התרת אפקט ה־'סטקסנט':
על המשכיות ושינוי בשיח על איומי הסייבר

מרים דאן קוולטי

מבוא

זה שנים אחדות שאיומי סייבר נמצאים על סדר היום הפוליטי והביטחוני. זמן לא רב לאחר שחוקרי מכון RAND, ג'ון ארקווילה ודויד רונפלדט, דיברו על כך ש"הלוחמה הקיברנטית (לוחמת סייבר) מגיעה!",[1] הפך צירוף המילים "לוחמת סייבר" לסיסמה הבולטת ביותר בשיח בנושאי מחשבים, ביטחון לאומי ומרחב קיברנטי (cyberspace). נתונה לחסדי האירועים וההתרחשויות שבכותרות, גברה ההתעניינות בנושא כל אימת שדווח באמצעי התקשורת על שימוש אגרסיבי במחשבים; היא שבה ודעכה כאשר נושאים אחרים תפסו את מרכז הבמה.

בשנת 2010 נפל דבר. הסטקסנט (Stuxnet), תולעת המחשב המתוחכמת שנוצרה כדי לחבל במערכות השולטות ומבקרות תהליכים תעשייתיים, הסעירה את הקהילה הבינלאומית במגוון דרכים והזניקה את נושא הסייבר אל מרחב החששות של הציבור ואל ראש רשימת האיומים. התוצאה היא, שעוד ועוד מדינות רואות במתקפות סייבר את אחד האיומים הביטחוניים העתידיים המרכזיים, אם לא הגדול שבהם. באיזו מידה מוצדקת ראייה זו, ומה באמת שינתה תולעת הסטקסנט בשיח?

מטרתו של מאמר זה לתת תמונה מאוזנת של תופעת לוחמת הסייבר. אדגים כיצד ומדוע התפתחה לוחמת הסייבר מהתפיסה הצרה, הנוגעת אך ורק לאינטראקציה צבאית, למשמעותה הרחבה, שנעשתה מנותקת ממלחמה במובנה הפשוט ומקיפה כמעט כל פעילות הנוגעת לשימוש אגרסיבי במחשבים. בעיקר תיעשה במאמר זה הבחנה בין צורות שונות של עימות סייבר, שתשמש בסיס להערכת סיכונים מיושבת ושקולה. בהמשך יודגם כיצד השיח על איומי הסייבר מתאפיין, ככל הנראה, בפחות מדי שינוי וביותר מדי המשכיות מכפי שנוטים

ד"ר מרים דאן קוולטי עומדת בראש יחידת המחקר 'הסכנה החדשה' במכון ללימודי ביטחון, צריך, שוויץ.

להודות כיום. דימוי האיום נשאר יציב משלהי שנות התשעים של המאה ה־20, ותולעת הסטקסנט לא חוללה שינוי משמעותי במצב הזה. הדבר נכון גם בנוגע לאמצעי־נגד מתוכננים או חזויים.

הֶקשרים ומשמעויות של לוחמת סייבר

חשיבותו של המושג לוחמת סייבר והשפעתו ניתנים להבנה בצורה הטובה ביותר בהקשר הרחב של מהפכת המידע, שעיצבה – ועדיין מעצבת – את התפיסות בדבר הזדמנויות וסכנות. בייחוד דומה כי הטכנולוגיות של מהפכת המידע וחידושים ארגוניים נלווים בשנות השמונים והתשעים שינו את אופי העימות ואת סוגי המבנים, הדוקטרינות והאסטרטגיות הצבאיות. לפיכך נראה כי מושג זה מרמז על הופעתה של לוחמה מסוג "חדש", שבה גורם המידע נהפך בהדרגה לחשוב יותר ויותר. התפתחות זו התאפשרה (אם לא הונעה) מסיומה של המלחמה הקרה וההגדרות המחודשות שבאו בעקבותיה למונחים כמו אויבים, מחשבה אסטרטגית והוצאה על ביטחון.

מלחמת המפרץ הראשונה, בשנת 1991, יצרה קו פרשת מים בכל הנוגע לחשיבה צבאית על לוחמת סייבר. עימות זה נתפס בעיני אסטרטגים צבאיים (בעיקר אמריקנים) כעימות הראשון בדור חדש של עימותים, שבהם הניצחון איננו מובטח רק בכוח הזרוע, והוא גם פועל יוצא של היכולת לנצח במלחמת המידע ולהבטיח "דומיננטיות של מידע". בעקבות מלחמה זו פורסמו אינספור ספרים בנושא,[2] והתגובה להתפתחויות הטכנולוגיות אחרי מלחמת המפרץ מצאה ביטוי גם במאמרי דוקטרינה חדשים שמיסדו את מרכיב המידע.

תחילה התאפיין השיח באופוריה רבה. אבל זמן קצר אחר־כך ניתנה תשומת לב רבה יותר לסיכונים הכרוכים בהתפתחות זו: גיבוש אסטרטגיות שלא מוקדו עוד ביכולת האויב, אלא סימנו את "זרימת המידע של היריב", הדגישו את הפגיעות הגבוהה יחסית של כוחות אמריקניים מרושתים. עם התקדמות הדיון על התקפות על מערכות מידע עוינות אפשריות, נידונו בהרחבה גם הסכנות האפשריות לרשתות נתונים אזרחיות. ארצות־הברית, כמעצמת־העל היחידה שנותרה, נתפסה כמי שנועדה מראש להפוך למטרה ללוחמה א־סימטרית. חשש נרחב קנה לו אחיזה בקרב הקהילה האסטרטגית, ולפיו אלו הצפויים לנחול כישלון נגד מכונת המלחמה האמריקנית עלולים לתכנן לפגוע קשות בארצות־הברית באמצעות תקיפת נקודות חיוניות שלה מבית, דהיינו תשתיות חיוניות[3]. המושג תשתית חיונית מכיל מגזרים כמו מידע וטלקומוניקציה, שירותים פיננסיים, אנרגיה ותשתיות, תחבורה ועוד רכיבים המשתנים ממדינה למדינה ובמהלך הזמן.[4] רוב המגזרים הללו מסתמכים על מרחב שלם של מערכות בקרה מבוססות תוכנה לפעולתם החלקה, האמינה והרציפה.

עם גידולן של רשתות מחשב והתרחבותן לעוד ועוד היבטים של חיי היומיום, השתנתה מטרת ההגנה ממה שנתפס כרשתות קנייניות מוגבלות (ממשלתיות, בעיקר צבאיות), אל החברה בכללותה – או ליתר דיוק, אל דרך החיים שלה, המתאפשרת באמצעות תת־המבנה הבלתי מופרע של הטכנולוגיה.[5] על בסיס זה התפתח איום הכולל שני צדדים הקשורים בקשר גומלין זה לזה. ראשית, פרספקטיבה פנימית, ולפיה עצם הקישוריות של מערכות תשתית מציבה סכנות מכיוון שהפרעות בתוכן עלולות להתפתח לאסונות גדולים במהירות רבה. חידושים בטכנולוגיית מידע ותקשורת הגבירו אפוא את הפוטנציאל לאסון של ממש בתשתיות חיוניות באמצעות הגדלה ניכרת באפשרות שסיכונים מקומיים יהפכו לסיכונים מערכתיים. שנית, פרספקטיבה עם מבט כלפי חוץ מתמקדת בהגברת הנכונות של שחקנים זדוניים לנצל נקודות תורפה בלא היסוס או מגבלות. מאחר שמערכות תשתית חיוניות משלבות ערכים סמליים ואינסטרומנטליים, התקפתן הופכת לחלק חשוב בהיגיון המודרני של השמדה, המבקשת להשיג השפעה מרבית.

ממד הסייבר גם מעצב מחדש את המרחב למשהו שאינו נטוע עוד במקום או בנוכחות. "האויב" הופך לישות מרוחקת ונטולת פנים, נעלם גדול שכמעט בלתי אפשרי לאתרו. מצב זה מוביל לשני מאפיינים חשובים של ייצוג האיום: ראשית, יכולת ההגנה על מרחב מתבטלת – אין מקום מוגן מפני התקפה או מפני התמוטטות קטסטרופלית. שנית, האיום הופך אוניברסלי כביכול משום שהוא נמצא כעת בכל מקום.

הפנומנולוגיה של הסייבר

לאור האמור לעיל, אין זה מפתיע לגלות, כי החשש מפני איומי סייבר הוא גדול כל כך. אך כל משקיף יוכל להיווכח עד כמה האיומים הם בלתי מוגדרים. לאחר שחרג מגבולותיו הצבאיים, הפך המושג מטושטש מאוד: לוחמת סייבר מתייחסת כעת לכל תופעה הכרוכה בשימוש הרסני או משבש בצורה מכוונת את עבודת המחשבים.

ערפול קונספטואלי שכזה מקשה עלינו להבין מה קורה בעימותים "סייבריים",[6] ואילו סוגים של אמצעי־נגד נדרשים להתמודדות עם אירוע ספציפי. ברוס שנייר (Bruce Schneier), טכנולוג אבטחה ומחבר בעל שם בינלאומי, מבחין בין סייבר־ונדליזם (cybervandalism), כלומר השחתה של אתר אינטרנט; סייבר־פשע (cybercrime), תופעה של גנֵבת קניין רוחני, סחיטה המבוססת על איום בתקיפה מסוג מתקפה מבוזרת למניעת שירות (DDoS), מרמה המבוססת על גנבת זהות וכיוצא באלה; סייבר־טרור (cyberterrorism), פריצה למערכת מחשב כדי לגרום להתכת כור גרעיני, לפתיחת סכר, או כדי לגרום להתנגשות בין שני מטוסים; ולוחמת סייבר (cyberwar).[7] שנייר משתמש במונח לוחמת סייבר במובן של

שימוש במחשבים לשיבוש פעילויות של מדינת אויב, ובייחוד התקפות המכוונות על מערכות תקשורת.

הסיווג של שנייר בונה מערך של איומי סייבר מתעצמים ומסלימים – משלב אחד בסולם לזה שבא אחריו, ההשפעות האפשריות וכן ההיקף והעוצמה מסלימים. בשנים האחרונות נוכחנו לגלות כי סייבר־ריגול (cyberespionage) וסייבר־חבלה (cybersabotage) נעדרים מהסולם. עם זאת יצוין, שקווי הגבול בין הפעילויות השונות מטושטשים מאוד. כאשר מתרחש אירוע שגרם נזק, קשה לקבוע אם הנזק הוא תוצאה של התקפה זדונית, פגם ברכיב מסוים או תאונה. על אף המטרות השונות, הכלים והטקטיקות המשמשים צבאות, ארגוני טרור ועבריינים במרחב הסייבר – דומים מאוד, אם לא זהים. פירוש הדבר, במקרה של התרחשות התקפה, קשה מאוד לזהות מי עומד מאחוריה ובאיזה סוג של תופעה מדובר.

יודגש שוב, הקושי בהבחנה בין התופעות השונות אין משמעו שההבחנה איננה נחוצה; ההפך הוא הנכון. **ראשית**, היתרון בתפיסה של "חומרת ההשפעות" שהיא מסייעת לקובעי מדיניות לתעדף בתיאוריה – דבר חשוב ביותר. רק התקפות מחשב שתוצאותיהן הרסניות או גורמות שיבושים חמורים צריכות להיחשב סוגיה של ביטחון לאומי, ולפיכך מחייבות תשומת לב הניתנת לאירועים שמהווים איום קיומי. מתקפות הגורמות לשיבוש של שירותים לא חיוניים, או שהן בעיקר מטרד יקר, אינן נכללות בקטגוריה זאת.[8] **שנית**, הגדרה צרה ומדויקת מסייעת לעקוף סכנות אחרות הטמונות בתיוג אירוע מסוים כ"מלחמה", למשל לפטור קורבנות של התקפה מאחריותם להשלכות הנובעות מרשלנותם שלהם בכל הנוגע לאבטחת מחשב או יצירת לחץ להשיב מלחמה נגד "פורצי מחשבים", אמיתיים או מדומים.[9] **שלישית**, הגדרת התופעות מדגימה בבירור היכן מרכז הכובד – בחקירות מחשב קפדניות. יש לחקור כל אירוע בקפדנות. כפי שמציין שנייר: "בדיוק כשם שכל מקרה של ירי אינו בהכרח פעולה מלחמתית, כך כל מתקפת אינטרנט מוצלחת, בלי קשר למידת חומרתה, אינה בהכרח פעולה של לוחמת סייבר. מתקפת סייבר המשתקת את רשת החשמל עשויה להיות חלק ממערכה של לוחמת סייבר, אך היא גם עשויה להיות פעולה של סייבר־טרור, סייבר־פשע או אפילו – אם היא מבוצעת בידי נער בן ארבע־עשרה שלא מבין באמת מה הוא עושה – סייבר־ונדליזם. הסיווג הספציפי מותנה במניעים של מחולל המתקפה ובנסיבות ההתקפה [...] בדיוק כמו בעולם האמיתי".[10]

הערכת סיכונים

הדברים לעיל מעלים את השאלה: עד כמה נמצאים אנו במצב של סכנה? עימותים במרחב המדומה הם בבחינת מציאות זה יותר מעשור – בכל עימות פוליטי, כלכלי וצבאי יש היבטים המתרחשים בתוך האינטרנט וסביבו. יתרה מכך, פעילויות

פליליות ופעילויות ריגול בעזרת טכנולוגיות מידע ותקשורת מתרחשות בכל יום. אך בכל ההיסטוריה של רשתות מחשבים, היו רק דוגמאות בודדות להתקפות חמורות שהיה להן הפוטנציאל לשבש או אף שיבשו בפועל – בצורה חמורה – פעילויות של מדינה. בודדות יותר הדוגמאות למתקפות סייבר שגרמו לאלימות פיזית נגד בני אדם או רכוש. הרוב המכריע של התקפות הסייבר הן מדרגה נמוכה וגורמות אי־נוחות, ולאו דווקא לשיבוש חמור או לשיבוש לטווח ארוך. למעשה ברור כיום, כי הסבירות להתרחשותה של לוחמת סייבר "טהורה" (או אסטרטגית) נמוכה ביותר, וסבירות גבוהה יותר מיוחסת למתקפות על מערכות מחשבים בשיתוף עם צורות התקפה אחרות, פיזיות.[11]

האם הערכה זו השתנתה בשנה החולפת? סיווג התולעת סטקסנט אכן מהווה אתגר. מסתובבים אלפי סיפורים והשערות על התולעת, על מקורותיה ועל כוונותיה.[12] סיפורים כתובים ברמה זו או אחרת, וכולם מכילים חלקי תצרף (פאזל) שאינם ניתנים לחיבור מלא ושלם. חלקי התצרף מרמזים על כך שרק למדינה אחת או לכמה מדינות – ההיגיון הרגיל של "מי צפוי להרוויח" מצביע על ארצות־הברית או על ישראל – היו היכולת והאינטרס לייצר ולשחרר את תולעת הסטקסנט כדי לחבל בתוכנית הגרעין של איראן. אף־על־פי שהעולם לא יידע כנראה לעולם לבטח מי עומד מאחורי קוד התוכנה הזה, מרבית המתכננים האסטרטגיים נכונים להאמין כי "מהלומה דיגיטלית ראשונה" התרחשה, ותיבת פנדורה הווירטואלית נפתחה.

עם זאת, גם אם נניח את התרחיש הקיצוני ביותר, ולפיו רוב המדינות בעולם פיתחו נשק סייבר יעיל ורב עוצמה, או יצליחו לפתח נשק מסוג זה בעתיד הקרוב (הנחה המוטלת בספק), עצם קיומן וזמינותן של יכולות כגון אלה אין פירושו שייעשה בהן בהכרח שימוש. נראה כי תחום הסייבר מוביל בני אדם להניח, כי מאחר שיש להם נקודות תורפה הן בהכרח ינוצלו. בכל זאת, בנושאי אבטחה וביטחון יש לבצע הערכת איומים קפדנית. הערכה כזאת מצריכה העמקה יסודית בשאלה: "למי יש האינטרס והיכולת לתקוף אותנו, ומה הוא צפוי להרוויח מכך?" בעבור מדינות דמוקרטיות רבות, הסיכון של מלחמה נדחק לשוליים. הסיכון של מתקפת סייבר בהיקפים החמורים ביותר צריך להישקל באותה הרצינות.

התרת אפקט תולעת ה'סטקסנט'

פרסום הקוד של תולעת הסטקסנט ופרטים רבים נוספים כבר הובילו להתקפות של מערכות מחשבים רבות נוספות. לפיכך מערכות SCADA – מערכות מחשב המנטרות ומפקחות על תהליכים תעשייתיים ותשתיתיים – צפויות לשמש מטרה לכל פורץ מחשבים בעתיד הנראה לעין. למצב זה נלווית סכנה אינהרנטית של תופעות מכוונות ולא מכוונות – אם כי חשוב לציין כי השיח בנושא תשתיות

חיוניות עוסק באיום על מערכות ה־SCADA זה יותר מעשור. כמו כן, מזה זמן רב מצפים מומחים לאירוע בסדר גודל רציני במרחב הסייבר. מנקודת מבט זו, תולעת הסטקסנט איננה הפתעה גדולה, אלא דווקא אישור למה שדנו בו וחששו מפניו במשך שנים. אף־על־פי שהיא מיקדה את תודעת הפוליטיקאים בשלבים היותר חמורים של איומי הסייבר, באופן זמני לפחות אין היא משנה את הסבירות להתרחשות אירוע של סייבר־טרור או לוחמת סייבר.

תולעת הסטקסנט גם אינה משנה את השיטות והכלים הזמינים להתמודדות עם איומי סייבר. הכוונה למשל לאמצעי אבטחת מידע, או לפעילויות המגוונות והרבות, המושגים והתהליכים הנכללים ב"הגנה על תשתיות חיוניות" (CIP). ההתייחסות ל־CIP דומה למדי במדינות רבות:[13] מבוקשות שותפויות הדוקות עם המגזר העסקי ועם שותפים בינלאומיים, בעיקר כדי להחליף מידע בנוגע לאיומים שונים ולמגוון סוגיות. לאחרונה גם ניכרת התרחקות מהמושג "הגנה", ומעבר לשימוש במושג "גמישות".[14] גמישות איננה מושג חדש כמובן, אך עלייתו הנוכחית מלמדת על שינוי חשוב בחשיבה. בעוד אמצעי הגנה נועדו למנוע התרחשות של שיבושים, הגמישות מקבלת את העובדה ששיבושים מסוימים הם בלתי נמנעים.

לחשיבה כזאת נודעת חשיבות רבה, ועליה להיות מושרשת בתודעת הפוליטיקאים ובתודעת כלל האוכלוסייה. רשתות מידע לעולם אינן יכולות להיות "מוגנות" מן ההיבט של הביטחון הלאומי. ההפך הוא הנכון: שומה על תקריות סייבר להתרחש, מכיוון שאין דרך להימנע מהן. במילים אחרות: אפילו ההגנות המושלמות ביותר לא יוכלו להבטיח ששום דבר חמור לא יתרחש בעולם המרושת.

מדינות נוטות להגיב בכוח לאתגר כזה ומנסות להגביר את רמת הביטחון בכל האמצעים. אך אין לטעות ולראות במרחב הסייבר עוד "תחום" שאפשר לנקוט בו פעולה צבאית לפי שיקול דעת. כדי שיהיה אפשר להמשיך ליהנות מיתרונותיו של עידן הסייבר, חשוב ללמוד באופן מעשי איך לחיות עם חוסר ביטחון. מלבד מגבלות משפטיות ואסטרטגיות, שיובאו ודאי בחשבון בכל התלבטות אם להשתמש במתקפות סייבר ככלי נשק אם לאו, המכשולים הגדולים ביותר צריכים להיות חששות מפני השלכות שליליות שאינן ניתנות לשליטה. ראשית, השלכות עלולות להיווצר ישירות עקב התלות ההדדית בין משאבים חיוניים שונים. שנית, השלכות שליליות עלולות להיות מורגשות באמצעות ההשפעה של אמון מעורער במרחב הקיברנטי, מה שיגרום להשלכות מזיקות לכלכלה העולמית.[15]

באמצעות העברת סוגיה מסוימת, במשתמע או במפורש, לתחום של ביטחון לאומי ופעולות צבאיות, נוטים להכפיף אותה לכללי משחק סכום אפס, שבהם הרווח של צד אחד הוא ההפסד של הצד האחר. עם זאת, ההיגיון של מרחב הסייבר הוא אחר. בדומה לפיקוח על החלל והימים, הפיקוח של מרחב הסייבר מחייב נורמות עולמיות מוסכמות. הדרכים הזמינות כיום ל"בקרת נשק" בזירה זו הן בעיקר

חילופי מידע וגיבוש נורמות, בעוד הניסיונות לאסור לחלוטין את האמצעים של לוחמת סייבר, או להגביל את הזמינות של נשק־סייבר צפויים להיכשל. הקשיים לא צריכים למנוע מהקהילה הבינלאומית לאמץ מגבלות אחראיות וריסון עצמי בשימוש בנשק הסייבר, ולחשוב על דרכים חדשות וחדשניות לשפר את ההגנה על רשתות מחשב חיוניות בלי להפריע ליכולתו של הציבור לחיות ולעבוד בביטחון באינטרנט.

הערות

1 John Arquilla and David F. Ronfeldt, "Cyberwar is Coming!", *comparative Strategy* vol. 12, no. 2 (1993), pp. 141-165.

2 Greg Rattray, *Strategic Warfare in Cyberspace*, Cambridge 2001; Michael O'Hanlon, *Technological Change and the Future Warfare*, Washington 1999.

3 Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*, London 2008.

4 Elgin Brunner and Manuel Suter, International CIIP Handbook 2008/2009, Zurich: Center for Security Studies, 2009.

5 Myriam Dunn Cavelty, "Cyber-Security", in Peter Burgess (ed.), *Routledge Handbook of New Security Studies*, London 2010, pp. 154-162.

6 Chris Demchak, "Cybered Conflicts as a New Frontier", *Atlantic Council*, October 28, 2010, http://www.acs.org/new_atlanticist/Cybered-conflict-new-frontier

7 Bruce Schneier, "Schneier on Security: A Blog Covering Security and Security Technology," Post: "cyberwar," June 4, 2007, http://www.schneier.com/blog/archives/2007/06/cyberwar.html

8 Cf. Clay Wilson, *Computer Attack and Cyber-terrorism: Vulnerabilities and Policy Issues for Congress, Congressional Research Report for Congress*, Washington 2003; Dorothy Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," in John Arquilla and David F. Ronfeldt (eds.), *Networks and Netwars: The Future of Terror, Crime and Militancy*, Santa Monica 2001, pp. 239-288.

9 Martin Libicki, *Defending Cyberspace and Other Metaphors*, Washington 1997, p. 38.

10 Schneier, http://www.schneier.com/blog/archives/2007/06/cyberwar.html

11 Peter Sommer and Ian Sommer, "Reducing Systemic Cybersecurity Risk, OECD/IFP Project on Future Global Shocks, 2011," www.oecd.org/dataoecd/3/42/46894657.pdf

12 שתי דוגמאות בולטות הן:
Mark Clayton, Stuxnet malware is 'weapon' out to destroy ... Iran's Bushehr nuclear plant? September 21, 2010, http://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant; William J. Broad, John Markoff and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, January 15, 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

13 Myriam Dunn Cavelty and Manuel Suter, "Public-Private Partnerships are no Silver

Bulled: An Expanded Governance Model for Critical infrastructure Protection", *International Journal of Critical Infrastructure Protection* Vol. 2, No. 4 (2009), pp. 179-187.

14 Christine Pommerening, "Resilience in Organizations and Systems: Background and Trajectories of an Emerging Paradigm", in *Critical Thinking: Moving from infrastructure Protection to infrastructure Resilience*, *CIP Program Discussion Papers Series*, (Washington 2007), pp. 9-22.

15 Andrew Rathmell, "Controlling computer Network Operations", *Information & Security: An International Journal* 7 (2001), pp. 121-144.