התפתחויות בלוחמת הסייבר של איראן 2013–2014

גבי סיבוני וסמי קרוננפלד

במהלך 2013 הפכה איראן לאחד השחקנים המרכזיים בזירת לוחמת הסייבר הבין־לאומית. ההתפתחות הזו הנה תוצאה של הבשלת תהליכי בניין כוח הן בהקשרי הגנה והן באלה ההתקפיים מחד ושחרור הרסן לביצוע מתקפות בעולם מצד מקבלי ההחלטות באיראן מאידך. הפעילות האיראנית מראה קפיצת מדרגה בכל הקשור ביכולות הטכנולוגיות והמבצעיות שלה. המאמר בוחן את ההתקדמות והפעילות של מערך הגנת הסייבר האיראני ואת השימוש ביכולות אלו גם לריסון המתנגדים מבית ובוחן גם את היכולות ההתקפיות בעיקר דרך בחינת מתקפות סייבר המיוחסות לגורמים איראניים ולשליחים ובעלי ברית של איראן.

מילות מפתח: סייבר, איראן, בטחון סייבר, הגנת סייבר, בידול רשתות.

מבוא

גורם בכיר בחברת אבטחת הסייבר CrowdStrike דֵרג בתחילת 2013, בראיון למכון המחקר האמריקאי Atlantic Council את איראן ב"מעגל השלישי" (Third Tier) בכל הקשור ליכולותיה לפעול במרחב הסייבר, והעריך כי יכולות לוחמת הסייבר שלה נחותות משמעותית מיכולותיהן של מדינות "המעגל הראשון", כגון ארצות הברית, רוסיה ובריטניה, ושל מדינות "המעגל השני", דוגמת סין. תפיסה זו משקפת גם את הערכותיהם של מומחי מודיעין ואנשי ממשל מערביים רבים.

איראן נתפסת כמי שביכולתה להטריד את מערכי האבטחה המערביים ולפגוע במטרות "רכות", אך חסרה את הידע והאמצעים להוציא אל הפועל מתקפות סייבר

ד"ר גבי סיבוני הינו ראש התכניות ביטחון סייבר וצבא ואסטרטגיה במכון למחקרי ביטחון לאומי

סמי קרוננפלד הוא בוגר תואר מוסמך בחוג ליחסים בינלאומיים באוניברסיטה העברית בירושלים ולשעבר מתמחה בתכנית ביטחון סייבר במכון למחקרי ביטחון לאומי

אסטרטגיות.[1] עם זאת, במהלך 2013 הפכה איראן לאחד השחקנים המרכזיים בזירת לוחמת הסייבר הבין־לאומית. נראה כי התפתחות זו היא תוצאה של שילוב בין שחרור מדוד של הרסן מצד מקבלי ההחלטות האיראניים בכל הקשור לפעילות התקפית במרחב הסייבר, ובין קפיצת מדרגה איכותית של מערך לוחמת הסייבר האיראני, אשר הפתיע מומחים מערביים רבים בהיקפי פעילותו, בתחכומו המקצועי ובבחירה השאפתנית של מטרותיו.

אירועים דוגמת מתקפת ה־Stuxnet שפגעה קשות במערך הצנטריפוגות של איראן, והמחאה הנרחבת שליוותה את הבחירות שם בשנת 2009 – מחאה שלרשתות החברתיות ולמרחב האינטרנט היה חלק גדול בארגונה ובהסלמתה – מיצבו את זירת הסייבר כזירה מרכזית בחשיבותה בעיני המשטר האיראני. הניסיון של איראן באירועים אלה ובמתקפות סייבר אחרות שספגה הובילו אותה להקים מערך סייבר נרחב, הכולל מסגרות מבצעיות בעלות מִדרג פיקודי ומקצועי, המתמחות במגוון תחומים. איראן השקיעה יותר ממיליארד דולר בפיתוחים טכנולוגיים, בהקמת תשתיות ובאימון כוח אדם הגנתי והתקפי.[2] אסטרטגיית הסייבר האיראנית נקבעת ומפוקחת על ידי הדרגים הגבוהים ביותר, ביניהם הנשיא, מפקד משמרות המהפכה ושרים בכירים, המכהנים ב"מועצה העליונה למרחב הסייבר" – הגוף הבכיר המתכלל את פעילות הסייבר של המדינה.[3]

מאמר זה מבקש להציג תמונה עדכנית של הפעילות האיראנית במרחב הסייבר. המאמר מחולק לשני חלקים: החלק הראשון בוחן את ההתקדמות והפעילות של מערך הגנת הסייבר האיראני ואת השימוש ביכולות אלו גם לריסון המתנגדים מבית; החלק השני בוחן את הממד ההתקפי, בעיקר דרך בחינת מתקפות סייבר המיוחסות לגורמים איראניים ולשליחים ובעלי ברית של איראן. תובנות מסכמות ניתנות בסוף המאמר.

תפיסת ההגנה

תפיסת ההגנה האיראנית במרחב הסייבר משולבת עם הפעילות האיראנית לנטרול איומי פנים מצד מתנגדי המשטר. לאור זאת, איראן שואפת לייצר הגנה רב־שכבתית, המשלבת בין טכנולוגיות אבטחה, ניטור ופיקוח ובין מנגנוני אכיפה פיזית הרודפים באופן אגרסיבי אחר פעילי רשת הפועלים נגד המשטר במרחב הסייבר. איראן פועלת לשם כך בשלושה צירים מרכזיים: ראשית, יצירת מעטפת הגנה נגד תקיפות סייבר על תשתיות חיוניות ומידע רגיש, כמו מתקפת Stuxnet שפגעה בתוכנית העשרת האורניום האיראנית; שנית, נטרול פעילות הסייבר של גורמי אופוזיציה ומתנגדי משטר, עבורם מהווה מרחב הסייבר פלטפורמה מרכזית לתקשורת, הפצת מידע וארגון פעולות נגד המשטר; שלישית, הרחקה של תכנים

ורעיונות מערביים ופוגעניים ממרחב הסייבר הפנים־מדינתי – רעיונות העשויים לתרום להתפתחותה של "מהפכה רכה" שתפגע ביציבות המשטר.

היעדים והעקרונות האופרטיביים של מערך הגנת הסייבר האיראני מוכתבים על ידי "המועצה העליונה למרחב הסייבר" ומוצאים אל הפועל על ידי גופי ממשל מרכזיים, כמו "ארגון ההגנה הפסיבית" (The Passive Defensive Organization) המשתייך לצבא, "המועצה לתרבות מהפכנית" הכפופה למנהיג העליון, וכן המשטרה האיראנית ומשרד התקשורת.[4] חלק מהתשתיות הטכנולוגיות והארגוניות אותן הקימה איראן הבשילו במהלך השנה האחרונה לכדי גופים מבצעיים המחזקים משמעותית את פעילות ההגנה האיראנית במרחב הסייבר.

פרויקט בידול הרשתות – מתנתקים מהעולם

תוכנית בידול הרשתות הינה אחת מאסטרטגיות ההגנה המרכזיות של המשטר האיראני במרחב הסייבר. הפרויקט החל לקרום עור וגידים כבר ב־2009, כאשר היעד של איראן הוא העברת כלל פעילות הסייבר במדינה לרשת תקשורת פנים־מדינתית המנותקת מה־World Wide Web ומכונה "חלאל" (Halal Internet). הרשת האיראנית תוכננה לפעול ברוח הנורמות המוסלמיות־שיעיות אותן מעודד הממשל ולהעניק לו שליטה ופיקוח מלאים על התכנים, המידע והמשתמשים בה. בעיני המשטר, הקמת רשת אינטרא־נט והפרדת מרחב הסייבר האיראני מהמרחב הגלובלי הן צעד מרכזי בחיזוק ההגנה מפני מתקפות סייבר וריגול, בעצירת החדירה של רעיונות מערביים אנטי־משטריים ובנטרול האופוזיציה הפנימית.[5]

עדויות ראשונות להפעלתה של הרשת האיראנית התגלו באוקטובר 2012, כאשר חוקרי סייבר אמריקאיים, בשיתוף עם מקורות פנים איראניים, הצביעו על כך שספקיות האינטרנט האיראניות החלו להקצות שתי כתובות IP לכל מחשב המחובר לרשת האינטרנט – כתובת רשת רגילה לצד כתובת רשת פנים־איראנית אליה ניתן לגשת רק מתוך המדינה. החוקרים העריכו כי הרשת הפנים איראנית מסוגלת לנהל כ־17 מיליון כתובות IP, וכי יותר מ־10,000 מחשבים ביתיים, מסחריים וממשלתיים התחברו אליה במהלך 2012. במהלך 2013 החלה רשת "חלאל" לצבור תכנים (מצונזרים ומפוקחים כמובן), תוך מתן דגש רב לפיתוח גרסאות מקומיות של שירותי רשת פופולריים, כגון דואר אלקטרוני, רשתות חברתיות, תקשורות וידאו ואודיו, אתרי מפות ואתרי וידאו.[6]

ביולי 2013 חנך המשטר האיראני שירות דואר אלקטרוני, post.ir@, אשר כלל האזרחים חויבו להירשם אליו ואשר תוכנן להוות את צינור הקשר המרכזי בין האזרח לבין זרועות הממשל השונות. השירות, שיש לו תמיכה בפרסית, אנגלית, צרפתית וערבית, מסוגל לספק כתובות דואר אלקטרוני לכמאה מיליון משתמשים, כאשר לכל משתמש מוקצית תיבת דואר בת חמישים מגה־בייט, אותה ניתן להרחיב

עד לשני ג'יגה־בייט. פתיחת תיבת הדואר מחייבת את האזרח לתת את שמו וכתובתו, ונראה כי התכתובות המועברות בו אינן מוצפנות – תנאים המאפשרים למשטר לקיים פיקוח הדוק על המשתמשים ועל התכתובות.[7] בדצמבר 2012 השיקה רשות השידור הממלכתית של איראן אתר דמוי "Youtube" תחת השם Mehr, המציג תכנים מפוקחים ומאפשר לגולשים להעלות תכנים משלהם, תחת כללי צנזורה קפדניים.[8] הרשויות האיראניות גם אסרו על שימוש בתוכנות אבטחת מידע זרות ופיתחו מערכת אנטי־וירוס מקומית, המכונה Padvish. על פי מקורות באיראן, מערכת זו יכולה להגן גם על רשתות ולמנוע חדירה של תוכנות זדוניות.[9]

כדי להגדיל את מספר המשתמשים ברשת "חלאל" ובשירותי הרשת האיראניים, ליווה המשטר את הפעלתה בהרחבת השימוש באמצעים טכנולוגיים ובחקיקה, המגבילים את אפשרויות האזרח האיראני להתחבר לרשת האינטרנט הגלובלית: הרשויות האיראניות חסמו את השימוש בתוכנות voice over IP, כמו Skype ו־Google Talk. כמו כן, נחסמו לשימוש רבות מרשתות ה־VPN, TOR ותוכנות עוקפות סינון, המהוות כלים מרכזיים בעקיפת הפיקוח והצנזורה הממשלתיים על מרחב הסייבר.[10] בנוסף לכך, רשויות הסייבר האיראניות החלו להאט באופן מכוון אתרי אינטרנט ושירותי רשת חיצוניים (בעיקר שירותים של חברת Google, שהם פופולריים מאד באיראן), לעיתים עד כדי שישה אחוזים מהמהירות הרגילה. כמו כן, הרשויות מבצעות חסימות אקראיות של אתרים ושרותים (Migrating blocks) ומגבילות מאד את תעבורת הרשת המוצפנת. פעולות אלו מערימות קשיים טכניים, חוקיים ופסיכולוגיים על האזרח האיראני המבקש לגלוש ברשת האינטרנט הגלובלית, ולמעשה דוחפות אותו להשתמש ברשת "חלאל" המפוקחת והמצונזרת.[11]

פיתוח טכנולוגיות הגנה ופיקוח

כהשלמה למאמצי בידול הרשתות, איראן משקיעה רבות גם בפיתוח טכנולוגיות ואמצעי הגנת סייבר מתוצרת מקומית, וזאת כדי להקטין את תלותה במוצרים זרים העשויים להיות "סוסים טרויאניים". בדצמבר 2013, בטקס מתוקשר בו נכחו בכירים בממסד הביטחוני האיראני, ביניהם שר ההגנה הגנרל Hossein Dehqan ומפקד מערך ההגנה האזרחית בריגדיר־גנרל Gholam Reza Jalali, נחשפו 12 פיתוחים טכנולוגיים פרי התעשייה האיראנית, ביניהם טלפון סלולרי מאובטח האמור לספק למשתמשים קו תקשורת חסין לציטוטים. בנוסף הוצגו בכנס מערכת הפעלה מאובטחת למחשבים שאמורה לבטל את התלות האיראנית במערכות ההפעלה האמריקאיות; מכשיר GPS; מערכת תקשורת אופטית; תוכנות ומערכות נגד תוכניות זדוניות ו־Firewall; מערכת לזיהוי מתקפות סייבר; ומכשור למרכזי אבטחת מידע.[12] בנוסף לכך, סוכנות הידיעות האיראנית ISNA דיווחה כי איראן

הכניסה לשימוש מערכת הגנת סייבר כלל־ארצית העונה לשם Shahpad. על פי ראש הפרויקט, Mohammad Naderi, המערכת מאפשרת היתוך מידע ממגוון תחנות קצה וחיישנים ומייצרת תמונת מצב קיברנטית מדינתית כוללת. בעת התקפה Shahpad מיידעת באופן מידי את מרכזי אבטחת המידע במדינה, ומאפשרת להם להגיב במהירות ולפעול לבלימת המתקפה.[13]

איראן אינה מסתמכת אך ורק על פיתוח מקומי לחיזוק יכולת אבטחת הסייבר שלה. בספטמבר 2012 היא חתמה על הסכם לשיתוף פעולה טכנולוגי נרחב עם קוריאה הצפונית, הכולל גם שיתוף פעולה בתחום טכנולוגיות המידע. על פי מומחים, קיימת סבירות גבוהה כי שתי המדינות, אשר ספגו בעבר מתקפות סייבר ורואות בזירה זו מוקד אסטרטגי חשוב, ישלבו כוחות במסגרת הסכם זה לפיתוח טכנולוגיות אבטחת מידע, ניטור ואף התקפה.[14]

איראן גם משתפת פעולה עם סין בתחום הסייבר, ובעבר רכשה מחברת ZTE Corp. הסינית מערכת מעקב המאפשרת ניטור של שמע, הודעות טקסט וגלישת אינטרנט.[15] שיתופי הפעולה עם מדינות אלו ומדינות נוספות, דוגמת רוסיה, מסייעים רבות לחיזוק מערך הגנת הסייבר האיראני וליכולתה של איראן לעקוב אחר האינטרנט ואחר אזרחיה.

חיזוק מערכי ההגנה

מעֵבר להיבטים הטכנולוגיים, שמה איראן דגש מיוחד על חיזוק היכולת של גופי המדינה השונים להתמודד עם מתקפות סייבר ולבלום אותן. מערך הסייבר האיראני ביצע מספר תרגילי הגנת סייבר מקיפים, במהלכם אומנו יחידות אזרחיות וצבאיות. בנוסף, נערך תרגיל לוחמת סייבר כחלק מתרגיל ימי של משמרות המהפכה במצרֵי הורמוז במהלך דצמבר 2012. במסגרת התרגיל שוגרה מתקפת סייבר נגד רשת המחשבים של הצי, במטרה לשלוף מידע ולהחדיר תוכנות זדוניות. מפקדי התרגיל הכריזו כי המתקפה התגלתה ונחסמה על ידי מערכי הגנת הסייבר של הצי.[16]

בפברואר 2013 דיווחה סוכנות הידיעות האיראנית Fars, המקורבת למשטר, על תרגיל מקיף של כוחות היבשה של משמרות המהפכה, במהלכו תורגלו ונבחנו מערכות הגנת הסייבר של הארגון.[17] תרגיל נוסף נערך באוקטובר 2013, כחלק מתרגיל הגנה כולל של "ארגון ההגנה הפסיבית". במסגרת תרגיל זה אומנו ונבדקו מערכי הגנת הסייבר של גופי ממשל מרכזיים, ביניהם מתקני הגרעין, רשת רכבות המטרו של טהראן, רשות השידור האיראנית, נמלים, הבנק המרכזי וספקי תקשורת סלולריים. על פי מפַקד "ארגון ההגנה הפסיבית", נמצאו ונסגרו פרצות אבטחה רבות במערכי הגנת הסייבר של הארגונים ובעקבות התרגיל הוחלט על הקמת מרכז הגנת סייבר במתקן הגרעיני בנתאנז.[18]

ריסון מתנגדי המשטר

את המהלכים הטכנולוגיים שמבצעת איראן במטרה להגן על מרחב הסייבר שלה היא משלימה בפעילות אכיפה פיזית אגרסיבית נגד מתנגדי המשטר במדינה, העושים במרחב הסייבר שימוש חתרני נרחב. שחקן מרכזי במאמצי המשטר האיראני לשלוט במרחב הסייבר היא משטרת הסייבר, FATA, שהוקמה בתחילת 2011 תחת פיקוד המשטרה האיראנית. במהלך השנה האחרונה הפכה FATA לאגרסיבית יותר במאמציה לאכוף את מגבלות הצנזורה ולמנוע פעילות חתרנית במרחב הסייבר. אנשי היחידה פועלים לאיתור ולכידה של בלוגרים, עיתונאי רשת ופעילי אופוזיציה, המפיצים רעיונות ודעות שאינם עולים בקנה אחד עם עמדות המשטר.

האגרסיביות הרבה המאפיינת את פעילותה של משטרת הסייבר האיראנית נגד מתנגדי המשטר זכתה לתהודה עולמית בנובמבר 2012, בעקבות דיווחים על מותו של הבלוגר האיראני Sattar Beheshti בבית כלא בקרבת טהראן. בהשתי, שנעצר על ידי FATA יום לאחר שפרסם בלוג בו מתח ביקורת חריפה על מערכת המשפט האיראנית (אותה כינה "בית המטבחיים" של ח'מנהאי), מת כתוצאה ממסכת עינויים והכאות קשה מצד אנשי משטרת הסייבר.[19] הפרסום על מותו הביא לגל ביקורות בתוך איראן ומחוץ לה. כתוצאה מכך, הטיל האיחוד האירופי סנקציות על FATA ועל גורמים אחרים שהיו מעורבים במוות, ביניהם שופטים והאחראי על הצנזורה באיראן.[20] הלחץ הבין־לאומי אמנם הוביל לפיטוריו של מפקד משטרת הסייבר בעיר טהראן,[21] אך על פי ארגוני זכויות אדם בין־לאומיים FATA ממשיכה באסטרטגיית המעצרים הנרחבת שלה ופועלת באגרסיביות לאיתור ולענישה של איראנים היוצאים נגד המשטר ברשתות החברתיות ובבלוגים.[22] משטרת הסייבר האיראנית אף הידקה בחודשים האחרונים את הפיקוח על מוסדות הקפה־אינטרנט הפופולריים באיראן וסגרה עשרות מהם עקב אי־עמידה בחוקי הרישום וההגבלה המחמירים של המדינה.[23]

הפיקוח והאכיפה של המשטר הפכו לאינטנסיביים ונרחבים במיוחד בחודשים שהובילו לבחירות לנשיאות ב־14 ביוני 2013. יומיים לפני הבחירות פרסמה "גוגל" כי אנשיה איתרו ובלמו מתקפת "דיוג" (phishing) ששוגרה על ידי גורמים בתוך איראן וכִוונה נגד עשרות אלפי חשבונות דואר אלקטרוני של אזרחים איראניים. המתקפה כללה שליחה של דואר אלקטרוני שהוסווה כדואר תחזוקה של מערכת Gmail וביקש את הגולש להזין את שם המשתמש וסיסמת הדואר האלקטרוני שלו. המידע המוזן הועבר ישירות לתוקפים ואִפשר להם גישה חופשית לתיבות הדואר האלקטרוני של המשתמש.[24] ניתוח המתקפה העלה חשד כי מדובר באותם תוקפים איראניים אשר תקפו את שרתי החברה ההולנדית DigiNotar ב־2011.[25] אמנם, מטרות התקיפה לא הובהרו, אך נראה כי קיים קשר הדוק בינה לבין

מערכת הבחירות וכי התוקפים רצו לאפשר לשלטונות האיראניים לאסוף מידע על פעולותיהם ודעותיהם של אזרחים איראניים ולפעול נגד גורמים "בעיתיים".[26] בנוסף, בשבועות שהובילו לבחירות התקיימה מתקפת סייבר נרחבת נגד אתרי אופוזיציה ותקשורת איראניים. קבוצת האקרים העונה לשם "The Unknown Cyber Jihad" וטוענת כי היא קשורה לארגון חזבאללה, פרצה למספר אתרי אופוזיציה איראניים והחליפה את תוכנם בהודעה נגד מתנגדי המשטר. כמו כן, אתרי אופוזיציה מרכזיים, כגון אתר התנועה הקומוניסטית באיראן, אתר התנועה הירוקה ואתרי זכויות אדם, נחסמו למשך שעות רבות על ידי המשטר, ועשרות פעילי רשת ועיתונאים נעצרו ונכלאו על ידי כוחות הביטחון האיראניים.[27]

הפעילות האיראנית נגד האופוזיציה ומתנגדי המשטר השתכללה והתפתחה מאז האירועים שליוו את בחירתו מחדש של אחמדינג'אד ב־2009. בעוד שבאותה שנה האופוזיציה השתמשה בקלות יחסית במרחב הסייבר לארגון הפגנות, להפצת רעיונות ולהעברת מידע על המתרחש באיראן החוצה (בעיקר על ידי שימוש ברשתות VPN), בבחירות 2013 מערך הסייבר האיראני היה ערוך ומוכן מבחינה טכנולוגית ואופרטיבית כדי לשלוט בשיח שהתקיים במרחב האינטרנט הפנימי ולנטר פעילות חתרנית ויציאת מידע מתוך איראן.

נראה, כי נכון להיום, מערך הגנת הסייבר האיראני נדרש עדיין לעבור כברת דרך כדי שיוכל להתמודד באופן אפקטיבי ועקבי עם מתקפות סייבר ברמת תחכום גבוהה, דוגמת Stuxnet ו־Flame, ולמנוע כל חדירה של תכנים או רעיונות חיצוניים. יש המתארים מערך זה כלא יותר מאשר גרסה מאולתרת ומאורגנת פחות של "חומת" הסייבר הסינית.[28] עם זאת, קפיצת המדרגה הטכנולוגית והארגונית שביצעה איראן בשנה האחרונה מעידה כי יש לה עקומת למידה חדה וכי היא עשויה לגבש מערך הגנה יעיל ומקיף מוקדם מהצפוי.

הממד ההתקפי – חיפוש אחר מתקפות "איכות"

הרפובליקה האסלאמית של איראן רואה בלוחמת הסייבר פלטפורמה יעילה המאפשרת לפגוע ביריבות בעלות עליונות צבאית ברורה, ובד בבד לשמור על מרווח הכחשה שימנע הוקעה בין־לאומית או אף סנקציות ומתקפות נגד. תפיסה זו הביאה את איראן להשתמש בלוחמת הסייבר ככלי מרכזי לתקיפת מטרות מערביות בתגובה לסנקציות וכאמצעי להרתעת הסלמה בפעילותן של מדינות המערב נגד איראן. היקפן, יעדיהן והצלחתן היחסית של מתקפות סייבר שהתרחשו בשנה האחרונה ושויכו לגורמים איראניים מעידים על התעצמות היכולות העומדות לרשותה של איראן. אנשי מודיעין וממשל בישראל ובארצות הברית אף הביעו דאגה מקצב ההתפתחות הגבוהה של יכולות לוחמת הסייבר האיראניות.[29]

גורמים מערביים משייכים את ההתקדמות בתוכנית לוחמת הסייבר של איראן להצלחתה לשלב בין היכולות, הידע וכוח האדם המוכשר הצומח בפקולטות האיראניות למדעי המחשב[30] ובין הניסיון והיכולות הגבוהות של קהילת ההאקרים האיראנית, שרבים מחבריה מזדהים עם המשטר ועם מטרותיו. קהילת ההאקרים האיראנית היא אחת הקהילות הדומיננטיות והפעילות בעולם, ועדויות מצביעות על קשרים בין קבוצות שונות שלה לבין משמרות המהפכה. השימוש בהאקרים, אשר קשריהם לממסד האיראני לוטים בערפל, מעניק לאיראן מרחב עמימות ויכולת להכחיש את מעורבותה בפעילות סייבר זדונית ובלתי חוקית כאשר העקבות מובילים אליה.

אחת מקבוצות ההאקרים האיראניות המובילות היא Ashiyane Digital Security Team, הנתפסת כבעלת קשרים למשמרות המהפכה וחבריה מונעים על ידי תפיסות אידיאולוגיות התומכות במשטר האיראני ובמהפכה.[31] Ashiyane דורגה על ידי האתר Zone-H, המתמחה בניתוח פעילות של האקרים במרחב הסייבר, במקום השני בעולם במספר אתרי האינטרנט שחבריה הצליחו לפרוץ ולהשחית, לרוב על ידי החלפת התוכן בצלמית של הקבוצה או בתעמולה פרו איראנית. נכון לתחילת נובמבר 2013, מיוחסות לקבוצה יותר מ־6,000 פריצות.[32] בין האתרים שנפרצו על ידי חברי Ashiyane נמצאים 26 אתרי ממשל ברזילאיים, ובכללם האתר של המשטרה הצבאית, וכן אתרי ממשל באנגליה ובפקיסטן.[33] על פי אתר האינטרנט Zone-H, מלבד Ashiyane, שבע קבוצות האקרים איראניות נוספת נמצאות בין ארבעים קבוצות ההאקרים הפעילות בעולם בכל הקשור להשחתת אתרים (defacement website). מתקפות השחתה אמנם נחשבות לקלות יחסית, אך הן מעידות על יכולות טכניות גבוהות ובמקרים רבים הן מהוות שלב ראשוני בהתפתחותן של קבוצת ההאקרים איראניות לכיוון מתקפות מתוחכמות והרסניות יותר. דוגמה להתפתחות כזו היא Ajax Security Team, קבוצת האקרים איראנית, שהחלה לפעול ב־2010 והתמקדה במתקפות השחתת אתרים. דוח של קבוצת FireEye המנתח לעומק את פעילותה מצביע על טרנספורמציה מסוכנת. ראשית חברי הקבוצה, שבתחילה פעלו בעיקר במטרה להוכיח את כישוריהם (הם אף תקפו אתר ממשלתי איראני), עברו תהליך פוליטיזציה והחלו למקד את מתקפותיהם בחברות אמריקאיות ובמתנגדי משטר בתוך איראן. במקביל לכך, חלה גם הסלמה בדפוסי התקיפה של הקבוצה, אשר זנחה את מתקפות השחתת האתרים ועברה לריגול קיברנטי, הכולל איסוף מידע בקנה רחב כנגד מתנגדי משטר, תוך שימוש בתוכנות Malware מתקדמות ובטכניקות דיוג. תפקידו של המשטר בתהליך אבולוציה זה וקשריו עם קבוצת Ajax אינם ברורים, אך אין ספק כי פעילות הקבוצה עולה בקנה אחד עם ניסיונות המשטר לשלוט במרחב האינטרנט הפנימי ורדיפתו אחר מתנגדים.[34]

גורם נוסף שתורם להתקדמות המהירה בתוכנית לוחמת הסייבר האיראנית הם הקשרים המתהדקים של מערך הסייבר האיראני עם פושעי סייבר, האקרים ומומחי אבטחת מידע, בעיקר רוסים, המוכנים "להשכיר" את יכולותיהם בכסף. גורמים אמריקאיים רואים קשרים אלה כמרכיב מרכזי בקפיצת המדרגה האיראנית, וחבר הקונגרס מייק רוג'רס, ראש ועדת המודיעין, אף ציין כי בגל תקיפות סייבר נגד אתרי בנקים אמריקאיים, אשר יוחס לגורמים איראניים, ניתן היה לאתר סימנים למעורבות של גורמים רוסיים.[35] לצד כוח האדם ה"מיובא", ביכולתה של איראן גם לרכוש "נשק" סייבר מתוחכם וחזק המוצע בשוק השחור לכל המוכן לשלם את המחיר הנדרש. נשק סייבר זה מאפשר לאיראנים להעצים במהירות את יכולותיהם ומסוכנותם.[36]

ההתקדמות ביכולות לוחמת הסייבר האיראניות משתקפת בסדרה של מתקפות שהתרחשו במהלך המחצית השנייה של 2012 וב־2013, אשר עשו שימוש בטכניקות מתוחכמות יותר, תקפו יעדים איכותיים יותר והתרחשו בהיקפים משמעותיים יותר מאשר תקיפות מוקדמות יותר שיוחסו לאיראן. מתקפה אחת שיוחסה לגורמים איראניים החלה בספטמבר 2012 ונמשכה גם לתוך 2013, כללה תקיפה רחבת היקף של אתרי האינטרנט של בנקים ומוסדות פיננסיים מרכזיים בארצות הברית. המתקפה תוארה על ידי מומחה לאבטחת מידע כ"חסרת תקדים בהיקפה ובמידת יעילותה". ייחודיותה ואיכותה נעוצות בשיטת הפעולה אותה נקטו התוקפים: במקום לתקוף דרך פרצות במחשבים בודדים, הם ניתבו את מתקפותיהם דרך רשתות המחשוב של מרכזי מידע. מרכזי מידע אלה, המופעלים על ידי חברות כגון "גוגל" ו"אמָזון", מורכבים מרשתות מחשבים ענקיות המחברות בין מאות, ולעיתים אלפי שרתים ומחשבים, ומספקות שירותי "ענן" למספר רב של חברות ועסקים ברחבי העולם. התוקפים הצליחו להשתלט על חלק מ"ענני" מחשוב אלה ולהשתמש בעוצמת המִחשוב האדירה שלהם כפלטפורמה למתקפות על אתרי בנקים וחברות פיננסיות בארצות הברית. מומחי אבטחה תיארו מהלך זה כ"מקבילה הקיברנטית של הפיכת גוּר של צ'יוואווה לגודזילה יורקת אש".[37]

קבוצת האקרים המכנה עצמה "לוחמי הסייבר של עז א־דין אל־קסאם" קיבלה אחריות על התקפת מניעת שירות נגד אתרי האינטרנט של בנקים אמריקאיים מרכזיים, ביניהם Citigroup, Bank of America ו־HSBC. חברי הקבוצה ניצלו את פלטפורמת המחשוב של מרכזי המידע וניתבו נפחים עצומים של תעבורת רשת לאתרי הבנקים, מה שהביא לקריסתם ומנע את גישת הלקוחות לחשבונותיהם. בנוסף לשימוש בתעבורת רשת, השתמשו התוקפים בטכניקה המכונה Encrypted DDoS. שיטה זו מנצלת את מנגנוני הצפנת המידע של הבנקים עצמם – מנגנונים שפעולתם צורכת משאבי מערכת רבים. התוקפים הציפו את אתרי הבנקים

בפעולות הדורשות הצפנה, ובכך גרמו להאטה ולפגיעה משמעותית בפעילותם. עם זאת, במהלך המתקפות לא נפרצו חשבונות בנק ולא נגנבו כספי לקוחות.[38]

מומחי אבטחת מידע מציינים שהיכולות הגבוהות הנדרשות לביצוע מתקפה בהיקף נרחב כל כך ובתחכום רב כל כך מצביעות על מעורבותה של מדינה. לתקיפה נגד תשתיותיה הפיננסיות של מדינה, במיוחד של מעצמה כלכלית כמו ארצות הברית, משמעויות חמורות והיא עשויה להביא לנזקים כלכליים כבדים עקב הפגיעה בשגרת הפעילות הפיננסית של חברות מסחריות ובתי אב רבים.

למרות היעדר הוכחות פיזיות והכחשה איראנית, בכירים בממשל ובשירותי המודיעין של ארצות הברית משוכנעים כי איראן היא העומדת מאחורי המתקפות, כתגובה לסנקציות הבין־לאומיות עליה ולמתקפות הסייבר שפגעו בתשתיותיה ונתפסות בעיניה כמעשה ידיהן של ארצות הברית וישראל. מזכיר ההגנה האמריקאי דאז, ליאון פאנטה, התייחס למתקפות נגד הבנקים ואמר כי מדובר ב"הסלמה משמעותית", מבלי שהזכיר את שמה של איראן.[39]

גל תקיפות נוסף המיוחס לגורמים איראניים התמקד בחברות תשתית ואנרגיה אמריקאיות והחל לתפוס תאוצה בחודשים הראשונים של 2013, עד אשר הסוכנות האמריקאית להגנת המולדת החליטה בחודש מאי להוציא באופן חריג אזהרה לחברות האנרגיה והתשתיות בדבר עליית מדרגה באיום הסייבר על רשתות המחשוב שלהן. האזהרה ציינה כי אין מדובר במתקפות שגרתיות של גניבת מידע, ריגול תעשייתי ופגיעה במערכות מנהליות, אלא במתקפות המבקשות להשתלט על מערכי הבקרה שלהן ולפגוע בפעילותן הפיזית או באמצעי הבטיחות של תשתיות קריטיות, דוגמת מערכות הולכת גז ונפט ומערכות חשמל. הממשל האמריקאי אמנם לא הצהיר באופן רשמי כי הממסד האיראני הוא העומד מאחורי גל המתקפות, אך מומחים ואנשי ממשל ציינו כי ישנן עדויות המצביעות על מוצאן בשטחה של איראן וכי הוצאתן אל הפועל מחייבת תמיכה כלשהי מצד הגורמים השולטים במרחב הסייבר האיראני.[40] התחזקות עתידית של הסנקציות נגד שוק האנרגיה האיראני,[41] עשויה להוביל את איראן למהלך אסטרטגי נגד שוק האנרגיה הבין־לאומי, הן כצעד הרתעתי והן כדי להגביר את הדרישה לנפט שלה.

מומחים מתארים את המתקפות על רשתות המחשוב של חברות האנרגיה האמריקאיות כמהלך נרחב של איסוף מידע, לימוד ובחינה, אשר נועד לייצר תשתיות ידע וניסיון לטובת מתקפה עתידית על מערכות בקרה המפעילות ומווסתות את פעילותן של תשתיות קריטיות. פגיעה במערכות אלו עשויה להביא לנזק משמעותי ואף לאובדן חיים בקנה מידה נרחב. ואכן, במהלך המתקפות הצליחו התוקפים לעקוף חלק ממערכות האבטחה ולאסוף מידע על המבנה שלהן, יכולותיהן ופרצות האבטחה הקיימות בהן.[42] בכיר בחברת אבטחת המידע Mandiant אמר כי לפחות במקרה אחד הצליחו חוקריו לשייך את המתקפה

לקבוצת האקרים איראנית, אשר קשריה עם המשטר אינם ברורים. לדבריו, מטרת התוקפים, אשר נעו בתוך מערכות המחשוב האמריקאיות ולמדו את מערכי הגילוי והאבטחה שלהן, היא לצבור ניסיון בפעילות ברשתות "חיות" ולתור אחר נקודות חולשה.[43] בכירים אמריקאיים ציינו כי ההתקפות על חברות האנרגיה וההצלחות היחסיות של הפורצים מעידות כי יכולות הסייבר ההתקפיות העומדות לרשותה של איראן משתפרות ומתפתחות במהירות.[44] היה ואיראן תשיג יכולות תקיפה אפקטיביות נגד מערכות בקרה של תשתיות חיוניות, הדבר עשוי להוות איום אסטרטגי על יריבותיה.

תקיפה משמעותית נוספת שיוחסה לאיראן אירעה בספטמבר 2013, כאשר גורמים רשמיים בארצות הברית דיווחו על פריצה לרשת מחשבים לא מסווגת של הצי האמריקאי. הגורמים ציינו כי המתקפה נעשתה על ידי קבוצת האקרים הפועלים בשירות הממשל האיראני או בהסכמתו ותמיכתו. הרשת שנפגעה היא הרשת הפנימית של הצי האמריקאי, אשר אמנם אינה מסווגת, אך משמשת בין השאר להתכתבויות והתקשרויות וכוללת מידע רגיש, כגון כתובות דואר אלקטרוני של ראשי הצי ושל בכירי ממשל. גורמים בממשל דיווחו כי התוקפים הצליחו לחדור למערכת הניהול של הרשת, אך לטענתם לא נגנב מידע בעל ערך משמעותי ולא נפרצו תיבות דוא"ל. מדאיגה במיוחד הייתה העובדה שהפורצים הצליחו להמשיך ולפעול ברשת המחשבים של הצי גם אחרי שגורמי הביטחון האמריקאיים דיווחו על סילוקם מהרשת. התחכום האיראני שהתגלה בתקיפה זו מהווה סימן נוסף להתפתחות ולהתקדמות ביכולות הפריצה האיראניות ועל נכונותה של איראן לפעול גם נגד יעדי סייבר צבאיים.[45]

מלבד שרשרת המתקפות נגד מוסדות אמריקאיים, גורמים המזוהים עם איראן קיבלו על עצמם בשנה האחרונה אחריות גם למתקפות סייבר נגד מוסדות ישראליים. ביוני 2013 הצהיר ראש הממשלה בנימין נתניהו כי חלה עלייה משמעותית בתקיפות הסייבר האיראניות על תשתיות מחשוב חשובות בישראל.[46] במהלך דצמבר 2013 וינואר 2014 טענה קבוצת האקרים אסלאמית, המכנה עצמה The Islamic Cyber Resistance Group (ICRG) כי ביצעה מספר מתקפות סייבר איכותיות נגד גורמים בישראל ובמזרח התיכון כנקמה על חיסולו של בכיר חזבאללה חסן לקיס. הקבוצה, הזוכה לסיקור נרחב מצד סוכנות הידיעות האיראנית Fars, טוענת כי הצליחה לחדור למערכות השליטה של רשות התעופה האזרחית של ישראל ולשהות במערכת במשך חודשים מבלי להתגלות. אנשי הקבוצה טוענים כי הצליחו לגנוב מידע רגיש ואף יכלו להשתלט על מערכות הניווט והתקשורת של הרשות ולגרום לאסון אווירי באם היו בוחרים לעשות כך.[47] אנשי ICRG גם הצהירו כי הצליחו לחדור לשרתי המחשוב של צה"ל ולגנוב מידע סודי, כגון תיקים אישיים של חיילי צה"ל, רשימות של בעלי תפקידים, סיסמאות,

כתובות מגורים ודואר אלקטרוני וקודים צבאיים. פרט למתקפות על ישראל, הצהיר ארגון ICRG כי הצליח לפרוץ למאגר מידע של הצבא הסעודי ולמחשבים של חברות הנמצאות בבעלות משפחת בן־לאדן.[48] עם זאת, גורמים בישראל קבעו כי המתקפות בהן התפארה הקבוצה לא התרחשו מעולם וכי מדובר בלא יותר מאשר תעמולה ולוחמה פסיכולוגית מצד איראן.

ברקע המאבקים הללו עומדת תעלומת מותו של איש משמרות המהפכה מוג'תבא אחמדי שנמצא מת בתחילת אוקטובר 2013. דיווחים במערב קובעים כי מדובר בבכיר ששימש כמפקד מטה לוחמת הסייבר של משמרות המהפכה. בתחילה יוחס מותו לישראל, אך משמרות המהפכה הכחישו זאת נחרצות וקבעו כי היה תוצאה של "תאונה מוזרה".[49] למרות הערפול הרב סביב האירוע, לא ניתן לפסול את ההשערה כי למותו של אחמדי היו השלכות על פעילות הארגון בזירת הסייבר.

מערך שליחים ללוחמת סייבר

לצד חיזוק מערך הסייבר המדינתי ושיתוף הפעולה עם קהילת ההאקרים באיראן, מתעצמים הניסיונות איראניים להרחיב ולחזק את יכולות לוחמת הסייבר בהן מחזיקות בעלות בריתה. נראה כי איראן מבקשת לייצר מערך יעיל של שליחים הפועלים עבורה במרחב הסייבר. אחד ממרכזי הכובד של פעילות איראנית זו הוא הזירה הסורית, שלה משמעות אסטרטגית עבור איראן. עם תחילת העימותים בין משטר אסד לבין כוחות המורדים, החלו האיראנים לממן, לצייד ולאמן את כוחות הביטחון הסוריים באמצעי ניטור ושליטה על מרחב הסייבר ששימש כפלטפורמה מרכזית למורדים לארגון הפעילות נגד המשטר. יועצים ומומחים איראניים אימנו וחיזקו את משטרת הסייבר הסורית וסייעו לה לעקוב אחר רשתות המחשבים והסלולר במדינה ולפגוע ביכולתם של המורדים להעביר מסרים ומידע הן בתוך המדינה והן אל מחוץ לה.[50]

שחקן מרכזי בהקשר זה הוא "צבא סוריה האלקטרוני" (Syrian Electronic Army – SEA). קבוצה זו של האקרים תומכי אסד החלה לפעול ב־2011, ובמהלך השנה הראשונה לפעילותה ביצעה בעיקר מתקפות "ונדליזם" חובבניות יחסית נגד אתרים בעלי רמת אבטחה נמוכה, שתקיפתם אינה דורשת יכולת טכנית גבוהה: מתקפות spam, הצפת מערכות הטוקבק של פורומים ואתרי חדשות שונים וכדומה.[51] במהלך 2012 החל SEA להוציא אל הפועל פעילויות מורכבות יותר נגד אתרים בעלי רמת אבטחה המחייבת ידע טכני ויכולות גבוהות יחסית. מומחי סייבר ואנשי ממשל מערביים מיחסים קפיצת מדרגה זו למעורבותם והדרכתם של מומחי לוחמת סייבר איראניים, אשר מאמנים ומציידים את פעילי הארגון. מייקל היידן, שעמד בעבר בראש ה־CIA וה־NSA, אף קבע כי קבוצת ההאקרים הסורית הינה שליח איראני לכל דבר ועניין.[52]

התפתחותו של SEA באה לידי ביטוי בשנה האחרונה בגל מתקפות נגד אתרים של גורמי תקשורת וארגוני זכויות אדם, אותם הוא תופס כעוינים למשטר אסד. בין השאר, תקפו חברי SEA אתרי חדשות מובילים ביניהם "ניו יורק טיימס", BBC, "אל־ג'זירה", "וושינגטון פוסט" ו־The Huffington Post. כמו כן תקף הארגון את אתר Human Rights Watch המספק מידע על מספר האזרחים שנפגעו בקרבות בסוריה. חברי הארגון אף הצליחו להסב נזק משמעותי כאשר השתלטו על חשבון ה"טוויטר" של סוכנות הידיעות AP ופרסמו ידיעה כוזבת בדבר מתקפה כביכול על הבית הלבן ופגיעה בנשיא אובמה. הידיעה יצרה פאניקה מיידית בוול סטריט והביאה לצניחת מניות ולנזק שהוערך ב־136 מיליארד דולר. באפריל 2013 קיבל SEA על עצמו אחריות להפלת שרתי הרשת החברתית "טוויטר" ולהפניית הגולשים באתר הגיוס של חיל המארינס לאתר תעמולה נגד המורדים.[53]

לאחרונה נראה כי SEA עשה קפיצת מדרגה נוספת ביכולותיו ומתחיל להפעיל טכניקות וכלי תקיפה מתוחכמים יותר, כגון דיוג, תוכנות זדוניות ו"סוסים טרויאניים". כלים אלה אפשרו לארגון להוציא אל הפועל התקפות איכותיות נגד שרתים של חברות תקשורת אינטרנט, כגון אינדקס הטלפונים הגדול בעולם TrueCaller, שירות ההודעות והווידיאו Tango, ואפליקציית התקשורת Viber. במהלך מתקפות אלו הצליחו התוקפים לגנוב כמויות עצומות של מידע, כגון פרטי אנשים וכתובות מייל, אשר ייתכן מאד שהועברו לידי המודיעין הסורי ושימשו לפעילות נגד מתנגדי המשטר ולריגול.[54] סוכנות הידיעות האיראנית Fars אף דווחה כי הארגון תקף את מערכת המים של העיר חיפה,[55] אולם התמונות שצורפו לידיעה הראו ש־SEA חדר אך ורק למערכת בקרת ההשקיה של אחד מיישובי הצפון בישראל.[56] עם זאת, התקיפה והחדירה למערכת הבקרה של תשתית ישראלית מצביעות על ניסיון של SEA להתרחב גם לשיטות ומטרות מתקדמת יותר של לוחמת סייבר.

יכולות מתקדמות אלו, אשר מומחים רבים רואים אותן כתוצר של אימון, הכוונה וסיוע איראניים, הפכו את SEA לגורם משמעותי במרחב הסייבר, ואת לוחמת הסייבר בכלל למרכיב משמעותי באסטרטגיית ההרתעה הסורית. כשסוריה ביקשה למנוע תקיפה אמריקאית, בתגובה לשימוש של כוחות אסד בנשק כימי, שלחו אנשי SEA הודעה לסוכנות "רויטרס" כי במקרה של תקיפה אמריקאית בסוריה, הארגון יסלים את מתקפותיו ויפעל נגד מטרות משמעותיות יותר. ריצ'רד קלארק, יועץ הבית הלבן לשעבר לנושאי אבטחת סייבר ולוחמה בטרור, העריך כי במקרה של מתקפה אמריקאית על סוריה, כל תגובה של גורמים סוריים במרחב הסייבר תתבצע בסיוע גורמים איראניים.[57]

בנוסף לתמיכה ביכולות הסייבר של משטר אסד, ממשיכה איראן את תמיכתה המסורתית במערך הסייבר של בעל בריתה וחסותה הקרוב, חזבאללה, שהפך

לשחקן פעיל בתקיפת ישראל.[58] דו"ח של מרכז מאיר עמית מצביע על מעורבות ותמיכה עמוקות של איראן במערך אתרי האינטרנט של חזבאללה. מערך זה מהווה פלטפורמה לתעמולה ולאינדוקטרינציה של רעיונות המהפכה האסלאמית וכולל תעמולה פרו־איראנית, פולחן אישיות של המנהיג העליון ח'מנהאי ושל מנהיג חזבאללה חסן נסראללה, ותעמולה אנטי־ישראלית ואנטישמית. התוכן באתרים אלה נקבע בשיתוף עם איראן ובכפוף לאסטרטגיית התעמולה האיראנית וחלק מהם אף מופעלים מתוך שטחה של איראן על ידי מקורבים לשלטון.[59]

תובנות מסכמות

יכולות לוחמת הסייבר של איראן מתקדמות באופן עקבי וכבר היום היא מהווה גורם משמעותי שאין לזלזל בכוונותיו. ניתן להעריך שההחלטה האיראנית לפעול באופן נרחב במרחב הסייבר נובעת משני מניעים עיקריים: הראשון נוגע לעובדה שאיראן ספגה מתקפות סייבר חמורות. כמי שחוותה על בשרה את העוצמה והיכולות של תקיפה בתווך הקיברנטי, היא מכירה בחשיבות ההקמה של יכולות הגנה, לצד בנייה והפעלה של יכולות תקיפה. המניע השני של איראן נוגע להתפתחות הטכנולוגית העולמית, וכנגזר מכך האיראנית, המאפשרת להרחיב את תמהיל הפעולה גם למרחב הקיברנטי ולא רק לזה הפיזי. התפתחות זו משתלבת בצורה מיטבית עם תפיסת האסטרטגיה האסימטרית של איראן.

ניתוח מתקפות הסייבר המיוחסות לאיראן ושלוחותיה מצביע על מגוון רחב של מטרות, יעדים ושיטות פעולה. אחת המסקנות העולות ממאמר זה היא, שבתקופה האחרונה הבשילו יכולות הסייבר של איראן הן במרחב ההגנתי והן במרחב ההתקפי. על אף שנדמה שיכולות אלו עדיין נחותות ביחס ליכולות הסייבר של מעצמות טכנולוגיות מובילות, נראה שהאיראנים מגשרים על הפערים במהירות וביעילות.

אחת המגמות המסוכנות ביותר בפעילות הסייבר ההתקפית של איראן היא פעולה נגד מערכות הליבה המבצעיות של ארגונים ומדינות. מערכות אלו, השולטות בתהליכי ייצור, אספקה ושירותים חיוניים ומבקרות אותם, עלולות להיות מטרה לתקיפה איראנית. פעולות הגישוש, הסריקה והלמידה שהתגלו במערכות המחשוב של חברות אנרגיה אמריקאיות ויוחסו לגורמים איראניים, ניתנות רק לפרשנות אחת: איראן מנסה ליצור יכולת ונגישות לתשתיות קריטיות. נגישות כזאת עלולה לא להתגלות כלל, ותוכל להיות מופעלת בעתיד לצרכים התקפיים לפי החלטה איראנית. מתקפה מוצלחת על מערכות בקרה של מתקני אנרגיה, גז ומים עשויה לגרום לנזק משמעותי. ניתן לכאורה לקבל, במסגרת כללי המשחק, פעולות של ריגול וגניבת מידע במרחב הסייבר, אך לא ניתן ואין להסכים

כלל להשלמה עם ניסיונות חדירה למערכות בקרה של מתקני תשתית אזרחיים. ניסיונות כאלה מחייבים תגובה חריפה.

נדמה שההבנה שאיראן מהווה איום משמעותי על יריבותיה במרחב הסייבר כבר מניעה שיתוף פעולה הדוק בין מדינות המאוימות על ידי יכולות אלו. אולם אין להסתפק אך ורק בשדרוג המודיעין והעמקת יכולות ההגנה; אלה לעולם לא יספיקו מול יריב נחוש ובעל יכולות מבצעיות, מודיעיניות וטכנולוגיות. מרחב הסייבר מאפשר מִנעד רחב של פעולות להעברת מסרים באמצעותו, מתחת לסף של מלחמה פיזית. פעולות אלו ידרשו להדגים את הנזק שייגרם לאיראן אם תמשיך לפעול ללא ריסון נגד מטרות רגישות. לאחרונה פורסמו פרטים על מבצע לתקיפת סייבר רחבת היקף בסוריה שהוכן על ידי ה־NSA באביב 2011, סמוך לפרוץ מלחמת האזרחים במדינה.[60] אם דיווח זה נכון, הרי שהכנת מהלומה קיברנטית נגד איראן, לצד הדגמה מעת לעת של יכולות איכותיות, יוכלו לסייע לרסן את פעולתה במרחב התשתיות הקריטיות.

עד שתימצא נוסחת הפלא הטכנולוגית לזהות ברמה גבוהה של ודאות הניתנת להוכחה משפטית את מקור התוקפים במרחב הסייבר, ניתן במקרים לא מעטים להסתפק גם בעדויות נסיבתיות באשר למקור התקיפה, ולפעול מול מקור זה בחריפות במרחב הסייבר, מתחת לסף מלחמה פיזית.

מעל כל אלה, העמקת שיתוף הפעולה בין המדינות הדמוקרטיות היא אבן יסוד בהתמודדות עם איראן ושלוחותיה. שיפור הקשר המבצעי, המודיעיני והטכנולוגי הינו חיוני. כך גם שיפור שיתוף הידע באשר לשיטות וכלים בהם עושים איראן ושלוחיה שימוש. בנוסף לכך, ישראל עשויה למצוא בעלי ברית נגד מלחמת הסייבר האיראנית גם בקרב המשטרים הסוניים באזור המפרץ, ובראשם הממלכה הסעודית, המאוימים באופן קבוע ואף נפגעו בעבר בידי גורמים איראניים. תחום הגנת הסייבר, שישראל היא שחקן מוביל בו, עשוי לשמש כבסיס ליצירת דו־שיח אסטרטגי פורה בסוגיות אזוריות נרחבות יותר, כגון האיום האיראני במובנו הכולל, המשבר בסוריה והסוגיה הפלסטינית.

התנהלותו התוקפנית של מערך הסייבר האיראני מבליטה את אופיו הטוטליטרי של המשטר באיראן. הפיקוח ההדוק והחודרני, הפוגע בחופש הביטוי והדיבור של אזרחי איראן, לצד האלימות והאגרסיביות המאפיינות את פעילותם של גופים כמו משטרת הסייבר, מהווים תמונת מראה לתדמית אותה מבקש לקדם משטר רוחאני במטרה לסדוק את משטר הסנקציות הבין־לאומי על איראן. ישראל ומדינות נוספות יכולות להשתמש בפעילותה של איראן במרחב הסייבר כפלטפורמה הסברתית המבליטה את אופייה הטוטליטרי והתוקפני של הרפובליקה האסלאמית.

מציאות זו, של ההתפתחות המהירה ביכולת לוחמת הסייבר של איראן ושל שלוחיה ובעלי בריתה, מחייבת את ישראל, כמו גם מדינות מערביות אחרות, לפעול

באופן נחרץ ושיטתי לשימור עליונותן האיכותית והמבצעית במרחב הסייבר. חשיבותו של מרחב זה לתפיסת הביטחון הישראלית, והדחיפות שביצירת "כיפת ברזל" דיגיטלית, הודגשו היטב בדבריו של רמטכ"ל צה"ל, רב־אלוף בני גנץ: "ישראל חייבת להיות ברמה המעצמתית בסייבר... אין לחכות עם הסיפור הזה".[61]

הערות

1 Barbara Slavin and Jason Healey, *Iran: How a Third Tier Cyber Power Can Still Threaten the United States*, The Atlantic Council, 2013, http://www.atlanticcouncil.org/images/publications/iran_third_tier_cyber_power.pdf.

2 Yaakov Katz, "Iran Embarks on $1b. Cyber-Warfare Program", *The Jerusalem Post*, December 18, 2011, http://www.jpost.com/Defense/Article.aspx?id=249864.

3 Gabi Siboni and Sami Kronenfeld, "Iran and Cyberspace Warfare", *Military and Strategic Affairs*, Vol. 4, No. 3 (Dec. 2012), pp. 77-99.

4 שם.

5 Majid Rafizadeh, "Iran's 'Halal' Version of the Internet", *Al-Arabiya News*, July 12, 2013, http://english.alarabiya.net/view-renderer?mgnlUuid=cb92c5e3-f973-45ce-8d46-12b8fb4dfe17.

6 Sara Reardon, "First Evidence for Iran's Parallel Halal Internet", *New Scientist*, October 10, 2012, http://www.newscientist.com/article/mg21628865.700-first-evidence-for-irans-parallel-halal-internet.html#.UnZubT4UHVI

7 Saeed Kamali Dehghan, "Iran Launches 'National Email Service'", *The Guardian*, July 9, 2013, http://www.theguardian.com/world/2013/jul/09/iran-launches-national-email-service

8 "Iran launches own 'YouTube' website", *AFP*, December 9, 2012, http://en-maktoob.news.yahoo.com/iran-launches-own-youtube-website-121634740.html

9 Trend F. Karimov, "Iran Introduces Domestically-made Antivirus Padvish", *Trend News Agency*, June 30, 2013, http://en.trend.az/capital/it/2166121.html /

10 חסימה זו התבצעה בין השאר באמצעות הפצה מתוכננת של תוכנות זדוניות שהוסוו כתוכנות עוקפות סינון, דבר שאִפשר למשטר להתחקות אחר רשתות בלתי חוקיות.

11 Urt Hopkins, "Why Iranians might Actually Use the Censored "Halal Internet", *The Daily Dot*, April 25, 2013, http://www.dailydot.com/society/iran-halal-private-internet-blocked-censorship; Small Media, *Iranian Internet Infrastructure and Policy Report*, February-March 2013, http://smallmedia.org.uk/InfoFlowReportMARCH.pdf.

12 "Iran Unveils 12 Cyber Products", *Fars News*, December 14, 2013, http://english.farsnews.com/newstext.aspx?nn=13920923001322.

13 "Iran Launches Home-made Defense Shield", *ISNA*, December 9, 2013, http://isna.ir/en/news/92091812343/Iran-launches-home-made-defense-shield /

14 Alastair Stevenson, "Iran and North Korea Sign Technology Treaty to Combat Hostile Malware", *V3*, September 3, 2012, http://www.v3.co.uk/v3-uk/news/2202493/iran-and-north-korea-sign-technology-treaty-to-combat-hostile-malware#.

15 Steve Stecklow, "Chinese Firm Helps Iran Spy on Citizens", *Reuters*, March 22, 2012, http://graphics.thomsonreuters.com/12/03/IranChina.pdf.

16 "Iran for the First Time Stages Cyber Warfare Drill", *Al-Arabiya*, December 31, 2012, http://www.alarabiya.net/articles/2012/12/31/257960.html.

17 "Drones, Cyber-Defense Feature in Iran Guards Drill", *The Jerusalem Post*, February 23, 2013, http://www.jpost.com/Iranian-Threat/News/Drones-cyber-defense-feature-in-Iran-Guards-drill.

18 "Iran Holds Defense Exercises", *Trend*, October 22, 2013, http://en.trend.az/news/politics/2203465.html; "Iran Carries Out Drills to Detect Cyber Vulnerabilities", *Tasnim News Agency*, October 22, 2013, http://www.tasnimnews.com/english/Home/Single/172473.

19 "Iranian Blogger who Told Supreme Leader Khamenei 'Your Judicial System... is nothing but a Slaughterhouse' Tortured to Death in Prison", *MEMRI*, November 19, 2012, http://www.memri.org/report/en/0/0/0/0/0/0/6819.htm.

20 European Parliament Resolution of November 22, 2012 on the Human Rights Situation in Iran, Particularly Mass Executions and the Recent Death of the Blogger Sattar Beheshti, *The European Parliament*, November 22, 2012, http://www.europarl.europa.eu/document/activities/cont/201301/20130109ATT58696/20130109ATT58696EN.pdf.

21 Thomas Erdbrink, "Head of Tehran's Cybercrimes Unit is Fired over Death of Blogger", *The New York Times*, December 1, 2012, http://www.nytimes.com/2012/12/02/world/middleeast/after-death-of-sattar-beheshti-iranian-blogger-head-of-tehrans-cybercrimes-unit-is-fired.html.

22 "Intelligence Ministry Admits Arresting News Providers, Blames Foreign Media", *Reporters Without Borders*, February 20, 2013, http://en.rsf.org/iran-intelligence-ministry-admits-20-02-2013,44099.html; "Iran: Two Arrested for 'Insulting Regime Officials' on their Facebook Page", *National Council of Resistance of Iran*, July 10, 2013, http://www.ncr-iran.org/en/news/human-rights/14138-iran-two-arrested-for-insulting-regime-officials-on-their-facebook-pa.

23 "Tehran Closes Dozens of Internet Cafes", *Mohabat News*, July 27, 2013, http://www.mohabatnews.com/index.php?option=com_content&view=article&id=7222:tehran-closes-dozens-of-internet-cafes&catid=35:inside-iran&Itemid=278.

24 Eric Grosse, "Iranian Phishing on the Rise as Elections Approach", *Google Blog*, June 12, 2013, http://googleonlinesecurity.blogspot.co.il/2013/06/iranian-phishing-on-rise-as-elections.html.

25 Siboni and Kronenfeld, "Iran and Cyberspace Warfare", 2012.

26 Betsy Isaacson, "Iran's Pre-Election Phishing Scheme Detected, Disrupted by Google", *The Huffington Post*, June 13, 2013, http://www.huffingtonpost.com/2013/06/13/iran-phishing-google_n_3435811.html.

27 "Iranian Authorities Target Internet, Media before Elections", *CPJ*, June 13, 2013, http://www.cpj.org/2013/06/iranian-authorities-target-internet-media-before-e.php; Helle Dale, "Iran Clamps down on Dissidents before Election", *The Foundry*, June 12, 2013, http://blog.heritage.org/2013/06/12/iran-clamps-down-on-dissidents-before-election.

28 Neal Ungerleider, "Iran's 'Halal Internet' is really a 'Filternet'", *Fast Company*,

2013, http://www.fastcompany.com/3009714/irans-halal-internet-is-really-a-filternet.

29 Thom Shanker & David E. Sanger, "U.S. Helps Allies Trying to Battle Iranian Hackers", *New York Times*, June 8, 2013, http://www.nytimes.com/2013/06/09/world/middleeast/us-helps-allies-trying-to-battle-iranian-hackers.html?nl=todayshea dlines&emc=edit_th_20130609&_r=4&pagewanted=all&

30 Siboni and Kronenfeld, "Iran and Cyberspace Warfare".

31 Frank J. Cilluffo, *The Iranian Cyber Threat to the United States*, *A Statement before the U.S. House of Representatives Committee on Homeland Security Subcommittee on Counterterrorism and Intelligence and Subcommittee on Cybersecurity, Infrastructure, Protection and Security Technologies*, April 26, 2012, p. 5.

32 http://www.zone-h.org/stats/notifierspecial.

33 "Brazilian Military Police & 26 Govt Websites Hacked by Ashiyane Digital Security Team", *Hackread*, January 28, 2013, http://hackread.com/brazilian-military-police-26-govt-websites-hacked-by-ashiyane-digital-security-team.

34 Nart Villeneuve, Ned Moran, Thoufique Haq and Mike Scott, "Operation Saffron Rose", Fire-eye, 2014.

35 Julian E. Barnes and Siobhan Gorman, "U.S. Says Iran Hacked Navy Computers ", *The Wall Street Journal*, September 27, 2013, http://online.wsj.com/news/articles/SB10001424052702304526204579101602356751772; Adam Kredo, Mike Rogers, "China, Iran and Russia Launching Cyber Attacks Against U.S.", *The Washington Free Beacon*, July 22, 2013, http://freebeacon.com/mike-rogers-china-iran-and-russia-launching-cyber-attacks-against-u-s.

36 Shanker and Sanger, "U.S. Helps Allies Trying to Battle Iranian Hackers".

37 Nicole Perlroth and Quentin Hardy, "Bank Hacking Was the Work of Iranians, Officials Say", *The New York Times*, January 8, 2013, http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html?pagewanted=1&_r=1&ref=iran&&version=meter+at+6&region=FixedCenter&pgtype=Article&priority=true&module=RegiWall-Regi&action=click.

38 שם.

39 Julian E. Barnes and Siobhan Gorman, "Iran Blamed for Cyberattacks ", *The Wall Street Journal*, September 27, 2013, http://news.walla.co.il/?w=/15/2569449.
"איראן שיגרה מתקפת סייבר עוצמתית על בנקים בארה"ב", **וואלה**, 9 בינואר 2013, http://news.walla.co.il/?w=//2605254.

40 Ellen Nakashima, "U.S. Warns Industry of Heightened Risk of Cyber Attack", *The Washington Post*, May 10, 2013, http://www.washingtonpost.com/world/national-security/us-warns-industry-of-heightened-risk-of-cyberattack/2013/05/09/39a04852-b8df-11e2-aa9e-a02b765ff0ea_story.html;
ראו בנוסף ניתוח על היכולות הנדרשות לצורך ביצוע מתקפת סייבר ברמה גבוהה: גבי סיבוני, דניאל כהן ואביב רוטברט, "איום ארגוני הטרור במרחב הסייבר", **צבא ואסטרטגיה**, כרך 5, גיליון 3, המכון למחקרי ביטחון לאומי, דצמבר 2013, http://d26e8pvoto2x3r.cloudfront.net/uploadImages/systemFiles/pdf;
Nicole Perlroth & David E. Sanger, "New Computer Attacks Traced to Iran, Officials Say", *The New York Times*, May 24, 2013, http://www.nytimes.com/2013/05/25/world/middleeast/new-computer-attacks-come-

from-iran-officials-say.html?_r=1&.

41 לעת כתיבת מאמר זה מתנהל משא ומתן בין איראן למעצמות בנושא הגרעין. אין לשלול את האפשרות שעיצומי האנרגיה יחוזקו במידה ושיחות אלה יעלו על שרטון.

42 Siobhan Gorman & Danny Yadron, "Iran Hacks Energy Firms, U.S. Says", *The Wall Street Journal*, May 23, 2013, http://online.wsj.com/news/articles/SB10001424127887323336104578501601108021968.

43 Chris Strohm, "Iran-Based Hackers Traced to Cyber Attack on U.S. Company", *Bloomberg News*, May 14, 2013, http://www.businessweek.com/news/2013-05-14/iran-based-hackers-traced-to-cyber-attack-on-company-inside-u-dot-s-dot.

44 Shanker and Sanger, "U.S. Helps Allies Trying to Battle Iranian Hackers".

45 Barnes and Gorman, "U.S. Says Iran Hacked Navy Computers".

46 Gili Cohen, "Netanyahu Confirms: U.S. is Working with Israel on Cyber Defense, Iranian Attacks Increasing", *Ha'aretz*, June 9, 2013, http://www.haaretz.com/news/diplomacy-defense/.premium-1.528728.

47 "Israel's Aviation Agency Under Muslim Hackers' Control for Months", *Fars News*, January 8, 2013, http://english.farsnews.com/newstext.aspx?nn=13921018001457.

48 "Saudi Army, Al-Qaeda Company, Israeli Army Hacked in Revenge for Assassination of Hezbollah Leader", *Fars News*, December 16, 2013, http://english.farsnews.com/newstext.aspx?nn=13920925001699.

49 Damien McElroy and Ahmad Vahdat, "Iranian Cyber Warfare Commander Shot Dead in Suspected Assassination", *The Telegraph*, October 2, 2013, http://www.telegraph.co.uk/news/worldnews/middleeast/iran/10350285/Iranian-cyber-warfare-commander-shot-dead-in-suspected-assassination.html; Lisa Daftari, "Internal Plot, not Israel, Eyed in Latest Hit on Iranian Scientist", *Fox News*, October 8, 2013, http://www.foxnews.com/world/2013/10/08/internal-intrigue-not-israel-eyed-in-latest-hit-on-iranian-scientist.

50 Simon Tisdall, "Iran Helping Syrian Regime Crack down on Protesters, say Diplomats", *The Guardian*, May 9, 2011, http://www.theguardian.com/world/2011/may/08/iran-helping-syrian-regime-protesters; Lisa Daftari, "Iranian General Admits 'Fighting every Aspect of a War' in Defending Syria's Assad", *Fox News*, August 28, 2012, http://www.foxnews.com/world/2012/08/28/iranian-general-admits-fighting-every-aspect-war-in-defending-syria-assad; Geneive Abdo, "How Iran Keeps Assad in Power in Syria", *Foreign Affairs*, August 25, 2011, http://www.foreignaffairs.com/articles/68230/geneive-abdo/how-iran-keeps-assad-in-power-in-syria.

51 Ronald Deibert, "Waging the Cyber War in Syria", *National Post*, May 21, 2013, http://fullcomment.nationalpost.com/2013/05/21/ronald-deibert-waging-the-cyber-war-in-syria.

52 Joseph Menn, "Syria, Aided by Iran, could Strike back at U.S. in Cyberspace", *Reuters*, August 29, 2013, www.reuters.com/article/2013/08/29/us-syria-crisis-cyberspace-analysis-idUSBRE97S04Z20130829.

53 Sarah Hurtubise, "Syrian Hacker Army could be Advancing with Iranian Help", *The Daily Caller*, April 9, 2013, http://dailycaller.com/2013/09/04/syrian-hacker-army-could-be-advancing-with-iranian-help; Andrea Peterson, "The Post Just Got Hacked

by the Syrian Electronic Army. Here's Who they Are", *The Washington Post*, August 15, 2013, http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/15/the-post-just-got-hacked-by-the-syrian-electronic-army-heres-who-they-are.

54 Kenneth Geers and Ayed Alqartah, "Syrian Electronic Army Hacks Major Communications Websites", *FireEye*, July 30, 2013, http://www.fireeye.com/blog/technical/cyber-exploits/2013/07/syrian-electronic-army-hacks-major-communications-websites.html.

55 "Syrian Electronic Army Reveals Documents of Haifa Hack", *Fars News Agency*, June 15, 2013, http://english2.farsnews.com/newstext.php?nn=9203180050.

56 Elad Salomons, "Did the Syrian Electronic Army Attack Haifa's Water Supply SCADA System?", *Water Simulation*, June 5, 2013, http://www.water-simulation.com/wsp/2013/06/05/did-the-syrian-electronic-army-attack-haifas-water-supply-scada-system.

57 Menn, "Syria, Aided by Iran, could Strike back at U.S. in Cyberspace".

58 Olivia Goldhill and Reuters, "Benjamin Netanyahu: Iranian Cyber Attacks on Israel 'Non-Stop'", *The Telegraph*, June 10, 2013, http://www.telegraph.co.uk/technology/10110381/Benjamin-Netanyahu-Iranian-cyber-attacks-on-Israel-non-stop.html.

59 *Terrorism in Cyberspace: Hezbollah's Internet Network*, The Meir Amit Intelligence and Terrorism Information Center, 2013, http://www.terrorism-info.org.il/en/article/20488.

60 David E. Sanger, "Syria War Stirs New U.S. Debate on Cyberattacks", *The New York Times*, February 24, 2014, http://www.nytimes.com/2014/02/25/world/middleeast/obama-worried-about-effects-of-waging-cyberwar-in-syria.html?hp&_r=2.

61 Amos Harel & Gili Cohen, "2014: Iran out, Global Jihad in", *Ha'aretz*, February 1, 2014, http://d26e8pvoto2x3r.cloudfront.net/uploadimages/systemfiles/iran%20out,%20global%20jihad%20in.pdf.