Yuval Ne'eman Workshop
for Science, Technology
and Security

מאמרים נבחרים לסיכום שנת 2014

אגד מאמרים פרי עטם של חוקרי
סדנת יובל נאמן למדע, טכנולוגיה ובטחון

תוכן העניינים

על המחברים 3
מאמרים 6

1. דבורה האוסן-כוריאל: דברי מבוא 6
2. יצחק בן ישראל: האבולוציה של הסייבר 8
3. קרן אלעזרי: חמש הבעיות הגדולות שהתגלו בשנה האחרונה 15
4. מני ברזילי: חברות פרטיות במלחמת הסייבר 19
5. דגנית פייקובסקי וגיל ברעם: סיכום שנת 2014 בפעילות החלל בעולם 26
6. טל דקל: רשתות חברתיות ומאמצים מבוססי מיקור המונים ככלי לניהול מצבי חירום סיכום ומגמות 34
7. ליאור טבנסקי: The Current State of Cyber Warfare 42
8. יונדב פרי: היכן עובר הגבול בין פשיעת סייבר ובין לוחמת סייבר 47
9. רועי צזנה: הרחפנים מגיעים 50
10. מתן שרף: מז"פ בסייבר – אתגר הייחוס 58

על המחברים

יצחק בן ישראל

אלוף (במיל.) פרופ׳ יצחק בן ישראל משמש כראש מרכז הרב-תחומי ללימודי סייבר באוניברסיטת תל אביב (ICRC). כמו כן, הוא משמש כראש סדנת יובל נאמן למדע, טכנולוגיה וביטחון החל משנת 2002. בנוסף, משמש כיו״ר סוכנות החלל הישראלית ויו״ר המועצה הלאומית למחקר ופיתוח – מולמו״פ, משרד המדע. פרופ׳ בן ישראל זכה בפרסי ביטחון ישראל בשנים 1972 ו-2001. (Itzik@tau.ac.il)

קרן אלעזרי

קרן אלעזרי היא מומחית אבטחה בינלאומית, ועוסקת בניתוח טרנדים בשוק אבטחת המידע העולמי ובייעוץ אסטרטגי בתחום הסייבר. ב-2014 הייתה קרן האישה הישראלית הראשונה שהוזמנה להרצות בכנס TED הבינלאומי. היא עוסקת בתחום אבטחת המידע משנת 2000, בתפקידים שונים בחברות אבטחה מובילות, ארגונים ממשלתיים ותאגידים בינלאומיים כמו Verint, PwC ו- AT&T . מאמריה התפרסמו כתבי עת כגון WIRED ו- Scientific American. ב-2012 קרן לימדה ב- Singularity University. כיום היא עמיתה בכירה בסדנת יובל נאמן. קרן היא בעלת תואר ראשון בהיסטוריה ופילוסופיה של המדעים והרעיונות מאוני׳ ת״א, תואר שני בלימודי בטחון מאוני׳ ת״א ובתעודת ההסמכה CISSP למומחי אבטחת מידע. (kerene@gmail.com)

מני ברזילי

מר ברזילי מנכ״ל FortyTwo ומומחה בינ״ל בתחום הביקורת, אבטחת המידע והסייבר. מני ניהל את המחלקה לביקורת מערכות מידע בקבוצת בנק הפועלים וזאת לאחר מגוון תפקידים בביקורת הפנימית, במשך כ- 10 שנים. בתוך כך, היה מבקר ה- IT של כלל חברות הבנות בקבוצה: ישראכרט, פועלים סהר, פעילים, פועלים שוקי הון וכו׳. עוד בעברו היה מני מנהל אבטחת המידע של המערך הטכנולוגי בחיל המודיעין. מני חבר בפורום הסייבר הבכיר של סדנת יובל נאמן באוניברסיטת תל-אביב. (me@mennyb.com)

גיל ברעם

גב׳ ברעם היא תלמידת דוקטורט בתכנית המצטיינים בחוג למדע המדינה שבאוניברסיטת תל-אביב, ובעלת תואר שני (בהצטיינות) בלימודי ביטחון מאוניברסיטת תל-אביב. כמו כן, גיל חוקרת בסדנת יובל נאמן למדע, טכנולוגיה וביטחון, מתמחה בתחומי המדיניות הקיברנטית של ארה״ב וישראל, אסטרטגיה ויחסים בין-לאומיים.
(glbaram@gmail.com)

טל דקל

מר דקל הוא חוקר בסדנת יובל נאמן למדע, טכנולוגיה וביטחון באוניברסיטת תל-אביב. מחקרו עוסק בסוגיות הקשורות לביטחון בחלל, למערכות ניווט לוויניות ולרשתות חברתיות מבוססות מיקום. טל משתתף קבוע בסדנאות של ארגון ה- ICG של האו״ם, העוסק בבניית יכולות בתחום מערכות הניוט הלוויניות. הוא בוגר תלפיות בעל תואר ראשון בפיזיקה ובמתמטיקה ובעל תואר שני בהנדסת אלקטרואופטיקה.
(tal@taldekel.com)

דבורה האוסן-כוריאל

עו״ד האוסן-כוריאל היא חוקרת בסדנת יובל נאמן, במרכז מינרבה בפקולטה למשפטים של אוניברסיטת חיפה ובמרכז הבינתחומי. היא מתמחה בהיבטים המשפטיים והמדיניים של ביטחון סייבר, רגולציית סייבר ומערכות טלקום. כעת היא משתתפת בצוות הבין-לאומי שמגבש את מדריך טאלין 2, יוזמה למיפוי כללי המשפט הבין-לאומי החלים במרחב; והיא גם יועצת לדיני אינטרנט וסייבר במשרדי Zeicher, Ellman& Krause בניו יורק. (deborah@cyberregstrategies.net)

ליאור טבנסקי

מר טבנסקי הוא מומחה סייבר ביחסים הבינלאומיים (cyber power) שמשלב מצוינות אקדמית עם כ-15 שנות ניסיון מעשי בניהול רשתות מחשב. ליאור הינו דוקטורנט בחוג למדע המדינה, חוקר במרכז הבינתחומי למחקר סייבר ע״ש בלווטניק וחוקר בסדנת יובל נאמן למדע, טכנולוגיה וביטחון, כולם באוניברסיטת תל-אביב. ליאור מפרסם מאמרים ויועץ בנושאי סייבר אסטרטגיים לגופים עסקיים וממשלתיים. (LiorT@tauex.tau.ac.il)

יונדב פרי

מר פרי הוא עמית סדנת יובל נאמן למדע טכנולוגיה וביטחון באוניברסיטת תל-אביב. הוא מרצה ומומחה לרשתות ועוסק בתחומים של אבטחת סייבר ורשתות. יונדב עבד בתפקידים בכירים בחברות היי-טק, הרצה בעשרות רבות של קורסים בנושאי רשתות דיגיטליות והיה חבר בארגוני תקינה בין-לאומיים. (yonadav@gmail.com)

דגנית פייקובסקי

ד״ר פייקובסקי מתמחה ביחסים בינלאומיים, אסטרטגיה ומדיניות חלל. היא עמיתה בכירה בסדנת יובל נאמן למדע טכנולוגיה וביטחון, ומלמדת בתוכנית לתואר שני בלימודי ביטחון באוניברסיטת תל-אביב. דגנית היא עמיתת פוסט-דוקטורט במכון דיוויס ליחסים בינלאומיים באוניברסיטה העברית, ועמיתת מחקר במכון למדיניות חלל באוניברסיטת ג׳ורג׳ וושינגטון בארה״ב. כמו כן משמשת דגנית כיועצת בנושא מדיניות מו״פ בחלל למועצה הלאומית למחקר ופיתוח. (deganit.paik@gmail.com)

רועי צזנה

ד״ר צזנה בעל דוקטורט בננו-טכנולוגיה, והוא עמית בסדנת יובל נאמן. מחקריו עוסקים בעיקר בניתוח טכנולוגיות מפציעות וחדשניות וחיזוי השפעותיהן על האדם והחברה, ומתנהלים בשיתוף פעולה עם חברות פרטיות, משרדי הממשלה והאיחוד האירופי. רועי הינו בעל טור קבוע במגזין הטכניון, וספרו ״המדריך לעתיד״ יצא לאור לאחרונה והתפרסם כבר בארבע מהדורות. (Roey@post.tau.ac.il)

מתן שרף

מר שרף הוא מנכ״ל ומייסד חברת Weboxer, המתמחה במחקר, פיתוח אסטרטגי ומתן פתרונות בתחום הסייבר. מתן בעל ניסיון בין-לאומי עשיר בפרויקטים של ייעוץ, אינטגרציה והדרכה לבנקים, לחברות טלקום ולספקי אינטרנט מובילים ברחבי העולם. מתן בוגר קורס תכנות של ממר״מ ויוצא היחידה הטכנולוגית של חיל המודיעין. בעבר, מתן עבד בפרויקט תהיל״ה במשרד האוצר ובחברת Check Point במשך 9 שנים שבהן כיהן כחוקר, יועץ במחלקת Professional Services, וכמנהל תחום ההכשרות. (Matan@web-boxer.com)

מאמרים

דבורה האוסן-כוריאל: דברי מבוא

החוברת בפניכם כוללת מאמרים פרי עטם של חוקרי סדנת יובל נאמן למדע, טכנולוגיה וביטחון באוניברסיטת תל-אביב. המאמרים נכתבו בתחילת שנת 2015, במטרה לשקף שינויים ותמורות עיקריים בתחומים שונים של בטחון הסייבר - כגון הממשק הרצוי בין המגזר הפרטי לבין גורמים ממשלתיים, התפתחויות בעולם ההאקרים, ההתמודדות עם פשע מקוון, המורכבות של אתגר הייחוס, הממשק בין סייבר וחלל, ועוד.

העובדה שחוקרי סדנת יובל נאמן מביאים זוויות רבות של פרספקטיבה וגישות מקצועיות מגוונות אינה מקרית. הסדנה מובילה בשנים האחרונות, הן באוניברסיטת תל-אביב והן מחוץ לכתליה, את התהליך של גיבוש ההבנה שקיימת חשיבות - ואף הכרח - בעיסוק אקדמי רב-תחומי בפעילות במרחב הסייבר של כלל השחקנים: מדינות, ארגונים ויחידים. העיסוק של הסדנה במחקר סביב שאלות שמתעוררות במרחב החמישי התחיל למעשה לפני כארבע וחצי שנים, בשלהי שנת 2010 ועד חודשי הקיץ בשנת 2011, כשכינס פרופסור איציק בן ישראל את מיזם הסייבר הלאומי ע״פ בקשת ראש הממשלה בנימין נתניהו. מאז אותה התקופה, בה התקיימו עשרות ישיבות בין כ-80 משתתפים, כל אחד מומחה להיבט אחר של פעילות במרחב, הסדנה משמשת אכסניה פעילה ללימוד רב-תחומי, עדכני וחדשני של סוגיות מגוונות בתחום. כעת, בתמיכה המלאה של הנהלת האוניברסיטה, ויחד עם שותפי ליבה כמו מטה הסייבר הלאומי והמרכז הבינתחומי למחקר סייבר ע״ש בלווטניק, הסדנה פועלת לקידום ההבנה של האקדמיה הישראלית והחברה הישראלית כולה שמרחב הסייבר מהווה אזור פעילות אנושית חשובה ביותר.

המאמרים בספר זה פורסים בפני הקורא הזדמנויות רבות להרחיב אופקים וירטואליים. בפתח הספר, **איציק בן ישראל** משתף בראייתו הייחודית של תהליך האבולוציה של תופעת הסייבר, לוחמת הסייבר והמעבר בין אבטחת מידע לאבטחת סייבר, לקראת עתיד של טכנולוגיית סייבר.

קרן אלעזרי ממשיכה בניתוח חמשה אתגרים שנתגלעו בשנה האחרונה במרחב, עם פרספקטיבה על הצורך בניהול נבון של מערכות מידע. **מני ברזילי** מתמקד בסוגיה

החשובה של פעילותן של חברות פרטיות במלחמת הסייבר; כשהפרדיגמה של "מלחמת סייבר" נבחנת על ידי **ליאור טבנסקי** מזווית הראייה של מדעי המדינה. הגבול בין מלחמת סייבר לפשע מקוון, שאינו תמיד ברור דיו, נבחן על ידי **יונדב פרי**. שתי סוגיות חדשניות מנותחות על ידי **טל דקל** - המינוף של רשתות חברתיות ככלי ניהולי במצבי חירום - **ורועי צזנה** - רחפנים. החיבור העמוק בין פעילות בחלל והשימוש במרחב הסייבר בשנת 2014 מתואר ומנותח על ידי **דגנית פייקובסקי וגיל ברעם**. לבסוף, בעיית הייחוס של פעילות במרחב נבחנת על ידי **מתן שרף**, במאמר האחרון של הספר.

אנו מאחלים לכם קריאה מהנה – ובעיקר, קריאה שמעוררת שאלות, תהיות ודילמות לגבי המשך הדרך המשותפת של כולנו במרחב הסייבר.

בברכה,
דבורה האוסן-כוריאל, עו"ד
חוקרת בסדנת יובל נאמן

<u>מבוא</u>

התופעה הידועה בשם "לוחמת סייבר", נעשתה בשנים האחרונות ידועה לכל. היא כוללת מגוון גדול של תופעות כמו פריצה למאגרי מידע ממוחשבים של ממשלות, גניבת כספים באמצעות הוראות בנקאיות מזויפות, פרסום מספרי כרטיסי אשראי, "נעילת" אתרי מחשב כסחיטה ושחרורם תמורת כופר, השחתת אתרי מחשב, שיתוק ופגיעה בתחנות כוח, במערכי תובלה (כולל תעבורה ימית ואווירית), פגיעה במתקנים רגישים (כמו הצנטריפוגות במתקן ההעשרה האיראני בנתאנז), ריגול בין מדינות וריגול מסחרי (גניבת סודות מסחריים), שימוש ברשתות כמו האינטרנט להפצה מיידית של מסרים שנועדו להשפיע על דעת הקהל ועוד ועוד.

כדי לעשות סדר בג'ונגל הסייבר, מוצע בחלקו הראשון של מאמר זה לחלק את התופעות למשפחות לפי (1) סוג התוקף; (2) כוונת התקיפה; ו-(3) סוג הנזק הנגרם. שלושת המאפיינים הללו יכולים להיות לעזר רב בהבנת התופעה וסיווגה. בחלקו השני של המאמר אתאר בקצרה את השלבים השונים שעברו על עולם הסייבר החל מראשיתו בשנות השמונים של המאה העשרים ועד היום.

<u>חלק ראשון: סיווג תופעות הסייבר</u>

(1) מי התוקף?

באופן גס ניתן לחלק את התוקפים למשפחות הבאות:

א. אינדיבידואל הפועל על דעת עצמו ובכוחות עצמו. לקבוצה זו שייכים פעמים רבות עובדים ממורמרים מתוך הארגון המונעים לעיתים ע"י בצע כסף ולעיתים על ידי סיבות אחרות כמו נקמה.

ב. קבוצה של אינדיבידואלים המאחדים כוחות למען מטרה משותפת היכולה להשתנות מתקיפה לתקיפה. דוגמה: אנונימוס

ג. ארגונים (כולל חברות מסחריות) הפועלים למען מטרה קבועה. מטרה זו יכולה להיות לפעמים פשע (רווח כספי), לפעמים מטרה אידאולוגית ולעיתים פוליטית.

ד. מדינות

(2) מהי כוונת התקיפה?

הכוונות יכולות להיות רבות ומגוונות. עיון באירועי הסייבר של השנים האחרונות מראה שרובן נופלות תחת הכותרות הבאות:

א. פשע
הכוונה לסוגי פשע שונים, החל מגניבה וסחיטה של כסף, דרך נקמה, וכלה בפשעי שנאה.

ב. איסוף מודיעין
גם תחת כותרת זו נכללות תופעות רבות כמו ריגול בין מדינות, גניבת מידע בעל ערך מסחרי, גניבת סודות תעשייתיים וכולי.

ג. השפעה על קהל רחב
טכנולוגיית המיחשוב המודרנית מאפשרת הפצה מהירה של מסרים לקהלים עצומים בלחיצת כפתור אחת. דוגמה מצוינת לניצול יכולת זו היא השימוש שעושה דאע"ש בסרטוני העריפה המופצים ביוטיוב.

ד. טרור
פעולות טרור נועדו, בסופו של דבר, להטיל פחד על אוכלוסיה מסוימת במטרה להשיג מטרה שהיא בדרך כלל פוליטית. מלבד השימוש במרחב הסייבר להשגת השפעה, יכולים ארגוני הטרור גם לגרום לפגיעה בנכסי מחשב לצורך זה.

ה. מלחמה
המחשב הראשון נבנה לפני 70 שנה עבור הצבא האמריקאי, ומאז הוא קטן במימדיו ועולה בביצועיו כל שנה (בהתאם לחוק מור לפיו כל שנה וחצי מוכפל מספר הטרנזיסטורים שאפשר לארוז על שבב בגודל נתון). כיום אין כמעט מכשיר שאינו מכיל שבב (צ'יפ) של מחשב: החל במכונת הכביסה והטלפון הנייד, דרך המכונית וכלה במטוסים ואפילו בפצצות "חכמות". התמחשבות מהירה זו יצרה מצב בו פגיעה במחשבים נהפכה לנקודת תורפה דרכה אפשר לנטרל כמעט כל מערכת חיונית המבוקרת מחשב, כולל מערכות צבאיות כמו מטוסים, טנקים, מערכות שליטה ובקרה וכולי.

יתרה מכך, ההתמחשבות המהירה של כמעט כל מערכת אזרחית נותנת כיום בידי הצבאות כלים לפגיעה באויב ע"י שיתוק מערכות התשתית החיוניות שלו.

(3) סוג הנזק הנגרם

טכנולוגיית הסייבר מאפשרת לגרום נזק למערכות שונות ומגוונות. בתור נקודת פתיחה אפשר להעזר כאן בחלוקה המטאפיסית של הפילוסוף קרל פופר (1902-1994) של כל מה שקיים בעולם לשלושה סוגים: גוף, נפש ומידע. הסוג הראשון כולל את עולם החומר והוא אוביקטיבי, הסוג השני כולל את המצבים המנטליים והוא סובייקטיבי, ואילו הסוג השלישי מכיל את תוצרי הידע שלנו שהם תוצאה של שילוב בין פעילות מנטלית (סובייקטיבית) והעולם החומרי (האובייקטיבי). בהתאם לחלוקה זו אפשר לתאר את סוגי הנזק באופן הבא:

א. נזק פיסי
השימוש שנעשה בווירוס הסטאקסנט למשל מדגים זאת היטב. תוצאתו הייתה קריסה פיסית של הצנטריפוגות שהעשירו אורניום.

ב. נזק מנטלי/פסיכולוגי
לתחום זה שייכות הן הפעולות הנוגעות להשפעה ע"י רשתות המחשבים (סרטוני היוטיוב של דע"ש למשל) והן חלק גדול מפעילויות הטרור.

ג. נזק למידע
זה כולל כמובן גניבת מידע, שיבושו, מניעת השימוש בו וכדומה.

<u>**חלק שני: האבולוציה של הסייבר**</u>

בהסתכלות אחורה על השלבים השונים בהתפתחות תפיסת הלוחמה במרחב הסייבר, אפשר לציין מספר שלבים בולטים שיפורטו להלן.

1. בראשית היה המודיעין

הייעוד של גופי המודיעין הוא כמובן איסוף מידע על גורמים המאיימים על הביטחון. לשם כך עוסקים גופי המודיעין, מאז ומתמיד, בריגול, ציתות לשיחות, צילום וכיוצא בזה. ההתפתחות המהירה של טכנולוגיית המיחשוב גרמה לכך שגופי הביון נאלצו לחדור למחשבים על מנת למלא את יעודם הקלאסי. התופעה התחילה לפני כמה עשורים כאשר מרכזיות הטלפונים התחלפו ממתגים מכניים לצמתי מחשב. בנוסף, המדיה הממוחשבת הפכה לאמצעי העיקרי לאכסון מידע וטיפול בו. אפילו ברמה האישית אנו שומרים כיום את המידע האישי שלנו, למשל - תמונות, במחשב (או אפילו ב"ענן") ולא עוד בתיקיה פיסית כמו אלבומי תמונות למשל. כדי למלא את יעודם הקלאסי, נאלצו איפוא גופי

המודיעין לאמץ טכניקות של חדירה למחשבים. מנגד התפתחה הדיסציפלינה,הקרויה בשם אבטחת מידע, של הגנה על המידע האצור במחשבים.

2. לוחמת מידע

המודיעין מילא תפקיד חשוב בלוחמה מתחילת ההיסטוריה האנושית. עם זאת הטכנולוגיה של המאה העשרים, ובמיוחד זו הקשורה במחשבים וברשתות התקשורת ביניהם, הביאה לעליה דרמטית בתפקידו של המודיעין בזמן אמת (זמ״א). לראשונה ניתנה האפשרות להזין מידע שנאסף במקום אחד, כמעט ללא השהיה, ללוחם הנמצא במקום אחר והזקוק למידע זה לצורך הלחימה. נפתח עידן מערכות השליטה והבקרה הממוכנות ואלו יצרו, לצד היתרונות הגלומים בהם, גם נקודת תורפה חדשה.

בתחילת שנות התשעים הבשילו מערכות המחשב במידה מספקת עד שבתורת הלחימה החדשה שנוסחה אז ע״י ארה״ב - תורת המהפכה בעניינים צבאיים (Revolution in Military Affairs -RMA) - הוגדר תחום חדש שנקרא ״לוחמת מידע״ (Information Warfare). הכוונה הייתה לשבש, לעוות ולמנוע את השימוש של הצבא היריב במידע הנחוץ לו ללחימה (לצד אבטחת המידע בצד שלנו).

3. נשק סייבר

במקביל, חוק מור והמזעור הביאו לכך שהמחשב נעשה קטן מספיק כדי להיכנס לכל פלטפורמת לחימה. מחשבי ניווט והפצצה הוכנסו למטוסים ולקחו על עצמם חלק ממשימות הטייס, וכך גם באוניות ובטנקים. המזעור הנוסף הביא לכך שהמחשבים חדרו אפילו לנשק עצמו, וכך נפתח עידן החימוש החכם (הוא ״חכם״ משום שיש לו מוח מלאכותי, דהיינו מחשב). התפתחות זו הובילה צבאות מסוימים (וביניהם צה״ל), כבר בתחילת שנות התשעים, לבחון את האפשרות להשתמש בטכנולוגיית הסייבר (שהייתה כבר מפותחת דיה לצורכי איסוף מידע) גם כנשק: אם ברצוני לנטרל את מטוסי האויב למשל, אני יכול לעשות זאת ע״ פגיעה קינטית בהם (באמצעות תותחי נ״מ או טילים), באמצעות שיבוש פעולתם האלקטרונית (לוחמה אלקטרונית) או באמצעות שיבוש המחשבים במטוסים ע״י וירוסים כאלו או אחרים. עד כמה שזה עשוי להיראות תמוה כיום, האחריות על פיתוח התחום הוטלה בדרך כלל על גופי המודיעין דווקא, משום שרק להם הייתה אז המיומנות והידע הדרושים לחדירה למחשבים.

כך למשל, כאשר כותב שורות אלו יזם בזמנו הקמת יחידה בצה״ל שתעסוק בסייבר כנשק, בתחילת שנות התשעים, הוא מצא אוזן קשבת בגופי המודיעין בלבד.

4. מאבטחת מידע לאבטחת סייבר

חיש מהר התברר שהיכולת להשתמש בסייבר כנשק, כנגד מערכות צבאיות, אינה כה פשוטה. נמצא שיותר קל לשבש מערכות אזרחיות דווקא, בתנאי שהן מבוקרות מחשב. העיסוק בנושא הוביל את מעצבי תורת הביטחון של ישראל להבנה שישראל עצמה, בהיותה המדינה הממוחשבת ביותר במזרח התיכון, יכולה להיות פגיעה מאד להתקפה כזו. הבנה זו הובילה לכך שבשנת 2002 (שוב, ביוזמת מספר אנשים וביניהם כותב שורות אלו שהיה אז ראש מפא״ת במשהב״ט), החליטה ממשלת ישראל להקים גוף חדש - הרשות לאבטחת מידע בשירות הביטחון הכללי - שתפקידו הוגדר כפיקוח (בתחום הסייבר) על תשתיות לאומיות קריטיות, כמו ייצור חשמל, אספקת מים וכדומה. ישראל הייתה אז אולי המדינה הראשונה בעולם שהתכוננה, הלכה למעשה, למלחמת סייבר עתידית.

זו הייתה למעשה תוצאה של הבנה עמוקה יותר ממה שנראה על פני השטח: התברר שהתלות של מערכות קריטיות בבקרה של מחשבים, גדלה עד כדי כך שניתן היה לגרום, באמצעות שיבוש הבקרים, לנזק פיסי של ממש ולא עוד רק נזק למידע. תם למעשה עידן אבטחת המידע, והחל עידן אבטחת הסייבר.

5. מאבטחת סייבר ארגונית לאבטחת סייבר לאומית

הניסיון המצטבר באבטחת הסייבר על ארגונים כמו חברת החשמל, הוביל להתפתחות נוספת בחשיבת הסייבר של ישראל. התברר כי כמעט בלתי אפשרי ״לעטוף״ מחשב או שרת בודד, או מערך ארגוני של מחשבים ושרתים, בהגנה שתבודד אותו מפני חדירה. כמו בכל הגנה (גם כנגד תקיפה פיסית) יש צורך לצאת קדימה ולתפוס את התוקף בדרכו למטרה, ומוטב לתפוס אותו אפילו בבסיס היציאה שלו. אבל, ה״ווירוסים״ למיניהם אינם טסים באוויר החופשי ומדביקים את מחשב המטרה באופן ישיר, אלא הם עוברים דרך ערוצי התקשורת שלו למחשבים אחרים. כדי להשיג הגנה יעילה, יש איפוא צורך בניטור כל מערך התקשורת וזו כבר משימה לאומית.

יתרה מכך, הלך והתברר כי הדרך לחדור למחשבי המטרה, אינה רק באמצעות האינטרנט, או כל רשת תקשורת מחשבים אחרת, אלא גם היא יכולה להיות פיסית: באמצעות דיסק-און-קי למשל, או מדפסת. הפיקוח מחייב איפוא התייחסות לא רק לרשתות התקשורת אלא לכל שרשרת הספקים.

בשנת 2011 הגיש הח״מ דו״ח לראש הממשלה, שמינה אותו כשנה קודם לעמוד בראש צוות רב תחומי שמנה כשמונים מומחים, ובו המלצות למה שנדרש לעשות ברמה הלאומית כדי להיות מוכנים לאיומי הסייבר העתידיים. הצוות בחן את הנושא מזווית ראייה רחבה

מאד ושאל את השאלה הכללית יותר: מה צריך לעשות כדי לבנות מערכת חיה ונושמת שתעקוב באופן שוטף אחרי התפתחות הטכנולוגיה והאיומים, תייצר פתרונות באופן "אוטומטי" וכולי. לשם כך נדרשנו להמליץ על צעדים הנוגעים לא רק לטכנולוגיה אלא גם לבניין הכוח; לשילוב בין התעשייה, האקדמיה וגורמי הביטחון; לחינוך בבתי הספר; להקמת מרכזי מצוינות באקדמיה; לפתרון סוגיות הייצוא; להקמת תשתיות לאומיות קריטיות (כמו מחשבי על וסימולטורים); לרגולציה וכולי. כל אלו נהפכו להחלטת ממשלה בשנת 2011 והוקם מטה הסייבר הלאומי במשרד ראש הממשלה לפקח, לתכנן, ולנצח על העבודה כולה.

6. איזון בין צרכי הביטחון והגנה על הפרטיות

החלטת הממשלה ב-2011 הותירה בעיה אחת ללא פיתרון: כיצד מאזנים בין הגנה יעילה מחד, המחייבת ניטור מערכות ורשתות תקשורת בכל המרחב האזרחי, ובין הצורך להגן על פרטיות האזרח? לשם כך הוקם שוב צוות בראשותי והמלצתו הפכה להחלטת ממשלה בינואר 2015. בעיקרון מדובר בהקמת רשות לאומית חדשה להגנת מרחב הסייבר האזרחי, שלא תהא כפופה לשירותי המודיעין (ובכללם לשירות הביטחון הכללי). הרשות תהא גם היא במשרד ראש הממשלה, ובימים אלו היא מוקמת.

7. מאבטחת סייבר לטכנולוגיית סייבר

מה צופן העתיד? טכנולוגיית המיחשוב אינה עוצרת. חוק מור ממשיך בינתיים לעבוד, ולא רחוק היום בו נבצע את הקפיצה הבאה - לטכנולוגיית מיחשוב קוונטי (במעבדות יש כבר דגמים עובדים של מחשבים כאלו) - שתגדיל את ביצועי המחשבים בפקטור שקשה לעכלו (פי 10 בחזקת 30). הספרות (ועולם הטכנולוגיה) עסוקים בתכנון של בית חכם, אינטרנט של דברים, וכו'. הרעיון פשוט: הבה נהפוך כל מכשיר בחיינו (מקרר, רכב, מכונת כביסה, וכו') למכשיר מבוקר מחשב ונקשור את כל הדברים הללו ברשת תקשורת שתהיה "אינטרנט של דברים". זה יאפשר לנו לשלוט מרחוק בכל חפץ. נוכל למשל להדליק את הדוד הביתי (בהוראה מהטלפון שלנו) כמה שעות לפני שנחזור מחו"ל או לאוורר את הבית וכו'. המפליגים אינם מסתפקים בכך אלא מדברים על עיר חכמה ואפילו על מדינה חכמה. כל זה לא יתאפשר ללא רמת אבטחה מינימלית. אם נשאיר פרצות אבטחה, יוכלו גורמים חורשי רעה (וכאלו יימצאו תמיד) לנצל את כל ההתפתחויות הללו לטרור, פשע, גרימת נזק בלתי הפיך וכדומה.

העתיד מחייב איפוא רמת אבטחת מינימלית שתאפשר את כל החידושים הללו. אנו נמצאים בפיתחה של תקופה בה אבטחת הסייבר אינה עוד מטרה בפני עצמה (דהיינו אבטחת כל מה שמבוקר מחשב). היא למעשה טכנולוגיה "מאפשרת" (enabler) שבלעדיה

לא נוכל להתקדם בכיוון הרצוי. זו הסיבה לכך שאפילו המונח "אבטחת סייבר" נראה כבר מיושן, ויש להחליפו במונח "טכנולוגיית סייבר".

3. קרן אלעזרי: חמש הבעיות הגדולות שהתגלו בשנה האחרונה

אלפי מוחות מן הטובים בעולם, המלווים במיליארדים של דולרים, שקועים בפיתוח טכנולוגיות אבטחה חדשות ובהגנה על מרחב הסייבר. ובכל זאת, מדי שבוע אנו למדים על פריצה חדשה לתוך ארגון גדול או על פגיעות שתאפשר לתוקף זדוני להשתלט מרחוק על מערכות החשמל. בקיץ 2010, לפני ארבע שנים, נחצה "קו פרשת הסייבר": העולם כולו גילה שתולעת מחשב שכונתה סטוקסנט (Stuxnet) הצליח לשבש את פעילות צנטריפוגות העשרת האורניום בנתנז, איראן. חמש עשרה אלף שורות של קוד מחשב – תוכנה – השפיעו פיזית על מערך מורכב של תשתיות גרעין. אך מדוע הפרצות האלו אפשריות? ומי באמת שומר על כולנו במרחב הסייבר? כדי לרדת לשורשי הבעיה, יש לשאול תחילה "מהו סייבר?".

מעטים יודעים מהו מקור הביטוי, אך כדאי להתחקות אחריו. בשנות ה-40 של המאה העשרים לימד המתמטיקאי האמריקני נורברט ווינר במכון הטכנולוגי MIT בבוסטון. בשנים שלאחר מלחמת העולם השנייה בחן פרופסור ווינר את השינויים מרחיקי הלכת שהביאו עמן טכנולוגיות תקשורת חדשות כמו רדיו וטלפון. הוא זיהה שמערכות חדשות לחלוטין של **שליטה, תקשורת ובקרה** מתחילות לשנות את פני האנושות. בשנת 1948 פרסם ספר פורץ דרך שבו תיאר את התיאוריה המדעית החדשה שלו באשר לתפקודן של **מערכות שליטה, תקשורת, בקרה והיזון חוזר בין בני אדם ובין מכונות**.[1] לתיאוריה הזו קרא ווינר "קיברנטיקה". אך למעשה, ווינר לא המציא את המונח – כנהוג בעולם המדעי, הביטוי הושאל מהיוונית הקלאסית. ביוון העתיקה, ערש הדמוקרטיה, שלטו ערי המדינה היווניות בים התיכון ביד רמה. לכל ספינה יוונית היה מפקד, שתפקידו היה להורות לחותרים ולמחזיקים במפרשים כיצד לפעול – האיש שהחזיק בהגה והחליט לאן ובאיזה מהירות תשוט ספינתו. היוונים קראו לאדם הזה κυβερνήτης – קיברנטס. בעברית אנו קוראים לו קברניט. בימינו אנו, המרחב הקיברנטי כולל גם את מערכות השליטה המרוחקת שמאפשרות לכלי רכב בלתי מאויש לסייר על פני מאדים, אך גם את הציוצים של NASA בשם אותו כלי רכב ברשת החברתית טוויטר. אם כך, אבטחת עולם הסייבר, או המרחב הקיברנטי, משמעותה הגנה על ערב רב של טכנולוגיות ושל תהליכי שליטה ותקשורת שונים המחברים את העולם הדיגיטלי עם העולם הפיזי, ולא רק הגנה על סודיות מאגרי מידע, כפי שחשבנו בעבר. וזוהי מטלה מורכבת מאין כמותה – בשל הסיבות שלהלן.

1. במשך שנים, אחת הבעיות החשובות בעולם האבטחה הייתה גילוי פגיעויות תוכנה. פגיעויות הן טעויות, "באגים", שנובעות מטעות מתכנת או מעיצוב תוכנה כושל. פורצים

1 *Cybernetics: Or Control and Communication in the Animal and the Machine.* Wiener, Norbert. Paris, Hermann & Cie & Camb. Mass. (MIT Press) ISBN 978-0-262-73009-9; 1948, 2nd revised ed. 1961

ופושעים יודעים למצוא טעויות אלו ולנצל אותן כדי לאלץ את התוכנה לפעול בדרך בלתי צפויה ולאפשר להם לשלוט במערכת. על פי סקירה של כל פגיעויות התוכנה ב-25 השנים האחרונות,[2] סביבות מחשוב ספורות בלבד היו המקור לרוב הפגיעויות. מדובר במערכות שכולנו מכירים וכולנו נשענים עליהן. מערכות ההפעלה של אפל, מייקרוסופט וגם לינוקס החופשית בולטות ברשימה, לצד תוכנות בסיסיות כמו ג׳אווה מבית Sun/Oracle ו-Flash של אדובי. אך בשנים הקרובות ייאלצו מומחי אבטחה לחפש פתרונות להגנה לא רק על סביבות מחשוב פגיעות אלו אלא גם על סביבות מחשוב חדשות, על פרוטוקולים של תקשורת וניווט מבוססי רדיו ולוויין, על מערכות הפעלה חדשות שמפעילות מכוניות, בתים חכמים וטכנולוגיות רפואיות המחוברות לגוף האנושי.

ובכך נעוצה הבעיה: אין רשות אחת בנמצא, ממשלה אחת או יצרן טכנולוגיות אחד שמסוגלים להקיף את כלל מרחב הטכנולוגיות הללו, לפקח עליהן או למצוא את כל הפגיעויות. למעשה, ההפך הוא הנכון: על יצרניות תוכנה, רכב או טכנולוגיות אחרות מופעל לחץ אדיר להוציא מוצרים חדשים לשוק מהר ככל האפשר, לפני המתחרים, ולכן עומד לרשותם זמן קצר יותר כדי לנתח פגיעויות ולחפש פרצות אבטחה. אבל זאת איננה כל הבעיה.

2. האמת היא שמשאבים אדירים, שהיקפם מגיע לעשרות מיליוני דולרים, מושקעים באופן פעיל כדי להשאיר פרצות פתוחות. במסגרת תגליותיו של אדוארד סנודן בשנה האחרונה (2014) נחשף גם התקציב שעמד לרשות הסוכנות לביטחון לאומי של ארצות הברית NSA לקנייה של פגיעויות תוכנה, המכונות ״Zero Day״, בשוק השחור. אלו הן פגיעויות שאינן ידועות ליצרן התוכנה בעת הגילוי שלהן, ולכן הן משמשות מעין ״נשק סודי״ כל עוד הן נשארות כפרצות שאין להן מענה. תגלית נוספת מהשנה האחרונה היא כי אותה סוכנות עצמה שילמה סכום של עשרה מיליון דולר לחברת צופן ידועה על מנת להבטיח שהחברה תכניס באופן יזום רכיב רנדומיזציה חלש לתוך מוצרי הצופן שלה. מוצרים אלו משמשים מאות אלפי ארגונים בעולם, והכנסת הרכיב תשאיר אותם, למעשה, חשופים בפני הסוכנות. רק לפני מספר חודשים, התגלה שבמשך שנתיים נכללה פגיעות בתוכנת OPEN SSL הפופולרית, שמשמשת אתרי אינטרנט רבים כדי לספק קישוריות מוצפנת ב-SSL, חולשה שגם אותה כנראה ניצלו ב-NSA. אין הסכמה באשר לתוקפם של גילויים אלו, אך המסמכים שנחשפו מציגים תמונה קודרת מאוד לגבי המחויבות של סוכנויות ביטחון, כגון ה-NSA, לרמת הביטחון של המשתמשים באינטרנט, גם אם מדובר באזרחים או בתאגידים אמריקנים שה-NSA אמור להגן עליהם.
למעשה, אפשר להניח שסוכנויות ביטחון אחרות ברחבי העולם משקיעות אף הן מאמצים רבים ותקציבים משלהן ברכישת פגיעויות ״Zero Day״ ובניצולן, מבלי שחברות התוכנה

2 25 *Years Of Vulnerabilities: 1988-2012 Sourcefire Research Report* https://www.sourcefire.com/25yearsofvulns

מודעות לכך. מנגד, קבוצות פשע מאורגן סוחרות באותן פגיעויות ובכלי פריצה אחרים. ערכה של הכלכלה האפלה של כלי הפריצה (exploits) הוא עשרות מיליוני דולרים, על פי הערכה של מכון RAND. מכאן, השורה התחתונה ברורה: סכומי כסף גדולים מאוד מושקעים על מנת להשאיר את העולם פגיע, וגם מי שסבור שהוא מוגן, בדרך כלל פגיע הרבה יותר מהידוע לו.

3. הפגיעות הרבה נובעת מכך שכולנו – חברות מסחריות, ארגונים ציבוריים ואנשים פרטיים – חוליות חלשות באותה שרשרת, ובעידן הנוכחי כולנו תלויים וירטואלית בשותפים, בספקים, בלקוחות ובתשתיות מחשוב ומערכות מידע של ארגונים אחרים. אפילו חברות כמו ענקית הקמעונאות Target , שמשקיעה מיליוני דולרים בתקציבי אבטחת מידע ובטכנולוגיות חדישות, יהיו פגיעות. במקרה זה מדובר בכך שאחד מספקי התחזוקה של Target, חברת Fazio שמנהלת מערכות קירור ונטילציה, כלל לא טרח להתקין אפילו תוכנת אנטי וירוס בסיסית. בשנים האחרונות גילינו שגם חברות ביטחוניות, שמפתחות את כלי הנשק של העתיד בתקציבי מחקר של מיליארדי דולרים, נותרות פגיעות לריגול דיגיטלי. למשל, חברת לוקהיד מרטין הודתה בשנת 2011 כי חוותה חדירה ממושכת ומתוחכמת, ככל הנראה מצד האקרים בשירות ממשלת סין.[3]

מתחקיר האירוע עולה כי כוונת התוקפים הייתה לתקוף את חברת RSA, שסיפקה ללוקהיד מרטין רכיבי הזדהות חזקים בשם SecureID, שנועדו לאבטח גישה למידע מסווג. אבל דווקא אמצעי אבטחה זה שימש לבסוף את התוקפים, שפרצו תחילה לחברת EMC, תאגיד-העל שאליו שייכת RSA, וממנה הגיעו למידע שאפשר להם לזייף גישה באמצעות מנגנוני ה-SecureID. הפריצה הממוחשבת הראשונית לחברת EMC התאפשרה בגלל פריט דואר אלקטרוני אחד, פשוט, שנשלח לאנשי מחלקת כוח האדם של התאגיד. לדוא״ל צורף קובץ אקסל, שבו הסתירו התוקפים את כלי הנשק שלהם: התקפה שמנצלת פגיעות בתוכנת פלאש מבית חברת אדובי. גם מקרה זה מדגים שלגופים ביטחוניים, לענקיות תוכנה ולתאגידי אבטחה – לכולנו בעצם – יש חוליות חלשות החשופות לניצול.

4. לבעיה זו יש גם פן נוסף: אנשים פרטיים וגם ארגונים רבים סבורים שאבטחת המרחב הקיברנטי איננה בעיה שלהם. כמה פעמים שמעתם חברים שחושבים ש״הארגון שלנו לא מעניין אף אחד״, ״מדוע שמישהו ירצה לפרוץ לחשבון הפייסבוק שלי״ וכדומה? אבל מרגלי סייבר בשירות מדינות זרות ופושעים מאורגנים מנצלים את התמימות הזו: הם רואים בכלל הנכסים הדיגיטליים של כולנו כר פורה של תשתיות שאפשר להשתמש בהן כדי לצאת למתקפה הבאה או להרוויח כסף. חשבונות המדיה החברתית שלנו נפרצים כדי לקדם פרסומות ש״גונבות קליקים״ וכדי להפיץ תוכנה זדונית. שרתי הענן שלנו הופכים

3 N. Hodge and I. Sherr, Lockheed Martin Hit by Security Breach, 27 May 2011, http://online.wsj.com/news/articles/SB10001424052702303654804576350083016866022

להיות בסיס לשיגור מתקפות מניעת שירות DDoS או מערכות להפצת תוכנות זדוניות. המחשבים בבית ובמשרד, המחוברים תמידית לרשת, מודבקים בקלות בסוס טרויאני והופכים לחיילים ברשת מחשבים BotNet בשליטת פושעים, שאפשר גם להשכירה לפושעים אחרים למטרות פליליות למיניהן. משאבי המחשוב והתקשורת שלנו חשובים בעבור אלו הרוצים להרוויח או לגנוב סודות. אבל גם אם אין סודות להסתיר או כסף להפסיד, הרי אותם אנשים וארגונים שאינם מתקינים תוכנות אנטי-וירוס (פשוט כי "אין להם מה להסתיר") מהווים משאבים תמימים המאפשרים לפושעים ולמרגלים לעשות כרצונם ולהמשיך לתקוף את כולם.

5. אחת הבעיות הקשות ביותר באבטחת עתידנו הדיגיטלי היא, ככל הנראה, שהאי-בהירות באשר ל"מלחמות הסייבר" מותירה את הדיון, ולכן גם את הפתרונות ואת האחריות, במישור הביטחוני והצבאי. אך האמת היא שכולנו נמצאים בקווים הקדמיים של מלחמות הסייבר ואיננו מודעים לכך. לוחמת סייבר וריגול דיגיטלי נקשרים בדמיוננו ללוחמים מיומנים ומאומנים, לאשפי מחשב ולאנשי צבא שנקראו לדגל ושומרים על כולנו בשדה הקרב הדיגיטלי. אבל דימוי זה כלל אינו מדויק. אנשי אבטחה בשירות המדינה והצבא אמנם שומרים על מערכות המידע הממלכתיות (במידה כזו או אחרת של הצלחה), אבל במרחב הסייבר אין חזית צבאית ועורף אזרחי, להפך: הארגונים שאליהם מכוונות מרבית מתקפות הסייבר הם דווקא הגופים האזרחיים – חברות ותאגידים מסחריים, ספקיות שירותי האינטרנט והטלפוניה, גופי התשתיות כגון חברת החשמל, מקורות ורשות שדות התעופה. במרחב הסייבר אין פתרון דמוי "כיפת ברזל", מערכת צבאית שיכולה להגן על המרחב האזרחי. ואף אילו הייתה כזו, ייתכן שכדי לממש הגנה צבאית על "העורף הדיגיטלי" היה עלינו לוותר על אחד מערכי היסוד של החברה הדמוקרטית: קישוריות חופשית מניטור ומבקרה ממשלתית.

לסיכום, את הקווים הקדמיים של שדה הקרב הדיגיטלי מאיישים לא רק חיילים וחיילות, אלא בעיקר מנהלי מערכות מידע ומפעילי תשתיות התקשורת האזרחיות, וגם אזרחים פרטיים - ויש להכיר בכך.

4. מני ברזילי: חברות פרטיות במלחמת הסייבר

מאז שחר האנושות...

מאז שחר האנושות בני אדם נלחמים אלו באלו. מאבקים הם חלק בלתי נפרד מהפולקלור של דתות ושל תרבויות רבות ושונות. נדמה אף שלמאבקים יש תפקיד עיקרי בגיבוש התפיסה הדתית והתרבותית ובליכודו של העם הנאבק. במאבקים אלו כלולים קרבות, מלחמות, כיבושים, עלייה של אימפריות, סיפורי הישרדות וגבורה וגם מוות והקרבה עצמית.

תקופתנו הנוכחית אינה שונה. אף שהאנושות הצליחה להגיע להישגים מרחיקי לכת ומרתקים בתחומי הרפואה, הפילוסופיה, האמנות, הטכנולוגיה ועוד, אנו עדיין נלחמים אלו באלו ללא הרף – ולא ניראה סוף לכך באופק. אולם אין זה מאמר פוליטי או מוסרי כלל וכלל, אלא דווקא כזה העוסק בהיבטים הביטחוניים הקשורים במציאות זו.

סייבר-תפוחים

לפני כמה ימים, כאשר ישבתי עם חבר בבית קפה, ניגשה אלינו מלצרית נחמדה נושאת מגש ועליו כוס גדולה ושאלה: "סייבר-תפוחים?". כן, נדרשו לי שניות אחדות (רבות, אני מודה) להבין שהיא אמרה בעצם "סיידר". אך בעולם שבו אנו שומעים את המילה "סייבר" בכל מקום ובכל זמן, אולי הטעות נסלחת.

לא בִּכְדִי אנו שומעים על עולם הסייבר בתכיפות כה רבה. עימות יכול להתקיים בארבע זירות לוחמה מרכזיות[4] – יבשה, ים, אוויר וחלל. ממד הסייבר הפך זה מכבר זירה חמישית, ואולי אף הזירה הפעילה מכולן. מאפיינה הייחודיים של זירה זו מייצרים מגמות לחימה חדשות.

מדוע זירת הסייבר כה פעילה? התשובה היא – לגיטימציה. זירת הסייבר מעניקה הכשרים לתקיפות, דבר שלא קיים בזירות האחרות. מדינה יכולה להפעיל אלפי אנשי טכנולוגיה שיעסקו בפעילות התקפית במשך עשרים וארבע שעות ביממה ושבעה ימים בשבוע – והעולם ימשיך כסדרו. לעומת זאת, מה יקרה אם מדינה תחליט לשגר טיל קונבנציונלי אחד ויחיד אל עבר מדינה אחרת? ברור לכול שבמקרים רבים הדבר יוביל לפרוץ מלחמה רחבת היקף.

---

4 יש זירות לוחמה נוספות אך הן מרכזיות פחות – כגון זירת הלוחמה הכלכלית, הפסיכולוגיה, הפוליטית וכדומה.

תורת הלחימה

לפי תורת הלחימה הקלאסית, תקיפה צבאית כנגד מדינה צפויה להיות מלווה בתקיפה של התשתיות הקריטיות בה. זאת לשם השגת נזק מקסימלי והכרעה מהירה של הנתקף. מה נכלל בהגדרה של תשתיות קריטיות? מדובר בנכסים אשר זמינותם נדרשת באופן מהותי לשם תפקודה התקין של המדינה[5]. בתוך קבוצה זו נכללות תשתיות חשמל, מים, תחבורה, ממשל, פיננסים, טלקומוניקציה, רפואה, שירותי חירום ועוד. ראוי לציין כי הדוקטרינה הצבאית המקובלת מתייחסת מזה זמן רב לתקיפה של מטרות אזרחיות ועסקיות לחלוטין, כדוגמת בנקים (שהם חלק מהתשתית הפיננסית), לשם מְקסום הנזק ואפקט התקיפה.

האיום הקלאסי של שמציבה מדינה אחת על גופים אזרחיים של מדינה אחרת מתמקד בשני גורמים: (1) תשתיות קריטיות; (2) תקיפה שמטרתה שיבוש הפעילות. לכן, בזמנים ללא לחימה פעילה, הגופים האזרחיים המרכיבים את אותן תשתיות קריטיות לא היו צריכים לחשוש מפגיעות ברמה היום-יומית. אך עתה השתנה המצב. אנו עדים למקרים בהם מדינות תוקפות חברות אזרחיות. מקרים אלו כוללים גם חברות שאינן תשתיות קריטיות.

מרגלים בפייסבוק

בפברואר 2014 הרצֵיתי בכנס RSA אשר התקיים בסן פרנסיסקו (בשיתוף עם הילה מלר). ההרצאה, שכותרתה "מרגלים בפייסבוק",[6] עסקה בין השאר בהיבט מסוים הקשור באירועי אדוארד סנודן (עובד לשעבר ב-NSA שהתפרסם לאחר שהדליף לציבור מידע מסווג רב על תכניות המעקב של הסוכנות).

אחת התכניות הראשונות שנחשפו לעיני הציבור בפרסומי סנודן היא "פריזמה". פריזמה היא תכנית לאיסוף סיגינט[7] באמצעות הקמה של מערכת לשליפת מידע ישירות מתוך מאגרי המידע של חברות ענק כגון פייסבוק, גוגל, מייקרוסופט ואפל. כלומר, ל-NSA הייתה אפשרות לגשת לכמות עצומה של מידע פרטי ואישי של חלק גדול מהאנשים על פני כדור הארץ, ואין זה מפתיע.

5 Infracritical: comparison of US and international definitions of infrastructure. http://www.infracritical.com/images/cip-sectors5.jpg

6 http://www.rsaconference.com/events/us14/agenda/sessions/1068/foreign-spies-and-facebook-the-undeniable-truth

7 Sigint – Signals Intelligence – מודיעין אותות

כצפוי, פרסומי סנודן גררו ביקורת ציבורית נרחבת כלפי הממשל האמריקני ובפרט כלפי ה-NSA. בעקבות ביקורת זו פעלה הסוכנות להסביר לעולם כי תכנית פריזמה ותכניות דומות היו "כלי מרכזי בסיכול פעולות טרור מסביב לעולם".[8]

לאמירה זו השלכות רבות ומעניינות, אך אחת החשובות לענייננו היא זו: טענת ה-NSA כי תכנית פריזמה תרמה לסיכול פעולות טרור היא, למעשה, הכרזה בריש גלי כי המידע המאוחסן בחברות פרטיות כגון פייסבוק וגוגל הוא מידע מודיעיני רב-ערך. זהו מידע שארצות הברית עצמה משתמשת בו לשם קידום האינטרסים הביטחוניים שלה. ארצות הברית היא, ככל הנראה, המדינה בעלת יכולות איסוף המודיעין העוצמתיות ביותר, והיא יכולה לבחור כל מקור מודיעיני חלופי. ובכל זאת, היא השקיעה משאביה דווקא באיסוף נתונים מתוך מאגרי פייסבוק ומאגרי חברות פרטיות נוספות, חברות שתכליתן ליישם תהליכים עסקיים תקינים ולהרוויח.

ומה עושה רוסיה?

סוכנות ה-NSA יכולה לאלץ את החברות האמורות לשתף פעולה ולאפשר לה לגשת למידע המבוקש. זאת כיוון שכל החברות הללו הן חברות אמריקניות הכפופות לחוק האמריקני. בכך בעצם מתאפשר לסוכנות להשיג את המידע בכסות החוק.

ועכשיו עולה השאלה העיקרית לענייננו – מה תעשה רוסיה כדי להשיג גישה למידע זה? מה תעשה סין? מה תעשה כל מדינה אחרת? הרי ברור כי לכל ארגון בִּיוּן בעולם יש אינטרס לקבל נגישות למידע המאוחסן בידי החברות הפרטיות האמורות. זהו, כאמור, מידע מודיעיני רב-ערך. ואל לנו לטעות, השאלה היא שאלה של זמן ושל שיטה. או אולי עלינו לשאול – "האם למדינות שונות בעולם כבר יש גישה למאגרי המידע בפייסבוק, בגוגל ובחברות אחרות?".

אפשר לצפות שמדינות ישתמשו בכלים מודיעיניים קלאסיים ומקובלים לשם השגת המידע האמור. ארגז הכלים המודיעיניים מכיל כמובן גם פעילות איסוף באמצעות "יומינט"[9], כלומר הפעלת סוכנים ומרגלים. אמנם התפיסה "מרגל מדינתי בחברה אזרחית" אינה מקובלת, אך בעצם מבחינת עלות-תועלת, הדבר משתלם מאוד: חברות עסקיות מכילות מידע רב-ערך והן ממשיכות לאסוף אותו כל העת, רמת הסיכון שכרוכה בהחדרת סוכן לחברה נמוכה מאוד, ואין צורך בתחקיר ביטחוני ובבדיקת פוליגרף לשם קבלת המשרה.

---

8 http://blogs.wsj.com/cio/2013/07/31/general-keith-alexander-speaks-about-prism-at-black-hat/

9 Human Intelligence

ויש נקודה חשובה נוספת שבגללה הכנסת מרגל לחברה אזרחית אטרקטיבית כל כך. בעבר, ארגוני ביון שאפו לגייס אנשי דרג בכיר כמרגלים, וככל שהמגויס היה בכיר יותר כך תועלתו רבה יותר. לפי תפיסה זו, גיוס גנרל בצבא רוסיה עדיף על גיוס חייל זוטר. אך היום, בעידן המידע, למעשה ההפך הוא הנכון: החיילים הזוטרים הם בעלי הנגישות הגדולה ביותר לנתונים (אדוארד סנודן, למשל) ולכן הם יכולים להיות סוכנים בעלי הערך הרב ביותר. חיילים אלו יכולים להיות בתוך צוות אנשי התמיכה למשל, או בתוך קבוצת אנשי תחזוקת המערכות ובסיסי הנתונים, והם יהיו מרגלים רבי-ערך מאוד. יש עובדים רבים יותר בדרג זה, ורמת הנאמנות שלהם לארגון צפויה להיות פחותה. לכן האתגר לגייס או להחדיר מרגל הוא פשוט יותר.

תקיפה לשם השגת מודיעין

ניתוח הבעיה מהיבט זה חושף בפנינו את אחד החידושים המעניינים שמביא אִתו עידן המידע בכל הקשור לאיום הייחוס של השוק האזרחי והעסקי. חברות מסחריות רבות אוגרות מידע רב-ערך שארגוני ביון עשויים לחשוק בו, ולכן ייתכן שתהיינה יעד לתקיפה. מובן שלא מדובר רק בפייסבוק ובגוגל. אפשר למצוא דוגמאות רבות לחברות שיש להן מידע מודיעני רב-ערך, למשל: חברות כרטיסי אשראי, שניתוח נתונים שלהן יכול לחשוף תכניות לנסיעה לחו״ל, מיקום נוכחי, סודות בריאותיים, הרגלים וכדומה; בנקים בארצות הברית, שניתוח המידע שבהם יכול לחשוף את כל מקבלי השכר מה-NSA ואולי את רמת בכירותם (לפי גובה השכר); בתי חולים, שיכולים לחשוף מידע בריאותי (לשם סחיטה או לניצול חולשות); חברות המייצרות אפליקציות ניווט, שיודעות מהו מיקומנו ומכירות את לוח הזמנים הקבוע שלנו; חברות סלולאר; חברות תחבורה, ועוד.

כאמור, זהו איום מתמשך ויום-יומי, ובהתאם לכך חברות חייבות להתייחס אליו כאיום טקטי ומיָדי.

מערכת היחסים בין המדינה ובין גופים במגזר הפרטי

האם חברות פרטיות ערוכות להתמודד עם מאמצי ביון של מדינות ולסכל אותם? האם זהו תפקידן? ואם נשווה למתרחש בעולם הפיזי: אמנם במדינות רבות מוצבים שומרים בכניסה לסניפי בנקים, למשל, אך ברור לכול שבעת פלישה צבאית אין זה תפקידם להגן על הבנק מחיילים ומטנקים של מדינה זרה.

זירת הסייבר היא זירה מורכבת יותר, ובכל הקשור להגנה מפני איום מדינתי קשה להגדיר מהם תחומי האחריות של החברה המסחרית ומהם תחומי האחריות של המדינה. באופן ספציפי יותר, אם חברת פייסבוק מותקפת על ידי סוכנות המודיעין הרוסית FIS(Foreign

Intelligence Service), למשל, מי אחראי להגן על פייסבוק? הרי ברור שלרוסיה יש עניין להשיג מידע שאגור בחברות אזרחיות בארצות הברית, וכמו כן ברור שלממשל האמריקני יש עניין להגן על מאגרי מידע אלו. האם ה-NSA צריך לערוך תחקירים ביטחוניים לעובדים המשרתים בתפקידים רגישים בפייסבוק?

שאלת חלוקת האחריות בין המדינה למגזר הפרטי היא שאלה מהותית. ואף שגורמים רבים בעולם דנים בהיבטים שונים של סוגיה זו, **לעת עתה אין לה מענה**. יש הטוענים שהאיום המדינתי צריך להיענות על ידי המדינה בלבד, שכן לחברה האזרחית אין כלים מתאימים להתמודד עם איום זה. עם זאת, יש להכיר בכך שזוהי סוגיה מורכבת ולא בקלות אפשר להכריע בה, בין השאר בשל שני גורמים אלו:

(1) תפיסת המרחב שונה. שלא כמו בעולם הפיזי, אי-אפשר להציב בקלות כוחות צבאיים בין המדינה התוקפת לארגון הנתקף. מנגד, כאשר מדינה רוצה להגביר את מעורבותה במערכות הארגוניות, היא נתקלת בהתנגדות רבה, הן מצד החברה הן מצד לקוחותיה.

(2) בתהליך תקיפה שמבצעים האקרים שמממנות מדינות יש מרכיבים רבים המשותפים לכל תקיפה סטנדרטית. אמנם אפשר לצפות שמדינות ישקיעו מאמץ רב יותר בתקיפה וכן יוכלו להפעיל אמצעים מורכבים יותר (כגון סוכנים, מרגלים ורכיבי חומרה שטופלו), אך ברוב המקרים סביר שבתהליך התקיפה ייעשה שימוש גם בטכניקות ובכלים סטנדרטיים. ולכן, במקרים רבים גם כלי ההגנה המשמשים בהתמודדות עם האיום הסטנדרטי ועם האיום המדינתי זהים. בהתאם לכך, מאמציה של החברה העסקית להתמודד עם האיום הסטנדרטי יכולים כבר היום להיות יעילים במידה מסוימת לשם התמודדות עם האיום המדינתי.

בשל גורמים אלו, יש הצדקה לחזק את מערך ההגנה הקיים בארגונים כך שיוכל להתמודד עם איומים בעלי רמת מורכבות גבוהה יותר בסיוע תמיכה תהליכית-היקפית של גורמים ממשלתיים. כאמור, סוגיה זו, באשר לחלוקת האחריות בין המגזר הפרטי למדינה, טרם הוכרעה.

סוני וצפון קוריאה

מקרה נוסף המייצג את הטשטוש ההולך וגובר בין המגזר הפרטי למגזר הביטחוני הוא הפרשה המתוקשרת של חברת סוני ומדינת צפון קוריאה (SoNKo).
סיפור המקרה התחיל עם פרסום העובדה שסוני הפיקה סרט סטירי ושמו "ריאיון סוף" (The Interview), אשר מתאר התנקשות במנהיג צפון קוריאה קים ג'ונג און בידי זוג עיתונאים שמגיעים לראיין אותו.

ביוני 2014 פנה ז'ה-סונג-נאם, שגריר צפון קוריאה באו"ם, במכתב למזכ"ל האום ובו אמר כי "יש להתייחס לתמיכה בהפקה ובהפצה של סרט כזה... כתמיכה בטרור וכאקט של מלחמה".[10] עוד הוסיף כי "הרשויות בארצות הברית צריכות להגיב מיד תגובה הולמת ולאסור את המשך ההפקה וההפצה של הסרט... אחרת היא (ארצות הברית) תהיה אחראית לעידוד ולמתן חסות לפעילות טרור".

בהמשך, קבוצה של האקרים אשר הזדהו בשם "שומרי השלום" (Guardians of Peace) אף איימו על סוני בהתקפה בסגנון "9/11".[11] סת' רוגן, במאי הסרט ושחקן בו, הגיב לאיומים בחשבון הטוויטר שלו ואמר כי "בדרך כלל לא קורה שאנשים רוצים להרוג אותי בגלל אחד הסרטים שלי **לפני** ששילמו את 12 הדולר הנדרשים בעבורו...".[12]
בדצמבר 2014 התפרסם כי האקרים פרצו למחשבי חברת סוני והדליפו מידע רב, ובכללו סרטים חדשים שטרם פורסמו ותכתובות אימייל פרטיות של עובדי החברה. את הפריצה ייחסו אנשי ה-FBI, שחקרו את המקרה, לצפון קוריאה (בהקשר לכך ראו באגד מאמרים זה את מאמרו של מתן שרף, העוסק באתגר הייחוס).

בהתייחסות למקרה אמר נשיא ארצות הברית ברק אובמה כי "צפון קוריאה יצרה נזק רב... ואנחנו נגיב באופן פרופורציונלי במקום, בזמן ובאופן שייראה לנו לנכון... אנחנו לא יכולים לחיות בחברה שבה דיקטטור כלשהו מפעיל צנזורה בארצות הברית... אני מבין את החלטתה של סוני כחברה פרטית ומודאגת, אבל חבל שהם לא דיברו אִתי קודם...".[13]
מקרה זה מייצג היבט נוסף במערכת היחסים הצבאית-אזרחית: זירת הסייבר מספקת למדינות הזדמנות להעביר מסרים פוליטיים באמצעות תקיפה של חברות מסחריות. סוני מצאה את עצמה בתפקיד מרכזי בחזית הבין-לאומית המדינית בין צפון קוריאה ובין ארצות הברית. ככל הנראה, תקיפה מחוץ לזירת הסייבר כנגד סוני לא תהיה פשוטה כל כך. בזירת הסייבר יכולה מדינה זרה לתקוף חברה אזרחית בלא שזו תיחשב תקיפה של המדינה שבה נמצאת החברה. אך מה היה קורה אם צפון קוריאה הייתה תוקפת את משרדי סוני בעולם הפיזי?

אנו נדרשים לשוב ולשאול, מה יכולה סוני לעשות כדי למנוע פריצות כאלו בעתיד. האם יש לסוני הכלים להתמודד עם צפון קוריאה? האם זהו תפקידה? האם הממשל האמריקני אמור להתערב ולעזור? לשאלות אלו עדיין אין תשובה.

גוגל וסין

10 http://uk.reuters.com/article/2014/07/09/uk-northkorea-un-film-idUKKBN-0FE21B20140709
11 http://techcrunch.com/2014/12/16/sony-hackers-threaten-911-attack-on-movie-theaters/
12 https://twitter.com/sethrogen/status/481811214737997825
13 http://www.cnn.com/2014/12/19/politics/fbi-north-korea-responsible-sony/

בנושא זה של מדינות הפועלות נגד חברות פרטיות ראוי להזכיר את "מבצע אורורה" (Operation Aurora) משנת 2009. מבצע אורורה הוא שם שניתן לאוסף של התקפות סייבר כנגד גוגל, אדובי, יאהו וחברות פרטיות אחרות. את ההתקפות הללו ייחסו גוגל וגורמים אחרים לממשלת סין (כפי שהוצג במסמכים בנושא שפורסמו על ידי ויקיליקס[14]), בין השאר לנוכח ניסיונותיהם של התוקפים להיכנס לתיבות אימייל אישיות של פעילים למען זכויות אדם בסין.

בעקבות פריצה זו החליטה גוגל להפעיל סנקציות אחדות נגד סין, ובהן הפסקת הצנזורה על תוצאות החיפוש ב-Google.cn (גוגל בגרסתו הסינית), שהחברה יישמה לבקשת הממשל הסיני. גוגל הודיעה גם כי היא מבינה שמשמעות החלטה זו עלולה להיות סגירת משרדיה בסין.[15]

בסרטי מדע בדיוני רבים מתואר עתיד שבו חברה פרטית הופכת להיות שליטה בעולם וגיבורי הסרט מנסים להילחם בה. והנה כבר לפני שנים אחדות היינו עדים למקרה שבו חברה פרטית מפעילה סנקציות נגד מדינה – נגד אחת המדינות החזקות בעולם.

והסוף...

לא, אין עדיין סוף טוב לסיפור מאבקי הסייבר בין מדינות לבין חברות. אין זו נקודת שיא ברמת העימות המתקיים בעולם הסייבר אלא רק תחילתה של תקופה. יתרה מזו, מקרים אלו מעידים על הבאות – חברות פרטיות ימשיכו להיות מטרות מרכזיות בזירת הסייבר, במערכה הביטחונית ובמערכת היחסים הסבוכה בין מדינות. ככל שהאנושות תהפוך טכנולוגית יותר, כך יגבר כוחן של חברות טכנולוגיות ותגבר נטייתן של מדינות לתקוף אותן. עלינו להמשיך ולהעמיק את הדיון ולהגדיר מחדש את המדיניות, את מערכת היחסים ואת תהליכי העבודה בין המדינה ובין המגזר הפרטי לשם התמודדות אפקטיבית עם האיומים המתהווים.

14 /http://techcrunch.com/2010/12/04/wikileak-china-google-cables
15 http://googleblog.blogspot.co.il/2010/01/new-approach-to-china.html

5. דגנית פייקובסקי וגיל ברעם: סיכום שנת 2014 בפעילות החלל בעולם

הפעילות העולמית בתחום החלל בשנת 2014 התאפיינה בהתנהלות לנוכח מתחים פוליטיים במערכת הבין-לאומית, שאינם נוגעים ישירות לפעילותן של ממשלות במרחב זה. בעיקר בא לידי ביטוי המתח שהתעורר באביב 2014 בין רוסיה לבין ארצות הברית ומדינות נוספות בעקבות המשבר באוקראינה. במישור המסחרי החלה שנת 2014 ברוח אופטימית, עם ציפייה להתקדמות משמעותית בדרך להגשמת חלום המיזמים הפרטיים בחלל ובראשם הטיסות המאוישות המסחריות לחלל. אולם, בעקבות שתי ההתרסקויות שאירעו באוקטובר בשני מיזמים פרטיים שונים לפיתוח טיסות מסחריות לחלל, נראה כי הדרך למימוש החזון עוד ארוכה. בסקירה זו נציג את המגמות העיקריות שאפשר לאפיין בפעילות העולמית בחלל בשנת 2014.

התבוננות כוללת על חקר החלל בשנה החולפת מעוררת את המחשבה כי מתחזק מחדש הקשר שבין חקר החלל ובין המאבקים הפוליטיים על פני כדור הארץ. המדינות המובילות בחלל פועלות להגיע רחוק יותר מכדור הארץ ועמוק יותר בחלל. ארצות הברית, רוסיה, סין, הודו, יפן וסוכנות החלל של אירופה הכריזו בשנים האחרונות על שאיפתן להגיע לירח, למאדים ולמחוזות רחוקים אף יותר בטיסות בלתי מאוישות ובטיסות מאוישות. מקצתן אף החלו במאמצים למימוש החזון.

משימות מסוג זה מקובעות בהוויה העולמית כאמות מידה לקדמה טכנולוגית. הן מקנות למדינה העוסקת בהן מעמד גבוה במערכת הבין-לאומית ומעידות על מסוגלותה ועל עוצמתה הכוללת. הדבר בא לידי ביטוי בהקצאת משאבים, וכן בהצהרות של מקבלי החלטות ואנשי מקצוע בסוכנויות החלל השונות באשר לחשיבותם של פרויקטים אלו ולמשמעות ההישגים שיושגו בהם. בין ההישגים המשמעותיים יש להתייחס למשימת רוזטה של סוכנות החלל של אירופה, שהגיעה לשיאה עם נחיתת הגשושית פִילֶה על השביט 67P. בנאומו באירוע לכבוד נחיתת הגשושית, הדגיש מנכ״ל הסוכנות ז׳אן ז׳ק דורדיין את ההישג הפוליטי כאשר אמר: ״We are the first to do this, and that will stay forever״.[16]

הודו רשמה הישג חשוב כאשר רכב החלל, ששיגרה אל עבר מאדים בסוף שנת 2013, נכנס בהצלחה למסלול סביב מאדים ואף שידר תמונות לכדור הארץ. הצלחת המשימה הוכיחה

16 *Comet 67P becomes landing site for Philae in historic touchdown*, **The Guardian**, 13 November 2014. http://www.theguardian.com/science/2014/nov/12/rosetta-mission-philae-historic-landing-comet

כי גם בתקציב צנוע של מדינה מתפתחת אפשר להגיע להישג כזה.[17] נוסף על כך, בדצמבר 2014 הצליחה הודו לבצע ניסוי שבו שיגרה לחלל והחזירה קפסולה בלתי מאוישת. זהו שלב חשוב בדרך לתכנית מאוישת.[18]

לצורך מימוש המשימות השאפתניות להגיע שוב לירח ומשם גם למאדים, יש צורך במשגרים רבי עוצמה בעלי כושר נשיאה של מטענים גדולים וכבדים במיוחד. בארצות הברית, ברוסיה ובסין החלו לפתח משגרים מסוג זה בעלי יכולת נשיאה של יותר מ-100 טון. המעניין הוא שנוסף על השקעת משאבים ברמה הלאומית, בחלק מהמקרים יש עניין לשלב גם משימות במודל שלPPP (שותפות ממשלתית מסחרית). לדוגמה, נאס״א בוחנת את האפשרות לשלב לוויינים מסחריים במשימותיה לירח ולמאדים.[19]

בתחום הטיסות המאוישות לחלל, ראוי להתייחס לשני נושאים עיקריים. הנושא האחד הוא המתח שבין רוסיה לארצות הברית על רקע המשבר באוקראינה, המאיים להשפיע על תפקודה של תחנת החלל הבין-לאומית ועל פעילותם של האסטרונאוטים והקוסמונאוטים החיים בה. הנושא השני הוא עתיד הטיסות המאוישות הפרטיות לחלל.

המשבר בין רוסיה לבין ארצות הברית הוכיח מחדש שלטיסות מאוישות לחלל יש ערך אסטרטגי רב בעיני שתי המדינות, ועל כן הן מהוות קלף אסטרטגי במאבק ביניהן. רוסיה הודיעה כי אין בכוונתה להאריך את משך פעילותה בתחנת החלל הבין-לאומית וכי ברצונה להפנות את המשאבים הללו לפרויקטים חדשים. היא אף הודיעה כי הפרויקט המרכזי שלה יהיה חקר הירח ויכלול הקמת מחנה על הירח.[20] מנגד, ארצות הברית מעוניינת להאריך את משך פעילותה של תחנת החלל. לנוכח תלותה הנוכחית ברוסיה לשיגור אסטרונאוטים לתחנה, הודיעה נאס״א על התקשרות עם חברות פרטיות אמריקניות לצורך טיסות אל

---

17 S. Choudhury and J. Sugden, *How India Mounted the World's Cheapest Mission to Mars*, **The Wall Street Journal - India,** Sep 23, 2014. http://blogs.wsj.com/indiarealtime/2014/09/23/how-india-mounted-the-worlds-cheapest-mission-to-mars/

18 *India launches biggest ever rocket into space*, **Space Daily**, Dec 18, 2014. Staff Writers, http://www.spacedaily.com/reports/India_launches_biggest_ever_rocket_into_space_999.html

19 B. Pavlischev, *First space tourists to fly around Mars and Venus in 2021*, **Space Travel**, Mar 13, 2014. http://www.space-travel.com/reports/First_space_tourists_to_fly_around_Mars_and_Venus_in_2021_999.html

20 P.B. de Selding, U.S., *European Space Chiefs Urge Public To Look Past Russian Rhetoric*, **Space News**, May 23, 2014. http://spacenews.com/40666us-european-space-chiefs-urge-public-to-look-past-russian-rhetoric/?_wcsid=F74CC0BF4C22D3FF83FC59B6FB3D476433FDA26192541BE0B571B18A98549D57

התחנה וממנה.[21] ראוי לציין כי יכולת כזו עדיין לא הבשילה.

מעבר להיבט האסטרטגי, החלטתה של נאס״א היא מסר של אמון ביכולת של השוק הפרטי לפתח את הטכנולוגיה הדרושה ברמת הבטיחות הנדרשת לביצוע טיסות מסחריות מאוישות לחלל, ואמון בכדאיות הכלכלית של המהלך. עם זאת, ההשקעה של השוק הפרטי בטיסות מאוישות אינה מובנת מאליה. בתחילת שנת 2014 היו הציפיות להתקדמות בתחום זה גבוהות. בינואר נרשמו הצלחות אחדות, ובהן טיסת ניסוי מוצלחת לחללית של וירג'ין גלקטיק, שהמריאה בהצלחה לגובה של 71 אלף רגל (כ-21,540 מטרים) מעל פני כדור הארץ.[22] הצלחה נוספת באותו חודש הייתה לחברת Orbital Sciences, ששיגרה בשנית חללית אספקה לתחנת החלל הבין-לאומית.[23]

למרות ההתפתחויות החיוביות הללו, אירעו באוקטובר 2014 , בהפרש של ימים ספורים, שני כישלונות. האחד היה התרסקות המשגר של Orbital Sciences, שנשא חללית אספקה לתחנת החלל הבין-לאומית, והשני – התרסקות החללית של חברת וירג'ין גלקטיק בטיסת ניסוי, שבה נהרג אחד הטייסים. הייתה זו מכה קשה לפעילות הפרטית בחלל. התאונות עוררו דיון מחודש בהיתכנות הטכנולוגית ובכדאיות הכלכלית בעבור השוק הפרטי. כותרות העיתונים שעסקו בנושא הכריזו על סופו של חלום תיירות החלל, ובהמשך לכך היו שקראו לחדול מפעילות זו בטענה שמדובר בסיכון מיותר. יש להניח שגם אם תאונות אלו יעכבו את התהליך, בחינה מדוקדקת של הסיבות שהובילו לכשלים תאפשר להסיק את המסקנות המתבקשות ולשכלל את הכלים הטכנולוגיים.

בשנים האחרונות רווחה מגמה של העמקה והרחבה של שיתופי הפעולה הבין-לאומיים בתחום החלל. שני תמריצים הניעו מגמה זו: הראשון, הצורך להתמודד עם צמצום המשאבים העומדים לרשות קידום פרויקטי חלל; השני, תופעות ובעיות שההתמודדות עמן מחייבת שיתוף פעולה מצד מספר רב של מדינות, כגון הטיפול בפסולת חלל, על מנת להבטיח את הפעילות התקינה של מערכות החלל בכללותן. אולם בשנה החולפת, בשל החרפת המתח בזירה הבין-לאומית, אפשר לזהות האטה בנכונות לשתף פעולה ועלייה בתחרותיות וברצון לבסס יכולת עצמאית. לדוגמה, עתידה של ספינת הדגל של שיתוף הפעולה בחלל, תחנת החלל הבין-לאומית, עמד במרכזו של הוויכוח בין ארצות הברית

21 I. Klotz, *Commercial Crew Partners Get Extension*, **Space News**, June 27, 2014. http://spacenews.com/41043commercial-crew-partners-get-extension/

22 Staff Writer, *SpaceShipTwo soars to 71,000 feet above Earth during test*, **Space Travel**, Jan 10, 2014. http://www.space-travel.com/reports/SpaceShipTwo_soars_to_71000_feet_above_Earth_during_test_999.html

23 Staff Writers, *Orbital Sciences launches second mission to space station*, **Space Travel**, Jan 09, 2014. http://www.space-travel.com/reports/Orbital_Sciences_launches_second_mission_to_space_station_999.html

לבין רוסיה על רקע המשבר בנושא אוקראינה. בתחום מערכות הניווט הלוויינים ניכר הצורך בעצמאות טכנולוגית. רוסיה פועלת לשדרוג המערך שלה ולהרחבתו, וכך גם אירופה, סין, הודו ואף יפן. מנגד, ארצות הברית פועלת לשימור מעמד מערך ה-GPS שלה.

ובכל זאת, יש מספר לא מבוטל של דוגמאות לשיתופי פעולה. ארצות הברית וצרפת פעלו להידוק הקשרים ביניהן. בינואר 2014 חתמו סוכנויות החלל בשתי המדינות על הסכם לשיתוף פעולה בנושא שיגור כלי רכב נוסף למאדים בשנת 2016, במסגרת InSight mission.[24] דוגמה נוספת היא הידוק היחסים הנרקם בין ארצות הברית ליפן. כחלק מיוזמת החלל של טוקיו (Tokyo's space initiative) שואפת יפן להגביר את שיתוף הפעולה שלה עם ארצות הברית בתחום החלל. מבחינת ארצות הברית, הדבר משתלב באסטרטגיה הצבאית שלה באסיה ובחיפוש אחר שותפים שיאפשרו לה להרחיב את הכיסוי הלוויני שלה באזור.[25]

רוסיה פועלת להידוק קשריה עם סין. שתי המדינות הסכימו על הקמת שלושה מנגנונים לשיתוף פעולה ביניהן, ובכלל זה על קבוצת עבודה בנושא שיתופי פעולה בתחום החלל.[26] בין הנושאים שבהם מעוניינות שתי המדינות לשתף פעולה נמצא תחום הניווט הלווייני, כאשר מטרתן לייצר אלטרנטיבה למערכת ה-GPS האמריקנית.[27] סין ממשיכה במאמציה להדק קשרים עם מדינות חדשות בתחום החלל וגם עם מדינות ותיקות. לדוגמה, במרץ 2014 נחתם הסכם שיתוף פעולה בין סין לבין צרפת. ביטוי ממשי ראשון להסכם הוא פיתוח משותף של לוויין אסטרונומי שיבחן התפרצויות קרינת גמא

---

24 M. Hoffman, *NASA taps French space hub for 2016 mars exploration partnership; C. Bolden comments,* **Executive Gov,** Feb 11, 2014.

http://www.executivegov.com/2014/02/nasa-cnes-partner-for-2016-mars-exploration-project-charles-bolden-comments/?utm_source=ExecutiveGov+Daily+RSS+Feed&utm_campaign=56fa4ca913-RSS_EMAIL_CAMPAIGN&utm_medium=email&utm_term=0_36a0a71ec1-56fa4ca913-80419289

25 Staff Writers, *US looks to Japan space program to close Pacific communications gap,* Space War, Aug 7, 2014.

http://www.spacewar.com/reports/US_looks_to_Japan_space_program_to_close_Pacific_communications_gap_999.html

26 P.J. Blount, *China-Russia Sign Cooperation Agreement,* **Res Cummunis**, May 27, 2014. http://rescommunis.olemiss.edu/2014/05/27/china-russia-sign-cooperation-agreement/?utm_source=rss&utm_medium=rss&utm_campaign=china-russia-sign-cooperation-agreement

27 Staff Writers, *Russia may join forces with China to compete with US, European satnavs*, **GPS Daily**, Jun 10, 2014. http://www.gpsdaily.com/reports/Russia_may_join_forces_with_China_to_compete_with_US_European_satnavs_999.html

(gamma-ray-burst astronomy satellite), פרויקט שעליו הוכרז באוגוסט. הלוויין ישוגר בשנת 2021 על גבי המשגר הסיני Long March.[28]

כבר הוזכר כי הבטחת הביטחון והקיימות בחלל הוא נושא חשוב באינטראקציה שבין המדינות. אינטראקציה זו מלווה במתח מסוים – בין הרצון והצורך של מדינות לשמור על חופש הפעולה שלהן בחלל ולהגן על מערכות החלל שלהן ובין הצורך לשמור על סביבת החלל ולשתף פעולה לשם כך. לעתים יש סתירה בין פעולות אלה. לדוגמה, השמירה על הקיימות של סביבת החלל מחייבת את המדינות לנהוג על פי כללים מסוימים שעשויים להקשות על חופש הפעולה שלהן בחלל. נוסף לכך, יכול להיווצר מתח בשל הצורך לשתף פעולה, ובעיקר לשתף במידע, על רקע של חוסר אמון שמקורו באפשרות להשתמש במידע לשימוש דו-תכליתי, לעתים אגרסיבי.

בשנים האחרונות התנהלו כמה תהליכים בין-לאומיים במטרה לגבש כללי התנהלות והסכמות באשר להבטחת השימוש בחלל והקיימות בסביבת החלל. באביב 2014 נרשמה התקדמות בנושא עם פרסום הטיוטה הרביעית של הקוד להתנהלות בחלל. הטיוטה מבטאת את התפיסה שלפיה לכל מדינה יש גישה חופשית לחלל למטרות שלום, והיא קוראת לכל המדינות לשמור על שלמות העצמים הקיימים בחלל. בטיוטה זו הושמט הסעיף הנוגע ל״התחשבות באינטרסים הביטחוניים הלגיטימיים של המדינות״, אך הודגשה הזכות להגנה עצמית.[29] הטיוטה הנוכחית מספקת מנגנונים ליצירת שקיפות רבה יותר, אך האתגר הוא לגשר על הפערים ולאפשר בניית יחסי אמון בין המדינות.
במאי 2014 התקיים בלוקסמבורג מפגש לדיון פתוח בטיוטת הקוד, שבו השתתפו משלחות משמונים מדינות לערך, בהן גם משלחת מישראל. המפגש היה חיובי, אולם נותרו פערים הנוגעים לתחולת הקוד. ארצות הברית, מדינות האיחוד האירופי ומדינות נוספות – ביניהן קנדה ואוסטרליה, למשל – מעוניינות בגישה הוליסטית שלפיה יחול הקוד על כלל הפעילות בחלל. לעומתן, רוסיה וסין ומדינות נוספות מצדדות בגישה מצמצמת שלפיה יחול הקוד רק על פעילות אזרחית ומסחרית, ואילו הפעילות הצבאית תטופל במסגרות אחרות. המתח האסטרטגי בין ארצות הברית לרוסיה משפיע גם על נושא זה ומרחיק את האפשרות להגיע להסכמות. ההתקדמות במישור הדיפלומטי הרב-צדדי סובלת מהאטה ואף מקיפאון, וכעת עתידו של הקוד הבין-לאומי להתנהלות בחלל לוט בערפל.

בשלב זה, התרומה המשמעותית של הקוד לשיח על ביטחון וקיימות בחלל היא בהצבת

28 P.B. de Selding, *China, France Join Forces on Astronomy Mission,* **Space News**, Aug 4, 2014. http://spacenews.com/41479china-france-join-forces-on-astrono-/my-mission

29 R.P. Rajagopalan, *EU's New Space Code: A Significant Improvement*, **Space News**, Nov 11, 2013. http://www.spacenews.com/article/opinion/38115eu%E2%80%99s-new-space-code-a-significant-improvement

נורמה ברורה נגד יצירת פסולת חלל, וזו נחשבת לליבת הקוד.
במקביל לפעילות זו, המשיכו רוסיה וסין לקדם תהליך בנושא מניעת מרוצי חימוש בחלל ובקרת נשק בוועידה לפירוק הנשק של האו"ם (Conference on Disarmament). ביוני הגישו השתיים נוסח חדש להצעתן לאמנה למניעת הצבה של נשק בחלל, ה-PPWT.[30],[31] ארצות הברית מתנגדת להצעה זו. לטענתה, הטיוטה המוצעת אינה שוויונית ולא ניתן לפקח על ביצועה, ועל כן היא אינה תורמת להגברת הביטחון של כלל המדינות. ההתנגדות האמריקנית נובעת מהחשש כי סין ורוסיה מפתחות מערכות נשק בחלל.[32]

למרות הקושי במישור הרב-לאומי, אפשר לזהות מודעות הולכת וגוברת במדינות שונות להכרח לטפל בנושאים חשובים לסביבת החלל. מקצת המדינות פועלות באופן בלתי תלוי כדי לצמצם את פסולת החלל שהן מייצרות או לנטר את העצמים הנמצאים בחלל. דוגמאות לכך הן שדרוג ותגבור של מערכות מעקב אחר עצמים בחלל שמטרתם לספק מידע והתרעה מפני התנגשויות צפויות, והסכמים לשיתופי פעולה בין מדינות שלא על בסיס הסכמה בין-לאומית רחבה. במאי 2014 חתמו ארצות הברית, אוסטרליה, בריטניה וקנדה על הסכם לשיתוף פעולה (MOU) בנושא מודעות מצבית בחלל (Space Situational Awareness Activities).[33] רוסיה הודיעה כי היא פועלת לשדרג את יכולותיה לזיהוי עצמים בחלל וכי בשנים הקרובות תקים רשת תחנות לייזר-אופטיות מתקדמות במטרה להגדיל את יכולתה זו.[34] באירופה נעשים מאמצים לפתח יכולות אירופיות למעקב אחר עצמים בחלל.[35] בספטמבר הודיעה סוכנות החלל של יפן כי כאשר ישוגר משגר הלוויינים הקטנים החדש אפסילון, ייכנס השלב העליון למסלול נמוך דַיו על מנת שיחזור במהרה

30 PPWT – Treaty on Prevention of the Placement of Weapons in Outer Space and of the Threat

31 *U.S. Opposes New Draft Treaty from China and Russia Banning Space Weapons*, **The Washington Free Beacon,** June 19, 2014. http://missilethreat.com/u-s-/opposes-new-draft-treaty-from-china-and-russia-banning-space-weapons

32 P.J. Blount, *Space at the Conference on Disarmament*, **Res Communis**, June 27, 2014. http://rescommunis.olemiss.edu/2014/06/27/space-at-the-conference-on-disarmament/?utm_source=feedly&utm_reader=feedly&utm_medium=rss&utm_campaign=space-at-the-conference-on-disarmament

33 M. Gruss, *UK Joins List of US Allies Agreeing To Strengthen Space Surveillance Sharing*, **Space News**, Sep 25, 2014. http://www.spacenews.com/article/military-space/41995uk-joins-list-of-us-allies-agreeing-to-strengthen-space-surveillance

34 Staff Writers, *Russia Plans to Boost Space Monitoring Capability by 2018*, **Space Daily,** Sep 22, 2014. http://www.spacedaily.com/reports/Russia_Plans_to_Boost_Space_Monitoring_Capability_by_2018_999.html

35 Staff Writers, *ESA's bug-eyed telescope to spot risky asteroids*, **Space Daily**, Sep 12, 2014. http://www.spacedaily.com/reports/ESAs_bug_eyed_telescope_to_spot_risky_asteroids_999.html

לאטמוספרה של כדור הארץ ולא ייוותר בחלל פרק זמן ממושך.[36] בצרפת חוקק חוק בנושא חלל, שמטרתו להגביל היווצרות של פסולת חלל הנוצרת משאריות משגרים ולחייב את מי שמשגר לחלל להבטיח חזרה מהירה לאטמוספרה ונחיתה מעל מקור מים.[37] גם סין הודיעה כי היא מקדמת מדיניות ורגולציה בכל הנוגע לשיגור אזרחי לחלל, רישום של עצמים בחלל, מניעה והפחתה של פסולת חלל.[38]

מתקיימת גם פעילות לפיתוח פתרונות טכנולוגיים להתמודדות עם פסולת החלל ולניקוי החלל. לדוגמה, סוכנות החלל של אירופה הודיעה כי היא בוחנת אפשרות לפתח רכב חלל שמטרתו ללכוד לוויינים שסטו ממסלולם סביב כדור הארץ, בגובה 800 עד 1000 ק"מ (Derelict Satellites Adrift - DeOrbit). המשימה תבוצע בהתאם לדירקטיבה Clean Space Initiative.[39]

ביטחון החלל נוגע גם להתמודדות עם שיבוש ומניעת השימוש במערכות חלל. ביוני 2014 דיווחה Eutelsat, שמספקת שירותי תקשורת רבים למדינות המזרח התיכון ואפריקה, כי הפרעות מסוג jamming הן הגורם לכ-15% מבעיות התקשורת שמהן סבלה החברה בשנת 2013, לעומת 5% בשנת 2010.[40] הדבר מחדד את החשיבות של אבטחת התקשורת באמצעות לוויינים. כחלק מתופעה זו יש גם עיסוק הולך וגובר בממשק שבין עולם הסייבר לעולם החלל. דו"חות אחדים שפרסמו במהלך השנה מכוני מחקר וגם חברות פרטיות הצביעו על כך שאיום הסייבר על מערכות חלל הוא איום משמעותי. כך לדוגמה, מדו"ח של המועצה ליחסי חוץ (Council on Foreign Relations) שפורסם באפריל עולה, כי ארצות הברית הופכת פגיעה יותר ויותר לטרור חלל, מכיוון שתשתיותיה נסמכות על

36 P.B. de Selding, *JAXA Addresses Debris Issue with Epsilon Small-satellite Launcher,* **Space News,** Sep 30, 2014. http://www.spacenews.com/article/launch-report/4203865th-international-astronautical-congress-jaxa-addresses-debris-issue

37 P. B. de Selding, *French Debris-mitigation Law Could Pose Issue for Arianespace*, **Space News,** April 10, 2014. http://www.spacenews.com/article/launch-report/40171french-debris-mitigation-law-could-pose-issue-for-arianespace

38 Staff Writers, *China expects to introduce space law around 2020,* **Space Daily**, Nov 19, 2014. http://www.spacedaily.com/reports/China_expects_to_introduce_space_law_around_2020_999.html

39 Staff Writers, Space agency studying ways to capture derelict satellites, space junk, Space Mart, Feb 21, 2013. http://www.spacemart.com/reports/Space_agency_studying_ways_to_capture_derelict_satellites_space_junk_999.html

40 P.B. de Selding, *Eutelsat Blames Ethiopia as Jamming Incidents Triple*, **Space News**, June 6, 2014, http://spacenews.com/40818eutelsat-blames-ethiopia-as-jamming-incidents-triple/

לוויינים שפגיעים מאוד לפסולת חלל וכן לתקיפה קיברנטית.[41]

באוגוסט פורסם דו"ח של המפקח הכללי במחלקת המסחר בארצות הברית המתריע על חולשות באבטחת תחנות קרקע של מערכות לווייני מזג אוויר Joint Polar Satellite System (JPSS). על פי הדו"ח, מדובר בבעיות תוכנה שניתנות לתיקון כמו תוכנות שאינן מעודכנות, פתרונות אבטחה חסרים, מתן הרשאות לגורמים שאינם מורשים, תוכנות שאינן מותאמות כראוי ועוד. למרות ההתרעה על בעיות האבטחה הנושא לא טופל, ובסוף ספטמבר אירעה חדירה ככל הנראה למערכות של המינהל הלאומי לאוקיינוסים ואטמוספירה NOAA. האירוע נחשף רק ב-20 באוקטובר, ו-NOAA לא דיווחה לרשויות המתאימות עד ראשית נובמבר.[42]

גם באירופה מזהים את איום הסייבר כאיום משמעותי על מערכות חלל. לדעת בכיר בסוכנות האירופאית להגנה EDA, החיבור שבין הסייבר לחלל הוא עקב אכילס של אירופה, המחייב היערכות וטיפול בכל הרמות.[43] תעשיית תקשורת הלוויינים העולמית הכריזה על יוזמה גלובלית חדשה להקמת כוח משימה בנושא איומי סייבר, במטרה להאיץ את נושא ההתמודדות עם איומי הסייבר הגוברים נגד לוויינים.[44]
כל אלו ועוד הפכו את 2014 לשנה רבת פעילות ועניין בתחום החלל.

41 Staff Writers, *Space terrorism, floating debris pose threats to US*, **Space Mart**, Apr 27, 2014. http://www.spacemart.com/reports/Space_terrorism_floating_debris_pose_threats_to_US_999.html לקריאה נוספת על איום הסייבר על מערכות חלל ראו:

http://www.foreignaffairs.com/articles/142690/deganit-paikowsky-and-gil-baram/space-wars

42 M. Flaherty, J. Samenow and L.Rein, *Chinese hack U.S. weather systems, satellite network*, **The Washington Post**, November 12, 2014. http://www.washingtonpost.com/local/chinese-hack-us-weather-systems-satellite-network/2014/11/12/bef1206a-68e9-11e4-b053-65cea7903f2e_story.html

43 הדברים נאמרו על ידי מר ריני גוס מה-EDA בכנס שהתקיים באתונה ביוני 2014 שכותרתו חלל וביטחון.

44 *GVF Rallies International Support for Protection of C-band from IMT*, **Global VSAT Forum**, 23 November 2012, http://gvf.org/

6. טל דקל: רשתות חברתיות ומאמצים מבוססי מיקור המונים ככלי לניהול מצבי חירום – סיכום ומגמות[45]

תקציר

שנת 2014 נפתחה בהתרסקות מטוס והסתיימה בהתרסקות מטוס.בשנה זו נחשפו משתמשי הרשת לזוועות ולמלחמות אזרחיםומאידך נוצרו ברשת קהילות ענק שהתארגנו לפעולות הצלה משותפות.

רשתות חברתיות משנות את דרכי התקשורת בין פרטים ובין ארגונים, ויוצרות קהילות חדשות. לקהילות חדשות אלו יש מאפיינים המאפשרים להן לפעול במרוכז למען מטרות הקהילה בהיקף ובמהירות גדולים מאי פעם. התפתחות בתשתיות הניווט הלווייני, הורדת חסמי הכניסה לשימוש בטלפונים חכמים ומגוון הישומונים בתחם הניווט והתקשורת – כל אלו מייצרים הזדמנויות חדשות ברשתות החברתיות. השינויים מתרחשים הן ברמת מבנה הקהילות והן ברמת התחביר והמדיה היוצרת את השיח בין המשתמשים.

גם בשנת 2014 בלטו ישומונים פרי פיתוח ישראלי שהפכו ויראליים בתוך ימים. זאת לצד התקדמות בשירותים אותן מספקות החברות הגדולות בשוק, גוגל ופייסבוק. אנו צופים כי השילוב בין התפתחות התשתיות ,הנגשת הטלפונים החכמים והתפתחויות בעולם האפליקציות ייצור מתווה חדש לניהול מצבי חירום . מתווה זה יחייב את מקבלי ההחלטות וארגוני הסיוע לערוך התאמות מהירות ואולי אף לחשוב מחדש על הכלים שבהם ראוי לנהל מצבי חירום.

במאמר זה נסקור בקצרה את ההתפתחויות הטכנולוגיות ,את מגוון הישומונים הרלוונטים לניהול מצבי חירום, ואסכם במבט צופה אל העתיד את התנהלות הקהילה באירועי חירום עתידיים.

מה בין רשתות חברתיות, רשתות חברתיות מבוססות מיקום ומאמצים

45 מאמר זה הוא סיכום של עבודה הנעשית בסדנת יובל נאמן וב- International Committee for GNSS (ICG), תת ועדה של UNOOSA. חלקים מעבודה זו הוצגו בכנס מס' 93 של סדנת יובל נאמן: "30 שנה לסוכנות החלל הישראלית – שימושים אזרחיים בחלל" וכן ב-: United Nations/Abdus Salam International Centre for Theoretical Physics Workshop on the Use of Global Navigation Satellite Systems for Scientific Applications. http://www.unoosa.org/pdf/sap/2014/trieste-gnss/29_.pdf

מבוססי מיקור המונים?

רשת חברתית (Social network) היא מבנה חברתי המורכב מקבוצה של מספר גורמים חברתיים (כגון אנשים או ארגונים), המקיימים ביניהם מערכת של קשרים.
רשת חברתית מבוססת מיקום היא מבנה חברתי הבנוי מפרטים המחוברים על ידי תלות הדדית הנגזרת ממיקומם בעולם הפיזי ומהאינטרסים, מההתנהגויות ומהפעילויות המשותפות להם.[46]

ישומונים מבוססי חישת המונים הינם רכיב קריטי בבנית הרשתות החברתיות מבוססות המיקום ישומונים אלה שימוש בטלפונים חכמים כדי לאסוף ולחלוק אינפורמציה על המשתמש וסביבתו באמצעות תרומה אקטיבית או פסיבית של משתמשים למען מטרה משותפת[47].

מיקור המונים הוא תהליך של ביצוע משימה או קבלת שירות באמצעות שימוש בקהילה במקום בספקי שירותים מסורתיים. ייחודן של רשתות חברתיות ומאמצים מבוססי מיקור המונים הוא יכולתם לצבור תכולה משמעותית בהינתן משאבים מוגבלים, למשל פרק זמן קריטי לביצוע משימה, מיעוט משאבים לרבות משאבי רשת או צורך בכוח עבודה רב לביצוע משימה נתונה. ייחוד זה מתחדד בעת התאוששות מאסון, עקב הצורך לממש משאבים מוגבלים בזמן קצר ובאופן ממוקד למטרות שונות. יכולות אלו של הרשתות החברתיות מאפשרות בנייה מחדש של קהילות שיתמכו זו בזו וכן בנייה של קהילות פונקציונליות למטרה ספציפית.

התפתחויות טכנולוגיות בשנת 2014

שנת 2014 הייתה שנה רוויה בחידושים טכנולוגיים, אשר השפיעו על התפתחות בתחום הרשתות החברתיות. חידושים רבים צצו ויצרו השפעה מיָדית על מיליונים של משתמשים.
רשתות חברתיות בכלל ורשתות חברתיות מבוססות מיקום בפרט מתבססות על איסוף

46 "… A social structure made up of individuals connected by the interdependency derived from their locations in the physical world … a given timestamp and the location history … [and their] common interests, behavior, and activities." Source : http://research.microsoft.com/en-us/projects/lbsn

47 Mobile crowd sensing apps leverage consumer mobile devices (e.g., smart phones, GPS gadgets, and cars) to collect and share information about the user or the environment, either interactively or autonomously, towards a common goal." Source: web.engr.illinois.edu/~hanj/APP/I1/I1.1_Lei.ppt Hui Lei, Fan Ye IBM T. J. Watson Research

ועל הנגשת מידע למשתמשים מתוך טלפונים חכמים. הטכנולוגיות המונגשות למשתמשים הן טכנולוגיות למציאת מיקום, טכנולוגיות רשת ואפליקציות העושות שימוש בחיישני המכשיר.[48] טכנולוגיות הקשורות ספציפית ברשת החברתית מאפשרות שיטות תקשורת חדשות בקהילה על פי דרישה (Pull) או בדחיפה (Push), לפי הגדרות המשתמש.

בתחום הנגשת מערכות הניווט הגלובליות (Global Navigation Satellite Systems-GNSS) לאוכלוסייה חלה התפתחות משמעותית השנה. מאז הודעתה של סין בשלהי שנת 2012 על כך שמערכת Baidu[49] החלה לתת שירות מלא למשתמשים באיזור אסיה-פסיפיק, ישנם כמה אזורים בכדור הארץ מכוסים באופן רציף על ידי ארבע מערכות ניווט לווייניות.[50] המשמעות המִיָּדית למשתמשים היא כי אפשר לקבל מיקום מדויק ומהיר בזמינות ובאיכות שירות גבוהה גם באזורים עירוניים. בפברואר 2014 הודיעה חברת קוואלקום (Qualcomm) על השקת המעבד Snapdragon 610 לטלפונים חכמים. מעבד זה מכיל יכולת קליטה ועיבוד של שלוש רשתות GNSS (GPS, GLONASS ו-Baidu). המעבד הוטמע והושק כבר השנה בטלפון החכם HTC Desire 820 של חברת HTC וכן בסדרת הפרימיום Samsung Galaxy Note 4.

מספר המשתמשים בטלפונים חכמים הגיע השנה ל 1.75 מיליארד בני אדם, עם צפי לחצות את רף שני מיליארד המשתמשים עד שנת 2017.[51] אחד ממנועי הצמיחה המשמעותיים בשוק הטלפונים החכמים הוא ההתרחבות הגלובלית של יצרניות הענק הסיניות ZTE, וואווי, לנובו, שיואמי ואופו. הדבר מתבטא בהשקות תכופות של מכשירים מבוססי אנדרואיד באיכות טובה ובמחיר הולך ויורד. רכישת Motorola Mobility על ידי לנובו, יצרנית המחשבים הניידים הגדולה בעולם, מצביעה על כוונת החברות הסיניות להיכנס כיצרניות לגיטימיות לשווקים נוספים בעולם ולמכור בהם.

התפתחות משמעותית הסתמנה בשנת 2014 גם בתחום מבנה הטלפון החכם. מכירת Motorola Mobility על ידי גוגל חשפה פרויקט מרתק שעליו גוגל לא הייתה מוכנה לוותר. החל בשנת 2011 רכשה גוגל סדרה של פטנטים הקשורים לפיתוח טלפון חכם מודולרי. בשנת 2011 היא רכשה את הפטנטים של חברת מודו הישראלית. שנה אחר כך רכשה

48 החיישנים שבהם נהוג להשתמש הם מצלמות מתקדמות, חישת תנועה, זעזועים, גובה, לחץ ברומטרי ורעש. בטלפונים החדשים, יחידות לוגיות המסופקות עם המכשירים מאפשרות להבין את מצבו של המשתמש.

49 Baidu היא מערכת ניווט לוויינית סינית המבוססת על קונסטלציית לוויינים ותחנות קרקע, המאפשרות למשתמש בעל מקלט ייעודי למצוא את מיקומו העצמי.

50 GPS האמריקנית , GLONASS הרוסית, Baidu הסינית ו- QZSS היפנית

51 http://www.emarketer.com/Article/Smartphone-Users-Worldwide-Will-Total-175-Billion-2014/1010536 - 1.75B users

בעסקת ענק את Motorola Mobility בסכום של 12.5 מיליארד דולר. בשנת 2014 מכרה גוגל את חטיבת היצור ללנובו, אך השאירה בחטיבת האנדרואיד של החברה פרויקט יחיד Google Ara–, העוסק בפיתוח פלטפורמת שלד חיצוני פריק לטלפון חכם. פרויקט זה יאפשר למשתמשים לרכוש ולהרכיב לעצמם טלפון חכם עם מגוון יישומים במחיר מטרה של חמישים דולר ליחידה בסיסית. במבנה המוצע כיום תכלול יחידה זו מעבד, משדר Wi-Fi, מסך וסוללה. הדגם הראשון של המכשיר יושק בחודשים הקרובים בפורטו ריקו במסגרת פיילוט של הפרויקט.

עולם הישומונים סיפק בשנת 2014 מגוון חידושים. בחודש אוקטובר הכריזה פייסבוק על כניסתה לתחום מצבי החירום עם שירות Safety Check.[52] בהודעה לתקשורת מטעם החברה הוצג אסון הצונמי ביפן כגורם שהביא את מהנדסי החברה ביפן לפתח את השירות. השירות מאפשר העברת הודעה קצרה וממוקדת "I'm Safe" לחברים בעת אסון. את השירות יאפשרו המשתמשים עצמם, והוא יופעל על ידי פייסבוק בעת אסון. שרת המערכת יקבע אם משתמש נמצא באזור אסון בהתבסס על תכונת התיוג הגיאוגרפי ""Nearby Friends, עיר מגורים או מקום ההתחברות לאינטרנט. משתמשים באזור אסון יוכלו להודיע באמצעות השירות שהם בריאים ושלמים. ההודעה תפורסם רק לחברים של המשתמש. בצילומי מסך של השירות נראה כי אין אפשרות לדווח אם המשתמש במצוקה ומה מהותה. כמו כן נראה כי אין אפשרות להוסיף תיוג גיאוגרפי להודעה. הודעה זו לתקשורת באה על רקע הפיכת Google Person Finder, שפותח על ידי צוות התגובה של גוגל בעת אסון רעידת האדמה בהאיטי, לסטנדרט באירועי אסון.

רשתות חברתיות שפותחו בארץ שינו השנה את הדרך שקהילות מתקשרות בה. אפליקציית FireChat הוצגה לציבור במרץ 2014. האפליקציה זכתה לפרסום רב ולשימוש נרחב בהונג-קונג[53] ובעירק.[54] בשני המקרים אפשרה האפליקציה, בעת מחאה אזרחית וכיבוי הרשתות הסלולריות והאינטרנט, להעביר הודעות על בסיס האינטרנט האלחוטי (Wi-Fi) והבלוטותי (Bluetooth) של המשתמשים. אפליקציה זו היא הסנונית הראשונה בגל של אפליקציות שיאפשרו ליצר רשת אינטרנט מקומית על בסיס המשתמשים גם בלא תשתית

52 הודעה לתקשורת בנוגע לשירות http://newsroom.fb.com/news/2014/10/introducing-safety-check/ (אוחזר בתאריך 15 לינואר 2015).

53 קריאה נוספת על השימוש באפליקציה בעת ההפגנות בהונג קונג ועל ההד התקשורתי שהאפליקציה זכתה לו: http://edition.cnn.com/2014/10/16/tech/mobile/tomorrow-transformed-firechat/ (אוחזר בתאריך 15 לינואר 2015).

54 קריאה נוספת על השימוש באפליקציה בעת ההפגנות בעירק ועל ההד התקשורתי שהאפליקציה זכתה לו:

http://www.theguardian.com/technology/2014/jun/24/firechat-updates-as-40000-iraqis-download-mesh-chat-app-to-get-online-in-censored-baghdad (אוחזר בתאריך 15 לינואר 2015).

רשת חיצונית. אנו צופים כי במצבי אסון יהפכו אפליקציות מעין אלו להיות חבל הצלה לאוכלוסייה באזורים פגועים.

הישומון YO, מבית מובּלי של היזם מושיק חוגג, פותחה בשמונה שעות בלבד ורכשה מאות אלפי משתמשים בתוך ימים ספורים.[55] אפליקציה זו מאפשרת תקשורת בין חברים באמצעות הברה אחת "YO". היא מאפשרת תקשורת מבוססת קונטקסט ונטולת שפה בין חברים ברשת.

באסון רעידת האדמה בהאיטי היה מחסום השפה חסם משמעותי בסיוע לאוכלוסייה. מאז אסון הצונמי ביפן אנו מזהים מגמה של מעבר לשימוש בהודעות בעלות רוחב פס צר בעת אסון.[56] רשתות חברתיות ואפליקציות כדוגמת "YO" מייצרות כלים חדשים להתנהלות בעת אירוע חירום, תוך אפשור יצירת קשר מבוסס הקשר בהנתן מחסור במשאבי רשת בין פרטים וארגונים .

האירועים המהותיים בארץ ובעולם בשנת 2014

שנת 2014 נפתחה בארץ בהפקת לקחים מתפקוד כלל המערכות בסופה "אלקסה", שניתקה את ירושלים מעורקי החיים שלה למשך כמה ימים.[57] בהמשך השנה נעלם מטוס נוסעים, ובסופה התרסק מטוס נוסעים וסופת ענק שטפה את הפיליפינים. בשנה זו נעשה שימוש ברשת להפצת שנאה ורשע מחד גיסא, ומאידך גיסא הפכה הרשת למקום שבו מאמצים שיתופיים יוצרים קהילות פונקציונליות המתגייסות ומסייעות באירועי חירום בהיקפים שלא נראו כמותם עד כה.

המטוס המלזי – טיסה MA370 של חברת מלזיה איירליינס – התרסק במרץ 2014 בנסיבות תמוהות. המקרה עורר אפקט תקשורתי גלובלי. שעות אחדות לאחר היעלמותו המסתורית הודיעה החברה המלזית רשמית על אבדן קשר עם המטוס.[58] יום אחרי ההיעלמות הוציאה חברת Digital Globe[59] משימת צילום לוויינית לכל האזורים שבהם

55 עוד על האפליקציה: /http://techcrunch.com/2014/08/12/yo-grows-up (אוחזר בתאריך 15 לינואר).

56 מיד לאחר האסון נדחו שמונים אחוז משיחות הקול על ידי ספקיות התקשורת כדי לשמור על הרשת מנפילות עקב עומסי יתר. על נושא זה אפשר לקרוא בהרחבה בפרסום של הסדנה מכנס מס' 93 של סדנת יובל נאמן: "30 שנה לסוכנות החלל הישראלית – שימושים אזרחיים בחלל".

57 על ההשפעות רחבות ההיקף של הסופה במזרח התיכון אפשר לקרוא בכתבה זו: http://www.reuters.com/article/2013/12/13/syria-crisis-alexa-idUSL6N0JS1BE20131213

58 http://abcnews.go.com/International/malaysia-airlines-flight-missing-en-route-china/story?id=22827892

59 חברת צילום לווייני אזרחית אמריקנית, המספקת צילומי לוויין לגופים אזרחיים בהפרדה מרחבית של פחות ממטר. בין לקוחותיה חברת גוגל ופלטפורמת Google Maps.

אמור היה המטוס להימצא. תמונות הלוויין הועלו לפלטפורמת מיקור המונים בשם Tomnod. פלטפורמה זו פותחה על ידי היזם הישראלי שי הר נוי, ו-Digital Globe רכשה אותה בשנת 2013.[60] הפלטפורמה מאפשרת למשתמשים לצפות בצילומי לוויין ברזולוציה גבוהה, זאת כאשר הצופה אינו יודע מהו מיקומה הגיאוגרפי של התמונה כדי למנוע ניצול לרעה של הפלטפורמה. המשתמשים סורקים את צילומי הלוויין תוך שהם נדרשים לסמן במערכת אם זיהו כתמי שמן, שברים של מטוס, סירות מתנפחות או כל דבר אחר. על בסיס מיקור המונים, המערכת מייצרת אזורי עניין שבהם מצאו משתמשים רבים ממצאים חריגים, ומעבירה אותם למומחי פיענוח. תרומת ההמונים באירוע זה הייתה משמעותית: יותר מ-115,000 מתנדבים הצטרפו למאמצי האיתור בשעות הראשונות להעלאת המערכת. מאה מיליון דפי לוויין נסקרו, "נוקו" וסומנו בתוך 34 שעות על ידי משתמשים מכל העולם. שני מיליון חיתוכי תמונות לווייניות נסקרו בכל 10 דקות על ידי המתנדבים במערכת. חברת Digital Globe ומפתחי המערכת לא צפו כמות משתמשים כה גדולה במערכת, ולכן לאחר כמה שעות קרס האתר. מלבד השימוש ב-Tomnod, אירוע זה כרך יחדיו כמה רשתות חברתיות: משתמשי הרשתות החברתיות Redit,[61] טוויטר ו-CNN iReport[62] השתתפו בפיענוח התעלומה. משתמש CNN iReport מרק סרבר ניתח את אחת התמונות שבה הוא מצא, לטענתו, חלקי מטוס והעלה את הניתוח למערכת. דיווח ה-iReport שלו מדורג שמיני בפופולריות שלו בסי-אן-אן בכל הזמנים.[63]

הסופה הטרופית בפיליפינים Hagupit (Rubi) Typhoon

הסופה הטרופית "האגופיט", או בשמה המקומי "רובי", פגעה באזור הפיליפינים ב-4 בדצמבר 2014. ב-6 בדצמבר חדרה הסופה לתוך האי Eastern Samar באזור, עם עצמת רוח מרבית של 210 קמ"ש, מלווה בגשמים ובשיטפונות. ב-10 בדצמבר עזבה הסופה את אזור הפיליפינים תוך שהיא מותירה אחריה נזקים כבדים.[64]

הכנותיה של ממשלת הפיליפינים לקראת הסופה היו רחבות מאוד וכללו היערכות משמעותית בתחום הרשתות החברתיות, תוך הכנה ויידוע הציבור בכלי המדיה החברתית הזמינים לאוכלוסייה.[65] ממשלת הפיליפינים בנתה פורטל אינטרנטי באתר הממשלתי

60 קריאה נוספת על הרכישה: http://www.digitalglobeblog.com/2013/04/08/tomnod/
61 Redit היא רשת חברתית שמאפשרת לאנשים להיות כתבים ולדווח על אירועים בעצמם.
62 CNN iReport היא פלטפורמה להעלאה ולדירוג של תכנים חדשותיים על ידי משתמשים; כתבה שמדורגת על ידי הקהל מתפרסמת באתר של סי-אן-אן.
63 עוד על הוויראליות של מאמצי האיתור בכתבה זו: http://edition.cnn.com/2014/03/12/us/malaysia-airlines-plane-crowdsourcing-search/ (אוחזר ב-15 בינואר 2015).
64 http://www.gov.ph/crisis-response/typhoon-ruby/ צוטט בתאריך 15 ינואר 2015
65 http://www.gmanetwork.com/news/story/391145/news/nation/typhoon-ruby-hagupit-person-finder-and-crisis-map צוטט בתאריך 15 בינואר 2015.

וכן יידעה את כלי המדיה ואת אתרי החדשות והפורומים בכלים העומדים לרשות האוכלוסייה. הממשלה השתמשה בשבעה hashtags שונים לשם הכוונת האוכלוסייה ומעקב אחרי דיווחים בטוויטר, וביקשה מהמשתמשים לסווג הודעות.[66] מערכת Google Person Finder הופעלה עוד לפני הסופה[67] כדי לאפשר לאנשים להודיע על מצבם ולחפש פרטים על קרוביהם. צוותי גוגל בפיליפינים פתחו טרם הסופה עמוד להודעות חירום (public alert page) וכן "מפת אסון" (crisis map), שאפשרו לאוכלוסייה להתעדכן במצב הסופה בכל רגע. ההכנה המדוקדקת כללה גם שימוש בערוץ יוטיוב כדי לשתף את הציבור בתמונות של האזורים שנפגעו ושל מאמצי השיקום.

כמה מהמובילות בתחום אפליקציות מיקור המונים המבוססות על מיקום הן ישראליות. אפליקציות ניווט כגון Waze נמצאות בשימוש של אחוז ניכר מן האוכלוסייה. הישראלים נוטים לאמץ אפליקציות חברתיות, אך הפוטנציאל הטמון בהן אינו ממומש במלואו בהקשר של ניהול מצבי חירום ובקשר שבין המשתמשים באפליקציות ובין הגורמים המכווינים את האוכלוסייה בעת אירוע חירום.

דוגמה לחוסר התיאום אפשר היה לראות במהלך הסופה אלקסה בדצמבר 2013, שפגעה בכל המזרח התיכון תוך שהיא מורידה כמות גדולה מאוד של משקעים. הסופה זכורה במיוחד בארץ בשל חסימת הגישה לירושלים ושיתוק החיים בה למשך ימים אחדים.
מערכת הניווט Waze היא מערכת המבוססת על מיקור המונים. בינואר 2013, באירוע שבו הוצפו נתיבי איילון, חוותה החברה תקלה חמורה.[68] התקלה אירעה עקב ריבוי המשתמשים במערכת. כיוון שלפי שרתי מערכת Waze לא הייתה בנתיבים המוצפים תנועת רכבים, הופנו כל הנהגים באזור לנתיבי איילון. כתוצאה מן ההפניות המרובות וחסימת הנתיבים נוצרו פקקים אדירים בכל גוש דן. אירוע זה היה אירוע מכונן, ובעטיו הוסיפו מפתחי המערכת אפשרות למקם מחסום (Roadblock). אפשרות מערכת זו מבוססת על מיקור המונים המגובה על ידי מפעיל המערכת. מיקום המחסומים הופעל בהצלחה ביום העצמאות באותה שנה.

כאשר החלה הסופה אלקסה, נחסמו עשרות כבישים על ידי משתמשי המערכת באמצעות מיקור המונים. במקביל, מקבלי ההחלטות – רשות חירום לאומית, המשטרה והצבא –

---

66 RubyPH (Storm Coverage) ; #ReliefPH (For aid and relief efforts);#RescuePH# (For those in need of rescue) ; #SafeNow (For resolved #RescuePH tweets); #FloodPH (To report floods); #TracingPH (To report missing people); #WalangPasok (To report no classes).

67 עמוד הנחיתה של מערכת Google Personfinder http://google.org/personfinder/2014-hagupit/

68 עוד על התקלה במערכת Waze אפשר לקרוא בכתבה:
http://www.calcalist.co.il/internet/articles/0,7340,L-3592477,00.html

הודיעו בערוצי התקשורת כי כל הדרכים לירושלים חסומות. באותו בוקר ערכנו ניסוי מבוקר באמצעות מערכת Waze. ביקשנו מהמערכת לקבוע לנו ציר ניווט מתל-אביב לירושלים, שכל הדרכים אליה היו חסומות באותה עת. המערכת מצאה בעבורנו נתיב שדרכו אפשר היה לכאורה להגיע לירושלים בתוך שעה ועשר דקות. בפועל כל הדרכים היו חסומות, אך הנתיב שבחרה המערכת כלל כנראה כביש שמשתמשי המערכת לא נסעו בו והוא לא דווח כחסום. במדינה שבה יותר ממיליון משתמשים במערכת, היה צפוי כי יתקיים קשר בין מפעילי המערכת ובין הרשויות, ובעת אירוע חירום מסוג זה ייחסמו כל הדרכים. כמו כן, ראוי שיינתן כלי לנהגים התקועים בדרכים להזעיק חילוץ כחלק מתכונות המערכת, דבר שבפועל לא קרה.

לסיכום, הכלים שבהם קהילות משתמשות יום-יום לתקשורת יהיו הכלים שבהם הן יתקשרו בעת חירום. בעִתות חירום, כאשר המשאבים נמצאים במחסור, חשיבותן של רשתות חברתיות תגבר וערכן יעלה. פחות דרכים פנויות ופחות אמצעים לחלוקה דורשים יותר שיתוף ויותר סולידריות, ובכך מצטיינות רשתות חברתיות בכלל ורשתות חברתיות מבוססות מיקום בפרט.

בשנת 2014 ראינו שקהילות בעת מצוקה מייצרות לעצמן פתרונות הן ברמת התשתית והן ברמת האפליקציה, כדי לשמור על הקהילה ועל חוסנה. אנו צופים התחזקות של מגמה זו ומצפים שיתבצעו חיבור או אינטגרציה בין הרשתות לבין מקבלי החלטות וקהילת המשתמשים, גם כדי לאפשר לקהילה להגביר את חוסנה וגם כאמצעי אלטרנטיבי יעיל וזול להעברת הנחיות.

7. ליאור טבנסקי: The Current State of Cyber Warfare

Abstract

The article sets the stage for discussion of cyber warfare with concise definitions of the main concepts, followed by descriptions of new risks and current responses. Furthermore, some of the major controversies in the cyber war debate are presented and critically discussed. We conclude that cyber security is in dire need of interdisciplinary scholarship that would promote an informed debate and responses through a democratic decision making process.

Setting the stage

Cyberspace, a domain created not by nature but by human beings, has emerged to provide tremendous benefits, but also to present new risks. Recently, cyber security has become a national policy issue. Driven predominantly by national security concerns, democracies have formulated national cyber strategies.

Consistent definitions are essential. Cyberspace refers to inter-connected information technology infrastructures comprised of computers, computer embedded systems, telecommunication networks, the Internet and the WWW, including the information transmitted and processed within these systems. The public Internet is only one part of cyberspace. Other parts include mission-specific systems that vary widely in size and complexity and control the function of various obscure processes; these control functions gradually become computerized. The term "cyber", derived from Greek, refers to the control element.

For over two decades we have been hearing: "Cyberwar is coming!" In a way unsurprising to scholars familiar with the Realist theory of international relations, the idea of cyber war emerged alongside cyberspace conceptualization and then its realization. History and philosophy show that scientific developments do not alter human nature enough to eradicate violent conflict. While the potential for using cyberspace in a conflict is obvious, the currently prevailing properties of cyberspace make fundamental concepts of attack, defense, and ultimately war inadequate. However, even experienced defense and IT professionals all too often confuse acts of cyber crime and espionage with cyber attacks. Failing to conceptualize what cyber warfare is and, more importantly, what it is not, skews perception and results in faulty policy-making.

We now turn to a critical examination of the major issues in the cyber war debate. We will discuss the significance of threats, the adequacy of the cyber war metaphor, the promise and problems of emergent responses and the securitization critique. Finally, we outline an approach for the future.

Risks and materialization

Technologically identical methods are used to gain unauthorized access to computer resources for most cyber operations, regardless of the intended purpose: crime, terrorism, industrial espionage, military espionage, or warfare. Indeed, novel cyber attacks on critical national infrastructure are likely to severely disrupt social activities if successful. It has become theoretically possible to exploit the properties of today's cyberspace to attack strategic targets remotely. Furthermore, the attacker risks significantly less in cyber space due to the widespread use of vulnerable commercial off-the-shelf technologies, the difficulty of distinguishing a glitch from malicious action, and the challenges of identifying the attackers.

The discovery of "Stuxnet" was the major driver for national cyber security. The threshold leading from cyber exploitation (espionage and criminal data theft) to physically-destructive and politically-motivated cyber attack was crossed in a spectacular manner. It remains the only known manifestation of a novel phenomenon: successful exploitation of cyberspace to target the control a layer of a complex industrial process in order to achieve a destructive goal, all while avoiding military confrontation.

"Cyber War"?

As noted above, the unique properties of information and cyberspace make some of the familiar concepts inadequate. This paradoxical state of affairs testifies to the fundamental novelty of cyberspace that renders even millennia-old concepts unsatisfactory. Stuxnet demonstrated just how sophisticated and precise cyber-weapons could be, but to evaluate all cyber weapons' strategic effectiveness according to this specific case assumes a too narrow perspective. But website defacement, distributed denial-of-service (DDoS), massive cyber espionage -

all are labelled "attacks"; some espionage operations are often upgraded to the "advanced persistent threat" status, and the whole scene is called "cyber war". War is a central experience of mankind that always had gruesome properties. "War is an act of force to compel the enemy to do our will;" it consists of several universal elements, famously formulated by Clausewitz. Centrally, war is a violent act, where a threat of force and violence are instrumental to achieve a political goal. None of the denial of service, web hacking, espionage are even potentially violent; even when Stuxnet is considered - no cyber incident has yet been violent nor caused the loss of human life. Since none of the cyber events have yet met the requirements to constitute a war, we should relinquish the "cyber war" metaphor, at least for the time being.

National interventions in cyberspace

The proponents of the Internet as a self-organizing global commons met national security strategies as well as the accompanying regulations and surveillance with disapproval. Yet, perhaps unsurprisingly, reliable evidence shows that the global commons ideal shunning state-led interventions is very remote from reality. Even liberal democracies employ domestic measures, such as content filtering and persistent surveillance for national policy ends, while confronting some opposition on legal, civil liberty and privacy grounds. The recent official national cyber strategies in developed democracies demonstrate a retreat from the long-term libertarian ideology that originally had shaped Internet policy,

The idea of the Internet delimited into national sovereign networks was disdained in the West: pundits labeling this scenario with the unambiguously negative term "balkanization". However, the trend of national intervention in cyber is inevitable: once the crucial importance of cyberspace is acknowledged, no state can stay away from trying to assert cyber power. A constructive debate should focus on the decision-making process and the character of actions selected by national governments, instead of decrying the loss of an ideal.

Militarization of cyberspace: meanings and outcomes

Developed states have recognized the inadequacy of a laissez-faire approach to

cyber, but only after repeated cyber breaches increased the perceived insecurity, national cyber security policies became politically feasible. Analyzing the national responses to cyber security challenges reveals a pronounced trend towards concentration of capacity in defense and intelligence circles. The accompanying over-classification of the decision-making process regarding the means, goals, strategies and activities severely stifles the public voice, increasing the conflict with the citizens' civil liberties. The severe suppression of the public participation in the unfolding policy debate is anti-democratic. In practice, over-classification will be counter-productive. Cyber security is one of the pronounced cases of multi-stakeholder governance where a subordination of all its facets to the national security establishment's perspective cannot provide a net-benefit outcome.

However acknowledging this problem does not necessarily lead to the securitization interpretation to which the critical security studies scholars adhere. For the "Copenhagen School", securitization is an extreme version of politicization that enables the use of extraordinary means in the name of security. But what if the strategic environment has undergone such a technology-driven change that means previously considered extraordinary become vital? The vulnerabilities of cyberspace can be attributed to a protracted market failure of the IT industry. The business sector is justly recognized as essential for many facets of cyber security - but the sector cannot go it alone. It also should not: just as we do not expect citizens or companies to defend from air-to-surface missiles by themselves, we cannot reasonably expect cyber security without a national security effort.

The defense apparatus has an indispensable role to play in national cyber security and resilience, but it should be closer controlled by democratic mechanisms.

Cyber security: from a technical-military to a democratic approach

We cannot afford blissful ignorance regarding our changing environment. This essay started with a brief conceptualization of the central phenomena, and then critically assessed three major issues in the cyber debate. These points are stressed. The new risks and threats are real, making cyber security necessary. We as

individuals, as well as societies, cannot go on unprotected. "Cyber War", however, appears to be an inappropriate analogy.

The ideal of cyberspace as a global commons has been mostly forsaken. A significant national intervention in cyberspace, including the Web, is inevitable. Yet this in itself is not a negative phenomenon.

The concentration of power in the defense establishment is detrimental to cyber power because of the accompanying damage to civil liberties, the democratic process and long-term effectiveness. The national cyber strategies, as well as the practice of liberal democracies have indeed come into conflict with civil liberties. This does not necessarily have to be the case. However, adopting the securitization perspective is not the appropriate way towards balancing the values for societal resilience.

Cyber security is not simply a clear-cut technical issue. It is a strategic, political, and social phenomenon with all the accompanying messy nuances. Therefore cyber reality must be examined with a scientific rigor by all disciplines, enabling an informed public debate. It is both morally essential and rationally effective for the responses to be formulated through a democratic process.

8. יונדב פרי: היכן עובר הגבול בין פשיעת סייבר ובין לוחמת סייבר

בעשור האחרון, רשת האינטרנט היא אחד ממחוללי השינוי הבולטים בעולם. ככל הנראה תרמה הרשת להשתנות החברה האנושית בתקופה כה קצרה אף יותר ממהפכת הדפוס ומהמהפכה התעשייתית. בין היתר, הפכה הרשת גם כלי עיקרי לפשיעה כלכלית (פשיעת סייבר), וגורם דומיננטי בעימותים בין מדינות ובעימותים בין ארגוני טרור למדינות (לוחמת סייבר).

כאן עולה תופעה חשובה במדינות העולם המפותח – בעשור האחרון הפכה רשת האינטרנט לאחת התשתיות החיוניות במדינה, בדומה לרשתות החשמל, המים, התחבורה והתקשורת. שיבוש או הפסקה בפעולת הרשת יגרמו להשבתה כמעט מוחלטת של הפעילות הפיננסית, המסחר הקמעוני והסיטוני, שירותי התעופה והתקשורת הסדירה בין הממשל לתושבים. כשם שמדינה משקיעה מאמצים ומשאבים רבים כדי להגן על רשת החשמל מפני פגיעות עוינות, כך עליה לעשות גם בהגנה על תשתיות האינטרנט ובהבטחת שרידותה של הרשת במצבים של תקיפה עוינת, אסונות טבע וכדומה.

המתקפה על חברת סוני בארצות הברית בסוף 2014 היא עליית מדרגה משמעותית בשימושים העוינים באינטרנט. פורצים עלומים חדרו באמצעות האינטרנט למחשבי חברת סוני, ומשכו מהם כמות אדירה (כ-100 טרה-בייט) של מסמכים ושל תכתובות פנימיות של החברה, וכן כמה סרטים שעדיין לא פורסמו. חלק מאותם מסמכים וסרטים פורסם ברשת וגרם מבוכה רבה לסוני. הפורצים מחקו גם חומר רב ממחשבי החברה, וגרמו להשבתת מערכות המידע שלה למשך כשבועיים. בכך אין חידוש רב – מאז קיום הרשת היא משמשת גם לפריצה למחשבים, ומיליוני מחשבים כבר נפרצו באמצעותה בעבר. החידוש הוא בהיבטים הנוספים של האירוע. ראשית, הרקע לפריצה הוא כוונתה של סוני להפיץ סרט חדש – "ריאיון סוף", המתאר התנקשות בחייו של שליט צפון קוריאה. במקביל לפריצה, פרסמה צפון קוריאה התראות לחברת סוני לבל תפיץ את הסרט, והדבר העלה חשדות רבים כי הממשל הצפון קוריאני הוא שעומד מאחורי הפריצה. יש לציין כי מושמעות גם טענות אחרות, למשל שהתקיפה בוצעה על ידי עובדת ממורמרת שפוטרה. תחילה נכנעה סוני לאיומים והודיעה כי היא מבטלת את הפצת הסרט, אך לאחר מכן חזרה בה והחלה בהפצה. באותו זמן אירעו תקיפות כבדות על תשתיות האינטרנט של צפון קוריאה, שהביאו לניתוקה המוחלט מהרשת לימים אחדים. תוך כדי האירועים החלו ארצות הברית וצפון קוריאה לפרסם התראות זו לזו כי הן שומרות לעצמן את הזכות להגיב על התקיפות בזמן ובאופן שייראה להן לנכון.

כאן מתבררת שוב תכונה חשובה וידועה של הפעילות העוינת ברשת – "בעיית הייחוס", חוסר האפשרות לזהות בוודאות את הגורם התוקף. עד כה לא הצליחה ארצות הברית

להראות בוודאות כי צפון קוריאה היא שתקפה את סוני, ובמקביל לא הצליחה צפון קוריאה להראות כי ארצות הברית היא שהשביתה את האינטרנט במדינה. המצב הוא אפוא תיקו של "סבירות גבוהה" ששתי המדינות אכן תקפו זו את זו. (בעיתונות הישראלית פורסם כי "גורמים ישראלים המצויים בפרטי החקירה מעריכים כי קוריאה הצפונית אכן עומדת מאחורי ההתקפה, וכי יש דמיון רב בין מאפייני התקיפה ובין התקפה על חברת הנפט הסעודית אראמקו בעבר".)

בהנחה כי זוהי בקירוב האמת, אנו רואים לראשונה אירוע שבו מדינה (צפון קוריאה) תוקפת חברה עסקית (סוני) במדינה אחרת. עד כה מקובל היה להבחין בין לוחמת סייבר, שהצדדים בה הם מדינות וארגוני טרור, לבין פשיעת סייבר, שהצדדים בה הם ארגוני פשע וגופים כלכליים. לוחמת הסייבר מיועדת לגרום נזקים ליריב, ואילו פשיעת סייבר מיועדת להביא רווח כלכלי לתוקף. כאן נשברו הכללים. לפנינו מדינה התוקפת חברה עסקית, כדי להביא לתוצאות מסוג אחר – הרתעה והפחדה במטרה למנוע פגיעה תדמיתית בראש המדינה. מעבר לכך, הנה מדינה (ארצות הברית) היוצאת לפעולה התקפית על מדינה אחרת כתגמול (והרתעה לעתיד) על גניבת מסמכים מחברה עסקית.
התקיפה על צפון קוריאה השביתה אמנם את האינטרנט במדינה, אך דווקא במדינה זו היו לכך השלכות מעטות. מעריכים כי רק לחמישה אחוזים מתושבי צפון קוריאה יש גישה לאינטרנט, ועל כן הנזק, אם אכן היה, הוא מזערי. עם זאת, זוהי קריאת אזהרה למדינות המפותחות. אילו היה גורם עוין מצליח להשבית את האינטרנט בישראל (היו בעבר ניסיונות לעשות זאת על ידי פגיעה במערכת ה-DNS), היה הדבר משתק כמעט כליל את הפעילות הכלכלית והעסקית ופעילויות נוספות רבות במדינה. הזכרנו כבר כי רשת האינטרנט היא אחת התשתיות החיוניות במדינה, בדומה לרשתות החשמל, המים, התחבורה והתקשורת הטלפונית. ידועה תקיפה על תשתיות האינטרנט באסטוניה, שהתרחשה בשנת 2007 ושיתקה את הכלכלה במדינה למשך יותר משבוע. אז הכריזה נאט"ו כי אינה רואה במתקפה "וירטואלית" מעין זו פעולת לוחמה המצדיקה תגובה צבאית.

במהלך שנת 2014 התפרסמו פרטיהן של תקיפות אינטרנט רבות על מחשבי חברות עסקיות בארצות הברית, בעיקר רשתות קמעוניות גדולות, שבהן השיגו התוקפים (שנותרו עלומים) פרטים אישיים, כולל פרטי כרטיסי אשראי ומספרי זיהוי של מאות מיליוני אזרחים. בעניין זה ראוי לציין שבשנת 2011 נפרצו מחשבי חברת סוני והפורצים גנבו פרטים אישיים של כ-100 מיליון משתמשי פלייסטיישן. נשאלת השאלה – אם התקיפה הנוכחית על סוני נחשבת לפעילות התקפית עוינת ברמה הלאומית, האם זהו גם דינן של התקיפות על הרשתות הקמעוניות? הרי בשני המקרים מדובר בגניבת מסמכים, וכל ההבדל הוא באופי המסמכים שנגנבו, ובשיוכם (שאינו ודאי) של התוקפים לשלטונות מדינה זרה.

כאן עולה שאלה נוספת – מה הם גבולות התשתית החיונית? האם על חברות לצפות כי המדינה תהיה האחראית הבלעדית או העיקרית ליישום אמצעי הגנה מפני חדירה למחשביהן? לחילופין, האם על המדינה לצפות כי כל חברה וארגון במדינה ישקיעו סכומי עתק וכוח אדם מקצועי רב כדי להגן על עצמם בעולם שבו כל הגבולות פרוצים? האם המדינה אמורה להרשות ולעודד פעילות של "תקיפות נגד" – של החברות המותקפות על הארגונים ועל המדינות שמהם בוצעה התקיפה?

טשטוש הגבולות ועירוב התחומים בין פשיעה ללוחמה הם רק אחד המאפיינים של עולם הסייבר בשנה האחרונה. היבטים נוספים הם המעבר הכמעט מלא של פעילויות הפשע ברשת מתקיפות שמבצעים בודדים לתקיפות שמבצעים ארגוני פשיעה, אשר לרשותם עומדים אמצעים כלכליים רבים וכוח אדם מיומן. כך נגרמה עליית מדרגה במידת התחכום של התקיפות וברמה המקצועית הגבוהה של כלי התקיפה (תוכנות זדוניות, או APT[69]). עם זאת, מרבית התקיפות שזכו לפרסום התחילו בהונאה פשוטה – תקיפת "פישינג" ממוקדת (spear phishing) על יחידים בארגון הנתקף. בתקיפת פישינג מנסה התוקף להונות את האדם שאליו נשלחת הודעת דוא"ל, כך שיתפתה לפתוח קובץ מצורף או להפעיל לינק לאתר כלשהו. בצעד זה משיגים התוקפים את דריסת הרגל הראשונה ברשת של החברה הנתקפת, כדי להחדיר לתוכה כלי APT מתוחכמים ומוסתרים היטב. ניתוחים סטטיסטיים מראים כי במרבית הארגונים שהותקפו פעל APT במחשבי הארגון הנתקף במשך כמה חדשים עד שנתגלה לראשונה. לדעתי, במרבית המדינות לא נערכות הדרכות והנחיות מספקות לעובדים המשתמשים במחשב בדבר הדרכים והאמצעים שיש לנקוט כדי להימנע מלהיות קרבן לתקיפות פישינג.

החקיקה הלאומית והבין-לאומית אינה עומדת בקצב ההתקדמות הטכנולוגית של שיטות הפשיעה והלוחמה ברשת, ועל כן במקרים רבים גם אם זוהו התוקפים לא ניתן להרשיעם בדין על מעשיהם. בחסות ארגון נאט"ו, פורסם בשנת 2013 "מדריך טאלין למלחמת סייבר", המהווה מאמץ ראשון לרכז את כללי המשפט הבין-לאומי הרלוונטי לפעילות עוינת ברשת בין מדינות. עם זאת, החסר רב מן הקיים בתחום זה.

69 advanced persistent threat – APT

9. רועי צזנה: הרחפנים מגיעים

על מה אתם חושבים כשאתם קוראים את המילים "כלי טיס"?

על פי רוב, מיד עולה בדמיונכם תמונה של מטוס גדול הנושא מאות נוסעים ליעדיהם. או אולי מסוק הסוקר את התנועה בכבישים. אם אתם עוסקים בביטחון, אולי אתם חושבים על כלי טיס לא-מאוישים, מהסוג שבו השתמשו במלחמותיה של ארצות הברית בעיראק ובאפגניסטן בעשור האחרון: כלים כמו הפְּרֶדטור ששוקל יותר מטון, נושא טילי הלפָיֵיר נגד טנקים וטילי סטינגר נגד מטוסים ומופעל מרחוק על ידי טייס מיומן.

נראה, אם כן, שאינכם חושבים על רחפנים: כלי טיס במשקל של פחות מחמישה קילוגרמים, עם מערך משוכלל של חיישנים ואמצעי בקרה עצמית שמאפשרים לכל אזרח מן השורה להטיס אותם אחרי אימון קצר. הרחפנים נכנסו לשימוש בקרב הציבור רק בשלוש השנים האחרונות, אבל כבר בשנת 2014 הם התחילו לשנות את כל התפיסות הקיימות, מכיוון שאלו הם כלי הטיס של כולם: בשנה האחרונה החלו ראשי עיריות להשתמש בהם,[70] משטרת ישראל מנצלת אותם לסיורים אוויריים בירושלים,[71] ואפילו ילדים משתמשים בהם להנאתם.

העולם העסקי גילה לאחרונה שרחפנים הם השקעה נפלאה בהווה ולעתיד. לפי דו"ח שהפיצה חברת "מחקר וינטרגרין" בתחילת 2015, שוק כלי הטיס הלא-מאוישים בארצות הברית עמד בשנת 2014 על 609 מיליון דולרים, וצפוי להגיע ל-4.8 מיליארד דולרים עד 2021.[72] הרחפנים צפויים להשתלב כמעט בכל שוק ותחום: הם יישאו משאות בעבור אמזון וחברות משלוחים אחרות, יפקחו אחר גידולים חקלאיים בשדות, ינטרו צינורות גז ונפט, ישמשו חיישנים ניידים לזיהום אוויר ויספקו לנו תמונות "סלפי" מרשימות מן האוויר. כן, גם פושעים ישתמשו בהם, והם כבר משתמשים בהם היום.[73]

70 חסון, נ', "מזל"ט מאבטח את הרכבת הקלה בירושלים," הארץ, 21 ביולי, 2014. Available: http://www.haaretz.co.il/news/local/1.2382848 [Accessed 1 15 2015]

71 משטרת לואי דה-פינס, "משטרת פתח-תקווה השתמשה ברחפנים של עיריית פ"ת לצרכי איתור פעילות חשודה," משטרת לואי דה-פינס, 1 בנובמבר, 2014. Available: http://bit.ly/1LQbegN

72 ReportsnReports, "Commercial Drones Market: Unmanned Aerial Systems (UAS) 2015 - 2021 Forecast and Analysis," ReportsnReports, 1 2015. Available: http://www.reportsnreports.com/reports/323186-commercial-drones-highways-in-the-sky-unmanned-aerial-systems-uas-market-shares-strategies-and-forecasts-worldwide-2015-to-2021.html. [Accessed 15 1 2015]

73 I. Hughes, "Criminals 'using flying drones fitted with heat-seeking cameras' to spot and raid cannabis farms," Mirror, 21 4 2014. Available: http://www.mirror.co.uk/news/uk-news/criminals-using-flying-drones-fitted-3438207.[Accessed 15 1 2015].

נסיקתם של הרחפנים בדומה לטכנולוגיות מערערות רבות, מעטים צפו מראש את התפתחותם המהירה של הרחפנים. "הרחפנים לא היו עד לפני שלוש שנים. פתאום זה פרץ, ואנחנו מנסים להתאים את הרגולציה", אמר בני דוידור, מנהל מחלקת מערכי כלי טיס בלתי מאוישים (כטב"ם) אזרחיים ברשות התעופה האזרחית (רת"א), לקראת סוף 2014. דוידור משקף בדבריו את תסכולם של הרגולטורים, שנאלצים להתמודד עם סוגיית הרחפנים ולהבין מה הכללים החלים עליהם.[74] אך מדוע לא חזה איש מראש את הגעתם של הרחפנים לשוק?

כפי הנראה, הסיבה היא שהרחפנים הגיעו לכדי מימוש בזכות טכנולוגיות אחדות שהתפתחו במהירות באותה העת, ושילובן יחד באותו כלי יצר ישות חדשה הגדולה יותר מסכום חלקיה.

מקים אוניברסיטת הסינגולריות, פיטר דיאמנדיס, תיאר לאחרונה ארבעה כיווני התפתחות טכנולוגיים מקבילים שאפשרו את פריצתם המהירה של הרחפנים:[75]
התפתחות טכנולוגיית הניווט הלווייני והמַקלֵטים: תוך שלושים שנה, ירדה עלות המקלטים פי עשרת אלפים ממחירה המקורי, ומשקלם צנח פי מאה אלף. משקלם של המקלטים כיום הוא פחות מגרם אחד, ועלותם מגיעה לפחות מחמישה דולרים.

התפתחות מערכות לבקרה עצמית: יחידות לאומדן תאוצה ומנח גוף הרחפן עלו בעבר מיליוני דולרים. כיום הן זמינות בעלות של דולר.

מצלמות דיגיטליות: המצלמות הדיגיטליות כיום זולות פי מאה וקטנות פי אלף מהמצלמות הדיגיטליות הראשונות שפיתחה חברת קודאק.

אמצעי תקשורת אלחוטיים: שיפורים עצומים ביכולת העברת מידע בין מכשירי קצה הביאו לכך שכל אדם יכול כיום לשלוט ברחפן באמצעות הטלפון החכם.
מעניין לציין שאותן מגמות התפתחות טכנולוגיות הביאו גם ליצירתם של הטלפונים החכמים, שמעלים אתגרים דומים לאלו שבפניהם ניצבים הרחפנים היום. בעיקר משותפת לשני תוצרים טכנולוגיים אלו הדילמה המתמדת בין הכוח שניתן לכל אזרח לבין הצורך בהגנה על אחרים מפני פלישה לפרטיותם.

74 דומבה, ע' ר', "רגולציה בעידן הרחפנים," 7 באוקטובר, 2014. Available:http://bit.ly/1NpeKjn

75 C. Anderson, "Peter Diamandis on the future of drones," DIY Drones, 10 8 2014. Available: http://diydrones.com/profiles/blogs/peter-diamondis-on-the-future-of-drones[Accessed 15 1 2015]

פרטיות והשגחה עליונה

"ברגע שאיבדת את פרטיותך, אתה מבין שאיבדת דבר יקר ערך עד מאוד." -בילי גרהאם
בשנת 1985 קיבלה משטרת סנטה קרוז הודעה אנונימית שדנטה סיראולו, תושב קליפורניה, מגדל מריחואנה בחצרו כשהיא מוסתרת מעין הציבור מאחורי שתי גדרות. המשטרה לא הצליחה לקבל צו חיפוש בקלות, אך היא עשתה מעשה: שוטרים עלו על מטוס פרטי ובחנו את החצר מרום של שלוש מאות מטרים. על סמך הראיות המחשידות שראו, הוצא צו חיפוש בבית – והצמחים המפלילים אכן התגלו.

סיראולו טען כי למשטרה לא הייתה זכות לפלוש לפרטיותו מן האוויר, אך בית המשפט שלל את הטיעון ונימק שלכל שוטר יש זכות לטוס באוויר ולצפות במתרחש על האדמה. אפשר בהחלט לערער על הרציונל של בית המשפט (וסיראולו אכן עשה זאת לאחר מכן בבית המשפט לערעורים וזוכה), אך נימוקי הנגד של השופטים היו מעניינים יותר. השופט פאוול ייצג את דעת המיעוט (ארבעה שופטים לעומת חמישה) וכתב כי לסיראולו הייתה זכות לצפות לכך שפרטיותו תישמר גם מן השמים, מכיוון ש"הסיכון לפגיעה ממשית בפרטיות ממטוסים מסחריים או פרטיים כמעט אינו קיים... הסכנה שנוסע במטוס כזה יבחין בפעילויות פרטיות ויקשר אותן לאנשים מסוימים היא פשוט טריוויאלית מכדי שנגן מפניה."[76]

פאוול צדק בדבריו בשנת 1985, כאשר העלאת מטוס או מסוק לאוויר הייתה מטלה מורכבת ומסובכת, שחייבה השקעת משאבים מרובים ואימון בתפעול כלי טיס. היום, הזנקת רחפן לאוויר ושימוש בו כדי לצלם את חצרו של אדם פרטי הפכה להיות טריוויאלית ביותר. במצב עניינים זה, אין פלא שגופי שיטור בעולם בוחנים כיצד להשתמש ברחפנים כדי לאסוף נתונים על פושעים פוטנציאליים, ועורכי דין ורגולטורים בוחנים את נבכי החוקים כדי להבין מה המגבלות שצריכות הרשויות להטיל על השימוש ברחפנים.

בישראל, בהתאם להיותנו מדינת היי-טק מפותחת מחד גיסא ומדינה בעלת צרכים ביטחוניים מאידך גיסא, אנו רגילים להשתמש בטכנולוגיות מתקדמות להגנה על האזרח – לעתים תוך כדי התעלמות מהחוק הקיים ועקיפתו. בהתאם לכך, משטרת פתח תקווה השתמשה בשני רחפנים (שהיו בבעלות העיריה) כדי לצלם בשנת 2014 אזורים וחפצים ברשות פושעים.[77] בלשים משטרתיים (לכאורה) תועדו משתמשים או מתאמנים בשימוש

76 Legal Information Institute, "California v. Ciraolo," Legal Information Institute, 19 5 1986. Available: http://www.law.cornell.edu/supremecourt/text/476/207.

77 משטרת לואי דה-פינס, "משטרת פתח-תקווה השתמשה ברחפנים של עיריית פ"ת לצרכי איתור פעילות חשודה," משטרת לואי דה-פינס, 1 בנובמבר, 2014. Available http://bit.ly/1LQbegN

ברחפן בהרצליה,[78] ובנובמבר 2014 הודתה דוברת משטרת ישראל כי בכוונת המשטרה לרכוש רחפנים לפעילות מבצעית.[79] זו הייתה הודאה שהגיעה באיחור, מכיוון שהחל ביולי 2014 כבר פטרלו רחפנים בגובה מאה מטרים מעל הרכבת הקלה בירושלים. מפעיליהם אמנם לא היו שוטרים מן המניין אלא עובדים של חברת בלייד וורקס הישראלית, אך אלו שלטו ברחפנים ממקום ישיבתם בתחנת המשטרה בשועפאט.[80]

בצד היתרונות הגדולים והברורים שהרחפנים יכולים לספק לגופי שיטור ואבטחה – חקר אירועי טרור ופשיעה, סיורים שימנעו אירועים עתידיים – אי-אפשר שלא להסכים שהם אכן מהווים איום על הפרטיות. כפי שכתב הסנטור צ׳אק גראסלי בשנת 2013: ״המחשבה על רחפנים ממשלתיים, המזמזמים מעלינו ומנטרים פעילויותיהם של אזרחים שומרי חוק, אינה עולה בקנה אחד עם משמעות החיים בחברה חופשית.״[81] ברור שבשנים הקרובות יידרש המחוקק בישראל להגדיר מהם זכויותיהם של האזרחים לפרטיות, כאשר החדירה לפרטיותם יכולה להגיע מהשמיים בכל רגע. סוגיה סבוכה במיוחד עלולה לנבוע מצילומים אקראיים, מכיוון שהרחפנים מתעדים פעילויות כל העת. האם מוצדק להתעלם, למשל, מהתמונות שצילם רחפן המנטר את התנועה בכבישי העיר, ותוך כדי כך גם תיעד מעשה אלימות? ואם נחליט שניתן להשתמש בתמונות אלו כראיה במשפט, האם אין הצדקה לשלוח רחפנים לסיורים קבועים ברחובות ובכבישים? ומה דינן של תמונות שצולמו – מבלי להתכוון – מבעד לחלון ביתו של אדם במהלך סיור שגרתי כזה, ומתעדות אותו בעיצומה של פעילות פלילית?

אלו הן שאלות תקֵפות. דווקא בעקבות השנה האחרונה, שבה היינו עדים לשימוש ברחפנים על ידי גופים משטרתיים, הן עתידות להיות דחופות ובהולות יותר, ובתי המשפט יאלצו להתמודד עמן במוקדם או במאוחר.

סוגיית הפרטיות נוגעת רק לפן אחד של נושא הרחפנים, ויש שיאמרו שהיא מיטיבה עם הפושעים דווקא, מאחר שהיא מגנה עליהם מפני כוחות השיטור. מנגד – אותם רחפנים עצמם יכולים לשמש גם בידיהם של פושעים למטרות זדון.

78 קנאביס, "הצעצוע החדש של משטרת ישראל: מצלמות מעופפות (וידאו)," קנאביס, 24 במאי, 2014. Available:http://bit.ly/1LxsVUp
79 קנאביס, "המשטרה מודה לראשונה: "בקרוב נפעיל רחפנים בפעילות מבצעית"," קנאביס, 13 בנובמבר, 2014. Available:http://bit.ly/1uIJrcd
80 רועי ינובסקי, "חדש: המזל"ט שישמור על הרכבת הקלה". Mynet, 20 7 2014

Available: http://www.mynet.co.il/articles/0,7340,L-4546313,00.html. [Accessed 15 1 2015]
.B. Sasso, "Senators fear drones 'buzzing overhead'," The Hill, 20 3 2013 81
Available:[http://thehill.com/policy/technology/289337-senators-worry-about-do-
.mestic-drone-surveillance.[Accessed 15 1 2015]

פשיעה וטרור מן השמיים

בשנה האחרונה שלחתי סקר קצר למומחים בתחום הרחפנים, וביקשתי מהם לציין מתי לדעתם יתחילו פושעים אינדיבידואליים וארגוני פשיעה להשתמש בכלי הטיס למטרותיהם. וזוהי התשובה, שאינה משתמעת לשתי פנים: כבר בשנת 2014 אמורה הטכנולוגיה להיות זמינה לגורמי הפשיעה למיניהם.
המציאות תומכת בדעותיהם של המומחים. כמה פעילויות בעלות גוון פלילי שנחשפו בשנת 2014 כוללות:

• כנופיות השתמשו ברחפנים כדי לאתר בניינים המשמשים לגידול מריחואנה ולבזוז אותם. הרחפנים מצוידים במצלמות אינפרה-אדום, המזהות בקלות את חוות המריחואנה העירוניות בשל החום הרב שמפיצים בתוכן האורות לצורך הגידול ההידרופוני.[82]

• קרטלי סמים במקסיקו משתמשים ברחפנים שונים, גם מייצור עצמי, להברחת סמים אל מעבר לגבול בין מקסיקו לארצות הברית. מאז 2012 תועדו כ-150 רחפני סמים שחצו את הגבול כשהם נושאים מטען כולל של שני טון קוקאין וסמים אחרים. הקרטלים במקסיקו שוכרים עובדים מחברות רחפנים קיימות כדי לפתח רחפנים המותאמים במיוחד לשימושיהם.[83]

• רחפן מליטא שימש להברחת סיגריות דרך הגבול עם רוסיה. לפי הדיווחים, מוטת הכנפיים של הרחפן הגיעה לאורך של ארבעה מטרים, והוא נשא מטען סיגריות של 11 קילוגרמים.[84]

• בסוף 2013 ובמשך 2014 דווח כי בתי כלא שונים בקנדה חווים 'מגיפה' של

---

82 I. Hughes, "Criminals 'using flying drones fitted with heat-seeking cameras' to spot and raid cannabis farms," Mirror, 21 4 2014. Available: http://www.mirror.co.uk/news/uk-news/criminals-using-flying-drones-fitted-3438207.[Accessed 15 1 2015].

83 Chivis, "Mexican Cartel Unmanned Aerial Vehicles (Narco Drones)," Borderland Beat, 4 8 2014. Available: http://www.borderlandbeat.com/2014/08/mexican-cartel-unmanned-aerial-vehicles.html.[Accessed 15 1 2015].

84 J. Koebler, "The Lithuanian Mob Was Smuggling Cigarettes Into Russia with a Drone," Motherboard, 16 5 2014. Available: http://motherboard.vice.com/read/the-lithuanian-mob-was-smuggling-cigarettes-into-russia-with-a-drone.] Accessed 15 1 2015].

הברחות סמים מעל החומות, באמצעות רחפנים.[85] התופעה התפשטה גם לבית כלא אחד לפחות בג׳ורג׳יה.[86] בשנה מהדרך הרגילה להברחת סמים – באמצעות אריזתם בכדורי טניס והשלכתם מעל החומות – ברחפנים אפשר לשלוט ממרחק של יותר מקילומטר, ולכן קשה יותר לגלות את המבריח ולעצור אותו.[87]

• באמצע משחק כדורגל טעון בין סרביה לאלבניה, שיגר אחד האוהדים רחפן שנשא דגל בעל מסרים אנטי-סרביים. הרחפן חלף מעל המגרש והלהיט את הרוחות; השוער הסרבי תפס את הדגל והותקף מיד על ידי שני שחקנים אלבניים. הקטטה התפתחה והתגברה במהירות, והאוהדים החלו לזרום מהיציעים כדי לתקוף את השחקנים האלבניים באגרופים ולידות חפצים. המשחק הופסק תוך דקות ספורות ולא התחדש.[88] לא ברור אם אפשר להגדיר את המקרה פשע, אך זוהי דוגמה למצב החדש שבו כל אדם יכול להעלות כלי טיס לאוויר. מפעיל הרחפן טרם נתפס, ומעטים הסיכויים שיתגלה.

שתי תכונותיהם הבולטות של הרחפנים הן יכולתם להגיע ולתצפת על מקומות שהגישה אליהם אמורה להיות מוגבלת, והעובדה שיכולת זו נתונה עתה לכל אדם שרוצה ויכול לרכוש מכשיר כזה. שתי תכונות אלו מתאימות את הרחפנים גם לביצוע מעשי טרור ופיגועים. נכון להיום טרם נחשפו מעשי טרור באמצעות רחפנים, אך מסקירת השימוש ברחפנים על ידי פושעים קשה לפקפק בכך שגם טרוריסטים ינצלו אותם בעתיד הקרוב. ניסיונות לבצע פיגועים באמצעות כלי טיס בלתי-מאוישים תועדו כבר בעבר, כגון ניסיון (שסוכל) לרסק מטוס קטן, לא מאויש אך עמוס בחומרי נפץ, לתוך הפנטגון.[89]

במחקר שהוצג בכנס למערכות לא-מאוישות בשנת 2013, סקרו קלאס ג׳אן דה קראקר ורוב ואן דה וייל את הסכנות הביטחוניות שברחפנים. קראקר ווייל התרשמו במיוחד

85 M.-A. Russon, "Drones Used to Deliver Drugs to Prisoners in Canada," International Business Times, 29 11 2013. Available: http://www.ibtimes.co.uk/drones-delivers-drugs-prison-canada-contraband-inmates-526190. [Accessed 15 1 2015].

86 WALB News, "Crooks get creative to smuggle contraband," WALB News, 23 11 2013. Available: http://www.walb.com/story/24047984/crooks-get-creative-to-smuggle-contraband. [Accessed 15 1 2015].

87 B. Anderson, "How Drones Help Smuggle Drugs Into Prison," Motherboard, 10 3 2014. Available: http://motherboard.vice.com/read/how-drones-help-smuggle-drugs-into-prison. [Accessed 15 1 2015].

88 K. Gilsinan, "The Flag-Flying Drone That Sparked a Soccer Brawl," The Atlantic, 15 10 2014. Available: http://www.theatlantic.com/international/archive/2014/10/the-flag-flying-drone-that

89 K. Johnson, "Man accused of plotting drone attacks on Pentagon, Capitol," USA Today, 29 9 2011. Available: http://usatoday30.usatoday.com/news/washington/story/2011-09-28/DC-terrorist-plot-drone/50593792/1. [Accessed 15 1 2015].

מיכולתם של הרחפנים לניווט אוטונומי, מיכולתם לחמוק מרדאר ומיכולתם לשאת כלי נשק קטלניים. בהתאם לכך, הם פיתחו ארבעה תרחישים שבהם מבוצעים פיגועים באמצעות רחפנים, כדלקמן:[90]

1. במהלך אירוע חשוב באצטדיון, משגר מחבל רחפן עם מכונת ירייה מאחד הבניינים הסמוכים, ושולט עליו מרחוק. הרחפן מגיע למרכז האצטדיון ומתחיל לירות סביב. גם אם הרחפן אינו מצליח להתמודד עם הרתע, הציבור מוכה הפאניקה מנסה להימלט מהאצטדיון, ורבים נפגעים ונרמסים. מעניין לראות את הדמיון בין תרחיש זה לבין האירוע הממשי שבו שימש רחפן כדי להלהיט את הרוחות במשחק כדורגל ב-2014, עד לפיצוץ המשחק ולפגיעה בשחקנים.

2. מחבל משגר רחפן לתוך מתחם מבוצר. במרכז המתחם משחרר הרחפן חומר לחימה כימי הגורם לפגיעות קלות יחסית בגוף, אך פוגע פגיעה חמורה בתחושת הביטחון של החיילים שבמתחם.

3. מחבל משגר להק של רחפנים לשדה תעופה. אלו מתפוצצים ישירות מעל מטוסים ופוגעים בהם פגיעה משמעותית.

4. מחבל שולח רחפן להתנקש בחייו של פוליטיקאי המרצה בכינוס תחת כיפת השמיים. הפוליטיקאי מוגן אמנם על ידי קיר זכוכית מחוסמת, אך הרחפן עובר מעל הקיר ומפיל מטען חבלה שמתפוצץ סמוך לפוליטיקאי. פיגוע זה דומה למקרה שאירע בסוף שנת 2013, שבו הנחית חבר המפלגה הפיראטית הגרמנית רחפן סמוך לראשה של הקנצלרית אנגלה מרקל בעת אירוע ציבורי. הרחפן אמנם לא הסב לה נזק, אך אילו היה נושא מטען חבלה כלשהו, אפילו זעיר, תוצאות האירוע היו אז שונות ועגומות מאוד.[91]

להתמודד עם האיום

כיצד אפשר להתמודד עם איום הרחפנים? ראשית, יש להבין שהטכנולוגיה כבר קיימת, והיא תישאר זמינה בעשורים הקרובים. ממש כמו הטלפונים החכמים הנמצאים היום בכל יד, המחשב האישי שבכל בית, הרכב הפרטי – הרחפנים מקנים לפרט יכולות של איסוף מידע, תיאום פעולות ושינוע אווירי שבעבר היו שמורות לגופים ביטחוניים בלבד.

90 S. Gallagher, "German chancellor's drone "attack" shows the threat of weaponized UAVs," Ars Technica, 19 9 2013. Available: http://arstechnica.com/information-technology/2013/09/german-chancellors-drone-attack-shows-the-threat-of-weaponized-uavs/. [Accessed 15 1 2015].

91 ibid.

לכל הטכנולוגיות הללו יש תכונה משותפת נוספת: כולן תרמו לחברה וקידמו אותה באופן משמעותי, צד בצד עם הפגיעה בפרטיות, היכולת להזיק באמצעות וירוסי מחשב והפגיעה בנפש בכבישים. אנו מוכנים לשאת בנזקים הללו כדי ליהנות מהכוח שהטכנולוגיות מקנות לנו.

הרחפנים יכולים לספק לחברה האנושית מגוון עצום של יכולות ושימושים: לשאת חבילות ממחסני אמאזון אל בתי הלקוחות, לנטר את התנועה בכבישים, לספק דיווחים על מזג האוויר, לעבור מעל שדות של גידולים ולזהות אזורים הנגועים בטפילים או זקוקים למים, לסייר לאורך פסי רכבת או צינורות גז ונפט, לשמש שרתים אלחוטיים ברום גבוה בעבור אזורי הספר, לעקוב אחר פושעים, לצלם תמונות וסרטים מזוויות שלא היו אפשריות בעבר. אפשר להשתמש ברחפנים לעוד שימושים רבים אחרים, שכיום קשה לנו אף להעלות בדעתנו.

והם יכולים גם לשמש לפשיעה ולטרור. המחוקק וגופי הביטחון ינסו להגביל את הרחפנים בדיוק מסיבות אלו, ועלינו – המתבוננים קדימה – מוטלת החובה לדחוף למציאת נקודת שיווי המשקל העדינה שבין איסור גורף ובין פריצה מוחלטת של הגבולות. דרך זו לא תהיה פשוטה, וקרוב לוודאי שכבר בשנים הקרובות נהיה עדים לפיגוע באמצעות רחפן.

10. מתן שרף: מז"פ בסייבר – אתגר הייחוס

מרחב הסייבר מוכר כיום, בין השאר, כמימד לוחמה וכזירת פשיעה. אולם, בשונה מזירות פשע בעולם הפיזי, שבהן אפשר לזהות בנקל ראיות מפלילות שקושרות את העבריינים לזירת הפשע, חוקרים וגופי אכיפה במרחב הסייבר נתקלים בקושי ייחודי בבואם לנתח מתקפות ואירועים ולגלות את מקור ההתקפה. קושי זה, הידוע בשם "אתגר הייחוס", הופך את מרחב הסייבר לקרקע פורייה לפעילות התקפית אנונימית, ויש בקרב הפועלים בזירה הבין-לאומית שמנצלים עובדה זו לתועלתם. מאמציהם של החוקרים לזהות את מקור המתקפה משתנים בהתאם לסוג המתקפה; כך למשל, כאשר מדובר במלחמת סייבר או בטרור סייבר, עיקר המאמץ הוא לאתר את מדינת המקור של המתקפה, בעוד שכאשר מדובר בפשיעת סייבר, האתגר מתבטא באיתור האדם או הארגון האחראיים למתקפה.

פעמים רבות, הקושי הראשוני הוא בעצם ההבחנה בין תקלה במערכת לבין כשל שהוא תוצר של קוד זדוני. לא אחת יוחסו בשוגג תקלות בציוד ובמערכות קריטיות למתקפות סייבר. במקרה מפורסם שהתרחש בשנת 2011, חשדו חוקרים שהאקרים פרצו למחשבי מערכות הבקרה על משאבות המים של מדינת אילינוי.[92] על פי החשד, התוקפים הפעילו וכיבו את המשאבות ברצף עד שהמשאבות כשלו, ובכך סיכנו את אספקת המים ל-13 מיליון תושבי המדינה. החשד לתרחיש סייבר עלה לאחר שבמהלך חקירת האירוע התגלה שכחצי שנה קודם לתקלה בוצעה התחברות למערכת באמצעות הממשק לניהול מרחוק ממחשב ברוסיה. העיתונות מיהרה לדווח על מתקפת סייבר, אולם בדיקה נוספת גילתה שמנהל חברת האינטגרציה שסייעה בהקמה של תשתית המחשבים שהה ברוסיה בחופשה משפחתית באותה עת, ובאחד הימים התבקש להתחבר למערכת ולסייע לפתור תקלה.
במאמר זה אסקור את הסיבות להיות הבעיה קשה לפתרון, אציג כמה מהפתרונות שאפשר כבר היום ליישם, ואציע רעיונות נוספים להתמודדות עם אתגר הייחוס. כל זאת – מתוך שאיפה לשפר את יכולותינו לחשוף את מדינת המקור ובמידת האפשר גם את זהות התוקף.

מהות הקושי

לשיטתי, אתגר הייחוס נובע משלושה גורמים עיקריים:

המרחב הווירטואלי – ישנם הבדלים מסוימים שנובעים מהתכונה הפיזיקלית הבסיסית ביותר של מרחב הסייבר, שהיא הייצוג הדיגיטלי של אותות חשמליים באמצעות ספרות בינאריות. המידע הבינארי הוא חסר ייחוד; העתק ומקור זהים לחלוטין ואין דרך לדעת מה קדם למה. בתנאים אלו, זיהוי גניבה של מידע קשה במיוחד, כי המשמעות של "לגנוב"

92 http://www.wired.com/2011/11/water-pump-hack-mystery-solved/

למעשה מוחלפת ב-״להעתיק״. העותק המקורי יכול להישאר על מחשב הקורבן ללא הפרעה ובה-בעת הוא מופץ ברחבי המרחב הווירטואלי.

מוחשיות המתקפה – אתגר הייחוס בזירת לוחמת הסייבר בין מעצמות מקבל ממד נוסף. בעוד שתוכנות זדוניות בעבר, כגון וירוסים ותולעים, תוכננו לייצר נזק מִיָּדִי ומוחשי, מתקפות סייבר עשויות להתרחש במהלך שנים רבות מבלי שיהיה ביטוי מורגש לקוד הזדוני במערכת. הדוגמה המפורסמת ביותר לכך היא התקפת הסייבר כנגד מתקן העשרת האורניום באיראן, שעל פי חלק מהסברות נמשכה לפחות שנתיים בטרם התגלתה.[93]

רכיבי חומרה זדוניים – תופעה חמורה שהתגלתה בשנים האחרונות היא החדרה של קוד זדוני לתוך רכיבי חומרה עוד בשלבי הייצור. עוד בשנת 2008 פורסמו מקרים של רכיבי זיכרון USB, מכשירי ניווט GPS ואף מחשבים נישאים שהודבקו בתוכנות זדוניות עוד בטרם יצאו את שערי המפעל.[94] לאחרונה, הופצו דיווחים אחדים על רכיבי תקשורת נגועים ברוגלות ובתוכנות זדוניות אחרות. תופעה זו מקשה עוד יותר על חקירת אירוע, שכן ההדבקה בתוכנה הזדונית נעשתה עוד לפני שהמכשיר הותקן וחובר לרשת (קרי, אין עקבות). בחלק מהמקרים הקוד הזדוני צרוב על רכיבי חומרה, דבר המקשה על הליך הניתוח של המתקפה, כפי שיוסבר בהמשך.

חילוץ ראיות למקור התוכנה מתוך הקוד הזדוני

ארגוני ביון וחברות האבטחה המובילות משקיעים מאמצים ניכרים בניתוחן של מתקפות בניסיון להבין את אופן פעילותן ולקבוע את מקורן. את הנתונים שקוד עשוי להכיל אחלק לשלושה סוגים של מידע: (1) פקודות התוכנה, (2) מטא-דאטה הקשור לקוד הזדוני, (3) הערות שנכתבו על ידי המפתח לצורכי ביאור הקוד שנכתב. שלוש שיטות אלו מבוססות על ההנחה, שאינה ברורה מאליה, שלחוקרים יש גישה לקוד המקורי, בשלמותו או בחלקו. השאלה שנשאלת בהקשר לכך היא: מהיכן משיגים החוקרים את הקוד הזדוני המקורי? בהתאם ל-״מיטב מסורת״ שיתוף המידע באינטרנט, מקצת קטעי קוד מוצאים את דרכם לאתרי שיתוף שונים. במקרים שבהם אי-אפשר להשיג את הקוד עצמו, אפשר לאתר את הקבצים הזדוניים שנשתלו במערכת ולחלץ מתוכם את הקוד.[95] טכניקה זו מאפשרת לנו לבחון את האופן שבו התוקפים מימשו את ההתקפה ולזהות דפוסי פעולה מוכרים. להלן יובאו שלוש דוגמאות לראיות שאפשר לחלץ.

93 http://www.reuters.com/article/2013/02/26/us-cyberwar-stuxnet-idUSBRE91P0PP20130226

94 http://www.scmagazine.com/ibm-distributed-infected-usb-drives-at-conference/article/170862/

95 Disassembly היא טכניקה להמרה של קוד מכונה (קבצי הפעלה, קבצי DLL וכדומה) לפסבדו-קוד, קרי – שורות קוד בשפת תכנות ״גבוהה״ כגון שפת C.

מורפולוגיה ומוסכמות (סטנדרטים) של קוד תוכנה

כאשר בוחנים קוד של תוכנה, ישנם סממנים לשפת המקור של כותבי התוכנה. מדובר במאפיינים כגון האופן שבו מילים מסוימות מאויתות (למשל center באיות אמריקני לעומת centre באיות אנגלי), שמות שניתנו לאובייקטים בקוד וכדומה. במקרים מובהקים יותר, אפשר לזהות את שפת המקור. לדוגמה, מתכנתים מאיטליה נוטים לערבב מילים באנגלית ובאיטלקית, וכך יוצא ששם של פונקציה עשוי להיות IsUtenteTrue, כאשר Utente פירושו באיטלקית user.

יתרה מכך – באופן טבעי, מרכיבים תרבותיים ואפילו העדפות "אמנותיות" של כותבי התוכנה באים לידי ביטוי כאשר הם בוחרים שמות לרכיבים בקוד שהם כותבים. על פי מקורות גלויים, באחת התיאוריות שקושרות את מדינת ישראל לקוד הזדוני של התולעת סטוקסנט נטען שמופיעה בקוד רמיזה לשם "ושתי", בהתייחסות לסיפור מגילת אסתר שבו סוכלו כוונותיו הזדוניות של המן הפרסי (איראן של ימינו) להשמיד את היהודים.[96]

מטא-דאטה הקשור בתוכנה

שורות הקוד שנכתבו על ידי כותב התוכנה עשויות להכיל מידע נוסף שמקורו בסביבת הפיתוח ששימשה את מפתח הקוד הזדוני. מידע זה יכול לסייע לחוקרים לבסס את מקור ההתקפה. למשל, אחת הראיות לכאורה למעורבות של צפון קוריאה בתקיפה שהתרחשה בחברת סוני הייתה ממצא שגילה ה-FBI, שהקוד הזדוני נכתב על מערכות מחשב שהותקנה בהן תמיכה בשפה הקוריאנית. סוגי מידע נוספים עשויים להיות זמינים לחוקרים, למשל הערות Assert[97] והודעות Debug[98], שכותבי התוכנה הוסיפו בתהליך הפיתוח ושכחו למחוק. כלים אלו מותירים שובל של ראיות אשר כוללות תיעוד של ריצת הקוד על המערכת המודבקת, והן מאפשרות לחוקרים להציץ אל תהליך החשיבה שליווה את פיתוח התוכנה.

96 מבוסס על מידע שנחשף בעבר בפומבי.

97 מנגנון שמשמש מפתחי קוד בתהליך הפיתוח ונועד להבטיח את יציבות התוכנה ולתעד כשלים חמורים.

98 הודעות מערכת שמפתחי התוכנה הוסיפו במהלך פיתוח הקוד על מנת לעקוב אחר ביצוע הפקודות ולאתר תקלות בקוד.

```
// Handler to resize the content container when the browser is resized.
var _resizeTimeOutID;
_window.resize(function () {

    // This technique coalesces the calls to 'adjustContentContainer'
    // so it only fires once the browser is truly done resizing and
    // not fired multiple times during resizing.
    window.clearTimeout(_resizeTimeOutID);
    _resizeTimeOutID = window.setTimeout(adjustContentContainerFromResizeEventHandler, 10);
});

// Only valid in browsers that implement the HTML5 navigation
// pushState and accompanied APIs. When change to the navigation
// state is recognized then the page attempts to load the requested page.
_window.on('popstate', function (event) {

    this._popStateEventCount++;

    // Only process if the event fires as the result of the
    // back or forward button being clicked - skip if
    // the event is being raised on the page load.

    // This skips processing for WebKit browsers the first
    // time the event is raised.
    if ($.browser.webkit && this._popStateEventCount == 1) {
        return;
    }
```

הערות בגוף הקוד לצרכי ביאור

פרויקטים של תקיפה בסייבר הם פרויקטי פיתוח מורכבים, ובכך אינם שונים מפרויקטים אחרים של תוכנה. מדובר במתכנתים רבים שכל אחד מהם כותב מרכיבי קוד שונים. בפרויקטים כאלו יש נוהלי פיתוח שמחייבים את כותבי הקוד להוסיף הערות לגוף הקוד. הערות אלו משמשות לחוקרים כר פורה להפקת מידע, וזאת משום שבניגוד לקוד עצמו, שנכתב בדרך כלל באנגלית,[99] במקרים מסוימים ההערות נכתבות בשפת האם של המפתחים. גם במקרים שבהם ההערות נכתבו באנגלית, אפשר בכל זאת להקיש מרכיבי זהות של המפתחים (כגון לאום) מדרך הניסוח באנגלית.

ניתוח של תיעוד ועקבות

במקרים מסוימים, כגון אירועים שבהם הקוד הזדוני נשתל בתוך רכיבי חומרה בהליכי הייצור, אין לחוקרים גישה לקוד. ביולי 2014 פורסם דו"ח של חברת TrapX, אשר זיהתה שסורקים ייעודיים מתוצרת סין מכילים בתוכם רכיבי קוד זדוני שתוקפים מערכות ERP, ועל פי החשד גונבים מידע פיננסי.[100]

99 יש מספר לא מבוטל של שפות תכנות שאינן באנגלית או כאלו המבוססות על סימנים וסמלים ולא על שימוש במילים. רשימה אפשר למצוא במאמר מוויקיפדיה: http://en.wikipedia.org/wiki/Non-English-based_programming_languages

100 http://www.trapx.com/wp-content/uploads/2014/07/TrapX_ZOMBIE_Report_Final.pdf

במקרים אלו, שבהם אין אפשרות לחקור את הקוד הזדוני, אפשר להתחקות אחר הפעילות הזדונית ולבחון מאפיינים שמסגירים את פעילותה של המתקפה. כך למשל, בארגון שבו מיושמים אמצעי בקרה וניטור אפשר לבחון רשומות שנשמרות בציוד קצה ובקבצי מערכת ולאתר פרטי זהות (כגון כתובות IP, שמות דומיין, חשבונות אינטרנט, וכדומה) של השרתים שהמערכות הנגועות מתקשרות עמם, לאתר את המידע שעובר באותם ערוצי תקשורת ועוד.

למעשה, ככל שהמתקפה רחבה יותר ומתרחשת על פני כמה זירות, כך גדלה הסבירות למצוא עקבות ברשומות של ציודי תקשורת ושרתים ברחבי האינטרנט, שדרכם זרם המידע. רשומות אלו עשויות לעזור לחוקרים להתחקות אחר מקור המתקפה ואחר הישויות השונות שהשתתפו בה.

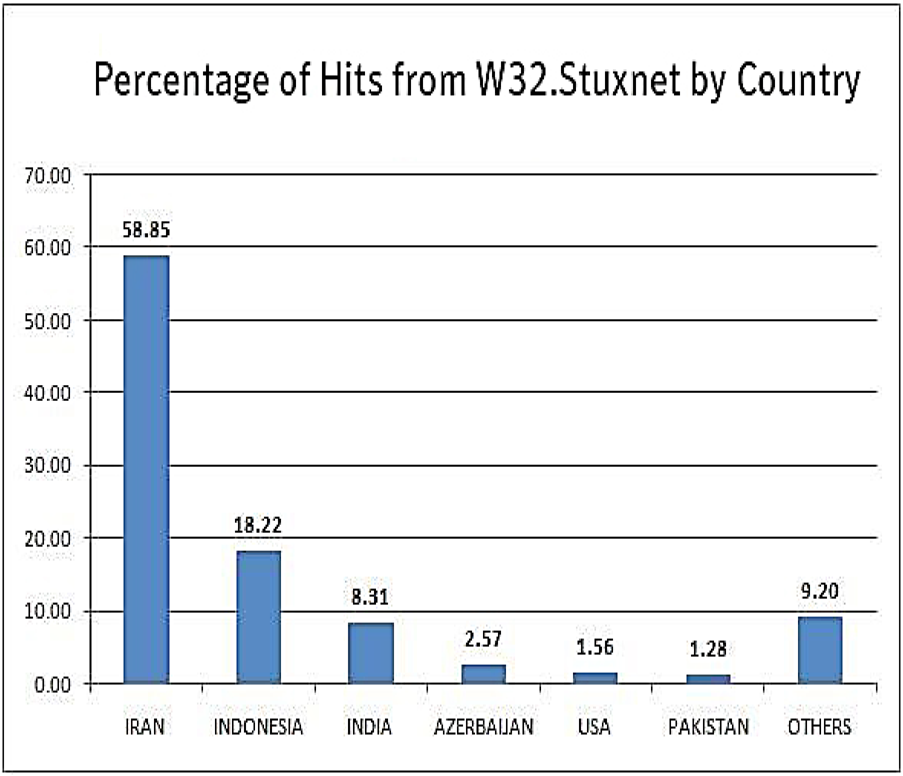
ניתוח ההתנהגות של התוכנה הזדונית

כאשר בוחנים לעומק מאפיינים והיבטים התנהגותיים מסוימים של הקוד הזדוני, מתגלה שכמו לכל לתוכנה אחרת, גם לקוד הזדוני יש מאפיינים ייחודיים שעשויים לסייע לזהות את יוצריו. יש להדגיש – בדרך כלל, דפוסי ההתנהגות של התוכנה הזדונית לא יסגירו את זהות האדם שכתב אותה, אולם יש בכוחם לכוון לזהות מקור ההתקפה, או לכל הפחות לשלול אפשרויות מסוימות. כך או כך, לכל מתכנת, חברת תוכנה ומוסד אקדמאי יש נטיות או העדפות באשר לאופן יישומה של תוכנת מחשב. נטיות אלו הן מעין ״טביעת אצבע״ של מפתח התוכנה, וחוקרים מנוסים יודעים להבדיל בין שיטות שונות ולזהות תבניות מוכרות.

יעד התקיפה

דו״ח של חברת סימנטק על שיעור ההדבקה של מחשבים באחד הווריאנטים של הקוד הזדוני של התולעת סטוקסנט, גילה תמונה מחשידה ביותר.[101] לחוקרים הסתבר שכ-60% מכלל הדבקות המחשבים התרחשו באיראן. מובן שנתון זה הוא חסר פרופורציה לאחוז המשתמשים באינטרנט באיראן מתוך אוכלוסיית העולם, ולכן הוא עשוי להעיד שלקוד הזדוני הוגדרו פרמטרים ייחודיים שנועדו לתקוף מטרות מסוימות ולהימנע מאחרות. דבר זה יכול למקד את תשומת הלב בגורמים בעולם שלהם האינטרס הגדול ביותר לסכל את תכנית הגרעין של איראן. ברור, אם כך, מדוע לאחר פרסום המחקר נשמעו יותר ויותר

101 https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf



טענות כי ארצות הברית וישראל הן העומדות מאחורי המתקפה.

וקטור התקיפה

ערוץ החדירה ודרכי הפצה של הקוד הם מאפיין משמעותי שעשוי לסייע לזהות את מקור התקיפה. ככלל, אפשר לטעון שככול שערוץ התקיפה ייחודי יותר ומצריך משאבים רבים יותר, כך אפשר להסיק שמאחורי התקיפה עומד ארגון גדול ובעל אמצעים. לדוגמה, במהלך מבצע צוק איתן התגלתה התקפה מסוג תקיפת ״פישינג״ ממוקדת בשם ״Gholee״. בדו״ח שפרסמה חברת ClearSky צוין שהקוד הזדוני הופץ למחשבי הקורבנות באמצעות הודעת דוא״ל עם צרופה שהכילה מאקרו והודעה שקראה למשתמש לאפשר להריץ את המאקרו במחשבו.[102] שיטה זו, שמסתמכת על ניצול גורם אנושי[103] כדי להדביק את המטרה בקוד הזדוני, היא שיטה פשוטה למדי, ולכן גם יעילה. היא מאפיינת בדרך כלל תוקפים בעלי

102 http://www.clearskysec.com/gholee-a-protective-edge-themed-spear-phish-/ing-campaign

103 שיטה הידועה בשם הקולקטיבי ״Social Engineering״.

רמה טכנולוגית נמוכה ומשאבים מוגבלים. דוגמה למצב ההפוך אפשר לראות בפריצה לרשת הקמעונאות האמריקנית Target, שבה, על פי הפרסום, חדרו התוקפים לארגון בכמה שלבים נפרדים, ערכו מחקר מקדים ומיפו את נקודות החולשה של הארגון. הם בחרו לתקוף חברה שנתנה שירות לארגון[104] (במקרה זה, חברת התחזוקה של המזגנים), והשתמשו בה על מנת לחדור לרשת המחשבים של Target.

התחמקות מגילוי (Stealth)

מאפיין נוסף של הקוד הזדוני שאפשר לבחון הוא הטכניקות להסוואה ולהיטמעות שבהן השתמשו. כך, באופן פרדוקסלי, העובדה שהתוקפים בחרו להשתמש בשיטה מסוימת על מנת להתחמק מגילוי, עשויה להיות הדבר אשר יסגיר את זהותם. אפשר, למשל, לסווג את המתקפה לפי האופן שבו כלי התקיפה מיישמים את ערוצי ההתקשרות לצורך השליטה של התוקף על המערכת ולפי מנגנוני חילוץ המידע מהמערכת הנתקפת. ארגונים בעלי יכולות טכנולוגיות מפותחות ישתמשו בגישה לרשתות חברתיות ובקידוד מידע בתוך קבצי מדיה (סטנוגרפיה) ושימוש בפרוטוקולי רשת נפוצים (Tunneling) כגון ICMP ו-DNS. זאת בעוד שתוקפים מתוחכמים פחות עשויים לפתוח ערוצי תקשורת ישירים עם שרתים שבשליטתם.

רמת התחכום

בעבר, אחד המאפיינים הברורים של מתקפה שביצע ארגון גדול או אף מדינה היה ניצול חולשות לא מוכרות (DayZero) לצורך הדבקה והפצה של הקוד הזדוני. מומחים (ואני בכללם) מסתייגים מבדיקה זו, כיוון שזמינותן של חולשות אלו ברשתות כמו הרשת האפלה (WebDark) במחירים "שווים לכל נפש" משמעה שלא רק לגופי ביון ולמעצמות יש גישה לחולשות מסוג זה. עם זאת, יש לזכור שכדי שהתוקף יוכל לנצל את החולשה, על הקורבן להיות פגיע בנקודה זו. לכן אפשר להניח שככול שהחולשה המנוצלת ממוקמת ברכיב תוכנה או בשירות רשת נדירים יותר, כך גבוהה הסבירות שהתוקף מכיר היכרות קודמת את מערכות הקורבן. יכולות איסוף מודיעין ברמה גבוהה עשויות להצביע על מעורבות של תוקף בעל משאבים גדולים ולמקד את החשד במעורבות של ארגון פשיעה או אף של מעצמה.

טעויות בזיהוי

השיטות המתוארות לעיל משמשות חוקרים מדי יום הן לשם זיהוי מקורות התקיפה

104 סוג זה של מתקפה נקרא התקפה על "שרשרת האספקה", קרי – לא מתקפה ישירה על משאבי הארגון אלא מתקפה עקיפה באמצעות גורם אחר שנחשב למורשה ולכן נהנה מגישה לא מבוקרת.

הן לחשיפת המעורבים. אולם, אליה וקוץ בה: חלק מהשיטות הללו חשופות לטעויות ואף עלולות להוביל להסקת מסקנות מוטעות ונמהרות. יתרה מזו, אין זה מן הנמנע שתוקפים, ודאי המתוחכמים שבהם, משתמשים בידע זה על מנת להטעות את החוקרים ואף להפליל אחרים. כך למשל, ארגון המנסה לטשטש את עקבותיו עשוי לבחור בכוונה בערוץ הפצה פשוט כגון הודעת דוא״ל עם צרופה כדי שההתקפה תיראה לא מתוחכמת. במקרים אחרים, תוקפים לא יהססו להקים תשתיות נרחבות במדינות זרות כדי לשכנע את החוקרים שמקור ההתקפה הוא אחר, לשתול ראיות מפלילות לכאורה בקוד ועקבות אחרים כפי שתואר לעיל, והכול במטרה ליצור הסחה ולהסיט את החוקרים מגילוי המקור האמתי.

IP מפליל

דוגמה למצב שבו חוקרים הגיעו למסקנות נמהרות הובאה בפתח המאמר, בתיאור תקיפת משאבות המים של מדינת אילינוי. בחקירת המקרה נעשה שימוש בכתובות IP כראיה למקור המתקפה. הנחת היסוד התבססה על כך שכתובות IP פומביות הן מזהה חד-חד ערכי של מחשב רשת ברשת האינטרנט.[105] כתובות אלו מנוהלות על ידי גופי האסדרה הבין-לאומיים ומוקצות כאשכולות של טווחי כתובות לכל מדינה בעולם. המשמעות היא שאפשר, לכאורה, לקשר בין כתובת IP לבין המדינה שלה הוקצה אותו אשכול טווח כתובות.

ההסתייגות המתבקשת נובעת מהעובדה שתוקפים יכולים להסוות את כתובת ה-IP של מקור ההתקפה בשיטות רבות, ולגרום לכך שהתקשורת של מחשבי הקורבן תתרחש מול מחשבים שנמצאים במדינה אחרת. לדוגמה, לצרכי קיום התקשורת יכול התוקף להשתמש בשרתי Proxy, בשירותי מחשוב ענן, או אף בשרתים מסחריים ידועים כגון פורומים ורשתות חברתיות. שיטה מקובלת נוספת להסוות את מקור ההתקפה היא לתקוף מחשב ברשת אחרת ולשתול בו תוכנת שליטה. כך למעשה, המחשב שמבצע את התקיפה הוא עצמו קורבן של תקיפה ואינו הגורם המקורי שתקף את הארגון.

עם זאת, יש להתחשב בכך שלגופי ביון מתקדמים כגון NSA יש אמצעים טכנולוגיים שמאפשרים לחשוף את מסלול התקשורת המלא, ממחשבו של הקורבן ועד מחשבו של התוקף. באחד המסמכים שהדליף אדוארד סנודן ביולי 2013, נחשפה תכנית בשם X-KeyScore. על פי הדיווח, כחלק מהתכנית שתל ה-NSA רכיבי חישה בנקודות גישה

105 למעט במקרים שבהם השתמשו בפרוטוקול anycast לצרכי שימוש חוזר בכתובות חוקיות באמצעות שרתי Root DNS.

שונות בתשתיות האינטרנט, המאפשרות לו להתחקות אחר תקשורות מידע ברחבי עולם.[106]

דמיון מדומה

המתקפה האחרונה על חברת סוני היא דוגמה מצוינת לאתגר הגדול בייחוס ההתקפה. אירוע שבתחילתו נראה כמו מתקפה נוספת של פושעי סייבר בעלי מניעים כלכליים, קיבל תפנית באחת כאשר עלתה הסברה שמדובר במאמץ של הממשל הקוריאני למנוע את הפצת הסרט ״ריאיון סוף״. בסופו של דבר, הולידה הסברה הודעה רשמית של ה-FBI המפנה אצבע מאשימה כלפי הממשל הצפון-קוריאני.[107] ימים אחדים לאחר מכן, חברה פרטית, שניתחה את תכתובות עובדי סוני שהודלפו כחלק מהמתקפה, פרסמה ממצאים המעידים, לטענתה, שמקור ההתקפה הוא עובדים לשעבר שפעלו ממניעים של נקמה לאחר שפוטרו.

מבין כל הסברות שהוצגו, נראה שהתשתית הראייתית הענפה ביותר היא זו של הממשל האמריקני, שבין השאר מבוססת על הדו״ח שפרסמו המשרד לביטחון המולדת (DHS) וה-FBI (אפשר להניח שהיא מבוססת על מקורות נוספים שלא פורסמו).[108] הראיות המוצגות בדו״ח זה מצביעות על הדמיון הרב בין המתקפה על סוני לבין המתקפה על מוסדות בדרום קוריאה. המקטרגים על סברה זו טוענים שהדמיון הוא תוצר של תופעה מקובלת בעולם החדירות למחשבים (האקינג) והיא השימוש החוזר בקוד ובכלים שנעשו זמינים באינטרנט. חברת האבטחה CyActive גורסת שתוכנות זדוניות כמעט לעולם אינן נכתבות מהיסוד, אלא מתבססות על גרסה מוקדמת יותר של תקיפה ידועה כלשהי.[109] במחקרה מתואר כי לעתים מדובר בשימוש בטכניקה קיימת, כמו השימוש ברשתות Bot לניהול התקשורת עם המערכת המותקפת, המוכר עוד משנת 2011. במקרים אחרים מדובר ב-״ערכות פשיעת סייבר״ כגון Infostealer, אשר משמשות תוקפים שוב ושוב בהתקפות על ארגונים שונים. על פי גישה זו, אין זה מן הנמנע שיימצאו דמיון רב ואף חפיפה בין מתקפות, גם כאשר לא קיים קשר של ממש בין אירועי תקיפה שונים.

ומה צופן העתיד?

להערכתי, אתגר הייחוס ימשיך להעסיק את קהילת הסייבר בשנים הקרובות. המרוץ בין התוקפים ובין המגנים בשדה הקרב, שבו הראשונים עוסקים בשכלול שיטות ההסוואה

106 http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

107 http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation

108 מקור (מצריך רישום למערכות OSAC):
https://www.osac.gov/pages/ResourceLibraryDetails.aspx?cid=16796

109 http://www.cyactive.com/

בעוד האחרונים מנסים לחשוף את מקורות המתקפה, ילך ויגבר. יתרונות ההסוואה שמספק העולם הווירטואלי הופכים אותו לזירה מושכת יותר ויותר בעבור רבים, ולכן סביר להניח שהבעיה תחריף עם השנים ומאמצינו לשפר את יכולותינו אל מול אתגר הייחוס יתגברו.

עם זאת, יש לזכור שמאמץ זה הוא רק מרכיב אחד מתוך מכלול המנגנונים שיש לטייב בזירת ההתמודדות של הגנת הסייבר. ארגונים חייבים להמשיך להשקיע במנגנוני ניטור, יישום שכבות בקרה ושמירה על "היגיינת סייבר".[110]

110 ראו מאמרי בנושא: www.web-boxer.com/articles-and-videos/Cyber_Hygiene.pdf