חלק 2

אסטרטגיית הסייבר של איראן, המוסדות והיכולות

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

שיתוף פעולה בינלאומי

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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