מבט על, גיליון 536, 3 באפריל 2014

התפתחויות בלוחמת הסייבר של איראן 2013 - 2014

גבי סיבוני וסם קרוננפלד

בתחילת 2013 תיאר גורם בכיר בחברת אבטחת הסייבר CrowdStrike, את איראן כמדינת דרג השלישי (Third Tier) בקשר ליכולותיה לפעול במרחב הסייבר והעריך כי יכולותיה נחותות משמעותית מיכולותיהן של המדינות המובילות כגון ארצות הברית, רוסיה ובריטניה וסין. איראן נתפסה כמי שביכולתה להטריד את מערכי אבטחת המידע המערביים, אך חסרה את הידע והאמצעים להוציא אל הפועל מתקפות סייבר אסטרטגיות. 2013 סדקה במידה רבה הנחות אלו כאשר איראן התקדמה והתייצבה כאחד השחקנים הפעילים בזירת הסייבר הבינלאומית. התקדמות זו ניתן לשייך לשילוב בין שחרור מסוים של הרסן מצד מקבלי ההחלטות האיראניים בכול הקשור לפעילות התקפית במרחב הסייבר, לבין קפיצת מדרגה איכותית של מערך לוחמת הסייבר האיראני, אשר הפתיע מומחים מערביים רבים בהיקפי פעילותו, תחכומו המקצועי ובחירת מטרותיו השאפתנית.

תפיסת ההגנה - מתנתקים מהעולם

ניסיון העבר שצברה איראן באירועים כגון מתקפת Stuxnet והמהומות שליוו את בחירות 2009, לימד אותה על חשיבותו של מערך הגנת סייבר יעיל ועל שליטה אפקטיבית במרחב האינטרנט. לשם כך, איראן פועלת בשלושה צירים מרכזיים, המבנים יחדיו מערך סייבר הגנתי רב ממדי. (1) יצירת מעטפת הגנה כנגד תקיפות סייבר על תשתיות חיוניות ומידע רגיש; (2) נטרול פעילות הסייבר של גורמי אופוזיציה ומתנגדי משטר; (3) הרחקה של תכנים ורעיונות מערביים ממרחב הסייבר הפנים-מדינתי, רעיונות אשר עשויים לתרום להתפתחותה של "מהפכה רכה" שתפגע ביציבות המשטר.

בכל שלושת הצירים הללו עבר מערך הגנת הסייבר האיראני שדרוג משמעותי במהלך 2013. שידורג אשר נבע בעיקר מהבשלה של טכנולוגיות ומערכים ארגוניים. ראשית, איראן העלתה לאוויר רשת אינטרא-נט פנים-מדינתית ומבודלת, אשר מאפשרת לה שליטה הדוקה על התכנים במרחב הסייבר במדינה. שנית, איראן השקיעה בפיתוח טכנולוגיות ואמצעי הגנת סייבר מתוצרת מקומית במטרה להקטין את תלותה במוצרים זרים העשויים להוות "סוסים טרויאניים". כמו-כן, המשטר האיראני הגביר את האכיפה הפיסית כנגד מתנגדי המשטר הפועלים באינטרנט בעיקר באמצעות שימוש אגרסיבי במשטרת הסייבר. בנוסף לכך, רשויות הסייבר האיראניות מיסדו שגרה של אימונים, תרגילים וביקורות בקרב המוסדות הביטחוניים והאזרחיים של המדינה. השפעתם של צעדים אלו באה לידי ביטוי במהלך הבחירות בחודש יוני 2013, כאשר מערך הסייבר האיראני פעל ביעילות והצליח במידה רבה לשלוט בשיח במרחב האינטרנט הפנימי ולנתר פעילות חתרנית.

נראה כי כיום, מערך הגנת הסייבר האיראני עדיין נדרש לעבור כברת דרך בכדי להתמודד באופן אפקטיבי ועקבי עם מתקפות סייבר ברמת תחכום גבוהה כדוגמת ה-Stuxnet, אך קפיצת המדרגה הטכנולוגית והארגונית שביצעה איראן בשנה האחרונה מעידה כי לאיראנים עקומת למידה חדה וכי הם עשויים לגבש מערך הגנה יעיל ומקיף מוקדם מהצפוי.

הממד ההתקפי – חיפוש אחר מתקפות "איכות"

הרפובליקה האסלאמית רואה בזירת הסייבר גם פלטפורמה התקפית יעילה המאפשרת לפגוע ביריבות בעלות עליונות צבאית ברורה ובד בבד לשמור על מרווח הכחשה שימנע הוקעה בינלאומית או אף סנקציות ומתקפות נגד. במהלך 2013 הפכה לוחמת הסייבר לכלי מרכזי בידי איראן לשם תקיפת

התפתחויות בלוחמת הסייבר של איראן 2013 – 2014 **המכון למחקרי ביטחון לאומי**
מאת: **גבי סיבוני וסם קרוננפלד** **מבט על**, גיליון 536, 3 באפריל 2014

מטרות מערביות בתגובה לסנקציות וכאמצעי להרתעת הסלמה בפעילותן של מדינות המערב כנגד איראן. היקפם, יעדיהם והצלחתם היחסית של מתקפות סייבר, שהתרחשו בשנה האחרונה ושויכו לגורמים איראניים, מעידים על התעצמות היכולות העומדות לרשותה של איראן. גורמים מערביים משייכים את ההתקדמות בתוכנית לוחמת הסייבר להצלחתה של איראן לשלב בין היכולות, הידע וכוח האדם הצומחים בפקולטות האיראניות למדעי המחשב לבין הניסיון והיכולות הגבוהות של קהילת ההאקרים האיראנית, אשר רבים מחבריה מזדהים עם המשטר ועם מטרותיו. בנוסף לכך גם הקשרים המתהדקים של מערך הסייבר האיראני עם פושעי סייבר, האקרים ומומחי אבטחת מידע, רוסים בעיקר, אשר מוכנים ל"השכיר" את יכולותיהם בתמורה לכסף, תורמים להתקדמות המהירה בתוכנית לוחמת הסייבר האיראנית. לצד חיזוק מערך הסייבר האורגני, איראן אף פועלת להרחיב ולחזק את יכולות לוחמת הסייבר של בנות בריתה. נראה כי האיראניים מבקשים לייצר מערך יעיל של שליחים הפועלים עבורם במרחב הסייבר. אחד ממרכזי הכובד של פעילות איראנית זו היא הזירה הסורית שם איראן תומכת בארגון ההאקרים "צבא סוריה האלקטרוני" (Syrian Electronic Army - SEA), אשר הולך והופך לגורם משמעותי יותר ויותר במרחב הסייבר.

ההתקדמות ביכולות לוחמת הסייבר האיראניות נשקפת מסדרה של מתקפות שהתרחשו במהלך המחצית השנייה של 2012 וב-2013 ושיוחסו לאיראן. מתקפות אלו עשו שימוש בטכניקות מתחכמות, תקפו יעדים איכותיים והתרחשו בהיקפים משמעותיים יותר מאשר תקיפות איראניות בעבר. בין המתקפות הבולטות שיוחסו לאיראן ניתן למצוא תקיפה רחבת היקף על אתרי האינטרנט של בנקים ומוסדות פיננסיים מרכזיים בארצות הברית, אשר תוארה על ידי מומחה אבטחת מידע כ"חסרת תקדים בהיקפה ובמידת יעילותה". גל תקיפות נוסף, המיוחס לגורמים איראניים, התמקד בחברות תשתית ואנרגיה אמריקאיות והתאפיין במתקפות על מערכי בקרה, מתקפות אשר עשויות לפגוע בפעילותן הפיסית או באמצעי הבטיחות של תשתיות קריטיות כדוגמת מערכות הולכת גז ונפט ומערכות חשמל. בשנה האחרונה גורמים המזוהים עם איראן לקחו אחריות גם על מתקפות סייבר כנגד מוסדות ישראלים וביוני 2013 הצהיר ראש ממשלת ישראל בנימין נתניהו כי חלה עלייה משמעותית בתקיפות הסייבר האיראניות כנגד תשתיות מחשוב חשובות בישראל.

ההתפתחות המהירה ביכולת לוחמת הסייבר של איראן ושל שלוחיה ובני בריתה, מחייבת את ישראל, כמו גם מדינות מערביות אחרות, לפעול באופן נחרץ ושיטתי לשימור עליונותן האיכותית והמבצעית במרחב הסייבר. חשיבותו של מרחב הסייבר לתפיסת הביטחון הישראלית והדחיפות שביצירת "כיפת ברזל" דיגיטאלית הודגשו היטב בדבריו של רמטכ"ל צה"ל רב אלוף בני גנץ: "ישראל חייבת להיות ברמה המעצמתית בסייבר...אין לחכות עם הסיפור הזה".