

איום ארגוני הטרור במרחב הסייבר

גבי סיבוני, דניאל כהן, אביב רוטברט

מטרת מאמר זה היא לדון באיום הטרור במרחב הסייבר ולבחון את אמיתות התפיסות שהתגבשו בשנים האחרונות כלפי איום זה וכן לבחון מהן היכולות ששחקן לא מדינתי יכול להשיג והאם יכולות אלה עלולות להוות איום ממשי על ביטחון הלאומי של מדינות. ניתוח האיומים העיקריים שבפניהם עומדת מדינה בראייה רב שנתית ולאור שינויים צפויים במאזן האסטרטגי שלה מחייב הצגת הגורמים המאיימים על המדינה, תוך זיהוי שורשי האיום וסיבותיו. לפיכך, מאמר זה יבחן האם הטרור, שהשפעתו בדרך כלל טקטית יוכל לעשות (ואולי כבר עשה) את המעבר ליכולת של נשק סייבר בעל השפעות אסטרטגיות, נשק בעל נזק רחב היקף או לאורך זמן, מהסוג שמוריד מדינות על ברכיהן וגורם למערכות קריטיות לקרוס.

מילות מפתח: מרחב הסייבר, סייבר טרור, נשק קיברנטי, ארגוני טרור, שחקנים לא מדינתיים, סייבר פשע, מערכות מידע ארגוניות, מערכות ליבה מבצעיות, יכולת אכוונה מודיעינית, יכולת טכנולוגית.

מבוא

סרט הראינוע הראשון שהוצג בפני קהל נעשה על ידי האחים לומייר ב־1895. הסרט הראה רכבת נכנסת לתחנה, לכאורה לכיוון הצופים באולם. הצופים, שהיו משוכנעים שהרכבת מתקרבת אליהם, צרחו בבהלה וברחו מהבניין. בסרט הקולנוע הראשון שהוקרן אי פעם, נדמה היה לצופים שהם רואים מולם מציאות.¹

ד"ר גבי סיבוני הינו חוקר בכיר וראש תכנית לוחמת סייבר במכון למחקרי ביטחון לאומי. דניאל כהן הינו עמית מחקר ומתאם תכנית לוחמת סייבר במכון למחקרי ביטחון לאומי. אביב רוטברט הינו מלגאי תכנית ניובאור במכון למחקרי ביטחון לאומי ותלמיד לתואר שלישי בבית הספר למדעי המחשב באוניברסיטת תל-אביב.

המחברים מבקשים להודות לנעם ק. מהמטה הקיברנטי הלאומי, לדורון אברהם וקרן ח'טקביץ, מתמחים בתכנית לוחמת סייבר במכון למחקרי ביטחון לאומי, על סיועם בהכנת מאמר זה.

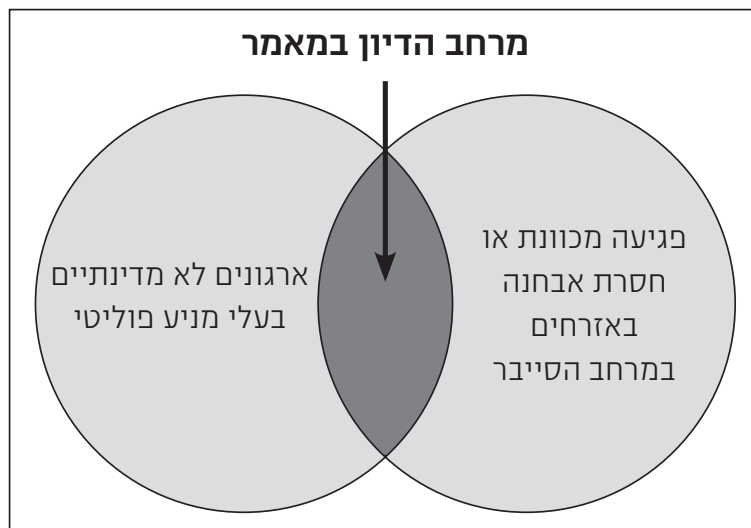
איום טרור הסייבר הוא נושא בו מתערבבים לעיתים המציאות והדמיון. אם נבחן את אחת התפיסות המרכזיות במרחב הסייבר – ההתמודדות עם איומי טרור – ניווכח כי רציונל התפיסה (שהחלה להתפתח לאחר אירועים מעצבים מתחילת שנות האלפיים, כגון "באג המילניום" ופיגועי 11 בספטמבר 2001) הוא שהעולם נראה כבשיאו של תהליך הנמצא מעבר לעידן המודרני והטכנולוגי – עידן הנעדר גבולות מגוננים, ובו מדינות חדירות למידע, לרעיונות, לאנשים ולחומרים; בקיצור, עולם פתוח. הטרור שנלקח בחשבון באיום הייחוס בעולם כזה הוא טרור מסוג חדש: איום, בו טרוריסט הנמצא במרתף נידח בקצה העולם הוא בעל פוטנציאל נזק המשנה לחלוטין את מאזן הכוחות על ידי יכולת חדירה למערכות ביטחוניות או לכליות חשובות בכל מדינה ומדינה ברחבי העולם והשגת מידע רגיש מהן, כמו גם יכולת לגרום להרס של מערכות.²

האם המציאות של 11 בספטמבר 2001, בה ארגון טרור התכונן במשך כשנתיים לפיגוע, כולל הכשרת טייסים בקורס טיס, שלבסוף השתמשו בסכינים יפניות פשוטות לבצע מגה פיגוע, יכול לחזור על עצמו במרחב הסייבר? האם תרחיש, בו ארגון טרור ישלח קבוצת טרוריסטים כסטודנטים לקורסים רלוונטיים במדעי המחשב, יחמש אותם באמצעים טכנולוגיים נגישים לכל, ויבצע באמצעותם ובאמצעות היכולות שרחשו מגה פיגוע טרור במרחב הסייבר הוא מציאותי או דמיוני? כדי לתת מענה לשאלה זו יש לבחון, ראשית, מהן היכולות ששחקן לא מדינתי מסוגל להשיג והאם יכולות אלו עלולות להוות איום ממשי על ביטחון הלאומי של מדינות. ניתוח האיומים העיקריים שבפניהם עומדת מדינה, בראייה רב-שנתית ולאור שינויים צפויים במאזן האסטרטגי שלה, מחייב הצגת הגורמים המאיימים על המדינה, תוך זיהוי שורשי האיום וסיבותיו.

אין עוררין על כך שגורמים לא מדינתיים, ארגוני טרור ועבריינים ממנפים את מרחב הסייבר למטרותיהם ומפיקים תועלת מתחום שבו כולם ניצבים באותה נקודת זינוק, תחום המאפשר גם לשחקנים יחידים קטנים להשפיע, ובאופן שאינו נמצא ביחס ישר לגודלם. אסימטריה זו מייצרת סביבה סכנות שונות, שבעבר לא משכו את תשומת הלב ואת האנרגיות של המעצמות. השאלה היא האם פעילותם של גורמים אלה במרחב הסייבר היא איום בעל פוטנציאל לנזק גדול ורחב היקף? ואם כן, מדוע הוא לא התממש עד כה?

מאמר זה יבחן האם התקפות של ארגוני טרור במרחב הסייבר, שהשפעתן עד היום היא בדרך כלל טקטית, יוכלו להשתדרג (ואולי כבר השתדרגו) לכלל יכולת להפעיל נשק סייבר בעל השפעות אסטרטגיות, נשק היכול לגרום נזק רחב היקף ו/או לאורך זמן, מהסוג ש"מוריד מדינות על ברכיהן" וגורם למערכות קריטיות לקרוס. מטרת מאמר זה היא לדון באיום הטרור במרחב הסייבר ולבחון את אמיתות התפיסות שהתגבשו בשנים האחרונות כלפי איום זה.

המאמר מתרכז בפעולות של ארגונים לא מדינתיים בעלי סדר יום ומטרות פוליטיות, גם אם אלה מופעלים או נתמכים לעיתים על ידי מדינות. זאת, כדי להבדיל בין אותם ארגונים לבין פעולות המבוצעות ישירות על ידי מדינות שאינן בתחום עיסוקו של מאמר זה, או על ידי ארגוני פשיעה או ארגונים אחרים בעלי מטרות שהן בעיקר בעלות אופי פלילי. לצורך המאמר, פעולת טרור של ארגון לא מדינתי במרחב הסייבר תוגדר כפעולה במרחב זה, שמטרתה לפגוע באופן מכוון או חסר אבחנה באזרחים. כך, לדוגמה, פעולה לשיבוש אתר אינטרנט של בנק מסחרי על ידי ארגון לא מדינתי, שלו מטרות פוליטיות, תוגדר כפעולת טרור במרחב הסייבר. לצורך המחשה ניתן להתבונן בתרשים הבא, המתאר את מרחב הדיון במאמר זה:



המתודולוגיה של המחקר

מספר אבני דרך נדרשו לצורך בחינת פעילותם של ארגוני הטרור במרחב הסייבר. הראשונה שבהן הייתה זיהוי המניעים לשימוש במרחב הסייבר במסגרת המאבק הפוליטי אותו מנהלים ארגוני הטרור. כך ניתן לזהות שני מניעים עיקריים לשימושים אלה: הראשון הינו השימוש במרחב הסייבר לצרכי תמיכה בפעילות הטרור, ובעיקר לצרכי גיוס כספים ופעילים, או לצורך הלבנת כספים לצרכי הפעילות; השני הינו השימוש בכלים במרחב הסייבר שיספקו את הפגיעה בפועל ביעדים שקבע לעצמו ארגון הטרור, וזאת לצד שימוש באמצעים אלימים אחרים. כאן נבחן שיתוף הפעולה שבין ארגונים לא מדינתיים לבין מדינות המפעילות אותם והתומכות בפעילות הטרור שלהם.

אבן הדרך השנייה של המחקר חייבה בחינה והבנת עומק של היכולות עליהן יכולים ארגוני הטרור להניח יד. זאת, מתוך הבנה שלא כל מפעיל מחשב, יהיה זה גאון טכנולוגי ככל שיהיה, יוכל לייצר פיגוע טרור אפקטיבי ומשמעותי, ותוך

בחינת ההנחה שפגיעה משמעותית במרחב הסייבר תמשיך להיות נחלתן של מדינות עתירות טכנולוגיה ומחייבת משאבים לא מבוטלים – הן מודיעיניים והן טכנולוגיים. עם הבנת סל היכולות הטכנולוגיות והמודיעיניות הרלוונטיות של ארגוני הטרור, נדרש היה לבחון האם זוהו פעולות של ארגונים כאלה בפועל. לבסוף, נעשה ניתוח של כלל הממצאים במטרה לגבש תובנות והמלצות מסכמות כחלק מהמענה.

ניתוח יכולות

מרחב הסייבר מסייע להעמקת ידע ורכישת יכולות. בנוסף, הטכנולוגיה מסייעת ליצירת רשת תקשורת אנונימית.³ כמו כן, מרחב הסייבר משמש מצע להרחבת השותפים לפעילות טרור. לעומת גיוס פעילי טרור במרחב הפיזי, מרחב הסייבר מאפשר הגדלה משמעותית של מאתר המשתתפים בפעילות, גם אם במקרים רבים נעשה שימוש בשותפים "משוטטים", המופעלים על ידי ארגונים ומדינות באצטלה של פגיעה במסד. תופעות כאלו ניתן היה לראות באירועי התקיפה של האקרים על יעדים ישראלים ב-7 באפריל 2013,⁴ כאשר חלק מהפעילים במתקפה קיבלו הכוונה, באמצעות אתרי אינטרנט בכיסוי, באשר לשיטות הפעולה וליעדים לתקיפה. שימוש בתחושות אנטי-ממסדיות של צעירים, כמו גם בתחושות כלליות נגד המערב או מדינת ישראל, מאפשר הרחבה משמעותית של מאתר הפעילים וכן מייצר מסה משמעותית המאפשרת את פעולת טרור הסייבר. לדוגמה, נטען שבמצע "עמוד ענן" נרשמו יותר ממאה מיליון מתקפות סייבר על אתרים ישראלים,⁵ וכי פעילים לא מעטים הופעלו במהלך אותו מבצע ובהתקפות המשך שלו, באמצעות הכוונה שמאחוריה עמדו ככל הנראה איראן וגרורותיה.⁶

סל היכולות והאמצעים של ארגוני טרור במרחב הסייבר מוגבל מצד אחד בשל קשר הדוק ונגישות טכנולוגית, שהינה בדרך כלל נחלתן של מדינות בעלות יכולות טכנולוגיות מתקדמות ושל חברות בעלות יכולות טכנולוגיות משמעותיות, ומן הצד השני – נגיש לשוק החופשי המאפשר מסחר בכלי נשק קיברנטיים ובימידע בעל ערך לתקיפה. גורם מסייע בבניית יכולות אלו הוא מדינות התומכות בטרור, המעוניינות להשתמש במתווך (Proxy) כדי להסתיר את זהותן כיוזמות תקיפה על יעד מסוים. בנוסף, נדרש ארגון הטרור להכשרת מומחים ולצבירת ידע על שיטות איסוף מודיעין, שיטות תקיפה ואמצעים להסוואת כלי תקיפה, כדי לחמוק ממערכות הגנה ביעד.

המחקר מראה שעד עתה אין לארגוני הטרור את התשתית המדעית והטכנולוגית העצמאית לפיתוח כלי סייבר בעלי יכולות לגרום נזק משמעותי, וכי הם חסרים את היכולת לבצע איסוף מודיעין איכותי למבצעים (מל"ם). היכולות

של ארגוני הטרור לקיים פעילות פוגענית במרחב הסייבר ייבחנו, אפוא, תחת אילוצים אלה.

ככלל, יש להפריד בין שלושה מרחבי תקיפה בסיסיים: תקיפה של שער הארגון, בעיקר אתרי אינטרנט, וזאת באמצעות תקיפות, מניעת שירות או השחתה של אתרים; תקיפה של מערכות המידע הארגוניות;⁷ ולבסוף, התקיפה המתוחכמת (והמורכבת) ביותר – תקיפת מערכות הליבה המבצעיות⁸ של הארגון, הנוגעות לליבה התפעולית שלו, למשל מערכות בקרה תעשייתיות.⁹ טרור הסייבר נגד מדינה ואזרחיה יכול להתבצע במספר רמות תחכום, כאשר בכל רמה נדרשות יכולות הן בהיבט הטכנולוגי והן בהיבטי ההשקעה בצד התוקף. הנזק שאפשר לגרום נמצא ביחס ישיר לרמת ההשקעה.

תקיפת שער הארגון

כאמור, ברמה הבסיסית ביותר ניתן לתקוף את שער הארגון, כלומר את אתר האינטרנט שלו, החשוף לציבור. הרמה הפשוטה ביותר של טרור קיברנטי מתאפיינת בהתקפות המונעות שירות, מפריעות לשגרת החיים, אך לא גורמות לנזק מהותי, בלתי הפיך או מתמשך. התקפות כאלו מכונות "התקפות מניעת שירות מבוזרות" (DDoS – Distributed Denial of Service), ומהותן היא גרימת עומס פניות אל מחשב או שירות אינטרנטי מסוים, באופן שחורג מסף היכולת שלו לספק מענה. בכך משיגים למעשה השבתה של השירות. פניות תמימות ואמיתיות לא ייענו, מכיוון שהשירות עמוס בהתמודדות שלו עם הפניות מצד התוקף.

התקפות DDoS אותן יבצע ארגון טרור¹⁰ נדרשות להיות אפקטיביות ולהימשך פרק זמן סביר, כדי שמספר רב ככל האפשר של אנשים יבחינו במתקפה וייפגעו ממניעת השירות. יעדים מתאימים למתקפה כזו יכולים להיות, בין היתר, בנקים, שירותי סלולר, חברות טלוויזיה בכבלים ובלווין, ושירותי בורסה (מסחר וחדשות). לרשימה זאת ניתן להוסיף גם אפליקציות סלולריות נפוצות, ששיבוש הגישה אליהן יכול לגרום למטרד, דוגמת: WAZE, גישה לשירותי דואר אלקטרוני וליומן פגישות, וגם אפליקציות לשיחות על גבי רשת האינטרנט (Voice Over IP).

שיטה נוספת לתקיפת שער הארגון היא תקיפות על שרתי DNS – שרתים המשמשים לניתוב תעבורת האינטרנט. תקיפה כזו תביא לכך שאנשים המבקשים לגשת לאתר או לשירות מסוים יגיעו בפועל לאתר אחר, אליו התוקפים מעוניינים לנתב את התעבורה. תקיפה דומה אך פשוטה יותר יכולה להתבצע ברמת המחשב הבודד במקום ברמת שרת ה־DNS הכללי; כלומר, התקשורת ממחשב בודד תנותב לאתר של התוקף במקום לאתר האמיתי אליו המשתמש מנסה לגלוש. הנזקים שתקיפות כאלו יכולות לגרום נעים מגניבת מידע, דרך מניעת שירות מלקוחות וכתוצאה מכך פגיעה עסקית בשירות שהותקף, ועד פגיעה תדמיתית בשירות:

התוקף יכול להפנות את התעבורה אל דף המכיל תעמולה ומסרים אותם הוא רוצה להציג לציבור.

שיטה פופולרית ויחסית פשוטה לפגיעה תדמיתית בשער הארגון היא השחתת אתר האינטרנט שלו. ההשחתה (Defacement) כוללת שתילת מסרים פוגעניים בעמוד הראשי, הכנסת תעמולה שהתוקפים מעוניינים להפיץ לקהל רחב ופגיעה תדמיתית (ואולי גם עסקית) בארגון, הנתפס כלא מוגן ולא מאובטח מפני תוקפים פוטנציאליים.

תקיפת מערכות המידע של הארגון

רמת הביניים במדרג הפגיעה במרחב הסייבר מכילה תקיפות של מערכות המידע והמחשוב של הארגון, דוגמת שרתים, מערכות מחשב, מאגרי נתונים, רשתות תקשורת ומכונות לעיבוד נתונים. התחכום הטכנולוגי הנדרש ברמה זו גבוה יותר מהנדרש לצורך תקיפת שער הארגון. רמה זו מחייבת השגה של נגישות למחשבי הארגון דרך עובדים בארגון או באמצעים אחרים. הנזק אותו ניתן לגרום בסביבה הווירטואלית כולל פגיעה בשירותים חשובים כמו בנקים, שירותי סלולר ודואר אלקטרוני.

קו ברור מפריד בין התקיפות המתוארות כאן ובין האיומים של הטרור הקיברנטי הפיזי: בדרך כלל לא ניתן לצפות בתקיפות אלו לנזק פיזי, אולם ההסתמכות על שירותים וירטואליים והנגישות אליהם עלולה בכל זאת לייצר פגיעה משמעותית. דוגמה לכך ניתן לראות בתקיפה באמצעות וירוס המחשבים Shamoon,¹¹ שפגע במחשבי חברת הנפט הסעודית ערמקו (Aramco) באוגוסט 2012. התקיפה, גם אם לא פגעה במערכות הליבה המבצעיות של החברה, הצליחה להשבית עשרות אלפי מחשבים ברשת הארגונית שלה, תוך גרימת נזק משמעותי באמצעות מחיקת מידע ממחשבי הארגון והאטת פעילותו לאורך זמן.¹²

תקיפת מערכות הליבה המבצעיות של הארגון

הרמה הגבוהה ביותר במדרג סיכון התקיפה הינה התקיפה של מערכות הליבה המבצעיות והתפעוליות של הארגון. לדוגמה, ניסיון פגיעה בתשתיות קריטיות פיזיות כמו תשתיות הולכת מים, חשמל, גז, דלק, מערכות בקרה על תחבורה ציבורית, או מערכות תשלומים בנקאיות. זאת, על ידי מניעת אספקת השירות החיוני לזמן מסוים, או במקרה החמור אף גרימה של נזק פיזי באמצעות פגיעה במערכות הפיקוד והבקרה של הארגון הנתקף.

מתקפה מוצלחת עלולה לגרום לשחרור חומרים מסוכנים לאוויר ולפגיעה פיזית באוכלוסייה גדולה. זוהי הנקודה בה פיגוע וירטואלי עלול לייצר נזק פיזי, וההשפעות עלולות להיות הרסניות. בעקבות חשיפת ה־Stuxnet עלתה המודעות

לצורך להגן על מערכות בקרה תעשייתיות, אך מכאן ועד יישום בפועל של פתרונות הגנה עדיין הדרך ארוכה. את הפער הזה יכולים לנצל גורמי טרור, למשל על ידי יצירת קבוצת מומחים מתחומי המחשוב ואוטומציה של תהליכים, לצורך יצירת וירוס המסוגל לפגוע במערכות אלו.¹³

דרך נוספת להשגת נשק קיברנטי-פיזי עשויה להתפתח מהשוק השחור של נשק הסייבר ומהתרחבותו גם לתחום של תשתיות פיזיות, וזאת בנוסף על הנשק הווירטואלי אותו הוא מציע כבר היום. יש לציין כי עד כתיבת שורות אלו, תרחיש זה טרם התממש בפועל, אך מכיוון שמדובר בנשק קיברנטי מורכב ויקר, ייתכן והמסחר בו מתנהל במחשכי האינטרנט באופן חשאי.¹⁴ זוהי, כאמור, המדרגה הגבוהה ביותר של פיגוע סייבר, והעלויות והנזקים הנגרמים ממנו הם גבוהים בהתאמה, כפי שניתן ללמוד מהתולעת Stuxnet.¹⁵

פיתוח יכולות תקיפה, בין של מדינות ובין של ארגוני טרור, מחייב תמהיל מתעצם של יכולות לפעולה במרחב הסייבר בשלושה מרכיבים עיקריים: יכולות טכנולוגיות, יכולת הכוונה מודיעינית לקביעת היעדים (ייצור מטרות) ויכולת מבצעית.

יכולות טכנולוגיות

אופייה המבוזר של רשת האינטרנט מקל מאד על הסוחרים בנשק קיברנטי. ואכן, האקרים וסוחרים רבים מנצלים את היתרונות הללו ומציעים כלי סייבר ושירותי תקיפה במרחב הסייבר לכל דורש. כך התפתח שוק מגוון ומשוכלל מאד של סחר במוצרי סייבר למגוון מטרות, כאשר טווח המחירים נע בין דולרים בודדים לתקיפה פשוטה וחד-פעמית של מניעת שירות, לאלפי דולרים עבור שימוש בחולשות שאינן מוכרות ויכולות לאפשר לתוקף דילוג לתוך מערכת מחשב מוגנת ביותר. שוק זה צומח בזכות מרחב הסייבר, על גבי תשתיות של רשתות חברתיות ופורומים המאפשרים תקשורת אנונימית בין סוחרים לקונים.¹⁶ תופעה מעניינת לה אנו עדים בתקופה האחרונה היא יציאתם של סוחרים אלה ממחשכי הרשת האפלה אל האור. ניתן למצוא אותם ברשת החברתית הפופולרית ביותר, "פייסבוק".¹⁷

בבלוג של חברת אבטחת המידע RSA¹⁸ מתוארת מציאות חדשה, שבה הסוחרים מציעים את מרכולתם לא רק כמוצר, אלא כשירות שלם הכולל התקנת שרתי פיקוד ובקרה, הדרכה על השימוש בכלים ואפילו הנחות ומבצעים ואפשרות לרכוש רק מודולים מסוימים מתוך כלי התקיפה, כדי להוזיל את המחיר. במצב זה של פריחת השוק נשאלת השאלה, האם וכיצד ארגוני טרור יכולים לעשות שימוש לתועלתם בכל הידע והכלים שהצטברו בשוק הפשיעה הקיברנטי?

כדי לענות על שאלה זו, נצטרך לבחון את הפער בין שפע הכלים והיכולות המוצעים כיום למכירה חופשית באינטרנט, לבין הצרכים של ארגוני טרור. השוק

של כלי התקיפה כיום מוכוון לארגוני פשיעה קיברנטית, ובעיקר לצרכי הונאות, גניבת כסף מחשבונות בנק תמימים והתחזות, תוך איסוף פרטים של כרטיסי אשראי, מספרי חשבון בנק, תעודות זיהוי וכתובות מגורים, סיסמאות כניסה לאתרים פיננסיים ועוד. כלים אלה לא מתאימים בהכרח לצרכי ארגון הטרור. עם זאת, ארגוני טרור רבים יכולים לכלול גם מרכיבים של ארגון פשיעה קיברנטי כדי לאסוף כסף למימון פעילות הטרור המרכזית שלהם. המטרה המרכזית של ארגוני הטרור – גרימת נזק משמעותי והפחדה – יכולה להתבצע במספר דרכים, בדרגות קושי וחומרה שונות. הכלים מעולם הפשיעה הקיברנטית יכולים לסייע רבות בתקיפות לשיבוש שירות (DDoS), או בגניבת כמויות גדולות של מידע רגיש מחברות שאינן מוגנות מספיק (למשל מידע על כרטיסי אשראי ממאגרי מידע לא מאובטחים) – דבר שיעזור, קרוב לוודאי, חרדה בציבור. יחד עם זאת, גרימת נזק למערכות הבקרה דורשת כבדת דרך נוספת מצדם של הטרוריסטים, שכן משימתם מורכבת הרבה יותר מגניבת כרטיסי אשראי וכלי הפשיעה הקיברנטיים לא משרתים אותה. באשר לרמת הביניים שתוארה לעיל, הנוגעת לפגיעה במערכות המידע של הארגון, נראה כי קיימים בעולם הפשיעה כלים היכולים לסייע לטרור הסייבר. אמנם, נדרשת התאמה מסוימת של כלים אלה, כמו למשל התאמה מגניבת מידע למחיקת מידע, אולם מדובר בכבדת דרך קטנה יותר, שמפתחי הווירוסים יסכימו, קרוב לוודאי, לבצע אותה עבור ארגוני טרור תמורת תשלום מתאים.

יכולת הכוונה מודיעינית

אחד המרכיבים המרכזיים בתהליך תכנון פיגוע קיברנטי הוא בחירת יעד או קבוצת יעדים שהפגיעה בהם תביא ליצירת האפקט הרצוי מבחינת ארגון הטרור. לצורך זה על גוף הטרור לרכז רשימת גופים המהווים פוטנציאל ליעדי פגיעה. כבר כיום קיימת טכנולוגיה חינומית שמספקת כלים המקלים על ביצוע משימה זו. למשל, באמצעות הרשתות החברתיות "פייסבוק" ו"לינקד-אין", ניתן לאתר מיהם העובדים באגפי המחשוב של חברות תשתית, חברות מזון ועוד. אם ניקח לדוגמה את חברת החשמל, מחקרים אקדמיים¹⁹ מראים כי ניתן למפות ללא קושי רב את אגפי החברה, לאתר את העובדים במחלקות השונות ולברור את העובדים להם יש גישה למערכות המבצעיות של החברה.²⁰ אם עובדים אלה מודעים לחשיבותה של אבטחת המידע ולא ניתן בשל כך לתקוף אותם ישירות, אפשר לאתר בני משפחה וחברים שלהם באמצעות "פייסבוק" ולתקוף דרכם את היעד המבוקש. רשתות חברתיות מהוות מקור חשוב לריגול ואיסוף מידע עסקי ואישי על חברות וארגונים,²¹ וארגוני טרור יכולים לעשות בקלות שימוש במידע המופץ בהן לתועלתם.

קיים גם צורך למפות את מערך המחשוב של הארגון המותקף, להבין אילו מחשבים מחוברים לרשת, אילו מערכות הפעלה ותוכנות הגנה מותקנות בהם, אילו הרשאות יש לכל מחשב, ודרך אילו מחשבים ניתן לשלוט במערכת הבקרה של הארגון. לדוגמה, אם ארגון טרור ירצה לשלוט על התפקוד של טורבינת ייצור חשמל, המשימה המוטלת עליו, אף על פי שהיא טכנית יותר וקשה יותר ממיפוי המבנה הארגוני של החברה, קלה היום במיוחד לאחר פרסום עבודתו של האקר "כובע לבן" שערך את "מפקד האינטרנט" הראשון בהיסטוריה.²²

באמצעות רשת ענפה של רובוטים (תוכנות המושתלות על מחשבים וממתינות לפקודה ממרכז הפיקוד והבקרה איתן הן מתקשרות), ערך אותו האקר רשימה של 1.3 מיליארד כתובות IP הנמצאות בשימוש, ועל חלקן הוא פרסם גם נתונים טכניים, כמו סוג השערים הפתוחים, לאילו בקשות מגיבות הכתובות הללו ועוד. תוצאות המפקד מפורסמות באינטרנט באופן חופשי לכל דורש. עבור האקר בעל כוונות זדון, אלה לפעמים כל הנתונים הנדרשים כדי לבצע תקיפה ולהשתלט על מערכת מחשב של אדם פרטי או ארגון. כך ניתן למפות מבנה ארגוני של חברה, ואם הרשת שלה אינה מוגנת מספיק – גם לדלות מידע על המחשבים הנמצאים בשימוש עובדי החברה.

הגנה טובה ומודעות לאבטחת מידע יכולות להקשות מאד על האקרים וטרוריסטים לבצע את הפעולות שתוארו לעיל. ארגונים להם מערכות מבצעיות קריטיות מפעילים לרוב שתי רשתות מחשוב: האחת חיצונית, המקושרת לאינטרנט, והשנייה פנימית, המנותקת פיזית מהאינטרנט ומחוברת למערכות הבקרה התעשייתיות של הארגון. מפקד האינטרנט אינו מכיל נתונים על רשתות פנימיות מבודדות, מכיוון שהן לא נגישות דרך האינטרנט. תקיפה של רשתות אלו דורשת מודיעין, משאבים ומאמץ גדול מאד, וספק אם קיימים ארגוני טרור המסוגלים לבצע תקיפות כאלו. כאן באה לעזרתם של ארגוני הטרור עבודת מחקר נוספת שנערכה על ידי חוקרים מאוניברסיטת ברלין,²³ המציגה על גבי מפה של "גוגל" (שמציעה לחוקרים, כחלק משירות המפות שלה, להציג ולשתף מידע גיאוגרפי שאספו) מספר רב של מערכות בקרה תעשייתיות (ICS) הפרוסות בכל העולם ומחוברות לרשת האינטרנט. המידע המוצג במפה לקוח מתוך מאגר מידע עצום הנגיש בחינם לכל דורש דרך האתר Shodan,²⁴ אשר הופך את חייו של האקר טרוריסט לקלים יותר. שירות זה נעזר במידע אותו אספה חברת "גוגל" לצורך שירותי המיפוי והפרסום מבוססי המיקום שלה, והפכה אותו לנגיש לציבור. ייתכן שהאקרים שפרצו לאחרונה לרשתות ביתיות של מאות ישראלים עשו שימוש בשירותיו של אתר Shodan כדי לאסוף מודיעין לתקיפה, ואולי גם כדי להשיג כלים (תחמושת קיברנטית) לביצועה בפועל.²⁵

יכולת מבצעית

לאחר איסוף המודיעין וייצור או רכישה של הכלים הטכנולוגיים לקראת התקיפה, על מתכנני הטרור הקיברנטי לעבור לפעילות אופרטיבית. זהו השלב של ביצוע התוכנית בפועל, המנוהל באמצעות וקטור תקיפה.²⁶ הכוונה במושג זה היא לשרשרת פעולות המתבצעות על ידי התוקפים, כאשר כל פעולה מהווה מדרגה אחת בדרך ליעד הסופי וכוללת, בדרך כלל, שליטה מלאה או חלקית על מערכת מחשב או על מערכת בקרה תעשייתית. בווקטור תקיפה לא ניתן לדלג על מדרגות, וכדי להתקדם למדרגה מסוימת, יש לוודא שכל השלבים שלפניה הסתיימו בהצלחה.

השלב הראשון בווקטור תקיפה הוא, בדרך כלל, יצירת נגישות ליעד. שיטה נפוצה מאד ומוצלחת ליישומו במרחב הסייבר מכונה Spoofing²⁷ או זיוף. יש דרכים שונות לעשות שימוש בשיטה זו, כאשר המשותף לכולן הוא זיוף הזהות של שולח הודעה כדי שנמען ההודעה יבטח בתוכן ולא יהסס לפתוח קישור בתוך ההודעה. למשל, קל מאד לשלוח דואר אלקטרוני לעובד בחברת החשמל, שהוזכרה לעיל, כאשר השולח המזייף משתמש בכתובת של עמית לעבודה, בן משפחה או אדם קרוב אחר. מטרת התוקף במקרה זה היא לגרום לנמען ההודעה לבטוח בתוכן ההודעה ולפתוח דבוקות המצורפות אליה, או להיכנס לכתובות אינטרנט המופיעות בתוכה.

זיוף דואר אלקטרוני הוא שיטת תקיפה הקיימת שנים רבות. בהתאם לכך גם פותחו אמצעי הגנה נגדה אלא שגם התוקפים צברו ניסיון. כיום ניתן להצביע על אירועים שבהם נשלח דואר אלקטרוני הנראה תמים לחלוטין, תפור לנמען ומכיל התייחסות אישית אליו, ובתוכו קיימים מסמכים הנוגעים ישירות לתחום עיסוקו. כתובת השולח במקרים אלה הייתה מזויפת והופיעה ככתובת של עמית לעבודה. ברגע שהנמען פתח את הדואר האלקטרוני, המחשב שלו נדבק בוירוס ללא ידיעתו. שיטת הזיוף יכולה להועיל כאשר היעד הוא מחשב המחובר לרשת האינטרנט ויש אפשרות לשלוח אליו הודעות, אך במקרים מסוימים לא זה המצב. רשתות המוגנות ברמה גבוהה יהיו, בדרך כלל, מנותקות מהעולם החיצון באופן פיזי, כלומר לא יהיה קישור פיזי (גם לא אלחוטי) ביניהן ובין רשת בעלת רמת אבטחה נמוכה יותר. במקרה כזה יצטרך התוקף לנקוט צעד אחר או נוסף בווקטור התקיפה – הדבקת רשת היעד בוירוס באמצעות החדרתו על גבי מכשירים שפועלים גם ברשת הלא מוגנת וגם ברשת המוגנת. דוגמה לכך הם התקני Disk On Key, המשמשים כאחסון נייד ונוח של קבצים. כאשר התקפה כזו מצליחה, התוקף משיג גישה אל ציוד טכנולוגי השייך לקורבן (מחשב, מחשב כף יד, טלפון חכם), והשלב הראשון בווקטור התקיפה – יצירת נגישות ליעד – מסתיים. בתרחישים מסוימים הצעד הזה הוא החשוב והמשמעותי ביותר מבחינת התוקף. למשל, כאשר הושגה בדרך זו

נגישות לרשת מבצעית של חברה, ומטרתו של הטרוריסט היא לחבל באותה הרשת ולמחוק מתוכה מידע, האתגר העיקרי הוא להשיג גישה ליעד. פעולת המחיקה והחבלה קלות יותר, בהנחה שהווירוס שהושתל ברשת מופעל ברמת הרשאות מספיק גבוהה. אך בתרחישים מורכבים יותר, כאשר הטרוריסט מעוניין לגרום נזק משמעותי ולהשיג אפקט הפחדה גדול יותר, נדרשת השקעה לא מבוטלת בצעדים הבאים בווקטור התקיפה.

חברת "לוקהיד־מרטיין", שהייתה קורבן להתקפת סייבר, מציעה מתודולוגיה לניתוח פעולות התקפיות במרחב הסייבר, אותה היא מכנה "שרשרת הקטל הקיברנטית"²⁸. על פי מתודולוגיה זו, מתקפת סייבר מורכבת בנויה משבע אבני דרך, המקבילות לפעולות של הכנת המבצע ויצירת וקטור התקיפה. הצעד הראשון הוא איסוף מודיעין על היעד. לאחר מכן יש לבחור את כלי הנשק הקיברנטי המתאים לתקיפה, ואז לשגר אותו אל היעד. הצעד הבא כולל ניצול חולשה אצל מחשב היעד, שתאפשר לשתול קובץ זדוני במערכת שלו, ולאחר מכן להתקין את הכלי באופן שיוכל לבצע פעולות בתוך המערכת. השלב הבא הוא יצירת תקשורת בין הכלי ובין שרתי הפיקוד והבקרה של התוקף, כדי שניתן יהיה להנחות את הכלי ולקבל ממנו דיווח על המתרחש במחשב הקורבן. השלב האחרון בשרשרת הקטל הוא ביצוע פעולות אקטיביות בתוך מחשב הקורבן, כמו מחיקה, התפשטות של הכלי, השתלטות על התקנים פיזיים הנגישים מהמחשב ועוד. המונח "שרשרת קטל קיברנטית" נבחר במטרה להדגיש כי כדי שהתוקף יצליח לבצע פיגוע קיברנטי, הוא צריך לצלוח את כל אבני הדרך מבלי להתגלות ומבלי שגישתו אל היעד תיחסם. ארגון טרור המבקש לפגוע במערכות מבצעיות יצטרך לבצע את כל השלבים בשרשרת. אלו הן פעולות מתקדמות ומורכבות שארגוני טרור בדרך כלל לא ידעו לבצע בעצמם. אם היעד מוגן ברמה נמוכה מאד, לא תידרש יכולת טכנולוגית גבוהה מהתוקף כדי לייצר פגיעה או השחתה; אך ברוב המקרים יצטרכו הטרוריסטים לרכוש מוצרים או שירותים מהאקרים מומחים. במילים אחרות, הם יצטרכו לבצע "מיקור חוץ".

טרוריסטים ימצאו בשוק מוצרי הסייבר ההתקפיים יכולות נגישות ליעד שאינן בעלות רשת מבודלת. באותו שוק הם ימצאו גם מוצרי תקיפה, וניתן להניח שימצאו גם מוצרים לניהול מבצעים ברשת היעד (בדומה לממשק הניהול של הסוס הטרואני SpyEye²⁹). למרות כל זאת, טרם זוהו כלים זמינים ברשת המאפשרים תקיפה של המערכות המבצעיות של הארגון. הנגישות לכלים אלה אמנם אפשרית,³⁰ אך היא משימה הדורשת משאבי כוח אדם רב (מרגלים, פיזיקאים, מהנדסים), השקעה כספית (בפיתוח כלי תקיפה ובדיקתו בתנאי מעבדה על ציוד אמיתי) וזמן רב כדי לאתר חולשות ולבנות וקטור תקיפה מוצלח.

סוגי התקיפות במרחב הסייבר

ניתן לאפיין מספר סוגי תקיפה במרחב הסייבר, הן לפי רמת הנזק הצפויה והן לפי עוצמת ההשקעה המודיעינית, הטכנולוגית והמבצעית. ברוב המקרים קיימת הלימה בין שני המדדים. הסקירה להלן מציירת תמונה של יכולות ארגון שאינו מדינתי לפעול במרחב הסייבר.

תקיפה חובבנית

זוהי פעולה הנעשית באמצעות כלים המוכרים (ברוב המקרים) לחברות אבטחת המידע ומזוהים על ידי תוכנות ההגנה הסטנדרטיות. נגד כלים אלה פותחו הגנות ולפיכך הם עשויים להיות אפקטיביים רק מול מטרות שאינן מוגנות. שימוש בכלים כאלה נעשה, בדרך כלל, למטרות לימוד או משחק בלבד, מכיוון שרק במקרים נדירים הם יכולים לשמש לגניבת מידע בעל ערך או לחבלה במערכות מחשב מוגנות. אמנם, יש להם יכולות ריגול וחבלה, אך אלו הן ברמת תחכום נמוכה.

תקיפה קלה

זוהי תקיפה שלא מושקעים בה מאמצים רבים, ועיקר הפעילות בה היא חיפוש כלים מוכנים ברשת האינטרנט או רכישתם מידי חברות המתמחות בכך. תקיפות מסוג זה בדרך כלל לא יצליחו לפגוע בגופים בעלי מודעות לאבטחת מידע (גופים מדינתיים, צבאיים, תעשיות מתקדמות), אבל יוכלו לחדור למחשבים פרטיים ולגנוב מהם מידע ואף לחבל בהם. תקיפות אלו הינן ברוב המקרים חד-פעמיות (גניבת קובץ חשוב, מחיקת כונן), אך לעיתים יכולות להיות חלק מתקיפה ארוכה יותר, כמו למשל במקרה של גניבת ה-DNS (Domain Name System) של המחשב המאפשרת מעקב אחר הפעילות שלו ברשת האינטרנט.

הכלים בהם ייעשה שימוש בתקיפה קלה לא יכללו מודולים שונים של תוכנה, אלא רכיב קוד אחד שעלותו זולה, המבצע את כל הפעולות של הכלי. רכיב קוד זה יהיה כתוב בצורה שלא מאפשרת לשנות או להרחיב בקלות את יכולותיו ויהיה מוכוון מטרה. חיפוש באינטרנט ורכישה בסכומים שלא עולים על כמה אלפי דולרים יוכלו לספק לכל דורש נשק סייבר בעל יכולות מצומצמות.

בקטגוריה זו של תקיפה נכלל גם השימוש ברשת סוכני תוכנה (בוטנט) לתקיפות DDoS. יצירת הרשת היא פעולה מורכבת יותר, אך מרגע שנוצרה, היא יכולה לשמש למבצעי DDoS רבים. ניתן גם להשכיר אותה לשימוש לכל דורש לצורך מניעת שירות מאתרים שונים שאינם מוגנים ברמה גבוהה מפני תקיפה כזו.

תקיפה בינונית

זוהי תקיפה המסוגלת לגרום נזק משמעותי, או לבצע פעולות ריגול מתקדמות, אבל בעלות נמוכה יותר מאשר תקיפה חמורה (ראו להלן). בפעולה כזאת לא יהיה, בדרך כלל, שימוש בחולשות ייחודיות חדשות (כיוון שהן יקרות מאד), אלא בחולשות מוכרות או מוכרות חלקית, שיעד התקיפה עדיין אינו מוגן מפניהן. הפעולה לא תכלול מודולים יקרים למימוש ובדיקה, דוגמת אה שפותחו עבור "סטוקסנט". יחד עם זאת, פעולה כזאת, באמצעות מודולים לתקיפה של מערכות מחשב (מחיקה, שיבוש) ומודולים לריגול, יכולה להיות יעילה מאד במסגרת תקיפה בטווחי זמן קצרים למטרות הרס (כי לא ייעשה מאמץ להסתיר את ההרס; הדבר יקר מדי), או לריגול נגד קורבן שלא מאבטח את מערכותיו ברמה גבוהה.

העלות של תקיפה בינונית פחותה משמעותית מעלותה של תקיפה חמורה: פחות שנות אדם, ללא ציוד חומרה ייחודי ויקר להשגה וללא רכישה של חולשות חדשות ויקרות, אלא של חולשות זולות יותר המספיקות לצורך חדירה למערכות המחשוב של הקורבן, תוך ידיעה שהן עלולות להתגלות ולהיחסם בעתיד הלא רחוק. קטגוריית התקיפה הבינונית כוללת גם וירוסים המסוגלים להתפשט ברשת מחשבים (תולעים) ולהמתין לפקודה מהמפעיל שלהם. מודל תקיפה כזה שימושי במיוחד ליצירת רשת סוכני תוכנה רובוטיים, המשמשת למבצעי DDoS. כמו כן נכללת בקטגוריה זו תקיפת DDoS נגד אתרים מוגנים, הדורשת תחכום מצד התוקף והכרת מערכת ההגנה ביעד.

תקיפה חמורה

המדובר בפעולה שהושקעו בפיתוחה משאבים רבים של כוח אדם, מחשוב וכסף, ואשר נבדקה באופן יסודי במעבדה קודם להפעלתה. פעולה כזאת מנצלת חולשות לא מוכרות (אשר יתנו למפעילי התקיפה טווח זמן רחב להפעלתה עד שיתגלו וייסגרו). בדרך כלל זו פעולה שתוסווה כדי להותיר עקבות מעטות. כלי התוכנה יכיל מספר מודולים, שחלקם עשויים להיות מיועדים לחבל במערכות תוכנה או חומרה ייעודיות שנמצאות אצל הקורבן (למשל "סטוקסנט"), ולא יפעלו בשום מקרה אחר, כדי להפחית אפשרות לזיהוי.

פעולת תקיפה חמורה עשויה להכיל מגוון רחב מאד של מודולים, בהתאם למטרה שאותה היא נועדה לתקוף, כגון מודולי ריגול – חיפוש קבצים או מידע ושליחתו למפעיל; ומודולי תקיפה והסוואת התקיפה – חבלה בצנטריפוגות תוך כדי הטעייה של מערכת הבקרה כדי שתדווח שהן תקינות. העלות של תקיפה כזו תהיה שנות אדם רבות, מחשוב מתקדם ולפעמים גם מערכות חומרה וציוד בדיקה שנועד לדמות את הזירה בה יפעל הקוד המפגע, למשל צנטריפוגות עם מערכות בקרה של חברת "סימנס" במקרה של "סטוקסנט".

הטבלה הבאה מסכמת את ההבדלים בין תקיפות הסייבר השונות, וזאת באמצעות רשימת קריטריונים המאפשרת להבחין באופן ברור בין סוגי נשק סייבר על פי מדרג יכולות. הפרמטרים מתחלקים למספר קטגוריות: הראשונה כוללת את מעטפת נשק הסייבר ואת היכולת שלו להגיע אל יעדו ולפעול בו באופן חופשי מבלי שייחסם. שני הפרמטרים הראשונים נכללים בקטגוריה זו. חשיבותם היא בכך שהם מאפשרים סביבת עבודה נוחה לתוקף, היודע שהוא יכול לחדור אל יעדיו ולבצע בהם פעולות בזמן ובאופן הנדרש, מבלי לחשוש מסגירת היכולת או מחשיפה של הנשק והסרתו. שלושת הפרמטרים הבאים מהווים קטגוריה שנייה, המתייחסת ליכולת הנשק הקיברנטי לבצע את פעילותו העיקרית ביעד, בין אם מדובר בגניבת מידע, הריסתו, פגיעה ושיבוש אלקטרוניים או פיזיים. כלי הנשק השונים בקטגוריה זו נבדלים על פי האלגוריתמים שהם מיישמים לטובת ריגול ביעד ועל פי יכולותיהם לשבש מערכות ממוחשבות ופיזיות. יכולת פגיעה פיזית תהווה מדרגה עליונה בקטגוריה זאת. הקטגוריה האחרונה מייצגת שני פרמטרים הקשורים להתנהלות הכלי בתוך רשת היעד, ומידת היכולת והחופש שהוא נותן למפעיליו לנהל את המבצע ביעד. יכולות גבוהות בקטגוריה זו נחשבות לכאלו שמאפשרות לעדכן את כלי הנשק על ידי שליחת מודולים מרחוק, שינוי הגדרות המשימה, שליחת פקודות לכלי והגדרת יעדים מודיעיניים חדשים עבורו. כמו כן, כלים מתוחכמים יידעו לנהל מבצע איסוף גדול ברשת היעד, על ידי התפשטות בין מחשבים שונים ואיסוף מרוכז ומתואם של מידע מתוכם.

ההבדלים בין תקיפות הסייבר

תקיפה חובבנית	תקיפה קלה	תקיפה בינונית	תקיפה חמורה	
נמוכה	טובה	טובה	טובה מאוד	יכולות חדירה למערכות
נמוכה	בינונית	טובה	טובה מאוד	יכולות הסוואת הפעילות
בינונית	טובה	טובה מאוד	טובה מאוד	יכולות ריגול
נמוכה	טובה	טובה מאוד	טובה מאוד	יכולות פגיעה במערכות מחשוב
נמוכה	נמוכה	נמוכה	טובה	יכולות פגיעה במערכות פיזיות המקושרות למערך המחשוב
נמוכה	נמוכה	טובה	טובה מאוד	יכולות התפשטות
נמוכה	בינונית	טובה	טובה מאוד	יכולות תקשורת מול שרת בקרה

ניתן ללמוד מהטבלה כי הקריטריונים המבדילים באופן משמעותי את יכולות התקיפה החמורה (המצויה בידי מדינות מעטות) משאר יכולות התקיפה בסייבר הם היכולת להתפשט ברשת, לקיים תקשורת מול שרת הבקרה ולפגוע במערכות פיזיות המקושרות למערכות המחשוב. אלו הן הפעולות הדורשות את התחכום הרב ביותר בייצור תקיפות סייבר. רק מדינות מעטות נגישות לידע וליכולת לייצר כלי נשק מסוג זה. העמודה "תקיפה קלה" בטבלה משקפת את מדרגת הכניסה הנמוכה למרחב הלחימה הקיברנטי. ניתן לראות כי גם כלי נשק קטנים המצויים בידי גורמים לא-מדינתיים מסוגלים לחדור למערכות מחשב בצורה טובה, לבצע ריגול ברמה טובה מאד, ואם הם מיועדים לכך – גם לחבל במערכות המחשב אליהן הם חדרו. מכיוון שיכולת ההסוואה שלהם היא בינונית, הם לא יוכלו לשהות במערכת המותקפת זמן רב כמו כלי נשק כבדים או בינוניים, ולכן יצטרכו להשיג את מטרותיהם בטווח זמן קצר.

פעילות במרחב הסייבר המיוחסת לארגוני טרור

פרק זה מפרט פעולות טרור במרחב הסייבר בהתאם לתיחום שפורט לעיל, כלומר פעולות שמטרתן פגיעה מכוונת או חסרת אבחנה באזרחים, וזאת באמצעות פעולה במרחב הסייבר של ארגונים לא מדינתיים בעלי סדר יום ומטרות פוליטיות, גם אם אלה מופעלים או נתמכים לעיתים על ידי מדינות.

אחת ההתקפות המתועדות הראשונות של ארגון טרור נגד מערכות מחשוב מדינתיות התרחשה בסרי-לנקה על ידי לוחמי הגרילה "הנמרים הטמילים" ב-1998. שגרירויות של סרי-לנקה ברחבי העולם הוצפו במשך שבועיים בכ-800 הודעות דואר אלקטרוני ביום עם המסר: "אנחנו נמרי האינטרנט השחורים ואנחנו הולכים לשבש את מערכות התקשורת שלכם". יש הטוענים כי מסר זה השפיע על המקבלים אותו וזרע חשש ופחד בשגרירויות.³¹ מספר שנים לאחר מכן, ב-3 במארס, 2003, כת יפנית בשם Aum Shinrikyo ("האמת העליונה") ערכה מתקפה קיברנטית מורכבת שכללה השגת מידע רגיש הנוגע למתקני גרעין ברוסיה, אוקראינה, יפן ומדינות נוספות, תוך ניסיון לתקוף את מערכות אבטחת המידע של המתקנים. המידע הוחרם וניסיון התקיפה נכשל לפני שהארגון הצליח לפעול.³²

תקיפה באמצעות שליח התקיימה בינואר 2009 בישראל. באירוע זה התקיפו האקרים את תשתית האינטרנט של ישראל בתגובה למבצע "עופרת יצוקה" ברצועת עזה. התקיפה בוצעה על יותר מחמישה מיליון מחשבים. בישראל משערים שהיא נעשתה ממדינות שהיו חלק מברית המועצות לשעבר, בהוראה ובתשלום של גורמי חמאס וחזבאללה.³³ בינואר 2012, קבוצת האקרים פרו-פלסטיניים הקוראת לעצמה "Nightmare" הפילה למשך זמן קצר את אתר הבורסה לניירות ערך בתל אביב ואת אתר חברת "אל על" ושיבשה את פעילות אתר "הבנק הבינלאומי

הראשון". בהתייחסות לכך מסר דובר חמאס ברצועת עזה כי "החדירה לאתרים ישראלים פותחת מרחב חדש של התנגדות ומלחמה אלקטרונית חדשה נגד הכיבוש הישראלי".³⁴

מלחמת האזרחים בסוריה הביאה לפעילות התקפית ערה מצד ארגון "הצבא הסורי האלקטרוני" (Syrian Electronic Army – SEA) – קבוצה אינטרנטית המורכבת מהאקרים תומכי משטר אסד, התוקפת את קבוצות האופוזיציה הסוריות תוך שימוש בטכניקות של מניעת שירותים ומידע או פריצה לאתרים ושינוי תוכנם. הקבוצה הצליחה להוציא לפועל פעולות שונות הפוגעות בעיקר באתרי האופוזיציה הסורית, כמו גם באתרי אינטרנט מערביים. פעילות אחרונה זו שלה מכוונת בעיקר כלפי אתרי מדיה, תרבות וחדשות ברשתות מערביות. הקבוצה הצליחה לפרוץ ליותר מ-120 אתרים, ביניהם, *The Financial Times*, *The Telegraph*, *The Washington Post*, *Al Arabia*.³⁵ הייתה באפריל 2013, בעת ש"הצבא הסורי האלקטרוני" פרץ לחשבון הטוויטר של *Associated Press* ושתל "ציוץ" מזויף, שבו נאמר שהבית הלבן הופץ ושבאותה מתקפה נפצע נשיא ארצות הברית. המשמעות המיידית של הודעה זו הייתה צניחה חדה בשווקים הפיננסיים בארצות הברית ובמדד דאו ג'ונס למשך כמה דקות.³⁶ הארגון גם חשוד בניסיון חדירה למערכות שליטה ובקרה של מערכות מים. כך, למשל, ב-8 במאי 2013 פורסם בסוכנות ידיעות איראנית צילום מסך של מערכת ההשקיה של קיבוץ סער.³⁷

במהלך מבצע "עמוד ענן" ברצועת עזה ב-2012 וכן בחודשים שלאחריו, ערכה קבוצת האקרים המכנה עצמה "OpIsrael" תקיפות³⁸ נגד אתרים ישראלים על רקע הסכסוך הישראלי-פלסטיני, בשיתוף עם "אנונימוס". בין היתר נפגעו אתר משרד ראש הממשלה, אתר משרד הביטחון, אתר משרד החינוך, אתר המשרד לאיכות הסביבה, אתר התעשייה הצבאית, אתר הלשכה המרכזית לסטטיסטיקה, אתר האגודה למלחמה בסרטן, האתר הרשמי של לשכת נשיא המדינה ועוד עשרות אתרים ישראלים קטנים. הקבוצה פרסמה כי הסיבות לתקיפה היו פגיעה בזכויות אדם של פלסטינים והפרת החוק הבין-לאומי על ידי ישראל.

באפריל 2013, קבוצת האקרים פרו-פלסטיניים, בשם "לוחמי הסייבר של עז א-דין אל קסאם" המזוהה עם הזרוע הצבאית של חמאס, לקחה אחריות להתקפה על אתר האינטרנט של חברת אמריקן אקספרס. אתר החברה ספג התקפת DDoS אינטנסיבית שנמשכה כשעתיים ושיבשה את האפשרות של לקוחות החברה להשתמש בשירותיו. בניגוד להתקפות DDoS טיפוסיות, כמו אלה שמבוצעות על ידי "אנונימוס" ומבוססות על רשת מחשבים שנפרצו ואוגדו לבוטנט הנשלט ע"י התוקף, ההתקפה של עז א-דין אל קסאם השתמשה בסקריפטים שהופעלו על גבי שרתי רשת פרוצים, יכולת המאפשרת גיוס רחב פס גדול יותר לביצוע המתקפה.³⁹

אירוע זה שייך למגמה הכוללת התעצמות יכולות הסייבר של חמאס, בין השאר, בשכלול המערכה המודיעינית האיסופית כנגד צה"ל, ואיום השתלטות עוינת על מכשירי סלולר של אנשי צבא וחשיפת סודות באמצעותם.⁴⁰

תקיפות סייבר עצמאיות של ארגוני טרור

ניתוח התקפות ארגוני הטרור במרחב הסייבר מראה שסף הכניסה הנמוך למתקפות מסוימות והנגישות לכלי תקיפה קיברנטיים לא הובילו למעבר של ארגוני הטרור לתקיפות בעלות פוטנציאל נזק גדול ומתמשך. ארגוני הטרור פעלו עד כה בעיקר בתקיפת שער הארגון. כלי התקיפה העיקרי היו מתקפות למניעת שירות והתקפות בסדר גודל של תקיפה חובבנית עד תקיפה בינונית. הסיבה העיקרית לכך היא שסל היכולות והאמצעים של ארגוני הטרור במרחב הסייבר הינו מוגבל, ועד עתה אין להם התשתית המדעית והטכנולוגית העצמאית לפיתוח כלי סייבר בעלי יכולות לגרום נזק משמעותי. בהתחשב בכך שארגוני הטרור חסרים את היכולת לבצע איסוף מודיעין איכותי למבצעים (מל"ם), הסבירות לביצוע תקיפת סייבר משמעותית שלהם נראית נמוכה.

כדי שארגון טרור יוכל לפעול עצמאית ולהוציא לפועל פיגוע משמעותי במרחב הסייבר, יידרשו מגוון יכולות, בהן: יכולות איסוף מודיעין מדויק על היעד, רשתות המחשבים והמערכות שלו; רכישה או פיתוח של כלי סייבר מתאימים; מציאת קצה חוט לחדירה לארגון; הסוואת כלי התקיפה תוך כדי השתלטות על המערכת; ולבסוף – ביצוע המתקפה בזמן ובמקום אשר יפגיעו וישיגו תוצאה משמעותית. נראה שפעולה עצמאית של ארגון טרור, ללא גורם מדינתי התומך בו, אינה דבר מובן מאליו. אולם, אין לגזור מכך גזרה שווה באשר לארגונים הנתמכים ואף מופעלים על ידי מדינות בעלות יכולות משמעותיות.

קיימת אפשרות לתקיפות של ארגוני טרור תוך שימוש במיקור חוץ. אם נבחן את ארגוני הפשע, ניוכח כי ארגונים אלה עשו קפיצת דרך משמעותית בשנים האחרונות. מעבדת קספרסקי (Kaspersky) חשפה לאחרונה קבוצה חדשה של תוקפים, ככל הנראה בהזמנת ארגוני פשע או בהזמנה של מדינה על רקע ריגול תעשייתי. מדובר בקבוצה של האקרים בשם Icefog, המתמקדת בפגיעה בשרשרת האספקה של הארגון בצורה ממוקדת (בשיטת "תקוף וברח"), בעיקר במגזרי תעשיות צבאיות ברחבי העולם.⁴¹ התפתחות נוספת חלה בתפוצת קודים זדוניים, תוך שימוש של מעבדות פשע ברשת השחורה (DarkNet), שהגבירה את הנגישות לקודים קיימים למטרות תקיפה. ארגוני פשע עושים כבר כיום שימוש בקודים קיימים לתקיפת מערכות פיננסיות על ידי שכפולם והפיכתם לקודי מוטציה.⁴² האפשרות שארגוני טרור יעשו שימוש ויקנו שירותי תקיפה מהאקרים שכירי חרב, וכן יעשו שימוש עתידי בקודי מוטציה, על בסיס וריאציה של קודים קיימים

לתקיפת מטרות, היא ריאלית בעתיד הקרוב, ואין להתעלם ממנה בבניית איום הייחוס במרחב הסייבר לתקיפות שער הארגון ואפילו מערכות המידע שלו. לכן, ישנה סבירות גבוהה לכך שבשנים הקרובות תחול התקדמות ביכולות התקיפה הקיברנטית של ארגוני טרור, שיתבססו על רכישת יכולות מתקדמות יותר על ידיהם ותרגומן לתקיפות על מערכות המידע של ארגונים (ולא רק על שער הארגון). יכולת לבצע מתקפה שתכלול חדירה למערכות המבצעיות ותפגע בהן היא מורכבת למדי. הצורך ביכולות מודיעין ויכולות החדרה ברמה גבוהה, שקיימות רק אצל מספר מדינות מצומצם, גורם לכך שפעולה התקפית תהיה מדינתית, ולכן לא נראתה עד היום התקפה מוצלחת של שחקן לא מדינתי על מערכות הליבה המבצעיות של ארגון כלשהו. אף שתקיפה כזו טרם זוהתה, ניתן לראות עליה במגמת השיפור ביכולות הטכנולוגיות של שכירי החרב הפועלים במרחב הסייבר לצרכי פשיעה והונאה. מתוך כך ניתן להניח, שתמורת תגמול מתאים יסכימו גורמים טכנולוגיים פליליים לייצר כלים שיוכלו לבצע תקיפות על מערכות הליבה המבצעיות של תשתיות קריטיות ושל חברות מסחריות. גורמים אלה יוכלו להעמיד את מרכולתם גם לטובת ארגוני טרור.

המלצות להתמודדות ברמה הלאומית

מגוון האיומים במרחב הסייבר הוא רחב. ההגנות הבסיסיות מפני איומים אלה לא צריכות להבדיל בצורה מהותית בין מקורותיו של האיום. לכן, המחשבה כי ניתן ליצור הגנה ייעודית במרחב הסייבר דווקא מול איומים של גורמי טרור, נראית לא מעשית. אדרבא, תפיסת המענה לאיומים לפגוע במרחב הסייבר על ידי ארגוני טרור אינה צריכה ואף אינה יכולה להיות שונה מהותית מתפיסת המענה הכוללת לאיומים במרחב זה.

תפיסת ההגנה היסודית בפני איומי הסייבר צריכה להתבסס על מספר מרכיבי יסוד: מודיעין; מענה הגנתי רב־שכבתי; מענה התקפי; הסברה; מענה אזרחי.

מודיעין

מרכיב היסוד הראשון בהתגוננות מפני איומי הסייבר הוא המודיעין, ובמסגרתו איסוף מודיעין שיתבסס על הכוונה לאור הערכות מצב. בהקשר זה קיימת חשיבות לזיהוי האיומים ולהכוונת גורמי האיסוף מול מידע הנוגע לגורמי טרור המבקשים לפעול במרחב הסייבר. כפי שנכתב לעיל, במקרים רבים עומדות מדינות מאחורי הפעילות של ארגוני טרור, ולכן מודיעין הנאסף בהקשר המדינתי יוכל לספק מידע גם בהקשר של ארגוני טרור המסונפים או מופעלים על ידי אותה מדינה.

תחום המודיעין מהווה נדבך חיוני מאין כמוהו בהתמודדות עם איומים במרחב הסייבר. היכולת לאסוף ולנתח מידע רב מאפשרת כיום לייצר מודיעין איכותי

הן ברמה המדינתית והן, במקרים לא מעטים, ברמת ארגונים ועסקים המנטרים באופן קבוע את רשתות המידע והתקשורת. זאת, כדי לאתר התנהגויות אנומליות העשויות להעיד על תקיפה העתידה להתרחש, או ללמד על פעילות חריגה ברשת המחשבים. בהקשר זה ראוי להדגיש, כי העובדה שמדינה דוגמת איראן תומכת, ולעיתים אף מפעילה, ארגוני טרור, מחייבת את ארגוני המודיעין במערב לנטר לא רק את מדינת היעד אלא גם את הארגונים המסונפים לה. בהקשר של איראן המדובר בחזבאללה, בחמאס, וב"הצבא הסורי האלקטרוני".

מענה הגנתי הכולל מספר שכבות

המדובר בהגנה היקפית ובהגנה על נכסים חיוניים, הכוללת יכולות שימור פעולה גם אחרי חדירה של קוד מפגע וסיכול מקדים של גורמים פעילים, למשל על ידי חשיפה של מידע מודיעיני לרשויות החוק במדינות בהן מתבצעת הפעילות וביצוע פעילות סיכול באמצעות כלים משפטיים במדינות אחרות. כך יתכן שיבוש של היכולת להפעיל את הקוד המפגע קודם שזה הופץ.

מענה התקפי לאיומים

מרכיב זה בהתמודדות עם איומי הסייבר כולל שני רבדים: הרובד הראשון נוגע ליכולת לפעול התקפית באמצעות מהלומה מקדימה, במרחב הסייבר ולעיתים גם מחוצה לו, כנגד משאבי הסייבר בארגון טרור (תשתיות, מימון, אתרים ופעילים). הרובד השני נוגע ליכולת לבצע פעולת תגמול אחרי התקיפה ואחרי זיהוי מספק של הגורמים לתקיפה. מהלומה זו לא חייבת להיות מתוחמת רק למרחב הסייבר ויכולה אף לכלול מרכיבים פיזיים של ממש. בחלק מהמקרים נדרשת הסדרה חוקית של הפעילות ההתקפית, כדי לאפשר אפקטיביות של המענה. במקרים לא מעטים ניתן לזהות את שרשרת הפעולה כאשר מדינות (דוגמת איראן) מפעילות ארגונים לא מדינתיים (דוגמת חזבאללה ו"הצבא הסורי האלקטרוני"), כשכולם יחד מפעילים גורמים בעלי עניין ואף גורמים משוטטים ברשת לצורך הגדלת יכולות התקיפה. הצורך להפעיל מערכת רחבה של תוקפים מחייבת הכולנה במספר הקשרים: הראשון שבהם נוגע לקביעת המטרות אותן יש לתקוף; השני נוגע לעיתוי התקיפות; והשלישי נוגע לכלים לביצוע ההתקפות. כל אלה מחייבים הקמה של אתרים ופורומים ייעודיים אליהם מופנה המידע. פעילות זו יוצרת נקודת תורפה, מאחר וניתן לפעול לשיבוש ולשיטוי וכך לייצר בלבול, תוך הקהיה של עוקץ התקיפה שתוכנן על ידי מובילי התקיפה.

פעילות הסברה

ניתן להניח שפעילות הסברה לא תהייה אפקטיבית מול הגרעין הקשה של הפעילים בהתקפות הסייבר. לפעילות המניעה ההסברתית שתי מטרות: הראשונה

היא הגדלת המודעות לאפשרות שתוקפים עלולים להיפגע כתוצאה מפעילות סיכול במדינה בה הם שוהים (למשל, חשיפה שלהם לגורמי האכיפה במדינה); השנייה היא החשיפה של העומדים מאחורי ההתארגנות. כאמור, במקרים רבים התוקפים המשוטים לא יודעים כלל שהם מופעלים על ידי מדינות וארגוני טרור. לפיכך, באמצעות פעולות כאלו יתכן וניתן יהיה לצמצם במידה מסוימת את היקף התופעה.

ארגון המענה האזרחי במרחב הסייבר

נקודות התורפה של מערכת הסייבר האזרחית בישראל מהוות פְּרָצָה הקוראת לגנב עבור ארגוני הטרור. ההגנות החלשות יחסית על מערכות אלו מאפשרות לארגוני הטרור לפעול באופן שאינו מסובך מול מטרות במרחב זה. מאחר ומערכת הסייבר האזרחית מייצרת חולשות מובנות, יש להסדיר את המענה האזרחי במרחב הסייבר, ויפה שעה אחת קודם. יש לציין, בהקשר זה, המלצה של המכון למחקרי ביטחון לאומי לממשלת ישראל להסדיר את ההגנה של מרחב הסייבר האזרחי באופן שיוכל לספק מענה הולם לאיומים.⁴³

ארגוני הטרור טרם חצו את הרף המבצעי והטכנולוגי המאפשר להם לפעול באופן עצמאי מול ישראל ומדינות אחרות במערב בתחום לוחמת הסייבר. אולם, התפתחות שוק התקיפה הפלילי עלולה ליצור יכולות תקיפה משמעותיות. התפתחות זאת, לצד המשענת וההכוונה המודיעינית והמבצעית של מעצמות טכנולוגיות דוגמת איראן, יכולה לגרום לפעילות מסוכנת בתחום הסייבר גם מצדם של ארגוני טרור. לכן, ראוי יהיה לא לזלזל באיום זה. אף שטרם נצפתה פעילות משמעותית של ארגוני טרור בתחום הסייבר, התפתחות האיום בתחום זה מחייבת התארגנות מתאימה.

הערות

- 1 מיכל אביעד, **קולנוע תיעודי**, תל אביב, חידקל, 2007, עמ' 5.
- 2 ראו למשל: חיים פס ודן מרידור (עורכים), **הקרב של המאה ה-21: דמוקרטיה נלחמת בטרור, פורום עיון**, המכון הישראלי לדמוקרטיה, ירושלים, תשס"ז-2006, עמ' 25.
- 3 ראו למשל TOR – תוכנה המסייעת ליצירת אנונימיות ברשת. כל שכבה מוצפנת וכל תחנה במסלול מקלפת את השכבה שלה ומעבירה לתחנה הבאה. עיקרון זה נקרא "ניתוב בצ'ל" (The Onion Router – TOR), <https://www.torproject.org/>
- 4 Oded Yaron, "Hackers Plan Cyber Attack against Israeli Targets in April", *Haaretz*, March 14, 2013 <http://www.haaretz.com/news/diplomacy-defense/hackers-plan-cyber-attack-against-israeli-targets-in-april.premium-1.509214>.
- 5 "שטייניץ: האיום הצבאי על ישראל הפך גם לאיום טרור סייבר", **גלובס**, 9 ביולי 2013, <http://www.globes.co.il/news/article.aspx?did=100086069>
- 6 ראו התבטאות של ראש הממשלה בנימין נתניהו בנושא זה: "נתניהו: גידול משמעותי במתקפות הסייבר מאיראן וגרורותיה", **גלובס**, 9 ביוני 2013,

- 7 <http://www.globes.co.il/news/article.aspx?did=1000851092>
הכוונה היא לכל מערכת המאחסנת, משנעת או מעבדת מידע ארגוני, בין אם היא מקושרת לרשת האינטרנט ובין אם לא, ובין אם היא מהווה חלק מליבת העשייה העסקית של הארגון ובין אם לא.
- 8 מערכת ליבה מבצעית של הארגון היא החומרה שעל גביה והתוכנה אשר באמצעותה מנוהלים תהליכי הליבה של הארגון (בין אם הוא ארגון ביטחוני או ארגון עסקי אזרחי). זו מערכת ששיבוש או הריסה שלה יכולים להפסיק את פעילות הארגון או חלקים ממנו, עד כדי גרימה של נזק פיזי במקרים מסוימים.
- 9 מערכת בקרה תעשייתית (ICS) היא כלי המשלב רכיבי תוכנה וחומרה ונועד לפקח על תהליך פיזי של ייצור תהליכי. המערכת כוללת חיישנים לניטור התהליך המבוקר ופקדים לשליטה על תהליך זה. המערכת עשויה לכלול גם חיבור לרשתות מחשבים אחרות של הארגון ולעיתים אף לרשת האינטרנט.
- 10 סוג התקפות זה נעשה גם על ידי אקטיביסטים ואנרכיסטים בצורה עצמאית, או בשליחות והכוונה של ארגוני טרור.
- 11 “Shamoon Virus Targets Energy Sector Infrastructure”, *BBC News Technology*, August 17, 2012, <http://www.bbc.co.uk/news/technology-19293797>
- 12 באירוע זה הוחדר קוד זדוני למערכת המחשוב של ערמקו, וכתוצאה מכך הושבתו כ-30,000 מחשבים.
- 13 ראלף לנגר, הרצאה בנושא אבטחת מערכות בקרה תעשייתיות, ועידת הסייבר השנתית, המכון למחקרי ביטחון לאומי, 4 בספטמבר 2012, <http://youtube/sBsMA6Epw78>
- 14 “The Disturbing World of the Deep Web, Where Contract Killers and Drug Dealers Play their Trade on the Internet”, *Daily Mail*, October 11, 2013, <http://www.dailymail.co.uk/news/article-2454735/The-disturbing-world-Deep-Web-contract-killers-drug-dealers-ply-trade-internet.html>
- 15 Jesse Emspak, “Why We Won’t Soon See another Stuxnet Attack”, *Tech News Daily*, July 24, 2011, <http://www.technewsdaily.com/7012-stuxnet-anniversary-look-ahead.html>
- 16 Aditya K. Sood, Richard J. Enbody, “Crimeware-as-a-Service – A Survey of Commoditized Crimeware in the Underground Market”, *International Journal of Critical Infrastructure Protection*, Volume 6, Issue 1, March 2013, <http://www.sciencedirect.com/science/article/pii/S1874548213000036>
- 17 עמוד ב"פייסבוק", בו מוצעים למכירה נשקי סייבר: <https://www.facebook.com/groups/53807916899/>
- 18 Limor Kessem, “Zeus FaaS Comes to a Social Network Near You”, RSA, Speaking of Security, April 2013, <http://blogs.rsa.com/zeus-faas-comes-to-a-social-network-near-you/>
- 19 Michael Fire, Rami Puzis, Yuval Elovici, “Organization Mining Using Online Social Networks”, <http://arxiv.org/pdf/1303.3741v2.pdf>
- 20 Aviad Elishar, Michael Fire, Dima Kagan, Yuval Elovici, “Homing Socialbots: Intrusion on a Specific Organization’s Employee Using Socialbots”, International Workshop on Social Network Analysis in Applications (SNAA), August 2013.
- 21 Fernando M. Pinguelo, Bradford W. Muller, Norris McLaughlin, P.A. Marcus, “Is Social Media a Corporate Spy’s Best Friend? How Social Media Use may Expose your Company to Cyber-Vulnerability”, *Bloomberg Law*, <http://about.bloomberglaw.com/practitioner-contributions/is-social-media-a-corporate-spys-best-friend/>

- Internet Census 2012, Carna Botnet, 22
<http://internetcensus2012.bitbucket.org/paper.html>
- מפת מערכות סקאדה בעולם: <http://goo.gl/maps/nqnan> 23
- האתר Shodan, המכיל מידע שימושי להאקרים: <http://www.shodanhq.com/> 24
- גילי כהן, "האקרים תקפו רשתות ביתיות של מאות ישראלים", **הארץ**, 11 בספטמבר 2013, <http://www.haaretz.co.il/misc/2.444/.premium-1.2117098> 25
- וקטור תקיפה: <http://searchsecurity.techtarget.com/definition/attack-vector> 26
- מתקפת זיוף: <http://www.webopedia.com/TERM/S/spoof.html> 27
- Eric M. Hutchins, Michael J. Cloppert, Rohan M. Amin, "Intelligence-driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains", *Leading Issues in Information Warfare & Security Research*, 1 (2011), p. 80. 28
- Doug Macdonald, "A Guide to SpyEye C&C Messages", Fortinet, February 15, 2011, <http://blog.fortinet.com/a-guide-to-spyeye-cc-messages> 29
- Thomas Rid, "Cyber-Sabotage Is Easy", *Foreign Policy*, July 23, 2013. http://www.foreignpolicy.com/articles/2013/07/23/cyber_sabotage_is_easy_i_know_i_did_it?pa 30
- Dorothy E. Denning, *Cyberterrorism, Testimony before the Special Oversight Panel on Terrorism*, Committee on Armed Service, U.S House of Representatives, May 23, 2000, p. 269 31
<http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>
- לכרונולוגיה של פעולות של Aum Shinrikyo ראו: http://cns.miis.edu/reports/pdfs/aum_chrn.pdf 32
- Paul Everard, "NATO and Cyber Terrorism", in: *Center of Excellence Against Terrorism, Response to Cyber Terrorism*, Ankara, Turkey, 2008, pp.118-126, <http://www.nato.int/docu/review/2013/Cyber/timeline/EN/> 33
- דניאל כהן ואביב רוטברט, "תפוצת נשק קיברנטי במרחב הסייבר", **צבא ואסטרטגיה**, כרך 5, גיליון 1, מאי 2013. 34
- Dylan Love, "10 Reasons To Worry About The Syrian Electronic Army", *Business Insider*, May 22, 2013, <http://www.businessinsider.com/syrian-electronic-army-2013-5?op=1#ixzz2h728aL8P> 35
- Peter Foster, "'Bogus' AP tweet about explosion at the White House wipes billions off US markets", *The Telegraph*, April 23, 2013, <http://www.telegraph.co.uk/finance/markets/10013768/Bogus-AP-tweet-about-explosion-at-the-White-House-wipes-billions-off-US-markets.html> 36
- יניר מגנה ועודד ירון, "מומחה ישראלי אמר ש'הצבא הסורי האלקטרוני' תקף בישראל – והכחיש", **הארץ**, 25 במאי 2013, <http://www.haaretz.co.il/news/politics/1.2029071> 37
- אמיר בוחבוט, "מתקפת סייבר: הופלו אתרי משרד ראש הממשלה, הביטחון והחינוך", **וואלה חדשות**, 7 באפריל 2013, <http://news.walla.co.il/?w=/90/2630896> 38
- נמרוד צוק, "פיגוע סייבר: לוחמי עז א דין אל קסאם הולמים באמריקן אקספרס", **כלכליסט**, 2 באפריל 2013, 39
- <http://www.calcalist.co.il/internet/articles/0,7340,L-3599061,00.html>
- לי ירון, "מחלקת ביטחון מתריעה: יכולות הסייבר של חמאס התעצמו", **במהנה**, 14 בנובמבר 2013, עמ' 19. 40
- "Kaspersky Lab Exposes 'Icefog': a new Cyber-espionage Campaign Focusing on 41

Supply Chain Attacks, September 26, 2013

http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_exposes_Icefog_a_new_cyber-espionage_campaign_focusing_on_supply_chain_attacks

42 להרחבה בנושא קוד מוטציה ראו: כהן ורוטברט, "תפוצת נשק קיברנטי במרחב הסייבר", **צבא ואסטרטגיה**, כרך 5, גיליון 1, מאי 2013.

43 גבי סיבוני, "מענה לאומי להגנה אזרחית בסייבר", מסמך עמדה למקבלי החלטות,

המכון למחקרי ביטחון לאומי, אפריל 2013, <http://heb.inss.org.il/index.aspx?id=4354&articleid=5904>