מרחב הסייבר והביטחון הלאומי

מבחר מאמרים

גבי סיבוני, עורך

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

מרחב הסייבר והביטחון הלאומי

מבחר מאמרים

גבי סיבוני, עורך

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

המכון למחקרי ביטחון לאומי (חל"צ)
חיים לבנון 40
ת.ד. 39950
תל־אביב 6997556

info@inss.org.il
http://www.inss.org.il

ISBN: 978-965-7425-50-3

הביא לדפוס: משה גרונדמן
עיצוב גרפי: מיכל סמו־קובץ, המשרד לעיצוב גרפי, אוניברסיטת תל־אביב

המכון למחקרי ביטחון לאומי (חל"צ)

המכון למחקרי ביטחון לאומי, המשלב בתוכו את מרכז יפה למחקרים אסטרטגיים, הוקם ב־2006.

מטרותיו של המכון למחקרי ביטחון לאומי הן שתיים: הראשונה – לבצע מחקר בסיסי, העומד במבחן אמות המידה האקדמיות הגבוהות ביותר והעוסק בתחומי הביטחון הלאומי של ישראל, המזרח התיכון והמערכת הבינלאומית. השנייה – לתרום לדיון הציבורי ולעבודת הממשל בנושאים הנמצאים – או אמורים להימצא – בראש סדר היום הביטחוני של ישראל.

קהל המטרה של המכון הוא דרג מקבלי ההחלטות, מערכת הביטחון, מעצבי דעת הקהל בישראל, הקהילה האקדמית העוסקת בתחומי הביטחון בישראל ובעולם, והציבור המתעניין באשר הוא.

תוכן

3 | **הקדמה**

7 | **הגנת נכסים ותשתיות קריטיות מפני תקיפה קיברנטית – הממד הסטטוטורי**
גבי סיבוני

15 | **המרחב הקיברנטי וארגוני הטרור**
יורם שוייצר, גבי סיבוני ועינב יוגב

23 | **הגנה על תשתיות קריטיות מפני איום קיברנטי**
ליאור טבנסקי

39 | **מה עומד מאחורי לוחמת הסייבר של סין**
גבי סיבוני וי"ר

53 | **פשע קיברנטי – סכנה לביטחון הלאומי?**
ליאור טבנסקי

69 | **לוחמת הסייבר של איראן**
גבי סיבוני וסמי קרוננפלד

89 | **תפוצת נשק קיברנטי במרחב הסייבר**
דניאל כהן ואביב רוטברט

107 | **כישלון שיטות הגנת הסייבר הקלאסיות – מה הלאה?**
אמיר אורבוך, גבי סיבוני

הקדמה

יכולות המחשוב והתקשורת ותפוצתן הגלובלית של מערכות המידע גורמות לכך שמדינות חשופות לפגיעה בהן, בין אם על ידי גורמים פליליים ובין אם על ידי גורמים עוינים. למעשה, רוב המערכות בחברה מפותחת תלויות בתשתית מחשוב ומידע. התלות ההולכת וגוברת בטכנולוגיית מידע ובתקשורת מביאה לידי כך שפגיעה במחשבים ובתהליכי זרימת מידע עלולה להוביל לפגיעות פיזיות ממשיות. כלומר, ניתן לשבש מערכות ניהול, שליטה ובקרה באמצעות שינויים בתוכנת המחשב, ללא צורך בתקיפה פיזית. היכולת הטכנולוגית הגבוהה של ישראל בתחומי המחשוב והתקשורת מקנה לה יתרונות עצומים בכל תחומי העשייה ובביטחון בפרט, ומאפשרת לה לפעול במרחב זה הן לצורכי סיכול והן להשגת יתרונות בשדה הקרב המודרני. אולם, התלות הגוברת במחשבים עלולה להיות גם נקודת תורפה המחייבת מענה.

קובץ מאמרים זה מציג חלק מתוצרי המחקר שהופקו במסגרת תוכנית לוחמת סייבר במכון הנתמכת על ידי קרן ג'וזף וג'נט ניובאוואר, פילדלפיה, ארצות הברית. המאמרים בחוברת זו פורסמו בכתב העת **צבא ואסטרטגיה** והינם פרי עטם של חוקרי המכון. תוכנית המחקר עוסקת במגוון היבטים, ביניהם: בניית מסגרת למושגי יסוד בתחום לוחמת הסייבר, ניתוח יכולות לוחמת הסייבר במדינות המייצרות לישראל ולעולם עניין מיוחד, דוגמת סין ואיראן. נושאים נוספים בתוכנית המחקר הם בחינת ההשפעות של עולם הפשע על הביטחון הלאומי, התפוצה של נשק סייבר, ניתוח כישלון שיטות ההגנה ההיקפית בסייבר ובחינת כיווני מענה חדשים, והצעות לקידום רגולציה בתחום הגנת הסייבר של המגזר האזרחי.

במהלך השנה האחרונה הוקם במכון למחקרי ביטחון לאומי פורום סייבר – מדיניות ואסטרטגיה. הפורום הוקם, כדי לתת מענה לפער הקיים בשיח שבין שתי סביבות: הסביבה הטכנולוגית, שבה פועלים גורמים רבים ובה התפתח ידע רב מאוד – בישראל (ובעולם), והסביבה האסטרטגית ופיתוח המדיניות. פורום זה מאפשר לייצר שיח בלתי־אמצעי בין חברות טכנולוגיות לבין גורמי מדיניות ואסטרטגיה, ובכך לפתח תובנות ייחודיות לטובת ביצור הגנת הסייבר של ישראל בפרט, וקידום הנושא בארץ ובעולם.

בברכה,

גבי סיבוני, עורך
ראש תוכנית לוחמת סייבר, המכון למחקרי ביטחון לאומי

הגנת נכסים ותשתיות קריטיות מפני תקיפה קיברנטית – הממד הסטטוטורי

גבי סיבוני

מבוא

התפתחותן של מערכות המחשוב והתקשורת בעשורים האחרונים השפיעה על הביטחון הלאומי של מדינות, ובכללן של מדינת ישראל. מערכות אלו ותפוצתן הגלובלית גרמו למדינות להיות חשופות לפגיעה במרחב הקיברנטי שלהן על ידי גורמים שונים ומגוונים, בהם מדינות עוינות, ארגוני טרור, גורמים פליליים ואף פרטים הפועלים מתוך אתגר אישי או מתוך מניעים אנרכיסטיים. רוב המערכות בחברה מפותחת תלויות בתשתיות מחשוב ומידע, והתלות בטכנולוגיות אלו גורמת לכך שפגיעה במחשבים ובתהליכי זרימת מידע עלולה לשבש, לשתק ולעיתים אף לגרום לפגיעות פיזיות של ממש במערכים חיוניים. כך, למשל, ניתן לשבש מערכות ניהול, שליטה ובקרה באמצעות שינויים בתוכנת המחשב, ללא צורך בתקיפה פיזית שלהן. ניתן להעריך כי פני העימותים בעתיד ישתנו ללא הכר ויתבססו במידה רבה על לוחמה קיברנטית.

עוצמתה של מדינה נמדדת על ידי שילוב בין העוצמה הכלכלית, החברתית והמדעית שלה ובין העוצמה הצבאית. תפקידה של העוצמה הצבאית הוא להגן על האזרחים והטריטוריה כדי שאלה יוכלו לשמר ולפתח את העוצמה הכלכלית. פגיעותו של המרחב הקיברנטי לתקיפות באמצעות מערכות תקשורת ומחשבים, מביאה לשינוי דרמטי במשוואה זו. לראשונה ניתן לפגוע אנושות בעוצמה הכלכלית של מדינות על ידי שיתוק מערכים כלכליים ואזרחיים שלהן, ללא הפעלת כוח אש ותמרון כוחות. יכולות המדינות לפעול במרחב הקיברנטי, הן לצרכי הגנה והן לצרכי מתקפה, יתפסו בעתיד, קרוב לוודאי, מקום משמעותי לצד היכולות הצבאיות הקלאסיות.

אל"ם (מיל.) ד"ר גבי סיבוני הוא ראש תכנית צבא ואסטרטגיה ותכנית לוחמת סייבר במכון למחקרי ביטחון לאומי.

מאמר זה ראה אור לראשונה ב**צבא ואסטרטגיה**, כרך 3, גיליון 1, מאי 2011, עמ' 81–88.

בצד קִדמה, רווחיות ורווחה שאפיינו מדינות רבות בעשורים האחרונים, נחשפו בשנים האחרונות אותן מדינות, ובכלל זה גורמי הייצור ואספקת השירותים הלאומיים בהן, לאיומים חדשים, שטרם ניתנה הדעת כיצד ראוי להתמודד עימם. עד לפני שנים לא רבות התעשייה (הפרטית והציבורית) הייתה מוגנת על ידי המדינה. כך, למשל, תחנת כוח ליצור חשמל, בין אם הייתה בבעלות פרטית ובין אם הייתה בבעלות ציבורית, הייתה חשופה לפגיעה פיזית שלא בגין תאונה רק באם המדינה הייתה נקלעת למלחמה פיזית של ממש. תפקידה של המדינה היה להבטיח את ההגנה על התשתיות, המוסדות הכלכליים, מפעלי תעשייה ועוד. מוסדות ציבוריים היו מוגנים על ידי המדינה מעצם קיומם במרחב הטריטוריאלי הנתון למרותה ושליטתה.

מדיניות ההפרטה שצברה תאוצה בעשורים האחרונים הפקידה בידיים פרטיות חלקים נרחבים ממפעלי התשתית שבאופן מסורתי היו בידי הריבון: תקשורת, תחבורה, חשמל, אנרגיה, תעשיות כבדות ועוד. לצידן של התעשיות המסורתיות עלו וצמחו תעשיות חדשות בתחומי הטכנולוגיה העילית, המהוות מרכיב נכבד בתל"ג של מדינות רבות.

בשל ההבנה האוניברסלית כי "המגן על הכל אינו מגן על כלום",[1] פיתחו מדינות שונות דרכים להגן בעיקר על התשתיות והמערכות הקריטיות לתפקודן. במדינת ישראל הוקמה בשנת 2002 הרשות הממלכתית לאבטחת מידע, ה"מופקדת על הנחיה מקצועית של הגופים המונחים שבאחריותה בתחום אבטחת תשתיות מחשב חיוניות מפני איומי טרור וחבלה בתחום אבטחת מידע מסווג ומפני איומי ריגול וחשיפה".[2] בהקשר זה הוקמה ועדת היגוי במועצה לביטחון לאומי, שתפקידה לבחון את סיכוני אבטחת המידע, ונקבע כי הכללים שתקבע יחולו על כמה גופים ומוסדות שמערכות המידע שלהם הוגדרו כקריטיות, בהם חברת החשמל, בנקים, משרדי ממשלה וכדומה. הוועדה גם הוסמכה להחליט על הוספת גופים לרשימה זו מעת לעת.[3]

הגופים בשירות הציבורי הנדרשים להגנה מפני התקפה קיברנטית נמצאים זה מכבר תחת הנחיית הרשות לאבטחת מידע. עם זאת, התפתחויות במבנה הכלכלה הישראלית הביאו לכניסה של גורמים, תהליכים, נכסים ופרויקטים חדשים, שפגיעה בהם היא בעלת פוטנציאל נזק משמעותי ברמה הלאומית. מצב זה חושף ומגדיל באופן קבוע את מגוון התורפות והמטרות לתוקפים במרחב הקיברנטי. לאור זאת, קיימת חשיבות רבה ליכולת לזהות ולבחון את הגורמים הנוספים שפעילותם מחייבת הנחיה של הרשות לאבטחת מידע.

לא תמיד ניתן לַכַּמֵת נזק אפשרי זה רק להיבטים הכספיים שלו או להשפעתו על התל"ג. נזקים משמעותיים יכולים להיגרם גם לנכסים וערכים בעלי חשיבות

לאומית. כך, לדוגמה, בארצות הברית תוכניות ההגנה מופעלות גם על אתרי מורשת וזיכרון.[4]

מאמר זה מבקש להציע גישה שתאפשר לקיים תהליך שיטתי, תוך שימוש בכלים סטטוטוריים קיימים, בעזרתו ניתן יהיה לזהות גופים נוספים (בעיקר מהסקטור הפרטי) שפגיעה בהם עלולה להשפיע על הביטחון הלאומי, ולחייבם להפעיל מנגנוני הגנה מתאימים על הנכסים והתשתיות הקריטיות שלהם.

על מה להגן?

במסמך של המשרד האמריקאי לביטחון פנים סוקר פטריק בֶּגְס[5] כיצד רואים הגורמים המוסמכים בארצות הברית את מערך התשתיות והמשאבים הקריטיים להגנה ואת הממשק של אלה עם מערך התשתיות הקיברנטיות והפיזיות.

מיפוי התשתיות הקריטיות להגנה בארצות הברית כולל את התחומים הבאים: מים, אנרגיה, תקשורת, תחבורה, תעשייה כימית, חקלאות ותעשיית מזון, מערכות מידע, בנקאות ושירותים פיננסיים ומסחריים, שירותי בריאות, ולבסוף נכסים בעלי חשיבות לזיכרון הלאומי האמריקאי (אנדרטאות, אתרי מורשת וכדומה). תחומים אלה נשענים על שני מרכיבי תשתית בסיסיים: הראשון נוגע למרכיבי התשתית הפיזית דוגמת תחנות כוח, סכרים, נמלי ים ואוויר, כבישים, מסילות ברזל, תשתיות הולכה למיניהן,[6] בתי חולים, מפעלים ועוד. המרכיב השני נוגע לתשתיות הקיברנטיות, בהן: מערכות תוכנה, חומרה, שרתי אינטרנט, מערכות שליטה ובקרה ושירותי מידע.

כדי לאפשר את הבסיס המתאים לגיבוש תוכניות הגנה, מפעיל המשרד האמריקאי לביטחון פנים מתודולוגיה בשם "סקירת עמידות קיברנטית"[7] של גופים ותשתיות קריטיות השייכים לסקטורים שתוארו לעיל. גישה זו מאפשרת לגבש תמונת מצב לגבי מספר היבטים, בהם: הגדרת נכסים קריטיים להגנה, ניהול התקשורת, מרכיבי המשכיות השירות, ניהול טכנולוגי, היקף התלות במרכיבים חיצוניים, ניהול אירועים ותאונות, יכולת הערכת מצב, איתור וניהול תורפות ועוד. כתוצאה מסקירה זו, יכולים מקבלי ההחלטות לקבל תמונת מצב ולגבש תוכנית פעולה לשיפור העמידות הקיברנטית של הארגון.

משאותר הארגון או הגוף שעליו יש להפעיל את המתודולוגיה, התהליך הינו שיטתי וסדור. הבעיה היא שאנו חסרים עדיין את הדרך בה ניתן לאתר את הגופים והארגונים שיידרשו לתהליך זה.

המצב בישראל דומה למדי. הרשות לאבטחת מידע מביאה מעת לעת לאישור ועדת ההיגוי במטה לביטחון לאומי (המועצה לביטחון לאומי לשעבר) רשימה של גופים נוספים שיידרשו להעמיק את הגנתם ולעמוד בהנחיות האבטחה של

הרשות, אולם אין בנמצא תהליך סטטוטורי שיטתי ומחייב שיאפשר איתורם של גופים כאלה.

העובדה כי תחום או סקטור המהווה תשתית קריטית מורכב ממספר רב של גופים ומערכות (מאות ולעיתים אלפים), גורמת לכך שאין משמעות להגנה על הסקטור ככזה. הביטוי בפועל של ההגנה נוגע לפעולות הנעשות על ידי ארגונים, חברות, מתקנים ותהליכים ספציפיים השייכים לאותו סקטור. השאלה הנשאלת היא כיצד ניתן לאתר את הגופים האלה, במיוחד כאשר כמעט לכל חברה עסקית או משרד ממשלתי ממשק עם הסקטורים המוגדרים במסגרת התשתיות הקריטיות להגנה. לדוגמה: הגנה על תשתיות אספקת המים ואיכותם בישראל אינה נוגעת רק לתהליכים בחברת "מקורות", כי אם גם לעשרות ספקי מים אחרים, אגודות, תאגידי מים, מתקני התפלה והולכה, מתקני טיפול בשפכים, מתקני טיפול והולכת קולחים ועוד. חלק גדול של מתקנים אלה מופעל על ידי יזמים פרטיים, שההפעלה של מנגנוני הגנה אינה בראש מעייניהם. המצב הזה חל גם על תחומים רבים נוספים.

זאת ועוד, במקרים רבים יש להגן גם על מערכות משיקות וקשורות לגורמים המוּנְחים. להלן דוגמה הממחישה היבט זה: מפעל תעשייתי שנקבע כי הוא מהווה מרכיב חיוני פועל תחת ההנחיה של הרשות לאבטחת מידע. לעיתים מפעל זה תלוי בפעולתו ביצרנים אחרים ("יצרני לוויין" קטנים יותר) המספקים תשומות (לעיתים קריטיות) לתהליך הייצור של המפעל המוגן. במקרים רבים נמצא כי חלק מ"גורמי לוויין" אלה אינם נכללים בקבוצת התשתיות הקריטיות להגנה, ולכן אינם מפעילים תהליכי הגנת מידע מסַפקים. כך, יתכן כי פגיעה קיברנטית בגורמים אלה עלולה לגרום לנזקים משמעותיים במפעל המוגן.

השימוש בטכנולוגיות מידע בישראל הוא נרחב מאוד, הן בסקטורים הציבוריים והן בסקטורים הפרטיים. ישראל מספקת, אפוא, כר מטרות נרחב לתוקף הקיברנטי הפוטנציאלי. לכן, איתור גופים נוספים, שפעילותם מחייבת הנחייה של הרשות לאבטחת מידע, הינו מטלה חיונית לצורך בניית מערכת הגנה אופטימאלית. סקרים הנערכים מעת לעת ומידע המועבר ממשרדי הממשלה השונים חיוניים בתהליך זה אולם אינם מספקים. יש ליצור תהליך מובנה שיאפשר שיפור משמעותי, בעיקר בכל הקשור למיזמים מסוימים בסקטור הפרטי החשופים לפגיעה קיברנטית, אשר השפעתה עלולה להיות רחבה ואף להגיע לרמה הלאומית.

התהליך המוצע: שימוש בכלים סטטוטוריים קיימים

עיקרי ההצעה לשיפור המצב שתואר לעיל נוגעים להכנסת תחום ההגנה הקיברנטית כמרכיב מובנה בתהליך הסטטוטורי הקיים, וזאת הן בשלבי ההקמה של מיזם (אישורו בוועדות התכנון השונות) והן בתהליך התפעול שלו (חוק רישוי עסקים). מוצע, כי במסגרת תהליכי התכנון במדינה יידרש כל מיזם המוגש

לאישור בוועדות התכנון להגיש תסקיר עמידות קיברנטית. תסקיר זה יהווה הכלי הסטטוטורי העיקרי לצורך איתור ובחינת חשיפתו של המיזם לאפשרות של התקפות קיברנטיות ולגיבוש תהליכי הגנה נגד חשיפות אלו. התסקיר גם יספק לרשות לאבטחת מידע כלי לאיתור וניהול מערך התשתיות הקריטיות להגנה במדינה. לצד זאת, תוכל הרשות הרלוונטית הממונה על רישוי המיזם – רישוי המחייב חידוש עיתי – לבדוק את העמידה המתמשכת של הגוף הנבחן בהוראות ההגנה הקיברנטית.

כדי להסביר הצעה זו יש להרחיבה ולפרטה. הקמה של כל מיזם במדינת ישראל, ובכלל זה מיזמי תשתיות לאומיות, מחייבת עמידה בתהליכי התכנון הסטטוטורי הנוהג בישראל. כך, מיזמים הכרוכים בבניית מתקנים ומבנים מחויבים לקבל את אישורן של ועדות התכנון השונות בהתאם לעניין: מקומיות, מחוזיות וארצית. הבדיקה של מסמכי התכנון המוגשים לאישור הגורם התכנוני בישראל הינה כלי הבקרה המרכזי של הרשויות על מיזמים אלה. במסגרת המסמכים המוגשים לבחינת ועדות התכנון כיום, ניתן למצוא מסמכים הנוגעים לכיבוי אש, להיבטים של בריאות הציבור, להיבטים סביבתיים, לטיפול בחומרים מסוכנים, להגנת העורף ועוד. מסמכים אלה מגדירים את הצעדים אותם ינקוט היזם כדי לעמוד בדרישות המתחייבות בכל תחום. אלה עוברים לבקרת גורמי הרגולציה המוסמכים, המפעילים מומחים שתפקידם להביא לכך שבסופו של התהליך יוכל המיזם להיות מוקם והאינטרס והביטחון הציבורי בתחומים השונים נשמרים.

במדינת ישראל נדונים מדי שנה עשרות מיזמים, שפגיעה בהם עלולה לפגוע בביטחון הלאומי. לדוגמה: מתקני תשתית, מתקני טיפול במים ובשפכים, מערכות הולכה, פרויקטים תחבורתיים, מתקני אנרגיה ותקשורת. לצד אלה נדונים הרחבות והקמות של מפעלי תעשייה ועוד מגוון רחב מאוד של פרויקטים שונים. פגיעה קיברנטית בפרויקטים ובמיזמים אלה, או בחלקם, עלולה לגרום נזק לכלכלת המדינה לא רק בצורה ישירה, כגון היעדר יכולת לספק שירות חיוני, אלא גם בצורה של פגיעה מסחרית ביכולת של חברות ישראליות שהותקפו לספק את מוצריהן למשך זמן נתון.

אחת הדוגמאות שיש בהן כדי לבאר את התהליך המוצע הינה הדרישה להגיש תסקיר השפעה על הסביבה. מטרתו של התסקיר הינה לאתר ולבחון את המִפגעים הסביבתיים העלולים להיגרם כתוצאה מהקמת המיזם ואת הדרכים למזער פגיעה זו לרמה נסבלת. הגשתו של התסקיר מעוגנת בתקנות התכנון והבנייה (משנת 1982, ובגרסתן הסופית משנת 2003). מקורו של התסקיר הינו בהתעוררות המודעות הציבורית בארצות הברית לנושאים הסביבתיים, אשר הביאה בשנת 1970 לחקיקת חוק המחייב הכנה של תסקירי השפעה על הסביבה כחלק מהתהליך התכנוני שם.

לצד המרכיב התכנוני למיזמים חדשים ניתן, כאמור, לעשות שימוש גם בתהליך רישוי העסקים המחייב חידוש עיתי, כדי לוודא שפעלת המיזם לאורך שנים עומדת בקריטריונים מתחייבים בתחומים שונים, כולל בתחום האבטחה מפני התקפה קיברנטית. שופט בית המשפט העליון לשעבר, מישאל חשין, קבע באחד מפסקי דינו: "מטרתו של החוק [לרישוי עסקים] היא לשמור ולהגן על ערכים שונים הנתפסים בחברתנו כערכים חשובים... כך הוא הערך של שלום הציבור, כך הוא הערך של שמירה על בריאות הציבור ובטיחותו, כך הוא הערך של שמירה על איכות הסביבה ואיכות החיים... להגנה על מטרות [ה]חברה..."[8] מדברי השופט חשין ניתן להסיק כי הכלים אותם מספק חוק רישוי עסקים ניתנים לשימוש גם לצורך הגנה קיברנטית וכי זו עולה בקנה אחד עם מטרותיו. בכך הם מאפשרים כלי בקרה חוקי נוסף בידי הרשות לאבטחת מידע, שבאמצעותו היא תוכל לוודא כי גם מיזמים קיימים יעמדו בקריטריונים מתחייבים, ובמקרים מסוימים אף לדרוש מבעלי עסקים פרטיים להגיש תסקיר עמידות קיברנטית ולחייבם למלא אחר הנחיות הביטחון.

כאמור לעיל, מיזמים בתהליך הקמה, ובמקרים מסוימים כאלה שכבר הוקמו, יידרשו על פי ההצעה להגיש תסקיר עמידות קיברנטית לבחינת הרשות לאבטחת מידע, כדי שזו תוכל לוודא שהוראות הגנה חיוניות מתקיימות. ניתן להציע כמה קווים מנחים לתוכנו של תסקיר זה, כמו גם לגורמים שיוסמכו לערוך אותו ולהגישו, וכן לגורמים שיוסמכו לבדוק אותו. מבחינה סטטוטורית, תחולת התסקיר צריכה להיות גורפת ועליה לחול על כל הבקשות, אלא אם ניתן לכך פטור מהגורם המוסמך. אולם מבחינה מעשית, תידרש הרשות לאבטחת מידע לקבוע אמות מידה שיגדירו את המיזמים והפרויקטים שלגביהם תתקיים חובת הגשת התסקיר. אמות מידה אלו יוכלו להתייחס למספר מרכיבים, כמו גודלו של המיזם, הסקטור אליו הוא משתייך (לדוגמה, מיזם הפועל בסקטור האנרגיה, גז טבעי וכדומה), הממשקים של מיזם זה עם גורמים הנמצאים כבר תחת הנחיית הרשות לאבטחת מידע, והיבטים שונים הנוגעים לתחולת הנזק של תקיפה קיברנטית על הגוף.

משהוחלט כי על גוף להגיש תסקיר עמידות קיברנטית, יופעל התהליך לאור אבני הדרך הבאות:

א. **הנחיות לתסקיר** – הרשות לאבטחת מידע תהיה אחראית להכין הנחיות לביצוע התסקיר. על הנחיות אלו להיות מותאמות למיזם או לגוף הקונקרטי. מוצע כי ההנחיות יכללו כמה מרכיבים, בהם: מיפוי פוטנציאל הנזק כתוצאה מתקיפה קיברנטית; מיפוי תורפות המיזם או התוכנית; הוראות שיאפשרו מזעור החשיפה והנזק.

ב. **הכנת התסקיר** – התסקירים יוכנו באחריותו ובמימונו של היזם. לצורך הכנה זו ייעשה שימוש ביועצים שייבחרו מתוך קבוצת יועצים ייעודיים שיוכשרו

ויוסמכו על ידי הרשות לאבטחת מידע. יועצים אלה יפעלו לאור ההנחיות להכנת התסקיר.

ג. **בדיקת התסקיר** – בדיקת התסקיר תבוצע באחריות הרשות לאבטחת מידע. גם כאן תוכל הרשות לעשות שימוש ביועצים חיצוניים שיוכשרו ויוסמכו לבדיקה של תסקירים. עלות הבדיקה תוכל להיות מוּחלת על היזם. בתהליך זה ייתכנו מספר מעגלי הערות ותשובות בין גורמי הרשות לאבטחת מידע ובין הנבדק.

ד. **אישור התסקיר** – בחינה ואישור התסקיר ייעשו על ידי הגורמים המוסמכים ברשות לאבטחת מידע, שגם תקבע את המשך הנחיית הגוף שמסר את התסקיר. אישור זה גם יוכל להתייחס להיבטים הנוגעים להתניות לרישוי העסק, כמו גם להוראות שיש להחיל על תוכניות היזם.

כאמור, השימוש בחוק רישוי עסקים מהווה פלטפורמה מתאימה ליישום הוראות והנחיות בתחום ההגנה מפני מתקפה קיברנטית. עם זאת, בשל מגבלות החלות על כל הקשור לביטחון וזליגה של מידע, נדרש יהיה להגדיר תהליך זה כתהליך ממודר, שאינו פתוח לציבור הרחב אלא רק לגורמים מוסמכים.

סיכום

האיומים על חברות אזרחיות גדלים והולכים, לא רק בשל היכולות לתקוף אותן על ידי מתחרים עסקיים אלא גם בשל החשיפה שלהן לתקיפות של גורמים עוינים. גורמים אלה מזהים את פוטנציאל הנזק לתשתית הכלכלית של המדינה, הגלום בפגיעה בחברות אלו.

מדינות נוטות להגן בעיקר על גופים להם זיקה ישירה לביטחון הלאומי. עם גופים אלה ניתן היה למנות עד לא מכבר בעיקר את משרדי הממשל, גופי מודיעין וביטחון, חברות העוסקות בייצור ביטחוני רגיש ומסווג, תשתיות קריטיות קלאסיות דוגמת חשמל, מים, תחבורה וכדומה. ההיגיון שהגדיר מי זכאי להיכנס לרשימה זו נגזר מהתפיסה האסטרטגית הקלאסית – רשימת התשתיות הלאומיות המוּעדות לפורענות במקרה של מלחמה, שפגיעה בהן עלולה לגרום לפגיעה ישירה בכושר הלחימה והעמידה של המדינה. כיום ברור שפגיעה בחברות אזרחיות, דוגמת חברת התרופות "טבע", חברות לייצור מזון כמו "תנובה" ו"שטראוס", חברות כבלים, טלוויזיה ואינטרנט, חברות ביטוח ועוד, וכן אתרי זיכרון ומורשת, עלולה לגרום לנזקים לא מבוטלים למדינה ולפגוע במרקם החיים של אזרחיה.

הקמת הרשות לאבטחת מידע וועדת ההיגוי במועצה (מטה) לביטחון לאומי הייתה צעד ראשון בכיוון המתאים. עתה, עם התגברות ההבנה שהמרחב הקיברנטי הופך לנגד עינינו למרחב לחימה של ממש, יש לשפר את העמידות של מדינת ישראל וכלכלתה מול תקיפות מסוג זה. הכנסה של תחום ההגנה מפני מתקפה קיברנטית לתוך התהליכים הסטטוטוריים במדינת ישראל תוכל לאפשר בקרה

קבועה ושיטתית על חסינותה של מערכת ההגנה הקיברנטית של ישראל ושיפור מתמשך של אמצעי ההתגוננות.

הערות

1 אמירה זו מיוחסת בדרך כלל לפרידריך הגדול.
2 אתר האינטרנט של הרשות הממלכתית לאבטחת מידע:
http://www.shabak.gov.il/about/units/reem/pages/default.aspx
3 גל מור, "אושרה תכנית לאבטחת מידע בממשלה", ynet, 11 בדצמבר 2002.
http://www.ynet.co.il/articles/1,7340,L-2310234,00.html
4 Patrick Beggs, *Securing the Nation's Critical Cyber Infrastructure*, U.S. Department of Homeland Security, February 25, 2010.
5 שם. פטריק בגס הינו ראש תחום הערכת ביטחון קיברנטי בחטיבה לביטחון קיברנטי במשרד לביטחון פנים של ארצות הברית.
6 המונח תשתיות הולכה משמש כדי לתאר תשתיות המוליכות מים, שפכים, קולחים, גז, נפט, חשמל, סיבי תקשורת וכדומה.
7 Cyber Resiliency Review (CRR).
8 השופט חשין, רשות ערעור פלילי (רע"פ) 4270/03, מדינת ישראל נגד תנובה.

המרחב הקיברנטי וארגוני הטרור

יורם שוייצר, גבי סיבוני ועינב יוגב

מבוא

באחת הסצנות בסרט "מת לחיות 2" (ארצות־הברית 1990) משתלטים טרוריסטים על מערכות המחשוב, בקרת התעבורה, והתקשורת האווירית, מתחזים לפקחי טיסה, נותנים נתונים כוזבים ובתוך סופת שלגים מנחים את טייסי המטוס ויושביו להתרסקות קטלנית על מסלול הנחיתה. לא היה ביכולתם של גורמי הביטחון לתת מענה וסיוע, וגיבור הסרט ג'ון מקליין (בגילום ברוס ויליס), נותר חסר אמצעים להושיע מלבד עמידה חסרת תכלית בערפל על מסלול הנחיתה ונפנוף לעברו של המטוס בשני לפידים מאולתרים. לכאורה מדובר בעוד פנטזיה הוליוודית שאפשר לבטלה כגוזמה, וזו אף שודרגה בסרט המשך – "מת לחיות 4". ואולם פיגועי ה־11 בספטמבר 2001, והשינויים וההתפתחויות באיומים הביטחוניים בעשור האחרון, מצביעים על כך שגם התסריטים הדמיוניים ביותר שנרקמו באולפני הוליווד, יכולים למצוא ביטוי מעשי במרחב הציבורי והביטחוני של ימינו.

השימוש במרחב הקיברנטי כזירה מרכזית ללוחמה בין אויבים או בין מדינות יריבות היה מאז ומעולם קרקע פורייה לפנטזיות ולסצנות מרהיבות בקולנוע. ואולם מרחב זה, ששימש בעבר תפאורת רקע לסצנות מלחמה הוליוודיות, הולך ותופס מקום מרכזי כזירה חשובה, שבה, כך מסתמן, ינוהלו מלחמות העתיד, וכאחת הזירות שיתבצעו בה פעולות עוינות בין גורמים יריבים. יש אפשרות שבין גורמים אלה יימצאו גם ארגוני טרור, שעד כה השתמשו בעיקר בפעילות פיזית אלימה כדי לקדם את האינטרסים שלהם, ולעתים גם את אלו של שולחיהם. נוכח איומים אלו, הקימו מדינות במערב בשנים האחרונות רשויות מיוחדות שנועדו להיערך לקראת פעולות לוחמניות תוך שימוש באמצעים טכנולוגים חדשניים נגד יעדי תשתית אסטרטגיים. מאמר זה מתמקד בניתוח היתרונות והמגבלות העלולים להביא לידי

יורם שוייצר עומד בראש פרויקט הטרור במכון למחקרי ביטחון לאומי.
אל"ם (מיל.) ד"ר גבי סיבוני הוא ראש תכנית צבא ואסטרטגיה ותכנית לוחמת סייבר במכון למחקרי ביטחון לאומי.
עינב יוגב היא עוזרת מחקר בפרויקט הטרור במכון למחקרי ביטחון לאומי.

מאמר זה ראה אור לראשונה ב**צבא ואסטרטגיה**, כרך 3, גיליון 3, דצמבר 2011, עמ' 33–39.

כך שארגוני טרור ישתמשו בכלים קיברנטיים כדי לתקוף תשתיות קריטיות של מדינות, מוסדות וסמלי שלטון, תשתיות ומערכות עסקיות ותעשייה, וכן יעדים אזרחיים ציבוריים למיניהם. כן נבחן האם מדובר באיום ממשי ומידי, או שמא זהו איום פוטנציאלי רחוק, השב ועולה מעת לעת כחלק מהשיח הכללי בתחום זה.[1]

האיום הקיברנטי מצד קבוצות טרור

חמש קבוצות עיקריות משתמשות כיום, או שיש להן פוטנציאל לשימוש בעתיד, בכלי תקיפה קיברנטיים: (1) מדינות המפתחות יכולות התקפיות והגנתיות כחלק (גדל והולך) מיכולות הפעלת הכוח שלהן; (2) גורמים פליליים המונעים בעיקר מאינטרסים פליליים־עסקיים; (3) חברות עסקיות הפועלות בעיקר בתחום ההגנתי מכיוון שהיקף ההתקפות במרחב הקיברנטי בהקשרים עסקיים גדל והולך במידה ניכרת, אולם חלק מהן עלולות לפנות לאפיק של התקפה על חברות מתחרות; (4) ארגוני טרור, שמשום היתרונות הגלומים בשימוש במרחב זה ומשיקולי עלות־תועלת בעבורם עלולים לנסות ולבצע התקפות טרור קיברנטי; (5) גורמים "אנרכיסטיים", המתנגדים 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.

תחום התקיפה הקיברנטית, שאליו עלולים להיכנס ארגוני הטרור נושא בחובו פוטנציאל לשינוי במאזן הכוחות בחברה, משום העוצמה שהוא מעניק לתוקפים, ובייחוד לארגוני טרור הפועלים בנחיתות ביחסי הכוחות הא־סימטריים בינם לבין יריביהם. בניית יכולת במרחב הזה עשויה לאפשר להם לתקוף מתקנים, תהליכים מערכתיים ואתרים של יריבים ולגרום נזקים פיזיים כבדים וליצור השפעה פסיכולוגית ניכרת בחברה ובציבור המותקפים, וזה תוך כדי יכולת פעולה בממדים נוספים על אלה המוכרים לנו כיום מפעולות הטרור הקונבנציונליות, כגון פיגועי התאבדות, הפעלת מטעני חבלה, התבצרות עם בני ערובה, חטיפות כלי תעבורה ובני אדם. לתקיפה קיברנטית יש כמה יתרונות: ראשית, הימנעות מנוכחות פיזית ביעד המותקף. אפשר לנסות ולפגוע מרחוק ברשתות תקשורת ובמערכות בקרה של מתקנים ותהליכים וכך להימנע מהצורך להתמודד עם מכשולים פיזיים ומערכות אנושיות. שנית, היקף הנזק – תקיפה קיברנטית איננה מתקיימת בחלל פיזי בלבד אלא יש לה פוטנציאל לפגיעה קשה ומתמשכת במערכות בקרה ותשתית. בעוד רוב פיגועי הטרור מתוחמים בזמן ובמקום,[2] הפיגוע הקיברנטי מעצים את היבטי החרדה וההפחדה הכרוכות בהשפעות הפסיכולוגיות של מעשה הטרור. שלישית, טשטוש זהויות ומקור ההתקפה – במרחב הקיברנטי קל יותר לעמעם ולטשטש זהויות וגבולות שבין מדינות. גורמי הטרור יכולים לתקוף קיברנטית תוך כדי טשטוש זהויות וביצוע הטעיות לגבי מקור התקיפה. למשל, לתקוף בתוך

מדינת היעד תוך כדי שימוש בכתובות של מדינה ידידותית. כך יתקשה המותקף לזהות את המקור האמיתי של התקיפה. רביעית, יחס עלות־תועלת מיטבי – השימוש בפלטפורמה קיברנטית לצורכי תקיפות טרור מגלם יחס עלות־תועלת מיטבי מבחינתו של ארגון הטרור, שהוא נחות ברמת המשאבים והיכולות לעומת המדינות שאותן הוא תוקף. בהנחה שארגוני טרור יעדיפו מטרות מוגנות פחות על פני אלה המוגנות היטב, הרי שהם יוכלו לתקוף תוך כדי יצירת נגישות על־ידי החדרת מפגעים שיחדירו קודים זדוניים לאתרי היעד, או תוך שימוש בטכנולוגיה העומדת להיות זמינה למדי לקהלים רחבים. חמישית, טרור אל־הרג – באמצעות תקיפות קיברנטיות יכול ארגון הטרור לגרום נזקים ניכרים בלי פגיעה פיזית והרג ישיר. כך הוא יוכל להשיג הישגים באמצעות הפחדה ושיבוש מרקם החיים בלבד, דבר שיעניק למבצעיו יכולת הגנה והסבר לוגי למעשיהם בלי ששפכו דם אלא רק גרמו לנזק בדמים. חדשנות הפעולה תבטיח אף היא פרסום רב לארגוני הטרור, ואף כניסה לתחום פיגועי מיקוח־אל־הרג, שלאחר הדגמות ידרשו תמורות באיימם בפגיעה קיברנטית.

מושמעת טענה שארגוני טרור אינם מעוניינים במרחב הקיברנטי משום שהם מעדיפים פעולות ראוותניות של שפיכות דמים, בעלות נראות גבוהה בהרבה מהאלמוניות המאפיינת כביכול פעולות חבלה באמצעות המרחב הקיברנטי.[3] ואולם טענה זו אינה מתיישבת עם התפיסה הבסיסית של השימוש באסטרטגיית הטרור, הגורסת שהפעילות הטרוריסטית צריכה להתמקד בניסיון לצמצם את פערי העוצמה במאבק עם יריב שעוצמתו רבה יותר, ביצוע פעולות הרסניות תוך כדי חיפוש נקודות תורפה במערכי ההגנה שלו כדי לחדור מבעדן, והשגת עמדת יתרון במחיר נסבל ההולם את האמצעים הדלים יחסית העומדים לרשות מחוללי הטרור. כבר היום אפשר לראות, שארגוני טרור מהג׳יהאד העולמי עושים שימוש רב, אם כי מוגבל ועדיין לא מפותח יחסית, במרחב הקיברנטי כדי להביא יתרונות אלו לידי מימוש. במחקר שבחן את היכולת ואת השימושים בתחום הקיברנטי של ארגוני ג׳יהאד,[4] נמצאו מאפיינים עיקריים המשמשים לבנייה ולשיפור התשתית הארגונית והמבצעית של ארגוני הטרור בתחומים האלה:

- **תעמולה** – שימוש לצרכי הפצת רעיונות, פסיקות, הנחיות, נאומים ודעות של אנשי דת ומנהיגי טרור;
- **גיוס ואימון** – שימוש לצורכי איתור וגיוס של חברים פוטנציאליים, וכן העברת חומרי הכשרה והדרכה באמצעות הרשת;
- **גיוס כספים ומימון** – שימוש ברשת לגיוס כספים במסווה של ארגוני צדקה וסיוע, ושימוש לגִיבת זהויות וכרטיסי אשראי;
- **תקשורת** – שימוש ברשת כגורם לתקשורת מבצעית תוך שימוש בכלים מגוונים ובהם כלי הצפנה זמינים;

- **איתור מטרות ומודיעין** – שימוש במידע ברשת לשם איתור מטרות ומחקר מודיעיני.

המעבר של ארגוני הטרור משימוש לוגיסטי ותעמולתי לשימוש אופרטיבי באמצעים קיברנטיים עלול לבוא לידי ביטוי בביצוע פיגוע דרמתי וחדשני, זול למדי בעלותו אך עם תהודה רבה ולעתים עם נזק בהיקף גדול ביותר, אפילו אם נעשה בחתימה נמוכה או אפילו בשמירה על אנונימיות של מבצעיו. לכן כל ארגון טרור, ובעיקר אלה השואפים לפרסום וליצירת אפקט פסיכולוגי על ציבור יריביהם, רואה בפיגוע כזה אתגר חשוב ושאיפה ראויה, שכדאי להתאמץ בעבורו. חדשנות גם תבטיח למבצעים פרסום בינלאומי ואת היותם דגם לחיקוי. לפיכך ארגונים תת־מדינתיים שיכולתם הטכנולוגית נמוכה משל מדינות שבהן הם נאבקים, עלולים להצטרף למגמה של ניצול הטכנולוגיה המתקדמת הנדרשת ללוחמה הקיברנטית, בייחוד, אבל לא כתנאי הכרחי, אם יזכו לסיוע של מדינות תומכות או אם יצליחו לרכוש בעצמם יכולת כזאת בעתיד על־ידי גיוס אנשים בעלי הכשרה מתאימה בתחום הזה, שיוכלו להביא לידי ביטוי כישורים יוצאי דופן בתחום.

גם למדינות תומכות טרור יש במרחב הקיברנטי כוח משיכה רב להפעלת ארגוני שליח: האנונימיות הטמונה בשימוש כזה, הקושי להוכיח את זהות המפעיל, יכולת ההכחשה (deniability) הגבוהה של מדינות בנוגע למעורבותן נוחה יותר, והגמול בדמות גרימת הנזק הרב ליריב. יתר על כן, גם אם יעלה כלפיהן חשד, יהיה קשה להוכיח את אשמתן, ובכל מקרה "פיגוע קיברנטי" עשוי להיחשב מקומם פחות את הציבור הנפגע מפיגוע טרור בנשק חם הגורם שפיכות דמים גדולה, אפילו שהנזק בעטיו של הראשון רב ביותר, ואף עלול לעלות בהרבה על הנזק לרכוש ולחיי אדם הנגרמים מפעולת טרור אלימה ומדממת.

למרות היתרונות של תקיפה קיברנטית שתוארו לעיל, עדיין לא נודעה תקיפה שהאחראים לה הם גורמי טרור. בניית יכולת ממשית בתחום התקיפה הקיברנטית מחייבת מעבר של סף מודיעיני וטכנולוגי לא מבוטל. בשלב זה סביר להניח שלארגוני הטרור יש קושי לאתר, לגייס ולתחזק יכולת ונגישות טכנולוגית גבוהה ביותר המאפשרת להגיע לסף הזה. אמנם הישענות על יכולת של מדינות תומכות טרור עשויה לספק מענה ולו חלקי למגבלה זאת, אולם אין בה, לפחות בשלב הנוכחי, כדי לייצר לארגוני הטרור מצע טכנולוגי יציב ומשמעותי הנדרש לקיומה של יכולת תקיפה קיברנטית אפקטיבית. כן ניצבים ארגוני הטרור בפני מגבלות הפעילות במרחב הקיברנטי הגלוי (רשת האינטרנט). זהו חיסרון מובהק ואתגר לא מבוטל לארגוני טרור, שכן יכולת המעקב והמודיעין הקיברנטי של מדינות ומעצמות טכנולוגיות מאפשרת להן לזהות התנהגויות חשודות ברשת, לאתר התארגנויות ולהתגונן מפניהן ומפני איומים ספציפיים.

נקודות תורפה ומענים

אף־על־פי שעד כה לא הצליחו ארגוני הטרור להתגבר על המכשולים להשגת יכולת תקיפה קיברנטית, המערכות האזרחיות והפגיעה במרקם החיים השגרתי נותרו ככל הנראה היעדים המועדפים שלהם. אלו הן נקודות התורפה העיקריות, ויכולת הגנתן פחותה מזו של המערכות הביטחוניות. סביר להניח שחיזוק ההגנה על תשתיות לאומיות חיוניות דוגמת מערכות אספקת חשמל, מים ותקשורת, תוביל את ארגוני הטרור לנסות לפגוע ביעדים מוגנים פחות השייכים למגזר האזרחי והעסקי. אף שבמקרים רבים מערכות ממגזרים אלה אינן נכללות בקבוצת התשתיות הקריטיות המוגנות, הרי מבחינת ארגוני הטרור המתקפה יכולה לספק תוצאה אפקטיבית בעיקר בהיבטי הדימוי והפגיעה בביטחון הבסיסי של התושבים.

חלק נכבד בבניית מערך הגנה כנגד תקיפת סייבר הוא כללי ואינו תלוי במקור האיום, בין שמקורו בארגוני טרור, ובין שמקורו בגורמים מדינתיים או בגורמים פליליים. כך בהיבטים הארגוניים דוגמת הרשות לאבטחת מידע בישראל ומשרדים המתמחים בהגנת סייבר במדינות שונות, וכך בחלק ממרכיבי ההגנות מתחום מערכות המידע והאבטחה הכוללת. לעומת אלה, אל מול ארגוני טרור המבקשים להפעיל כלים קיברנטיים, נדרשים שני רכיבים ייעודיים, המחייבים פיתוח ושכלול מתמשך.

מודיעין – איסוף אקטיבי של מודיעין מדויק ואיכותי מחייב פעילות איסוף ממגוון מקורות ובהם מקורות גלויים, וממוחשבים ומרשתות של ארגוני הטרור. לצורך זה יש לפתח יכולות לשהות במערכות האלה בצורה סמויה ולהזרים מידע בצורה פעילה ומתמשכת. לשם כך יש להתגבר על הפרישה הגלובלית הרחבה המאפיינת את ארגוני הטרור, המשתמשים בחדרי דיונים רבים ברשת, ומעבירים מסרים במילות קוד ייחודיות. גורמי המודיעין נדרשים לבנות יכולת ליירט תשדורות אלה ולפענחן בקבועי זמן רלבנטיים, ובה בעת לספק לגורמי ההגנה הקיברנטית את הכלים להגן מפני הפעולות המתוכננות ואף לשבש אותן.

שיבוש – בשונה מהקמה של מערכות הגנה, שאינן מנסות למנוע את התקיפה אלא למנוע את הצלחתה, מטרת השיבוש היא לסכל את ביצוע התקיפה או לפגוע במהלכיה. הקמת מערך שיבוש אפקטיבי כנגד תקיפות קיברנטיות של ארגוני טרור מחייב ניטור ובקרה מודיעיניים שיוכלו לזהות את ההתארגנות לתקיפה טרם התרחשותה, ולפעול ביעילות לסיכולה. היבט זה נשען בעיקר על יכולת איסוף של מודיעין טקטי הן במחשבים והן ברשתות התקשורת שארגוני הטרור משתמשים בהן.

לעתים, נעשים ניסיונות שיבוש שאינם מופנים לכוונת תקיפה מסוימת, אלא כניסיון לפגוע בתשתיות הארגוניות של ארגון היעד. ניסיון כזה אירע למשל באנגליה כאשר המודיעין הבריטי השחית את גיליונו המקוון של כתב העת האנגלי

Inspire של ארגון אל־קאעדה. בנוסף, בשנים האחרונות הג׳יהאד האלקטרוני על מרכיביו מהווה יעד לתקיפות סייבר מזדמנות, שרובן מיוחסות לממשלות של מדינות מערביות: אתר הטאליבן הושחת חדשות לבקרים, וכן הותקפו פורומים ג׳יהאדיסטיים אקסקלוסיביים ואתרים פונדמנטליסטיים עתירי פרופיל. מנגד רשויות אמריקניות, סעודיות והולנדיות דולות מידע מודיעיני יקר ערך על אודות טרור אסלאמי פוטנציאלי מאתרים ג׳יהאדיסטיים המשמשים ״מלכודות דבש״ (honeytraps) למודיעין איכותי.[5]

בצד אלה חובה להעמיק את הגנת המערכות האזרחיות שהן נקודות התורפה הגדולות ביותר, ולכן הן המטרות המועדפות על ארגוני הטרור. ממשלת בריטניה למשל החלה לנקוט אמצעים חקיקתיים רבים הכוללים אישור שימוש באמצעים פולשניים, כגון ציטוט לשיחות טלפון, מעקבים אחרי תנועות דואר אלקטרוני בתיקים משטרתיים הקשורים לעברות טרור, טרפוד תהליכי רדיקליזציה דרך האינטרנט ואימון ייעודי של יחידות משטרה להתמודד עם איום סייבר.[6] עם זאת, ברוב המדינות ההגנה על המערכות האזרחיות עודנה בחיתוליה. עיקר משאבי המדינות בתחום ההגנה הקיברנטית מוקצים למערכות הביטחוניות ולמה שקרוי תשתיות לאומיות קריטיות. העמקת ההגנה על המערכות האזרחיות מחייבת שידוד מערכות לאומי, החייב להיתמך ברגולציה מתאימה.[7]

סיכום

במפגש שהתקיים בניו יורק בדצמבר 2001, זמן לא רב לאחר מתקפת הטרור בארצות־הברית, שטח הפילוסוף ז׳אק דרידה את תפיסתו על התמורות שחוללו בעולם פיגועי ה־11 בספטמבר 2001. לשיטתו פיגועים אלו הם עדיין חלק מ״תיאטרון האלימות העתיק״, העולם הממשי והנראה, שבו דברים עדיין מתנהלים ב״סדר ברור וגדול״. ואולם לדבריו, המרחב הקיברנטי מציב איום חמור יותר על עולמנו הפוליטי והפיזי – הסכנות הטמונות בו משנות את היחס בין טרור, במובן הפסיכולוגי וההיסטורי של התקפה אלימה, לבין המושג טריטוריה. כעת, בעידן הטכנו־מדעי החדש, האיום שהכרנו בעבר כממשי, נהפך לאיום בלתי נראה, שקט ומהיר ובלא שפיכות דמים, שלדברי דרידה הוא גרוע יותר מפיגועי ה־11 בספטמבר, שכוונו כלפי מקום ידוע בזמן מסוים. כעת אנו ניצבים נוכח אתגר המאיים על מרקם החיים החברתיים־הכלכליים, מרקם שכולנו קשורים ותלויים בו, בכל נקודה ובכל רגע.[8]

ההתפתחויות והחידושים הטכנולוגים המהירים בשנים האחרונות במרחב הקיברנטי אכן יצרו שדה לחימה שבו חוברות ומאוגדות להן בו בזמן אוכלוסיות מגוונות ורבות, מקומיות ובינלאומיות, שהן יעד נחשק לפעילותם של ארגונים תת־מדינתיים. נכון לעת הזאת טרם נודעה תקיפה קיברנטית של גורמי טרור ולכן

האיום אינו נראה מיידי. הגורמים הרוצים לנצל את המרחב הקיברנטי למטרות זדון צריכים לעבור סף גבוה בשלושה רכיבים חיוניים: השגת מודיעין איכותי, נגישות ויכולת לפצח מערכות מחשוב המוגנות בטכנולוגיה גבוהה, וכן כושר חישוב ומחשוב גבוהים. ואולם היתרונות שבהשגת היכולת הקיברנטית, שפורטו במאמר זה, עלולים לשמש להם תמריץ לפתח, לרכוש או לגייס יכולת כזאת בעתיד. השגת שליטה ביכולות הטכנולוגיות והמודיעיניות המתקדמות הנדרשות במרחב הקיברנטי, צפויה להעניק לגורמים כאלה יכולת לשבש את אורח החיים התקין של אוכלוסיות הנחשבות יריבות, לערער את אמונתן בממשליהן ותזכה אותם בעוצמה ובחשיפה תקשורתית שחשיבותן רבה. לפיכך חייבות מדינות המערב להתכונן בהתמדה כדי לקדם את פני הרעה הצפויה הזאת ולשפר את יכולת המודיעין ואת יכולת ההגנה על המערכות האזרחיות. בד בבד עליהן לבנות מודיעין מדויק ויכולת הגנה על המערכות הביטחוניות ועל התשתיות הלאומיות הקריטיות ויכולת לשבש התארגנויות ותקיפות קיברנטיות של ארגוני טרור. הפקרתו של המרחב הקיברנטי האזרחי, שהוא מטרה לארגוני טרור, עלולה להביא בעתיד לידי תוצאות הרות אסון, שבשעת מבחן יציבו את גורמי הביטחון, כמו את גיבור הסרט "מת לחיות 2", בנסותם להציל מטוסים מתרסקים כשבידיהם לפידים בוערים בלבד.

הערות

1 השימוש במינוח טרור קיברנטי במאמר זה הוא בהקשר של השימוש בכלים קיברנטיים העלול לשמש ארגוני טרור לצורך תקיפת תשתיות כלכליות ומערכות אזרחיות במדינות יעד.

2 אפשר להחריג כאן פיגועים דוגמת התקיפה ב־11 בספטמבר 2001 בארצות־הברית, שהשפיעה גלובלית על מערכי הבטיחות בתעופה.

3 שמואל אבן ודוד סימן־טוב, **לוחמה במרחב הקיברנטי: מושגים, מגמות ומשמעויות לישראל**, המכון למחקרי ביטחון לאומי, מזכר 109, יוני 2011, עמ' 42.

4 *Examining the Cyber Capabilities of Islamic Terrorist Groups*, Institute for Security Technology Studies at Dartmouth College, Technical Analysis Group, March 2004.

5 Adam Rawnsley, "Stop the presses! Spooks hacked al-Qaida online mag," *Wired*, June 3, 2011, http://www.wired.com/dangerroom/2011/06/stop-the-presses-spooks-hacked-al-qaida-online-mag/June 4, 2011.

6 "Warning of rise in cyber-terrorism," *The Independent*, July 12, 2011, http://www.independent.co.uk/news/uk/crime/warning-of-rise-in-cyberterrorism-2312434.html, (July 14, 2011).

7 גבי סיבוני, "הגנת נכסים ותשתיות קריטיות מפני תקיפה קיברנטית – הממד הסטטוטורי", **צבא ואסטרטגיה**, כרך 3, גיליון 1, מאי 2011.

8 ז'אק דרידה, מתוך ג'יובנה בוראדורי, **פילוסופיה בזמן טרור – שיחות עם הברמאס ודרידה**, תל־אביב, הקיבוץ המאוחד, 2004, עמ' 173–174.

הגנה על תשתיות קריטיות מפני איום קיברנטי

ליאור טבנסקי

מבוא

תפקוד החברה המודרנית מבוסס על מארג סבוך של תשתיות שונות: אנרגיה, תקשורת, תחבורה, מזון ועוד. מאמר זה עוסק באיום הקיברנטי המתפתח על תשתיות מידע חיוניות (Critical Information Infrastructure). המאמר נועד לתרום לדיון ציבורי מושכל באיום הקיברנטי על תשתיות חיוניות, תוך התמקדות בסוגיות המיוחדות לו הדורשות התייחסות בין־תחומית, בגישות להתגוננות מפניו, במענה הישראלי הקיים ובאתגרים המתפתחים. פיתוח הדיון הציבורי עשוי להוביל לשיפור ההגנה על תשתיות לאומיות במגזר האזרחי והציבורי.[1]

המאמר נפתח בהמשגת נושא התשתיות החיוניות ודן במקורותיו, ייחודו וחדשנותו של האיום. בהמשך נדונים רבדים של ההתמודדות עם האיום, בהקבלה מושגית לעולם התוכן הצבאי. המענה הישראלי הקיים נסקר בקצרה, ובעקבותיו מודגשים האתגרים המרכזיים של האיום הקיברנטי למדיניות הציבורית. לבסוף מוצגים כיווני מחקר ופעולה עתידיים.

"תשתית מידע חיונית": ביאור והמשגה

תשתית (Infrastructure) היא מערכת המשלבת מתקנים שונים ומאפשרת לבצע פעולות שונות. היא כוללת, בין השאר, צנרת הולכת מים מבארות לבתים ולשדות, כבישים סלולים, גשרים וצמתים המאפשרים תנועה של אנשים וסחורות, תעופה, תקשורת, דלק, בריאות ועוד. בעידן המידע, התשתיות המסורתיות הופכות לתשתיות מידע עקב שיבוץ המחשבים בהן. בנוסף לכך, נוצרו תשתיות חיוניות חדשות, שהן על טהרת המידע: מאגרי מידע ממוחשבים המכילים נתונים חשובים כגון רישומי ההון במערכת הבנקאית, קניין רוחני מדעי וטכני ועצם הלוגיקה המתוכנתת שמנהלת תהליכי ייצור ותהליכים עסקיים שונים. בעידן המידע, המושג

ליאור טבנסקי הוא חוקר בתכנית לוחמת סייבר במכון למחקרי ביטחון לאומי.

מאמר זה ראה אור לראשונה ב**צבא ואסטרטגיה**, כרך 3, גיליון 2, נובמבר 2011, עמ' 63-77.

"תשתית" כולל גם מרכיבים ממוחשבים. כשאומרים היום תשתית מתכוונים בהכרח לתשתית מידע (Information Infrastructure).

אחד המאפיינים של תשתית הוא התלות של תחומי עיסוק שונים בה. בעבר, התלות נבעה מקשרי גומלין פיזיים או גיאוגרפיים בלבד. עם התפתחות המרחב הקיברנטי, הכולל מערכות תקשורת מידע ואמצעים ממוחשבים לשליטה ובקרה אוטומטית, נוצרו קשרי גומלין נוספים היוצרים פגיעות נוספת. מדובר בקשרי גומלין ממוחשבים (למשל, שליטה ובקרה באמצעים אלקטרוניים ומרחוק) ולוגיים (למשל, השוק הפיננסי הבינלאומי כגורם המשפיע על תשומות ותפוקות של התשתיות החיוניות), המהווים חידושים שלא היו מתקיימים ללא טכנולוגיות המידע. לכן, כדאי להבחין בין תשתית במובן המילוני המסורתי ובין השימוש המודרני במושג זה, המכיל ממד קיברנטי.

תשתית מוגדרת חיונית כאשר סבורים ששיבוש תפקודה יוביל למשבר כלכלי־חברתי משמעותי, בעל פוטנציאל לערעור היציבות בחברה ועם השלכות פוליטיות, אסטרטגיות וביטחוניות. מדינות שונות מציגות הגדרות שונות למונח "תשתית חיונית",[2] אך המשותף לכולן הוא שמדובר בתשתית בעלת ממד ממוחשב, בה תלויות מערכות פיזיות נוספות, שפגיעה בתפקודה עלולה לגרום לנזק רחב בממד הפיזי.[3]

אפשר לזהות שלושה מקורות להגדרת תשתית כקריטית: הראשון – המשקל הסמלי של התשתית. כך, למשל, שיבוש עוין של אמצעי התקשורת המסורתיים המשמשים את המדינה להעברת מסרים לאזרחים יפגע באופן מיידי ביכולת התפקוד של השלטון. יתרה מזאת, בטווח הארוך יפגע שיבוש כזה קשות באמון האזרחים בממשלה או אף במשטר הקיים. מדינות דמוקרטיות אחדות כוללות את אתרי המורשת, המוזיאונים, הארכיונים והאנדרטאות שלהן בתשתית החיונית הראויה להגנה גם מפני איום קיברנטי.[4]

השני – התלות המיידית בתשתית, כגון רשת החשמל או רשת המחשבים, בהן תלויים רוב התהליכים בחברה. חדירת המחשוב וקישורו ברשתות ממוחשבות יצרו מצב שבו המערכות הממוחשבות מהוות תשתית בפני עצמה. המרחב הקיברנטי עצמו הוא דוגמה מייצגת לתשתית שהפכה לקריטית בגלל הממשק של רוב הפעילות בחברה עם רשתות התקשורת הממוחשבות.

השלישי – קשרי גומלין מורכבים: המגמה המואצת של הוספת יכולות קישוריות יוצרת השפעות לא צפויות מעבר לרמה המקומית ("אפקט הפרפר").[5] יש להניח שקשרי הגומלין בין התשתיות השונות אינם מוכרים במלואם, וכֶשל של רכיב אחד עלול לגרום למגוון רחב של תוצאות ונזקים. אפשר לחלק את סוגי הכשל לשלושה טיפוסים:

1. כשל הנגרם מִסיבה משותפת (Common Cause Failure). למשל, מתקנים שונים (מאגר דלק, שדה תעופה ותחנת כוח) הממוקמים בסמיכות גיאוגרפית עשויים להיפגע ממקרה בודד של הצפה. קשה לראות מתקפה קיברנטית שתגרום במישרין לכשל מסוג זה.
2. כשל מידרדר (Cascading): שיבוש מערכת בקרה בתשתית אחת (מים) גורם לשיבוש בתשתית שנייה (תחבורה: למשל הצפת קו רכבת), גם אם זו אינה תלויה בה במישרין. מתקפה קיברנטית יכולה לגרום במישרין לכשל מסוג זה.
3. כשל מסלים (Escalating): שיבוש תשתית אחת (למשל, רשת תקשורת) פוגע במאמץ לתקן תפקוד של תשתיות אחרות שנפגעו מגורם אחר (שירותי חירום, מסחר, שליטה מרחוק).[6] מתקפה קיברנטית יכולה לגרום במישרין לכשל מסוג זה.

להדגמת חשיבותן של תשתיות קריטיות והמשמעות של פגיעה בהן ניתן להשתמש במגזר התעופה המסחרית. מגזר זה משך את תשומת לבם של אויבי המדינות המפותחות והביא אותם לנקוט שורה של צעדים נגדו: חטיפת טיסות מסחריות, פיגועי ספטמבר 2001 בארצות הברית וניסיונות טרור נוספים באמצעות מטוסי נוסעים.

התעופה האזרחית מהווה תשתית שעל בסיסה מתקיימות פעילויות מגוונות בחברות המפותחות. התחבורה האווירית המסחרית הובילה ב־2009 יותר משני מיליארד נוסעים ב־28 מיליון טיסות של 27 אלף מטוסים הפועלים מ־3,670 שדות תעופה מסחריים בעולם.[7] בנוסף לטיסות המסחריות מאכלסים את המרחב האווירי כלי טיס צבאיים (חלקם בלתי מאוישים) ופרטיים. חוקים, תקנות ונהלים פנים־מדינתיים, לצד שיתוף פעולה בין־לאומי, מסדירים את ההיבט האדמיניסטרטיבי של ענף התעופה.

שדות התעופה קשורים זה לזה בתנועת המטוסים המתוכננת, ומערכת בקרת התנועה האווירית בכל אתר נתון היא חלק מתשתית התעופה הבין־לאומית. הבקרה האווירית מבוססת על מערכות ממוחשבות: אמצעי גילוי, ניטור, מעקב, אוטומציה, תקשורת, שליטה ובקרה ועוד. שיבוש התפקוד התקין של מערכת הבקרה האווירית יפגע בתנועה האווירית כולה.

חדשנות האיום

בשנים האחרונות אנו עדים להתגברות הדאגה מפני הפגיעות האפשרית של התשתיות המונחות ביסוד החברה המודרנית המפותחת.[8] עצם התעוררות הדיון הזה כעת אמורה להפתיע. תשתיות חיוניות היו חיוניות תמיד וחשיבותן גלויה לכול. סכסוכים בין־לאומיים ופנימיים שונים קיימים ומתפתחים ברחבי

העולם, ובמלחמה סביר לצַפות לניסיונות לפגוע בתשתית החיונית של היריב, במטרה להחליש ולהכניע אותו. לנין וטרוצקי הורו לפעיליהם במהלך המהפכה הבולשביקית ב־1917 להשתלט על הדואר, הטלפון, הטלגרף, גשרים ותחנות רכבת. במלחמות ממושכות, כמו במלחמת העולם השנייה, נעשו ניסיונות לפגוע בתשתית חיונית כדי לשבש את כושר הלחימה ואת רוח האויב.[9] תשתיות חיוניות של מדינה, יהיו אשר יהיו, הן יעד טריוויאלי במהלך סכסוך. לכן, ארגונים ומדינות עמלו לאורך כל ההיסטוריה על מערכי הגנה: הסוואה, שמירה, ביצור, כוח מגן, הרתעה וכיוצא באלה. מדוע, אפוא, גבר דווקא לאחרונה החשש מפני פגיעה בתשתיות חיוניות, ועוד במדינות החזקות ביותר?[10]

אין עוררין על העובדה כי המדינות המפותחות נהנות מעליונות צבאית מוחלטת על פני אויביהן השונים. מדינות אלו לא חוו מלחמות בשטחן בעשרות השנים האחרונות. ישראל היא המדינה המפותחת היחידה הנמצאת תחת איום צבאי מתמשך המתממש בצורות שונות (מתקפות טילים ב־1991, רקטות בצפון המדינה ובדרומה,[11] ומחבלים מתאבדים בשנים 2000–2005). כמה מהמדינות המפותחות נפגעו ממעשי איבה שפגעו ישירות באזרחיהן, תוך עקיפת עוצמתן הצבאית שהייתה אמורה להגן עליהם. מתקפות הטרור לא יכלו לאיים על המדינות המותקפות, אולם הן הצליחו לגרום לשינוי מדיניותן בצורה זו או אחרת.

תשתית חיונית היא מטרה מפתה לאויב, יהיה זה ארגון טרור או מדינה עוינת. בכל צורות המלחמה המסורתיות, זהות האויב מתגלה בוודאות לאחר התקיפה, כי זו חייבת להתבצע באמצעות הגעה פיזית של חימוש אל המטרה. גם במקרה של שיגור טילים לא קיים ספק באשר למיקום אתר השיגור. חטיפות טיסות מסחריות בשנות השבעים של המאה הקודמת, פיגועי המתאבדים בריכוזי אזרחים בישראל, הפיגועים בארצות הברית בספטמבר 2001 והפיגועים במדריד ב־2004 ובלונדון ב־2005 גם הם דרשו נוכחות פיזית של המפגעים במקום התקיפה.

זיהוי האויב חיוני לצעדי תגובה ולהרתעה. ניתן לומר שמה שמנע פגיעה בתשתיות החיוניות בעבר היה כוח המגן שניצב בדרכי האויב, ובמיוחד ההרתעה שהבטיחה לגבות ממנו מחיר כבד. מצב עניינים מוכר זה הגיע לקצו עם התפתחות המרחב הקיברנטי. לראשונה בהיסטוריה ניתן לתקוף מטרות איכות (כמו תשתית חיונית) מבלי להגיע פיזית אל המקום בו הן נמצאות, מבלי להתמודד עם כוחות המגן ומבלי להיחשף. במצב הנוכחי ניתן להשתמש לרעה בתשתית הממוחשבת הקיימת כדי לשבש או להשבית מערכת חשובה, וזאת באמצעות חדירה אל רשת התקשורת, אל התוכנה או החומרה של מחשבי הפיקוד והבקרה.[12] האיום נובע מהפגיעות שמקורה במאפייני המרחב הקיברנטי הקיים.[13] המאפיינים המיוחדים של המרחב הקיברנטי גורמים לכך שהאתגר שבאיום הקיברנטי שונה באופן מהותי מהאתגרים שבאיומים המסורתיים.

רבדים בהתמודדות

כאמור, מאמר זה עוסק רק באיום הקיברנטי על הממד הממוחשב של התשתיות, לאור ההבנה שאיום כזה הפך לאפשרי, זמין ומשמעותי ועלול לשבש את תפקוד החברה המפותחת.

ההתמודדות עם האיום על תשתיות מידע חיוניות כוללת מניעה, התרעה, זיהוי וגילוי ההתקפה, תגובה, ניהול המשבר, בקרת נזקים וחזרה לתפקוד מלא. כאשר בוחנים התמודדות עם איומים על הביטחון הלאומי, מקובל לחלק את הדיון לרמות הטקטית, המבצעית והאסטרטגית. מאמר זה מציע לדון בהתמודדות עם האיום על תשתיות מידע חיוניות בחלוקה לכמה רבדים: טכנולוגי; טכני־מבצעי; אופרטיבי; אסטרטגי־לאומי.

הרובד הטכני מתמקד במערכת ממוחשבת ארגונית, שהיא הפעילות הנפוצה ביותר בתחום. לאור נפח הפעילות הגדול, משתמשים לעתים קרובות בהיבט הטכני של "אבטחת מידע", בעוד שמדובר במושג שמתייחס הן להגנה על תשתיות חיוניות והן לביטחון הקיברנטי בכלל. בנוסף לכך, מתפתחת פעילות הבוחנת את הסוגיה במבט לאומי כולל. זו תיקרא להלן "הרובד הלאומי" של הביטחון הקיברנטי.

כל הרבדים נדרשים להתמודד עם האיום, אולם לאור המיקוד השונה כדאי להבחין בין שכבות ההגנה הללו. החלוקה המוצעת תסייע להבחין במהות אתגרי ההגנה על תשתיות חיוניות כמקרה פרטי של הביטחון הקיברנטי.

הרבדים הטכניים – הרמות הטקטית והמבצעית

מכיוון שהאיום נגזר ממאפייני טכנולוגיות המחשבים, בדרך כלל מחפשים את המענה לו בקרב אנשי המחשבים. כצפוי, הפתרונות המוצעים מבוססים גם הם על טכנולוגיות המחשבים. הבעיה נתפסת כסוגיה טכנית, ולכן הפתרון המוצע הוא הנדסי. השכבות הטכנית והמבצעית בהתמודדות עם האיום הקיברנטי, שמקורן במקצועות ההנדסה, המתמטיקה והמחשבים, מתמקדות בזיהוי פגיעויות במערכת ממוחשבת ארגונית ומחפשות מענה הנדסי שיצמצם פגיעות זאת. טבלה 1 מרכזת סוגיות נפוצות שעמן מתמודדים הרבדים הטכניים של ההגנה.[14]

האמצעי העיקרי במאמץ לבנות עמידות[15] הוא השקעה בגיבוי, ביתירות, בהפרדה וכדומה. כידוע, מערכות ממוחשבות חשובות נבנות פעמיים, באתרים נפרדים, כדי לזכות ביכולת להמשיך לתפקד במקרה של פגיעה פיזית במערכת.

אספקת המענה לבעיות ההנדסיות שזוהו מתבצעת כיום לרוב באמצעות השוק הפרטי. תעשיית אבטחת המידע היא תחום עסקי ענֵף שתיאורו חורג מגבולות מאמר זה. בחלוקה המוצעת כאן, אבטחת מידע נמצאת ברבדים הטכניים־מבצעיים. אבטחת מידע היא דיסציפלינה מתפתחת המרכזת משאבים רבים למחקר ופיתוח, שירותי יעוץ ומיקור חוץ, תעשיית מוצרי אבטחה וכיוצא

טבלה 1: מרכיבים ומאפיינים פגיעים במערכות וברשתות מחשב

תיאור המרכיב	סיווג טכני
סיסמאות גישה להתקנים ומערכות נשארו בהגדרות ברירת המחדל.	ניהול סיסמאות
סיסמאות נשמרות ומועברות ללא הצפנה.	
סיסמאות גישה לא מוחלפות.	
אבטחה פיזית לוקה בחסר.	אבטחת גישה פיזית
קיימת אפשרות גישה לציוד קריטי לאנשים שאינם עוסקים בציוד זה.	
ניהול הרשאות משתמשים לקוי מאפשר לעובד זוטר גישה לתהליך קריטי.	אבטחת גישה מחשובית
"חומת אש" מוגדרת כך שמאפשרת סוגי תקשורת מיותרים.	
הרשת התהליכית אינה מופרדת מהרשת המשרדית.	
האפשרות לגישה מרחוק למערכת המחשוב הושארה פתוחה.	
קיימת אפשרות גישה למערכת המחשוב ברשת אלחוטית.	
תהליך הגישה מרחוק משתמש בפרוטוקול פתוח ובסיסמאות חלשות.	
יצרן המערכת סיפק עדכוני אבטחה אולם אלה לא הותקנו במערכת.	ניהול תצורה
הרשאות מַנהלן הוענקו למשתמשי המערכת.	
גישה לרכיבי המערכת החיונית לא מנוטרת; לא נאסף מידע יומן (Log).	
מידע יומן לא נבדק באופן שוטף.	

באלה. שוק אבטחת המידע העולמי צפוי לגדול ל־125 מיליארד דולר ב־2015, ורוב ההכנסות ממנו יגיעו אל חברות אמריקאיות ואירופיות המציעות חבילות משולבות של שירותים ומוצרים טכניים יחד עם יעוץ עסקי־טכנולוגי.[16]

סוגיית הביטחון הקיברנטי, ובמיוחד ההגנה על תשתיות חיוניות, נוצרה עקב השינוי הטכנולוגי. תחילה היה צפוי פתרון טכני לבעיה שמקורה טכני. אולם נראה שמתפתחת הבנה שההתמודדות לא יכולה להסתכם ברובד הטכני־מבצעי לבדו, שכֵּן לא תיתכן נוסחה הנדסית מדויקת להתמודד עם האיום הקיברנטי: מבנה החברה, ערכיה ומוסדותיה הם חלק בלתי נפרד מהסביבה.

הרובד הלאומי – הרמה האסטרטגית

הרובד הלאומי העליון בוחן את האיום על תשתיות חיוניות במסגרת תפיסת הביטחון הלאומי, במיקוד לאומי החורג מגבולות של ארגון או של תהליך עסקי. זוהי גישה הרואה בהגנה על תשתיות מידע חיוניות חלק ממשימת ההגנה על החברה בכללותה. ההגנה על תשתיות המידע הופכת למעשה להגנה על חברה מבוססת־ידע.[17]

אבטחת המידע, העומדת במרכז הרובד הטכני, היא חלק הכרחי אך בלתי מספיק בראייה האסטרטגית. אפשר לומר שהרובד הלאומי העליון מבוסס על הרבדים הטכניים והמבצעיים הבסיסיים, אולם הגישה הרחבה לא מסתפקת בתיקון הבעיות המקומיות של המערכות הארגוניות. בהקבלה לתחום הצבאי, הרובד האסטרטגי זקוק לרמה מבצעית נאותה, אך זו אינה מספיקה להשגת המטרה האסטרטגית.

בראייה לאומית רחבה, נדרשת מדיניות לאומית כוללת בתחום ההגנה על תשתיות חיוניות, שבנוסף על היסודות ההנדסיים תביא בחשבון היבטים חברתיים, פוליטיים, כלכליים וארגוניים מורכבים. כן נדרש גורם ארגוני שמסוגל להביא בחשבון את מכלול קשרי הגומלין המורכבים בין התשתית החיונית ובין תפקוד תקין של החברה והמדינה. זהו ללא ספק אתגר מורכב למדיניות ציבורית, בהתחשב במגבלות המבניות של השירות הציבורי מצד אחד ובחוסר המיקוד האסטרטגי של גורמי השוק הפרטי מצד שני.

הרובד הלאומי של ההגנה זקוק לפעולות חוצות ארגונים, בגיבוי של סמכות אפקטיבית. כפי שהמדינה מגינה על כלל המרחב הפיזי שלה, כך היא רואה צורך מְתגבר להגן על כלל המרחב הקיברנטי שלה, על אף מאפייניו המיוחדים המקשים על המשימה. התפתחות האיומים הקיברנטיים הפכה את הממשלות ללקוחות העיקריים של שירותי ההגנה.

סוגיות לקובעי המדיניות

מהפכת המידע ממשיכה לשנות את הסביבה האסטרטגית ומשפיעה בדרכים מורכבות על מגוון סוגיות חברתיות, תרבותיות וכלכליות. סוגיית הביטחון הקיברנטי, ובפרט ההגנה על התשתיות החיוניות, נמצאת כבר על סדר היום הציבורי והממשלתי. הניסיון הקצר מראה שעל אף הדמיון הרב במקור האיום, קיימים הבדלים במסגרת הדיון ובסוגי הפתרונות המוצעים במדינות שונות. מכיוון שהאיום הוא דומה, ההסבר לשונות הוא תפקיד המוסדות החברתיים בדיון ובקביעת המענה.

איזו תשתית היא חיונית?[18]

הדיון בתחום ההתגוננות צריך להתחיל מקביעת סדרי עדיפויות. הערכה ומדידה של רמת הסיכון ברכיבים, מחשבים ומערכות היא תנאי הכרחי להתמודדות יעילה. במדעים המדויקים ובהנדסה קיימות שיטות מתמטיות למדידת יחסי הגומלין והתלות בין רכיבים למערכות. הכלים הללו נמצאים בשימוש גם ברבדים הטכניים של ההגנה על תשתיות חיוניות. עם זאת, דרושות שיטות משופרות להערכת סיכונים הנובעים מקשרי גומלין מסועפים בין מערכות טכנולוגיות מורכבות המשובצות בתשתיות החיוניות.

הערכת מידת החיוניות הלאומית של תשתית חייבת להתייחס למכלול הערכים, היעדים והכוחות החברתיים. לפיכך, מידת החשיבות היחסית של תשתית, וכתוצאה מכך מידת ההשקעה הציבורית הנדרשת להגנתה, אינן נגזרות מנוסחה הנדסית ודורשות דיון ציבורי רחב ומושכל. המוסדות הפוליטיים הייצוגיים הם האכסניה לדיון כזה בחברה דמוקרטית. לאור אילוצי המערכת הפוליטית, סביר להניח שדיון מסוג זה יהיה ארוך ולעתים מתסכל. עם זאת, רק בתהליך פוליטי משתף ניתן יהיה לעצב מענה מיטבי לאיום בטווח הארוך.

פגיעות קיברנטית: סוגיה טכנית, סיכון כלכלי או איום ביטחוני?

אילו משמעויות פוטנציאליות יש לצמיחת המרחב הקיברנטי בכלל ולפגיעה בתשתיות קיברנטיות חיוניות בפרט? הנושא חורג בבירור מתחומי העיסוק של מחשבים, הנדסה ואבטחת מידע אל עבר השאלה: מהו תפקיד המדינה בהגנה הקיברנטית על תשתיות חיוניות? האם זו משימה צבאית, אזרחית למחצה, "הגנת המולדת" או משימה אזרחית־מסחרית? התשובה משפיעה במישרין על הפתרון המוצע ויש לה השלכות פוליטיות, תקציביות וארגוניות רחבות. עד לא מכבר ההנחה הייתה שמדובר בסוגיה טכנית בעיקרה, והמענה הופקד לפיכך בידי אנשי המחשבים. חברות מסחריות סיפקו פתרונות טכניים למגזר הצבאי, המסחרי והאזרחי, והממשלות לא שיחקו תפקיד משמעותי. כיום ברור שתשובה מיטבית יכולה להתקבל רק בדיון משותף בין מגזרים וגורמים שונים בחברה, מכיוון שהיא נגזרת מערכי החברה, מהמבנה הפוליטי והחברתי ומתפיסת הביטחון הלאומי.

מציאת האיזון בין ערכי החופש, אידיאולוגיית השוק ודרישות הביטחון

התשתיות החיוניות, והמידע הנחוץ לתפקודן התקין נוגעים בכל תחומי החיים של האזרח. הם מעוררים סוגיות רבות הנוגעות לזכויות האזרח, כגון פרטיות, חיסיון והליך הוגן; לעוצמה יחסית של מדינה, אזרחים ותאגידים; ולהקצאת כספי ציבור. לכן, האתגר המרכזי שבעיצוב מדיניות ההגנה על תשתיות חיוניות מפני איום קיברנטי אינו טכני או מבצעי, אלא אתגר של ראייה לאומית־אסטרטגית

כוללת. הגנה על תשתיות חיוניות אינה נחלתם הבלעדית של מהנדסי המערכות ואנשי המחשוב; המענה המיטבי לאיום קיברנטי בכלל ולאיום על התשתיות החיוניות בפרט ייווצר רק באמצעות דיון ציבורי רחב במסגרת המערכת הפוליטית הדמוקרטית.

השוק הפרטי וביטחון קיברנטי

האופי המבוזר של הפעילות הכלכלית בעידן של שינוי טכנולוגי מהיר, הגלובליזציה וההפרטה משפיעים על האיום הקיברנטי. כלכלת השוק הגלובלית הביאה לכך שחלקים נרחבים מהתשתית החיונית נמצאים בבעלות פרטית.[19] התלות ההדדית חסרת התקדים בסחר בין־לאומי היא אחד הביטויים הבולטים של הגלובליזציה וההפרטה. המדינות המתועשות מייבאות את רוב המזון הגולמי שאזרחיהן צורכים ומייצאות מוצרים מוגמרים ושירותים. קמעונאי המזון אינם מחזיקים מלאים מעבר לכמה ימי צריכה טיפוסית ומסתמכים על המשך התפקוד הבלתי מופרע של המערכת הלוגיסטית המסועפת המסוגלת לספק מענה לביקושים בזמן קצר.[20] לאור החומרה של שיבושים באספקת מזון, יתכן ששרשרת האספקה הזו תהפוך ל"תשתית מידע חיונית".

חברות פתוחות (Open Societies),[21] בעלות כלכלה חופשית, נרתעות ממעורבות המדינה בתהליכים עסקיים. כל ניסיון למעורבות המדינה בתהליכי השוק נתקל בחשדנות בעולם השוק החופשי. כך, למשל, הטענות הנשמעות נגד רגולציה ממשלתית של האינטרנט מקורן באידיאולוגיה המלווה שוק זה. הפתרון שאומץ עד כה היה רגולציה ממוקדת: מאז אמצע שנות התשעים של המאה העשרים פותחו ואומצו בארצות הברית עשרות תקנים מפורטים לאבטחת מידע במגזרים ותעשיות שונות[22] ונוסדו ארגונים לפיקוח ובקרה. אולם, במשבר הפיננסי העולמי של 2008 הדגימה המערכת הפיננסית המסחרית את סכנות הבעלות הפרטית על תשתית חיונית הכפופה לרגולציה.

הדיון בנושא ההגנה על תשתיות חיוניות בארצות הברית עובר בשנה האחרונה מְדגש על מנגנוני השוק ו"שיתוף פעולה פרטי־ציבורי" וולונטרי לעבר מודל המקנה סמכויות נרחבות לממשל להנחות גופים עסקיים ולפקח על ביצוע הנחיותיו.[23] גם בישראל קיימת רגולציה של התשתיות החיוניות, ואף עלתה הצעה להרחיבה גם לעסקים קטנים.[24]

שוק מוצרי המחשב והביטחון הקיברנטי

השימוש במערכות האבטחה צריך להיות קל לכל משתמש, לצרוך משאבי מחשב מעטים ולא לפגום בתפקוד מערכת הליבה או בחוויית המשתמש. המצב בשוק בתחום זה אינו מעודד: ההשקעה בביטחון משנית לעומת היציאה המהירה לשוק;

ההשקעה הנדרשת לבדיקות העמידות והאמינות קשה שבעתיים בסביבה פרטית־מסחרית, המודדת הישגים בקיצור זמן ההחזר של השקעה ראשונית ובצמצום הוצאות שלא קשורות לפעילות הליבה, ומוגנת במנגנוני האחריות המוגבלת. ליצרני מערכות המחשב אין כיום תמריץ להשקיע בהגברת האמינות והביטחון. אבטחה נתפסת כפונקציה חיצונית הנוספת על מערכות הליבה, לעתים באמצעות יצרן אחר שלא זוכה לשיתוף פעולה מהיצרן המקורי. ניתן לסכם ולקבוע כי רמת האמינות ואבטחת המידע ברוב מוצרי התוכנה, החומרה ותקשורת מערכות המחשוב לוקה היום בחסר, וכי אין ספק שפגיעות רחבה זו תרמה לעליית האיום הקיברנטי.

לאור נסיבות חוקיות, כלכליות ותחרותיות, קשה לצפות לשיתוף פעולה וולונטרי בין פירמות פרטיות בתחומים אלה. יחד עם זאת, אין לשאוף או לצפות להלאמה כתנאי להגברת הביטחון הקיברנטי. מה שדרוש הוא הגברת מעורבות המדינה בהכוונת השוק החופשי לאור האיומים הקיברנטיים.

המענה הישראלי

אבטחת מידע רגיש והגנה על תשתיות ממוחשבות אינן מהוות נושאים חדשים במדינת ישראל. מאז 1996 קיבלה הממשלה החלטות הנוגעות להתגוננות מפני איומים קיברנטיים.[25] מתווה ההגנה על תשתיות ממוחשבות עוצב בהחלטה ב/84: "אחריות להגנה על מערכות ממוחשבות במדינת ישראל" של ועדת השרים לענייני ביטחון לאומי, מ־11 בפברואר 2002. זאת ההחלטה שעל בסיסה מופעל עד היום המענה הישראלי לאיום הקיברנטי על תשתיות מידע חיוניות. המענה שנקבע בהחלטה כולל הקמת ועדת היגוי עליונה הבוחנת מעת לעת את זהות הגופים שחיוני להגן עליהם והקמת היחידה הממלכתית להגנה על המערכות הממוחשבות (הרשות לאבטחת מידע). גוף אחרון זה נמצא במסגרת השב"כ ומנחה את הגופים שהוגדרו כחיוניים בנושא ביטחון המחשוב, מפקח על ביצוע ההנחיות ומוסמך לנקוט סנקציות נגד המפרים אותן. הגופים המונחים נושאים בעלויות ההגנה הנדרשת. גופים חשובים נוספים הנמצאים תחת אחריות משרד ממשלתי פועלים בהתאם להנחיות המקצועיות של הרשות אך אינם מפוקחים על ידה. גופי הביטחון השונים פועלים להגנה על תשתיותיהם הייחודיות באופן עצמאי, ללא הנחיה פורמאלית של הרשות לאבטחת מידע.

בהשוואה למצב בזירה הבין־לאומית, נראה שישראל הייתה בזמן קבלת ההחלטה מתקדמת יחסית למדינות אחרות בעיצוב ובביצוע ההגנה על התשתיות החיוניות ברמה הלאומית. אולם המרחב הקיברנטי המשיך להתפתח מאז בקצב מהיר ונוצרו מערכות וקשרי גומלין חדשים, שלא בהכרח ניתנים להגדרה כתשתית לאומית חיונית. כך, למשל, עסקים קטנים ובינוניים תלויים בספקי תקשורת

מסחריים ומבצעים את פעילויות הליבה על גבי האינטרנט הפתוח. התפתחות זו של חדירת יישומים מסחריים וצרכניים על בסיס "מחשוב ענן" מעלה סוגיות חדשות ומצביעה פעם נוספת על חשיבותו הגוברת של המרחב הקיברנטי בכל תחומי החיים.

המענה הישראלי לצורך בהספקת הגנה לתשתיות מרכזיות חיוניות נוסד לפני קרוב לעשור, אולם אינו מסַפק ראייה כוללת של התחום האזרחי־מסחרי המתפתח במרחב הקיברנטי. לפיכך, כדאי לבחון מחדש את האתגרים הקיימים והצפויים, ובעקבותיהם את המענה הרצוי.[26]

בעקבות "המיזם הקיברנטי הלאומי" החליטה ממשלת ישראל באוגוסט 2011:

> לפעול לקידום היכולת הלאומית במרחב הקיברנטי ולשיפור ההתמודדות עם האתגרים הנוכחיים והעתידיים במרחב הקיברנטי: לשפר את ההגנה על תשתיות לאומיות שהן חיוניות לקיומם של חיים תקינים במדינת ישראל ולחסנן ככל הניתן מפני התקפה קיברנטית, תוך קידום מעמדה של ישראל כמרכז לפיתוח טכנולוגיות מידע, וזאת תוך עידוד שיתוף הפעולה בין האקדמיה, התעשייה והמגזר הפרטי, משרדי הממשלה והגופים המיוחדים... לאור זאת, בהמשך להחלטת ועדת שרים לענייני ביטחון לאומי ב/84 מיום 11 בדצמבר 2002, ומבלי לפגוע בסמכות שניתנה לגורם אחר על פי כל דין והחלטות ממשלה [מוחלט]:
>
> 1. להקים מטה קיברנטי לאומי (להלן המטה) במשרד ראש הממשלה.
> 2. להסדיר את האחריות לטיפול בתחום הקיברנטי.
> 3. לקדם את יכולת ההגנה על המרחב הקיברנטי בישראל ולקדם מחקר ופיתוח בתחום הקיברנטי וחישוב העל.[27]

החלטת הממשלה עשויה להוביל להסדרה משופרת של המענה הישראלי לאיום הקיברנטי בכלל ולאיום על התשתיות החיוניות בפרט.

סיכום

הממד הקיברנטי ניצב במוקד הדיון המחודש בהגנה על תשתיות לאומיות חיוניות. מאפייני המרחב הקיברנטי מאפשרים לפגוע בתפקוד התשתית החיונית מבלי להיות פיזית בקרבת המטרה ומבלי להסתכן בגילוי חד־משמעי בידי הצד המותקף. מכיוון שכל התשתיות הושפעו ממהפכת המידע וכולן כוללות כיום מרכיבים ממוחשבים המשמשים בעיקר לשליטה ובקרה, השינוי הטכנולוגי המהיר יצר גם איום ביטחוני חדש. זה עורר דיון מחודש על התשתיות החיוניות והגנתן, דיון המוקדש כולו לאיום הקיברנטי. האיום הקיברנטי על תשתיות מידע חיוניות הוא אולי הביטוי המסוכן ביותר של תחום הביטחון הקיברנטי. איום חדש זה מצטרף לשורה ארוכה של איומים ולא מחליף אותם.

המאמר הציג את המושג "תשתית חיונית" ודן בהגדרת החיוניות, בתיאור מקורות הפגיעות ובמאפייני האיום. בהמשך תיאר המאמר רבדים בהתמודדות עם האיום החדש, המוחשי והמיידי, המציב אתגרי מדיניות מורכבים הדורשים התמודדות. המאמר סקר בקצרה את הסוגיות המרכזיות לדיון; כל אחת מהן ראויה לדיון אקדמי ויישומי רב־תחומי ללא דיחוי.

רוב המדינות מפעילות כיום רגולציה משפטית וטכנית במגזרים נבחרים. מדינת ישראל מגינה מאז 2002 על תשתיות שהיא הגדירה כחיוניות באמצעות פיקוח והנחיה של גוף ייעודי. עם זאת, התפתחות המרחב הקיברנטי הותירה את חלקו האזרחי הלא־חיוני בלתי מוגן, ובמקביל העלתה את רמת הפגיעות.

אף שבמבט ראשון נראה כי נושא ההגנה על תשתיות מידע חיוניות משתייך לתחום המחשבים, כשעוסקים בו מתברר שרצוי להרחיבו מעֵבר לעיסוק הטכני. ההמלצה המרכזית היא, אפוא, להגביר את הדיון הציבורי בנושאי הביטחון הקיברנטי, כדי לכלול בו שיקולים חברתיים ותרבותיים רחבים, ובהמשך לאפשר התמודדות מיטבית איתו ברמה הלאומית־אסטרטגית, מתוך ראייה לאומית כוללת.

לאחרונה יזמה ממשלת ישראל את "המיזם הקיברנטי הלאומי", הצפוי להתניע טיפול במכלול הסוגיות. המלצות הוועדה הבין־תחומית שעסקה בנושא זה טרם פורסמו, אולם ברור שרק תהליך מושכל של עיצוב מדיניות יכול לצמצם את רמת הסיכון בה נתונות מדינת ישראל ויתר המדינות המפותחות.

האתגר המרכזי בתחום ההגנה על תשתיות חיוניות מפני איום קיברנטי אינו אתגר טכני; זהו אתגר אסטרטגי ופוליטי.

הערות

1 המאמר נכתב לפני התנעת "המיזם הקיברנטי הלאומי", אשר עסק בהרחבה גם בנושא הנדון במאמר, אולם המלצותיו טרם פורסמו בפומבי.

2 להלן הגדרה אמריקאית מ־2003 לתשתיות מידע חיוניות: "תשתיות מידע חיוניות הן מערכות ומתקנים שהריסתם או שיבוש תפקודם (באמצעים ממוחשבים) יגרמו לאחד או יותר מאלה: מספר נפגעים הדומה לתוצאה של הפעלת נשק להשמדה המונית; פגיעה ביכולת זרועות הממשל לספק לציבור שירותים בסיסיים ולהבטיח את ביטחון האזרחים; פגיעה ביכולת תפקוד של פירמות עסקיות ושיבוש התפקוד הכלכלי; השפעה לרעה על המשק עקב פגיעה בתפקוד של מערכות תשתית חיוניות; שיבוש התפקוד חותר תחת אמון הציבור במוסדות השלטון והמשק הלאומי: US Government, White House, Homeland Security Presidential Directive Number 7, *Critical Infrastructure Identification, Prioritization and Protection*, December 17, 2003.

3 Elgin Brunner and Manuel Suter, *International CIIP Handbook 2008/2009: An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies*, Zurich, Center for Security Studies (CSS), ETH Zürich (Swiss Federal Institute of Technology), 2008; John Moteff, Claudia Copeland and John Fischer, *Critical Infrastructures: What Makes an Infrastructure Critical?*,

Washington, D.C., Congressional Research Service, Library of Congress, 2002; Myriam Dunn, "The Socio-Political Dimensions of Critical Information Infrastructure Protection (CIIP)", *International Journal of Critical Infrastructures,* Vol. 1, No. 2-3, 2005; US Department of Homeland Security, *National Infrastructure Protection Plan (NIPP) 2009*, http://www.dhs.gov/xprevprot/programs/editorial_0827.shtm; Tyson Macaulay, *Critical Infrastructure: Understanding Its Component Parts, Vulnerabilities, Operating Risks and Interdependencies*, Boca Raton, FL., CRC Press, 2009; Robert Radvanovsky, *Critical Infrastructure: Homeland Security and Emergency Preparedness*, Boca Raton, FL., CRC/Taylor & Francis, 2006.

4 למשל: אוסטרליה וארצות הברית. נראה שמדינות אלו מיחסות חשיבות רבה להיסטוריה הפוליטית שלהן כמרכיב מרכזי בזהות הלאומית הקבוצתית ובחוסן החברתי והמדיני:
International CIIP Handbook 2008/2009, Table 1; DHS, DoI: *National Monuments & Icons: Critical Infrastructure and Key Resources, Sector-Specific Plan,* May 2007, p. 17, http://www.dhs.gov/xlibrary/assets/nipp-ssp-national-monuments-icons.pdf

5 "תורת הכאוס" מנסה להתמודד עם קשיים מסוג זה בשיטות מתמטיות.

6 פגיעה ברמת התפקוד של השלטון, שפוגעת בשירות לאזרח, יוצרת הסלמה: אמון הציבור בממשל צונח, מה שעשוי להתבטא בשינוי פוליטי (במשטר ייצוגי הדבר יתבטא בהחלפת ממשלה) ואף משטרי (מהפכה במשטר סמכותני, או שינוי מבנה המשטר בדמוקרטיה).

7 IATA (International Air Transport Association), *Air Transport Facts* (2009), http://www.iata.org/pressroom/facts_figures/fact_sheets/Pages/economic-social-benefits.aspx. ארגון IATA מייצג 93% מהתנועה האווירית הסדירה בעולם.

8 ארצות הברית הייתה החלוצה בתחום זה, כאשר ב־1996 יזמה דיון ברמה נשיאותית בנושא:
United States. President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection*, Washington, D.C., U.S. G.P.O., 1997.

9 במבצע ההפצצות האסטרטגיות במלחמת העולם השנייה בעלות הברית ריכזו מאמץ אווירי לתקיפת מפעלים גרמניים לייצור מסבים כדוריים, שמני סיכה, מתקני זיקוק וצמתי מסילות רכבת. המבצע נועד לפגוע בכושר הייצור של אמצעי לחימה.

10 כאמור, ארצות הברית מובילה את הטיפול בנושא הפגיעות הקיברנטית מאמצע שנות התשעים של המאה הקודמת, בהיותה בעלת עוצמה טכנולוגית וצבאית עצומה ומעמד של מעצמת־העל היחידה.

11 מאז שנת 2001 משגרים ארגוני הטרור רקטות ופצצות מרגמה מרצועת עזה לעבר יישובי הנגב. עד היום גרמו הרקטות ל־19 הרוגים, ופצצות המרגמה ל־10 הרוגים, ושיבשו קשות את אורח החיים באזור. לאחר הסלמה יצאה ישראל בדצמבר 2008 למבצע "עופרת יצוקה", שהסתיים בהצלחה צבאית. ירי תלול מסלול מרצועת עזה נמשך עד היום, אם כי בהיקף קטן יותר מאשר לפני המבצע.

12 היתכנות השימוש באמצעי קיברנטי לגרימת נזק פיזי הוצגה בניסויים. רשת CNN שידרה כי בניסוי Aurora שהוזמן על ידי המשרד לביטחון הפנים של ארצות הברית ונערך ב־Idaho National Labs, שידור הוראות למערכת שליטה ובקרה של מערכת ייצור חשמל הביא לכך שגנרטור יצא משימוש ובהמשך התפוצץ.

13 להלן סיכום האתגרים הנובעים ממאפייני המרחב הקיברנטי הקיים היום: הפגיעות

הרבה של מערכות ממוחשבות; קושי להבחין בין תקלה לתקיפה; קושי לקשר בין אירוע לתוצאה; קושי להתחקות אחר מקור הפגיעה; קושי לזהות את התוקף, גם אם מקור הפגיעה ידוע; שימוש רחב בטכנולוגיות מסחריות מן המדף; ריבוי השחקנים בתחום לאור סף הכניסה הנמוך. לדיון על המרחב הקיברנטי בהקשר לביטחון הלאומי ראו: ליאור טבנסקי, "לחימה במרחב הקיברנטי: מושגי יסוד", **צבא ואסטרטגיה**, כרך 3, גיליון 1, אפריל 2011.

14 Jason Stamp, et al., *Common Vulnerabilities in Critical Infrastructure Control Systems*, Sandia National Laboratories, 2003, http://www.sandia.gov/ccss/documents/031172C.pdf

15 עמידות או חוסן (resilience) היא יכולת המערכת לספוג פגיעה ולחזור לפעולה תקינה במהרה. במערכות ממוחשבות התוצאה מושגת על ידי שחזור המצב המקורי ("חזרה בזמן") או על ידי התאמה מהירה לאילוצים החדשים (הסתגלות).

16 http://www.strategyr.com/Information_Security_Products_and_Services_Market_Report.asp

17 James der Derian and Jesse Finkelstein, "Critical Infrastructures and Network Pathologies: the Semiotics and Biopolitics of Heteropolarity", in: Myriam Dunn Cavelty and Kristian Søby Kristensen, *Securing "the Homeland": Critical Infrastructure, Risk and (In)Security*, London, New York, Routledge, 2008.

18 קיימת שונות רבה בין הגדרת התשתית הקריטית ובין האמצעים הננקטים להגנתה במדינות השונות. ראו: Brunner and Suter, International CIIP Handbook 2008/2009. ההיבט האזרחי של הגנה על תשתיות חיוניות בישראל נקבע ב"חוק להסדרת הביטחון במקומות ציבוריים, התשנ"ח־1998". החוק מסמיך את שירות הביטחון הכללי להנחות גופים ציבוריים שונים בתחומי האבטחה הפיזית, אבטחת מידע ואבטחת מערכות ממוחשבות חיוניות, לפי פירוט המופיע בתוספות לחוק. בחוק זה נקבעו עונשים על אי מילוי הוראותיו, הכוללים קנס אזרחי ומאסר בפועל. ב־2003 הוקמה הרשות הממלכתית לאבטחת מידע (רא"ם), "המופקדת על הנחיה מקצועית של הגופים המונחים שבאחריותה בתחום אבטחת תשתיות מחשב חיוניות מפני איומי טרור וחבלה, בתחום אבטחת מידע מסווג ומפני איומי ריגול וחשיפה", http://www.shabak.gov.il/about/units/reem/pages/default.aspx

19 רוב התחבורה הציבורית בארצות הברית ויותר מ־85% ממגזר האנרגיה בארצות הברית נשלטים בידי חברות מסחריות פרטיות. כ־85% מהתקשורת של משרד ההגנה האמריקאי עוברים ברשתות מסחריות.
http://training.fema.gov/EMIWeb/IS/IS860a/CIKR/energy1.htm

20 מדינת ישראל, מכוח מצבה הגיאו־פוליטי, מחזיקה מלאי מזון וציוד כדי להבטיח את צרכי המשק בשעת חירום. "הרשות העליונה למל"ח – מזון ומשכ"ל" במשרד התמ"ת היא הגוף האחראי על נושא זה.

21 הכוונה למושג של פילוסוף המדע קרל פופר. ראו: קרל רימונד פופר, **החברה הפתוחה ואויביה**, מתרגם: אהרן אמיר, עורך: יוסף אגסי, הקדמה: יובל שטייניץ, ירושלים, שלם, 2003.

22 ראו למשל ריכוז פרסומים של מכון התקנים האמריקאי: http://csrc.nist.gov/publications/PubsFL.html
וכן התקנים למגזר החשמל של North American Electric Reliability Corporation Standards (NERC) CIP-002-3 through CIP-009-3, http://www.nerc.com/fileUploads/File/Standards/Revised_CIP-002-1_FAQs_20090217.pdf http://www.nerc.com/fileUploads/File/Standards/Revised_

Implementation_Plan_CIP-002-009.pdf

23 CSIS Commission on Cybersecurity for the 44th Presidency, *Cybersecurity Two Years Later: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency,* Washington, D.C., Center for Strategic and International Studies, 2011.

24 גבי סיבוני, "הגנת נכסים ותשתיות קריטיות מפני תקיפה קיברנטית – הממד הסטטוטורי", **צבא ואסטרטגיה**, כרך 3, גיליון 1, אפריל 2011.

25 ראו לדוגמה: החלטת ממשלה 1886 בק/9 מ־20 במארס 1997: הקמת ועדת היגוי לנושאי מחשוב בכל משרד ממשלתי; החלטת ממשלה 3582 בק/77 מ־16 במארס 1998: אחריות לנושא אבטחת מידע במשרדי הממשלה; החלטת ממשלה 4956 בק/179 מ־23 במארס 1999: הוקמה המועצה לאבטחת מידע רגיש במשרד ראש הממשלה; החלטת ממשלה תמ/80 מ־26 בנובמבר 2000 בעניין האחריות על אבטחת המידע הממוחשב בצה"ל ושיתוף הפעולה עם הגורמים האזרחיים; החלטת ממשלה תמ/14 מ־18 ביולי 2001: רשת פנימית מאובטחת לשימוש משרדי הממשלה.

26 כאמור, המאמר נכתב לפני פרסום המסקנות של "המיזם הקיברנטי", אשר עסק בין היתר בנושא ההגנה על המרחב הקיברנטי האזרחי.

27 הודעת מזכיר הממשלה בתום ישיבת הממשלה מיום 7 באוגוסט 2011, סעיף ד': קידום היכולת הלאומית במרחב הקיברנטי, http://www.pmo.gov.il/PMO/Secretarial/Govmes/2011/08/govmes070811.htm

מה עומד מאחורי לוחמת הסייבר של סין

גבי סיבוני וי"ר

兵之形, 避實而擊虛
"במלחמה הדרך היא להימנע ממה שחזק ולתקוף את מה שחלש"
(סון טסו, **אמנות המלחמה**)

מבוא

סין מפתחת זה כמה שנים יכולות מבצעיות בתחום לוחמת הסייבר. למרות ההכחשות של הממשל הסיני מקובלת בקרב החוקרים התפיסה שסין עומדת מאחורי שורה של מתקפות סייבר[1] על ארצות־הברית,[2] יפן,[3] צרפת,[4] אוסטרליה[5] ומדינות נוספות במערב.[6] ההגדרה של תקיפת סייבר היא: חדירה שלא ברשות למערכות המחשוב והתקשורת של יחידים ושל ארגונים לשם ריגול וגנבת מידע, זאת כדי לשבש את תפקודן או לפגוע בהן, וכן לשם פגיעה במערכות נוספות המבוססות עליהן – לעתים אף עד כדי גרימת נזק פיזי.

הפעילות של סין בלוחמת הסייבר מנוהלת באינטנסיביות ובאגרסיביות. נראה כי סין מתמקדת באיסוף נרחב של מידע מודיעיני ומסחרי במגוון תחומים – החל בחברות בעלות ידע טכנולוגי ייחודי וכלה בארגונים בעלי מידע פיננסי וכלכלי, כמו תקיפת המחשבים של קרן המטבע הבין־לאומית בסוף 2011.[7] ואולם, העובדה שהותקפו גם חברות וארגונים המספקים שירותים חיוניים ותשתיות תקשורת מעידה כי ייתכן שקיימים מניעים נוספים. לנוכח זאת, מתעוררות השאלות: מה עומד מאחורי המתקפות והאם ניתן לזהות את המתווה האסטרטגי שעל־פיו פועלת סין במערב בכלל, ובארצות־הברית בפרט. לשם כך יש לבחון את האסטרטגיה שגיבשה סין בתחום לוחמת הסייבר, את הגופים העוסקים בכך בסין בשנים האחרונות ואת המשאבים המושקעים למימוש היעדים שסין מבקשת

אל"ם (מיל.) ד"ר גבי סיבוני הוא ראש תכנית צבא ואסטרטגיה וראש תכנית לוחמת סייבר במכון למחקרי ביטחון לאומי.
י"ר הוא עובד בכיר במשרד ראש הממשלה.

מאמר זה ראה אור לראשונה ב**צבא ואסטרטגיה**, כרך 4, גיליון 2, ספטמבר 2012, עמ' 43–56.

להשיג באמצעות הלוחמה הזאת. מקובלת ההנחה שלפני שנת 2009 הופנו רוב התקיפות שיוחסו לסין נגד רשתות של גורמי צבא וממשל, כמו מבצע Titan Rain שהופעל נגד ארגונים ממשלתיים בארצות־הברית,[8] ומבצע GhostNet נגד מטרות דיפלומטיות באו"ם. לעומת זאת, בשנים האחרונות התקיפות המיוחסות לסין נערכו נגד מטרות אזרחיות, בהן תשתיות לאומיות בעלות חשיבות קריטית, חברות המהוות חוליות בשרשרת הנגישות לאותן המטרות וחברות שתקיפתן משרתת צורך כלכלי־מסחרי.

בשנים האחרונות נערכו תקיפות על תשתיות שהיו בבחינת קפיצת־מדרגה. הראשונה הייתה סדרת התקיפות Shady RAT שהחלו באמצע 2006 ונמשכו עד פברואר 2011.[9] סדרת התקיפות השנייה הייתה מבצע Aurora שהיה מתוחכם במיוחד ובו הותקפה בין היתר חברת Google המהווה תשתית חיונית ברמה העולמית. התקיפות האלה נערכו מאמצע 2009 ועד דצמבר אותה השנה. סדרת התקיפות השלישית – שלה היו הדים רבים בתקשורת – הייתה על חברת RSA, חברה העוסקת באבטחת מידע ושרתי אינטרנט והמספקת בין היתר שירותי SecureID והרשאות כניסה חד־פעמיות (One Time Password - OTP). השערת המחקר במאמר הזה היא שניתוח המידע הגלוי שהתפרסם בנוגע לתקיפות האחרונות מאפשר לאשש את ההנחה שסין עומדת מאחורי התקיפות האלה, ואף לזהות התאמה בין האסטרטגיה של סין בתחום לוחמת הסייבר לבין בחירת יעדי המתקפה.

הניתוח כלל בחינה של מאפייני החברות שהותקפו כדי לזהות מניעים אפשריים לתקיפה, לדוגמה: תקיפה של חברות וארגונים ספקי טכנולוגיה מאפשרת נגישות לטכנולוגיה עילית, לטכנולוגיה צבאית וכדומה. ניתן להניח שהמניעים לתקיפות כאלה הם גנבה של יכולות וריגול תעשייתי של מדינות או של חברות מתחרות. תקיפה של חברות וארגונים מן המגזר הפיננסי, המגזר הכלכלי ואף המגזר הפוליטי מאפשרת נגישות למודיעין בעל ערך בתחומים האלה. לעומת זאת, הערך המודיעיני לשימוש מידי של תקיפת חברות המספקות תשתיות חיוניות ושירותי תקשורת נמוך בדרך־כלל באופן יחסי. השגת נגישות, ולו לחלק מספקי שירותי התקשורת והאינטרנט במערב ובארצות־הברית, עלולה להקנות לתוקף יכולת לפגוע בשירותים האלה.

האסטרטגיה של סין בתחום לוחמת סייבר

האסטרטגיה של סין בתחום לוחמת הסייבר גובשה בעשור הקודם, זאת במסגרת תהליך מודרניזציה עמוק שעבר צבאה. בבסיס האסטרטגיה עומדת ההבנה שצבא סין נמצא בנחיתות מובנית ביחס לצבאות במערב, כמו צבא ארצות־הברית בכל הקשור ללוחמה קינטית. לנוכח זאת התגבשה ההבנה שכדי להתמודד עם יריב

בעל יתרון טכנולוגי בתחום תעבורת המידע יש לשבש את נגישותו למידע הזה. התפיסה נוגעת להנחתת מהלומה משולבת מקדימה הכוללת את המרכיבים הבאים: מתקפת סייבר, מתקפה אלקטרונית ומתקפה קינטית על רשת המידע ומוקדי הטכנולוגיה הצבאית של היריב. המהלומה הזאת תוביל להיווצרות "נקודות עיוורות" שיאפשרו לכוחות הסיניים לפעול ביעילות רבה יותר.[10] ההנחה של סין היא שבאמצעות שיבוש תעבורת המידע ניתן לפגוע באופן משמעותי ביכולות של היריב המתוחכם ולהשיג יתרון בשלבים הראשונים של העימות.

האסטרטגיה שפותחה בסין בעשור האחרון רואה במבצעי רשת מוכללים[11] פלטפורמה מרכזית לפיתוח התחום. האסטרטגיה הזאת מושתתת על שילוב בין ארבעה סוגים של מבצעים:[12] תקיפת רשתות מחשבים, לוחמה אלקטרונית הכוללת אמצעי נגד אלקטרוניים ומכ"ם, הגנת רשת מחשבים וניצול רשתות מחשבים (exploitation).[13] התפיסה המשולבת הזאת מקנה לסין יכולת מבצעית רב תחומית המאפשרת לה מיצוי של הכוח לשם תקיפת היריב. אחד המרכיבים המרכזיים באסטרטגיה של סין הוא שליטה על תעבורת המידע של היריב, זאת על בסיס ההנחה שליריביה של סין (בעיקר מדינות המערב, בייחוד ארצות־הברית) יש תלות רבה בטכנולוגיה המבוססת על תעבורת מידע. בבסיס האסטרטגיה הסינית עומדת ההנחה שבעת עימות, היכולת לפגוע בתעבורת המידע תאפשר לסין להשיג יתרון בשדה הקרב הפיזי.

כמה פרסומים מנתחים בפירוט את הגופים העיקריים בצבא סין בתחום מבצעי הרשת.[14] במאמר הזה נסתפק בתיאור שני גופים מרכזיים בצבא: המחלקה השלישית (במטה הכללי של צבא שחרור העם – PLA), האחראית על מודיעין סיגינט, והמחלקה הרביעית, האחראית על מודיעין אלינט ולוחמה אלקטרונית. במחלקה השלישית עובדים מומחים במגוון תחומים: טכנאים, מומחי מחשבים, מומחים לשפות, מומחי מודיעין ועוד. ההיקף הנרחב של פעילותה של המחלקה ומגוון המשימות המוטלות עליה עושים אותה מתאימה לביצוע מבצעי סייבר ברשת. למחלקה הזאת יש תחנות איסוף רבות הפזורות ברחבי סין, והיא אחראית על איסוף מודיעין בתחום השמע והנתונים ועל מיצויו, הפקתו והערכתו. המחלקה הזאת אחראית כנראה גם על איסוף מידע פנימי בצבא סין לצורכי ביטחון ואבטחת מידע פנים. להערכת כמה חוקרים במערב, היקף כוח־האדם הפועל במסגרת המחלקה השלישית הוא למעלה מ־130,000 איש.[15] המחלקה הרביעית, האחראית על מבצעי מודיעין אלקטרוני (אלינט) ולוחמה אלקטרונית, פועלת כנראה גם בתחום מבצעי רשת משולבים.[16] נראה שהמחלקה השלישית היא הגוף המרכז את כלל הפעילות בתחום הזה.[17]

נוסף על הארגון הצבאי קיימת בסין קהילת פצחנים[18] גדולה מאוד. הקהילה הזאת מעורבת כנראה גם בפעילות להשגת יעדים לאומיים. קבוצות כאלה קיבלו

אחריות על כמה תקיפות. נראה שאף כי ממשלת סין פועלת לאכיפת החוק הסיני האוסר על פעילות כזאת, היא מעלימה עין מן הפעילות, ואף תומכת חומרית בחלק ממנה – מעין מיקור חוץ לפעילות הממשלה בתחום הסייבר.[19] נוסף על כך מגייס צבא סין אזרחים ליחידות מיליציית הרשת שלו המגיעים מקרב קהילת הפצחנים וחברות טכנולוגיה.[20] המיליציה הזאת משולבת בפעילות הצבא אף כי החברים בה הם מתנדבים ואינם מקבלים שכר.

יש לציין שלעומת התפיסה הרווחת בקרב חוקרי פעילות הסייבר של סין, קיימים חוקרים הטוענים כי הפעילות הזאת נועדה בראש ובראשונה לצורכי פנים, וכי מדינות המערב אינן צריכות לחשוש ממנה יתר על המידה בכל הנוגע לאיום על מרחב הסייבר שלהן. לטענתם, היכולות מפותחות בעיקר לצורכי בקרה על מתנגדי המשטר, שליטה על התכנים המגיעים לאזרחי סין וצרכים פוליטיים שעיקרם שימור השלטון.[21] אף כי ניתן להסכים לטענה הכללית שמשטרים טוטליטריים, ובהם סין, עושים שימוש ביכולות סייבר גם לצרכים פוליטיים,[22] המציאות שונה – יעיד על כך רצף אירועי הסייבר שמקורם בסין בשנים האחרונות.

אחד המרכיבים העיקריים באסטרטגיה של סין הוא הצורך בנגישות לתשתיות התקשורת של היריב. הנגישות הזאת קריטית למימוש יעדיהם, ובלעדיה יתקשו לייצר "נקודות עיוורות" אצל היריב. יצירת נגישות אפקטיבית ברשתות תקשורת מחייבת פעילות תשתיתית לאורך זמן ובהיקף נרחב. תקיפת רשתות התקשורת של היריב יכולה להתבצע רק אם קיימת אליהן נגישות קבועה לאורך זמן, המספקת הן מודיעין איכותי והן יכולות להתקין באופן חשאי רכיבי תוכנה זדוניים שאותם ניתן להפעיל ביום פקודה. הנגישות הזאת מחייבת תחזוקה ושימור לאורך זמן בשל שינויים קבועים שעושה היריב במערכי התקשורת והמידע שלו ומכיוון שהוא מתקין מערכות הגנה חדשות העלולות לחשוף את הפעילות.

תקיפות הסייבר של סין

בשש השנים האחרונות התגלו לא מעט תקיפות סייבר המיוחסות לסין. חשיפת המבצעים האלה שופכת אור על שיטות הפעולה של סין. על פני הדברים, אלה היו מבצעי איסוף, ובאמצעות ניתוחם ניתן לזהות את טכניקות התקיפה הבסיסיות ולהקיש על המדיניות של התוקף ועל שיטות פעולה שלו, במקרה הזה – סין. מן התקיפות ניתן ללמוד על גישה של מעצמה שמטרתה להשיג נגישות תשתיתית נרחבת מאוד, והיא אינה מסתפקת ביעד נקודתי. במקרה של מבצע Aurora המטרה הייתה השגת גישה למנגנון הססמאות של Google ולתוכנת בקרת הגרסאות. במקרה של תקיפת RSA המטרה הייתה השגת גישה לרשת הפנימית שבה נוהל מידע הקשור למערכת SecureID היכול לשמש במשך הזמן להתקפה יעילה יותר על חברות אחרות העושות שימוש במערכת, ובהן חברות ביטחוניות וחברות אחרות

בעלות פעילות רגישה. טכניקות התקיפה שזוהו היו דומות מאוד זו לזו. אלה היו מתקפות מאורגנות היטב שנעשה בהן שימוש משולב ב־social engineering,[23] חולשות תוכנה, בהתקנת כלים שוהים, בהרחבת נגישות תוך ארגונית ובשאיבת מידע רב. נקיטת הפעולות השיטתיות האלה במשך כל השנים האחרונות מחזקת את הטענה שהתקיפות היו מאורגנות ושאותם גופים יזמו אותן, ומחלישה את הטענה שהתקיפות האלה בוצעו על־ידי פצחנים מזדמנים. אישוש נוסף לטענה הזאת ניתן למצוא בניתוח שבוצע על־ידי אנשי הקונצרן הביטחוני האמריקני נורת'רופ גרומן.[24] הניתוח הזה עשה שימוש בכמה אבני בוחן כדלהלן:

א. דמיון ב"התנהגות מקלדת" (keyboard behavior) – זיהוי של מאפייני התנהגות דומים בפעולת התוקפים בתקיפות שונות. למשל, תקיפת חלקי מידע בעל מאפיינים דומים ושימוש בכלים דומים.

ב. היקף ההכנות המקדימות – התוקפים נקטו פעולות שחייבו הכנות וידע מקדים שנבע כנראה מפעולה מקדימה שנעשתה במשך כמה חודשים לפני ביצוע התקיפה בפועל. לדוגמה, התוקפים הכירו את ארכיטקטורת הרשת שאותה תקפו.

ג. המשמעת של התוקפים – התוקפים התאפיינו במשמעת גבוהה. לדוגמה, הם לא פתחו קבצים לפני העתקתם כדי לסקור באופן ראשוני את התוכן. ככל הנראה הם פעלו על־פי מידע מוקדם.

מבצע Nitro

מבצע **Nitro** כלל סדרת תקיפות שרובן נערכו מסוף יולי עד אמצע ספטמבר 2009. המידע על המבצע פורסם על־ידי חברת סימנטק.[25] ההנחה היא שהיעד העיקרי של המבצע היה ריגול טכנולוגי. המבצע התנהל בכמה גלים שהתבצעו ברציפות וניתן לאפיין אותם על־פי יעדי התקיפה. בתחילה הותקפו ארגוני זכויות אדם בסין, אחריהם הותקפו תעשיות מנועים ובחודשים האחרונים לפני שנחשפו הותקפו 29 חברות בתחום הכימיה. החברות שהותקפו היו ברשימת Fortune 100 העוסקות במחקר ופיתוח כימי וחומרים מיוחדים, בעיקר לתעשיית הרכב הצבאית, וחברות העוסקות בהקמת תשתיות לתעשיות כימיות ובייצור חומרים מתקדמים. שיטת התקיפה הייתה דומה לזו שננקטה בתקיפות נוספות שביצעו הסינים (ראו להלן) וכללה את המרכיבים הבאים:

א. שליחה של קוד מפגע שהוסווה בדרך־כלל כעדכון אבטחה. נשלחו כמויות גדולות של דואר אלקטרוני לארגונים ללא התאמה אישית. זאת בניגוד למבצעים אחרים שבהם הושקעו מאמצים רבים יותר בהתאמת הדואר האלקטרוני לנמען.

ב. התקנת דלת אחורית (סוס טרויאני) במחשב היעד.

ג. הגברת הנגישות ברשת המותקפת תוך שימוש בשרידים של סיסמאות שנמצאו על המחשב שהותקף כדי להגיע לשליטה במחשב המרכזי ברשת.
ד. איסוף החומר בשרתי ביניים ושידורו מחוץ לרשת. בסך־הכול הותקפו כ־100 מחשבים, מהם 29 – של חברות שעסקו בתחום הכימיה ו־19 נוספים – של גופים במגזר הביטחוני. רוב החברות שהותקפו היו בארצות־הברית (כ־30%) בבנגלדש (כ־20%) ובבריטניה (כ־15%). יתר המחשבים היו בכ־20 מדינות ברחבי העולם.

מבצע Aurora

מבצע Aurora כלל סדרת תקיפות שהחלו באמצע 2009 ונמשכו עד דצמבר 2009. על התקיפות דיווחה לראשונה חברת Google בינואר 2010. מהחברה נמסר כי תוקפים חדרו לחשבונות gmail של פעילי זכויות אדם סינים הפועלים בארצות־הברית, באירופה ואף בסין.[26] גם חברת Adobe דיווחה על תקיפה במסגרת אותו מבצע. בסך־הכול הותקפו לפחות 34 ארגונים וחברות.[27] חברת אבטחת המידע McAfee ערכה ניתוח של התקיפה הזאת. ממצאי הניתוח עלה שמטרת התקיפה הייתה השגת נגישות לקוד המקור של החברות שהותקפו, בפרט לתוכנת ניהול הגרסאות Periscope שבה משתמשות מאות חברות תוכנה גדולות. החברה אפיינה כמה שלבים בתהליך התקיפה:[28]

א. מפעיל המחשב המותקף קיבל דואר אלקטרוני או מסר מידי שנראה תמים ממען שלכאורה היה בטוח.
ב. המפעיל התפתה והפעיל את הקישור המצורף להודעה אשר הוביל לשרת שהכיל קוד זדוני.
ג. סייר האינטרנט במחשב המותקף הוריד קוד בינארי שהוסווה כקובץ תמונה והפעיל דלת אחורית שהתקשרה לשרת שליטה שהיה ממוקם בטייוואן.
ד. התוצאה – התוקפים השיגו שליטה מלאה על המחשב, ובאמצעותו – על מידע רגיש שהיה מקושר ברשת.

השיטה הזאת ננקטה ברבות מן התקיפות המכונות APT (Advanced Persistent Threat). בתחילה המשמעות של המונח הזה הייתה תקיפות מתוחכמות על רשתות צבא וממשל, אך כיום נעשה במונח הזה שימוש כדי לציין תקיפה בעוצמה רבה (עוצמה של מדינה) על מטרה אזרחית.

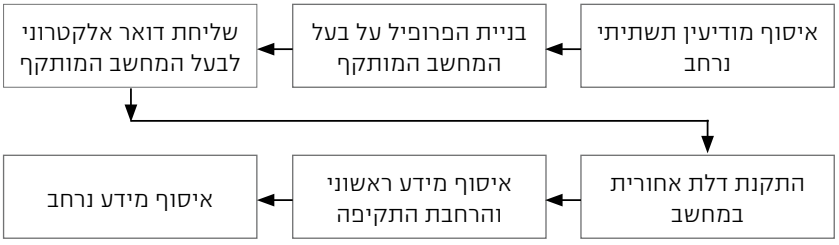
גלי התקיפה Night Dragon ו־Shady RAT

גלי התקיפה החלו באמצע 2006 ונמשכו עד פברואר 2011. חברת McAfee, שהשיגה נגישות לשרת שליטה אחד שבו עשו התוקפים שימוש, זיהתה בשרת הזה, לאחר ניתוח של קובצי לוג,[29] כי הותקפו כ־70 יעדים.[30] לנוכח העובדה

שהושגה נגישות לשרת שליטה אחד בלבד, ניתן להניח שלתקיפה הזאת היו יעדים נוספים. בניתוח אופיינו החברות שהותקפו ומשכי־הזמן שבהם המחשבים בחברות האלה היו בשליטת השרת אשר דרכו שאבו התוקפים מידע רגיש. הניתוח של חברת McAfee סיפק תמונה בנוגע לחברות שהותקפו – חברות ממשל (21 חברות), תעשייה ואנרגיה (6 חברות), תקשורת, מחשבים ואלקטרוניקה (13 חברות), תעשייה ביטחונית (13 חברות) ופיננסים (6 חברות). בהקשר הזה בולטות התקיפות על חברות הנפט והגז של נורווגיה.[31] תקיפה של חברות המהוות תשתית לאומית, כמו חברות אנרגיה, יכולה להעיד על רצון ליצור נגישות לפגיעה בעתיד בתשתיות האלה.

תקיפת RSA

תקיפת RSA מספקת מצע לניתוח עומק בשל העובדה שאחד מן השרתים שהיה מעורב בה בוטנט[32] בהיקף של כ־2,000 מחשבים. חדירה לשרת המרכזי של הבוטנט אִפשרה לנתח את רשימת המחשבים הנגועים שמהם התקבלה רשימה של 763 חברות.[33] התקיפה דווחה לראשונה על־ידי RSA במרס 2011.[34] ניתן לתאר את השלבים של התקיפה, ששיטתה אפיינה תקיפות אחרות, כדלהלן:



להלן הסבר על תהליך התקיפה המתואר:

איסוף מודיעין תשתיתי נרחב – השלב המקדמי לתקיפה הנו איסוף של מודיעין תשתיתי נרחב על הגוף שאותו מתכוונים לתקוף. המודיעין הזה נאסף בדרך־כלל מתוך הרשתות החברתיות וממידע גלוי אחר. מטרת המידע היא לאתר ממלאי תפקידים המועמדים לתקיפה, כדי שאלה יוכלו להוות את הנתיב שדרכו ניתן יהיה לפעול בצורה המיטבית בתוך הארגון המותקף. לדוגמה, באירוע תקיפת RSA נבחרו שתי קבוצות קטנות של עובדים. אלה לא היו בהכרח יעד התקיפה הסופי אלא נבחרו כנראה משום שהתוקפים העריכו שיהיה נוח להתחיל את התקיפה באמצעות המחשבים של העובדים האלה.

בניית הפרופיל של בעל המחשב המותקף – לאחר איתור יעדי החדירה נבנה פרופיל של המותקפים. הפרופיל הזה מחייב בניית תמונת מידע מלאה דיה כך

שתתאפשר יצירת הודעת דואר אלקטרוני שתיראה למקבל המותקף כהודעה תמימה ולא תעורר את חשדו. יש לזכור שאיסוף מידע כזה ובניית פרופיל מתאים מחייבת אף היא פעילות איסוף ענפה וממוקדת הדורשת ארגון ומשאבים לא מעטים (בפרט עובדים בעלי ידע באנגלית).

שליחת דואר אלקטרוני מפגע המותאם לבעל המחשב המותקף (ZeroDate spear phishing email) – שליחת הדואר האלקטרוני המפגע מחייבת נקיטת שתי פעולות. הראשונה היא בניית נוסח, מבנה ומראה של הודעה תמימה שתגרום לבעל המחשב העובד בארגון המותקף לא למחוק אותו ולפתוח את הקישורים בו. הדואר האלקטרוני נשלח לקבוצה ממוקדת של עובדים שנבחרו. לעתים מותאמת ההודעה לכל עובד בנפרד בהתאם לפרופיל שנבנה. הפעולה השנייה – הצמדת קובץ מצורף דבוקה, (attachment) להודעת הדואר האלקטרוני הכוללת חולשת אבטחה עם דלת אחורית. חולשות הן פרצות אבטחה בתוכנה המאפשרות להחדיר דרכן את הקוד המפגע. לעתים החולשה היא חולשה מקורית שזוהתה בתהליך איתור חולשות על־ידי המפגע (כך נעשה כנראה במבצע Aurora), ולעתים החולשה ידועה ומפורסמת (ZeroDate) כשהתוקף מסתמך על האפשרות שבמחשבי היעד עדיין לא הותקן טלאי תיקון לחולשה הזאת.[35] לדוגמה, בתקיפת RSA הנושא של הדואר האלקטרוני היה "Recruitment Plan 2011", וצורף אליו קובץ האקסל Recruitment plan 2011.xls. חולשת ה־ZeroDate הייתה CVE–0609–2011 ב־Adobe Flash. ברגע שאחד העובדים פתח את הקובץ במחשבו הוא נדבק בדלת אחורית. בעת התקיפה החולשה נחשבה לא ידועה, ולא היה לה עדכון אבטחה; העדכון הופץ כשבוע לאחר התקיפה.

התקנת דלת אחורית במחשב – הכוונה היא לקוד זדוני המותקן במחשב הנגוע ומאפשר לתוקף לשלוט עליו באמצעות שרת שליטה.[36] בדרך־כלל הדלת האחורית המותקנת יוצרת קשר עם שרת התוקף, ומשם היא מופעלת בהתאם להוראות המועברות מן השרת הזה על־ידי מפעילים אנושיים הפועלים בדרך־כלל במשמרות. הכיוון הזה של התקשורת – מתוך הארגון כלפי חוץ – מקשה על איתורה.

איסוף מידע ראשוני והרחבת התקיפה – בשלב הזה נאסף חומר ראשוני. למעשה, לכל מחשב מותקף מוצמדת קבוצת תקיפה המנתחת את תכולת המחשב ומנסה להעריך כיצד ניתן לאסוף מידע מן המחשב המותקף ואיזה מידע ניתן לאסוף ממנו. בדרך־כלל נעשית בשלב הזה הערכה בנוגע לנגישות של המחשב המותקף לשרתים ולמקורות מידע אחרים בארגון כדי לזהות את מפת הרשת ולהבין כיצד ניתן להרחיב את התקיפה.

איסוף מידע נרחב – זהו שלב האיסוף המרכזי המתרחש לאחר שנוצרה נגישות לשרתי החברה וזוהה המידע הנדרש. העברה של כמויות מידע גדולות באופן שאינו מעורר חשד ובדרך שאינה מאפשרת זיהוי על־ידי תוכנות ניטור המותקנות

בדרך כלל ברשתות של ארגונים גדולים הנה פעולה מורכבת. זו נעשית בדרך־כלל באמצעות מחשב אחר ברשת שהנגישות שלו וההרשאות שלו הן ברמה גבוהה כך שהוא משדרג את ההרשאות של אותם שרתים לייצא מידע תוך שימוש בהצפנה ואלגוריתמים של דחיסת מידע. לדוגמה, במקרה של RSA הגיעו התוקפים בסופו של התהליך למחשב שבו נשמר מידע רגיש הקשור למערכת SecureID, שאִפשר בהמשך נגישות למידע בחברות אחרות.[37] כל זאת בצורה שעקפה את התראות חוקי מערכות הניטור בארגון.[38]

הגישה שתוארה לעיל מחייבת הקצאת משאבים מקצועיים רבים. בתקיפה הזאת פעלו כנראה שתי קבוצות במקביל באמצעות כלים שונים. הראשונה פעלה לאיתור המידע הנדרש ברשת החברה, והשנייה פעלה בנפרד כדי לייצר את ערוץ הוצאת המידע. ייתכן שפעלה אף קבוצה שלישית שתפקידה היה לשמר את הנגישות לשימוש מאוחר יותר בעתיד. הגישה הזאת מעידה על תפיסה של מעצמה הפועלת ברמה מקצועית גבוהה תוך השקעה במשאבים רבים של כוח אדם איכותי ושל יכולות מודיעין. ניתן לזהות בתקיפה הזאת כמה מרכיבים המעידים על כך שמאחוריה עומדת מעצמה וההערכה המקובלת היא שמדובר בסין. להלן פירוט המרכיבים האלה:

גישה תשתיתית – פריצה למנגנון הסמכאות החד־פעמי של החברה (OTP) במטרה להשיג נגישות רבה לחברות נוספות מצביעה על גישה של פעולה נרחבת המחייבת משאבים גדולים.

היקף התקיפה – בפרסומים הגלויים דווח על 763 מחשבים נגועים שנמצאו על אחד השרתים שהיה מעורב בתקיפת RSA. לפחות עבור חלק מן היעדים האלה היה צורך בפעילות ידנית מקדימה כפי שפורט בשיטת העבודה, כלומר, היה צורך באיסוף מידע מקדים על היעד, בבניית דואר אלקטרוני בשפה האנגלית ששימש כפתיון ובניתוח ראשוני של הנגישות. תקיפה בעוצמה רבה כזאת חייבה התארגנות תשתיתית ברמה של מעצמה ומעידה על כך שאין המדובר בפעולה של בודדים.

תוכנת הדלת האחורית Sykipot[39] – התוכנה הזאת, שהיא וריאנט של PoisonIvy,[40] משמשת בתקיפות של סין כפי שתוארו לעיל. נעשה בה שימוש (בגרסאות דומות) כבר ב־2006, והוא נמשך גם בתחילת 2012.[41] השימוש בתוכנה דומה (עם שינויים קלים באופן יחסי) מעיד על תיאום ארגוני בין תוקפים שונים במהלך השנים האחרונות.

סימנים מזהים – בתוכנת הדלת האחורית נמצאו קישורים חזקים לסין. על־פי ניתוח הטקסט בתוכנה זוהו סימנים מובהקים של השפה הסינית כולל שיירי מידע בשפה הסינית בקוד הבינארי (debug information). נוסף על כך אותרו הודעות שגיאה בשפה הסינית, ולבסוף, ספר המשתמש היחיד לגרסה של הדלת האחורית כתוב בסינית.

שרתי השליטה – ניתוח האתרים שבהם הוצבו שרתי השליטה, ושמהם הופעלו המחשבים הנשלטים, העלה כי רובם המכריע היו בסין (299 מתוך 329 שרתי שליטה).[42]

הממצאים האלה מאששים את ההנחה הבסיסית שסין עומדת מאחורי התקיפה שחייבה שימוש במערך ארגוני תשתיתי נרחב ושיטתי. לנוכח זאת, אין להתפלא על הודעתו של הגנרל קית' אלכסנדר ראש NSA שאישר לאחרונה כי סין עומדת מאחורי תקיפת RSA.[43]

רשימת 763 החברות שהופיעו באחד השרתים שהיה מעורב בתקיפת RSA נותחה כדי לבחון האם ניתן להפיק מן המידע הזה מסקנות בעלות ערך. הניתוח כלל איתור של החברה באינטרנט ואפיון עיסוקה. החברות אופיינו באחת משלוש קטגוריות: חברות טכנולוגיה שהותקפו כנראה לצורך ריגול טכנולוגי; חברות פיננסים וכלכלה שתקיפתן יכולה לאפשר גנֵבת מידע מסחרי; וספקי תקשורת. המשמעות של הממצא הזה בדרך־כלל היא שהמחשב הנגוע היה מחובר דרך ספק גישה ציבורי לאינטרנט (ISP).[44]

הניתוח מלמד שקרוב ל־80% מכלל החברות והארגונים שהותקפו היו בקטגוריית ספקי תקשורת. יתר ה־20% נחלקו בין חברות טכנולוגיה, חברות פיננסים ואחרות. הנתונים האלה מצביעים על פילוח בוטנט אופייני הכולל מספר רב של מחשבים נגועים השייכים לאנשים פרטיים שהתחברו לרשת באמצעות ISP. רוב המחשבים ברשימה (34%) היו מארצות־הברית. יתר המחשבים שהותקפו נחלקו בין כ־90 מדינות, בהם חמישה מישראל.

תובנות מסכמות

סדרות התקיפות מאז 2006 מצביעות על מעבר לתקיפה של חברות תשתית חיוניות הן בתחום התקשורת והן בתחום האנרגיה. בהקשר של תקיפת RSA קיימת אפשרות שרשימת החברות שנמצאה על השרת כללה רשימה אקראית של בוטנט שנבנתה על־ידי הסינים בתהליך שנמשך זמן רב לפני גילוי התקיפה כדי לשמש תשתית להתקפות בעתיד. מכל מחשב נגוע ניתן לשלוח דואר אלקטרוני למטרות תקיפה, להעביר קבצים או להסתיר את זהות התוקף. ואולם, קיימת האפשרות שחלק מן הרשימה הזאת אינו אקראי וכולל חברות שהן היעד המתוכנן של התקיפה.

הממצאים של התקיפות בשנים האחרונות מאששים את השערת המחקר ומאפשרים לקבוע שהתקיפות שתוארו הן חלק ממערכה סדורה ושיטתית המתבצעת על־ידי סין. ניתן לזהות התאמה בין האסטרטגיה של סין בתחום לוחמת סייבר לבין בחירת חלק מיעדי התקיפה, בעיקר אלה הנוגעים לתשתיות חיוניות. הן תקיפת גוגל במבצע Aurora, הן תקיפות Shady RAT, וכמובן תקיפת

RSA מצביעות על מעבר לתפיסה מערכתית הכוללת יעדי תקשורת ויעדי תשתית חיוניים. האסטרטגיה של סין, שמטרתה לפגוע במרחבים החלשים והפחות מוגנים של היריב במהלך המקדים להפעלת הכוח הקינטי, מחייבת פעולה נרחבת ליצירת נגישות לאורך זמן לתשתיות חיוניות, בהן תשתיות תקשורת. יש לציין שבניגוד למבצעי איסוף הרועשים מטבעם, ולכן מתגלים מעת לעת, קשה יותר לגלות מבצעי תשתית להשגת נגישות ליום פקודה לגילוי וייתכן אף כי לא יתגלו כלל.

נוסף על התקיפות שהוזכרו לעיל, הואשמה סין באפריל 2011 ביירוט של לא פחות מ־15% מתעבורת האינטרנט.[45] לפיכך ההערכה היא שחלק מן התקיפות מיועדות ליצור נגישות מודיעינית לתעבורת האינטרנט וליירוט תשדורות לפני שהן מוצפנות. יש לזכור שהמסקנות במאמר הזה מתבססות על ידע שהצטבר כתוצאה מניתוח של מידע על תקיפות שהתגלו ופורסמו. מכיוון שלא ניתן תמיד לגלות תקיפות, ולעתים גם אם הן מתגלות הדבר אינו מתפרסם, ניתן להניח שסין מפעילה מבצעי סייבר נוספים. קשה לדעת מה מתרחש בדיוק בחברות מותקפות. אחת האפשרויות היא שהותקנה בהן דלת אחורית שונה מאלה שבהן נעשה שימוש לצורך שימור הנגישות וזו עלולה להיות מופעלת, לפי החלטה, כדי לפגוע בתשתית התקשורת הרלוונטית. יתֵרה מזו, דלת אחורית הנמצאת במצב רדום כמעט בלתי ניתנת לגילוי בטכנולוגיות ההגנה הקיימות כיום כמו תוכנות האנטי וירוס השונות.[46]

המשמעות של הדברים חמורה במיוחד בהקשר של ארצות־הברית שבה אינה רווחת הפרדה פיזית של רשתות התקשורת, כלומר, רווח שימוש באינטרנט "אזרחי"[47] גם במערכות המחשוב במתקנים ובארגונים רגישים, ואף בתשתיות לאומיות קריטיות כמו כורים גרעיניים לייצור חשמל ומערכות הבקרה של תשתיות התחבורה. זאת ועוד – בחלק מן המקרים עושה המערכת הביטחונית של ארצות־הברית שימוש נרחב בתשתיות האינטרנט האזרחיות, והפרדת הרשתות של מערכים מבצעיים רגישים אינה מפותחת דיה. זוהי חולשת אבטחה מהותית המאפשרת לתוקפים נגישות רבה לתשתיות האלה באמצעות תקיפה של מערכים אזרחיים פחות מוגנים. משמעות הדבר היא יצירת יכולת לשבש באופן חמוּר ביום פקודה את תהליכי העברת המידע. בשל החולשה הזאת, פגיעה מקדימה בתשתיות התקשורת והטלפוניה בעת עימות עלולה לשבש מערכים מבצעיים וביטחוניים המבוססים על התשתיות האלה.

המענה לחולשה הזאת מחייב תפיסה מערכתית כוללת, ולא ניתן להסתפק בניסיונות לשפר את ההגנות על ספקי תשתיות התקשורת כדי לנסות למנוע תקיפות בעתיד. השימוש ברשת האינטרנט לצורך תקשורת של מערכות רגישות אינו יכול להתבסס אך ורק על הרשאות גישה. מוגנות ככל שיהיו, ההרשאות האלה הן פרצה משמעותית בהגנה. אחד המרכיבים החשובים במענה לחולשה שתוארה

נוגע לבידול שבין רשתות תקשורת. מוצע לבודד את הרשתות המבצעיות של מגוון מערכות קריטיות – מערכות ביטחוניות, מערכות תקשורת מבצעית ומערכות פיקוד ובקרה של מתקנים המוגדרים תשתיות לאומיות קריטיות. היכולת להפעיל מערכות בקרה של מתקנים חיוניים באמצעות רשת האינטרנט עלולה להתגלות כאבן נגף ברגע שבו יחליט תוקף מתוחכם להפעיל דלתות אחוריות ביום פקודה.

הערות

1 Steve DeWeese, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, Northrop Grumman, October 9, 2009, p. 67.

2 Kenneth Lieberthal and Peter W. Singer, *Cybersecurity and U.S.-China Relations*, The Brookings Institution, February 2012.

3 ראו: מתקפה על חברת מיצובישי ביפן באוגוסט 2011, Hiroko Tabuchi, "U.S. Expresses Concern About New Cyberattacks in Japan", *New York Times*, September 21, , 2011. http://www.nytimes.com/2011/09/22/world/asia/us-expresses-concern-over-cyberattacks-in-japan.html?_r=1

4 *Chinese 'hacked French ministry for G20 data'*, *The Week, 8* Mar 2011, http://www.theweek.co.uk/technology/7229/chinese-%E2%80%98hacked-french-ministry-g20-data%E2%80%99

5 Erik Helin, "Fingers Point to China in Australian Prime Minister Hack", *Brick House Security*, March 30, 2011, http://blog.brickhousesecurity.com/2011/03/30/australia-pm-hack

6 ראו על תקיפת אתרי ממשל בקנדה: Greg Weston, "Hackers Attack Canadian Government", CBS News, February 16, 2011, http://www.cbc.ca/news/politics/story/2011/02/16/pol-weston-hacking.html

7 David Sanger and John Markoff, "IMF Reports Cyberattack Led to 'Very Major Breach'", *New York Time,* June 11, 2011, http://www.nytimes.com/2011/06/12/world/12imf.html

8 Nathan Thornburgh, "Inside the Chinese Hack Attack", *Time (US)*, August 25, 2005, http://www.time.com/time/nation/article/0,8599,1098371,00.html

9 Dimitri Alperovitch, *Revealed: Operation Shady RAT*, Version 1.1, McAfee, 2011, http://blogs.mcafee.com/mcafee-labs/revealed-operation-shady-rat

10 .DeWeese, 2009, p. 69.

11 Integrated Network Electronic Warfare

12 Tim Stevens, "Breaching Protocol – The Threat of Cyberespionage," *Jane's Intelligence Review*, March 2010, pp. 8-13.

13 Timothy L. Thomas, "Chinese and American Network Warfare", *Joint Forces Quarterly*, Vol. 38, p. 76. http://www.dtic.mil/doctrine/jel/jfq_pubs/1538.pdf

14 DeWeese, 2009, p.31; Mark A. Stoke, Janny Lin and L.C. Russell Hsiao, *The Chinese PLA Signal Intelligence and Cyber Reconnaissance Infrastructure,* Project 2049 Institute, November, 2011. pp. 6-14.

15 קיים קושי לאמת את ההערכה הזאת.

16 James Mulvenon, "PLA Computer Network Operations: Scenarios, Doctrine, Organizations and Capability", in: Roy Kamphausen, David Lai, and Andrew Scobell (eds.), *Beyond the Strait: PLA Missions Other Than Taiwan*, Washington, DC: National Bureau of Research, 2009, p. 273.

17 **שם.**

18 פצחן – Hacker, במנדרינית 黑客 Hēikè – מילולית "אורח שחור".

19 .Stevens, March 2010, pp. 8-13

20 Timothy L. Thomas, "Comparing US, Russian and Chinese Information Operations Concepts", Foreign Military Studies Office, Fort Leavenworth, KS 66048, February 2004, pp. 12-13.

21 Thomas Rid, "Think Again: Cyberwar - Don't fear the digital bogeyman. Virtual conflict is still more hype than reality", *Foreign Policy*, March 2012, http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?page=0,6

22 ראו פרסומים על ריגול הסייבר הסיני נגד הממשלה הטיבטית הגולה ופריצה לתשתית המחשב של הדלאי לאמה:. Stevens, 2010, pp. 8-13

23 בהקשר של המאמר הזה המונח מתאר את היכולת להונות את בעל המחשב המותקף תוך יצירת מצג המתאים לפרופיל שלו, כדי שיבצע פעולות שבהן התוקף מעוניין; לדוגמה, יגיב לדואר אלקטרוני המופנה אליו באופן מנוגד למדיניות האבטחה של הארגון שבו הוא עובד.

24 .Steve DeWeese, 2009, p. 60

25 Eric Chien and Gavin O'Gorman, *The Nitro Attacks, Stealing Secrets from the Chemical Industry*, Symantec Security Respond, 2011, www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf

26 ייתכן שלא היה קשר בין פריצה לחשבונות gmail של פרטים לבין התקיפה להשגת קוד המקור של google ו־Adobe.

27 Ariana Eunjung Cha and Ellen Nakashima, "Google China cyberattack part of vast espionage campaign, experts say", *Washington Post,* January14, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html

28 McAfee Labs and McAfee Foundstone Professional Services, *Protecting Your Critical Assets, Lessons Learned from "Operation Aurora",* http://www.mcafee.com/us/resources/white-papers/wp-protecting-critical-assets.pdf

29 קובצי לוג (log files) הם קבצים המתעדים באופן רציף ואוטומטי פעילות מוגדרת במחשב.

30 Alperovitch, 2011, p. 3. http://blogs.mcafee.com/mcafee-labs/revealed-operation-shady-rat

31 "Hackers attack Norway's oil, gas and defence businesses", BBC News, November 18, 2011, http://www.bbc.co.uk/news/technology-15790082

32 בוטנט הוא אוסף של סוכני תוכנה המותקנים במחשבים מארחים. במקרים רבים אלה הם מחשבים נגועים שהודבקו בסוכן התוכנה ללא ידיעת בעל המחשב. סוכני התוכנה יכולים להיות מופעלים בכפוף לתנאים קבועים מראש או על־ידי פקודות משרת שליטה.

33 Brian Kerbs, *Who Else Was Hit by the RSA Attackers*, October 2011, http://krebsonsecurity.com/2011/10/who-else-was-hit-by-the-rsa-attackers

34 Uri Rivner, *Anatomy of an Attack*, April 1, 2011, http://blogs.rsa.com/rivner/anatomy-of-an-attack

35 חולשות ZeroDate הן פרצות אבטחה בתוכנות המזוהות ומפורסמות ברבים. עם הפרסום ניתן בדרך־כלל מענה על־ידי המפתח טלאי תיקון המופץ ברבים. בדרך־ כלל עובר זמן בין הפצת טלאי התיקון עד להתקנתו במחשבי המשתמשים. חלון ההזדמנויות לתוקף הנו הזמן שבין פרסום החולשה לבין הזמן שבו מותקן טלאי התיקון במחשב היעד. בזמן הזה יכול התקף להחדיר קוד מפגע דרך אותה פרצה.

36 סמוך לנובמבר 2010 חלק ממחשבי החברות המותקפות כבר התקשרו לרשתות השליטה של התוקפים.

37 אחת החברות שהותקפו תוך שימוש במידע שהושג בתקיפת RSA הייתה לוקהיד מרטין – ראו: Mathew J. Schwartz, "Lockheed Martin Suffers Massive Cyberattack", *Information Week*, May 31, 2011, http://www.informationweek.com/news/government/security/229700151

38 בארגונים גדולים מותקנות בדרך־כלל מערכות המנטרות את התעבורה ברשת המחשבים כדי לאתר התנהגויות שאינן מקיימות את החוקים שהוגדרו מראש. למערכות האלה יש כמה שמות מקובלים כמו: SEIM – Security Event and Information Management או: NBA – Network Behavioral Analysis. בתוכנות האלה קיים מערך חוקים שמטרתו להתריע על פעילות לא מורשית או לא שגרתית ברשת וכן למנוע אותה.

39 Stephen Doherty et al. *The Sykipot Attacks,* December 14, 2011, http://www.symantec.com/connect/blogs/sykipot-attacks

40 Mathew J. Schwartz, "More Sykipot Malware Clues Point To China", *Information Week,* April 17, 2012, http://www.alvandsolutions.com/index.php?option=com_content&view=article&id=457%3Amore-sykipot-malware-clues-point-to-china&Itemid=136

41 Mathew J. Schwartz, "More Sykipot Malware Clues Point To China", *Information Week*, December 21, 2011, http://www.informationweek.com/news/security/attacks/232300940

42 2011 Kerbs, October.

43 Nicholas Hoover, "NSA Chief: China Behind RSA Attacks", *Information Week*, March 27, 2012, http://www.informationweek.com/news/government/security/232700341

44 Internet Service Provider.

45 Stew Magnuson, "Cyber Experts Have Proof That China Has Hijacked U.S.-Based Internet Traffic", *National Defense*, December 11, 2010 http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=249

46 Gunter Ollmann, *Serial Variant Evasion Tactics Techniques Used to Automatically Bypass Antivirus Technologies*, Damballa, 2009, http://www.damballa.com/downloads/r_pubs/WP_SerialVariantEvasionTactics.pdf

47 המונח אינטרנט אזרחי מציין תשתיות תקשורת אינטרנט שבהן עושה שימוש הציבור הרחב ושאין להן הגנה מיוחדת.

פשע קיברנטי – סכנה לביטחון הלאומי?

ליאור טבנסקי

מבוא

המרחב הקיברנטי, שנוצר עם התפתחות טכנולוגיות המחשבים והתקשורת הדיגיטלית, נכנס בעשורים האחרונים לחיינו. התקשוב מיושם לשיפור ולייעול תהליכי העבודה, הלמידה והבידור, והוא משפיע על דפוסי הפעולה כמעט בכל תחומי הפעילות האנושית. רשת האינטרנט נעשתה מסחרית ב־1988 והפכה לנדבך משמעותי במרחב הקיברנטי. היא מאפשרת נגישות זולה ומיידית לסוגים שונים של מידע, לשיתוף ידע, לעבודה משותפת מרחוק ועוד.

השלכות הפשע הקיברנטי על הביטחון הלאומי נגזרות מאופי השימוש בטכנולוגיה על ידי גורמים בעלי מניעים עוינים. המאמר מציע בחינה מוכוונת־מדיניות של משמעויות הפשע הקיברנטי והשפעתו על הביטחון הלאומי, מבלי להתבסס על הערכות כספיות של היקף הנזקים של הפשע הקיברנטי. המאמר מתאר את שיתוף הפעולה בין עבריינים, 'הפשע המאורגן' וארגונים עוינים, ודן במסחור של יכולות התקיפה הקיברנטיות, המתאפשר עם התפתחות הטכנולוגיה וצמיחת "השוק השחור" לשירותי מחשוב. יש הטוענים שהפשע הקיברנטי אינו מהווה כיום איום על הביטחון הלאומי, אולם, המאמר מזהה שני תנאים נפרדים שאם יתמלאו, הפשע קיברנטי עלול להפוך לאיום על הביטחון הלאומי.

הדרישה הציבורית לביטחון במרחב הקיברנטי עולה עם עליית המודעות לאיומים. גם ללא עלייה אובייקטיבית בהיקף הפשיעה, אין להניח שדרישה זו תצטמצם. אחריות המדינה לאזרחיה אינה נעצרת במרחב הקיברנטי, וגם בתחום זה יש להגדיר את ביטויה המעשי במסגרת תהליך פוליטי דמוקרטי, על יסוד עובדתי מוצק.

תופעת הפשע הקיברנטי

טכנולוגיות ממוחשבות מיושמות למטרות שינוי וייעול תהליכי הייצור והעבודה בכל תחומי החיים, והן לא פסחו על עולם הפשע. המחשוב מאפשר פירוק משימות

ליאור טבנסקי הוא חוקר בתכנית לוחמת סייבר במכון למחקרי ביטחון לאומי.

מאמר זה ראה אור לראשונה ב**צבא ואסטרטגיה**, כרך 4, גיליון 3, דצמבר 2012, עמ' 103-118.

ליחידות קטנות וביזור העיבוד; הרישות מאפשר גישה גלובלית למידע, והתמקדות בידע כמוצר בעל־ערך. ההגדרה המוצעת לפשע הקיברנטי היא:

שימוש במרחב הקיברנטי למטרות אסורות, תוך ניצול התכונות המיוחדות המאפיינות את המרחב הקיברנטי הקיים, כגון: מהירות ומיידיות, הפעלה מרחוק, הצפנה והסוואה שתורמות לקושי בזיהוי הפעולה והמפעיל, ניצול הערך העולה של המידע הדיגיטלי לסוגיו וטיפול חוקי ומשפטי משתנה במרחב הקיברנטי במדינות שונות.

הדיון בהגדרות של תופעת הפשע הקיברנטי ממשיך להתפתח. לפני למעלה מעשור תהה גרבוסקי, מה חדש בפשע הקיברנטי: האין אלה תופעות ותיקות שעושות שימוש בכלים חדשים?[1] אולם רוב החוקרים מנסים לנתח את הפשע הקיברנטי כתופעה ייחודית. מאג'יד יאר מסווג את תופעות הפשע לפי האובייקט הנפגע: נגד רכוש, אדם, מדינה.[2] שינדר וקרוס מבחינים בין העבירות לפי מידת האלימות: פשע אלים ואלים פוטנציאלי, בלתי־אלים (סחר בסמים, הלבנת הון) ופשע שעדיין נתפס "צווארון לבן" (פריצה למחשבים, גניבה והונאה).[3] לפי ההגדרה של וול – "the transformation of criminal or harmful behavior by networked technology"[4] – הפשע הקיברנטי התפתח בעקבות צמיחת התקשוב והמרחב הקיברנטי והאפשרויות החדשות להשגת מידע, לשיבושו או ליצירת מניפולציה של מידע למטרות רווח. נוסף לכך ממיין וול את עבירות הפשע הקיברנטי לשלושה טיפוסים: עבירות הנוגעות לשלמות ולתקינות מערכת המחשב (Hacking – פריצה למערכות), עבירות שמסתייעות במרחב הקיברנטי (תקשורת מוצפנת בין עבריינים, מכירת תרופות מזויפות) ועבירות הנוגעות לתוכן המידע הממוחשב (גניבת סודות, הפצת תוכן פוגעני). ניתן גם למיין את העבירות לפי תפקידו של המחשב.[5] גם "האמנה האירופית נגד הפשע הקיברנטי" מאמצת גישה דומה.[6]

המחשב כאמצעי לביצוע עבירה		
גישה לתוכן והפצתו: סודות ידע תוכן פוגעני	שיבוש המידע או המערכת בכוונת זדון גניבת זהות הונאה	שימוש בתקשורת הטרדה סחר בחומר אסור דוא"ל זבל

המחשב כמטרה של העבירה			
גישה לא מורשית:	החדרת קוד זדוני:	שיבוש של פעילות:	גניבה של שירות:
Hacking (פצחנות)	נוזקות, רוגלות, וירוסים	DDoS (מניעת שירות מבוזת)	שימוש בלתי־ מורשה

חלק ניכר מהפשיעה הקיברנטית אינו מהווה תופעה ייחודית או חדשנית: הטרדה, הונאה, תעמולה אסורה, פורנוגרפיה, גניבה, הלבנת הון, ריגול ועוד. בעבירות הללו נעשה שימוש במרחב הקיברנטי. הנדבך הנוסף הוא תופעות שכמעט

לא היו בנות־ביצוע לולא המרחב הקיברנטי: דוא"ל זבל, הונאת קליקים (Click fraud), תוכנות זדוניות (Malware) לסוגיהן, רשתות מחשבים שבויים (Botnet),[7] גניבת זהות דיגיטלית, הסוואה והצפנה[8] של מידע ותקשורת, חדירה ממחושבת למתקנים ממוגנים בעלי ערך רב וריגול אוטומטי מתמשך בארגונים מאובטחים, המוציא קניין אינטלקטואלי משליטתם.

פשיעה על כל סוגיה היא תופעה חברתית נפוצה. הסברים קרימינולוגיים לתופעה משלבים הנעה, הזדמנות, וקיומו של "שומר". ניתן לזהות שני סוגי מקורות להנעה האנושית לפעולה.[9] חלק ניכר מהמניעים להתנהגות עבריינית הנם אישיותיים־פנימיים (Intrinsic Motivation), והם אינם נקבעים בתהליך בחינה של שיקולי עלות־תועלת. אין סיבה להניח שבעקבות שימוש מוגבר בטכנולוגיה זו או אחרת, תשתנה ההתנהגות האנושית. לפיכך, אין זה מפתיע שבני־האדם משתמשים גם במרחב הקיברנטי למילוי צורכיהם ולרדיפה אחר מטרותיהם, הן באפיקים הנורמטיביים כגון לימודים, בידור, השכלה ועבודה, והן בפעולות האנושיות הוותיקות, כגון לחימה ופשע. האסכולה הקלאסית בקרימינולוגיה מתבססת על רעיון הבחירה החופשית והערכה מושכלת של תועלת צפויה בהתחשב בסיכוי להיענש, ומפרשת את ההנעה לביצוע עבירה כהחלטה כלכלית־מושכלת.[10] כלכלנים ופסיכולוגים עוסקים בניתוח ההתנהגות האנושית, כולל העבריינות, כנגזרת של שיקול עלות־תועלת מושכל. מכלול הנסיבות החיצוניות המשתנה יכול לעודד פשיעה קיברנטית: הדבר קורה כשאדם מזהה פוטנציאל גדל לרווח ומעריך שהמחיר – הסיכוי לענישה – נמוך מהתועלת הצפויה. הרחבת החיבוריות הדיגיטלית לצד עליית ערך המידע הממוחשב גורמות למצב שבו עולה ההנעה החיצונית (Extrinsic Motivation) להתנהגות עבריינית. בעוד מנגנוני אכיפת חוק מסודרים קיימים במדינות המפותחות, במרחב הקיברנטי החדש לא הדביקה תגובת המדינה את קצב השינוי הטכנולוגי. דוגמה טובה היא שוד בנק "מסורתי" לעומת גניבה ממוחשבת. האפשרות "המסורתית" לשוד כספים מסניף בנק כרוכה בהתגברות על מערכי האבטחה, ובסיכוי סביר להיקלע לעימות עם שומרים חמושים. גם אם השוד עצמו יסתיים בהצלחה, לאורך השנים נרדפים השודדים על ידי רשויות החוק. עם התפתחות המרחב הקיברנטי התאפשר ניצול של פגיעותו גם לגניבה מבנקים. למשל, נפוץ השימוש ברשתות בנות אלפי מחשבים שבויים (Botnet)[11] לגניבה מתמשכת של פרטי הזדהות לאתרי בנקאות, ושימוש בהם לגניבת סכומי כסף קטנים. לנוכח בעיית וידוא הזהות (Attribution) במרחב הקיברנטי, הסיכוי לזיהוי הפושע נמוך מאוד.[12] המוסדות הפיננסיים מודעים לסיכון העסקי הברור, ויחד עם מוסדות ההסדרה נוקטים אמצעי הגנה ומשקיעים בתחום אבטחת המידע, כדי לצמצם את מרחב ההזדמנויות לשודד הקיברנטי. עם זאת, הסיכון הפיזי המיידי מבחינת הגנב הקיברנטי עדיין נמוך מזה של שודד "מסורתי".

היקף הפשע הקיברנטי ונזקיו: הערכות בעייתיות

תופעת הפשע הקיברנטי נבחנת בדרך כלל בפרספקטיבות משפטיות (חקיקה וענישה), קרימינולוגיות (מניעים וארגון), כלכליות (תמריצים וערך) או טכניות (אבטחת מידע). משפטנים עוסקים בהצבת גבולות להתנהגות מקובלת ובסוגיות חוקיות של מניעה ואכיפה. קרימינולוגים מיישמים את הידע המקצועי להבנת התופעות החדשות. כלכלנים מתארים את מערכת התמריצים המשפיעים על תהליכי קבלת ההחלטות של שחקנים רציונליים. אנשי אבטחת מידע עוסקים בסוגיות טכניות של התשתית הטכנולוגית: תוכנה, חומרה ותקשורת, תוך התמקדות בפגיעויות השונות ובדרכי ההתגוננות. משפטנים, כלכלנים ואנשי אבטחת מידע שותפים לדעה שהיקף הפשיעה הקיברנטית ועוצמת הנזק שלה נמצאים בעלייה מהירה ומתמשכת. ההערכה נסמכת על העובדה שהיקף המידע הדיגיטלי גדל בקצב מעריכי, והחיבוריות של התקנים ממוחשבים מתרחבת אף היא. המרחב הקיברנטי מכיל מידע רב יותר, עם נקודות גישה פוטנציאליות רבות יותר לחדירה בלתי־מורשית. המסקנה היא שכל חדירה (Breach) חושפת היקף הולך וגדל של מידע.

הערכות כספיות של היקף הנזק של הפשע הקיברנטי מתפרסמות מאז שנות התשעים ועד היום. חברות האבטחה מובילות את המחקר בנושא, ומפרסמות דוחות למכביר. קיימות עשרות הערכות שונות, שמקורן במגזר העסקי והממשלתי בארצות־הברית, בבריטניה, ובמדינות מפותחות נוספות.[13] סקר של הבולשת הפדרלית (FBI) העריך את הנזק לעסקים אמריקאיים ב־65 מיליארד דולר בשנת 2005.[14] שר המסחר האמריקאי, גארי לוק, טען שהנזק השנתי לחברות אמריקאיות כתוצאה מזיוף ופיראטיות (שימוש בלתי־חוקי בקוד מחשב) עומד על 200–250 מיליארד דולר.[15]

דו"ח בריטי מציג תג מחיר של 27 מיליארד ליש"ט לשנה: הנזק השנתי לאזרחי בריטניה הוערך ב־3.1 מיליארד ליש"ט, למגזר העסקי 21 מיליארד ליש"ט ולממשלת בריטניה – 2.2 מיליארד ליש"ט נוספים.[16] בדו"ח של חברת סימנטק, מהמובילות בשוק אבטחת המידע, נאמד הנזק הכספי הישיר שגורם הפשע הקיברנטי ב־114 מיליארד דולר בשנה ב־24 מדינות.[17] הערכות נוספות נוקבות בסדר גודל של מאות מיליארדי דולרים בשנה.[18]

סכומי עתק אלה עוררו תהיות וספקנות, אולם השפעת הביקורת עד כה הייתה מוגבלת. לאחרונה פורסם נייר עמדה מאת שני חוקרים מחברת מיקרוסופט, שמנתח את התשתית הסטטיסטית הרעועה שביסוד הערכות הנזק של הפשע הקיברנטי, הנעשות באמצעות סקרים.[19] כיצד נוצרו ההערכות הללו? בחינה של שיטות המחקר מגלה באיזו קלות נוצרת הערכת־יתר של היקף הנזק. ראשית, חסר מידע על השימוש שנעשה (או לא נעשה) במידע שנחשף. ספורים המקרים שבהם

קיים מידע מוצק, בעוד היקף הנזק הפוטנציאלי הוא רחב. נניח שנפרץ מחשב שבו קובץ מאגר מידע המכיל אלף רשומות. נניח גם שמאגר המידע אינו מוצפן, והרשומות שבו כתובות בשפה טבעית. כל רשומה בקובץ מייצגת כרטיס אשראי תקף, על כל הפרטים הדרושים לשימוש בו: מספר, מספר CVV,[20] תוקף, שם, מס׳ תעודת זהות וכתובת הבעלים, וכן פרטי חשבון הבנק המנפיק. במצב זה הגנב רואה תמונה מלאה ואמיתית של המידע בקובץ, אולם גם במצב האופטימלי, הגנב אינו יכול להעריך את מלוא המשמעויות הכלכליות של המידע שהשיג. האם הפורץ יכול להעריך נכונה את הערך האמיתי של המידע שגנב? האם הקורבן, הנפרץ, יכול להעריכו כראוי? בגניבת קניין אינטלקטואלי – תוצר של מחקר ופיתוח, הקורבן נוטה לזהות כנזק של גניבת המידע את הרווח המרבי שהיה רוצה לקבל בתום תהליך הפיתוח, הייצור והשיווק. השימוש בסקר – שיטה המתאימה לבירור תופעה שקשה לצפות עליה וכן לגילוי היסטוריה של הנסקרים – הוא הדרך העיקרית ללמוד על היקף הנזק. הסקר מאפשר להגיע למספר גדול ומגוון יותר של משיבים המספקים הערכות משלהם לכמות האירועים והנזק, אך לשיטת הסקר יש גם מגרעות משמעותיות, המעסיקות אנשים מתחום מדעי החברה וסטטיסטיקאים.[21]

שנית, בהעדר מידע מספיק, משתמשים בשיטות סטטיסטיות כדי להגיע להערכה על בסיס פרטי מידע ספורים. בעיות המדידה קיימות בכל תחומי הדיון באיומים הקיברנטיים, והן בולטות במיוחד כשמנסים לסייע לדיון על ידי כימות הנזק בערכים כספיים. קיים קושי מהותי בהערכת הנזק, ועד כה נראה כי ההערכות הכספיות – שנוצרות בהפעלה גסה של שיטות הסטטיסטיות כדי להציג השערה על סמך נתונים מעטים – מובילות להערכות־יתר. נוסף לסוגיות של מהימנות שיטות המחקר, אמינות מקורות המידע והתאמת השיטה הסטטיסטית למחקר, קיימת בעיה נוספת. ההערכות הכספיות כוללות לרוב גם מרכיבים עקיפים של נזק. הערכות כספיות כוללות פגיעה במוניטין של הארגון שסבל מפריצה, השפעות שליליות על התנהגות הצרכנים עם השלכות מאקרו־כלכליות, סוגיות של דיני נזיקין, ביטוח, הוצאות נלוות ועוד.

שאלות מרכזיות בהבנת התופעה נותרו ללא מענה ברור: האם כדאי להעריך את הנזק על פי השימוש שבוצע בפועל במידע, במקום על פי הפוטנציאל המרבי? אולי צריך להתייחס לערך הכספי של יצירת המידע, במקום להערכת מחירו בשוק – כעת או בעתיד? ומה בדבר העלויות הנדרשות לאבטחה וחזרה לתפקוד תקין? תמונת המצב שעולה מתוך המקורות המקובלים אינה מהימנה, והנזק של הערכת־היתר עלול להתבטא ביצירת תגובת־נגד: זלזול בכוחו של הפשע הקיברנטי. ביסוס הדיון בפשע הקיברנטי על הערכות הנזק הכספיות פוגע בדיון מושכל בבעיה, וביכולת לעצב מדיניות ציבורית הולמת.

שיתוף פעולה בין עבריינים לבין גורמים עוינים

הממשק בין עבריינים "מקצועיים" והפשע המאורגן לבין ארגוני טרור אינו חדש. גם אם נתבונן רק במציאות החיים הישראלית, נזהה ששיתוף הפעולה מהסוג האמור גורם נזקים ברמה הלאומית. מאז שנת 1996 התנהל המאבק התקשורתי ברכישת "דיסקים צרובים" תוך טענה שהרווח מופנה למימון טרור פלסטיני,[22] כחלק מקשר אמיץ בין שירותי הלבנת הון לבין צרכנים כמו ארגוני הטרור.[23] תופעה ענֵפה של גניבת מכוניות מישראל לשטחי יהודה ושומרון ליוותה את "החוויה הישראלית" לאורך שנים ארוכות. הבעיה כמעט לא טופלה ברמה הלאומית, שכן האיום לא נתפס כבעיה ביטחונית: הנזק כוסה בידי חברות הביטוח וגולגל בהדרגה אל המבוטחים, המשטרה לא פעלה מחוץ לגבולות הריבונות הישראלית והצבא – שהפעיל מחסומים ביטחוניים קבועים על צירי תנועה ראשיים – בחר להימנע מעיסוק בפושעים ה"פליליים". בתקופת "אינתיפאדת המתאבדים" חל שינוי בדרכי הפעולה של אותם פושעים פליליים: ארגוני הטרור גייסו את מומחיותם של גנבי הרכב הפלסטיניים כדי להשתמש במכוניות עם לוחיות ישראליות לתעבורה, וגם כדי למצוא נתיבים לחדירת מעגלי האבטחה ולהובלת אמצעי לחימה ומחבלים מתאבדים ללב הערים.

אפשרויות המעבר בין רצועת עזה לישראל מוגבלות יותר מאשר ביהודה ושומרון. חפירת מנהרות לכיוון רפיח המצרית נועדה לספק נתיבי הברחה לצרכים שונים. עסקי ההברחה יוצרים רווח כספי גדול לחופרי המנהרות ולמפעיליהן, והתעשייה מתקיימת למרות מאמצי הסיכול הישראליים. המנהרות הפכו לבעיית ביטחון לאומי עקב הברחת אמצעי לחימה וחומרים שונים מחצי־האי סיני לרצועת עזה, והברחת מחבלים מהרצועה לסיני.[24] המומחיות של ארגוני הפשע בחפירת מנהרות אפשרה את המתקפה ליד כרם־שלום ב־25 ביוני 2006, שבה נהרגו שני חיילים וחייל נוסף נחטף לשבי חמאס. במקרה זה, המומחיות הטכנית של חופרי המנהרות נוצלה בבירור לפגיעה בביטחון הלאומי של ישראל.

חלק מהבדואים בסיני מתפרנסים ממומחיותם כנווטים בשטח, ומספקים לאורך עשרות שנים "שירותי הברחה" לתוך מדינת ישראל. "הסחורה" המוברחת כללה בעבר הלא־רחוק מאות נשים עבור תעשיית המין וסמים. בשנים האחרונות מוברחים אלפי אפריקאים לגבול ישראל. יש הטוענים שאלה מהווים אתגרים משמעותיים, אבל לא בעיה אמיתית לביטחון הלאומי. אולם, הערכה זו משתנה ככל שהמומחיות של המבריחים משמשת לביצוע מתקפות טרור על ישראל.[25] הברחת מחבלים מעזה דרך סיני לישראל אפשרה את פיגוע הטרור בכביש 12 ב־18 באוגוסט 2011, שם נרצחו שמונה ונפצעו ארבעים ישראלים. הברחת המחבלים ואמצעי הלחימה הכניסה את העיר אילת לטווח של ירי רקטות.[26] ההברחות הללו מסַכנות בצורה ברורה ומיידית את הביטחון הלאומי.

בחינה מחודשת של משמעות הפשע הקיברנטי

אם נתבונן עתה בפשע הקיברנטי, נגלה שגם כאן קיים שיתוף פעולה מסחרי דומה. בשנים האחרונות התפתח "שוק שחור" של מומחים טכניים ו"רועֵי" רשתות מחשבים שבויים, המפתח ומספק כלים ושירותים טכניים בתשלום.[27] השוק השחור של שירותי הסייבר Crimeware as a Service (CaaS) גורם נזקים כלכליים במדינות המפותחות, אף שהערכות הנזק הכספיות הנפוצות מוּטות מאוד כלפי מעלה.

מי שמעדיף לפעול בכוחות עצמו ואין בידיו משאבי מחקר ופיתוח מגלה שכלי נשק קיברנטיים (חבילות תוכנה זדוניות – toolkits)[28] זמינים לכול בהורדה מהאינטרנט, לרוב בתשלום של עשרות עד אלפי דולרים. הידע הוא מוצר בלתי־נדלה; כך, שיתוף האחר ביכולות שהיו זמינות לך אינו פוגע בעוצמתך.[29] על רקע זה נוצר המצב שבו כלים עוצמתיים זמינים לכל דורש בעלות שולית. הרושם הנפוץ – שהמרחב הקיברנטי מקל גריפת רווח מפעילות עבריינית – לא נעלם מארגוני הפשע.[30]

צמיחת כוח המחשוב ופריסת רשת האינטרנט אפשרו אמצעי חדש לביצוע פשיעה קיברנטית רחבת־היקף: רשתות של מחשבים שבויים "Botnet . זהו מקבץ של מחשבים אישיים המחוברים לרשת, שהושתלה בהם תוכנה זדונית המאפשרת שליטה מרחוק ביכולות המחשבים הללו, וזאת מבלי לגרום לשיבוש פעולתם התקין. "הדבקת" המחשבים המחוברים לאינטרנט נעשית באמצעות ניצול פרצות ידועות – שהמשתמשים ומנהלי המערכות לא טיפלו בהם – להחדרת תוכנה זדונית. עקב ההיצע הגבוה, מחיר השימוש ב־Botnet נגיש כמעט לכול: חברת **מק'אפי** העריכה ב־2007 שכ־5% מהמחשבים האישיים המחוברים לרשת בעולם הם מחשבים שבויים.[31]

אחת התופעות החדשות היא Advanced Persistent Threat (APT), או Adaptive Persistent Attack (APA)[32] – שימוש מורכב ורב־שלבי בכלי נשק קיברנטיים לביצוע משימות מתמשכות וסמויות. התוקף אינו פועל בהיקף רחב כדי לנצל פגיעויות מוכרות, אולם היעד מוגדר היטב. התוקף משתמש במגוון של כלים התפורים למשימה, חלקם ייחודיים. תקיפה כזו מורכבת משלבים רבים, ויכולה להימשך לאורך חודשים ושנים. התוקף מתחיל באיסוף מודיעין על המבנה הארגוני של המטרה, וזיהוי בעלי־תפקידים בכירים שיש להם הרשאות גישה למרב המידע בארגון. איסוף המידע האישי נעשה תוך שימוש בפרטים גלויים ושיתוף המידע הפרטי ברשתות החברתיות. לאחר זיהוי אנשי המפתח, נעשה מהלך ממוקד כדי להדביק אותם. אחת השיטות היא SpearPhishing: החדרת 'סוס טרויאני' באמצעות הודעת דוא"ל ממוקדת, משולֵח מהימן ועם תוכן רלוונטי, שחודרת את מנגנוני הסינון על ידי שימוש במידע האישי שנאסף. פתיחת ההודעה מאפשרת החדרת 'סוס טרויאני': נוֹזקה לגישה מרחוק Remote

Access Tool (RAT) למשאבי המחשוב בארגון, על ידי יצירת תקשורת ממחשב מורשה ברשת הפנימית. עם השגת הגישה, הפושע הממוצע פועל במהירות כדי להשיג מידע בעל־ערך ולממש אותו. לא כך בהתקפת APA, כשהמטרה היא גישה סמויה לאורך זמן, תוך התעלמות מפיתויים כספיים מיידים. ההתקפה נמשכת לאורך זמן רב, בין היתר, כדי להתגבר על מערכות למניעת דלף המידע. במהלך ההתקפה נעשות בדיקות לזיהוי סף התגובה של המערכת, ובמידת הצורך המידע הנגנב נחלק למנות קטנות, מוסווה בתוך תקשורת לגיטימית ועובר מבלי לגרות את מערכות ההגנה. ההתקפה הממוקדת נדירה יותר ממתקפות סטטיסטיות, שכן היא יקרה באופן ניכר: APA מצריכה איסוף מודיעין שיטתי, יכולת תכנון וניסוי ואורך־רוח לביצוע המשימה הממושכת.

בפרספקטיבה כלכלית נוצר מצב שמצד ההיצע, קבוצות ההאקרים (פצחנים) שהצליחו לפתח וליישם כלי תוכנה לשליטה במאות אלפי מחשבים יצרו, למעשה, שירות בעל ערך כלכלי. מצד הדרישה, לקוחות שונים – האקרים אחרים, חוקרים פרטיים, עבריינים, ארגוני ריגול וארגוני פשע גדולים – מצאו שימושים שונים למוצר זה. כך נוצר מודל עסקי Crimeware as a Service (CaaS) – העתק "שחור" של מודל Software as a Service (SaaS), המנחה את תעשיית שירותי המחשוב מאז 2001.[33] ההצדקה הכלכלית של המודל ברורה: מעתה, הלקוח אינו נדרש לרכוש ציוד מחשב כדי להשתמש בשירותי מחשב. הלקוח יכול לרכוש רק את השירות המדויק שהוא זקוק לו ממפעילים גדולים, ולהשתמש בו על גבי הרשת, בתקשורת סטנדרטית. המודל עבר גלגולים אחדים במשך השנים, וכיום הוא מוכר בזִמלוּל (Buzzword) 'מחשוב ענן' (Cloud Computing). היקף השוק העולמי לשירותי המחשוב באופן זה מוערך ב 14.5 מיליארד דולר בשנת 2012.[34]

הבה נבחן את תופעת "השוק השחור" מנקודת המבט של ביטחון לאומי. קיומו של "שוק שחור" למכירת אמצעי לחימה קיברנטיים, שירותי פיתוח ומיקור־חוץ גורם לכך שרמת המיומנות הטכנית הנדרשת לכניסה לתחום הפשע הקיברנטי יורדת, שכן הפושע אינו נדרש להחזיק ביכולת לפתח בעצמו את כלי הפריצה ואת שיטות הפעולה. אותה תשתית טכנולוגית דרושה לחדירה ולשימוש בלתי־מורשים במשאבי מחשב, הן אם החדירה נועדה לרווח כספי והן לחבלה.[35] כך מתגלה סיכון נוסף: השימוש בכלים הקיימים למטרות חבלה ופגיעה בתשתיות חיוניות – במקום למטרות הצפויות של הונאה לצורך גניבה ויצירת רווח כספי מהיר – עלול לגרום נזק ביטחוני לאומי. המשך התפתחותם של מנגנוני הפשע הקיברנטי הופך, אפוא, לבעיית ביטחון לאומי. ההגנה על תשתיות חיוניות (CIP) היא הסוגיה החשובה ביותר בתחום הביטחון הקיברנטי, והשוק השחור של אמצעי לחימה קיברנטיים מחריף אותה. המסחור של יכולות טכניות ומבצעיות מאפשר לגורמים רבים – ובהם ארגוני טרור קטנים ואף יחידים – גישה למשאבים

עוצמתיים, שעלולים לשמש ככלי נשק קיברנטיים. קבוצת איומי הייחוס מתרחבת, אפוא, מעבר למדינות ולארגוני הטרור המוכרים, וצריכה לכלול כל גורם שיכול להשתמש בשירותים המסחריים שמציעים ארגוני הפשע הקיברנטי. עם זאת, כשקיימת השקעה מדינתית מתמשכת במחקר ופיתוח, היכולות הטכנולוגיות הרווחות בשוק מפגרות בהכרח אחר הטכנולוגיה שמפתחים בזרועות הביטחון ובאקדמיה. לפיכך, היכולות הזמינות בשוק יהיו פחותות מאלה הזמינות לארגונים מדינתיים בעלי אמצעים של מחקר ופיתוח עצמאיים, שנהנים מגיבוי מדינתי מבחינת משאבים וארגון.

לקראת מימוש אחריות המדינה לביטחון קיברנטי

חוקרים ומעצבי מדיניות זקוקים לביאור המשמעויות של התופעה. ההערכות הכספיות של נזקי הפשע אינן מספקות בסיס מוצק להבנת התופעה ולעיצוב מדיניות. לפיכך נדרשת בחינה של סדרי העדיפויות המיטביים, לנוכח תמונת המציאות ומגוון האילוצים והמגבלות.

גם ללא הסכמה על הערכת הנזק הישיר והעקיף שגורם הפשע הקיברנטי, הוא עדיין משפיע על תפקודם של אזרחים, ארגונים והחברה בכלל. אזרחים ועסקים קטנים נפגעים באופנים שונים מפשע קיברנטי. דוא"ל זבל, הונאות אינטרנטיות, גניבת זהות דיגיטלית, פגיעה בפרטיות, סחיטה, ריגול כלכלי ופגיעה בקניין רוחני ואינטלקטואלי – כולן תופעות נפוצות, שפוגעות מדי פעם בחלק מהאזרחים והארגונים. אף שנראה כי הערכות הנזק מוּטות כלפי מעלה, התפתחות המרחב הקיברנטי מגדילה את היקף הנפגעים הפוטנציאליים, ומרחיבה עוד יותר את מגוון הדרכים שבהן ניתן לבצע פשעים ועבירות נגד אזרחים וארגונים. לאור המודעות העולה בד־בבד עם התרחבות מעשי הפשע, יש להניח שהאזרחים במדינות המפותחות ידרשו שהמדינה תנקוט פעולות על מנת לספק ביטחון אישי וקבוצתי גם במרחב הקיברנטי. החשיפה התקשורתית הגוברת של אירועי אבטחת מידע ומתקפות קיברנטיות מצביעה על עניין גובר בסכנות הפשע הקיברנטי. סביר לצפות להופעת דרישה ראשונית של אזרחים שהמדינה, על זרועותיה, תפעל לספק ביטחון לאומי ואישי גם במרחב הקיברנטי.

המדינה אחראית על החוק והסדר ועל ביטחון אזרחיה, והיא נדרשת לפעול למזעור הנזק לאזרחיה. המדיניות תתפתח מתוך הבנת המשמעויות הרחבות של התופעה, ומתוך דיון ציבורי מושכל. להלן סוגיות אחדות לפיתוח דיון כזה:

רוב התופעות הנפוצות שנכללות בפשע קיברנטי אינן נוגעות לענייני ביטחון לאומי. מה המשמעות של הפצת שנאה ועידוד הסתה נגד היהודים או מדינת ישראל, תוך השחתת אתרי אינטרנט ישראליים, הפצת תעמולה תוך שימוש בשיטות דוא"ל זבל וחדירה לחשבונות פרטיים ברשתות החברתיות, יצירת

סרטונים וקמפיינים ברשת, הפוגעים ברגשות הציבור? האזרחים עלולים לחוש בלתי־מוגנים במרחב הקיברנטי, וכבודם של המדינה ושל רבים מאזרחיה עלול להיפגע כתוצאה מעלילות שווא. ברמה הלאומית, מעבר לתחום המקצועי של יחסי־ציבור, זהו נזק זניח.

מה המשמעות של הונאה נפוצה – גניבת זהות דיגיטלית, ושימוש בלתי־מורשה בפרטים של אמצעי התשלום לגניבת כספי האזרח? כאשר אזרח נופל קורבן לפשע, רשויות המדינה נדרשות וחייבות להתייחס ולטפל בנושא. לרשות המדינה עומד מגוון רחב של דרכי טיפול מערכתיות ופרטניות, ויש לבאר את משמעות האירועים על מנת לבחור מדיניות הולמת. אולם מבחינת הביטחון הלאומי, קשה לראות נזק ברמה הלאומית – כל עוד מדובר בשיעורי פגיעה נמוכים יחסית, גם כשאלה גבוהים משיעור התפוצה של פשע "מסורתי". אם פעילות הפשיעה הקיברנטית תתגבר ותהיה ממושכת ובהיקף רחב, עצם אמונם של האזרחים במוסדות המדינה צפוי להיפגע בשל חוסר יכולתם לספק סביבה בטוחה.

המצב הנוכחי במדינות המפותחות אינו משביע רצון. אם "ציות תמורת הגנה" הוא תמצית החוזה החברתי בין האזרחים למדינה, היא אינה ממלאת את חלקה בחוזה בתחום הפשע הקיברנטי. המענה לאתגרים החדשים מצריך, קודם כול, הבנה ברורה של התופעות ומשמעותן. תהליכי התגובה, יצירת המדיניות ואכיפתה מחייבים עדכוני תקינה וחקיקה. פעולות החקיקה, שמדרך הטבע מפגרות אחר ההתפתחות הטכנולוגית, נמצאות בסמכותה הבלעדית של המדינה. זרועות האכיפה הריבוניות הפועלות בהתאם לתשתית החוקית הלאומית יידרשו להקצות יותר משאבים למניעה, לחקירה ולענישה בתחום הפשע הקיברנטי. על אף אופיו הבינלאומי של המרחב הקיברנטי, המדינה היא הגורם הבלעדי שנושא באחריות לביטחונם האישי של אזרחיה. הסכמים בינלאומיים כגון "אמנת בודפשט – אמנה על פשעי מחשב" של מועצת אירופה[36] והיוזמות המתנהלות באו"ם,[37] בארגון הכלכלות המפותחות[38] ובאיגוד הטלקום העולמי (ITU[39]) – כל אלה מגבירים את שיתוף הפעולה בין רשויות ריבוניות. שיתוף פעולה בינלאומי עשוי לסייע לרשויות ריבוניות להילחם טוב יותר בתופעה, אך לא ניתן לראות בהסכמים בינלאומיים תחליף למדיניות ריבונית עצמאית. ראשית, שיתוף פעולה בין מדינות במערכת הבינלאומית האנרכית אפשרי במידה מוגבלת בלבד, ועל סמך אינטרס משותף. ייתכן שהמדינות הדמוקרטיות המפותחות יצליחו לגבש הסדרים בינן לבין עצמן, אולם הפער בהגדרת האיום ביניהן לבין המדינות הסמכותניות (אוטוריטריות) נראה רחב מדי. הדיון האמריקאי בנושא מתמקד בריגול התעשייתי המתמשך נגד הקניין האינטלקטואלי, פרי המחקר והפיתוח של המגזר העסקי והממשלתי בארצות־הברית. לאורך שנים, גובר החשש של גורמים בכירים בקהילה העסקית והממשלתית מפני אובדן היתרון הכלכלי והאסטרטגי של ארצות־הברית בעולם

כמעצמה מדעית־טכנולוגית חדשנית מובילה. למעשה, 'אובדן' אינו המונח הנכון, שכן הידע אינו הולך לאיבוד אלא נגנב במאמץ מדיני שיטתי, מאורגן ורחב־היקף של סין להזניק את עוצמתה הכלכלית והצבאית באמצעות העתקת סודות המחקר האמריקאי.[40] הדיון בנושא זה עובר בבירור מתחומי הכלכלה, אבטחת המידע או המשפטים לשיח ביטחוני, כמעט לוחמני.[41] סין, מצדה, דוחה האשמות אלו על הסף, ומודאגת מערעור יסודות המשטר הסיני כתוצאה מהשימוש המערבי באינטרנט, בשם ערכי חופש הביטוי.

שנית, הסמכות והריבונות של המדינה בשטחה מאפשרת לקדם מדיניות עצמאית: חקיקת חוקים ואכיפתם אינה תלויה בהסדר בינלאומי. בישראל, האירוע המכונה "פרשת ההאקר הסעודי" מדגים את חריגת הדיון מגבולות אבטחת המידע אל הרמה הביטחונית. בתחילת 2012 פרסם מי שהזדהה כ־0xOmar רשימת פרטים אישיים ומספרי כרטיס אשראי של אלפי אזרחים ישראלים.[42] הפרטים שפורסמו היו ברובם המכריע ישנים, ומתוך כ־380 אלף הרשומות, היו כמה אלפים של מספרי אשראי תקפים. הנזק הישיר שנגרם לבעלי הכרטיסים עומד על אפס: חברות האשראי ביטלו את הכרטיסים והנפיקו חדשים, וממילא, כל שימוש בלתי־מורשה בכרטיס מכוסה בידי החברות. היקף הנתונים שנחשפו גם הוא אינו חריג: מדי יום נגנבות ברשת האינטרנט מיליוני רשומות מסוג זה. הפרטים נארזים לפי פרמטרים שונים, ונמכרים כ־"Dumps" ללקוחות ב"שוק השחור" שתואר לעיל.[43]

התברר שמדובר היה בהתקפה פשוטה: הושתלה רוגלה (spyware) במספר אתרי סחר ישראליים, והיא העבירה נתונים שמפעילי האתרים הללו שמרו תוך הזנחת יסודות אבטחת המידע. על אף חוסר המורכבות והעדר נזק ממשי לאזרחים שהמתקפה גרמה, הפרשה זכתה לכיסוי תקשורתי נרחב ומתמשך במשך כשלושה שבועות, שבתחילתו התאפיין בפאניקה. האירוע הוצג כטרור אנטי־ישראלי, שכן במקום לממש את הרווח הכספי מהפריצה, בחר הפורץ להשתמש בו כדי לזרוע פחד בקרב ישראלים.

ניתן לנתח את האירוע במגוון דרכים: אפשר לומר שהאזרחים חסרי מודעות לאבטחה, שהתקשורת חסרת אחריות ומנפחת עניין שולי וגורמת לפאניקה, שבעלי אתרי האינטרנט התרשלו ופשעו באי־אבטחת המידע שאספו, ושהמדינה התרשלה ביצירת סביבה בטוחה למסחר אינטרנטי ובשמירה על נתונים אישיים. אולם בכל ניתוח, המסקנה המתבקשת היא שדרושה הגברת ביטחונם האישי והקיבוצי של האזרחים במרחב הקיברנטי. בסופו של דבר הדרישה מופנית למדינה, שנושאת באחריות לביטחון אזרחיה. ניתן ורצוי לדון בהגדרת התופעות הבלתי־רצויות והפליליות במרחב הקיברנטי, במידת הביטחון הראויה, בחלוקת האחריות ובהגברת מודעות המשתמשים, בהרחבת גבולות המעורבות הממשלתית הרצויה ובדילמות נוספות הרלוונטיות לנושא. במדינה דמוקרטית, הסוגיות הללו

ילובנו במסגרת דיון ציבורי ותהליך פוליטי. אין להניח שהדרישה לביטחון במרחב הקיברנטי תיעלם, שהבעיה תיפתר מעצמה או שהמדינה תוכל להתנער מאחריותה לביטחון אזרחיה. במקרה הישראלי האמור, אין כל מניעה שרשויות המדינה יגיבו לדרישות השונות של האזרחים ויערכו שינויים בסביבה המשפטית והרגולטורית, כדי להגביר את אבטחת המידע באתרי המסחר האלקטרוני. ויתור על ניסיונות הסדרה והאכיפה במרחב הקיברנטי יאפשר למגוון סוגי הפשע הקיברנטי להמשיך להתפתח ולשגשג, עד לרמה שהדבר יציב איומים של ממש על סוגיות הביטחון הלאומי: הספקת שירות לגורמים עוינים לצורך ביצוע מתקפות קיברנטיות, והגברת היקף הפשיעה לרמה שתערער את הביטחון האישי ואת הסביבה העסקית במדינה.

סיכום – ממשק מסוכן: הפשע הקיברנטי כסיכון הביטחון הלאומי

הפשע הקיברנטי מתפתח ומאתגר את המדינות המפותחות באופנים שונים. המידע הקיים על מקרי הפשע הקיברנטי מגיע מהדוחות התקופתיים של גופים העוסקים בנושא: חברות ייעוץ, מחשוב, אבטחת מידע ורשויות אכיפת חוק. לנוכח הבעיות המובנות בזיהוי התופעה, השימוש הגס בשיטות סטטיסטיות להשגת אומדן כמותי והכללת הנזק העקיף בהערכות הכספיות – המידע הקיים אינו מהימן. נראה שההערכות הכספיות מציגות הטיה קבועה להערכת־יתר. אולם, אף על פי שהערכות בדבר היקף הפשע מוּטות כלפי מעלה, לפשע הקיברנטי יש פוטנציאל מסוכן.

במאמר זה נבחנה משמעות התופעה ביחס לביטחון הלאומי. הניתוח מעלה שטווח רחב של פשיעה קיברנטית אינו מהווה סכנה לביטחון הלאומי. תופעות כמו גניבה וריגול תעשייתי, הונאה, תוכן פוגעני, פשעי שנאה, השחתת אתרים, מניעת גישה לשירות וכדומה – עלולות להפוך לבעיות ביטחון לאומי רק אם היקפן יתרחב מאוד והשפעתן תהיה ממושכת. לכן, כבר עתה ראוי להקדיש משאבים לצמצום הסכנה, ולהקשות על הפושעים הקיברנטיים לפעול בתחום זה.

ניסיון העבר מלמד שגורמים עוינים משתמשים בשירותים וביכולות של ארגוני הפשע, ומגייסים את מומחיותם להשגת מטרות מבצעיות. בשל קצב ההתפתחות הטכנולוגית, יכולות המחשוב המתקדמות הנוכחיות יהפכו בעוד שנים אחדות למוצרי־מדף זולים. "השוק השחור" של שירותי המחשוב מנגיש את היכולות המתקדמות למגוון רחב של גורמים, ומרחיב את העדויות המצטברות על השימוש בשירותיו. הדבר מגביר את החשש שגם במרחב הקיברנטי קיים ומתפתח שיתוף הפעולה בין גורמים עבריינים לבין ארגונים עוינים.

על יסוד הניתוח שהוצג במאמר זה, מוצע להתמקד בשני ממשקים מרכזיים בין הפשע הקיברנטי לבין הביטחון הלאומי. הראשון – מדינת הלאום היא הגורם

האחראי לביטחונם האישי והקיבוצי של אזרחיה. אזרחים וארגונים נפגעים לעתים בצורות שונות מפשע קיברנטי. היקף הנזק אינו ברור: הערכות הנזק הרבות שמשמשות בדיון אינן אמינות, ומוטות כולן כלפי מעלה. גם ללא הסכמה על ההיקף ומידת הפגיעה באזרחים, בארגונים ובמדינות, המדינה נדרשת להגיב להזדמנויות ולאתגרים של המציאות המתפתחת. עם התפשטותו המתמשכת של המרחב הקיברנטי לכל תחומי החיים, יש להניח שיגברו הדרישות מן המדינה לנקוט פעולות על מנת לספק ביטחון אישי ולאומי גם במרחב הקיברנטי. חרף אופיו הבינלאומי של המרחב הקיברנטי, המדינה תיאלץ להרחיב עד מאוד את עיסוקה בביטחון הקיברנטי. קווי המתאר של המעורבות המדינתית במרחב הקיברנטי מתבהרים בשנים האחרונות, כשאחת הסוגיות הטעונות בתחום היא המתח בין ערך הפרטיות האישית לבין ערך הביטחון הלאומי. במדינה דמוקרטית, תהליך עיצוב המדיניות הממשלתית בתחום הפשע הקיברנטי יהיה כרוך בדיון ציבורי, במאבק פוליטי ובטיפול משפטי ממושך.

הממשק השני – המסחור של יכולות טכניות ומבצעיות מנמיך את רף הכניסה לזירת הלחימה הקיברנטית, מרחיב את איומי הייחוס מעבר למדינות ולארגוני טרור גדולים ומכביד את הנטל על רשויות הביטחון הלאומיות. ארגוני הפשע מציעים משאבים, תשתית ואף שירות ללקוחות תמורת תשלום סביר. אפשר לנצל את השוק הזה לא רק לביצוע פשע שמניעיו כספיים, אלא גם לפגיעה ישירה בביטחון הלאומי. ההגנה על תשתיות חיוניות מפני איום קיברנטי היא סוגיה מרכזית בביטחון הלאומי, וחשיבותה עולה לנוכח התפוצה של גורמי הסיכון הפוטנציאליים, שיכולים לרכוש אמצעי לחימה ולגייס "לוחמים" ב"שוק השחור" של פושעי הסייבר.

לאור ניתוח משמעויות התופעה וזיהוי הממשקים המסוכנים בין הפשע הקיברנטי לביטחון הלאומי שהוצגו במאמר, מומלץ למקד כבר עתה תשומת־לב מדינתית בטיפול בהם, על מנת למנוע החרפת האיום. המדינה צריכה להגביר את מעורבותו ביצירת ביטחון קיברנטי, אולם היא אינה יכולה לפתור את הבעיה לבדה. מימוש אחריות המדינה לביטחון הקיברנטי מחייב שיתוף פעולה בין בעלי העניין במגזר העסקי, האקדמי, הציבורי והביטחוני, כדי לספק ביטחון לאומי ואישי למדינה ולאזרחיה במרחב הקיברנטי.

הערות

1 P. N. Grabosky, "Virtual Criminality: Old Wine in New Bottles?" *Social & Legal Studies,* 10(2), 2001, pp.243-249.

2 Majid Yar, *Cybercrime and society: crime and punishment in the information age*. London: Sage Publications, 2006.

3 M. Cross, D. L. Shinder, *Scene of the cybercrime*, Burlington, MA: Syngress, 2008.

4 David S. Wall, *Cybercrimes: The transformation of crime in the information age*, Cambridge, Polity, 2007, p.10.

5 Alkaabi, A., G. M. Mohay, A. J. McCullagh and A. N. Chantler. *Dealing with the problem of cybercrime*", Conference Proceedings of 2nd International ICST Conference on Digital Forensics & Cyber Crime, October 4–6, 2010, Abu Dhabi. http://eprints.qut.edu.au/38894/1/c38894.pdf

6 Offences against the confidentiality, integrity and availability of computer data and systems, Computer-related offences, Content-related offences CoE, "Convention on Cybercrime" Budapest, 2001 http://conventions.coe.int/Treaty/en/Treaties/html/185.htm

7 מדובר בכמה מחשבים, הנגועים בתוכנה זדונית, שמאפשרת שליטה מרחוק ושימוש סמוי ביכולות המחשבים הללו. השימוש הנפוץ ביכולת הוא למשלוח דוא"ל זבל, התקפה של מניעת שירות מבוזרת וגניבה מתמשכת של מידע. ראו: https://www.checkpoint.com/products/anti-bot-software-blade/anti-bot-software-blade-landing-page.html

8 הרעיון להצפנה באמצעות מפתח ציבורי Public key encryption – עומד ביסוד האלגוריתם RSA, שפותח בידי Ron Rivest, Adi Shamir, Leonard Adleman והוצג ב־1978. הפטנט עליו פג בשנת 2000. התוכנה Pretty Good Privacy (PGP) , המאפשרת שימוש חופשי בהצפנה חזקה באמצעות מפתח ציבורי, פותחה ב־1991.

9 Ryan, Richard M. and Edward L. Deci, "Intrinsic and Extrinsic Motivations: Classic Definitions and New Directions." *Contemporary Educational Psychology,* vol. 25, no, 1, 2000, pp. 54-67.

10 Piquero, Alexis Russell, and Stephen G. Tibbetts. *Rational Choice and Criminal Behavior: Recent Research and Future Challenges*, New York: Routledge, 2002.

11 מספר המחשבים הנגועים לבדו אינו יכול לשמש מדידה הולמת לעוצמת הרשת והנזק הפוטנציאלי Plohmann, Daniel, Elmar Gerhards-Padilla, and Felix Leder. *Botnets: 10 Tough Questions,* ENISA, 2011.

12 David S. Wall, *Cybercrimes: The transformation of crime in the information age,* p. 221.

13 ראו למשל: דו"ח GAO-07-705-Cybercrime, עמ' 16–17, יוני 2007. http://www.gao.gov/assets/270/262608.pdf

14 *BI Computer Crime Survey*, p.10, 2005. http://ww.fbi.gov/publications/ccs2005.pdf

15 Secretary of Commerce, Gary Locke (Remarks at the Washington International Trade Association, Washington, D.C., July 22, 2009).
Hathaway, Melissa E. "Falling Prey to Cybercrime: Implications for Business אצל and the Economy," Chapter 6 in: *Securing Cyberspace: A New Domain for National Security*, Queenstown: Aspen Institute, February 2012.

16 Office of Cyber Security & Information Assurance in the UK Cabinet Office and BAE Detica: "The Cost of Cyber Crime", 2011, http://www.cabinetoffice.gov.uk/sites/default/files/resources/the-cost-of-cyber-crime-full-report.pdf

17 "Norton Study Calculates Cost of Global Cybercrime: $114 Billion Annually", http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02

18 Lesk, M. "Cybersecurity and Economics," *IEEE Security & Privacy,* vol. 9, no. 6, 2011, p.76; Carl Bialik, "A Cybercrime Stat's Nine Lives", *The Wall Street Journal*, September 26, 2007, http://blogs.wsj.com/numbersguy/a-cybercrime-stats-nine-

lives-194/tab/print/

19 Florencio, Dinei, and Cormac Herley. "Sex, Lies and Cybercrime Surveys." Microsoft Research, 2012.
המחקר עובד והופיע כמאמר המערכת בניו יורק טיימס.
Florêncio, Dinei, and Cormac Herley. "The Cybercrime Wave That Wasn't" *The New York Times*, April, 15, 2012, https://www.nytimes.com/2012/04/15/opinion/sunday/the-cybercrime-wave-that-wasnt.html?_r=3&hpw

20 Card Verification Value – הקוד הסודי שמודפס על הצד האחורי של הכרטיס. השימוש בו מוודא את תקפות פרטי הכרטיס במקרים שזה לא נקרא באמצעות העברת הפס המגנטי.

21 הדיון חורג מגבולות המאמר. ראו פרק על סקרים אצל: Dane, Francis C. *Evaluating Research: Methodology for People Who Need to Read Research*. Los Angeles: Sage, 2011.

22 "דיסקים מזויפים הם כסף לטרור האסלאמי" 16 בינואר 2003, http://www.ynet.co.il/articles/0,7340,L-2378873,00.html

23 Hunt, J. "The New Frontier of Money Laundering: How Terrorist Organizations Use Cyberlaundering to Fund Their Activities, and How Governments Are Trying to Stop Them," *Information and Communications Technology Law,* vol. 20, no. 2, 2011, pp. 133-152.

24 שב"כ, "סקירה בנושא השימוש שעושה חמאס בתווך התת־קרקעי ברצועה", נובמבר 2000, http://www.shabak.gov.il/publications/study/Pages/hamas-tunnel-report.aspx

25 שב"כ, "הברחות אמל"ח לרצועת עזה מאיראן דרך סודאן וסיני", מאי 2011, http://www.shabak.gov.il/publications/study/Pages/Sudan120511.aspx?webid=a3db3c16-25d8-423d-98df-eb1b9253ab93

26 http://www.terrorism-info.org.il/malam_multimedia/Hebrew/heb_n/html/ipc_272.htm

27 Kshetri, Nir. "The Global Cybercrime Industry and Its Structure: Relevant Actors, Motivations, Threats, and Countermeasures," In: *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*, edited by Nir Kshetri. Heidelberg; London: Springer, 2010; Glenny, Misha. *Darkmarket: Cyberthieves, Cybercops, and You*. New York, NY: Alfred A. Knopf, 2011.

28 אפשר לסווג את כלי הנשק הקיברנטיים לפי השימוש המיועד: malware – תוֹקעה: תוכנה זדונית שמיועדת לשבש בסתר פעילות תקינה של מערכת ממוחשבת ולפגוע בתהליך שמנוהל באמצעות מערכת זו; spyware – רוֹגלה: תוכנה זדונית שמיועדת לאסוף נתונים בסתר ולעתים להעביר אותם ברשת; Scanners – מוכרות לאיתור פגיעויות; Remote and local exploits – לניצול פגיעות מוכרת; Network Sniffers – להאזנה לתקשורת; Backdoor tools, Trojans – לגישה מרחוק ולהוצאת מידע.

29 ראו: Isaac Ben Israel, Lior Tabansky. "An Interdisciplinary Look at Security Challenges in the Information Age." *Military and Strategic Affairs*, vol. 3, no. 3, December 2011, p. 24.

30 Williams. "Organized Crime and Cybercrime: Synergies, Trends and Responses," *Global Issues,* vol. 6, no. 2, 2001, p. 5.

31 McAfee "Virtual criminology report: Organized Crime and the Internet," December 2007. ראו גם: "Kaspersky reveals price list for botnet attacks", July 23, 2009, http://www.computerweekly.com/news/1280090242/Kaspersky-reveals-price-list-for-

botnet-attacks נראה שמחיר השימוש ממשיך לרדת.

32 ג'פרי קאר, 2 בנובמבר 2011, http://jeffreycarr.blogspot.com/2011/11/words-matter-dump-apt-for-apa.html

33 *Software as a Service: Strategic Backgrounder*. Washington, D.C.: Software & Information Industry Association, February 28, 2001, http://www.siia.net/estore/pubs/SSB-01.pdf

34 https://www.gartner.com/it/page.jsp?id=1963815

35 ליאור טבנסקי, "לחימה במרחב הקיברנטי: מושגי יסוד." **צבא ואסטרטגיה**, כרך 3, גיליון 1, מאי 2011.

36 CoE – "Convention on Cybercrime," מאז 2001, אשררו את האמנה 30 מתוך 46 המדינות החתומות עליה.

37 T. Maurer, *Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities regarding Cybersecurity*, Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011.

38 OECD, "Communique on Principles for Internet Policy-Making", June 29, 2011.

39 ITU, *National Cybersecurity Strategy Guide*, September 2011.

40 McConnell, Mike, Michael Chertoff, and William Lynn, "China's Cyber Thievery Is National Policy-and Must Be Challenged," *The Wall Street Journal*, January 27, 2012; Clarke, Richard. "How China Steals Our Secrets," *The New York Times,* April 2, 2012; Gardels, Nathan. "Cyberwar: Former Intelligence Chief Says China Aims at America's Soft Underbelly," *New Perspectives Quarterly,* vol. 27, no. 2, 2010, pp. 15-17; Brenner, Joel. *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*. New York: Penguin Press, 2011; U.S.-China Economic and Security Review Commission (USCC), *2009 Report to Congress of the U.S.-China Economic and Security Review Commission.*

41 ראו: Dunn, *Securing 'the Homeland'*

42 רועי גולדנברג, "בנק ישראל: נגנבו פרטי 15 אלף כרטיסי אשראי", **גלובס**, 3 בינואר 2012, http://www.globes.co.il/serve/globes/printwindow.asp?did=1000712125

43 Dump: a stolen credit card or bank accounts and the associated customer data; Holt, T. J., and E. Lampke, "Exploring Stolen Data Markets Online: Products and Market Forces," *Criminal Justice Studies,* vol. 23, no. 1, 2010.

לוחמת הסייבר של איראן

גבי סיבוני וסמי קרוננפלד

מבוא

בשנים האחרונות גוברת ההבנה בקרב הציבור ומקבלי ההחלטות במדינות שונות, שמרחב הסייבר מחייב התייחסות מתאימה כאל מרחב לחימה של ממש – מרחב המספק כר נרחב ונקודות תורפה רבות לפעולה של תוקפים החפצים לשבש מערכות מידע, ואף לפגוע פגיעה פיזית במערכים של תשתית חיונית, המבוקרים על ידי מערכות בקרה תעשייתיות. כתוצאה מכך, עולה היקף ההשקעות ומתעצמים תהליכי בניין הכוח של מדינות רבות בתחום יכולות פעולה (הגנה, איסוף מודיעין ויכולות התקפיות) במרחב הסייבר בקצב גובר והולך. משנפגעה איראן על ידי מתקפת Stuxnet – שניתן להגדירה כאחת מהתקפות הסייבר ההרסניות ביותר – היא פועלת במרץ רב לשיפור ההגנה במרחב הסייבר מצד אחד, ומצד שני – לבניית יכולות איסוף מודיעין ויכולות התקפיות במרחב הסייבר.

מטרות ההגנה של איראן במרחב הסייבר כפולות. הראשונה – הרצון למנוע הישנות מתקפה דוגמת מתקפת Stuxnet וחדירות למחשבים אירניים לצורכי איסוף מודיעין, כגון הווירוסים 'דוקו' ו־Flame. בהקשר זה, מטרות הפעילות האיראנית דומות לאלה של מדינות רבות בעולם, המבקשות להגן על תשתיות חיוניות שלהן. המטרה השנייה נוגעת לרצון לשמור על שרידות המשטר האיראני על ידי מעקב וחסימה של מידע ושירותים מהציבור האיראני. במקרים רבים, הכלים להשגת שתי המטרות דומים. לדוגמה: הניסיון האיראני ליצור רשת תקשורת מבודלת באיראן, או הניתוק של שרותי 'גוגל' במדינה.[1]

עם זאת נמצאת איראן בתהליך רחב של בניין כוח גם בהקשר ההתקפי, מתוך ההבנה שבכל עימות עתידי, השימוש במרחב הסייבר הוא בעל חשיבות מכרעת להשגת היעדים מול אויבי המדינה. מטבע הדברים, קיים קושי רב באיסוף מידע גלוי באשר ליכולות הסייבר האיראניות, ובייחוד ביחס ליכולות ההתקפיות של

אל"ם (מיל.) ד"ר גבי סיבוני הוא ראש התכניות צבא ואסטרטגיה ולוחמת סייבר במכון למחקרי ביטחון לאומי.
סמי קרוננפלד הוא מתמחה בתכנית לוחמת סייבר במכון למחקרי ביטחון לאומי.

מאמר זה ראה אור לראשונה ב**צבא ואסטרטגיה**, כרך 4, גיליון 3, דצמבר 2012, עמ' 69-88.

המדינה. אורו של הזרקור על פעילות הסייבר של איראן הועצם לאחרונה, עקב חשד שאיראן הייתה מעורבת במספר אירועי סייבר חמורים, ביניהם גניבה של הרשאות אבטחה באינטרנט, תקיפת הרשת הארגונית של חברת הנפט הסעודית ולבסוף – חדירה למחשבי בנקים מרכזיים בארצות־הברית. מאמר זה מבקש להציג תמונה עדכנית ביחס למספר מרכיבים בתהליך הפיתוח של איראן בתחום הסייבר. חלקו הראשון הינו ניתוח של האסטרטגיה האיראנית במרחב הסייבר. החלק השני מפרט את המענה הארגוני והאופרטיבי של איראן לאסטרטגיה שגובשה. חלק זה בוחן שלושה מרכיבים: תשתיות ההכשרה ופיתוח כוח האדם הטכנולוגי בתחום הסייבר, תהליכי התעצמות טכנולוגיים ותהליכי בניין הכוח הכוללים בתחום הסייבר. לבסוף נבחנות מספר פעולות סייבר המיוחסות לאיראן, תוך ניסיון לגבש תובנות באשר לדרך שבה מוליכה אירן את פעילותה בסייבר, בשילוב ניסיון לבחון את ההשלכות על מדינת ישראל ועל מדינות אחרות במערב.

האסטרטגיה האיראנית במרחב הסייבר

תפקידן של רשתות התקשורת והמידע בהתנעת המהומות שפרצו לאחר הבחירות לנשיאות איראן ביוני 2009 ושל אירועי 'האביב הערבי', יחד עם מתקפות הסייבר באיראן, העניקו לזירה זו מקום מרכזי בתפיסת הביטחון הכוללת של המשטר האיראני. עדות לחשיבות הנושא בעיני מקבלי ההחלטות באיראן ניתן למצוא בהתייחסותו הישירה של המנהיג העליון, ח'אמנאי, להזדמנויות ולסכנות הטמונות במרחב הקיברנטי, בעת הכרזתו על הקמת "מועצת סייבר עליונה" במרס 2012 – שתורכב מבכירי השלטון, ותפעל לתכנון וליישום אסטרטגיית פעולה אחידה ומוכללת לזירת הסייבר.[2] מועצה זו אמנם החלה את עבודתה לאחרונה, אך עם זאת, ניתוח הפעילות האיראנית במרחב הסייבר בשנים האחרונות מצביע על קיומה של אסטרטגיית סייבר איראנית בעלת מטרות ויעדים ברורים.

שני נדבכי יסוד עומדים בבסיס תפיסת הפעולה של איראן במרחב הסייבר. הראשון נוגע לפיתוח יכולות הגנה מפני מתקפות של מדינות וגורמים עוינים, לצד פיתוח יכולות שיאפשרו לפעול מול מתנגדי המשטר מבית. הנדבך השני נוגע לפיתוח יכולות התקפיות שיאפשרו לאיראן להילחם במה שנתפס בעיניה כעליונות ושליטה אמריקאית ביכולות ובתשתיות האינטרנט הגלובליות.

בכל הקשור לתפיסת ההגנה, פועלת איראן להגשמת שתי מטרות מרכזיות בזירת הסייבר.[3] ראשית, היא מבקשת ליצור מעטפת טכנולוגית יעילה ומתקדמת, שתגן על תשתיות חיוניות ועל מידע רגיש מפני מתקפות סייבר כדוגמת מתקפת Stuxnet, שפגעה בתוכנית העשרת האורניום האיראנית והשביתה יותר מאלף צנטריפוגות במתקן ההעשרה בנתנז.[4] שנית, איראן מבקשת לבלום ולסכל פעילות סייבר של גורמי אופוזיציה ומתנגדי משטר, שעבורם מהווה מרחב הסייבר

פלטפורמה מרכזית לתקשורת, להפצת מידע ולארגון פעולות נגד המשטר. נוסף לכך, המשטר מבקש למנוע חדירה דרך מרחב הסייבר של רעיונות מערביים ושל מידע הנוגד את האינטרסים שלו, ובכך לבלום תהליכים של "מהפכה רכה" שתפגע באחיזתו במדינה וביציבותו. בהקשר לפיתוח היכולות ההגנתיות, יש לציין גם את הידיעות על התוכנית האיראנית לייצר רשת תקשורת עצמאית ומבודלת[5] – אשר לעיתים מוכחשות על ידי גורמים רשמיים איראניים,[6] אולם ככל שנוקף הזמן, נראה כי יש ממש בידיעות אלה.[7]

בהקשר למרכיב ההתקפי, אסטרטגיית הסייבר האיראנית רואה זירה זו בראש ובראשונה כזירה מרכזית במסגרת דוקטרינת הלוחמה הא־סימטרית, המהווה עיקרון מרכזי בתפיסת הפעלת הכוח האיראנית. לוחמת סייבר, בדומה לטקטיקות א־סימטריות מובהקות יותר כגון טרור ולוחמת גרילה, נתפסת בעיני איראן ככלי יעיל ואפקטיבי המאפשר לפגוע באופן משמעותי בעורפו של אויב בעל עליונות צבאית וגאו־אסטרטגית. מומחים בנושא מעריכים כי במקרה של הסלמת העימות בסוגיית הגרעין בין איראן לבין המערב, תחתור איראן להוציא לפועל מתקפת סייבר נגד תשתיות מרכזיות כגון תשתיות אנרגיה, מוסדות כלכליים, מערכות תחבורה ועוד, בתוך שטחה של ארצות־הברית.[8] מאמר מערכת שפורסם בעיתון האיראני Kayhan (המזוהה עם ח'אמנאי) ביולי 2011 אף רמז לכוונה איראנית זו, באומרו כי על ארצות־הברית להיזהר מפני תקיפה של שחקן "בלתי־נודע במקום כלשהו בעולם" על תשתיותיה החיוניות ביותר.[9]

נוסף לרמה הצבאית־אסטרטגית, המשטר האיראני ותומכיו משתמשים בלוחמה התקפית במרחב הסייבר גם כדי לפגוע בפעילות הסייבר של מדינות מערביות ושל מתנגדי משטר באיראן. קבוצות פצחנים (האקרים) איראניות, שלרוב אינן שייכות באופן רשמי לממסד אך הן קשורות אליו, יוזמות באופן קבוע מתקפות סייבר שונות כדוגמת הפלת אתרי אינטרנט, החדרת תוכן פרו־איראני, גניבת מידע, הונאות אשראי, פגיעה בספקי שרות וניתוב מחדש של תנועת רשת.[10] ערוץ פעולה נוסף שניתן לייחס אותו לפן ההתקפי של אסטרטגיית הסייבר האיראנית הוא התעמולה. המשטר האיראני מבין את חשיבותו של מרחב הסייבר בעיצוב התפיסות והשקפות העולם של קהלים רחבים בתוך איראן ומחוץ לה, ומשקיע רבות ביצירת מערך תעמולה גדול ופעיל, המאדיר את המשטר ופוגע ביריביו. על מנת לממש מטרות אסטרטגיות אלו משקיעה איראן משאבים לא־מבוטלים ביצירת מארג צפוף, מיומן ורב־שכבתי של יכולות סיכול, שליטה, ניטור ותקיפה במרחב הסייבר.

המענה הארגוני והאופרטיבי

כדי לממש את מטרותיה האסטרטגיות במרחב הסייבר, החלה איראן לפעול בנחישות לחיזוק יכולות הסייבר העומדות לרשותה. על פי דיווחים, החליטה איראן להשקיע כמיליארד דולר בפיתוח טכנולוגיות וברכישתן, וכן בגיוס ובהכשרת מומחים, שיקדמו ויחזקו את יכולותיה ההגנתיות וההתקפיות בזירת הסייבר.[11] מספר מרכיבים שלובים בתהליכי בניית המענה האופרטיבי והארגוני בתחום הסייבר: הראשון שבהם נוגע לבניית תשתית הכשרה ופיתוח של כוח אדם במכוני המחקר ובאקדמיה, השני נוגע למאמץ פיתוח טכנולוגי רחב־היקף והשלישי – לתהליכי בניין הכוח הכוללים פיתוח דוקטרינה והקמה של ארגונים, והסדרת סמכויות פעולה למימוש דוקטרינה זו.

הכשרה ופיתוח כוח אדם

תשתיות ההכשרה והפיתוח הטכנולוגי של מערך הסייבר האיראני ממוקמות בראש ובראשונה באוניברסיטאות ובמכונים הטכנולוגיים הפרוסים ברחבי המדינה. באיראן רשת ענפה של מוסדות להשכלה גבוהה ולמחקר אקדמי, העוסקים במחקר ובהכשרה בתחומי טכנולוגיות המידע, הנדסת מחשבים ותקשורת.[12] בין המוסדות המובילים בתחום זה ראוי להזכיר את האוניברסיטה הטכנולוגית שריף (Sharif University of Technology) מוסד הממוקם בטהראן ומציע תארים מתקדמים בהנדסת מחשבים, בהנדסת אלקטרוניקה ובמתמטיקה.[13] באוניברסיטה זו פועלים שני מכוני מחקר המתמקדים בטכנולוגיות תקשורת ומידע: Advanced Information and Communication Technology Center[14] ו־Advanced Communication Research Institute.[15] מוסד נוסף הראוי לאזכור בכל הקשור לתחום ביטחון המידע הוא האוניברסיטה הטכנולוגית אמיר כביר (Amirkabir University of Technology). באוניברסיטה זו, הממוקמת גם היא בטהראן, מחלקה למתמטיקה ומדעי המחשב ומחלקה להנדסת מחשבים וטכנולוגיית המידע. נראה כי במוסד זה מתמקדים בנושא אבטחת המידע, כאשר המחלקה להנדסת מחשבים מציעה מספר קורסים מתקדמים בביטחון מידע,[16] ומפעילה מעבדה מחקרית המתמחה בביטחון מידע[17] ומעבדה לניתוח מערכות מאובטחות.[18]

פרט למחקר ולהכשרה במוסדות האקדמיים, הממשל האיראני משקיע כספים רבים בקידום ובתמיכה בחברות טכנולוגיה העוסקות בטכנולוגיות מידע ותקשורת מחשבים. ההשקעה האיראנית מתבצעת הן באופן ישיר על ידי גופים ממשלתיים כגון משרד המדע, והן דרך מימון והקמת חממות לתמיכה בחברות טכנולוגיה שהשלטון מעוניין בהן.[19] גוף ממשלתי מרכזי בכל הקשור לטכנולוגיות מידע הוא המכון Iran Telecommunications Research Center, המתמחה במחקר טכנולוגיות מידע ותקשורת, והינו הזרוע המחקרית והמקצועית של משרד המידע והתקשורת.

המכון מפעיל ומכשיר צוותי מחקר מתקדמים בתחומים שונים, ובכללם אבטחת מידע.[20] גוף ממשלתי נוסף המקדם מחקר בתחום טכנולוגיות המידע הוא הלשכה לשיתוף פעולה טכנולוגי (TCO-Technology Cooperation Office). גוף זה משתייך למשרד הנשיא ומטרתו המוצהרת היא לשפר את שיתוף הפעולה הטכנולוגי עם מדינות אחרות. הארגון מנחה ויוזם פרויקטים מחקריים בתחומים רבים, ביניהם טכנולוגיות מידע.[21] הוא סומן על ידי האיחוד האירופי וגורמים אחרים במערב כמעורב בתוכנית הגרעין.[22]

נוסף להשקעות ישירות מצד גופים ממשלתיים, הממשל האיראני מפעיל גם חממות טכנולוגיות שבהן מתבצע מחקר בתחום אבטחת המידע. בין מרכזי טכנולוגיה אלה ניתן למצוא את הגן הטכנולוגי Paradis Technology Park המכונה "עמק הסיליקון האיראני". הוא הוקם בשנת 2001 ביוזמת משרד הנשיא וה־TCO, ופועלות בו למעלה מארבעים חברות העוסקות בטכנולוגיות תקשורת ומידע.[23] חממה טכנולוגית נוספת היא Guilan Science and Technology Park, המהווה מרכז לתמיכה בחברות בתחילת דרכן, וב־v רשומות מספר חברות העוסקות בתחומי אבטחת מידע.[24]

התעצמות טכנולוגית

פרט לפיתוח ולהכשרת מערך סייבר חזק, פעלה איראן גם במישור הטכנולוגי על מנת לקדם את מטרותיה האסטרטגיות בזירת הסייבר. תחום אחד שבו השקיעה איראן רבות הוא השליטה במרחב הסייבר הפנים־מדינתי ובתנועות המידע שבו. הממשל האיראני רכש ופיתח בשנים האחרונות מערכות טכנולוגיות מתקדמות, המאפשרות לעקוב ולנטר את תנועות המידע ברשתות המחשבים והסלולר במדינה. Telecommunication Co. of Iran – חברת הטלקומוניקציה הגדולה באיראן הנמצאת בשליטה ממשלתית – רכשה מחברת ZTE Corp הסינית מערכת מעקב המסוגלת לנטר מידע בקווי טלפון, ברשתות מחשב ובקווי סלולר. מערכת זו נקנתה כחלק מעסקה כוללת בין שתי החברות, המוערכת בכ־130 מיליון דולר. העסקה כללה מוצרים ממערכת ZMXT, המתוארת על ידי החברה הסינית כמערכת ניטור משולבת (Integrated monitoring system). המוצרים שנרכשו על ידי איראן מאפשרים ניטור שֶמע, הודעות טקסט וגלישת אינטרנט.[25]

נוסף לניטור ולמעקב, המשטר האיראני פועל גם לפיתוח טכנולוגיות חסימה וסינון של אתרים. כיוון שהסנקציות מונעות מאיראן רכישה של מסנני מידע מערביים, יזם הממשל פרויקט פנים־איראני של פיתוח טכנולוגיות סינון וחסימה. חברת Amnafzar – חברה לטכנולוגיות מידע בעלת קשרים עם המשטר – פיתחה טכנולוגיית סינון מידע המכונה SEPAR. מערכת זו מתעדכנת באופן קבוע ומשנה תכופות את אסטרטגיית הסינון שלה, כדי להתמודד עם ניסיונות עקיפה.[26] בעזרת

טכנולוגיה זו הצליח המשטר להגביל באופן ניכר את זרימת המידע אל המדינה ובתוכה. מחקר של OpenNet Initiative (יוזמה משותפת של מספר מוסדות, ביניהם האוניברסיטאות הרווארד וטורונטו) שהתפרסם במרס 2009 מצא שאיראן היא אחת המדינות המובילות בעולם בסינון ובחסימת אתרים, לצד מדינות כגון סין, צפון־קוריאה, סוריה ומיאנמר.[27]

טכנולוגיות אלו מעניקות לאיראן שליטה הדוקה יחסית במרחב הסייבר המדינתי, אך עם זאת, שאיפת המשטר היא שליטה מוחלטת במידע, ברעיונות ובגישה למרחב הסייבר האיראני. על מנת להשיג שליטה כזו פתחה איראן בפרויקט הקמת רשת אינטרנט לאומית עצמאית, הנבדלת מהרשת העולמית. לשיטתה של איראן, הקמת הרשת הלאומית המכונה Halal תאפשר למשטר שליטה מלאה בתכנים שאליהם נחשף הציבור, תפגע קשות במתנגדי המשטר, אשר חלק גדול מפעילותם מתבצע ברשת, ותקטין משמעותית את האפשרות לחדירת וירוסים ויישום מתקפות סייבר אחרות על תשתיות איראניות. פרויקט הרשת הלאומית החל לקרום עור וגידים בשנת 2009, כאשר הרשויות האיראניות הורו לחברות במדינה להעביר את פעילותן הרשתית לשרתים ולמרכזי מידע בתוך המדינה. במהלך 2012 דווח כי איראן מפתחת שירות דואר אלקטרוני פנימי, מערכת הפעלה עצמאית, מנוע חיפוש וכלים נוספים המיועדים לשימוש ברשת החדשה.[28] באוגוסט האחרון הצהיר שר התקשורת האיראני, רזה טגיפור (Reza Taghipour), כי איראן תתנתק מהרשת העולמית בתוך 18 חודשים.[29] אך עם זאת, מומחים במערב קובעים כי המשטר באיראן יתקשה להתנתק באופן מלא מהרשת החיצונית.[30]

איראן מבקשת ליישם את אסטרטגיית בידול הרשתות גם במגזר הביטחוני, ולהקים רשת תקשורת מודיעינית לאומית שתהיה מנותקת מהרשת הגלובלית.[31] סנונית ראשונה של מאמץ זה היא Basir – רשת פנים־ארגונית של 'משמרות המהפכה' שנחשפה במרס 2012. ידיעות על הרשת מתארות אותה כמעין רשת סלולר סגורה, שייתכן כי היא מופעלת על ידי תחנות ממסר ייעודיות. הרשת אמורה לספק לארגון קווי תקשורת מוצפנים ויעילים, גם בתרחיש של מתקפת סייבר כוללת על תשתיות התקשורת והמידע במדינה. לא ברור האם מדובר גם ברשת מידע, או רק ברשת קולית.[32]

בניין הכוח

באשר לתהליכי בניין הכוח בתחום הסייבר – מערך ההכשרה והפיתוח הנרחב העומד לרשותה של איראן אִפשר לרפובליקה האסלאמית להקים מערך סייבר נרחב בעל יכולות מגוונות, הגנתיות והתקפיות כאחת. בעשור האחרון החלה איראן במהלך אסטרטגי של הרחבת מערך הסייבר הלאומי, כאשר סוכנויות וגופי סייבר הוקמו כמעט תחת כל סוכנות ממשלתית רלוונטית. מטרתה של איראן היא

ליצור מערך ארגוני סייבר הירכי ומגוון עם אסטרטגיית פעולה ברורה, הקצאת משאבים מתוכננת, חלוקת תחומי אחריות ויכולות שימור והפצה של ידע ומידע.

גולת הכותרת של תהליך התעצמות הסייבר האיראני היא, כפי שהוזכר לעיל, הקמתה של "המועצה העליונה למרחב הסייבר". מועצה זו הוקמה במרס 2012 בהוראת המנהיג העליון, ח'אמנאי, והיא הסמכות הבכירה במדינה בכל הקשור למרחב הסייבר.[33] בתפקיד ראש המועצה מכהן נשיא איראן, ובין היתר, חברים בה בכירים כדוגמת מפקד 'משמרות המהפכה', ראש המג'לס, שרי המדע, התקשורת והתרבות, מפקד המשטרה ונשיא ארגון התעמולה האסלאמית. בסמכות המועצה לקבוע את מדיניות הסייבר הלאומית, והנחיותיה מחייבות את כלל הגופים האיראניים הפועלים בתחום. בחסות המועצה מתוכנן לקום "מרכז סייבר לאומי" אשר יתכלל את כלל פעילות הסייבר האיראנית, ירכז ויפיץ מידע והנחיות ויפקח על מילוי הוראות המועצה על ידי כלל הגופים הרלוונטיים.

מערך הסייבר האיראני מורכב ממספר רב של ארגוני סייבר הפועלים בתחומים שונים ומשתייכים באופן רשמי לגופי ממסד. ארגון מרכזי אחד בעל אוריינטציה הגנתית בעיקרה הוא "מפקדת הגנת סייבר", שפועלת במסגרת "ארגון ההגנה הפסיבית של איראן", המשויך למטה הכללי של הכוחות המזוינים.[34] לצד אנשי צבא, חברים בארגון סייבר זה גם נציגי משרדים ממשלתיים כגון משרד התקשורת, ההגנה, המודיעין והתעשייה, ומטרתו המרכזית היא לפתח דוקטרינת הגנה מקיפה למוסדות ולתשתיות המדינה נגד איומי סייבר.[35] הגוף הינו הגנתי בעיקרו, ונכון להיום לא נראה כי הארגון עסק בפעילות סייבר התקפית. גוף סייבר נוסף בעל אופי הגנתי הוא מרכז אבטחת המידע המכונה MAHER , שהוקם ופועל במסגרת המשרד לתקשורת וטכנולוגיות מידע. המרכז אחראי בראש ובראשונה על הפעלה של צוותי תגובה מהירה (Computer Security Incident Response Teams), במקרה של אירועי חירום ומתקפות סייבר. נוסף לכך, המרכז מכשיר כוח אדם מיומן, מפתח דרכי פעולה לטיפול במשברי סייבר ומהווה מרכז לאגירה ולהפצה של ידע בתחום אבטחת המידע. באחריות המרכז להגן על כלל אתרי האינטרנט הממשלתיים, כמו גם על אתרי חברות פרטיות הפועלות באופן רשמי ורשומות במשרד התקשורת. צוותי המרכז הם אלה שהופעלו על מנת לבלום ולסכל את פעולותיהם של הווירוסים Flame ו־Stuxnet שתקפו באיראן.[36]

ארגוני סייבר נוספים הפועלים באיראן מתמקדים באכיפה ובשליטה על פעילות סייבר פנים־איראנית הנוגדת את האינטרסים של המשטר. ביולי 2009 הוקמה על ידי "המועצה הגבוהה למהפכה תרבותית" הכפופה למנהיג העליון "ועדה לזיהוי אתרים בלתי־מאושרים". בוועדה זו חברים, בין השאר, התובע הכללי, מפקד המשטרה, הממונה על כלי התקשורת הממשלתיים ושרי ממשלה שונים (מודיעין, תקשורת, תרבות, מדע ועוד). באחריות הוועדה לאתר אתרי

אינטרנט שתוכנם ופעילותם אינם עולים בקנה אחד עם דרישות המשטר ורצונותיו, ובסמכותה להורות על חסימת גישה לאתרים אלה.[37] בשנת 2011 הוקמה יחידת הסייבר המשטרתית FETA.[38] משימתה העיקרית של יחידה זו היא התמודדות עם פשעי אינטרנט: הונאה, גניבת מידע, איומים וכדומה, אך באחריותה לפעול גם נגד עבריינות פוליטית וביטחונית במרחב הסייבר – משימה המהווה בפועל את עיקר פעילותה.[39] כמו כן אחראית FETA גם על ניטור, מעקב ושליטה במשתמשי האינטרנט באיראן, תוך דגש על משתמשי "אינטרנט קפה" הפרוסים ברחבי המדינה, ומאפשרים גלישה אנונימית במידה מסוימת.[40]

בכל הקשור ליכולות ההתקפיות של מערך הסייבר האיראני, התמונה שקופה וברורה במידה פחותה. באופן טבעי, 'משמרות המהפכה' הם השחקן המרכזי בכל הקשור להקמה ולהפעלה של מערך סייבר התקפי. מומחי סייבר במערב קובעים כי יכולות הסייבר של 'משמרות המהפכה' מציבות את איראן בין המדינות המתקדמות בעולם בתחום לוחמת הסייבר.[41] ניתוח של מכון המחקר Defense Tech מ־2008[42] העריך כי מערך הסייבר של 'משמרות המהפכה' מעסיק כ־2,400 אנשי צוות, ולרשותו תקציב של 76 מיליון דולר (נכון לאותה תקופה). בין יכולות לוחמת הסייבר שאותן מייחס המכון למשמרות המהפכה ניתן למצוא: פיתוח תוכנות מחשב נגועות על ידי השתלה של קוד זדוני בתוכנות מחשב מזויפות; פיתוח יכולות חסימה לרשתות תקשורת מחשבים ורשתות Wi-Fi; פיתוח קודי מחשב זדוניים (וירוסים ותולעי מחשב) המסוגלים להפיץ עצמם ברשתות ולפגוע במחשבי יעד; כלים לחדירה למחשבים ולרשתות כדי לאסוף מודיעין ולהעבירו לשרתים מרוחקים; פיתוח של 'כלים שוהים' המותקנים במחשבי היעד ומופעלים בצורה מושהית, או לפי פקודה משרתי שליטה.

נוסף ליכולות לוחמת המידע, 'משמרות המהפכה' פועלים גם ליצירת מערך לוחמה אלקטרונית שיכול לחסום מערכות מכ"ם ותקשורת. הארגון משקיע רבות ברכישת מערכות לוחמה אלקטרונית,[43] אשר בשילוב עם יכולות לוחמת סייבר יהוו כלי אפקטיבי לפגיעה במערכות האלקטרוניות של ארצות־הברית ושל בעלות־בריתה בשעת עימות צבאי.[44] על פי הצהרות של 'משמרות המהפכה', עוצמתה של איראן בתחום לוחמת הסייבר באה לידי ביטוי בלכידת מטוס הריגול הבלתי־מאויש של ארצות־הברית בדצמבר 2011.[45]

פרט ליחידות לוחמת הסייבר האורגניות, ישנן עדויות גם לקשרים בין 'משמרות המהפכה' לבין קבוצות פצחנים איראניות, הפועלות נגד אויבי המשטר בתוך איראן וברחבי העולם. השימוש ב"מיקור חוץ" מאפשר למשמרות המהפכה ולאיראן לשמור על ריחוק ולהתכחש להאשמות בדבר מעורבותה של איראן בלוחמה ובפשעי סייבר. קבוצת פצחנים איראנית אחת – שמומחים סבורים כי היא קשורה למשמרות המהפכה – היא Ashiyane Digital Security Team.[46] חברי קבוצה

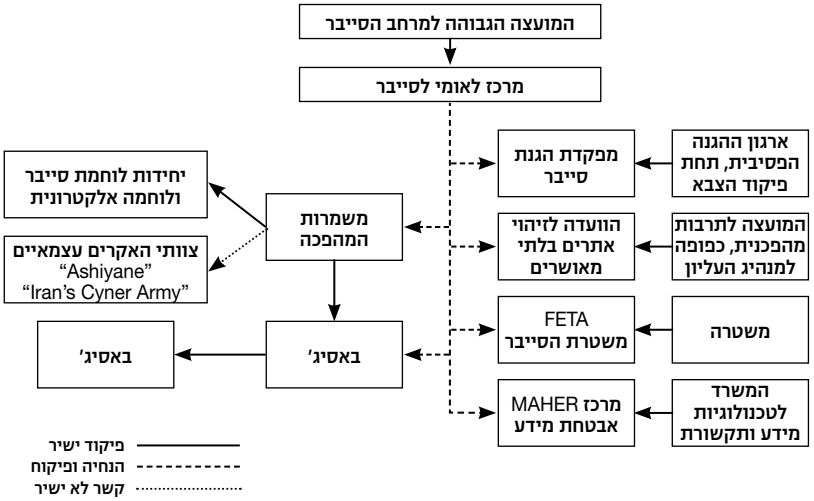
זו מוּנָעים על ידי תפיסות אידאולוגיות התומכות במשטר האיראני ובמהפכה, ומכוונים את התקפותיהם נגד אויבי המשטר. קבוצת Ashiyane מאמנת פצחנים ומקנה להם יכולות גבוהות,[47] אשר מנוצלות לאחר מכן הן לפעילות פוליטית הכוללת החדרה של תעמולה פרו־איראנית לאתרים מערביים וישראליים והפלתם, והן לפשעי סייבר (הונאות אשראי, גניבת זהות ופריצה למאגרי מידע ולמוסדות פיננסיים). נוסף לכך מקיימת הקבוצה פורום בשם War Games, שבו היא עורכת תחרויות פריצה בין פצחנים, כאשר בין המטרות ניתן למצוא גם חברות תשתיות אמריקאיות.[48]

קבוצת פצחנים נוספת הנתפסת כבעלת קשרים למשמרות המהפכה היא Iran's Cyber Army.[49] הארגון מורכב מפצחנים ומומחי מחשבים הפועלים בזהות בדויה, ומכריזים על עצמם כשייכים לארגון. פעולותיו העיקריות של צבא הסייבר האיראני כוללות: פריצה והחדרת תוכן פרו־איראני לאתרים מערביים, השתלטות על תעבורת מידע ותיעולה מחדש, פריצה לחברות ביטחון מידע מערביות ופגיעה באתרים של מתנגדי המשטר.

גם ארגון הבסיג' הכפוף למשמרות המהפכה נעשה פעיל בזירת הסייבר עם הקמתה בשנת 2010 של "מועצת הסייבר של הבסיג'". פעילות הבסיג' מתמקדת בראש ובראשונה ביצירת תעמולה פרו־איראנית במרחב הסייבר. הבסיג' מגייס ומדריך אלפי אירנים בכתיבת תוכן, ולאחר מכן מפעיל כיתות מחשבים מאורגנות, שמתוכן מופעלים עשרות אלפי בלוגים התומכים במשטר, וכן מעלים הפעילים תגובות וחומרים התומכים בשלטון ברשתות חברתיות, בפורומים ובאתרים מרכזיים באיראן ומחוצה לה.[50] עם זאת, הבסיג' מבקש לפתח גם יכולות סייבר מתקדמות יותר, ומשתמש במדריכים מתוך יחידות הסייבר של 'משמרות המהפכה' על מנת להכשיר פצחנים בעלי יכולות תקיפה גבוהות.[51]

אם כן, ניתן לראות כי בשנים האחרונות הקימה איראן מערך סייבר נרחב המקיף תחומי פעילות רבים, ולרשותו עומדות יכולות מגוונות. התרשים הארגוני שלהלן מתאר את המבנה ההיררכי של מערך הסייבר במדינה, כפי שהוא עולה מתוך הניתוח לעיל:

ניתן לראות התקדמות משמעותית בפיתוח תחום הסייבר באיראן. בתחום ההגנתי פועלת איראן במלוא המרץ לייצר יכולות הגנה ובידול, כדי להתמודד עם ניסיונות חדירה לרשתות ולתשתיות חיוניות במדינה. קשה לספק תמונה אמינה בהקשר לפיתוח היכולות ההתקפיות בתחום הסייבר. החלק הבא במאמר בוחן מספר פעולות כאלה.



פעולות סייבר המיוחסות לאיראן

בדצמבר 2011 הובילה חשיפה של תוכנית תחקירים של רשת הטלוויזיה Univision לחקירה אמריקאית בדבר מעורבותם של גורמים איראניים רשמיים במזימת סייבר נגד ארצות־הברית. תחקירני הרשת, שהצליחו להסתנן לתוך קבוצת פצחנים מקסיקנית שפעלה נגד מטרות אמריקאיות, צילמו בסתר פגישה בין נציגי הקבוצה לבין שגריר איראן במקסיקו. בפגישה שנערכה בשגרירות, ביקשו הראשונים לבדוק את האפשרות לקבלת תמיכה ומימון מממשלת איראן לטובת ביצוע מתקפות סייבר נגד מטרות אמריקאיות, ביניהן הפנטגון, ה־CIA, ה־FBI ומתקני גרעין בתחומי ארצות־הברית. בצילומים נראה השגריר האיראני במקסיקו דאז, מוחמד חסן גהאדרי, מציג שאלות ואף מציע דרכי פעולה אפשריות נוספות. השגריר הדגיש שאיראן מבקשת להשיג מידע מודיעיני לגבי האפשרות של תקיפה אמריקאית נגדה, ובסוף השיחה ביקש לשמור על קשר והבטיח להעביר ההצעה לממונים עליו.[52] ניתן להניח שניסיון זה לא היה יחידי, וכי איראן פועלת לגייס בעולם גורמים שיוכלו לשרת את מטרותיה ההתקפיות במרחב הסייבר.

קביעה ודאית של זהות תוקפים במרחב הסייבר היא פעולה מורכבת המחייבת הקצאה של משאבים רבים ושיתוף פעולה בין־לאומי. לכן, קשה לקבוע בוודאות מי עומד מאחורי פעולות רבות במרחב הסייבר. למרות זאת, במקרים רבים ובאמצעות תבחינים נסיבתיים ניתן לקבוע ברמה גבוהה של ודאות מיהו העומד מאחורי הפעילות. במסגרת מאמר זה נבחנו שלוש פעולות. הראשונה – תקיפה של שתי חברות אבטחה למטרת גניבה של הרשאות אבטחה באינטרנט, השנייה

נוגעת לתקיפת מוסדות פיננסיים גדולים בארצות־הברית והאחרונה הינה תקיפת חברת הנפט הסעודית Aramco.

מתקפה על החברות DigiNotar ו־Comodo

במהלך שנת 2011 בוצעו שתי מתקפות על חברות המספקות הרשאות SSL.[53] הראשונה על חברת Comodo מארצות־הברית והשנייה על חברת DigiNotar מהולנד. חברת האבטחה האמריקאית Comodo הותקפה במהלך חודש מרס 2011. נגנבו מספר הרשאות, ביניהן הרשאות לתחומים (domain) של שרותי דואר אינטרנטיים דוגמת Google, אולם אלה בוטלו בטרם נעשה בהן שימוש על ידי הגורם התוקף. למעשה, גורם המקבל אישור לתחום mail.google.com, יכול לגנוב סיסמאות של Gmail ו"לחטוף" חשבונות של משתמשים. כך גם מי שמקבל אישור מזויף לתחום Microsoft.com יוכל להתקין תוכנות זדוניות במחשבי הקורבנות. מדיווח של החברה על האירוע עולים הממצאים הבאים:[54]

1. בתקיפה זו לא היו מאפיינים של עבריינות סייבר.
2. התוקפים היו מאורגנים וידעו במדויק ומראש את מבוקשם – דבר המצביע על מעורבותו של ארגון מדינתי בתקיפה.
3. מקור המתקפה היה בעיקר איראן (לפי זיהוי כתובת IP).
4. אתר האינטרנט שבו נבדקו ההרשאות הגנובות מוקם באיראן, והופרד מהרשת מייד לאחר גילוי המתקפה על ידי חברת Comodo.

תקיפת חברת Comodo לא הצליחה להשיג את מטרתה. ההתקפה זוהתה וטופלה בטרם נעשה שימוש בהרשאות הגנובות. שונה היה המצב בחברת DigiNotar ההולנדית. מאגרי החברה שהייתה הרשות המרכזית בהולנד להרשאות SSL הותקפו בחודשים יוני עד אוגוסט 2011. במהלך התקיפה, שקיבלה את הכינוי "טוליפ שחור", נגנבו תעודות המשמשות לאימות אתרים, כולל תעודה המשמשת לאימות שם התחום google.com, המאפשרת לתוקף התחזות וניתוב מחדש של שרתי Gmail.[55]

ניתוח שהזמינה חברת DigiNotar (שעקב אירוע זה פשטה את הרגל וחדלה להתקיים) הראה שנגנבו וזויפו 531 תעודות, וכי עיקר השימוש בהרשאות הגנובות היה לצורכי חדירה לחשבונות דוא"ל של משתמשים, בעיקר באיראן. הניתוח הראה שהתקיפה אפשרה חדירה ליותר מ־300,000 מחשבים, רובם המכריע באיראן (מעל 99%).[56] קשה לקבוע בוודאות את מקור התקיפה, אולם לדעת מומחים, מקורה באיראן והיא נועדה, ככל הנראה, לצורכי בטחון פנים במדינה,[57] בעיקר בשל הסיבות הבאות: יעדי המתקפה וההיקף הנרחב של משתמשים שהותקפו, וכן הודעות שהושארו באתר החברה שהצביעו על מעורבות של איראנים בפעולה.

מתקפה על מוסדות פיננסיים בארצות־הברית

דיווח שהופץ בארצות־הברית בחודש ספטמבר 2012 מעלה כי סמוך למועד זה הותקפו מספר מוסדות פיננסיים בארצות־הברית, ביניהם אתרים השייכים לבנק אוף אמריקה (Bank of America), לבנק מורגן צ'ייס ולבנק סיטיגרופ. להערכת גורמים בארצות־הברית, התקפות הסייבר נגד מוסדות פיננסיים אמריקאיים לא נערכו על ידי פצחנים אקראיים, אלא מומנו ככל הנראה על ידי איראן, והן בוצעו בתגובה לסנקציות שהוטלו על המדינה על ידי ארצות־הברית.[58]

בעקבות זאת, מרכז לניתוח ולשיתוף מידע פיננסי בארצות־הברית [59] פרסם התראה לבנקים בארצות־הברית בעניין תקיפות סייבר שמטרתן גניבת זהויות באמצעות דואר אלקטרוני, סוסים טרויאניים וכלים זדוניים המסוכלים לקלוט הקשות מקלדת – כל זאת כדי לחלץ שמות של משתמשים, עובדים וסיסמאות. אף שגם בנקים גדולים הותקפו, רוב הקורבנות של תקיפות אלה היו עסקים קטנים ובינוניים, בנקים קטנים וחברות אשראי. קבוצה הקרויה "לוחמי הסייבר של עז א־דין אל קאסם" הודיעה שהיא תקפה את בנק אוף אמריקה (BofA) ואת הבורסה של ניו־יורק בתגובה לסרט שפגע בנביא מוחמד, שהתפרסם בתחילת ספטמבר 2012. התקפות אלה, כפי שתוארו בהתראה, מצביעות על כך שהתוקפים הצליחו להשיג מידע רב וגישה לרשתות הבנקים לפחות במספר מקרים, וכן הצליחו להשיג אישורי כניסה מעובדי בנק ולעקוף את מנגנוני ההגנה.[60]

מתקפה על חברת Aramco

במהלך אוגוסט 2012, כנראה תוך סיוע פנימי של גורם בעל נגישות גבוהה למחשבי החברה, הותקפו כ־30,000 מחשבים של חברת Aramco הסעודית ומחשבי חברת הגז ResGas מקטר ההתקפה בוצעה באמצעות וירוס מחשב הידוע בשם Shamoon. לדעת מומחים, זוהי אחת ההתקפות ההרסניות ביותר שבוצעה נגד חברה אחת. וירוס המחשב התפשט דרך שרתי מחשבי החברה ופגע במידע שנשמר בהם. מומחי החברה טוענים שהנזק היה מוגבל למחשבים משרדיים, ולא השפיע על המערכות התפעוליות ומערכות הבקרה.[61]

חברת סינמטק זיהתה את הווירוס לראשונה בחודש אוגוסט 2012. בניתוח שערכו גורמים בחברה ובחברות אבטחה נוספות עלו כמה ממצאים:[62]

1. הווירוס Shamoon נועד לתקוף מחשבים במערכת המחשוב הארגוני (IT) ולא מחשבי מערכות בקרה. וירוס זה אינו שייך לקטגוריה של כלי לוחמת סייבר מתוחכמים דוגמת Stuxnet, שתקף את תוכנית הגרעין של איראן בשנת 2010.
2. מטרת התקיפה של הווירוס לא הייתה ריגול או איסוף מידע, כי אם השמדה מוחלטת של נתונים ופגיעה במחשבי היעד.

3. כותבי הקוד המפַגע אינם נראים כשייכים לעילית התחום (כמו כותבי קוד Stuxnet או Flame). קיימים ממצאים המראים שהגורמים העומדים מאחורי כתיבת הקוד אינם מתכנתים בעלי פרופיל מקצועי גבוה במיוחד, והושארו בו שגיאות קידוד רבות. אולם הם היו מיומנים דיים לייצר קוד הרסני במיוחד.
4. הווירוס הוחדר למחשבי החברה באמצעות משתף פעולה מתוך החברה, שהייתה לו גישה ישירה למערכת. נראה שהוא השתמש בהתקן USB על מנת להחדיר את הווירוס לתוכה.
5. כותבי הקוד עשו שימוש בחלק מתמונת דגל אמריקאי שרוף כדי להסתיר את תוכן הקבצים במחשבים הנגועים – פעולה המראה על שיוך פוליטי או דתי־אסלאמי מסוים של כותבי הקוד.
6. בקוד של מנגנון המחיקה של ה־Shamoon הטמיעו מפתחי הווירוס את השם Wiper. כינוי דומה מופיע בקוד הווירוס Flame, שתקף את מחשבי חברת הנפט האיראנית. הקבלה זו מעלה את החשד כי המתקפה על Aramco היא פעולת תגמול איראנית, בתגובה למתקפת Flame.

קבוצה בשם 'חרב הצדק' (The Cutting Sword of Justice), קיבלה אחריות לתקיפה וטענה שהיא כוּונה נגד מקור ההכנסה העיקרי של ערב־הסעודית, שהואשמה בביצוע פשעים במדינות כגון סוריה ובחריין. עוד טענה הקבוצה, שווירוס המחשב אִפשר להם גישה לסודות רבים. אולם נכון לכתיבת שורות אלה, טרם פורסם כל מידע רלוונטי בנושא. דיווחים על התקפות דומות על חברות נפט וגז באזור המפרץ העלו את החשד שתקיפות אלה היו חלק ממהלך רחב של מדינה. בדברים שאמר לאחרונה שר ההגנה האמריקאי, ליאון פאנטה, הוא רמז על מעורבות איראנית בתקיפה. בכיר לשעבר בממשל האמריקאי היה גלוי יותר, כשאמר שהממשל מאמין כי איראן עומדת מאחורי המתקפות במפרץ.[63]

ניתוח שערך מומחה האבטחה ג'פרי קאר (Jeffrey Carr)[64] מארצות־הברית מעלה מספר טיעונים הקושרים את איראן למתקפה זו. איראן היא המדינה היחידה שיש לה נגישות לקוד המקור Wiper, שממנו נוצר ככל הנראה הווירוס Shamoon. לפי הדיווח של חברת קספרסקי,[65] הקוד Wiper ששימש לתקיפת משרד האנרגיה האיראני באפריל 2012 שימש גם את יוצרי Shamoon. לאיראן מוטיבציה גבוהה לתקוף את חברת הנפט הסעודית בשל הסנקציות המחריפות על איראן בתחום האנרגיה. כמו כן, נבדק חשד לקשר של ארגון חזבאללה לתקיפה. מספר עובדים לבנוניים של חברת Aramco נעצרו ונחקרו בהקשר זה.

תובנות מסכמות

פיתוח יכולות הסייבר של איראן צריך להטריד את ישראל, וכמובן גם את ארצות־הברית, כמו גם מדינות נוספות במערב. בעקבות התעוזה בניסיון החיסול של

שגריר ערב־הסעודית בארצות־הברית, מציעים מומחים בארצות־הברית לא לזלזל בכוונות וביכולות האיראניות להעיז ולתקוף תשתיות חיוניות בארצות־הברית. כמו שאר העולם, ניתן להניח שגם איראן – שהייתה קורבן לאחת ממתקפות הסייבר ההרסניות ביותר – למדה היטב את לקחי תקיפת Stuxnet, והיא מבינה את הפוטנציאל ההרסני הגלום בפיתוח כלי תקיפה שיוכלו לפגוע במערכות בקרה תעשייתיות, ובכך לגרום נזק פיזי.

פיתוח האסטרטגיה האיראנית ותהליכי בניין הכוח שבאו בעקבותיה מצביעים על התארגנות שיטתית בניסיון להוות שחקן משמעותי בתחום לוחמת הסייבר. מומחים מדווחים על התקדמות מתמדת ביכולות ובמבצעי הסייבר של איראן. ראוי לשים לב לדברי אחד מהם, שאמר לאחר דיווח על מתקפת סייבר על מוסדות בנקאיים בארצות־הברית המיוחסת לאיראן: "[תוכנית הסייבר של איראן] דומה לתוכנית הגרעין, היא אינה מתוחכמת במיוחד אבל מתקדמת מדי שנה."[66] אין לזלזל ביכולות הטכנולוגיות של איראן. התשתית המדעית במדינה מפותחת ומאגר ההון האנושי רב. לכן, ניתן להעריך שתוך תקופה לא־ארוכה תוכל איראן להוות גורם משמעותי ברמה עולמית בתחום זה. הערכה זו מקבלת חיזוק מהמתקפה על מחשבי חברת Aramco, שבעקבותיה אמר ג'יימס לואיס (James A. Lewis), מומחה לביטחון סייבר, שאיראן הייתה מהירה יותר בפיתוח יכולות התקפיות, ונועזת יותר בהפעלה שלהן משניתן היה לצפות.[67] בדרך כלל, הפעילות שנחשפת הינה קצה הקרחון של פעילות בלתי־גלויה נוספת. מצד שני, שכלול ההגנה של איראן מחייב את הגורמים בעלי העניין להתארגן לפעולה בסביבה של רשתות מבודדות, או אף רשת תקשורת איראנית מבודדת מרשת האינטרנט. אף כי האתגר בהקמה של רשת כזו ובבידודה המוחלט הוא עצום, הרי ניתן לאתר דרכי פעולה גם בסביבה כזו. תפיסת הגנה זו תהווה אתגר לא־מבוטל לגורמים בעלי עניין בביצוע מהלכים במרחב הסייבר באיראן.

מתוך הפעולות המיוחסות לאיראן שתוארו לעיל, ניתן להפיק מספר תובנות. הניסיון האיראני להשיג הרשאות SSL מצביע על פעילות מול קבוצות גדולות של אזרחים יותר מאשר כלפי יעדים ממוקדים כמו מדינות או חברות וארגונים. ככל הנראה, הדבר נוגע לצורכי זיהוי ומעקב על גורמים פנימיים באיראן. עם זאת, הניסיון הנצבר בפעילות מסוג זה יאפשר פעילויות גם מול יעדים ממוקדים יותר דוגמת ארגונים ומדינות. ראוי לציין שאף כי הפעילות שנחשפה מצביעה על ארגון ושיטתיות, נדמה שאיראן טרם חצתה את הרף הטכנולוגי והארגוני כדי להוות גורם בעל תחכום רב. אולם, המוטיבציה האיראנית יחד עם תהליכי בניין הכוח והיכולות הטכנולוגיות במדינה יאפשרו לה לצעוד לכיוון זה במהירות רבה.

תקיפת חברת Aramco מעלה תובנות נוספות. הראשונה נוגעת לעובדה שההגנה המקובלת מפני איומים המגיעים דרך רשת האינטרנט אינה מספקת. רוב

המומחים מקבלים את ההנחה שהחברה לא חסכה השקעות בהגנה מפני איומים המועברים דרך רשת האינטרנט. הווירוס ההרסני לא התגלה על ידי מערכות ההגנה, והוחדר כנראה על ידי גורם פנימי בחברה, שהיה בעל הרשאה מתאימה. מערכות ההגנה הקיימות והסטנדרטיות אינן בנויות לספק הגנה מפני איומים ממוקדים (APT) וקוד זדוני בלתי־מוכר (zero date ואחרים). לכן גובר הצורך בפיתוח כלים שיוכלו לספק הגנות טובות יותר מפני איומים כאלה. אחד הכיוונים המתפתח הוא כלים שיתבססו על זיהוי, חסימה ונטרול של התנהגות אנומלית ובלתי־רצויה במחשבים מותקפים. כלים כאלה יוכלו לנטרל איומים גם אחרי שהקוד הזדוני הצליח לחדור למחשב היעד. התובנה השנייה נוגעת למטרות התקיפה, שנועדה בעיקר להשמיד מידע באופן גורף וללא אבחנה בעשרות אלפי המחשבים של חברת הנפט הסעודית, ופחות (אם בכלל) לאסוף מידע. אם פעילות מודיעין במרחב הסייבר יכולה להיחשב לגיטימית בחלק מהמקרים, הרי תקיפה רחבת־היקף כזו על ידי איראן על מטרה אזרחית מסמנת כי איראן עוברת לפעולות תגמול. הדבר צריך להטריד את הממונים על ההגנה במדינות רבות. דבריו של שר ההגנה האמריקאי, ליאון פאנטה, על הצורך לבוא חשבון עם הגורמים העומדים מאחורי תקיפה זו ממחישים זאת.[68] אולם, מה שיקבע יהיה מבחן המעשה ולא מבחן המילים.

כמי שנפגעה מהתקפת הסייבר ההרסנית ביותר עד כה, ניתן להעריך שאיראן מבינה היטב את הפוטנציאל הגלום בתחום זה, וכי היא תפעל לפתח יכולות כאלה משל עצמה בעתיד. לנוכח זאת, תהליכי בניין הכוח השיטתיים שפורטו לעיל יובילו את איראן תוך זמן לא רב להיות שחקן משמעותי בשדה הקרב הקיברנטי ולתקיפה של תשתיות חיוניות במדינות העוינות את איראן, כגון ארצות־הברית וישראל, תוך יצירת בידול מרבי במקרה של חשיפה וגילוי הפעילות. איראן מפעילה קהילות של פצחנים "אזרחיים" תוך ניסיון ליצור בידול בין אלה לבין הממשל והארגונים האיראניים. גישה זו דומה למתרחש במקומות נוספים בעולם, דוגמת סין ורוסיה, והיא מאפשרת למדינות להתנער מאחריות ולגלגל את המעשה לפתחם של אזרחים. כך יימשך הקושי הרב בשיוך פעולות הסייבר ההתקפיות למדינה האיראנית.

מיקוד פעילות הסייבר של איראן בישראל ובמדינות מערביות אחרות מחייב התארגנות הגנתית ייעודית. נדרשת תפיסה עדכנית בכל הקשור להגנות במרחב הסייבר. התחכום של התוקפים מחייב, לצד הגנות גנריות, גם פעילות הגנה המבוססת על מודיעין. לפיכך ולנוכח תהליכי ההתפתחות של איראן, חייבת מדינת ישראל להציב את תחום הסייבר האיראני במקום גבוה בסדר־העדיפות המודיעיני ובפעילות המסכלת. הדבר נועד לאתר ולסכל בעוד מועד התארגנויות לפעולות התקפיות. בדומה לתוכנית הגרעין האיראנית, האתגר אינו רק של מדינת ישראל, אלא של מדינות נוספות רבות במערב, כמו גם מדינות המפרץ, ותעיד על

כך ההתקפה על מחשבי חברת Aramco. לכן, יש ליזום שיתוף פעולה בין־מדינתי רחב ככל האפשר בתחום המודיעין והסיכול של פעולות סייבר איראניות.

לצד זאת, על מדינת ישראל להמשיך לבנות מענה הגנתי אפקטיבי. מענה זה צריך להתמקד בשלוש שכבות הסייבר הרלוונטיות במדינה: הראשונה – שכבת ארגוני הביטחון הנדרשים לבחון באופן קבוע את החשיפה ליכולות הסייבר של איראן, ולוודא שהם אינם מצליחים לפעול ולפגוע ביכולות חיוניות של מערכת הביטחון. השכבה השנייה נוגעת למערך התשתיות החיוניות במדינה, המונחות על ידי הרשות לאבטחת מידע מתוקף החלטת ממשלה. גם כאן, האתגר מחייב פעילות מתמדת בייחוד בכל הקשור להבנת תמונת האיום, לשיתוף מידע בין גורמים שונים ולהתאמת המענה לאיום זה. לבסוף, אין לזלזל ביכולות האיראניות לנסות לפגוע בעסקים ובתעשייה שאינם מונחים על ידי רשויות המדינה. עסקים ותעשייה במגזר הפרטי פועלים ברוב המקרים בעיקר להגנת נכסי המידע שלהם, וקשה לדרוש מהם להתגונן מפני האפשרות שיותקפו במרחב הסייבר על ידי מדינה זרה כמו איראן. לכן, החשיבות המכרעת של המטה הקיברנטי הלאומי שהוקם לאחרונה כגורם המתכלל ומי שיכול לקדם תהליכי אסדרה ושיתוף מידע ומודיעין בהתאם למפת האיומים המתפתחת.

הערות

1 Art Keller, "The Great Persian Firewall, Should we care that Iran just turned off Google?", *Foreign Policy*, September 28, 2012, http://www.foreignpolicy.com/articles/2012/09/28/Iran_firewall_google?page=full

2 הצהרתו של ח'מאנאי בעת ההכרזה על הקמת המועצה באתרו הרשמי: http://farsi.khamenei.ir/message-content?id=19225

3 Ilan Berman, *The Iranian Cyber Threat to the U.S. Homeland*, Statement before the U.S. House of Representatives Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies and Subcommittee on Counterterrorism and Intelligence, April 26, 2012, pp 1-3, http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20-%20Berman.pdf

4 CBS News, *Iran Confirms Stuxnet Worm Halted Centrifuges*, 29 November 29, 2010, http://www.cbsnews.com/stories/2010/11/29/world/main7100197.shtml

5 Kevin McCaney, *Iran building a private, isolated Internet, but can it shut out the world?* CGN, April 10, 2012, http://gcn.com/articles/2012/04/10/iran-building-separate-isolated-internet.aspx

6 Agence France Presse, *Iran denies has plan to cut Internet access*, AFP, 10 April 2012, http://www.google.com/hostednews/afp/article/ALeqM5h4e57x6CYbsavza1PeDuQP7Bf9Vg

7 Amir Taheri, *Iran will launch its national internet next week but not for the reasons you might think*, September 20, 2012, http://www.opednews.com/articles/Iran-will-launch-its-natio-by-Amir-Taheri-120919-83.html

8 Brian Ross, *What Will Happen to the US If Israel Attacks Iran?* ABC News, 5 March 2012, http://abcnews.go.com/Blotter/israel-attacks-iran-gas-prices-cyberwar-terror-threat/story?id=15848522

9 Ilan Berman, p 4.

10 Reza Marashi, *The Islamic Republic's Emerging Cyber War*, National Iranian American Council, April 30, 2011, http://www.niacouncil.org/site/News2?page=NewsArticle&id=7318

11 Yaakov Katz, Iran embarks on $1b. cyber-warfare program, *The Jerusalem Post*, 18 December 18, 2011, http://www.jpost.com/Defense/Article.aspx?id=249864

12 Patterson, J.P & M.N. Smith, *Developing a Reliable Methodology for Assessing the Computer Network Operations Threat of Iran*, Master's Thesis, Monterey, CA: Naval Postgraduate School, 2005, pp. 17-22, http://www.fas.org/irp/eprint/cno-iran.pdf

13 אתר אוניברסיטת שריף: http://www.sharif.ir/web/en

14 אתר המכון: http://www.aictc.com/web/content/main

15 אתר המכון: http://acri.sharif.ir/en/Default.asp

16 פירוט הקורסים המתקדמים: http://ceit.aut.ac.ir/autcms/courses/courseOfferingView.htm?level=M.Sc&depurl=computer-engineering&lang=en&cid=70317

17 אתר המעבדה לביטחון מידע: http://ceit.aut.ac.ir/autcms/labs/verticalPagesAjax/labHome.htm?id=3350532&depurl=computer-engineering&lang=en&cid=147776

18 אתר המעבדה למערכות מאובטחות: http://ceit.aut.ac.ir/autcms/labs/verticalPagesAjax/labHome.htm?id=3369580&depurl=computer-engineering&lang=en&cid=147732

19 Patterson, J.P & M.N. Smith, pp. 29-35.

20 פעילות המכון בתחום אבטחת המידע: http://www.itrc.ac.ir/itrc-secure-en.php

21 התייחסות להשקעה בטכנולוגיות מידע באתר של TCO: http://citc.ir/newpages/page27.aspx?lang=Fa

22 The Wisconsin project on nuclear arms control, *Iran Watch*, January 3, 2011, http://www.iranwatch.org/suspect/records/technology-cooperation-office.htm

23 רשימת החברות ב־Paradis Technology Park: http://www.techpark.ir/?/content/142

24 אתר Guilan Science Park: http://www.gstp.ir/modules.php?name=Content&pa=sho&pid=16

25 *S*teve Stecklow, "Chinese firm helps iran spy on citizens," Reuters, March 22, 2012, http://graphics.thomsonreuters.com/12/03/IranChina.pdf

26 Reza Marashi, 2011, ; עלון מידע המציג את טכנולוגית ה־SEPAR ומצביע על הקשר בין המשטר לבין פיתוחה: http://www.iranascience.com/1-home/newsletters/21-Web%20Filters.pdf

27 OpenNet Initiative, Country Study: *Internet Filtering in Iran 2004-2005*, 16 June 2009, http://opennet.net/research/profiles/iran

28 Kevin McCaney, "Iran building a private, isolated Internet, but can it shut out the world?" ,GCN ,10 April 2012, http://gcn.com/articles/2012/04/10/iran-building-separate-isolated-internet.aspx

29 Robert Tait, "Iranian state goes offline to dodge cyber-attacks," *The Telegraph*, 5 August 2012, http://www.telegraph.co.uk/news/worldnews/middleeast/iran/9453905/Iranian-state-

goes-offline-to-dodge-cyber-attacks.html

30 Cyrus Farivar, "Security researcher unearths plans for Iran's halal Internet," *Ars Technica*, 17 April 2012, http://arstechnica.com/tech-policy/2012/04/iran-publishes-request-for-information-for-halal-internet-project/

31 Robert Tait, 2012.

32 Ali Akbar Dareini and Brian Murphy, "Iran Internet Control: Tehran Tightens Grip On Web," The Huffington Post, 16 April 2012, http://www.huffingtonpost.com/2012/04/16/iran-internet-control_n_1429092.html?ref=world

33 Emily Alpert and Ramin Mostaghim, "Iran's supreme leader calls for new Internet oversight council," *Los Angeles Times*, 7 March 2012, http://latimesblogs.latimes.com/world_now/2012/03/iran-internet-council-khamenei.html

34 *Structure of Iran's Cyber Warfare*, BBC Persian, p. 1. http://nligf.nl/upload/pdf/Structure_of_Irans_Cyber_Operations.pdf

35 "Iran is formulating strategic cyber defense plan: official," *Tehran Times*,15 June 2012, http://tehrantimes.com/politics/98761-iran-is-formulating-strategic-cyber-defense-plan-official

36 מבנה המרכז ותפקידיו מפורטים באתרו הרשמי: http://www.certcc.ir/index.php?newlang=eng

37 "Structure of Iran's Cyber Warfare," BBC Persian, pp. 4-5.

38 "Iran to crack down on web censor-beating software," *Hürriyet Daily News*, 22 September 2012, http://www.hurriyetdailynews.com/iran-to-crack-down-on-web-censor-beating-software.aspx?pageID=238&nID=22789&NewsCatID=374

39 Structure of Iran's Cyber Warfare, p. 4.

40 בינואר 2012 חוקק המשטר מערכת חוקים לשם מעקב וניטור הגולשים מתוך האינטרנט קפה ברחבי המדינה. חוקים אלו מאפשרים ל־FETA ליצור "ספר משתמשים" של כלל הגולשים הארעיים במדינה ולנטר פעילות נגד המשטר במרחב הסייבר. Farnaz Fassihi, "Iran Mounts New Web Crackdown," *The wall Street Journal*, 6 January 2012, http://online.wsj.com/article/SB10001424052970203513604577142713916386248.html

41 lIan Berman, p. 4.

42 Kevin Coleman, "Iranian Cyber Warfare Threat Assessment," *Defense Tech*, 23 September 2008, http://defensetech.org/2008/09/23/iranian-cyber-warfare-threat-assessment

43 Stephen Trimble, "Avtobaza: Iran's weapon in alleged RQ-170 affair?" *The DEW Line*, 5 December 2011, http://www.flightglobal.com/blogs/the-dewline/2011/12/avtobaza-irans-weapon-in-rq-17.html

44 Frank J. Cilluffo, *The Iranian Cyber Threat to the United States*. A Statement before the U.S. House of Representatives Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence and Subcommittee on Cyber security, Infrastructure Protection and Security Technologies, 26 April 2012, p. 5. http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20-%20Cilluffo.pdf

45 Scott Peterson, "Iran's cyber prowess: Could it really have cracked drone," *The Christian Science Monitor*, 24 April 2012, http://www.csmonitor.com/World/Middle-East/2012/0424/Iran-s-cyber-prowess-Could-it-really-have-cracked-drone-codes

46 Frank J. Cilluffo, p. 5.

47 Patterson, J.P & M.N. Smith, pp. 44-49.

48 Iftach Ian Amit, *Cyber [Crime|War],* Linking State Governed Cyber Warfare with Online Criminal Groups, paper presented at DEFCON 18 conference, 31 July 2010, http://www.defcon.org/images/defcon-18/dc-18-presentations/Amit/DEFCON-18-Amit-Cyber-Crime-WP.pdf

49 Khashayar Nouri, *Cyber Wars in Iran*, Institute for War & Peace Reporting, 23 July 2010, http://iwpr.net/report-news/cyber-wars-iran

50 Golnaz Esfandiari, "Basij Members Trained To Conquer Virtual World," Payvand Iran News, 21 August 2010, http://www.payvand.com/news/10/aug/1206.html

51 Jeffrey Carr, "Iran's Paramilitary Militia Is Recruiting Hackers," *Forbes*,12 January 2011, http://www.forbes.com/sites/jeffreycarr/2011/01/12/irans-paramilitary-militia-is-recruiting-hackers/

52 Bob Beauprez, "Iranian Cyber-Attack Plot against U.S. Exposed in Mexico," Townhall, 13 December 2011, http://finance.townhall.com/columnists/bobbeauprez/2011/12/13/iranian_cyberattack_plot_against_us_exposed_in_mexico/page/full/

53 SSl - Secure Socket Layer הנו פרוטוקול לתקשורת מאובטחת באינטרנט, המוודא שהשרת שאליו מתחבר הלקוח הנו השרת הנכון, תוך הצפנת המידע בין דפדפן הלקוח לבין השרת. ניתן לרכוש מפתחות SSL מספקים מורשים. גניבת מפתחות מאפשרת לגורם (שיש לו שליטה על תשתית הרשת) להסיט גולשים לאתרים מזויפים המתחזים להיות אתרים חוקיים, וכך לקבל גישה למידע חסוי של המשתמש.

54 דיווח החברה מה־13 במארס 2011, http://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html

55 Eva Galperin, Seth Schoen and Peter Eckersley, *A Post Mortem on the Iranian DigiNotar Attack*, Electronic Frontier Foundation, 13 September 2011, https://www.eff.org/deeplinks/2011/09/post-mortem-iranian-diginotar-attack

56 Fox-It, Interim Report, *DigiNotar Certificate Authority breach "Operation Black Tulip"*, 5 September 2011.

57 Toby Sterling, "Iran Involvement Suspected In DigiNotar Security Firm Hacking," HuffPost Tech, 5 September 2011, http://www.huffingtonpost.com/2011/09/05/iran-diginotar-hack_n_949517.html

58 Gerry Smith, "Cyber Attacks Against US Banks Sponsored By Iran, Lieberman Says," The Huffington Post, 9 September 2012, http://www.huffingtonpost.com/2012/09/21/cyber-attacks-banks-iran-lieberman_n_1904846.html

59 זהו ארגון שמטרתו לנתח ולשתף מידע בין הגורמים הפיננסיים לגבי איומים על שירותים פיננסיים חיוניים בארצות־הברית. (Financial Services Information Sharing and Analysis Center FS-ISAC)

60 Jaikumar Vijayan, "U.S. banks on high alert against cyberattacks," *Computerworld*, 20 September 2012, http://www.computerworld.com/s/article/print/9231515/U.S._banks_on_high_alert_against_cyberattacks

61 Jim Finkle, "Exclusive: Insiders suspected in Saudi cyber-attack," Reuters, 7 September 2012, http://in.reuters.com/article/2012/09/07/net-us-saudi-aramco-hack-idINBRE8860CR20120907

62 Kelly Jackson Higgins, "Shamoon Code 'Amateur' But Effective," Dark Reading, 11

September 2012, http://www.darkreading.com/advanced-threats/167901091/security/attacks-breaches/240007179/shamoon-code-amateur-but-effective.html

וגם Nicole Perlroth, "Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," *New York Times*, 23 October 2012, http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?_r=1&adxnnl=1&pagewanted=all&adxnnlx=1351084069-1i53F0BCczNEGcP8ut3n4A&

63 Associated Press, "Panetta hints Iran behind Gulf cyberattacks," CBS News,12 October 2012, http://www.cbsnews.com/8301-202_162-57531088/panetta-hints-iran-behind-gulf-cyberattacks

64 Jeffrey Carr, "Who's Responsible for the Saudi Aramco Network Attack?" Blogspot, 27 August 2012, http://jeffreycarr.blogspot.co.uk/2012/08/whos-responsible-for-saudi-aramco.html

65 Global Research & Analysis Team, "Shamoon the Wiper - Copycats at Work," Kaspersky Lab Expert, Securelist, 16 August 2012, https://www.securelist.com/en/blog?print_mode=1&weblogid=208193786

66 "Iranian hackers attacked three largest U.S. banks as part of cyber campaign: sources," National post from Reuters, 21 September 2012, http://news.nationalpost.com/2012/09/21/iranian-hackers-attacked-three-largest-u-s-banks-as-part-of-cyber-campaign-sources

67 Nicole Perlroth, 23 October 2012.

68 Associated Press, 12 October 2012.

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.

מאמר זה ראה אור לראשונה ב**צבא ואסטרטגיה**, כרך 5, גיליון 1, אפריל 2013, עמ' 49–65.

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 זדוני[3] 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 סינטַקטי (מִבני) 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 הסַרְכָזות בפּוּרים 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 מדַי, וגורמי בקרה והנדסה יכולים לבצעה. 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 בווירוסים 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 פוטנציאלי[10] (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 ידידותיות, 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 למגִנים, 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 ארמקו באוגוסט 2012[14] 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, שתקֵף לעימות מזוין, אמור לחול על מצב ההתקפה החדש. [17]

עידן המידע מאופיין בפעילות מדינתית גוברת בתחומי כלכלה, תשתיות אזרחיות, ביטחון לאומי, ביטחון אזרחי, תקשורת בין־ארגונית, חינוך, ניהול 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 מטרתם. 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 – מונָעים 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 בווירוסים 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 מחשוב כמאה 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 דמוריליזציה 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. שגרירויות 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 בשגרירויות.[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 ישראליים והדלפת מספרי

כרטיסי אשראי של אזרחים ישראליים בזמן העימות. "אנונימוס" אף פרסם רשימה של יותר מ־650 אתרים ישראליים, 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 ופשיעה 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 מונָעים 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	שימוש בנשק קיברנטי לניטור	מניעת שימוש ליכולת פסיכולוגית
המדינה			
מדינות רבות	יכולת תקיפה יכולה לגרום נזק פיזי (על פי מומחים) ולכן לא מן הנמנע כי מדינות רבות יפתחו יכולת זו בעתיד הקרוב.	יכולת ניטור לצורכי ביון ומודיעין.	יכולת זו היא פשוטה יחסית, ומדינה עלולה לחשוש שתיתקף על ידי מדינה אחרת בעזרת נשק מתקדם.
ארה"ב	המשאבים הדרושים לשימוש יכולת זו הם מצביל ליכולתם של מדינות רבות אחרות.	שימוש בנשק קיברנטי לצורכי ביון ומודיעין.	בשימוש ארגוני טרור, לדוגמה, כדי לגרום נזק פיזי.
סין	המשאבים הדרושים לשימוש יכולת זו הם מצביל ליכולתם של מדינות רבות אחרות.	שימוש בנשק קיברנטי לצורכי ביון ומודיעין.	
רוסיה	המשאבים הדרושים לשימוש יכולת זו הם מצביל ליכולתם של מדינות רבות אחרות.	שימוש בנשק קיברנטי לצורכי ביון ומודיעין.	
צפון קוריאה			
איראן			
ארגוני טרור	המשאבים הדרושים לשימוש יכולת זו הם מצביל ליכולתם של מדינות רבות אחרות.	שימוש בנשק קיברנטי לצורכי ביון ומודיעין.	
ארגוני פשיעה			
גורמים בודדים			

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 שאִפשרו 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 חולשה[31] במערכת המותקפת. חולשה יכולה להתבטא ברכיב תוכנה שבכתיבתו 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 Sql Injection, XSS ואחרות. אבל נניח שעל אותו שרת שבו מאוחסן האתר המאובטח נמצא אתר נוסף, חסר חשיבות ולא מאובטח בכלל. ניתן לתקוף את האתר הנוסף ודרכו להגיע אל המחשב המאחסן 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 כעַרפול (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 פליים[36] 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 לנצל[37] 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 הפִּרצה במערכת, הפצת טלאי אבטחה לכלל משתמשי התוכנה והתקנתו על המחשבים. השלב של סגירת הפרצה שדרכה חדר קוד זדוני למערכת הוא מורכב, כיוון שלאחר תיקון הפִּרצה 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 (MiniFlame[39]) 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 פיננסיות – 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 המרְכז: 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 מחשוב, לרוב בעלת אופי של גניבת מידע או שיבוש תהליכים במערכת, ואשר מורץ ללא ידיעת בעל המערכת או אישורו.

4 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

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 Cooparation, 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 המחשוב 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 שווייצר, 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 Guardian ו־McAfee
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, Hacktivism and Cyber terrorism, 269.

26 גיא גרימלנד ואחרים, "מתקפת סייבר", *TheMarker*, 16 בינואר, 2012.
http://www.themarker.com/markets/1.1618274

27 אור הירשאוגה 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 לווירוס מתחום הביולוגיה, המשתלט על תא חי ומנצל את כל המנגנונים של התא לצרכיו.

34 רננה 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.

כישלון שיטות הגנת הסייבר הקלאסיות – מה הלאה?

אמיר אורבוך, גבי סיבוני

מבוא

שיטות ההגנה הקלאסיות הנהוגות בעולם בעשרות השנים האחרונות אינן מצליחות לעצור התקפות פוגעניות (malware) מודרניות העושות שימוש בפרצות אבטחה שאינן מוּכרות (ולכן אין להן עדיין תיקון), שנקראות חולשות יום־אפס (zero-day vulnerabilities). דוגמאות להתקפות אלה על מחשבים ועל רשתות תקשורת של ארגונים עסקיים ושל ספקי תשתיות ושירותים חיוניים וקריטיים הן וירוסים, תולעים, דלת אחורית, סוסים טרויאניים – כלי ניהול/גישה מרחוק (RATs). שיטות ההגנה הקלאסיות, הכוללות אמצעי תוכנה וחומרה והמתבססות על חומות אש (FireWall), חתימות וחוקים (rules), תוכנות אנטי־וירוס, סינון תוכן, מערכות איתור חדירה (IDS) ודומיהם נכשלות לחלוטין בהגנה מפני איומים לא־מוּכרים, דוגמת איומים המבוססים על חולשות יום־אפס ואיומים חדשים. איומים מתוחכמים וחמקניים אלה מתחזים להיות מידע ונתונים אמינים וחוקיים במערכת, ולכן מערכות ההגנה הקלאסיות אינן מספקות את המענה ההגנתי הדרוש. מערכות ההגנה המקובלות כיום מגֻנות מפני התקפות מוּכרות על סמך חתימות ידועות וניתוח לאחור של התקפות, על מנת לייצר באופן היוריסטי,[1] אבל הן חסרות תועלת מול ההתקפות המתרבות והולכות שאינן מוכרות, וחסרות כל חתימה. לפתרון בעיה זו דרושים חשיבה ופתרונות אחרים. מאמר זה מציע גישת הגנה עדכנית, שבבסיסה ניתוח מידע רגיש שעליו יש להגן, למטרת זיהוי התנהגויות אנומליות.[2] המידע המנותח כולל את פעילות התקשורת הארגונית (datasilos) כמקור להבנת

פרופ׳ אמיר אורבוך הנו חבר סגל בית הספר למדעי המחשב באוניברסיטת תל־אביב וחוקר במסגרת תוכנית ניובאוור ללוחמת סייבר במכון למחקרי ביטחון לאומי.
אל״מ (מיל.) ד״ר גבי סיבוני הוא ראש תוכנית צבא ואסטרטגיה וראש תוכנית לוחמת סייבר במכון למחקרי ביטחון לאומי.
מאמר זה נכתב בסיועו של אביב רוטברט, תלמיד לתואר שלישי, מלגאי בתוכנית ניובאוור במכון למחקרי ביטחון לאומי.

מאמר זה ראה אור לראשונה ב**צבא ואסטרטגיה**, כרך 5, גיליון 1, אפריל 2013, עמ׳ 37–48.

התנהגות לא־רגילה (אנומליות), המעידה ברוב המקרים על קיום פוגענים במערכת. המאמר מציע להתבסס על הנתונים שעליהם יש להגן כמקור ידע לפיתוח מערכת ההגנה. ניתוח אנליטי של נתונים מסיביים (BIG-DATA Analytics) יאפשר זיהוי פוגענים כאלה תוך בניית מודל המאפשר אמינות גבוהה של זיהוי ומזעור התרעות השווא (false positive), המהוות אתגר לכל מערכת הגנה.

התפתחות האיומים והמגבלות של שיטות ההגנה המסורתיות

התקפות הסייבר הראשונות על מחשבים התבססו על וירוסים או תולעים המשכפלים עצמם ומתפשטים במהירות. אולם טכנולוגיית האנטי־וירוס נכשלה לחלוטין ונמצאה לא יעילה באיתור סוסים טרויאניים, שהתנהגותם שונה לחלוטין משל וירוסים. באופן מסורתי, מערכות ההגנה התפתחו כדי להגן מפני וירוסים מוכרים, מאחר שקיים קושי מהותי לזהות וירוסים אלה על פי התנהגותם ולא על פי מאפייני הזיהוי שלהם (חתימה). כך ניתן היה לייצר בסיסי מידע עם חתימות של וירוסים, ולהשוות קבצים ותקשורת המגיעים למחשבים מול חתימות אלה. גישה זו חייבה את יצרני תוכנות הגנה לעקוב באופן מתמשך אחר התפתחות הוירוסים כדי לייצר חתימה שלהם, ועל ידי כך להפיץ עדכונים ללקוחות כדי לאפשר להם לעדכן במהירות האפשרית את המערכות שבהן מותקנות תוכנות ההגנה שמתבססות על חתימות אלה. ההתפתחות הנרחבת בפיתוח וירוסים ופוגענים שונים וגידול עצום במספרם גרמה וגורמת לתהליך בלתי־אפשרי, המחייב השקעה של משאבים רבים בעדכון מתמשך של מאגרי נתוני החתימות של תוכנות אנטי־וירוס.

ניתן לחלק את סיכוני מתקפות סייבר באופן גס למשפחות הבאות: נוזקות, רוגלות, תולעים וסוסים טרויאניים (הפותחים 'דלתות אחוריות'[3]). חלוקה המתייחסת יותר למושא התקיפה כוללת: התקפות מתמשכות מתקדמות (Advanced Persistent Threats or APTs), שהחלו במתקפות סייבר של מדינות נגד רשתות צבאיות וארגוני ממשלה, ובשנים האחרונות התפתחו לתקיפה בעוצמה מדינתית של רשת ארגונית או תשתית קריטית אזרחית, ותקיפות של מערכות בקרה תעשייתיות המופעלות על ידי מחשבים (SCADA), כגון סטקסנט (Stuxnet). כך, מערכות של תשתיות חיוניות הנשלטות באמצעות מערכות בקרה תעשייתיות שבהן שולט פרוטוקול ה־SCADA חשופות לפגיעה העלולה להשבית את השירות החיוני, או אף לגרום נזק פיזי. נוסף לאלה – מתקפות על מערכות אלחוטיות ותחנות שידור ניידות, שימוש ברשתות חברתיות לצורכי הפצת רוגלות, נוזקות, ותקיפה של שירותי אחסון ומחשוב בענן.

מרחב התקיפה בסייבר ניתן לחלוקה הכוללת שני סוגי תקיפות שמנצלות חולשות רבות, כולל חולשות של יום־אפס:

תקיפות כלליות (Broadcast Attacks) – תקיפות המנסות לפגוע במחשבים ללא כל אבחנה. במסגרת תקיפות אלה ניתן למצוא גם הדבקה רחבה של סוכני תוכנה על מנת ליצור רשת שלמה של מחשבים שבויים (Botnet), וזאת כדי לגרום למחשבים אלה להפעיל מאוחר יותר פקודות עצמאיות, או למשוך פקודות מתוך שרת שליטה. כאמור לעיל, בדרך כלל, כשמידע על איומים חדשים מגיע לחברות האנטי־וירוס מזהים את חתימתם או חוקרים אותם באופן היוריסטי, וכך, באמצעות עדכונים שוטפים, ניתן להגן על המחשבים מפני תקיפות אלה. לאור קהל המטרה הנרחב, סביר להניח שהמידע על איומים כאלה יגיע במהרה לחברות הרלוונטיות ויוכנס לגרסאות עתידיות של מוצריהן. בחלק מהמקרים, מטרת תקיפה מסוג זה היא להגיע לכמות גדולה של מחשבים, למשל: עובדים (במקרה של התקפה על רשת ארגונית) או לקוחות (במקרה של התקפה על מוסד פיננסי, ניסיון לגנוב כרטיסי אשראי שבהם נעשה שימוש באינטרנט וכו'). לאחר הדבקת המחשב מותקן בו סוס טרויאני, המאפשר גניבת מידע או גישה מרחוק. תקיפות כאלה כוללות קוד זדוני מסוגים שונים, ואף קודים המשתַנים מהדבקה להדבקה, כדי להקשות את הגילוי באמצעות חתימה (וירוס רב־צורתי – Polymorphic Viruses). עדיין לא קיימת הגנה מלאה, משום שמפתחי סוסים טרויאניים בוחנים בצורה עקבית האם תוכנות האנטי־וירוס כבר זיהו את הקוד המפַגע וייצרו את החתימה או את קבוצת החוקים ההיוריסטיים המיירטת אותו. ברוב המקרים, אם מערכות הגילוי מצליחות לזהות את הקוד המפַגע, המפתחים מבצעים שינויים בדרך ההדבקה או ההפעלה שלו, כדי למנוע את הגילוי. לפיכך, קיימים סוסים טרויאניים רבים המצליחים להתחמק באופן עקבי מגילוי על ידי תוכנות ההגנה מובילות.

תקיפות ממוקדות (Targeted Attacks) – תקיפות אלה מתוכנתות במיוחד לצורך ספציפי ומנצלות חולשות שאינן מוכרות במערכות ההפעלה או בתוכנות מוכרות ונפוצות, תוך איתור עצמאי של חולשות חדשות. מטבע הדברים, הרוב המכריע של תוכנות האנטי־וירוס מבוסס על הגנת חתימה, הן אינן מסוגלות לזהות ולמנוע תקיפות מסוג זה, וקהל המטרה המצומצם מאפשר לתקיפות כאלה לחמוק "מתחת למכ"ם" של יצרני האנטי־וירוס. ראוי לציין שעולם האיומים מתפתח בצורה מהירה לכיוון של מתקפות ממוקדות על יעדים איכותיים.

תעבורת הנתונים ברשת תקשורת מודרנית היא רבה מאוד, בשל הצורך לספק שירותים רבים לתחנות קצה מסוגים שונים, ביניהן: מחשבים אישיים, תחנות עבודה, שרתים, מתגים וציוד תקשורת, ועוד יחידות רבות ומגוונות. באלה עושים שימוש משתמשים רבים, שברובם הגדול אינם בעלי גישת אבטחה כלשהי. כתוצאה מתופעה זו, התקפות APT מתמקדות לא רק במכונות אלא גם באנשים, לדוגמה: דרך השימוש ברשתות חברתיות. כך למשל, ההתקפה על חברת RSA שכוונה

לאנשים בארגון, והצליחה לחדור למערכות מאובטחות ביותר.[4] בשנים האחרונות אנו עדים לעלייה דרמטית בהיקף של התקפות חדשות מתוחכמות ולא מתועדות, בעלות אופי חמקני. הדבר מתבטא הן בקבוצת התקיפות הכלליות והן באלה הממוקדות. התקפות אלה מתגברות על כל ההגנות הקלאסיות והתקניות של החברות המובילות את תחום ההגנה כיום. מאחורי פיתוח אמצעי התקיפה עומדות השקעות בקנה־מידה גדול של מדינות ושל ארגוני פשיעה, כשהיקף הנזקים הוא רחב מאוד.[5] למעשה, קיימת עלייה עצומה בכמות הפוגענים המצליחים לחדור את כל מערכות ההגנה הקיימות, והמתגברים על כל ההגנות הקלאסיות המתבססות על חתימות וחוקים. העלייה הינה במאות אחוזים משנת 2011 עד ימים אלה.[6]

מערכות ההגנה הקיימות כיום מתבססות בעיקר על מניעה וסיכול של איומים מוּכרים, תוך שימוש בחתימות ובחוקים ידועים מראש. מערכות אלה אינן יכולות לגלות מתקפות יום־אפס שאין להן חתימה ידועה ברגע נתון. כך גם מתקשות המערכות הללו לזהות סוסים טרויאניים ודלתות אחוריות, כשלהתקפות מתוחכמות וחמקניות רבות אין חתימות ידועות. הם חודרים כמעט לכל מערכת מחשוב משום שהם נראים כנתונים וקודים חוקיים ואינם נראים פוגעניים. תקיפות מצליחות לחדור לרשתות הארגוניות ולמחשבי הקצה למרות כל מערכות ההגנה, בשל העובדה כי ההופעה וההתנהגות הראשונית של הפוגענים נראית חוקית ותקינה. נוסף לכך, רוב המערכות המבצעיות כיום בנויות לטיפול בסוג מסוים של התקפה, ואין להן יכולת לטפל במגוון גדול של התקפות שונות בעלות מוטציות וגרורות.

אחת הדרכים לאתר תקיפות שאינן מוּכרות ושאינן חתומות באמצעות תוכנות ההגנה המקובלות היא על ידי זיהוי התנהגות א־נורמלית של קודים שוהים במערכות הארגוניות, השונה מההתנהגות נורמלית של מרבית הנתונים. התנהגות שונה זו תסגיר את הקודים הזדוניים. בגישה זו, התנהגות לא־רגילה של רכיב תוכנה המנסה לבצע פעילות שאינה מורשית יכולה להוות בסיס אפשרי לזיהוי ולמניעת מתקפות. יצרני תוכנות ההגנה בעולם מבינים את האתגר ופועלים כדי לספק יכולות זיהוי כאלה. אולם, כאן טמון האתגר המשמעותי ביותר – הקושי לספק כלי אמין שלא יפיק התרעות שווא ושלא יפגע בצורה משמעותית בחוויית המשתמש. התרעות השווא הנן אחד האתגרים המשמעותיים ביותר של מערכות הגנה. התרעת שווא נוצרת כאשר המערכת מתריעה על קוד חוקי שהתנהגותו נורמלית, ומגדירה אותו כקוד זדוני או כחשוד ככזה. עומס רב מדי של התרעות שווא כאלה פוגע בצורה מהותית ביכולת העבודה במערכות המחשוב, ועלול לגרום למשתמשים לאבד את האמון במערכת ההגנה. אתגר שני הוא המענה לקוד זדוני החומק ממערכת ההגנה. תופעה זו קרויה false negative – כאשר מתקבלת תוצאה הנראית שלילית, אך למעשה היא חיובית. (בדומה לנשא נגיף של מחלה

חמורה, המקבל תוצאות בדיקת מעבדה שליליות באשר לנוכחות הנגיף בגופו). שני אתגרים אלה הנם ליבת העיסוק בתחום מערכות ההגנה בכלל, ובתחום השימוש בניתוח התנהגות אנומלית של קוד זדוני במערכות מידע בפרט.

זיהוי אנומליות כגישה למענה אופרטיבי

מאמר זה יתרכז בדיון על הגנה המבוססת על איתור אנומליות ברשתות תקשורת, ברבדיה השונים. הבעיה רחבה יותר וכוללת את הצורך בזיהוי אנומליות של קודים זדוניים שהוחדרו בנקודות תורפה בתוכנות וביישומים (applications). גישת הגנה זו אינה נדונה במאמר זה, אלא אם כן, הקוד הזדוני נחשף בתקשורת הארגונית. למרות האמור לעיל, ניתן להניח שחלק מהרעיונות המוזכרים מתאימים גם למציאת אנומליות בתוכנות וביישומים.

אנומליות שהוצעו לראשונה בשנת 1987[7] הן סטיות מההתנהגות המצופה, שהיא ההתנהגות הנורמלית. ההנחה הבסיסית עבור כל מערכת למציאת אנומליות היא שלנתונים זדוניים (malicious) יש מאפיינים שאינם קיימים בהתנהגות הנורמלית שאופיינה בזמן הלמידה. מאז פותחו תיאוריות ומתודולוגיות נוספות המתבססות על גישות של למידת מכונה (Machine Learning) ועל תורת האינפורמציה[8] כגון רשתות עצביות,[9] מכונת וקטורים תומכים (support vector machine),[10] אלגוריתמים גנטיים[11] ועוד רבים אחרים. כמו כן קיימות גישות רבות העושות שימוש בכריית נתונים לשם מציאת קוד זדוני.[12] סקירה כללית על איתור אנומליות מובאת במאמרם של Chandola & Banerjee[13], וכן מובא מחקר על שיטות לאיתור קוד זדוני.[14]

אחת הגישות לאיתור התקפות על נתונים מרשתות תקשורת נעשית באמצעות ניטור (monitoring) האנומליות של הפעילות הרשתית, על ידי מציאת הסטייה מפרופיל נורמלי שנלמד מנתונים שפירים (תקינים, לא־פוגעניים). מתודולוגיה זו מתבססת על כלים שנלקחו ממחקרים על למידת מכונה,[15] אנליזה מתמטית וסטוכַסטית[16], סטטיסטיקה, כריית נתונים, תורת הגרפים, תורת האינפורמציה, גיאומטריה, תורת ההסתברות ותהליכים אקראיים, ועוד. כלים של למידת מכונה וכריית נתונים בשילוב המתודולוגיות שהוזכרו משמשים בהצלחה בתחומים רבים אחרים כמו מערכות להמלצת מוצרים של Amazon,[17] Netflix,[18] זיהוי תווים אופטי,[19,20] תרגום של שפה טבעית,[21] זיהוי דוא"ל זבל (spam).[22] למידת מכונה עוסקת בפיתוח אלגוריתמים שיאפשרו למחשב ללמוד על סמך דוגמאות. קיימת למידה מונחית של נתונים ידועים מראש (supervised), שבה יודעים מראש את המשמעויות הנכונות של הפרמטרים, כלומר, לנתונים יש תוויות סיווג (labeled); בלמידה בלתי־מונחית (unsupervised) מטרת האלגוריתמים היא למצוא ייצוג

פשוט של הנתונים, ללא תוויות סיווג. למידה מונחית מוגבלת יותר מבחינת תכולת הנתונים הנלמדים, אבל מצד שני, התוצאות אמינות יותר ולכן היא עדיפה.

הלמידה הראשונית נעשית על קבוצת נתונים "בריאה", שניתן להניח שאין בה פוגענים כלשהם. קבוצה זו נקראת קבוצת הלימוד (training set). רצוי בדרך כלל ששיטת הלמידה תדע לאבחן האם חלק מקבוצת הלימוד כולל פוגענים עד אחוז מסוים מסך־כל הנתונים. ברור שאם רוב קבוצת הלימוד מכיל פוגענים, אזי הם יילָמדו ויזוהו כנתונים נורמליים. כחלק מתהליך הסינון מופעל לעיתים תהליך הנקרא 'הסרת חריג החשוד כחריג' (outlier removal), שמוציא מקבוצת הלימוד נתונים הנראים כרעשים או זיהום.

קבוצת הלימוד מנותחת על ידי מגוון שיטות מתמטיות קיימות, לצד שיטות חדשניות. באמצעות תהליך זה ניתן לאתר את המאפיינים הנורמליים של הנתונים הנבחנים. למידה מסוג זה נקראת One Class. לעומתה קיימת שיטה שבה המאפיינים נלמדים על ידי השוואת קבוצת לימוד המכילה נתונים נקיים ולא־נקיים (לדוגמה: דוא"ל עם או בלי ספאם), הנקראת Binary Class. קבוצת הלימוד נגזרת מתוך מסת הנתונים הנצברת והנשמרת בארגון יחד עם נתונים חדשים הנשמרים באופן שוטף. למטרה זו פותחו שיטות ללמידת הנתונים המאפיינים את ההתנהגות הנורמלית. הבנת הגיאומטריה[21] של הנתונים הנלמדים היא אחת משיטות הניתוח, אולם קיימות שיטות נוספות. לדוגמה: בתהליך המתואר להלן מתואר מבנה כללי אפשרי של אלגוריתמים המופעלים והמעבדים את קבוצת הלימוד, במטרה למצוא את המאפיינים של ההתנהגות הנורמלית (התקינה):

1. פירוק כל יחידת נתונים בסיסית של תקשורת או אירוע למאפיינים (features, parameters).
2. כימות היחסים בין המאפיינים. קיימות מספר שיטות לאפיון היחסים הללו. שיטת גרעין (kernel Method)[23] היא אחת מהמתודולוגיות הנפוצות שבעזרתה מגדירים יחסים בין המאפיינים. בדרך כלל נעשה שימוש בפונקציות מרחק מתמטיות להגדרת היחסים הללו. אלה הם יחסי קִרבה וריחוק שמגוון תכונות מקיימות ביניהן. לאחר שלב זה נשמרים היחסים שבין נתוני התקשורת או האירועים.
3. הורדת ממד (dimension) הנתונים. בדרך כלל ממד הנתונים גבוה והוא נקבע לפי כמות המאפיינים שמרכיבים יחידת תקשורת בסיסית או יחידת אירוע בסיסית. לכן מורידים את ממד הנתונים[22] (לדוגמה, מעשרה מימדים לשניים) תוך שימור היחסים והקוהרנטיות בין המאפיינים שאותרו בשלב הקודם. הדבר דומה לפעולת דגימה שבה בוחרים בצורה מושכלת רק חלק קטן מהנתונים המקוריים, שמייצגים אותם בצורה נאמנה. נדרשת חדשנות מתמטית, אלגוריתמית וחישובית כדי לעבד נתונים מממד גבוה שיתאימו למחשב ושייצגו בצורה טובה

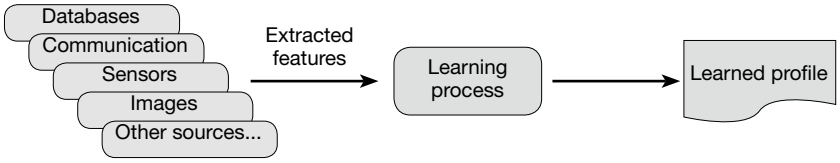
ומהימנה את נתוני המקור. הדגימה שמטרתה לצמצם את נפח הנתונים יכולה להיות אקראית, וניתן להוכיח שהיא משמרת את הקוהרנטיות של הנתונים. לשם כך יש שיטות מתמטיות רבות. אחת השיטות לייעול החישובים כדי לבנות מייצג קומפקטי של נתונים רבי־ממדים היא בניית מילונים (dictionaries),[24] שגורמים להאצה בחישובים תוך שימור היחסים והתכונות שאותרו לפני הורדת הממד. שיטות אחרות להאצת החישובים מאפשרות דילול (sparsification) של הנתונים[24,25] מטרת הגישות הללו היא אפיון הפרופיל הנורמלי של הנתונים מתוך קבוצת הלימוד, תוך התגברות על הבעיות החישוביות הכבדות בעיבוד קבוצת הלימוד. פעולת הלמידה היא בדרך כלל כבדה מבחינה חישובית. פעולה זו נעשית ברקע (offline) ואינה נדרשת לפעול בזמן אמת. שיטות נפוצות הנן: PCE,[25] LLE,[26] ISOMAP,[27] ועוד.

השיטות שתוארו לעיל מאפשרות לעבד ביעילות את קבוצת הלימוד שהיא "כבדה" ואף עלולה להיות בלתי־אפשרית מבחינה חישובית. מטרת עיבוד קבוצת הלימוד היא לאפיין את ההתנהגות הרגילה (הנורמלית) של נתוני הלימוד על סמך הבחינה של קבוצת הלימוד ועל בסיס היחסים שהוגדרו בין המאפיינים של הנתונים והאירועים של קבוצת הלימוד, בהנחה שהלמידה והמסקנות ממנה ישקפו את ההתנהגות הנורמלית של כל הנתונים החדשים העתידיים, שלא היו חלק מקבוצת הלימוד. ככל שנפח הנתונים של קבוצת הלימוד גדול יותר והמאפיינים רבים ומגוונים יותר, מאפייני ההתנהגות הנורמלית שהוסקו מקבוצת הלימוד יהיו אמינים יותר. אבל אז הסיבוכיות החישובית עולה, ולכן צריך להשקיע מאמץ רב בייצור אלגוריתמים שהם יעילים מבחינה חישובית ויכולים לטפל בנפחי נתונים גדולים.

התהליך המתואר מפרט מודל למידה אפשרי המייצר אפיון של ההתנהגות הנורמלית של הנתונים העתידיים בעזרת הפרופיל הנורמלי של קבוצת הלימוד. מכאן ואילך בודקים את המאפיינים של כל נתון חדש שמגיע או של אירוע חדש. מעבדים את המאפיינים הללו כדי לראות האם הם סוטים מהפרופיל הנורמלי שנלמד ונקבע בזמן הלימוד (אנומליה). הסטיות מהפרופיל הנורמלי צריכות לאתר את המתקפות המאופיינות כמתקפות יום־אפס. בשיטה שתוארה עד כה לא משתמשים בחתימות אלא במציאת סטיות התנהגותיות מהפרופיל הנורמלי שנוצר מעיבוד קבוצת הלימוד.

תרשים 1 הוא תיאור של תהליך הלמידה שתואר לעיל. התרשים מראה גם את מגוון המקורות שמהם נשאב המידע לצורכי הלימוד הראשוני.

תרשים1: תהליך הלמידה



השיטות הללו ונגזרותיהן למציאת פוגענים על ידי ניטור ההתנהגות של הנתונים ניתנות להפעלה בשני אופנים שונים, המשלימים זה את זה באופן השימוש בהם, כשהמשותף הוא למידה ברקע (offline) של נתוני התקשורת מהפרוטוקול שדרכו מגיעים הנתונים לארגון (כמו למשל: port 443 (HTTPS), UDP port 53 (DNS) ,TCP port 80 (HTTP), TCP שהם גם פרוטוקלי web), ובניית הפרופיל שמתאר את ההתנהגות הנורמלית של נתוני הפרוטוקול המסוים שאותו יש לבדוק, על פי קבוצת הלימוד.[28]

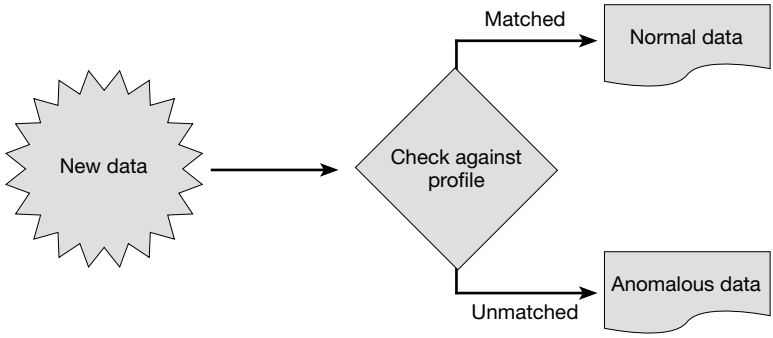
1. **הפעלה בזמן אמת** – האלגוריתם למציאת אנומליות בנתוני תקשורת (ממומש בתוכנה או בחומרה) ממוקם בכניסה לארגון, אחרי שעבר את כלי ההגנה הרגילים של IDS, IPS FireWalls (חתימות וחוקים אֶפשרו לו להיכנס), ואז הוא בודק כל יחידת תקשורת – האם התנהגותה מתאימה לפרופיל הנורמלי שנלמד מקבוצת הלימוד. אם הוא התגלה כאנומליה, דרכו לתוך הארגון נחסמת. היות שלא משתמשים בחתימות, הניתוח של מהות האנומליה ייעשה אוטומטית או ידנית.
2. **הפעלה ברקע** – מציאת פוגענים ברקע. נתוני התקשורת שנכנסו לארגון דרך כל מערכות ההגנה נראים כנתונים חוקיים ומתחילים לפעול לאחר מכן, כמו רשת מרגלים שנטמעים בסביבה ומתחילים לפעול בזמנים עתידיים. לצורך כך יש לעבד לוגים ואירועים שהתרחשו בעבר ומתרחשים כעת. כדי לעבד מידע של לוגים שנשמרו וחדשים שמגיעים משתמשים כיום בטכנולוגיית Security Information and Event Management (SIEM). SIEM היא מערכת ניטור אבטחת מידע נפוצה ברשתות ארגוניות, ומשמשת כמקום מרכזי לשמירה ולפענוח של לוגים ואירועים של נתוני התקשורת. SIEM היא הארכיון של כל נתוני התקשורת והאירועים, ובעזרתה אפשר לבצע ניתוחים "משפטיים" (forensic) למציאת אנומליות.

ניתן להפעיל את השיטות למציאת אנומליות שתוארו במאמר על הנתונים ש־SIEM אספה. אפשר להפעיל גם כלי כריית נתונים אחרים על נתוני ה־SIEM. ל־SIEM יש שתי פונקציות (מרכיבים) עבור ניהול הביטחון: Security information management (SIM) ו־Security event management (SEM). בשיטה שעושה

שימוש בנתונים של SIEM צריך להפעיל בהתמדה את המתודולוגיה למציאת אנומליות כדי לאתר את פעולתם של הפוגענים, כאשר יפעלו במועד עתידי כלשהו.

תרשים 2 מתאר תהליכים לבדיקת המידע לאור תוצאות ניתוח הלמידה.

תרשים 2: תהליך הזיהוי



שימוש ב BIG-DATA למציאת אנומליות – הנתונים והאירועים מכתיבים את אופן הזיהוי

הרעיון המרכזי בבסיס מציאת האנומליות כפי שתואר לעיל הוא אפיון ההתנהגות של הנתונים בקבוצת הלימוד, והסקה מהם על התנהגות הנתונים שלא השתתפו בקבוצת הלימוד, כלומר, אפיון הנתונים החדשים שיגיעו. במילים אחרות, הנתונים מכתיבים את העיבוד, והדבר מתבטא באלגוריתמים שמכוונים ללמוד את הנתונים כפי שהם ולהסתגל אליהם. זאת בניגוד לכל ההגנות מפני פוגענים הקיימות כיום, שאין להן שום קשר להתנהגות הנתונים, אלא הן מחפשות דפוסים (patterns) של פוגענים ידועים זה כבר. במקרה של נתוני תקשורת, מנתחים את הנתונים מכל יחידת אינפורמציה של הפרוטוקול שאותו מנטרים. מוצאים את היחסים ביניהם על סמך שיטות גרעין ומשכנים אותם באופן לא־לינארי במרחבים עם ממד נמוך יותר. כך מורידים את ממד הנתונים שבדרך כלל הוא גבוה, והדבר מאפשר למצוא אנומליות באופן יעיל.

הנתונים שבהם נחפש אנומליות הם נתונים שמכונים כיום BIG-DATA. אלה נתונים בהיקף עצום הנאספים מכלל מקורות המידע הזמינים ברשת הארגונית. בארגונים רבים הם נשמרים על ידי מתודולוגיית SIEM. לפי אריק שמידט, מנהלה־לשעבר של גוגל, כמות נתונים של חמישה אקסה־בייט (Exabyte) [29] נוצרו משחר הציוויליזציה ועד שנת 2003. לטענתו של שמידט, כמות זו נוצרת עתה כל יומיים.

להלן מספר דוגמאות ליצירה של BIG-DATA: הבורסה של ניו יורק (NYSE) מייצרת מדי יום 1TB של נתונים, Facebook מייצר כל יום 20TB של נתונים דחוסים והמאיץ ב־CERN שבשווייץ מייצר מדי יום 40TB של נתונים. לפי דוח שפורסם[30], נפח הנתונים גדֵל פי שניים מדֵי שנה, ולפחות מחצית מן העסקים שומרים את הנתונים במשך שלוש שנים לפחות, לצרכים אנליטיים. חלקם מחויבים לפי חוק לשמור נתונים אלה במשך מספר שנים. מקורות חדשים בכמויות עצומות צצים כל הזמן בעסקים שונים כמו שירותים (utilities). חלק ניכר (80%) מנתונים אלה אינם מובְנים (unstructured), ולכן אינם ניתנים לשימוש יעיל בארגון. BIG-DATA הפך מקור לכריית מידע המאפשר לאתר פוגענים. לחברות רבות וידועות יש BIG-DATA יומיומי, כמו Facebook, Google, Amazon, LiveJournal, Wikipedia וזו רשימה חלקית מאוד. BIG-DATA נשמר כיום גם בענן. כמות הנתונים שנאגרת בכל ארגון היא עצומה ואף גדֵלה עם הזמן. כדי לטפל בנפחי נתונים גדולים (data silos) פותחו כלים לעיבוד BIG DATA שאינם קשורים לכריית נתונים או למציאת אנומליות כגון Hadoop[31], MapReduce[32] ו־Memcached[33,34] – מסדי נתונים מקביליים[35] עצומים שמאפשרים לבצע שאילתות מהירות עליהם. בנוסף מפתחים "צינורות" תקשורת רבים (חברת Mellanox) להעברה מהירה של כמויות הנתונים הללו. מאמץ רב מושקע בפיתוח כלים מתקדמים לעיבוד יעיל של BIG-DATA. לכן, הוא יכול להיות מקור למציאת קשת נרחבת של אנומליות התנהגותיות מתוחכמות של פוגענים שונים.

סיכום

כדי לעבד BIG-DATA ולאתר פוגענים "איכותיים" ביעילות, יש לשלב בין כל השיטות שהוזכרו לעיל. הוזכרו כלים שרובם לא־לינאריים, המצמצמים את הנפח של BIG-DATA שהוא רב־ממדי בלי לפגוע בקוהרנטיות של הנתונים, תוך הקפדה על יעילותם של האלגוריתמים, כדי לטפל בנפחי נתונים עצומים. צירוף השיטות שהזכרנו במאמר זה הוא: ביצוע למידה מתוך קבוצה קטנה של נתונים, הפעלת שיטת גרעין על הנתונים שקובעת את היחסים (המרחקים) בין נקודת הדגימה, הורדת ממד הנתונים על ידי דגימה בדידה או אקראית של הנתונים. הדבר מדלל את הנתונים וכך מקבלים "שיכון" יעיל של BIG-DATA רב־ממדי במרחב עם ממד נמוך יותר משמעותית, ובו מבצעים את זיהוי האנומליות. בניית מילונים והפעלה של אלגוריתמים חכמים ויעילים, יחד עם כלים לעיבוד BIG-DATA – כל אלה פותחים אפשרויות רבות למציאת פוגענים בכל ארגון, על ידי אפיון ההתנהגות הנורמלית ואיתור סטיות ממנה.

הגישה המוצעת היא שילוב בין אנליזה של BIG-DATA בעלת יעילות חישובית גבוהה וכלים מתקדמים למציאת אנומליות שהן הפוגענים של מתקפות יום־אפס

שאין להם עדיין חתימות ודפוסי התנהגות ידועים. המתודולוגיה שנדונה כאן חייבת למצוא "סיכה" באוקיינוס של נתונים.[36] נקודת המוצא היא שהאלגוריתמים המוצעים מתאימים את עצמם ומסתגלים לנתונים עצמם. הנתונים הם שמכתיבים את אופן פעולת האלגוריתמים. המתודולוגיה המוצעת במאמר משלבת הבנת מבנה הנתונים על ידי למידה מתוך קבוצה קטנה, והסקת מסקנות לגבי ההתנהגות העתידית של הנתונים שלא השתתפו בקבוצת הלימוד. מתודולוגיה זו מסוגלת לאתר פוגענים שפעילותם מיידית, וכאלה שנכנסו לארגון ופועלים מאוחר יותר כמו סוסים טרויאניים.

הערות

1 באופן היוריסטי הנו באמצעות חוקים המסייעים לגילוי הקוד המַגע.

2 התנהגות אנומלית של קוד תוכנה או מידע הנה התנהגות לא־רגילה (לא־אופיינית), המעלה חשד לקיומו של פוגען במערכת.

3 פרצת אבטחה המאפשרת גישה למחשב ללא צורך באימות זהות. יכולה לנבוע משגיאת תכנות, מפרצה מכוונת בקוד מקור או כתוצאה מהתקנת תוכנה ייעודית (כגון סוס טרויאני).

4 Gabi Siboni and Y. R., "What Lies behind Chinese Cyber Warfare", *Military and Strategic Affairs*, Volume 4, No. 2, (September 2012), pp. 43-56.

5 Symantec, "Internet Security Threat Report 2011" *Trends, Vol. 17*, April 2012.

6 *FireEye Advanced Threat Report - 1H*, 2012. http://www2.fireeye.com/advanced-threat-report-1h2012.html

7 D.E., Denning, "An Intrusion-Detection Model, IEEE Trans*", Software Eng.,* Vol. SE-13 (2), 1987, pp. 222-232.

8 W. Lee and D. Xiang, "Information-Theoretic Measures for Anomaly Detection", in *Proc. IEEE Symposium on Security and Privacy*, 2001.

9 Z. Zhang, J. Li, C. Manikopoulos, J. Jorgenson, and J. Ucles," HIDE: a Hierarchical Network Intrusion Detection System Using Statistical Preprocessing and Neural Network Classification", in *Proc. IEEE Workshop on Information Assurance and Security*, 2001.

10 W. Hu, Y. Liao, and V. R. Vemuri, "Robust Anomaly Detection Using Support Vector Machines", in *Proc. International Conference on Machine Learning*, 2003.

11 C. Sinclair, L. Pierce, and S. Matzner, "An Application of Machine Learning to Network Intrusion Detection", in *Proc. Computer Security Applications Conference*, 1999.

12 M. A. Siddiqui, *Data mining methods for malware detection*, PhD Dissertation, University of Central Florida, 2008.

13 V. Chandola, A. Banerjee, V. Kumar, "Anomaly detection: A survey", *ACM Computing Surveys (CSUR)*, 41(3), article 15, 2009.

14 N. Idika, A.P. Mathur, *A survey of malware detection techniques*, Dept. of Computer Science, Purdue University, 2007.

15 R. Sommer and V. Paxson, "Outside the Closed World: On Using Machine Learning For Network Intrusion Detection", *Proc. IEEE Symposium on Security and Privacy*, May 2010.

16 תהליכים סטוכסטיים הם תהליכים שבהתפתחות שלהם במשך הזמן מעורבת מידה מסוימת של אקראיות בכל רגע נתון.

17 G. Linden, B. Smith, and J. York, "Amazon.com Recommendations: Item-to-Item Collaborative Filtering", *IEEE Internet Computing*, vol. 7, no. 1, pp. 76–80, 2003.

18 J. Bennett, S. Lanning, and N. Netflix, "The Netflix Prize", in *Proc. KDD Cup and Workshop*, 2007.

19 L. Vincent, Google Book Search: "Document Understanding on a Massive Scale", 2007.

20 R. Smith, "An Overview of the Tesseract OCR Engine", in *Proc. International Conference on Document Analysis and Recognition*, 2007.

21 F.J. Och and H. Ney, "The Alignment Template Approach to Statistical Machine Translation", *Comput. Linguist.*, vol. 30, no. 4, pp. 417–449, 2004.

22 P. Graham, "A Plan for Spam", in *Hackers & Painters*, O'Reilly, 2004.

23 B. Scholkopf and A. J. Smola, *Learning with Kernels: Support Vector Machines, regularization, Optimization, and Beyond*, The MIT Press, 2002.

24 M. Elad, "Sparse Redundant Representations", From *Theory to Applications*, Springer, 2010.

25 I.T. Jolliffe, *Principal Component Analysis*, Springer, New York, 1986.

26 S.T. Rowels, L.K. Saul, "Nonlinear dimensionality reduction by locally linear embedding", *Science*, Vol. 290 no. 5500 pp. 2323-2326, (2000).

27 J.B. Tenenbaum, V. de Silva and J.C. Langford, "A global geometric framework for nonlinear dimensionality reduction", *Science*, Vol. 290 no. 5500 pp. 2319-2323, (2000).

28 גישה זו מאפשרת גם בקרת ביצועים, ניתוח התנהגות משתמשים, ניתוח יחסי אדם־מכונה ובקרת תהליכים.

29 Exabyte = billion billion bytes

30 http://techcrunch.com/2010/08/04/schmidt-data/

31 http://hadoop.apache.org

32 J. Dean and S. Ghemawat. *MapReduce: Simplified Data Processing on Large Clusters*, *OSDI*, 2004.

33 L. Gavish, *New Caching policies for MEMCACHED*, M.Sc Thesis, Tel Aviv University, 2012.

34 B. Fitzpatrick. "Distributed caching with memcached", *Linux Journal*, 2004, http://hadapt.com/

35 M. Baker, D. Turnbull, G. Kaszuba, "Finding Needles in Haystacks (the Size of Countries)" *Blackhat*, Amsterdam, Netherlands, March 14-16, 2012.

INSS Memoranda, April 2012 – Present

No. 127, May 2013, Zvi Magen, *Russia and the Middle East: Policy Challenges*.

No. 126, April 2013, Yehuda Ben Meir and Olena Bagno-Moldavsky, *The Voice of the People: Israeli Public Opinion on National Security 2012*.

No. 125, March 2013, Amos Yadlin and Avner Golov, *Regime Stability in the Middle East: An Analytical Model to Assess the Possibility of Governmental Change* [Hebrew].

No. 124, December 2012, Shlomo Brom, ed. *In the Aftermath of Operation Pillar of Defense: The Gaza Strip, November 2012*.

No. 123, December 2012, Shlomo Brom, ed. *In the Aftermath of Operation Pillar of Defense: The Gaza Strip, November 2012* [Hebrew].

No. 122, September 2012, Emily B. Landau and Anat Kurz, eds., *Arms Control Dilemmas: Focus on the Middle East*.

No. 121, July 2012, Emily B. Landau and Anat Kurz, eds., *Arms Control Dilemmas: Selected Issues* [Hebrew].

No. 120, July 2012, Meir Elran and Alex Altshuler, eds., *The Complex Mosaic of the Civilian Front in Israel* [Hebrew].

No. 119, June 2012, Meir Elran and Yehuda Ben Meir, eds., *Drafting the Ultra-Orthodox into the IDF: Renewal of the Tal Law* [Hebrew].

No. 118, June 2012, Zvi Magen, *Russia in the Middle East: Policy Challenges* [Hebrew].

No. 117, May 2012, Shmuel Even and David Siman-Tov, *Cyber Warfare: Concepts and Strategic Trends*.

No. 116, April 2012, Yoel Guzansky, *The Gulf States in a Changing Strategic Environment* [Hebrew].