להגנת וירוס הסטקסנט

ג'יימס א. לואיס

גילויים חדשים על הווירוסים 'סטקסנט' (Stuxnet) ו'פליים' (Flame) עוררו שוב מקהלה של אזהרות דחופות מפני סכנות מלחמת סייבר והצורך בפעולה. אך השאלה המטרידה יותר שעולה בעקבות חשיפת הווירוסים היא – אם לוחמת סייבר היא נושא כה קריטי – מדוע אנשים כה רבים מחזיקים במידע כה שגוי לגביה? הדעה ש"'סטקסנט' או 'פליים' הגבירו את הסיכון מעידה על הבנה לקויה של מידת הסיכון שכבר קיימת במרחב הסייבר, של התדירות הגבוהה של פעולות סייבר זדוניות[1] שכבר מתקיימות בחסותן של מדינות ושל הצמיחה המהירה ביכולות הלוחמה של מדינות רבות. לכן, נכון יותר לראות את 'סטקסנט' ו'פליים' כפרק נוסף בתחרות המתמשכת בין ארצות־הברית, איראן ורוסיה.

האמונה ש'סטקסנט' מגביר את הסיכון לארצות־הברית או לבעלות־בריתה מתבססת על מספר הנחות מוצא שגויות. תפיסות הטוענות למכות נגד, נזק נלווה או פתיחת 'תיבת פנדורה' אינן מתקבלות על הדעת לאור היקף הפיתוח והשימוש בטכניקות מתקפת סייבר במהלך שלושת העשורים האחרונים. 'סטקסנט' לא חשף יכולת לוחמה חדשה שאחרים יזדרזו להעתיק. מתקפת סייבר היא יכולת מודיעינית וצבאית מוכרת שנמצאת בשימוש במשך שנים רבות. ההערכה היא שכארבעים מדינות מצטיידות ביכולות לוחמת סייבר או השיגו אותן כבר,[2] לרבות היכולת לשגר מתקפות סייבר. רוב התוכניות הלאומיות אפופות סודיות, ואין הסכמה בשאלה עד כמה החוק הבינלאומי הקיים, שתקף לעימות מזוין, אמור לחול על מצב ההתקפה החדש. עם זאת, כל צבא מתקדם כבר מצויד ביכולת לוחמת סייבר, ומדינות רבות אחרות שואפות להשיגה.

ההאשמה כלפי תפקידה של ארצות־הברית ב'סטקסנט' לא הייתה הפתעה מיוחדת. רוב המדינות כבר הגיעו למסקנה שארצות־הברית הייתה אחראית לכך, ולא נדהמו להיווכח שתוכנה הופכת לכלי התקפי ולאמצעי כפייה. השימוש

ג'יימס א. לואיס הוא חוקר בכיר ומנהל של תכנית למדיניות טכנולוגית ומדיניות ציבורית במרכז ללימודים אסטרטגיים ובינלאומיים – Center for Strategic and International Studies (CSIS).

בטכניקות סייבר ככלי מודיעין החל בשנות השמונים. מתקפת סייבר מצד צבאות החלה בשנות התשעים.[3] פיתוח טכניקות סייבר התקפיות הואץ בשנות האלפיים, כאשר התרחבה זמינותן של רשתות גלובליות מהירות, והאינטרנט הפך מכלי עזר לתשתית מרכזית לפעילות כלכלית וממשלתית. בין אם מדובר בלוחמה שהיא "מוכוונת רשת" או לוחמה ב"תנאי מידוע" (informatized conditions – כפי שסין מגדירה זאת), מתקפת סייבר אינה חדשה למתכננים צבאיים.

מריגול למתקפה

למרות ש'סטקסנט' ו'פליים' התקבלו בהתלהבות כמבשרי עידן מלחמת הסייבר, גישה זו שגויה בכמה מישורים. מתקפת סייבר אינה דבר חדש, ולמרות שחבלה עשויה לערב שימוש בכוח, לא כל פעולת חבלה שקולה לפעולת מלחמה. ההתייחסות ל'סטקסנט' ו'פליים' כאל לוחמת סייבר מנציחה את ההנמקה האנלוגית השגויה והמוגזמת שדבקה בחקירת תחום אבטחת סייבר מראשית ימיה. יש לראות ב"מתקפת" סייבר ארסנל חדש של כלים לכפייה, לריגול ולמתקפה, יותר מאשר קטגוריית עימות ייחודית וחסרת־תקדים.

הקו המפריד בין ריגול למתקפה במרחב הסייבר הוא דק מאוד. יכולות החדירה לרשת והשליטה בה, שנדרשות לשם ריגול, עלולות לשמש לשיבוש שירותים חיוניים. יריב שמצליח להשיג גישה מבוקרת לרשת יכול גם לפגוע ואולי אף להרוס. אפשר לראות במתקפת סייבר סוג של "חימוש" ("weaponization") של מודיעין האותות (SIGINT) – המרת איסוף מידע פסיבי בשיבוש אקטיבי. פירוש הדבר הוא – אם למקם את המונח "פירוק נשק קיברנטי" בהקשרו הנכון – שאיסור על מתקפת סייבר יחייב גם איסור על ריגול – פעילות ששום מדינה לא תסכים לזנוח.

'פליים' היה רק אחד מבין תוכניות רבות לאיסוף מודיעין שנמצאות באינטרנט. כיום ידוע על כתריסר תוכניות דוגמת 'פליים' ששימשו לריגול סייבר. הטכנולוגיה שינתה את האופן שבו מדינות מרגלות זו אחר זו, וריגול סייבר הפך למרכיב מרכזי בתוכניות לאומיות לאיסוף מידע. האינטרנט יצר את מה שקציני מודיעין מכנים "תור הזהב" של הריגול.

"תור הזהב" הזה נכנס כבר לעשור השלישי שלו. בתחילת שנות השמונים השתמשו שירותי הביון הרוסיים בהאקרים (פצחנים) ממערב־גרמניה כדי לחדור לצבא ארצות־הברית, לחקור רשתות ולשאוב מידע. שירותי הביטחון הסיניים ניהלו מערכות ארוכות ומוצלחות נגד הרשתות של ארצות־הברית ובעלות־בריתה, והיו מעורבים בריגול תעשייתי נרחב בחסות המדינה. אם 'סטקסנט' הצביע לכיוון ארצות־הברית וישראל כמדינות שעשויות להפיק את הרווח הגדול ביותר משיבוש מאמצי הגרעין של איראן, ניתן לשאול איזו מדינה עשויה להרוויח מהשקעת משאבים עצומים במעקב אחר פעילי זכויות אדם בטיבט. ב־15 השנים האחרונות,

תוכניות איסוף רבות כמו 'פליים' הפכו ציבוריות. יש להניח שקיימות תוכניות נוספות המוסתרות טוב יותר. לצורכי ריגול, טכניקות סייבר הן במידה רבה הרחבה של יכולות מודיעין אותות מסורתיות, ומבחינתה של סין, מדובר בהרחבה של גישה מבוזרת העושה שימוש בסוכנים אזרחיים רבים, כפי שניתן לראות בתוכניותיה של סין לאיסוף מידע אנושי.

הן סין והן רוסיה משתמשות באקספלויטים (קודי מקור של פקודות תוכנה משבשות) בסייבר בדרכים שונות מאשר פעילויות הסייבר של שירותי המערב, מבחינת החשיבות והפוטנציאל שלהן לגרימת חוסר יציבות. שתי המדינות מסתמכות על גורמים שלוחים (פרוקסי) – פצחנים (האקרים) פרטיים הפועלים על פי הכוונת המדינה למטרות ממשלתיות. גורמים אלה מספקים דרגה קלושה למדי של יכולת הכחשה (במקרה שמשקיף רציני כלשהו אכן מאמין שסין ורוסיה אינן שולטות ברשתות שלהן), לצד חזית קדמית של תוקפים שיכולים לגונן על פעולות המדינה, ואם נדרש, גם "יקריבו" אותם על מנת לפייס מדינות אחרות. השלוחים הרוסיים התמקדו בפשעים פיננסיים, והסינים התמקדו בריגול תעשייתי. שתי המדינות מספקות רמה מסוימת של הדרכה ותמיכה לשלוחים שלהן, ומתעקשות רק על כלל מרכזי אחד – שלא יפעלו נגד יעדים מבית. כל עוד כלל זה נשמר, ובמקביל השלוחים מבצעים את המשימות שהמדינה מעבירה להם, הם חופשיים לפעול נגד מטרות בארצות אחרות. פצחנים רוסיים היו אחראיים לאקספלויטים נגד אסטוניה וגאורגיה (בגאורגיה היה תיאום מדויק עם תוכניות הצבא הרוסי),[4] ואילו הסינים היו אחראיים לשאיבת נתונים מיעדים צבאיים וכלכליים רבים, בארצות־הברית ובמדינות אחרות.

לעומת זאת, ארצות־הברית ובעלות־בריתה אינן עושות שימוש בשלוחים מטעמן לצורך מעורבות בפשעים פיננסיים בחסות המדינה, וארצות־הברית אינה מעורבת בריגול תעשייתי. הדוקטרינה האמריקנית לשימוש בטכניקות סייבר כהרחבה של אמצעי כפייה מסורתיים דוגלת בגישה שונה, אם כי בהחלט לא חסרת־תקדים.

מתקפת סייבר ותהליך ההתחמשות (Weaponization) של מודיעין האותות

יכולות כמו אלה של 'סטקסנט' משקפות שנים של פיתוח וניסויים בניצול רשתות דיגיטליות להשגת כוח צבאי. וירוס 'סטקסנט' צויד ביכולות הרס מתקדמות משום שתוכנן להשפיע על מערכות בקרה תעשייתיות – מחשבים ייעודיים המפעילים מכונות – אך למעשה הוא היה רק הרחבה ושיפור של טכניקות מתקפת תוכנה קיימות. היכולת להשתמש בתוכנה לשיבוש מערכות בקרה תעשייתיות ולגרום הרס פיזי הומחשה כבר בניסוי שנערך במעבדה הלאומית של איידהו (ארצות־

הברית) ב־2005. ההערכה היא שחמש מדינות מחזיקות ביכולת זו – ארצות־הברית, בריטניה, ישראל, רוסיה וסין, ומדינות רבות נוספות מנסות להשיג אותה. בהקשר זה ארצות־הברית יכולה להיחשב "ראשונה בין שוות", אך יש לה שותפים למעמד זה (או כמעט שותפים) בתחום מתקפת סייבר. 'סטקסנט' עשוי להיחשב ל"נשק" המתקדם ביותר מסוג זה (חותמת איכות אמריקנית נוספת), אך בשום אופן לא מדובר ביכולת ייחודית.

מתקפת סייבר היא אופציה נוספת הזמינה למתכננים צבאיים. במקרה של 'סטקסנט' למשל, המתכננים יכלו לשקול את היתרונות והחסרונות של מתקפת סייבר מול מתקפה אווירית, צוות מבצעי מיוחד, חבלנים או טילים. תורות הלחימה הקיימות הורחבו והותאמו למצב התקיפה החדש. מדינות יצרו יכולות מתקפת סייבר ופיתחו דוקטרינות ואסטרטגיות לשימושן. דוקטרינות לאומיות אלה אינן זהות בכל המדינות. אנו נמצאים בתקופת התנסות, שבה המדינות מעריכות יכולת צבאית חדשה זו וחוקרות מהי הדרך הטובה ביותר לנצל אותה. נוסף לשימוש שעשתה רוסיה ב"מתקפת" סייבר באסטוניה ובגאורגיה, והשימוש לכאורה שעשתה ישראל בסוריה, ראינו כיצד רוסיה וסין אוספות מידע לצורך מתקפות על תשתיות אמריקניות חיוניות (על פי ראש הסוכנות האמריקנית לביטחון לאומי),[5] ומשתמשות באיראן נגד ישראל ומדינות המפרץ. ארצות־הברית השתמשה במתקפות סייבר בשנות התשעים במהלך העימות עם סרביה, ונגד ההגנה האווירית של עיראק בין מלחמות המפרץ.

ארצות־הברית, רוסיה, סין ומדינות נוספות, כוללות בדוקטרינה שלהן לגבי שימוש צבאי במתקפת סייבר גם מתקפה על תשתיות חיוניות. הדוקטרינה הגלויה רומזת על כך שכל מדינה מקבלת החלטות על השימוש במתקפת סייבר באופן עקבי לתכנון השימוש שלה בסוגים אחרים של נשק ארוך־טווח – כגון שקלול יתרונות התקיפה, הסיכון בהסלמה והפוטנציאל לנזק נלווה. ניתן לראות בדוקטרינה האמריקנית כמה קוים מקבילים לחשיבה על הפצצה אסטרטגית ולשימוש בהפצצה אווירית להפחתת הנכונות והיכולת של האויב להתנגד, במקביל להימנעות מעימות ממושך עם כוחות צבאיים. הדוקטרינה הרוסית שמה דגש רב יותר על הפרת היציבות הפוליטית ועל שיבוש מערכות פיקוד צבאיות באמצעות טכניקות סייבר, בדומה לדוקטרינה הסובייטית שדגלה במכות פתיחה חזקות נגד נאט"ו באמצעות תקיפת תשתית חיונית. הדוקטרינה הסינית עמומה יותר, אך הדיון הציבורי מתמקד במתקפות על תשתיות במטרה לשבש יכולת אמריקנית להתערב במשברים אזוריים.[6]

כאשר בוחנים מתקפת סייבר בהקשר של קבלת החלטות צבאיות (בהנחה ששחקנים מדינתיים ושחקנים לא־מדינתיים חולקים לרוב תהליכי תכנון צבאי דומים), עולות ההשלכות של השימוש בה. הסבירות שמדינות ישגרו לעבר ארצות־

הברית או בעלות־בריתה מתקפת סייבר שתגרום נזק פיזי לא גברה בעקבות חשיפת 'סטקסנט', ובאותה מידה, אין סיכוי שמדינות אלה יפסיקו את השימוש בטכניקות סייבר לצורכי ריגול וכפייה פוליטית. הסיבה שאיננו עדים למתקפות שיכולות לגרום לארצות־הברית ולבעלות־בריתה נזק פיזי, הרס או נפגעים (בניגוד לריגול או לפשע) מצד המדינות שמחזיקות ביכולת כזו היא שמדינות אלה מעריכות שהסיכון לתגובה אלימה גבוה מדי. זו גם הסיבה שמונעת מהן לשגר מטוסים או טילים נגד ארצות־הברית. עם זאת, החוק והנוהג הבינלאומי אינם מצדיקים שימוש בכוח כתגובה לריגול ולפשע, וכך נעשה הסיכון לתגובה אלימה כזו נמוך וסביר.

הימנעות זו מתקיפה עשויה להשתנות ככל שמדינות אחרות, עם דרגת סובלנות אחרת כלפי סיכון, דוגמת איראן, ישיגו יכולות מתקדמות למתקפת סייבר, או כאשר גורמים שמעריכים באופן מופרז את יכולתם להישאר סמויים ישיגו יכולות מתקדמות. מה שאיננו יודעים הוא עד כמה התקדמו שחקנים לא־מדינתיים ביכולתם לפתח טכניקות הרסניות דומות. העובדה היחידה שאין עליה מחלוקת היא שעד היום לא ראינו שחקנים לא־מדינתיים המעורבים במתקפות כאלה. דבר זה עשוי לשקף היעדר מניע או יכולת, ולא ניתן להעריך באיזו מהירות עשויים גורמים אלה להשיג יכולת לבצע מתקפות דוגמת 'סטקסנט'.

לזכותם של מתכנני 'סטקסנט' ייאמר, שהוא נכתב בזהירות מספקת על מנת למנוע נזק נלווה. ייתכן שתוקפים אחרים לא יהיו כה זהירים, אך אין קשר בין עובדה זו לבין יכולת הגישה לקוד 'סטקסנט'. יריבים פוטנציאליים ממשיכים להתמודד עם אותם שיקולי בעד ונגד בהחלטתם האם להשתמש בכוח נגד ארצות־הברית, והם ימשיכו להירתע מהתגובה האפשרית של צבא ארצות־הברית לנוכח כל המשאבים הצבאיים שעומדים לרשותו מעבר למתקפת סייבר. אפשר שגורמים אלה יישענו על 'סטקסנט' כחלק מהצדקה ציבורית למתקפה, אך יהיה זה תירוץ בלבד ולא חלק מקבלת ההחלטות שלהם. הסיכוי שמדינות ישגרו מתקפת סייבר נגד ארצות־הברית או בעלות־בריתה בעקבות חשיפת 'סטאקסנט' אינו גבוה יותר מאשר הסיכוי שקדם לחשיפתו.

לאופן השימוש של צבאות בפוטנציאל של מתקפת סייבר יש השלכות המסבירות מדוע 'סטקסנט' ו'פליים' לא שינו באמת את מהלך העניינים. כמו לכל נשק, גם למתקפת סייבר יש מאפיינים משלה. מתקפות סייבר יכולות להיות מהירות וחשאיות ולהוות סיכון פוליטי מופחת בחלק מהתרחישים. החיסרון שלהן הוא תוצאה הרסנית פחות. מתכנן המתקפה ישקול היבטים אלה, ויעריך את הסבירות שמתקפת הסייבר תשיג את האפקט המבוקש ב"עלות" הנמוכה ביותר בהשוואה לאפשרויות מתקפה אחרות. בחלק מהתרחישים עדיפה מתקפת סייבר. החלופות ל'סטקסנט' כללו צוותי חבלה, התקפות אוויריות, ירי טילים או אפילו כיבוש שטח בידי כוחות קונבנציונליים. די ברשימה קצרה זו – שכל האפשרויות

בה כרוכות בסיכון רב יותר לאבידות, לאלימות ולהסלמה – כדי להראות מדוע מתקפת סייבר הייתה עדיפה.

יש מדינות שכבר עושות שימוש סדיר במתקפות סייבר בדרכים שמשרתות את צורכיהן. לאחרות יש יכולת להוציא לפועל מתקפה דוגמת 'סטקסנט', אך האסטרטגיה שלהן שמה דגש על יעדים אחרים, ועד היום לא היה להן עניין בגרימת נזק פיזי. רוסיה וסין הציגו יכולות מתקדמות, וביכולתן לשגר מתקפות דוגמת 'סטקסנט' אילו היה הדבר נתפס בעיניהן כמועיל. העובדה שהעימות בתחום סייבר נותר ברובו נסתר מעיני הציבור לפני 'סטקסנט', אין פירושה שהוא לא התקיים.

הנחה שגויה נוספת היא ש'סטקסנט' היה אירוע דוגמת הירושימה, בכך שהתיר את הרסן מכוח צבאי הרסני חדש וחסר־שליטה. אלא שכאן אין איש כאופנהיימר שידקלם בעקבות 'סטקסנט': "עתה הפכתי אני לכוח המוות, משמיד העולמות".[7] למרות הרצון המפתה לכאורה להשוות בין מתקפת הסייבר לנשק גרעיני, השוואה זו מופרכת מיסודה. גם לנשק גרעיני בקנה־מידה קטן ביותר יש כוח הרס עצום, אך למתקפות סייבר אין. הן מהוות נשק תמיכה, היעיל בעיצוב שדה הקרב לטובת המשתמש בו, אך השפעתן אינה כמו של הרס המוני או קטלני, ואין בכוחן להוות איום קיומי על מדינות. לכל היותר, ניתן להשוות מתקפת סייבר לטילים שמאפשרים מכה מהירה למרחק רב, עם מרכיב גדול יותר של סודיות (אולי), לצד תוצאה הרסנית פחות. יכולת הרס מוגבלת זו – אין פירושה שניתן לקדם בברכה שיבוש שנגרם מבהלה פיננסית מלאכותית או מהפסקת חשמל שנמשכת שבועות ארוכים, אך עלינו להימנע גם מהגזמה בהשפעה המיוחסת למתקפת סייבר.[8] 'סטקסנט' הפנה את תשומת הלב לפגיעותה של התוכנה המודרנית, אך הכוח ההרסני של מתקפת סייבר אינו קרוב כלל לזה של נשק גרעיני, או אפילו לזה של מתקפה בנשק קינטי.

התחרות האזורית

קוד 'סטקסנט' זמין עתה לציבור, ויש החוששים שיהיו מי שישתמשו בו שוב, אולם יש בכך התעלמות מאחת המגבלות העיקריות של מתקפת סייבר – בדרך כלל מדובר באקספלויט חד־פעמי. ברגע שהמתקפה חושפת שגיאות תִכנות חדשות ("zero days") או אחרות במערכות ההפעלה או במערכות בקרה תעשייתית, הן לרוב מתוקנות. קוד 'סטקסנט' שנגיש לציבור היה חלק מאקספלויט גדול ומורכב יותר, שכלל מגוון טכניקות ריגול. הקוד היה רק חלק מהאקספלויט, ואינו מספיק כשלעצמו. אם 'סטקסנט' ישוגר שוב הוא לא יפעל. ההוכחה הטובה ביותר לכך היא שבעוד מערכות רבות ברחבי העולם נדבקו בווירוס, רק אחת ניזוקה – באיראן.

איראן עלולה לגלות רצון לנקום על 'סטקסנט', אך אין זה חדש לאיראנים שארצות־הברית ומדינות אחרות מעורבות במבצעים חשאיים שמיועדים לעכב

את תוכניתם הבלתי־חוקית לפיתוח נשק גרעיני, ובאותה מידה, האיראנים מעולם לא הסתירו את תמיכתם באלימות נגד ארצות־הברית או ישראל. איראן אחראית למותם של אנשי סגל אמריקניים בביירות, במפרץ הפרסי ובעיראק. 'סטקסנט' הוא פרק נוסף בעימות שמתקיים בחשאי ומתלקח מדי פעם בין ארצות־הברית לבין איראן, כבר למעלה משלושים שנה.

איראן לא היססה גם להביע איומים, ולא הסתירה את רצונה לפתח ולהשתמש בטכניקות מתקפת סייבר. רטוריקה ארסית מצד מנהיגי איראן נגד ישראל עשויה להיות התרברבות גרידא שנועדה לקהל הביתי, אך אין בכך כדי להצדיק אותה. למדינות יש אחריות על אמירות פומביות של מנהיגיהן. לנוכח האיומים שנשמעו, ועל רקע ההפרות החוזרות של המחויבות הבינלאומית ביחס לנשק גרעיני, יהיה זה תמוה לומר שפעולה סמויה הכרוכה בשימוש בתוכנה נגד תוכנית הגרעין האיראנית אינה ראויה, מה גם שלא נגרמו פגיעות בנפש או נזק נלווה.[9]

המסקנה שארצות־הברית הייתה מעורבת ב'סטקסנט' גם היא אינה מפתיעה. לארצות־הברית היסטוריה של נקיטת פעולות חשאיות נגד משטרים אגרסיביים ובלתי־דמוקרטיים. היכולת פותחה במלחמת העולם השנייה (בחסות הבריטים), ושוכללה והורחבה במהלך המלחמה הקרה. אולם ארצות־הברית מעולם לא השתמשה בכוח חשאי נגד מדינה דמוקרטית או נגד מדינה שאינה מהווה כל איום על השלום הבינלאומי. ניתן להטיל ספק ביכולתה של ארצות־הברית לזהות איומים על השלום, ואכן נעשו טעויות רבות בעבר, אך איראן אינה אחת מהן. במקרים רבים עדיפה פעולה חשאית על פני תגובות צבאיות אחרות, שכן היא מפחיתה את הסיכון לעימות ישיר או להרחבת הסכסוך. פעולה חשאית היא שביל הזהב בין הסכמה שבשתיקה לבין מלחמה גלויה, היא כלי לגיטימי נוסף להגנתה של מדינה, גם אם יש מי שיתנגדו לכך.

ארצות־הברית מצדיקה התערבויות אלה בכך שהיא מובילה קואליציה של מדינות המגֵנות על הדמוקרטיה – תפקיד שהוטל עליה בעקבות מלחמת העולם השנייה והמלחמה הקרה. תפקיד זה היה מקובל באופן כללי על הקהילה הדמוקרטית בין השנים 1941 ל־1990. גם אם איננו מקבלים את הטענה שארצות־הברית עדיין עומדת בראש קואליציה של מדינות להגנה על הדמוקרטיה, סיבה טובה המצדיקה נקיטת אמצעים אקטיביים כתגובה היא התנהגותה של איראן, המאיימת על ביטחונה של ארצות־הברית ועל שלום העולם.

היתרונות של 'סטקסנט' הם רבים, והצער היחידי שעלינו לחוש הוא שהתגלה מוקדם מדי. שיגור 'סטקסנט' הציב סיכון פוליטי נמוך הרבה יותר מאשר התקפות אוויריות. לא היה נזק נלווה, ולא שידור טלוויזיוני של בניינים עולים באש ואזרחים מבוהלים. לא הופל טייס ולא הוצעד ברחובות טהראן בדרך למתקן העינויים. הפיכת הקוד לנשק מלחמה עלתה הרבה פחות מאשר מטוס F16 אחד.

ההקשר הפוליטי החסר

הדגש שהושם על מלחמת סייבר בדיון הציבורי על 'סטקסנט' ו'פליים', הביא לכך ששאלות חשובות נותרו ללא התייחסות. כאשר אנו רואים שהיריב "חושף במקרה" פעולה חשאית ומורכבת, ובייחוד אם הדבר קורה יותר מפעם אחת, עלינו לשקול הסברים שאינם צירוף מקרים גרידא. ההשערה שכדאי להתעמק בה היא החיבור האפשרי בין חשיפת הווירוסים הללו לבין רוסיה. הגילויים בנוגע לוירוס 'פליים' שירתו סדר־יום פוליטי רוסי רחב יותר, שעניינו משילות אינטרנט (internet governance) ואבטחת סייבר. הצבת 'סטקסנט' ו'פליים' בהקשר של ריגול ופעולה פוליטית חשאית עשויה לספק הסבר טוב יותר מאשר ההתמקדות בלוחמה, בייחוד כאשר האופן שבו פורסם המידע על 'פליים' עולה בקנה אחד עם מניפולציה פוליטית שנועדה לזכות בתמיכה במפגשים רב־צדדיים בנושא משילות אינטרנט, שעתידים היו להתקיים במהלך 2012. רוסיה ומדינות אחרות רוצות שאיגוד הטלקומוניקציה הבינלאומי (ITU) ישחק תפקיד גדול יותר באבטחת סייבר ובמשילות אינטרנט. תפקיד גדול יותר של ה־ITU יחתור תחת כל מה שנתפס כ"הגמוניה" אמריקנית במרחב הסייבר, ואולי אף יפחית את הסיכון לרוסיה, כתוצאה מהגישה הבלתי־מוגבלת למידע שהאינטרנט מציע. רוסיה עשויה אף לחתור ל"הכפשת" השימוש במתקפות סייבר ולהשיג תמיכה רחבה באמנה האוסרת שימוש בנשק דוגמת 'סטקסנט', כחלק ממאמציה לערער תחום שנתפס כיתרון של הצבא האמריקני. מדובר בתכסיס ידוע ביחסים בינלאומיים – הצעת מגבלות המכרסמות ביכולתו של היריב יותר מאשר בזו של המציע (בדומה למאמצים בשנות השמונים לתמרן את פירוק הנשק הגרעיני באירופה כדי להפחית מיכולותיהן של מדינות נאט"ו יותר מאלה של החברות בברית ורשה).

בכל הקשור לנושא זה קיימים קישורים בלתי־שגרתיים: מנכ"ל החברה שחשפה את 'פליים' היה דובר לא־רשמי של ממשלת רוסיה בוועידת הסייבר בלונדון ב־2011. בנובמבר 2011 הכריזו החברה שלו ו־ITU על הקמת שותפות לקידום אבטחת סייבר גלובלית.[10] החברה טוענת שחשפה את 'פליים' לאחר ש־ITU ביקשה ממנה – בקשה שהייתה חסרת־תקדים כשלעצמה – לבחון פריצות נתונים במזרח־התיכון, ועל בסיס זה הכריזה ITU על אזהרה גלובלית של אבטחת סייבר, שגם היא הייתה חסרת־תקדים.[11] ייתכן שהדברים הם בדיוק כפי שהם, אולם השערה חלופית שלא ניתן לדחות אותה על הסף, היא שמדובר בתמרון פוליטי גדול יותר שתכננו הרוסים, על מנת להשפיע על השקפתן של מדינות מפתח. השימוש בגורם שלוח (פרוקסי) לפרסום מידע מזיק על היריב הוא טכניקת ביון מוכרת, ורוסיה נשענת באופן ניכר על גורמים שלוחים בשיטות ריגול הסייבר שלה. מצבים חריגים אלה מרמזים ומצביעים על השערות חלופיות, שהסבירה ביותר היא ששירותים

מערביים יצרו את 'פליים' כדי לרגל אחר איראן, וכי רוסיה ניצלה את החשיפה למטרות פוליטיות.

בשנים האחרונות החלו רוסיה וסין (לעתים דרך 'ארגון שנגחאי לשיתוף פעולה') לפתח אסטרטגיה בינלאומית שתיצור אינטרנט המותאם יותר לאינטרסים שלהן. הן מאמינות שהשליטה הדומיננטית של המערב במידע היא חלק מאסטרטגיה גדולה יותר של הגמוניה, ולא רק תהליך שצמח מתוך כישלון המדינה להחזיק בלעדית במדיה. בעוד הן יכולות לדכא את האזרחים שלהן, הן אינן יכולות לדכא מקורות מידע זרים. רוסיה וסין השקיעו רבות בצְנזור טכנולוגיות, אך גם ביקשו הסכמה בינלאומית להגדרת מידע כנשק שחובה לפקח עליו. האינטרנט יוצר לחצים פוליטיים שלא קל למשטרים רודניים לשלוט בהם, והוא יכול להוות איום עליהם (באיזה היקף – זוהי שאלה אחרת). מאמצים נרחבים אלה להגביל את הגישה למידע ולהחליש את ארצות־הברית הם ההקשר הפוליטי של 'פליים'.

באותו זמן לערך ש'פליים' ו'סטקסנט' משכו תשומת לב כה רבה, תוכנת ריגול נוספת הצליחה לחמוק בשקט. שירות פרוקסי פופולרי (שמאפשר למשתמשי אינטרנט לחמוק מפיקוח ממשלתי) נפגע כך שכל אדם שהוריד את תוכנת הפרוקסי הוריד גם תוכנה זדונית שסיפקה את שם המשתמש ואת שם המחשב, ותיעדה את כל הקשות המקלדת. התוכנה הזדונית Simurgh פגעה באלפי אנשים. החוקרים שאיתרו אותה – אנשי Munk School שבאוניברסיטת טורונטו – מאמינים שהיא נועדה למתנגדי משטר איראניים וסוריים.[12] התוכנה הזדונית יצרה סיכון גבוה הרבה יותר מאשר 'פליים', אך לא זכתה להתייחסות כה מרעישה, וה־ITU לא הוציא אזהרה גלובלית בעקבותיו. הסבר אפשרי לחריגות זו הוא ש'פליים' מתאים לסדר־יום פוליטי רחב יותר מאשר Simurgh.

הקשר בין 'פליים' לבין משא־ומתן בינלאומי על אבטחת הסייבר (ומשילות אינטרנט), מספק רקע חשוב למאמצים הרב־צדדיים להפוך את מרחב הסייבר לבטוח יותר. אחד ההיבטים שלא זכו לתשומת לב בפרשנות הציבורית בנושא לאחרונה הוא שהסיכון החדש ממתקפת סייבר הפך לחלק מסדר־היום הבינלאומי בתחום האבטחה כבר לפני שנים אחדות, כאשר החלו לצוץ הסיכונים הביטחוניים והצבאיים מקישוריות גלובלית במהירות גבוהה. מרחב הסייבר, שכמעט אינו נשלט או מאובטח, הפך עתה מקור לחוסר יציבות בינלאומית. מדינות חוששות מהסלמה שתהפוך בהיסח הדעת לעימות קינטי (צבאי) נרחב יותר מאשר מההשפעה המעשית של מתקפת סייבר, בהתחשב בפוטנציאל המוגבל לנזק שהיא נושאת. דיאלוג רציני בנוגע לאפשרויות הפחתת הסיכון מתקיים לפחות מאז שרוסיה הפעילה טכניקות סייבר נגד אסטוניה ב־2007. ה"מתקפות" נגד אסטוניה ב־2007 היוו סכנה רבה יותר ליציבות הבינלאומית מאשר 'סטקסנט', שכן הן איימו לעורר עימות מזוין בין מדינות נאט"ו לבין רוסיה.

כתוצאה מכך, מתקיימים דיונים בפורומים רשמיים רבים בשאלה כיצד להפחית את הסיכון ולהגביר את היציבות, ביניהם קבוצת מומחי הממשל מטעם האו"ם (UN's Group of Government Experts), הארגון למען יציבות ושיתוף פעולה באירופה (Organization for Stability and Cooperation in Europe), הפורום האזורי של אסיה (Asian Regional Forum) וועידת לונדון (London Conference) Process. ארגון מדינות אמריקה (Organization of American States) ערך מפגשים בנושא אבטחת סייבר. ארצות־הברית, רוסיה וסין מעורבות בדיאלוגים בנושא, וארצות־הברית משתתפת בדיונים דומים עם בעלות־בריתה הקרובות. תיאורם של 'סטקסנט' ו'פליים' כסכנה חמורה חדשה הוא אמצעי רטורי להשגת יתרון במשא־ומתן, יותר מאשר ניתוח רציני של מצב הביטחון הבינלאומי.

מסקנות

צבאות שמצטיינים בקדמה טכנולוגית יצרו טכניקות סייבר, ויעשו בהן שימוש כדי לקדם את האינטרסים שלהם. גם אם אין מדובר ב"לוחמה", בכל זאת קיים עימות. אם 'סטקסנט' ו'פליים' מהווים סיכון כלשהו, הסיכון הוא שחוסר ידע צבאי ורקע הולם למשא־ומתן על אבטחת סייבר, לצד מה שנראה כאמונות טפלות בנוגע למתקפת סייבר – הם אלה שיסכלו את המאמצים להפוך את מרחב הסייבר לבטוח ויציב יותר. 'סטקסנט' ו'פליים' לא היו אפוקליפטיים. למעשה הם אינם חדשים במיוחד, וודאי שאינם מבשרי עידן חדש של לוחמה. הטכנולוגיה מעצבת מחדש את הלוחמה מאז המהפכה התעשייתית. אולי הדבר אינו לרוחנו, אך נדיר שמדינות וארגונים חמושים ינטשו יכולת חדשה. מדינות עשויות לדחות נשק להשמדה המונית, אך למעט זאת הכל קביל, ומתקפת סייבר אינה יוצאת מכלל זה. מדינות ימשיכו לנהוג כפי שתמיד נהגו, ופשוט ינצלו טכנולוגיות חדשות להשגת מטרותיהן.

הערות

1 ניתן להגדיר פעולת סייבר זדונית כתוכנה שנשלחת באמצעות רשתות דיגיטליות להשגת גישה לא־חוקית למחשבי היעד, ומבצעת פקודות ללא הרשאת הבעלים.

2 James A. Lewis, Katrina Timlin, "Cybersecurity and Cyberwarfare," UNIDIR Resources, 2001, www.unidir.org/pdf/ouvrages/pdf-1-92-9045-011-J-en.pdf

3 ספרו של קליפורד סטול (Clifford Stoll): *The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage* (New York: Doubleday, 1989) מספק פרטים על ריגול סייבר סובייטי בשנות השמונים. אמנם התקיים דיון ציבורי מועט בלבד על מתקפות סייבר מצד ארה"ב נגד סרביה בשנות התשעים, אך פקידים אמריקניים סיפקו פרטים בראיונות.

4 US Cyber Consequences Unit, "Overview by the US CCU of the cyber campaign against Georgia," August 2009, http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf.

5 The Guardian, "Militarisation of Cyberspace: How the Global Power Struggle Moved Online," April 2012, http://www.guardian.co.uk/technology/2012/apr/16/militarisation-of-cyberspace-power-struggle

6 ראו לדוגמה:
Steve DeWeese, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, Northrop Grumman, October 2009.

7 רוברט אופנהיימר, המדען שעמד בראש פרויקט פיתוח פצצת האטום, ציטט משפט זה מתוך ה"בהגאוואד גיטה" (Bhagavad Gita), בעקבות הניסוי המוצלח הראשון.

8 תרחישי "סייבר־בדומה־לגרעין" כרוכים בשרשרת ארוכה של הנחות מפוקפקות על ההשפעה הפוליטית של מתקפה ועמידות המטרה. לדיון מפורט, ראו:
James Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats," CSIS, December 2002, http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf.

9 ראו לדוגמה:
Robert Wright, "How Obama's Cyberweapons Could Boomerang," *The Atlantic*, June 2012; Misha Glenny, "We will Rue Stuxnet's Cavalier Deployment," *Financial Times*, June 2012, http://www.ft.com/cms/s/0/6b674600-afc7-11e1-a025-00144feabdc0.html#axzz25KCLvt33;
או:
Jason Healy, "Stuxnets are not in the US National Interest: An Arsonist Calling for Better Fire Codes," Atlantic Council June 2012.
שימו לב שהאירוע שעורר זעקה זו לא היה המתקפה עצמה אלא סיפור חדשותי על המתקפה, שממחיש את תפקידה של המדיה בדיונים אלה. רעש תקשורתי אינו מדד טוב לסיכון ממשי.

10 "ITU Teams Up with Kaspersky Lab for ITU Telecom World 2012," http://www.kaspersky.com/about/news/business/2012/ITU_Teams_Up_with_Kaspersky_Lab_for_ITU_Telecom_World_2012.

11 Kaspersky Lab and ITU Research Reveals New Advanced Cyber Threat," http://www.kaspersky.com/about/news/virus/2012/Kaspersky_Lab_and_ITU_Research_Reveals_New_Advanced_Cyber_Threat/.

12 Munk School of Global Affairs, "Iranian Anti-Censorship Software 'Simurgh' Circulated with Malicious Backdoor," May 2012, https://citizenlab.org/2012/05/iranian-anti-censorship-software-simurgh-circulated-with-malicious-backdoor-2/.