איום הסייבר האיראני

צ'ק פריליך

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
אוניברסיטת תל אביב TEL AVIV UNIVERSITY

מזכר 231
פברואר 2024

איום הסייבר האיראני

צ'ק פריליך

איום הסייבר האיראני

צ׳ק פרייליך

מחקר זה נסמך על הספר *Israel and the Cyber Threat: How the Start-Up Nation Became a Global Cyber Power*, מאת צ׳ארלס (צ׳ק) פרייליך, מתיו כהן וגבי סיבוני, הוצאת אוניברסיטת אוקספורד, 2023. המחבר מודה למו״ל ולעמיתיו על הרשות להשתמש בחומר זה.

המכון למחקרי ביטחון לאומי

משלב בתוכו את מרכז יפה למחקרים אסטרטגיים, הוקם בשנת 2006. למכון שתי מטרות מוצהרות: הראשונה היא לערוך מחקרים בסיסיים בנושאי הביטחון הלאומי של ישראל, המזרח התיכון והמערכת הבינלאומית, וזאת על פי אמות המידה האקדמיות הגבוהות ביותר, והשנייה – לתרום לדיון הציבורי ולעבודת הממשל בנושאים שנמצאים, או ראוי שיימצאו, בראש סדר היום הביטחוני של ישראל.

קהלי המטרה של המכון למחקרי ביטחון לאומי הם דרג מקבלי ההחלטות, מערכת הביטחון, מעצבי דעת קהל בישראל, הקהילה האקדמית העוסקת בתחומי הביטחון בישראל ובעולם והציבור המתעניין באשר הוא.

המכון מפרסם מחקרים שלדעתו ראויים לתשומת הלב הציבורית ושומר על מדיניות נוקשה של אי־משוא פנים. הדעות המובעות בפרסומים הן של המחברים בלבד, ואינן משקפות בהכרח את העמדות של המכון, של נאמניו או של האישים ושל הגופים התומכים בו.

המכון למחקרי ביטחון לאומי
חיים לבנון 40
ת.ד 39950
רמת־אביב
תל־אביב 6997556

info@inss.org.il
http://www.inss.org.il/he
ISBN: 978-965-7840-03-0

עורכת הסדרה: ד״ר ענת קורץ, מנהלת המחקר, המכון למחקרי ביטחון לאומי
עורכת התרגום: יעל ברהמס
הגהה: מירה ילין
הביא לדפוס: עמר ויקסלבאום, המכון למחקרי ביטחון לאומי

עיצוב גרפי: מיכל סמו קובץ, המשרד לעיצוב גרפי, אוניברסיטת תל אביב
עיצוב העטיפה: שי ליברובסקי, המכון למחקרי ביטחון לאומי

דפוס: דיגיפריט זהב בע״מ

תוכן העניינים

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.

איום הסייבר האיראני

הרפובליקה האסלאמית של איראן חייבת להימנות
עם החזקות בעולם בתחום הסייבר.
עלי ח׳מינאי, המנהיג העליון של איראן

בתחילת העשור השני של המאה ה־21 הייתה איראן אחת המדינות הראשונות שגיבשו אסטרטגיית סייבר לאומית סדורה, ובכלל זה הקמת המוסדות החיוניים ופיתוח היכולות הטכנולוגיות והמבצעיות הנדרשות. עם השנים גדלו בהתמדה יכולות הסייבר של איראן, וכיום היא מובילה עם קוריאה הצפונית את רשימת מעצמות הסייבר העולמיות מן המעגל השני, אחרי מעצמות הסייבר מן המעגל הראשון – ארצות הברית, רוסיה, סין, בריטניה וישראל. יכולות הסייבר שלה ימשיכו ככל הנראה לגדול ולהשתפר בזכות המומחיות שלה עצמה ובזכות סיוע רוסי וסיני.

באיראן, כמו במשטרים סמכותניים אחרים, יחס המשטר לסייבר הוא דו־ערכי. איראן רואה בסייבר אמצעי חתרני לקידום ערכים מערביים מזיקים ולחיזוק האופוזיציה מבית ואיום על יציבות המשטר ועל הישרדותו. מנגד, הוכח כי הסייבר הוא אמצעי יעיל להפצת התעמולה של המשטר, לעיצוב דעת הקהל ולהשגת שליטה בעם. הסייבר הפך גם למרכיב חשוב בעימות האסימטרי שאיראן מנהלת נגד יריבותיה החזקות ממנה, והיא משתמשת בו בנפרד או בשילוב עם פעולות טרור ועם לוחמת גרילה. הסייבר תפס אפוא מקום חשוב בדוקטרינת הביטחון הלאומי הכוללת של איראן, והיא הפכה לאחת השחקניות ההתקפיות הפעילות ביותר בסייבר כיום.

ישראל וארצות הברית הן היריבות העיקריות של איראן בתחום הסייבר. לפי דיווחים, מאז שנת 2010 איראן מנהלת עם ישראל מערכה מתמשכת של מהלומות קינטיות ומהלומות סייבר הדדיות, ובמידה פחותה גם עם ארצות הברית. איראן ביצעה שורה של תקיפות סייבר גם נגד מדינות אחרות במזרח התיכון ובעולם. תקיפות אלו הוכיחו את חשיבות הסייבר לאיראן כאמצעי להשגת יעדיה הפוליטיים והצבאיים בלי אלימות פיזית ישירה ועד כה בלי סיכון רב להסלמה. תקיפות הריגול בסייבר הניבו לה מידע חשוב ושימשו אמצעי לגיוס מחבלים. מבצעי התודעה בסייבר שימשו את המשטר לקידום מטרותיו הנוגעות למדינות אחרות ולדיכוי האופוזיציה המקומית.

מטרתו של מחקר זה להציג ניתוח מקיף ועדכני של הסייבר האיראני – האסטרטגיה, המוסדות הרלוונטיים ובעיקר דרך הפעולה. לשם כך יוצג תיאור מפורט של כל תקיפות הסייבר החשובות שאיראן ביצעה משנת 2010 ועד דצמבר 2023, לרבות תקיפות שיבוש והרס, מבצעי ריגול ומבצעי תודעה.

איראן לא פרסמה רשמית את אסטרטגיית הביטחון הלאומי הכוללת שלה, ולא עשתה כך גם בתחום הסייבר. הניתוח שלהלן נסמך אפוא על המידע המצומצם הזמין, על התבטאויות חלקיות של גורמים רשמיים, על הספרות העוסקת בתפיסת הביטחון הלאומי הכוללת של איראן ועל התנהגותה הנגלית הן בתחום הסייבר והן בתחום הקינטי.

במחקר חמישה חלקים. בחלק 1 מוצג רקע כללי קצר על הסייבר, על איום הסייבר ועל מה שמייחד את הסייבר מתחומי עימות אחרים. קוראים הבקיאים בנושאים אלה מוזמנים לדלג ישירות לחלק 2; מוצגת בו אסטרטגיית הסייבר של איראן וכן המוסדות שבנתה והיכולות שפיתחה כדי ליישם אותה. בחלק 3 מפורטות תקיפות הסייבר העיקריות שאיראן ביצעה, על פי דיווחים, נגד שחקניות במזרח התיכון, נגד ארצות הברית ונגד מדינות ברחבי העולם. בחלק 4 מתואר איום הסייבר האיראני על ישראל. בחלק 5 נאמדת ההשפעה הממשית של תקיפות איראן עד כה, ומוצגת שורה של מסקנות בנוגע למדיניות הנדרשת.

חלק 1

סייבר

סקירה כללית

איום הסייבר האיראני הוא רק פן אחד של מהפכת המידע האדירה שסחפה את העולם בעשורים האחרונים. כיום הקהילה הבינלאומית יוצרת ביומיים בלבד כמות נתונים השווה בגודלה לכמות שנוצרה מאז ראשית הזמן ועד 2003. בשנת 2019 היה מחשב כמעט במחצית מבתי האב ברחבי העולם. בשנת 2021 כבר היו כ־15 מיליארד טלפונים ניידים, ובשנת 2022 יותר מ־26 מיליארד מכשירים היו מחוברים לאינטרנט.[1] כל מחשב וטלפון מייצגים התקדמות טכנולוגית וחברתית, אך גם משמשים פתח אפשרי לפעילות סייבר זדונית. מהפכת הבינה המלאכותית (AI) היא רק בתחילתה.

בשנים 2005–2019 נגנבו נתונים אישיים של יותר מ־11.5 מיליארד בני אדם ביותר מ־9,000 תקיפות סייבר. בשנת 2012 נאמדה עלות פשיעת הסייבר העולמית ב־8.4 טריליון דולר, והיא צפויה להכפיל את עצמה עד שנת 2025.[2] בתקיפות כופרה הקורבנות נתבעים לשלם כדי לקבל בחזרה גישה למערכות שלהם שהתוקפים הצפינו, והן כיום מובילות את הפשיעה בסייבר ואת תקיפות הסייבר שמניעיהם פוליטיים. לפי הפורום הכלכלי העולמי, פריצות בקנה מידה גדול של אבטחת סייבר הן מחמשת הסיכונים החמורים ביותר שהעולם מתמודד איתם.[3]

1 Statista, "Share of households with a computer at home worldwide from 2005 to 2019"; "Forecast number of mobile devices worldwide from 2020 to 2025 (in billions)"; Josh Howarth, "80+ Amazing IoT Statistics (2023-2030)," exploding topics, March 16, 2023.

2 Mike Isaac and Sheera Frenkel, "Facebook Security Breach Exposes Accounts of 50 Million Users," *New York Times*, September 28, 2018; Brian Fung, "Uber Reaches $148 Million Settlement over its 2016 Data Breach, which Affected 57 Million Globally," *Washington Post*, September 26, 2018; Nicole Perlroth, "All 3 Billion Yahoo Accounts Were Affected by 2013 Attack," *New York Times*, October 3, 2017; Tara Siegel Bernard, Tiffany Hsu, Nicole Perlroth, and Ron Lieber, "Equifax Says Cyberattack May Have Affected 143 Million in the U.S." *New York Times*, September 7, 2017; The Economist, "The Big Data Breach Suffered by Equifax Has Alarming Implications," September 16, 2017; Statista, "Estimated Cost of Cybercrime Worldwide 2017-2028."

3 U.S. Department of Homeland Security, "Cybersecurity Strategy," 2018, 2; Shoshana Solomon, "Israeli Entrepreneur Calls for NATO-Style Cybersecurity," *Times of Israel*, January 31, 2018.

לתקיפות סייבר על הצבא עשויות להיות השלכות חמורות במיוחד. הן עלולות להשבית מערכות נשק או לפגוע בדיוק שלהן, לשבש את התקשורת ואף להשפיע על המורל של החיילים ושל החברה האזרחית. לתקיפות סייבר מוצלחות על מטרות חיוניות שאינן צבאיות עשויה להיות השפעה מערכתית על יכולות הלחימה של מדינה. תמיר פרדו, ראש המוסד לשעבר, סבור כי "הסייבר הפך למקבילה השקטה של נשק גרעיני ולנשק האולטימטיבי שיכול פשוט לפרק מדינות. צבאות נועדו להגן על גבולות לאומיים, אבל הגבולות הפכו חסרי משמעות, ושדה הקרב עבר במידה רבה מהזירה הצבאית לאזרחית".[4] ואומנם תקיפות סייבר על תשתיות אזרחיות ועל יכולות חיוניות אחרות עלולות להסב נזק הרסני יותר ממתקפה גרעינית. פצצות גרעיניות הן הרסניות, אבל ההשפעות שלהן הן מקומיות, או אזוריות אם שולבו עם אמצעים צבאיים. ההשפעות הקטלניות של נשקי סייבר יהיו איטיות יותר, אבל עלולות להיות מערכתיות.[5] תקיפות סייבר הן למעשה מלחמה באמצעים אחרים.

לדוגמה, אם מתקפת סייבר תצליח להשבית את רשת החשמל של מדינה או אפילו רק חלקים מרכזיים שלה, היא תוכל לשתק את הכלכלה ואת הצבא של המדינה ולעצב את תוצאת העימות. תקיפות נגד מערכות מים, תקשורת או תחבורה עלולות לגרום לקטל המוני מקור, מהתייבשות, מתאונות דרכים ומתקלות חמורות בתחבורה. הן יכולות להוריד רכבות מן הפסים, להשבית רמזורים או להשתלט על מטוסי נוסעים מסחריים בעת הטיסה. תקיפות סייבר יכולות להשתלט על מערכות הניטור של כורים גרעיניים, בתי זיקוק או מפעלים כימיים, ולגרום להשבתתם או לגרוע מכך. תקיפות על מוסדות פיננסיים יכולות להעביר כספים בין חשבונות או למנוע גישה לחסכונות ולהשקעות, מה שיוביל לכאוס כלכלי. רישום אוכלוסין ומקרקעין, מאגרי מידע אוניברסיטאיים, שרשראות הפצה של מוצרים חקלאיים ושל מזון, מערכות לייצור רכב, אלקטרוניקה ותרופות ומערכות למענה בחירום – כולם יהיו בסכנת שיבוש או השבתה.

4 תמיר פרדו, ריאיון עם המחבר.

5 Joseph S. Nye, *The Future of Power: Its Changing Nature and Use in the Twenty-first Century* (New York: Hachette Book Group, 2011), 212; Jeremy Straub, "Hackers Could Kill More People than a Nuclear Weapon," *LiveScience.com*, August 27, 2019; United States Subcommittee on Emergency Preparedness, Response and Communications and the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies (2014); Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to do About It* (HarperCollins, 2010).

אחת ההשפעות המובהקות של הסייבר היא על איסוף מודיעין ועל מבצעי מודיעין. בעבר נאלצו סוכנויות ביון להקדיש משאבים רבים לפיתוח של נכס בודד. בשנת 2020 פגעה רוגלה רוסית בעשרות מטרות רגישות, חלקן ביטחוניות, בארצות הברית, בקנדה, במקסיקו, בבריטניה, בבלגיה, בספרד, באיחוד האמירויות ובישראל.[6] פצחנים המזוהים עם סין ביצעו תקיפות סייבר מסיביות נגד חברות טכנולוגיה ומוסדות פיננסיים בארצות הברית, ביפן ובאירופה, ונזקן הוערך בטריליוני דולרים.[7]

תחום הסייבר הפך לאמצעי חשוב לשמירה על הסדר בתוך מדינה. "חומת האש הגדולה של סין" משמשת לשליטה בגישה של משתמשים מקומיים לאינטרנט ולמעקב אחריה. סין משתמשת גם בבינה מלאכותית, בתוכנות לזיהוי פנים ובטלפונים סלולריים כדי לנהל מעקב גלובלי אחר יריביה הפוליטיים. ברוסיה ניהול תעבורת האינטרנט המקומית הוא ריכוזי, וברשת המקומית יש "נקודות חנק" (chokepoints) שנועדו לחסום גישה לרשת העולמית. איראן משתמשת בקמפיינים של מעקב סייבר כדי לרגל אחר מתנגדי משטר בחו"ל וכדי לדכא את האופוזיציה המקומית.[8] רבים מן המתכנתים ומן היצרנים של התוכנות ושל החומרות המשמשות כמעט את כל המכשירים האלקטרוניים (מחשבים, טלפונים חכמים, מכשירים רפואיים, מכוניות, טילים, מטוסים וכו') חיים במדינות שמשטרן סמכותני. המצב הזה מגדיל את הסיכוי שגורמים אלה יתקינו קוד נסתר במוצרים שלהם למטרות ריגול או הרס.

מבצעי תודעה בסייבר, בעיקר נגד מערכות בחירות במערב, הם אפקטיביים במיוחד. מבצעי סייבר סיניים כוונו נגד הקמפיינים לנשיאות של ברק אובמה ושל ג'ון מקיין כבר ב־2008, ושל ג'ו ביידן ב־2020.[9] התקיפה הרוסית על הבחירות לנשיאות ארצות הברית ב־2016 הייתה כנראה מבצע הסייבר הידוע ביותר שנערך אי פעם. ייתכן שהוא היה חלק

6 David E. Sanger, Nicole Perlroth, and Julian E. Barnes, "As Understanding of Russian Hacking Grows, So Does Alarm," *New York Times*, January 2, 2021.

7 Zolan Kanno-Youngs and David Sanger, "U.S. Accuses China of Hacking Microsoft," *New York Times*, July 19, 2021; Adam Segal, *The Hacked World Order: How Nations Fight, Trade, Maneuver and Manipulate in the Digital Age* (New York: Public Affairs, 2017), 8.

8 Segal, *Hacked World Order*, 7–9; U.S. Cyberspace Solarium Commission, Report (March 2020), 9-10, 17; Laura Rosenberger, "Making Cyberspace Safe for Democracy." *Foreign Affairs* (May/June 2020); Ronen Bergman and Farnaz Fassihi, "Iranian Hackers Found Way Into Encrypted Apps, Researchers Say," *New York Times*, September 18, 2020.

9 David E. Sanger, *The Perfect Weapon: War, Sabotage and Fear in the Cyber Age* (New York: Crown, 2018), 18; Tim Starks, "Russia, China and Iran Trying to Hack Presidential Race, Microsoft Says," *Politico*, September 10, 2020.

ממאמץ אסטרטגי רחב שנערך ב־19 מדינות ונועד לפצל את המחנה המערבי, להחליש את נאט"ו ולערער את האמון בתהליכים ובמוסדות דמוקרטיים.[10]

ידוע רק על מקרה אחד שבו לתקיפת סייבר הייתה השפעה קטלנית ישירה, אך תקיפות סייבר גרמו שוב ושוב לנזק פיזי, והיכולת שלהן רק הולכת וגדלה. גם אם רוב תקיפות הסייבר נכשלות, מספרן עצום ולכן גם ההצלחות הבודדות הצפויות להן עשויות להספיק כדי לערער את אמון הציבור במערכת לאומית או בינלאומית מסוימת. טכנולוגיית סייבר, מומחיות בסייבר ונשק סייבר זמינים לרכישה בשוק שחור מקוון ופורח. במחיר לא גבוה אפשר לרכוש יכולת בסיסית, וכמה מן היכולות המתוחכמות מסוגלות לחדור אפילו למערכות ממשלתיות ומסחריות מוגנות היטב. מידע שנגנב מממשלות ומגופים פרטיים זמין גם הוא לרכישה. חברה אחת אפילו מספקת מסד נתונים ובו המיקום וכתובות האינטרנט של מאות מיליוני מחשבים פגיעים ברחבי העולם ומציעה חבילות יעדים לתקיפה.[11]

התלות העמוקה בסייבר של שחקניות מדינתיות המתאפיינות בקדמה טכנולוגית היא בכל תחומי החיים המודרניים, והיא מספקת ליריבים מדינתיים ולא מדינתיים חלשים מגוון הזדמנויות לחולל נזק. תקיפות סייבר הן אטרקטיביות במיוחד מכיוון שהן בדרך כלל זולות יותר מן הקינטיות, מספקות אנונימיות ויכולת הכחשה שבתקיפה מסוג אחר קשה להשיג, והן אינן זקוקות לטריטוריה או לתשתית לאומית. תקיפה מתמשכת על רשתות אינטרנט מסחריות או ממשלתיות שאינן מוגנות דיין עלולה לכרסם אט־אט בכלכלה הלאומית ובמורל הציבורי ולכפות על היריב ויתורים שאינם רצויים לו. עם זאת, לרוב השחקנים האלה אין את

10 Daisuke Wakabayashi and Scott Shane, "Twitter, With Accounts Linked to Russia, to Face Congress Over Role in Election," *New York Times*, September 27, 2017; Craig Timberg and Tony Romm, "New Report on Russian Disinformation, Prepared for the Senate, Shows Operation's Scale and Sweep," *Washington Post*, December 17, 2018; Julian Barnes, "Russians Tried, but Were Unable to Compromise Midterm Elections, U.S. Says," *New York Times*, December 21, 2018.

11 Shane Harris, *@War: The Rise of the Military-Internet Complex* (Eamon Dolan/Mariner, 2014), 103–105; Chris Bing, "Chinese-authored Spyware Found on More than 700 Million Android Phones," *Cyber Scoop*, November 15, 2016; Jeremy Hsu, "U.S. Suspicions of China's Huawei Based Partly on NSA's Own Spy Tricks," *IEEE Spectrum*, March 26, 2014; Stan Schroeder, "CIA, FBI, NSA: We Don't Recommend Huawei or ZTE Phones," *Mashable*, February 14, 2018; The Economist, "The WannaCry Attack Reveals the Risks of a Computerised World," May 20, 2017; Lillian Ablon, Martin C. Libicki, and Andrea A. Golay, *Markets for Cybercrime Tools and Stolen Data* (Santa Monica: Rand Corporation, 2014), ix, 370.

היכולת הנדרשת כדי לחדור ליעדים מוגנים היטב. לשם כך נדרשת יכולת להקים צוותים מקצועיים רבים בעלי מגוון מיומנויות המסוגלים לפתח תקיפות על מערכות יעד ספציפיות. זהו תהליך עתיר משאבים וזמן.[12]

ארגוני טרור משתמשים בסייבר לתכנון מבצעי, לגיוס אנשים, להדרכה, לגיוס כספים, לתקשורת, לריגול, לתעמולה ולמבצעי תודעה. אל־קאעדה, דאעש וארגוני טרור אחרים הצהירו מפורשות על רצונם להשתמש בתקיפות סייבר כדי לגרום לנזק פיזי ישיר.[13]

מה מייחד את הסייבר?

תחילה כמה הגדרות קצרות.

תקיפות על רשתות מחשבים (Computer Network Attacks, CNA) משבשות מערכות ורשתות מחשב, פוגעות בהן, מונעות גישה אליהן, משחיתות ואפילו משמידות אותן (כלומר חבלת סייבר), ועשויות לשמש למטרות הרתעה.

תקיפות לניצול רשתות מחשבים (Computer Network Exploitation, CNE) חודרות בחשאי למערכות מחשב ותקשורת כדי לאסוף מידע, לשנות או למחוק אותו (כלומר ריגול סייבר), ומשמשות למבצעי מודיעין ולדיכוי התנגדות פנימית.

תקיפות השפעה על רשתות מחשבים (Computer Network Influence, CNI), נקראות גם "מבצעי תודעה בסייבר", פועלות על מידע ועל אמצעי תקשורת כדי להשפיע על תפיסותיהם של יחידים, של קבוצות או של הציבור הרחב, בתוך המדינה או מחוצה לה. הן יכולות לשמש לקידום מטרות פוליטיות, לשיבוש מערכות בחירות ואף לערעור הלגיטימיות והיעילות של ממשלה.

12 Herbert S. Lin, "Offensive Cyber Operations and the Use of Force," *Journal of National Security Law and Policy* 4, no. 63 (2010): 66; Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no. 3 (2013): 378–379, 396–397; Ivanka Barzashka, "Are Cyber-Weapons Effective?" *The RUSI Journal* 158, no. 2 (2013): 51; Trey Herr, "PrEP: A Framework for Malware & Cyber Weapons," *Cyber Security Policy and Research Institute*, George Washington University (March 12, 2014): 8.

13 Lin, "Offensive Cyber Operations," 66; Lindsay, "Stuxnet and the Limits of Cyber Warfare," 378–379, 396–397; Barzashka, "Are Cyber-Weapons Effective?" 51; Herr, "PrEP," 8; Michael Kenney, "Cyber-Terrorism in a Post-Stuxnet World," *Orbis* 59, no. 1 (2015): 123; Yoram Schweitzer, Gabi Siboni, and Einav Yogev, "Cyberspace and Terrorist Organizations," *Military and Strategic Affairs* 5, no. 3 (2013): 21.

מבחינות רבות תקיפות סייבר דומות לתקיפות קינטיות בעולם הפיזי, ואפשר להתמודד איתן באמצעות יישום גישות ואסטרטגיות דומות. עם זאת, לתקיפות סייבר יש כמה מאפיינים שבגינם ראוי לראות בהן תחום נפרד של עימות המחייב טיפול שונה.

הבדל חשוב ראשון בין תקיפות קינטיות לתקיפות סייבר הוא המהירות שבה הן מתרחשות. תקיפות סייבר מתרחשות כהרף עין, דבר שמקשה על הכנת הגנות מפניהן, מלבד הגנות אוטומטיות, ומונע ממקבלי ההחלטות את הזמן הדרוש לגיבוש תגובה שקולה. מנגד, כמה מן השלבים של תקיפות סייבר מתוחכמות מתחוללים במהירות של בני אנוש, לאורך חודשים ואף שנים, ובכלל זה תכנון התקיפות, איסוף מודיעין, פיתוח קוד מותאם למערכות יעד ספציפיות והיערכות מבצעית.[14]

גם למדינות חזקות ומתקדמות טכנולוגית אין מונופול על השימוש בכוח בסייבר. תקיפות קינטיות יכולים לבצע שחקנים מדינתיים או ארגוני טרור; כל מי שמצויד במחשב יכול לבצע תקיפת סייבר ולגרום ולו למידה מסוימת של נזק. חלק מיכולות המחשוב המתקדמות ביותר, שבעבר היו שייכות אך ורק לשחקנים מדינתיים ולתאגידים גדולים, נגישות כעת לכול. מדינות חלשות או שחקנים לא מדינתיים בעלי ממון יכולים לפתח יכולות סייבר צבאיות עוצמתיות ולהשיג תוצאות חסרות תקדים.[15]

בניגוד לכל כלי הנשק האחרים, קונוונציונליים או לא קונוונציונליים, לאמצעי הלחימה בסייבר אין מגבלות גיאוגרפיות ואין אילוצי זמן ומרחב. אפשר לשגר אותם בו־זמנית ברחבי העולם נגד מספר בלתי מוגבל של מטרות ולחצות באמצעותם גבולות בלי שמדינות ידעו אפילו שהרשתות שלהן נפרצו ושריבונותן הופרה.[16]

14 Clarke and Knake, *Cyber War*, 31; Ben Buchanan *The Cyber Security Dilemma: Hacking, Trust, and Fear between Nations* (New York: Oxford, 2017), 42.

15 Lucas Kello, "The Meaning of the Cyber Revolution," *International Security* 38, no. 2 (2013): 36; Jonathan Silber, "Cyber Vandalism – Not Warfare," *Ynet*, January 26, 2012; R. Bebber, "Information War and Rethinking Phase 0." *Journal of Information Warfare* 15 no. 2 (2016): 39–52; F. J. Cilluffo and J. R. Clark, "Building a Conceptual Framework for Cyber's Effect on National Security," *Journal of Information Warfare* 15, no. 2 (2016): 7; Segal, *Hacked World Order,* 12.

16 Eviatar Matania, Lior Yoffe, and Michael Mashkautsan, "A Three Layer Framework for a Comprehensive National Cyber-Security Strategy," *Georgetown Journal of International Affairs* 27, no. 3 (2016): 77–84; Clarke and Knake, *Cyber War*, 31; Kello, "The Meaning of the Cyber Revolution," 22.

לכל מערכות הנשק, אפילו הגרעיניות, יש השפעה מקומית בלבד; אולם לתקיפות סייבר עשויה להיות השפעה מערכתית או כלל־ארצית. תקיפה קינטית מצד שחקן מדינתי או לא מדינתי עלולה להשמיד בנק, בית חולים, מכ"ם או מתקן תקשורת צבאי. תקיפת סייבר, לעומת זאת, עלולה להפיל מערכת פיננסית או מערכת בריאות שלמה, לקלקל ולשבש את מערכות ההתרעה המוקדמת ואת מערכות הפיקוד והשליטה של האויב ולפגוע ביכולתו להגיב. שיבוש כלל־ארצי או אפילו אזורי בלבד של רשת החשמל של היריב עלול לגרום לכאוס חברתי, כלכלי וצבאי.[17]

בניגוד לתקיפות קינטיות, נדיר שתקיפות סייבר יגרמו לנזק פיזי ישיר או לאובדן חיים, וריגול סייבר יכול להתבצע מרחוק בלי לסכן את חיי המרגלים. את רמת הדיוק של נשק הסייבר קשה להשיג בתקיפות קינטיות, ולכן אפשר למזער את הנזק היקפי שלו גם כאשר המטרות נמצאות בלב אוכלוסייה אזרחית. אפשר לתכנן מראש שההשפעות של נשק הסייבר יהיו זמניות או הפיכות. עם זאת, ההשפעות העקיפות של נשק הסייבר עלולות לגרום לנזק פיזי וקטלני נרחב.[18]

ייחוס תקיפה קינטית לשחקן מדינתי או לא מדינתי הוא בדרך כלל פשוט וברור. תקיפות סייבר אפשר להסוות ביתר קלות, ואפשר להסב באמצעותן נזק בלי להשאיר עקבות. אפשר שהיעד לתקיפה אפילו לא ידע שהותקף. עם זאת, מדינות ואפילו חברות פרטיות שיפרו מאוד בשנים האחרונות את יכולות המודיעין הטכנולוגיות והפורנזיות שלהן, ובעקבות זאת את היכולת שלהן לזהות מי עומד מאחורי מתקפה.[19]

17 Constance Douris, "Cyber Assault on Electric Grid Could Make U.S. Feel Like Post-Hurricane Puerto Rico," *Forbes*, February 6, 2018.

18 Thomas Rid, *Cyber War Will Not Take Place (*London: C. Hurst and Co, 2013), viii; Jan Trobisch, *Challenges in the Protection of US Critical Infrastructure in the Cyber Realm* (School of Advanced Military Studies, US Army Command and General Staff College, Fort Leavenworth, KS, 2014), 4; David E. Sanger, "Why Hackers Aren't Afraid of Us," *New York Times*, June 16, 2018; George Perkovich and Ariel (Eli) Levite, eds. *Understanding Cyber Conflict: 14 Analogies* (George University Press, 2017), 45, 116; Michael P. Fischerkeller and Richard J. Harknett, "Deterrence is Not a Credible Strategy for Cyberspace," *Orbis* 61, no. 3 (2018): 382.

19 Shmuel Even and David Siman-Tov, *Cyber Warfare: Concepts and Strategic Trends*, Memorandum No. 117 (Tel Aviv: INSS, 2012), 32–33; Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Rand Corporation, 2009), xiv-xv; Clarke and Knake, *Cyber War,* 45, 51; Silber, "Cyber Vandalism – Not Warfare"; Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks." *The Journal of Strategic Studies* 38, no. 1–2 (2015): 7.

כלי הנשק הקונוונציונליים והבלתי קונוונציונליים יכולים לשמש נגד מגוון רחב של מטרות, אולם נשק סייבר מתוחכם (שאינו אלא קוד מחשב) מיועד לתקוף מטרה מסוימת, ודי בשינויים קלים במטרה כדי שיהפוך לחסר תועלת. לדוגמה, קוד שפותח כדי לתקוף מערכת טילי קרקע־אוויר מסוימת לא יועיל נגד מערכת אחרת מאותו סוג או נגד מערכת טילי אוויר־אוויר.[20]

בעבר נאלצו סוכנויות ביון להתאמץ ולהסתכן כדי לאסוף מידע מסווג ואפילו לא מסווג. כיום, בעזרת מערכות נתוני עתק (ביג דאטה), הן מסוגלות לעבד כמויות אדירות של מידע לא מסווג; כל פרט מפרטיו אולי שולי, אך מכולם יחד אפשר להפיק מידע חיוני. מדינות רבות מנהלות זה מכבר מבצעי תודעה; הסייבר מציע מגוון פלטפורמות שאפשר להגיע דרכן ישירות, מיידית ובזול למספר עצום של אנשים ברחבי העולם או לקהלים ממוקדים במיוחד.

20 Martin C. Libicki, "Second Acts in Cyberspace," in *Bytes, Bombs and Spies: The Strategic Dimensions of Offensive Cyber Operations*, ed. Herbert Lin and Amy Zegart (Brookings, 2019), 137; Austin Long, "A Cyber SIOP? Operational Considerations for Strategic Offensive Cyber Planning," in *Bytes, Bombs and Spies: The Strategic Dimensions of Offensive Cyber Operations*, ed. Herbert Lin and Amy Zegart (Brookings, 2019), 121.

חלק 2

אסטרטגיית הסייבר של איראן, המוסדות והיכולות

בתחילת העשור השני של המאה ה־21 הובילו שני גורמים מרכזיים את איראן להאיץ את פיתוח יכולות הסייבר שלה, שעד אז היו מוגבלות. הראשון היה השימוש האפקטיבי של האופוזיציה באינטרנט שנועד לעורר ולשמר לאורך זמן את המחאות ההמוניות בעקבות זיוף הבחירות לנשיאות ב־2009. המשטר הצליח בסופו של דבר לדכא את ההפגנות, אך גם קיבל הוכחה ברורה לאיום שהטכנולוגיה החדשה מציבה למעמדו וליציבותו.[21] הגורם השני היה תקיפת הסטקסנט הדרמטית נגד תוכנית הגרעין של איראן ב־2010, שלפי דיווחים הייתה מבצע חבלת סייבר אמריקני־ישראלי משותף. סטקסנט הייתה תקיפת הסייבר הראשונה הידועה שגרמה לנזק פיזי, והיא המחישה את הפגיעות הרבה של איראן ועוררה זעזוע לאומי עמוק. בתגובה האיצה איראן את פיתוח יכולות הסייבר שלה, שעד אז היו בסיסיות בלבד.[22]

מומחים מסכימים כי יכולות הסייבר של איראן התקדמו מאז במידה ניכרת, אך חלוקים בשאלת רמת התחכום שלהן בפועל. יש הסוברים שאיראן לא פיתחה מערכת אבטחת סייבר אקולוגית מתוחכמת, שהיא סובלת מבריחת מוחות חמורה ושהיא לא הגיעה לרמת המקצועיות המצופה משחקנית מתקדמת. מומחים אלה מאמינים כי המטרות האמריקניות, האירופיות והישראליות החשובות מוגנות ברמה העולה על יכולותיה של איראן. יש הסוברים גם שרמת התחכום של הגנת הסייבר בישראל מפחיתה את יכולתה של איראן להסב לה פגיעה קשה, ושאיראן היא עדיין מעצמת סייבר ממעגל שלישי. טענה זו, אם היא נכונה,

21 Collin Anderson and Karim Sadjadpour, *Iran's Cyber Threat: Espionage, Sabotage and Revenge* (Carnegie Endowment for International Peace, 2018), 10–11; Gabi Siboni and Sami Kronenfeld, "Iran and Cyberspace Warfare," in *Cyberspace and National Security – Selected Articles*, ed. Gabi Siboni (Tel Aviv: Institute for National Security Studies, 2013), 81–103; Kristina Kausch and Lior Tabansky, "Cybered Conflict in the Middle East," Mediterranean Dialogue Series No. 15 (Konrad Adenauer Stiftung, 2018), 9; Gabi Siboni, Léa Abramski, and Gal Sapir, "Iran's Activity in Cyberspace: Identifying Patterns and Understanding the Strategy," *Cyber, Intelligence and Security* 4, no. 1 (2020): 22.

22 Sanger, *The Perfect Weapon,* 46–49; Segal, *Hacked World Order*, 5; Sam Jones, "Cyber Warfare: Iran Opens a New Front," *Financial Times*, April 26, 2016; Siboni and Kronenfeld, "Iran and Cyberspace Warfare."

יכולה להסביר מדוע עד היום התמקדו רוב התקיפות האיראניות ב"מטרות קלות", כלומר תקפו אתרים שהגנתם חלשה באמצעים שאינם מתוחכמים דיים.[23]

מומחים אחרים מעריכים שאיראן נמנית כעת עם מובילות המעגל השני של מעצמות הסייבר העולמיות, ושואפת להצטרף למובילות המעגל הראשון. הערכת האיומים הכלל־עולמיים של ארצות הברית לשנת 2022 קבעה כי "המומחיות והנכונות הגוברות של איראן לנהל מבצעי סייבר אגרסיביים הופכות אותה לאיום גדול על אבטחת הרשתות והנתונים של ארצות הברית ושל בעלות בריתה".[24] לדברי ראש מערך הסייבר הלאומי של ישראל לשעבר, איראן היא אחת מחמש המדינות הפעילות ביותר בתחום הסייבר ואחת הבודדות שמבצעות תקיפות לא רק למטרות מודיעין והשפעה, אלא גם לשם הרס.[25]

התומכים בגישה זו טוענים שאיראן השקיעה רבות במערכת הסייבר האקולוגית שלה, ובכלל זה בתי ספר ואוניברסיטאות. על פי דיווחים, עד שנת 2016 השקיעה איראן יותר ממיליארד דולר בשנה ביכולות הסייבר שלה, לעומת שני מיליארד הדולר שהשקיעה בריטניה, אחת ממעצמות הסייבר המובילות בעולם. לפי נתונים איראניים, תקציב הסייבר של איראן זינק פי 12 בשנים 2013–2021, ותוכנית חומש שנידונה ב־2020 העלתה את האפשרות להגדיל עוד את הכלכלה הדיגיטלית של איראן מ־6.5 אחוזים מן התמ"ג ל־10 אחוזים עד שנת 2025. לפי דיווחים, בסוף העשור השני של המאה ה־21 למדו כ־18 אחוזים מן הסטודנטים האיראנים מדעי המחשב, ושירות צבאי חובה שימש אמצעי לתעל בוגרים בעלי ידע טכנולוגי למנגנוני הביטחון של המדינה, ובהם משרד המודיעין ומשמרות המהפכה.[26]

23 Anderson and Sadjadpour, *Iran's Cyber Threat,* 13, 14, 31, 35–36, 52; International Institute for Strategic Studies, "Cyber Capabilities and National Power: A Net Assessment," Research Papers (June 28, 2021); David Shamah, "Official: Iran, Hamas Conduct Cyber-Attacks Against Israel," *Times of Israel*, August 13, 2015.

24 Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," (2022), 1.

25 Siboni, Abramski, and Sapir, "Iran's Activity in Cyberspace," 22; Robert McMillan, "Iranian Hackers Have Hit Hundreds of Companies in Past Two Years," *Wall Street Journal*, March 6, 2019; Jones, "Cyber Warfare"; Office of the Director of National Intelligence. "Annual Threat Assessment of the US Intelligence Community," (2021), 14.

26 Jones, "Cyber Warfare"; Siboni, Abramski, and Sapir, "Iran's Activity in Cyberspace," 22; International Institute for Strategic Studies, "Cyber Capabilities"; Pierre Pahlavi, "Digital Hezbollah and Political Warfare in Cyberspace," *National Interest*, October 31, 2022; Michael Sulmeyer, *Cyberspace: A Growing Domain for Iranian Disruption* (Washington DC: Center for Strategic and International Studies, 2017), 38.

בשנת 2012 הייתה איראן אחת המדינות הראשונות שהקימו את המוסדות הדרושים ליישום אסטרטגיית סייבר לאומית. "מועצת מרחב הסייבר העליונה" (Supreme Cyber Space Council) הופקדה על התכנון והיישום של אסטרטגיית סייבר לאומית משולבת.[27] "מרכז הסייבר הלאומי" (National Cyber Center) מרכז את פעילות הסייבר הכוללת של איראן, אוסף ומפיץ מידע רלוונטי והנחיות מדיניות ומפקח על יישום המדיניות. "הארגון הלאומי להגנה פסיבית" (National Passive Defense Organization) אחראי על הגנת תשתיות לאומיות חיוניות, ו"פיקוד הגנת הסייבר" (Cyber Defense Command) מרכז את מבצעי הסייבר של הצבא (ארטש). "מרכז מאהר לאבטחת מידע" (Maher Information Security Center) הוא צוות החירום של איראן לענייני מחשוב. "הוועדה לזיהוי אתרים לא מורשים" (Committee for Identifying Unauthorized Sites) ו־FATA (ראשי תיבות בפרסית של "משטרת ייצור והחלפת מידע") פועלים כמשטרת סייבר ומנטרים את השימוש באינטרנט כדי לדכא התנגדות מקומית ולמנוע פשעי סייבר.[28] מלבד כל הגופים הללו פועלים גם "משרד המודיעין והביטחון" (Ministry of Intelligence and Security) הוותיק, האחראי על מודיעין אותות, ו"משרד טכנולוגיות המידע והתקשורת" (Ministry of Information and Communication Technology).

לפי דיווחים, עד שנת 2015 גייסו משמרות המהפכה אלפי עובדים לשורותיהם, והפכו לשחקן הסייבר הבולט באיראן. "הארגון ללוחמה אלקטרונית ולהגנת סייבר" הוא האחראי העיקרי על מבצעי הסייבר ההתקפיים. משמרות המהפכה גם מספקים הכוונה מבצעית ותומכים במבצעי הסייבר של ארגוני השלוחים של איראן כגון חזבאללה.[29]

27 עם חברי המועצה נמנים, בין השאר, הנשיא, יושב ראש הפרלמנט, ראש רשות השידור של הרפובליקה האסלאמית של איראן, מפקד הצבא, מפקד משמרות המהפכה, שר ההגנה ושר טכנולוגיות המידע והתקשורת.

28 Congressional Research Service, "Iranian Offensive Cyber Attack Capabilities" January 13, 2020; Jordan A. Brunner, "The (Cyber) New Normal: Dissecting President Obama's Cyber National Emergency," *Jurimetrics Journal* 57 no. 3 (2017): 397–431; Ersin Cahmutoğlu, *Iran's Cyber Power* (Ankara: iRAM: Center for Iranian Studies, April 2021), 14–15; Giacomo Spadoni, "IRGC Cyber-Warfare Capabilities," (International Institute for Counterterrorism, 2019).

29 Congressional Research Service, "Iranian Offensive Cyber Attack Capabilities"; Brunner, "The (Cyber) New Normal"; Siboni and Kronenfeld, "Iran and Cyberspace Warfare," 82, 87–88; Cahmutoğlu, *Iran's Cyber Power*, 14–15.

הבסיג׳, כוח צבאי למחצה הכפוף למשמרות המהפכה ואחראי על הסדר הפנימי, הצהיר שאלף גדודי סייבר פזורים ברחבי המדינה. הבסיג׳ מפקיד את העיסוק בתקיפות סייבר בידי כחמישים קבוצות האקטיביסטיות (hacktivists) עצמאיות המתחרות זו בזו על זכייה במכרזי הסייבר של הבסיג׳, ולכל אחת מהן דרכי פעולה ומטרות משלה. כמה מן הקבוצות המוכרות יותר הן ״צבא הסייבר האיראני״, ״קבוצת ההתנגדות של הסייבר האסלאמי״ ו״צוות האבטחה הדיגיטלית אשייאן״. דוגמאות אחרות הן קבוצות ה״חתלתולים״.[30] קבוצת Flying Kittens אוספת מידע מודיעיני על ממשלות זרות ועל תאגידים חשודים; קבוצת Magic Kittens מתמקדת במתנגדים מקומיים; קבוצת Domestic Kittens עוקבת אחר מתנגדי משטר באיראן, בארצות הברית, בבריטניה ובמקומות אחרים; קבוצת Charming Kittens משתמשת בפלטפורמות של הרשתות החברתיות כדי להגיע למטרות כאלה ואחרות; וקבוצת Cutting Kittens מייצרת כלי חדירה לאתרים. את פעילויות הסייבר של הבסיג׳ מתאמת ״מועצת הסייבר של הבסיג׳״. את כמה מן הפעילויות הללו מבצעים שלושה ״מכונים״: מבנא (Mabna), רנא (Rana) ונסר (Nasr). מכון מבנא מסייע לאוניברסיטאות איראניות ולארגוני מדע ומחקר לקבל גישה למשאבים מדעיים זרים.[31]

כמו בתחומים אחרים של לוחמה אסימטרית איראן נוקטת מגוון אמצעים כדי להסוות את פעולות הסייבר שלה ולשמר יכולת הכחשה. נוזקה שתיוחס בפומבי לאיראן תינטש קרוב לוודאי בעקבות החשיפה. החברות בקבוצות שתוארו לעיל משתנה ללא הרף, ולכן הגבולות ביניהן מיטשטשים. על פי דיווחים, משמרות המהפכה מעסיקים מתווכים מהימנים ומוציאים דרכם חוזים למיקור חוץ כדי להסוות טוב יותר את עקבותיהם; לעיתים מועסקים כמה קבלנים באותו מבצע. מבנה הפיקוד של משמרות המהפכה, הבסיג׳ וקבוצות ההאקטיביסטים הוא נזיל, ולכן פעילותם בלתי צפויה וקשה במיוחד להערכה. הערפול מחריף עוד יותר בגלל אי־השקיפות המאפיינת את תהליכי קבלת ההחלטות באיראן ואת דרכי השליטה של

30 את השמות של קבוצות ה״חתלתולים״, כמו את השמות של רוב מתקפות הסייבר, נתנו חברות אבטחת הסייבר העולמיות המובילות, והם משמשים אמצעי זיהוי. רוב הקבוצות הללו מוכרות גם בשמות אחרים. Charming Kittens לדוגמה מכונים גם APT 35, ולקבוצות אחרות יש מספרי APT שונים. Static Kittens ידועים גם בשם MuddyWater.

31 Jones, ״Cyber Warfare״; Congressional Research Service, ״Iranian Offensive Cyber Attack Capabilities״; Anderson and Sadjadpour, *Iran׳s Cyber Threat,* 17; International Institute for Strategic Studies, ״Cyber Capabilities and National Power״; Tom Brewster, ״Persian Paranoia: America׳s Fear of Iranian Cyber Power,״ *The Guardian*, August 29, 2014; Cahmutoğlu, *Iran׳s Cyber Power*, 15; Gordon Corera, ״Iran ׳Hides Spyware in Wallpaper, Restaurant and Games Apps,׳״ *BBC News*, February 8, 2021.

המשטר על מנגנוני הביטחון. נראה שקבוצות ההאקטיביסטים נהנות לכל הפחות מאישור שבשתיקה של הממסד הפוליטי והביטחוני.[32]

אסטרטגיית הסייבר של איראן התפתחה בשלושה שלבים עיקריים. בשלב 1, בשנים 2009–2011, נשמעה קריאת ההשכמה והופעלה התגובה הראשונית להפגנות בעקבות בחירות 2009 ולתקיפת סטקסנט בשנה שלאחר מכן. בשלב 2, בשנים 2012–2018, הוקמו מוסדות הסייבר שפורטו לעיל, התחיל שיתוף הפעולה בתחום הסייבר עם רוסיה ועם סין, והחל מעבר ממבצעי סייבר הגנתיים ברובם למבצעים התקפיים, בעיקר למטרות מודיעין. בשלב 3, משנת 2019 ואילך, בנתה איראן בנק מטרות ובו תשתיות ויעדים ביטחוניים ואחרים ברחבי העולם, והוסיפה להרחיב את המבצעים ההתקפיים, בפרט את מבצעי התודעה, ובמקרים רבים את התקיפות המשלבות CNA, CNE, CNI וכופרה.[33] כפי שיוצג להלן, רבות מפעילויות הסייבר של איראן לאורך השנים היו בעלות אופי תגובתי, תגובות לתקיפות שהיא ייחסה לישראל או לארצות הברית.

מבחינתה של איראן, ארצות הברית מציבה את האיום הגדול ביותר על ביטחונה הלאומי ואת האיום הקיומי היחיד על עתיד הרפובליקה האסלאמית. ישראל נחשבת לאיום חמור ופעיל במיוחד, אך לא קיומי.[34] מדינות אחרות באזור, בייחוד במפרץ, נחשבות גם הן לאיומים משמעותיים, אף שהם התמתנו במידת מה בזכות הירידה במתיחות באביב 2023. תפיסת האיום של איראן ואסטרטגיית הביטחון הלאומי שלה נטועות בתחושה עמוקה של חולשה ופגיעות הנובעת מן הפרקים הכושלים בהיסטוריה האיראנית והפרסית ומן ההכרה כי היכולות הקונוונציונליות המוגבלות שלה אינן משתוות ליכולותיהן של יריבותיה הגדולות.

תחושה עמוקה זו של חולשה הובילה להחלטה לא רק להרתיע את אויבי איראן ולהתגונן מפניהם, אלא גם לפתח יכולות התקפיות אפקטיביות שבאמצעותן היא תוכל לקדם את האינטרסים שלה ולהרחיב את השפעתה מחוץ לגבולותיה. לוחמה אסימטרית הפכה זה

32 Jones, "Cyber Warfare"; Sulmeyer, *Cyberspace*, 39; Dorothy Denning, "Explainer: How Iran's Military Outsources its Cyberwarfare Forces," *Navy Times*, January 23, 2020; Anderson and Sadjadpour, *Iran's Cyber Threat,* 13.

33 Danny Citrinowicz and Jason Brodsky, "Iran's Cyberspace Evolution," *The Dispatch*, April 12, 2022; Boaz Dolev and David Siman-Tov, "Iranian Cyber Influence Operations Against Israel Disguised as Ransomware Attacks," Special Publication, *INSS*, January 27, 2022.

34 Ali Akbar, "Iran's Regional Influence in Light of its Security Concerns," *Middle East Policy* 28 no. 3–4 (2021); Raz Zimmt, "The Israeli Threat—The View From Iran," *Bein HaKtavim*, Dado Center for Interdisciplinary Military Research, forthcoming fall 2023.

מכבר למרכיב חיוני באסטרטגיית הביטחון הלאומי של איראן. היא נועדה לקזז את יתרון הכוח של יריבותיה, והסייבר זכה לתפקיד חשוב בה. הסייבר מתאים במיוחד לתרבות האסטרטגית של איראן השמה דגש על עמימות, על יכולת הכחשה ועל שימוש בשלוחים.[35] לשם כך פיתחה איראן יכולות סייבר התקפיות למטרות שיבוש והרס, ריגול ומבצעי תודעה.

בעבור איראן האינטרנט והסייבר הם שילוב של טוב ורע. מצד אחד, הם כלים חתרניים להפצת ערכי המערב והאופוזיציה המקומית ומציבים איומים פוטנציאליים על יציבות המשטר ועל הישרדותו – מטרתו העיקרית של השלטון. מצד אחר, הוכח שהאינטרנט הוא גם אמצעי יעיל לעיצוב דעת הקהל ולשליטה על הציבור. למטרה זו, ובהשראת המודלים הסמכותניים שלה – סין, רוסיה וקוריאה הצפונית – יצרה איראן מכונת תעמולה גדולה ויעילה בסייבר להפצת מדיניות המשטר ועיקרי האמונה השיעית, באיראן ומחוצה לה.[36]

איראן הצליחה להשיג שליטה יעילה למדי על מרחב הסייבר הלאומי שלה. היא חיקתה את המודל הסיני והקימה את "רשת המידע הלאומית" (National Information Network, NIW) – אינטראנט לאומי נפרד. פרויקט NIW החל בשנת 2009, כשהמשטר הנחה חברות מקומיות להתחיל להעביר את פעילות הרשת שלהן לשרתים ולמרכזי נתונים הממוקמים באיראן עצמה; המטרה הסופית הייתה לארח שם את כל האתרים האיראניים. לפי דיווחים, איראן גם פיתחה בעבור NIW שירות דואר אלקטרוני עצמאי, מערכת הפעלה, מנוע חיפוש וכלים אחרים. ה־NIW הושלם רשמית ב־2016, אך העבודה נמשכת ופרויקטים חדשים של תשתית ענן ומרכז נתונים נחנכו בשנת 2020.[37]

35 Ariane M. Tabatabai, *Iran's Authoritarian Playbook: The Tactics, Doctrine, and Objectives behind Iran's Influence Operations* (Washington DC: Alliance for Securing Democracy, 2020), 3, 8; Scott Jasper, *Strategic Cyber Deterrence: The Active Cyber Defense Option* (Rowman and Littlefield, 2017), 41; Kausch and Tabansky, "Cybered Conflict in the Middle East," 8; Micah Loudermilk, "Iran Crisis Moves into Cyberspace." Policy Watch 3151, *Washington Institute for Near East Policy*, July 9, 2019; Siboni and Kronenfeld, "Iran and Cyberspace Warfare," 81–82; Anderson and Sadjadpour, Iran's Cyber Threat, 12.

36 Loudermilk, "Iran Crisis"; Sulmeyer, *Cyberspace*, 34–35; Siboni and Kronenfeld, "Iran and Cyberspace Warfare," 81–103; Siboni, Abramski, and Sapir, "Iran's Activity in Cyberspace," 35.

37 Mahsa Alimardani, "Iran Declares 'Unveiling' of its National Intranet," *Advox*, September 2, 2016; Siboni and Kronenfeld, "Iran and Cyberspace Warfare," 81–103.

ה־NIW מאפשר לאיראן להתמודד ביתר יעילות עם השפעות תרבותיות ופוליטיות זרות, לנטר פעילות זדונית ולזהות את מקורותיה ולהפחית את פגיעותה של איראן לתקיפות סייבר מבחוץ ולהתנגדות האופוזיציה מבית. בשנת 2019, בשיא ההפגנות של אותה שנה – אולי האתגר הגדול ביותר שעמד בפני המשטר עד אז – סגרו באמצעות NIW את הגישה לאינטרנט ברחבי איראן למשך שבוע. בכך הצליח המשטר למנוע מן האופוזיציה גיוס נוסף לשורותיה ולהסתיר עדויות לצעדים החריגים שנקט כדי לדכא את ההתנגדות, לרבות, לפי דיווחים, הרג של מאות וכליאה של אלפים.[38] ה־NIW שימש שוב ובהרחבה לדיכוי המחאות הגדולות אף יותר שפרצו בסוף 2022 בעקבות הריגת צעירה שסירבה לכסות את שערה בחג׳אב כנדרש בחוק האיראני. הגישה לאינטרנט ולסלולר נמנעה ממיליוני איראנים כדי להכשיל את המאמצים לארגן את ההפגנות וכדי להאט את המומנטום שלהן.[39]

איראן מנהלת מבצעי סייבר המקדמים את יעדיה הלאומיים המרכזיים, והיעד החשוב ביותר הוא להבטיח את היציבות ואת אריכות הימים של הרפובליקה האסלאמית. עם יעדיה האחרים נמנים: שמירה על ערכי האסלאם וציוויו; הגנה על שלמותה הטריטוריאלית ועל אוכלוסייתה של איראן; קידום הצמיחה הסוציו־אקונומית ורווחת העם האיראני; הפצת התאולוגיה האיראנית וההשפעה האיראנית ברחבי האזור; השגת הגמוניה אזורית; שמירה על קשרים בינלאומיים חזקים ועל מעמדה כמעצמה עולמית חשובה; הדיפת המאמצים האמריקניים לבלום את איראן, בייחוד בנושא הגרעין; ערעור ההשפעה האמריקנית באזור;[40] בלימה והחלשה של ישראל, ובסופו של דבר השמדתה.

שיתוף פעולה בינלאומי

שיתוף הפעולה עם שחקניות אחרות, בעיקר עם רוסיה וסין, תרם במידה ניכרת ליכולות הסייבר של איראן. בשנת 2015 חתמו רוסיה ואיראן על הסכם שיתוף הפעולה הראשון שלהן בתחום הסייבר, ועד מהרה נחתמו הסכמים נוספים וחשובים יותר. מערכת הגנת

38 Lily Hay Newman, "How the Iranian Government Shut Off the Internet," *Wired*, November 17, 2019; Carol Morello and Missy Ryan, "U.S. Says Iranian Forces May Have Killed More Than 1,000 Protestors," *Washington Post*, December 5, 2019.

39 Vivian Lee, "Despite Iran's Efforts to Block Internet, Technology Has Helped Fuel Outrage," *New York Times*, September 29, 2022; Benoit Faucon, "Iran Restricts Internet Access as Women's Rights Protests Spread," *Wall Street Journal*, September 22, 2022.

40 Tabatabai, *Iran's Authoritarian Playbook*, 3, 6–8; Anderson and Sadjadpour, *Iran's Cyber Threat,* 42.

הסייבר של משמרות המהפכה פותחה, לפי דיווחים, בסיוע רוסי ואולי גם סיני, וייתכן שהיא הפכה למבצעית בשנת 2015.[41] בשנת 2016 הסכימו רוסיה ואיראן לשתף פעולה ב"פירוק המונופול [...] של השליטה המערבית החד־צדדית" בעולם התוכנה, אות אפשרי שאיראן מתעניינת בחלופות הרוסיות ל־Windows ול־Office של מיקרוסופט. במזכר הבנות משנת 2017 שעניינו שיתוף פעולה בתחומי טכנולוגיית מידע ותקשורת (ICT), צוינו "פיקוח על האינטרנט, אבטחת רשת [...] וחיבור בינלאומי לאינטרנט". ביוזמת איראן הוקמה בשנת 2018 ועדה דו־צדדית לשיתוף פעולה בתחום התקשורת כדי להילחם ב"טרור התקשורת המערבית". הוועדה הוקמה בעקבות מזכר הבנות נוסף שהגדיר אמצעים לקידום סיקור תקשורתי הדדי חיובי, להגברת ההפקה המשותפת של תוכן, לשלילת נרטיבים תקשורתיים מערביים ולהרחבת שיתוף הפעולה בעניין אמצעים לקיהול (targeting) של קהלי יעד זרים.[42]

בשנים 2019–2020 הוקמו קבוצות עבודה רוסיות ואיראניות משותפות כדי לספק לאיראן יכולות למעקב אחר אזרחים באמצעות טכנולוגיית זיהוי פנים וטכנולוגיות אחרות, כדי לקדם שיתוף פעולה ברשתות 5G ובפיתוחי בינה מלאכותית וכדי להגדיל את ההשקעות הרוסיות בחברות סייבר איראניות, לרבות השקעות רב־צדדיות אפשריות בשיתוף טורקיה ואזרבייג׳ן. בשנת 2020 הושג הסכם למאבק ב"לחץ המידע הגובר מן המערב [...] שנועד להכפיש את רוסיה ואת איראן".[43]

הסכם דו־צדדי רחב עוד יותר בין איראן לרוסיה "לשיתוף פעולה באבטחת מידע" נחתם בשנת 2021. על פי דיווחים, ההסכם עסק בתחומים הבאים: אבטחת סייבר והעברות טכנולוגיה, לרבות אמצעים לאיתור תקיפות סייבר; דיכוי התנגדות מקומית; תיאום דיפלומטי באו"ם ובפורומים רב־צדדיים אחרים לצורך קידום נורמות סייבר וחוקי סייבר בינלאומיים התואמים את האינטרסים הרוסיים והאיראניים; וכן אספקה אפשרית של תוכנת מעקב רוסית מתקדמת לאיראן לצורך פריצה לטלפונים ולמחשבים של מתנגדים ושל יריבים. אין לכך ראיות ישירות, אולם ההערכה היא כי את כמה מן הטכנולוגיות והמתודולוגיות שרכשה מרוסיה העבירה איראן לחזבאללה ולמיליציות שותפות אחרות.[44]

41 Cyber Threat Brief, *Flash Critic*, November 29, 2015.

42 John Hardie and Annie Fixler, "Russia-Iran Cooperation Poses Challenges for US Cyber Strategy, Global Norms," *C4ISR*, February 8, 2021.

43 Hardie and Fixler, "Russia-Iran Cooperation"; Setareh Behroozi, "We are in Iran for Cooperation, not to Sign Memorandums: Russian Official," *Tehran Times*, June 24, 2019.

44 Omree Wechsler, "The Iran-Russia Cyber Agreement and U.S. Strategy in the Middle East," *Council on Foreign Relations*, March 15, 2021; Morgan Demboski and IronNet Threat

המלחמה באוקראינה הובילה להעמקת שיתוף הפעולה האסטרטגי בין איראן לרוסיה, ולפי כמה מן הדיווחים הוא מקיף גם את תחום הסייבר. הפרטים דלים, ולא ברור עד כמה שיתוף הפעולה הזה חורג מהסכמי עבר. אות אפשרי הוא מעורבותם לכאורה של פצחנים המזוהים עם רוסיה בתקיפות סייבר איראניות נגד ישראל, כגון הקמפיין השנתי #OpIsrael וקמפיין "יום ירושלים האיראני" (ראו להלן).[45]

גם חברות סיניות השקיעו רבות בתשתית הסייבר של איראן. בשנת 2021 חתמו סין ואיראן על הסכם שיתוף פעולה אסטרטגי נרחב ל־25 שנים המספק, בין היתר, סיוע סיני בבניית תשתית טלקומוניקציה 5G באיראן, גישה למערכת הסינית החדשה לניווט לווייני גלובלי "ביידו" (Beidou) וסיוע בהשגת שליטה איראנית רבה יותר על מרחב הסייבר שלה, ככל הנראה באמצעות חיזוק נוסף של רשת NIW. ייתכן שסין גם הסכימה לספק לאיראן יכולות סייבר חדשות, לרבות יכולות הנחוצות לאיסוף מודיעין.[46] חברות סיניות מכרו יכולות צילום ובינה מלאכותית למשמרות המהפכה ולמיליציית הבסיג'. הטכנולוגיה תוכננה במקור לאכיפת חוקי תנועה, אך שינתה ייעוד בעת ההפגנות ההמוניות בסוף 2022 והחלה לשמש את המשטר האיראני באכיפת קוד הלבוש האיראני על נשים, בזיהוי מפגינים ובמעצרם.[47]

45 Research and Intelligence Teams, "Analysis of the Iranian Cyber Attack Landscape," *IronNet*, September 15, 2021; Hardie and Fixler, "Russia-Iran Cooperation"; Dov Lieber, Benoit Faucon, and Michael Amon, "Russia Supplies Iran With Cyber Weapons as Military Cooperation Grows," *Wall Street Journal*, March 27, 2023. Lieber, Faucon, and Amon, "Russia Supplies Iran"; Avi Davidi, "Iranian-Russian Cooperation on Hack Attacks May Challenge Israeli Cyber Supremacy," *Times of Israel*, April 18, 2023.

46 Farnaz Fassihi and Steven Lee Myers, "Defying U.S., China and Iran Near Trade and Military Partnership," *New York Times*, July 11, 2020; Farnaz Fassihi and Steven Lee Myers, "China, With $400 Billion Iran Deal, Could Deepen Influence in Mideast," *New York Times*, March 27, 2021; Eyal Pinko, "Iranians Developing the Cyber Capabilities of Hezbollah," *Israel Defense*, March 30, 2021; Golnaz Esfandiari, "Iran to Work With China to Create National Internet System," *Radio Free Europe, Radio Liberty*, September 4, 2020.

47 Benoit Faucon and Liza Lin, "U.S. Weighs Sanctions for Chinese Companies Over Iran Surveillance Buildup," *Wall Street Journal*, February 4, 2023; Michael Lee, "Chinese Facial recognition Technology Helping Iran to Identify Women Breaking Strict Dress Code: Report," *Fox News*, January 12, 2023.

חלק 3

תקיפות הסייבר הגדולות שביצעה איראן ברחבי העולם

בחלק זה יפורטו התקיפות העיקריות שאיראן ביצעה עד היום נגד מדינות ברחבי העולם. התקיפות נגד ישראל יובאו בחלק הבא.[48]

תקיפות שיבוש והרס (CNA). את כמה מן התקיפות הראשונות שיוחסו לאיראן ביצע "צבא הסייבר האיראני" – קבוצת פצחנים המזוהים עם משמרות המהפכה. בשנת 2009, בתגובה להפגנות ההמוניות שפרצו בעקבות הבחירות לנשיאות שנערכו באותה שנה, ביצע צבא הסייבר האיראני כמה תקיפות של השחתת אתרי אינטרנט ושל מניעת שירות מבוזרת (DDoS) נגד אתרי אינטרנט וכלי חדשות המזוהים עם ארגוני אופוזיציה.[49]

בשנים 2012–2013, ככל הנראה בתגובה למבצע סטקסנט, ביצעה קבוצת פצחנים איראנית תקיפות DDoS נגד 46 מוסדות פיננסיים אמריקניים גדולים, ובהם ג'יי־פי מורגן, צ'ייס, ולס פארגו ואמריקן אקספרס. התקיפות כונו "אבאביל" (Ababil); הן התבצעו ב־176 ימים שונים ונעלו בפני לקוחות את חשבונותיהם. הפגיעה המיידית הייתה בעיקר במוניטין – ירידה באמון הלקוחות ביכולתם של המוסדות המותקפים בפרט ושל מערכת הבנקאות האמריקנית בכלל לספק שירותים פיננסיים מאובטחים. אולם בטווח הארוך המחיר ששילמה תעשיית הפיננסים האמריקנית היה עצום – המוסדות שהותקפו ומוסדות פיננסיים אחרים נאלצו להוציא מיליארדי דולרים על הגנות סייבר מתוחכמות ביותר.[50]

ב־2012 פתחה איראן באחת מתקיפות הסייבר ההרסניות ביותר אי פעם נגד חברת הנפט הלאומית של ערב הסעודית "ארמקו" (Aramco). הווירוס "שאמון" מחק נתונים מ־30 אלף מחשבים ומעשרת אלפים שרתים; הוא השמיד כמעט את כל המידע הארגוני של "ארמקו" והביא את החברה לסף קריסה. עיבוד העסקאות האוטומטי של "ארמקו" הושבת, העובדים נאלצו לעבד ידנית עסקאות נפט בשווי מיליארדי דולרים, ובמשך כמה ימים אף נאלצה החברה לספק נפט בחינם. מתקפה דומה נוהלה זמן קצר לאחר מכן נגד רשות הגז הטבעי של קטר. הווירוס הזדוני "שאמון" צץ לאחר מכן בכמה הזדמנויות:

48 בכמה מן המתקפות המתוארות בחלק זה הייתה גם ישראל יעד לתקיפה, אך משני בחשיבותו.

49 United Against Nuclear Iran, "The Iranian Cyber Threat," (September 2022), 5–8.

50 Sanger, *The Perfect Weapon,* 50; Loudermilk, "Iran Crisis"; United Against Nuclear Iran, "The Iranian Cyber Threat,".

ב־2016 הוא מחק נתונים מאלפי מחשבים בסוכנות התעופה האזרחית של ערב הסעודית ובארגונים אחרים; ב־2017 הוא תקף 15 סוכנויות וארגונים ממשלתיים סעודיים; וב־2018 הוא תקף חברות אנרגייה וטלקומוניקציה וסוכנויות ממשלתיות.[51]

ב־2013 הצליחו האיראנים להשתלט על שערי ההצפה של סכר בניו יורק. אף על פי שלאחר מכן נמצא כי התקיפה השיגה תוצאה מוגבלת בלבד, היא עוררה בשעתה דאגה עמוקה מיכולתה של איראן לפגוע בתשתיות חיוניות, והייתה לה השפעה ניכרת על החשיבה האמריקנית. בשנת 2021 הסיק המודיעין האמריקני שאיראן אכן פיתחה יכולת לנהל תקיפות אפקטיביות נגד תשתיות חיוניות בארצות הברית.[52]

הסכם המעצמות על תוכנית הגרעין האיראנית מ־2015 (JCPOA) היה יעד בפני עצמו לפעילות סייבר איראנית. לפי דיווחים, קודם לחתימה עליו תכננה איראן תקיפות נגד רשתות חשמל, מפעלי מים, מערכות תחבורה, מוסדות פיננסיים ויעדים נוספים באירופה ובארצות הברית.[53] תקיפה אחרת השמידה נתונים ברשתות של קזינו בלאס וגאס; בעליו הוא יהודי אמריקני ידוע התומך בישראל וביקר בגלוי את הסכם הגרעין. הפרישה של ארצות הברית מן ההסכם ב־2018 ובעקבותיה מדיניות ה"מקסימום לחץ" על איראן האיצו את חידוש התקיפות, בהן תקיפות שמחקו נתוני מחשב ביותר מ־200 חברות תשתית, תעופה, ייצור והנדסה בארצות הברית, בבריטניה, בגרמניה, בערב הסעודית, בהודו ובמדינות אחרות.[54]

51 Sanger, *The Perfect Weapon,* 51–52; Reuters, "Aramco Says Cyberattack Was Aimed at Production," *New York Times*, December 9, 2012; Sulmeyer, *Cyberspace*, 37; Denning, "Explainer"; U.S. Cyberspace Solarium Commission, *Report*, 12; Siboni, Abramski, and Sapir, "Iran's Activity in Cyberspace," 22.

52 Shimon Prokupecz, Tal Kopan, and Sonia Moghe, "Former Official: Iranians Hacked into New York Dam," *CNN*, December 22, 2015; Dustin Volz and Jim Finkle, "U.S. Indicts Iranians for Hacking Dozens of Banks, New York Dam," *Reuters*, March 24, 2016; Sanger, *The Perfect Weapon,* 47–48; Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," (2021), 14.

53 Siboni and Kronenfeld, "Iran and Cyberspace Warfare," 31; Siboni, Abramski, and Sapir, "Iran's Activity in Cyberspace," 22; Brewster, "Persian Paranoia,"; Courtney Kube, Carol E. Lee, Dan De Luce, and Ken Dilanian, "Iran Has Laid Groundwork for Extensive Cyberattacks on U.S., Say Officials," *NBC News*, July 20, 2018.

54 Anderson and Sadjadpour, *Iran's Cyber Threat,* 40; Tabatabai, *Iran's Authoritarian Playbook,* 17; McMillan, "Iranian Hackers Have Hit Hundreds of Companies"; Loudermilk, "Iran Crisis"; Nicole Perlroth, "Chinese and Iranian Hackers Renew Their Attacks on U.S. Companies," *New York Times*, February 18, 2019; Raphael Satter, "AP Exclusive: Iran Hackers Hunt Nuclear Workers, US Targets," *AP*, December 13, 2018.

בשנת 2019, בניסויים שערכו ככל הנראה בנוגע ליכולתם להרחיב את השיבוש וההרס בעתיד, תקפו פצחנים איראנים, על פי החשד, מוסדות של בחריין – הסוכנות לביטחון לאומי, משרד הפנים, משרד סגן ראש הממשלה, רשות החשמל והמים וחברת "אלומיניום בחריין", אחת מענקיות היתוך המתכות בעולם. לפי דיווחים, התקיפות היו דומות לתקיפת הנוזקה "שאמון" נגד חברת "ארמקו" הסעודית. בשנת 2020 תקף וירוס "דסטמן" (Dustman), שדמה גם הוא ל"שאמון", את חברת הנפט הלאומית של בחריין. הפעם רק חלק ממחשבי החברה הושבתו זמנית.[55]

בשנת 2021 תכנן "צוות מודיעין 13", יחידת סייבר איראנית חשאית, תקיפה נגד תשתיות חיוניות של כמה מדינות מערביות. לא ברור אם אכן הייתה כוונה להוציא את התקיפה לפועל באותה עת או רק לאסוף מידע לשימוש עתידי. כמה מן התקיפות המדוברות נועדו לשבש, בין היתר, את המונים האוטומטיים של מכלי תחנות דלק – פגיעה שעלולה הייתה לגרום להתפוצצותם, את מערכות מי הנֵטֶל באוניות משא – פגיעה שעלולה הייתה לגרום לנזק חמור, ואת התקשורת הימית.[56]

בשנת 2021 ניסו פצחנים איראנים לפגוע במערכות מחשב של בית החולים לילדים בבוסטון, אחד המרכזים הגדולים ביותר לרפואת ילדים בארצות הברית. לו הצליחה, הייתה התקיפה עלולה להשפיע על הטיפול הרפואי השוטף ובחירום. המניעים לתקיפה לא היו ברורים, אך ייתכן שהיא הייתה מרכיב בקמפיין כופרה רחב יותר של פצחנים המזוהים עם קבוצת Charming Kittens (APT34). הותקפו גם מאות מטרות בארצות הברית, בבריטניה, באוסטרליה, בקנדה וברוסיה, ובכלל זה תחנות כוח ואתרי תשתית חיוניים אחרים. נראה כי הקורבנות היו יעדים מזדמנים שמערכות המחשב שלהם נמצאו פגיעות לתקיפות, ולא יעדים שנבחרו בקפידה.[57]

55 Bradley Hope, Warren P. Strobel, and Dustin Volz, "High-Level Cyber Intrusions Hit Bahrain Amid Tensions With Iran," *Wall Street Journal*, August 7, 2019; Catalin Cimpanu, "New Iranian Data Wiper Malware Hits Bapco, Bahrain's National Oil Company," *ZDNet*, January 8, 2020; King Faisal Center for Research and Islamic Studies, *Iran's Cyberattacks Capabilities*, Special Report (January 2020), 31.

56 Yonah Jeremy Bob, "Secret Iran Hacking Plans Against West Revealed – Report," *Jerusalem Post*, July 27, 2021.

57 Dustin Volz, "FBI Chief Blames Iran for Cyberattack on Boston Children's Hospital," *Wall Street Journal*, June 1, 2022; David Braue, "Iranian Hackers Targeting Australian Infrastructure," *ACS*, September 26, 2022; Nassim Khadem, "Australians Urged to be

ניסיונותיה של טורקיה בשנת 2021 לנרמל את יחסיה עם איחוד האמירויות הערביות, עם ערב הסעודית ועם ישראל היו לכאורה המניע לתקיפה מסוג "דיוג ממוקד" (spear phishing) שביצעה קבוצת Static Kittens (מכונה גם MuddyWater) נגד אתרים ממשלתיים ופרטיים חשובים בטורקיה. הודעות טקסט לגיטימיות לכאורה ממשרדי הבריאות והפנים של טורקיה נועדו לפתות את נמעניהן לפתוח קישורים זדוניים. ייתכן שהתקיפות היו המשך לתקיפות קודמות שבוצעו משנת 2015 ואילך נגד חברות חשמל ואוניברסיטאות טורקיות.[58] בשנת 2022 בוצעו כמה תקיפות כופרה איראניות נגד יעדים ממשלתיים ומסחריים בהודו, לרבות נגד מערכות ביטחון, חינוך ובנקאות.[59]

בשנת 2022 המטירה איראן על אלבניה את תקיפות הסייבר ההרסניות ביותר שנוהלו נגד בעלת ברית של נאט"ו מאז התקיפה הרוסית נגד אסטוניה 15 שנים קודם לכן. אלבניה הפכה מושא לזעמה של איראן ב־2014, כאשר הסכימה לבקשת ארצות הברית לתת מקלט לארגון מוג׳אהדין ח׳לק.[60] הפצחנים, ככל הנראה Charming Kittens, כבר הצליחו שנה קודם לכן לחדור לשרתי ממשלת אלבניה, אך בפעם הזאת הפעילו שורה של תקיפות מחיקת מידע שפגעו במערכות המחשב ומחקו מידע השייך לשירותי המודיעין, למשטרה ולמשמר הגבול של אלבניה. זהותם של יותר מאלף מודיעים סמויים של המשטרה הודלפה בטלגרם, וכן נתוני הבנקים האישיים של יותר מ־30 אלף אנשים ותכתובות דואר אלקטרוני של נשיא אלבניה לשעבר.

אלבניה הגיבה בניתוק קשריה הדיפלומטיים עם איראן – המקרה הידוע הראשון של תקיפת סייבר שהובילה לתוצאה כזו. בתגובה הפעילו הפצחנים האיראנים גל תקיפות שני והשביתו מערכות ומחקו מידע המשמש לביקורת גבולות ומכס, לרבות נתונים על כל מי שנכנס לאלבניה או יצא ממנה ב־17 השנים שקדמו לתקיפה. הפצחנים גם הדליפו את השמות, את כתובות הדואר האלקטרוני ואת מספרי הטלפון של 600 קציני מודיעין אלבנים, וכן פרטים על מבצע מודיעין אלבני ותכתובת דואר אלקטרוני בין משרדי ממשלה לשגרירויות של אלבניה. אלבניה שקלה להפעיל, לראשונה על רקע מתקפת סייבר, את

Vigilant Against Continued Cyber Attacks From Iran׳s Regime," *Australian Broadcasting Company*, January 24, 2023.

58 Menkse Tokyay, "Iran-Linked Hacker Group Targets Turkey׳s Cyber Network," *Arab News*, February 17, 2022.

59 Sana Shakil, "Cyber Attacks by Iran Hackers on Rise," *New Indian Express*, March 6, 2022.

60 ארגון אופוזיציה מוביל באיראן שחותר להפלת המשטר.

סעיף 5 של אמנת נאט"ו, שעניינו הגנה הדדית, אך לבסוף נמנעה מכך. בתחילת 2023, מועד כתיבת שורות אלה, הפריצות האיראניות למערכות אלבניות נמשכות.[61]

תקיפות ריגול (CNE). בשנת 2011 פרצו פצחנים איראנים ל־DigiNotar – הרשות ההולנדית לאימות דיגיטלי. התקיפה אפשרה להם לרגל אחר התקשורת המוצפנת של עשרות אלפי אזרחים איראנים.[62]

ב־2011, ב"מבצע Newscaster", יצרו פצחנים איראנים בטוויטר, בפייסבוק וברשתות חברתיות אחרות פרופילים מזויפים של עיתונאים בעלי קשרים הדוקים לגורמי ממשל. הם גם הקימו אתר חדשות מזויף כדי לאסוף מידע רגיש על יחסי ארצות הברית וישראל, על המשא ומתן שהתנהל אז עם איראן בנוגע לגרעין, על תוכניות פיתוח נשק ועל סוגיות ביטחוניות כלליות. יותר מאלפיים מחשבים נפגעו, רובם בארצות הברית, ובהם מחשבים של מאות אנשי ביטחון בכירים בעבר ובהווה, של אנשי משרד החוץ ושל גורמים רשמיים אחרים. בכירים ביותר מעשר חברות אמריקניות וישראליות המספקות שירותים בתחום הביטחון היו גם הם יעד לתקיפה. התקיפה התגלתה רק ב־2014.[63]

בשנים 2013–2014 השיגה תקיפה איראנית שליטה על 16 אלף מערכות מחשב בארצות הברית, בבריטניה ובמדינות אחרות. תקיפה אחרת פרצה לרשתות של חברות תעופה, חברות אנרגייה וחברות ביטחוניות, ולאינטראנט של הצי וחיל הנחתים האמריקניים.[64]

61 Andrew Higgins, "A NATO Minnow Reels From Cyberattacks Linked to Iran," *New York Times*, February 25, 2023; Maggie Miller, "Albania Weighed Invoking NATO's Article 5 over Iranian Cyberattack," *Politico*, October 5, 2022; United Against Nuclear Iran, "The Iranian Cyber Threat," (September 2022); Mark Pomerleau, "US Cyber Forces Wrap Up Deployment to Albania in Response to Iranian Cyberattacks," *DefenseScoop*, March 23, 2023; Fjori Sinoruka, "FBI: Iranian Hackers Accessed Albanian Systems Over Year Ago," *Balkan Insight*, September 22, 2022; United States Institute for Peace, "Albania Cuts Ties With Iran Over Cyberattack," September 12, 2022.

62 Sue Halpern, "Should the U.S. Expect an Iranian Cyberattack?" *New Yorker*, January 6, 2020.

63 Ellen Nakashima, "Iranian Hackers Are Targeting U.S. officials Through Social Networks, Report Says," *Washington Post*, May 29, 2014; Nicole Perlroth, "Cyberespionage Attacks Tied to Hackers in Iran," *New York Times*, May 29, 2014; Stephen Ward, *Insight Partners*, May 28, 2014; Pierluigi Paganini, "Past and Present Iran-Linked Cyber-Espionage Operations," *InfoSec*, February 20, 2017.

64 Segal, *Hacked World Order*, 151.

בשנים 2013–2017 הצליחו פצחנים איראנים לחדור למערכות המחשב של 320 אוניברסיטאות, רובן בארצות הברית אך כמה מהן גם בישראל. חשבונותיהם של יותר מ־100 אלף אנשי אקדמיה הותקפו, כ־8,000 מהם נפרצו בהצלחה, ונגנבו כמויות אדירות של מידע ושל קניין רוחני.[65] תקיפה אחרת נגד 76 אוניברסיטאות בארצות הברית, בישראל ובמדינות אחרות ניסתה להשיג גישה לקניין רוחני ולמחקרים שעדיין לא פורסמו; היא נחשפה רק ב־2018.[66]

תקיפה אחרת החלה ב־2014 ונמשכה עד לחשיפתה ב־2019. היא השתמשה בהנדסה חברתית כדי לגנוב מידע רגיש מיותר מ־1,800 חשבונות של חברות טכנולוגיה אמריקניות לתעופה, חלל ולוויין.[67] בשנים 2014–2020 בוצע קמפיין ריגול סייבר גדול שעל פי דיווחים היה מסוגל לפרוץ את מערכות ההודעות המוצפנות של וואטסאפ וטלגרם ולעקוב, בין השאר, אחר מתנגדי משטר איראנים ואחר קבוצות אופוזיציה ומיעוטים דתיים ואתניים באיראן, בארצות הברית, בקנדה ובאיחוד האירופי.[68]

בשנת 2015 ניסתה תקיפה המזוהה עם איראן להשיג גישה תמידית למערכות המידע המשמשות את חברי הבונדסטאג הגרמני ואת צוותיהם. ניסיון החדירה השפיע על פעילות הבונדסטאג במשך כמה ימים והניב לתוקפים כמות רבה של מידע. תקיפות אחרות שהתרחשו באותה עת אספו נתונים על תשתית גרמנית חיונית כגון תחנות כוח.[69]

עוד ב־2015, בשיאו של המשא ומתן שהוביל להסכם הגרעין, פרצו פצחנים איראנים לחשבונות הדואר האלקטרוני האישיים של חברי צוות המשא ומתן האמריקני, בכירים אמריקנים אחרים, חברי קונגרס שמתחו ביקורת על איראן ואנשי תקשורת. לאחר פרישת ארצות הברית מן ההסכם ב־2018 הוציאה איראן לפועל מבצעי ריגול בסייבר נגד בכירים

65 U.S. Department of Justice, "Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of The Islamic Revolutionary Guards Corps," Press Release, March 23, 2018.

66 Anthony Cuthbertson, "Iranian Hackers Attack UK Universities to Steal Research Secrets," *The Independent*, August 24, 2018.

67 Rachel Weiner, "Iranian Men Accused of Hacking U.S. Aerospace Companies," *Washington Post*, September 17, 2020.

68 Bergman and Fassihi, "Iranian Hackers Found Way". עם היעדים הבולטים במיוחד נמנו: מוג׳אהדין ח׳לק (MEK); ארגון ההתנגדות הלאומית של אזרבייג׳ן, הפועל למען זכויות המיעוט האזרי הגדול באיראן; תושבי המחוז האיראני הבדלני סיסטן ובלוצ׳סטן; עיתונאי "קול אמריקה" (Voice of America) וארגון זכויות אדם.

69 BBC News, May 13, 2016; Laurens Cerulus, *Politico*, May 22, 2020.

במשרד האוצר, במחלקת המדינה ובמשרד ההגנה האמריקניים שהיו מעורבים בהטלת הסנקציות. היא גם גנבה סודות תאגידיים מ־200 חברות תשתית, תעופה, ייצור והנדסה.[70]

בשנת 2016 הפעילו פצחנים איראנים סדרה של תקיפות נגד ספקים של שירותי אינטרנט ונגד חברות טלקומוניקציה במפרץ הפרסי; מאוחר יותר הן התרחבו ותקפו גם סוכנויות ממשלתיות בארצות הברית וב־12 מדינות באירופה. בשנת 2016 פרץ מכון "מבנא" לרשתות של לפחות 320 אוניברסיטאות ב־21 מדינות, בהן ארצות הברית, אוסטרליה, קנדה, סין, גרמניה, יפן וישראל, ולרשתות של קרוב ל־50 חברות פרטיות ברחבי העולם. התקיפה סיפקה גישה לחומרי מחקר חסויים.[71]

בשנת 2017 פגעו פצחנים איראנים בפרטי הכניסה לחשבונות של אלף חברי פרלמנט בריטים וצוותיהם, של יותר מאלף פקידי משרד החוץ ושל 7,000 שוטרים. אותם פצחנים תקפו את הפרלמנט האוסטרלי ב־2019, כחלק מקמפיין ריגול סייבר רב־שנתי, וכן אתרים ממשלתיים, דיפלומטיים וצבאיים בקנדה ובניו זילנד.[72]

בשנים 2018–2019 התחזו פצחנים המזוהים עם איראן למגייסים ברשת לינקדאין מטעם אוניברסיטת קיימברידג׳ ומוסדות אחרים; הם שלחו "הצעות עבודה" מזויפות לעובדים בממשלות, בחברות תשתית, בחברות אנרגייה ובחברות אחרות ברחבי המזרח התיכון כדי לפתות אותם להוריד תוכנות זדוניות. בשנת 2019 תכנן, ואולי אף ביצע, מכון "רנא" תקיפה על אתרי ההזמנות של חברות תעופה ונסיעות כדי לקבל גישה לרשימות הנוסעים ולנתוניהם האישיים. רוב היעדים היו ככל הנראה איראנים שנחשדו בפעילות נגד המשטר, אך ייתכן שכמה מהם היו ישראלים. גם קבוצת Remix Kittens (APT39) ניהלה תקיפה דומה.[73]

70 Corey Dickstein, "Military Warns of Iranian Hackers Targeting American Troops With Fake Job Website," *Stars and Stripes*, October 4, 2019; Anderson and Sadjadpour, *Iran's Cyber Threat,* 31, 40; McMillan, "Iranian Hackers Have Hit Hundreds of Companies"; Loudermilk, "Iran Crisis"; Perlroth, "Chinese and Iranian Hackers Renew Their Attacks."

71 Spadoni, "IRGC Cyber-Warfare."

72 Perlroth, "Chinese and Iranian Hackers Renew Their Attacks"; Ewen MacAskill, "Iran to Blame for Cyber-Attack on MPs' Emails – British Intelligence," *The Guardian*, October 13, 2017; Steven Erlanger, "British Parliament Hit by Cyberattack, Affecting Email Access," *New York Times*, June 24, 2017; Ken Dilanian, "Iran-Backed Hackers Hit Both U.K., Australian Parliaments, Says Report," *NBC*, February 28, 2019.

73 King Faisal Center for Research and Islamic Studies, *Iran's Cyberattacks,* 34–35, 40.

בשנת 2019 נפרצו מחשבים של ממשלים מקומיים, בנקים ומערכת הדואר בבריטניה, ונגנבה זהותם של אלפי עובדים, אולי כהכנה לחדירה עמוקה יותר ליעדים אלה בעתיד. במתקפה אחרת השתמשה קבוצת Elfin (APT33), המתמחה באתרי אינטרנט בעלי חולשות מוכרות, בתקיפות "דיוג ממוקד" כדי לקבל גישה לפחות לארבעים מוסדות ממשלתיים ומחקריים ולחברות מסחריות ותעשייתיות בערב הסעודית, בארצות הברית ובמקומות אחרים. התקיפות היו ככל הנראה למטרות ריגול, אך ייתכן גם שהיו הכנה לתקיפות הרס עתידיות. בתקיפה אחרת השתלטה קבוצת Elfin על מערכות ארגוניות של שמות דומיין (Domain Name System, DNS)[74] והגיעה דרכן לאלפי עובדים של יצרניות נפט וגז, יצרני ציוד כבד, ספקי תשתיות טלקומוניקציה ואינטרנט וממשלות בערב הסעודית, בגרמניה, בהודו, בבריטניה ובארצות הברית.[75]

בשנת 2019 חסמה מיקרוסופט 99 אתרים ששימשו פצחנים איראנים לביצוע תקיפות CNE רב־שנתיות נגד סוכנויות ממשלתיות, עסקים ואנשים פרטיים בוושינגטון הבירה. באותה שנה ניסו פצחנים איראנים להשיג גישה למערכות המידע של הפנטגון באמצעות הקמת אתר אינטרנט שנועד כביכול לשרת את הצרכים של יוצאי צבא בחייהם האזרחיים, אך למעשה שתל תוכנות זדוניות במחשביהם. החשש של פיקוד הסייבר האמריקני ושל המשרד לביטחון המולדת מפני תקיפות סייבר איראניות נגד מטרות ממשלתיות ומסחריות אמריקניות גבר עד כדי כך שהם פרסמו אזהרה מיוחדת לציבור באמצע שנת 2019.[76]

בשנת 2020, זמן קצר לאחר שארצות הברית חיסלה את קאסם סולימאני, מפקד כוח קודס של משמרות המהפכה, חידשו פצחנים איראנים את ניסיונותיהם לחדור לרשת החשמל של ארצות הברית; קבוצת Refined Kittens (APT33) פתחה בתקיפת ריסוס סיסמאות נגד חברות חשמל, נפט וגז אמריקניות;[77] וקבוצה אחרת הקשורה אליה ניסתה להשיג גישה לחברות דומות באמצעות ניצול נקודות התורפה שלהן ברשת הווירטואלית

74 מרכיב ליבה בתשתית אינטרנט המשמש "ספר טלפונים" של הרשת וחיוני לתפעולה.

75 King Faisal Center for Research and Islamic Studies, *Iran's Cyberattacks,* 36–38, 41.

76 Dickstein, "Military Warns of Iranian Hackers"; Ellen Nakashima and Spencer Hsu, "Microsoft Says it Has Found Iranian Hackers Targeting U.S. Agencies, Companies and Middle East Advocates," *Washington Post*, March 27, 2019; Zak Doffman, "U.S. Military Warns Outlook Users to Update Immediately Over Hack Linked to Iran," *Forbes*, July 3, 2019; U.S. Department of Homeland Security, "CISA Statement on Iranian Cybersecurity Threats," *CISA.gov*, January 3, 2020.

77 בתקיפות ריסוס סיסמאות הפצחנים מנחשים מאות או אלפי סיסמאות נפוצות כדי לפרוץ לחשבונות משתמשים.

הפרטית (Virtual Private Networking, VPN). ייתכן שהתקיפות נועדו להכשיר את הקרקע לתקיפות הרס עתידיות.[78]

בשנת 2020 ביצעה קבוצת Charming Kittens תקיפת דיוג שנועדה להשיג גישה לתכתובות דואר אלקטרוני, לכונני אחסון בענן, ליומנים ולפרטי התקשרות של עשרים אנשים וארגונים. עם יעדי התקיפה נמנו: שני עובדים של ארגון Human Rights Watch, פעילה למען זכויות נשים, פעיל למען פליטים לבנונים, קבוצת אינטרס אמריקנית הפועלת נגד איראן, דיפלומטים, אנשי אקדמיה ופוליטיקאים. אל אחד מעובדי ארגון Human Rights Watch נשלחה הודעת וואטסאפ מזויפת מעובד של מכון מחקר לבנוני. במתקפה נגד קבוצת האינטרס האמריקנית United Against Nuclear Iran הפעילו התוקפים דומיין שהתחזה לדומיין האמיתי של הקבוצה.[79]

כמה תקיפות ריגול סייבר נוספות התרחשו בשנת 2020: נחשף מבצע איסוף מודיעין רב־שנתי שפעל נגד אנשי אקדמיה, חברות נסיעות ותקשורת, אתרים ממשלתיים, מתנגדי משטר ועיתונאים איראנים ביותר מ־30 מדינות בצפון אמריקה, באסיה, באפריקה ובאירופה; פצחנים המזוהים עם איראן גנבו תכתובות סודיות ורגישות מספקים בתחום הביטחון, ממכוני מחקר, מארגונים לא ממשלתיים, מאוניברסיטאות וממממשלות אפגניסטן וערב הסעודית; ופצחנים איראנים פרצו לחשבונות הדואר האלקטרוני של כמה משתתפים חשובים בוועידת מינכן לביטחון, המפגש השנתי המרכזי של גורמי הביטחון הלאומי, ושל משתתפים בפסגת ה־G20, ככל הנראה כדי לאסוף מידע על החשיבה האסטרטגית שלהם. גם חשבון הדואר האלקטרוני של הקנצלרית אנגלה מרקל נפרץ.[80]

78 Andy Greenberg, "Iranian Hackers Have Been 'Password-Spraying' the US Grid," *Wired*, January 9, 2020; Garance Burke and Jonathan Fahey, "AP Investigation: US Power Grid Vulnerable to Foreign Hacks," *Associated Press,* December 21, 2015; Kube, Lee, De Luce, and Dilanian, "Iran Has Laid Groundwork"; Industrial Cyber, "New Dragos report Reveals Iranian Hackers Targeting U.S Power Grid Amid Tensions Between Two Nations," January 13, 2020.

79 Tzvi Joffre, "Iran-Backed Hackers Targeting Activists, Journalists, Politicians – HRW," *Jerusalem Post*, December 5, 2022.

80 Weiner, "Iranian Men Accused of Hacking"; FBI Boston, "FBI Releases Cybersecurity Advisory on previously Undisclosed Iranian Malware Used to Monitor Dissidents and Travel and Telecommunications Companies," September 17, 2020; AP, "Microsoft Says Iranian Hackers Targeted Conference Attendees," October 28, 2020; Kate Connolly, "Russian Hacking Attack on Bundestag Damaged Trust, Says Merkel," *Guardian*, May 13, 2020.

בשנת 2021 הותקפו בשני מבצעי ריגול סייבר 1,200 מתנגדי משטר איראנים, חברי קבוצות אופוזיציה וכורדים באיראן, בארצות הברית, בבריטניה ובמקומות אחרים. על פי דיווחים, המבצע הראשון השתמש באתר בלוג איראני, בערוצי טלגרם ובהודעות טקסט כדי לפתות כ־600 קורבנות משבע מדינות להוריד נוזקה. המבצע השני החל למעשה כבר ב־2007 ובו ריגלו אחר מתנגדי משטר ואחרים ב־12 מדינות, ובהן שוודיה, דנמרק, הולנד, ארצות הברית, עיראק והודו.[81]

אותם פצחנים שבשנים 2018–2019 התחזו בלינקדאין למגייסים מטעם אוניברסיטת קיימברידג׳ כדי לפתות את קורבנותיהם להוריד נוזקות, התחזו בשנת 2021 לעובדים של מגוון חברות – רשתות מלונות, חברות רפואיות, חברות תעופה ועוד – והשתמשו בחשבונות פייסבוק לאותן מטרות. הפצחנים ניהלו קשר ממושך, לעיתים במשך חודשים, עם כמה מן היעדים האמריקניים, הבריטיים והאירופאיים – עדות ברורה למאמץ הרב שנדרש כדי להוציא לפועל את התקיפה.[82] מאוחר יותר באותה שנה הפכו מאמצי ה״גיוס״ האיראניים מסוכנים במיוחד: גרמנים, שוודים והולנדים קיבלו ״הצעות עבודה״ שהיו מצורפות להן נוזקות, אך הפעם חיפשו הפצחנים מומחיות וטכנולוגיות רגישות הדרושות לבניית נשק להשמדה המונית.[83]

בשנת 2021 התחזו פצחנים איראנים לאנשי אקדמיה מאוניברסיטה בריטית מובילה והזמינו מומחים מארצות הברית ומבריטניה לכינוס בנושא ביטחון במזרח התיכון. לחיצה על ״קישור לרישום״ סיפקה לפצחנים גישה למחשבי הקורבנות ומידע על מדיניות החוץ של מדינותיהם, בפרט בכל הנוגע לסוגיית הגרעין האיראני.[84]

בשנת 2022 הצליחו פצחנים המזוהים עם איראן לפרוץ לענף אזרחי בממשל הפדרלי של ארצות הברית, ייתכן שלמחלקה לביטחון המולדת, ככל הנראה כדי לאסוף מודיעין בעבור תקיפות הרס עתידיות. בשנת 2023 הצליחה קבוצת Charming Kittens לחדור

81 Corera, ״Iran ׳Hides Spyware״; Demboski and IronNet Threat Research and Intelligence Teams, ״Analysis of the Iranian Cyber Attack.״

82 Demboski and IronNet Threat Research and Intelligence Teams, ״Analysis of the Iranian Cyber Attack.״

83 Tim Stickings, ״Berlin Security Service Blames Iran for Cyber Attack on German Companies,״ *The National News*, May 12, 2021; Nakashima and Hsu, ״Microsoft Says it Has Found Iranian Hackers.״

84 Demboski and IronNet Threat Research and Intelligence Teams, ״Analysis of the Iranian Cyber Attack.״

לתשתית אמריקנית חיונית, לרבות לנמלי ים ולמערכות תחבורה ואנרגייה. גם במקרה זה ייתכן שהפריצות היו הכנה לתקיפות הרס עתידיות שיבוצעו בבוא העת בתגובה לתקיפות אמריקניות או ישראליות נגד איראן.[85]

ב־2023 התחזו Charming Kittens לחוקרים בריטים בכירים ממכון RUSI (Royal United Services Institute) היוקרתי כדי לבסס קשר עם מומחים לענייני נשק גרעיני ממכוני מחקר אמריקניים. תקיפת הדיוג התמקדה בפחות מעשרה יעדים והתקינה נוזקה במערכות המותקפות; היא הייתה חלק ממבצע לאיסוף מודיעין על תהליך קבלת ההחלטות האמריקני.[86]

ב־2023 סיפקה חברה המזוהה עם איראן שירותי פיקוד ושליטה לעשרים קבוצות פצחנים מסין, מהודו, מקוריאה הצפונית, מפקיסטן, מרוסיה ומוויטנאם, ובכלל זה למפעילי תקיפות כופרה, לסוחרי תוכנות ריגול ולשחקנים מדינתיים.[87] ככל הנראה השירותים סופקו, בין השאר, כדי להשיג מודיעין על פעילות הקבוצות.

פצחנים המזוהים עם משמרות המהפכה פיתחו יישומים מזויפים לטלפונים ניידים המדמים את חנויות היישומים של אפל ושל גוגל (Apple Store, Google Play) כדי להפיץ באמצעותם רוגלות למטרות מעקב אחר התנגדות מקומית ודיכויה. היעדים העיקריים הם איראניים, אך יישומים כאלו עלולים לחשוף מיליוני משתמשים ברחבי העולם למעקב של משמרות המהפכה. יישומי מסרים מזויפים של Kik, של טלגרם ושל PlusMessenger שימשו כדי להשיג נתונים ומסרוני אודיו ווידאו מ־660 מטרות במזרח התיכון, צבאיות ברובן.[88]

85 Carly Page, "Iran-Backed Hackers Breached a US Federal Agency that Failed to Patch Year-Old Bug," *Yahoo News*, November 17, 2022; Tim Starks, "An Iranian Hacking Group Went on the Offensive Against US Targets, Microsoft Says," *Washington Post*, April 18, 2023.

86 Derek Johnson, "Iranian Hacking Group Impersonating Nuclear Experts to Gain Intel from Western Think Tanks," *SC Media*, July 6, 2023.

87 Spadoni, "IRGC Cyber-Warfare"; King Faisal Center for Research and Islamic Studies, *Iran's Cyberattacks*, 33.

88 Ionut Arghire, "Iran-Run ISP 'Cloudzy' Caught Supporting Nation-State APTs, Cybercrime. Hacking Groups," *Securityweek.com*, August 1, 2023

מבצעי תודעה (CNI). איראן משתמשת יותר ויותר במבצעי תודעה בסייבר כדי להשיג את יעדיה האסטרטגיים והפוליטיים. היא מנהלת אותם בעשרות מדינות ושפות באמצעות אתרי חדשות רבים, רשתות חברתיות, יוטיוב ועוד.[89]

אתרי אינטרנט מזויפים מייצרים, מפיצים ומעצימים מסרים המותאמים במיוחד לקהל האמריקני, הלטיני, האפריקני או המזרח־תיכוני. איראן מצטיירת באתרים אלה כחברה אחראית ושוחרת שלום בקהילה הבינלאומית התומכת במדוכאים ומתנגדת למחנה התוקפני שמובילה ארצות הברית וחברות בו ישראל, מדינות המפרץ ומדינות אירופה. לפי אתרים אלה כוחה של איראן נובע מצדקת אמונתה, ערכיה ומדיניותה, המנוגדים לצביעות המערבית ולהסתמכות האמריקנית על כפייה כלכלית ועל כוח צבאי. תשומת לב מיוחדת מוקדשת להפצת התאולוגיה השיעית, רעיונות המהפכה האיראנית ומדיניות המשטר ולתמיכה בתנועות שיעיות אזוריות בניגריה, בתאילנד, בהודו ובמקומות אחרים.[90]

בשנת 2011 פתחה איראן במבצע תודעה ברשתות החברתיות שנועד לקדם את העמדות האיראניות ואת המדיניות האמריקנית התואמת את האינטרסים של איראן כגון הצורך בהסכם גרעין, ולהפיץ מסרים נגד ערב הסעודית וישראל ובעד הפלסטינים. בשנת 2018, בעקבות רצח העיתונאי הסעודי ג׳מאל חאשוקג׳י, פיתחה איראן בוטים, אתרי חדשות מזויפים ופרופילי טוויטר כדי להוסיף ולערער את הקשרים בין ארצות הברית לערב הסעודית ולייצר לחץ בינלאומי על ערב הסעודית.

בשנת 2018 נחשפו שלושה מבצעי תודעה גדולים של איראן. הראשון, ״Ayatollah BBC״, כבר פעל במשך כשש שנים. אתרים איראניים מזויפים התחזו לכמה מתחנות הרדיו המערביות הגדולות שמשדרות בפרסית, כגון BBC ו־Voice of America, כדי לפגוע באמינותן, והאתרים האמיתיים נחסמו במנועי החיפוש האיראניים. הוקמו גם אתרי חדשות ״עצמאיים״ לכאורה, והם הפיצו דברי הסתה ודיסאינפורמציה על האתרים האמיתיים. המבצע השני נמשך גם הוא כשש שנים; הוקמו בו עשרות או אפילו מאות אתרי חדשות מזויפים, והוא פנה לקהל גלובלי. כל אחד מן האתרים התחזה לארגון תקשורת מקומי,

89 Clint Watts, ״Rinse and Repeat: Iran Accelerates its Cyber Influence Operations Worldwide,״ *Microsoft.com* May 2, 2023; Jack Stubbs and Christopher Bing, ״Exclusive: Iran-Based Political Influence Operation – Bigger, Persistent, Global,״ *Reuters*, August 28, 2018.

90 Tabatabai, *Iran's Authoritarian Playbook*, 3, 6–8, 18; Danny Citrinowicz and Ari Ben-Ami, ״The Iranian Information Revolution: How Iran Utilizes Social Media and Internet Platforms to Incite, Recruit and Create Negative Influence Campaigns,״ *European Eye on Radicalization*, Report 30, July 2022.

ובמקרים מסוימים שם בראש חומרים חזותיים ואחרים כותרות מזויפות שאינן קשורות לתוכן המופיע תחתיהן. המבצע השלישי יצא לפועל מייד לאחר רצח העיתונאי הסעודי ג׳מאל חאשוקג׳י; הוא כוון לקהל סעודי ונועד ללבות רגשות נגד המשטר בממלכה.[91]

בשנת 2019 יצא לדרך מבצע תודעה נוסף, דומה באופיו לקודמיו שתוארו לעיל, אך הפעם היה מדובר בהתחזות לארגוני החדשות של העיתונים הגדולים, ובהם הגרדיאן והאינדיפנדנט. אולם בניגוד לריבוי המאמרים המזויפים במבצעים שתוארו שלעיל, במקרה זה האתרים המזויפים התמקדו בכל פעם בכתבה מזויפת אחת כדי להעצים את השפעתה.[92]

בשנת 2019 התחזו חשבונות טוויטר מזויפים רבים לאזרחים אמריקנים אמיתיים, בהם כמה מועמדים רפובליקנים, כדי להפיץ תוכן שלילי על ישראל ועל ערב הסעודית. בכמה מקרים השתמשו הפצחנים בתצלומים ובתכנים שנלקחו מן החשבונות האמיתיים של המועמדים הפוליטיים, וכך הקשו מאוד על ההבחנה בינם ובין המזויפים. בשנים 2019–2020 נחשפו מיליוני משתמשים בפייסבוק, בטוויטר, באינסטגרם וביוטיוב לקמפיין מדיה חברתית רחב היקף שמתח ביקורת על פרישת ארצות הברית מהסכם הגרעין ועל מדיניותה כלפי ישראל, תימן וסוריה.[93]

בשנת 2020 השתלטה ארצות הברית על 92 דומיינים ששימשו את משמרות המהפכה לניהול קמפיינים של הסברה ברחבי העולם. ארבעה מן הדומיינים הללו התחזו לערוצי חדשות לגיטימיים לכאורה וניסו להשפיע על מדיניות הפנים והחוץ של ארצות הברית.

91 David Siman-Tov and Ohad Zaidenberg, ״Influence Operations: A Combination of technological Attacks and Content Manipulation,״ *INSS Special Publication*, March 11, 2021.

92 Siman-Tov and Zaidenberg, ״Influence Operations.״

93 King Faisal Center for Research and Islamic Studies, *Iran´s Cyberattacks,* 35; Tabatabai, *Iran´s Authoritarian Playbook*, 14; Jack Stubbs and Katie Paul, ״Facebook Says it Dismantles Disinformation Network Tied to Iran´s State Media,״ Reuters, May 5, 2020; Ellen Nakashima, Josh Dawsey, and Matt Viser, ״China, Iran Targeting Presidential Campaigns With Hacking Attempts, Google Announces,״ *Washington Post*, June 4, 2020; Craig Timberg, Elizabeth Dwoskin, Tony Romm, and Ellen Nakashima, ״Sprawling Iranian Influence Operation Globalizes Tech´s War on Disinformation,״ *Washington Post*, August 21, 2018; Craig Timberg and Tony Romm, ״It´s not just the Russians Anymore as Iranians and Other Turn Up Disinformation Efforts Ahead of 2020 Vote,״ *Washington Post*, July 25, 2019; Jay Greene, Tony Romm, and Ellen Nakashima, ״Iranians Tried to Hack U.S. Presidential Campaign in Effort that Targeted Hundreds, Microsoft Says,״ *Washington Post*, October 4, 2019.

אתר איראני מזויף ששמו "אמריקן הראלד טריביון" שילם לאזרחים אמריקנים כדי שיכתבו מאמרים התומכים בעמדות איראן, ומאמרים אלה זכו אחר כך לאזכורים חוזרים ופורסמו בתקשורת האיראנית כדי ליצור רושם של תמיכה ציבורית אמריקנית רחבה בעמדות איראן. בשנת 2020, זמן קצר לאחר חיסול מנהיג משמרות המהפכה הבכיר קאסם סולימאני, השתלטו פצחנים איראנים על אתר האינטרנט של סוכנות אמריקנית האחראית על הפצת פרסומים ממשלתיים והשתילו תמונה של הנשיא טראמפ מדמם. קמפיינים אחרים של תודעה התמקדו בקבוצות אתניות ועדתיות בעיראק, בלבנון, במפרץ הפרסי, בסוריה ובאפגניסטן.[94]

במבצעי התודעה ניסו שוב ושוב האיראנים לעורר מחלוקות בין יריבותיה של איראן ובתוכן. איראן ניצלה את הרשתות החברתיות כדי להחריף את המתחים הגזעיים, הסוציו־אקונומיים והפוליטיים הקיימים ממילא בארצות הברית, ולעיתים קרובות השוותה אותם למתחים שהיא עצמה חווה ביחסיה עם ארצות הברית. בשנת 2020, בעקבות הריגת עצור אמריקני שחור בידי שוטר שהצמיד את ברכו לצוואר העצור עד שמת מחנק, טען הנשיא רוחאני שגם ארצות הברית לוחצת את הברך שלה על צווארה של איראן. המנהיג העליון ח׳מינאי ומנהיגים איראנים אחרים שיתפו בטוויטר מסרים התומכים בתנועת Black Lives Matter, וטענו כי שני העמים, האיראני והאמריקני, הם קורבנות הצביעות ומדיניות הדיכוי של השלטון האמריקני, וכי ארצות הברית מרבה לבקר את מדיניות זכויות האדם של מדינות אחרות בזמן שמיעוטים אתניים ודתיים, נשים וקהילת הלהט״ב בארצות הברית צריכים להילחם על זכויותיהם. עוד הם טענו כי העובדה שאירופה שותקת בנוגע להפרות זכויות האדם בארצות הברית בעודה מבקרת את ההפרות של זכויות האדם באיראן, היא ביטוי נוסף לצביעות המערבית.

איראן גם לא חדלה ממאמציה לחבל בבחירות בארצות הברית. בבחירות המקדימות לנשיאות ב־2016 ניסו פרופילים ברשתות החברתיות המקושרים לאיראן לקדם את הקמפיין של ברני סנדרס מכיוון שיריבתו הילרי קלינטון נחשבה לניצית יותר ממנו כלפי איראן. בבחירות לקונגרס בשנת 2018 התחזו פצחנים איראנים לבוחרים אמריקנים ולמועמדים פוליטיים באמצעות יותר מ־7,000 חשבונות טוויטר מזויפים. בבחירות לנשיאות בשנת 2020 ניסתה איראן להשפיע ישירות על התוצאה לטובת ג׳ו ביידן. לאחר שדונלד טראמפ ביטא בגלוי את

94 Kate O׳Flaherty, "DoJ Unveils Iran Disinformation Campaign—Seizes 92 Domains Violating U.S. Sanctions," *Forbes*, October 9, 2020; Halpern, "Should the U.S. Expect an Iranian Cyberattack?"; Tabatabai, *Iran׳s Authoritarian Playbook*, 18, 20.

גישתו הניצית כלפי איראן, ולאחר שפרש מהסכם הגרעין והטיל עליה סנקציות חמורות, חששה איראן שאם ייבחר מחדש הוא עלול לפעול להחלפת המשטר בטהראן. פצחנים של משמרות המהפכה התחזו לתומכי טראמפ מן הימין הקיצוני, השתמשו בכתובות דואר אלקטרוני שהצליחו להשיג בשל תצורה שגויה של מאגר רישום הבוחרים ושלחו עשרות אלפי מיילים מאיימים לבוחרים דמוקרטים בשלוש מדינות מתנדנדות. "לפי רישומכם אתם דמוקרטים", התריעו בהודעה, "ואנחנו יודעים זאת כי קיבלנו גישה לכל מערכת ההצבעה. הצביעו לטראמפ ביום הבחירות, או שנרדוף אתכם". פצחנים של משמרות המהפכה שלחו גם הודעות דואר אלקטרוני שצורפו להן סרטונים מוליכי שולל. הסרטונים נועדו לערער את אמון הבוחרים בתהליך הבחירות ולהגביר את החששות שטראמפ עצמו כבר הצית בדבר הונאה בפתקי הצבעה שנשלחו בדואר.[95]

המאמצים האיראניים לערער את האמון בתקינותו של תהליך הבחירות נמשכו גם לאחר סיום הבחירות. Pioneer Kittens פרצו למערכת ששימשה ממשל מקומי לפרסום תוצאות בחירות; לתקיפה לא הייתה יכולת להשפיע על תוצאות הבחירות, אבל הייתה לה יכולת להעביר דיווח שגוי על התוצאות, וכך ליצור את הרושם שהיו זיופים במערכת הבחירות ולפגוע באמון הציבור בתוצאותיה. במקרה חמור אחר פרסם אתר "אויבי העם" המזוהה עם איראן איומים במוות נגד מי שהפריכו את טענות טראמפ על הונאת בחירות,

95 Julian E. Barnes and David E. Sanger, "Iran and Russia Seek to Influence Election in Final Days, U.S. Officials Warn," *New York Times*, October 21, 2020; Ellen Nakashima, Amy Gardner, Isaac Stanley-Becker, and Craig Timberg, "U.S. Government Concludes Iran Was Behind Threatening Emails Sent to Democrats," *Washington Post*, October 22, 2020; Ellen Nakashima, Amy Gardner, and Aaron Davis, "FBI Links Iran to Online Hit List Targeting Top Officials Who've Refuted Trump's Election Fraud Claims," *Washington Post*, December 22, 2020; Tabatabai, *Iran's Authoritarian Playbook,* 11, 15–16; National Intelligence Council, "Foreign Threats to the 2020 Federal Elections," (March 10, 2021), 5–7; Miles Parks, "View From the Ground at Washington DC Protests; Misinformation Spreads Online," *NPR*, June 4, 2020; Brian Bennett, "Exclusive: Iran Steps up Efforts to Sow Discord Inside U.S.," *Time*, June 7, 2021; David E. Sanger and Julian E. Barnes, "United States Indicts Iranian Hackers in Voter Intimidation Effort," *New York Times*, November 18, 2021; Phil Muncaster, "US: Iran Was Behind Proud Boys Email Campaign," *Infosecurity Magazine*, October 22, 2020; Lily Hay Newman, "How Iran Tried to Undermine the 2020 US Presidential Election," *Wired*, November 18, 2021.

ובהם עובדים במערכת הבחירות, מושלי מדינות, ראש ה־FBI ומומחה סייבר בכיר במשרד לביטחון המולדת.[96]

ייתכן שאיראן עמדה גם מאחורי אתר האינטרנט "Mapping Project"; מוצגים בו מיקומיהם של ארגונים יהודיים ושל גופי אכיפת חוק וביטחון במדינת מסצ'וסטס שבארצות הברית. האתר איים על הקהילה היהודית והזהיר כי לכל ארגון "יש כתובת, כל רשת אפשר לשבש". יותר משני שלישים מ־505 המיקומים המוצגים באתר הם של תחנות משטרה או של בסיסים צבאיים; של משרדי המחלקה לביטחון פנים, ה־FBI והשירות החשאי; ושל יצרני נשק הקשורים לממשלה.[97]

לפי דיווחים, איראן ביקשה להתסיס מחלוקות פנימיות גם בבריטניה. לדף הפייסבוק "Free Scotland", המזוהה עם איראן ותומך בעצמאות סקוטלנד, יש יותר מ־20 אלף עוקבים. "Britishleft.com" הוא אחד מכמה אתרים מזויפים המקדמים מסרים נגד ערב הסעודית ונגד ישראל. אתר אחר, כביכול מן העיר ברמינגהם שבבריטניה, מפיץ חומרים שנלקחים מערוץ תקשורת איראני שבבעלות המדינה. קמפיין התודעה בסייבר הוא חלק ממאמץ איראני רחב שמטרתו להשפיע על העמדות הפוליטיות בבריטניה, בין היתר באמצעות השקעה במוסדות דת ותרבות בריטיים.[98]

אותם פצחנים איראנים שניהלו את קמפיין התודעה נגד הבחירות האמריקניות ב־2020 גנבו והדליפו בשנת 2023 את השמות ואת פרטי הקשר של יותר מ־200 אלף מנויים של המגזין הצרפתי הסאטירי "שרלי הבדו". התקיפה הייתה ככל הנראה בתגובה לסדרה של קריקטורות ביקורתיות נגד המנהיג העליון שפרסם המגזין בשיאן של ההפגנות נגד המשטר

96 Joseph Menn, "Iran Gained Access to Election Results Website in 2020, Military Reveals," *Washington Post*, April 24, 2023; Christina A. Cassidy and Frank Bajak, "US Cyberwarriors thwarted 2020 Iran Election Hacking Attempt," *AP*, April 25, 2023; Nakashima, Gardner, Stanley-Becker, and Timberg, "U.S. Government Concludes Iran Was Behind Threatening Emails"; Nakashima, Gardner, and Davis, "FBI Links Iran to Online Hit List; Tabatabai, *Iran's Authoritarian Playbook*, 11, 15–16; National Intelligence Council, "Foreign Threats"; Parks, "View From the Ground at Washington DC Protests"; Sanger and Barnes, "United States Indicts Iranian Hackers"; Newman, "How Iran Tried to Undermine the 2020 US Presidential Election."

97 Benjamin Weinthal, "Iran May Be Behind BDS 'Hit List" Targeting Boston Jews – Report," *Jerusalem Post*, March 5, 2023.

98 Charles Hymas, "Iran Targets UK Political System With Fake Websites," *The Telegraph*, June 6, 2021; Paul Stott, *Iranian Influence Networks in the United Kingdom: Audit and Analysis* (Henry Jackson Society, June 2021).

באיראן. הפצחנים השתמשו בחשבונות טוויטר מזויפים כדי להעצים את ההשפעה של המידע שדלף.[99]

99 Zeba Siddiqui, "Iran Behind Hack of French Magazine Charlie Hebdo, Microsoft Says," *Reuters*, February 3, 2023.

חלק 4

איום הסייבר האיראני על ישראל

רקע כללי

ישראל היא היריבה העיקרית של איראן בתחום הסייבר, כמו בכל שאר התחומים. קודם לעיסוק באיום הסייבר האיראני על ישראל, חשוב להציג את ההקשר האסטרטגי הרחב של האיום שאיראן מציבה בפני ישראל. המנהיג העליון ח׳מינאי ומנהיגים איראנים אחרים שבו וקראו במשך עשרות שנים להשמדתה של ישראל והתייחסו אליה, בין היתר, כאל ״גידול סרטני״ שיש להסירו.[100] בשנת 2014 אף הצהיר ח׳מינאי בפומבי על תוכנית בת תשעה סעיפים להשמדת ישראל.[101]

האיבה האיראנית כלפי ישראל היא מהותית, ואינה נובעת ממדיניות זו או אחרת שישראל יכולה לשנות כדי לגאול עצמה ממנה. ההתנגדות של איראן היא לעצם קיומה של ישראל. מבחינה זו היא שונה מאוד מן האיבה שאיראן רוחשת כלפי ארצות הברית או ערב הסעודית, שתי יריבותיה העיקריות האחרות, שלצד ישראל הן היעד של מרבית תקיפות הסייבר האיראניות. אם ארצות הברית ״תתקן את דרכיה״ ותערוך שינויים חשובים במדיניותה כלפי איראן והאזור, תוכל הרפובליקה האסלאמית לחיות איתה בשלום יחסי ובשיתוף פעולה, גם אם לא בחום רב. המחלוקות התאולוגיות, האסטרטגיות והכלכליות בין איראן לערב הסעודית הן היסטוריות ובעלות שורשים עמוקים. עם זאת, הן העלימו לאחרונה עין מן המחלוקות הללו והחלו בתהליך התקרבות, זמני לפחות.

מבחינתה של ישראל הרטוריקה האיראנית רחוקה מדיבורי סרק. להפך, מאז נוסדה הרפובליקה האסלאמית הקדישה איראן מאמצים ומשאבים רבים לפעילותה נגד ישראל. שיקול הדעת שאיראן נוקטת כדי להשיג את יעדיה בכל הנוגע לישראל, היותה מתקדמת למדי, גדולה, בעלת משאבים ולא רחוקה מאוד גיאוגרפית מישראל – כל אלה יחד הופכים

100 Amir Vahdat and Jon Gambrell, ״Iran Leader Says Israel a ׳Cancerous Tumor׳ to be Destroyed,״ *AP*, May 22, 2020; Tamar Pileggi, ״Khamenei: Israel a ״׳Cancerous Tumor׳ that ׳Must be Eradicated,׳״ *Times of Israel*, June 4, 2018; CNN Staff, ״Iran Leader Urges Destruction of ׳Cancerous׳ Israel,״ *CNN*, December 15, 2000.

101 Stuart Winer and Marissa Newman, ״Iran Supreme Leader Touts 9-Point Plan to Destroy Israel,״ *Times of Israel,* November 10, 2014.

אותה ליריבה המתוחכמת והמסוכנת ביותר של ישראל בכל הזמנים. אין ספק ששום גורם ישראלי אחראי לא יכול להרשות לעצמו להקל ראש בחומרתו של איום זה.

כיום תוכנית הגרעין של איראן היא האיום העיקרי על ביטחונה הלאומי של ישראל והאיום הקיומי היחיד שעומד בפניה. הסבירות שאיראן תשתמש אי פעם בנשק גרעיני נגד ישראל היא כנראה נמוכה מאוד, אבל ההשלכות האפשריות הן בלתי נסבלות, ולכן על ישראל להתייחס לתוכנית הגרעין האיראנית בכובד ראש. עם זאת, האיום הסביר יותר נובע מן המעמד והעוצמה שיכולת גרעינית תעניק לאיראן; היא תאפשר לה ולשלוחיה להחריף את תוקפנות העימות התת־גרעיני נגד ישראל. יתרה מכך, מעצם נוכחותו של נשק גרעיני, גם אם ברקע בלבד, עימותים אזוריים מוגבלים עלולים להסלים בעתיד לעימותים המציבים איום קיומי.

זאת ועוד, אם איראן תשיג נשק גרעיני, מדינות נוספות, כגון טורקיה, ערב הסעודית, מצרים ואולי אפילו איחוד האמירויות, עשויות גם הן לחתור לכך. מזרח תיכון ובו מספר רב של שחקניות בעלות גרעין הוא תרחיש בלהות שאין לו מענה. בניגוד ליריבויות הגרעיניות בין ארצות הברית לרוסיה, בין ארצות הברית לסין או בין הודו לפקיסטן, איראן חותרת במפורש להשמדת יריבתה. המעצמות הגרעיניות הללו עשו מאמצים רבים כדי למנוע את המשברים ביניהן או למתן אותם, אולם סביר להניח שבין שחקניות בעלות גרעין במזרח התיכון יהיו ערוצים מוגבלים בלבד לתקשורת ולניהול המשברים. יתרה מזו, איראן וערב הסעודית הן תאוקרטיות, וגם אם הן "שחקניות רציונליות", הרציונליות של תאוקרטיות עשויה להיות שונה מן הרציונליות של מדינות אחרות, וכל הבדל קטן עלול להיות קריטי. הסיכויים לשימוש בפועל בנשק גרעיני במזרח התיכון, בפרט אם יהיו באזור כמה שחקניות בעלות גרעין, גבוהים הרבה יותר מבמקומות אחרים בעולם ומדאיגים מאוד.

בניגוד ליכולתה להציב איום גרעיני, יכולותיה הצבאיות הקונוונציונליות של איראן הן מוגבלות ואינן צפויות להציב איום גדול בפני ישראל בזמן הקרוב. אומנם לאיראן יש ארסנל גדול ומתעצם של טילי שיוט, טילים בליסטיים וכלי טיס בלתי מאוישים (כטב"ם) המסוגלים לפגוע בישראל, אבל האיום המרכזי שהיא מציבה הוא עקיף, באמצעות חזבאללה, ארגון השלוחים שלה בלבנון. ההערכה היא שאיראן חימשה את חזבאללה בארסנל חסר תקדים של כ־150 אלף טילים ורקטות ויותר מאלפיים כטב"מים. בעימות גדול עלול חזבאללה לשגר טילים לעבר ישראל מדי יום במשך שבועות ולגרום נזק חמור לעורף האזרחי שלה.[102]

102 Jerusalem Post Staff, Tovah Lazaroff, "Israel is Updating Attack Plans Against Iran's Nuclear Sites – Gantz," *Jerusalem Post*, March 15, 2021; Anna Ahronheim, "Hezbollah

זאת ועוד, הטילים שאיראן מספקת כעת לחזבאללה מדויקים יותר מבעבר, ומנקודת מבטה של ישראל ייתכן שהם משנים את כללי המשחק. טילים מדויקים יאפשרו לחזבאללה לשבש פעולות הגנתיות והתקפיות של צה"ל באמצעות שיגור טילים על מערכות נגד טילים (נ"ט) ועל בסיסים צבאיים, לפגוע בתהליכי הפיקוד והבקרה של ישראל באמצעות ירי על מטרות – החל מלשכת ראש הממשלה דרך מפקדות צה"ל ועד צמתים של תקשורת צבאית – ולפגוע בכלכלה ובחברה במדינה באמצעות ירי על תשתיות לאומיות חיוניות ועל מרכזי אוכלוסייה. אומנם היכולות ההתקפיות ואמצעי ההגנה מפני טילים שבידי ישראל יפחיתו את האיום, אך לא יוכלו לנטרל כליל ארסנל בגודל הזה. לשום יריב ערבי אחר לא הייתה מעולם היכולת לשבש בסדר גודל כזה את העורף האזרחי והצבאי של ישראל.[103]

איראן עסוקה גם במאמץ מתמשך לבסס נוכחות צבאית קבועה בסוריה ולהעביר דרכה נשק לחזבאללה בלבנון. עד כה הצליחה ישראל במידת מה להאט את המאמץ הזה, אולם ההתבססות נמשכת. עתידה ארוך הטווח של סוריה אינו ברור, אך סביר להניח שהיא תישאר תחת השפעה איראנית כבדה ותשמש לטהראן, לפחות במידת מה, בסיס מבצעי קדמי נגד ישראל. ההשלכות מבחינת ישראל חמורות, והן עלולות אף להוביל להתנגשות ישירה עם איראן החורגת מן העימות הצבאי העקיף שכבר מתנהל. נוכחותה של איראן בסוריה מפעילה לחץ גם על יחסי ישראל ורוסיה, השחקנית המרכזית השנייה בסוריה, משום שרוסיה פרסה שם את מערכת הטילים נגד מטוסים (נ"מ) המתקדמת ביותר שלה, והציבה שם גם בסיסי אוויר וים. איראן גם פרסה בעיראק ובתימן טילים וכטב"מים המסוגלים להגיע לישראל.

בניגוד ליריבות הערביות של ישראל בעבר, איראן וחזבאללה אינם שואפים להביסה בטווח הזמן הקרוב שכן הם מבינים שאין ביכולתם להשיג מטרה זו. במקום זאת הם אימצו אסטרטגיה ארוכת טווח של "התשה עד להשמדה", ולמימושה הם משתמשים במגוון כלי נשק וטקטיקות שמטרתם לנטרל חלקית את העליונות הטכנולוגית של ישראל, למנוע ממנה ניצחון ולפגוע במורל האוכלוסייה בישראל. חזבאללה ממקם בכוונה את משגרי הטילים שלו בלב האוכלוסייה האזרחית בלבנון כדי שאזרחים לבנונים ייפגעו מן התקיפות הישראליות להשמדת המשגרים וייווצר לחץ בינלאומי על ישראל להפסיק את הלחימה בטרם תשיג

Has Some 2,000 Unmanned Aerial Vehicles – ALMA," *Jerusalem Post*, December 22, 2021; Yonah Jeremy Bob, "IDF Intel Chief: We'll Keep Peace in North Despite Hezbollah Provocations," *Jerusalem Post*, July 11, 2023.

103 Charles D. Freilich, *Israeli National Security: A New Strategy for an Era of Change* (Oxford: Oxford Press, 2018), 154–160.

את יעדיה הצבאיים. המאמצים ההתקפיים של חזבאללה מתמקדים בראש ובראשונה באוכלוסייה האזרחית של ישראל באמצעות התקפות מסיביות וממושכות של טילים.[104]

תקיפות הסייבר של איראן נגד ישראל

בחלק זה יוצג תיאור מפורט של תקיפות הסייבר המרכזיות שאיראן ביצעה נגד ישראל. כמה מן התקיפות היו מרכיב בקמפיינים נרחבים נגד עוד מדינות, ואחרות היו תקיפות משולבות (שילוב מרכיבים של תקיפות CNA, CNE, CNI וכופרה). התקיפות שיפורטו סווגו על פי מטרתן העיקרית.

תקיפות CNA (שיבוש והרס). בשנת 2012 פתחו פצחנים המזוהים עם איראן במתקפה נגד שרתי המחשבים של משטרת ישראל. היה צורך לנתק את שרתי המשטרה מכל חיבור למערכות חיצוניות ולבודד כל רשת עד שהוסרו כל החדירות לשרתים. צוות גדול עבד שבוע שלם סביב השעון כדי להשלים את המשימה.[105]

אחת התקיפות האיראניות הראשונות נגד תשתיות לאומיות חיוניות בישראל התרחשה ב־2014, בעימות עם חמאס באותה שנה ("צוק איתן"). פצחנים איראנים פתחו בתקיפה רחבת היקף נגד מערכת התקשורת האזרחית וניסו לגרום לעומס יתר במערכת ה־DNS של ישראל.[106] תקיפה איראנית אחרת נגד תשתית לאומית חיונית התרחשה ב־2015 או ב־2016. הפצחנים האמינו כנראה שעלה בידם לפגוע קשות ברשת החשמל של ישראל ואולי אף במתקן גרעיני. אולם בפועל הרשתות שהותקפו היו "מלכודות דבש" שמטרתן להסיט את התקיפות ממטרותיהן האמיתיות ולחשוף את כוונותיו ואת יכולותיו של האויב. עם זאת, עצם הנכונות והתעוזה של התוקפים לצאת לתקיפות שעלולות להוביל להסלמה עוררו דאגה, וכפי שיפורט להלן, זו לא הייתה תקיפת הסייבר האיראנית האחרונה נגד מטרות בישראל הקשורות לגרעין.

בשנים 2019–2020 שוב בוצעה סדרה של תקיפות נגד התשתית החיונית של ישראל, ככל הנראה בידי משמרות המהפכה, הפעם נגד מערכות אספקת המים והביוב. הגנת הסייבר של ישראל חסמה בהצלחה את התקיפות עד אפריל 2020, כאשר תקיפה שהופעלה דרך

104. Freilich, *Israeli National Security,* chapter 3.

105. Shamah, "Official: Iran, Hamas Conduct Cyber-Attacks"; David Shamah, "How Israel Police Computers Were Hacked: The Inside Story," *Times of Israel*, October 28, 2012.

106. Yaakov Lappin, "Iran Attempted Large-Scale Cyber-Attack on Israel, Senior Security Source Says," *Jerusalem Post*, August 17, 2014; Brewster, "Persian Paranoia."

שרתים בארצות הברית השתלטה על מערכות הבקרה של שש תחנות לטיפול במים ובביוב ושיבשה אותן. התקיפה זוהתה במהירות ולא נגרם נזק, אך אילו הצליחו התוקפים הם היו יכולים להעלות את כמויות הכלור וכימיקלים אחרים המוזרקים למערכת המים לרמות שעלולות להיות קטלניות.[107] הדאגה בישראל הובילה לכינוס ישיבה מיוחדת של הוועדה לביטחון לאומי. ראש מערך הסייבר הלאומי הגדיר את התקיפה "נקודת מפנה בהיסטוריה של לוחמת הסייבר המודרנית" והדגיש כי זו הפעם הראשונה שיריבה של ישראל משתמשת בתקיפת סייבר כדי להסב נזק קטלני.[108]

שבועות ספורים בלבד לאחר מכן שוב הייתה מערכת המים על הכוונת, הפעם של שתי תקיפות מוגבלות יותר מקודמתן, האחת נגד משאבות מים חקלאיות בגליל והשנייה נגד תשתית במרכז הארץ. ההגנות של ישראל שוב הוכיחו את עצמן, ושום מתקפה לא צלחה. עם זאת, התקיפות הללו הוכיחו שתקיפות הנגד שישראל ביצעה, על פי דיווחים, בתגובה על הניסיונות הקודמים לתקוף אותה, לא השיגו את ההרתעה המיוחלת.[109]

התקיפות נגד מערכת המים היו חלק מסדרה מתמשכת של תקיפות ותקיפות נגד בין איראן לישראל, בתחום הקינטי ובתחום הסייבר, משנת 2019 ועד היום. התקיפות האיראניות הגיעו בגלים. ביולי 2020 שוגרו 19 אלף תקיפות סייבר נגד חברות ישראליות; בנובמבר הגיע המספר ל־33,600.[110] Hackers of Saviors, קבוצת האקטיביסטים המזוהה עם איראן

107 Ahiya Raved, "Cyber Attack Targeted Israel's Water Supply, Internal Report Claims," *Ynet*, April 26, 2020; Ynet staff, "Report: Iran Behind Hack of Israeli Water Authority Sites," *Ynet*, May 7, 2020; Amos Harel, "With Cyberattack on Iranian Port, Tehran Gets a Warning: Civilian Installations Are a Red Line," *Haaretz*, May 20, 2020; Yonah Jeremy Bob, "Israeli Cyber Czar Warns of More Attacks From Iran," *Jerusalem Post*, May 28, 2020; Yonah Jeremy Bob, "The Coming Cyber Winter is Worse Than all Estimates," *Jerusalem Post*, December 10, 2020; Amitai Ziv, "The Iranians Read the Reports about Israel's Cyber Error, and Succeeded to Embarrass it," *The Marker*, May 31, 2020; TOI Staff, "Israel Behind Cyberattack that Caused 'Total Disarray' at Iran Port – Report," *Times of Israel*, May 19, 2020; Staff, "Iranian Cyberattacks on Israeli Facilities Thwarted for a Year – Report," *Jerusalem Post*, June 7, 2020; Tal Shahaf, "Israel Unprepared for Iranian Attack on Water Supply, Officials Warn," *Ynet*, February 17, 2021; Government of Israel; Prime Minister's Office, National Cyber Directorate. "Annual Report" (2021).

108 Bob, "Israeli Cyber Czar."

109 TOI Staff, "Cyber Attacks Again Hit Israel's Water System, Shutting Agricultural Pumps," *Times of Israel*, July 17, 2020.

110 Meir Orbach and Golan Hazani, "Israel's Supply Chain Targeted in Massive Cyberattack," *Calcalist*, December 13, 2020.

ותומכת במאבק הפלסטיני, תזמנה בשנת 2020 את התקיפות שלה כך שיתבצעו ביום ירושלים האיראני. למרות האזהרות של מערך הסייבר הלאומי, הצליחו הפצחנים לנצל נקודת תורפה בשרתים של אתר אירוח מוביל והשחיתו אלפי אתרים ישראליים באמצעות שתילת הודעות נאצה וקריאות להשמדת ישראל. הם ניסו גם לפתות משתמשים להוריד תוכנות זדוניות; לו הורדו היו מוחקות לחלוטין את הנתונים ממחשבי המשתמשים. עם היעדים המותקפים נמנו עיריות, חברת תרופות, רשתות מזון וחברות פרטיות אחרות, ארגונים לא ממשלתיים ורשות מים אזורית.[111]

בשנת 2020 פתחה Static Kittens בתקיפה שנראתה בתחילה כמו תקיפת כופרה, אך ייתכן שהיא הייתה הקדמה לתקיפת הרס גדולה. קמפיין ריגול סייבר שביצעה Agrius, קבוצת פצחנים אחרת המזוהה עם איראן, אכן התפתח לתקיפות הרסניות של מחיקת מידע.[112] בשנת 2021 תקפו Siamese Kittens את שרשרות האספקה של חברות מחשוב וטלקומוניקציה ישראליות; הם התחזו לעמיתים העובדים בחברות דומות בתעשייה וניסו לחדור למחשבי הקורבנות שלהם, ככל הנראה כדי להכין את הקרקע לתקיפה של מחיקת מידע או לתקיפת כופרה.[113]

בשנת 2022 עלו התקיפות נגד ישראל מדרגה. פצחנים איראנים, ככל הנראה מקבוצת Charming Kittens, תקפו בהצלחה שורה ארוכה של חברות אנרגייה ישראליות, לרבות תחנות כוח, בתי זיקוק ונפט וצינורות גז טבעי. הפצחנים הצליחו לגנוב נתונים רגישים, ובכלל זה קניין רוחני ומידע פיננסי, אך לא הצליחו לשבש את הפעילות השוטפת של החברות. שבועות ספורים לאחר מכן בוצעה תקיפה דומה, ככל הנראה שוב בידי Charming Kittens, נגד אל על ובזק. הבורסה לניירות ערך בתל אביב נסגרה לכמה שעות לאחר שתקיפת DDoS הציפה את השרתים שלה בתנועה שמנעה מן המשתמשים את הגישה אליהם.[114]

בשנת 2022 השביתו Charming Kittens (APT34) את מערכת בקרת התנועה האווירית בנתב"ג וגרמו לשיבוש הפעילות בנמל התעופה ואף לסגירתו למשך כמה שעות. לא נגרם נזק לתשתית הפיזית של שדה התעופה, אך היה צורך לבטל טיסות רבות ושובשה תנועתם

111 Ynet reporters, "Host of Israeli Sites Targeted in Massive Cyber-Attack," *Ynet* May 21, 2020; Ran Bar-Zik, "Thousands of Websites Defaced in Cyberattack Calling for the 'Destruction of Israel,'" *Haaretz,* May 21, 2020; Government of Israel, Prime Minister's Office, National Cyber Directorate, "Annual Report" (2021).

112 Demboski and IronNet Threat Research and Intelligence Teams, "Analysis of the Iranian Cyber Attack"; Yuval Mann, *Ynet*, November 10, 2021.

113 Demboski and IronNet Threat Research and Intelligence Teams, "Analysis of the Iranian Cyber Attack."

114 Tomer Ganon, *Jerusalem Post*, March 8, 2022 and April 12, 2022; David Sanger and Ronen Bergman, *New York Times*, March 8, 2022.

של הנוסעים. הפצחנים גם הפיצו וירוס שהדביק את המחשבים בשדה התעופה והחריף את שיבוש הפעילות בו. תקיפת DDoS מנעה מנוסעים להזמין טיסות או לבצע צ׳ק־אין.[115]

בשנת 2022 שיבשו Hackers of Saviors את פעילותה של חברת לוגיסטיקה בנמל אשדוד. ייתכן שהתקיפה הייתה פעולת תגמול על תקיפה גדולה שישראל ביצעה שנה קודם לכן, על פי דיווחים, נגד נמל איראני בתגובה על התקיפות האיראניות על מערכת המים בישראל.[116]

תקיפה חסרת תקדים בגודלה ובהיקפה המזוהה עם משמרות המהפכה גרמה בשנת 2022 למערך הסייבר הלאומי להכריז על מצב חירום. תקיפת ה־DDoS שיבשה זמנית את אתרי האינטרנט של כמה משרדי ממשלה, בהם משרד ראש הממשלה. תקיפה אחרת של MuddyWater שיבשה את האתרים של משרד הביטחון ושל משרד ראש הממשלה, אך לא השיגה את מטרתה העיקרית – לשבש את התשתית החיונית של ישראל.[117]

תקיפה של Charming Kittens נגד רשת החשמל בשנת 2022 הצליחה להסב נזק לכמה תחנות כוח ולתחנות משנה, ומאות אלפי אנשים נותרו בלי חשמל במשך שעות. ייתכן שגם מערכת המים ואתרי תשתית חיונית אחרים הותקפו.[118]

תקיפת סייבר רחבה שבוצעה בתחילת 2023 תוכננה להתרחש בו־זמנית עם הקמפיין השנתי #opIsrael המזוהה עם הפלסטינים ועם יום ירושלים האיראני; היא כוונה נגד אוניברסיטאות ישראליות ונגד שורה של יעדים ממשלתיים ומסחריים. המידע הזמין אינו חד־משמעי, אך ייתכן שאת התקיפות ביצעו פצחנים המזוהים עם המודיעין הרוסי ופועלים במסווה איראני, פרי שיתוף הפעולה הגובר בין שתי המדינות בעקבות המלחמה באוקראינה. התקיפות שיבשו זמנית את אתרי האינטרנט של גופים רבים: רוב הבנקים וחברות התקשורת בישראל, שירותי הדואר, חברות החשמל והמים, מערכת ההתרעה של פיקוד העורף מפני ירי רקטות, רשויות נמלי ישראל, הרשות לניירות ערך, עמוד הפייסבוק של ראש הממשלה נתניהו, משרד הבריאות ושירותי רפואת חירום, כמה מערכות עיתון

115 Judah Ari Gross, *Times of Israel*, May 24, 2022 and May 25, 2022; *Haaretz*, May 11, 2022.

116 Rafael Kahan, *Calcalist*, February 1, 2022; Genia Wilenski, *The Marker*, January 31, 2022; Nevo Trebelsi, *Globes*, January 31, 2022.

117 Amos Harel, *Haaretz*, March 15, 2022; Yaniv Kubovich and Oded Yaon, *Haaretz*, March 14, 2022; Yaniv Halperin, *Anashim Umachshevim*, March 14, 2022; Yaron Avraham and Nir Dvori, *N12*, March 14, 2022; Raphael Kahan, *Calcalist*, March 14, 2022; Stav Namer et al, *Maariv*, March 14, 2022; Daniel Salame, *Ynet*, March 14, 2022; Report by FireEye Mandiant, January 24, 2022.

118 Judah Ari Gross, *Times of Israel*, March 8, 2022; Ellen Nakashima and Adam Entous, *Washington Post*, March 9, 2022; David E. Sanger and Ronen Bergman, *New York Times*, March 8, 2022.

וערוצי טלוויזיה, צ׳ק פוינט – חברת אבטחת הסייבר המובילה בישראל, ואפילו האתרים הציבוריים של המוסד והשב״כ.[119]

מדי שנה מתמודד צה״ל עם מאות ניסיונות לפרוץ את הגנותיו ולחדור למערכות מחשוב ולרשתות צבאיות, לרבות מבצעיות.[120] מערכת ההתרעה המוקדמת של פיקוד העורף הותקפה בכמה הזדמנויות, לרבות בכמה מסבבי העימות עם חמאס. אילו הצליחו התוקפים, הם היו יכולים להפעיל התרעות שווא או למנוע שימוש במערכת בעת הצורך. בשנת 2020 זוהתה פריצה לשרשרת האספקה האזרחית של צה״ל, ובכלל זה לספקי גז ומזון שמפעילותם ומדרכי פעולתם אפשר להסיק מידע חשוב על פעולות צה״ל.[121]

תקיפות CNE (ריגול). תקיפות CNE איראניות מתמקדות בגורמי ביטחון ישראלים, בתעשיות ביטחוניות ואפילו במדעני גרעין. פצחנים איראנים אף ניסו שוב ושוב להשיג מידע על התפיסה האסטרטגית של ישראל באמצעות תקיפות ריגול נגד אנשי אקדמיה הקשורים למערכת הביטחון. לשם כך הם התחזו לעמיתים ולמכרים אישיים של אנשי האקדמיה וביקשו לשמוע את הערכותיהם לאמיתן, לא כפי שהן פורסמו במאמריהם. כדי להעניק אמינות לתקיפות, הפצחנים חקרו את תכתובות הדואר האלקטרוני השוטפות של היעדים לתקיפה ואף השתתפו בעצמם בכמה מהן.[122] בכמה מקרים היו התקיפות נגד מטרות ישראליות חלק מקמפיינים נרחבים נגד עוד מדינות בעולם, אך הן פורטו כאן מכיוון שהמרכיב הישראלי בהן היה ניכר.

המתקפה על ״מאגר תמר״ החלה, על פי הערכות, במועד כלשהו בשנים 2011–2014; פצחנים איראנים השתמשו, על פי דיווחים, בשיטות של דיוג ממוקד ושל הנדסה חברתית כדי לפתות קצינים ישראלים לשעבר, עובדים של חברות ייעוץ ביטחוניות ואנשי אקדמיה להוריד נוזקה שהתחזתה לקובצי וורד ואקסל מצורפים. הנוזקה הכילה ״רישום הקשות״ –

119 Raphael Kahan, *Haaretz*, April 5 and April 21, 2023; Daniel Salame and Raphael Kahan, *Haaretz*, April 14, 2023; Jerusalem Post Staff, ״Israeli Cyber Security Website Briefly Taken Down in Cyberattack,״ *Jerusalem Post*, April 4, 2023; Jerusalem Post Staff, ״United Hazalah Hit By Tens of Thousands of Cyberattacks Past Two Days,״ *Jerusalem Post*, April 5, 2023; Jerusalem Post Staff, ״Israel Independence Day Cyberattack Takes Down Major News Websites,״ *Jerusalem Post*, April 26, 2023; Ofir Dor, ״׳Unsophisticated Iranian Cyberattack׳ Temporally Downs Israeli Bank Sites, Post Office,״ *Haaretz*, April 14, 2023; TOI Staff, ״Website of Israeli Port Hacked; Sudanese Group Said to Claim Responsibility,״ *Times of Israel*, April 26, 2023.

120 Itam Elmadon, *N12,* January 21, 2021; Yoav Limor, *Israel Hayom*, February 7, 2019.

121 Yoav Limor, *Israel Hayom*, February 7, 2020 and June 11, 2020.

122 Ayala Hasson, ״Iranian Hackers Posed as General Yadlin and Gained Information from an Israeli Researcher,״ *Channel 13*, November 20, 2020.

קוד מחשב המאפשר לפצחנים לתעד כל הקלדה של המשתמשים, לצלם צילומי מסך ולהעתיק קבצים ללא ידיעתם.[123]

בשנת 2012 תקף קמפיין דיוג ממוקד כ־800 מנהלים עסקיים בתחומי התשתיות החיוניות והשירותים הפיננסיים, וכן גורמים רשמיים ועובדי שגרירות. הקורבנות פתחו קבצים שצורפו לדואר האלקטרוני או לחצו על קישורים למאמרי חדשות, וכך הורידו תוכנות זדוניות שהעניקו לפצחנים גישה למחשביהם. 54 מן הקורבנות היו ישראלים.[124] מאז 2013 תקפו Copy Kittens סוכנויות ממשלתיות, חברות ביטחוניות, חברות של טכנולוגיית מידע, מוסדות אקדמיים ורשויות עירוניות בישראל, בארצות הברית, בערב הסעודית, בטורקיה, בירדן ובגרמניה. כל אחת מן התקיפות החלה בקובץ נגוע שצורף להודעת דואר אלקטרוני ובדרך כלל הותאם בקפידה לתחומי העניין של הקורבן.[125]

בשנים 2013–2017 חדרו פצחנים איראנים בהצלחה למערכות המחשב של 320 אוניברסיטאות, בעיקר בארצות הברית אך גם בישראל ובמקומות אחרים. יותר מ־100 אלף חשבונות אקדמיים הותקפו, כ־8,000 מהם נפרצו, וכמויות אדירות של מידע ושל קניין רוחני נגנבו. בתקיפה אחרת נגד 76 אוניברסיטאות בארצות הברית, בישראל ובמדינות אחרות היה ניסיון להשיג גישה לקניין רוחני ולמחקר שעדיין לא פורסם; היא נחשפה רק ב־2018.[126]

בשנת 2014 תקפו Rocket Kittens מוסדות אקדמיים ישראליים, ספקים בתחום הביטחון ועוד, וכן יעדים במזרח התיכון. בכמה מן המקרים התחזו הפצחנים למהנדסים ישראלים, לרבות למהנדס אחד מוכר במיוחד, כדי לייצר אמינות בקרב הקורבנות שלהם ולהגדיל את הסבירות שיורידו את התוכנה הזדונית. בתקיפות השתמשו במסרוני טקסט, בהודעות פייסבוק, בדואר אלקטרוני, בדיוג ממוקד ובעוד מגוון טכניקות. בהודעות היו שגיאות שאפשר היה לזהות בקלות, ובדרך כלל הן לא היו מתוחכמות, אך התבלטו בעיקשותן –

123 ClearSky Research Team, "Rocket Kitten 2 – Follow-Up on Iran Originated Cyber-Attacks." Clearsky.com, September 1, 2015.

124 United Against Nuclear Iran (UANI), "The Iranian Cyber Threat." *UANI* (May 2020).

125 ClearSky Research Team, "Rocket Kitten 2 – Follow-Up on Iran Originated Cyber-Attacks," Clearsky.com, September 1, 2015.

126 U.S. Department of Justice, "Nine Iranians Charged"; Cuthbertson, "Iranian Hackers Attack UK."

השיטה של הפצחנים הייתה להציף את הקורבנות בתקיפות עד שמישהו יטעה ויוריד את התוכנה הזדונית.[127]

בשנת 2017 התחזו פצחנים של Copy Kittens למשרד ראש הממשלה ולאתרי חדשות ישראליים ותקפו שגרירויות ישראליות בחו"ל ושגרירויות זרות בישראל. הפצחנים השתמשו בתשתית סייבר שנמצאת בעיקר מחוץ לאיראן – בארצות הברית, ברוסיה ובהולנד – כדי לטשטש את עקבותיהם.[128]

בשנת 2017 התחזו OilRig לחברת תוכנה ישראלית ידועה ושלחו הודעות דואר אלקטרוני זדוניות בעלות אישורי אבטחה מזויפים ל־120 סוכנויות ממשלתיות, מוסדות אקדמיים, חברות מחשבים ואנשים פרטיים בישראל. מתקפת הדיוג ניצלה נקודות תורפה בתוכנת וורד של מיקרוסופט כדי לפרוץ לרשימות אנשי הקשר של הקורבנות ולהשתמש בהן להרחבת התפוצה של התקיפה.[129] בתקיפות אחרות של OilRig נתקפו לפחות חמש חברות ישראליות לטכנולוגיית מידע, כמה מוסדות פיננסיים ושירותי הדואר; אתרים מזויפים התחזו לדף הרשמה לכינוס ב"אוניברסיטת אוקספורד" ולאתר להגשת מועמדות לעבודה; ואתר האינטרנט של ישראייר שוכפל כדי לשלוח דרכו קובץ אקסל זדוני ליעדי המתקפה.[130]

בשנת 2018 תקפו Charming Kittens, על פי דיווחים, מדעני גרעין ישראלים כדי להשיג גישה למידע רגיש. בהונאת דיוג מתמשכת נשלחו למדענים הודעות דואר אלקטרוני ובהן קישורים לאתר מזויף של "סוכנות ידיעות בריטית".[131] התקיפות הופעלו כמעט על בסיס יומי, ולפי אחד הדיווחים היו מעורבות בהן 11 קבוצות פצחנים של משמרות המהפכה.[132] באותה שנה, במבצע שיוחס לאיראן, נשלפו כמויות גדולות של מידע על מטרות ישראליות ואחרות במזרח התיכון, בארצות הברית, באירופה וברוסיה, וכן על חברות טלקומוניקציה ועל חברות תעופה וחלל גלובליות. הקמפיין הממוקד נמשך ככל הנראה שלוש שנים לפחות,

127 ClearSky Research Team, "Rocket Kitten 2 – Follow-Up on Iran Originated Cyber-Attacks," Clearsky.com, September 1, 2015.

128 ClearSky Research Team, "Iranian Threat Agent OilRig Delivers Digitally Signed Malware, Impersonates University of Oxford," *Clearsky.com,* January 25, 2017.

129 Gwen Ackerman and Alisa Odenheimer, "Israeli Official Says First Wave of Cyber Hack Was Thwarted," *Bloomberg*, April 26, 2017; Anshel Pfeffer, "Why Netanyahu Failed to Mention the Iranian Link to the Cyberattack on Israel," *Haaretz*, April 27, 2017.

130 Clearsky Research Team, "Iranian Threat Agent OilRig."

131 TOI Staff, "Iran Hackers Reportedly Tried to Phish Israeli Nuclear Scientists," *Times of Israel*, January 30, 2018.

132 NoCamels, February 1, 2018.

אך לא זוהה בזכות שימוש בסוס טרויאני לגישה מרחוק (Remote Access Trojan, RAT) שכבר הוכיח עצמו בעבר ותוכנן כך שיחמוק מכלי אנטי־וירוס ומאמצעי אבטחה אחרים.[133]

שנת 2019 סימנה תפנית מסוכנת בתקיפות הריגול האיראניות. קבוצה בהובלת איראן הפועלת מתוך סוריה ניסתה ככל הנראה לגייס אנשים בישראל לביצוע פיגועים. ייתכן שאיראן עמדה גם מאחורי המאמצים של חזבאללה ושל חמאס באותה תקופה להשתמש באינטרנט לגיוס ערבים ישראלים ופלסטינים למטרות טרור וריגול נגד ישראל.[134]

Pay2Key, קבוצה המזוהה ככל הנראה עם Fox Kittens, תקפה בשנת 2020 את התעשייה האווירית הישראלית. ייתכן שהתקיפה חדרה למערכות נגד טילים, לכטב"מים ולנשק מונחה שמייצרת החברה.[135] בשנת 2021 נחשפה תקיפה של Fox Kittens שהתפשטה במשך שנתיים במערכות של חברות ישראליות רבות וחדרה למידע מסווג ברמות שונות.[136] לא ברור אם התקיפה נגד התעשייה האווירית הייתה מרכיב במבצע הזה.

בשנת 2020 התחזו פצחנים איראנים לעמוס ידלין, ראש אמ"ן לשעבר וראש המכון למחקרי ביטחון לאומי (INSS) באותה עת. התקיפה התחזתה להודעת טקסט שהגיעה לכאורה מחשבון הוואטסאפ של ידלין, ובה בקשה מאנליסט ממכון אחר להגיב על מחקר של INSS שעדיין לא פורסם ושהתוקפים השיגו, מן הסתם שלא כחוק.[137]

בשנים 2020–2021 ביצעו Charming Kittens קמפיין דיוג נגד 25 מומחים אמריקנים וישראלים בכירים המתמחים במחקר גנטי, נוירולוגי ואונקולוגי. המניע למתקפה אינו ברור.[138] בשנת 2021 התחזה המודיעין האיראני באינסטגרם לנשים מושכות וניסה לפתות אנשי עסקים ישראלים לפגישות בחו"ל, לכאורה למטרות עסקיות או רומנטיות, אך למעשה כדי לפגוע בהם או לחטוף אותם.[139] קבוצת Agrius חזרה לפעול באמצעות קמפיין ריסוס

133 Zev Stub, "Newly-Found Iranian Cyber-Espionage May Pose 'Real Threat' to Israel," *Jerusalem Post*, October 7, 2021.

134 Yoav Zitun, "Shin Bet: Iran Tried to Enlist Israelis, Palestinians for Espionage, Terror," *Ynet*, July 24, 2019.

135 Tal Shahaf, *Ynet*, March 13, 2021; Amitai Ziv, "'Iranian Attacker Impersonating Russians': Inside Recent Attacks on Israel," *Haaretz*, May 5, 2021.

136 Dolev and Siman-Tov, "Iranian Cyber Influence Operations."

137 Hasson, "Iranian Hackers Posed as General Yadlin."

138 Demboski and IronNet Threat Research and Intelligence Teams, "Analysis of the Iranian Cyber Attack."

139 Yaniv Kubovich, "Iran Used Instagram to Try and Lure Israelis to Meetings Abroad, Shin Bet and Mossad Say," *Haaretz,* April 12, 2021.

סיסמאות נגד חשבונות Office של יצרנים ישראליים ואמריקניים המייצרים לווויינים, כטב"מים, מכ"מים ועוד. עשרים חברות נפרצו בהצלחה. תקיפה על מאגרי המידע של שירותי הדואר ושל כמה חברות פרטיות הצליחה בשנת 2022 לדלות פרטים אישיים של מאות אלפי אנשים.[140]

Charming Kittens עמדו בשנת 2022 מאחורי סדרת תקיפות על חברות ישראליות, ובכלל זה ספקים בתחום הביטחון, חברות טכנולוגיה ומוסדות פיננסיים, שנועדה לגנוב נתונים רגישים, לרבות קניין רוחני ומידע פיננסי.[141] בשנת 2022 ניסו Refined Kittens (APT33) לפרוץ את מערכות המחשוב של כמה סוכנויות ממשלתיות ישראליות, לרבות משרדי הביטחון והחוץ ומערך הסייבר הלאומי, כדי להשיג מידע רגיש על היכולות הצבאיות של ישראל. הפצחנים השתמשו במגוון שיטות, כגון הודעות דיוג בדואר האלקטרוני ואתרים זדוניים. נזק מסוים נגרם לשרתים בודדים של משרד הביטחון, והפצחנים הצליחו להשיג גישה לכמה מן המערכות שהותקפו. שבועות ספורים לאחר מכן תקפו שוב Refined Kittens את משרד הביטחון ושיבשו כמה אתרי אינטרנט.[142]

בשנת 2022 השתמשו Helix Kittens (APT34, OilRig) בדיוג ממוקד, בהנדסה חברתית ובשיטות אחרות כדי לתקוף מוסדות פיננסיים ישראליים, ובהם בנק הפועלים ובנק לאומי. התקיפה הצליחה לפרוץ למערכות היעד ולגנוב נתונים רגישים, לרבות מידע על לקוחות ורשומות פיננסיות, אך לא גרמה להפסדים כספיים גדולים. בשנת 2022 תקפו APT36 בהצלחה את משרד האוצר והשיגו גישה למידע רגיש על המערכת הפיננסית של ישראל.[143]

ב־2023 חדרו Charming Kittens למערכות של 32 חברות ישראליות מענפי הביטוח, הרפואה, מערכות המידע, השירותים הפיננסיים ועוד.[144] מטרת התקיפות אינה ידועה, אך סביר להניח שהן נועדו להשיג מידע רגיש, וייתכן שגם לגרום מבוכה לישראל.

140 Demboski and IronNet Threat Research and Intelligence Teams, "Analysis of the Iranian Cyber Attack"; Yuval Mann, *Ynet,* November 10, 2021.

141 David E. Sanger, *New York Times*, January 24, 2022; Dan Lamothe and Felicia Sonmez, *Washington Post*, January 25, 2022.

142 Reuters, February 15, 2022; Eli Lake and Naama Stern, Reuters, February 25, 2022; Judah Ari Gross, *Times of Israel*, February 24, 2022; FireEye Mandiant Report, February 2022 Cyberattack on Israeli Government Websites.

143 FireEye Mandiant report, February 14, 2022; Microsoft Threat Intelligence Center, January 24, 2022; Judah Ari Gross, *Times of Israel*, April 25 and April 27, 2022.

144 Raphael Kahan, "Iranian Hackers Break into Networks of More than 30 Companies in Israel," *Ynet*, November 9, 2023, https://www.ynetnews.com/business/article/rjrs5pn02.

באותה שנה ביצעו קבוצות פצחנים המזוהות עם משמרות המהפכה, לרבות LionTail, את אחד ממבצעי המודיעין המתוחכמים ביותר שבוצעו נגד ישראל (ונגד ערב הסעודית וירדן) וגנבו מידע רב. אחת התקיפות חדרה למצלמות ישראליות שבבעלות פרטית המוצבות בסמוך לגבול לבנון הרגיש.[145]

תקיפות CNI (תודעה). מבצעי תודעה היו עד כה מרכיב מרכזי בפעולות הסייבר של איראן נגד ישראל. כמו מבצעי התודעה שלה נגד ארצות הברית ומדינות אחרות, גם מטרתם של מבצעי התודעה של איראן נגד ישראל היא להתסיס מחלוקות פנימיות, לסתור את עמדותיה של ישראל בנושאים חשובים ולחזק את ההרתעה הכללית של איראן.[146] מבצעי תודעה ממלאים תפקיד גם במאמציה הכוללים של איראן לבודד את ישראל ולחתור תחת הלגיטימיות הבסיסית שלה.

"תל אביב טיימס", אתר איראני מזויף בשפה העברית הפועל מאז 2013, זוכה לעשרות אלפי צפיות חודשיות בישראל. הוא גונב מאמרים מכלי תקשורת ישראליים ועורך בהם שינויים קריטיים שנועדו לתמוך באג׳נדה של איראן.[147] ב־2014 השיגו פצחנים המזוהים עם איראן שליטה זמנית על הבלוג ועל דף הטוויטר של צה"ל והזהירו כי הכור הגרעיני בדימונה נפגע מטילים ועומד להתפוצץ. צה"ל החזיר לידיו את השליטה על המערכת מהר למדי, אך בינתיים חששו אזרחים רבים מן הגרוע מכול.[148]

בשנת 2016 יצא לפועל מבצע תודעה מסוכן מאוד. אתר המזוהה עם איראן פרסם ציטוט כוזב של שר הביטחון דאז משה יעלון שאמר לכאורה שאם פקיסטן תשלח כוחות לסוריה כדי להילחם בדאעש, ישראל "תשמיד אותם במתקפה גרעינית". שר ההגנה הפקיסטני הגיב באזהרה פומבית כי "ישראל שוכחת שגם פקיסטן היא מדינה גרעינית".

145 Ronen Bergman, Aaron Krolik and Paul Mozur, "In Cyberattacks, Iran Shows Signs of Improved Hacking Capabilities," *New York Times*, October 31, 2023.

146 Tabatabai, *Iran's Authoritarian Playbook*, 15–19.

147 Times of Israel Staff, *Times of Israel*, September 6 and November 30, 2018; Stubbs and Bing, "Exclusive: Iran-Based Political Influence Operation."

148 Jerusalem Post Staff, *Jerusalem Post,* July 4, 2014; Siboni and Kronenfeld, "Iran and Cyberspace Warfare"; Kayla Ruble, "Syrian Hackers Hijack IDF Twitter Sparking Fears of Nuclear Leak," *Vice*, July 17, 2014; Mohammad J. Herzallah, "Israeli Fights Wire with Wire," *Newsweek*, July 27, 2009; TOI Staff, "Iran Hackers Reportedly Tried to Phish Israeli Nuclear Scientists."

משרד הביטחון הישראלי חשש מאוד מהסלמה אפשרית לעימות עם מעצמה גרעינית עוינת ומיהר להבהיר שהידיעה מזויפת.[149]

בשנת 2019 זוהו לפחות 350 חשבונות מזויפים בפייסבוק, בטוויטר ובטלגרם עם Countdown 2040, אתר איראני הטוען שישראל תחדל להתקיים בשנת 2040. החשבונות המזויפים התחזו לאתרי חדשות לגיטימיים והפיצו מדי חודש מידע בדוי לכחצי מיליון אנשים בישראל. הידיעות החדשותיות משוכתבות ב־Countdown 2040 באופן המעודד שיח מפלג בישראל על נושאים שנויים במחלוקת, כגון ביקורת על ראש הממשלה נתניהו, אי־שוויון כלכלי, הטרדה מינית, עוני ומערכת המשפט. הקמפיין נועד במקור להחריף את המתיחות בישראל על רקע הסכסוך הישראלי־פלסטיני, אך בעקבות ההכרזה על הקדמת הבחירות, התאימו אותו התוקפים בזריזות מבצעית מרשימה לקמפיין השפעה על תוצאות הבחירות.[150]

בשנת 2019, בניסיון נוסף לזרוע מחלוקת בישראל, פורסם באתר של מרכז בלפר באוניברסיטת הרווארד דיווח המבוסס לכאורה על הרצאה שנשא שם ראש המוסד לשעבר תמיר פרדו. בציטוט כוזב של פרדו שהופיע בדיווח נאמר ששר הביטחון אביגדור ליברמן, יליד רוסיה, הודח לאחר שנחשף כחפרפרת רוסית. בפועל – האתר של המרכז שוכפל, ליברמן הודח מסיבות אחרות לגמרי והמאמר כולו היה בדיה מוחלטת.[151]

מאז שנת 2020, אם לא קודם לכן, קבוצת Emennet Pasargad, אותה קבוצת האקטיביסטים איראנים שתקפו את הבחירות לנשיאות ארצות הברית באותה שנה, מפעילה מבצעי תודעה נגד ישראל. בשנים 2020–2022 היא התחזתה ל־Hackers of Savior, קבוצת האקטיביסטים פלסטינית, וניהלה ארבעה קמפיינים בסייבר נגד כמה מגזרים בישראל, בעיקר ביום ירושלים האיראני או במועד קרוב אליו. חברי הקבוצה התחזו גם לפושעי סייבר כדי לפתוח במבצע "פריצה והדלפה" (lock-and-leak) נגד מוקד טלפוני ישראלי. כדי להגביר את השפעת התקיפות, חברי הקבוצה משתמשים בהרחבה באתרי

149 TOI Staff, "Cyber Firm Says Three Iran-Run Sites are Targeting Israelis With Fake News," *Times of Israel,* September 6, 2018; TOI Staff, "Iran Duped Pakistan into Israel Nuke Threat as Tiny Part of Huge Fakery Campaign," *Times of Israel*, November 30, 2018.

150 Roi Rubenstein, "Report: Iranian Bot Army Trying to Influence Israeli Elections," *Ynet*, January 31, 2019; R. Shamir and E. Bachar, "Defending Israel Selections from Cyber Attack – What Should Be Done?" (January 2019), 12.

151 Scott Shane and Ronen Bergman, "New Report Shows How a Pro-Iran Group Spread Fake News Online," *New York Times*, May 14, 2019.

אינטרנט משלהם, בטלגרם, בפרופילים מזויפים ברשתות החברתיות ובפורומים של פריצה מקוונת ושל סחר לא חוקי. המטרה היא לערער את האמון ברשתות המותקפות, לגרום לנזק למוניטין שלהן ולאובדן כספי, להוכיח את חולשת הגנת הסייבר של ישראל ולקדם מסרים אנטי־ישראליים.[152]

בשנת 2020 ביקשו פצחנים איראנים להחריף את המתיחות בין ממשלת נתניהו לציבור ששררה על רקע טיפול הממשלה במשבר הקורונה. הפצחנים יצרו חשבונות בעלי מראה רשמי בפייסבוק ובאינסטגרם, וצברו 1,100 ו־9,500 עוקבים בהתאמה; עם זאת, לא הושקע מאמץ רב כדי לגרום לחשבונות להיראות אותנטיים.[153]

בשנים 2020–2021, עם דעיכת משבר הקורונה, פתחו פצחנים איראנים בקמפיין תודעה שנועד להעמיק את המשבר הפוליטי שישראל נקלעה אליו. זהותם של פילנתרופים יהודים אמריקנים נפרצה כדי לאסוף מידע על האופוזיציה של ראש הממשלה נתניהו. במידע זה השתמשו לאחר מכן חשבונות מזויפים בפייסבוק, בטוויטר, באינסטגרם ובטלגרם כדי להפיץ מסרים מתסיסים ואפילו אלימים שנועדו להכתים את האופוזיציה. לאחר שנתניהו הפסיד בבחירות דרש חשבון טלגרם לכלוא אותו ופרסם תמונה מזויפת שלו מאחורי סורג ובריח. הדמיון בין הטכניקות ששימשו את הפצחנים הללו ובין הטכניקות ששימשו את הפצחנים הרוסים בתקיפה על הבחירות בארצות הברית, מעיד על שיתוף פעולה אפשרי.[154]

פצחנים אחרים התחזו לפעילי אופוזיציה, הקימו אתר מזויף וניסו לשבש קבוצות וואטסאפ. פייסבוק הסירה שלושה חשבונות של פעילי אופוזיציה כביכול שפרסמו תוכן מסית, לרבות השוואות בין הימין הישראלי להיטלר. לתקיפה נוספת בפייסבוק היו 1,800 עוקבים, רובם אזרחים ישראלים שהפצחנים עצמם צירפו לרשימת העוקבים. בשנת 2021 תייג חשבון אינסטגרם באמצעות בוטים עשרות אלפי אזרחים ישראלים להודעות אופוזיציוניות. עשרה חשבונות פייסבוק וטוויטר שפעלו ביותר מתשעים קבוצות, רובן של הימין, פרסמו בשנת 2021 תוכן ביקורתי על השלטון דאז, ממשלת בנט־לפיד, וקראו להפגין נגד הממשלה.

152 Anna Ribeiro, "FBI Reveals Iranian Cyber Group Emennet Pasargad Executing Hack-and-Leak Operations Using False-Flag Personas," *Industrial Cyber*, October 21, 2022; Dennis Fisher, "FBI Warns of Attacks From Iranian Threat Group Emennet Pasargad," *Decipher*, October 21, 2022.

153 Facebook, *Threat Report The State of Influence Operations 2017–2020*, May 2021.

154 Sheera Frenkel, "Iranian Disinformation Effort Went Small to Stay Under Big Tech's Radar," *New York Times*, June 30, 2021; Omer Benjakob, "Iranian Accounts, Russian Tactics and Q: Israel Has Become a Disinformation Battlefield," *Haaretz*, April 21, 2021.

בכמה מן המקרים ניסו הפצחנים ליצור קשר ישיר עם פעילים פוליטיים המקורבים לראש הממשלה, ובמקרים אחרים הם התחזו לפעילים פוליטיים אמיתיים.[155]

פצחנים איראנים ניסו להתערב בבחירות בישראל בשנת 2022. לפני הבחירות קראו כ־40 חשבונות טוויטר מזויפים לפיצול של מפלגות הימין, ככל הנראה כדי להחליש אותן. בתקופת קמפיין הבחירות קראו אלפי ציוצים של פרופילים השייכים לכאורה לישראלים שמאלנים להחרים את הבחירות. הפרופילים פרסמו גם הודעות שנאה נגד הימין ונגד החרדים. מסרים דומים הופצו ביום הבחירות עצמו כדי לנסות להקטין את שיעור ההצבעה.[156] במקרה זה ייתכן שמטרת הפצחנים הייתה להחליש את המרכז־שמאל ולהוביל לניצחון הימין כדי לפגוע במעמדה הבינלאומי של ישראל ולהחליש את עמדתה האסטרטגית, כפי שאכן קרה. כמדווח, הניסיונות להשפיע על תוצאות הבחירות לא צלחו.[157]

בשנת 2022 הופעל קמפיין תודעה איראני אחר כדי לעורר פילוג פנימי בישראל. פצחנים בפייסבוק, בטלגרם ובפלטפורמות אחרות של הרשתות החברתיות התחזו לקבוצה לאומנית חרדית כדי לעודד מחאות של הימין הקיצוני נגד השלטון, ללבות רגשות נגד המשטרה בקרב הציבור החרדי ולהפיץ את הדעה שצירוף מפלגה אסלאמית לקואליציה פירושו שמוסלמים שולטים בישראל. התוקפים עשו מאמצים ניכרים כדי שהאתר המזויף ייראה אמיתי, יצרו דף של מאפייה פיקטיבית בעיר חרדית, השתמשו בזהות אמיתית של אדם חרדי שנפטר כמה שנים קודם לכן ועוד.[158]

בשנת 2022 פרסמה קבוצת הפצחנים האיראנית Moses Staff תמונות אישיות ומסמכי מס של ראש המוסד; הם ועוד מידע רפואי עליו נגנבו מן הטלפון האישי של אשת ראש המוסד. התקיפה נועדה, ככל הנראה, לגרום לראש המוסד מבוכה משום שהוא הגורם הבכיר המופקד על המאמץ הישראלי לבלום את איראן, אך גם כדי להרחיב את ההשפעה

155 Frenkel, "Iranian Disinformation Effort"; FakeReporter, "Rolling in the Deep: An Iranian Cross-Platform Influence Operation Summary."

156 Omer Benjakob, "Israel Election: Twitter Purges Foreign Influence Op to Suppress Voting," *Haaretz*, November 1, 2022; FakeReporter, "Rolling in the Deep."

157 עמוס הראל, "הפייק סביב המחאה: מסורת סובייטית, חיקוי איראני, עזרה ישראלית", **הארץ**, 11 ביוני 2023.

158 Tom Bateman, "Iran Accused of Sowing Israel Discontent With Fake Jewish Facebook Group," *BBC*, February 3, 2022.

הציבורית של התקיפה. Moses Staff פרסמו גם תמונות קשות מפיגוע טרור בירושלים שנגנבו ממצלמות אבטחה לא מוצפנות, כדי להוסיף ולהעצים את השפעת התקיפה.[159]

מיוני 2022 ועד מאי 2023 ביצעו גורמים המזוהים עם איראן, בעיקר Emennet Pasargad, 24 תקיפות תודעה, לעומת שבע בלבד ב־2021. רוב התקיפות התמקדו בישראל, כמו גם ביריבותיה של איראן במפרץ, ונועדו לעודד התנגדות פלסטינית, לזרוע פחד בקרב הציבור בישראל ולסכל את הנורמליזציה המתפתחת בינה ובין מדינות ערב.[160] קבוצות הפצחנים Hunters ו־NoVoice השתמשו במדיה החברתית, לרבות בוואטסאפ, בפייסבוק, בטוויטר, באינסטגרם ובטלגרם, כדי לנסות להחריף את המשבר הפנימי בישראל בעקבות "המהפכה המשפטית" שקודמה באותה תקופה. באחת התקיפות נקראו מתנגדי הרפורמה לתקוף שוטרים ומפגינים כאחד, ובמבצע בִּיוּש (shaming) אף הופצו צילומים של השוטרים, שמותיהם וכתובות מגוריהם. בתקיפה אחרת השתמשו הפצחנים בקבוצות וואטסאפ של תומכי הליכוד כדי לעודד עימותים עם המתנגדים "למהפכה המשפטית" ואף אלימות נגדם. תקיפות אחרות לעומתן עודדו התנגדות למפגינים התומכים ברפורמה.[161]

תקיפות משולבות. רוב תקיפות ה־CNA שאיראן ביצעה עד 2022 כוונו למדינות אחרות ולא לישראל, למעט חריגות בודדות ובראשן התקיפה הכושלת נגד מערכת המים של ישראל ב־2020. התקיפות נגד ישראל היו בעיקר למטרות שיבוש או ריגול, והיו גם כמה מבצעי תודעה. אולם באמצע שנת 2020 חל מפנה, ורוב התקיפות הפכו למשולבות – שילוב של תקיפות שיבוש, תקיפות ריגול, מבצעי תודעה ותקיפות כופרה.

בפרט מאז אמצע שנת 2022 איראן ממנפת את מבצעי התודעה שלה בסייבר כדי להעצים את יכולות הסייבר ההתקפיות שלה וכדי לנסות לערער את תחושת הביטחון של

159 Haim Golditch, *Ynet*, December 24, 2022; Yaniv Kubovich, "Iranian Hackers Post Footage of Jerusalem Bombing, Taken by Large Security Agency," *Haaretz*, November 24, 2022; Michael Horovitz, "Report: Iran Hacked Israeli Cameras a Year Ago; Defense Officials Knew, Didn't Act," *Times of Israel*, December 19, 2022; Itamar Eichner and Yuval Mann, *Ynet*, April 4, 2022.

160 Clint Watts, "Rinse and Repeat: Iran Accelerates its Cyber Influence Operations Worldwide," *Microsoft.com,* May 2, 2023.

161 David Siman-Tov, "Attempted Foreign Influence as a Challenge to Israel's National Resilience: Using the Judicial Overhaul Protests to Deepen Internal Rifts," *INSS Insight* No. 1741, June 26, 2023; Bar Peleg, Josh Breineer and Omer Benjacob, "Iran, Russia or Both, A Foreign Influence Operation to Incite Violence in Israel is Reemerging," Haaretz, July 3, 2023.

ישראל. הרעיון הבסיסי היה להשתמש במבצעי תודעה כדי לקדם שינוי פוליטי ואסטרטגי ההולם את יעדי המשטר.[162] תקיפות שהתחזו לתקיפות כופרה הופעלו בעיקר למטרות של מבצעי תודעה.

בשנת 2020 נאלצה חברת התוכנה הישראלית "סאפיינס" לשלם 250 אלף דולר בביטקוין בעקבות מתקפת כופרה שבה פצחנים המזוהים עם איראן איימו להשבית את כל המערכת שלה. חברת "טאואר סמיקונדקטור" שילמה כופר של כמה מיליוני דולרים כדי שלא להפסיד ולו יום אחד של זמן ייצור. ייתכן שהתקיפה הייתה מרכיב בקמפיין רחב של Static Kittens נגד חברות ישראליות מובילות שנועד להיראות כמו תקיפת כופרה, אך בפועל היה דומה לתקיפת "שאמון" ההרסנית נגד חברת "ארמקו" הסעודית. התקיפה פגעה במערכות ההפעלה, "הגביע הקדוש" של תקיפות הסייבר, ולא רק במערכות המידע של חברת "טאואר סמיקונדקטור".[163]

באותה שנה הפעילה קבוצת Black Shadow (כנראה כינוי של Agrius, או APT36) תקיפת כופרה נגד "שירביט", חברת ביטוח הנותנת שירות בעיקר לעובדי ממשלה, לרבות עובדים של סוכנויות ביטחון רגישות כגון השב"כ. הפעם הציבו הפצחנים בכוונה מועדים לא מציאותיים לתשלום הכופר, וכאשר סירבה "שירביט" לשלם, פורסמו הנתונים הגנובים באינטרנט. במידע שפורסם היו, בין השאר, שמות המבוטחים, הסוכנויות שהם עבדו בהן, רישומים רפואיים חסויים, תכנים של שיחות וואטסאפ, כתובות מגורים ודואר אלקטרוני, מספרי תעודות זהות, מספרי טלפון, מספרי לוחיות רישוי ומספרים של כרטיסי אשראי.[164]

קבוצת הפצחנים Pay2Key ניצלה מערכות להתחברות מרחוק של עובדים כדי לבצע תקיפת כופרה מתוחכמת נגד שבע חברות ישראליות. ארבע מן החברות שילמו את הכופר.[165]

162 Microsoft Threat Intelligence, "Iran Turning to Cyber-Enabled Influence Operations For Greater Effect," May 2, 2023; Dolev and Siman-Tov, "Iranian Cyber Influence Operations."

163 Meir Orbach, *Calcalist*, June 14, 2020 and September 7, 2020; Omer Benjakob, "'Operation Quicksand': Iran-Linked Hackers Target Israel in 'New Cyberwar Phase,'" *Haaretz*, October 19, 2020; Amitai Ziv, "Cash-Strapped Over Coronavirus, Crime Organizations Unload Cyberattacks," *Haaretz*, September 21, 2020.

164 Bernard Brode, "The Shirbit Data Hack Was an Attack on National Security. Now What?" *Times of Israel*, December 18, 2020. According to one source, the attack against was conducted by Hezbollah. See Tal Shahaf, *Ynet*, October 29, 2021.

165 Omer Benjakob, "'It's Not About Money': Destructive Cyberattack Proves Israel Lacks One Key Thing," *Haaretz,* December 9, 2020; Hagay HaCohen, "Check Point Unveils New Iranian Cybercrime, Ransoming Companies' Data," *Jerusalem Post*, November

לאחר מכן תקפו Pay2Key את חברת "עמיטל", חברה המספקת תוכנות ייחודיות ל־70 אחוזים מחברות הלוגיסטיקה בישראל. לאחר שחדרו למערכת המחשוב של "עמיטל", פרצו Pay2Key למערכות של לפחות ארבעים מלקוחותיה, הדביקו גם אותם בכופרות, ובכך סיכנו חלק ניכר מכלל תעבורת המטענים האווירית והימית של ישראל. כמה מן החברות המותקפות היו ספקיות של שירותים לוגיסטיים למערכת הביטחון, ובמערכות שלהן עשוי היה להיות מידע רגיש על יבוא ויצוא נשק. לפחות שלוש מהן היו ספקיות של השירותים הלוגיסטיים המורכבים שנדרשו להפצת חיסון הקורונה.[166]

בתקיפה אחרת גנבו Pay2Key מידע קנייני על מוליכים למחצה חדשים שהיו אז בפיתוח של Havana Labs, חברת בת ישראלית של אינטל; המידע שנגנב היה חיוני לתוכניות העסקיות העתידיות של אינטל.[167] לאחר שנחשפה בשנת 2021 תקיפת ה־CNE שביצעו Pay2Key נגד התעשייה האווירית בישראל, עברה הקבוצה לתקיפה מסוג "פריצה והדלפה" והפיצה את הפרטים של כאלף משתמשים. בשלב זה תקפו Pay2Key כבר יותר מ־80 חברות ישראליות; רוב התקיפות היו מבצעי תודעה מבוססי תקיפות כופרה. טוויטר, טלגרם ואתר אינטרנט שתוכנן במיוחד למטרה זו שימשו להפצת המידע הגנוב, ואיומים רבים נגד ישראל פורסמו ברשתות החברתיות.[168]

בשנת 2021 תקפו Black Shadow בתקיפת כופרה את חברת הליסינג "KLS מימון רכב". כמו בתקיפה על "שירביט", ייתכן שגם המניע העיקרי של תקיפה זו היה להוכיח את חולשת ההגנות של ישראל ולפגוע במוניטין שלה. הפצחנים הצליחו למחוק חלק גדול משרתי החברה, ואפילו תוך כדי ניהול המשא ומתן על הכופר הפיצו מידע אישי באינטרנט

12, 2020; Meir Orbach, "Israeli Cybersecurity Giant Tracks Ranson Payments From New Cyber Attack to Iranian Nationals," *The Algemeiner*, November 12, 2020.

166 Tal Shahaf, *Ynet*, December 13, 2020 and December 15, 2020; Raphael Kahan, *Calcalist*, December 13, 2020; Orbach and Hazani, "Israel's Supply Chain Targeted in Massive Cyberattack."

167 Tal Shahaf, *Ynet*, December 13, 2020, December 15, 2020, and December 17, 2020; Raphael Kahan, Calcalist, December 13, 2020; Amitai Ziv, "Iran Suspected After Massive Cyberattack on Israeli Firms Revealed," *Haaretz*, December 13, 2020; Amitai Ziv, *Haaretz*, December 31, 2020; Tal Schneider, *Ynet*, December 20, 2020.

168 Tal Schneider, *Ynet*, December 20, 2020; Yonah Jeremy Bob, "Suspected Iranian Cyberattack Targets Israel Aerospace Industries," *Jerusalem Post*, December 20, 2020; Omer Benjakob, "Iranian Hackers Hit Top Israeli Defense Contractor, Data Leaked as Cyberattack Continues," *Haaretz*, December 20, 2020; Dolev and Siman-Tov, "Iranian Cyber Influence Operations."

בסדר גודל שגימד את התקיפה על "שירביט". הקבוצה פרצה גם לאתר האינטרנט של ארגון להט"ב מוכר בישראל. תחילה הם דרשו כופר, ולאחר מכן פרסמו שמות של כל חברי הארגון, תמונות מפורשות, העדפות מיניות, תוכן של צ'אטים והיסטוריה רפואית, לרבות חשיפה ל־HIV. תקיפה אחרת הדליפה את הנתונים האישיים של 1.5 מיליון מטופלים של רשת בריאות פרטית.[169] Networm, ככל הנראה רק שם חדש ל־Pay2Key, ביצעו תקיפות כופרה נגד חברת הלוגיסטיקה הישראלית "וריטס" ונגד הזכיינית הישראלית של רשת הבגדים H&M. שוב נראה שהמניע העיקרי היה לגרום למבוכה ולפגיעה במוניטין, וגם להרתיע את ישראל.[170]

בשנת 2021, בעקבות פריצת אבטחה נרחבת, הפיצו Moses Staff באינטרנט את הפרטים האישיים של כל החיילים המשרתים בחטיבה לוחמת של צה"ל, לרבות שמות, כתובות, מספרי טלפון, פרטי הכשרה, תפקיד, מצב רפואי נפשי ומצב סוציו־אקונומי. בצילומים שפורסמו בטלגרם נראתה הסביבה של מפעל הביטחון הרגיש "רפאל".[171]

בשנת 2022 שלחו Black Shadow הודעות דואר אלקטרוני ובהן דיוג ממוקד לעובדים של כמה מן המרכזים הרפואיים הגדולים בישראל. הם תבעו כופר של עשרה מיליון דולר בביטקוין ואיימו לפרסם מידע רפואי ופיננסי ומידע רגיש אחר על מטופלים אם דרישותיהם לא ייענו. הודעות הדואר האלקטרוני התחזו להודעות לגיטימיות ממקורות מהימנים, אך הכילו צרופות זדוניות. הפצחנים ניסו גם לנצל נקודות תורפה במערכות המחשוב של בתי החולים, לרבות במערכות של ציוד רפואי, כדי לשבש את פעילותם.[172]

בשנת 2023 תקפו Static Kittens את הטכניון. התקיפה נראתה בתחילה כמו תקיפת כופרה, אך היא הצפינה שרתים ושיבשה מערכות חיוניות. התוכנה הזדונית הותאמה במיוחד למערכות הטכניון, וככל הנראה התבססה על מיפוי כל הרשת של המכון. הטכניון נאלץ לנתק את מחשביו מן האינטרנט, להגביל את השימוש של הסגל ושל הסטודנטים

169 Adir Yanko, Tal Shahaf, and Hadar Gil-Ad, *Ynet*, November 1, 2021; Farnaz Fassihi and Ronen Bergman, "Israel and Iran Broaden Cyberwar to Attack Civilian Targets," *New York Times*, November 27, 2021.

170 Tal Shahaf, *Ynet*, March 13, 2021; Ziv, "Iranian Attacker Impersonating Russians."

171 Tal Shahaf and Nina Fuchs, *Ynet*, October 26, 2021; Tal Shahaf, *Ynet*, October 26, 2021; Michael Horovitz, *Times of Israel*, December 19, 2022.

172 Judah Ari Gross, *Times of Israel*, April 25, 2022 and April 27, 2022; Tomer Ganon, *Jerusalem Post*, April 12 and April 26, 2022.

במחשבים ולדחות כמה בחינות. הרטוריקה האנטי־ישראלית והפרו־פלסטינית הבוטה של הפצחנים בטלגרם מרמזת שייתכן שהמניע העיקרי שלהם היה פוליטי, לא פיננסי.[173]

חזבאללה

בתחילת שנות ה־80 של המאה ה־20 הקימה איראן את חזבאללה, ארגון השלוחים שלה בלבנון, לשתי מטרות: חיזוק הקהילה השיעית בלבנון והקמת בסיס מבצעי קדמי נגד ישראל. מאז סיפקה איראן לחזבאללה ארסנל טילים עצום, יכולות מתקדמות נגד מטוסים, כטב״מים, אמצעי לוחמה אלקטרונית ועוד.[174]

לפי אחד המקורות, משמרות המהפכה סיפקו תמיכה טכנית, חומרית ופיננסית מסיבית ליכולות הסייבר של הארגון. מקור אחר סבור שאיראן הפכה את חזבאללה לארגון הטרור המתוחכם והמשפיע ביותר כיום בתחום הסייבר, והוא משמש אמצעי בידי איראן להשגת יכולת הכחשה, להסטת תשומת הלב ממנה ולחיזוק אחיזתה בלבנון.[175] למרות ההערכות הללו, המידע הזמין על יכולות הסייבר של חזבאללה הוא מוגבל, וקשה להסיק ממנו מסקנות מושכלות. לא ידוע אם מיעוט המידע משקף את מיעוט יכולות הסייבר של חזבאללה או את יעילות הסודיות המבצעית שלו. סביר להניח שהאפשרות השנייה נכונה, לפחות חלקית.

תקיפות CNA (שיבוש והרס). בשנת 2015 נחשפה תקיפה רב־שנתית מתוחכמת של חזבאללה נגד צה״ל. התקיפה ניסתה לעקוף את ההגנות המובנות במחשבי צה״ל באמצעות תקיפת החברות המספקות לו את התוכנה.[176]

תקיפות CNE (ריגול). בשנת 2010 בוצעה תקיפה שאולי שימשה מודל לתקיפות מאוחרות יותר של חמאס. פצחנים של חזבאללה יצרו פרופיל פייסבוק מזויף של צעירה מושכת ששלחה ״בקשות חברות״ לחיילי צה״ל. כ־200 חיילים הגיבו וחשפו מידע על שמותיהם

173 TOI Staff, ״Israel Publicly Blames Iran for Cyberattack on Major University Last Month,״ *Times of Israel*, March 7, 2023; Roei Hahn and Yuval Mann, ״Leading Israeli Research Institute Falls Prey to Cyberattack,״ *Ynet*, December 2, 2023; Israel National Cyber Directorate, ״Iranian Government Sponsored Threat Actor Muddy Water Conducts Cyber Attack Against Israel,״ March 9, 2023.

174 Yonah Jeremy Bob, ״Iran Hackers Closer to Penetrating Israel US Drones Cyberdefense CEO,״ *Jerusalem Post*, November 21, 2022.

175 Pahlavi, ״Digital Hezbollah״; Benjamin R. Young, ״How Iran Built Hezbollah into a Top Cyber Power,״ *National Interest*, April 11, 2022.

176 Oded Yaron, ״Has Hezbollah's Cyber Spy Ring Been Exposed?״ *Haaretz*, April 8, 2015.

של אנשי צוות נוספים, ובכמה מן המקרים מסרו גם תיאורים מפורטים של בסיסים ואפילו סיסמאות. התקיפה התגלתה רק אחרי שנה.[177]

בשנת 2012 השיק צבא הסייבר של חזבאללה את Volatile Cedar, קמפיין ריגול שהשתמש בנוזקה מותאמת אישית כדי לתקוף ספקים צבאיים, חברות תקשורת, כלי תקשורת ואוניברסיטאות בישראל, בארצות הברית, בבריטניה, בכמה מדינות במזרח התיכון ובעוד מדינות. בשנת 2015 השתתפו פצחנים של חזבאללה בתקיפה שהוזכרה לעיל על "מאגר תמר", שהפעילה טכניקות של הנדסה חברתית נגד מגוון מטרות ישראליות, לרבות קציני צבא בדימוס וחברות לייעוץ ביטחוני.[178]

בשנת 2016 פרץ חזבאללה למערכות של מצלמות אבטחה במעגל סגור בבנייני ממשלה בחיפה ובתל אביב, לרבות במטה הכללי של צה"ל ובמשרד הביטחון, ופרסם את התמונות ברשתות חברתיות. אומנם הפריצה לא הייתה רגישה במיוחד, אך היא סיפקה לחזבאללה חומר תעמולתי ואפשרה לו לעקוב אחר הנכנסים לבניינים.[179]

קמפיין חמור יותר שבוצע באותה שנה השתמש ברשתות החברתיות כדי לגייס ערבים ישראלים ופלסטינים מן הגדה המערבית למטרות מודיעין וטרור. לפי דיווחים, אחד המעורבים היה בנו של מנהיג חזבאללה חסן נסראללה. באחת התקיפות הופעל גיוס מקוון לחטיפת ישראלים ולהעברת בני הערובה ללבנון, ובאחרת לביצוע פיגוע התאבדות. התקיפות החלו בדרך כלל ביצירת קשר דרך הפייסבוק ועברו אחר כך להתנהל בפלטפורמות של תקשורת מוצפנת. ישראל סיכלה את כל התקיפות הללו.[180]

בשנת 2021 הצליחו Cedars of Lebanon, פצחנים של חזבאללה, לנצל נקודות תורפה בשרתים של אורקל ושל אטלסיאן כדי לתקוף כ־250 חברות תקשורת, חברות אחסון אתרים וחברות תשתית בישראל, בארצות הברית, בבריטניה, במצרים, בירדן, בערב הסעודית,

177 Rid, *Cyber War Will Not Take Place*, 103.

178 Jeff Moskowitz, "Cyberattack Tied to Hezbollah Ups The Ante for Israel's Digital Defenses," *Christian Science Monitor*, June 1, 2015; Pahlavi, "Digital Hezbollah"; Lucas Ropek, "Hezbollah-Linked Cyber Unit Has Been Hacking Into Internet Companies for Years," *Gizmodo*, January 29, 2021; TOI Staff, "Iran Spying on Israel, Saudi Arabia with Major Cyberattacks," *Times of Israel*, June 14, 2015.

179 Ryan De Souza, "Israeli Security Camera Systems Targeted by Pro-Hezbollah Hackers," *Hackread*, February 21, 2016; Sagi Cohen, *Ynet*, June 15, 2015.

180 Michael Shkolnik and Alexander Corbeil, "Hezbollah's 'Virtual Entrepreneurs': How Hezbollah is Using the Internet to Incite Violence in Israel," *CTC Sentinel* 12, no. 9 October 2019.

באיחוד האמירויות, ברשות הפלסטינית ובעוד מדינות. לאחר שהתקיפות הצליחו לחדור למערכות היעד, עברו רובן להתנהל ידנית, אך כמה מהן אפשרו לתוקפים שליטה מרחוק. הקוד שהשתמשו בו היה דומה לקוד ששימש קבוצות פצחנים איראניות, ראיה לשיתוף פעולה הדוק. Cedars of Lebanon נחשפו לראשונה בשנת 2015, אך הצליחו להמשיך לפעול מתחת לרדאר בזכות אמצעים שנקטו כדי לא להשאיר עקבות דיגיטליים.[181]

בשנת 2022 דווח על תקיפת סייבר משותפת של איראן וחזבאללה על יוניפי"ל, כוח שמירת השלום של האו"ם המוצב בלבנון. התקיפה נועדה לגנוב חומרים הנוגעים לפעילות ולפריסה של יוניפי"ל.[182]

תקיפות CNI (תודעה). על פי דיווחים, צבא הסייבר של חזבאללה מנהל מחנות אימונים בלבנון כדי להקים "צבאות אלקטרוניים" ברחבי האזור. אלפי אקטיביסטים ברשתות החברתיות המזוהים עם איראן, מעיראק, מערב הסעודית, מבחריין, מסוריה וממקומות אחרים, עברו הכשרה מרוכזת בנושאי תעמולה ודיסאינפורמציה, כגון מניפולציה דיגיטלית של תמונות, ניהול חשבונות מזויפים ברשתות החברתיות, הפקת סרטוני וידאו ואמצעים לעקיפת הצנזורה של ספקיות המדיה החברתית.[183]

כמו באיראן, גם מבצעי התודעה של חזבאללה הם מרכיב חיוני באסטרטגיית הלוחמה האסימטרית ארוכת הטווח של הארגון. חזבאללה משתמש ברשתות חברתיות, כגון פייסבוק, טוויטר, יוטיוב, טלגרם, וואטסאפ וסיגנל, כדי להגיע דרכן לקהל אסלאמי ובינלאומי בסדר גודל חסר תקדים וכדי למצב את עצמו בראש "חזית ההתנגדות" לישראל. זאת ועוד, באמצעות הפלטפורמות החברתיות מגביר חזבאללה את השפעתם של מבצעי תודעה שמטרתם לפגוע במעמדה הבינלאומי של ישראל ולקדם לחץ בינלאומי עליה לעצור מבצעים

181 Amichai Stein, *Kan Hadashot*, January 28, 2021; Tal Shahaf, *Ynet*, January 28, 2021; Raphael Kahan, *Calcalist*, January 28, 2021; Yossi Hatoni, "Hezbollah Cyberattacked Hundreds of Companies, Also in Israel," *People and Computers*, January 28, 2021.

182 Amos Harel, Yaniv Kubovich, and Reuters, "Israel Accuses Iran, Hezbollah of Hacking UN Force in Lebanon," *Haaretz,* June 29, 2022; Emanuel Fabian, "Gantz Says Iran and Hezbollah Tried to Hack UN Peace Force, Steal Deployment Data," *Times of Israel*, June 29, 2022.

183 Wil Crisp and Suadad al-Salhy, "Exclusive: Inside Hizbollah's Fake News Training Camps Sowing Instability Across the Middle East," *The Telegraph*, August 2, 2020; Pahlavi, "Digital Hezbollah."

צבאיים טרם השיגה את יעדיה.[184] על פי דיווחים, מנהיג חזבאללה חסן נסראללה מאמין שמבצעי תודעה בסייבר יעילים להשגת מטרות חזבאללה אפילו יותר ממבצעים צבאיים.

זה זמן רב חזבאללה משלב לוחמה אסימטרית עם קמפיינים של תודעה. לחשבון הטוויטר של תחנת הטלוויזיה שלו אל־מנאר יש חצי מיליון עוקבים. הארגון גם מנהל יותר מ־20 אתרי אינטרנט בשבע שפות (ערבית, אזרית, אנגלית, צרפתית, עברית, פרסית וספרדית), מלבד הפעילות האמורה לעיל ברשתות החברתיות. הוא משתמש בפלטפורמות המדיה החברתית גם לגיוס לוחמים ופצחנים מרחבי העולם הערבי והבינלאומי.[185] לפי דיווחים, חזבאללה הצטרף לקמפיינים איראניים שנועדו לזרוע פילוג במדינות המערב. הוא חשוד גם בהפעלת מבצעי תודעה נגד אוכלוסיות ממוצא לבנוני בכמה מדינות במערב אפריקה.[186]

הג׳האד האסלאמי הפלסטיני

הג׳האד האסלאמי הפלסטיני הוא ארגון השלוחים של איראן בעזה. הארגון הצליח במשך שנתיים תמימות, 2012–2014, לחדור לתקשורת (הלא מוצפנת) של כטב״מים צה״ליים הפועלים מעל עזה. הפריצה אפשרה לו לנטר בזמן אמת את המודיעין שאספו הכטב״מים, וסייעה לו ולחמאס במאמצים להסתיר את הרקטות שלהם. הארגון פרץ גם למצלמות תנועה ישראליות, ובעזרת העדכונים החיים מהן הצליח לברר היכן נפלו טילים ולעקוב אחר תנועת כוחות צה״ל, וכך לשפר את דיוק השיגורים שלו. תקיפה אחרת עקבה אחר נחיתות והמראות של מטוסים בנמל התעופה בן־גוריון כדי לכוון טוב יותר את שיגורי הטילים בסבבי עימות ולשבש את התעופה האזרחית של ישראל. לעומת זאת, ניסיונות הג׳האד האסלאמי ליירט שיחות טלפון במערכות התקשורת הישראליות לא צלחו. איראן אימנה בעזה את פעילי הסייבר של הג׳האד האסלאמי, ובכמה מקרים גם באיראן עצמה.[187] יותר מזה לא ידוע הרבה על פעילות הסייבר של הג׳האד האסלאמי הפלסטיני.

184 Anshel Pfeffer, ״Israel Suffered Massive Cyber Attack During Gaza Offensive,״ *Haaretz*, June 15, 2009, Oded Yaron, ״Palestinians Behind Cyber Attacks on Israeli Army and Government Targets,״ *Haaretz*, February 16, 2015; Paul J. Springer, *Encyclopedia of Cyberwarfare* (ABC-Clio, 2017), 220–221.

185 Ron Ben-Yishai, *Ynet*, July 24, 2021; Pahlavi, ״Digital Hezbollah.״

186 Pahlavi, ״Digital Hezbollah.״

187 Gili Cohen, *Haaretz*, March 23, 2016; Yonah Jeremy Bob, *Jerusalem Post*, March 23, 2016.

15 קבוצות פצחנים המזוהות עם איראן ומשתפות פעולה זו עם זו במידה זו או אחרת, היו פעילות בשבועות הראשונים למלחמה עם חמאס שהחלה באוקטובר 2023. דומה שלפצחנים האיראנים לא היו תוכניות מוכנות מראש לתקיפות סייבר המותאמות למתקפת הפתע של חמאס; הם תקפו בתגובה לאירועים וניצלו הזדמנויות שהתעוררו. בתחילת המלחמה היו עיקר התקיפות לצורכי שיבוש וגרימת נזק, אך הן הוסבו תוך זמן לא רב לצורכי מודיעין והשפעה על התודעה.[188] בסוף החודש השלישי למלחמה לא נראה שלתקיפות אלו הייתה השפעה ממשית.

תקיפות CNA (שיבוש והרס) – בוצע מספר עצום של תקיפות, פשוטות למדי, להשחתה ולמניעת שירות מבוזרת (DDoS) נגד אתרי אינטרנט ישראליים, בפרט של חברות תקשורת ותוכנה, אך גם של מוסדות אחרים, כגון בנקים, מוסדות פיננסיים וגורמים ממשלתיים. בששת הימים הראשונים למלחמה ביצעו תקיפות ה־DDoS כמיליון ניסיונות התחברות בשנייה, ובשבועיים שלאחר מכן ירד מספר ניסיונות ההתחברות לכמאה אלף בשנייה (אתר ממוצע יכול להגיב לכעשרת אלפים בקשות כניסה המתרחשות בו־זמנית). נעשו גם ניסיונות חולפים לשבש את מערכות ההתרעה המוקדמת מפני ירי רקטות.[189]

אתר הג׳רוזלם פוסט הופל בתחילת המלחמה ליומיים–שלושה, כנראה כדי להקשות על ישראל להציג את עמדותיה בפני הקהילה הבינלאומית.[190] חמור מכך, קבוצת הפצחנים Agrius, המזוהה עם איראן, בשיתוף Cedars of Lebanon של חזבאללה, ניסו לשבש את הפעילות הרפואית של המרכז הרפואי הלל יפה. אומנם התקיפה סוכלה בטרם שיבשה את פעילות בית החולים, אך נגנב מידע רגיש רב על החולים.[191] בתקיפת דיוג נפרדת נשלחו הודעות דואר אלקטרוני מזויפות, לכאורה מעובדי חברת אבטחת סייבר, שהאיצו בנמענים

188 Israel National Cyber Directorate, ״The Cyber Dimension of the ׳Iron Swords׳ War: Insights and Means of Coping,״ December 24, 2023, https://www.gov.il/he/departments/news/published24122; ״Reactive and Opportunistic: Iran׳s Role in the Israel-Hamas War,״ *Microsoft.com*, November 9, 2023, https://www.microsoft.com/en-us/security/blog/2023/11/09/microsoft-shares-threat-intelligence-at-cyberwarcon-2023.

189 Raphael Kahan, ״Hamas Hackers Are Trying to Scare Israelis with Fake SMS Messages and News Sites,״ *Ynet*, October 25, 2023, https://www.ynetnews.com/business/article/hjoy4f8mp.

190 Raphael Kahan, ״Hamas Hackers.״

191 Israel National Cyber Directorate, ״Iran and Hezbollah Stand Behind the Cyberattack against the Ziv Hospital during the Iron Swords War,״ December 18, 2023, https://www.gov.il/he/departments/news/ziv181223.

להפעיל עדכוני אבטחה דחופים לתוכנות שברשותם. כדי שההודעות ייראו אמינות, הן אף כללו מידע אמיתי בנוגע לציוד שבשימוש הארגון המותקף. הנוזקה המצורפת להודעות אספה מידע על המערכות המותקפות בטרם השתמשה בתוכנת wiper כדי למחוק את כל מערכת המידע של הארגון. לתקיפה קדמה בחינה מדוקדקת של העובדים הטכניים בכל אחד מן הארגונים המותקפים כדי לגרום נזק מרבי.[192]

תקיפות CNE (ריגול) – עשרות חשבונות איראניים מזויפים במדיה החברתית, בפרט בטלגרם, ניסו לספק לחמאס מודיעין שימושי. בחלק מן המקרים הביעו הפרופילים המזויפים עניין בקשר רומנטי עם חיילי צה"ל כדי לפתותם לחשוף מידע על יחידותיהם ועל המבצעים שהיו מעורבים בהם. פניות נשלחו לאלפי חיילי צה"ל.[193]

תקיפות CNI (תודעה) – איראן הפיצה במדיה חברתית מידע רגשי טעון, מוטה ולעיתים אף שקרי לחלוטין כדי לקעקע את מעמדה של ישראל ולהטיל על ארצות הברית את האשמה בפשעי המלחמה שישראל ביצעה לכאורה. בדרך זו הגיעה איראן לקהל בינלאומי עצום בגודלו וסייעה לחמאס. חשבונות איראניים בפייסבוק ובטוויטר היללו את מעשי הטבח של חמאס נגד אזרחים ישראלים ועודדו התקפות נוספות נגדם.[194]

מבצעי ההסתה והדיסאינפורמציה נגד המתנגדים "למהפכה המשפטית", שהחלו עוד בטרם המלחמה, נמשכו בשבועותיה הראשונים. חשבונות פייסבוק, טוויטר, וואטסאפ, אינסטגרם וטלגרם שימשו לליבוי ולהעצמה של המתחים בחברה הישראלית בנוגע לסוגיות נפיצות, ובכלל זה מעמד ערביי ישראל ועמדות המזוהות עם הימין הישראלי הקיצוני.[195]

192 Israel National Cyber Directorate, "A New Fishing Attack from Iran Tries to Erase Information in Organizations," December 26, 2023, https://www.gov.il/he/departments/news/iranf5_2612.

193 Raphael Kahan, Ynet November 9, 2023

194 Steven Lee Myers and Sheera Frenkel, "In a Worldwide War of Words, Russia, China and Iran Back Hamas," *New York Times*, November 3, 2023, https://www.nytimes.com/2023/11/03/technology/israel-hamas-information-war.html.

195 Raphaela Goichman, "The Iranian Cyber Attacks – More Sophisticated and Destructive," *The Marker*, November 6, 2023, https://www.themarker.com/captain-internet/2023-11-06/ty-article/premium/0000018b-a44b-dc41-af9f-ef6bdcca0000.

חלק 5

מסקנות והמלצות

ההפגנות נגד המשטר ב־2009 ותקיפת הסטקסנט ב־2010 עוררו את העניין של איראן בתחום הסייבר, ומאז השתפרו יכולות הסייבר שלה במידה ניכרת. בעשור האחרון הפכה איראן לאחת המדינות הפעילות ביותר בלוחמת סייבר, והיא כנראה נמנית עם מובילות המעגל השני של השחקניות הגלובליות, או קרוב לכך. הכמות והתחכום של התקיפות שאיראן ניהלה גדלו, והיא הוכיחה יכולת להרוס, לשבש, לעוות, לחבל ולערער תשתיות לאומיות חיוניות, אינטרסים מסחריים, יכולות צבאיות, פוליטיקה פנימית, חוסן חברתי ודיפלומטיה בינלאומית. יכולותיה של איראן ימשיכו ככל הנראה להשתפר על בסיס יכולותיה שלה ובעקבות סיוע רוסי וסיני.

סביר להניח שאיראן סיפקה לחזבאללה יכולות סייבר מתקדמות, בדיוק כפי שעשתה בתחומים אחרים, אך הראיות הזמינות אינן מספיקות כדי לבסס מסקנה זו במלואה. קרוב לוודאי שהחוסר בראיות משקף את מגבלות המידע ולא את מגבלות יכולותיו של חזבאללה. על הג׳האד האסלאמי הפלסטיני יש מעט מידע; במקרה זה ייתכן שמיעוט המידע משקף את המציאות.

בלי לגרוע ולו במעט מעומק האיבה האיראנית כלפי ארצות הברית, ערב הסעודית ומעל לכול כלפי ישראל, חשוב להבין שרבות מפעולותיה של איראן בתחום הסייבר, כמו בתחומים אחרים, נושאות אופי תגובתי והגנתי. לשם המחשה, הפיתוח המהיר של יכולות הסייבר של איראן היה במידה רבה תגובה לתקיפת הסטקסנט, וכך היו גם תקיפת ״אבאביל״ נגד מוסדות פיננסיים אמריקניים והתקיפה נגד חברת ״ארמקו״ הסעודית. איראן הכינה והוציאה לפועל תקיפות סייבר לפני החתימה על הסכם הגרעין ב־2015 ואחריה, הגיבה באמצעי סייבר לחיסולו של מפקד כוח קודס של משמרות המהפכה קאסם סולימאני בידי כוחות אמריקניים, ועל פי דיווחים מנהלת בשנים האחרונות עם ישראל מערכת מתמשכת של מהלומות סייבר הדדיות, ובכלל זה התקיפות על מערכת המים של ישראל ועל נמל התעופה בן־גוריון.

לוחמה אסימטרית הפכה זה מכבר למרכיב חיוני באסטרטגיית הביטחון הלאומי של איראן, והיא נועדה לקזז את יתרונותיהן של יריבותיה החזקות. בניגוד ליריבי העבר של ישראל בעולם הערבי, איראן אינה מחפשת להביס את ישראל בטווח הקרוב משום שהיא

יודעת שאין ביכולתה להשיג מטרה זו. במקום זאת אימצה איראן אסטרטגיית התשה ארוכת טווח שנועדה לחבל בכוחה הצבאי של ישראל, לשחוק את מעמדה הבינלאומי ולערער את חוסנה החברתי כדי להוביל בסופו של דבר לקריסתה. עם השנים גברה חשיבותו של מרכיב הסייבר באסטרטגיית ההתשה הזאת, באסטרטגיית הביטחון הלאומי הכוללת של איראן ובכלים המדיניים שלה. הסייבר אף הולם מאוד את התרבות האסטרטגית של איראן ואת החשיבות הרבה שהיא מייחסת לעמימות, ליכולת הכחשה ולשימוש בשלוחים.

פעולות הסייבר של איראן התרחבו והפכו לגלובליות. היא תקפה מטרות בישראל, בארצות הברית ובערב הסעודית, וגם במדינות אחרות ברחבי העולם. עם הרשימה החלקית של המדינות שהיא תקפה נמנות צרפת, בריטניה, גרמניה, דנמרק, אלבניה, קנדה, אוסטרליה, ניו זילנד, הודו, יפן, בחריין, ירדן, עיראק, טורקיה ואפילו שתי בעלות בריתה החשובות ביותר – רוסיה וסין. סוגי המטרות שהיא תקפה מגוונים לא פחות: פרלמנטים; משרדי ממשלה, לרבות משרדי הגנה ומשרדי חוץ; ספקים בתחום הביטחון; מטרות צבאיות; משלחות דיפלומטיות; חברות תשתית חיונית, לרבות חשמל, מים ותקשורת, בקרת תעבורה אווירית, נפט וגז, בתי זיקוק וצינורות; מוסדות פיננסיים; ארגוני בריאות; חברות תעופה; חברות הייטק וייצור; ארגוני תקשורת; מוסדות אקדמיים; צוותי חשיבה; ארגונים לא ממשלתיים ועוד.

למרות היקף הפעילות של איראן בסייבר, היא עדיין רואה בו אמצעי משלים בלבד ולא אמצעי בפני עצמו. ככזה הוא נועד לתמוך ביכולות הדיפלומטיות, הכלכליות והצבאיות של איראן ולחזק את ההרתעה שלה. הסייבר נחשב גם אמצעי להגברה ולהעצמה של היכולות האסימטריות המסורתיות יותר של איראן, כגון טרור, שימוש בשלוחים ומבצעי תודעה בכלים מסורתיים. הסייבר הוא מכשיר חשוב במיוחד ללוחמה אסימטרית בעבור איראן מכיוון שיריבותיה המובילות, ובהן ארצות הברית וישראל, תלויות בסייבר הרבה יותר ממנה ולכן פגיעות יותר לתקיפה.

כמו מדינות אחרות, כגון ארצות הברית ובריטניה, גם איראן אימצה דוקטרינה צבאית גמישה ורחבת טווח. פירוש הדבר שהיא שומרת לעצמה את הזכות לנקוט הן פעולות התקפיות והן פעולות הגנתיות, בכל אמצעי שתמצא לנכון – קינטי, סייבר או שילוב שכיח יותר ויותר של תקיפות CNE, CNA ו־CNI.

דרך הפעולה של איראן מוכיחה בבירור שהיא לא אימצה מדיניות של "אי־שימוש ראשון" (no first use) בתחום הסייבר. לעומת זאת, אין כל סימן המעיד שאיראן שילבה בין אסטרטגיית הסייבר לאסטרטגיית הגרעין שלה – לא ברור אם היא רואה בתקיפות סייבר

מערכתיות מדרגת הסלמה הנמוכה מן הרמה הגרעינית, ואם שתי צורות התקיפה הן חלק מאסטרטגיית ביטחון לאומי אחת כוללת.

להלן סיכום הממצאים העיקריים של המחקר הנוגעים לתקיפות האיראניות מסוג CNE,CNA ו־CNI ולתקיפות משולבות, לעיתים גם עם תקיפות כופרה.

תקיפות CNA (שיבוש והרס). התקיפות "אבאביל" ו"שאמון" והתקיפות נגד אלבניה, בין השאר, הוכיחו את יכולתה של איראן לגרום לשיבוש כלכלי ניכר. התקיפות האיראניות נגד תשתיות לאומיות חיוניות בישראל, בארצות הברית ובאירופה עדיין לא גרמו להרס חמור, אך הוכיחו שיש בכוחן לעשות זאת. המודיעין האמריקני סבור כי איראן מסוגלת כיום לגרום לנזק, והתקיפות נגד מערכות אספקת המים ובקרת התעבורה האווירית של ישראל הוכיחו שיש בכוחן לגרום לנזק קטלני.

רוב תקיפות ה־CNA שאיראן הוציאה לפועל עד היום לא היו מתוחכמות, וההגנות של שחקניות הסייבר המתקדמות הספיקו בדרך כלל כדי למנוע נזק רב. רוב התקיפות היו נגד יעדים של המגזר הציבורי והפרטי שאינם מוגנים היטב, ובכך העניקו תוקף, לפחות חלקית, לטענה שההגנה על רוב המטרות הישראליות והמערביות החשובות תצליח להתמודד עם מרבית התקיפות פרט למתוחכמות ביותר. עם זאת, השחתות לא מתוחכמות ושיבושים של אתרי אינטרנט מסחריים וממשלתיים שביצעה איראן הצליחו לגרום לאי־נוחות לא מבוטלת ולהשפיע פסיכולוגית על הציבור או על אמון הצרכנים.

המידע הזמין אינו מספיק כדי להעריך במלואה את יכולתה של איראן לערוך מבצעי סייבר צבאיים אפקטיביים ומתמשכים, בניגוד לתקיפות על מטרות אזרחיות ומסחריות המוגנות פחות. מסיבות ברורות המדינות המותקפות וגם איראן עצמה נמנעות מלחשוף את יכולות הסייבר הצבאיות שלהן או פרטים על תקיפות סייבר צבאיות שהופעלו נגדן. איראן גם עדיין לא הראתה יכולות סייבר ברמה לאומית מערכתית. עם זאת, ייתכן שהיא שומרת את היכולות המתקדמות ביותר שלה לנסיבות "המתאימות". ברי שתחום הסייבר אכן מספק לאיראן ולבעלות בריתה ארגז כלים חשוב, שבאמצעותו היא יכולה לנהל מתחת לרדאר מבצעים שניתנים להכחשה.

תקיפות CNE (ריגול). עצם אופיו החשאי של עולם הריגול מקשה להעריך במלואה את האפקטיביות של תקיפות ה־CNE שאיראן ביצעה עד כה. לכל הפחות הן היו רבות והשיגו מידה מסוימת של מידע מסווג בעל משמעות. תקיפות CNE נועדו להשיג כמה מטרות. חלקן נועדו לאסוף מידע מודיעיני על תעשיות ביטחוניות, על תוכניות לפיתוח נשק, על יכולות

צבאיות כוללות, על מדיניות הגרעין של ישראל ועל החשיבה המדינית והאסטרטגית של ארצות הברית, ישראל והמערב. אחרות נועדו לסייע בהכנה של תקיפות CNA ו־CNI עתידיות, לרבות נגד חברות ביטחוניות, או כדי להשיג תובנות על היכולות המדעיות והטכנולוגיות של ישראל ומדינות אחרות. מבצעי CNE לגיוס מחבלים ולהכנה לפיגועי טרור הם איום גובר.

היתרון המודיעיני שאיראן וגורמים אחרים הרוויחו לכאורה מן התקיפות על החברות "שירביט" ו"KLS מימון רכב" הוא המקבילה הישראלית לנזק שנגרם לארצות הברית מן התקיפה הרוסית הידועה לשמצה על חברת SolarWinds (שגם ישראל הייתה קורבן משני שלה). המחדל המודיעיני שנחשף בתקיפות נגד "שירביט" ו־KLS הועצם באמצעות קמפיין התודעה האיראני שבוצע לאחריהן והפיץ את המידע הגנוב באינטרנט כדי לפגוע במוניטין של ישראל.

השימוש של איראן בתקיפות CNE למעקב אחר מתנגדי משטר באיראן ומחוצה לה ולדיכויים הוא, על פי דיווחים, אפקטיבי במיוחד. השליטה של איראן בעולם הסייבר באמצעות רשת NIW ובאמצעות מגוון כלי סייבר אחרים משמשת את המשטר כדי לדכא סבבים חוזרים של מחאות נגדו ומסייעת לו לבצר את יציבותו לטווח הארוך.

תקיפות CNI (תודעה). השימוש הנרחב של איראן במבצעי תודעה רק הולך וגדל. כמה מן המבצעים ניסו ליצור שסעים ומחלוקות פנימיות ולהחריפם, להשפיע על תהליכי בחירות ולערער את החוסן החברתי במדינת היעד, כפי שהוכיחו התקיפות החוזרות של איראן על מערכות הבחירות בארצות הברית ובישראל. תקיפות אחרות נועדו לשבש את היחסים בין מדינות ולהצית משברים שיש בכוחם להסלים, לעיתים אף לרמה הגרעינית, כמו במקרה של ישראל ופקיסטן. היו גם תקיפות שגרמו לנזק כספי לחברות פרטיות בעולם ולפגיעה במוניטין שלהן. אולם עד כה אף לא אחת מהן התקרבה להיקף ולתחכום של התקיפות שניהלה רוסיה נגד מערכת הבחירות האמריקנית ב־2016, ובפועל יעילותן הייתה מוגבלת. לא ידוע גם על מבצעי תודעה איראניים בסייבר ששיבשו תהליכים פוליטיים וממשלתיים חשובים או שעוררו מחלוקת חברתית גדולה. למרות זאת מספר התקיפות הללו עולה והדאגה גוברת.

מבצעי תודעה בסייבר הם מרכיב במאמצי המשטר האיראני לשמר את שלטונו, והם סיפקו לאיראן ולשלוחיה מגוון פלטפורמות יעילות להגיע דרכן למספר עצום של אנשים ברחבי העולם באופן ישיר ומיידי ובעלות מינימלית. מבצעי הסייבר גם סיפקו לאיראן כלים חדשים ובעלי ערך ליצירת לחץ בינלאומי על ישראל לעצור או לצמצם פעולות צבאיות

בטרם תשיג את יעדיה – הייתה להם השפעה שלילית על יכולתה של ישראל לנהל מלחמה ביעילות ועל מעמדה הבינלאומי.

תקיפות משולבות. השימוש הגובר בתקיפות CNA, CNE ו־CNI משולבות, לרוב גם עם תקיפות כופרה, הניב לאיראן תוצאות טובות למדי. דוגמה מייצגת היא ההפצה באינטרנט של מידע אישי על חברי קהילת הלהט"ב בישראל ועל כל חיילי חטיבה לוחמת של צה"ל. השימוש הרווח בתקיפות כופרה לשם השגת מידע ולא לשם רווח כספי הוא מאפיין ייחודי של העימות בין איראן לישראל.[196]

דרך הפעולה של איראן בסייבר עד כה שופכת אור על שלוש סוגיות קריטיות שהעסיקו את אנשי הביצוע בתחום הסייבר ואת התאורטיקנים. ראשית, היא מוכיחה את החשיבות שמייחסת איראן לתחום הסייבר לא רק משום היותו אמצעי להשגת יעדיה הפוליטיים והצבאיים, אלא גם משום שבשימוש בו יש סיכון נמוך להסלמה. במהלומות ההדדיות בין איראן לישראל בממד הסייבר ובממד הקינטי נראה שסכנת ההסלמה לא הרתיעה במידה רבה מפני המשך התקיפות או מפני עליית מדרגה בהן.

במבט לאחור, לאיראן הייתה סיבה טובה שלא לחשוש מהסלמה. הניסיון מלמד שארצות הברית הגיבה לתקיפות סייבר באמצעים קינטיים בשתי הזדמנויות בלבד, אף לא אחת מהן נגד איראן. על פי דיווחים, ישראל הגיבה לתקיפות סייבר באמצעים קינטיים רק פעמיים, בשני המקרים נגד חמאס, והשתמשה באמצעי סייבר בתגובה לתקיפות סייבר במקרים בודדים בלבד.[197] לפי דיווחים, ישראל אכן הגיבה לתקיפה האיראנית על מערכת המים שלה בתקיפה קשה יותר על נמל איראני; על תקיפה זו הגיבה איראן בתקיפות נוספות, אם כי מוגבלות בבירור, על מערכת המים של ישראל ועל מטרות אחרות. אולם שום צד לא המשיך להסלים. התקיפות המשולבות שאיראן ניהלה נגד ישראל בשנים האחרונות היו ללא ספק משבשות ויקרות, אבל לא קרובות להסלמה כמו מתקפות על תשתיות חיוניות או על מטרות צבאיות.

שנית, אם אכן נכונה הטענה כי רוב היעדים המערביים והישראליים החשובים מוגנים ברמה החורגת מיכולותיה של איראן, היא תומכת באסכולה המקצועית הטוענת כי הסייבר

196 Microsoft Threat Intelligence, "Iran Turning to Cyber-Enabled Influence Operations For Greater Effect," May 2, 2023; Dolev and Siman-Tov, "Iranian Cyber Influence Operations."

197 Borghard and Lonergan, "Cyber Operations"; Catalin Cimpanu, "Israel Bombed Two Hamas Cyber Targets," *The Record,* May 19, 2021; BBC Staff, *BBC*, June 9, 2021; Tal Shahaf, *Ynet*, May 21, 2021.

הופך בהדרגה לכלי הגנתי במקום התקפי. כאמור, יש גם הסבורים שיכולתה של איראן לגרום לנזק משמעותי לשחקניות סייבר מתוחכמות אף פוחתת.

שלישית, לעומת מומחי הסייבר הטוענים שעולם הסייבר מחזק שחקניות חלשות בשל האמצעים האסימטריים הנוספים שהוא מעמיד לרשותן כדי להתמודד עם עוצמתן הגדולה של יריבותיהן, יש מומחים הגורסים כי היכולות הטכנולוגיות המתוחכמות הנדרשות לשימוש יעיל בסייבר רק מחזקות את המדינות המתקדמות ממילא. נראה כי הניסיון במקרה האיראני מטה את הכף לטובת האסכולה השנייה. השימוש של איראן ביכולות הסייבר שלה הוא בהחלט מרכזי, אבל נראה שישראל, ארצות הברית ומדינות המערב מנצלות את הסייבר לצרכים סוציו־אקונומיים, דיפלומטיים וצבאיים רבים יותר. יתרה מזו, מדינות אלו מנצלות היטב כמה מן היתרונות הצבאיים האסימטריים שהסייבר מעניק לאיראן נוסף על הפעלת היכולות הקינטיות החזקות שלהן, ולכן נהנות משני העולמות. במילים אחרות, בשקלול הכולל הכף נוטה לטובת המדינות המתקדמות.

רביעית, אם הערכת איום הסייבר האיראני מתבססת על מספר התקיפות המוצלחות החשובות שהתרחשו עד היום ועל התוצאות שהן גרמו בפועל, אזי האיום הוא משמעותי אך מוגבל. מנגד, אם ההערכה מתבססת על הפוטנציאל הריאלי לשיבוש ולנזק עתידיים, אזי אי אפשר להתעלם מן האיום המתעצם. לכן לישראל אין ברירה אלא להמשיך להשקיע במערכת הסייבר האקולוגית שלה, בהגנת הסייבר האזרחית וביכולות צבאיות הגנתיות והתקפיות.

אסטרטגיית הסייבר של המגזר הציבורי והפרטי בישראל הייתה מן הראשונות מסוגה והתבססה על החלטות הממשלה שהתקבלו בשנים 2011–2015. אלא שהרבה השתנה מאז, ונדרשת בחינה מחודשת ומעמיקה. עם התחומים המחייבים בחינה מחודשת נמנים, בין היתר, המערכת הרגולטורית, המערכת האקולוגית, החוסן המערכתי, שיתוף הפעולה הבינלאומי והתיאום בין הגורמים השונים. האסטרטגיה החדשה חייבת לכלול יעדים ברורים ותוכנית עבודה רב־שנתית המבוססת על אמות מידה מוגדרות היטב.

צה״ל גיבש דוקטרינת סייבר מבצעית, אך לא אסטרטגיית סייבר צבאית כוללת. יתרה מזו, חלפו כבר שמונה שנים מאז החליט צה״ל להקים פיקוד סייבר מאוחד, ואז השהה את ההחלטה עד לבחינה נוספת.[198] כדי למקסם את יכולות הסייבר של ישראל, על צה״ל

198 Charles D. Freilich, Matthew S. Cohen, and Gabi Siboni, *Israel and the Cyber Threat: How the Start-Up Nation Became a Global Cyber Power* (Oxford: Oxford University Press, 2023), 250, 256, 257, 309.

לגבש אסטרטגיית סייבר צבאית כוללת ולשלבה עם שאר מרכיבי הכוח הלאומי של ישראל לכדי אסטרטגיית ביטחון לאומי אחת כוללת. יכולות סייבר אינן עומדות בפני עצמן, ואין להתייחס אליהן כך. על התשובה לשאלה כיצד ייראה מבנה הכוח החדש יש מחלוקת; כך או כך, יש לתת מענה לסוגיה.

כיום אין פורום סטטוטורי הכפוף לממשלה ואחראי בפועל לקביעה ולתיאום של סדרי העדיפויות הצבאיים והמודיעיניים בסייבר, לשילוב אסטרטגיות הסייבר האזרחיות והצבאיות ולהקצאת האחריות הארגונית ליישומן. אומנם יש הסדר בלתי פורמלי,[199] אבל הוא אינו ממצה את הפוטנציאל של ישראל, ויש לעדכנו.

את הבסת היריב, במובן המסורתי של שלילת יכולתו או ערעור רצונו להמשיך להילחם, אי אפשר להשיג באמצעי סייבר בלבד. במקום זאת, ישראל צריכה לחתור ל"עליונות סייבר" – היכולת להסב פגיעה או נזק ליריב שיהיו בלתי נסבלים בעבורו, או להפחית את חומרת התקיפות על ישראל לרמה שתאפשר לה להמשיך לתפקד ללא הפרעה ניכרת. אבל גם עליונות סייבר אינה עומדת לבדה, ויש לשאוף לעליונות מצטברת רב־תחומית,[200] כלומר ליישום הדרגתי מצטבר של כל מגוון היכולות העומדות לרשות ישראל (סייבר, קינטיות, דיפלומטיות וכלכליות). עליונות סייבר מודיעינית חשובה במיוחד בסביבת האיומים הקשה והייחודית של ישראל, הן למטרות התרעה מוקדמת והן ליכולות המודיעין הכוללות שלה.

שמירה על עליונות סייבר פירושה טיפוח מאגר לאומי של אנשי הסייבר המוכשרים ביותר בתחום האזרחי, המסחרי, האקדמי והצבאי, אלא שישראל מתמודדת עם מחסור ניכר בהון אנושי זה.[201] יש לפתח את תחום הסייבר בבתי הספר, באוניברסיטאות ובתוכניות ההכשרה למבוגרים. על צה"ל וסוכנויות המודיעין להמשיך לבחון דרכים חדשות לגיוס, להכשרה ולשימור של כוח אדם. הפיתוי של המגזר הפרטי, בארץ ובחו"ל, נותר אתגר לא מבוטל.

ישראל חייבת לגבש אסטרטגיה לאומית להתמודדות עם מבצעי תודעה חתרניים בסייבר שנועדו להחריף מתחים חברתיים, להשפיע על השיח הציבורי ולשבש תהליכי בחירות. ארצות הברית, בריטניה וצרפת הן רק חלק מן המדינות הדמוקרטיות שהחלו לטפל באיום זה, וישראל יכולה ללמוד מן הניסיון שלהן.

תוכנית הגרעין האיראנית נותרה האיום הצבאי הגדול ביותר על הביטחון הלאומי של ישראל. "דוקטרינת בגין" לעצירת תפוצת הגרעין יושמה עד היום פעמיים בלבד, נגד תוכנית

199. Freilich, Cohen, and Siboni, *Israel and the Cyber Threat,* 259.
200. Freilich, Cohen, and Siboni, *Israel and the Cyber Threat,* 79–80.
201. Freilich, Cohen, and Siboni, *Israel and the Cyber Threat,* 198.

הגרעין של עיראק ב־1981 ונגד תוכנית הגרעין של סוריה ב־2007. עד כה היא לא יושמה נגד תוכנית הגרעין האיראנית, לפחות לא במובן הקלסי של תקיפה אווירית. יש הסבורים כי ריבוי התקיפות הקינטיות ותקיפות הסייבר שישראל ניהלה, על פי דיווחים, כדי לחבל בתוכנית האיראנית, לעכב ולדרדר אותה, הן אמצעי חדש ליישום הדוקטרינה. מן המאמצים הללו וירוס סטקסנט הוא הידוע ביותר, ואולי גם המבשר הראשון של המציאות החדשה.[202] כך או כך, ישראל חייבת להבטיח שיהיו בידיה היכולות הקינטיות ויכולות הסייבר שימנעו מאיראן להשיג אי פעם יכולת גרעינית מבצעית.

ולבסוף, ארצות הברית היא השותפה העיקרית של ישראל בתחום הסייבר, כמו בכל שאר התחומים, ושיתוף הפעולה האזרחי והצבאי בין שתי המדינות הוא נרחב. בניגוד לרוב שיתופי הפעולה הצבאיים בין שתי המדינות, יכולות הסייבר של ישראל הן בעיקר תוצר של פיתוח מקומי, ולכן יש לה הרבה להציע לארצות הברית, ולא רק לקבל ממנה. חשוב שישראל תפעל להרחיב את שיתוף הפעולה בסייבר ככל האפשר, אך בה בעת למזער את הסיכונים לחופש הפעולה העצמאי שלה. עליה למסד שיח סייבר רשמי וקבוע בין גורמי הממשל הרלוונטיים ולנסח אותו במזכרי הבנות חדשים ומורחבים.[203]

202. Freilich, Cohen, and Siboni, *Israel and the Cyber Threat,* 318.
203. Freilich, Cohen, and Siboni, *Israel and the Cyber Threat,* 221, 330.

מקורות

Ablon, Lillian, Martin C. Libicki, and Andrea A. Golay. *Markets for Cybercrime Tools and Stolen Data*. Santa Monica: Rand Corporation, 2014.

Ackerman, Gwen and Alisa Odenheimer. "Israeli Official Says First Wave of Cyber Hack Was Thwarted." *Bloomberg*, April 26, 2017, https://www.bloomberg.com/news/articles/2017-04-26/israeli-official-says-first-wave-of-cyber-hack-was-thwarted#xj4y7vzkg.

Ahronheim, Anna. "Hezbollah Has Some 2,000 Unmanned Aerial Vehicles – ALMA." *Jerusalem Post*, December 22, 2021, https://www.jpost.com/middle-east/article-689470.

Akbar, Ali. "Iran's Regional Influence in Light of its Security Concerns." *Middle East Policy* 28, no. 3–4 (2021): 186–202.

Alimardani, Mahsa. "Iran Declares 'Unveiling' of its National Intranet." *Advox*, September 2, 2016, https://advox.globalvoices.org/2016/09/02/iran-declares-unveiling-of-its-national-intranet/.

Anderson, Collin and Karim Sadjadpour. *Iran's Cyber Threat: Espionage, Sabotage and Revenge*. Carnegie Endowment for International Peace, 2018.

AP. "Microsoft Says Iranian Hackers Targeted Conference Attendees." October 28, 2020, https://apnews.com/article/germany-hacking-iran-email-saudi-arabia-807fe633c5388341f19a050414f65669.

Arghire, Ionut. "Iran-Run ISP 'Cloudzy' Caught Supporting Nation-State APTs, Cybercrime Hacking Groups." *SecurityWeek*, August 1, 2023, https://www.securityweek.com/iran-run-isp-cloudzy-caught-supporting-nation-state-apts-cybercrime-hacking-groups/.

Barnes, Julian. "Russians Tried, but Were Unable to Compromise Midterm Elections, U.S. Says." *New York Times*, December 21, 2018, https://www.nytimes.com/2018/12/21/us/politics/russia-midterm-election-influence-coates.html.

Barnes, Julian E. and David E. Sanger. "Iran and Russia Seek to Influence Election in Final Days, U.S. Officials Warn." *New York Times*, October 21, 2020, https://www.nytimes.com/2020/10/21/us/politics/iran-russia-election-interference.html.

Barzashka, Ivanka. "Are Cyber-Weapons Effective?" *The RUSI Journal* 158 no. 2 (2013): 48–56.

Bar-Zik, Ran. ״Thousands of Websites Defaced in Cyberattack Calling for the ׳Destruction of Israel.׳״ *Haaretz,* May 21, 2020, https://www.haaretz.com/israel-news/2020-05-21/ty-article/.premium/thousands-of-websites-defaced-in-cyberattack-calling-for-the-destruction-of-israel/0000017f-e104-df7c-a5ff-e37e01bb0000.

Bateman, Tom. ״Iran Accused of Sowing Israel Discontent With Fake Jewish Facebook Group.״ *BBC*, February 3, 2022, https://www.bbc.com/news/world-middle-east-60229146.

Bebber, R. ״Information War and Rethinking Phase 0.״ *Journal of Information Warfare* 15 no. 2 (2016): 39–52.

Behroozi, Setareh. ״We are in Iran for Cooperation, not to Sign Memorandums: Russian Official.״ *Tehran Times*, June 24, 2019. https://www.tehrantimes.com/news/437369/We-are-in-Iran-for-cooperation-not-to-sign-memorandums-Russian.

Benjakob, Omer. ״Iranian Accounts, Russian Tactics and Q: Israel Has Become a Disinformation Battlefield.״ *Haaretz*, April 21, 2021, https://www.haaretz.com/israel-news/tech-news/2021-04-21/ty-article/iranian-accounts-russian-tactics-and-q-israel-has-become-a-disinfo-battlefield/0000017f-e827-df2c-a1ff-fe77db160000.

___. ״Iranian Hackers Hit Top Israeli Defense Contractor, Data Leaked as Cyberattack Continues.״ *Haaretz*, December 20, 2020, https://www.haaretz.com/israel-news/tech-news/2020-12-20/ty-article/.premium/iranian-hackers-hit-israel-aerospace-industries-leak-data-as-cyberattack-continues/0000017f-df09-d856-a37f-ffc918470000.

___. ״Israel Election: Twitter Purges Foreign Influence Op to Suppress Voting.״ *Haaretz*, November 1, 2022, https://www.haaretz.com/israel-news/security-aviation/2022-11-01/ty-article/.premium/israel-election-twitter-purges-foreign-influence-op-to-suppress-voting/00000184-337c-d0c7-affe-7b7efb650000.

___. ״׳It׳s Not About Money׳: Destructive Cyberattack Proves Israel Lacks One Key Thing.״ *Haaretz,* December 9, 2020, https://www.haaretz.com/israel-news/tech-news/2020-12-09/ty-article/.highlight/its-not-about-money-destructive-cyberattack-proves-israel-lacks-one-key-thing/0000017f-e184-d568-ad7f-f3efed670000.

___. ״׳Operation Quicksand׳: Iran-Linked Hackers Target Israel in ׳New Cyberwar Phase.׳״ *Haaretz*, October 19, 2020, https://www.haaretz.com/israel-news/tech-news/2020-10-19/ty-article/iran-hackers-israel-new-phase-cyberwar-operation-quicksand/0000017f-e1a0-df7c-a5ff-e3fa7d400000.

Bennett, Brian. "Exclusive: Iran Steps up Efforts to Sow Discord Inside U.S." *Time*, June 7, 2021, https://time.com/6071615/iran-disinformation-united-states/.

Bergman Ronen and Farnaz Fassihi. "Iranian Hackers Found Way Into Encrypted Apps, Researchers Say." *New York Times*, September 18, 2020, https://www.nytimes.com/2020/09/18/world/middleeast/iran-hacking-encryption.html.

Bernard, Tara Siegel, Tiffany Hsu, Nicole Perlroth, and Ron Lieber. "Equifax Says Cyberattack May Have Affected 143 Million in the U.S." *New York Times*, September 7, 2017, https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html.

Bing, Chris. "Chinese-authored Spyware Found on More than 700 Million Android Phones." *Cyber Scoop*, November 15, 2016, https://cyberscoop.com/android-malware-china-huawei-zte-kryptowire-blu-products/.

Bob, Yonah Jeremy. "The Coming Cyber Winter is Worse Than all Estimates." *Jerusalem Post*, December 10, 2020, https://www.jpost.com/israel-news/the-coming-cyber-winter-is-worse-than-all-estimates-651696.

___. "IDF Intel Chief: We'll Keep Peace in North Despite Hezbollah Provocations." Jerusalem Post, July 11, 2023, https://www.jpost.com/israel-news/article-750010.

___. "Iran Hackers Closer to Penetrating Israel US Drones Cyberdefense CEO." *Jerusalem Post*, November 21, 2022, https://www.jpost.com/middle-east/iran-news/article-722964.

___. "Israeli Cyber Czar Warns of More Attacks From Iran." *Jerusalem Post*, May 28, 2020, https://www.jpost.com/israel-news/israeli-cyber-czar-warns-of-more-attacks-from-iran-629577.

___. "Secret Iran Hacking Plans Against West Revealed – Report." *Jerusalem Post*, July 27, 2021, https://www.jpost.com/international/secret-iran-hacking-plans-against-west-revealed-report-674992.

___. "Suspected Iranian Cyberattack Targets Israel Aerospace Industries." *Jerusalem Post*, December 20, 2020, https://www.jpost.com/breaking-news/suspected-iranian-cyberattack-targets-israel-aerospace-industries-652731.

Borghard, Erica D and Shawn W. Lonergan. "Cyber Operations as Imperfect Tools of Escalation." *Strategic Studies Quarterly* (2019): 122–145.

Brantly, Aaron Franklin. *The Decision to Attack: Military and Intelligence Cyber Decision-Making*. Athens: University of Georgia, 2018.

Braue, David. ״Iranian Hackers Targeting Australian Infrastructure.״ *ACS*, September 26, 2022, https://ia.acs.org.au/article/2022/iranian-hackers-targeting-australian-infrastructure.html.

Brewster, Tom. ״Persian Paranoia: America׳s Fear of Iranian Cyber Power.״ *The Guardian*, August 29, 2014, https://www.theguardian.com/technology/2014/aug/29/iran-cyber-power-america-networks.

Brode, Bernard. ״The Shirbit Data Hack Was an Attack on National Security. Now What? *Times of Israel*, December 18, 2020, https://blogs.timesofisrael.com/deconstructing-the-shirbit-data-breach-now-what/.

Brunner, Jordan A. ״The (Cyber) New Normal: Dissecting President Obama׳s Cyber National.״ Jurimetrics Journal 57, no. 3 (2017): 397–431.

Buchanan, Ben. *The Cyber Security Dilemma: Hacking, Trust, and Fear between Nations*. New York: Oxford, 2017.

Burke, Garance and Jonathan Fahey. ״AP Investigation: US Power Grid Vulnerable to Foreign Hacks.״ *Associated Press,* December 21, 2015, https://apnews.com/general-news-c8d531ec05e0403a90e9d3ec0b8f83c2.

Cahmutoğlu, Ersin. *Iran׳s Cyber Power*. Ankara: iRAM: Center for Iranian Studies, April 2021.

Cassidy, Christina A. and Frank Bajak. ״US Cyberwarriors thwarted 2020 Iran Election Hacking Attempt.״ *AP* April 25, 2023, https://apnews.com/article/election-security-iran-2020-voting-cybersecurity-c2faa52ffa3009f53232e4d89053980c.

Cilluffo, F. J. and Clark, J. R. ״Building a Conceptual Framework for Cyber׳s Effect on National Security,״ *Journal of Information Warfare* 15, no. 2 (2016):1–16.

Cimpanu, Catalin. ״Israel Bombed Two Hamas Cyber Targets.״ *The Record,* May 19, 2021, https://therecord.media/israel-bombed-two-hamas-cyber-targets.

___. ״New Iranian Data Wiper Malware Hits Bapco, Bahrain׳s National Oil Company.״ *ZDNet*, January 8, 2020, https://www.zdnet.com/article/new-iranian-data-wiper-malware-hits-bapco-bahrains-national-oil-company/.

Citrinowicz, Danny and Ari Ben-Ami. ״The Iranian Information Revolution: How Iran Utilizes Social Media and Internet Platforms to Incite, Recruit and Create Negative Influence Campaigns.״ *European Eye on Radicalization*, Report 30, July 2022.

Citrinowicz, Danny and Jason Brodsky. ״Iran׳s Cyberspace Evolution.״ *The Dispatch*, April 12, 2022.

Clarke, Richard A. and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to do About It*. HarperCollins, 2010.

Clearsky Research Team. ״Iranian Threat Agent OilRig Delivers Digitally Signed Malware, Impersonates University of Oxford.״ Clearsky.com, January 25, 2017, https://www.clearskysec.com/2017/01/.

___. ״Rocket Kitten 2 – Follow-Up on Iran Originated Cyber-Attacks.״ Clearsky.com, September 1, 2015, https://www.clearskysec.com/rocket-kitten-2/.

CNN Staff. ״Iran Leader Urges Destruction of ׳Cancerous׳ Israel.״ CNN, December 15, 2000, http://edition.cnn.com/2000/WORLD/meast/12/15/mideast.iran.reut/.

Cohen, Daniel and Danielle Levin. ״Operation Protective Edge: The Cyber Defense.״ In *The Lessons of Operation Protective Edge*, eds. Anat Kurz and Shlomo Brom (Tel Aviv: Institute for National Security Studies, 2014), 59–63.

Cohen, Matthew S., Charles (Chuck) D. Freilich, and Gabi Siboni. ״Israel and Cyberspace: Unique Threat and Response.״ *International Studies Perspectives* 17, no. 3 (2016): 307–321.

Cohen, Matthew S., Charles D. Freilich, and Gabi Siboni. ״Four Big ׳Ds׳ and a Little ׳r׳: A New Model for Cyber Defense.״ *Cyber, Intelligence, and Security* 1 no. 1(2017): 21–36.

Congressional Research Service. ״Iranian Offensive Cyber Attack Capabilities.״ (January 13, 2020), https://crsreports.congress.gov/product/pdf/IF/IF11406.

Connolly, Kate. ״Russian Hacking Attack on Bundestag Damaged Trust, Says Merkel.״ *Guardian*, May 13, 2020, https://www.theguardian.com/world/2020/may/13/russian-hacking-attack-on-bundestag-damaged-trust-says-merkel.

Conti, Gregory and David Raymond. *On Cyber: Towards an Operational Art for Cyber Conflict*. Kopidion 2017.

Corera, Gordon. ״Iran ׳Hides Spyware in Wallpaper, Restaurant and Games Apps,׳״ *BBC News*, February 8, 2021. https://www.bbc.com/news/technology-55977537.

Cornish, Paul, ed. *Oxford Handbook of Cyber Security*. Oxford University Press, 2021.

Crisp, Wil and Suadad al-Salhy. ״Exclusive: Inside Hizbollah׳s Fake News Training Camps Sowing Instability Across the Middle East.״ *The Telegraph*, August 2, 2020, https://www.telegraph.co.uk/news/2020/08/02/exclusive-inside-hezbollahs-fake-news-training-camps-sowing/.

Cuthbertson, Anthony. ״Iranian Hackers Attack UK Universities to Steal Research Secrets.״ *The Independent*, August 24, 2018, https://www.independent.co.uk/tech/iran-hackers-uk-university-cyber-attack-security-cobalt-dickens-a8506406.html.

Cyber Threat Brief. *Flash Critic*. November 29, 2015.

Davidi, Avi. ״Iranian-Russian Cooperation on Hack Attacks May Challenge Israeli Cyber Supremacy.״ *Times of Israel*, April 18, 2023, https://www.timesofisrael.com/iranian-russian-cooperation-on-hack-attacks-may-challenge-israeli-cyber-supremacy/.

De Souza, Ryan. ״Israeli Security Camera Systems Targeted by Pro-Hezbollah Hackers.״ *Hackread*, February 21, 2016, https://www.hackread.com/israeli-security-camera-systems-targeted-by-hezbollah-hackers/.

Demboski, Morgan and IronNet Threat Research and Intelligence Teams. ״Analysis of the Iranian Cyber Attack Landscape.״ *IronNet*, September 15, 2021, https://www.ironnet.com/blog/iranian-cyber-attack-updates.

Demchak, Chris C. *Wars of Disruption and Resilience*. University of Georgia Press, 2011.

Denning, Dorothy. ״Explainer: How Iran׳s Military Outsources its Cyberwarfare Forces.״ *Navy Times*, January 23, 2020, https://www.navytimes.com/news/your-navy/2020/01/23/explainer-how-irans-military-outsources-its-cyberwarfare-forces/.

Dickstein, Corey. ״Military Warns of Iranian Hackers Targeting American Troops With Fake Job Website.״ *Stars and Stripes*, October 4, 2019, https://www.stripes.com/theaters/middle_east/military-warns-of-iranian-hackers-targeting-american-troops-with-fake-jobs-website-1.601787.

Doffman, Zak. ״U.S. Military Warns Outlook Users to Update Immediately Over Hack Linked to Iran.״ *Forbes,* July 3, 2019, https://www.forbes.com/sites/zakdoffman/2019/07/03/u-s-cyber-command-warns-millions-of-outlook-users-of-malicious-hack-linked-to-iran/?sh=b29bce326fd4.

Dolev, Boaz and David Siman-Tov. ״Iranian Cyber Influence Operations Against Israel Disguised as Ransomware Attacks.״ Special Publication. INSS, January 27, 2022.

Dor, Ofir. ״׳Unsophisticated Iranian Cyberattack׳ Temporally Downs Israeli Bank Sites, Post Office.״ *Haaretz*, April 14, 2023, https://www.haaretz.com/israel-news/2023-04-14/ty-article/.premium/unsophisticated-iranian-cyberattack-temporally-downs-israeli-bank-sites-post-office/00000187-7fd6-dc6c-a5ff-7fd77fad0000.

Douris, Constance. "Cyber Assault on Electric Grid Could Make U.S. Feel Like Post-Hurricane Puerto Rico." *Forbes*, February 6, 2018, https://www.forbes.com/sites/constancedouris/2018/02/06/cyber-assault-on-electric-grid-could-make-u-s-feel-like-post-hurricane-puerto-rico/.

Economist. "The Big Data Breach Suffered by Equifax Has Alarming Implications." September 16, 2017, https://www.economist.com/finance-and-economics/2017/09/16/the-big-data-breach-suffered-by-equifax-has-alarming-implications.

___. "The WannaCry Attack Reveals the Risks of a Computerised World." May 20, 2017, https://www.economist.com/leaders/2017/05/20/the-wannacry-attack-reveals-the-risks-of-a-computerised-world.

Esfandiari, Golnaz. "Iran to Work With China to Create National Internet System." *Radio Free Europe*, *Radio Liberty*, September 4, 2020, https://www.rferl.org/a/iran-china-national-internet-system-censorship/30820857.html.

Even, Shmuel and David Siman-Tov. *Cyber Warfare: Concepts and Strategic Trends*, Memorandum No. 117 (Tel Aviv: INSS, 2012).

Fabian, Emanuel. "Gantz Says Iran and Hezbollah Tried to Hack UN Peace Force, Steal Deployment Data." *Times of Israel*, June 29, 2022, https://www.timesofisrael.com/gantz-says-iran-and-hezbollah-attempted-to-hack-unifil-steal-deployment-infomation/.

Facebook. *Threat Report: The State of Influence Operations 2017–2020*, May 2021, https://about.fb.com/wp-content/uploads/2021/05/IO-Threat-Report-May-20-2021.pdf.

FakeReporter, "Rolling in the Deep: An Iranian Cross-Platform Influence Operation Summary," Rolling_in_the_Deep_Summary.pdf (fakereporter.net).

Fassihi, Farnaz and Ronen Bergman. "Israel and Iran Broaden Cyberwar to Attack Civilian Targets." *New York Times*, November 27, 2021, https://www.nytimes.com/2021/11/27/world/middleeast/iran-israel-cyber-hack.html.

Fassihi, Farnaz and Steven Lee Myers. "Defying U.S., China and Iran Near Trade and Military Partnership." *New York Times*, July 11, 2020, https://www.nytimes.com/2020/07/11/world/asia/china-iran-trade-military-deal.html.

Fassihi, Farnaz and Steven Lee Myers. "China, With $400 Billion Iran Deal, Could Deepen Influence in Mideast." *New York Times*, March 27, 2021, https://www.nytimes.com/2021/03/27/world/middleeast/china-iran-deal.html.

Faucon, Benoit. ״Iran Restricts Internet Access as Women׳s Rights Protests Spread.״ *Wall Street Journal*, September 22, 2022, https://www.wsj.com/articles/iran-restricts-internet-access-as-womens-rights-protests-spread-11663874073.

Faucon, Benoit and Liza Lin. ״U.S. Weighs Sanctions for Chinese Companies Over Iran Surveillance Buildup.״ *Wall Street Journal*, February 4, 2023, https://www.wsj.com/articles/u-s-weighs-sanctions-for-chinese-companies-over-iran-surveillance-buildup-11675503914.

FBI Boston. ״FBI Releases Cybersecurity Advisory on previously Undisclosed Iranian Malware Used to Monitor Dissidents and Travel and Telecommunications Companies.״ September 17, 2020, https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-releases-cybersecurity-advisory-on-previously-undisclosed-iranian-malware-used-to-monitor-dissidents-and-travel-and-telecommunications-companies.

Fischerkeller, Michael P. and Richard J. Harknett. ״Deterrence is Not a Credible Strategy for Cyberspace.״ *Orbis* 61, no. 3 (2018): 381–393.

Fisher, Dennis. ״FBI Warns of Attacks From Iranian Threat Group Emennet Pasargad.״ *Decipher*, October 21, 2022, https://duo.com/decipher/fbi-warns-of-attacks-from-iranian-threat-group-emennet-pasargad.

Freilich, Charles D. *Israeli National Security: A New Strategy for an Era of Change*. Oxford Press, 2018.

Freilich, Charles D., Matthew S. Cohen, and Gabi Siboni. *Israel and the Cyber Threat: How the Start-Up Nation Became a Global Cyber Power*. Oxford: Oxford Press, 2023.

Frenkel, Sheera. ״Iranian Disinformation Effort Went Small to Stay Under Big Tech׳s Radar.״ *New York Times*, June 30, 2021, https://www.nytimes.com/2021/06/30/technology/disinformation-message-apps.html.

Fung, Brian. ״Uber Reaches $148 Million Settlement over its 2016 Data Breach, which Affected 57 Million Globally.״ *Washington Post*, September 26, 2018, https://www.washingtonpost.com/technology/2018/09/26/uber-reaches-million-settlement-over-its-data-breach-which-affected-million-globally/.

Government of Israel, Ministry of Intelligence, National Intelligence Directorate. ״Foreign Interference and Influence on Social Media in Israel״, May 7, 2023.

Greenberg, Andy. ״Iranian Hackers Have Been ׳Password-Spraying׳ the US Grid.״ *Wired*, January 9, 2020, https://www.wired.com/story/iran-apt33-us-electric-grid/.

Greene, Jay, Tony Romm, and Ellen Nakashima. "Iranians Tried to Hack U.S. Presidential Campaign in Effort that Targeted Hundreds, Microsoft Says." *Washington Post*, October 4, 2019, https://www.washingtonpost.com/technology/2019/10/04/iran-tried-hack-us-presidential-candidates-journalists-effort-that-targeted-hundreds-microsoft-finds/.

HaCohen, Hagay. "Check Point Unveils New Iranian Cybercrime, Ransoming Companies' Data." *Jerusalem Post*, November 12, 2020, https://www.jpost.com/israel-news/check-point-unveils-new-iranian-cybercrime-ransoming-companies-data-648928.

Hahn, Roei and Yuval Mann. "Leading Israeli Research Institute Falls Prey to Cyberattack," *Ynet*, December 2, 2023, https://www.ynetnews.com/business/article/syjobiuti.

Halpern, Sue. "Should the U.S. Expect an Iranian Cyberattack?" *New Yorker*, January 6, 2020, https://www.newyorker.com/tech/annals-of-technology/should-the-us-expect-an-iranian-cyberattack.

Hardie, John and Annie Fixler. "Russia-Iran Cooperation Poses Challenges for US Cyber Strategy, Global Norms." *C4ISR*, February 8, 2021, https://www.c4isrnet.com/thought-leadership/2021/02/08/russia-iran-cooperation-poses-challenges-for-us-cyber-strategy-global-norms/.

Harel, Amos. "With Cyberattack on Iranian Port, Tehran Gets a Warning: Civilian Installations Are a Red Line." *Haaretz*, May 20, 2020, https://www.haaretz.com/middle-east-news/iran/2020-05-20/ty-article/.premium/cyberattack-on-iran-marks-a-clear-red-line/0000017f-f4f9-d5bd-a17f-f6fb54c40000.

Harel, Amos, Yaniv Kubovich, and Reuters. "Israel Accuses Iran, Hezbollah of Hacking UN Force in Lebanon." *Haaretz,* June 29, 2022, https://haaretz.com/israel-news/2022-06-29/ty-article/.premium/israel-accuses-iran-hezbollah-of-hacking-un-force-in-lebanon/00000181-ae8d-dacc-a9f7-eedf37450000.

Harris, Shane. *@War: The Rise of the Military-Internet Complex*. Eamon Dolan/Mariner, 2014.

Hasson, Ayala. "Iranian Hackers Posed as General Yadlin and Gained Information from an Israeli Researcher.", *Channel 13*, November 20, 2020, https://13news.co.il/item/news/politics/security/iran-hackers-1162861/.

Hatoni, Yossi. "Hezbollah Cyberattacked Hundreds of Companies, Also in Israel." *People and Computers*, January 28, 2021, https://www.pc.co.il/news/331154/.

Herr, Trey. ״PrEP: A Framework for Malware & Cyber Weapons.״ *Cyber Security Policy and Research Institute*. George Washington University, March 12, 2014.

Herzallah, Mohammad J. ״Israeli Fights Wire with Wire.״ *Newsweek*, July 27, 2009.

Hope, Bradley, Warren P. Strobel, and Dustin Volz. ״High-Level Cyber Intrusions Hit Bahrain Amid Tensions With Iran.״ *Wall Street Journal*, August 7, 2019, https://www.wsj.com/articles/high-level-cyber-intrusions-hit-bahrain-amid-tensions-with-iran-11565202488.

Horovitz, Michael. ״Report: Iran Hacked Israeli Cameras a Year Ago; Defense Officials Knew, Didn׳t Act.״ *Times of Israel*, December 19, 2022, https://www.timesofisrael.com/report-iran-hacked-israeli-cameras-a-year-ago-defense-officials-knew-didnt-act/

Howarth, Josh. ״80+ Amazing IoT Statistics (2023-2030).״ Explodingtopics.com, March 16, 2023, https://explodingtopics.com/blog/iot-stats.

Hsu, Jeremy. ״U.S. Suspicions of China׳s Huawei Based Partly on NSA׳s Own Spy Tricks.״ *IEEE Spectrum*, March 26, 2014, https://spectrum.ieee.org/us-suspicions-of-chinas-huawei-based-partly-on-nsas-own-spy-tricks.

Hymas, Charles. ״Iran Targets UK Political System With Fake Websites.״ *The Telegraph*, June 6, 2021, https://www.telegraph.co.uk/politics/2021/06/06/iran-targets-uk-political-system-fake-websites/.

Industrial Cyber. ״New Dragos report reveals Iranian hackers targeting U.S power grid amid tensions between two nations.״ January 13, 2020, https://industrialcyber.co/industrial-cyber-attacks/new-dragos-report-reveals-iranian-hackers-targeting-u-s-power-grid-amid-tensions-between-two-nations/.

International Institute for Strategic Studies. ״Cyber Capabilities and National Power: A Net Assessment.״ Research Papers. (June 28, 2021). https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---a-net-assessment___.pdf.

Isaac, Mike and Sheera Frenkel. ״Facebook Security Breach Exposes Accounts of 50 Million Users.״ *New York Times*, September 28, 2018, https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html.

Israel National Cyber Directorate. ״Iranian Government Sponsored Threat Actor Muddy Water Conducts Cyber Attack Against Israel.״ March 9, 2023, https://www.gov.il/en/departments/news/_muddywater.

Jasper, Scott. *Strategic Cyber Deterrence: The Active Cyber Defense Option*. Rowman and Littlefield, 2017.

Jerusalem Post Staff. "Israel Independence Day Cyberattack Takes Down Major News Websites." *Jerusalem Post*, April 26, 2023.

___. "Israeli Cyber Security Website Briefly Taken Down in Cyberattack." *Jerusalem Post*, April 4, 2023.

___. "United Hazalah Hit By Tens of Thousands of Cyberattacks Past Two Days." *Jerusalem Post*, April 5, 2023.

Jerusalem Post Staff and Tovah Lazaroff. "Israel is Updating Attack Plans Against Iran's Nuclear Sites – Gantz." *Jerusalem Post*, March 15, 2021, https://www.jpost.com/israel-news/gantz-reveals-classified-hezbollah-target-map-during-fox-news-interview-661029.

Joffre, Tzvi. "Iran-Backed Hackers Targeting Activists, Journalists, Politicians – HRW." *Jerusalem Post*, December 5, 2022, https://www.jpost.com/middle-east/iran-news/article-724088.

Derek Johnson, "Iranian Hacking Group Impersonating Nuclear Experts to Gain Intel from Western Think Tanks." *SC Media*, July 6, 2023, https://www.scmagazine.com/news/an-iranian-hacking-group-is-impersonating-nuclear-experts-to-gain-intel-from-western-think-tanks.

Jones, Sam. "Cyber Warfare: Iran Opens a New Front." Financial Times, April 26, 2016, https://www.ft.com/content/15e1acf0-0a47-11e6-b0f1-61f222853ff3.

Kanno-Youngs, Zolan and David Sanger. "U.S. Accuses China of Hacking Microsoft." *New York Times*, July 19, 2021, https://www.nytimes.com/2021/07/19/us/politics/microsoft-hacking-china-biden.html.

Kausch, Kristina and Lior Tabansky. "Cybered Conflict in the Middle East." *Mediterranean Dialogue Series* No. 15, Konrad Adenauer Stiftung, 2018.

Kello, Lucas. "The Meaning of the Cyber Revolution." *International Security* 38, no. 2 (2013): 7–40.

Kenney, Michael. "Cyber-Terrorism in a Post-Stuxnet World." *Orbis* 59, no. 1 (2015): 111–128.

King Faisal Center for Research and Islamic Studies. *Iran's Cyberattacks Capabilities*, Special Report, January 2020.

Kube, Courtney, Carol E. Lee, Dan De Luce, and Ken Dilanian. "Iran Has Laid Groundwork for Extensive Cyberattacks on U.S., Say Officials." *NBC News*, July 20, 2018, https://nbcnews.to/2uFfKi0.

Kubovich, Yaniv. "Iran Used Instagram to Try and Lure Israelis to Meetings Abroad, Shin Bet and Mossad Say." *Haaretz*, April 12, 2021, https://www.haaretz.com/israel-news/2021-04-12/ty-article/.highlight/iranian-intelligence-used-instagram-to-try-and-lure-israelis-abroad-shin-bet-says/0000017f-ef6c-d497-a1ff-efec462c0000.

___. "Iranian Hackers Post Footage of Jerusalem Bombing, Taken by Large Security Agency." *Haaretz*, November 24, 2022, https://www.haaretz.com/israel-news/2022-11-24/ty-article/.premium/iranian-hackers-breach-major-israeli-security-agency/00000184-a988-dd96-ad8c-eba817250000.

Kuperwasser, Yossi and David Siman-Tov, Eds., *The Cognitive Campaign: Strategic and Intelligence Perspectives*. Memorandum No. 197 (Tel Aviv: Institute for National Security Studies, 2019).

Lappin, Yaakov. "Iran Attempted Large-Scale Cyber-Attack on Israel, Senior Security Source Says." *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.

Lee, Michael. "Chinese Facial recognition Technology Helping Iran to Identify Women Breaking Strict Dress Code: Report." *Fox News,* January 12, 2023, https://www.foxnews.com/world/chinese-facial-recognition-technology-helping-iran-identify-women-breaking-strict-dress-code-report.

Lee, Vivian. "Despite Iran's Efforts to Block Internet, Technology Has Helped Fuel Outrage." *New York Times*, September 29, 2022, https://www.nytimes.com/2022/09/29/world/middleeast/iran-internet-censorship.html.

Libicki, Martin C. *Cyberdeterrence and Cyberwar*. Rand Corporation, 2009.

___. "Second Acts in Cyberspace." In *Bytes, Bombs and Spies: The Strategic Dimensions of Offensive Cyber Operations*, edited by Herbert Lin and Amy Zegart. Brookings, 2019.

Lieber, Dov, Benoit Faucon, and Michael Amon. "Russia Supplies Iran With Cyber Weapons as Military Cooperation Grows." *Wall Street Journal*, March 27, 2023, https://www.wsj.com/articles/russia-supplies-iran-with-cyber-weapons-as-military-cooperation-grows-b14b94cd.

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

Lin, Herbert and Amy Zegart. *Bytes, Bombs and Spies: The Strategic Dimensions of Offensive Cyber Operations*. Brookings, 2019.

Lindsay, Jon R. "Stuxnet and the Limits of Cyber Warfare. *Security Studies* 22, no. 3 (2013): 365–404. https://doi.org/10.1080/09636412.2013.816122.

Long, Austin. "A Cyber SIOP? Operational Considerations for Strategic Offensive Cyber Planning." In *Bytes, Bombs and Spies: The Strategic Dimensions of Offensive Cyber Operations*, edited by Herbert Lin and Amy Zegart. Brookings, 2019.

Loudermilk, Micah. "Iran Crisis Moves Into Cyberspace." Policy Watch 3151, *Washington Institute for Near East Policy* (July 9, 2019). https://www.washingtoninstitute.org/policy-analysis/iran-crisis-moves-cyberspace.

Matania, Eviatar and Eldad Tal-Shir. "Continuous Terrain Remodelling: Gaining the Upper Hand in Cyber Defence." *Journal of Cyber Policy* 5, no. 2 (2020): 285–301. https://doi.org/10.1080/23738871.2020.1778761.

Matania, Eviatar, Lior Yoffe, and Michael Mashkautsan. "A Three Layer Framework for a Comprehensive National Cyber-Security Strategy." *Georgetown Journal of International Affairs* 27, no. 3 (2016): 77–84.

McMillan, Robert. "Iranian Hackers Have Hit Hundreds of Companies in Past Two Years." *Wall Street Journal*, March 6, 2019. https://www.wsj.com/articles/iranian-hackers-have-hit-hundreds-of-companies-in-past-two-years-11551906036.

Menn, Joseph. "Iran Gained Access to Election Results Website in 2020, Military Reveals." *Washington Post*, April 24, 2023.

Microsoft Threat Intelligence. "Iran Turning to Cyber-Enabled Influence Operations for Greater Effect." May 2, 2023.

Miller, Maggie. "Albania Weighed Invoking NATO's Article 5 over Iranian Cyberattack." *Politico*, October 5, 2022, https://www.politico.com/news/2022/10/05/why-albania-chose-not-to-pull-the-nato-trigger-after-cyberattack-00060347.

Morello, Carol and Missy Ryan. "U.S. Says Iranian Forces May Have Killed More Than 1,000 Protestors." *Washington Post*, December 5, 2019, https://www.washingtonpost.com/world/national-security/trump-administration-alleges-iran-has-killed-more-than-1000-protesters/2019/12/05/e9c11a76-1775-11ea-bf81-ebe89f477d1e_story.html.

Moskowitz, Jeff. "Cyberattack Tied to Hezbollah Ups The Ante for Israel's Digital Defenses." *Christian Science Monitor*, June 1, 2015, https://www.csmonitor.com/World/Passcode/2015/0601/Cyberattack-tied-to-Hezbollah-ups-the-ante-for-Israel-s-digital-defenses.

Muncaster, Phil. "US: Iran Was Behind Proud Boys Email Campaign." *Infosecurity Magazine*, October 22, 2020, https://www.infosecurity-magazine.com/news/us-iran-was-behind-proud-boys/.

Nakashima, Ellen. "Iranian Hackers Are Targeting U.S. Officials Through Social Networks, Report Says." *Washington Post*, May 29, 2014. https://www.washingtonpost.com/world/national-security/iranian-hackers-are-targeting-us-officials-through-social-networks-report-says/2014/05/28/7cb86672-e6ad-11e3-8f90-73e071f3d637_story.html.

Nakashima, Ellen, Josh Dawsey, and Matt Viser. "China, Iran Targeting Presidential Campaigns With Hacking Attempts, Google Announces." *Washington Post*, June 4, 2020, https://www.washingtonpost.com/national-security/china-iran-targeting-presidential-campaigns-with-hacking-attempts-google-announces/2020/06/04/45a64e78-a692-11ea-b619-3f9133bbb482_story.html.

Nakashima, Ellen, Amy Gardner, and Aaron Davis. "FBI Links Iran to Online Hit List Targeting Top Officials Who've Refuted Trump's Election Fraud Claims." *Washington Post*, December 22, 2020, https://www.washingtonpost.com/national-security/iran-election-fraud-violence/2020/12/22/4a28e9ba-44a8-11eb-a277-49a6d1f9dff1_story.html.

Nakashima, Ellen, Amy Gardner, Isaac Stanley-Becker, and Craig Timberg. "U.S. Government Concludes Iran Was Behind Threatening Emails Sent to Democrats." *Washington Post*, October 22, 2020, https://www.washingtonpost.com/technology/2020/10/20/proud-boys-emails-florida/.

Nakashima, Ellen and Spencer Hsu. "Microsoft Says it Has Found Iranian Hackers Targeting U.S. Agencies, Companies and Middle East Advocates." *Washington Post*, March 27, 2019. https://www.washingtonpost.com/local/legal-issues/microsoft-says-it-has-found-iranian-hackers-targeting-us-agencies-companies-and-middle-east-advocates/2019/03/27/8056c51e-50a0-11e9-8d28-f5149e5a2fda_story.html.

National Intelligence Council. "Foreign Threats to the 2020 Federal Elections, March 10, 2021, https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf.

Newman, Lily Hay. "How Iran Tried to Undermine the 2020 US Presidential Election." *Wired*, November 18, 2021, https://www.wired.com/story/iran-2020-election-interference/.

___. "How the Iranian Government Shut Off the Internet." *Wired*, November 17, 2019, https://www.wired.com/story/iran-internet-shutoff/.

Nye, Joseph S. *The Future of Power: Its Changing Nature and Use in the Twenty-first Century*. New York: Hachette Book Group, 2011.

O'Flaherty, Kate. "DoJ Unveils Iran Disinformation Campaign—Seizes 92 Domains Violating U.S. Sanctions." *Forbes*, October 9, 2020. https://www.forbes.com/sites/kateoflahertyuk/2020/10/09/doj-unveils-iran-disinformation-campaign-seizes-92-domains-violating-us-sanctions/.

Office of the Director of National Intelligence. "Annual Threat Assessment of the U.S. Intelligence Community." (2021).

___. "Annual Threat Assessment of the U.S. Intelligence Community." (2022), https://www.odni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf.

Orbach, Meir. "Israeli Cybersecurity Giant Tracks Ranson Payments From New Cyber Attack to Iranian Nationals." *The Algemeiner*, November 12, 2020, https://www.algemeiner.com/2020/11/12/israeli-cybersecurity-giant-tracks-ransom-payments-from-new-cyber-attack-to-iranian-nationals/.

Orbach, Meir and Golan Hazani. "Israel's Supply Chain Targeted in Massive Cyberattack." *Calcalist*, December 13, 2020.

Page, Carly. "Iran-Backed Hackers Breached a US Federal Agency that Failed to Patch Year-Old Bug." *Yahoo News*, November 17, 2022.

Pahlavi, Pierre. "Digital Hezbollah and Political Warfare in Cyberspace." *National Interest*, October 31, 2022, https://nationalinterest.org/feature/digital-hezbollah-and-political-warfare-cyberspace-205558.

Parks, Miles. "View From the Ground at Washington DC Protests; Misinformation Spreads Online." *NPR*, June 4, 2020.

Perkovich, George and Ariel (Eli) Levite, eds. *Understanding Cyber Conflict: 14 Analogies.* Washington DC: Georgetown University Press, 2017.

Perlroth, Nicole. "All 3 Billion Yahoo Accounts Were Affected by 2013 Attack." *New York Times*, October 3, 2017, https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html.

___. "Chinese and Iranian Hackers Renew Their Attacks on U.S. Companies." *New York Times*, February 18, 2019, https://www.nytimes.com/2019/02/18/technology/hackers-chinese-iran-usa.html.

___. "Cyberespionage Attacks Tied to Hackers in Iran." *New York Times*, May 29, 2014, https://archive.nytimes.com/bits.blogs.nytimes.com/2014/05/29/cyberespionage-attacks-tied-to-hackers-in-iran/.

Pfeffer, Anshel. "Israel Suffered Massive Cyber Attack During Gaza Offensive." *Haaretz*, June 15, 2009, https://www.haaretz.com/2009-06-15/ty-article/israel-suffered-massive-cyber-attack-during-gaza-offensive/0000017f-f6ac-ddde-abff-feedb26c0000.

___. "Why Netanyahu Failed to Mention the Iranian Link to the Cyberattack on Israel." *Haaretz*, April 27, 2017, https://www.haaretz.com/israel-news/2017-04-27/ty-article/why-netanyahu-failed-to-link-iran-to-cyberattack-on-israel/0000017f-e858-dea7-adff-f9fb5c720000.

Pileggi, Tamar. "Khamenei: Israel a "Cancerous Tumor' that 'Must be Eradicated." *Times of Israel*, June 4, 2018, https://www.timesofisrael.com/khamenei-israel-a-cancerous-tumor-that-must-be-eradicated/.

Pinko, Eyal. "Iranians Developing the Cyber Capabilities of Hezbollah." *Israel Defense*, March 30, 2021, https://www.israeldefense.co.il/en/node/49094.

Pomerleau, Mark. "US Cyber Forces Wrap Up Deployment to Albania in Response to Iranian Cyberattacks." *DefenseScoop*, March 23, 2023, https://defensescoop.com/2023/03/23/cyber-forces-wrap-up-deployment-to-albania-in-response-to-iranian-cyberattacks/.

Prokupecz, Shimon, Tal Kopan, and Sonia Moghe. "Former Official: Iranians Hacked into New York Dam." *CNN*, December 22, 2015. https://edition.cnn.com/2015/12/21/politics/iranian-hackers-new-york-dam/index.html.

Raved, Ahiya. "Cyber Attack Targeted Israel's Water Supply, Internal Report Claims." *Ynet*, April 26, 2020, https://www.ynetnews.com/article/HJX1mWmF8.

Reuters. "Aramco Says Cyberattack Was Aimed at Production." *New York Times*, December 9, 2012, https://www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-took-aim-at-its-production.html.

Ribeiro, Anna. "FBI Reveals Iranian Cyber Group Emennet Pasargad Executing Hack-and-Leak Operations Using False-Flag Personas." *Industrial Cyber*, October 21,

2022, https://industrialcyber.co/critical-infrastructure/fbi-reveals-iranian-cyber-group-emennet-pasargad-executing-h.

Rid, Thomas. *Cyber War Will Not Take Place.* London: C. Hurst and Co, 2013.

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

Ropek, Lucas. "Hezbollah-Linked Cyber Unit Has Been Hacking Into Internet Companies for Years." *Gizmodo*, January 29, 2021, https://gizmodo.com/latest?startTime=1611974820316.

Rosenberger, Laura. "Making Cyberspace Safe for Democracy." *Foreign Affairs* (May/June 2020), https://www.foreignaffairs.com/articles/china/2020-04-13/making-cyberspace-safe-democracy.

Rubenstein, Roi. "Report: Iranian Bot Army Trying to Influence Israeli Elections." *Ynet*, January 31, 2019, https://www.ynetnews.com/articles/0,7340,L-5455991,00.html.

Ruble, Kayla. "Syrian Hackers Hijack IDF Twitter Sparking Fears of Nuclear Leak." *Vice*, July 17, 2014.

Sanger, David E. *The Perfect Weapon: War, Sabotage and Fear in the Cyber Age*. New York: Crown, 2018.

Sanger, David E. and Julian E. Barnes. "United States Indicts Iranian Hackers in Voter Intimidation Effort." *New York Times*, November 18, 2021, https://www.nytimes.com/2021/11/18/us/politics/iranian-hackers-voter-intimidation-indicted.html.

Sanger, David E., Nicole Perlroth, and Julian E. Barnes. "As Understanding of Russian Hacking Grows, So Does Alarm." *New York Times*, January 2, 2021, https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html.

Satter, Raphael. "AP Exclusive: Iran Hackers Hunt Nuclear Workers, US Targets." *AP*, December 13, 2018, https://apnews.com/article/0d4dcaab0e134cf6a1c6ce6be3b7b6a8.

Schneier, Bruce. "8 Ways to Stay Ahead of Influence Operations." *Foreign Policy* (August 12, 2019), https://foreignpolicy.com/2019/08/12/8-ways-to-stay-ahead-of-influence-operations/.

Schroeder, Stan. "CIA, FBI, NSA: We Don't Recommend Huawei or ZTE Phones." *Mashable*, February 14, 2018, https://mashable.com/article/nsa-fbi-cia-huawei.

Schweitzer, Yoram, Gabi Siboni, and Einav Yogev. "Cyberspace and Terrorist Organizations." *Military and Strategic Affairs* 5 no. 3 (2013): 17–26.

Segal, Adam. *The Hacked World Order: How Nations Fight, Trade, Maneuver and Manipulate in the Digital Ages*. New York: Public Affairs, 2017.

Shahaf, Tal. ״Israel Unprepared for Iranian Attack on Water Supply, Officials Warn.״ *Ynet*, February 17, 2021, https://www.ynetnews.com/article/rJW2Cjcb00.

Shakil, Sana. ״Cyber Attacks by Iran Hackers on Rise.״ *New Indian Express*, March 6, 2022, https://www.newindianexpress.com/thesundaystandard/2022/mar/06/cyber-attacks-by-iran-hackers-on-rise-2426859.html.

Shamah, David. ״How Israel Police Computers Were Hacked: The Inside Story.״ *Times of Israel*, October 28, 2012, https://www.timesofisrael.com/how-israel-police-computers-were-hacked-the-inside-story/.

___. ״Official: Iran, Hamas Conduct Cyber-Attacks Against Israel.״ *Times of Israel*, August 13, 2015, https://www.timesofisrael.com/official-iran-hamas-conduct-cyber-attacks-against-israel/.

Shamir, R. and Bachar, E. ״Defending Israel Selections from Cyber Attack – What Should Be Done?.״ Israel Democracy Institute, *Policy Study* 136, (January 2019).

Shane, Scott and Ronen Bergman. ״New Report Shows How a Pro-Iran Group Spread Fake News Online.״ *New York Times*, May 14, 2019, https://www.nytimes.com/2019/05/14/world/middleeast/iran-fake-news-report.html.

Shkolnik, Michael and Alexander Corbeil. ״Hezbollah׳s ׳Virtual Entrepreneurs׳: How Hezbollah is Using the Internet to Incite Violence in Israel.״ *CTC Sentinel* 12, no. 9 October 2019, https://ctc.westpoint.edu/hezbollahs-virtual-entrepreneurs-hezbollah-using-internet-incite-violence-israel/.

Siboni, Gabi, Léa Abramski, and Gal Sapir. ״Iran׳s Activity in Cyberspace: Identifying Patterns and Understanding the Strategy.״ *Cyber, Intelligence and Security* 4, no. 1 (2020): 21–40.

Siboni, Gabi and Sami Kronenfeld. ״Iran and Cyberspace Warfare.״ In *Cyberspace and National Security – Selected Articles*, edited by Gabi Siboni, 81–103. Tel Aviv: Institute for National Security Studies, 2013.

Siddiqui, Zeba. ״Iran Behind Hack of French Magazine Charlie Hebdo, Microsoft Says.״ *Reuters*, February 3, 2023, https://www.reuters.com/business/media-telecom/iran-behind-hack-french-magazine-charlie-hebdo-microsoft-says-2023-02-03/.

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

Siman-Tov, David and Shmuel Even. "A New Level in the Cyber War between Israel and Iran." *INSS Insight* no. 1328, June 3, 2020.

Siman-Tov, David and Ohad Zaidenberg. Influence Operations: A Combination of Technological Attacks and Content Manipulation." *INSS Special Publication*, March 11, 2021, https://www.inss.org.il/he/publication/cyber-attack-and-manipulations/.

Sinoruka, Fjori. "FBI: Iranian Hackers Accessed Albanian Systems Over Year Ago." *Balkan Insight*, September 22, 2022, https://balkaninsight.com/2022/09/22/fbi-iranian-hackers-accessed-albanian-systems-over-year-ago/.

Solomon, Shoshana. "Israeli Entrepreneur Calls for NATO-Style Cybersecurity." *Times of Israel*, January 31, 2018.

Spadoni, Giacomo. "IRGC Cyber-Warfare Capabilities." Herzliya: International Institute for Counterterrorism (ITC), 2019. https://ict.org.il/UserFiles/IRGC%20Cyber-Warfare%20Capabilities.pdf.

Springer, Paul J. *Encyclopedia of Cyberwarfare*. ABC- Clio, 2017.

Staff. "Iranian Cyberattacks on Israeli Facilities Thwarted for a Year – Report." *Jerusalem Post*, June 7, 2020, https://www.jpost.com/breaking-news/iranian-cyber-attacks-on-israeli-water-facilities-thwarted-for-a-year-report-630592.

Starks, Tim. "An Iranian Hacking Group Went on the Offensive Against US Targets, Microsoft Says." *Washington Post*, April 18, 2023.

___. "Russia, China and Iran Trying to Hack Presidential Race, Microsoft Says." *Politico*, September 10, 2020, https://www.politico.com/news/2020/09/10/russia-china-iran-cyberhack-2020-election-411853.

Statista. "Estimated Cost of Cybercrime Worldwide 2017-2028." https://www.statista.com/statistics/1280009/cost-cybercrime-worldwide/.

___. "Forecast number of mobile devices worldwide from 2020 to 2025 (in billions)." https://www.statista.com/statistics/245501/multiple-mobile-device-ownership-worldwide/;

___. "Share of households with a computer at home worldwide from 2005 to 2019." https://www.statista.com/statistics/748551/worldwide-households-with-computer/.

Stickings, Tim. "Berlin Security Service Blames Iran for Cyber Attack on German Companies." *The National News*, May 12, 2021, https://www.thenationalnews.com/world/europe/berlin-security-service-blames-iran-for-cyber-attack-on-german-companies-1.1221570.

Stott, Paul. *Iranian Influence Networks in the United Kingdom: Audit and Analysis*. (Henry Jackson Society, June 2021), https://henryjacksonsociety.org/wp-content/uploads/2021/06/HJS-Iranian-Influence-Networks-in-the-UK-Report-HR-web-1.pdf.

Straub, Jeremy. "Hackers Could Kill More People than a Nuclear Weapon." LiveScience.com, August 27, 2019, https://www.livescience.com/cyberattacks-could-kill-more-than-nuclear-attacks.html.

Stub, Zev. "Newly-Found Iranian Cyber-Espionage May Pose 'Real Threat' to Israel." *Jerusalem Post,* October 7, 2021, https://www.jpost.com/jpost-tech/newly-found-iranian-cyber-espionage-may-pose-real-threat-to-israel-681196.

Stubbs, Jack and Christopher Bing. "Exclusive: Iran-Based Political Influence Operation – Bigger, Persistent, Global." *Reuters*, August 28, 2018, https://www.reuters.com/article/us-usa-iran-facebook-exclusive-idINKCN1LD2R9.

Stubbs, Jack and Katie Paul. "Facebook Says it Dismantles Disinformation Network Tied to Iran's State Media." *Reuters,* May 5, 2020, https://www.reuters.com/article/us-iran-facebook-idUSKBN22H2DK.

Sulmeyer, Michael. *Cyberspace: A Growing Domain for Iranian Disruption*. Washington DC: Center for Strategic and International Studies, 2017.

Tabatabai, Ariane M. *Iran's Authoritarian Playbook: The Tactics, Doctrine, and Objectives behind Iran's Influence Operations*. (Washington DC: Alliance for Securing Democracy, 2020). https://securingdemocracy.gmfus.org/wp-content/uploads/2020/09/Irans_Authoritarian_Playbook.pdf.

Timberg, Craig, Elizabeth Dwoskin, Tony Romm, and Ellen Nakashima. "Sprawling Iranian Influence Operation Globalizes Tech's War on Disinformation." *Washington Post*, August 21, 2018, https://www.washingtonpost.com/technology/2018/08/21/russian-iran-created-facebook-pages-groups-accounts-mislead-users-around-world-company-says/.

Timberg, Craig and Tony Romm. "It's not just the Russians Anymore as Iranians and Other Turn Up Disinformation Efforts Ahead of 2020 Vote." *Washington Post*, July 25, 2019, https://www.washingtonpost.com/technology/2019/07/25/its-not-just-russians-anymore-iranians-others-turn-up-disinformation-efforts-ahead-vote/.

___. "New Report on Russian Disinformation, Prepared for the Senate, Shows Operation's Scale and Sweep." *Washington Post*, December 17, 2018, https://www.washingtonpost.com/technology/2018/12/16/new-report-russian-disinformation-prepared-senate-shows-operations-scale-sweep/.

TOI Staff. "Cyber Attacks Again Hit Israel's Water System, Shutting Agricultural Pumps." *Times of Israel*, July 17, 2020. https://www.timesofisrael.com/cyber-attacks-again-hit-israels-water-system-shutting-agricultural-pumps/.

___. "Cyber Firm Says Three Iran-Run Sites are Targeting Israelis With Fake News." *Times of Israel,* September 6, 2018, https://www.timesofisrael.com/cyber-firm-says-iran-run-sites-target-israelis-with-fake-news/.

___. "Iran Duped Pakistan into Israel Nuke Threat as Tiny Part of Huge Fakery Campaign." *Times of Israel*, November 30, 2018, https://www.timesofisrael.com/iran-duped-pakistan-into-israel-nuke-threat-as-tiny-part-of-huge-fakery-campaign/.

___. "Iran Hackers Reportedly Tried to Phish Israeli Nuclear Scientists." *Times of Israel*, January 30, 2018, https://www.timesofisrael.com/iran-hackers-reportedly-tried-to-phish-israeli-nuclear-scientists/.

___. "Iran Spying on Israel, Saudi Arabia with Major Cyberattacks." *Times of Israel*, June 14, 2015, https://www.timesofisrael.com/iran-spied-on-israel-saudi-arabia-with-major-cyberattack/.

___. "Israel Behind Cyberattack that Caused 'Total Disarray' at Iran Port – Report." *Times of Israel*, May 19, 2020, https://www.timesofisrael.com/israel-said-behind-cyberattack-that-caused-total-disarray-at-iran-port-report/.

___. "Israel Publicly Blames Iran for Cyberattack on Major University Last Month." *Times of Israel*, March 7, 2023, https://www.timesofisrael.com/israel-publicly-blames-iran-for-cyberattack-on-major-university-last-month/.

___. "Website of Israeli Port Hacked; Sudanese Group Said to Claim Responsibility," *Times of Israel*, April 26, 2023, https://www.timesofisrael.com/websites-of-israeli-port-hacked-sudanese-group-said-to-claim-responsibility/.

Tokyay, Menkse. "Iran-Linked Hacker Group Targets Turkey's Cyber Network." *Arab News*, February 17, 2022, https://www.arabnews.com/node/2027016/middle-east.

Trobisch, Jan. *Challenges in the Protection of US Critical Infrastructure in the Cyber Realm*, School of Advanced Military Studies, US Army Command and General Staff College, Fort Leavenworth, KS, 2014.

U.S. Cyberspace Solarium Commission. *Report*, March 2020. https://www.solarium.gov/report.

U.S. Department of Homeland Security. ״CISA Statement on Iranian Cybersecurity Threats.״ CISA.gov, January 3, 2020, https://www.us-cert.gov/ncas/current-activity/2019/06/24/CISA-Statement-Iranian-Cybersecurity-Threats.

___. ״Cybersecurity Strategy.״ 2018, https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf.

U.S. Department of Justice. ״Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guards Corps.״ Press Release, March 23, 2018, https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary.

United Against Nuclear Iran (UANI). ״The Iranian Cyber Threat.״ *UANI.* (May 2020).

___. ״The Iranian Cyber Threat.״ (September 2022), 5–8, https://www.unitedagainstnucleariran.com/sites/default/files/UPDATE%20-%20The%20Iranian%20Cyber%20Threat_9.7.22_JC_JMB_CMJ.pdf.

United States Institute for Peace. ״Albania Cuts Ties With Iran Over Cyberattack.״ September 12, 2022, https://iranprimer.usip.org/blog/2022/sep/09/albania-cuts-ties-iran-over-cyberattack.

United States, Subcommittee on Emergency Preparedness, Response and Communications and the Subcommittee on Cyber Security, Infrastructure Protection and Security Technologies. ״Cyber Incident Response.״ (2014).

Vahdat, Amir and Jon Gambrell. ״Iran Leader Says Israel a ׳Cancerous Tumor׳ to be Destroyed.״ AP, May 22, 2020, https://apnews.com/article/a033042303545d9ef783a95222d51b83.

Valeriano, Brandon, Benjamin Jensen, and Ryan C. Maness. *Cyber Strategy: The Evolving Character of Power and Coercion.* New York: Oxford University Press, 2018.

Valeriano, Brandon and Ryan C. Maness. *Cyber War Versus Cyber Realities.* New York: Oxford University Press, 2015.

Volz, Dustin and Jim Finkle. ״U.S. Indicts Iranians for Hacking Dozens of Banks, New York Dam.״ *Reuters*, March 24, 2016, https://www.reuters.com/article/ctech-us-usa-iran-cyber-idCAKCN0WQ1JF.

Volz, Dustin. ״FBI Chief Blames Iran for Cyberattack on Boston Children׳s Hospital.״ *Wall Street Journal*, June 1, 2022, https://www.wsj.com/articles/fbi-chief-blames-iran-for-cyberattack-on-boston-childrens-hospital-11654096382.

Wakabayashi, Daisuke and Scott Shane. "Twitter, With Accounts Linked to Russia, to Face Congress Over Role in Election." *New York Times*, September 27, 2017, https://www.nytimes.com/2017/09/27/technology/twitter-russia-election.html.

Watts, Clint. "Rinse and Repeat: Iran Accelerates its Cyber Influence Operations Worldwide." Microsoft.com May 2, 2023, https://blogs.microsoft.com/on-the-issues/2023/05/02/dtac-iran-cyber-influence-operations-digital-threat/.

Wechsler, Omree. "The Iran-Russia Cyber Agreement and U.S. Strategy in the Middle East." *Council on Foreign Relations*, March 15, 2021, https://www.cfr.org/blog/iran-russia-cyber-agreement-and-us-strategy-middle-east.

Weiner, Rachel. "Iranian Men Accused of Hacking U.S. Aerospace Companies." *Washington Post*, September 17, 2020, https://www.washingtonpost.com/local/legal-issues/iranian-men-accused-of-hacking-us-aerospace-companies/2020/09/17/1a55f442-f8e7-11ea-89e3-4b9efa36dc64_story.html.

Weinthal, Benjamin. "Iran May Be Behind BDS 'Hit List" Targeting Boston Jews – Report." *Jerusalem Post*, March 5, 2023, https://www.jpost.com/diaspora/antisemitism/article-733382.

Winer, Stuart and Marissa Newman. "Iran Supreme Leader Touts 9-Point Plan to Destroy Israel." *Times of Israel,* November 10, 2014, https://www.timesofisrael.com/iran-supreme-leader-touts-9-point-plan-to-destroy-israel/.

Yaron, Oded. "Has Hezbollah's Cyber Spy Ring Been Exposed?" *Haaretz*, April 8, 2015, https://www.haaretz.com/2015-04-08/ty-article/.premium/has-hezbollahs-cyber-spy-ring-been-exposed/0000017f-e0c1-df7c-a5ff-e2fb9bec0000.

___. "Palestinians Behind Cyber Attacks on Israeli Army and Government Targets." *Haaretz*, February 16, 2015, https://www.haaretz.com/2015-02-16/ty-article/.premium/palestinians-behind-cyber-attacks-on-israeli-targets/0000017f-dbff-d856-a37f-ffff6f160000.

Ynet reporters. "Host of Israeli Sites Targeted in Massive Cyber-Attack." *Ynet* May 21, 2020, https://www.ynetnews.com/article/SkXO1amsU.

Ynet staff. "Report: Iran Behind Hack of Israeli Water Authority Sites." *Ynet*, May 7, 2020, https://www.ynetnews.com/article/By2gZO1198.

Young, Benjamin R. "How Iran Built Hezbollah into a Top Cyber Power." *National Interest*, April 11, 2022, https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/how-iran-built-hezbollah-top-cyber.

Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown, 2014.

Zimmt, Raz. "The Israeli Threat—The View From Iran." *Bein HaKtavim*, Dado Center for Interdisciplinary Military Research, forthcoming, Fall 2023.

Zitun, Yoav. "Shin Bet: Iran Tried to Enlist Israelis, Palestinians for Espionage, Terror." *Ynet*, July 24, 2019, https://www.ynetnews.com/articles/0,7340,L-5556631,00.html.

Ziv, Amitai. "Cash-Strapped Over Coronavirus, Crime Organizations Unload Cyberattacks." *Haaretz*, September 21, 2020, https://www.haaretz.com/israel-news/tech-news/2020-09-21/ty-article/.premium/cash-strapped-over-coronavirus-crime-cartels-unload-cyberattacks/0000017f-e3ac-d9aa-afff-fbfc13ab0000.

___. "Iran Suspected After Massive Cyberattack on Israeli Firms Revealed." *Haaretz*, December 13, 2020, https://www.haaretz.com/israel-news/tech-news/2020-12-13/ty-article/.premium/iran-suspected-after-massive-cyberattack-on-israeli-firms/0000017f-dbe1-df9c-a17f-fff95fab0000.

___. "'Iranian Attacker Impersonating Russians': Inside Recent Attacks on Israel." *Haaretz*, May 5, 2021, https://www.haaretz.com/israel-news/tech-news/2021-05-05/ty-article/iranians-impersonating-russians-inside-cyberattacks-on-israel/0000017f-e1e1-d7b2-a77f-e3e7baaf0000.

___. "The Iranians Read the Reports about Israel's Cyber Error, and Succeeded to Embarrass." *The Marker*, May 31, 2020, https://www-themarker-com.ezproxy.bgu.ac.il/technation/2020-05-31/ty-article/.premium/0000017f-dbed-d856-a37f-ffedd3c00000

איראן היא אחת המדינות הראשונות שגיבשו אסטרטגיית סייבר לאומית, ובכלל זה פיתוח של מוסדות המדינה החיוניים והיכולות הטכנולוגיות הדרושות. כיום איראן היא אחת המדינות הפעילות ביותר בתחום הסייבר, ונחשבת למובילה במעגל השני של השחקניות הגלובליות. תקיפות הסייבר של איראן הוכיחו את יכולתה לשבש מטרות אזרחיות ומסחריות, תשתיות לאומיות חיוניות ויכולות צבאיות. מבצעי הריגול ומבצעי התודעה שלה בסייבר נרחבים במיוחד, ואת עיקר מאמציה בסייבר היא מכוונת נגד ישראל וארצות הברית.

מחקר זה מציג ניתוח מקיף ועדכני של האסטרטגיה, המוסדות ודרך הפעולה של איראן בתחום הסייבר. חמשת חלקיו מציגים: רקע כללי על איום הסייבר ועל ההבדלים בינו ובין תחומי עימות אחרים; אסטרטגיית הסייבר של איראן, המוסדות והיכולות שפיתחה; תקיפות הסייבר העיקריות של איראן נגד ארצות הברית ונגד שחקניות אחרות במזרח התיכון ובעולם; איום הסייבר האיראני על ישראל; הערכת ההשפעה בפועל של התקיפות שאיראן ביצעה עד כה, מסקנות והמלצות למדיניות.

ד"ר צ'ק פרייליך, חוקר בכיר במכון למחקרי ביטחון לאומי (INSS), שירת יותר מעשרים שנה במערכת הביטחון של ישראל ושימש חוקר בכיר וסגן ראש המטה לביטחון לאומי. הוא היה עמית בכיר במרכז בלפר שבאוניברסיטת הרווארד ולימד מדעי המדינה באוניברסיטאות הרווארד, קולומביה, NYU ותל אביב. פרייליך מתמחה באסטרטגיית הביטחון הלאומי של ישראל, בתהליכי קבלת ההחלטות בישראל בענייני חוץ ובטחון, במדיניות האמריקנית במזרח התיכון וביחסי ארצות הברית וישראל. הוא העורך הבכיר של כתב העת Israel Journal of Foreign Affairs.

פרייליך הוא מחברם של הספרים: *Zion's Dilemmas: How Israel Makes National Security Policy* (הוצאת קורנל 2012); תפיסת הביטחון הלאומי של ישראל: אסטרטגיה חדשה לעידן של תמורותה (הוצאת מודן 2019; המקור -באנגלית בהוצאת אוקספורד 2018); *Israel and the Cyber Threat: How the Startup Nation Became a Global Cyber Power* (הוצאת אוקספורד 2023). הוא פרסם מאמרים אקדמיים רבים ויותר מ־220 מאמרי דעה, מופיע תדיר בתקשורת הישראלית והבינלאומית ומרצה בפני מגוון רחב של קהלים.