המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
INCORPORATING THE JAFFEE CENTER FOR STRATEGIC STUDIES
TEL AVIV UNIVERSITY אוניברסיטת תל-אביב

מבט על, גיליון 521, 27 בפברואר 2014

הצבא האלקטרוני הסורי (SEA) – **האם האיום אמתי?**

דניאל כהן ודניאל לוין

האיום של טרור הסייבר יצר דימוי של מחבל הנמצא במקום מרוחק ומבודד וגורם נזק אדיר באמצעות חדירה למערכות אבטחה או למערכות כלכליות דרך מרחב הסייבר. דימוי זה נפוץ במיוחד באמצעות פעילותו של הצבא האלקטרוני הסורי (SEA – Syrian Electronic Army). האקרים של SEA שמתקפותיהם מכוונות לאתרי אינטרנט פופולריים הציבו את האיום והדימוי הללו בחזית של תפיסת האיום העולמית. אולם במהלך בחינת האיום של טרור הסייבר יש לבדוק את היכולות הממשיות של ארגוני טרור דוגמת SEA בזירת הסייבר, ולברר האם אכן טמון במתקפות הסייבר שלהם איום רב-עוצמה.

המידע הקיים והמתועד על SEA מתאר את הארגון כקבוצה של האקרים אקטיביסטים פוליטיים צעירים, התומכים בנשיא סוריה בשאר אל-אסד במלחמת האזרחים במדינה באמצעות ביצוע פעולות סייבר זדוניות נגד האופוזיציה הסורית ואתרי אינטרנט מערביים. זהותם של חברי ה-SEA אינה ידועה, והקבוצה מגדירה עצמה כמבוזרת. רבים מאמינים כי פרט להודעות התמיכה של הארגון בבשאר אל-אסד, קיים קשר בינו לבין ממשלת סוריה. הארגון נרשם במקור בחברת המחשוב הסורית (SCS – Syrian Computer Society) שאסד עמד בראשה בשנות התשעים, והדבר חיזק את ההשערה שמקורו של SEA ב-SCS. אסד כינה את ה-SEA "צבא וירטואלי במרחב הסייבר", והארגון החזיק בדומיין על גבי שרת של ממשלת סוריה טרם השעייתו לזמן בלתי-מוגבל ביוני 2013, עם מעצרם של בכירים בממשל הסורי. ההשערות לגבי שיתוף הפעולה הממשלתי ממשיכות להתקיים, אם כי הראיה המוצקה היחידה למעורבות זו היא יכולתו של הארגון לפעול במסגרת המשטר המגביל, וכפי שאמר המומחה ל-SEA הלמי נומן (Helmi Noman), נראה כי הקשרים מסתכמים ב"תמיכה שבשתיקה" (http://goo.gl/crZAF1).

SEA מתמקד בעיקר במתקפות על שערי כניסה (gateways). הרמה הבסיסית ביותר של מתקפת סייבר היא תקיפת דפי האינטרנט של שער הכניסה לארגון, החשוף מטבעו לציבור. אנשי SEA פורצים לאתרים אלה באופן סדיר, וגניבת סיסמאות נחשבת להצלחתם הגדולה ביותר. עד כה פרצה קבוצת הסייבר ליותר מ-120 אתרים, לרבות גופי תקשורת מובילים דוגמת *פיינשל טיימס*, *הטלגרף*, *וושינגטון פוסט* ו*אל-ערביה*, וכן לאתרי תקשורת צד שלישי כגון *וייבר* ו*טנגו*. אחת המתקפות המשמעותיות והאפקטיביות ביותר התרחשה באפריל 2013, כאשר אנשי ה-SEA פרצו לחשבון הטוויטר של סוכנות החדשות Associated Press (AP) ושתלו בו ציוץ שלפיו הבית הלבן הופצץ והנשיא אובמה נפגע. ההשלכה המיידית הייתה ירידה חדה למשך מספר דקות בהיקף של למעלה מ-100 מיליארד דולר בשווקים הפיננסיים בארצות-הברית ובמדד דאו ג'ונס. SEA תקף גם חשבונות טוויטר של אתרי בידור שאינם מקדמים את מטרותיו כגון *E! Online* ו-*The Onion* – עובדה המעלה את הסברה שהארגון נהנה במיוחד מתשומת הלב שהוא משיג עקב חשיפתו לאתרים הלא-קשורים והבלתי-מעורבים.

SEA הופיע לראשונה באפריל 2011 כאשר ביצע פעולות של השחתה ושליחת דואר זבל בקבוצות פייסבוק באמצעות פרסום הלוגו של הארגון והודעות תמיכה באסד, כגון "מצטערים, איננו רוצים להרוס את האתר הרשמי שלכם, אך פעולות הממשלה הבריטית, עמדותיה נגד סוריה והתערבותה בענייניה הפנימיים של סוריה אילצו אותנו לפעול ולפרוץ לאתר שלכם". ב-19 בינואר 2014 תקף הארגון והשחית 16 אתרים ממשלתיים סעודיים, פרסם הודעות המאשימות את ערב-הסעודית בפעילות טרור והשבית את פעולתם של כל 16 האתרים. חברת מיקרוסופט מהווה מטרה למתקפות חוזרות ונשנות של הארגון, שפרץ לחשבונות דואר אלקטרוני באמצעות גניבת סיסמאות בפעם השנייה בחודשים האחרונים. הוא השיג פרטים אישיים של משתמשי

מיקרוסופט ועובדיו ופרסם אותם. עם זאת, ההיבט המדאיג ביותר היה הצהרתו של ה-SEA עם השעיית התקפתו, שאותה צייץ זמן קצר לאחר מכן: "עדיין לא סיימנו את התקפותינו על מיקרוסופט, התכוננו לפגיעות נוספות". לאחרונה תקף SEA את *פייפל* בריטניה ואת *פורבס* והציף את אתריהם בהודעות תמיכה במשטר הסורי. לגבי תקיפת פייפל הצהיר SEA שלא נפגעו נתונים אישיים של משתמשים, וכי מטרת המתקפה הייתה להגיב על סירובה של פייפל לאפשר לסורים להשתמש במערכת ההפעלה שלה.

הפרסום הניתן לכל אחת מהמתקפות של SEA יוצר תשומת לב תקשורתית, המדגישה את הצורך הדחוף באבטחת סייבר בקהילת התקשורת. פרשנים טוענים שקיימים אמצעים מעטים בלבד לבלימתה של סוריה בהקשר זה, שכן היא נחשבת למדינה הערבית הראשונה בעלת צבא אינטרנטי ציבורי. אולם אף על פי שמתקפות הסייבר של SEA גורמות שיתוק ושיבושים, רק לעתים רחוקות הן גורמות נזק מהותי, בלתי-הפיך או ארוך-טווח, והן מביכות יותר מאשר הרסניות.

כיום מוגבלת פעילותו של SEA למתקפות על פורומים ציבוריים והיא מתמקדת בהשחתה ובפריצה לאתרי אינטרנט ציבוריים ולדפי רשתות חברתיות. הסיבה העיקרית להיקף מוגבל זה היא מכשול הנגישות לטכנולוגיה שבו נתקלים ארגוני טרור. האינטרנט מאפשר מסחר באמצעי לוחמת סייבר, המאפשרים ל-SEA לרכוש בנקל את הכלים הנדרשים למתקפות על שערי כניסה. אכן, ההאקרים והסוחרים מנצלים יתרונות אלה ומציעים כלי סייבר ושירותי מתקפות סייבר לכל המעוניין. אולם, מתקפות סייבר מתוחכמות יותר אינן בגדר אפשרות סבירה, שכן השגת האמצעים לביצוען מוגבלת למדינות בעלות מומחיות טכנולוגית מתקדמת או לארגוני טרור הפועלים בחסות מדינות.

SEA לא התפתח לנקודה שבה הוא מסוגל לגרום נזק בלתי-הפיך. חסר לו המודיעין האיכותי הנחוץ לצורך פעולות סייבר וכן כוח אדם רב בהיקף הנדרש, השקעה כספית וזמן לאיתור הנקודות הרגישות. SEA מצליח בביצוע מתקפות בהיקף נמוך, אשר בזמן ובמקום המתאים יש בכוחן לגרום נזק באמצעות תופעות לוואי, כדוגמת המתקפה על חשבון הטוויטר של סוכנות AP. עם זאת, הדימוי של המחבל הבודד המחולל אסון הוא מוטעה, שכן טרור הסייבר שבוצע עד כה על ידי SEA אינו יכול לגרום נזק בר-קיימא לטווח ארוך.