מבט על, גיליון 858, 27 בספטמבר 2017

מלחמת המעצמות בסייבר והבחירות בארצות הברית

גבי סיבוני ודודי סימן-טוב

בסוף יולי 2016 וסמוך לפתיחת ועידת המפלגה הדמוקרטית לקראת הבחירות לנשיאות בארצות הברית, פורסמו באתר "ויקיליקס" מיילים מביכים מחשבונותיהם של בכירים במטה המפלגה. הפורצים הצליחו להשיג גישה מלאה לרשת מטה הבחירות של הוועידה הדמוקרטית הלאומית, הכוללת דוא"ל, מזכרים ומחקרים שנעשו עבור מועמדים דמוקרטים לקונגרס. ההערכה הייתה שהפורצים היו מרוסיה. בראיון שהעניקה המועמדת הדמוקרטית לנשיאות הילרי קלינטון לרשת "פוקס" היא האשימה את שירותי הביון הרוסיים בפריצה למחשבי הוועידה הדמוקרטית ובפרסום הדוא"ל וציינה כי יש דיווחים אמינים אשר להתערבות רוסית, שנועדה לשבש את הבחירות. הנחת העבודה של גורמי האכיפה בארצות הברית הינה שאכן האקרים רוסיים פרצו לרשת המחשבים המשמשת את מטה הוועידה הדמוקרטית כחלק ממתקפת סייבר על גופים של המפלגה הדמוקרטית. היחידה לביטחון לאומי במשרד המשפטים האמריקאי חוקרת באיזו מידה מתקפות הסייבר האלה מעידות על מעורבות ממשית של רוסיה במערכת הבחירות לנשיאות.

בהקשר דומה, מנהיג המיעוט הדמוקרטי בסנאט, הארי ריד מנבאדה, הזהיר מפני ניסיונות של האקרים רוסים לזייף את תוצאות הבחירות לנשיאות. הוא קרא ל-FBI לחקור אפשרות שהאקרים זרים חדרו בשבועות האחרונים למאגרי הנתונים של ועדות הבחירות המרכזיות של מדינת אילינוי וניסו לחדור למאגרים של אריזונה. ההערכה היא שבמסגרת חדירות אלה נגנבו כמאתיים אלף רשומות של בוחרים. החששות מתמקדים באפשרות של מחיקת מאגרים הכוללים שמות מצביעים או ניסיון אחר לפגוע באמינות הבחירות. ריד הזהיר מפני התערבות רוסית בהליך ההצבעה באופן "רחב יותר ממה שידוע ועשוי להיות מכוון גם לזיוף תוצאות ההצבעה הרשמיות". לדבריו, בכירי מודיעין אמריקאים התריעו בתדרוכים אחרונים שקיימו כי נשיא רוסיה ולדימיר פוטין שואף לחבל בהליך הבחירות. בעקבות החששות הללו הציע השר לביטחון פנים של ארצות הברית לנציגי ועדות הבחירות את עזרת הממשל הפדראלי באבטחת מערכות המחשב שלהן.

מיד לאחר פרסום דבר התקיפה של מטה המפלגה הדמוקרטית חשפה חברת קספרסקי מערך ריגול קיברנטי מתקדם ורחב היקף – המכונה Project Sayron — ברוסיה. מוערך כי מערך זה פועל ברוסיה זה מספר שנים, אך עיתוי חשיפתו אינו מקרי ומלמד שגם ארצות הברית פועלת במרחב הסייבר הרוסי. הרוסים משייכים את התקיפה לארצות הברית ושרות ביטחון הפנים של רוסיה – ה-FSB – ציין כי התקיפה התבצעה גם נגד גופים ביטחוניים. ניתן להניח, שגם פרסום דבר הפריצה וגניבת נוזקות סודיות מה-NSA קשורים למאבק הזה בין האמריקאים לרוסים. חיזוק לכך ניתן לאחר שאדוארד סנודן, המקבל מקלט ברוסיה ואף יתכן שהוא מופעל על ידה, פרסם הערכה שלפיה רוסיה עומדת מאחורי הפריצה הזו.

ההסלמה הקיברנטית בין רוסיה לארצות הברית באה על רקע פעילות סייבר התקפית רוסית בסוריה ובאוקראינה וככל הנראה במדינות נוספות במזרח אירופה. ניתן להניח, שתקיפות אלה נועדות לשדר עוצמה ויכולת טכנולוגית רוסית, בעיקר לצרכי הרתעה. כן ניתן לשער שהתקיפות בארצות הברית באות על רקע דומה ותכליתן לנצל את הבחירות כהזדמנות לזכות את היכולות הרוסיות בחשיפה רחבה.

התקיפות בארצות הברית מהוות חידוש במספר הקשרים: הראשון הינו ההבנה, שמערכת בחירות במדינה דמוקרטית מהווה תשתית לאומית קריטית, ולכן יש לפעול כדי להגן עליה. אפשרויות הפעולה בסייבר רבות ומגוונות: החל בשיבוש הצבעות מקוונות וכלה בזיוף התוצאות עצמן. במעגל שני, גם זיוף של סקרים או מניפולציה בהודעות לבוחר עלולים לגרום שיבוש מערכתי של הבחירות, באופן שיעלה בקנה אחד עם האינטרס של התוקף – מתוך המדינה, ממפלגה יריבה, או ממדינה אחרת.

ואכן, באחרונה נשמעו בארצות הברית קולות הדוחקים בממשל להבהיר לרוסיה כי התקפה מצדה על ההליך הדמוקרטי תזכה לתגובה הולמת, ושזו לא תהיה מוגבלת בהכרח למרחב

הסייבר. האירועים המדוברים אף ממחישים ומגבירים את הצורך לפתח נורמות בינלאומית, שיצמצמו את אפשרויות הפגיעה הקיברנטית במערכות בחירות. בראשית שנות האלפיים הייתה ישראל חלוצה בהקשר זה, כשהגדירה – לצרכי הגנה – תשתיות קריטיות לתפקודה של המדינה, וביניהן מערכות חשמל, אנרגיה ותקשורת. בהמשך נוספו לרשימה מערכות כספים (בנקאות ומסחר אלקטרוני). מערכת בחירות הינה תשתית קריטית מסוג חדש – היא מהווה "בטן רכה" האופיינית רק למדינות הדמוקרטיות. ניתן לפגוע בה במגוון דרכים, החל משיבוש נקודתי של הצבעה עד שיבוש מערכתי, שעלול לכרסם באמון הבוחרים בנבחריהם ובאמינות השיטה הדמוקרטית עצמה. שיבוש של מערכת בחירות יכול להתמקד ביום הבחירות, המהווה נקודת תורפה ראשית, וכן יכול להתפרס על פני חודשים, שבמהלכם ניתן לשבשה באמצעות מניפולציות על בחירות מקדימות, זיוף סקרים, ולוחמה פסיכולוגית בתקשורת. באירועים המדוברים הומחשה תעוזה רוסית מול תגובתיות אמריקנית, ונראה שטרם נאמרה המילה האחרונה בהתגוששות זו (רבים מייחסים לרוסיה אינטרס שהמועמד הרפובליקאי ייבחר).

עניין שני שנחשף, לצד בניית יכולות התקפיות חשאיות של מדינות במרחב הסייבר, הוא החשיפה המכוונת של נכסים נצורים במרחב הסייבר בעיתוי רלוונטי. כלומר, אם בעבר ניתן היה לחשוב כי התוקף הקיברנטי עושה זאת בעיקר לשם איסוף וריגול או לשם שיבוש תפקוד של מערכות ותהליכים קריטיים בעת הצורך, מתחוורת תופעה של צבירת נכסים ופרסומם בעיתוי שנראה לתוקף רלוונטי לטובת קידום האינטרסים שלו. זאת, גם במחיר של אובדן אותם נכסים. מכאן עולה גם הקשר ההדוק בין לוחמת הסייבר לתחום התודעה והלוחמה הפסיכולוגית. ניתן לראות כי התוקפים הרוסיים – או לפחות תוקפים בעלי זיקה לרוסיה – אינם חוששים לאבד נכסים קיברנטיים, ובלבד שיוכלו לקדם אינטרס שלהם. יצוין כי חשיפה יזומה של נכסים קיברנטיים מנוגדת לטבען של קהילות מודיעין מערביות, אשר מעדיפות בדרך כלל פעולה במישור החשאי.

היבט נוסף נוגע לרלוונטיות של מלחמת הסייבר לשגרת היחסים בין המעצמות, לא רק למלחמה "קונבנציונלית". דומה שאנו עדים למלחמה קיברנטית מסוג חדש, המתנהלת מתחת לסף הידיעה הציבורי כשלא תמיד מי עומד מאחורי המהלכים. ההשפעה של פגיעה בהליך הדמוקרטי, בין היתר באמצעות חשיפה מגמתית של חומרים העלולים להשפיע על ההצבעה של קהלי יעד, למשל, היא פעולה בעלת משמעויות אסטרטגיות רחבות ביותר. כנראה שעל רקע המתחים בין רוסיה לארצות הברית, ואפשר שגם בין מדינות אחרות, כבר מתנהלת בפועל מלחמה קיברנטית, שהציבור אינו מודע לה. כן אפשר שזו רק שאלה של זמן עד שהמלחמה הקיברנטית תוגדר כ"מלחמה" ותאתגר את ההגדרות המקובלות של המושגים: שגרה, חרום ומלחמה.

דומה שאנו עדים למלחמה קיברנטית מסוג חדש, המתנהלת מתחת לסף הידיעה הציבורי כשלא תמיד ברור מי עומד מאחורי המהלכים. ההשפעה של פגיעה בהליך הדמוקרטי, בין היתר באמצעות חשיפה מגמתית של חומרים העלולים להשפיע על ההצבעה של קהלי יעד, למשל, היא פעולה בעלת משמעויות אסטרטגיות רחבות ביותר.