יכולות הסייבר של איראן: הערכת האיום לאינטרסים הכלכליים והביטחוניים של ישראל

סם כהן

איראן ממשיכה לפתח וליישם מגוון יכולות סייבר, שהולכות ונעשות מתוחכמות יותר ויותר, וזאת כדי לתמוך באינטרסים האסטרטגיים שלה וליצור יכולת לבצע פשיעה כלכלית ממוחשבת. ליכולות אלו של איראן השפעה שלילית וישירה על ישראל, בהיותה יעד למתקפות סייבר נרחבות שנוהלו על ידי שותפיה של איראן או ישירות על ידי ההנהגה הפוליטית בטהראן. כדי להעריך את האיום האסטרטגי המדובר, משרטט המאמר את המטרות והמאפיינים של פעילות הסייבר האיראנית המכוונת נגד ישראל, ובכלל זה מתקפות על בנקים, חברות תעופה, צה"ל ותשתיות קריטיות. המאמר סוקר בקצרה את תולדות האינטרנט והתקשורת באיראן ומעריך את היכולות הטכניות של קבוצות המקושרות לממשל האיראני הפועלות בשיטה של "מאמץ תקיפה מתמיד" ("advanced persistent threat"). בסיכום קובע המאמר כי אסטרטגיה של הרתעה באמצעות תגובה, שתשכיל לנצל את יתרונותיה של ישראל בתקיפת רשתות מחשב ובניצול חולשות ברשת, עשויה להעניק לה יכולת משמעותית, אם כי לא נשולת סיכונים, לנטרל את יכולות הסייבר של איראן ההולכות ומשתפרות במהירות.

מילות מפתח: מתקפת סייבר, ישראל, איראן, אסטרטגיית סייבר התקפית, שחקן איום, קבוצות APT, מתקפת רשת מחשבים, ניצול חולשה ברשת מחשבים

סם כהן מתמחה כיום במדיניות הבטחת סייבר פדרלית ב־Telecommunications Industry Association (TIA) בוושינגטון הבירה. ההשקפות והדעות המובאות במאמר זה הן שלו בלבד ואינן מייצגות או משקפות בהכרח את אלו של מעסיקיו או של ארגונים אחרים אליהם הוא קשור.

מבוא

פעילות הסייבר של איראן אחראית לכמה ממתקפות המחשב היקרות, המתוחכמות והמאורגנות ביותר שהופנו כלפי גופי ממשל ישראליים והמגזר העיסקי בארץ. הסנקציות הבין־לאומיות, שהמשיכו לדרדר את הכלכלה האיראנית ולפגוע ביכולת השפעתה של איראן בזירה הבין־לאומית, יצרו לה תמריץ גיאו־פוליטי להוציא לפועל מִבצעי סייבר התקפיים ולהיות מעורבת בפעילות לא חוקית נגד יריבתה האסטרטגית ישראל. במקביל, התשתית הכלכלית, הצבאית והלאומית בישראל, המשמשת להעברת מידע ולקידום קישוריות אפקטיבית, נסמכת בצורה הולכת וגוברת על מערכות ורשתות דיגיטליות החשופות לפגיעה. איראן היטיבה לנצל פגיעויות אלו כדי לפעול נגד האינטרסים האזוריים של ישראל, ועשתה זאת תוך הקפדה על טביעת אצבע פוליטית מוגבלת שלה. מתקפות איראניות גדולות ניצלו פגיעויות בתשתיות קריטיות, הופנו כלפי קניין רוחני ופגעו במערכות מחשוב בתחומים מבצעיים של צה"ל.

שחקני מפתח במרחב הסייבר האיראני (כמו משרד המודיעין, מועצת הסייבר של הבסיג' והקבוצות APT33 ו"אשייאן") הוכיחו רמה גבוהה יחסית של תחכום במתקפות נגד ישראל. בנוסף לכך, איראן ממשיכה לגבש ולארגן את משאבי הסייבר הלאומיים שלה לכדי אסטרטגיה העוסקת באופן פעיל בחיפוש חולשות ופגיעויות במערכות מידע של תשתיות ושל המגזר העיסקי והצבאי בישראל, כדי לאפשר את ניצול החולשות והפגיעויות שלהן בעיתות שלום ומלחמה גם יחד.

מאמר זה מבקש לטעון כי אסטרטגיית הסייבר ההתקפי של איראן, בשילוב עם ההתקדמות הכוללת בתחום המחשוב במדינה, מהווה איום אסטרטגי ארוך טווח על האינטרסים הכלכליים והביטחוניים של ישראל. מול הנטייה להעמיד במוקד הדיון האסטרטגי בישראל את תוכניות הטילים והגרעין של איראן ואת תמיכתה של טהראן בטרור, מאמר זה מבקש להדגיש את הצורך של ישראל לתת עדיפות גם ליכולות ההתקפיות וליכולות ההרתעה שלה במרחב הסייבר, כדי לתת מענה הולם לאיום הסייבר האיראני.

מפת דרכים והיקף הניתוח

החלק הראשון של המאמר יציג סקירת רקע קצרה על היסטוריית המחשבים והרשת באיראן. במסגרת זו הוא יסקור את התפתחות הידע בתחום אבטחת המחשבים באיראן, כמו מידת ההתעניינות של הציבור בקורסי מחשב באוניברסיטאות, וכיצד שוק העבודה באיראן מתפתח בהתמדה באופן התומך בתעשיית טכנולוגיית המידע והתקשורת (ICT) ונותן מענה לביקוש הגובר לאנשי מקצוע בתחום אבטחת הסייבר. החלק השני של המאמר יציג סקירה קצרה של "מתקפות רשתות מחשב"

(CNA) ו"מתקפות ניצול חולשה ברשתות מחשב" (CNE), כדי להוסיף הֶקשר לממד הטכנולוגי ולהיקף של כמה מפעילויות הסייבר האיראני שיידונו בהמשך.

החלק השלישי, שיתאר את התפתחות אסטרטגיית הסייבר של איראן, יבחן את המתקפות שערכו איראן וגורמים הקשורים אליה לפני ואחרי אירוע התולעת "Stuxnet", וכיצד גורמי הפיקוד, כגון "צבא הסייבר האיראני" (ICA) ו"מועצת הסייבר של הבסיג'", אימצו גישה חדשה למבצעי סייבר התקפיים המכוונים נגד אויבי איראן, ובמיוחד נגד ישראל. חלק זה יתאר גם את המרכיב הגיאו־פוליטי הייחודי של פעילות הסייבר ההתקפית של איראן. פעולותיה של איראן במרחב הסייבר, המתואמות עם שותפות פוליטיות אזוריות, ייבחנו במקרה בוחן מספר 1, ופעולות הסייבר של איראן במהלך המשא ומתן על הסכם הגרעין והסנקציות עליה יידונו כמקרה בוחן מספר 2.

החלק הרביעי של המאמר יעריך את היכולות הטכניות של שחקני מפתח באיום הסייבר האיראני, שתקפו בעבר את ישראל. הניתוח לא יקיף את כל השחקנים הרלוונטיים, אלא יבחן את האיומים המתוחכמים ביותר, במטרה להעריך את סיכוני הסייבר הנשקפים מאיראן למערכות המידע ולרשתות הנתונים בישראל.

החלק החמישי והאחרון יגדיר את הצורך בשינוי מדיניותה של ישראל לעֵבר מדיניות שבה פעילות הסייבר האיראנית תקבל מעמד של איום אסטרטגי, בדומה לאיום המיוחס לתוכניות הגרעין והטילים הבליסטיים של איראן. למרות שקשה להשוות את איום הסייבר לאיום הפיזי המיידי הנשקף מנשק גרעיני וממערכות השיגור שלו, מתקפות הסייבר המקושרות לאיראן הן איום פעיל ומתמשך הגורם נזק עקבי ומהווה איום מתמשך על האינטרסים המסחריים והביטחוניים של ישראל. חלק זה יציע לישראל גישה התקפית אפשרית, אותה היא תוכל ליישם כדי לאזן את הסיכונים האסטרטגיים הנובעים מהיכולות הגוברות של הסייבר האיראני.

היסטוריה עכשווית של מחשבים וטכנולוגיות המידע והתקשורת באיראן

כבר בשנת 1993 החל מסעוד סאפארי, ראש "המועצה העליונה לאינפורמטיקה באיראן", לקדם יוזמה לאומית להקמת רשת תקשורת נתונים ייעודית שתפעל באמצעות תשתית הטלפון באיראן.[1] מספר שנים לאחר השקת היוזמה, חנכה איראן את ספק שירותי האינטרנט (ISP) המסחרי הראשון שלה. בפברואר 1995 החל ספק האינטרנט החדש להציע גישה לאינטרנט, בעיקר באזור עיר הבירה טהראן,

1 David Banisar and Patricia Melendez, "Tightening the Net Part 2: The Soft War and Cyber Tactics in Iran", *Article 19 Free Word Center: Civic Space Unit*, March 2017, p. 12, https://www.article19.org/data/files/medialibrary/38619/Iran_report_part_2-FINAL.pdf.

בשיתוף עם "מכון נדה רָיָנֶה" (NRI), שהוא ארגון ללא מטרות רווח המסונף לממשל המוניציפלי של טהראן. באותה שנה חיזקה "חברת הטלקומוניקציה האיראנית" (TCI), בשיתוף עם "חברת תשתיות הטלקומוניקציה" (TIC) שבבעלות המדינה, את המונופול שלה באמצעות רכישת "שערי אינטרנט" (internet gateways) בין־לאומיים, תוך שהיא משתלטת על ספק האינטרנט המקומי היחיד.[2]

ב־1994 הודיעה "חברת הטלקומוניקציה האיראנית" על פיתוחה של רשת מיתוג־מנות בפריסה ארצית, בשם "IranPac".[3] כמה חודשים לאחר מכן הוקמה חברה ציבורית משותפת בשם "חברת תקשורת הנתונים של איראן" (DCI), במטרה להשתלט ולפקח על "IranPac", תוך הרחבת השימוש המסחרי והממשלתי בה. עוד שלושה גופים היו מעורבים בשוק תקשורת הנתונים המקומי באמצע שנות התשעים: חברה פרטית בשם "Pars Supaleh", "המכון למחקרים בפיסיקה ומתמטיקה תיאורטיות" (IPM) ומרכז לחקר נתונים בשם "Iranian Pek Data Outreach Center".[4]

בשנים 1996 ו־1997 התחילה "חברת תקשורת הנתונים של איראן" ליצור קשרים בין־לאומיים בין הרשת המקומית המתפתחת שלה ובין האינטרנט העולמי.[5] ההתפתחות המרכזית הראשונה הגיעה לאחר ש־DCI נכנסה לשותפות עם חברת תקשורת קנדית בשם "Teleglobe", שכיום נקראת "VSNL International Canada". "Teleglobe" פעלה בשיתוף עם "Intelsat" – חברת לוויינים מלוקסמבורג – כדי לספק לאיראן לראשונה שירותי לוויין (uplink) שיהיו משולבים ישירות במערכת של "IranPac".[6] זמן קצר לאחר מכן נכנסה DCI למיזם משותף עם משרד התקשורת הכווייתי ועם חברת HNS ("Hughes Network Systems") האמריקאית.[7] המיזם התמקד הפעם בגישה של DCI לשתי רכזות של מסופי לוויין זעירים (VSAT) בכוויית, המופעלים על ידי HNS, במטרה להגדיל במידה משמעותית את השטח הגיאוגרפי באיראן שיוכל ליהנות משירות ייעודי של אינטרנט והעברת נתונים, וזאת בנוסף לשיפור מהירות האינטרנט הארצית. בהמשך התרחב המיזם וכלל את חברת "Gulfsat" שבשליטה ממשלתית כווייתית, שביחד עם HNS סיפק

2 Grey E. Burkhart, "National Security and the Internet in the Persian Gulf Region", March 1988, https://web.archive.org/web/20070703041209/http://www.georgetown.edu/research/arabtech/pgi98-4.html.

3 Ibid.

4 Babak Rahimi, "CyberDissent: The Internet in Revolutionary Iran", *MERIA, Middle East Review of International Affairs Journal* 7, no. 3 (September 2003): 2-3.

5 Open Research Network, "Iran's Telecom and Internet Sector: A Comprehensive Survey", *Network Startup Resource Center: Oregon University* 1, no. 1 (June 1999): 12-13.

6 Ibid.

7 Burkhart, "National Security and the Internet in the Persian Gulf Region".

לממשלת איראן וללקוחותיה המסחריים שירות תקשורת אמין, המאפשר חיבורים מרוחקים וגישור לרשתות זרות, לרבות לצמתים המשרתים את אירופה, אסיה, המזרח התיכון ושוקי צפון אפריקה.[8]

איראן נתנה עדיפות להקמת תשתית אינטרנט ארצית חזקה, שבהדרגה הפכה נגישה לרוב האוכלוסייה, למרות ששירותי השידור ברשת היו איטיים ודמי המנוי היקרים היו חסם לאוכלוסיות נמוכות־ההכנסה במדינה. DCI שמה לה למטרה להגיע ל־300,000 משתמשים ממשלתיים ברשת שלה עד 1998, עם תוכניות להציע לציבור לרכוש מודמים לשימוש פרטי באותה שנה.[9] יעד זה השפיע באופן מהותי על סביבת האינטרנט באיראן: נכון ל־2001 היו בטהראן לבדה 1,500 בתי קפה שהציעו שירותי אינטרנט.[10] איראן הפכה לאחת המדינות המובילות במזרח התיכון במספר בתי הקפה המציעים שירותי אינטרנט באזור מטרופוליטני גדול. כיום, שוק ספקי שירותי האינטרנט באיראן הפך למגוון יותר, עם ספקיות ממשלתיות כמו "Irancell" ו"Hamrah Aval", שיש להן 67 מיליון משתמשים. כמעט 30 מיליון מהם נהנים מגישה לשירותי נתונים סלולריים מדור שלישי או רביעי.[11]

תשתית אינטרנט ארצית ותעשיית מחשבים ייעודית פועלות ומבוססות באיראן מזה שלושים שנה לפחות. הנוכחות של עמוד שדרה תקשורתי זה והנגישות המסחרית והפרטית הגוברת לאינטרנט לאחר 1998 הביאו להתפתחותה של אוכלוסייה איראנית בעלת אוריינות דיגיטלית בחומרות ובתוכנות. הדבר בא לידי ביטוי, בין השאר, ברשימת הקורסים הטכניים שמציעות האוניברסיטאות הגדולות באיראן. כך, למשל, "האוניברסיטה הטכנולוגית שריף" בטהראן פיתחה תוכנית לימודים ייעודית לאבטחה ומניעת פריצות, שבה סטודנטים לתואר ראשון ושני במדעי המחשב לומדים את יסודות הפצחנות (hacking), אבטחת סייבר ומדיניות אבטחת המידע.[12] תוכנית הלימודים כוללת קורסי מבוא Kali ו־Backtrack במערכות הפעלה, בדיקות חדירה לרשתות אלחוטיות, הזרקת SQL, חדירה למערכות IDS ול"חומות אש" וזיהוי פרצות אבטחה עבור XSS בתוכנות/יישומים מבוססי אינטרנט.[13]

בשנת 2013 השיקה איראן תוכנית לימודים ארצית לתלמידי בתי הספר התיכוניים, עם דגש על "סקריפטינג" ופצחנות.[14] סוכנות הידיעות "FARS" האיראנית דיווחה

8 Open Research Network, "Iran's Telecom and Internet Sector: A Comprehensive Survey", pp. 12, 15-16.

9 Rahimi, "CyberDissent: The Internet in Revolutionary Iran", pp. 233.

10 Ibid., p. 4.

11 Burkhart, "National Security and the Internet in the Persian Gulf Region".

12 Banisar and Melendez, "Tightening the Net Part 2: The Soft War and Cyber Tactics in Iran", pp. 32, 57.

13 Ibid., p. 58.

14 Ginger Hill, "Iran Adds Hacking to Their High School Curriculum", *Security Today*, September 4, 2013, https://securitytoday.com/articles/2013/09/04/iran-adds-hacking-

כי קורסים מסוימים יתמקדו בפריצה למערכות מחשוב התומכות בכלי טיס בלתי מאוישים, וכי תלמידים מיומנים בתחום מדעי המחשב ילמדו טכניקות לבקרת גישה מרחוק והרשאות.[15] רבים מתלמידים אלה מופנים בבוא העת לתוכניות אבטחת מידע ואבטחת סייבר באוניברסיטאות של טהראן.

התרחבות תשתית תקשורת הנתונים והאינטרנט באיראן בשנות התשעים הביאה לצמיחתה של תעשיית אבטחת מחשבים ארצית. סביר להניח שהתרחבות זו, בשילוב עם הגברת היצע הקורסים באוניברסיטאות והביקוש הגובר במגזר הפרטי למומחים ברשתות, בקידוד ובניהול נתונים, יגבירו את התחכום הדיגיטלי של איראן ואת מאגר הכישרונות הלאומי שלה לתמיכה במתקפות סייבר. גם גניבת הקניין הרוחני שמבצעת ממשלת איראן צפויה להמשיך ולתרום לכך, שכן טכנולוגיות מחשב זרות יאפשרו להאיץ את ההתפתחויות הטכנולוגיות בשוק המקומי.

מהם "מתקפת רשת מחשבים" ו"ניצול חולשת רשת מחשבים"

כדי להבין כיצד איראן ממנפת את מרחב הסייבר למטרותיה הגיאו־פוליטיות, הכלכליות והביטחוניות, חשוב לדעת להבחין בין סוגים שונים של פעילות סייבר. מבלי להבין את ההבדלים הטכניים, קשה יותר להסביר מדוע טהראן הייתה מעורבת במבצע מסוים, אֵלו שחקנים נהנו במיוחד ממתקפה או ממבצע ריגול כלשהו, וכמה יֶדע או יכולת טכנית נדרשו כדי להוציא לפועל את המבצע בהצלחה.

כדי להבהיר הבדלים טכניים אלה, נסקור בחלק זה של המאמר בקצרה את שלושת מרכיבי הפעולה העיקריים של אסטרטגיית הסייבר או לוחמת הסייבר: "ניצול חולשת רשת מחשבים" (CNE), "מתקפת רשת מחשבים" (CNA) ו"הגנת רשת מחשבים" (CND). ניתן לכנות שלושה מרכיבים אלה ביחד בשם הכולל "מִבצעי רְשתות מחשב" (CNO). מדובר במושג רחב, המשמש לתיאור תהליכי מחשוב צבאיים ואזרחיים גם יחד, אשר מנצלים את הרשתות הדיגיטליות ואת מערכות המידע, הנכסים והנתונים המחוברים אליהן למטרות אסטרטגיות. "מבצעי רשתות מחשב" מאפשרים לארגונים לתקוף ולשבש את רשתות המחשב של היריב, להגן על התשתית הידידותית המחוברת לאינטרנט ועל מערכות מידע פנימיות מפני תקיפה או ריגול, ולפרוץ לרשתות מחשבים לצורך איסוף מודיעין.[16]

---

to-their-high-school-curriculum.aspx.

15 Ibid; Micah D. Halpern, "Iran's Teaching Hacking in High School", *Huffington Post,* August 30, 2013, https://www.huffingtonpost.com/micah-d-halpern/iran-hacking-school_b_3836482.html.

16 Clay Wilson, "Information Operations, Electronic Warfare and Cyberwar: Capabilities and Related Policy Issues", *Congressional Research Service: Report for Congress Foreign Affairs, Defense and Trade Division*, March 2007, pp. 5-6.

מתקפת "ניצול חולשת רשת מחשבים" משמשת למטרות "מודיעין, מעקב וסיור" (ISR), כחלק מהיערכות למתקפה גדולה או כדי לאפשר פעילות ריגול בתוך מערכות ממוחשבות.[17] פעולות כאלו מתבצעות בדרך כלל באמצעות החדרת כלים ותהליכים לרשת המותקפת, ולאחר מכן חיפוש איטי אחר חולשות אבטחה נוספות שינוצלו במועד מאוחר יותר. מתקפת "ניצול חולשת רשת" יכולה להיות מבצע מותאם אישית, המחפש פיסת מידע ספציפית או חודר למקור מידע ספציפי, כמו למשל מאגר רשומות של עובד, או לשרת דואר אלקטרוני המפיץ מידע רגיש ברשת. מתקפות כאלו, שאינן מותאמות במיוחד אלא מיועדות לפעול כמערכת ריגול כללית, ארוכה וממושכת, מתנהלות בדרך כלל כך, שהגורמים הפורצים נודדים ברחבי הרשת המותקפת באמצעות העלאת רמת ההרשאות של המשתמש וקביעת הרשאות ברמת הבסיס או ברמה הניהולית, וממפים את כל הנכסים בתוך הרשת כדי להבין היכן מוחזקים הנתונים הרלוונטיים.

"מתקפת רשת מחשבים" מוגדרת כפעולות המשבשות או משמידות מידע או תהליכי נתונים, השוכנים במחשב המותקף או נתמכים על ידי הרשת המותקפת.[18] הכלים המשמשים ל"מתקפת רשת מחשבים" דומים לאלה המשמשים למתקפת "ניצול חולשה" בהיבט של פגיעה ביעד, אך בניגוד אליה, הם מיועדים לשבש מערכות ולא רק לאסוף מודיעין. "מתקפת רשת מחשבים" יכולה להסב נזק פיזי, כלכלי, ואסטרטגי. לדוגמה, מתקפות מסוג "מניעת שירות מבוזרת" (DDoS) מנסות להפוך את שירות הרשת לבלתי זמין על ידי הצפתו בתעבורה ממקורות מרובים. בדרך כלל הדבר מתאפשר באמצעות botnet עם שרת פיקוד ושליטה זדוני המתאם את תשתית ההתקפה הכוללת.[19] סוג כזה של "מתקפת רשת מחשבים" מציב אתגר בעיקר למוניטין ולכספים של חברות או ממשלות, שכן מסוף הבנקאות המקוון של הבנק או פורטל השירותים החברתיים של הממשלה עשויים להיות בלתי נגישים לפרק זמן מסוים. "מתקפת רשת מחשבים" חמורה יותר יכולה לכלול תקרית שבה יותקן יישום המכיל תוכנות זדוניות לוגיות ברשת המותקפת, אשר יביא להשחתת מערכות מידע מרכזיות או למחיקה, שינוי או הצפנה של נתונים בתמורה לדרישת כופר. לדוגמה, "מתקפת רשת מחשבים" העושה שימוש בתוכנה זדונית, המאפשרת לתוקף שליטה אינטראקטיבית מרחוק על נקודת קצה או מערכת מידע, תוכל לאפשר לתוקף להורות למחשב לכבות את אספקת החשמל

17 Kim Zetter, "Hacker Lexicon: What are CNE and CNA?" *WIRED*, July 16, 2006, https://www.wired.com/2016/07/hacker-lexicon-cne-cna/.

18 Ibid.

19 Andrew Shoemaker, "How to Identify a Mirai-Style DDoS Attack", *Imperva Incapsula: Security Reports*, April 10, 2017, https://www.incapsula.com/blog/how-to-identify-a-mirai-style-ddos-attack.html.

לציוד תעשייתי מסוים, וכך ליצור שגיאת הפעלה חמורה במתקן תשתית קריטית או במפעל עיסקי.

פעילות "הגנת רשת מחשבים" מוגדרת כאמצעי הגנה המשמש להגנה על מידע, מחשבים ורשתות מפני שיבוש, ניצול או הרס מקריים או מכוונים.[20] פעילות "הגנת רשת מחשבים" יכולה לכלול כלים המנטרים באופן פסיבי, מונעים או מגיבים לפעולות מחשב לא מורשות, כגון "חומת אש" או הצפנת נתונים אדפטיבית, או לכלול אמצעים אקטיביים יותר, כגון ניטור מחשבים של האויב מבפנים במטרה לקבוע את יכולותיהם וכוונותיהם, או כדי לשלב "מודיעין איומים" (threat intelligence) בתוך תוכניות אבטחת סייבר ממשלתיות ועיסקיות.[21] משימה מרכזית של פעילות "הגנת רשת מחשבים" היא לשפר את שלמות המידע הארגוני, תוך מתן יכולות תגובה מספיקות לצוותי האבטחה הבולמים אירועי סייבר, מחסלים אותם ומשקמים את המערכת לאחריהם.

התפתחות אסטרטגיית הסייבר וגורמי הפיקוד האיראניים

במהלך ראיון שהתקיים ב־2015 עם ערוץ התקשורת האיראני "Defa Press", הצהיר מפקד המטה הכללי של הסייבר באיראן, בְּהרוּז אֶסבָּאטי, כי "יכולות סייבר ואבטחת סייבר חשובות לא פחות מהנושא הגרעיני".[22] הערה זו מתַמצתת את החשיבות העליונה מבחינה אסטרטגית שאיראן מייחסת ליכולת להגן ולתקוף באמצעות רשתות דיגיטליות. כבר בתחילת שנות האלפיים ניתן היה לייחס מתקפות פוליטיות מקומיות לארגוני פצחנים בתוך איראן, אך פעולות לתקיפת יריבים זרים בחסות איראנית ממשלתית התחילו להופיע לראשונה רק ב־2007, לאחר שמשמרות המהפכה הקימו את "המרכז לחקר הפשע המאורגן".[23] אנשי

20 Wilson, "Information Operations, Electronic Warfare and Cyberwar: Capabilities and Related Policy Issues", pp. 5-6.

21 James Mulvenon, "The PLA and Information Warfare", in *The People's Liberation Army in the Information Age*, ed. James C. Mulvenon and Richard H Yang (Santa Monica, CA: Rand Corporation, 1999), pp. 185-186; Larry Hollingsworth, "Blacking Threats With CND: Protect Your Network From Hackers & Attackers", *MIL Corporation*, June 2018, https://www.milcorp.com/service-areas/cyber-security/computer-network-defense/.

22 Paul Bucala and Caitlan Shayda Pendleton, "Iranian Cyber Strategy: A View from the Iranian Military", *American Enterprise Institute: Critical Threats Project*, November 24, 2015, p. 7, https://www.criticalthreats.org/analysis/iranian-cyber-strategy-a-view-from-the-iranian-military.

23 Colin Anderson and Karim Sadjadpur, "Iran's Cyber Threat: Espionage, Sabotage and Revenge", *Carnegie Endowment for International Peace*, January 4, 2018, pp. 10-11, 60, https://carnegieendowme nt.org/2018/01/04/iran-s-cyber-threat-introduction-pub-75138.

מודיעין וגורמים רשמיים במערב רואים במרכז זה את ארגון הפצחנים הראשון בחסות ממשלת איראן ואת ההתגייסות הרשמית הראשונה של איראן למאמץ התקפי במרחב הסייבר.

ב־2009 התחילו משמרות המהפכה לגייס אנשי מקצוע לכוחות הסייבר שלהם וליחידה הצבאית המקורבת אליהם, שנקראה "צבא הסייבר האיראני" (ICA).[24] מפקד משמרות המהפכה, חוסיין חמדאני, הודיע בשנת 2010 כי "מועצת הסייבר של הבסיג'" – ישות סייבר נוספת תחת פיקוד משמרות המהפכה – הכשירה 1,500 אנשי מקצוע בתחום ביטחון הסייבר, כחלק מחיזוק הגישה ההתקפית וממערך הריגול שלה.[25] עוד קודם לכן, בשנת 2009, קראו ראשי יחידת הסייבר של הבסיג' במפורש לבצע מתקפה דיגיטלית "נגד פעולות של הישות הציונית".[26]

ב־2010 החדירו ישראל וארצות הברית תולעת מחשב זדונית למתקני תוכנית הגרעין של איראן. התולעת נקראה "Stuxnet", ו"מטען הנפץ" המתקדם שלה כלל ארבע מתקפות "אפס ימים"' שונות, שהשפיעו על מערכות ההפעלה "Windows" ועל תוכנת ההפעלה התעשייתית של חברת "סימנס".[27] התולעת התפשטה במערכות מידע ובנקודות קצה מסחריות וממשלתיות, עד שהגיעה, בסופו של דבר, לצמתים קריטיים במערכות לפיקוח ובקרה על נתונים (SCADA) במתקני ייצור הגרעין האיראניים. "Stuxnet" פגעה בבקרים מתוכנתים (PLC) מרכזיים, אשר הפעילו את הציוד התעשייתי באתרים הגרעיניים הללו, והתוצאה הייתה הרס של 984 צנטריפוגות ומכונות נוספות ששימשו את איראן להעשרת אורניום כחלק מתוכנית הנשק שלה.[28] בשנים שלאחר מכן התרחשו התקפות דומות על מערכות בקרה תעשייתיות איראניות, שהיו גם הן פרי שיתוף פעולה אמריקאי־ישראלי. כך, גרסאות של התוכנות הזדונית "Flame" ו־"Wiper" תקפו בקרים מתוכנתים במתקני ייצור הנפט והגז הטבעי באיראן, וכן מרכיבים נוספים בתשתית הקריטית של המדינה, כמו המערכת הארצית לביצוע העברות פיננסיות.[29]

24 Ashley Wheeler, "The Iranian Cyber Threat", *Phoenix TS: Tech Roots Project*, September 12, 2013, https://phoenixts.com/blog/the-iranian-cyber-threat-part-1-irans-total-cyber-structure/; Banisar, "Tightening the Net Part 2: The Soft War and Cyber Tactics in Iran", p. 7.

25 Michael Connell, "Deterring Iran's Use of Offensive Cyber: A Case Study", *CNA Analysis and Solutions and Defense Technical Information Center (DTIC)*, October 2014, https://apps.dtic.mil/dtic/tr/fulltext/u2/a6 17308.pdf.

26 Banisar, "Tightening the Net Part 2: The Soft War and Cyber Tactics in Iran", p. 33.

27 Kim Zetter, "An Unprecedented Look at the World's First Digital Weapon", *WIRED: Security Reports*, November 3, 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

28 Ibid.

29 Elinor Mills, "Behind the 'Flame' Malware Spying on Mideast Computers", *CNET*, June 4, 2012, https://www.cnet.com/news/behind-the-flame-malware-spying-on-

איראן ראתה במתקפת "Stuxnet" ובמתקפות הדומות שבאו אחריה הוכחה לאופן שבו יריביה משתמשים במרחב הסייבר כנשק ומנצלים נקודות תורפה במערך האבטחה הדיגיטלי שלה. התגובה הראשונית שלה הייתה הגנתית ונועדה למנוע ולרכך את נקודות התורפה שאפשרו את הצלחת מתקפות "Stuxnet", "Flame" ו־"Wiper". כך, למשל, לאחר מתקפת "Stuxnet" ב־2010, הקימה איראן את "פיקוד הגנת הסייבר", וכן מחלקה חדשה לביטחון סייבר תחת "ארגון ההגנה הפסיבית", כדי להגן על מערכות מידע מקומיות מפני יריבים זרים שחדרו לרשתות מפתח.[30] יחד עם זאת, איראן גם הכניסה שינוי דרמטי בגישה ההתקפית שלה בסייבר והתחילה להפנות משאבים מודיעיניים, ביטחוניים ותעשייתיים לתחום ההתקפי ולצורך חדירה לתוך רשתות האויב. היה זה שינוי אסטרטגי, ששם את הדגש לא רק על התמודדות עם פשיעה פיננסית ממוחשבת וגניבת קניין רוחני במטרה לשמור על כלכלת המדינה, אלא גם על מינוף מרחב הסייבר ככלי לאומי חדש להשגת מטרות גיאו־פוליטיות.

הדגש שאיראן שמה על יצירת יכולות וביצוע פעולות התקפיות בסייבר הינו רלוונטי לא רק לישראל, אלא גם לאינטרסים הכלכליים והביטחוניים של מדינות נוספות (שכן ערב הסעודית, ארצות הברית ומדינות אירופיות ומזרח תיכוניות נוספות נחשבות, גם הן, ליריבותיה של טהראן), אך ברור כי ארגוני הפצחנים האיראניים התמקדו בישראל כמטרה עיקרית. כך, למשל, ב־2014 שוגרו לעברה "מתקפת ניצול חולשה ברשתות מחשב" בשם "Operation Newscaster" ו"מתקפת רשתות מחשב" שנקראה "Thamar Reservoir" – שתיהן מבצעים איראניים המאופיינים בטקטיקות, בטכניקות ובנהלים ייחודיים, שכוונו נגד אנשי צבא ישראליים ונושאי תפקידים רשמיים.[31]

חברת האבטחה "ClearSky Cybersecurity" ביצעה הערכה כמותית של מתקפת "Thamar Reservoir", וגילתה כי ישראל הייתה יעד ל־14 אחוזים מכלל המתקפות ומבצעי ההנדסה החברתית שלה – נתון שמיקם אותה במקום השני כמדינת יעד למתקפות לאחר ערב הסעודית. ארצות הברית, בריטניה, קנדה ומדינות מערביות אחרות היו נתונות, כל אחת, לפחות משלושה אחוזים מהמאמץ האיראני המתואם.[32]

---

mideast-computers-faq/.

30 Banisar, "Tightening the Net Part 2: The Soft War and Cyber Tactics in Iran", p. 8; Connell, "Deterring Iran's Use of Offensive Cyber: A Case Study", p. 4.

31 ClearSky Research Team, "Thamar Reservoir: An Iranian Cyber-Attack Campaign against Targets in the Middle East", *ClearSky Cybersecurity, Inc.*, June 2015, https://www.clearskysec.com/wp-content/uploads/2015/06/Thamar-Reservoir-public1.pdf; Jim Finkle, "Iranian Hackers use Fake Facebook Accounts to Spy on U.S., Israel and others", *Reuters*, May 29, 2014, https://www.reuters.com/article/iran-hackers/iranian-hackers-use-fake-facebook-accounts-to-spy-on-u-s-others-idUSL1N0OE2CU20140529.

32 ClearSky Research Team, "Thamar Reservoir", p. 12.

נתונים דומים קיימים גם לגבי מתקפת "Operation Newscaster" ומחזקים את התפיסה, שלמרות שלאסטרטגיה ההתקפית של איראן יש מטרות ויעדים רבים, מערכות המידע הישראליות זוכות אצלה לעדיפות אסטרטגית מרכזית.

מקרה בוחן מספר 1: השותפים האזוריים של שחקן האיום

בשנים שלאחר מתקפת "Stuxnet" של שנת 2010, התחילו גורמים איראניים למצות באגרסיביות את נקודות התורפה של ישראל במרחב הסייבר. במסגרת זו החל שיתוף פעולה איראני עם קבוצות פצחנים של חמאס וחזבאללה, אשר ביחד עם איראן שיגרו "מתקפות רשתות מחשב" ו"מתקפות ניצול חולשה ברשתות מחשב" נגד השב"כ, פיקוד העורף, משרד ראש הממשלה, משרד הביטחון, בנק ירושלים, חברת התעופה "אל־על", מפלגות "הליכוד" ו"קדימה", וכן נגד פעילות מבצעית בצה"ל.[33] לפי הודעה רשמית של ראש הממשלה בנימין נתניהו ב־2013, מתקפות מחשב איראניות אחרות ניסו לחדור לרשתות תקשורת מקומיות של "מערכות לאומיות חיוניות".[34] בהודעה נאמר עוד כי איראן התחילה להתמקד בתשתיות מים, חשמל ופיננסים, בנוסף לאתרי שירותים חברתיים המופעלים על ידי הממשלה.

על פי כתבה ב"ג'רוזלם פוסט", אחד הפצחנים המובילים של חמאס היה מאג'ד בן ג'ואד עודה, שהצליח לחדור לרשתות תקשורת הנתונים של צה"ל וניתב נתונים מכטב"מים של צה"ל שריחפו מעל רצועת עזה לידי מפקדי חמאס.[35] החל משנת 2012 זכו אותם מפקדים להזרמה ישירה ובזמן אמת של סרטוני מעקב אווירים שהועברו מכלי הטיס הישראליים. ב־2015 כבר הצליח עודה לחלץ את אותות מערכת המיקום הגלובלית (GPS) מהכטב"מים אליהם פרץ, ואפשר בכך לפעילי חמאס הבכירים להעתיק את כוחותיהם ואת כלי הנשק שלהם הרחק אל מחוץ לשטחים הנתונים למעקב ישראלי.[36] כוחות הביטחון הישראליים עצרו את עודה, וב־2016 הוא הורשע בעבירות של ריגול, קשירת קשר, מגע עם סוכני אויב וחברות בארגון לא חוקי.

איראן פעלה עם חמאס גם כדי לתמוך בפעילות הסייבר של הארגון במטרה לשבש את הפעילות הצבאית והפוליטית של ישראל ברצועת עזה. כך, למשל, במהלך

---

33 Gabi Siboni, Matthew Cohen and Charles Freilich, "Israel and Cyberspace: Unique Threat and Response", *International Studies Perspectives* 17, no. 3 (August 2016): 309-310.

34 Jeffrey Heller and Maayan Lubel, "Iran Ups Cyber Attacks on Israeli Computers: Netanyahu", *Reuters*, June 9, 2013, https://www.reuters.com/article/us-israel-iran-cyber/iran-ups-cyber-attacks-on-israeli-computers-netanyahu-idUSBRE95808H20130609.

35 Yonah Jeremy, "Islamic Jihad Member Convicted in Plea Bargain For IDF Drones", *Jerusalem Post*, January 2017, https://www.jpost.com/Israel-News/Islamic-Jihad-member-convicted-in-plea-bargain-for-hacking-IDF-drones-480092.

36 Ibid.

הלחימה עם חמאס ב־2012, ישראל עמדה מול מערכה מתוחכמת בסייבר שניסתה להשבית אתרי אינטרנט ממשלתיים ופעילות במוסדות פיננסיים פרטיים, כולל בנק שעבר "מתקפת מניעת שירות מבוזרת", שהייתה קשורה לתשתית ידועה של שרת איראני.[37] גם במהלך המערכה נגד חמאס בשנת 2014 נרשמו אירועי סייבר, שבמסגרתם חוותה היחידה לאבטחת מידע של צה"ל פריצה זמנית למערכת המידע שלה, ו"הצבא האלקטרוני הסורי" – גוף פצחנות המסונף לאיראן – הצליח לפגוע באתר האינטרנט של צה"ל ולהעלות באופן זמני מסרים פוליטיים שהשמיצו את הפעולות הצבאיות הישראליות.[38]

דוגמה נוספת לתיאום בין איראן ובין בעלות הברית הגיאו־פוליטיות האזוריות שלה הם יחסיה עם "צבא הסייבר של חזבאללה". חברת אבטחת המידע הישראלית "צ'ק פוינט" מייחסת לארגון זה שורה של פריצות לגופים עיסקיים וממשלתיים בישראל בין השנים 2013 ל־2015.[39] הקמפיין של הארגון, שקיבל את השם "Volatile Cedar", היה מתקדם יחסית ומתוכנן היטב, והתוקפים פעלו בסבלנות כדי לא להיחשף, בעודם עוסקים בסריקות לאיתור נקודות תורפה ברשת החיצונית. גרסה מותאמת של התוכנה הזדונית שלהם, המכונה "Explosive", פעלה כ"סוס טרויאני" ואפשרה לתוקפים לבסס שליטה אינטראקטיבית מרחוק על שרתים ומערכות מידע המופנים כלפי חוץ. לאחר מכן השתמשו התוקפים בנכסים אלה כדי לסובב אותם כלפי השרתים הפונים פנימה, וכך יכלו לפרוס מודולים אחרים של התוכנה הזדונית ב"מארחים" (Hosts) של הרשת.[40] המאפיינים הטכניים של התוכנה הזדונית מצביעים על כך שהיא פותחה על ידי איראן, ולאחר מכן הועברה ל"צבא הסייבר של חזבאללה", דבר שעולה בקנה אחד עם המגמה הכללית של רשויות הסייבר באיראן, המבקשות להפיץ משאבי הדרכה וטכנולוגיה לגורמי איום הקשורים לחזבאללה.[41]

בנוסף לשותפים הזרים, ניצלה איראן גם קבוצות פרטיות של פצחנים במשרה חלקית לביצוע פעולות סייבר מתוחכמות פחות, אך כאלו שתאמו את יעדי

37 Siboni, Cohen and Freilich, "Israel and Cyberspace: Unique Threat and Response", p. 312.

38 Ibid.

39 Ben Shaefer, "The Cyber Party of God: How Hezbollah Could Transform Cyberterrorism", *Georgetown Security Studies Review*, March 11, 2018, http://georgetownsecuritystudiesreview.org/2018/03/11/the-cyber-party-of-god-how-hezbollah-could-transform-cyberterrorism/.

40 Threat Intelligence and Research Team, "Volatile Cedar", *Check point Software Technologies*, March 30, 2015, pp. 1-2, https://www.checkpoint.com/downloads/volatile-cedar-technical-report.pdf.

41 Anderson and Sadjadpur, "Iran's Cyber Threat: Espionage, Sabotage and Revenge", p. 21.

המדיניות שלה. לדוגמה, קבוצה פרטית שמכנה את עצמה "Charming Kitten" הייתה אחראית בשנת 2018 למתקפות מסוג "Man-In-the-Browser", באמצעות הכלי "browser exploitation framework" (BEF) נגד מספר רב של כלי תקשורת יהודיים בארצות הברית התומכים בישראל.[42] מתקפות דומות נערכו נגד ארגון איפא"ק, נגד יהודים בפוליטיקה ובאקדמיה ברחבי העולם ונגד ארגונים התומכים בפעולות הישראליות ברצועת עזה או בלבנון.[43]

מקרה בוחן מספר 2: הסכם הגרעין ואסטרטגיית הסייבר של האיראן

השימוש בפעילות סייבר התקפית כמנגנון תגובה להתפתחויות ביטחוניות אזוריות הפך לאופציית מדיניות שגורה של איראן, במיוחד נגד אינטרסים ישראליים. בהתבסס על הדוגמאות הקודמות שנותחו, ברור כי איראן מנהלת, יחד עם שותפותיה האזוריות, מבצעי סייבר באופן סדיר במטרה לשגר התקפות משולבות והתקפות מותאמות ספציפית לעבר מוסדות מסחריים וממשלתיים בישראל. מתקפות ומבצעי ריגול אלה נוטים להתרחש בתקופות של פעילות ביטחונית באזור, כגון פשיטות ישראליות לרצועת עזה או ללבנון. מגמה זו מלמדת כי פעילות הסייבר ההתקפית האיראנית קשורה באופן הדוק לאינטרסים הגיאו־פוליטיים של איראן ומותאמת אליהם בכל זמן נתון.

גישה אסטרטגית זאת אינה מאפיינת בהכרח את מדיניות הסייבר של מדינות אחרות, כגון רוסיה או סין. כך, למשל, רוסיה וסין, שלשתיהן יש מאגרי כישרונות ותשתית טכנית העולים לאין שיעור על התחכום, ההכשרה, המשאבים והיכולת של איראן, פועלות כשחקניות מערכתיות עקביות בתחום הסייבר ומוציאות לפועל מתקפות סייבר באופן קבוע וללא קשר לתנאים הגיאו־פוליטיים.[44] אמנם, מצב זה נכון גם לגבי שחקני סייבר מסוימים באיראן, כמו אלה המתמקדים בפשיעה פיננסית, אך מדובר בשחקנים ששליטת הממשל האיראני בהם היא פחותה ושמידת התיאום שלהם עם סדרי העדיפויות שלו נמוכה יחסית. כאלה, למשל, הם הפצחנים האיראניים העצמאיים שהיו אחראים לפריצה ל־HBO ב־2015, לאחר החתימה על הסכם הגרעין עם איראן והסרת הסנקציות הבין־לאומיות מעליה.[45] גם השינויים

---

42 Oded Yaron, "Iranian Hackers Tried to Impersonate Israeli Cyber-Security Company", *Haaretz*, July 9, 2018, https://www.haaretz.com/israel-news/premium-iranian-hackers-break-into-israeli-cybersecurity-site-1.6263629.

43 Anderson and Sadjadpur, "Iran's Cyber Threat: Espionage, Sabotage and Revenge", p. 35.

44 Mark Pomerleau, "DoD Releases First New Cyber Strategy in Three Years", *The Fifth Domain,* September 18, 2018, https://www.fifthdomain.com/dod/2018/09/19/department-of-defense-unveils-new-cyber-strategy/.

45 Andy Greenberg, "The Iran Nuclear Deal's Unraveling Raising Fears of Cyber Attacks", *WIRED*, May 9, 2018, https://www.wired.com/story/iran-nuclear-deal-

בתדירות "מתקפות רשת מחשבים" ו"ניצול חולשת רשת מחשבים" האיראניות אינם אופייניים לשחקניות הסיניות והרוסיות, ומדגישים את הייחודיות של האיום האיראני כלפי ישראל, בהיותו אסטרטגי וארוך טווח במהותו.

עדות להתאמתו של דפוס הפעולה של הסייבר האיראני להתפתחויות הגיאו־פוליטיות ניתן היה לראות בעת המשא ומתן על הסכם הגרעין עם איראן והסרת הסנקציות. פקידי ממשל אמריקאים ציינו כי בתקופה שהובילה למשא ומתן, בשנים 2013 ו־2014, הוציאה איראן לפועל מבצעי סייבר גדולים שגרמו נזקים כספיים משמעותיים לחברות במערב ובמזרח התיכון, וביניהן חברות בארצות הברית, קנדה, בריטניה, ישראל, ערב הסעודית ואפילו טורקיה.[46] בעקבות מתקפות הסייבר הנרחבות הצהירה התובעת הכללית של ארצות הברית דאז, לורֶטה לינץ', כי "התקפות אלו היו נחושות, שיטתיות ורחבות היקף".[47]

מייקל דניאל, נשיא "Cyber Threat Alliance", הסביר ב־2017 כי "ברגע שאיראן החליטה שהיא אכן מעוניינת להתיישב ליד השולחן ולנהל משא ומתן רציני, היא נקטה באופן טבעי שורת צעדים בשלל זירות שביטאו נסיגה מפעילותה המתעמתת".[48] איראן הרחיבה באופן משמעותי את פעילות הסייבר ההתקפית שלה במהלך תקופת הסנקציות שקדמה למשא ומתן, והפחיתה פעילות זו במהירות רבה ברגע שההסכם התקרב לשלב החתימה. אין ספק כי השינוי בתנאים הגיאו־פוליטיים בין 2014 ל־2015 הביא לצמצום המערכה האגרסיבית של איראן בסייבר, שאפיינה את השנתיים שקדמו לכך. לדברי לוי גונדרט, אנליסט בחברת המודיעין הפרטית "Recorded Future" המתמחה באיראן, "רוב המתקפות ההרסניות אירעו לפני 2015. אז נחתם הסכם הגרעין עם איראן".[49]

בעוד שהמשא ומתן וההסכם הרשמי שנחתם עם איראן ב־2015 עיכבו את פעילות הסייבר של איראן נגד אויביה, להחלטת הנשיא טראמפ במאי 2018 לסגת באופן רשמי מהסכם הגרעין הייתה השפעה הפוכה. חברת אבטחת המחשבים "CrowdStrike" פרסמה דוח המזהה שינוי בולט שחל בפעילותן של קבוצות פצחנים

---

cyberattacks/.

46 Kate Brannen, "Abandoning Iranian Nuclear Deal Could Lead to New Wave of Cyber Attacks", *Foreign Policy*, October 2, 2017, https://foreignpolicy.com/2017/10/02/abandoning-iranian-nuclear-deal-could-lead-to-new-wave-of-cyberattacks/.

47 Dustin Voltz, "U.S. Indicts Iranians for Hacking Dozens of Banks, New York Dam", *Reuters*, March 24, 2016, https://www.reuters.com/article/usa-iran-cyber/u-s-indicts-iranians-for-hacking-dozens-of-banks-new-york-dam-idUSL2N16W1I4.

48 Brannen, "Abandoning Iranian Nuclear Deal Could Lead to New Wave of Cyber Attacks".

49 Greenberg, "The Iran Nuclear Deal's Unraveling Raising Fears of Cyber Attacks".

איראניים 24 שעות בלבד לאחר הכרזת טראמפ על היציאה מההסכם.[50] פעילות זו כללה מתקפות גניבת זהות (spear-phishing), שתוכננו על בסיס הנדסה חברתית וכללו צרופות זדוניות שנשלחו בדואר אלקטרוני והותאמו במיוחד לפריצה לתוכניות אבטחת סייבר ממשלתיות ועיסקיות ספציפיות. הדוח מציין שהדואר האלקטרוני נשלח בעיקר למנהלים מסחריים ולאנשי צבא בכירים בארצות הברית, אך גם אנשי צבא ופוליטיקאים בכירים של בעלות ברית של ארצות הברית, כמו ישראל, היו יעד למתקפה.[51] ההכנות הנרחבות שהושקעו במתקפה מעידות כי איראן כיוונה את עיתויה כתגובה גיאו־פוליטית להצהרתו הרשמית של הנשיא טראמפ, וחיזקו בכך את ההנחה שאסטרטגיית הסייבר ההתקפי של איראן צמודה לתנודות ביעדיה האסטרטגיים ולשינויים החלים בסדרי העדיפויות של הביטחון הלאומי שלה.

איראן טרם פרסמה מסמך מקיף אחד המתאר את אסטרטגיית הסייבר הכוללת שלה או את המטרות, היעדים, המדיניות והשיטות של מִבצעיה ההתקפיים. עם זאת, הצהרות פומביות רשמיות של ממשלת איראן, בשילוב עם מתקפות CNA ו־CNE שניתן לייחס לאיראן, ואשר ניסו לנצל באופן ממוקד נקודות תורפה בישראל ואצל בעלות בריתה, ממחישות כיצד איראן התקדמה במדיניות הסייבר שלה מאז עמדת המגננה שאפיינה אותה לפני תקרית "Stuxnet". כך, למשל, ב־2017 הצהיר פרנק סִילוּפוֹ, מנהל "המרכז לביטחון הסייבר והמולדת" בארצות הברית, כי "איראן השקיעה בשנים האחרונות רבות בבניית יכולות למתקפות על רשתות מחשב ומתקפות ניצול חולשה. תקציב הסייבר האיראני זינק בתקופת הנשיא רוחאני פי 12 והפך את איראן לאחת מחמש מעצמות הסייבר המובילות. איראן גם משלבת פעולות סייבר באסטרטגיה ובדוקטרינה הצבאית שלה".[52] דגש חדש זה על אסטרטגיה התקפית, בשילוב ההידרדרות ביחסים הביטחוניים בין טהראן לירושלים, ממקמים את פעילות הסייבר האיראנית בחזית האיומים האסטרטגיים על ישראל.

---

50 Nicole Perlroth, "Without Nuclear Deal, U.S. Expects Resurgence in Iranian Cyberattacks", *The New York Times*, May 11, 2018, https://www.nytimes.com/2018/05/11/technology/iranian-hackers-united-states.html.

51 Ibid; Zack Whittaker, "Iran likely to Retaliate with Cyberattacks after Nuclear Deal Collapse", *ZDNet*, May 9, 2019, https://www.zdnet.com/article/iran-poised-to-launch-cyberattacks-after-nuclear-deal-collapses/.

52 Eric Auchard, "Once 'Kittens' in Cyber Spy World, Iran Gains Prowess: Security Experts", *Reuters*, September 20, 2017, https://uk.reuters.com/article/us-iran-cyber/once-kittens-in-cyber-spy-world-iran-gains-prowess-security-experts-idUKKCN1BV1VA.

היכולות הטכניות של הסייבר האיראני: ניתוח השחקנים המרכזיים

כדי לדעת מהם הסיכונים הטכניים והמדיניים העומדים בפני ישראל, יש לבחון את מידת התחכום של שחקני האיום המרכזיים באיראן. הבחינה תכלול, אמנם, רק חלק קטן מסביבת הסייבר האיראני, אך היא תתמקד במומחי הסייבר המנוסים ביותר של איראן ובדרך בה הם משפרים במהירות את הידע הטכני שלהם כדי לתמוך בגישה ההתקפית, ובכלל זה בהתקפות המכוונות כלפי תשתיות ומערכות מידע צבאיות ומסחריות בישראל.

APT33 היא קבוצת פצחנים איראנית שזוהתה לראשונה על ידי חברת אבטחת המחשבים האמריקאית "FireEye". הקבוצה אחראית לשורה של פריצות לתשתיות, לענפי בנקאות, תעופה וחלל ולתעשיות פטרוכימיות בישראל, ארצות הברית, בריטניה, דרום קוריאה וערב הסעודית.[53] מתקפות בשיטת ATP ("מאמץ תקיפה מתמיד") הן מתקפות מחשב זדוניות, שבהן אדם או ארגון משיגים גישה לא מורשית לרשת ונותרים בלתי מזוהים במשך תקופה ממושכת, במהלכה הם ממפים את הרשת לצורך זיהוי פגיעויות נוספות בה, מעלים את רמת הרשאות המשתמש שלהם, או טוענים "דלתות אחוריות" כדי לאפשר אינטראקציה מרחוק.

נהוג לקשר מתקפות "מאמץ תקיפה מתמיד" עם גורמים מדינתיים, בשל המשאבים הכספיים, היכולות והתשתיות שבדרך כלל נדרשים לכך. ואכן, תיאור זה הולם את יחסי קבוצת APT33 עם ממשלת איראן.

חברת "FireEye" וחברת אבטחת הסייבר הרוסית "Kaspersky Lab" פרסמו שתיהן דוחות המפרטים את הקשרים העֲנֵפים המורכבים בין APT33 ובין "מכון נאסר" של ממשלת איראן, שהוא גוף ביצוע המופעל במשותף על ידי יחידת הסייבר של הבסיג', המהווה חלק ממשמרות המהפכה, ומשרד המודיעין האיראני.[54] דוחות של ממשלות ארצות הברית וישראל מצביעים גם הם על כך שרבים מהאנשים הקשורים ל־APT33 עבדו בעבר בקבוצות אחרות של פצחנים איראניים, ואפילו בממשל האיראני עצמו.

למרות שקבוצת APT33 אינה אמורה לפעול רק נגד ישראל, היא ביצעה פעולות מותאמות ומורכבות ביותר נגדה, שפגעו ושיבשו מערכות מידע ישראליות. הקבוצה

53 Thomas Brewster, "Meet APT33: A Gnarly Iranian Hacker Crew Threatening Destruction", *Forbes*, September 20, 2017, https://www.forbes.com/sites/thomasbrewster/2017/09/20/iran-hacker-crew-apt33-heading-for-destructive-cyberattacks/#5b5693174a48.

54 Jacqueline O'Leary, Josiah Kimble and Kelli Vanderlee, "Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and Has Ties to Destructive Malware", *FireEye: Threat Research Team*, September 20, 2017, https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html.

משתמשת באופן קבוע בתוכנית "טרויאנית" מורכבת בשם "Dropshot", המאפשרת לתוכנות זדוניות לעקוף מערכות אנטי וירוס ולהפעיל תוכניות לא זדוניות בסביבות של "ארגז חול" וירטואלי, כדי למנוע זיהוי על ידי צוותי אבטחה.[55] הסברה היא שהתוכנה הזדונית נגזרה מקוד דומה ששימש קבוצת פצחנים איראנית מתקדמת נוספת בשם "חרב הצדק" ("Sword of Justice"), שהייתה אחראית על פיתוח ושיגור של התוכנה הזדונית המשוכללת וההרסנית "Shamoon" בשנת 2012.[56]

קבוצת APT33 השתמשה גם בגרסאות חדשות של "Nanocore" ו־"Netwire", שהן "סוסים טרויאנים" המעניקים גישה מרחוק (RAT) ותפקדו כמטעני נפץ עבור כלי ה־"Dropshot" שלהם, כשהם מספקים לקבוצה יכולת מלאה לחדור למערכות מוגנות, לאתר חולשות נוספות, לשאוב או למחוק נתונים ולהסיר עקבות מיומני רישום ואבטחה.[57] הדבר הִקשה מאוד על ניתוח הסיבות למתקפה וייחוסה ל־APT33, וכתוצאה מכך הקשה על פיתוח אמצעי נגד כמענה לפעולות הקבוצה.

קבוצת APT33 היא דוגמה לאחת מקבוצות הסייבר המתקדמות ביותר באיראן העוסקות בפעילות זדונית, המוציאה לפועל באופן שוטף מתקפות CNA ו־CNE נגד יריבים. פעילות הקבוצה עומדת בחזית אסטרטגיית הסייבר ההתקפי של איראן, ויש לה השפעה צבאית ישירה על ישראל. כך, למשל, מעריכים כי במהלך המערכה ברצועת עזה ב־2014 עמדה APT33 מאחורי הפריצה לרשת תקשורת אזרחית־צבאית להפצת מודיעין במרחב הלחימה.[58] חברות אבטחה פרטיות קישרו את APT33 למתקפות אלו בעקבות הטקטיקות, הטכניקות והנהלים, וכן הגרסאות של התוכנות הזדוניות שבהן נעשה שימוש. עם זאת, הרשת שהותקפה חוותה שיבושים בממסרי נתונים בין גורמי פיקוד ושליטה רק פרק זמן קצר, ולכן השפעת ההתקפה על המאמץ המלחמתי הכולל הייתה שולית.[59] יחד עם זאת, ולמרות שהמתקפה לא רשמה הצלחה מלאה, היא מדגימה כיצד איראן בונה יכולת טכנית שתאפשר לה לגבות מחיר של ממש במהלך מבצעים של צה"ל וממדיניותה הצבאית הכוללת של ישראל.

ישנם שחקני איום איראניים מתקדמים נוספים, הגורמים לפגיעה כלכלית משמעותית בישראל ומשפיעים על האינטרסים הכלכליים שלה. לדוגמה, קבוצת

---

55 Ibid.

56 Andy Greenberg, "New Group of Iranian Hackers Linked to Destructive Malware", *WIRED*, September 20, 2017, https://www.wired.com/story/iran-hackers-apt33/.

57 O'Leary, Kimble and Vanderlee, "Insights into Iranian Cyber Espionage: APT33".

58 Yaakov Lappin, "Iran Attempted Large-Scale Cyber Attack on Israel, Senior Security Source Says", *The Jerusalem Post*, August 17, 2014, https://www.jpost.com/Arab-Israeli-Conflict/Iran-attempted-large-scale-cyber-attack-on-Israel-senior-security-source-says-371339.

59 Ibid.

תקיפה איראנית בשם "COBALT DICKENS" ביצעה ב־2018 מתקפת CNA נגד מכוני מחקר, אוניברסיטאות ואנשי אקדמיה ברחבי העולם.[60] במסגרת זו נגנבו למעלה מ־15 מיליארד דפים של קניין רוחני ממסדי הנתונים וממאגרי המידע של מוסדות ב־21 מדינות. חברות אבטחה מעריכות את שווי הקניין הרוחני שנגנב בכ־3.4 מיליארד דולר.[61] גם האוניברסיטאות בישראל נפלו קורבן למתקפה זאת, אם כי ההפסדים המדויקים של כל אחת מהן לא פורסמו.[62] "COBALT DICKENS" מזוהים גם כשותפים של "מכון מָבְּנָה האיראני", שלו קשרים הדוקים עם גוף איראני אחר, "מכון נאסר". ארגונים אלה קושרו ל"מתקפת מניעת שירות" ולמתקפות מחשב אחרות על בנקים ישראליים, בנוסף לגניבת סודות מסחריים מחברות בישראל ומבעלות בריתה.[63]

קבוצה איראנית נוספת, המפעילה מאמץ תקיפה מתמיד, משמשת כמרכיב פעיל באסטרטגיית הסייבר ההתקפי של איראן ותוקפת באופן ספציפי את ישראל, היא "OilRig". קבוצה זו התחילה את פעילותה ב־2015 במתקפות גניבת זהות מוצלחות ובמתקפות מסוג "הרעלת DNS" נגד חברות עריכת דין, בנקים וספקי טכנולוגיית מידע חיצוניים הנותנים שירותים למגזר הפיננסי בישראל.[64] הנתונים על התקפות אלו ועל הנזקים הכספיים שהן הסבו מעורפלים ביותר וסובלים מתת־דיווח, ואף על פי כן ניתן ללמוד מהתקשורת הישראלית ומהצהרות ממשלתיות כי התקפות מסוימות פגעו במערכות מידע קריטיות הקשורות לענף כרטיסי האשראי, למסחר

60 John Kuhn, "COBALT DICKENS Targets Universities", *IBM X-Force Threat Exchange*, August 29, 2018, https://exchange.xforce.ibmcloud.com/collection/COBALT-DICKENS-Targets-Universities-4bdbb7eff5196b24ce4981abcffec11e.

61 Victoria Bekiempis and Larry McShane, "Iranian Hackers Stole $3.4B in Intellectual Property from Hundreds of Universities across the World", *Daily News*, March 23, 2013, https://www.nydailynews.com/news/crime/iran-hackers-breached-5-u-s-gov-computer-systems-prosecutors-article-1.3891703.

62 "Israeli University Compromised in Iran Hack", *Times of Israel*, March 24, 2018, https://www.timesofisrael.com/israeli-university-accounts-compromised-in-iran-hacking-scheme/.

63 Pierluigi Paganini, "Iran-linked COBALT DICKENS Group Targets Universities in New Phishing Campaign," *Security Affairs*, August 28, 2018, https://securityaffairs.co/wordpress/75710/cyber-warfare-2/cobalt-dickens-iran-attacks.html; Charlie Osborne, "Iranian Hackers Target 70 Universities Worldwide to Steal Research", *ZDNet*, August 24, 2018, https://www.zdnet.com/article/iran-hackers-target-70-universities-in-14-countries/; Brewster, "Meet APT33: A Gnarly Iranian Hacker Crew Threatening Destruction".

64 ClearSky Research Team, "Iranian Threat Agent OilRig Delivers Digitally Signed Malware, Impersonates University of Oxford", *ClearSky Cybersecurity Inc.*, January 5, 2017, https://www.clearskysec.com/oilrig/.

בבורסה ולדיווחים על מדדים. לפי הדיווח של "Palo Alto Networks", "OilRig" גם הצליחו לפרוץ למוסדות פיננסיים ולגופים טכנולוגיים בערב הסעודית.[65]

"OilRig" היא דוגמה לשחקן איום איראני בעל יכולת הולכת וגדלה. אחת מהטקטיקות והטכניקות שהקבוצה נוקטת היא שליחת קבצים מצורפים זדוניים של "אקסל" לעובד בארגון היעד של המתקפה. ברגע שהעובד פותח את הקובץ המצורף, אותו קובץ מציג תוכן דמה של גיליון אלקטרוני ומתקין גרסה של התוכנה הזדונית "HELMINTH". תוכנה זו פותחת "דלת אחורית" המקשרת את נקודת הקצה לשרת של פיקוד ובקרה, וכך מקבל התוקף שליטה מרחוק על נקודת הקצה שנפרצה.[66] התוקפים השתמשו גם בטכניקות ערפול מתקדמות כדי להסוות את תשתית המתקפה שלהם ופרטים מסוימים על התוכנה הזדונית "HELMINTH" עצמה, באופן שפגע בחקירת האבטחה והציב אתגרים לתוכניות אבטחת הסייבר של המערכת הפיננסית בישראל.

השחקן האחרון שחשוב להזכירו לצורך ההערכה הטכנית של יכולות הסייבר האיראניות הוא צוות האבטחה הדיגיטלית "אשייאן", המכונה גם "NEST". "אשייאן" הוא שחקן ייחודי בתוך סביבת האיומים הכללית של איראן, שכן בנוסף לפעולותיו הזדוניות, הוא פועל גם כספק מרכזי של משאבי הדרכה והכשרה מקוונים עבור קהילת הפצחנים ואבטחת המחשבים באיראן.[67] לדוגמה, חברי "אשייאן" השתתפו ב"האקתונים" ובכנסי אבטחה בעיר קום שבאיראן, אליהם הם הוזמנו כדוברים מרכזיים.[68] חברי הקבוצה סקרו בסמינרים סגורים באירועים אלה שיטות טקטיות וטכניות לחדירה לשרתי "לינוקס", מתקפות "מניעת שירות מבוזרת" ומתקפות להזרקת SQL. נכון לשנת 2017, 363,949 חברים היו רשומים להדרכה בקורסים המקוונים של הארגון, הכוללים מסרטוני הדרכה ועד מעבדות אינטראקטיביות, ומתמקדים בבקרת גישה, בהעלאת רמת ההרשאות, בניתוח וסריקה של מערכות הפעלה, בניהול רשתות ופריצה אליהן, בקריפטוגרפיה, באבטחת דואר אלקטרוני ובפיתוח "סוסים טרויאניים" מרחוק (RAT).[69]

---

65 Robert Falcone and Bryan Lee, "The OilRig Campaign: Attacks on Saudi Arabian Organizations Deliver Helminth Backdoor", *Palo Alto Networks*, May 26, 2016, https://researchcenter.paloaltonetworks.com/2016/05/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/.

66 Ibid.

67 Dorothy Denning, "Following the Developing Iranian Cyberthreat", *Scientific American*, December 12, 2017, https://www.scientificamerican.com/article/following-the-developing-iranian-cyberthreat/.

68 Banisar and Melendez, "Tightening the Net Part 2: The Soft War and Cyber Tactics in Iran", p. 34.

69 Ibid.

מתקפות ה־CNA וה־CNE הזדוניות של "אשייאן" אינן מתוחכמות, ממוקדות או עתירות משאבים כמו אלו של שחקני איום גדולים אחרים כגון APT33. ב־2017 ייחסו חברות אבטחת סייבר ל"אשייאן" את ההשחתה ושיבוש השירות של 500 אתרים ישראליים ומערביים – אירוע שהתרחש במהלך כניסת צה"ל לרצועת עזה ב־2009.[70] הארגון היה אחראי גם על התקפות נרחבות מסוג "מניעת שירות מבוזרת" ב־2010, שפגעו באלף אתרי אינטרנט בארצות הברית, בריטניה וצרפת, ובאו כתגובה לתמיכתן של מדינות אלו בקבוצות של פעילים אנטי־איראניים.[71]

כאמור, למרות ההשפעה הפוליטית והפיננסית של פעולות אלו, התחכום הטכני שלהן לא הגיע לרמה של שחקני האיום הדומיננטיים באירן. עם זאת, משאבי הלימוד הטכניים והמקצועיים ביותר ש"אשייאן" מציעים לפצחנים האירניים הופכים שחקן זה, ללא ספק, לגורם מסייע מרכזי בהתפתחות איום הסייבר ההתקפי של אירן, וזאת בזכות ההכשרה ורשת ההדרכה המקוונת שלו. ממשלת אירן עצמה הכירה במעמד שרכש הארגון בקרב קהילת הפצחנים, וגורמים כמו האייתוללה מפאתֶם שיראזי (סמכות דתית שיעית), משטרת הסייבר של אירן (FATA) וראשי משמרות המהפכה שיבחו את עבודתו.[72]

השחקנים המתוחכמים שצוינו לעיל אמנם מייצגים קבוצת מיעוט בסביבת האיומים הכוללת של אירן, אך ניכר שקבוצות הקשורות לממשלה האירנית או פועלות ישירות עימה הופכות ליותר ויותר מתקדמות. יתרה מזו, סדר הגודל, המורכבות וההיקף של מתקפת "COBALT DICKENS" ב־2018 (אף שלא כוונה רק כלפי מוסדות ישראליים) ממחישים כיצד שאיפות הסייבר של אירן גדלות במקביל ליכולות הטכניות שלה ולמשאביה. המטרות הכלכליות והצבאיות הספציפיות שישמשו יעדים לפעולות התקפיות עתידיות של אירן יעברו התאמה ככל שמיומנותם הטכנית של שחקני האיום המרכזיים תשתפר. עם זאת, המטרה הכללית של ניצול מרחב הסייבר ככלי אסטרטגי להפעלת לחץ על ישראל תישאר קבועה.

שינוי במדיניות האסטרטגית: יצירת משקל נגד לאיום הסייבר האירני

הדיגיטציה המהירה של תשתיות קריטיות והשימוש הגובר בטכנולוגיות מידע ותקשורת (ICT) רגישות בישראל, הפכו אותה לזירה הפגיעה לגורמי איום אירניים. בשנת 2011 אמר ראש הממשלה בנימין נתניהו בכנס ביטחון סייבר בתל אביב:

70 Denning, "Following the Developing Iranian Cyberthreat".

71 Ibid.

72 Banisar and Melendez, "Tightening the Net Part 2: The Soft War and Cyber Tactics in Iran", p. 34.

"ככל שאנו ממוחשבים יותר, כך אנחנו פגיעים יותר. לכן, אין מנוס מלהתמודד עם הבעיה בצורה שיטתית וממוקדת יותר".[73] באותו כנס אמר ראש מערך הסייבר של השב"כ כי "רשתות ישראליות, שהן קריטיות לתקשורת, למערכות תחבורה, לכספים ולאספקת חשמל ומים, חשופות כולן למתקפה. הדבר מהווה איום משמעותי על הביטחון הלאומי".[74] התייחסויות אלו מלמדות שישראל אימצה מזה כמה שנים נקודת מבט אסטרטגית על מרחב הסייבר. ואכן, ב־2015, למשל, נעשו רפורמות גדולות במדיניות, שהרחיבו את תפקידיהן ואת יכולותיהן של "הרשות הלאומית לביטחון הסייבר", "מערך הסייבר הלאומי", "הרשות לאבטחת מידע" ופיקוד הסייבר של צה"ל שבוטל מאז.[75] למרות זאת, חברת החשמל, האחראית על אספקת החשמל בישראל, חוותה בשנת 2016 השבתה בת יומיים של מערכת המידע שלה בעקבות מתקפת APT.[76] לצד המחויבות שהביע ראש הממשלה בשנת 2011 לשיפור אבטחת הסייבר, מתקפה זו הוכיחה שאיום הסייבר על מדינת ישראל רק החמיר, וכי מענים קודמים לא הצליחו לצמצם את האיום הטכנולוגי והאסטרטגי הזה.

הגישה המסורתית לאיתור והגנה מפני מתקפת סייבר לא תצליח להתמודד עם היכולות והכוונות האיראניות, וזאת בשל אופיו הגיאו־פוליטי של האיום. לדוגמה, רוסיה היא שחקן סייבר בעל מוטיבציה בהקשר של הפעילות הפיננסית בישראל, ולכן היא עוסקת בעיקר בגניבת קניין רוחני, בהונאת זהות ובעבירות של עסקאות פיננסיות באמצעות המחשב.[77] הערמת מכשולים והצבת חסמים בפני פעולות הסייבר של רוסיה בעזרת אסטרטגיה להגנת רשת מחשבים (CND) מפחיתות את התשואה הכספית שהשחקנים הרוסיים קוצרים בהשוואה לזמן, לכישרון ולעלויות הטכניות שעליהם להשקיע בהכנת מתקפות כאלו וביצוען. בניגוד לרוסים, המוטיבציה של איראן להפעיל מתקפות סייבר בישראל היא אסטרטגית וגיאו־פוליטית. אמנם, ישנם מקרים של שחקנים איראניים שהתמקדו ביעדים פיננסיים ובתחום הקניין הרוחני בישראל (כגון "COBALT DICKENS"), אך גורמי האיום האיראניים מתמקדים באופן גורף למדי באינטרסים הביטחוניים והכלכליים של

73 Matthew Kalman, "Israel Vulnerable to Cyber Attack, Leaders Warn", *MIT Technology Review*, June 15, 2011, https://www.technologyreview.com/s/424302/israel-vulnerable-to-cyber-attack-leaders-warn/.

74 Ibid.

75 Deborah Housen-Couriel, "National Cyber Security Organization: Israel", *Cyber Defense Center of Excellence NATO* 2, no. 4 (February 2017): 11-12.

76 Danna Harman, "Israel's Electrical Grid Targeted by 'Severe Cyberattack'" *Haaretz*, January 26, 2016, https://www.haaretz.com/israel-news/.premium-israel-s-electrical-grid-targeted-by-severe-cyberattack-1.5396042.

77 Ronen Bergman, "Israel is under Massive Chinese, Russian Cyber Espionage Attack", *YNet News Magazine*, July 31, 2018, https://www.ynetnews.com/articles/0,7340,L-5320392,00.html.

ישראל בדרך שפוגעת ומפעילה לחץ על ממשלת ישראל ברמה האסטרטגית, ולא בחברה עיסקית מסוימת או במטרה שתניב יתרון כספי לטהראן.

אסטרטגיה של "הרתעה באמצעות הכחשה" עוזרת למנף את תעשיית אבטחת הסייבר המתקדמת בישראל ויעילה כדי להבטיח שקבוצות איראניות פחות מתוחכמות לא יקבלו תמריץ לתקוף אותה. למרות זאת, על ישראל לפתח וליישם במקביל אסטרטגיה של "הרתעה באמצעות תגובה", שתתמקד בסייבר. ההיבט המרכזי באסטרטגיה של "הרתעה באמצעות תגובה" הוא האיום במחיר בלתי נסבל בתגובה למכה ראשונה מצד היריב, או במקרה זה, קמפיין ריגול או מתקפת CNA גדולה מצד איראן. פעולת התגמול המסיבית של כוחות הסייבר האיראניים לאחר מתקפת "Stuxnet" של 2010 מלמדת שטהראן צפויה לראות באסטרטגיה של "הרתעה באמצעות תגובה" של ישראל איום אסטרטגי ממשי על האינטרסים האיראניים, ובכלל זה על שלמות התשתית האנרגטית שלה, המנגנון הצבאי ומיזמים מסחריים. יתרה מזו, מתקפות ה־"Wiper" ו־"Flame", שבאו בעקבות "Stuxnet", חיזקו את התפיסה שישראל מחזיקה ביתרון איכותי מובהק בפעילויות סייבר התקפיות על פני איראן. ישראל צפויה להקטין את סיכון הסייבר מאיראן אם תיישם מדיניות תגובה פומבית וגלויה, שתבטיח פעולת תגמול בתגובה למתקפות סייבר גדולות שישגרו קבוצות איראניות.

התמקדות באסטרטגיית הכחשה בלבד תהיה בעלת השפעה מזערית על תפיסתה של איראן, הרואה בפעולת סייבר נגד ישראל הכרח גיאו־פוליטי. ישראל לעולם לא תוכל לאבטח לחלוטין את התשתית הלאומית והצבאית שלה או את הגופים המסחריים החשובים במדינה מפני סיכוני סייבר, ופירוש הדבר הוא שטהראן תוכל תמיד להשקיע משאבים פיננסיים, טכניים ואנושיים שיאתרו וינצלו נקודות תורפה, וכל זאת ללא תלות במחיר.

חשוב שישראל תמנף את כישרונות הסייבר הלאומיים ואת תעשיית ביטחון הסייבר שלה כדי להתגונן מפני איומים לא אסטרטגיים מצידן של מדינות אחרות (כמו רוסיה), או של תוקפים פחות מנוסים מתוך איראן עצמה. לצד זאת, ישראל נדרשת לנסח אסטרטגיה התקפית חדשה, שתיתן מענה לשיפור המתמיד ביכולת הסייבר האיראנית. התפיסה של "הרתעה באמצעות תגובה" בסייבר מציעה את המודל הנכון, ארוך הטווח והמשתלם ביתר מבחינה כלכלית כדי ליצור משקל נגד למטרותיה האסטרטגיות של איראן כלפי ישראל במרחב הסייבר.