

תפוצת נשק קיברנטי במרחב הסייבר

דניאל כהן ואביב רוטברט

מבוא

מרחב הסייבר הינו תופעה שעיקרה ניצול השדה האלקטרומגנטי לצרכים אנושיים באמצעות טכנולוגיה. במאמר זה ייטען כי טכנולוגיה זו היא סוג של נשק. ההגדרה המילונית המסורתית לנשק היא "שם כולל לכלים שהאדם משתמש בהם כדי להכריע את האויב".¹ "נשק קיברנטי" הוא, לפיכך, נשק המאפשר פגיעה שמטרתה להכריע את האויב באמצעות פגיעה במערכות המקושרות למרחב הקיברנטי. נשק קיברנטי ניתן להפעלה כנשק אל-הרג, וכולל את היכולת לגרום הרס רב ופגיעה קשה בתפקוד, בלי להחריב תשתיות פיזיות או לקטול חיי אדם. הסביבה האסטרטגית-קיברנטית כוללת שימוש בנשק קיברנטי לפעולות חדירה למערכות האויב לצורך ריגול, לוחמה פסיכולוגית, הרתעה, נזק למערכות תקשוב או ליעדים פיזיים. יש להבחין בין יכולת התקפית רחבה וממושכת על יעדים אסטרטגיים ובעלי יכולת הגנה גבוהה, לבין התקפה שעלולה לגרום נזקים מקומיים או זמניים. יכולת תקיפה מהסוג הראשון שמורה לעת עתה בידי מספר מצומצם של מדינות, ונדרשים לה משאבים גדולים. לעומת זאת, ליכולת מהסוג השני נדרשת עלות נמוכה, ולכן כבר כיום ניתן לראות סימנים לייצור נשק המוני אשר זמין גם בשוק החופשי, ונמצא בשימוש של ארגוני טרור ופשע.

לוחמה קיברנטית הופכת להיות אחד מדפוסי הפעולה ההתקפיים בשימושן של מדינות המבקשות להגן על האינטרסים שלהן מפני מדינות או ארגונים עוינים. יעידו על כך התקפות הסייבר האחרונות שהתפרסמו בתקשורת, כגון המתקפה המיוחסת לאיראן על חברות נפט במפרץ הפרסי ועל בנקים אמריקאיים, ומנגד, התקפות המיוחסות לארצות-הברית ולישראל נגד מתקני הגרעין של איראן.² למציאות זו מספר סיבות, וביניהן: היכולת לבצע מתקפה ממוקדת, יכולתו של

דניאל כהן הוא מתאם תכניות לוחמת סייבר וצבא ואסטרטגיה במכון למחקרי ביטחון לאומי אביב רוטברט הוא תלמיד לתואר שלישי, מלגאי בתכנית ניובאוור במכון למחקרי ביטחון לאומי

התוקף להסוות את עצמו והיכולת של הקורבן להסתיר את אירוע התקיפה, ובכך להימנע מההכרח לתקוף חזרה. מרחב הסייבר מאפשר למדינות בעלות משאבים ויכולות טכנולוגיות גבוהות להשתמש בארסנל נשק לצורכי תקיפות סייבר. מנגד, מדינות חסרות משאבים יכולות גם הן להצטייד בנשק התקפי ולפעול במרחב הסייבר, אם כי בהיקף מצומצם ובעל פוטנציאל נזק מועט יותר.

תופעה ייחודית במרחב הסייבר שאינה נמצאת במרחבי לחימה אחרים היא היכולת הגבוהה להתגונן מפני וירוסים או קוד זדוני³ אחר, כאשר נעשה בו כבר שימוש בעבר והוא התגלה על ידי גופי אבטחה.⁴ לכאורה, נשק סייבר עשוי להיות חד-פעמי ולהפוך חסר תועלת ברגע שזוהה ונחתם.⁵

אך האם כל שנות-האדם שהושקעו בפיתוח קודים זדוניים מתוחכמים יורדות לטמיון ברגע אחד, כאשר ההתקפה מתגלה ונחתמת?

מאמר זה ינסה להראות כי לא כך הם פני הדברים. עם התגברות התקיפות במרחב הסייבר, יגברו תפוצת הכלים ויכולות הסייבר בעולם. אחת הסיבות העיקריות לכך היא שניתן לעשות שימוש בנשק סייבר, כדוגמת קוד זדוני ששימש לתקיפה אחת, גם בתקיפות אחרות, וזאת לאחר הסבתו. בהשאלה מעולם הביולוגיה, קוד זה יכונה "קוד מוטציה". הוא בעל מאפיינים פונקציונליים דומים (עד כדי זהות מוחלטת) לקוד האב שממנו הוא נוצר. ההבדל בין קוד האב לקוד המוטציה הוא סינטיקטי (מבני) בלבד ולא סמנטי, במטרה לחמוק מהרדאר של תוכנות לזיהוי פוגענים.

מכך ניתן להסיק כי נפילת קוד זדוני לידי יריב בעל מוטיבציה ויכולת נותנת לצד המותקף נשק שב"חימוש" מתאים, תוך ביצוע פעולות מורכבות כגון הנדסה לאחור (Reverse Engineering),⁶ יכול להיות מנוצל לשימוש רב-פעמי. כמו כן, שימוש יעיל יכול להיעשות על ידי תוקף שמכיר את הנשק ויכול לשנות אותו על פי צרכיו לביצוע מתקפות נוספות.

אנו מצויים בעיצומה של מלחמת סייבר שקטה, שפרטים מעטים מאוד ממנה דולפים לתקשורת, אך העמימות אינה יכולה להישמר לנצח. נתבונן לדוגמה בהתפתחות של תחום כלי-הטיס הבלתי-מאוישים (כטב"ם). בימיו הראשונים היה התחום עטוף במעטה חשאיות. היכולת להפעיל כלי-טיס בלתי-מאויש למטרת ריגול ובהמשך לתקיפה הייתה נתונה בידיהן של מדינות מעטות, ואלו עשו שימוש מחושב וזהיר בטכנולוגיה, על מנת שלא לחשוף אותה לעיני היריב. עם התגברות השימוש בכלים בלתי-מאוישים נפרצה חומת העמימות, וכיום ניתן למצוא תיאורים מפורטים בתקשורת על המדינות שעושות שימוש בכלי-טיס אלה, על המטרות שהיו נתונות לתקיפות מן הסוג הזה, על היכולות והמגבלות של כלים כאלה, ועוד. גם ארגוני הטרור למדו היטב את כלי הנשק החדש-ישן שהופעל נגדם בהצלחה על ידי מדינות, ופיתחו דרכים להתגונן מפניו. תוצאה נוספת של השימוש הנרחב

בכטב"מים והחשיפה התקשורתית שבאה בעקבותיו היא פתיחה של מרוץ חימוש, שגרם למדינות רבות לנסות להיכנס ל"מועדון היוקרתי" של אלה המחזיקים בנשק זה לצורכי ריגול ותקיפה.⁷ גם מדינות תומכות טרור נכנסו למרוץ,⁸ וארגוני טרור הפועלים בחסותן של מדינות אלו נהנו גם הם מ"פירות ההשקעה": איראן השיגה יכולת הפעלת כלי-טיס בלתי-מאוישים, ולא עבר זמן רב עד שיכולת זו מצאה את דרכה אל ארגוני הטרור חמאס וחזבאללה.

היכולת לבצע מתקפה במרחב הסייבר לשיבוש מערכות בקרה תעשייתיות ויצירת הרס פיזי (כפי שנעשה בהחדרת וירוס 'סטקסנט' ויצירת נזק למערכות הסרפזות בפזורים גרעיניים באיראן) היא יכולת שיש כיום, על פי ההערכות, למספר מצומצם של מדינות, ומדינות רבות נוספות חותרות להשגתה. בכך יש למעשה תהליך התחמשות בנשק לחימה מסוג חדש, המאפשר פגיעה והרס ממרחק רב. יכולת לבצע מתקפה שתפגע בתהליך התעשייתי אינה מורכבת מדי, וגורמי בקרה והנדסה יכולים לבצע. לעומת זאת, כדי להבין ולנתח לעומק את התהליך התעשייתי במטרה המותקפת, יש צורך ביכולות מודיעין ויכולות החדרה ברמה מדינתית גבוהה.

גם שחקנים לא-מדינתיים במרחב הסייבר, ובראשם ארגוני פשע וטרור, עלולים לעשות שימוש או שכבר עשו שימוש בעבר בווריאציות של קודים זדוניים קיימים והסבתם לצורכי הארגון. כך קרה במקרה ב-2012, כאשר ארגוני פשע השתמשו בוורוסים קיימים ומוכרים בשם Zeus ו-SpyEye, שבהם ערכו שינויים משלהם, והצליחו בעזרתם למשוך כ-78 מיליון דולר מבנקים ברחבי העולם.⁹ ככל שתגבר הנגישות לקודים קיימים, במקביל להגברת היכולת של יחידים או ארגונים קטנים לבצע הסבות, כך תתפשט תפוצת הקודים הזדוניים למטרות תקיפה בעולם הפיננסי, למטרת השגת רווחים כלכליים לארגוני פשיעה, ואף תתפשט בקרב ארגוני טרור לשם השגת מטרות חברתיות, אידאולוגיות ופוליטיות, על ידי הפחדה ושיבוש שגרת החיים האזרחית.

יכולות השחקנים במרחב הסייבר

המעבר מהעידן התעשייתי לעידן המידע הפיק תוצר חדש בדמות מרחב הסייבר (או המרחב הקיברנטי). התפתחותו של עידן המידע קשורה לצמיחת טכנולוגיות תקשורת, בקרה ומחשוב. לצמיחה זו ישנן משמעויות חברתיות וכלכליות עמוקות. לשנת 2008 יש משמעות סמלית בכך שלראשונה חצה מספר המחשבים הביתיים את רף המיליארד (רובם מחשבים המחוברים לאינטרנט), ובאותה שנה דווח כי מספר האנשים בעולם שיש ברשותם טלפונים סלולריים עלה על מספר האנשים שאין להם מכשיר סלולרי. כל מחשב או טלפון כזה יכול לשמש דלת כניסה למרחב הסייבר ונשק לתוקף פוטנציאלי¹⁰ (או להוות בעצמו מטרה לתקיפה).

ההתפתחויות הטכנולוגיות המהירות בעידן המידע יוצרות במרחב הסייבר מאפיינים ותכונות ייחודיות, המאפשרים הפעלה מהירה נגד יריבים המצויים הרחק מתחומי התוקף. התפתחויות אלה עשויות לשנות גם את פניו של שדה הקרב המודרני, והן יוצרות זירות לחימה שבהן השחקן הלא־מדינתי הוא למעשה שחקן מרכזי, המפעיל (יותר מבעבר) את השפעתו על מדיניות ממשלות ומוסדות בינלאומיים. הלחימה בקוסובו בשנים 1996–1999 מאופיינת כמלחמה הראשונה במרחב האינטרנטי. שחקנים מדינתיים ולא־מדינתיים השתמשו ברשת להפצת מידע, להפצת תעמולה וליצירת דמוניזציה ליריבים. האקרים השתמשו ברשת בעת הלחימה ככלי לחימה הן נגד יוגוסלוויה והן נגד נאט"ו, על ידי הפרעה למערכות מחשוב ממשלתיות והשתלטות על אתרים ממשלתיים. יחידים ואקטיביסטים השתמשו ברשת להפצת מסרים מתוך אזור הלחימה.¹¹

דוגמה נוספת ניתן למצוא בלחימה באסטוניה. החל מאפריל 2007 ובמשך שלושה שבועות, הותקפה אסטוניה בסוג מתקפות המכונה "מניעת שירות מבוזרת" (DDoS - Distributed Denial of Service). גל המתקפות כלל פגיעה באתרי מוסדות שלטון, בבנקים ובמערכות עיתונים. ההתקפה החלה לאחר עימות עם רוסיה סביב הפגנות המיעוט הרוסי באסטוניה, ולכן רמזו גורמים באסטוניה ונאט"ו על מעורבות מדינתית רוסית בביצוע המתקפות.¹²

למרחב הסייבר יש משמעויות נרחבות בכל הקשור להפעלת כוח צבאי, פעילות חבלנית, פעילות פשע מאורגן, ריגול ומודיעין. בכל הקשור להפעלת כוח, תקיפת מחשבים אינה זקוקה לבסיס מדינתי, והיא יכולה להיעשות גם על ידי ארגונים ואף יחידים. נוסף לכך, התקיפה יכולה להתנהל גם בין מדינות ידודות, בתחרות להשיג מודיעין דיפלומטי וכלכלי.

מאפיין ייחודי של מרחב הלוחמה הקיברנטי, שאינו מצוי בשום מרחב לוחמה אחר, הוא היכולת ההדדית של התוקף והקורבן להסתיר בצורה מושלמת כמעט את דבר המתקפה. מעצם טבעו של המרחב הקיברנטי, התוקף יכול לבצע את הפעולה ההתקפית ממרחק גיאוגרפי רב מאוד מהמטרה שלו, ולהשתמש בטכניקות הסוואה שימנעו באופן מוחלט כמעט את חשיפתו. הקורבן, מן הצד השני, יכול תמיד לטעון שהנזק שנגרם למערכות שלו נובע מתקלה בחומרה או בתוכנה, ובכך להימנע מפגיעה תדמיתית ומהכורח להגיב או לאיים בתגובה כלפי מבצע ההתקפה. תוצאה ישירה של מאפיין ההסתרה במרחב הקיברנטי היא חשיפה מועטה מאוד בתקשורת של מקרי תקיפות. אך מהמעט שכן מתפרסם בעיתונות ניתן ללמוד על גידול בהיקף ובתחכום של המתקפות הקיברנטיות. כל המעצמות כבר מעורבות בצורה זו או אחרת בלוחמת סייבר,¹³ ומדינות רבות נוספות משקיעות בפיתוח התקפות והגנות על המרחב הקיברנטי. לוחמת הסייבר משתלבת באופן מושלם במלחמה הקרה שמתרחשת בין ה"מזרח" ל"מערב", כיוון שהיא מאפשרת

לאיים על היריב או לפגוע בו מבלי להכריח אותו להגיב. מתקפה קיברנטית שלא פורסמה ושום גורם לא קיבל עליה אחריות היא מתקפה שהקורבן אינו מרגיש מחויב להגיב עליה, אבל עדיין מבין היטב את הרמז שנשלח לעברו מכיוון התוקף. זוהי מהותה של מלחמה קרה.

בצד ההגנתי, עם התרחבות השימוש בנשק הסייבר, נוצרת מודעות רבה יותר לסכנות הטמונות בנשק זה ולפוטנציאל ההרס שביכולתו להסב מבחינה ביטחונית, כלכלית ותדמיתית. מודעות זו מביאה להשקעה של משאבים רבים בפיתוח מערכות תוכנה מוגנות ומאובטחות יותר, ובאבטחת מתקנים ותשתיות קריטיות במדינות שונות. כמו בכל מאבק בין תוקפים למגנים, גם בתחום הסייבר הייתה ידם של התוקפים על העליונה כאשר החל להתפתח מרחב הלחימה הקיברנטי. אך כעת נראה שהפער הולך ומצטמצם, ככל שיותר ויותר גופים פועלים לאבטח את תשתיות התקשוב שלהם.

אחד ממאפייני מרחב הסייבר הוא הקושי לזהות את התוקף. בניגוד לתקיפת מטוסי הצי המלכותי היפני בפרל הרבור (1941) שהביאה להכרזת מלחמה אמריקאית רשמית על יפן, תקיפת סייבר גדולה כגון התקיפה על חברת אראמקו באוגוסט 2012¹⁴ נמצאת כיום בוויכוח בקרב מומחי אבטחה לגבי זהות התוקף, למרות הפניית אצבע מאשימה לגורם מדינתי (איראן). מאפייני מרחב הסייבר גם מקשים את ההבחנה בין פגיעה מכוונת לתקלה ואת האפשרות לייחס פעולה לגורם מסוים (attribution), ולכן גם מקשים על המותקפים להגיב על תקיפה. יש הטוענים כי מאפייני המרחב הקיברנטי כיום מקנים יתרון לתוקף לעומת המגן.¹⁵ חמש קבוצות עיקריות משתמשות כיום, או שיש להן פוטנציאל לשימוש בעתיד, בכלי תקיפה קיברנטיים.¹⁶

מדינות – מדינות מפתחות יכולות התקפיות והגנתיות כחלק מיכולות הפעלת הכוח שלהן. הערכות סבירות הן שכארבעים מדינות מצטיידות ביכולות לוחמת סייבר או השיגו אותן כבר, לרבות היכולת לבצע מתקפות סייבר. רוב התוכניות הלאומיות הן חשאיות, ואין הסכמה בשאלה עד כמה החוק הבינלאומי הקיים, שתקף לעימות מזוין, אמור לחול על מצב ההתקפה החדש.¹⁷

עידן המידע מאופיין בפעילות מדינתית גוברת בתחומי כלכלה, תשתיות אזוריות, ביטחון לאומי, ביטחון אזרחי, תקשורת בין-ארגונית, חינוך, גיהול מוסדות שלטון ועוד. בהתאם, מדינות ברחבי העולם מגדילות את השקעתן בתחום ההגנה על מערכות ממוחשבות – השקעה המתבטאת במשאבים המוקצים לנושא, ובפיתוח של טכנולוגיות ותפיסות הגנה ייעודיות.¹⁸ במקביל, שירותי ביטחון ומודיעין מאמצים כלים של המרחב הקיברנטי להשגת מטרותם. טכנולוגיות המידע גם מעניקות לשירותי ביון מדינתיים מגוון רחב של אמצעים ודרכים לביצוע המשימה. למדינות יש יכולת לבצע כניסה גם למערכות מחשב סגורות על ידי

החדרת סוכן או הפעלת סוכן, ועל ידי התערבות במערכת האספקה והחדרת רכיבים "נגועים" למטרה היריבה.

מאפייני מרחב הסייבר המקשים את זיהוי התוקף יכולים לאפשר למדינה תוקפת יתרון בהפעלת שליח (Proxy), שיבצע או יקבל אחריות על תקיפת מדינה או חברה עסקית במדינה יריבה.

במרחב הסייבר המדינתי נחשפו במהלך 2012 שלוש תוכנות קוד זדוני חדשות: פליים, גאוס ומיני-פליים. פליים מהווה דוגמה של תוכנה זדונית מורכבת שהתקיימה לאורך זמן מבלי להיחשף, תוך איסוף נתונים ומידע.

פליים היא תוכנה גדולה במונחים של וירוסים (20 מגה-בייט), שבדרך כלל מסתמכים על היותם קטנים כדי לחמוק מזיהוי. התוכנה כוללת מאפיינים של סוס טרויאני, והיא אפשרה למפעיליה לפתוח "דלתות אחוריות" במערכות מחשבים כדי לאסוף מידע ולהעביר אותו לשרתים מרוחקים ברחבי העולם. בנוסף, התוכנה מסוגלת להקליט אודיו באמצעות המיקרופונים המותקנים במחשבים, לצלם צילומי מסך ולהתחבר למכשירי בלוטות' באזור התקיפה.

סוג כזה של התקפה שעקב מורכבותו מיוחס לתוקף מדינתי משפיע לא רק על מוסדות ממשלתיים, אלא גם על עסקים ותשתיות של חברות עסקיות הנמצאות בקשרים עסקיים עם גופים ממשלתיים.¹⁹

ארגוני פשע – מונעים בעיקר מאינטרסים פליליים ועסקיים; ארגוני פשע מאורגן משתמשים בהאקרים, ובעיקר במפעילי רשתות שבויות למטרות רווח: גניבת זהות, הונאה, דואר זבל, פורנוגרפיה, הסוואת פעילות פלילית, הלבנות הון וכיוצא באלה. כשמונים אחוזים מהפשע באינטרנט מבוצע על ידי ארגוני פשע.²⁰

נשיא האינטרפול, קהו בון הואי, טען כי הבנקים בארצות-הברית מאבדים מדי שנה 900 מיליון דולר כתוצאה מפשעי מחשב.²¹ במהלך הרבעון הראשון של 2012 דווח כי ארגוני פשע יצרו וריאציות בוורוסים קיימים ומוכרים בשם Zeus ו-SpyEye, לטובת מתקפה על בנקים באירופה ובאמריקה. ההתקפה זוהתה לראשונה באיטליה, שבה הותאם הקוד בצורה ממוקדת לבנקים השונים. לאחר מכן זוהתה תקיפה בעלת מאפיינים דומים בבנקים גרמניים והולנדיים. בהמשך התפשטו התקיפות לאמריקה הלטינית ולארצות-הברית. התוקפים הצליחו לגנוב לפחות 78 מיליון דולר בהעברות מחשבונות של כשישים מוסדות פיננסיים.²²

הערכות של אנליסטים בכירים הן שהאקרים מצליחים לגנוב כמיליארד דולר בשנה ממוסדות פיננסיים. יש המעריכים כי שלוש מכנופיות הפשע הגדולות הפועלות בתחום מצליחות לגנוב באמצעות מערכות מחשב כמה מיליון דולר בשנה, בעוד שבגניבה קונוונציונלית מבנקים אמריקאיים נגנבו על פי ה-FBI בשנת 2010 רק 43 מיליון דולר.²³

חברות עסקיות – פועלות בעיקר בתחום ההגנתי, כיוון שהיקף ההתקפות במרחב הקיברנטי בהקשרים עסקיים הולך וגדל במידה ניכרת, אולם חלק מהן עלולות לפנות (או שכבר פנו) לאפיק של התקפה על חברות מתחרות לצורך ריגול עסקי. כמו כן, חברות עסקיות מתמודדות בהגנה במרחב הסייבר מול אתגרים טכנולוגיים כגון הגנה על תשלום מקוון, אבטחת שידורי וידיאו בזמן אמת, אבטחת אפליקציות לטלפון חכם ואתגרים נוספים רבים.

ארגוני טרור – יתרונות הגלומים בשימוש במרחב הסייבר מנוצלים על ידי גורמים חבלניים על מנת להעביר מסרים מוצפנים, לגייס תומכים, לרכוש מטרות, לאסוף מודיעין, להסוות פעילות וכדומה.

משיקולי עלות/תועלת, ארגוני טרור אף משתמשים במרחב הסייבר לביצוע התקפות קיברנטיות. התקפות אלה תורמות להשפעה על דעת הקהל לשם העברת מסרים פוליטיים, ועד ביצוע דמורליזציה והפחדה על מנת לשבש את שגרת החיים של האזרח. ארגוני טרור ממקדים את הפעילות הקיברנטית ההתקפית נגד סמלי שלטון כגון אתרי מוסדות ממשלתיים ותקשורתיים.

אחת ההתקפות הראשונות המתועדות של ארגון טרור נגד מערכות מחשוב מדינתיות התרחשה בסרי-לנקה על ידי לוחמי הגרילה "הנמרים הטמיליים" ב-1998. שגרירות של סרי-לנקה ברחבי העולם הוצפו במשך שבועיים בכ-800 הודעות דוא"ל ביום עם המסר "אנחנו נמרי האינטרנט השחורים ואנחנו הולכים לשבש את מערכות התקשורת שלכם".²⁴ יש הטוענים כי מסר זה השפיע וזרע חשש ופחד בשגרירות.²⁵

בישראל, בינואר 2012, קבוצת האקרים פרו-פלסטיניים הקוראת לעצמה "Nightmare" הפילה למשך זמן קצר את אתרי הבורסה לניירות ערך בתל-אביב וחברת התעופה הלאומית אל על, ושיבשה את פעילות אתר הבנק הבינלאומי. בהתייחסות לכך מסר דובר חמאס ברצועת עזה כי "החדירה לאתרים ישראלים פותחת מרחב חדש של התנגדות ומלחמה אלקטרונית חדשה נגד הכיבוש הישראלי".²⁶

גורמים "אנרכיסטיים" – מתנגדים למערכת הממסדית הקיימת מעוניינים לחבל בה מבפנים או מבחוץ ויבקשו לתקוף את מערכת המחשוב, שהיא כיום הבסיס לניהולה, בכוונה לשבש ואף להרוס את הסדר החברתי ואת מרקם החיים במדינה. למשל, קבוצות אקטיביסטים או יחידים התוקפים אתרי אינטרנט כדי להשתיל בהם מסר פוליטי, או פועלים לשבירת מנגנוני צנזורה וחשיפת סודות. בנובמבר 2012, בזמן מבצע "עמוד ענן" בעזה, הודיעו גורמים בממשלת ישראל על מאה מיליון ניסיונות לתקיפות סייבר מקוונות נגד שירותי האינטרנט הממשלתיים בישראל.²⁷ ארגון "אנונימוס" המייצג קונספט תיאורטי של קהילת האקרים אקטיביסטים קיבל אחריות על הפלת אתרים ישראלים והדלפת מספרי

כרטיסי אשראי של אזרחים ישראלים בזמן העימות. "אנונימוס" אף פרסם רשימה של יותר מ-650 אתרים ישראלים, שלטענתו נפגעו או הופלו כתוצאה מהתקפות האקטיביסטים.²⁸

בכיר בממשל האמריקאי דיבר על כך ש"כמה תריסרי מתכנתים מוכשרים יכולים לגרום נזק רב".²⁹ עם זאת, יש להבחין בין יכולת התקפית על יעדים אסטרטגיים של אויב בעל יכולות הגנה מתקדמות לבין יכולת לגרום נזקים מקומיים טקטיים. ההצטיידות בכלי נשק קיברנטיים בקרב השחקנים השונים נעשית בהתאם ליכולות ולמגבלות השחקנים להקים כוח קיברנטי בעל יכולות התקפיות, והיא מושפעת גם מהאינטרסים ומהצרכים של כל שחקן ושחקן.

שימוש בנשק קיברנטי לתקיפת יעדים אסטרטגיים במרחב הפיזי והסייבר מצריך יכולת השמורה, לפי שעה, למספר מצומצם של מדינות בעלות יכולות ומשאבים טכנולוגיים ברמה גבוהה. לעומת זאת, ישנה "מדרגת כניסה נמוכה" וכלי נשק קיברנטיים בעלי יכולת פגיעה עם נזקים טקטיים. יכולת ייצור המוני של כלי נשק קיברנטיים כאלה היא מהירה ובעלות נמוכה יחסית, חלקם אף זמינים בשוק החופשי. מדינות מנצלות את מרחב הסייבר כדי להשיג יתרון ולקדם את האינטרסים שלהן באמצעות איסוף מידע, השגת כושר פגיעה ביכולותיו של מי שנתפס כאויב, ועוד. גם שחקנים לא-מדינתיים כגון ארגוני טרור ופשעה ממנפים את מרחב הסייבר למטרותיהם, ומפיקים תועלת במרחב המתיר גם לשחקנים קטנים להשפיע באופן שאינו יחסי לגודלם.

מטבלה 1 ניתן ללמוד כי השחקן המדינתי מסוגל להשיג יכולות תקיפה בכל הקטגוריות. למדינות יש צרכים מגוונים (ריגול, פגיעה בתעשיות של מדינת אויב) וגורמים מרסנים (הימנעות מפגיעה בחפים מפשע ויצירת נזק סביבתי רב, אשר יובילו לפיתוח נשק סייבר לתקיפה קיברנטית במקום לתקיפה פיזית, או נשק לתקיפה פסיכולוגית, כמו התרעה לפני הפצצה, שתאפשר להימנע מפגיעה באזרחים). שאר השחקנים במרחב הסייבר הם בעלי אינטרסים וצרכים ממוקדים יותר: לארגוני טרור יש יכולות ומשאבים מצומצמים יותר, והם מונעים על ידי אינטרס של השגת מטרות פוליטיות ואידאולוגיות באמצעות פגיעה במערכות פיזיות (עדיין לא נרשם אירוע כזה), ריגול או לוחמה פסיכולוגית; ארגונים עסקיים, לעומת זאת, יהיו מעוניינים בעיקר בריגול עסקי, ולעיתים גם בשיבוש הפעילות של המתחרים; ארגוני פשע מעוניינים בעיקר בהשגת נכסים וכסף במרמה, ולכן יתמקדו בתקיפת מערכות קיברנטיות ובריגול שיתמוך בפעילות כזו (איסוף כרטיסי אשראי ופרטים מזהים לצורך תקיפה).

טבלה 1: סל יכולות הנשק הקיברנטי של השחקנים השונים במרחב הסייבר

שימוש בנשק קיברנטי לתקיפת המרחב הפיזי	שימוש בנשק קיברנטי לתקיפת מרחב הסייבר	שימוש בנשק קיברנטי לריגול	מניעת שירות ולוחמה פסיכולוגית
<p>בשל המשאבים הרבים הנדרשים לכך, כיום יש רק למספר מדינות מצומצם יכולת ביצוע מתקפת סייבר בעלת נזק פיזי למגן (על פי הערכות סבירות, יכולת זו קיימת בארצות-הברית, בשראף, ברוסיה, בסין ובבריטניה).</p> <p>מדינות רבות נוספות מנסות או היו מעוניינות להגיע לסף יכולת תקיפה פיזית.</p>	<p>המשאבים הנדרשים לכך הם בסדר גודל בינוני, ומספר המדינות בעלות יכולת תקיפה אלקטרונית רב יותר ממספרן בסעיף התקיפה הפיזית.</p> <p>מדינות יכולות לבצע תקיפה אלקטרונית ו/או להשתמש ב"שליחים" לביצוע מתקפה אלקטרונית.</p>	<p>המדינות המובילות בתחום ריגול תעשייתי ומודיעיני הינן רוסיה וסין, ויש הטוענים כי גם ארצות-הברית וישראל. לצורך מימוש יכולת זו נדרשים משאבים רבים, ולכן "מועדון" המדינות בעלות יכולת זו הוא מצומצם. מתוך נקודת מוצא שריגול הוא המקצוע השני העתיק בעולם, ושרוב המדינות מפעילות אמצעי ריגול בצורה כזו או אחרת, תוכנות ריגול להפעלה ביעדים בתוך המדינה ומוחוץ לה ייעשו נפוצות עם הרחבת הנגישות לטכנולוגיות המקנות יכולת ריגול במרחב הסייבר.</p>	<p>יכולת זו היא פשוטה יחסית, ומדינה עלולה להשתמש בה בעת עימות עם מדינה אחרת באמצעות הפעלת שליחים.</p>
<p>המשאבים הנדרשים כיום למימוש יכולת זו הם מעבר ליכולתם של ארגוני טרור, ישנו מדינות המשתמשות בארגוני טרור לביצוע מתקפות טרור, ולכן לא מן הנמנע כי נעשה או ייעשה בהם שימוש גם לביצוע מתקפות סייבר פיזיות.</p>	<p>המשאבים הנדרשים למימוש יכולת זו הם מעבר ליכולתם של ארגוני טרור, למעט שימוש כ"שליח" של מדינה.</p>	<p>למימוש יכולת זו נדרשים משאבים רבים, אבל היא נדרשת כאחד מצורכי ארגון הטרור, ולכן לא מן הנמנע שהוא יפעל להגתה (למרות שלכאורה, לנשק זה נדרשים משאבים מורכבים-יחסית להשגה).</p>	<p>בשימוש ארוגני טרור, במטרה להפר את שגרת החיים ולעורר חרדה ופאניקה בקרב האזרחים.</p>
<p>שימוש ארוגני פשעי על מנת לבצע פעמים פיננסים, סחיטת ארגונים עסקיים ובעלי ממון.</p>	<p>מבצעים פעולות ריגול הנדרשות לצורך ביצוע פשעים אחרים: גניבת נתוני זהו, כרטיסי אשראי.</p>	<p>מבצעים פעולות ריגול ליצירת יתרון עסקי מול ארגון מתחרה.</p>	<p>יכולת הנמצאת בשימוש של אקטיביסטים, במטרה להעברת מסרים על ידי שיבוש מערכות ממשלחיות ואזרחיות.</p>
<p>יכולת שניתן לנצל למשל, לפגיעה במתחרים. בהשבתת אתר או שירות של ארגון מתחרה.</p>	<p>יכולת שניתן לנצל למשל, לפגיעה במתחרים. בהשבתת אתר או שירות של ארגון מתחרה.</p>	<p>יכולת שניתן לנצל למשל, לפגיעה במתחרים. בהשבתת אתר או שירות של ארגון מתחרה.</p>	<p>יכולת שניתן לנצל למשל, לפגיעה במתחרים. בהשבתת אתר או שירות של ארגון מתחרה.</p>

איום השימוש הרב־פעמי בנשק קיברנטי

כל מתקפת סייבר חדשה שמתגלה מקרבת את הפיכתו של נשק הסייבר לנחלת הכלל. עם התגברות השימוש בכלים ללוחמת סייבר, לא מן הנמנע שנשק קיברנטי מתוחכם ובעל יכולת לביצוע נזק אסטרטגי יהפוך לחזון נפרץ, וגרסאות שלו ימצאו את דרכן לידיהן של מדינות תומכות טרור וארגוני טרור.³⁰ כדוגמה, אפשר להתבונן על המתקפה על אתרי הגרעין האיראניים באמצעות וירוס סטקסנט (stuxnet). ההתקפה פעלה במשך שנים באופן חשאי, אך ברגע שהתגלתה היא הביאה למחקר ולניתוח מעמיקים ביותר של קוד הוירוס, ולניסיון להבין את כל ההיבטים שאפשרו את הצלחתו. תוצאות הניתוח יכולות לשמש באופן מיידי לפיתוח של וירוסים חדשים בעלי עקרונות פעולה דומים לאלה של סטקסנט. הסוד נחשף, הנשק התפשט. מבחינה תיאורטית, הימצאות וניתוח קוד זדוני בידי חברות ומומחי אבטחה עשויה לחשוף את הוירוס כלפי חוץ לגורמים שונים, החל ממדינות ועד ארגוני טרור. הנשק הקיברנטי לא יישאר לעד נחלתם של מעטים. קיימת סברה שלפיה הנשק הקיברנטי הינו חד־פעמי, והדבר יהווה גורם מרסן בשימוש בו וגורם מאט בפיתוח של כלי לוחמת סייבר חדשים, בשל הצורך לחדש כל העת והימנעות משימוש בכלי נשק שהתגלה כבר ונחתם על ידי תוכנות ההגנה. סברה זו לא הוכיחה את עצמה, ומהתבוננות בשטח ניתן להבחין שדווקא ההפך הוא הנכון – הווה אומר, קיים שימוש חוזר נרחב בכלי לוחמת סייבר שעוברים שינויים על מנת לאפשר להם לחמוק מהרדאר של תוכנות ההגנה. הצלחתה של מתקפת סייבר תלויה בניצול מוצלח של חולשה³¹ במערכת המותקפת. חולשה יכולה להתבטא ברכיב תוכנה שבכתבתו לא הובאו בחשבון שיקולי אבטחה מספיקים של קוד, ברכיב חומרה שניתן לחדור אליו ולגרום לו לבצע פעולות הרסניות או בפרוטוקול תקשורת לא מאובטח. על מנת שמערכת תיחשב מאובטחת, כל ההיבטים שצוינו צריכים להיבדק ולהיות מאובטחים בנפרד. מספיקה פרצה קטנה באחד מהם על מנת לאפשר חדירה והשתלטות על המערכת כולה. לדוגמה, אתר אינטרנט המחזיק מידע רגיש ומאובטח ברמה גבוהה מאוד, כך שאינו פגיע להתקפות רשת כמו XSS, SQL Injection, ואחרות. אבל נגיח שעל אותו שרת שבו מאוחסן האתר המאובטח נמצא אתר נוסף, חסר חשיבות ולא מאובטח בכלל. ניתן לתקוף את האתר הנוסף ודרכו להגיע אל המחשב המאוחסן את האתרים שהם מטרה. ברגע שמשתלטים על המחשב, כל מערכות ההגנה של האתר המאובטח כבר אינן רלוונטיות והוא נפרץ.

נשק קיברנטי שהתגלה ונחתם אמנם נחסם לשימוש בצורתו המקורית, אך מכאן ועד לחסימה הרמטית והפיכת כל הקוד שפותח ללא־רלוונטי – המרחק עדיין רב. ראשית, כל כלי תקיפה מורכב ממספר מודולים (רכיבי תוכנה). בין היתר, ניתן למנות את המודול האחראי להסוואת הכלי במערכת המותקפת, מודולים שונים

לאיסוף מידע, מודול לאחסון המידע ומודול לשליחת המידע אל שרתי הפיקוד והבקרה של הכלי. אם סוס טרויאני התגלה ונחתם, ניתן לעשות שימוש חוזר בחלק מן המודולים שלו, כאשר אלה משולבים בתוך קוד של סוס טרויאני אחר. שילוב כזה ייצור כלי תקיפה חדש שעשוי לחמוק מתחת לרדאר של מערכות אנטי-וירוס. דרך אחרת לשימוש חוזר בקוד זדוני היא על ידי הסוואתו בשיטות המוכרות מעולם התוכנה כערפול (obfuscation)³² ואריזה (packing)³³. אלה יכולות לעיתים לשנות את הקוד הזדוני באופן שהוא לא יתגלה על ידי תוכנת הגנה. לבסוף, גם אם לא יתאפשר שימוש בקוד שהתגלה, ניתן לפתח קוד מוטציה המבוסס על רעיונות ואופני פעולה דומים ומנצל את אותן החולשות כמו הקוד המקורי.

טענה זו נתמכת על ידי השימוש בווריאציות השונות של הווירוס פליים שהתפרסם לאחרונה בתקשורת. גם לאחר שהתגלה הווירוס המקורי, נגזרות שונות שלו המשיכו לתקוף מחשבי יעד ללא הפרעה, עד שהתגלו גם הן.³⁴ גם הווירוס סטקסנט, שנחשב למתוחכם ביותר שהתגלה עד כה, פתח דלת לרבים שיבואו אחריו ויחקו את שיטות הפעולה שלו.³⁵ למעשה, ניתן לומר בסבירות גבוהה כי פליים³⁶ וסטקסנט יחדיו ממחישים באופן הברור ביותר את יכולת השימוש החוזר בקוד זדוני, כיוון שהם חולקים קוד רחב במשותף. אף על פי שהם נועדו למטרות שונות לחלוטין (ריגול ופגיעה במערכות בקרה תעשייתיות, בהתאמה) קיימות מספר פונקציות ששניהם צריכים למלא: חדירה למערך המחשבים של הארגון, הסוואת קיומו של הכלי, ניתוח הרשת הארגונית והתפשטות בתוכה על מנת למצוא מחשבי יעד ערכיים. את הפונקציות הללו ניתן לממש בשני כלי הנשק באמצעות אותו קוד, שנכתב ונבדק פעם אחת בלבד. היתרונות ביכולת השימוש באותו הקוד עבור שני כלים שונים הם עצומים, כיוון שתהליך ייצור נשק סייבר הוא ארוך ויקר. תהליך מציאת החולשות הוא מורכב מאוד, ודורש לעיתים מאות שעות עבודה של אנשים מיומנים. זהו תהליך שאינו מבטיח תוצאה בסופו, אף אם הושקעו בו מאמצים רבים. יתרה מכך, גם כאשר נמצאה חולשה, על מנת לנצל³⁷ אותה ולחדור דרכה למערכת מחשב יש להשקיע עוד עבודה רבה כדי לחבר את הקוד המתאים, ולבנות את הקבצים שיוכלו לעשות שימוש בחולשה. ייתכן גם שלא תימצא דרך לנצל את החולשה מפאת המורכבות שלה, ואז יהיה צורך להתחיל במחקר נוסף למציאת חולשה אחרת, קלה יותר לניצול. לכן, כאשר יצרן נשק סייבר מפתח יכולת חדירה למערכת הוא ישאף לנצל אותה בכמה תרחישים שונים ובכלים שונים, כדי למקסם את הרווח מההשקעה שלו. מנגד, ככל שיהיה שימוש רב יותר ומגוון יותר ביכולת סודית מסוימת, יגברו הסיכויים שהיא תיחשף ותיחסם לשימוש. עובדה זו מהווה גורם מרסן בשיקוליו של יצרן נשק סייבר לגבי התפשטות הכלים ושימוש ביכולת בתרחישים נוספים.

לכאורה היה צפוי כעת כי לאחר שהתוכנות הזדוניות התגלו ודבר החולשות והניצול שלהן התפרסם ברבים, התוכנות שבהן התגלו החולשות יעודכנו מייד (למשל מערכת ההפעלה windows), והעדכון יופץ לכל מחשב שבו מותקנת מערכת כזו, וכך בעצם יהפכו כל המחשבים לחסינים מפני קוד זדוני המנצל את החולשות המדוברות. אך לא כך הדבר. תהליך ההגנה על מערכות מפני קוד זדוני שהתגלה כולל ארבעה שלבים עיקריים: גילוי החולשה שבה השתמש הקוד, סגירת הפרצה במערכת, הפצת טלאי אבטחה לכלל משתמשי התוכנה והתקנתו על המחשבים. השלב של סגירת הפרצה שדרכה חדר קוד זדוני למערכת הוא מורכב, כיוון שלאחר תיקון הפרצה על התוכניתנים לוודא גם שתפקוד המערכת לא נפגע בעקבות השינוי שנעשה. יש צורך לבחון בזהירות את השפעות התיקון ולהריץ תרחישי בדיקה שונים כדי לוודא תקינות. בהתאם למורכבות המערכת, התהליך עשוי להימשך שבועות עד חודשים רבים.

יתרה מזאת, גם לאחר שפותח והופץ עדכון אבטחה (טלאי), אנשים רבים אינם מעדכנים באופן אוטומטי את המחשבים שלהם, ובמיוחד נכון הדבר בחברות אשר להן רשת תקשורת פנימית המנותקת מרשת האינטרנט. במקרה כזה, מחשבי הרשת הפנימית יעודכנו רק כאשר אחראי האבטחה יעביר באופן יזום את עדכון התוכנה מהאינטרנט אל תוך הרשת הפנימית. שתי סיבות אלו מביאות לכך שניתן לנצל חולשות גם זמן רב אחרי שהן התגלו ופורסמו.

תופעה מעניינת הקשורה בעדכוני האבטחה מזכירה את התופעה הידועה בשם "מלכוד 22". כאשר חברת מייקרוסופט, למשל, נתקלת בבעיית אבטחה במערכת ההפעלה שלה, היא מפתחת עדכון אבטחה ומעוניינת להפיץ אותו לכל המשתמשים החשופים לבעיית האבטחה. אבל ברגע שהעדכון מופץ, גם האקרים וכותבי קוד זדוני נעשים מודעים לקיומו, ויכולים לנתח אותו ולהבין איזו בעיית אבטחה הוא פותר – ובהתאם לזאת לכתוב קוד זדוני שמנצל את חור האבטחה שמייקרוסופט עצמה חשפה בפניהם. מובן שהקוד הזדוני יוכל לפעול רק במערכות שלא הותקן בהן עדכון האבטחה, אך למרבה הפלא יש לא מעט כאלה, גם של משתמשים פרטיים שאינם טורחים לעדכן את המחשב שלהם באופן תדיר, ובמיוחד בחברות שבהן נדרשת פעולה יזומה של אנשי המחשוב כדי לעדכן את מערך המחשבים בחברה. מצב זה יוצר חלון זמן של כמה ימים או יותר, שבו האקרים יכולים לנצל את פרצות האבטחה לפני שייסגרו. זוהי דוגמה לשימוש חוזר בקוד זדוני שמתאפשר באמצעות ניצול לרעה של תהליך הפצת עדכוני האבטחה. בדרך כלל, חברת מייקרוסופט מפיצה עדכוני אבטחה לתוכנות שלה ביום שלישי השני בכל חודש, ויום זה זכה לכינוי "Patch Tuesday"³⁸. בהתאם לזאת, יום רביעי שלאחר מכן מכונה "Exploit Wednesday", כיוון שביום זה מנתחים האקרים את

עדכוני האבטחה ומתחילים לנצל אותם כדי לחדור למחשבים שעדיין לא הספיקו להתעדכן.

היכולת ליצור נשק סייבר חדש המבוסס על נשק קיים או על חולשה שפורסמה איננה תמיד מיידית ופשוטה. ההאקרים שמנצלים את עדכוני האבטחה של מייקרוסופט כדי לגלות את קיומן של חולשות במערכת ההפעלה "חלונות" צריכים להשקיע זמן בניתוח הטלאי, ובהשוואת הקבצים שהוא מתקן לקבצים המקוריים לפני התיקון (כדי לזהות היכן בדיוק התבצע התיקון, כיוון ששם נמצאת החולשה). לבסוף הם גם צריכים למצוא דרך לנצל את החולשה. תהליך זה עשוי להימשך בין ימים לשבועות, כתלות במורכבות הטלאי ובנחישות של ההאקר. לעומת זאת, ניתוח מעמיק של כלי מתוחכם כמו פליים ידרוש זמן רב יותר, וכוח אדם מקצועי ומיומן יותר. בדרך כלל, ניתוח כזה נעשה על ידי מדינות או חברות אבטחה ולא על ידי אנשים פרטיים. לדוגמה, נשק הסייבר מיני-פליים (MiniFlame³⁹) שנותח באופן מעמיק על ידי חברת קספרסקי. ניתוח זה, שארך מספר חודשים ודרש משאבי כוח-אדם רבים, בוצע על מנת לפתח הגנה מפני הכלי ולהפיץ אותו בקרב לקוחות החברה. אבל תוצרי הניתוח יכולים לשמש בסיס לקוד מוטציה, העושה שימוש בטכניקות דומות ולעיתים אף בחלק מהקוד של הנשק המקורי. אם תוצרים אלה ידלפו מחברת קספרסקי לגורמים המפתחים נשק סייבר, לא יהיה זה מפתיע לגלות כלים חדשים החולקים קוד משותף עם המיני-פליים אך מופעלים על ידי תוקפים אחרים, נגד מטרות אחרות (ייתכן שאף נגד היוצר הראשוני של הנשק – אפקט הבומרנג).

בשנים האחרונות חווה העולם מגמת עלייה בתקיפות סייבר הדורשות יכולת התקפית רחבה וממושכת, ונגד יעדים אסטרטגיים ובעלי יכולת הגנה גבוהה. יכולת זו קיימת כיום רק במספר מועט של מדינות, אך לא מן הנמנע שמגמת העלייה לא תיעצר ומדינות נוספות ישיגו יכולות כאלו, גם לצורכי הגנה וגם להתקפה. מגמה זו תקפה גם לשוק עבריינות הסייבר העולמי.⁴⁰ ברוסיה, לדוגמה, ישנם סימנים המעידים על כך שגורמי פשע מאורגן החלו להצטרף "באמצעות שיתוף נתונים וכלים" כדי להגדיל את רווחיהם.⁴¹ דו"ח של מעבדת קפרסקי לסיכום שנת 2012 חשף כי היקף ההתקפות של קודים זדוניים ברשת האינטרנט בקרב לקוחות החברה כמעט הכפיל את עצמו במהלך שנת 2012 לעומת 2011 (מ-946,393,693 התקפות ב-2011 ל-1,595,587,670 ב-2012). התקפות אלה כוללות התקפות רשת ב-202 מדינות. ארגוני פשע השתמשו ב-6,537,320 דומיינים ייחודיים ככלים לביצוע התקפות פינגסיות – כשני מיליון וחצי יותר משנת 2011.⁴²

סיכום

מדינות ושחקנים לא־מדינתיים רבים מצויים במרוץ חימוש חשאי במרחב הסייבר. מפת האינטרסים של השחקנים השונים מעידה על כך שהתקפות מסוגים שונים במרחב זה דורשות מגורמים מדינתיים להיות ערוכים למגוון התקפות אפשריות. במקביל, תכונות ומאפייני שדה הקרב הקיברנטי מציבים בפני התוקף דילמות הנובעות מהיותו של הנשק הקיברנטי רב־פעמי, ולכן עצם השימוש בו חושף את יכולותיו בפני הקורבן, שיכול מצדו לעשות בו שימוש חוזר, כולל נגד התוקף עצמו (אפקט הבומרנג). כלי נשק בעלי יכולת הרס אסטרטגי (כגון סטקסנט) עלולים ליפול (או נפלו) בידי מדינות תומכות טרור וארגוני טרור ופשע, וישמשו בסיס לתקיפות סייבר. פיתוח עצמאי של כלי תקיפה קיברנטיים או רכישתם בשוק השחור עלולים להקנות לגורמים אלה יכולת ליצור נזק רב, אף אם כלים שהושגו באופן כזה אינם מגיעים לרמת תחכום של נשק קיברנטי המיוצר על ידי מדינות מתקדמות.

קיימת בעייתיות בהימצאות נשק קיברנטי בידי גורמים פרטיים, וכתוצאה מכך, תפוצה בלתי־מבוקרת שלו. לדוגמה, חוקר אבטחת מידע בכיר טען שקוד הסטקסנט נמצא ברשותו ואף הציע לשתף אותו עם אחרים.⁴³ במועד אחר טען מומחה שניתח את הסטקסנט כי קוד זה שקול לכלי נשק רב־עוצמה, אך כאשר נשאל מדוע אינו משמיד את העותק שברשותו – העדיף לא להשיב. מלבד דיון בשאלות אתיות ומוסריות, אנו סבורים כי יש מקום לביצוע הסדרה תוך־מדינתית ובינלאומית בנושא, אשר תקבע מנגנוני ויסות ואכיפה נגד תפוצת קוד זדוני. יש לשקול להגביל, ובמקרים מסוימים אף לאסור את ההחזקה בקודי מחשב זדוניים, מחשש שיגיעו לידיים הלא־נכונות שיעשו בהם שימוש לרעה. בעניין זה, ניתן אולי ללמוד מהמלחמה שמתנהלת נגד הפצת קניין רוחני שיש עליו זכויות יוצרים, כמו סרטים ומוזיקה.

כיום, ארסנל כלי הנשק הקיברנטיים בעלי יכולת פגיעה טקטית מצמצם את פער ההצטיידות בין מדינות לבין שחקנים לא־מדינתיים. לעומת זאת, מתרחב הפער בין מדינות בעלות ארסנל יכולות תקיפה נגד יעדים אסטרטגיים, לבין מדינות ושחקנים שאין ביכולתם להגיע לסף הכניסה הגבוה. לא מן הנמנע שמדינות ושחקנים נוספים יחתרו להשגת יכולת של נשק קיברנטי בעל כושר פגיעה פיזית, ומגמת העלייה הדרמטית באיומים במרחב הסייבר מחייבת כיווני פעולה להתמודדות עם איומים אלה. לכן קיים צורך חשוב להעלות לדיון את תפיסת כלי הנשק הקיברנטיים כנשק רב־פעמי שניתן לנצלו לתקיפות נוספות.

הערות

- 1 ראו: מילון אבן שושן המרכז: מחודש ומעודכן לשנות האלפים, הוצאת ליאור שרף, 2004.
- 2 Mark Ambinder, "Did America's Cyber Attack on Iran Make Us More Vulnerable?" *The Atlantic*, June 5, 2012.
<http://www.theatlantic.com/national/archive/2012/06/did-americas-cyber-attack-on-iran-make-us-more-vulnerable/258120/>
- 3 קוד מחשב שנכתב במטרה לבצע פעולה על מערכת מחשב, לרוב בעלת אופי של גניבת מידע או שיבוש תהליכים במערכת, ואשר מורץ ללא ידיעת בעל המערכת או אישורו. לדוגמה: כאשר מתגלה תוכנה זדונית על ידי חברת אנטי-וירוס, נוצרת חתימה אלקטרונית של אותו הווירוס ונשלחת לכל הלקוחות של החברה. באופן כזה, כאשר לקוח אחר יותקף על ידי אותו הווירוס, תוכנת האנטי-וירוס תזהה את ההתקפה על פי החתימה שנשלחה אליה, ותחסום אותה ביעילות.
- 5 שמואל אבן ודוד סימן-טוב, **לוחמה במרחב הקיברנטי**, מזכר 109, תל אביב: המכון למחקרי ביטחון לאומי (מאי 2012), עמ' 41.
[http://www.inss.org.il/upload/\(FILE\)1306930376.pdf](http://www.inss.org.il/upload/(FILE)1306930376.pdf)
- 6 תהליך של גילוי עקרונות טכנולוגיים והנדסיים של מוצר דרך ניתוח המבנה שלו ואופן פעולתו. לרוב, תהליך זה כולל פירוק המוצר למרכיבים וניתוח פרטני של דרך פעולתם של המרכיבים.
- 7 Drone Wars UK, "Mapping Drone Proliferation: UAVs in 76 Countries", *Global Research*, September 18, 2012,
<http://www.globalresearch.ca/mapping-drone-proliferation-uavs-in-76-countries/5305191>
- 8 William Troop, "Got Drones? The Problem With UAV Proliferation", *The World*, March 26, 2012, <http://www.theworld.org/2012/03/drones-proliferation/>
- 9 Dave Marcus and Ryan Sherstobitoff, "Disserting operation High Roller", *McAfee & Guardian Analytics*, 2012.
<http://www.mcafee.com/us/resources/reports/rp-operation-high-roller.pdf>
- 10 Martin C. Libicki, *Cyber deterrence and cyber war*, Rand, Project Air Force, 2009.
http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf
- 11 Dorothy E. Denning, Activism, "Hacktivism and Cyberterrorism, in Networks and Netwars, The future of terror, crime, and militancy", in *The Future of Terror, Crime, and Militancy*, Edited by John Arquilla and David Ronfeld, Rand Cooperation, 2001, 240.
http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf
- 12 Ian Trainor, "Russia accused of unleashing cyberwar to disable Estonia", *The Gaurdian*, 17 May, 2007.
- 13 שמואל אבן ודוד סימן-טוב, **לוחמה במרחב הקיברנטי**, עמ' 63.
- 14 באירוע זה הוחדר ב־15 באוגוסט 2012 קוד זדוני למערכת המחשב של אראמקו, חברת נפט סעודית בבעלות ממשלתית, ועל פי הדיווחים הוצאו כ־30,000 מחשבים מכלל שימוש.
- 15 יצחק בן ישראל, ליאור טבנסקי, "מבט בינתחומי על אתגרי הביטחון בעידן המידע", **צבא ואסטרטגיה**, כרך 3, גיליון 3 (דצמבר 2011), עמ' 25.
- 16 יורם שוייצר, גבי סיבוני ועינב יוגב, "המרחב הקיברנטי וארגוני טרור", **צבא ואסטרטגיה**,

- כרך 2, גיליון 3 (דצמבר 2011), עמ' 34.
- 17 James A. Lewis and Katrina Timlin, "Cybersecurity and Cyberwarfare," *UNIDIR Resources*, 2001. www.unidir.org/pdf/ouvrages/pdf-1-92-9045-011-J-en.pdf
- 18 רמי אפרתי וליאור יפה, "כך בונים הגנה קיברנטית לאומית", *Israel Defense*, 11 באוגוסט, 2012.
<http://www.israeldefense.co.il/?CategoryID=512&ArticleID=2960>
- 19 כגון תקיפות הנערכות נגד מטרות אזרחיות, בהן תשתיות לאומיות בעלות חשיבות קריטית, חברות המהוות חוליות בשרשרת הנגישות לאותן המטרות וחברות שתקיפתן משרתת צורך כלכלי.
- 20 אלי סניור, "האינטרפול: 1,000 התקפות סייבר בדקה בארץ", *YNET*, 8 במאי, 2012.
<http://www.ynet.co.il/articles/0,7340,L-4226242,00.html>
- 21 שם.
- 22 דו"ח של חברות McAfee ו-Guardian
Dave Marcus and Ryan Sherstobitoff, *Dissecting operation High Roller*, McAfee & Guardian Analytics, 2012.
http://www.guardiananalytics.com/researchandresources/researchstudies_resources/Dissecting_Operation_High_Roller_Research_Report.pdf
- 23 Greg Farrell and Michael A. Riley, "Hackers take \$1 billion a year as Banks blame their clients", *Bloomberg*, 5 August, 2011.
<http://www.bloomberg.com/news/2011-08-04/hackers-take-1-billion-a-year-from-company-accounts-banks-won-t-indemnify.html>
- 24 Dorothy E. Denning, *Cyber terrorism*, Testimony before the Special oversight on Terrorism, Committee on Armed Service, U.S House of Representatives, May 23, 2000.
<http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>
- 25 Dorothy E. Denning, *Activism, Hactivism and Cyber terrorism*, 269
- 26 גיא גרימלנד ואחרים, "מתקפת סייבר", *TheMarker*, 16 בינואר, 2012.
<http://www.themarker.com/markets/1.1618274>
- 27 אור הירשאווגה ונתי טוקר, "קרבות הסייבר נגד ישראל: 100 מיליון תקיפות, ללא הישגים משמעותיים", *TheMarker*, 22 בנובמבר, 2012.
<http://technation.themarker.com/hitech/1.1871058>
- 28 John D. Sutter, *Anonymos declares cyber war on Israel*, *CNN*, 19 November, 2012.
http://edition.cnn.com/2012/11/19/tech/web/cyber-attack-israel-anonymous/index.html?hpt=hp_c1
- 29 שמואל אבן ודוד סימן-טוב, **לוחמה במרחב הקיברנטי**, עמ' 23.
- 30 למשל תוכנית הסייבר של ארגון חזבאללה:
Ward Carroll, "Hezbollah's Cyber Warfare Program", *DEFENSETECH*, June 2, 2008,
<http://defensetech.org/2008/06/02/hezbollahs-cyber-warfare-program/>
- 31 חולשה היא תכונה של רכיב תוכנה / חומרה / פרוטוקול המאפשרת לעשות שימוש ברכיב זה שלא למטרה שעבורה נועד, באופן שיעניק יתרון למנצל תכונה זו. היתרון יכול להתקבל באחת או יותר מהדרכים הבאות: השתלטות על מערכת, שיבוש מערכת, השגת מידע מתוך המערכת.
- 32 ערפול קוד הוא טכניקה מעולם התוכנה שלוקחת קוד מחשב קיים המיועד לביצוע משימה מסוימת, ומשנה אותו באופן שהפונקציונליות שלו לא תיפגע, אך התוצר יהיה

- מספיק שונה מהמקור, באופן שתוכנות אנטי־וירוס לא יוכלו לזהות את התוצר כווירוס. תוכנות אנטי־וירוס המבוססות על זיהוי חתימות בקוד (חתימה בהקשר זה היא מקטע קוד שנועד לבצע פעולה מסוימת, שניתן לייחס אותה בסבירות גבוהה לתוכנה זדונית) יתקשו לזהות כווירוס קוד שעבר ערפול מוצלח, כיוון שכל החתימות המוכרות להן לא יופיעו בתוצר של תהליך הערפול.
- 33 אריזת קוד הינה סוג מתוחכם של ערפול קוד. בתהליך האריזה, קוד מחשב זדוני עובר שינוי צורה קיצוני כך שהוא כבר כלל לא נראה כמו קוד ריצה, אלא יותר כמו קובץ טקסט תמים. שיטה זו מונעת כמעט לחלוטין את היכולת של תוכנות אנטי־וירוס לגלות את הקוד הזדוני לפני שהוא מתחיל לבצע את פעולתו (למשל, בזמן החדירה של הווירוס למחשב, הוא לא יתגלה). קוד ארוז פועל על ידי תוכנת עזר תמימה, שכאשר היא מתחילה לרוץ היא קוראת את קובץ הטקסט שבו מסתתר הקוד הזדוני, מתרגמת את הטקסט לפקודות ריצה ובעצם הופכת בעצמה להיות וירוס. ניתן לדמות זאת לוירוס מתחום הביולוגיה, המשתלט על תא חי ומנצל את כל המנגנונים של התא לצרכיו.
- 34 רגנה אשוח, "Kaspersky חושפת את miniFlame – קוד זדוני שתוכנן לפעולות ריגול", *YedaTech*, 15 באוקטובר, 2012.
<http://www.yedatech.co.il/yt/news.jhtml?value=19827>
- 35 למאמר על ממשיכי הדרך של סטקסנט:
Steven Cherry, "Sons of Stuxnet", *IEEE*, December 14, 2011, <http://spectrum.ieee.org/podcast/telecom/security/sons-of-stuxnet>
- 36 על אודות פליים:
Aleks, "The Flame: Questions and Answers", *SECURELIST*, May 28, 2012, http://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers
- 37 ניצול חולשה (Exploit) הינו קוד מחשב או קובץ שנועד לנצל פגיעות או חולשה של מערכת מסוימת באופן שיעניק לכותב ה־Exploit יכולת חדירה או שיבוש של המערכת המותקפת. לדוגמה: תוכנה להצגת תמונות על מסך המחשב, שמכילה חולשה מסוימת המאפשרת להריץ קוד על המחשב המותקף. ניצול חולשה כזאת עשוי לבוא בצורת קובץ תמונה המכיל קוד שאותו מעוניין התוקף להריץ על המחשב המותקף. קובץ תמונה כזה צריך, כמובן, לא רק להכיל את הקוד אלא גם לדעת לנצל את החולשה, או את נקודת התורפה של התוכנה להצגת התמונות.
- 38 המילה Patch מתארת עדכון או טלאי אבטחה שמולבש על המערכת.
- 39 Global Research and Analysis Team, Kaspersky Labs, "miniFlame aka SPE: Elvis and his friends", *SECURELIST*, October 15, 2012.
http://www.securelist.com/en/analysis/204792247/miniFlame_aka_SPE_Elvis_and_his_friends
- 40 שוק זה הוערך ב־2011 בלמעלה מ־12.5 מיליארד דולר, כאשר הנתח של רוסיה בעוגה הוא כ־2.3 מיליארד דולר (קרוב לכפול מערכו המוחלט בהשוואה לשנה הקודמת).
להרחבה: http://group-ib.com/images/media/Group-IB_Report_2011_ENG.pdf
- 41 צ'ילופו, קרדאש וס. סלמואירגי, "תוכנית להרתעת סייבר: בניית יציבות באמצעות כוח", **צבא ואסטרטגיה**, כרך 4, גיליון 3, (דצמבר 2012), עמ' 5.
- 42 Denis Maselnnikov and Yuri Namestinkov, "Kaspersky Security Bulletin 2012. The overall statistics for 2012", *SECURELIST*, December 2012.
http://www.securelist.com/en/analysis/204792255/Kaspersky_Security_Bulletin_2012_The_overall_statistics_for_2012
- 43 כותבי מאמר זה נכחו באופן אישי בפגישה עם איש חברת אבטחת המידע בנובמבר 2012.