פעילותה של איראן במרחב הסייבר: זיהוי דפוסים והבנת האסטרטגיה

גבי סיבוני, לאה אברמסקי וגל ספיר

מאמר זה מציג את פעילות הסייבר המתפתחת של איראן, מתוך מטרה לזהות את הדפוסים העומדים מאחורי אסטרטגיית הסייבר שמיישם המשטר האיראני נגד איומים חיצוניים ופנימיים כאחד. המאמר פותח בתיאור פעולות הסייבר האיראניות, תוך התבססות על מידע שפרסמה הרפובליקה האסלאמית של איראן ועל דיווחים של חברות לאבטחת סייבר. לאחר מכן הוא מנתח את פעולות הסייבר של איראן. המאמר משרטט את המאפיינים והדינמיקה של פעולות הסייבר ההגנתיות וההתקפיות שלה, הן בזירה הפנימית והן בזירה החיצונית, ומציג ארבעה דפוסים נפוצים של פעילות הסייבר האיראנית שזוהו. לבסוף הוא מנתח את הממצאים העיקריים.

מילות מפתח: איראן, ביטחון סייבר, אסטרטגיית סייבר לאומית, בניין כוח, איומים פנימיים וחיצוניים, פעולה הגנתית והתקפית.

מבוא

המידע המוגבל על יכולות הסייבר של איראן עשוי היה להיות הגורם לכך שמשקיפים בין־לאומיים העריכו יכולות אלו בעשור האחרון בצורה שגויה. עם זאת, לאחרונה חל שינוי בתפיסת האיום האיראני. במהלך שבוע הסייבר 2019 שנערך בישראל, אישר יגאל אונא, ראש מערך הסייבר הלאומי, כי האיראנים נמנים על חמשת השחקנים המדינתיים הפעילים ביותר בתחום הסייבר. עוד ציין אונא כי "האיראנים פעילים ברציפות מזה זמן רב ביזימת מתקפות רחבות היקף, כולל מתקפות לאיסוף

פרופ' גבי סיבוני הינו ראש תוכנית ביטחון סייבר במכון למחקרי ביטחון לאומי. לאה אברמסקי היא מתמחה במכון למחקרי ביטחון לאומי. גל ספיר היא עוזרת מחקר בתוכנית ביטחון סייבר במכון למחקרי ביטחון לאומי.

מודיעין ומִבצעי השפעה, וכן מתקפות שנועדו להסב נזק והרס למערכות. איראן היא אחת המדינות היחידות שמוציאה לפועל מתקפות הרסניות".[1]

השינוי שהתרחש לאחרונה בדרך שבה נתפס האיום האיראני על ידי מדינות המערב מעורר תהיות לגבי העלייה ברמתן של היכולות האיראניות. לאור זאת, רצוי להגדיר את האיום האיראני ולתאר את המאפיינים של אסטרטגיית הסייבר הלאומית של איראן, אותה היא מיישמת נגד אויביה. מומחים אכן זיהו התעצמות בפעילות הסייבר האיראנית, והיא גם תועדה היטב על ידי חברות לאבטחת סייבר. על פי סקר של חברת "מיקרוסופט", שפורסם במארס 2019, קבוצות סייבר איראניות תקפו במהלך השנתיים האחרונות אלפי אנשים ויותר ממאתיים חברות ברחבי העולם, וגרמו לנזקים משמעותיים המוערכים במאות מיליוני דולרים.[2]

מאז ראשית המאה ה־21 הִשקיעה איראן חלק ניכר מתקציבה בשיפור יכולות הסייבר שלה. בשלוש השנים הראשונות לכהונתו הראשונה של הנשיא רוחאני (2013־2017) עלה תקציב הביטחון האיראני ב־1,200 אחוזים.[3] פרנק צ'ילופו, מנהל המרכז לביטחון הסייבר והמולדת וסגן נשיא אוניברסיטת ג'ורג' וושינגטון, הצהיר בשנת 2017 כי "בשנים האחרונות השקיעה איראן רבות בבניית יכולות למתקפת רשתות מחשב ולפריצה למחשבים. תקציב הסייבר של איראן קפץ תחת הנשיא רוחאני פי 12, והפך את איראן לאחת מחמש מעצמות הסייבר המובילות. איראן משלבת מבצעי סייבר גם באסטרטגיה ובדוקטרינה הצבאית שלה".[4]

שני אירועים בולטים מרכזיים היו בהתפתחות הפעילות האיראנית במרחב הסייבר. הראשון היה המחאה האזרחית שהתעוררה באיראן בשנת 2009 תחת השם "התנועה הירוקה", שקיבלה בכלי התקשורת הזרים את הכינוי "מהפכת הטוויטר". לאחר הבחירות לנשיאות איראן ב־2009 והניצחון של אחמדינג'אד על יריבו הראשי מוסאווי, יצאו המונים להפגין ברחובות איראן במחאה על תוצאות הבחירות.[5] המוחים לבשו ירוק – צבע הקמפיין של מוסאווי, שגם נתן את השם

1 The Israel National Cyber Directorate, "Iran Is a Main Cyber Threat on the Middle East", *Israel National Cyber Directorate*, June 26, 2019, https://www.gov.il/en/departments/news/unna_cyber_week_2019.

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

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

4 Sam Cohen, "Iranian Cyber Capabilities: Assessing the Threat to Israeli Financial and Security Interests", *Cyber, Intelligence and Security* 3, no. 1 (2019): 71-94.

5 "Editorial: Iran's Twitter Revolution", *The Washington Times*, June 16, 2009, https://www.washingtontimes.com/News/2009/Jun/16/Irans-Twitter-Revolution/.

לתנועת המחאה – וטענו לזיוף תוצאות הבחירות. למרות ניסיונות הדיכוי של המשטר, המפגינים נותרו פעילים עוד חודשים רבים לאחר מכן. הם ריכזו את מאמציהם בערוצי הרשתות החברתיות, כמו "טוויטר", "פייסבוק" ו"יוטיוב", הן למטרות ארגוניות והן כפלטפורמה להעברת עדכונים ומידע בתוך המדינה ומחוצה לה. השימוש יוצא הדופן שנעשה בטכנולוגיות מידע ותקשורת (ICT) עזר לחזק את התנועה, תוך שהממשלה נאבקת לסכל את פעילותה. התוצאה הייתה שהמשטר האיראני נאלץ לשפר את היכרותו עם מרחב הסייבר ואת מיומנותו לפעול בתוכו. פיתוח אסטרטגיית סייבר הפך מאז לצורך חיוני עבורו.

האירוע המרכזי השני היה מתקפת "סטקסנט" (Stuxnet), שנתפסת כגורם מכריע בחתירתה של איראן לגיבוש תוכנית לאומית לבניית יכולות הסייבר שלה. התוכנה הזדונית "סטקסנט" נחשפה בשנת 2010, לאחר שתקפה מערכות מחשב איראניות.[6] הפעילות המדויקת של "סטקסנט" נותרה בלתי ברורה – דבר שמלמד על תקופת פעילות ארוכה עד לחשיפתה.[7] היא גרמה להרס עצמי של כמעט אלף צנטריפוגות – כחמישית מכלל הצנטריפוגות שהיו פעילות במתקן ההעשרה הגרעיני של נתנז – ולעיכוב ניכר בתוכנית הגרעין האיראנית.[8] השפעת התוכנה הזדונית חשפה את הפגיעות שמדינות חוות לנוכח התחזקות הקישוריות בין מגזרים קריטיים. הופעתן של הטכנולוגיות החדשות גם הדגישה את הצורך בשיפור האבטחה, כדי לשמור ולהגן על מדינות במרחב הסייבר.

שני אירועים מרכזיים אלה, לצד הלחץ הכלכלי והעיכוב בתוכנית הגרעין האיראנית, עודדו את טיפוח החוסן החברתי והכלכלי במדינה. נראה כי השיטה האיראנית לטיפוח החוסן הייתה באמצעות "כלים היברידיים", כולל פעילויות סייבר. במובן זה, ניתן לראות בפיתוח יכולות הסייבר גם אמצעי של המשטר האסלאמי להתמודד עם יריבים מבית ומחוץ.

בחלק הבא של המאמר נבחן עובדות, אירועים, נתונים והצהרות רשמיות במטרה לזהות דפוסים נפוצים בפעילות הסייבר האיראנית ולהבין אותה. מאפיינים אלה יאפשרו לנו לאחר מכן לנתח ולהבין את מה שנתפס כאסטרטגיית הסייבר של איראן.

---

6 Josh Fruhlinger, "What Is Stuxnet, Who Created It and How Does It Work?", *CSO*, August 22, 2017, https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html.

7 The Israel National Cyber Directorate, "Iran is a Main Cyber Threat on the Middle East".

8 Taylor Armerding, "Whatever Happened to Stuxnet", *Synopsys*, January 17, 2019, https://www.synopsys.com/blogs/software-security/whatever-happened-to-stuxnet/.

התמודדות עם אויבים חיצוניים

המשטר האיראני הקים במהלך השנים מערך סייבר, הכולל קבוצות האקרים מאורגנות שפועלות תחת ארגוני הביטחון השונים של המדינה, וכן ארגונים עצמאיים הפועלים לטובת המשטר. בנוסף לכך, מספר ארגונים ומדינות במזרח התיכון זוכים לתמיכה איראנית ומתפקדים כשליחים יעילים של האינטרסים האיראניים בתחום הסייבר. מטרת חלק זה של המאמר היא להכיר את פעילות הסייבר של איראן ואת האופן שבו היא תומכת באסטרטגיית הסייבר של המשטר.

מבצע "אבָּאבִּיל" נחשב לאחת מההתקפות ההרסניות ביותר של איראן, והוא חלק מאסטרטגיית ההגנה שלה נגד ארצות הברית. המבצע, שהחל בשנת 2012, עדיין פעיל, וכולל גרסאות שונות וגלים של מתקפות מניעת שירות מבוזרת (DDoS).[9] הגל הראשון של המתקפה התמקד במערכת הפיננסית של ארצות הברית ותקף בנקים אמריקאיים, שבשעתם לא היו מוכנים לנֶפַח התנועה הפתאומי. המתקפה חסמה את האתרים והשרתים של אותם בנקים ומנעה מלקוחותיהם את היכולת להשתמש בשירותי בנקאות מקוונים. לוחמי סייבר על שם עז א־דין אל־קסאם, הקשורים ככל הנראה לממשלת איראן, קיבלו את האחריות למתקפה זו. במקרה זה השתמשה איראן בכוח הסייבר שלה באמצעות שחקן הנתון לחסותה כדי לתקוף את אחד מאויביה העיקריים – הממסד הפיננסי האמריקאי.

בשנת 2012 חדרה תוכנה זדונית הרסנית בשם "Shamoon" למערכות המחשב של ענקית הנפט הסעודית "ארמקו" וגרמה לנזקים רבים ולעלויות התאוששות גדולות. יש לראות בהתקפות נגד יעדים אסטרטגיים של ערב הסעודית ובעלות בריתה באזור, כמו RasGas בקטר, חלק מהאסטרטגיה ההגנתית האיראנית במרחב הסייבר.[10] גרסאות נוספות של התוכנה הזדונית תקפו ב־2016 יעדים חדשים, בעיקר משרדי ממשלה כמו משרד העבודה הסעודי, וכן חברות בערב הסעודית, כמו הבנק המרכזי של המדינה.[11] ב־2018 תקפו גלים חדשים של התוכנה הזדונית תעשיות קריטיות (נפט, אנרגיה, טלקומוניקציה) וארגונים ממשלתיים בכל רחבי האזור.

במאי 2016 דווח כי ארגון הממומן על ידי איראן השתמש באתרים ובשרתים כדי לתקוף כ־120 ארגונים ומוסדות ישראליים.[12] קבוצת ההאקרים, שבהמשך

9 "Operation Ababil DDoS Attack", *Radware*, https://security.radware.com/ddos-experts-insider/expert-talk/ddos-attacks-operation-ababil/.

10 "Operation Cleaver", *Cylance*, 2014.

11 Collin Anderson and Karim Sadjadpour, *Iran's Cyber Threat: Espionage, Sabotage and Revenge* (Washington DC: Carnegie Endowment for International Peace, 2018), pp. 1-57.

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

זוהתה בשם "OilRig",[13] פעלה בשמה של ממשלת איראן מאז שנת 2015. במאי 2017 תקפה אותה קבוצת האקרים מערכות מחשבים של קבלן ביטחון אמריקאי, הפעם תוך שימוש בכלי תקיפה שמקורם ברוסיה.[14] מומחי האבטחה של החברה האמריקאית ציינו כי מדובר במקרה הראשון של שיתוף פעולה בין האקרים איראניים להאקרים רוסיים שמוכרים את שירותיהם לכל המרבה במחיר. המתקפה חשפה גם את השדרוג המשמעותי ביכולותיהם של ההאקרים האיראניים. חודשים ספורים לאחר מכן הגיש משרד האוצר האמריקאי כתב אישום נגד חברת Ajily Software Procurement Group בגין היותה ארגון פשע בין־לאומי. הארגון האיראני השתמש בהאקרים כדי לגנוב מארצות הברית וממדינות מערביות אחרות תוכנות הנדסיות שניתן להשתמש בהן כדי לתכנן נשק מונחה GPS.[15] מתקפה זו הייתה חלק מיוזמות ההגנה של איראן בתגובה לסנקציות הכלכליות שהטילה עליה ארצות הברית. בניגוד למקרים הקודמים שנדונו כאן, מקרה זה עירב גניבה וריגול עיסקי והמחיש כיצד ממשלת איראן מגייסת את יכולותיה במרחב הסייבר כדי לעקוף את הסנקציות האמריקאיות ולייבא טכנולוגיה צבאית על ידי שכירת שירותיהם של האקרים.

ביוני 2014 נחשף כי ארגון טרור סייבר איראני, המזוהה עם משמרות המהפכה האיראניים, תקף מאות יעדים בישראל ובמזרח התיכון במשך כשנה. קבוצת ההאקרים, שנקראה "Ajax Team" או "Rocket Kitten", פעלה בשנים האחרונות במסגרת ארגוני הביטחון האיראניים.[16] המתקפה הרב־שלבית שמה לה כמטרה מגוון של יעדים, ובהם מדענים ישראלים, צוותי שגרירות, פקידי נאט"ו, מתנגדי משטר באיראן, משפחת המלוכה הסעודית ואחרים. מטרת המתקפה הייתה להשיג גישה למידע קריטי ולגנוב אותו. מומחים העריכו כי מדובר במערכת התקפית ממוקדת, מתוחכמת, קבועה ושיטתית, המבוססת על איסוף מודיעין ומידע ממוקד על היעדים. בנובמבר 2015 פרצו משמרות המהפכה לשרתי הדוא"ל והרשתות החברתיות של חברי הממשל של נשיא ארצות הברית לשעבר ברק אובמה, וחברת "פייסבוק" אישרה כי זיהתה ניסיונות להשתלט על פרופילים של עובדי ממשל אמריקאים.

13 Bryan Lee, Robert Falcone, "Behind the Scenes with Oil Rig", *Unit 42*, April 30, 2019, https://unit42.paloaltonetworks.com/behind-the-scenes-with-oilrig/.

14 Nicole Perlroth, "Web Defenders Detect Russian Hand in Iranians' Hacking Attempt", *The New York Times*, May 15, 2017, https://www.nytimes.com/2017/05/15/technology/web-defenders-detect-russian-hand-in-iranians-hacking-attempt.html.

15 "Ajily Software Procurement Group", *Iran Watch*, August 8, 2017, https://www.iranwatch.org/iranian-entities/ajily-software-procurement-group.

16 "Rocket Kitten: A Campaign with 9 Lives", *Check Point*, 2015.

ביולי 2017 פרסמה חברת מודיעין הסייבר ClearSky דוח על מבצע מודיעין סייבר איראני המכונה "Wilted Tulip".[17] בפעולה זו הצליחו האקרים איראניים, המכונים "CopyKittens", להשיג גישה למידע של מספר סוכנויות ממשלתיות בישראל.[18] ההאקרים השתמשו במגוון שיטות, ובכלל זה במתקפת Watering Hole, שכללה פריצה לאתרי חדשות, הדבקה שלהם ושליחת קישורים לשורה של קורבנות במסווה של מאמרים לגיטימיים, במטרה להשתלט על המחשבים שלהם. הרצון לזכות באמון הקורבנות ולגרום להם ללחוץ על הקישורים לאתרים הנגועים הביא את הקבוצה להשתמש ברשת מורכבת ואמינה יחסית של פרופילים ב"פייסבוק", שחלקם קיימים כבר שנים. כדי לחזק את האותנטיות של אותם פרופילים, הוקמו ברשת החברתית מספר אתרים (שנבנו בפלטפורמת בניית אתרים איראנית) וכן דפים עיסקיים. הקורבנות כללו סוכנויות ממשלתיות וחברות פרטיות במספר מדינות במזרח התיכון, כמו ישראל, ערב הסעודית וטורקיה, וכן במדינות מערביות, כמו ארצות הברית וגרמניה.

בשנת 2018 תקפה איראן יעדים ישראליים, תוך שימוש בתוכנה זדונית המכונה "מאדִי", וכן מכוני מחקר אמריקאיים וחברות ומוסדות אקדמיים, במטרה לגנוב מידע ומסמכים מיוֹתר מ־800 קורבנות.[19] בנובמבר 2019 הצהירה חברת "מיקרוסופט" כי זיהתה פעילות סייבר אינטנסיבית מצד קבוצת האקרים בשם "Phosphorous", שקשורה כנראה לממשלת איראן.[20] פעולת הסייבר כוונה נגד בכירי ממשל אמריקאים בהווה ובעבר, עיתונאים, אירנים המתגוררים מחוץ לאיראן, וכן מועמדים פוטנציאליים לבחירות לנשיאות ארצות הברית בשנת 2020 (אם כי לא צוין מי מהם). ההתקפה כללה יותר מ־2,700 ניסיונות לזהות חשבונות דוא"ל השייכים ליעדים הספציפיים, ולאחר מכן פגיעה ב־241 חשבונות כאלה.[21] מבצע מסוג זה, שמטרתו להתערב במערכות בחירות זרות, הפך למקור מרכזי לדאגה מאז שהממשל האמריקאי הגיע למסקנה שרוסיה הצליחה לשבש את תהליך הבחירות לנשיאות בשנת 2016. הניסיון לשבש בחירות זרות ולתקוף אנשים מחוץ לאיראן הוא חלק מהפעילות ההתקפית של איראן.

---

17 Eduard Kovacs, "Iranian CopyKittens Conduct Foreign Espionage", *Security Week*, July 25, 2017, https://www.securityweek.com/iranian-copykittens-conduct-foreign-espionage.

18 "Operation Wilted Tulip", *Clearsky Security and Trend Micro*, July 2017.

19 GReAT, "The Madi Campaign – Part I", *Kaspersky*, July 17, 2012. https://securelist.com/the-madi-campaign-part-i-5/33693/.

20 "Microsoft: Iranian Hackers Targeted a US Presidential Campaign", *Asharq Al-Awsat*, October 4, 2019, https://aawsat.com/english/home/article/1931446/microsoft-iranian-hackers-targeted-us-presidential-campaign.

21 Ibid.

התמודדות עם אויבים פנימיים

בעוד שלאחרונה נשמעו קריאות להגביל את הגישה לאינטרנט, למעשה איראן נקטה זה מכבר אמצעים המאפשרים למשטר לשלוט בגישתם של אנשים לקישוריות. ממשלת איראן משתמשת בשליטה שיש לה על הגישה לאינטרנט כאמצעי לשיבוש התקשורת במדינה, במיוחד בתקופות של תסיסה עממית. מאז 2009, כל מחאה המונית הובילה את המשטר להטיל מגבלות על הגישה לאינטרנט.[22] בנובמבר 2019, לאחר שהממשלה הודיעה על העלאה ניכרת במחירי הדלק, פרצו מחאות אזרחיות בטהראן ובערים איראניות אחרות. כוחות הביטחון האיראניים הגיבו בדיכוי אלים של המהומות ובהשבתה ארצית של האינטרנט למשך כמעט שבוע – מהלך שניתק לחלוטין את האזרחים מהרשת. מחאה זו הייתה דוגמה רלוונטית לשימוש שאיראן עושה בכוחה במרחב הסייבר למטרות פנימיות: למנוע מהאוכלוסייה לתקשר, להתארגן, לשתף מידע ולהפגין.[23]

מאמצי הרשויות לחסום את האינטרנט ולהגביל את הגישה של אנשים לפלטפורמות תקשורת באופן כללי, או לפתח פרויקט אינטרנט לאומי, הלכו והתגברו ומצאו את ביטוים בניסיונות להגביל את השימוש ב־VPN (רשת פרטית וירטואלית) בקרב האוכלוסייה. כך, למשל, ממשלת איראן חייבה את נותני שירותי האינטרנט לחתום על התחייבות הקובעת כי "הקמה והפצה של שירותי VPN ושירותי פרוקסי" אסורות.[24] בנוסף לניסיון למנוע מאנשים להשתמש ברשתות VPN, איראן מנסה ככל הנראה ליצור רשת VPN לאומית שתפקח על הגישה לאינטרנט של כל אזרח בהתבסס על מקצועו. כך עולה מהצהרה מ־11 בנובמבר 2019 של חמיד פאתחי, מנכ"ל "חברת תשתיות טלקומוניקציה" (TIC), שהיא חברה בבעלות ממשלתית.[25]

מאז שנת 2005 תמך המשטר האיראני, תחת הנהגתו של הנשיא ח'אתמי, ברעיון של רשת לאומית סגורה.[26] ב־2010 הוצג הפרויקט של יצירת רשת "אינטרנט חלאל"

22 Borzou Daragahi, "Massive Iranian Internet Shutdown Could Be Harbinger of Something Even Darker to Come, Experts Warn", *The Independent*, November 30, 2019, https://www.independent.co.uk/news/world/middle-east/iran-internet-shutdown-protests-communications-tehran-a9226731.html.

23 Amy Slipowitz, "The True Depth of Iran's Online Repression", *Freedom House*, December 2, 2019, https://freedomhouse.org/blog/true-depth-iran-s-online-repression.

24 "State-Developed VPN Would Determine Iranians' Internet Access Based on their Job", *Center for Human Rights in Iran*, November 21, 2019, https://iranhumanrights.org/2019/11/state-developed-vpn-would-determine-iranians-internet-access-based-on-their-job/.

25 Ibid.

26 Julie Kebbi, "Internet: l'Autre repression du régime iranien", *L'Orient-le-jour*, November 22, 2019, https://www.lorientlejour.com/article/1195979/internet-lautre-

באיראן, שנועד לשמור על ערכים איראניים ולמנוע חדירה של איומים זרים. רשת כזאת גם תאפשר לרשויות לשלוט על גורמים פנימיים ולעקוב אחרי מתנגדים פוטנציאליים.[27] היוזמה הופיעה זמן קצר לאחר חשיפת מתקפת "סטקסנט", והיא נתפסה כחלק מהצורך לתת מענה לסיכונים ולאיומים החדשים שהחלו להתעורר מול איראן. למרות הספקנות של משקיפים בנוגע להצלחתו של פרויקט כזה, מדינות נוספות החליטו לאמץ טקטיקה דומה. כך, למשל, רוסיה העבירה בנובמבר 2019 חוק שמאפשר למדינה ליצור אינטרנט למשתמשים רוסיים בלבד, שיהיה סגור לחלוטין בפני שחקנים חיצוניים ויישלט על ידי הרשויות הרוסיות, מה שמלמד על המניע האמיתי לקידומו של פרויקט כזה.[28]

הרעיון של "אינטרנט חלאל", המכוּנה גם "רשת המידע הלאומית של איראן" (SHOMA), התפתח על רקע הגברת המעקב באינטרנט אחר האוכלוסייה המקומית.[29] ואכן, שוב ושוב נשמעות קריאות של גורמי ממשל איראניים להגברת הפיקוח וההגבלות באינטרנט, והנשיא רוחאני נאלץ לספוג מתקפות תכופות של שמרנים, המאשימים אותו שהוא חלש ואינו מגיב בצורה מספקת לאיום הנובע מהאינטרנט.[30] לדוגמה, במאי 2019 קרא התובע הכללי של איראן, מוחמד ג'עפר מונתזרי, לחיזוק הפיקוח וההגבלות על האינטרנט. הוא הזהיר ישירות את שר התקשורת וטכנולוגיות המידע, מוחמד ג'וואד אזָרי ג'הרוֹמי,[31] שככל הנראה נתפס כרפורמיסט גדול מדי, כי יהיה עליו לתת את הדין על העיכובים ביישום ההגבלות החדשות ועל כך ש"האינטרנט הלאומי" לא הושק כפי שרצה המנהיג העליון עלי ח'מנאי.

במקביל למגבלות המרובות שאיראן מטילה על ענקיות תקשורת זרות, כמו "טלגרם" (אפליקציית מסרים מיידיים), המשטר מסייע בפיתוח פלטפורמות חלופיות על ידי מתן תמיכה טכנית ומשאבים כספיים לאפליקציות המסרים המיידיים האיראניות "סוֹרוּש" ו"בֵּייל", הפועלות ברמה הלאומית. אינדיקציה לכך שאיראן

---

repression-du-regime-iranien.html.

27 Christopher Rhoads and Farnaz Fassihi, "Iran Vows to Unplug Internet", *The Wall Street Journal*, May 28, 2011, https://www.wsj.com/articles/SB100014240527487048894045762773914490020 16.

28 Lucie Bras, "Russie: à quoi va ressembler le « Runet », le nouvel internet 100% russe contrôlé par Moscou?", *20Minutes*, November 5, 2019, https://www.20minutes.fr/high-tech/2644575-20191105-russie-quoi-va-ressembler-runet-nouvel-internet-100-russe-controle-moscou.

29 Slipowitz, "The True Depth of Iran's Online Repression".

30 "En Iran, la justice appelle à davantage de surveillance sur Internet", *Le Monde*, May 4, 2019, https://www.lemonde.fr/keyhani/article/2019/05/04/en-iran-la-justice-appelle-a-davantage-de-surveillance-sur-internet_5994643_5470831.html.

31 "Iran Prosecutor Warns Minister to Tame Social Media or Face Consequences", *Radio Farda*, May 5, 2019, https://en.radiofarda.com/a/iran-prosecutor-warns-minister-to-tame-social-media-or-face-consequences-/29922128.html.

מוכנה לעודד יצירת אפליקציות מקומיות ניתנה ב־2017, כאשר המדינה הציעה מענקי תמריץ של יותר מ־200,000 דולר למפתחי תוכנה שיצליחו להגיע למיליון משתמשים בפלטפורמת התקשורת שלהם.[32] גופים ממשלתיים נהנים מהמדיניות הרופפת בשאלת הפרטיות, המאפשרת להם לאסוף ולאחסן את נתוני המשתמשים – מצב שמהווה סכנה פוטנציאלית ללקוחות.[33] מכיוון שהמשטר האיראני משתמש בכוחו כדי לפקח על השימוש באינטרנט, הוא גם מצנזר את האינטרנט הקיים וגם מייצר חלופות שיאפשרו לו לממש שליטה רבה יותר ברשת.

ניתוח מבצעי הסייבר ובניין הכוח של איראן

מאז סוף העשור הראשון של המאה ה־21 מוכתבים האינטרסים האיראניים במרחב הסייבר על פי התפתחות סיכוני הסייבר והאיומים על המשטר האסלאמי. איראן השקיעה כמות רבה של משאבים כדי לפעול במרחב הסייבר, אותו היא רואה כשדה קרב פעיל נגד ארצות הברית ובעלות בריתה. היא עושה זאת תוך התקדמות בערוצים מרובים במקביל, הן כדי להגן על המשטר מפני התקפה מצד תרבות המערב והן כדי להשמיד פיזית תשתיות מערביות.[34] המשטר מוביל פעולות תגמול נגד אויבים המנסים לכאורה לתקוף את איראן, עורך מבצעי ריגול בסייבר שנועדו להשיג מידע על פעילותו ויכולותיו של האויב, וכן מקיים פעולות התקפיות שמטרתן להסב נזקים לאותם אויבים. בפורום השמיני להגנה אזרחית לאומית, שהתקיים בטהראן בנובמבר 2019, הודיע ראש ארגון ההגנה האזרחית של איראן, הגנרל גולאם רזה ג'לאלי, כי איראן מאמצת גישה הגנתית חדשה נגד האיומים ההיברידיים והרב־שכבתיים החדשים, ומפתחת מוצרי הגנה שישמשו אותה במרחב הסייבר.[35]

היעדים למתקפות הסייבר האיראניות הם מתנגדי המשטר במדינה, כמו גם יריביה של איראן במערב ובמזרח התיכון, ובהם ישראל וערב הסעודית. רבים מהיעדים הם ארגונים עם שיוך אזרחי, כמו מערכות אבטחה, חברות פרטיות, גורמים אקדמיים, פקידי ממשל ותשתיות ציבוריות. כמו בשנים קודמות, מתקפות הסייבר האיראניות ממשיכות להיות אפקטיביות הודות לרמה הגבוהה של תכנון המבצעים והגישה המערכתית שבה הם מוצאים לפועל. למרות שהמתקפות

32 "In Iran, State-Sanctioned Messaging Apps Are the New Hallmark of Internet Nationalization", *Global Voices*, October 24, 2018, https://advox.globalvoices.org/2018/10/24/in-iran-state-sanctioned-messaging-apps-are-the-new-hallmark-of-internet-nationalization/.

33 "Pressure on Web Service Providers in Iran to Ban Proxies", *BBC Persia*, November 23, 2019, https://www.bbc.com/persian/iran-50531178.

34 דעת המחברים בהתבסס על המחקר.

35 "Iran Opts for New Civil Defense Approach to Confront US Threats", *Fars News Agency*, November 5, 2019, https://en.farsnews.com/newstext.aspx?nn=13980814000432.

האיראניות אינן מתוחכמות מבחינה טכנולוגית, הרמה הטכנית שלהן עלתה בצורה ניכרת בשנים האחרונות.[36]

פיתוח תחום הסייבר מהווה ביטוי לחדשנות טכנולוגית ומחזק את מעמדה של איראן במערכת הבין־לאומית כמעצמה טכנולוגית אזורית. המשאבים הרבים שמשקיע המשטר בטהראן בסייבר נשאו פירות גם במגזר האזרחי, לאחר שתשתיות התקשורת במדינה הורחבו לאזורים הכפריים ומהירות הגלישה באזורים העירוניים עלתה.

בחלק הבא של המאמר יוצגו ארבע תבניות עיקריות המאפיינות את האסטרטגיה האיראנית במרחב הסייבר. הראשונה היא האסטרטגיה של "מידה כנגד מידה" בפעולות הסייבר ההגנתיות וההתקפיות, שמותאמת להתפתחויות הגיאו־פוליטיות ומציגה דפוס של פעולות התקפיות נגד אויבים חיצוניים; השנייה היא פיתוח יכולות סייבר פנימיות במטרה לבנות חוסן כלכלי, כלומר כדי להיות חלק מהכלכלה העולמית למרות הסנקציות הבין־לאומיות ולקחת חלק בחדשנות טכנולוגית. ניתן לסווג תבנית זאת כדפוס של האסטרטגיה האיראנית במרחב הסייבר בזירה הפנימית, הכוללת יוזמות התקפיות והגנתיות גם יחד; המאפיין השלישי של אסטרטגיית הסייבר האיראנית הוא התאמה למערך הערכים, הדת והתרבות של המשטר, הן באסטרטגיה ההתקפית וההגנתית והן כלפי פנים וכלפי חוץ; המאפיין הרביעי והאחרון הוא הניצול המלא של ערכת הכלים של הסייבר והיעדר מסגרת חוקית שתבדיל את הסייבר מתחומי פעילות אחרים. מצב זה מאפשר לאיראן לחזק את האסטרטגיה ההתקפית שלה נגד יריבים פנימיים וחיצוניים כאחד.

אסטרטגיית "מידה כנגד מידה" תוך התאמתה להקשר הגיאו־פוליטי

איראן האיצה את פעילותה במרחב הסייבר זמן קצר לאחר שנחשף וירוס "סטקסנט". שנתיים לאחר מכן, הסנקציות הכלכליות שהטילה ארצות הברית הובילו את הרפובליקה האסלאמית להשתמש בסייבר לתקיפת יריבתה האמריקאית. אפשר לכנות את האסטרטגיה האיראנית במרחב הסייבר כאסטרטגיה של "מידה כנגד מידה", מכיוון שהיא מתאימה את תגובותיה למתחים הגיאו־פוליטיים ברמה האזורית או הבין־לאומית כחלק מהאסטרטגיה ההתקפית שלה במרחב הסייבר נגד אויבים חיצוניים. השימוש בפעילות התקפית במרחב הסייבר כדי להגיב על אירועים גיאו־פוליטיים הוא מנגנון קבוע באיראן. משמעות הדבר היא שאסטרטגיית הסייבר האיראנית קשורה, שלא לומר תלויה, באינטרסים הגיאו־פוליטיים של איראן ומותאמת אליהם. זהו מרכיב מעניין המאפיין את אסטרטגיית הסייבר האיראנית,

36 Schaefer, "The Cyber Party of God: How Hezbollah Could Transform Cyberterrorism".

שכן מדינות אחרות (כמו סין או רוסיה) אינן מתכננות את אסטרטגיית הסייבר שלהן במיוחד כתגובה להתפתחויות גיאו־פוליטיות.[37]

ארצות הברית ראתה במבצע "אבאביל" את ההתקפה המשמעותית ביותר שאיראן ביצעה בתגובה לסנקציות הכלכליות הבין־לאומיות שהממשל האמריקאי כפה להטיל עליה בעקבות פיתוח תוכנית הגרעין האיראנית. התקפה זו הייתה משמעותית ברמתה ובעוצמתה, ומשרד החוץ האמריקאי הגיש ב־2016 כתב אישום נגד שבעה אזרחים איראניים שהיו קשורים למשמרות המהפכה, בגין חלקם באותה מתקפה.

המאפיין של התאמת אסטרטגיית הסייבר של איראן להתפתחויות גיאו־פוליטיות ניכר כבר במשא ומתן על הסכם הגרעין ("תוכנית הפעולה המשותפת"). גורמים רשמיים בארצות הברית ציינו כי בשנים 2013 ו־2014 – התקופה שקדמה להסכם – ביצעה איראן פעולות סייבר שהסבו נזק ניכר לחברות במערב ולאויביה של איראן במזרח התיכון.[38] כאשר הוטלו סנקציות על איראן ניתן היה להבחין בעלייה ברורה במספר המתקפות האיראניות במרחב הסייבר, בעוד שהסכם הגרעין השפיע ממשית על אסטרטגיית הסייבר של איראן, מכיוון שעם החתימה עליו ירדו תדירות המתקפות והיקפן. כאשר הנשיא טראמפ הודיע במאי 2018 על החלטתו לפרוש מהסכם הגרעין, חלה השפעה הפוכה: פחות מ־24 שעות לאחר מכן פתחה איראן בקמפיין אגרסיבי של מיילים מסוג "פישינג", שנשלחו לבעלות בריתה של ארצות הברית בחו"ל. היקף ההכנות הדרוש למתקפה כזאת מעיד על כך שהכוחות האיראניים הכינו אותה עוד לפני הכרזתו של טראמפ, ובחרו להוציאה אל הפועל בתגובה להחלטתו. ואמנם, מומחים זיהו אז עלייה מחודשת בפעולות הסייבר ההתקפיות שהגיעו מאיראן, מה שביטא שינוי של ממש במדיניות האיראנית.[39] על פי מומחי אבטחת סייבר, המאמצים האיראניים לתקוף מתקנים ואזרחים אמריקאיים במרחב הסייבר התגברו לאחר 2018 ובעקבות נסיגת ארצות הברית מהסכם הגרעין.[40]

---

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

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

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

40 "Iranian Hackers Wage Cyber Campaign amid Tensions with US", *Asharq Al-Awsat,* June 22, 2019, https://aawsat.com/english/home/article/1779921/iranian-hackers-wage-cyber-campaign-amid-tensions-us.

האסטרטגיה של "מידה כנגד מידה" כוללת גם את הפעילות שאיראן מבצעת מחוץ לגבולותיה באמצעות שליחים (by proxy). הגל השני של מבצע "Shamoon", בשנים 2016־2017, כלל התייחסויות לתימן ותמונה של הילד הסורי אלן כורדי, שהופיעה במכשירים מותקפים ונתפסה כנקמה על פעולות סעודיות בסוריה ובתימן. ביוני 2019 הודיעו החברות CrowdStrike ו־FireEye על התגברות פעולות הסייבר ההתקפיות של איראן.[41] פעילות התקפית זו באה זמן קצר לאחר שממשל טראמפ הטיל סנקציות חדשות על ענף הפטרוכימיה האיראני. על פי CrowdStrike, קבוצת ההאקרים "Refined Kitten", שמתקפת הסייבר מיוחסת לה, מנסה כבר שנים לפגוע בתעשיות הביטחון והאנרגיה האמריקאיות. בספטמבר 2019 הואשמה איראן בביצוע המתקפה נגד "ארמקו", אם כי היא הכחישה את הדברים והאשימה במתקפה את החותים (שיעים זיידים בתימן).[42] מתקפה זו הייתה בעלת השפעה משמעותית על יצרנית הנפט הגדולה בעולם ועיכבה את ייצור הנפט. עיתויה היה מיד לאחר שגורמים אמריקאיים רשמיים הצהירו כי תקפו את איראן במערכה סמויה ביוני 2019.

בניית חוסן: עקיפת הלחץ הכלכלי והובלת מהפכה בסייבר

בנוסף להקמתם של גופי סייבר חדשים והנהגת פיקוח על מרחב הסייבר, נראה כי ממשלת איראן משקיעה גם בחינוך הדור הבא,[43] וזאת כחלק מאסטרטגיה התקפית שמטרתה לבנות יכולות סייבר בזירה הפנימית. איראן השקיעה באופן מסיבי בתחום הסייבר באמצעות הקמת ארגונים רשמיים ותשתיות חדשות, וחלק ניכר מההשקעה מוקדש לחינוך. נראה כי גם הממשלה וגם גורמים לא מדינתיים מכירים בחשיבות לימודי הסייבר. כך, למשל, כמה אוניברסיטאות איראניות מציעות קורסים ללימוד פצחנות (האקינג).[44] לימוד רחב היקף של טכנולוגיות סייבר צפוי לסייע לפיתוח הענף, ואולי גם לשפר את מחויבות האזרחים למדינה בתחום זה.[45] מכיוון שקשה לבצע ייחוס נכון במרחב הסייבר, קבוצות לא רשמיות הקשורות למדינה יכולות לפעול לקידום האינטרסים המדינתיים. מקבלי ההחלטות באיראן הבינו את החשיבות שיש להשקעת סכומי כסף גדולים בלימוד התחום, מתוך ציפייה שבעקבות זאת יפתחו אנשים מחויבות לתמוך במדינה. אמנם,

41 Ibid.

42 Bruce Riedel, "Who are the Houthis, and Why Are we at War with them?", *Brookings*, December 18, 2017, https://www.brookings.edu/blog/markaz/2017/12/18/who-are-the-houthis-and-why-are-we-at-war-with-them/.

43 Veronika Netolická and Miroslav Mareš, "Arms Race 'in Cyberspace' – A Case Study of Iran and Israel", *Comparative Strategy* 37, no. 5 (2017): 414-429.

44 "Threat Intelligence Briefing Episode 11", *HP Security Research,* February 2014.

45 Netolická and Mareš, "Arms Race 'in Cyberspace'".

ההשקעה בחינוך לא תתורגם ישירות לתוספת של עובדי ציבור חדשים, אך היא תוכל להוביל להקמת קבוצות בעלות מוטיבציה עצמאית. בנוסף, הממשלה מראה עניין בתמיכה בחברות סטארט־אפ וחדשנות באיראן. בספטמבר 2019 החליטה ממשלת איראן להשקיע 225 מיליון דולר ב"קרן החדשנות האיראנית" מתוך כוונה לתמוך בחדשנות ולעודד חברות סטארט־אפ.[46]

ההשקעה בפיתוח יכולות סייבר כאמצעי להפוך למובילה בתחום זה מצביעה גם על כך שאיראן עוסקת בריגול סייבר במטרה לגנוב טכנולוגיה מיריבים ולהשיג מידע על יכולותיהם. התוכנה הזדונית "Madi" שהופעלה בשנת 2012, הפעילויות של "Rocket Kitten" בשנת 2014 והניסיונות של Ajily Software Procurement Group לייבא לאיראן תוכנות אמריקאיות גנובות באופן לא חוקי, הם כולם דוגמאות רלוונטיות לפעילות הריגול בסייבר של איראן. הפעילות האיראנית להשגת עוצמה טכנולוגית מלווה בדרך כלל בפעילות משבשת שנועדה לתקוף תשתיות קריטיות זרות, במיוחד בתחום האנרגיה והביטחון, כפי שמוכיח מזה שנים רבות האיום APT33 (המכונה גם "Elfin").[47]

פיתוח יכולות סייבר עשוי לשמש גם כאמצעי לעקיפת הלחץ הכלכלי על איראן ולגיוון מגזרי המשק, כחלק מאסטרטגיה הגנתית. בנייה ושיפור של יכולות הסייבר פירושם גם פיתוח של כלים טכנולוגיים חדשים. מטבעות וירטואליים, שהם דיגיטליים לחלוטין, עשויים לגלם את הכלים הכלכליים של מרחב הסייבר. נכון לעכשיו, המסחר במטבעות וירטואליים עדיין אסור ברפובליקה האסלאמית של איראן, אך לאחרונה הותרה שם כריית מטבעות וירטואליים כפעילות תעשייתית חוקית.[48] למשרד התעשייה, המסחר והכרייה של איראן יש את הסמכות המלאה לתת אישורים לכרייה מקומית, וכללים להסדרת פעילות זו אכן נוסחו בחוק. החוק החדש התקבל באיראן בתקופה שבה האיראנים כבר הפעילו כריית מטבעות וירטואליים, כדרך לעקוף את הסנקציות הכלכליות. החוק אמנם מגביל את האזורים הגיאוגרפיים שבהם מותר לכרות ומחייב אנשים לשלם עבור החשמל הנצרך, אך סגן שר האנרגיה האיראני, הומאיון חארי, כבר הצהיר כי הממשלה תאשר מהלך להחלת תעריפי חשמל נמוכים יותר על חוות כרייה, מה שצפוי לעודד את פעילות

46 "Iran Gov't Invests $225m in Innovation Fund", *Financial Tribune*, September 6, 2019, https://financialtribune.com/articles/sci-tech/99750/iran-gov-t-invests-225m-in-innovation-fund.

47 "Elfin: Relentless Espionage Group Targets Multiple Organizations in Saudi Arabia and U.S.", *Symantec*, March 27, 2019, https://www.symantec.com/blogs/threat-intelligence/elfin-apt33-espionage.

48 Marie Huillet, "Iranian Gov't Authorizes Cryptocurrency Mining as Industrial Activity", *CoinTelegraph*, July 29, 2019, https://cointelegraph.com/news/iranian-govt-authorizes-cryptocurrency-mining-as-industrial-activity.

הכרייה באיראן. יחד עם זאת, הצהרתו של השר האיראני נשמעת חשודה, מכיוון שהבנק המרכזי של איראן המליץ לאסור על תשלום במטבעות וירטואליים בתוך המדינה. זאת, בשעה שגורמי החברה האזרחית וחברות פרטיות מנסים לקדם שימוש במטבעות וירטואליים ברמה המקומית.

יתר על כן, בדצמבר 2019 הציע הנשיא רוחאני ליצור מטבע וירטואלי מוסלמי כדרך להילחם בהגמוניה הכלכלית האמריקאית. הייתה זו הפעם הראשונה שהמשטר האיראני הודיע באופן פומבי על כוונתו לייצר מטבע וירטואלי במטרה להימנע משימוש בדולר האמריקאי, וזאת כחלק מאסטרטגיה פיננסית הגנתית.[49]

בעוד שאיראן מפתחת כלי זה כחלק מהניסיון להתמודד עם הסנקציות הכלכליות הבין־לאומיות, ארצות הברית כבר נקטה פעולה נגד שני איראנים שלכאורה השתתפו בהעברת תשלומים לתוכנת הזדונית "SamSam". המשרד לבקרת נכסים זרים של משרד החוץ האמריקאי הכניס את השניים לרשימת הסנקציות שלו בגין פעילות בתחום הביטקוין. פירוש הדבר הוא שהם נכללים ברשימה השחורה ואינם יכולים לשלוח או לקבל כסף מיחידים או מנותני שירותים.[50]

שמירה על יציבות המשטר והפצת ערכיו

לאחר אירועי "התנועה הירוקה" של שנת 2009 הבינה איראן את הסכנה הטמונה בטכנולוגיות החדשות מבחינת יכולת ההתארגנות להבעת התנגדות ולהתקוממות פוטנציאלית. כחלק מתגובת המדינה לתופעה זאת, פיתחה איראן אסטרטגיה הגנתית והתקפית במרחב הסייבר, שיושמה הן בזירת הבית והן בחוץ. במסגרת הפעולות ההגנתיות בתוך המדינה ניסה המשטר לפקח על הפעילות במרחב הסייבר ולשלוט בתכנים המשותפים. על פי סקר שפורסם בשנת 2012, 27 אחוזים מאתרי האינטרנט היו אז חסומים באיראן,[51] מכיוון שנחשבו כנוגדים את הערכים המוסלמיים. יתר על כן, איסור כלל־ארצי מוּחָל למעשה על רוב הרשתות החברתיות, כולל "פייסבוק" ו"טוויטר".[52]

---

49 Helen Partz, "Iran Wants to Create Crypto to Confront 'Economic Hegemony' of US", *CoinTelegraph*, December 19, 2019, https://cointelegraph.com/news/iran-wants-to-create-crypto-to-confront-economic-hegemony-of-us.

50 "US Regulators Tie Two Bitcoin Addresses to Iranian Ransomware Plot", *CoinDesk*, November 28, 2018, https://www.coindesk.com/us-regulators-tie-two-bitcoin-addresses-to-iranian-ransomware-plot.

51 "Current State of Internet Censorship in Iran", *View DNS.info*, March 23, 2012, https://viewdns.info/research/current-state-of-internet-censorship-in-iran/.

52 Leyla Khodabakhshi, "Why Ordinary Iranians Are Turning to Internet Backdoors to Beat Censorship", *BBC News*, January 10, 2018, https://www.bbc.com/news/blogs-trending-42612546.

על פי ראיון עם התובע אחמד עלי מונתזרי, שמכהן כראש ועדת הצנזורה באינטרנט, איראן סגרה ב־2016 14,000 אתרי אינטרנט וחשבונות ברשתות מדי שבוע.[53] מונתזרי הסביר כי תוכן האתרים הללו, שהתנגדו לערכים איראניים ולדת, הצדיק את סגירתם, והוסיף כי המדינה נתונה למתקפה של תקשורת זרה ועוינת. טקטיקת ההתקרבנות הזו משמשת באיראן מפעם לפעם לצורך הטלת צנזורה והפצת תעמולה. בשנים 2017, 2018 ו־2019, במהלך ההפגנות העממיות באיראן, חסם המשטר כמה אתרים ופלטפורמות תקשורת, ובמקומות מסוימים הרשויות אפילו ניתקו את הגישה לאינטרנט.[54] כך, לדוגמה, הממשלה חסמה את "טלגרם", שהיא אחת מאפליקציות התקשורת הפופולריות ביותר באיראן. גורמים איראניים רשמיים, שככל הנראה הפיקו לקחים מאירועים קודמים, היו מעוניינים למנוע מהחברה האזרחית את הדרך לתקשר, ליידע ולהתארגן באמצעות פלטפורמה זו.

חלק מהמאמץ האיראני לפתח יכולות סייבר נובע מהרצון לשמור על התרבות האיראנית – מניע שהוא דפוס חוזר באסטרטגיה של איראן. הגורם התרבותי בא לידי ביטוי גם בפעילות הסייבר של איראן, ורבות מהמתקפות שהובילו גורמים איראניים נקשרו בצורה כזו או אחרת להצדקות דתיות או תרבותיות. אחת הסיבות לכך שאיראן מעוניינת להיות מובילה אזורית ובין־לאומית מבחינת חדשנות טכנולוגית היא הגאווה הלאומית.[55]

ראש ארגון ההגנה האזרחית של איראן, ג'לאלי, הדגיש בנובמבר 2019 את התפקיד הבולט שיש לאיראן בתחום הסייבר והוסיף כי המשטר פיתח יכולת הגנה בסייבר לפני כל מדינה אחרת, כולל ארצות הברית. לדבריו, מדינות רבות, כמו רוסיה וצפון קוריאה, מעוניינות לקבל הדרכה מכוחות הסייבר של איראן.[56] תחושת הגאווה הלאומית, הנקשרת לתפקיד של ההובלה הטכנולוגית, חיונית להבנת האסטרטגיה של איראן במרחב הסייבר. ואכן, מאז שנת 2010 הצליחה איראן להרחיב את הגישה לאינטרנט לאזורים כפריים ולשפר את הקישוריות

53 "Iran Bans 14 Thousand Websites and Accounts Weekly", *Al Arabiya*, December 8, 2016, https://english.alarabiya.net/en/media/digital/2016/12/08/Iran-bans-14-thousand-websites-and-accounts-weekly-.html.

54 "In Response to Protests, Iran Cuts Off Internet Access, Blocks Apps", *NPR*, January 3, 2018, https://www.npr.org/2018/01/03/575252552/in-response-to-protests-iran-cuts-off-internet-access-blocks-apps.

55 Gawdat Bahgat and Anoushiravan Ehteshami, "Iran's Defense Strategy: The Navy, Ballistic Missiles and Cyberspace", *Middle East Policy Council* 24, no. 3 (2017): 89-103.

56 "Iran Opts for New Civil Defense Approach to Confront US Threats", *Fars News Agency*, November 5, 2019, https://en.farsnews.com/newstext.aspx?nn=13980814000432.

בערים,[57] והפכה בכך לאחת המדינות המזרח תיכוניות עם המספר הגדול ביותר של משתמשים באינטרנט.

המשטר האיראני מחויב להפצת ערכיו גם מחוץ למדינה, וזאת כחלק מפעילות התקפית נגד "האויב". ב־2018 זיהתה חברת אבטחת הסייבר FireEye קמפיין לקידום נרטיבים פוליטיים איראניים.[58] המבצע כלל שימוש באתרי חדשות לא לגיטימיים וניצול זדוני של רשתות חברתיות. לפי הניתוח של חברת אבטחת הסייבר, היה זה שכפול של הניסיון הרוסי להשפיע על דעת הקהל הזרה בבחירות 2016 לנשיאות ארצות הברית. בספטמבר 2019 הודיע גולאם רזה סולימאני, מפקד ארגון הבסיג', על הקמת אלף גדודי סייבר ברחבי המדינה, באמצעות חשבונות של משתמשים תומכי משטר ברשתות החברתיות.[59] כל גדוד כזה מורכב מכ־500 חיילים. פירוש הדבר הוא שהמשטר שיגר כנראה לרשתות למעלה מחצי מיליון חשבונות התומכים במשטר. סולימאני לא אמר דבר ביחס לאמצעים ולתקציב ששימשו את ארגון הבסיג' כדי לממש פרויקט זה, אך הוסיף והצהיר כי "האויב הביע במספר הזדמנויות דאגה מנוכחותו המאורגנת של הנוער המהפכני במרחב הסייבר, מה שמשקף את המומנטום שנוצר. הנוכחות הזו רק תתרחב ותשתפר". עם זאת, חרף היוזמה החדשה להפצת דעות תומכות משטר באינטרנט, איראן צפויה להתמודד גם עם קשיים, לאחר ש"טוויטר" הסירה לאחרונה אלפי חשבונות שפעלו בגיבוי המדינה (כולל חשבונות שהוערכו כמקושרים לממשלת איראן).

מעֵבר לנחישות של איראן להגן על מערכת הערכים שלה, המשטר גם מנסה להילחם ברעיונות זרים וגם להפיץ את התעמולה שלו באמצעות מתקפות סייבר. לדוגמה, במסגרת מבצע "אבאביל" תבעו האקרים להסיר את "תמימות המוסלמים" – סרט שהופץ בשנת 2012 ונחשב כפוגע בכבוד המוסלמים.[60] מתקפת הסייבר לוּותה בהצדקה תרבותית, שהתבססה על העלבון שנגרם לתדמיתה של איראן. דוגמה נוספת להפצת תעמולה באמצעות הסייבר הייתה מתקפת התוכנה הזדונית "Shamoon" בשנת 2016, שבמהלכה הופצו במכשירים שנפגעו תמונות אנטי מערביות, כמו תמונה של שריפת דגלה של ארצות הברית. בהמשך צצה גרסה

57 Anoushiravan Ehteshami, "Iran: Stuck in Transition", *Journal of International and Global Studies* 9, no. 2 (2017): 186-188.

58 Ed Parsons and George Michael, "Understanding the Cyber Threat from Iran", *MWR Info Security*, April 17, 2019, https://www.f-secure.com/en/consulting/our-thinking/understanding-the-cyber-threat-from-iran.

59 "Nouveaux cyber-brigades en Iran", *PressTV*, September 7, 2019.

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

נוספת של "Shamoon", שהפיצה את התוכנה הזדונית למכשירים באמצעות פסוק של הקוראן.[61]

ניצול המאפיינים של הסייבר

מרחב הסייבר הוא תחום שבו יש לאיראן ולמדינות לא ליברליות הפריווילגיה לשחק שלא לפי הכללים של מדינות דמוקרטיות כמו ארצות הברית וישראל. ואכן, נראה שאיראן מנצלת את העובדה שאינה כפופה לאותם כללים כדי ליישם את האסטרטגיה ההתקפית שלה נגד אויבים מבית ומחוץ. מכיוון שמדובר במערכת ערכים שונה, איראן רואה חלק מהמעשים כמקובלים ואחרים כאסורים מבחינה אתית ומוסרית. לעומת זאת, המדינות המערביות, הדמוקרטיות והמפותחות פועלות בהתאם למערכת המשפטית שלהן, וגם נוטות לאמץ ולכבד את המשפט הבין־לאומי כחלק מהחשיבות הרבה שהן מייחסות לדעת הקהל.

בהיותה משטר לא ליברלי, איראן מרשה לעצמה להסדיר ולצנזר את מרחב הסייבר באופן מגביל ביותר, ושוללת מאזרחיה כלים בסיסיים להתחבר לעולם. גם המידע הנוגע לפעולות שהיא מבצעת בתחום הסייבר ברמה הלאומית מוסתר מהציבור. בעוד שמדינות דמוקרטיות נוטות להימנע מעמימות מתוך מחויבות לעקרונות משפטיים, במשטרים סמכותניים כמו איראן העמימות היא אמצעי נפוץ. איראן רחוקה מלהיות שקופה בכל הנוגע לפעילותה בנושא אבטחת סייבר ומידע, בעוד שמדינות דמוקרטיות מחויבות לשקיפות ברמה גבוהה ונושאות באחריות לכל החלטה שיקבלו. בכירי הממשל האיראני דוחים את תפיסת האחריותיות ונהנים מחופש פעולה רחב, מבלי לחשוש יתר על המידה מפני חוסר הסכמה מצד האוכלוסייה. מקרה מייצג היטב הוא הניסיון של איראן, שנחשף על ידי חברת "מיקרוסופט" בספטמבר 2019, לחדור לרשתות אמריקאיות ואירופיות באמצעות מבצע שהוביל הארגון "Phosphorous". בדומה לפעילות הרוסית בשנת 2016, איראן ניסתה, ככל הנראה, להשפיע על בחירות במדינות אחרות ולתקוף מועמדים פוטנציאליים לבחירות לנשיאות ארצות הברית בשנת 2020.

העמימות ויכולת ההכחשה של מתקפות הסייבר מאפשרות לתוקפים להשתמש בלוחמת סייבר בצורה סמויה. הדבר הופך את מרחב הסייבר לזירה מועדפת להתעמתות עם אויבים מבלי לחשוש מתגמול ישיר. סוגיה אחרת בהקשר זה היא הפעילות של קבוצות האקרים שהזיקה שלהן למשטר האיראני הינה מעורפלת. תופעה נוספת ההולכת ומתפתחת בפעילות הסייבר של איראן ומאפשרת לה את יכולת ההכחשה היא שיתוף פעולה עם קבוצות זרות. השימוש שעשו "OilRig"

61 Charlie Osborne, "Shamoon Data-Wiping Malware Believed to Be the Work of Iranian Hackers", *ZDnet*, December 20, 2018, https://www.zdnet.com/article/shamoons-data-wiping-malware-believed-to-be-the-work-of-iranian-hackers/.

בכלי סייבר רוסיים כדי לתקוף יעד אמריקאי בשנת 2017 הוא דוגמה לתיאום בין האקרים רוסיים להאקרים איראניים. היבט נוסף של יכולת ההכחשה בסייבר הוא החשיבות שיש לשליחים (proxies), קרי שחקנים מדינתיים או לא מדינתיים הנתמכים על ידי איראן ומבַצעים פעולות עצמאיות שעולות בקנה אחד עם האינטרסים האיראניים. שליחים כאלה של איראן פזורים בכל רחבי האזור, גם בקרב השיעים וגם בקרב הסונים (החותים בתימן, חמאס ברצועת עזה, חיזבאללה בלבנון וכן הלאה). העמימות שיוצרת פעולה הנעשית באמצעות שליחים מאפשרת לאיראן להכחיש בקלות את מעורבותה במבצעי סייבר. דוגמה לכך היא ההכחשה של איראן את ההאשמה נגדה כאילו היא זו שתקפה את מתקני הנפט הסעודיים בספטמבר 2019, וטענתה שמי שאחראים למבצע זה הם החותים

הדפוס האחרון שזוהה באסטרטגיית הסייבר הלאומית של איראן הוא היכולת שלה להכחיש את היותה יעד למתקפות. הצהרות פומביות של גורמים רשמיים באיראן, הטוענים כי הרפובליקה האסלאמית חסינה בפני מתקפות סייבר, הן דבר שכיח. דוגמה אחרונה להצהרות כאלו ניתן לראות בראיון עם ג'לאלי שפורסם בנובמבר 2019, בו אמר כי ניסיונות זרים לתקוף את איראן במרחב הסייבר לא צלחו בשנתיים האחרונות בזכות יעילותם של מנגנוני הביטחון האיראניים בתחום הסייבר.[62] דבריו באו במקביל להצהרות של גורמים רשמיים בארצות הברית על הצלחתו של מבצע סייבר סמוי באיראן, אשר השפיע על יכולתו של המשטר לתקוף מכליות נפט במפרץ הפרסי ביוני 2019.[63] שר התקשורת וטכנולוגיית המידע של איראן, מוחמד ג'וואד אזָרי ג'הרומי, אף הגדיל לעשות והצהיר שארצות הברית "ודאי חלמה" את המבצע.[64]

סיכום ומסקנות

איראן מציבה כיום איום סייבר משמעותי על המערכת הבין־לאומית. פעולותיה והאסטרטגיה שמאחוריהן הביאו גורמים מערביים רשמיים, יחד עם מומחים מהמגזר הפרטי, להאמין שאיראן מבקשת להציב את עצמה בשורה אחת עם מעצמות סייבר כמו רוסיה וסין. מומחים גורסים כי אם יכולותיה של איראן ימשיכו להתפתח, יש לצפות בסבירות רבה למתקפת סייבר איראנית שתפגע בתשתיות פיזיות.

ניתן לתאר את אסטרטגיית הסייבר ההתקפית של איראן כאסטרטגיה של "מידה כנגד מידה", הנשענת על הצדקה תרבותית, גאווה לאומית ויתרונות ייחודיים במרחב הסייבר. איראן צמחה להיות אחת משחקניות הסייבר המובילות בעולם.

62 "Iran Opts for New Civil Defense Approach to Confront US Threats".

63 Julian E. Barnes, "U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say", *The New York Times*, August 28, 2019, https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html.

64 Ibid.

המוניטין שהיא רכשה משרת את האסטרטגיה שלה ואת מאמציה להפעיל לוחמה אסימטרית נגד אויביה מבחוץ. המשטר האיראני משקיע משאבים רבים בפיתוח יכולות סייבר במגוון תחומים כדי לחזק את ההגנה שלו. תחום הסייבר גם נהנה מהשקעות אזרחיות, ומוסדות איראניים, כמו אוניברסיטת שריף, זוכים להערכה רבה.

האסטרטגיה ההגנתית של איראן מובלת על ידי הצורך לבנות חוסן כלכלי וטכנולוגי, וכן על ידי נחישותה לנטרל איומים פנימיים וחיצוניים. המשטר מכיר בחשיבות בנייתן של יכולות הגנה, לצד יכולות התקפה. בנוסף לכך, הוא משקיע מאמצים רבים ברכישת יכולות מעקב וניטור אחרי פעילות באינטרנט כדי להגן על עצמו, ומסתייע לשם כך בתוקפים מומחים מקרב השותפות הטבעיות שלו – סין, רוסיה וצפון קוריאה.

מניתוח מתקפות הסייבר האחרונות שיוחסו לאיראן עולה כי המשטר האיראני שם על הכוונת טווח רחב של אויבים, וביניהם מתנגדי משטר בתוך המדינה ומחוצה לה, שכנות קרובות כמו ישראל וערב הסעודית, ומדינות רחוקות כמו ארצות הברית ומדינות אירופה. איראן שיפרה את יכולות הסייבר שלה, גם אם לא ניתן עדיין להשוות אותן לאלו של ארצות הברית או ישראל. התקפות הסייבר של איראן הפכו ממוקדות יותר בשנתיים האחרונות. הן עושות שימוש במגוון רחב של כלים ושיטות, שתוכננו ובוצעו ברמה גבוהה של מקצועיות וסבלנות, ומאפשרים לה לגשר על הפערים הטכנולוגיים ולהגביר את היעילות. השאלה אם איראן הרוויחה או הפסידה ממאמציה ההתקפיים נגד יריביה החיצוניים מותנית במידת הקונצנזוס הפנימי, כאשר אינדיקטורים לו הם התשתית הלאומית וההגנתית והרטוריקה הציבורית.