורמים הודיים המרחיבים אזור זה מערבה ודרומה. לדוגמה, לפי שר החוץ ההודי לשעבר, ישוואנט סינהא (Yashwant Sinha):[8]

> "השכונה המורחבת [extended neighborhood] של הודו משתרעת מתעלת סואץ עד ים סין הדרומי, וכוללת בתוכה את מערב־אסיה,[9] המפרץ הפרסי מרכז־אסיה, מזרח־אסיה, האזור האסייתי של האוקיינוס השקט (Asia Pacific) ואזור האוקיינוס ההודי".

האינטרסים ההודיים המרכזיים באזורים אלה הם הגנה על אינטרסים הודיים באזור הכלכלי הבלעדי (EEZ)[10] , אבטחת נתיבי הסחר הימיים (S.L.O.C) עבור הודו העוברים בים הערבי והבטחת מעמדה באזורים אלה מול סין. בהקשר זה חשוב לציין את נתיבי הסחר המגיעים לים הערבי דרך תעלת סואץ והים האדום, ואת נתיבי הסחר המגיעים לים הערבי מן המפרץ הפרסי. כך לדוגמה, לפי מפקד הצי ההודי לשעבר, האדמירל סוריש מהטה (Sureesh Mehta):

> "במסגרת כלל האינטרסים הלאומיים והביטחוניים, האינטרס הצבאי־ימי המרכזי הוא להבטיח את ביטחוננו הלאומי, לספק הגנה מפני התערבות חיצונית, כך שהמטלות החיוניות של טיפוח צמיחה כלכלית ופעולות של פיתוח כלכלי יוכלו להתקיים בסביבה בטוחה. כתוצאה מכך, האסטרטגיה הצבאית־ימית של הודו תומכת במדיניותנו בנוגע ל'חופש לעשות שימוש בימים למען מטרותינו הלאומיות בכל הנסיבות'."

עם זאת, ניתן להצביע על אינטרסים נוספים. דוגמה בולטת לכך היא הקשרים "המיוחדים" בין הודו לאזור המפרץ הפרסי. למעשה, הודו ניהלה קשרים מסורתיים עם אזור המפרץ – קשרי הסחר והתרבות בין הצדדים הם עתיקי יומין. אמנם, קשרים אלה סטו מעט ממסלולם לאור עצמאותה של הודו, אך דומה שמבנה התמריצים הבסיסי המכתיב קשרים אלה תרם לשדרוג מחודש של הקשרים. כמו כן, הודו נהנית מהכנסות גבוהות מאוד מעובדים זרים הודיים במפרץ. יתרה מכך, מתהווה מעין קשר "טבעי" בין הצדדים: מדינות המפרץ נדרשות לטכנולוגיה, לידע ולמיומנות הודית, בעוד הודו נזקקת לאנרגיה ולהשקעות מן המפרץ. הווה אומר, מבחינתה של הודו מדובר בברית "טבעית", יציבה ונוחה לכל הצדדים.

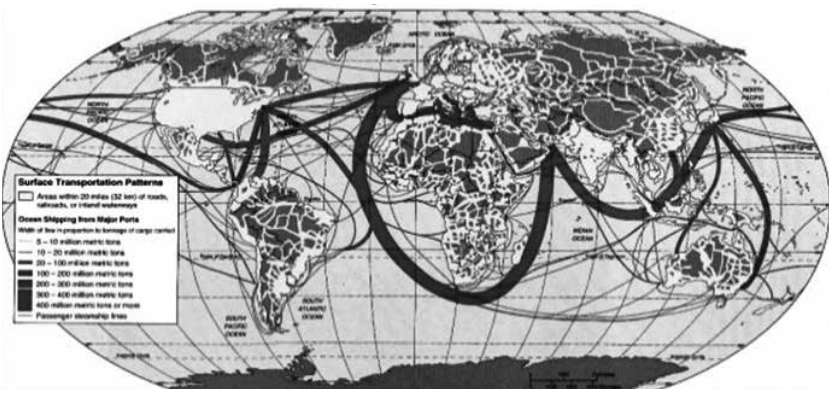
במידה רבה, אזור המפרץ משמש כמרחב עורף טבעי של הודו למסחר ולאספקת משאבים. חשיבותו של אזור זה רק גדלה עקב "צימאונה" הגובר של הודו למשאבי טבע. הצורך להרחיב ולגוון את מקורות האנרגיה (סוגים שונים של מקורות אנרגיה ומדינות מוצא) הוא חיוני להודו. חשוב להדגיש כי לא רק הודו לוטשת עיניים לעבר מקורות האנרגיה במפרץ, אלא גם מעצמות אחרות שביניהן יריבתה סין, הצמאה למשאבים. נסיגתה של ארצות־הברית מעיראק והנסיגה הצפויה מאפגניסטן מלבות את החשש מרִיק אפשרי נוכח היחלשות מעמדה של ארצות־הברית באזור. התפתחות פוטנציאל הפקת הנפט במדינות מזרח־אפריקה ושדות פעילים בסודאן ובמצרים מדגישים אף יותר את הצורך באבטחת נתיבי הסחר והגישה למקורות האנרגיה באזור.

כפי שניתן לראות מן המפה המצורפת, נתיבי הסחר ההודיים עוברים בסמוך למדינות קרן־אפריקה ולחצי־האי ערב, וכן בסמוך לחופה הדרומי של איראן ולמצר הורמוז, ומכאן העניין ההודי המובהק בהגנה על נתיבים אלה. יש להדגיש כי הסכנות השונות האורבות בנתיבי הסחר אינן תיאורטיות בלבד. כבר כיום, פיראטים הפועלים בסמוך לחופי סומליה תוקפים את אניות צי הסוחר ההודי. פיראטיות ימית זו והטרור הימי הבינלאומי מדאיגים במיוחד לאור ההתפתחות המהירה של פוטנציאל הפקת הנפט במזרח־אפריקה.

במובנים רבים, הצי האמריקני מספק כיום "מוצר ציבורי" המבטיח לכולם את חופש הסחר וזרימת המשאבים מן האזור. עם זאת, גם הצי האמריקני מוגבל בהיקף כוחותיו, האינטרסים האמריקניים אינם עולים תמיד בקנה אחד עם אלה של מדינות אחרות, וכל יוזמה של שיתוף פעולה בין הציים מתרחשת על פי התנאים האמריקניים. הודו חוששת כי לא תוכל להמשיך להסתמך באופן מלא ובלעדי על ארצות־הברית בנושא. חיכוכים בין הודו לבין ארצות־הברית נתגלעו כבר מאז 2003, על רקע היוזמה האמריקנית לפעולה ימית משותפת במסגרת PSI.[11]

בהקשר זה, חשוב להדגיש את מעמדה הייחודי של איראן המספקת להודו גישה קרקעית למרכז־אסיה.[12] זאת, בהעדר יכולת להגיע לאזורים אלה דרך יריבותיה (בעלות־הברית) סין ופקיסטן. ההודים מייחסים חשיבות רבה לפיתוח קשרים עם מדינות מרכז־אסיה. בין השאר, מדינות אלו נתפסות כמקור חשוב למשאבי טבע, אך גם כפוטנציאל גדול לאיומים ביטחוניים (כגון טרור). פרויקט הפיתוח השאפתני של נמל צ'ה באהאר (Chah Bahar) באיראן על ידי הודו הוא דוגמה טובה לכך. נמל זה שהודו סייעה בבנייתו אמור לשמש מסדרון הודי למרכז־אסיה. הודו מעורבת כיום בהנחת מסילת ברזל מהנמל לאפגניסטן. במקביל, הסיוע הכספי הנדיב שמעניקה הודו [13] לאפגניסטן, שני בהיקפו רק לסיוע האמריקני למדינה, הוא רק עדות אחת מני רבות לרצון ההודי "לפקוח עין" על מדינות מרכז־אסיה. הקשרים של איראן עם קבוצות סוניות קיצוניות באפגניסטן ובפקיסטן יכולים

נתיבי שייט בינלאומיים



גם לסייע להודו בריסון קבוצות אלו. למעשה, הודו זקוקה לאיראן כאיזון מסוים מול יריבתה, פקיסטן. בהקשר זה חשוב להזכיר כי הודו מעוניינת – באמצעות קשריה עם מדינות המפרץ – למנוע קרבה יתרה בין ערב־הסעודית ופקיסטן – בעלות־הברית הסוניות.

הקרנת עוצמה ועוצמה ימית

המושג "הקרנת עוצמה" (Power projection) מתייחס ליכולתה של מדינה להפעיל עוצמה מדינית, כלכלית, אסטרטגית וצבאית, לשם קידום יעדיה האסטרטגיים.[14] בין היתר, המרכיב הצבאי של הקרנת עוצמה מתייחס גם ליכולתה של מדינה להפעיל את כוחה הצבאי לפרק זמן ממושך, הרחק מגבולותיה הטריטוריאליים. יש להדגיש כי היכולת לבצע תקיפה נקודתית של מטרות הרחק משטחה הריבוני של המדינה התוקפת אינה מהווה הקרנה של עוצמה באופן מלא, כיוון שחסרה עדיין היכולת לפעולה מתמשכת לאורך הזמן.

באופן מסורתי נשענה הקרנת עוצמה על קיומה של עוצמה ימית (Sea-power). עוצמה זו מוגדרת כיכולת להשפיע "בים ומן הים" (At sea and from the sea).[15] נוסף על מרכיבים צבאיים, עוצמה זו כוללת מרכיבים רבים אחרים, ובכללם: צי סוחר, דיג, תעשיות ימיות, בניית אוניות ותיקונן. יש להדגיש כי עוצמה ימית היא יחסית ואינה מוחלטת, והיא משמעותית הן בזמן שלום והן בזמן במלחמה.

מרכיב צבאי מרכזי של עוצמה ימית הן ספינות קרב גדולות[16]. לספינות אלו יכולת שהייה ממושכת יותר, במרחק גדול יותר ועם יכולת אש גבוהה יותר, בהשוואה לספינות קטנות יותר ולמטוסי קרב ותקיפה. מרבית הפעולות של הקרנת עוצמה בעשורים האחרונים היו כרוכות בשימוש משמעותי בצי של 'מים כחולים', (עיראק, לוב, אפגניסטן, סומליה, פוקלנד).[17]

הפעלת הצי הרחק מנמלי הבית נעשית בדרך כלל במסגרת של כוחות משימה.[18] כוחות אלה כוללים מספר ספינות בעלות תפקידים שונים (נגד מטוסים, נגד צוללות, נגד טילים, איתור מוקשים, שיגור טילים), המשלימות ומגוננות זו על זו. כוחות המשימה התפתחו באופן היסטורי סביב נושאות המטוסים במהלך מלחמת העולם השנייה, וגם כיום בנויים כוחות משימה אלה סביב ספינת פיקוד גדולה כגון נושאת מטוסים או ספינת נחיתה אמפיבית (LPD/LDH). ספינות אלו, בהדחק (נפח) של 40,000–60,000 טון, מספקות עורף פיקודי ולוגיסטי לכוחות המשימה, ומאפשרות הפעלה של מטוסי קרב (כשמדובר בנושאות מטוסים). היכולת להפעיל מטוסים מלב ים משלבת את היתרונות של שני המרחבים ומאפשרת מהירות וגמישות תגובה של מטוס, יחד עם הטווחים ויכולת השהייה של ספינות. יחד עם זאת, בעוד נושאות מטוסים וספינות נחיתה אמפיביות מאפשרות ביצוע מגוון משימות של הקרנת עוצמה, הרי חלק מן המשימות – כגון הגנה על נתיבי סחר או מאבק בפיראטיות – אינן דורשות להתבסס על ספינות מסוג זה. כיום, רק כ־13 מדינות מפעילות נושאות מטוסים, ביניהן גם הודו.[19]

התעצמות הצי ההודי

בעשורים הראשונים לקיומו הורכב הצי ההודי בעיקר מספינות קטנות (פחות מ־3,000 טון), ומילא בעיקר משימות של הגנת המים הטריטוריאליים. עם זאת, כבר בשנת 1957 רכש הצי ההודי מבריטניה נושאת מטוסים "קלה" בשם ויקראנט (Vikrant). דגם זה שנבנה במהלך מלחמת העולה השנייה היה קטן יותר מנושאות מטוסים סטנדרטיות (20,000 לעומת 40,000 טון), ואִפשר הפעלה של מטוסי תקיפה בעלי טווח מוגבל. ספינה זו עמדה בראש קבוצת קרב של שלוש ספינות שהוצבו באיי אנדמן, ונטלה חלק במלחמת הודו־פקיסטן ב־1971, כאשר טייסות הקרב שלה תקפו נמלים מרוחקים בבנגלדש. לקחי המערכה הזו הביאו להכרה במגבלות הפעולה של הצי ההודי, יחד עם ההבנה בדבר הצורך בבנייה של צי מים כחולים.

בראשית שנות השמונים החלה הודו לרכוש משחתות ופריגטות נושאות טילים, בנוסף לספינות קטנות יותר שנועדו למשימות במים הטריטוריאליים. ספינות אלו נבנו תחילה בעיקר במספנות זרות בבריטניה וברוסיה, יחד עם פיתוח של תשתית מקומית לבניית ספינות גדולות. גם כיום נזקקת הודו לידע טכנולוגי רב בהטמעת מערכות נשק שונות על גבי הספינות.

בסוף שנות השמונים כלל הצי ההודי חמש משחתות, שלוש פריגטות, ארבע קורבטות, וכן שש צוללות נושאות טילי שיוט. זאת בנוסף לשתי נושאות מטוסים: ויקראנט הוותיקה, אשר הוצאה לבסוף משירות בשנת 1997, ונושאת מטוסים קלה נוספת בשם ויראט (Viraat), אשר נרכשה בשנת 1986 לאחר 17 שנות שירות בצי

הבריטי. בראשית שנות האלפיים כלל הצי ההודי נושאת מטוסים אחת, שמונה משחתות (7,000 טון), תשע פריגטות (4,000–5,000 טון), שמונה קורבטות (2,500–3,000 טון), וכן עשר צוללות נושאות טילי שיוט. לספינות אלו יכולת שיגור טילים לטווחים של 200–300 קילומטר, כולל טילי שיוט מתוצרת הודית.
הטבלה הבאה בוחנת את היקף הצי ההודי בראשית שנות האלפיים, ומשווה את מספר הפלטפורמות שהיו ברשותו עם מספר ציים אחרים בני התקופה: [20]

טבלה 1. השוואת מספר הפלטפורמות בצי ההודי אל מול ציים אחרים, בתקופה הנידונה.

	הודו	בריטניה	צרפת	סין	פקיסטן
נושאות מטוסים	1	3	1		
ספינות LPD		3	6		
צוללות בליסטיות		4	4	2	
צוללות נושאות טילי שיוט	10	12	8	9	11
משחתות	8	11	14	21	
פריגטות	9	20	24	12	6
קורבטות	8			28	

מתוך הטבלה ניתן להסיק כי הצי ההודי, אף כי אינו ניצב במישור אחד עם מעצמות ותיקות כגון צרפת ובריטניה, נמצא בתהליך מהיר של פיתוח יכולות להקרנת עוצמה במספר תחומים. התפתחותו של הצי ההודי בשנים אלו הינה משמעותית בהשוואה לציים אזוריים קטנים, דוגמת הצי הפקיסטני. מחקרים אחרים שהשוו בין ציים בעולם סווגו את הצי ההודי יחד עם סין, בדרגה אחת מתחת למעצמות האירופיות (בריטניה וצרפת), אך מעל ציים אזוריים כגון דרום־אפריקה וישראל. [21]

פרויקטים נוכחיים

בעשור האחרון מנהל הצי ההודי שורה של פרויקטים לבנייה של ספינות חדשות, אשר יעצימו ויחזקו את היקף היכולת שלו לפעול כצי של מים כחולים. פרויקטים אלה, אשר נבנים ברובם במספנות מקומיות, נמצאים בשלבים מתקדמים של מימוש, וחלקם אף עומדים לפני סיום. יחד עם זאת, פרויקטים אלה כוללים רכש של מערכות נשק ממדינות זרות. בחלק זה נסקור את הפרויקטים הללו ואת שלבי התקדמותם, בחלוקה לפי נושאות מטוסים, ספינות קרב וצוללות. [22]

נושאות מטוסים: בשנת 2004 החלה הודו בבנייה של שתי נושאות מטוסים חדשות וגדולות יותר. העסקה הראשונה, בין הודו לרוסיה, כללה מכירה של נושאת מטוסים רוסית "סטנדרטית"[23] מדגם קייב, אשר הושקה בשנת 1987 אך הוצאה משירות בשנת 1996. העסקה כללה שדרוג מלא של מערכות הספינה והוספה של מסלול המראה שני. חילוקי דעות על המחיר הביאו לעיכוב העסקה עד להשגת הסכם על עלות הפרויקט (2.35 מיליארד דולר) במרס 2010. ביוני 2012 החלה הספינה ויקראמאדיטיה (Vikramaditya) לבצע הפלגות מבחן, לקראת מסירתה לידי הצי ההודי.[24] הספינה, באורך 283 מ' ובנפח (הדחק) של 45,500 טון, תפעיל מטוסי קרב סטנדרטיים מדגם MiG-29K , וכן מסוקים ימיים מדגם Ka-31.

העסקה השנייה, לבניית נושאת מטוסים מתוצרת מקומית בשם ויקראנט (Vikrant), נחתמה עם מספנות קוצ'ין בשנת 2004. בשנת 2006 נקבע המבנה הסופי – נושאת מטוסים סטנדרטית באורך 260 מ' ובנפח של 40,000 טון. בדצמבר 2011 הושקה שלדת הספינה המציינת השלמה של כ־40% מן הפרויקט, עם צפי לעריכת הפלגות מבחן בסוף שנת 2014, וכניסה לשירות מבצעי במהלך 2015. הספינה אמורה לשאת מטוסי קרב סטנדרטיים מדגם MiG-29K, מטוסי קרב הודיים מדגם Tejas וכן מסוקים ימיים מדגם Ka-31.

כמו כן, ביוני 2007 נכנסה לשירות בצי ההודי ספינה אמפיבית מדגם LPD בשם Jalashwa, בנפח של 16,500 טון. ספינה זו, הנושאת מספר נחתות וכן מסוקי תובלה מדגם Sea King, התקבלה מעודפי הצי האמריקני והיא מאפשרת הנחתת כוחות מלב ים.

ספינות קרב: כדי להגדיל את מספרן של ספינות הקרב הגדולות ברשות הצי, מנהל הצי ההודי בעשור האחרון מספר פרויקטים לבנייה של משחתות ופריגטות חדשות, בעיקר עם מספנות מקומיות. פרויקטים אלה כוללים:

פרויקט A15 – לבניית שלוש משחתות מדגם כלכתה (Kolkata) בנפח של 7,000 טון במספנת Magazon במומבאי. הספינות מצוידות בטילי שיוט מדגם ברהמוס מתוצרת הודו, ובטילי הגנה אווירית (הגנ"א) מדגם ברק–8 מתוצרת ישראל. ספינה ראשונה מדגם זה נכנסה לשירות ב־2011, ואילו שאר הספינות נמצאות בשלבי בנייה מתקדמים.

פרויקט 17 – לבניית שלוש פריגטות מדגם שיבאליק (Shivalik) בנפח של 5,300 טון, על ידי מספנת Magazon במומבאי. הספינות מצוידות בטילי שיוט רוסיים מדגם SS-N-27 Club-N. פרויקט זה הושלם עם כניסתה לשירות של הספינה האחרונה מדגם זה, בשנת 2010.

פרויקט טלוואר – בניית שלוש פריגטות נוספות מדגם טלוואר (Talawar) בנפח של 4,000 טון, במספנה רוסית בקאלינינגרד. ספינות אלו יצטרפו לשלוש פריגטות מדגם זה שכבר סופקו לצי ההודי בראשית שנות האלפיים. הספינות מצוידות בטילי

שיוט מדגם ברהמוס ובטילים רוסיים מדגם Club-N. הספינה הראשונה נכנסה לשירות בשנת 2012, ואילו שאר הספינות נמצאות בשלבי בנייה מתקדמים.[25]

פרויקט 28 – לבניית עד 12 קורבטות נושאות טילים בנפח של 2,500 טון, במספנות בכלכתה. הספינות יצוידו בטילי Club-N ובטילי הגנ"א מדגם ברק-8 מתוצרת ישראל. ארבע ספינות ראשונות נמצאות בשלבים מתקדמים של בנייה, וכניסתה של הספינה הראשונה לשירות צפויה במהלך 2012.

מרבית הפרויקטים הללו כוללים גם מעורבות של התעשייה האווירית הישראלית, המספקת למספנות ההודיות מערכות מכ"מ וכן טילים להגנה אווירית והגנה נגד טילים מדגם ברק-8.

צוללות: מאז שנת 2004 מנהל הצי ההודי פרויקט לבניית צוללת מתוצרת מקומית הנושאת טילים בליסטיים. הצוללת ששמה אריאנט (Arihant) נמצאת מאז 2010 בתהליך של מבחנים ימיים, ואמורה להיות מוכרזת כמבצעית במהלך 2012. פיתוח היכולת לשגר טילים מצוללת נעשה במקביל להצלחתה של הודו בהשלמת פיתוח טיל בין־יבשתי מדגם "אגני".[26] כמו כן, ביוני 2012 השלים הצי ההודי תהליך של שדרוג עשר צוללות מדגם KILO הנושאות טילי שיוט, ונמצאות בשירות משנות התשעים. צוללות אלו קיבלו "הארכת חיים" וצוידו בטילי שיוט חדישים מדגם Club-S.[27] נוסף לכך חוכר הצי ההודי צוללת תקיפה רוסית מדגם Akula, המונעת בעזרת כור גרעיני ונושאת גם היא טילי שיוט.

לסיכום, בהתחשב בקצב ההתקדמות הנוכחי, יושלמו הפרויקטים הללו במהלך 2015, אזי יכלול הצי ההודי כמות של ספינות קרב גדולות המספיקה לעד שלושה כוחות משימה. יחד עם זאת, לאחר ההשלמה של נושאת המטוסים ויקרמאדיטיה יכלול הצי ההודי שתי נושאות מטוסים פעילות, וכן ספינה אמפיבית נוספת מדגם LPD. מספר זה של ספינות פיקוד יאפשר ציוות של שניים עד שלושה כוחות משימה. בהינתן הצורך ההודי לחלק את הצי בין פיקוד מזרחי לפיקוד מערבי, הרי ציוות של שלושה כוחות משימה יאפשר חופש פעולה רב יותר בהפעלת הצי במרחב של מפרץ עדן. לעומת זאת, הקמה של שני כוחות משימה בלבד תצמצם את מרחב הפעולה של הצי למרחב של מזרח הים הערבי.

משימות הקרנת עוצמה של הצי ההודי

בעשור האחרון, למרות מגבלות הכוח הימי העומד לרשותו, פועל הצי ההודי באופן מתמשך להקרנת יכולת ועוצמה בגבולות "השכונה המורחבת" שהתווה לעצמו. מאמץ זה כולל פעילות הודית מים סין הדרומי ועד מזרח הים התיכון. חלק משמעותי מן המאמץ ההודי מושקע בחלקו המערבי של האוקיינוס ההודי.[28]

דוגמה מרכזית למאמץ זה היא הגנה על חופש השיט והביטחון הימי. במסגרת משימה זו מפעילה הודו כבר כיום נוכחות קבועה בשני מוקדים עיקריים בים הערבי.

מאז 2008 מחזיקה הודו נוכחות קבועה של ספינת קרב במפרץ עדן, שמספקת הגנה לאוניות סוחר מפני התקפות פיראטים. בנוסף מחזיקה הודו נוכחות קבועה של מטוסי סיור וספינת קרב באיי סיישל, כדי לספק הגנה למרחב הכלכלי של האיים, וכן לתעבורה הימית במזרח־אפריקה. גידול נוסף בהיקף הכוחות של הצי ההודי עשוי להוביל לנוכחות קבועה של כוח משימה הודי במפרץ עדן, ולהגברת המעורבות ההודית במאבק בפיראטיות.[29]

דוגמה נוספת הינה הפגנת נוכחות ו"הצגת הדגל ההודי" באזורים חדשים. מאז ראשית שנות האלפיים מקיים הצי ההודי ביקור שנתי של שייטת הכוללת שלוש עד ארבע ספינות במפרץ עומאן, במפרץ הפרסי, בים סוף, ולעיתים גם במרחב הים התיכון. השייטת עורכת ביקורים בנמלים שונים באזור, וכן אימונים משותפים עם ציים מקומיים.[30] פעילות זו מבססת ומרחיבה את הקשרים בין הודו לבין מדינות האזור. עם הכניסה לשירות של נושאת מטוסים שנייה והגדלה נוספת בהיקף הצי ההודי, עשויים ביקורים אלה להתרחב לכדי נוכחות מתמשכת של קבוצת קרב הודית באזור מפרץ עומאן.

משימה נוספת של הצי היא הגנה על אזרחים הודיים במדינות זרות, ופינוי של אזרחים זרים ממדינות עימות. המחשה ליכולת ההודית בתחום זה ניתנה ביולי 2006, כאשר ארבע ספינות קרב הודיות פינו אזרחים זרים מלבנון, בעיצומן של התנגשויות בין ישראל לחיזבאללה.[31] פעולה הודית עתידית יכולה אף לכלול מעורבות והגשת סיוע במקרים של משבר הומניטרי, דוגמת המעורבות ההודית באירועי הצונאמי בשנת 2004.[32]

כמו כן, בעבר ביצע הצי ההודי פעולות הנחתה של כוחות יבשה משמעותיים במדינות רחוקות, כדי להתמודד עם הפיכות ומרידות נגד השלטונות המקומיים.[33] פעולות אלו נעשו במדינות־חסות, והן עשויות לשמש דוגמה לשלב חדש ביכולת הקרנת העוצמה ההודית – מעורבות צבאית במקומות מרוחקים יותר, שבהם מחזיקה הודו אינטרסים חיוניים בתחום הסחר והאנרגיה.

בשל האינטרסים ההודיים בגישה למרכז־אסיה, ייתכן כי הודו תראה צורך לעצמה להזהיר שחקנים אחרים מפני תקיפה של נמל צ'ה באהאר באיראן. מצב זה יכול להביא לעימות עם צד שלישי.

קשרי הציים של הודו וישראל ופוטנציאל פיתוחם

יחסי הודו־ישראל התפתחו במהירות מאז חידוש הקשרים הדיפלומטיים בין שתי המדינות בשנת 1992.[34] מבחינת תחבורתית ישראל היא "מדינת אי", כאשר 98% מסחר החוץ שלה מתבצע באמצעות נתיבי הים.[35] כיום עוברים נתיבי הסחר המשמעותיים עבור ישראל בים התיכון, אך בעבר הייתה גם חשיבות רבה לים האדום, וייתכן שזו תגבר שוב בעתיד. כמדינת אי, חייבת ישראל לשמור על נתיבי

הסחר הימיים ולפתח קשרים כלכליים וביטחוניים מעבר לים. לכן, קיים הגיון אסטרטגי לא־מבוטל בקידום שיתוף פעולה בין ישראל להודו בזירה הימית. מעבר לקשרי המסחר הענפים, חשוב להדגיש את ההיקף הנרחב של מכירת נשק ישראלי להודו ושדרוג שיתוף הפעולה המודיעיני בין הצדדים. עם זאת, לשיתוף פעולה זה יש גם מגבלות שונות, בין השאר לנוכח הקשרים הענפים של הודו עם איראן ומדינות ערב, ובשל קיומה של אוכלוסייה מוסלמית גדולה בהודו גופה.

עקב מגבלות אלו, שיתוף הפעולה בין הצבאות הינו מצומצם יחסית, והודו מעדיפה לשמור על פרופיל ציבורי נמוך במידת האפשר (בעיקר בהקשרים מדיניים וביטחוניים) של שיתוף פעולה זה. חרף זאת, מתקיים קשר מתמשך בין הצי ההודי לבין חיל הים הישראלי, הכולל ביקורים של אוניות הודיות בנמלים ישראליים,[36] לצד ביקורים הדדיים של קצינים בכירים משני הצדדים.[37] ביקורים אלה ממלאים תפקיד של הפגנת נוכחות באמצעות ספינות מלחמה, אשר תכליתה לשרת את מדיניות החוץ ולתת ביטוי לאינטרסים לאומיים חיוניים. היקף הביקורים ההדדיים חורג מן הצורך של אבטחת נתיבי שיט, ומצביע על מפגש האינטרסים בין הצדדים לגבי התמודדות עם האיום המתהווה בזירה הימית בעידן הגלובלי. תהליך הגלובליזציה העצים שורה של איומים מדינתיים ואחרים בזירה הימית: טרור ימי, פיראטיות, הפצה והברחות של אמצעי לחימה, סמים ומהגרים. ההתמודדות עם איומים אלה מחייבת ערנות ימית (M.D.A)[38] ומגבירה את התמריץ לשיתוף פעולה טכנולוגי ומבצעי בין הציים.

שיתוף הפעולה הטכנולוגי בין ישראל להודו התפתח בשנות התשעים, על רקע הצורך של התעשייה הביטחונית הישראלית למצוא לעצמה שווקים חדשים, יחד עם הצורך ההודי בטכנולוגיה צבאית מתקדמת. המשבר בתעשייה הביטחונית הרוסית, בשילוב עם רתיעה אמריקנית ממכירת נשק להודו, הובילו את הודו לחיפוש אחר מקורות חלופיים של טכנולוגיה מודרנית. התעשייה הביטחונית הישראלית זיהתה בזמן את פוטנציאל השוק ההודי, ובייחוד את הצורך ההודי בטכנולוגיה מודרנית בתחום הימי. שיתוף הפעולה הטכנולוגי נבע ממפגש אינטרסים בין שני הציים: הודו תבטיח לעצמה בקרת איכות טובה על הפרויקטים, טכנולוגיה מתקדמת ואפיוני מערכות המתאימים לזירה המודרנית. חיל הים הישראלי, באמצעות התעשיות, יוביל פיתוח ויצטייד במערכות שתקציבו המוגבל לא היה מאפשר (הן מבחינת ההשקעה בפיתוח והן מבחינת היקפי ההצטיידות) לולא שיתוף הפעולה עם הודו.

במסגרת שיתוף הפעולה הטכנולוגי בזירה הימית הצטיידה הודו במערכות טילי הגנה אווירית מדגם "ברק" וכן במערכות מכ"מ לספינות. בנוסף רכשה הודו מל"טים למשימות של סיור ימי, וכן מערכות מכ"מ ותצפית להגנת חופים, הנישאות על גבי בלוני הליום (צפלין). אין ספק שמבחינת ישראל, מדיניות היצוא

הביטחוני היא הסיבה והמסובב ביחסים המתפתחים בין הציים, אך הפוטנציאל ביחסים אלו הינו גדול יותר.

כיוונים עתידיים של שיתוף פעולה ימי ישראלי־הודי:

אחד האתגרים לחיל הים הישראלי הוא הקושי לפעול לאורך זמן הרחק מחופי ישראל. הצי ההודי יכול לאפשר לכלי שיט ישראליים גישה לנמלים לשם קבלת אספקה, בדומה לביקורן של ספינות הודיות בנמלים ישראלים – מהלך שירחיב מהותית את טווח הפעולה של חיל הים הישראלי.

שיתוף פעולה מתמשך בין הציים יוכל (בטווח הארוך) להכשיר את הקרקע להשתתפות ישראליות במבצעי שיטור ימיים בינלאומיים. מבלי לקבוע עמדה בנושא זה, להשתתפות ישראלית במבצעים מסוג זה יש ערך מדיני חיובי.

חיזוק הקשרים בין הציים יכול לאפשר שיתוף בפעילות מבצעית המתבצעת באופן סמוי מן העין. לדוגמה, ייתכן כי על בסיס שיתוף הפעולה המודיעיני הקיים יוכלו ספינות ישראליות, ואולי בעתיד גם ספינות הודיות, לעצור ספינות המבריחות אמצעי לחימה. אמנם, כיום קיימת סבירות נמוכה מאוד לכך שהודו תסכים לעצור ספינות איראניות, אך היא תוכל לסייע מאחורי הקלעים – מבחינה מודיעינית ולוגיסטית – להשתלטות של ספינות ישראליות על כלי שיט חשודים. חשוב להדגיש כי אין זה רצוי להסתמך באופן בלעדי בעניינים אלה על הצי האמריקני. למרות גודלו העצום של הצי האמריקני, גם ליכולותיו יש מגבלות. מעבר לכך, רצוי לגוון את מקורות המידע ולהגדיל את סל האפשרויות העומדות לפני ישראל.

כמו כן, שיתוף הפעולה המתמשך בין הציים יוצר קשרים אישיים בין קצינים הודיים וישראליים, וקשרים אלה נוטים לייצר ולפתח ערוצים של העברת מידע. כאמור, להודו קשרים ענפים עם מדינות המפרץ הפרסי, לרבות איראן ואפגניסטן, כמו גם עניין רב באיומי הטרור האסלאמי. כל אלה גם יחד מובילים לאינטרס משותף לחילופים שוטפים של מידע בעל ערך, תוך נקיטת אמצעי הזהירות הנדרשים.

יש להדגיש כי שיקולים פוליטיים ומדיניים של הודו עלולים להגביל את התפתחות שיתוף הפעולה. בין היתר, יש להביא בחשבון את העדפת ההודים לשימור מערכת היחסים בפרופיל נמוך יחסית, ואת חשיבות שימור הקשר שלהם עם איראן. עם זאת, אין זה מן הנמנע כי שינויים פוליטיים בתוך הודו ו/או התפתחויות אחרות יהפכו את התפתחות שיתוף הפעולה לריאלית מבחינה פוליטית. בסופו של יום, שני הצדדים נזקקים זה לזה, ולכן שיתוף הפעולה ביניהם הוא "טבעי". חשוב כי ישראל תתבונן בהודו מזווית ראייה כוללת, ולא תתמקד בעיקר בפוטנציאל יצוא הנשק להודו.[39] יצוא הנשק אמנם מינף את הקשרים לטובת ישראל, אך אין בו די למימוש הפוטנציאל בכלל, ולמימוש פוטנציאל היחסים בין

הציים בפרט. לפיכך, יש לראות בשיתוף פעולה זה יעד ישראלי מרכזי, שיש לחתור אליו בהתאם להתפתחויות ולהזדמנויות הנקרות בדרכה של ישראל.

הערות

1 לסקירה מקיפה על עלייתה של הודו, ראו: Sumit Ganguly and Rahul Mukherji, *India since 1980*, New York: Cambridge University Press, 2011.

2 לסקירה ביקורתית בנוגע לעלייתה של הודו, ראו: Sumit Ganguly, "Think Again: India's Rise", *Foreign Policy*, July 5, 2012.

3 כפי שניתן יהיה לראות בציטוטים המובאים בהמשך, "השכונה המורחבת" הוא ביטוי שגור בשיח ההודי בנוגע למדיניות חוץ.

4 Sea Lines Of Communication

5 String of Pearls

6 מקביל למנכ"ל משרד הביטחון בישראל

7 Shekhar Dutt, "Defense, Security, Diplomacy: India's National Interests," February 24, 2007. Accessible via www.associationdiplomats.org/specialevents. Identical formulation used in the Ministry of Defense, Annual Report 2006–2007 (New Delhi: Ministry of Defense, 2007).

8 Yashwant Sinha, "12th SAARC Summit and Beyond," February 3, 2004. http://meaindia.nic.in/speech

9 מקובל בהודו לכנות את החלק האסייתי של המזרח־התיכון, כמו גם חלק מן הקווקז, בשם מערב־אסיה. ההגדרה המדויקת של האזור איננה מוסכמת.

10 האזור הכלכלי הבלעדי, המכונה גם "המים הכלכליים" משתרע עד למרחק של 200 מייל מקו החוף של המדינה.

11 יוזמת PSI Proliferation Security Initiative, נועדה למנוע הובלה ימית של נשק להשמדה המונית ושל אמצעי שיגורו, דוגמת טילים בליסטיים.

12 לסקירה בנושא הקרנת העוצמה ההודית הכוללת התייחסות נרחבת לאיראן, ראו: David Scott, "India's "Extended Neighborhood" Concept: Power Projection for a Rising Power," *India Review*, vol. 8, no. 2, pp.107-143.

13 הודו עצמה נהנית מכספי סיוע חוץ של מדינות אחרות.

14 Dictionary of Military and Associated Terms. US Department of Defense, 2005.

15 Mahan, A. *The Interest of America in Sea-Power, Present and Future*, London: Sampson Low, Marston & Company, 1898.

16 ספינות בעלות נפח מעל 3,000 טון.

17 צי של 'מים כחולים' (Blue-water Navy) נבדל מצי "מים ירוקים" ביכולתו לפעול בלב ים, הרחק מחופי מדינת האם. ביטוי מודרני יותר הוא כוחות משלוח (Expeditionary Forces).

18 בשפה העברית, כפי שנהוגה בחיל הים הישראלי, אין מבחינים בין Task Force ל־Battle Group – בשני המקרים משתמשים במושג 'כוח משימה'. עם זאת, בשפה האנגלית כוחות משימה אלה – המיועדים להקרנת עוצמה ופועלים בהתאם למתווה המתואר בהמשך פסקה זו – מכונים Battle Groups.

19 יש להדגיש כי עצם קיומה של נושאת מטוסים בידי מדינה אינה הופכת אותה בהכרח לבעלת עוצמה ימית משמעותית (לדוגמה, תאילנד). נושאת המטוסים חייבת להיות חלק ממערך שלם לשם הקרנת עוצמה.

20 ההשוואה בין ציים, בניגוד להשוואה בין חילות ים, אינה לוקחת בחשבון את כלל התשתיות שברשותם. כמו כן, יש להדגיש כי השוואה בין פלטפורמות אינה מביאה

בחשבון את רמת האמצעים הטכנולוגיים המותקנים בהן.

21 סיווג מקובל בתחום הוא של החוקר גרוב: Eric Grove, *The Future of Sea Power*, Annapolis: Naval Institute Press, 1990.

22 המידע על פרויקטים אלה מגיע ברובו מתוך: *Jane's Fighting Ships 2011*

23 נושאות המטוסים נחלקות על פי גודלן לשלושה סוגים: נושאות מטוסים "קלות" בנפח עד 30,000 טון; נושאות מטוסים "סטנדרטיות" בנפח של 40,000–60,000 טון; נושאות מטוסים "סופר" בנפח מעל 100,000 טון.

24 Christopher P. Cavas, "Indian carrier begins sea trials", *Defense News*, June 8, 2012.

25 "Russian-Built Frigate Arrives in India", RIA Novosti, June 22, 2012, http://en.rian.ru/world/20120622/174181942.html

26 http://articles.latimes.com/2012/apr/19/world/la-fg-india-missile-test-20120419

27 Radyuhin, V. "Russia completes India's submarine modernization program", *The Hindu*, June 23, 2012.

28 Walter c. Ladwig, India and Military Power Projection: Will the "Land of Gandhi Become a Conventional Great Power?" *Asian Survey*, vol. 50, no. 6, 2007, pp. 1162–1183.

29 Scott, D. India's "Extended Neighborhood" Concept: Power Projection for a Rising Power, *India Review*, vol. 8, no. 2, 2009, pp.107-143.

30 אימונים משותפים עם מדינות המפרץ הפרסי נערכו בשנים 2002, 2004, 2007, ו־2011. Scott, D. India's drive for a 'blue water' navy. *Journal of Military and Strategic Studies*, vol. 10, no. 2, 2007.

31 http://www.bharat-rakshak.com/NAVY/Galleries/News/Sukoon/

32 http://en.wikipedia.org/wiki/Operation_Madad_%28Indian_Navy%29

33 Walter c. Ladwig, 2010, pp. 1162–1183.

34 לסקירה מקיפה, ראו: P. R. Kumaraswamy, *India's Israel Policy*, Columbia University Press, 2010.

35 ראו: **שנתון סטטיסטי ספנות ונמלים 2011** /http://spa.mot.gov.il/images/PDF/SHNATON/StatisticalYearBook11.pdf

36 ביקורים אחרונים של ספינות קרב הודיות בישראל התקיימו ביוני 2006 וביולי 2012 : http://www.haaretz.co.il/misc/1.1116116 http://news.walla.co.il/?w=/551/2554984

37 לסקירה קצרה לגבי היחסים בין הציים, ראו: http://www.gloria-center.org/2011/12/indo-israeli-defense-cooperation-in-the-twenty-first-century/

38 MDA- Maritime Domain Awareness. מושג זה עוסק בהבנה כוללת של כל נושא הקשור במרחב הימי. בכלל זה, הקשר בין המרחב הימי לנושאים ביטחוניים, כלכליים ודיפלומטיים. בעברית ניתן להגדיר מושג זה כ"ערנות ימית".

39 חשוב להדגיש כי ניתן לראות כיום מעורבות גוברת של גופים רבים, נוסף על משרד הביטחון, ביחסים עם הודו.

פשע קיברנטי – סכנה לביטחון הלאומי?

ליאור טבנסקי

מבוא

המרחב הקיברנטי, שנוצר עם התפתחות טכנולוגיות המחשבים והתקשורת הדיגיטלית, נכנס בעשורים האחרונים לחיינו. התקשוב מיושם לשיפור ולייעול תהליכי העבודה, הלמידה והבידור, והוא משפיע על דפוסי הפעולה כמעט בכל תחומי הפעילות האנושית. רשת האינטרנט נעשתה מסחרית ב־1988 והפכה לנדבך משמעותי במרחב הקיברנטי. היא מאפשרת נגישות זולה ומיידית לסוגים שונים של מידע, לשיתוף ידע, לעבודה משותפת מרחוק ועוד.

השלכות הפשע הקיברנטי על הביטחון הלאומי נגזרות מאופי השימוש בטכנולוגיה על ידי גורמים בעלי מניעים עוינים. המאמר מציע בחינה מוכוונת־מדיניות של משמעויות הפשע הקיברנטי והשפעתו על הביטחון הלאומי, מבלי להתבסס על הערכות כספיות של היקף הנזקים של הפשע הקיברנטי. המאמר מתאר את שיתוף הפעולה בין עבריינים, 'הפשע המאורגן' וארגונים עוינים, ודן במסחור של יכולות התקיפה הקיברנטיות, המתאפשר עם התפתחות הטכנולוגיה וצמיחת "השוק השחור" לשירותי מחשוב. יש הטוענים שהפשע הקיברנטי אינו מהווה כיום איום על הביטחון הלאומי, אולם, המאמר מזהה שני תנאים נפרדים שאם יתמלאו, הפשע קיברנטי עלול להפוך לאיום על הביטחון הלאומי.

הדרישה הציבורית לביטחון במרחב הקיברנטי עולה עם עליית המודעות לאיומים. גם ללא עלייה אובייקטיבית בהיקף הפשיעה, אין להניח שדרישה זו תצטמצם. אחריות המדינה לאזרחיה אינה נעצרת במרחב הקיברנטי, וגם בתחום זה יש להגדיר את ביטויה המעשי במסגרת תהליך פוליטי דמוקרטי, על יסוד עובדתי מוצק.

ליאור טבנסקי הוא דוקטורנט למדעי המדינה באוניברסיטת תל אביב. ליאור היה מלגאי בתכנית ניובאוור לתלמידי מחקר בשנים 2010–2012 במכון למחקרי ביטחון לאומי, אוניברסיטת תל־אביב.

תופעת הפשע הקיברנטי

טכנולוגיות ממוחשבות מיושמות למטרות שינוי וייעול תהליכי הייצור והעבודה בכל תחומי החיים, והן לא פסחו על עולם הפשע. המחשוב מאפשר פירוק משימות ליחידות קטנות וביזור העיבוד; הרישות מאפשר גישה גלובלית למידע, והתמקדות בידע כמוצר בעל־ערך. ההגדרה המוצעת לפשע הקיברנטי היא:

שימוש במרחב הקיברנטי למטרות אסורות, תוך ניצול התכונות המיוחדות המאפיינות את המרחב הקיברנטי הקיים, כגון: מהירות ומיידיות, הפעלה מרחוק, הצפנה והסוואה שתורמות לקושי בזיהוי הפעולה והמפעיל, ניצול הערך העולה של המידע הדיגיטלי לסוגיו וטיפול חוקי ומשפטי משתנה במרחב הקיברנטי במדינות שונות.

הדיון בהגדרות של תופעת הפשע הקיברנטי ממשיך להתפתח. לפני למעלה מעשור תהה גרבוסקי, מה חדש בפשע הקיברנטי: האין אלה תופעות ותיקות שעושות שימוש בכלים חדשים?[1] אולם רוב החוקרים מנסים לנתח את הפשע הקיברנטי כתופעה ייחודית. מאג'יד יאר מסווג את תופעות הפשע לפי האובייקט הנפגע: נגד רכוש, אדם, מדינה.[2] שינדר וקרוס מבחינים בין העבירות לפי מידת האלימות: פשע אלים ואלים פוטנציאלי, בלתי־אלים (סחר בסמים, הלבנת הון) ופשע שעדיין נתפס "צווארון לבן" (פריצה למחשבים, גניבה והונאה).[3] לפי ההגדרה של וול – "the transformation of criminal or harmful behavior by networked technology"[4] – הפשע הקיברנטי התפתח בעקבות צמיחת התקשוב והמרחב הקיברנטי והאפשרויות החדשות להשגת מידע, לשיבושו או ליצירת מניפולציה של מידע למטרות רווח. נוסף לכך ממיין וול את עבירות הפשע הקיברנטי לשלושה טיפוסים: עבירות הנוגעות לשלמות ולתקינות מערכת המחשב (Hacking – פריצה למערכות), עבירות שמסתייעות במרחב הקיברנטי (תקשורת מוצפנת בין עבריינים, מכירת תרופות מזויפות) ועבירות הנוגעות לתוכן המידע הממוחשב (גניבת סודות, הפצת תוכן פוגעני). ניתן גם למיין את העבירות לפי תפקידו של המחשב.[5] גם "האמנה האירופית נגד הפשע הקיברנטי" מאמצת גישה דומה.[6]

המחשב כאמצעי לביצוע עבירה		
גישה לתוכן והפצתו: סודות ידע תוכן פוגעני	שיבוש המידע או המערכת בכוונת זדון גניבת זהות הונאה	שימוש בתקשורת הטרדה סחר בחומר אסור דוא"ל זבל

המחשב כמטרה של העבירה			
גישה לא מורשית:	החדרת קוד זדוני:	שיבוש של פעילות:	גניבה של שירות:
Hacking (פצחנות)	נוזקות, רוגלות, וירוסים	DDoS (מניעת שירות מבוזת)	שימוש בלתי־ מורשה

חלק ניכר מהפשיעה הקיברנטית אינו מהווה תופעה ייחודית או חדשנית: הטרדה, הונאה, תעמולה אסורה, פורנוגרפיה, גניבה, הלבנת הון, ריגול ועוד. בעבירות הללו נעשה שימוש במרחב הקיברנטי. הנדבך הנוסף הוא תופעות שכמעט לא היו בנות־ביצוע לולא המרחב הקיברנטי: דוא"ל זבל, הונאת קליקים (Click fraud), תוכנות זדוניות (Malware) לסוגיהן, רשתות מחשבים שבויים (Botnet),[7] גניבת זהות דיגיטלית, הסוואה והצפנה[8] של מידע ותקשורת, חדירה ממחושבת למתקנים ממוגנים בעלי ערך רב וריגול אוטומטי מתמשך בארגונים מאובטחים, המוציא קניין אינטלקטואלי משליטתם.

פשיעה על כל סוגיה היא תופעה חברתית נפוצה. הסברים קרימינולוגיים לתופעה משלבים הנעה, הזדמנות, וקיומו של "שומר". ניתן לזהות שני סוגי מקורות להנעה האנושית לפעולה.[9] חלק ניכר מהמניעים להתנהגות עבריינית הנם אישיותיים־פנימיים (Intrinsic Motivation), והם אינם נקבעים בתהליך בחינה של שיקולי עלות־תועלת. אין סיבה להניח שבעקבות שימוש מוגבר בטכנולוגיה זו או אחרת, תשתנה ההתנהגות האנושית. לפיכך, אין זה מפתיע שבני־האדם משתמשים גם במרחב הקיברנטי למילוי צורכיהם ולרדיפה אחר מטרותיהם, הן באפיקים הנורמטיביים כגון לימודים, בידור, השכלה ועבודה, והן בפעולות האנושיות הוותיקות, כגון לחימה ופשע. האסכולה הקלאסית בקרימינולוגיה מתבססת על רעיון הבחירה החופשית והערכה מושכלת של תועלת צפויה בהתחשב בסיכוי להיענש, ומפרשת את ההנעה לביצוע עבירה כהחלטה כלכלית־מושכלת.[10] כלכלנים ופסיכולוגים עוסקים בניתוח ההתנהגות האנושית, כולל העבריינות, כנגזרת של שיקול עלות־תועלת מושכל. מכלול הנסיבות החיצוניות המשתנה יכול לעודד פשיעה קיברנטית: הדבר קורה כשאדם מזהה פוטנציאל גדל לרווח ומעריך שהמחיר – הסיכוי לענישה – נמוך מהתועלת הצפויה. הרחבת החיבוריות הדיגיטלית לצד עליית ערך המידע הממוחשב גורמות למצב שבו עולה ההנעה החיצונית (Extrinsic Motivation) להתנהגות עבריינית. בעוד מנגנוני אכיפת חוק מסודרים קיימים במדינות המפותחות, במרחב הקיברנטי החדש לא הדביקה תגובת המדינה את קצב השינוי הטכנולוגי. דוגמה טובה היא שוד בנק "מסורתי" לעומת גניבה ממוחשבת. האפשרות "המסורתית" לשוד כספים מסניף בנק כרוכה בהתגברות על מערכי האבטחה, ובסיכוי סביר להיקלע לעימות עם שומרים חמושים. גם אם השוד עצמו יסתיים בהצלחה, לאורך השנים נרדפים השודדים על ידי רשויות החוק. עם התפתחות המרחב הקיברנטי התאפשר ניצול של פגיעותו גם לגניבה מבנקים. למשל, נפוץ השימוש ברשתות בנות אלפי מחשבים שבויים (Botnet)[11] לגניבה מתמשכת של פרטי הזדהות לאתרי בנקאות, ושימוש בהם לגניבת סכומי כסף קטנים. לנוכח בעיית וידוא הזהות (Attribution) במרחב הקיברנטי, הסיכוי לזיהוי הפושע נמוך מאוד.[12] המוסדות הפיננסיים מודעים לסיכון העסקי הברור,

ויחד עם מוסדות ההסדרה נוקטים אמצעי הגנה ומשקיעים בתחום אבטחת המידע, כדי לצמצם את מרחב ההזדמנויות לשודד הקיברנטי. עם זאת, הסיכון הפיזי המיידי מבחינת הגנב הקיברנטי עדיין נמוך מזה של שודד "מסורתי".

היקף הפשע הקיברנטי ונזקיו: הערכות בעייתיות

תופעת הפשע הקיברנטי נבחנת בדרך כלל בפרספקטיבות משפטיות (חקיקה וענישה), קרימינולוגיות (מניעים וארגון), כלכליות (תמריצים וערך) או טכניות (אבטחת מידע). משפטנים עוסקים בהצבת גבולות להתנהגות מקובלת ובסוגיות חוקיות של מניעה ואכיפה. קרימינולוגים מיישמים את הידע המקצועי להבנת התופעות החדשות. כלכלנים מתארים את מערכת התמריצים המשפיעים על תהליכי קבלת ההחלטות של שחקנים רציונליים. אנשי אבטחת מידע עוסקים בסוגיות טכניות של התשתית הטכנולוגית: תוכנה, חומרה ותקשורת, תוך התמקדות בפגיעויות השונות ובדרכי ההתגוננות. משפטנים, כלכלנים ואנשי אבטחת מידע שותפים לדעה שהיקף הפשיעה הקיברנטית ועוצמת הנזק שלה נמצאים בעלייה מהירה ומתמשכת. ההערכה נסמכת על העובדה שהיקף המידע הדיגיטלי גדל בקצב מעריכי, והחיבוריות של התקנים ממוחשבים מתרחבת אף היא. המרחב הקיברנטי מכיל מידע רב יותר, עם נקודות גישה פוטנציאליות רבות יותר לחדירה בלתי־מורשית. המסקנה היא שכל חדירה (Breach) חושפת היקף הולך וגדל של מידע.

הערכות כספיות של היקף הנזק של הפשע הקיברנטי מתפרסמות מאז שנות התשעים ועד היום. חברות האבטחה מובילות את המחקר בנושא, ומפרסמות דוחות למכביר. קיימות עשרות הערכות שונות, שמקורן במגזר העסקי והממשלתי בארצות־הברית, בבריטניה, ובמדינות מפותחות נוספות.[13] סקר של הבולשת הפדרלית (FBI) העריך את הנזק לעסקים אמריקאיים ב־65 מיליארד דולר בשנת 2005.[14] שר המסחר האמריקאי, גארי לוק, טען שהנזק השנתי לחברות אמריקאיות כתוצאה מזיוף ופיראטיות (שימוש בלתי־חוקי בקוד מחשב) עומד על 200–250 מיליארד דולר.[15]

דו"ח בריטי מציג תג מחיר של 27 מיליארד ליש"ט לשנה: הנזק השנתי לאזרחי בריטניה הוערך ב־3.1 מיליארד ליש"ט, למגזר העסקי 21 מיליארד ליש"ט ולממשלת בריטניה – 2.2 מיליארד ליש"ט נוספים.[16] בדו"ח של חברת סימנטק, מהמובילות בשוק אבטחת המידע, נאמד הנזק הכספי הישיר שגורם הפשע הקיברנטי ב־114 מיליארד דולר בשנה ב־24 מדינות.[17] הערכות נוספות נוקבות בסדר גודל של מאות מיליארדי דולרים בשנה.[18]

סכומי עתק אלה עוררו תהיות וספקנות, אולם השפעת הביקורת עד כה הייתה מוגבלת. לאחרונה פורסם נייר עמדה מאת שני חוקרים מחברת מיקרוסופט,

שמנתח את התשתית הסטטיסטית הרעועה שביסוד הערכות הנזק של הפשע הקיברנטי, הנעשות באמצעות סקרים.[19] כיצד נוצרו ההערכות הללו? בחינה של שיטות המחקר מגלה באיזו קלות נוצרת הערכת־יתר של היקף הנזק. ראשית, חסר מידע על השימוש שנעשה (או לא נעשה) במידע שנחשף. ספורים המקרים שבהם קיים מידע מוצק, בעוד היקף הנזק הפוטנציאלי הוא רחב. נניח שנפרץ מחשב שבו קובץ מאגר מידע המכיל אלף רשומות. נניח גם שמאגר המידע אינו מוצפן, והרשומות שבו כתובות בשפה טבעית. כל רשומה בקובץ מייצגת כרטיס אשראי תקף, על כל הפרטים הדרושים לשימוש בו: מספר, מספר CVV,[20] תוקף, שם, מס׳ תעודת זהות וכתובת הבעלים, וכן פרטי חשבון הבנק המנפיק. במצב זה הגנב רואה תמונה מלאה ואמיתית של המידע בקובץ, אולם גם במצב האופטימלי, הגנב אינו יכול להעריך את מלוא המשמעויות הכלכליות של המידע שהשיג. האם הפורץ יכול להעריך נכונה את הערך האמיתי של המידע שגנב? האם הקורבן, הנפרץ, יכול להעריכו כראוי? בגניבת קניין אינטלקטואלי – תוצר של מחקר ופיתוח, הקורבן נוטה לזהות כנזק של גניבת המידע את הרווח המרבי שהיה רוצה לקבל בתום תהליך הפיתוח, הייצור והשיווק. השימוש בסקר – שיטה המתאימה לבירור תופעה שקשה לצפות עליה וכן לגילוי היסטוריה של הנסקרים – הוא הדרך העיקרית ללמוד על היקף הנזק. הסקר מאפשר להגיע למספר גדול ומגוון יותר של משיבים המספקים הערכות משלהם לכמות האירועים והנזק, אך לשיטת הסקר יש גם מגרעות משמעותיות, המעסיקות אנשים מתחום מדעי החברה וסטטיסטיקאים.[21]

שנית, בהעדר מידע מספיק, משתמשים בשיטות סטטיסטיות כדי להגיע להערכה על בסיס פרטי מידע ספורים. בעיות המדידה קיימות בכל תחומי הדיון באיומים הקיברנטיים, והן בולטות במיוחד כשמנסים לסייע לדיון על ידי כימות הנזק בערכים כספיים. קיים קושי מהותי בהערכת הנזק, ועד כה נראה כי ההערכות הכספיות – שנוצרות בהפעלה גסה של שיטות הסטטיסטיות כדי להציג השערה על סמך נתונים מעטים – מובילות להערכות־יתר. נוסף לסוגיות של מהימנות שיטות המחקר, אמינות מקורות המידע והתאמת השיטה הסטטיסטית למחקר, קיימת בעיה נוספת. ההערכות הכספיות כוללות לרוב גם מרכיבים עקיפים של נזק. הערכות כספיות כוללות פגיעה במוניטין של הארגון שסבל מפריצה, השפעות שליליות על התנהגות הצרכנים עם השלכות מאקרו־כלכליות, סוגיות של דיני נזיקין, ביטוח, הוצאות נלוות ועוד.

שאלות מרכזיות בהבנת התופעה נותרו ללא מענה ברור: האם כדאי להעריך את הנזק על פי השימוש שבוצע בפועל במידע, במקום על פי הפוטנציאל המרבי? אולי צריך להתייחס לערך הכספי של יצירת המידע, במקום להערכת מחירו בשוק – כעת או בעתיד? ומה בדבר העלויות הנדרשות לאבטחה וחזרה לתפקוד תקין? תמונת המצב שעולה מתוך המקורות המקובלים אינה מהימנה, והנזק של הערכת־היתר

עלול להתבטא ביצירת תגובת־נגד: זלזול בכוחו של הפשע הקיברנטי. ביסוס הדיון בפשע הקיברנטי על הערכות הנזק הכספיות פוגע בדיון מושכל בבעיה, וביכולת לעצב מדיניות ציבורית הולמת.

שיתוף פעולה בין עבריינים לבין גורמים עוינים

הממשק בין עבריינים "מקצועיים" והפשע המאורגן לבין ארגוני טרור אינו חדש. גם אם נתבונן רק במציאות החיים הישראלית, נזהה ששיתוף הפעולה מהסוג האמור גורם נזקים ברמה הלאומית. מאז שנת 1996 התנהל המאבק התקשורתי ברכישת "דיסקים צרובים" תוך טענה שהרווח מופנה למימון טרור פלסטיני,[22] כחלק מקשר אמיץ בין שירותי הלבנת הון לבין צרכנים כמו ארגוני הטרור.[23] תופעה ענֶפה של גניבת מכוניות מישראל לשטחי יהודה ושומרון ליוותה את "החוויה הישראלית" לאורך שנים ארוכות. הבעיה כמעט לא טופלה ברמה הלאומית, שכן האיום לא נתפס כבעיה ביטחונית: הנזק כוסה בידי חברות הביטוח וגולגל בהדרגה אל המבוטחים, המשטרה לא פעלה מחוץ לגבולות הריבונות הישראלית והצבא – שהפעיל מחסומים ביטחוניים קבועים על צירי תנועה ראשיים – בחר להימנע מעיסוק בפושעים ה"פליליים". בתקופת "אינתיפאדת המתאבדים" חל שינוי בדרכי הפעולה של אותם פושעים פליליים: ארגוני הטרור גייסו את מומחיותם של גנבי הרכב הפלסטיניים כדי להשתמש במכוניות עם לוחיות ישראליות לתעבורה, וגם כדי למצוא נתיבים לחדירת מעגלי האבטחה ולהובלת אמצעי לחימה ומחבלים מתאבדים ללב הערים.

אפשרויות המעבר בין רצועת עזה לישראל מוגבלות יותר מאשר ביהודה ושומרון. חפירת מנהרות לכיוון רפיח המצרית נועדה לספק נתיבי הברחה לצרכים שונים. עסקי ההברחה יוצרים רווח כספי גדול לחופרי המנהרות ולמפעיליהן, והתעשייה מתקיימת למרות מאמצי הסיכול הישראליים. המנהרות הפכו לבעיית ביטחון לאומי עקב הברחת אמצעי לחימה וחומרים שונים מחצי־האי סיני לרצועת עזה, והברחת מחבלים מהרצועה לסיני.[24] המומחיות של ארגוני הפשע בחפירת מנהרות אפשרה את המתקפה ליד כרם־שלום ב־25 ביוני 2006, שבה נהרגו שני חיילים וחייל נוסף נחטף לשבי חמאס. במקרה זה, המומחיות הטכנית של חופרי המנהרות נוצלה בבירור לפגיעה בביטחון הלאומי של ישראל.

חלק מהבדואים בסיני מתפרנסים ממומחיותם כנווטים בשטח, ומספקים לאורך עשרות שנים "שירותי הברחה" לתוך מדינת ישראל. "הסחורה" המובּרחת כללה בעבר הלא־רחוק מאות נשים עבור תעשיית המין וסמים. בשנים האחרונות מובּרחים אלפי אפריקאים לגבול ישראל. יש הטוענים שאלה מהווים אתגרים משמעותיים, אבל לא בעיה אמיתית לביטחון הלאומי. אולם, הערכה זו משתנה ככל שהמומחיות של המבריחים משמשת לביצוע מתקפות טרור על ישראל.[25]

הברחת מחבלים מעזה דרך סיני לישראל אפשרה את פיגוע הטרור בכביש 12 ב־18 באוגוסט 2011, שם נרצחו שמונה ונפצעו ארבעים ישראלים. הברחת המחבלים ואמצעי הלחימה הכניסה את העיר אילת לטווח של ירי רקטות.[26] ההברחות הללו מסַכנות בצורה ברורה ומיידית את הביטחון הלאומי.

בחינה מחודשת של משמעות הפשע הקיברנטי

אם נתבונן עתה בפשע הקיברנטי, נגלה שגם כאן קיים שיתוף פעולה מסחרי דומה. בשנים האחרונות התפתח "שוק שחור" של מומחים טכניים ו"רועֵי" רשתות מחשבים שבויים, המפתח ומספק כלים ושירותים טכניים בתשלום.[27] השוק השחור של שירותי הסייבר Crimeware as a Service (CaaS) גורם נזקים כלכליים במדינות המפותחות, אף שהערכות הנזק הכספיות הנפוצות מוּטות מאוד כלפי מעלה.

מי שמעדיף לפעול בכוחות עצמו ואין בידיו משאבי מחקר ופיתוח מגלה שכלי נשק קיברנטיים (חבילות תוכנה זדוניות – toolkits)[28] זמינים לכול בהורדה מהאינטרנט, לרוב בתשלום של עשרות עד אלפי דולרים. הידע הוא מוצר בלתי־נדלה; כך, שיתוף האחר ביכולות שהיו זמינות לך אינו פוגע בעוצמתך.[29] על רקע זה נוצר המצב שבו כלים עוצמתיים זמינים לכל דורש בעלות שולית. הרושם הנפוץ – שהמרחב הקיברנטי מקל גריפת רווח מפעילות עבריינית – לא נעלם מארגוני הפשע.[30]

צמיחת כוח המחשוב ופריסת רשת האינטרנט אפשרו אמצעי חדש לביצוע פשיעה קיברנטית רחבת־היקף: רשתות של מחשבים שבויים ־Botnet . זהו מקבץ של מחשבים אישיים המחוברים לרשת, שהושתלה בהם תוכנה זדונית המאפשרת שליטה מרחוק ביכולות המחשבים הללו, וזאת מבלי לגרום לשיבוש פעולתם התקין. "הדבקת" המחשבים המחוברים לאינטרנט נעשית באמצעות ניצול פרצות ידועות – שהמשתמשים ומנהלי המערכות לא טיפלו בהם – להחדרת תוכנה זדונית. עקב ההיצע הגבוה, מחיר השימוש ב־Botnet נגיש כמעט לכול: חברת **מק'אפי** העריכה ב־2007 שכ־5% מהמחשבים האישיים המחוברים לרשת בעולם הם מחשבים שבויים.[31]

אחת התופעות החדשות היא Advanced Persistent Threat (APT), או Adaptive Persistent Attack (APA)[32] – שימוש מורכב ורב־שלבי בכלי נשק קיברנטיים לביצוע משימות מתמשכות וסמויות. התוקף אינו פועל בהיקף רחב כדי לנצל פגיעויות מוכרות, אולם היעד מוגדר היטב. התוקף משתמש במגוון של כלים התפורים למשימה, חלקם ייחודיים. תקיפה כזו מורכבת משלבים רבים, ויכולה להימשך לאורך חודשים ושנים. התוקף מתחיל באיסוף מודיעין על המבנה הארגוני של המטרה, וזיהוי בעלי־תפקידים בכירים שיש להם הרשאות גישה למרב המידע בארגון. איסוף המידע האישי נעשה תוך שימוש בפרטים

גלויים ושיתוף המידע הפרטי ברשתות החברתיות. לאחר זיהוי אנשי המפתח, נעשה מהלך ממוקד כדי להדביק אותם. אחת השיטות היא SpearPhishing: החדרת 'סוס טרויאני' באמצעות הודעת דוא"ל ממוקדת, משולֵח מהימן ועם תוכן רלוונטי, שחודרת את מנגנוני הסינון על ידי שימוש במידע האישי שנאסף. פתיחת ההודעה מאפשרת החדרת 'סוס טרויאני': נוֹזקה לגישה מרחוק Remote Access Tool (RAT) למשאבי המחשוב בארגון, על ידי יצירת תקשורת ממחשב מורשה ברשת הפנימית. עם השגת הגישה, הפושע הממוצע פועל במהירות כדי להשיג מידע בעל־ערך ולממש אותו. לא כך בהתקפת APA, כשהמטרה היא גישה סמויה לאורך זמן, תוך התעלמות מפיתויים כספיים מיידים. ההתקפה נמשכת לאורך זמן רב, בין היתר, כדי להתגבר על מערכות למניעת דלף המידע. במהלך ההתקפה נעשות בדיקות לזיהוי סף התגובה של המערכת, ובמידת הצורך המידע הנגנב נחלק למנות קטנות, מוסווה בתוך תקשורת לגיטימית ועובר מבלי לגרות את מערכות ההגנה. ההתקפה הממוקדת נדירה יותר ממתקפות סטטיסטיות, שכן היא יקרה באופן ניכר: APA מצריכה איסוף מודיעין שיטתי, יכולת תכנון וניסוי ואורך־רוח לביצוע המשימה הממושכת.

בפרספקטיבה כלכלית נוצר מצב שמצד ההיצע, קבוצות ההאקרים (פצחנים) שהצליחו לפתח וליישם כלי תוכנה לשליטה במאות אלפי מחשבים יצרו, למעשה, שירות בעל ערך כלכלי. מצד הדרישה, לקוחות שונים – האקרים אחרים, חוקרים פרטיים, עבריינים, ארגוני ריגול וארגוני פשע גדולים – מצאו שימושים שונים למוצר זה. כך נוצר מודל עסקי Crimeware as a Service (CaaS) – העתק "שחור" של מודל Software as a Service (SaaS), המנחה את תעשיית שירותי המחשוב מאז 2001.[33] ההצדקה הכלכלית של המודל ברורה: מעתה, הלקוח אינו נדרש לרכוש ציוד מחשב כדי להשתמש בשירותי מחשב. הלקוח יכול לרכוש רק את השירות המדויק שהוא זקוק לו ממפעילים גדולים, ולהשתמש בו על גבי הרשת, בתקשורת סטנדרטית. המודל עבר גלגולים אחדים במשך השנים, וכיום הוא מוכר בזִמלוּל (Buzzword) 'מחשוב ענן' (Cloud Computing). היקף השוק העולמי לשירותי המחשוב באופן זה מוערך ב 14.5 מיליארד דולר בשנת 2012.[34]

הבה נבחן את תופעת "השוק השחור" מנקודת המבט של ביטחון לאומי. קיומו של "שוק שחור" למכירת אמצעי לחימה קיברנטיים, שירותי פיתוח ומיקור־חוץ גורם לכך שרמת המיומנות הטכנית הנדרשת לכניסה לתחום הפשע הקיברנטי יורדת, שכן הפושע אינו נדרש להחזיק ביכולת לפתח בעצמו את כלי הפריצה ואת שיטות הפעולה. אותה תשתית טכנולוגית דרושה לחדירה ולשימוש בלתי־מורשים במשאבי מחשב, הן אם החדירה נועדה לרווח כספי והן לחבלה.[35] כך מתגלה סיכון נוסף: השימוש בכלים הקיימים למטרות חבלה ופגיעה בתשתיות חיוניות – במקום למטרות הצפויות של הונאה לצורך גניבה ויצירת רווח כספי

מהיר – עלול לגרום נזק ביטחוני לאומי. המשך התפתחותם של מנגנוני הפשע הקיברנטי הופך, אפוא, לבעיית ביטחון לאומי. ההגנה על תשתיות חיוניות (CIP) היא הסוגיה החשובה ביותר בתחום הביטחון הקיברנטי, והשוק השחור של אמצעי לחימה קיברנטיים מחריף אותה. המסחור של יכולות טכניות ומבצעיות מאפשר לגורמים רבים – ובהם ארגוני טרור קטנים ואף יחידים – גישה למשאבים עוצמתיים, שעלולים לשמש ככלי נשק קיברנטיים. קבוצת איומי הייחוס מתרחבת, אפוא, מעבר למדינות ולארגוני הטרור המוכרים, וצריכה לכלול כל גורם שיכול להשתמש בשירותים המסחריים שמציעים ארגוני הפשע הקיברנטי. עם זאת, כשקיימת השקעה מדינתית מתמשכת במחקר ופיתוח, היכולות הטכנולוגיות הרווחות בשוק מפגרות בהכרח אחר הטכנולוגיה שמפתחים בזרועות הביטחון ובאקדמיה. לפיכך, היכולות הזמינות בשוק יהיו פחותות מאלה הזמינות לארגונים מדינתיים בעלי אמצעים של מחקר ופיתוח עצמאיים, שנהנים מגיבוי מדינתי מבחינת משאבים וארגון.

לקראת מימוש אחריות המדינה לביטחון קיברנטי

חוקרים ומעצבי מדיניות זקוקים לביאור המשמעויות של התופעה. ההערכות הכספיות של נזקי הפשע אינן מספקות בסיס מוצק להבנת התופעה ולעיצוב מדיניות. לפיכך נדרשת בחינה של סדרי העדיפויות המיטביים, לנוכח תמונת המציאות ומגוון האילוצים והמגבלות.

גם ללא הסכמה על הערכת הנזק הישיר והעקיף שגורם הפשע הקיברנטי, הוא עדיין משפיע על תפקודם של אזרחים, ארגונים והחברה בכלל. אזרחים ועסקים קטנים נפגעים באופנים שונים מפשע קיברנטי. דוא"ל זבל, הונאות אינטרנטיות, גניבת זהות דיגיטלית, פגיעה בפרטיות, סחיטה, ריגול כלכלי ופגיעה בקניין רוחני ואינטלקטואלי – כולן תופעות נפוצות, שפוגעות מדי פעם בחלק מהאזרחים והארגונים. אף שנראה כי הערכות הנזק מוּטות כלפי מעלה, התפתחות המרחב הקיברנטי מגדילה את היקף הנפגעים הפוטנציאליים, ומרחיבה עוד יותר את מגוון הדרכים שבהן ניתן לבצע פשעים ועבירות נגד אזרחים וארגונים. לאור המודעות העולה בד־בבד עם התרחבות מעשי הפשע, יש להניח שהאזרחים במדינות המפותחות ידרשו שהמדינה תנקוט פעולות על מנת לספק ביטחון אישי וקבוצתי גם במרחב הקיברנטי. החשיפה התקשורתית הגוברת של אירועי אבטחת מידע ומתקפות קיברנטיות מצביעה על עניין גובר בסכנות הפשע הקיברנטי. סביר לצפות להופעת דרישה ראשונית של אזרחים שהמדינה, על זרועותיה, תפעל לספק ביטחון לאומי ואישי גם במרחב הקיברנטי.

המדינה אחראית על החוק והסדר ועל ביטחון אזרחיה, והיא נדרשת לפעול למזעור הנזק לאזרחיה. המדיניות תתפתח מתוך הבנת המשמעויות הרחבות של התופעה, ומתוך דיון ציבורי מושכל. להלן סוגיות אחדות לפיתוח דיון כזה:

רוב התופעות הנפוצות שנכללות בפשע קיברנטי אינן נוגעות לענייני ביטחון לאומי. מה המשמעות של הפצת שנאה ועידוד הסתה נגד היהודים או מדינת ישראל, תוך השחתת אתרי אינטרנט ישראליים, הפצת תעמולה תוך שימוש בשיטות דוא"ל זבל וחדירה לחשבונות פרטיים ברשתות החברתיות, יצירת סרטונים וקמפיינים ברשת, הפוגעים ברגשות הציבור? האזרחים עלולים לחוש בלתי־מוגנים במרחב הקיברנטי, וכבודם של המדינה ושל רבים מאזרחיה עלול להיפגע כתוצאה מעלילות שווא. ברמה הלאומית, מעבר לתחום המקצועי של יחסי־ציבור, זהו נזק זניח.

מה המשמעות של הונאה נפוצה – גניבת זהות דיגיטלית, ושימוש בלתי־מורשה בפרטים של אמצעי התשלום לגניבת כספי האזרח? כאשר אזרח נופל קורבן לפשע, רשויות המדינה נדרשות וחייבות להתייחס ולטפל בנושא. לרשות המדינה עומד מגוון רחב של דרכי טיפול מערכתיות ופרטניות, ויש לבאר את משמעות האירועים על מנת לבחור מדיניות הולמת. אולם מבחינת הביטחון הלאומי, קשה לראות נזק ברמה הלאומית – כל עוד מדובר בשיעורי פגיעה נמוכים יחסית, גם כשאלה גבוהים משיעור התפוצה של פשע "מסורתי". אם פעילות הפשיעה הקיברנטית תתגבר ותהיה ממושכת ובהיקף רחב, עצם אמונם של האזרחים במוסדות המדינה צפוי להיפגע בשל חוסר יכולתם לספק סביבה בטוחה.

המצב הנוכחי במדינות המפותחות אינו משביע רצון. אם "ציות תמורת הגנה" הוא תמצית החוזה החברתי בין האזרחים למדינה, היא אינה ממלאת את חלקה בחוזה בתחום הפשע הקיברנטי. המענה לאתגרים החדשים מצריך, קודם כול, הבנה ברורה של התופעות ומשמעותן. תהליכי התגובה, יצירת המדיניות ואכיפתה מחייבים עדכוני תקינה וחקיקה. פעולות החקיקה, שמדרך הטבע מפגרות אחר ההתפתחות הטכנולוגית, נמצאות בסמכותה הבלעדית של המדינה. זרועות האכיפה הריבוניות הפועלות בהתאם לתשתית החוקית הלאומית יידרשו להקצות יותר משאבים למניעה, לחקירה ולענישה בתחום הפשע הקיברנטי. על אף אופיו הבינלאומי של המרחב הקיברנטי, המדינה היא הגורם הבלעדי שנושא באחריות לביטחונם האישי של אזרחיה. הסכמים בינלאומיים כגון "אמנת בודפשט – אמנה על פשעי מחשב" של מועצת אירופה[36] והיוזמות המתנהלות באו"ם,[37] בארגון הכלכלות המפותחות[38] ובאיגוד הטלקום העולמי (ITU[39]) – כל אלה מגבירים את שיתוף הפעולה בין רשויות ריבוניות. שיתוף פעולה בינלאומי עשוי לסייע לרשויות ריבוניות להילחם טוב יותר בתופעה, אך לא ניתן לראות בהסכמים בינלאומיים תחליף למדיניות ריבונית עצמאית. ראשית, שיתוף פעולה בין מדינות במערכת

הבינלאומית האנרכית אפשרי במידה מוגבלת בלבד, ועל סמך אינטרס משותף. ייתכן שהמדינות הדמוקרטיות המפותחות יצליחו לגבש הסדרים בינן לבין עצמן, אולם הפער בהגדרת האיום ביניהן לבין המדינות הסמכותניות (אוטוריטריות) נראה רחב מדי. הדיון האמריקאי בנושא מתמקד בריגול התעשייתי המתמשך נגד הקניין האינטלקטואלי, פרי המחקר והפיתוח של המגזר העסקי והממשלתי בארצות־הברית. לאורך שנים, גובר החשש של גורמים בכירים בקהילה העסקית והממשלתית מפני אובדן היתרון הכלכלי והאסטרטגי של ארצות־הברית בעולם כמעצמה מדעית־טכנולוגית חדשנית מובילה. למעשה, 'אובדן' אינו המונח הנכון, שכן הידע אינו הולך לאיבוד אלא נגנב במאמץ מדיני שיטתי, מאורגן ורחב־היקף של סין להזניק את עוצמתה הכלכלית והצבאית באמצעות העתקת סודות המחקר האמריקאי.[40] הדיון בנושא זה עובר בבירור מתחומי הכלכלה, אבטחת המידע או המשפטים לשיח ביטחוני, כמעט לוחמני.[41] סין, מצדה, דוחה האשמות אלו על הסף, ומודאגת מערעור יסודות המשטר הסיני כתוצאה מהשימוש המערבי באינטרנט, בשם ערכי חופש הביטוי.

שנית, הסמכות והריבונות של המדינה בשטחה מאפשרת לקדם מדיניות עצמאית: חקיקת חוקים ואכיפתם אינה תלויה בהסדר בינלאומי. בישראל, האירוע המכונה "פרשת ההאקר הסעודי" מדגים את חריגת הדיון מגבולות אבטחת המידע אל הרמה הביטחונית. בתחילת 2012 פרסם מי שהזדהה כ־0xOmar רשימת פרטים אישיים ומספרי כרטיס אשראי של אלפי אזרחים ישראלים.[42] הפרטים שפורסמו היו ברובם המכריע ישנים, ומתוך כ־380 אלף הרשומות, היו כמה אלפים של מספרי אשראי תקפים. הנזק הישיר שנגרם לבעלי הכרטיסים עומד על אפס: חברות האשראי ביטלו את הכרטיסים והנפיקו חדשים, וממילא, כל שימוש בלתי־מורשה בכרטיס מכוסה בידי החברות. היקף הנתונים שנחשפו גם הוא אינו חריג: מדי יום נגנבות ברשת האינטרנט מיליוני רשומות מסוג זה. הפרטים נארזים לפי פרמטרים שונים, ונמכרים כ־"Dumps" ללקוחות ב"שוק השחור" שתואר לעיל.[43]

התברר שמדובר היה בהתקפה פשוטה: הושתלה רוגלה (spyware) במספר אתרי סחר ישראליים, והיא העבירה נתונים שמפעילי האתרים הללו שמרו תוך הזנחת יסודות אבטחת המידע. על אף חוסר המורכבות והעדר נזק ממשי לאזרחים שהמתקפה גרמה, הפרשה זכתה לכיסוי תקשורתי נרחב ומתמשך במשך כשלושה שבועות, שבתחילתו התאפיין בפאניקה. האירוע הוצג כטרור אנטי־ישראלי, שכן במקום לממש את הרווח הכספי מהפריצה, בחר הפורץ להשתמש בו כדי לזרוע פחד בקרב ישראלים.

ניתן לנתח את האירוע במגוון דרכים: אפשר לומר שהאזרחים חסרי מודעות לאבטחה, שהתקשורת חסרת אחריות ומנפחת עניין שולי וגורמת לפאניקה, שבעלי אתרי האינטרנט התרשלו ופשעו באי־אבטחת המידע שאספו, ושהמדינה

התרשלה ביצירת סביבה בטוחה למסחר אינטרנטי ובשמירה על נתונים אישיים. אולם בכל ניתוח, המסקנה המתבקשת היא שדרושה הגברת ביטחונם האישי והקיבוצי של האזרחים במרחב הקיברנטי. בסופו של דבר הדרישה מופנית למדינה, שנושאת באחריות לביטחון אזרחיה. ניתן ורצוי לדון בהגדרת התופעות הבלתי־רצויות והפליליות במרחב הקיברנטי, במידת הביטחון הראויה, בחלוקת האחריות ובהגברת מודעות המשתמשים, בהרחבת גבולות המעורבות הממשלתית הרצויה ובדילמות נוספות הרלוונטיות לנושא. במדינה דמוקרטית, הסוגיות הללו ילובנו במסגרת דיון ציבורי ותהליך פוליטי. אין להניח שהדרישה לביטחון במרחב הקיברנטי תיעלם, שהבעיה תיפתר מעצמה או שהמדינה תוכל להתנער מאחריותה לביטחון אזרחיה. במקרה הישראלי האמור, אין כל מניעה שרשויות המדינה יגיבו לדרישות השונות של האזרחים ויערכו שינויים בסביבה המשפטית והרגולטורית, כדי להגביר את אבטחת המידע באתרי המסחר האלקטרוני. ויתור על ניסיונות הסדרה והאכיפה במרחב הקיברנטי יאפשר למגוון סוגי הפשע הקיברנטי להמשיך להתפתח ולשגשג, עד לרמה שהדבר יציב איומים של ממש על סוגיות הביטחון הלאומי: הספקת שירות לגורמים עוינים לצורך ביצוע מתקפות קיברנטיות, והגברת היקף הפשיעה לרמה שתערער את הביטחון האישי ואת הסביבה העסקית במדינה.

סיכום – ממשק מסוכן: הפשע הקיברנטי כסיכון הביטחון הלאומי

הפשע הקיברנטי מתפתח ומאתגר את המדינות המפותחות באופנים שונים. המידע הקיים על מקרי הפשע הקיברנטי מגיע מהדוחות התקופתיים של גופים העוסקים בנושא: חברות ייעוץ, מחשוב, אבטחת מידע ורשויות אכיפת חוק. לנוכח הבעיות המובנות בזיהוי התופעה, השימוש הגס בשיטות סטטיסטיות להשגת אומדן כמותי והכללת הנזק העקיף בהערכות הכספיות – המידע הקיים אינו מהימן. נראה שההערכות הכספיות מציגות הטיה קבועה להערכת־יתר. אולם, אף על פי שהערכות בדבר היקף הפשע מוּטות כלפי מעלה, לפשע הקיברנטי יש פוטנציאל מסוכן.

במאמר זה נבחנה משמעות התופעה ביחס לביטחון הלאומי. הניתוח מעלה שטווח רחב של פשיעה קיברנטית אינו מהווה סכנה לביטחון הלאומי. תופעות כמו גניבה וריגול תעשייתי, הונאה, תוכן פוגעני, פשעי שנאה, השחתת אתרים, מניעת גישה לשירות וכדומה – עלולות להפוך לבעיות ביטחון לאומי רק אם היקפן יתרחב מאוד והשפעתן תהיה ממושכת. לכן, כבר עתה ראוי להקדיש משאבים לצמצום הסכנה, ולהקשות על הפושעים הקיברנטיים לפעול בתחום זה.

ניסיון העבר מלמד שגורמים עוינים משתמשים בשירותים וביכולות של ארגוני הפשע, ומגייסים את מומחיותם להשגת מטרות מבצעיות. בשל קצב ההתפתחות

הטכנולוגית, יכולות המחשוב המתקדמות הנוכחיות יהפכו בעוד שנים אחדות למוצרי־מדף זולים. "השוק השחור" של שירותי המחשוב מנגיש את היכולות המתקדמות למגוון רחב של גורמים, ומרחיב את העדויות המצטברות על השימוש בשירותיו. הדבר מגביר את החשש שגם במרחב הקיברנטי קיים ומתפתח שיתוף הפעולה בין גורמים עבריינים לבין ארגונים עוינים.

על יסוד הניתוח שהוצג במאמר זה, מוצע להתמקד בשני ממשקים מרכזיים בין הפשע הקיברנטי לבין הביטחון הלאומי. הראשון – מדינת הלאום היא הגורם האחראי לביטחונם האישי והקיבוצי של אזרחיה. אזרחים וארגונים נפגעים לעתים בצורות שונות מפשע קיברנטי. היקף הנזק אינו ברור: הערכות הנזק הרבות שמשמשות בדיון אינן אמינות, ומוּטות כולן כלפי מעלה. גם ללא הסכמה על ההיקף ומידת הפגיעה באזרחים, בארגונים ובמדינות, המדינה נדרשת להגיב להזדמנויות ולאתגרים של המציאות המתפתחת. עם התפשטותו המתמשכת של המרחב הקיברנטי לכל תחומי החיים, יש להניח שיגברו הדרישות מן המדינה לנקוט פעולות על מנת לספק ביטחון אישי ולאומי גם במרחב הקיברנטי. חרף אופיו הבינלאומי של המרחב הקיברנטי, המדינה תיאלץ להרחיב עד מאוד את עיסוקה בביטחון הקיברנטי. קווי המתאר של המעורבות המדינתית במרחב הקיברנטי מתבהרים בשנים האחרונות, כשאחת הסוגיות הטעונות בתחום היא המתח בין ערך הפרטיות האישית לבין ערך הביטחון הלאומי. במדינה דמוקרטית, תהליך עיצוב המדיניות הממשלתית בתחום הפשע הקיברנטי יהיה כרוך בדיון ציבורי, במאבק פוליטי ובטיפול משפטי ממושך.

הממשק השני – המסחור של יכולות טכניות ומבצעיות מנמיך את רף הכניסה לזירת הלחימה הקיברנטית, מרחיב את איומי הייחוס מעבר למדינות ולארגוני טרור גדולים ומכביד את הנטל על רשויות הביטחון הלאומיות. ארגוני הפשע מציעים משאבים, תשתית ואף שירות ללקוחות תמורת תשלום סביר. אפשר לנצל את השוק הזה לא רק לביצוע פשע שמניעיו כספיים, אלא גם לפגיעה ישירה בביטחון הלאומי. ההגנה על תשתיות חיוניות מפני איום קיברנטי היא סוגיה מרכזית בביטחון הלאומי, וחשיבותה עולה לנוכח התפוצה של גורמי הסיכון הפוטנציאליים, שיכולים לרכוש אמצעי לחימה ולגייס "לוחמים" ב"שוק השחור" של פושעי הסייבר.

לאור ניתוח משמעויות התופעה וזיהוי הממשקים המסוכנים בין הפשע הקיברנטי לביטחון הלאומי שהוצגו במאמר, מומלץ למקד כבר עתה תשומת־לב מדינתית בטיפול בהם, על מנת למנוע החרפת האיום. המדינה צריכה להגביר את מעורבותו ביצירת ביטחון קיברנטי, אולם היא אינה יכולה לפתור את הבעיה לבדה. מימוש אחריות המדינה לביטחון הקיברנטי מחייב שיתוף פעולה בין בעלי

העניין במגזר העסקי, האקדמי, הציבורי והביטחוני, כדי לספק ביטחון לאומי ואישי למדינה ולאזרחיה במרחב הקיברנטי.

הערות

1 P. N. Grabosky, "Virtual Criminality: Old Wine in New Bottles?" *Social & Legal Studies,* 10(2), 2001, pp.243-249.

2 Majid Yar, *Cybercrime and society: crime and punishment in the information age*. London: Sage Publications, 2006.

3 M. Cross, D. L. Shinder, *Scene of the cybercrime*, Burlington, MA: Syngress, 2008.

4 David S. Wall, *Cybercrimes: The transformation of crime in the information age*, Cambridge, Polity, 2007, p.10.

5 Alkaabi, A., G. M. Mohay, A. J. McCullagh and A. N. Chantler. *Dealing with the problem of cybercrime*", Conference Proceedings of 2nd International ICST Conference on Digital Forensics & Cyber Crime, October 4–6, 2010, Abu Dhabi. http://eprints.qut.edu.au/38894/1/c38894.pdf

6 Offences against the confidentiality, integrity and availability of computer data and systems, Computer-related offences, Content-related offences CoE, "Convention on Cybercrime" Budapest, 2001 http://conventions.coe.int/Treaty/en/Treaties/html/185.htm

7 מדובר בכמה מחשבים, הנגועים בתוכנה זדונית, שמאפשרת שליטה מרחוק ושימוש סמוי ביכולות המחשבים הללו. השימוש הנפוץ ביכולת הוא למשלוח דוא"ל זבל, התקפה של מניעת שירות מבוזרת וגניבה מתמשכת של מידע. ראו: https://www.checkpoint.com/products/anti-bot-software-blade/anti-bot-software-blade-landing-page.html

8 הרעיון להצפנה באמצעות מפתח ציבורי Public key encryption – עומד ביסוד האלגוריתם RSA, שפותח בידי Ron Rivest, Adi Shamir, Leonard Adleman והוצג ב־1978. הפטנט עליו פג בשנת 2000. התוכנה Pretty Good Privacy (PGP), המאפשרת שימוש חופשי בהצפנה חזקה באמצעות מפתח ציבורי, פותחה ב־1991.

9 Ryan, Richard M. and Edward L. Deci, "Intrinsic and Extrinsic Motivations: Classic Definitions and New Directions." *Contemporary Educational Psychology,* vol. 25, no, 1, 2000, pp. 54-67.

10 Piquero, Alexis Russell, and Stephen G. Tibbetts. *Rational Choice and Criminal Behavior: Recent Research and Future Challenges*, New York: Routledge, 2002.

11 מספר המחשבים הנגועים לבדו אינו יכול לשמש מדידה הולמת לעוצמת הרשת והנזק הפוטנציאלי Plohmann, Daniel, Elmar Gerhards-Padilla, and Felix Leder. *Botnets: 10 Tough Questions,* ENISA, 2011.

12 David S. Wall, *Cybercrimes: The transformation of crime in the information age,* p. 221.

13 ראו למשל: דו"ח GAO-07-705-Cybercrime, עמ' 16–17, יוני 2007. http://www.gao.gov/assets/270/262608.pdf

14 *BI Computer Crime Survey*, p.10, 2005. http://ww.fbi.gov/publications/ccs2005.pdf

15 Secretary of Commerce, Gary Locke (Remarks at the Washington International Trade Association, Washington, D.C., July 22, 2009).

Hathaway, Melissa E. "Falling Prey to Cybercrime: Implications for Business אצל and the Economy," Chapter 6 in: *Securing Cyberspace: A New Domain for*

National Security, Queenstown: Aspen Institute, February 2012.

16 Office of Cyber Security & Information Assurance in the UK Cabinet Office and BAE Detica: "The Cost of Cyber Crime", 2011, http://www.cabinetoffice.gov.uk/sites/default/files/resources/the-cost-of-cyber-crime-full-report.pdf

17 "Norton Study Calculates Cost of Global Cybercrime: $114 Billion Annually", http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02

18 Lesk, M. "Cybersecurity and Economics," *IEEE Security & Privacy,* vol. 9, no. 6, 2011, p.76; Carl Bialik, "A Cybercrime Stat's Nine Lives", *The Wall Street Journal*, September 26, 2007, http://blogs.wsj.com/numbersguy/a-cybercrime-stats-nine-lives-194/tab/print/

19 Florencio, Dinei, and Cormac Herley. "Sex, Lies and Cybercrime Surveys." Microsoft Research, 2012.
המחקר עובד והופיע כמאמר המערכת בניו יורק טיימס.
Florêncio, Dinei, and Cormac Herley. "The Cybercrime Wave That Wasn't" *The New York Times*, April, 15, 2012, https://www.nytimes.com/2012/04/15/opinion/sunday/the-cybercrime-wave-that-wasnt.html?_r=3&hpw

20 Card Verification Value – הקוד הסודי שמודפס על הצד האחורי של הכרטיס. השימוש בו מוודא את תקפות פרטי הכרטיס במקרים שזה לא נקרא באמצעות העברת הפס המגנטי.

21 הדיון חורג מגבולות המאמר. ראו פרק על סקרים אצל: Dane, Francis C. *Evaluating Research: Methodology for People Who Need to Read Research*. Los Angeles: Sage, 2011.

22 "דיסקים מזויפים הם כסף לטרור האסלאמי" 16 בינואר 2003, http://www.ynet.co.il/articles/0,7340,L-2378873,00.html

23 Hunt, J. "The New Frontier of Money Laundering: How Terrorist Organizations Use Cyberlaundering to Fund Their Activities, and How Governments Are Trying to Stop Them," *Information and Communications Technology Law,* vol. 20, no. 2, 2011, pp. 133-152.

24 שב"כ, "סקירה בנושא השימוש שעושה חמאס בתוך התת־קרקעי ברצועה", נובמבר 2000, http://www.shabak.gov.il/publications/study/Pages/hamas-tunnel-report.aspx

25 שב"כ, "הברחות אמל"ח לרצועת עזה מאיראן דרך סודאן וסיני", מאי 2011, http://www.shabak.gov.il/publications/study/Pages/Sudan120511.aspx?webid=a3db3c16-25d8-423d-98df-eb1b9253ab93

26 http://www.terrorism-info.org.il/malam_multimedia/Hebrew/heb_n/html/ipc_272.htm

27 Kshetri, Nir. "The Global Cybercrime Industry and Its Structure: Relevant Actors, Motivations, Threats, and Countermeasures," In: *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*, edited by Nir Kshetri. Heidelberg; London: Springer, 2010; Glenny, Misha. *Darkmarket: Cyberthieves, Cybercops, and You*. New York, NY: Alfred A. Knopf, 2011.

28 אפשר לסווג את כלי הנשק הקיברנטיים לפי השימוש המיועד: malware – תוֹקעה: תוכנה זדונית שמיועדת לשבש בסתר פעילות תקינה של מערכת ממוחשבת ולפגוע בתהליך שמנוהל באמצעות מערכת זו; spyware – רוֹגלה: תוכנה זדונית שמיועדת לאסוף נתונים בסתר ולעתים להעביר אותם ברשת; Scanners – מוכרות לאיתור פגיעויות; Remote and local exploits – לניצול פגיעות מוכרת; Network Sniffers –

להאזנה לתקשורת; Backdoor tools, Trojans – לגישה מרחוק ולהוצאת מידע.

29 ראו: Isaac Ben Israel, Lior Tabansky. "An Interdisciplinary Look at Security Challenges in the Information Age." *Military and Strategic Affairs*, vol. 3, no. 3, December 2011, p. 24.

30 Williams. "Organized Crime and Cybercrime: Synergies, Trends and Responses," *Global Issues,* vol. 6, no. 2, 2001, p. 5.

31 McAfee "Virtual criminology report: Organized Crime and the Internet," December 2007. ראו גם: "Kaspersky reveals price list for botnet attacks", July 23, 2009, http://www.computerweekly.com/news/1280090242/Kaspersky-reveals-price-list-for-botnet-attacks נראה שמחיר השימוש ממשיך לרדת.

32 ג'פרי קאר, 2 בנובמבר 2011, http://jeffreycarr.blogspot.com/2011/11/words-matter-dump-apt-for-apa.html

33 *Software as a Service: Strategic Backgrounder*. Washington, D.C.: Software & Information Industry Association, February 28, 2001, http://www.siia.net/estore/pubs/SSB-01.pdf

34 https://www.gartner.com/it/page.jsp?id=1963815

35 ליאור טבנסקי, "לחימה במרחב הקיברנטי: מושגי יסוד." **צבא ואסטרטגיה,** כרך 3, גיליון 1, מאי 2011.

36 CoE – "Convention on Cybercrime," מאז 2001, אשררו את האמנה 30 מתוך 46 המדינות החתומות עליה.

37 T. Maurer, *Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities regarding Cybersecurity*, Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011.

38 OECD, "Communique on Principles for Internet Policy-Making", June 29, 2011.

39 ITU, *National Cybersecurity Strategy Guide*, September 2011.

40 McConnell, Mike, Michael Chertoff, and William Lynn, "China's Cyber Thievery Is National Policy-and Must Be Challenged," *The Wall Street Journal*, January 27, 2012; Clarke, Richard. "How China Steals Our Secrets," *The New York Times,* April 2, 2012; Gardels, Nathan. "Cyberwar: Former Intelligence Chief Says China Aims at America's Soft Underbelly," *New Perspectives Quarterly,* vol. 27, no. 2, 2010, pp. 15-17; Brenner, Joel. *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*. New York: Penguin Press, 2011; U.S.-China Economic and Security Review Commission (USCC), *2009 Report to Congress of the U.S.-China Economic and Security Review Commission.*

41 ראו: Dunn, *Securing 'the Homeland'*

42 רועי גולדנברג, "בנק ישראל: נגנבו פרטי 15 אלף כרטיסי אשראי", **גלובס**, 3 בינואר 2012, http://www.globes.co.il/serve/globes/printwindow.asp?did=1000712125

43 Dump: a stolen credit card or bank accounts and the associated customer data; Holt, T. J., and E. Lampke, "Exploring Stolen Data Markets Online: Products and Market Forces," *Criminal Justice Studies,* vol. 23, no. 1, 2010.

קול קורא להגשת מאמרים

כתב העת "צבא ואסטרטגיה" הינו כתב עת שפיט היוצא לאור שלוש פעמים בשנה בעברית ובאנגלית. עורך כתב העת הינו ד"ר גבי סיבוני.

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

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

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

ייבחנו מאמרים עם הערות שוליים ומראי מקום בהיקף של עד 4,500 מילים.

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

להגשת הצעות ולפרטים נוספים ניתן לפנות לח"מ.

בברכה

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