״צוק איתן״ מנקודת המבט של הגנת הסייבר

דניאל כהן ודניאל לוין

דניאל כהן הינו עמית מחקר ומתאם תכנית ביטחון סייבר במכון למחקרי ביטחון לאומי INSS, דניאל לוין הינה עוזרת מחקר ב- INSS

המאמר פורסם לראשונה בקובץ: ׳צוק איתן׳ - השלכות ולקחים, ענת קורץ ושלמה ברום, עורכים. המכון למחקרי ביטחון לאומי, תל אביב, 2014

לוחמת הסייבר הפכה זה מכבר למקור כוח חשוב בעבור מדינות. עם זאת, היא מהווה גם איום אסטרטגי על התשתיות החיוניות של מדינות, כאשר מאגרי המידע של תשתיות התקשורת, של אמצעי התקשורת, של הגופים הפיננסיים ועוד מתבססים יותר ויותר על מרחב הסייבר. צבאות במיוחד נעשו תלויים במידה רבה מאוד בטכנולוגיית הסייבר המתקדמת. ברמה הלאומית נמצאת ישראל בתהליך מיסודו של מערך לאומי משולב להגנת סייבר, ואתגר זה מחייב שיתוף פעולה בין המגזר האזרחי (השירות הציבורי והמגזר הפרטי) לבין הגופים הביטחוניים והצבאיים.

התמודדותה של מערכת הביטחון עם מתקפות הסייבר שכוונו לעבר המדינה במהלך מבצע ׳צוק איתן׳ היוותה מבחן ליישום מדיניות הממשלה בתחום הסייבר, והתאפיינה בשיפור של ממש בכל הנוגע לתיאום בין ארגוני ביטחון הסייבר, לרבות תפקוד מערכות ההגנה על טכנולוגיות המידע הישראליות, והרחבת שיתוף הפעולה בין המגזר האזרחי למגזר הביטחוני. מאמר זה יבחן את מתקפות הסייבר שבוצעו נגד ישראל במהלך ׳צוק איתן׳, וינתח אותן על בסיס שלושה גורמים רלוונטיים לישראל: היקף המתקפות, השחקנים שהניעו אותן והתקדמותה של ישראל בתחום ביטחון הסייבר.

היקף מתקפות הסייבר נגד ישראל

במקביל לכניסת כוחות צה״ל למערכה הקרקעית ברצועת עזה, חל גידול משמעותי במספר מתקפות הסייבר. אפשר לייחס את חלקן למתקפות יזומות של קבוצות פצחנים (האקרים) חובבים, ואילו מתקפות אחרות התאפיינו ברמת תחכום גבוהה יותר והתמקדו במערכות התקשורת הפועלות בישראל. אולם, עם סיום הפעילות הקרקעית חלה ירידה ניכרת במספר המתקפות[1].

אחת ממתקפות הסייבר הנרחבות ביותר במהלך המבצע התרכזה בחברות תקשורת ובספקי אינטרנט מקומיים, ונועדה לגרום לרשתות ישראליות לקרוס עקב מתקפות סייבר נועדו למטרות עומס יתר, תוך ניסיון להציף את רשת האינטרנט[2]. מתקפות הסייבר נועדו למטרות שונות – ממתקפות שמטרתן למנוע שירות (DDoS) ועד לפגיעה בקישורים בין שמות מתחם לכתובות IP (DNS) והן הצליחו לגרום להשבתתם של יותר מאלף אתרים ישראליים לא חיוניים, להשחתת אתרים נוספים, לחשיפת מאגרי מידע וגם לדליפת כל פריצה מעין מידע אישי של אזרחים, כגון סיסמאות כניסה למערכות ממוחשבות.[3] כל פריצה מעין זו יצרה עבור חמאס הזדמנויות נוספות לאיסוף מידע עם זיהוי יעדים פוטנציאליים חדשים, והארגון פיתח שיטות ואמצעים שהותאמו לכך במיוחד. לדוגמה, משלוח מסיבי של מסרונים על ידי חמאס, שהוצגו כאילו היה מקורם בשירות הביטחון הכללי, בעיתון ׳הארץ׳ או בחמאס עצמו.

מתקפות נוספות כללו שיבוש שידורים של לוויין פרטי-מהלך שאִפשר למסר תעמולתי של חמאס להבזיק בשידורי הלווין של ערוץ 2 ושל ערוץ 10 (חמאס ביצע

1

2

3

מתקפה דומה נגד ערוצי הטלוויזיה המסחריים במהלך מבצע 'עמוד ענן'.[4] דובר צה"ל וחשבון הטוויטר שלו נפלו אף הם קורבן למתקפת סייבר רחבת-היקף ביוזמת הצבא האלקטרוני הסורי (SEA) , שהעלה מסרים באנגלית ובערבית.[5] בנוסף תיאמו ביניהן כמה קבוצות גדולות של פצחנים מחאות סייבר מרובות נגד ישראל בשם"OpIsrael" - שיתוף פעולה שבוצע במהלך כל ימי המבצע, במגמה לקדם את סדר היום הפלסטיני.[6]

השחקנים שהניעו את המתקפות

בשנים האחרונות מגלים ארגוני טרור גדולים כמו חמאס וחזבאללה עניין גובר בתחום טרור הסייבר, בסיועה של איראן. במהלך מבצע "צוק איתן" טען צה"ל כי איראן מילאה תפקיד חשוב בהתגברות מתקפות הסייבר שכוונו למתקנים אזרחיים.[7] מתקפות אלו בוצעו במהלך המבצע על ידי קבוצות טרור סייבר הפועלות בחסות מדינה, כגון צבא הסייבר האיראני ו- SEA הסורי.

צה"ל והשב"כ שיתפו פעולה לכל אורך מבצע "צוק איתן" כדי לסכל מתקפות שתוכננו על ידי איראן לביצוע ב " יום אל -קודס " - אירוע נגד הציונות המאורגן מדי שנה על ידי ההנהגה האיראנית. במתקפה זו היו מעורבים פצחנים מכל רחבי העולם, שניסו להשבית אתרי אינטרנט ישראליים.[8]

קבוצה אחרת ששמה לה למטרה לפגוע בישראל, שלא ניתן היה לזהותה באופן חד משמעי עם העולם האסלאמי והערבי, הייתה קבוצת "אנונימוס". בכל הנוגע למתקפות של הקבוצה נגד ישראל היא נחלקת לשלושה תאים: ערבי, אסלאמי וכל השאר. קבוצת אנונימוס, שכבר יזמה בעבר מתקפות סייבר נגד ישראל, יכולה לכלול פצחנים ברמה גבוהה, אולם במבצע 'צוק איתן' החליטו חלקם שלא להשתתף בפעילות זו. הדבר עשוי להסביר את ההבדל בזהותם של הפצחנים בין מבצע "עמוד ענן" לבין 'צוק איתן'. במהלך מבצע 'עמוד ענן' התמודדה ממשלת ישראל עם יותר ממאה מיליון מתקפות סייבר במהלך שמונה ימים, שמקורן בכתובות אינטרנט מכל העולם, אך בעיקר מאירופה ומארצות הברית.[9]

לשם השוואה, במהלך מבצע 'צוק איתן' העריכה חברת ביטחון סייבר כי אפשר היה לשייך שבעים אחוזים ממתקפות הסייבר למקורות במדינות ערב ובעולם המוסלמי.[10]

התקדמותה של ישראל בביטחון הסייבר

ישראל נקטה גישה פרו אקטיבית ויישמה אסטרטגיית הגנה שתוכננה מבעוד מועד, עם יכולות תפעוליות מתקדמות, אשר הצליחה לספק הגנה וביטחון ברמה מקצועית גבוהה.[11] הן צה"ל והן השב"כ הצליחו לסכל כל ניסיון לשבש את פעולתן התקינה של רשתות ממשלתיות ושל תשתיות חיוניות, והשב"כ אישר כי הצליח להגן מפני כל מתקפות הסייבר על רשתות ומערכות ממשלתיות. אחת משיטות ההגנה התבטאה בחסימת כתובות אינטרנט זרות למשך שעתיים, עם תחילת מבצע 'צוק איתן'. השב"כ פעל באמצעות חטיבת הסייבר שלו ובתיאום עם קבלנים פרטיים, עם משרד התקשורת ועם אמצעי התקשורת, ונקט צעדי מניעה מפני מתקפות אלו.[12]

צה"ל שיתף פעולה עם רשת תקשורת משולבת של חיל המודיעין, אגף התקשוב ושל חברות סייבר הקשורות למשרד הביטחון, שסייעו בזיהוי כלל איומי הסייבר על ישראל ובהסרתם. ראש יחידת הגנת הסייבר בצה"ל ציין כי בוצעו ניסיונות לחדור

4

5

6

7

8

9

10

11

12

לרשתות של הצבא, אך הוא וידא כי ייעשה שימוש ביכולות הטכנולוגיות המתקדמות, כדי להבטיח שפריצות מעין אלה לא יצלחו.[13]

סיכום

ניסיונותיהם של תאי הסייבר בארגוני טרור לבצע מתקפות סייבר אסטרטגיות נגד ישראל לא צלחו עד כה, בעיקר מכיוון שפעילות זו מחייבת רמה גבוהה של תחכום מודיעיני ושל יכולות טכנולוגיות. סביר להניח כי ארגוני טרור משפרים את יכולות הסייבר שלהם ומפתחים אותן, כדי שיוכלו להוות איום עתידי בתחום הסייבר. איום זה מתאפיין בקשר הקיים בין ארגוני טרור לבין טרור הפועל בחסות מדינה, המטשטש לא אחת את זהותן של קבוצות הַ אקטיביסטים. מנקודת המבט של ביטחון הסייבר הישראלי, יש הכרח לזהות קשר זה כאיום על הביטחון הלאומי.

היישום של תקנות סייבר ושל צעדי מניעה בתחום זה נועד להפוך את הגנת הסייבר להכרח מובנה בהגנה על מדינת ישראל, ובכלל זה על המגזר האזרחי (הפרטי והציבורי). נדרש להכיר בכך שמגזרים אלה מהווים חלק מתשתית הביטחון הלאומי.[14]

במבצע 'צוק איתן' חל שיפור של ממש בתיאום בין ארגוני ביטחון הסייבר הישראליים השונים, ובכלל זה בתפקודן של מערכות טכנולוגיית המידע הביטחוניות ובתיאום בין המגזר האזרחי והביטחוני. הנאמר כאן מדגיש את הצורך המיידי בהתוויית דרכי הגנה על מרחב הסייבר האזרחי.[15]

---

13 IDF Blog, "The Attack against Israel You Haven't Heard About´ $XJXVW

14 http://www.idfblog.com/blog/2014/08/22/attack-israel-havent-heard/ Jonathan Lis and Oded Yaron, "Amid cyber attacks on Israel, security agency wins a battle ¿JKWLQJEDFN ´Haaretz, July 28, 2014, http://www.haaretz.com/news/diplomacy-defense/. premium-1.607479 See Anonymous sub-group, AnonGhost Pastebin: http://pastebin.com/Lq6geBuJ

15 "Watch: +DPDVKDFNVLQWR&KDQQHO□□EURDGFDVW□´The Jerusalem Post, July 14, 2014, http://www.jpost.com/Operation-Protective-Edge/WATCH-Hamas-hacks-into-Channel-10- broadcast-362767 SEA tweetsRQWKH,')7ZLWWHULQFOXGHG³/RQJ/LYH3DOHVWLQH³DQG´ :$51,1*: Possible nuclear leak in the region after 2 rockets hit'LPRQDQXFOHDUIDFLOLW\ ´ Daniel Cohen and Danielle /HYLQ ³&\EHU,Q¿OWUDWLRQ'XULQJ2SHUDWLRQ3URWHFWLYH(GJH ´ 6 Forbes, August 12, KWWS ZZZ IRUEHV FRP VLWHV UHDOVSLQ F\EHU LQ¿OWUDWLRQ during-operation-protective-edge/ Gabi Siboni and Sami Kronenfeld, "The Iranian Cyber Offensive during Operation Protective 7 (GJH ´INSS Insight, August 26, 2014, http://www.inss.org.il/index.aspx?id=4538&articleid=7583 ,')%ORJ ³7KH$WWDFNDJDLQVW,VUDHO

הערות

IDF Blog, “The Attack against Israel You Haven’t Heard About´ $XJXVW 1 http://www.idfblog.com/blog/2014/08/22/attack-israel-havent-heard/ Jonathan Lis and Oded Yaron, “Amid cyber attacks on Israel, security agency wins a battle 2 ¿JKWLQJEDFN ´Haaretz, July 28, 2014, http://www.haaretz.com/news/diplomacy-defense/. premium-1.607479 See Anonymous sub-group, AnonGhost Pastebin: http://pastebin.com/Lq6geBuJ 3 “Watch: +DPDVKDFNVLQWR&KDQQHO EURDGFDVW ´The Jerusalem Post, July 14, 2014, 4 http://www.jpost.com/Operation-Protective-Edge/WATCH-Hamas-hacks-into-Channel-10- broadcast-362767 SEA tweetsRQWKH,')7ZLWWHULQFOXGHG³/RQJ/LYH3DOHVWLQH³DQG´ :$51,1*: Possible 5 nuclear leak in the region after 2 rockets hit'LPRQDQXFOHDUIDFLOLW\ ´ Daniel Cohen and Danielle /HYLQ ³&\EHU,Q¿OWUDWLRQ'XULQJ2SHUDWLRQ3URWHFWLYH(GJH ´ 6 Forbes, August 12, KWWS ZZZ IRUEHV FRP VLWHV UHDOVSLQ F\EHU LQ¿OWUDWLRQ during-operation-protective-edge/ Gabi Siboni and Sami Kronenfeld, “The Iranian Cyber Offensive during Operation Protective 7 (GJH ´INSS Insight, August 26, 2014, http://www.inss.org.il/index.aspx?id=4538&articleid=7583 ,')%ORJ ³7KH$WWDFNDJDLQVW,VUDHO