לוחמת הסייבר של איראן

גבי סיבוני וסמי קרוננפלד

מבוא

בשנים האחרונות, גוברת ההבנה בקרב הציבור ומקבלי ההחלטות במדינות שונות שמרחב הסייבר מחייב התייחסות מתאימה כמרחב לחימה של ממש. מרחב המספק כר נרחב ותורפות רבות לפעולה של תוקפים החפצים לשבש מערכות מידע ואף לפגוע פגיעה פיזית במערכי תשתית חיונית המבוקרים על ידי מערכות בקרה תעשייתיות. כתוצאה, היקף ההשקעות ותהליכי בניין הכוח של מדינות רבות בבניית יכולות פעולה (הגנה, איסוף מודיעין ויכולות התקפיות) במרחב הסייבר עולה בקצב גובר והולך. מי שנפגעה על ידי מתקפת Stuxnet אותה ניתן להגדיר כאחת מהתקפות הסייבר ההרסניות ביותר, פועלת איראן במרץ רב כדי לשפר מצד אחד את ההגנה במרחב הסייבר ומצד שני כדי לבנות יכולות איסוף מודיעין ויכולות התקפיות במרחב הסייבר.

מטרות ההגנה של איראן במרחב הסייבר כפולות. הראשונה: הרצון למנוע השנות מתקפה דוגמת מתקפת Stuxnet וחדירות למחשבים אירניים לצרכי איסוף מודיעין דוגמת הוירוסים דוקו ולהבה. בהקשר זה מטרות הפעילות האיראנית דומה למה שנעשה במדינות רבות בעולם המבקשות להגן על תשתיות חיוניות שלהן. המטרה השניה נוגעת לרצון לשמור על שרידות המשטר האיראני על ידי מעקב וחסימה של מידע ושרותים מהציבור האיראני. במקרים רבים הכלים להשגת שתי המטרות דומים. לדוגמה: הנסיון האיראני ליצור רשת תקשורת מבודלת באיראן או הניתוק של שרותי גוגל במדינה.[1]

מן הצד השני, נמצאת איראן בתהליך רחב של בניין כוח גם בהקשר ההתקפי. זאת מתוך ההבנה שבכל עימות עתידי, השימוש במרחב הסייבר הנו קריטי להשגת היעדים מול אוייבי המדינה. מטבע הדברים קיים קושי רב לאסוף מידע גלוי באשר ליכולות הסייבר האיראניות ובייחוד באשר ליכולות ההתקפיות של המדינה. אורו של הזרקור על פעילות הסייבר של איראן הועצם לאחרונה לאחר החשד

ד"ר גבי סיבוני הוא ראש התכניות "צבא ואסטרטגיה" ו"לוחמת סייבר" במכון למחקרי ביטחון לאומי (INSS). סמי קרוננפלד הינו מתמחה בתכנית "לוחמת סייבר" במכון למחקרי ביטחון לאומי (INSS).

שאיראן הייתה מעורבת במספר ארועי סייבר חמורים. בהם גנבה של הרשאות אבטחה באינטרנט, תקיפת הרשת הארגונית של חברת הנפט הסעודית ולבסוף חדירה למחשבי בנקים מרכזיים בארצות הברית. מאמר זה מבקש לתת תמונה עכשווית באשר למספר מרכיבים בתהליך הפיתוח של איראן בסייבר. הראשון הנו ניתוח של האסטרטגיה האיראנית במרחב הסייבר. החלק השני מפרט את מענה הארגוני והאופרטיבי של איראן לאסטרטגיה שגובשה. חלק זה בוחן שלושה מרכיבים: תשתיות ההכשרה ופיתוח כוח האדם הטכנולוגי בתחום הסייבר, תהליכי התעצמות טכנולוגיים ולבסוף תהליכי בניין הכוח הכוללים בתחום הסייבר. לבסוף נבחנות מספר פעולות סייבר המיוחסות לאיראן מתוך הנסיון לגבש תובנות באשר לדרך בה מוליכה איראן את פעילותה בסייבר תוך הנסיון לבחון את הנגזרות מכך למדינת ישראל ולמדינות אחרות במערב.

האסטרטגיה האיראנית במרחב הסייבר

תפקידן של רשתות התקשורת והמידע בהתנעת המהומות שפרצו לאחר הבחירות לנשיאות ביוני 2009 ושל ארועי ה"אביב הערבי", יחד עם מתקפות הסייבר באיראן העניקו לזירה זו מקום מרכזי בתפיסת הביטחון הכוללת של המשטר האיראני. עדות לחשיבות הנושא בעיני מקבלי ההחלטות באיראן ניתן למצוא בהתייחסותו הישירה של המנהיג העליון ח'אמנאי להזדמנויות ולסכנות הטמונות במרחב הקיברנטי בעת הכרזתו על על הקמת "מועצת סייבר עליונה" במרץ 2012. מועצה אשר תורכב מבכירי השלטון, ותפעל לתכנון ויישום של אסטרטגיית פעולה אחידה ומוכללת לזירת הסייבר.[2] מועצה זו אומנם החלה את עבודתה לאחרונה, אך עם זאת ניתוח הפעילות האיראנית במרחב הסייבר בשנים האחרונות מצביעה על קיומה של אסטרטגיית סייבר איראנית בעלת מטרות ויעדים ברורים.

שני נדבכי יסוד עומדים בבסיס תפיסת הפעולה של איראן במרחב הסייבר. הראשון נוגע לפיתוח יכולות הגנה בפני מתקפות של מדינות וגורמים עויינים לצד פיתוח יכולות שיאפשרו לפעול מול מתנגדי המשטר מבית. ואילו הנדבך השני נוגע לפיתוח של יכולות התקפיות שיאפשרו לאיראן יכולת להתמודד התקפית מול מה שנתפס באיראן כעליונות ושליטה אמריקנית ביכולות ותשתיות האינטרנט הגלובליות.

בכל הקשור לתפיסת ההגנה, פועלת איראן להגשמת שתי מטרות מרכזיות בזירת הסייבר.[3] ראשית, איראן מבקשת ליצור מעטפת טכנולוגית, יעילה ומתקדמת, שתגן על תשתיות חיוניות ומידע רגיש מפני מתקפות סייבר כדוגמת מתקפת Stuxnet אשר פגעה בתוכנית העשרת האורניום האיראנית והשביתה יותר מ־1,000 צנטריפוגות במתקן ההעשרה בנתנאז.[4] שנית, אירן מבקשת לבלום ולסכל פעילות סייבר של גורמי אופוזיציה ומתנגדי משטר, עבורם מרחב הסייבר

מהווה פלטפורמה מרכזית לתקשורת, הפצת מידע וארגון פעולות כנגד המשטר. בנוסף לכך, המשטר מבקש למנוע חדירה של רעיונות מערביים ושל מידע הנוגד את האינטרסים שלו דרך מרחב הסייבר ובכך לבלום תהליכים של "מהפכה רכה" שתפגע באחיזתו במדינה וביציבותו. בהקשר לפיתוח היכולות ההגנתיות, יש לציין גם את הידיעות על התכנית האיראנית לייצר רשת תקשורת עצמאית ומבודלת.[5] ידיעות אשר לעיתים מוכחשות על ידי גורמים רשמיים איראניים[6] אולם ככל שנוקף הזמן נראה כי יש ממש בידיעות אלה.[7]

בהקשר למרכיב ההתקפי, אסטרטגיית הסייבר האיראנית רואה זירה זו בראש ובראשונה כזירה מרכזית במסגרת דוקטרינת הלוחמה הא־סימטרית, המהווה עיקרון מרכזי בתפיסת הפעלת הכוח האיראנית. לוחמת סייבר, בדומה לטקטיקות א־סימטריות קלאסיות יותר כגון טרור ולוחמת הגרילה, נתפסת בעיני איראן ככלי יעיל ואפקטיבי המאפשר לפגוע באופן משמעותי בעורפו של אויב בעל עליונות צבאית וגאו־אסטרטגית. מומחים בנושא מעריכים כי במקרה של הסלמה בקונפליקט הגרעין בין איראן לבין המערב, תחתור איראן להוציא לפעול מתקפת סייבר כנגד תשתיות מרכזיות כגון: תשתיות אנרגיה, מוסדות כלכליים, מערכות תחבורה ועוד, בתוך שטחה של ארה"ב.[8] מאמר מערכת בעיתון האיראני Kayhan ביולי 2011 (העיתון מזוהה עם ח'אמנאי) אף רמז לכוונה איראנית זו באומרו כי על ארה"ב להיזהר מפני תקיפה של שחקן "בלתי נודע במקום כול שהוא בעולם" על תשתיותיה החיוניות ביותר.[9]

בנוסף לרמה הצבאית־אסטרטגית, המשטר האיראני ותומכיו משתמשים בלוחמת התקפית במרחב הסייבר גם כדי לפגוע בפעילות הסייבר של מדינות מערביות ושל מתנגדי משטר באיראן. קבוצות האקרים איראניות, אשר לרוב אינן שייכות באופן רשמי לממסד אך בעלות קשרים אליו, יוזמות באופן קבוע מתקפות סייבר שונות כדוגמת, הפלת אתרי אינטרנט, החדרת תוכן פרו־איראני, גנבת מידע, הונאות אשראי, פגיעה בספקי שרות וניתוב מחדש של תנועה רשתית.[10] מימד פעולה נוסף אותו ניתן לייחס לפן ההתקפי של אסטרטגיית הסייבר האיראנית הוא המימד התעמולתי. המשטר האיראני מבין את חשיבותו של מרחב הסייבר בעיצוב התפיסות והשקפות העולם של קהלים רחבים בתוך איראן ומחוץ לה ומשקיע רבות ביצירת מערך תעמולה גדול ופעיל המאדיר את המשטר ופוגע ביריבו. על מנת לממש מטרות אסטרטגיות אלו משקיעה איראן משאבים לא מבוטלים ביצירת מארג צפוף, מיומן ורב שכבתי של יכולות סיכול, שליטה, ניטור ותקיפה במרחב הסייבר.

המענה הארגוני והאופרטיבי

כדי לממש את מטרותיה האסטרטגיות במרחב הסייבר, החלה איראן לפעול בנחישות לחיזוק יכולות הסייבר העומדות לרשותה. על פי דיווחים, החליטה איראן להשקיע כמיליארד דולר בפיתוח ורכש טכנולוגי ובגיוס והכשרת מומחים, אשר יקדמו ויחזקו את יכולותיה, ההגנתיות וההתקפיות, בזירת הסייבר.[11] מספר מרכיבים שלובים בתהליכי בניית המענה האופרטיבי והארגוני בתחום הסייבר: הראשון שבהם נוגע לבניית תשתית הכשרה ופיתוח של כוח אדם במכוני המחקר ובאקדמיה, השני נוגע למאמץ פיתוח טכנולוגי רחב היקף ואילו לבסוף לתהליכי בניין כוח הכוללים פיתוח דוקטרינה והקמה של ארגונים והסדרת סמכויות פעולה למימוש דוקטרינה זו.

הכשרה ופיתוח כוח אדם

תשתיות ההכשרה והפיתוח הטכנולוגי של מערך הסייבר האירני ממוקמים בראש ובראשונה באוניברסיטאות ובמכונים הטכנולוגיים הפרוסים ברחבי המדינה. באיראן רשת ענפה של מוסדות חינוך גבוהה ומחקר אקדמאי העוסקים במחקר והכשרה בתחומי טכנולוגיות מידע, הנדסת מחשבים ותקשורת.[12] בין מוסדות המובילים בתחום זה ראוי להזכיר את Sharif University of Technology, מוסד הממוקם בטהרן ומציע תארים מתקדמים בהנדסת מחשבים, הנדסת אלקטרוניקה ומתמטיקה.[13] האוניברסיטה מפעילה שני מכוני מחקר המתמקדים בטכנולוגיות תקשורת ומידע: Advanced Information and Communication Technology Center[14] ו־Advanced Communication Research Institute.[15] מוסד נוסף הראוי לאזכור בכול הקשור לתחום ביטחון המידע הוא Amirkabir University of Technology. אוניברסיטה זו, הממוקמת גם היא בטהרן, מפעילה מחלקה למתמטיקה ומדעי המחשב ומחלקה להנדסת מחשבים וטכנולוגית מידע. נראה כי במוסד זה קיימת התמקדות בנושא אבטחת המידע כאשר המחלקה להנדסת מחשבים מציעה מספר קורסים מתקדמים בביטחון מידע[16] ומפעילה מעבדה מחקרית המתמחה ביטחון מידע[17] ומעבדה לניתוח מערכות מאובטחות.[18]

פרט למחקר ולהכשרה במוסדות האקדמאיים, הממשל האיראני משקיע כספים רבים בקידום ותמיכה בחברות טכנולוגיה העוסקות בטכנולוגיות מידע ותקשורת מחשבים. ההשקעה האיראנית מתבצעת הן באופן ישיר על־ידי גופים ממשלתיים כגון משרד המדע והן דרך מימון והקמת חממות לתמיכה בחברות טכנולוגיה בהן לשלטון יש עניין.[19] גוף ממשלתי מרכזי בכול הקשור לטכנולוגיות מידע הוא מכון Iran Telecommunications Research Center, מכון המתמחה במחקר של טכנולוגיות מידע ותקשורת והינו הזרוע המחקרית והמקצועית של משרד המידע והתקשורת. המכון מפעיל ומכשיר צוותי מחקר מתקדמים בתחומים שונים ובכללם

אבטחת מידע.[20] גוף ממשלתי נוסף המקדם מחקר בתחום טכנולוגיות המידע הוא Technology Cooperation Office (TCO) המשתייך למשרד הנשיא ומטרתו המוצהרת היא לשפר את שיתוף הפעולה הטכנולוגי עם מדינות אחרות. הארגון מנחה ויוזם פרויקטים מחקרים בתחומים רבים ביניהם טכנולוגיות מידע.[21] גוף זה סומן על ידי האיחוד האירופאי וגופים אחרים במערב כמעורב בתוכנית הגרעין.[22]

בנוסף להשקעות ישירות מצד גופים ממשלתיים, הממשל האירני מפעיל גם חממות טכנולוגיות בהן מתבצע מחקר בתחום אבטחת המידע. בין מרכזי טכנולוגיה אלו ניתן למצוא את Paradis Technology Park המכונה "עמק הסיליקון האיראני". הפארק הוקם בשנת 2001 ביוזמת משרד הנשיא וה־TCO ופועלות בו מעל 40 חברות העוסקות בטכנולוגיות תקשורת ומידע.[23] חממה טכנולוגית נוספת היא Guilan Science and Technology Park, המהווה מרכז לתמיכה בחברות בתחילת דרכן ובו רשומות מספר חברות העוסקות בתחומי אבטחת מידע.[24]

התעצמות טכנולוגית

פרט לפיתוח והכשרת מערך סייבר חזק, איראן פעלה גם במישור הטכנולוגי בכדי לקדם את מטרותיה האסטרטגיות בזירת הסייבר. תחום אחד בו השקיעה אירן רבות הוא השליטה במרחב הסייבר הפנים מדינתי ובתנועות המידע בו. הממשל האיראני רכש ופיתח בשנים האחרונות מערכות טכנולוגיות מתקדמות המאפשרות לעקוב ולנתר את תנועות המידע ברשתות המחשבים והסלולר במדינה. חברת Telecommunication Co. of Iran, חברת הטלקומוניקציה הגדולה באיראן הנמצאת בשליטה ממשלתית, רכשה מחברת ZTE Corp הסינית מערכת מעקב המסוגלת לנטר מידע בקווי טלפון, רשתות מחשב וקווי סלולר. מערכת זו נקנתה כחלק מעסקה כוללת בין שתי החברות המוערכת בכ 130 מיליון דולר. העסקה כללה מוצרים ממערכת ZMXT, אותה מתארת ZTE כ־Integrated monitoring system. המוצרים שנרכשו על ידי איראן מאפשרים ניטור שמע, הודעות טקסט וגלישת אינטרנט.[25]

בנוסף לניטור ומעקב, המשטר האיראני פעל גם לפיתוח טכנולוגיות לחסימה וסינון של אתרים. מכיוון שמשטר הסנקציות מונע מאיראן רכישה של מסנני מידע מערביים, יזם הממשל פרויקט פנים־איראני של פיתוח טכנולוגיות סינון וחסימה. חברת Amnafzar, חברה לטכנולוגיות מידע בעלת קשרים למשטר, פיתחה טכנולוגית סינון מידע המכונה SEPAR. טכנולוגיה זו מתעדכנת באופן קבוע ומשנה את אסטרטגיית הסינון שלה לעיתים תכופות בכדי להתמודד עם ניסיונות עקיפה.[26] בעזרת טכנולוגיה זו הצליח המשטר להגביל מאד את זרימת המידע במדינה ולתוכה. מחקר של OpenNet Initiative (יוזמה משותפת של מספר מוסדות ביניהם אוניברסיטאות הרווארד וטורונטו) שהתפרסם במרץ 2009 מצא

את איראן כאחת המדינות המובילות בעולם בסינון וחסימת אתרים, לצד מדינות כגון סין, צפון קוריאה, סוריה ומיאנמר.[27]

טכנולוגיות אלו מעניקות לאירן שליטה הדוקה יחסית במרחב הסייבר המדינתי, אך עם זאת שאיפת המשטר היא שליטה אבסולוטית במידע, ברעיונות ובגישה למרחב הסייבר האיראני. על מנת להשיג שליטה כזו פתחה איראן בפרויקט הקמת רשת אינטרנט לאומית עצמאית, נבדלת מהרשת העולמית. לשיטה של איראן הקמת הרשת הלאומית המכונה Halal, תאפשר למשטר שליטה מלאה בתכנים אליהם נחשף הציבור, תפגע קשות במתנגדי המשטר אשר חלק גדול מפעולתם מתבצע ברשת ותקטין משמעותית את האפשרות לחדירת וירוסים ויישום מתקפות סייבר אחרות על תשתיות איראניות. פרויקט הרשת הלאומית החל לרקום עור וגידים ב 2009, כאשר הרשויות האיראניות הורו לחברות איראניות להעביר את פעילותן הרשתית לשרתים ולמרכזי מידע בתוך המדינה. במהלך 2012 הועלו דיווחים כי איראן מפתחת שרות דואר אלקטרוני פנימי, מערכת הפעלה עצמאית, מנוע חיפוש וכלים נוספים אשר מיועדים לשימוש ברשת החדשה.[28] באוגוסט האחרון הצהיר שר התקשורת האיראני, Reza Taghipour, כי איראן תתנתק מהרשת העולמית בתוך 18 חודשים.[29] אך עם זאת מומחים במערב קובעים כי המשטר באיראן יתקשה להתנתק באופן מלא מהרשת החיצונית.[30]

אירן מבקשת ליישם את אסטרטגיית בידול הרשתות, גם בסקטור הביטחוני ולהקים רשת תקשורת מודיעינית לאומית, אשר תהיה מנותקת מהרשת הגלובלית.[31] סנונית ראשונה של מאמץ זה היא Basir, רשת פנים־ארגונית של משמרות המהפכה שנחשפה במרץ 2012. ידיעות על הרשת מתארות אותה כמעין רשת סלולר סגורה שייתכן ומופעלת על ידי תחנות ממסר ייעודיות. הרשת אמורה לספק למשמרות המהפכה קווי תקשורת מוצפנים ויעילים גם בתרחיש של מתקפת סייבר כוללת על תשתיות התקשורת והמידע במדינה. לא ברור האם מדובר גם ברשת מידע או רק ברשת קולית.[32]

בניין כוח

באשר לתהליכי בניין הכוח בתחום הסייבר הרי שמערך ההכשרה והפיתוח הנרחב העומד לראשותה של איראן, אפשר לרפובליקה האסלאמית להקים מערך סייבר נרחב בעל יכולות מגוונות, הגנתיות והתקפיות כאחד. בעשור האחרון החלה אירן במהלך אסטרטגי של הרחבת מערך הסייבר הלאומי כאשר סוכניות וגופי סייבר הוקמו כמעט תחת כל סוכנות ממשלתית רלוונטית. מטרתה של איראן היא ליצור מערך ארגוני סייבר היררכי ומגוון בעל אסטרטגית פעולה ברורה, הקצאת משאבים מתוכננת, חלוקת תחומי אחריות ויכולות שימור והפצה של ידע ומידע.

גולת הכותרת של תהליך התעצמות הסייבר האיראני היא, כפי שהוזכר לעיל, הקמתה של "המועצה העליונה למרחב הסייבר". מועצה זו הוקמה במרץ 2012 בהוראת המנהיג העליון ח'אמנאי והיא מהווה את הסמכות הבחירה במדינה בכול הקשור למרחב הסייבר.[33] בתפקיד ראש המועצה מכהן נשיא איראן וחברים בה בין השאר בכירים כדוגמת מפקד משמרות המהפכה, ראש המג'לס, שרי המדע, התקשורת והתרבות, מפקד המשטרה ונשיא ארגון התעמולה האסלאמית. בסמכות המועצה לקבוע את מדיניות הסייבר הלאומית והנחיותיה מחייבות את כלל הגופים האיראניים הפועלים בתחום. תחת המועצה מתוכנן לקום "מרכז סייבר לאומי" אשר ייתכלל את כלל פעילות הסייבר האיראנית, ירכז ויפיץ מידע והנחיות וייפקח על מילוי הוראות המועצה על ידי כלל הגופים הרלוונטיים.

מערך הסייבר האיראני מורכב ממספר רב של ארגוני סייבר המשתייכים באופן פורמאלי לגופי ממסד שונים והינם בעלי תחומי פעילות שונים. ארגון מרכזי אחד, בעל אורינטציה ההגנתית בעיקרה הוא "מפקדת הגנת סייבר", הפועלת תחת "ארגון ההגנה הפאסיבית של אירן" המשויך למטה הכללי של הכוחות המזויינים.[34] לצד אנשי צבא, בארגון סייבר זה חברים גם נציגים ממשרדים ממשלתיים, כגון משרדי התקשורת, ההגנה, המודיעין והתעשייה ומטרתו המרכזית היא לפתח דוקטרינת הגנה מקיפה למוסדות ותשתיות המדינה כנגד איומי סייבר.[35] הגוף הינו הגנתי בעיקרו ונכון להיום לא נראה כי הארגון עסק בפעילות סייבר התקפית. גוף סייבר נוסף בעל אופי הגנתי הוא מרכז אבטחת המידע המכונה "MAHER" שהוקם ופועל תחת המשרד לתקשורת וטכנולוגיות מידע. המרכז אחראי בראש ובראשונה על הפעלה של צוותי תגובה מהירה (Computer Security Incident Response Teams) במקרה של אירועי חירום ומתקפות סייבר. בנוסף לכך המרכז מכשיר כוח אדם מיומן, מפתח דרכי פעולה לטיפול במשברי סייבר ומהווה מרכז לאגירה ולהפצה של ידע בתחום אבטחת מידע. באחריות המרכז להגן על כלל אתרי האינטרנט הממשלתיים כמו גם על אתר חברות פרטיות אשר פעולות באופן רשמי ורשומות במשרד התקשורת. צוותי המרכז הם אלו שהופעלו על מנת לבלום ולסכל את פעולותיהם של תוכנות Flame ו־Stuxnet שתקפו באיראן.[36]

ארגוני סייבר נוספים הפועלים באיראן מתמקדים בשליטה ובאכיפה כנגד פעילות סייבר פנים־איראנית הנוגדת את האינטרסים של המשטר. ביולי 2009 הוקמה על ידי "המועצה הגבוהה למהפכה תרבותית" הכפופה למנהיג העליון ה"וועדה לזיהוי אתרים בלתי מאושרים". בוועדה זו חברים בין השאר התובע הכללי, מפקד המשטרה, ראש כלי התקשורת הממשלתיים ושרי ממשלה שונים (מודיעין, תקשורת, תרבות מדע ועוד). באחריות הוועדה לאתר אתרי אינטרנט אשר תוכנם ופעילותם אינן עולות בקנה אחד עם דרישות ורצונות המשטר ובסמכותה להורות על חסימת גישה לאתרים אלו.[37] ב־2011 הוקמה יחידת סייבר

משטרתית, FETA [38] משימתה העיקרית של יחידה זו היא להתמודד עם פשעי אינטרנט: הונאה, גנבת מידע, איומים וכדומה אך באחריותה לפעול גם כנגד פשעים פוליטיים וביטחוניים במרחב הסייבר, משימה אשר בפועל מהווה את עיקר פעילותה.[39] בנוסף לכך FETA אחראית גם על ניטור, מעקב ושליטה במשתמשי האינטרנט באיראן, תוך דגש על משתמשי ה"אינטרנט קפה" הפרוסים ברחבי המדינה ומאפשרים גלישה אנונימית במידה מסוימת.[40]

בכל הקשור ליכולות ההתקפיות של מערך הסייבר האיראני התמונה הרבה פחות שקופה וברורה. באופן טיבעי, משמרות המהפכה הינם השחקן המרכזי בכל הקשור להקמה והפעלה של מערך סייבר התקפי. מומחי סייבר במערב קובעים כי יכולות הסייבר של משמרות המהפכה מציבות את איראן בין המדינות המתקדמות בעולם בכול הקשור ללוחמת סייבר.[41] ניתוח של מכון המחקר Defense Tech מ־2008,[42] העריך כי מערך הסייבר של משמרות המהפכה מעסיק כ 2,400 אנשי צוות והינו בעל תקציב של 76 מיליון דולר (נכון לאותה תקופה). בין יכולות לוחמת הסייבר אותן מייחס המכון למשמרות המהפכה ניתן למצוא: פיתוח תוכנות מחשב נגועות ע"י השתלה של קוד זדוני בתוכנות מחשב מזוייפות. פיתוח יכולות חסימה לרשתות תקשורת מחשבים ורשתות Wi-Fi. פיתוח קוד מחשב זדוני (וירוסים ותולעות מחשב) המסוגלים להפיץ עצמם ברשתות ולפגוע במחשבי יעד. כלים לחדירה למחשבים ולרשתות כדי לאסוף מודיעין ולהעבירו לשרתים מרוחקים. ולבסוף פיתוח של כלים שוהים המותקנים במחשבי היעד והמופעלים בצורה מושהית או לפי פקודה משרתי שליטה.

בנוסף ליכולות לוחמת המידע, משמרות המהפכה גם פועלים ליצירת מערך לוחמה אלקטרונית בעל יכולות לחסימת מערכות מכ"ם ותקשורת. הארגון משקיע רבות ברכישת מערכות לוחמה אלקטרונית,[43] אשר בשילוב עם יכולות לוחמת סייבר יהוו כלי אפקטיבי לפגיעה במערכות האלקטרוניות של ארצות הברית ובנות בריתה בעת עימות צבאי.[44] על פי הצהרות של משמרות המהפכה עוצמתה של אירן בתחום לוחמת הסייבר באה לידי ביטוי בלכידת מטוס הריגול הבלתי מאויש של ארצות הברית בדצמבר 2011.[45]

פרט ליחידות לוחמת הסייבר האורגניות, ישנן עדויות גם לקשרים בין משמרות המהפכה לבין קבוצות האקרים איראניות הפועלות כנגד אויבי המשטר בתוך איראן ובעולם. השימוש ב"מיקור חוץ" מאפשר למשמרות המהפכה ולאירן לשמור על ריחוק ולהתכחש להאשמות בדבר מעורבותה של איראן בלוחמת ופשיעת סייבר. קבוצת האקרים איראנית אחת, אשר מומחים רואים אותה כבעלת קשרים למשמרות המהפכה, היא Ashiyane Digital Security Team.[46] חברי קבוצה זו מונעים על ידי תפיסות אידיאולוגיות התומכות במשטר האיראני ובמהפכה ומכוונים את התקפותיהם כנגד אויבי המשטר. קבוצת Ashiyane מאמנת האקרים

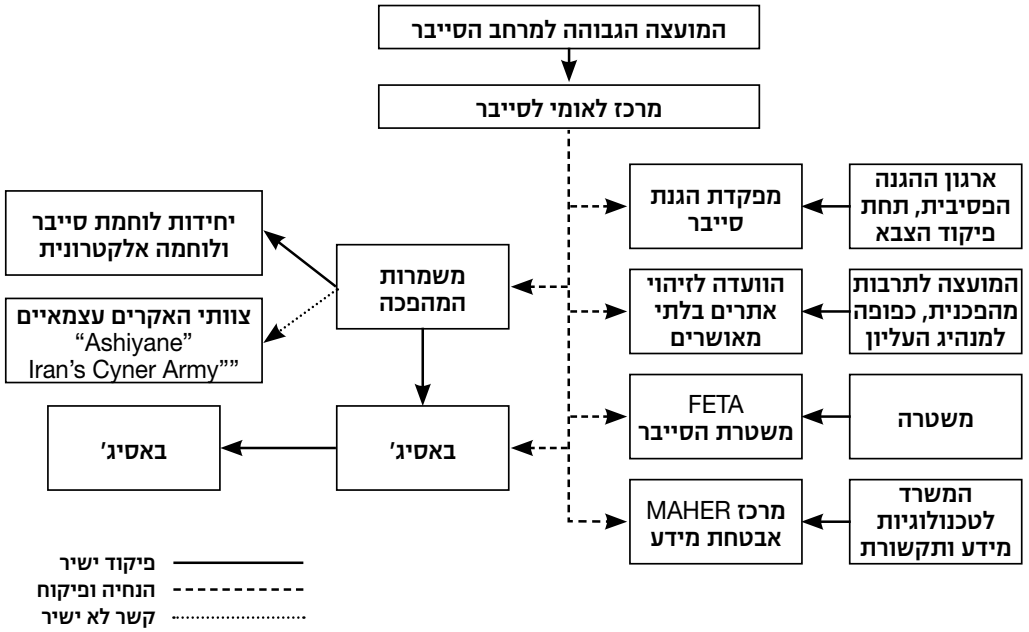
ומקנה להם יכולות גבוהות,[47] אשר מנוצלות לאחר מכן הן לפעילות פוליטית הכוללת הפלה והחדרה של תעמולה פרו־איראנית לאתרים מערביים וישראליים, והן לפשיעת סייבר (הונאות אשראי, גנבת זהות ופריצה למאגרי מידע ומוסדות פיננסיים). בנוסף לכך הקבוצה מקיימת פורום בשם War Games בו היא עורכת תחרויות פריצה בין האקרים כאשר בין המטרות ניתן למצוא בין השאר חברות תשתיות אמריקאיות.[48]

קבוצה האקרים נוספת הנתפסת כבעלת קשרים למשמרות המהפכה היא Iran's Cyber Army.[49] הארגון מורכב מהאקרים ומומחי מחשבים אשר פועלים תחת זהות בדויה ומכריזים על עצמם כשייכים לארגון. פעולותיו העיקריות של צבא הסייבר האיראני כוללות: פריצה והחדרת תוכן פרו־איראני לאתרים מערביים, השתלטות על תעבורת מידע ותיעולה מחדש, פריצה לחברות ביטחון מידע מערביות ופגיעה באתרים של מתנגדי משטר.

גם ארגון הבאסיג', הכפוף למשרות המהפכה, הפך לפעיל בזירת הסייבר עם הקמתה ב־2010 של "מועצת הסייבר של הבאסיג'". פעילות הבאסיג' מתמקדת בראש ובראשונה ביצירת תעמולה פרו־איראנית במרחב הסייבר. הבאסיג' מגייס ומדריך אלפי איראניים בכתיבת תוכן ולאחר מכן מפעיל כיתות מחשבים מאורגנות מהן הפעילים מפעילים עשרות אלפי בלוגים התומכים במשטר וכן מעלים תגובות וחומרים בעד השלטון ברשתות חברתיות, פורמים ואתרים מרכזיים באיראן ומחוץ לה.[50] עם זאת הבאסיג' מבקש לפתח גם יכולות סייבר מתקדמות יותר ומשתמש במדריכים מתוך יחידות הסייבר של משמרות המהפכה על מנת להכשיר האקרים בעלי יכולות תקיפה גבוהות.[51]

אם כן, ניתן לראות כי בשנים האחרונות הקימה איראן מערך סייבר נרחב, המקיף תחומי פעילות רבים והינו בעל יכולות מגוונות. התרשים הארגוני להלן מתאר את המבנה ההיררכי של מערך הסייבר במדינה כפי שהוא עולה מתוך הניתוח לעיל:

ניתן לראות התקדמות משמעותית בפיתוח תחום הסייבר באיראן. בתחום ההגנתי פועלת איראן במלא המרץ לייצר יכולות הגנה ובידול כדי להתמודד מול נסיונות חדירה לרשתות ותשתיות חיוניות במדינה. קשה לספק תמונה אמינה בהקשר לפיתוח היכולות ההתקפיות בתחום הסייבר. החלק הבא במאמר בוחן מספר פעולות כאלה.



פעולות סייבר המיוחסות לאיראן

בדצמבר 2011 הובילה חשיפה של תכונית תחקירים של רשת הטלוויזיה Univision לחקירה אמריקאית בדבר מעורבות גורמים איראניים רשמיים במזימת סייבר כנגד ארצות הברית. תחקירני הרשת, שהצליחו להסתנן לתוך קבוצת פצחנים מקסיקנית שפעלה כנגד מטרות אמריקאיות, צילמו בסתר פגישה בין נציגי הקבוצה לבין שגריר איראן במקסיקו. בפגישה שנערכה בשגרירות, ביקשו הראשונים לבדוק את האפשרות לקבלת תמיכה ומימון מממשלת איראן לטובת ביצוע מתקפות סייבר כנגד מטרות אמריקאיות ביניהן הפנטגון, ה־CIA, ה־FBI ומתקני גרעין בתחומי ארה"ב. בצילומים נראה השגריר האיראני במקסיקו דאז, מוחמד חסן גהאדרי, שואל שאלות ואף מציע דרכי פעולה אפשריות נוספות. השגריר הדגיש שאיראן מבקשת להשיג מידע מודיעיני לגבי האפשרות של תקיפה אמריקאית כנגדה ובסוף השיחה ביקש לשמור על קשר והבטיח להעביר ההצעה לממונים עליו.[52] ניתן להניח שנסיון זה לא היה בודד וכי איראן פועלת לגייס בעולם גורמים שיוכלו לשרת את מטרותיה ההתקפיות במרחב הסייבר.

קביעה וודאית של זהות תוקפים במרחב הסייבר הנה פעולה מורכבת המחייבת הקצאה של משאבים רבים ושיתוף פעולה בין לאומי. לכן קשה לקבוע בוודאות מי עומד מאחורי פעולות רבות במרחב הסייבר. למרות זאת, ניתן במקרים רבים ובאמצעות תבחינים נסיבתיים, לקבוע ברמה גבוהה של וודאות את העומד מאחורי הפעילות. במסגרת מאמר זה נבחנו שלוש פעולות. הראשונה הנה תקיפה של שתי חברות אבטחה למטרת גנבה של הרשאות אבטחה באינטרנט, השניה

נוגעת תקיפת מוסדות פיננסיים גדולים בארצות הברית והאחרונה הנה תקיפת חברת הנפט הסעודית Aramco.

מתקפה על חברות DigiNotar ו־Comodo

במהלך שנת 2011 בוצעו שתי מתקפות על חברות המספקות הרשאות SSL.[53] הראשונה על חברת Comodo מארצות הברית והשניה על חברת DigiNotar מהולנד. חברת האבטחה האמריקנית Comodo הותקפה במהלך חודש מרץ 2011. במהלך התקיפה נגנבו מספר הרשאות בהן הרשאות לתחומים (domain) של שרותי דואר אינטרנטיים דוגמת Google. אולם אלה בוטלו טרם שנעשה בהן שימוש על ידי הגורם התוקף. למעשה גורם המקבל אישור לתחום mail.google.com, יוכל לגנוב סמאות של Gmail ולחטוף חשבונות של משתמשים. כך גם מי שמקבל אישור מזוייף לתחום Microsoft.com יוכל להתקין תוכנות זדוניות במחשבי הקורבנות. מדיווח של החברה על הארוע עולים הממצאים הבאים:[54]

1. תקיפה זו נעדרה מאפיינים של פשיעת סייבר.
2. התוקפים היו מאורגנים וידעו במדוייק ומראש את מבוקשם. דבר המצביע על מעורבות של ארגון מדינתי בתקיפה.
3. מקור המתקפה היה בעיקר מאיראן (לפי זיהוי כתובת IP).
4. אתר האינטרנט בו נבדקו ההרשאות הגנובות מוקם באיראן והורד מהרשת מיד אחרי גילוי המתקפה על ידי חברת Comodo.

תקיפת חברת Comodo לא הצליחה להשיג את מטרתה. ההתקפה זוהתה וטופלה טרם שנעשה שימוש בהרשאות הגנובות. שונה היה המצב בחברת DigiNotar ההולנדית. מאגרי החברה שהייתה הרשות המרכזית בהולנד להרשאות SSL, הותקפו במהלך החודשים יוני עד ואוגוסט 2011. במהלך התקיפה, שקבלה את הכינוי "טוליפ שחור", נגנבו תעודות המשמשות לאימות אתרים כולל תעודה המשמשת לאימות שם התחום google.com המאפשרת לתוקף התחזות וניתוב מחדש של שרתי Gmail.[55]

ניתוח שהזמינה חברת DigiNotar (שבשל הארוע הזה פשטה את הרגל וחדלה מלהתקיים) הראה שנגנבו 531 תעודות מזוייפות ושעיקר השימוש בהרשאות הגנובות היה לצרכי חדירה לחשבונות מייל של משתמשים בעיקר באיראן. הניתוח הראה שהתקיפה אפשרה חדירה למעל ל 300,000 מחשבים רובם המכריע באיראן (מעל 99%).[56] קשה לקבוע בוודאות את מקור התקיפה אולם, לדעת מומחים, מקורה באיראן והיא נועדה ככל הנראה לצרכי בטחון פנים במדינה.[57] זאת בעיקר בשל הסיבות הבאות: יעדי המתקפה והיקף המשתמשים הרב שהותקפו, הודעות שהושארו באתר החברה שהצביעו על מעורבות של איראנים בפעולה.

מתקפה על מוסדות פיננסיים בארצות הברית

דיווח שהופץ בארצות הברית בחודש ספטמבר 2012, מעלה כי סמוך למועד זה הותקפו מספר מוסדות פיננסיים בארצות הברית בהם אתרים השייכים לבנק של אמריקה (Bank of America), לבנק מורגן צ'ייס ולבנק סיטיגרופ. להערכת גורמים בארצות הברית התקפות הסייבר כנגד מוסדות פיננסיים אמריקאים לא נערכו על ידי פצחנים אקראיים כי אם מומנו ככל הנראה על ידי איראן והיו בתגובה לסנקציות שהוטלו על המדינה על ידי ארצות הברית.[58]

בעקבות זאת, מרכז לניתוח ושיתוף מידע פיננסי בארצות הברית[59] פרסם התראה לבנקים בארצות הברית כנגד תקיפות סייבר שמטרתן גניבת זהויות באמצעות דואר אלקטרוני, סוסים טרויאנים וכלים זדוניים המסוכלים לקלוט הקשות מקלדת. כל זאת כדי לחלץ שמות של משתמשים, עובדים וססמאות. אף שגם בנקים גדולים הותקפו, רוב הקורבנות של תקיפות אלה היו עסקים קטנים ובינוניים, בנקים קטנים וחברות אשראי. קבוצה הקרויה "לוחמי הסייבר של עז א־דין אל קאסם" הודיעה שהיא תקפה את הבנק של אמריקה (BofA) ואת הבורסה של ניו יורק בתגובה לסרט שפגע במוחמד ושהתפרסם בתחילת ספטמבר 2012. ההתקפות אלה, כפי שתוארו בהתראה, מצביעות על כך שהתוקפים הצליחו להשיג מידע רב וגישה לרשתות הבנקים לפחות במספר מקרים כמו גם הצליחו התוקפים להשיג אישורי כניסה מעובדי בנק ולעקוף את מנגנוני ההגנה.[60]

מתקפה על חברת Aramco

במהלך אוגוסט 2012 וככל הנראה תוך סיוע פנימי של גורם בעל נגישות גבוהה למחשבי החברה, הותקפו כ 30,000 מחשבים של חברת Aramco הסעודית ועל מחשבי חברת הגד מקטאר ResGas. ההתקפה בוצעה באמצעות וירוס מחשב הידוע בשם Shamoon. לדעת מומחים זוהי אחת ההתקפות ההרסניות ביותר שנערכה כנגד חברה אחת. וירוס המחשב התפשט דרך שרתי מחשבי החברה ופגע במידע שנשמר בהם. מומחי החברה טוענים שהנזק היה מוגבל למחשבים משרדיים ולא השפיע על מערכות התפעוליות ומערכות הבקרה.[61]

חברת סינמטק זיהתה לראשונה בחודש אוגוסט 2012 את הוירוס. בניתוח שערכו גורמים בחברה ובחברות אבטחה נוספות עלו כמה ממצאים:[62]

1. וירוס Shamoon נועד לתקוף מחשבים במערכת המחשוב הארגוני (IT) ולא מחשבי מערכות בקרה. וירוס זה אינו שייך לקטגוריה של כלי לוחמת סייבר מתוחכמים דוגמת Stuxnet שתקף את תכנית הגרעין של איראן בשנת 2010.
2. מטרת התקיפה של הוירוס לא הייתה ריגול או איסוף מידע כי אם השמדה מוחלטת של נתונים ופגיעה במחשבי היעד.

3. כותבי הקוד המפגע אינם נראים כשייכים לעילית התחום (דוגמת כותבי קוד Stuxnet או להבה). קיימים ממצאים המראים שהגורמים העומדים אחרי כתיבת הקוד אינם מתכנתים בעלי פרופיל מקצועי גבוה במיוחד ושבקוד הושארו שגיאות קידוד רבות. אולם אלה היו מספיק מיומנים לייצר קוד הרסני במיוחד.
4. הוירוס הוחדר למחשבי החברה באמצעות משתף פעולה מתוך החברה, אשר הינו בעל גישה ישירה למערכת ואשר עשה שימוש ככול הנראה בהתקן USB על מנת להחדיר את הוירוס לתוכה.
5. כותבי הקוד עשו שימוש בחלק מתמונת דגל אמריקני שרוף כדי להסתיר את תוכן הקבצים במחשבים הנגועים. פעולה המראה על שיוך פוליטי אות דתי איסלאמי מסויים של כותבי הקוד.
6. בקוד של מכניזם המחיקה של ה־Shamoon הטמיעו מפתחי הוירוס את השם Wiper, כינוי דומה מופיע בקוד הוירוס Flame, שתקף את מחשבי חברת הנפט האיראנית. הקבלה זו מעלה את החשד כי המתקפה על Armco הינה פעולת תגמול איראנית בתגובה למתקפת Flame.

קבוצה בשם חרב הצדק (The Cutting Sword of Justice), לקחה אחריות על התקיפה וטענה שהתקיפה באה כנגד מקור ההכנסה העיקרי של ערב הסעודית שהואשמה בביצוע פשעים במדינות כגון סוריה ובחריין. עוד טענה הקבוצה שוירוס המחשב איפשר להם גישה לסודות רבים. אולם נכון לכתיבת שורות אלה טרם פורסם כל מידע רלבנטי בנושא. דיווחים על התקפות דומות על חברות נפט וגז באיזור המפרץ העלו את החשד שתקיפות אלה היו חלק ממהלך רחב של מדינה. מדברים שאמר שר ההגנה האמריקני ליאון פאנטה לאחרונה הוא רמז על מעורבות איראנית בתקיפה. בכיר לשעבר בממשל האמריקני היה גלוי יותר כשאמר שהממשל מאמין שאיראן עומדת מאחורי המתקפות במפרץ הפרסי.[63]

ניתוח שערך מומחה האבטחה Jeffrey Carr[64] מארצות הברית מעלה מספר טיעונים הקושרים את איראן למתקפה זו. איראן הנה המדינה היחידה שלה נגישות לקוד המקור Wiper ממנו נוצר ככל הנראה הוירוס Shamoon. לפי הדיווח של חברת קספרסקי[65] הקוד Wiper בו נעשה שימוש לתקוף את משרד האנרגיה האיראני באפריל 2012, שימש את יוצרי Shamoon. לאיראן מוטיבציה גבוהה לתקוף את חברת הנפט הסעודית בשל העיצומים המחריפים על איראן בתחום האנרגיה. בנוסף, נבדק חשד לקשר של ארגון חיזבאללה עם התקיפה. מספר עובדים לבנוניים של חברת Aramco נעצרו ונחקרו בהקשר זה.

תובנות מסכמות

פיתוח יכולות הסייבר של איראן צריך להטריד את ישראל וכמובן גם את ארצות הברית כמו גם מדינות נוספות במערב. בעקבות תעוזת נסיון החיסול של שגריר

ערב הסעודית בארצות הברית, מציעים מומחים בארצות הברית לא לזלזל בכוונות וביכולות האיראניות להעיז ולתקוף תשתיות קריטיות בארצות הברית. כמו שאר העולם, ניתן להניח שגם איראן שהיתה קורבן לאחת ממתקפות הסייבר ההרסניות ביותר, למדה היטב את לקחי תקיפת Stuxnet והיא מבינה את הפוטנציאל ההרסני הגלום בפיתוח כלי תקיפה שיוכלו לפגוע במערכות בקרה תעשייתיות ולגרום כך לנזק פיזי.

פיתוח האסטרטגיה האיראנית ותהליכי בניין הכוח שבאו בעקבותיה מצביעים על התארגנות שיטתית להוות שחקן משמעותי בתחום לוחמת הסייבר. מומחים מדווחים על התקדמות מתמדת ביכולות הסייבר ובמבצעי הסייבר של איראן. ראוי יהיה להקשיב לדברי אחד מהם שאמר לאחר דיווח על מתקפת סייבר על מוסדות בנקאיים בארצות הברית המיוחסת לאיראן: "[תכנית הסייבר של איראן] דומה לתכנית הגרעין, היא אינה מתוחכמת במיוחד אבל מתקדמת כל שנה."[66] אין לזלזל ביכולות הטכנולוגיות של איראן. התשתית המדעית במדינה מפותחת ומאגר ההון האנושי רב. לכן, ניתן להעריך שבתוך תקופה לא קצרה תוכל אירן להוות גורם משמעותי ברמה העולמית בתחום זה. הערכה זו מקבלת חיזוק מהמתקפה על מחשבי חברת Armco בעקבותיה אמר James A. Lewis, מומחה לביטחון סייבר שאיראן הייתה מהירה יותר בפיתוח יכולות התקפיות ונועזת יותר בהפעלה שלהן משניתן היה לצפות.[67] בדרך כלל, הפעילות שנחשפת הנה קצה הקרחון לפעילות בלתי גלויה נוספת. מצד שני, שכלול ההגנה של איראן מחייב את הגורמים בעלי העניין להתארגן לפעולה בסביבה של רשתות מבודלות או אף רשת תקשורת איראנית מבודלת מרשת האינטרנט. אף כי האתגר בהקמה של רשת שכזו ובבידולה המוחלט הנו עצום, הרי שניתן לאתר דרכים לפעול גם בסביבה שכזו. תפיסת הגנה זו, תהווה אתגר לא מבוטל לגורמים להם עניין בביצוע מהלכים במרחב הסייבר באיראן.

מתוך הפעולות המיוחסות לאיראן שתוארו לעיל, ניתן לגזור מספר תובנות. הנסיון האיראני להשיג הרשאות SSL מצביע על פעילות למול קבוצות גדולות של אזרחים ופחות למול יעדים ממוקדים דוגמת מדינות או חברות וארגונים. ככל הנראה הדבר נוגע לצרכי זיהוי ומעקב על גורמים פנימיים באיראן. אולם הנסיון הנצבר בפעילות מסוג זה יאפשר פעילויות גם מול יעדים ממוקדים יותר דוגמת ארגונים ומדינות. ראוי לציין שאף כי הפעילות שנחשפה מצביעה על ארגון ושיטתיות, הרי שנדמה שאיראן טרם חצתה את הרף הטכנולוגי והארגוני כדי להוות גורם בעל תחכום רב. אולם, המוטיבציה האיראנית יחד עם תהליכי בניין הכוח והיכולות הטכנולוגיות במדינה יאפשרו לה לצעוד לכיוון זה במהירות רבה.

תקיפת חברת Aramco מעלה מספר תובנות. הראשונה שבהם נוגעת לעובדה שההגנה הקלאסית מפני איומים המגיעים דרך רשת האינטרנט אינה מספקת.

רוב המומחים מקבלים את ההנחה שהחברה לא חסכה השקעות בהגנה מפני איומים המועברים דרך רשת האינטרנט. הוירוס ההרסני לא התגלה על ידי מערכות ההגנה, והוחדר ככל הנראה על ידי גורם פנימי בחברה שהיה בעל הרשאה מתאימה. מערכות ההגנה הקיימות והסטנדרטיות אינן בנויות לספק הגנה מפני איומים ממוקדים (APT) וקוד זדוני לא מוכר (zero date ואחרים). לכן גדל הצורך לפתח כלים שיוכלו לספק הגנות טובות יותר בפני איומים שכאלה. אחד הכיוונים המתפתח הנו כלים שיתבססו על זיהוי, חסימה ונטרול של התנהגות אנומאלית ובלתי רצוייה במחשבים מותקפים. כלים שכאלה יוכלו לנטרל איומים גם אחרי שהקוד הזדוני הצליח לחדור למחשב היעד. התובנה השניה נוגעת למטרות התקיפה שנועדה בעיקר להשמיד מידע באופן גורף וללא אבחנה בעשרות אלפי המחשבים של חברת הנפט הסעודית ופחות (אם בכלל) כדי לאסוף מידע. אם פעילות מודיעין במרחב הסייבר יכולה להחשב בחלק מהמקרים כלגיטימית הרי שתקיפה רחבת היקף שכזו על ידי איראן על מטרה אזרחית מסמנת מעבר של איראן לפעולות גמול. הדבר צריך להטריד את האחראיים על ההגנה במדינות רבות. דבריו של שר ההגנה ליאון פאנטה על הצורך לבוא חשבון גם הגורמים העומדים מאחורי התקיפה הזו ממחישים זאת.[68] אולם, מה שיקבע יהיה מבחן המעשה ולא מבחן המילים.

כמי שנפגעה מהתקפת הסייבר ההרסנית ביותר עד כה ניתן להעירך שאיראן מבינה היטב את הפוטנציאל הגלום בתחום זה ותפעל לפתח יכולות כאלה משל עצמה בעתיד. לאור זאת, תהליכי בניין הכוח השיטתיים שפורטו לעיל, יובילו את איראן, תוך זמן לא רב להוות שחקן משמעותי בשדה הקרב הקיברנטי לתקיפה של תשתיות חיוניות במדינות העויינות את איראן בהן: ארצות הברית וישראל. זאת תוך יצירה של בידול ככל האפשר במקרה של חשיפה וגילוי הפעילות. איראן מפעילה קהילות של פצחנים "אזרחים" תוך נסיון ליצור בידול בין אלה לבין הממשל והארגונים האיראניים. גישה זו, דומה למתרחש במקומות נוספים בעולם דוגמת סין ורוסיה, מאפשרת למדינות להתנער מאחריות ולגלגל את המעשה לפתחם של אזרחים. כך, ימשיך להיות קושי רב בשיוך פעולות הסייבר ההתקפיות למדינה האיראנית.

מיקוד פעילות הסייבר של איראן בישראל ובמדינות מערביות אחרות, מחייב התארגנות הגנתית ייעודית. נדרשת תפיסה עדכנית בכל הקשור להגנות במרחב הסייבר. התחכום של התקופים מחייב לצד הגנות גנריות גם פעילות הגנה המבוססת מודיעין. כך גם, ולאור תהליכי ההתפתחות של איראן, חייבת מדינת ישראל להציב את תחום הסייבר האיראני במקום גבוה בצי"ח המודיעיני והפעילות המסכלת. זאת כדי לאתר מבעוד מועד התארגנויות לפעולות התקפיות ולסכלן מבעוד מועד. בדומה לתכנית הגרעין האיראנית, האתגר אינו רק של מדינת ישראל

אלא של מדינות רבות נוספות במערב כמו גם מדינות המפרץ. ההתקפה על מחשבי חברת Aramco תעיד על כך. לכן יש ליזום שיתוף פעולה בין מדינתי רחב ככל האפשר בתחום המודיעין והסיכול לפעולות סייבר איראניות.

לצד זאת, על מדינת ישראל להמשיך ולבנות מענה הגנתי אפקטיבי. מענה זה צריך להתמקד בשלושת שכבות הסייבר הרלבנטיות במדינה: הראשונה הנה שכבת ארגוני הבטחון הנדרשים לבחון באופן קבוע את החשיפה ליכולות הסייבר של איראן ולוודא שאלו לא מצליחים לפעול ולפגוע ביכולות חיוניות של מערכת הבטחון. השכבה השניה נוגעת למערך התשתיות החיוניות במדינה המונחות על ידי הרשות לאבטחת מידע מתוקף החלטת ממשלה. גם כאן האתגר מחייב פעילות מתמדת בייחוד בכל הקשור להבנת תמונת האיום, ולשיתוף של מידע בין גורמים שונים וגזירת המענה המתאים לאיום הזה. ולבסוף אין לזלזל ביכולות האיראניות לנסות ולפגוע בעסקים ותעשייה שאינם מונחים על ידי כל גורם במדינה. עסקים ותעשייה בסקטור הפרטי פועלים ברוב המקרים בעיקר להגן על נכסי המידע שלהם וקשה לדרוש מהם להתגונן בפני האפשרות שיותקפו במרחב הסייבר על ידי מדינה זרה דוגמת איראן. לכן, חשיבותו הקריטית של המטה הקיברנטי הלאומי כגורם המתכלל ומי שיכול לקדם תהליכי אסדרה ושיתוף מידע ומודיעין בקשר למפת האיומים המתפתחת.

הערות

1 Art Keller, "The Great Persian Firewall, Should we care that Iran just turned off Google?" *Foreign Policy*, September 28, 2012, http://www.foreignpolicy.com/articles/2012/09/28/Iran_firewall_google?page=full

2 הצהרתו של ח'מאנאי בעת ההכרזה על הקמת המועצה באתרו הרישמי: http://farsi.khamenei.ir/message-content?id=19225

3 Ilan Berman, *The Iranian Cyber Threat to the U.S. Homeland*, Statement before the U.S. House of Representatives Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies and Subcommittee on Counterterrorism and Intelligence, April 26, 2012, pp.1-3, http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20-%20Berman.pdf

4 CBS News, *Iran Confirms Stuxnet Worm Halted Centrifuges*, November 29, 2010, http://www.cbsnews.com/stories/2010/11/29/world/main7100197.shtml

5 Kevin McCaney, *Iran building a private, isolated Internet, but can it shut out the world?,* CGN, April 10, 2012, http://gcn.com/articles/2012/04/10/iran-building-separate-isolated-internet.aspx

6 Agence France Presse, *Iran denies has plan to cut Internet access*, AFP April 10, 2012, http://www.google.com/hostednews/afp/article/ALeqM5h4e57x6CYbsavza1PeDuQP7Bf9Vg

7 Amir Taheri, *Iran will launch its national internet next week but not for the reasons*

you might think, September 20, 2012
http://www.opednews.com/articles/Iran-will-launch-its-natio-by-Amir-Taheri-120919-83.html

8 Brian Ross, *What Will Happen to the US If Israel Attacks Iran?* ABC News, March 5, 2012,
http://abcnews.go.com/Blotter/israel-attacks-iran-gas-prices-cyberwar-terror-threat/story?id=15848522

9 Ilan Berman, p. 4

10 National Iranian,Reza Marashi, *The Islamic Republic's Emerging Cyber War* American Council ,April 30, 2011,
http://www.niacouncil.org/site/News2?page=NewsArticle&id=7318

11 Yaakov Katz, *Iran embarks on $1b. cyber-warfare program*, The Jerusalem Post, December 18, 2011,
http://www.jpost.com/Defense/Article.aspx?id=249864

12 Patterson, J.P & M.N. Smith, *Developing A Reliable Methodology for Assessing the Computer Network Operations Threat of Iran*, Master's Thesis, Monterey, CA: Naval Postgraduate School. 2005. pp. 17-22, www.fas.org/irp/eprint/cno-iran.pdf

13 אתר אוניברסיטת שריף http://www.sharif.ir/web/en

14 http://www.aictc.com/web/content/main

15 http://acri.sharif.ir/en/Default.asp

16 פרוט הקורסים התמקדמים. http://ceit.aut.ac.ir/autcms/courses/courseOfferingView.htm?level=M.Sc&depurl=computer-engineering&lang=en&cid=70317

17 אתר המעבדה לביטחון מידע /http://ceit.aut.ac.ir/autcms/labs/verticalPagesAjax/labHome.htm?id=3350532&depurl=computer-engineering&lang=en&cid=147776

18 אתר המעבדה למערכות מאובטחות /http://ceit.aut.ac.ir/autcms/labs/verticalPagesAjax/labHome.htm?id=3369580&depurl=computer-engineering&lang=en&cid=147732

19 Patterson, J.P & M.N. Smith, pp. 29-35.

20 פעילות המכון בתחום אבטחת המידע: http://www.itrc.ac.ir/itrc-secure-en.php

21 התייחסות להשקעה בטכנולוגיות מידע באתר של TCO
http://citc.ir/newpages/page27.aspx?lang=Fa

22 Iran Watch, *the Wisconsin project on nuclear arms control*, Januar 3, 2011,
http://www.iranwatch.org/suspect/records/technology-cooperation-office.htm

23 רשימת החברות ב־Paradis Technology Park
http://www.techpark.ir/?/content/142

24 אתר Guilan Science Park
http://www.gstp.ir/modules.php?name=Content&pa=showpage&pid=16

25 *S*teve Stecklow, "chinese firm helps iran spy on citizens,"Reuters, March 22, 2012,
http://graphics.thomsonreuters.com/12/03/IranChina.pdf

26 Reza Marashi, 2011, עלון מידע המציג את טכנולוגית ה־SEPAR ומצביע על הקשר בין המשטר לבין פיתוחה
http://www.iranascience.com/1-home/newsletters/21-Web%20Filters.pdf

27 OpenNet Initiative, June 16, 2009, http://opennet.net/research/profiles/iran

28 Kevin McCaney, *Iran building a private, isolated Internet, but can it shut out the world*? ,GCN ,April 10, 2012,

http://gcn.com/articles/2012/04/10/iran-building-separate-isolated-internet.aspx

29 Robert Tait, *Iranian state goes offline to dodge cyber-attacks*, *The Telegraph*, August 5, 2012, http://www.telegraph.co.uk/news/worldnews/middleeast/iran/9453905/Iranian-state-goes-offline-to-dodge-cyber-attacks.html

30 Cyrus Farivar, *Security researcher unearths plans for Iran's halal Internet*, Ars Technica, April 17, 2012, http://arstechnica.com/tech-policy/2012/04/iran-publishes-request-for-information-for-halal-internet-project/

31 Robert Tait, 2012.

32 Ali Akbar Dareini and Brian Murphy, *Iran Internet Control: Tehran Tightens Grip On Web*, The Huffington Post, April 16, 2012, http://www.huffingtonpost.com/2012/04/16/iran-internet-control_n_1429092.html?ref=world

33 Emily Alpert and Ramin Mostaghim, *Iran's supreme leader calls for new Internet oversight council*, *Los Angeles Times*, March 7, 2012, http://latimesblogs.latimes.com/world_now/2012/03/iran-internet-council-khamenei.html

34 BBC Persian, *Structure of Iran's Cyber Warfare*, p.1, http://nligf.nl/upload/pdf/Structure_of_Irans_Cyber_Operations.pdf

35 *Tehran Times*, *Iran is formulating strategic cyber defense plan*: official, June 15, 2012, http://tehrantimes.com/politics/98761-iran-is-formulating-strategic-cyber-defense-plan-official

36 מבנה ותפקידי המרכז מפורטים באתרו הרשמי: http://www.certcc.ir/index.php?newlang=eng

37 BBC Persian, Structure of Iran's Cyber Warfare, pp 4-5.

38 "Iran to crack down on web censor-beating software," *Hürriyet Daily News*, September 22, 2012, http://www.hurriyetdailynews.com/iran-to-crack-down-on-web-censor-beating-software.aspx?pageID=238&nID=22789&NewsCatID=374

39 BBC Persian, Structure of Iran's Cyber Warfare, p.4.

40 בינואר 2012 חוקק המשטר מערכת של חוקים למעקב וניתור אחר משתמשי האינטרנט קפה. באמצעות חוקים אלו יכולה FETA, יצור "ספר משתמשים" של כלל הגולשים הארעיים במדינה ולנתר פעילות כנגד המשטר במרחב הסייבר.
Farnaz Fassihi, "Iran Mounts New Web Crackdown," *The wall Street Journal*, January 6, 2012, http://online.wsj.com/article/SB10001424052970203513604577142713916386248.html

41 lIan Berman, p. 4.

42 Kevin Coleman, *Iranian Cyber Warfare Threat Assessment*, Defense Tech, September 23, 2008, http://defensetech.org/2008/09/23/iranian-cyber-warfare-threat-assessment

43 Stephen Trimble, *Avtobaza: Iran's weapon in alleged RQ-170 affair?* The DEW Line, December 5, 2011, http://www.flightglobal.com/blogs/the-dewline/2011/12/avtobaza-irans-weapon-in-rq-17.html

44 Frank J. Cilluffo, *The Iranian Cyber Threat to the United States*. A Statement

before the 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, http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20-%20Cilluffo.pdf

45 Scott Peterson, *Iran's cyber prowess: Could it really have cracked drone*, *The Christian Science Monitor*, April 24, 2012, http://www.csmonitor.com/World/Middle-East/2012/0424/Iran-s-cyber-prowess-Could-it-really-have-cracked-drone-codes

46 Frank J. Cilluffo, p. 5.

47 Patterson, J.P & M.N. Smith, pp. 44-49.

48 Iftach Ian Amit, *Cyber[Crime|War]," paper presented at DEFCON 18 conference*, July 31, 2010, http://www.defcon.org/images/defcon-18/dc-18-presentations/Amit/DEFCON-18-Amit-Cyber-Crime-WP.pdf

49 Khashayar Nouri, *Cyber Wars in Iran*, Institute for War & Peace Reporting, July 23, 2010, http://iwpr.net/report-news/cyber-wars-iran

50 Golnaz Esfandiari, *Basij Members Trained To Conquer Virtual World* , payvand Iran News, August 21, 2010, http://www.payvand.com/news/10/aug/1206.html

51 Jeffrey Carr, "Iran's Paramilitary Militia Is Recruiting Hackers," *Forbes*, January 12, 2011, http://www.forbes.com/sites/jeffreycarr/2011/01/12/irans-paramilitary-militia-is-recruiting-hackers/

52 Bob Beauprez, *Iranian Cyber-Attack Plot against U.S. Exposed in Mexico*, Townhall, December 2011, http://finance.townhall.com/columnists/bobbeauprez/2011/12/13/iranian_cyberattack_plot_against_us_exposed_in_mexico/page/full/

53 SSl - Secure Socket Layer הנו פרוטוקול לתקשורת מאובטחת באינטרנט המוודא שהשרת אליו מתחבר הלקוח הנו השרות הנכון תוך הצפנת המידע בין דפדפן הלקוח לבין השרת. ניתן לרכוש מפתחות SSL מספקים מורשים. גנבת מפתחות מאפשרת לגורם (שלו שליטה על תשתית הרשת) להסיט גולשים לאתרים מזוייפים המתחזים להיות אתרים חוקיים וכך לקבל גישה למידע חסוי של המשתמש.

54 דיווח החברה: Comodo, March 31, 2011 http://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html

55 Eva Galperin, Seth Schoen and Peter Eckersley, *A Post Mortem on the Iranian DigiNotar Attack*, Electronic Frontier Foundation , September 13, 2011, https://www.eff.org/deeplinks/2011/09/post-mortem-iranian-diginotar-attack

56 Fox-It, Interim Report, *DigiNotar Certificate Authority breach "Operation Black Tulip,*" September 5, 2011.

57 Toby Sterling, *Iran Involvement Suspected In DigiNotar Security Firm Hacking*, HuffPost Tech, September 5, 2011, http://www.huffingtonpost.com/2011/09/05/iran-diginotar-hack_n_949517.html

58 Gerry Smith, *Cyber Attacks Against US Banks Sponsored By Iran*, Lieberman Says,

The Huffington Post, September 9, 2012, http://www.huffingtonpost.com/2012/09/21/cyber-attacks-banks-iran-lieberman_n_1904846.html

59 זהו ארגון שמטרתו לנתח ולשתף מידע בין הגורמים הפיננסיים באשר לאיומים על שרותים פיננסיים קריטיים בארצות הברית.
Financial Services Information Sharing and Analysis Center (FS-ISAC)

60 Jaikumar Vijayan, *U.S. banks on high alert against cyberattacks*, Computerworld, September 20, 2012, http://www.computerworld.com/s/article/print/9231515/U.S._banks_on_high_alert_against_cyberattacks

61 Jim Finkle, *Exclusive: Insiders suspected in Saudi cyber-attack*, Reuters, September 7, 2012, http://in.reuters.com/article/2012/09/07/net-us-saudi-aramco-hack-idINBRE8860CR20120907

62 Kelly Jackson Higgins, *Shamoon Code 'Amateur' But Effective*, Dark Reading, September 11, 2012, http://www.darkreading.com/advanced-threats/167901091/security/attacks-breaches/240007179/shamoon-code-amateur-but-effective.html
וגם
Nicole Perlroth, "Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," *The New-York Times*, October 23, 2012, http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?_r=1&adxnnl=1&pagewanted=all&adxnnlx=1351084069-1i53F0BCczNEGcP8ut3n4A&

63 Associated Press, Panetta hints Iran behind Gulf cyberattacks, CBS News ,October 12, 2012, http://www.cbsnews.com/8301-202_162-57531088/panetta-hints-iran-behind-gulf-cyberattacks

64 Jeffrey Carr, *Who's Responsible for the Saudi Aramco Network Attack?* Blogspot, August 27, 2012, http://jeffreycarr.blogspot.co.uk/2012/08/whos-responsible-for-saudi-aramco.html

65 Global Research & Analysis Team, *Shamoon the Wiper - Copycats at Work*, Kaspersky Lab Expert, August 16, 2012, https://www.securelist.com/en/blog?print_mode=1&weblogid=208193786

66 Reuters, *Iranian hackers attacked three largest U.S. banks as part of cyber campaign: sources*, September 21, 2012, http://news.nationalpost.com/2012/09/21/iranian-hackers-attacked-three-largest-u-s-banks-as-part-of-cyber-campaign-sources

67 Nicole Perlroth, October 23, 2012.

68 Associated Press, Panetta hints Iran behind Gulf cyberattacks, CBS News ,October 12, 2012, http://www.cbsnews.com/8301-202_162-57531088/panetta-hints-iran-behind-gulf-cyberattacks