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 אירנים 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 לווייניים, 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 "שיר־ביט", 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.