מבט על, גיליון 598, 25 באוגוסט 2014

תקיפת סייבר איראנית במהלך "צוק איתן"

גבי סיבוני וסמי קרוננפלד

על אף שבמוקד המערכה האחרונה בעזה נבחנו יכולותיו של צה"ל להתמודד עם איומי הרקטות והמנהרות, עדויות העולות עם שוך הקרבות מראות, כי ישראל נדרשה להתמודד במהלך מבצע צוק איתן גם מול אתגרים בזירת הסייבר. קצין בכיר בחיל התקשוב, האחראי על ההגנה של צה"ל, ציין, כי במהלך המבצע הוציאו גורמים איראניים אל הפועל מתקפת סייבר רחבת היקף כנגד מטרות ישראליות ובכללן גם ניסיונות לפגיעה ברשתות של המערכת הביטחונית והפיננסית. ניסיונות אלו אומנם נוטרלו במהירות ובקלות יחסית על-ידי גורמי הגנת הסייבר הישראלים, אך נראה, כי האיראנים משקיעים רבות בפיתוח יכולות תקיפה אפקטיביות כנגד מערכות תשתית והם עשויים להציב אתגר משמעותי בפני ההגנות הישראליות כבר בעתיד הנראה לעין.

ב-2013 יוחסה לאיראן סדרה של מתקפות כנגד אתרי האינטרנט של בנקים ומוסדות פיננסיים מרכזיים בארצות הברית. המתקפה תוארה על-ידי מומחה לאבטחת מידע, כ"חסרת תקדים בהיקפה ובמידת יעילותה" ובמהלכה עשו התוקפים שימוש בטכניקות מתוחכמות והראו, כי ביכולתם לפעול בהיקפים משמעותיים גם כנגד יעדי "איכות". לתקיפה נגד תשתיותיה הפיננסיות של מדינה משמעויות חמורות והיא עשויה להביא לנזקים כלכליים כבדים עקב הפגיעה בשגרת הפעילות הפיננסית של חברות מסחריות ובתי אב רבים.

עם זאת, מוקד מתקפת הסייבר במהלך מבצע "צוק איתן" היה מרחב האינטרנט האזרחי, כאשר גורמים איראניים לקחו חלק במה שתואר על ידי קצין התקשוב כמתקפה "חסרת תקדים בהיקפה ובאיכות מטרותיה". המתקפה האיראנית כוונה כנגד אתרי רשת צה"ליים כגון, אתרי פיקוד העורף ודובר צה"ל כמו גם כנגד תשתיות אינטרנט אזרחיות. התוקפים אף זכו להצלחה מסוימת כאשר הצליחו לפרסם הודעה שקרית בחשבון הטוויטר הרשמי של צה"ל בה נאמר, כי הכור הגרעיני בדימונה נפגע מירי רקטי וכי קיימת סכנה של דליפה רדיואקטיבית. בנוסף לכך חלק מהמתקפות כנגד ישראל שויכו ל"צבא סוריה האלקטרוני" (Syrian Electronic Army – SEA). קבוצת האקרים תומכי אסד, אשר פיתחה במהלך השנים יכולות תקיפה משמעותיות ותוארה על ידי מייקל היידן, ראש ה-CIA וה-NSA לשעבר, כשליח איראני לכל דבר ועניין.

מתקפת הסייבר כנגד המטרות הישראליות צברה תאוצה ככול שהפעילות הצבאית בשטח הורחבה והועמקה. אם בחלקו הראשון של המבצע נרשמה פעילות התקפית שולית ובלתי מאורגנת מצד גורמים פרו-פלסטיניים, הכניסה הקרקעית לרצועה הביאה, על פי ראש מחלקת הגנת הסייבר בצה"ל, לזינוק משמעותי בהיקף המתקפות כנגד ישראל ולעיתים אף בתחכומן. המתקפות הגיעו לשיאן ב-25 ביולי 2014, יום השישי האחרון של הרמדאן, המצוין באיראן כ"יום ירושלים", יום התנגדות לישראל ולציונות, כאשר גורמים איראניים בשיתוף האקרים מרחבי העולם, הוציאו אל הפועל מתקפה רחבה כנגד מספר רב של אתרים ישראלים במטרה לחסמם לתקופת זמן ארוכות. המתקפה נחסמה במאמץ משולב של גורמי צה"ל ושב"כ, אשר היו ערוכים לקראתה.

ניתוח הפעילות האיראנית במרחב הסייבר במהלך מבצע "צוק איתן" מצביע על הבשלה ביכולותיה האופרטיביות של הרפובליקה האסלאמית ומעיד, כי ביכולתה לנהל מבצע צבאי קיברנטי רחב היקף כנגד מגוון של מטרות ויעדים, תוך שימוש בספקטרום רחב של שיטות פעולה. מעבר לכך, ייתכן וההתמקדות האיראנית בזירת הסייבר במהלך "צוק איתן" מעידה על ראשיתו של תהליך בו

תקיפת סייבר איראנית במהלך "צוק איתן" **המכון למחקרי ביטחון לאומי**
מאת: **גבי סיבוני וסמי קרוננפלד** **מבט על**, גיליון 598, 25 באוגוסט 2014

לוחמת הסייבר תופסת את מקום הטרור הקלאסי ככלי המרכזי בדוקטרינת הלוחמה הא-סימטרית האיראנית. לוחמת הסייבר מאפשרת פגיעה משמעותית בעורפו של אויב בעל עליונות צבאית וגאו-אסטרטגית לצד הרחקת העדות ויכולת הכחשה – שני אלמנטים מרכזיים בעיני האיראנים. עם זאת, יכולות הסייבר האיראניות נכון להיום, עדיין נחותות ביחס ליכולותיהן של ישראל ושל המעצמות הטכנולוגיות המובילות, אך נראה שהאיראנים מגשרים על הפערים במהירות וביעילות.

גורמי ההגנה של ישראל הצליחו לסכל את המתקפה האיראנית אולם אין וודאות שכך יהיה בעתיד. בישראל טרם סוכמה תפיסת ההכנה הכוללת וטרם נקבע הגורם המוביל את ההגנה מול מתקפות רחבות כאלה. במרחב הסייבר של ישראל פועלים מגוון גופים בהם: צה"ל, השב"כ, המוסד, חברות וספקי תקשורת, בנק ישראל ובנקים מסחריים, משרדי ממשלה, משטרת ישראל, חברות אבטחה אזרחיות וגופים נוספים עוסקים בנושא. היעדר הסדרה של סמכויות במאמץ ההגנתי והסיכולי, עלולה לייצר חורים "בכיפת הברזל" הדיגיטאלית המגנה על ישראל ולאפשר לגורמים עויינים לפגוע בישראל.

הצלחת הסיכול האחרון מעידה יותר על יכולת שיתוף הפעולה והעבודה המתואמת בדרגים המקצועיים ופחות על הסדרת הסמכויות בין הארגונים השונים בישראל. אולם לא לעולם חוסן, מתקפות הסייבר ותהליכי בניין הכוח של איראן מתקדמים בקצב מהיר. איראן עשויה לאתגר את יכולת ההגנה של ישראל באופן משמעותי. לכן, חובה לקדם ולסכם בהקדם את ארגון הגנת הסייבר של ישראל ולקבוע את יחסי הגומלין בין הארגונים השונים הפועלים במרחב הזה. בנוסף, אין די במאמצי הגנה, ישראל יכולה וחייבת שלא להסתפק במאמצי סיכול אלא להוציא לפועל מכות מנע ומהלומות גמול על תוקפי הסייבר. אין כל סיבה שנחת זרועה של מדינת ישראל לא תונחת על מבקשי רעתנו גם במרחב הסייבר.