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).