תקציר

איראן הייתה אחת המדינות הראשונות שגיבשו אסטרטגיית סייבר לאומית סדורה, ובכלל זה הקמת המוסדות החיוניים ופיתוח היכולות הטכנולוגיות הדרושות. העניין האיראני בסייבר החל להתעורר בעקבות שתי התפתחויות עיקריות: ראשית, השימוש היעיל של האופוזיציה באינטרנט לשם ליבוי, ושימור לאורך זמן, של ההפגנות ההמוניות בעקבות זיוף תוצאות הבחירות לנשיאות ב־2009; ושנית, תקיפת סטקסנט (Stuxnet) הדרמטית ב־2010, שפגעה בתוכנית הגרעין האיראנית והייתה, כמדווח, מבצע משותף של ארצות הברית ושל ישראל. יכולות הסייבר של איראן הלכו וגדלו מאז בהתמדה, וכיום מקובל לדרג אותה בראש המעגל השני של מעצמות הסייבר העולמיות.

מטרתו של מזכר זה להציג ניתוח מקיף ועדכני של אסטרטגיית הסייבר ושל מוסדות הסייבר באיראן, ובעיקר של דרכי הפעולה האיראניות. בהיעדר מידע רשמי על אסטרטגיית הסייבר האיראנית, המחקר מסתמך על המידע הגלוי והמוגבל המצוי, על התבטאויות חלקיות של גורמים איראניים רשמיים, על הספרות הכללית העוסקת בתפיסת הביטחון הלאומי של איראן ועל פעילותה הנגלית הן בתחום הסייבר והן בתחום הקינטי. לשמה של מטרה זו המזכר מציג בפרוטרוט את תקיפות הסייבר האיראניות החשובות משנת 2010 ועד דצמבר 2023.

תחום הסייבר מציב בפני איראן אתגרים גדולים לצד יתרונות חשובים. איראן רואה בדאגה את תחום הסייבר כאמצעי חתרני להפצת ערכי המערב ולהעצמת האופוזיציה הפנימית, ומשום כך כאיום על המשטר. מנגד, הסייבר הפך בידי המשטר גם לאמצעי יעיל לעיצוב דעת הקהל ולשליטה על הציבור, כמו גם למרכיב חשוב באסטרטגיית העימות האסימטרי של איראן.

שלא כמו יריבותיה הערביות של ישראל בעבר, איראן אינה חותרת להביס את ישראל בטווח הקרוב לנוכח הבנתה שמטרה זו חורגת מיכולותיה. במקום זאת היא אימצה אסטרטגיית התשה ארוכת טווח שנועדה לפגוע בכוחה הצבאי של ישראל, לשחוק את מעמדה הבינלאומי ולערער את חוסנה החברתי, וכך להוביל בסופו של דבר לקריסתה. איראן גם מבינה שאין ביכולתה להציב איום קונוונציונלי משמעותי על ארצות הברית ועל שחקניות אחרות, ומשום כך חשיבותו של הסייבר כמרכיב באסטרטגיית העימות האסימטרי של איראן הולכת וגדלה. הסייבר גם הולם היטב את התרבות האסטרטגית האיראנית, ששמה דגש על העמימות, על יכולת ההכחשה ועל השימוש בשלוחים.

איראן מנהלת מבצעי סייבר נוסף על המבצעים בכלים האסימטריים המסורתיים שבידה, כגון הטרור ולוחמת הגרילה, ולעיתים אף במקביל אליהם, כדי לקזז את יתרונותיהן של יריבותיה החזקות יותר, כמו גם להרחיב ולהעצים את השפעתם של הכלים המסורתיים. תחום הסייבר חשוב במיוחד בעבור איראן מכיוון שיריבותיה העיקריות תלויות בו הרבה יותר ממנה, ולכן פגיעות יותר ממנה לתקיפות.

ישראל וארצות הברית הן היריבות העיקריות של איראן בתחום הסייבר, והיא מנהלת נגדן עימות שוטף, בעיקר מתחת לרדאר. תקיפות הסייבר האיראניות מכוונות גם נגד מדינות באירופה, במזרח התיכון ובשאר העולם, ונגד כמעט כל סוגי המטרות. איראן אימצה דוקטרינה צבאית רב־ממדית וגמישה, דהיינו היא שומרת לעצמה את הזכות לנקוט הן פעולה התקפית והן פעולה הגנתית בכל אמצעי שתמצא לנכון – קינטי או סייברי. יכולות הסייבר של איראן לא נועדו להיות עצמאיות אלא להשלים ולתמוך ביכולותיה הדיפלומטיות, הכלכליות והצבאיות ולחזק את הרתעתה.

האיבה האיראנית לארצות הברית, לערב הסעודית ולמדינות אחרות היא עמוקה, אך איבתה לישראל היא יסודית וכנראה בלתי ניתנת לשינוי. עם זאת, ובלי לגרוע מעומקה של איבה זו, חלק ניכר מפעילותה של איראן בתחום הסייבר, כמו גם בתחומים אחרים, הוא תגובתי. איראן החלה לפתח את יכולות הסייבר שלה בעיקר בתגובה לתקיפת סטקסנט; ביצעה כמה תקיפות סייבר לפני החתימה על הסכם הגרעין מ־2015 ואחריה; השתמשה באמצעי סייבר כדי להגיב בשנת 2020 על ההתנקשות האמריקנית בקאסם סולימאני, בכיר במשמרות המהפכה; ובשנים האחרונות, כמדווח, היא מנהלת מול ישראל מערכה מתמשכת של מהלומות סייבר הדדיות.

כדי להעריך את האפקטיביות של תקיפות הסייבר האיראניות עד היום, הן מוינו לארבע קטגוריות עיקריות: שיבוש והרס, ריגול, תודעה ותקיפות המשלבות פעולות מכמה קטגוריות או מכולן.

תקיפות שיבוש והרס. איראן הפגינה יכולת לגרום שיבוש משמעותי לפעילות כלכלית בישראל, בארצות הברית, באירופה, במזרח התיכון ובמקומות אחרים ואף להסב נזק לתשתיות לאומיות חיוניות. תקיפות נגד מערכות אספקת המים ובקרת התעבורה האווירית בישראל עלולות היו אפילו לגרום לנזק קטלני.

עם זאת, רוב תקיפות השיבוש וההרס שביצעה איראן עד היום לא היו מתוחכמות, ובדרך כלל הספיקו ההגנות שהופעלו נגדן כדי למנוע נזק רב. בפועל, רוב התקיפות התמקדו

ביעדים בעלי רמת הגנה נמוכה, מה שעשוי לרמוז כי איראן מאמינה שיעדים ישראליים ומערביים חשובים מוגנים היטב ואינם בטווח יכולותיה. אולם גם תקיפות השחתה ושיבוש בלתי מתוחכמות כנגד אתרי אינטרנט – עיקר התקיפות האיראניות עד כה – היוו מטרד לא מבוטל וגרמו נזק כספי משמעותי.

קשה, על בסיס המידע הגלוי הקיים, להעריך את יכולתה של איראן לבצע תקיפות סייבר צבאיות יעילות ומתמשכות, והיא טרם הפגינה יכולת לבצע תקיפות ברמה מערכתית. עם זאת, לא מן הנמנע שהיא שומרת את יכולותיה המתקדמות ביותר לנסיבות "המתאימות". ברי, מכל מקום, שהסייבר מאפשר לאיראן לבצע מתחת לרדאר תקיפות שיבוש והרס שקשה לזהות עימה.

מבצעי ריגול. עצם טבעו החשאי של עולם הריגול מקשה על היכולת להסיק מסקנות חד־משמעיות בנוגע ליעילות מבצעי הסייבר האיראניים בתחום זה. אפשר כן לקבוע, לכל הפחות, שאכן בוצעו תקיפות רבות מסוג זה ושבכמה מקרים הן אף הניבו מידע מסווג רב. חלק מן התקיפות אספו מודיעין הנוגע לתעשיות הביטחוניות, לתוכניות לפיתוח נשק וליכולות הצבאיות של כמה מדינות. בתקיפות אלו הושם דגש מיוחד על מדיניות הגרעין של ישראל ועל החשיבה המדינית והאסטרטגית של ארצות הברית, של המערב בכלל ושל ישראל. איראן ביצעה גם תקיפות ריגול בסייבר לצורכי טרור, או כדי להכין תקיפות הרס או מבצעי תודעה עתידיים. השימוש של איראן בסייבר היה אפקטיבי במיוחד למעקב אחר מתנגדי משטר, הן בתוך המדינה והן מחוצה לה, ולדיכויים. השליטה על תחום הסייבר סייעה למשטר לדכא סבבי מחאה חוזרים ונשנים ולבצר את המשך שלטונו.

מבצעי תודעה. מבצעי תודעה בסייבר הם מרכיב הולך וגדל במאמצי המשטר להפיץ תעמולה ולהגביר את התמיכה באמונותיו ובמדיניותו באיראן עצמה, באזור וברחבי העולם. מבצעי התודעה מספקים לאיראן ולשלוחיה מגוון פלטפורמות כדי להגיע להמונים במישרין, מיידית ובמחיר מזערי.

בחלק ממבצעי התודעה ביקשה איראן ליצור ולהחריף מחלוקות פנימיות אצל יריבותיה, להשפיע על תהליכי הבחירות שלהן ולערער את חוסנן החברתי. התקיפות האיראניות החוזרות ונשנות נגד מערכת הבחירות בארצות הברית ב־2020 הן דוגמה מובהקת לכך. תקיפות אחרות נועדו לשבש את יחסי החוץ של מדינות ולחרחר ביניהן משברים חמורים פוטנציאליים; במקרה אחד אף ניסה אתר איראני ליצור משבר גרעיני בין ישראל לפקיסטן.

מבצעי תודעה אחרים הסבו נזק כספי לממשלות ולחברות מסחריות ברחבי העולם ופגעו במוניטין שלהן.

מבצעי תודעה בסייבר סייעו לאיראן ולשלוחיה ליצור לחץ בינלאומי על ישראל כדי לצמצם מבצעים צבאיים שלה או לעוצרם בטרם עת, לפני שהספיקה להשיג את יעדיה. בכך הם פגעו ביכולתה של ישראל לנהל מבצעים צבאיים אפקטיביים ולשמר בו־בזמן את מעמדה הבינלאומי.

תקיפות משולבות. רוב תקיפות הסייבר שביצעה איראן מאז שנת 2020 שילבו מרכיבים של מבצעי שיבוש והרס עם מרכיבים של מבצעי ריגול ותודעה, לעיתים במסווה של תקיפות כופרה. איראן מינפה תקיפות משולבות אלו כדי להוסיף ולהעצים את ההשפעה של יכולות הסייבר ההתקפיות שלה או כדי לפצות על חסרונותיהן, והשימוש הגובר בהן הניב הישגים טובים יותר מן ההישגים של תקיפות מסוג אחד. השימוש בתקיפות כופרה בעיקר למבצעי תודעה ולא למטרות כספיות הוא מאפיין ייחודי של העימות האיראני עם ישראל.

שיטות הפעולה בסייבר שאימצה איראן עד כה שופכות אור על שלוש דילמות קריטיות המעסיקות הן את אנשי הביצוע בתחום הסייבר והן את התאורטיקנים. ראשית, הסייבר שימש בעבור איראן אמצעי יעיל לא רק ללוחמה אסימטרית אלא גם להפחתת הסיכונים להסלמה. מניתוח תקיפות הסייבר האיראניות הרבות המפורטות במחקר זה עולה כי יריבותיה כמעט שלא בחרו להסלים את המאבק בתגובה.

שנית, אם אכן נכונה הטענה שרמת ההגנה על יעדים חשובים במדינות המערב ובישראל חורגת מיכולתה של איראן לפגוע בהם, אזי היא תומכת במי שסבורים שתחום הסייבר הופך בהדרגה להגנתי יותר מהתקפי. יש אף הגורסים שיכולתה של איראן לגרום לנזק ניכר לשחקניות סייבר מתוחכמות הולכת ופוחתת. כך או כך, מדינות מתקדמות נהנות מאותם היתרונות הצבאיים האסימטריים שהסייבר מעניק לאיראן, אך בו־בזמן גם מפעילות את היכולות הקינטיות העדיפות שלהן ונהנות בכך מן היתרונות של שני העולמות.

שלישית, לעומת האסכולה הטוענת כי תחום הסייבר מחזק את השחקניות החלשות משום שהוא מספק להן אמצעים אסימטריים נוספים כדי לאזן את העוצמה העודפת של יריבותיהן, יש אסכולה אחרת הגורסת שהיכולות הטכנולוגיות המתוחכמות הנדרשות למבצעי סייבר אפקטיביים רק מוסיפות לחזק את המדינות המתקדמות ממילא. אומנם איראן הצליחה לרתום את תחום הסייבר לצרכיה, אבל נראה שישראל, ארצות הברית ומדינות המערב מצליחות לעשות זאת ביתר הצלחה, הן מבחינה חברתית־כלכלית והן מבחינה צבאית.

הניסיון במקרה האיראני, כך נדמה, מטה את הכף לטובת האסכולה השנייה, והמסקנה היא ככל הנראה שהסייבר רק מעצים את השחקניות המתקדמות מלכתחילה.

התנהגותה של איראן ממחישה שהיא לא אימצה בתחום הסייבר מדיניות של "אי־שימוש ראשון" (no first use). מנגד, אין סימנים לאינטגרציה בין אסטרטגיות הסייבר והגרעין של איראן, ואין סימנים שהיא רואה בתקיפות סייבר מערכתיות מדרגת הסלמה שמתחת לרמה הגרעינית, או ששני תחומים אלה הם חלק מאסטרטגיית ביטחון לאומי אחת כוללת.

עם השנים רבו מבצעי הסייבר של איראן ועלתה רמת התחכום שלהם. הם הפגינו יכולת לשבש, להרוס או לערער תשתיות לאומיות חיוניות, ארגונים מסחריים, יכולות צבאיות, מהלכים דיפלומטיים ותהליכים פוליטיים, ולפגוע בחוסנן החברתי של מדינות יעד. יכולותיה של איראן ימשיכו ככל הנראה להתחזק הן בגין יכולותיה שלה והן בגין סיוע הרוסי והסיני. אם מודדים את איום הסייבר האיראני לפי מספר התקיפות החשובות המוצלחות שבוצעו עד היום ולפי תוצאותיהן, אזי יש לראות בו איום משמעותי אך מוגבל. אולם אם מודדים את האיום על בסיס הפוטנציאל לשיבוש ולנזק עתידיים, אזי אין להפחית מממדיו.

אסטרטגיית הסייבר של ישראל למגזר הציבורי ולפרטי גובשה בשנים 2011–2015 והייתה מן הראשונות מסוגה. עם זאת, הרבה השתנה מאז ונדרש עדכון נרחב שלה. במישור הצבאי צה"ל גיבש דוקטרינת סייבר מבצעית, אך לא אסטרטגיית סייבר כוללת. יתרה מכך, חלפו כבר שמונה שנים מאז הושהתה ההחלטה להקים זרוע סייבר נפרדת, והסוגיה עדיין ממתינה להכרעה. מתחת לדרג הממשלתי אין פורום סטטוטורי האחראי, הלכה למעשה, לקביעת סדרי העדיפויות הצבאיים והמודיעיניים בתחום הסייבר ולאינטגרציה בין אסטרטגיות הסייבר האזרחית והצבאית. הדבר מחייב תיקון אם ישראל מעוניינת להביא לידי ביטוי מיטבי את יכולותיה בתחום הסייבר.

הכרעה מלאה של היריב במובן הקלסי, דהיינו שלילת יכולתו או ערעור רצונו להמשיך בעימות, בדרך כלל אינה יעד בר השגה בעימותים בסייבר. במקום זאת על ישראל לחתור ל"עליונות סייברית", כלומר להשיג את היכולת לגרום ליריב שיבוש או נזק בלתי נסבלים או, לחלופין, להפחית את עוצמת התקפותיו לרמה המאפשרת לישראל לתפקד ללא הפרעה ניכרת. כדי להשיג עליונות סייברית, יהיה על ישראל לחתור ליתרון מצטבר ורב־תחומי באמצעות שילוב הדרגתי של כל מגוון היכולות העומדות לרשותה (בסייבר ובתחומים הקינטיים, הדיפלומטיים והכלכליים). יהיה עליה גם לטפח מאגר לאומי של אנשי סייבר מוכשרים במיוחד ולהתגבר על המחסור הקיים בתחום זה כיום. ישראל חייבת גם לגבש אסטרטגיה לאומית לסיכול מבצעי התודעה של איראן בסייבר. ארצות הברית, בריטניה

וצרפת, כמו גם מדינות דמוקרטיות אחרות, כבר החלו להתמודד עם האיום הזה, וישראל יכולה ללמוד מניסיונן.

תוכנית הגרעין האיראנית נותרה האיום הצבאי הגדול ביותר על הביטחון הלאומי של ישראל. "דוקטרינת בגין", מרכיב המניעה באסטרטגיה הישראלית לסיכול תפוצת הגרעין, טרם יושמה במקרה האיראני, לפחות לא במובן הקלסי של תקיפה אווירית. מנגד, ייתכן שהתקיפות הקינטיות ותקיפות הסייבר הרבות המיוחסות לישראל, שנועדו לחבל בתוכנית האיראנית, הן אמצעי חדש ליישום הדוקטרינה. כך או כך, ישראל חייבת לוודא שיש בידיה היכולות הנדרשות כדי למנוע מאיראן להשיג יכולת גרעינית מבצעית.

לבסוף, ארצות הברית היא השותפה העיקרית של ישראל בתחום הסייבר. בניגוד לרוב תחומי שיתוף הפעולה הצבאי בין שתי המדינות, יכולות הסייבר של ישראל הן בעיקר תוצר של פיתוח מקומי, ויש לה הרבה להציע לארצות הברית בתחום זה, ולא רק לקבל ממנה. חשוב שישראל תשאף להרחיב ככל האפשר את שיתוף הפעולה עם ארצות הברית בתחום הסייבר, אך בה בעת למזער את הסיכון לחופש הפעולה העצמאי שלה. את הדיאלוג עם ארצות הברית בנושא הסייבר יש לעגן רשמית במזכרי הבנה חדשים ומורחבים.