איומים קיברנטיים על תהליכים דמוקרטיים

דודי סימן טוב, גבי סיבוני, גבריאל אראל

המעורבות המיוחסת לרוסיה בבחירות לנשיאות בארצות הברית ובצרפת מעלה שאלות באשר לצורך וליכולת של מדינות דמוקרטיות להגן על תהליך הבחירות שלהן. מאמר זה מצביע על החשיבות שיש לייחס לבחירות במדינה דמוקרטית כתשתית וכתהליך קריטיים ומציג את האיומים עליהן הנובעים מהתפתחויות קיברנטיות ותרבותיות. המאמר מציף את התובנה לפיה השימוש הנרחב ברשתות חברתיות ובערוצי תקשורת ישירים מאפשר לגורמים זרים להשפיע בצורה משמעותית על ההליך הדמוקרטי, וזאת לא על ידי השבתה של מערכות ההצבעה אלא באמצעות השפעה זרה על השיח הפוליטי. הדבר מהווה אתגר חדש למדינות דמוקרטיות, המחייב התארגנות וחשיבה חדשות.

מילות מפתח: בחירות, סייבר, הגנת סייבר, תשתית קריטית, רשתות חברתיות, חתרנות מדינית.

מבוא

ערכי היסוד של מדינות דמוקרטיות הם חירות, שוויון, השתתפות וזכויות אזרח. אחד המאפיינים המרכזיים של המדינה הדמוקרטית הינו קיומן של בחירות כלליות, חופשיות, חוזרות ונשנות במרווחי זמן הנקבעים בחוק. בחירות הן שיאו של ההליך הדמוקרטי ומהוות מרכיב מרכזי בבניית אמון הציבור במדינה ואמון האזרחים במוסדותיה.

בשנים האחרונות אנו עדים לניסיונות התערבות חיצונית ולפגיעה בהליכי הבחירות במדינות דמוקרטיות רבות בעולם באמצעות תקיפות קיברנטיות. את האיומים הקיברנטיים על הליך הבחירות במדינות דמוקרטיות ניתן לסווג לאיומים שמטרתם לשבש את ההליך עצמו באמצעות כלים טכנולוגיים שנועדו לפגוע

דודי סימן טוב הינו חוקר במכון למחקרי ביטחון לאומי. ד"ר גבי סיבוני הינו חוקר בכיר במכון למחקרי ביטחון לאומי ועומד בראש תוכנית ביטחון הסייבר שם. גבריאל אראל היא עוזרת מחקר במכון למחקרי ביטחון לאומי. המחברים מבקשים להודות לאל"ם ג' על תרומתו למאמר זה.

במערכות מידע ובמערכות הסיקור וההצבעה, ולאיומים מהותיים על המוסדות הדמוקרטיים בכללותם באמצעות פגיעה בשמם הטוב ובאמון הציבור בהם. בעוד שהאיום הראשון מוכר ומדינות נערכות היטב מולו, האיום השני, המופשט יותר, הינו חדש ומחייב חשיבה הולמת.

דו"ח של קהילת המודיעין האמריקאית, שהוגש לנשיא ארצות הברית בינואר 2017, מעריך כי רוסיה ניהלה קמפיין נרחב לערעור סיכוייה של המועמדת לנשיאות הילרי קלינטון ולקידום המועמד דונלד טראמפ, ועשתה זאת הן על ידי תקיפות סייבר חשאיות והן באמצעות מאמצי השפעה גלויים. להערכת קהילת המודיעין של ארצות הברית, גורמי סייבר של רוסיה פרצו למחשבי המפלגה הדמוקרטית האמריקאית כבר ביולי 2015 ועשו שימוש במידע שנאסף במסגרת פריצה זו.[1] מקרה זה מצטרף לדיווחים נוספים על חשד לחדירות קיברנטיות של רוסיה לגופי ממשל גם באירופה ולשיבוש מערכות בחירות שם.[2] רוסיה נחשדה בניסיון כושל להתערבות בבחירות לנשיאות בצרפת, שמטרתה הייתה לשבש את בחירתו של עמנואל מקרון, וזאת באמצעות פרסום ברשת של מידע שנגנב ממטה הבחירות שלו (שייתכן וחלקו היה מזויף).[3]

מקרה אחר של התערבות במערכות בחירות זרות הוא חשיפה של גורמים שעמדו מאחורי הטיית הבחירות במספר מדינות בדרום אמריקה. אנדֶרֶס סֶפּוּלְוֶדָה, שעמד לדבריו בראש צוות האקרים שפעלו בעשור האחרון במטרה להטות תוצאות בחירות במספר מדינות בדרום אמריקה, כמו למשל במקסיקו, סיפר כי צוות ההאקרים שלו התקין תוכנות ריגול במחשבים של יריבים, גנב אסטרטגיות של מערכות בחירות ותמרן את המדיה החברתית במטרה ליצור אווירה של התלהבות או של בוז ולגלוג.[4]

השוני בין שני המקרים שתוארו לעיל הינו ברור: מאחורי המקרה הראשון עומדת כנראה מעצמה, שניסתה להשפיע על תוצאות הבחירות לנשיאות בארצות הברית ובצרפת. במקרה השני עומדים גורמים פרטיים, שגויסו למהלך על ידי יריבים פוליטיים.

---

1 "Background to Assessing Russian Activities and Intentions in Recent US Elections: The Analytic Process and Cyber Incident Attribution", *Intelligence Community Assessment, ODNI*, January 6, 2017.

2 "לא רק ארה"ב: רוסיה מתערבת גם בבחירות באירופה", **YNET**, 10 בדצמבר 2016.

3 Eric Auchard and Felix Bate, "French Candidate Macron Claims Massive Hack as Emails Leaked", *Reuters*, May 6, 2017.

4 Jordan Robertson, Michael Riley, Andrew Willis, "How to Hack an Election", *Bloomberg*, March 31, 2016, https://www.bloomberg.com/features/2016-how-to-hack-an-election.

מאמר זה מתמקד באיום של התערבות מהסוג הראשון, אותו אנו מגדירים "חתרנות מדינית קיברנטית אסטרטגית". המאמר עוסק בנקודות התורפה של תהליך הבחירות במדינה דמוקרטית, המאפשרות התערבות זרה, ועושה זאת באמצעות ניתוח מרכיבי התהליך וחולשותיהם מול אפשרות של פגיעה קיברנטית. כמו כן מציג המאמר את הבחירות כתהליך קריטי ששיבוש שלו עלול לערער את היציבות הדמוקרטית ואת אמון הציבור במוסדות הדמוקרטיים ככלל.

בין תשתיות קריטיות לתהליכים קיברנטיים חיוניים

בראייה האמריקאית, תשתיות קריטיות הינן מערכות חיוניות, המהוות את הבסיס של החברה האמריקאית ותומכות בביטחונה, בכלכלתה ובמערכות הבריאות שלה. הגדרה זו מתייחסת ל־16 קטגוריות של מערכות וסוכנויות, שהממשל האמריקאי אחראי להבטיח את ביטחונן הפיזי והקיברנטי. קטגוריות אלו הן: התעשייה הכימית, הכוללת תעשיות רוקחות, כימיקלים לחקלאות וכימיקלים מיוחדים; תשתיות מסחר; תקשורת; תעשיות ייצור, כגון תעשיית המתכת; אנרגיה; סכרים; תעשיות ביטחוניות לייצור ותחזוקה של אמצעי לחימה ומערכות צבאיות; שירותי חירום; תשתיות פיננסיות; מגזר המזון והחקלאות; תשתיות ממשל; מערכות בריאות; מערכות מידע; תשתיות גרעיניות; תשתיות תחבורה; תשתיות מים.[5]

בישראל, תשתית חיונית להגנה קיברנטית היא תשתית ציבורית, בין אם היא נמצאת בבעלות ממשלתית ובין אם היא בבעלות פרטית, וההגנה עליה מחייבת הגנה פיזית, אבטחת מידע ואבטחת מערכות המחשוב שלה.[6] תשתית מוגדרת כקריטית כאשר פגיעה בה עלולה להוביל לנזק כלכלי־חברתי שיש לו פוטנציאל לערעור היציבות הכלכלית, החברתית או הביטחונית של המדינה. תשתיות קריטיות מורכבות לרוב משלושה מאפיינים עיקריים: משקלן הסמלי; התלות התפקודית של המדינה בהן, שכתוצאה ממנה כל פגיעה בהן עלולה להוביל לנזק מתמשך ולפגיעה בחיי אדם או לנזק כלכלי משמעותי; קשרי הגומלין עם תשתיות אחרות.[7] אל התשתיות הקריטיות המסורתיות (מערכות החשמל, התקשורת, הרכבות, צנרת הולכת המים והדלק, התעופה וכדומה) התווספו בשנים האחרונות תשתיות נוספות, כגון ספקיות אינטרנט וחלק מהמגזר הפיננסי. ההחלטה אם להגדיר תשתית כקריטית היא של ועדה בראשות ראש מטה הסייבר הלאומי וכרוכה בשינויי חקיקה. תשתית קריטית חייבת לעמוד ברגולציה לאומית להגנה בסייבר.

---

5 ההגדרה נלקחה מתוך אתר המשרד להגנת המולדת של ארצות הברית: https://www.dhs.gov/critical-infrastructure-sectors.

6 רועי גולדשמידט, "המרחב הקיברנטי וההגנה על תשתיות קריטיות", *הכנסת, מרכז המחקר והמידע*, 2013.

7 ליאור טבנסקי, "הגנה על תשתיות קריטיות מפני איום קיברנטי", **צבא ואסטרטגיה**, כרך 3 גיליון 2, נובמבר 2011.

הרגולציה נעשית באמצעות הנחיית גופי התשתית הקריטית על ידי ה"רשות לאבטחת מידע" (רא"ם) בשב"כ. חלק נרחב מסמכות ההנחיה של רא"ם נמצא בתהליך מעבָר ל"רשות הלאומית להגנת סייבר". שירותים ציבוריים אחרים, כגון חינוך, בריאות ומשפט, וגם מערכת הבחירות בישראל, אינם מוגדרים כתשתיות קריטיות המחויבות בהכוונה והנחיה של הגופים המוסמכים. יחד עם זאת, ועדת הבחירות המרכזית בישראל מקבלת הנחיה מרשות הסייבר הלאומית.

בארצות הברית נשמעו באחרונה קריאות לעדכון ההגדרה של תשתיות קריטיות ודרישות לכלול בתוכה גופים ותהליכים נוספים הפגיעים לתקיפות קיברנטיות, כגון מערכות בחירות וגופי מחקר ואקדמיה. קריאות אלו מתבססות על העלייה החדה בשימוש באינטרנט ובמערכות ממוחשבות בכלל המגזרים (ציבורי, עסקי, ממשלתי, פרטי, תשתיות ואקדמיה), המחייבת הגדרה מחדש של התשתיות. זאת, לאור הרגישות של מערכות מורכבות המבוססות על תשתיות תקשורת ומחשוב, ובכלל זה מערכות בחירות.[8]

תהליך בחירות דמוקרטי – איומים קיברנטיים מרכזיים

בחירות דמוקרטיות הן תהליך המורכב משחקנים וגורמים שונים המקיימים ביניהם קשרי גומלין. הפעילות והשימוש של מרכיבי ההליך הדמוקרטי בתשתיות, ובתוכן של המרחב הקיברנטי, הולכים ומתרחבים. תהליך הבחירות מורכב מארבעה שלבים המתקיימים בסדר כרונולוגי, כמפורט בתרשים שלהלן. האיומים הקיברנטיים המשמעותיים בתהליך זה, מפניהם נדרשות מדינות להתגונן, הינם תקיפה קיברנטית של תשתיות, איסוף מידע על מועמדים ומפלגות וניסיונות השפעה על התודעה.

חולשות סייבר בתהליך הבחירות

שיבוש, שינוי וזיוף מאגרי מידע

משרדי הממשלה האחראים על רישום ושמירת הפרטים האישיים של אזרחי המדינה ושל החברות עוברים בעשורים האחרונים תהליכים מתקדמים של דיגיטציה וייעול באמצעות הטמעה של מערכות ממוחשבות לרישום וניהול רשומות. מערכות אלו פגיעות מאוד למתקפות קיברנטיות, כפי שהוכח במדינות ג'ורג'יה, אילינוי ואריזונה בארצות הברית.[9] בשלוש מדינות אלו התגלו חדירות קיברנטיות למאגרי הרשומות, אשר עלולות היו להביא לגניבה או לחשיפת פרטיהם של כ־21 מיליון

8 Kate O'Keeffe and Byron Tau, "U.S. Considers Classifying Election System as 'Critical Infrastructure'," *Wall Street Journal,* August 3, 2016.

9 Dan Goodin, "US E-Voting Machines are (still) Woefully Antiquated and Subject to Fraud," *arsTechnica*, November 7, 2016.

אזרחים אמריקאים. לגניבת זהות, הדלפת פרטים ו/או שינוי שלהם יכולה להיות השלכה על ההליך הדמוקרטי כולו.

חשיפה של מבצע לשיבוש נתוני אזרחים או לפגיעה במקומות ההצבעה שלהם (למשל, הודעה מזויפת על מיקום הצבעה ואף אפשרות לפסילת קולות) עלולה לפגוע באמון הציבור במערכת הבחירות. דוגמה לכך ניתן לראות בבחירות הכלליות בקנדה בשנת 2011, בהן נעשו "מתיחות" על אזרחים, שבמסגרתן הודיעו להם טלפונית על מיקום שגוי של קלפי, כנראה במטרה לפגוע במוטיבציה של מצביעים לממש את זכות ההצבעה שלהם.[10]

בישראל, פרטי הבוחרים אינם נשמרים במאגרי המדינה וועדת הבחירות בלבד, אלא מועברים לכול מפלגה המתמודדת בבחירות. מצב זה יוצר נקודת תורפה באבטחת המידע על הבוחרים, אם כי עד היום טרם נחשפו ניסיונות לשיבושו

10 מתוך סיכום מנהלים של סמינר שנערך בקנדה לבחינה השוואתית של מערכות בחירות מרכזיות, http://www.elections.ca/content.aspx?section=res&dir=rec/tech/comp&document=p4&lang=e#ftn10.

בישראל. הדבר מעורר את הסוגיה כיצד ניתן להבטיח שימוש הולם במאגר הבוחרים ולפקח עליו בצורה אמינה.

שיבוש מערכות הצבעה ביום הבחירות

הצבעה בבחירות מחייבת אימות פרטים אישיים, כוללת הצבעה ידנית או ממוחשבת, ספירת קולות בקלפי והעברת הנתונים למערכת המרכזית. שיבוש של אחד מהתהליכים הללו יביא לפגיעה משמעותית בתהליך כולו. המערכות האלקטרוניות המסייעות לניהול יום הבחירות כוללות שירותים שונים: ניהול הרישום לקלפי ומימוש זכות הבחירה; יכולת בחירה אלקטרונית בקלפי (באמצעות מסך מגע או כרטיס אישי); יכולת בחירה אלקטרונית מרחוק על בסיס גישה לאינטרנט בלבד; סיוע לספירת הקולות. להרחבת השימוש במערכות הצבעה אלקטרוניות יש השלכות חיוביות ושליליות: מצד אחד, הטמעה של מערכת אלקטרונית תגדיל את השתתפות האזרחים בבחירות (יכולה לאפשר להם להצביע מהבית או ממכשירים ניידים); מצד שני, הסיכון לחדירה למערכת כזו ולשיבושה הינו גבוה ומחייב השקעת משאבים לאבטחה ותחזוקה שלה.[11]

מחקר שערך המכון לחקר ביטחון סייבר בארצות הברית, החוקר טכנולוגיות סייבר עבור תשתיות קריטיות, העלה כי מערכת ההצבעה הישירה, וכן מערכת הסריקה (Op Scan) הסורקת את כרטיסי ההצבעה והמערכות המבצעות את שקלול הנתונים ומאגרי המידע הממוחשבים, אינן מספקות הצפנה מקצה לקצה ומענה אבטחתי מתאים. כמו כן נמצא כי בקלפיות רבות בארצות הברית מופעלות מערכות אלו באמצעות מחשבים, שאינם מוגנים וניתנים לפריצה בקלות. עוד נקבע במחקר כי יריבים בעלי יכולות מתאימות יוכלו למצוא דרך לפגוע במערכות מקומיות ומפלגתיות בעלות רמת אבטחה נמוכה יותר ממערכות הבחירות הכלליות במדינה, וזאת על ידי החדרת נוזקות למחשבים, השבתת המערכות, גניבת מידע, חשיפתו או שיבושו.[12]

שיבוש ספירת הקולות

אופן ספירת הקולות בתום יום הבחירות משתנה ממדינה למדינה בהתאם לשיטת ההצבעה. בישראל, שיטת ההצבעה במערכות בחירות ארציות הינה ידנית, באמצעות פתקים הנספרים באופן ידני בקלפיות ומוזנים למערכת אלקטרונית המחשבת את שיעורי ההצבעה האזוריים לכדי חישוב ארצי סופי. סמינר שהתקיים בקנדה

11 Goodin, "US E-Voting Machines are (still) Woefully Antiquated and Subject to Fraud,"

12 James Scott and Drew Spaniel, "The Painfully Vulnerable Election System and Rampant Security Theater", *ICIT Blog, Institute for Critical Infrastructure Technology*, October 24, 2016.

בשנת 2014, לבחינה השוואתית של מערכות בחירות מרכזיות בין בריטניה, קנדה, ארצות הברית, אוסטרליה, ניו זילנד והודו, הגיע למסקנה כי כלל הגופים המעורבים בתהליכי בחירות יידרשו בעתיד להתמודד עם אתגרים הנובעים מהתפתחות של מערכות מבוססות רשת ועם השלכותיהם על מערכות הבחירות, ובכלל זה אבטחה של תהליכי הצבעה מקוונים או מרחוק, וכן אבטחה של מאגרי נתונים ומערכות של ספירת קולות.[13]

פרסומים רבים בארצות הברית מצביעים על האפשרויות שבאמצעותן ניתן להשפיע על מערכות לספירת קולות ולזייף את הכרטיסים המפעילים את מערכות הבחירה הישירה האלקטרונית. כך, למשל, בחלקים מארצות הברית נכנסה לשימוש מערכת הצבעה ישירה אלקטרונית המבוססת על זיהוי באמצעות כרטיס אישי והצבעה על בסיס מסך מגע. מערכת זו שומרת את הנתונים ומאפשרת להדפיס פלט בסוף יום הבחירות, הכולל את חלוקת הקולות באותו קלפי. מתברר כי ניתן לזייף הצבעות באמצעות שימוש בכרטיס מזויף המאפשר שינוי של הנתונים במסך, מחיקת קולות ואף מחיקת מועמדים.[14] זאת ועוד, למרות הזיהוי באמצעות כרטיס, ניתן לחדור מרחוק למערכות אלו ולשבש את ספירת הקולות ואפילו את הפילוח שלהם. בחירה אלקטרונית, המבוססת על מחשבים נגישים לאינטרנט, קלה עוד יותר להתערבות חיצונית, להונאה ולפגיעה בתהליך הבחירות הכללי.[15]

פגיעה באמון הציבור באמצעות השפעה על תכנים בשיח הציבורי

כאמור, לצד תהליך הבחירות קיימים גורמים נוספים המהווים בסיס לאמון הציבור במדינה ובמוסדותיה. אחד החוקרים הצביע על שורת מאפיינים המהווים את המרכיבים המשמעותיים ביותר באמון הציבור בממסדים הפוליטיים במדינה דמוקרטית: תקשורת עצמאית, דעת קהל אקטיבית, מערכת משפטית עצמאית, רמת מחייה הוגנת (שירותי בריאות, דיור, חינוך ותעסוקה) ובחירות חופשיות. פגיעה ברכיבים אלה עלולה להשפיע באופן משמעותי על תחושת הביטחון האישי של האזרח במדינתו ועל אמון הציבור בממסדי המדינה ובשירות הציבורי בכלל.[16]

---

13 מתוך סיכום מנהלים של הסמינר: http://www.elections.ca/content.aspx?section=res&dir=rec/tech/comp&document=p4&lang=e#ftn10.

14 Goodin, "US E-Voting Machines are (still) Woefully Antiquated and Subject to Fraud".

15 Dimitris A. Gritzalis, *Secure Electronic Voting* (Springer Science & Business Media, 2012).

16 מתוך הרצאת פרופ' מרקו מאייר בכנס "סייבר, פוליטיקה ובחירות", סדנת יובל נאמן למדע, טכנולוגיה וביטחון, אוניברסיטת תל אביב, 17 בינואר 2017.

הופעתם בשנים האחרונות של מרחבי שיח ותקשורת חדשים (בדגש על המדיה החברתית) הביאה להתפתחות שיח פוליטי וציבורי נרחב הפונה לקהל מגוון יותר מאשר בתקשורת המסורתית ומאפשר קשר ישיר ובלתי אמצעי עם האזרחים והבוחרים. שינוי זה הביא להגברת השימוש באינטרנט כמרחב לגיוס פעילים ותמיכה, להעברת מסרים ולניהול מסעי בחירות. האינטרנט כבר אינו נחלתם של גורמי השיווק והפרסום בלבד. ניתן לזהות פעילות ענפה של מועמדים לבחירות במערכות תקשורת שונות, ואף ניסיונות השפעה של מדינות עוינות על דעת הקהל המתגבשת ברשתות החברתיות ובמרחבי הרשת.[17]

הגנה על תהליכים דמוקרטיים מחייבת אפוא להוסיף לאיומים הישירים שהוגדרו לעיל איומים במרחב התודעתי, שעלולים להשפיע באופן קריטי על ההליך הדמוקרטי, וכתוצאה מכך על אמון הציבור בו. בהקשר זה מתעוררת דילמה הנוגעת לצורך ליצור הבחנה בין מהלכים לגיטימיים במאבק פוליטי ובין התערבות בלתי לגיטימית של גורמים זרים. ההגנה מפני איומים כאלה אינה נוגעת להיבטי הסייבר הישירים (הגנת תחנות קצה, שרתים, רשתות וכדומה), אלא להגנה מפני התערבות בתוכן המסרים בשיח הפוליטי. השאלה העומדת לדיון נוגעת לגבולות התקשורת החופשית: האם היא כוללת את אזרחי המדינה ומנהיגיה בלבד, או גם גורמים חיצוניים (דוגמת מדינות זרות וארגוני טרור), שהתערבותם אינה לגיטימית ונועדה לשבש את ההליך הדמוקרטי. במילים אחרות, ניתן אולי להשלים עם מניפולציות, שקרים ושמועות כחלק לגיטימי במאבק הפוליטי בתוך המדינה, אולם לא ניתן לקבל התערבות זרה העלולה לערער את ביטחון האזרחים במוסדות המדינה ולהביא לערעור היציבות בה.

מבנה הרשתות החברתיות מאפשר לתוכן להפוך ל"ויראלי" באמצעות שיתוף רחב, המגביר את החשיפה והפרסום של תוכן מסוים על בסיס התנועה והתגובות שהוא מייצר. לכן, מספיק שכמה מאות משתמשים (אמיתיים או מדומים) ייצרו תוכן שיפנה לקהל יעד ספציפי, כדי שהמסר יהפוך ל"ויראלי" ויעורר שיח ציבורי, אליו יצטרפו גורמי התקשורת המסורתיים. כל הנאמר לעיל מצביע על כך שיש מקום לבחון כיצד ניתן למנוע מניפולציות של גורמים חיצוניים על התהליכים הדמוקרטיים במדינה – בחירות כלליות, תהליכים פנים־מפלגתיים, תהליכים משפטיים וכדומה.

כאמור, בשנים האחרונות נחשפו מספר ניסיונות המיוחסים לרוסיה להשפיע על השיח הפוליטי במדינות המערב. יש הגורסים כי ניסיונות ההשפעה וההתערבות במערכות הבחירות במדינות אחרות מבטאים כוונה של רוסיה לערער את האמון של אזרחי המערב בהליך הדמוקרטי בכלל ובמערכות הבחירות בפרט, תוך יצירת

17 אזי לב־און וארז כהן, **מקושרים: פוליטיקה וטכנולוגיה בישראל**, האגודה הישראלית למדע המדינה, ירושלים, 2011.

תחושה של היעדר יכולת של המערכת להגן על פרטיות אזרחיה ולשמור על הליך דמוקרטי נקי.[18] דומה שבשנים האחרונות רוסיה אכן עושה את המרב מבחינתה כדי להשפיע על דעת הקהל במדינות שיש לה אינטרסים בהן, כגון אוקראינה והרפובליקות הבלטיות, וכן גרמניה, הולנד וצרפת, המסמלות את הגורמים המשמעותיים ביותר באיחוד האירופי. דוגמאות לכך הן: חדירה קיברנטית לבונדסטאג בגרמניה בשנת 2015 בניסיון לאסוף מודיעין שיפגע במפלגת השלטון, והניסיון להתערבות במשאל העם שהתקיים בהולנד באפריל 2016, שנערך בעקבות דרישה לבטל את הסכם הסחר של האיחוד האירופי עם אוקראינה משנת 2014. סקר שבחן את עמדות המצביעים נגד ההסכם העלה כי מרבית הנימוקים שהם נתנו היו נימוקי כזב, שלא היו מבוססים על עובדות, וככול הנראה מקורם היה בתעמולה רוסית.[19] בנוסף לנאמר לעיל, נרשמו ניסיון רוסי להשפיע על ה"ברקזיט" של בריטניה מהאיחוד האירופי, ניסיון להשפיע על מערכת הבחירות בארצות הברית לטובתו של דונלד טראמפ, וניסיון שכשל להשפיע על הבחירות בצרפת מספר חודשים מאוחר יותר.

הדוגמאות שהובאו לעיל מלמדות על העלייה בפרסום מידע פוליטי או אסטרטגי באמצעות רשתות חברתיות או באמצעות אתרים שמתמחים בחשיפה (דוגמת "וויקיליקס") במטרה להשפיע על דעת הקהל ועל השיח הציבורי. גורמים המעוניינים להשפיע על השיח ועל תוצאות הבחירות יכולים לעשות זאת באמצעות חשיפה של מידע, אמיתי או מזויף, בעיתוי מתאים. חשיפה כזו מיועדת ליצור ספק בדבר כשרותו של המועמד ומאפשרת הפצת שמועות שיפגעו במועמדותו. הדוגמאות הללו גם מראות כיצד ניתן להשפיע על בחירות באמצעות הפצה של ידיעות כוזבות, פרסום סקרים שקריים, יצירת הד תקשורתי סביב דיווח כזב שיש לו השלכה על מדיניות חוץ, והדלפת מידע אישי ומביך על מועמדים. כל אלה יכולים להשפיע על תהליכים דמוקרטיים ועל יחסים בין מדינות.

ההבנה כי קיימת עלייה בשימוש באסטרטגיה זו מחייבת דיון מקיף בהרחבת ההתגוננות במדינה דמוקרטית נגד איום זה.[20] יתר על כן, גם אם תהיה הגנה מלאה על ההיבטים הטכנולוגיים של תהליך הבחירות, עדיין ניתן יהיה להשפיע על ההליך הדמוקרטי כולו. זהו אחד האתגרים המרכזיים העומדים בפני הגנה על כל מערכת בחירות: לא די בהגנה על תשתיות ומערכות טכנולוגיות; נדרש גם מענה הגנתי

18 Keir Giles, "Russia's 'New' Tools for Confronting the West", *Chatham House, Russia and EuroAsia Programme*, March 2016.

19 Anne Appelbaum, "The Dutch just Showed the World how Russia Influences Western European Elections", *The Washington Post*, April 8, 2016.

20 מתוך שימוע של ראש המרכז לסייבר והגנת המולדת בפני ועדת הקונגרס האמריקאי להגנת המולדת ותת־הוועדה לסייבר, הגנת תשתיות וטכנולוגיות ביטחון, 25 בפברואר 2016, http://docs.house.gov/meetings/HM/HM08/20160225/104505/HHRG-114-HM08-Wstate-CilluffoF-20160225.pdf

על השיח כולו מפני זיהום אנטי דמוקרטי חיצוני. אם בעבר הדגש היה על מניעת השבתה של מערכות התקשורת והמחשבים, בעידן של האיום החדש התוקף דווקא מעוניין שמערכות אלו יפעלו כדי שיוכל להזרים בהן את מסריו המניפולטיביים.

גורמים מאיימים על תהליך הבחירות הדמוקרטי

האיום הקיברנטי על מערכות בחירות יכול לבוא לידי ביטוי בהתערבות של מעצמות או של מדינות זרות, בפשיעה בין־לאומית או בפעילות טרור. ההבחנה בין סוגי האיום נעשית על פי זהות התוקף, המוטיבציה שלו לתקיפה, מורכבות ותחכום התקיפה והמשאבים שעמדו לרשותו כדי לבצעה. בבחינת אופן ההגנה על הליך הבחירות או על תשתית קריטית אחרת, ניהול הסיכונים צריך לכלול ניתוח של השחקנים בעלי המוטיבציה והיכולת לפגוע בתהליך הבחירות הדמוקרטי.[21] מאמר שפורסם בארצות הברית, אשר ניתח את הרגישות של תהליך הבחירות לאור ניסיונות ההתערבות הרוסיים, בחן, בין היתר, מיהם השחקנים השונים העלולים להוציא לפועל תקיפה קיברנטית נגד מרכיבי מערכת הבחירות בארצות הברית ומנה ביניהם מדינות עוינות, יריבים פנימיים ומפגעים בודדים (האקרים), כמו גם גורמים הפועלים ממניעים אידיאולוגיים, כגון קהילות "אנונימוס" או "וויקיליקס", או ארגונים ממומנים בעלי אידיאולוגיה פוליטית הפועלים להשפיע על הבחירות באמצעות קמפיינים מסיביים ברשתות ובקרב צעירים.[22]

המניעים של מדינות יריבות להתערב במערכות בחירות של מדינות אחרות משתנים בהתאם ליעד התקיפה. מניע מרכזי יכול להיות הרצון לערער את תחושת הביטחון האישי ואת אמון הציבור בהליך הדמוקרטי כולו. ההבנה כי דעת הקהל משפיעה על אופן קביעת המדיניות מניעה מדינות יריבות להתסיס אזרחים נגד המסגרת הדמוקרטית, ובעיקר נגד הממשל והפוליטיקה הפנים־מדינתית. מניע נוסף להתערבות במערכת בחירות במדינה זרה הוא הרצון להשפיע על תוצאות הבחירות. לכן, הגורמים המתערבים ישקיעו את משאביהם במספר ערוצים: השפעה על דעת הקהל באמצעות תעמולה, כמו למשל באמצעות שתילת "טרולים" הפועלים במרחב הרשת נגד הממסד, ולעיתים נגד קהילת האינטרנט, הפצה של תגובות שליליות ומשלהבות נגד מידע מסוים, חדירה לאתרים, הפצה של ספאם ועוד, ערעור דעת הקהל ואמונו במערכת והדלפת מידע רגיש על המועמדים היריבים. לאותם גורמים המתערבים במערכת הבחירות עשוי להיות גם מניע של ריגול ואיסוף מודיעין, כולל גניבת מידע רגיש על המועמדים או על מטה הבחירות שלהם, כפי שנעשה בקיץ 2016 בהדלפת דואר אלקטרוני מוועידת המפלגה הדמוקרטית בארצות הברית.

21 גולדשמידט, "המרחב הקיברנטי וההגנה על תשתיות קריטיות".

22 Scott, Spaniel, "The Painfully Vulnerable Election System and Rampant Security Theater".

סיכום

מאמר זה הציג את האיומים על מערכות בחירות אל מול התפתחויות קיברנטיות ותרבותיות והצביע על החשיבות של ראיית מערכות בחירות כתשתיות וכתהליכים קריטיים. המסקנה היא כי נדרשת הגנה כוללת על תהליך הבחירות, משום שהשפעה חיצונית עליו עלולה לערער מהיסוד את אמון הציבור בממסד הפוליטי במדינתו ובערכי הדמוקרטיה בכלל. גורמים בכירים במערך הסייבר הלאומי של ישראל מגלים הבנה לחשיבות ההגנה על מערכות המחשבים של ועדת הבחירות המרכזית ועל מאגר הבוחרים, ומסכימים כי ייתכן ונדרש גם שינוי חקיקה שיגדיר מערכות אלו כתשתיות קריטיות. יחד עם זאת, דומה שלא קיימת הבנה מספקת באשר להגנה הנדרשת על השיח הפוליטי מפני זיהומים חיצוניים.

מערכת בחירות הינה "בטן רכה" במדינה דמוקרטית, ותקיפתה עלולה להשפיע הן על המדינה והן על המועמדים. על מדינות המערב לשקול להרחיב את ההתייחסות ואופני המענה לאיומים על הליכים דמוקרטיים, כמו הגנה על השיח התקשורתי מפני זיהום והגנה על מפלגות, וזאת לצד הגנה על ועדות הבחירות ועל מנגנוני ההצבעה. הגנה על פלח אחד בלבד מהמערכת הכוללת לא תספיק. הניסיונות להשפיע על בחירות באמצעות חשיפה ופרסום של מידע שנאגר במערכות מחשב של מפלגות או מועמדים, שחלקם הצליח ככול הנראה, מחייבים להגביר את ההגנה על מערכות אלו. אותם ניסיונות גם מעוררים את השאלה בדבר אחריותה של המדינה להכוונת ההגנה הקיברנטית על מוסדות פוליטיים.

מאמר זה לא דן במענים לאיומים המוצבים בפני מערכת הבחירות במדינה דמוקרטית, וזאת מתוך כוונה לאפשר, בשלב ראשון, יצירת שיח על איומים אלה, בדגש על האיומים החדשים על השיח הפוליטי במדינה דמוקרטית. הפניית הזרקור אל איומים חיצוניים מדגישה את תפקידה של המערכת הביטחונית במדינה לבלום איומים של חתרנות מדינית. הדבר גם מחייב אותה להגדיר את האיומים ולתחם אותם באופן שלא יפגע בחופש הביטוי מצד אחד, אך ישמור על השיח הפוליטי מפני התערבות לא לגיטימית מצד שני.

הייחוד שבהגנה על תהליך הבחירות או על שאר ההליכים הדמוקרטיים, כמו שלטון החוק וחופש הביטוי, הוא שאין מדובר בשמירה על תפעול התשתית בלבד, אלא בהגנה על אמון הציבור במערכת – הישג חמקמק בהרבה, שניתן לערער עליו בדרכים שונות ומגוונות. המאמר הציג לפיכך את הצורך בהגנה על מערכת המחשבים המתפעלים את מערכת הבחירות – צורך שקיימת לגביו הסכמה רחבה – ולצידו גם את הצורך בהגנה על השיח הפוליטי מפני זיהום חיצוני, שתכליתו לערער את אמון הציבור במערכת הדמוקרטית כולה – צורך שעדיין לא קיימת הכרה רחבה בו, בין השאר משום שהוא מאתגר עקרונות דמוקרטיים, כמו שמירה על חופש הדיבור (במדיה החברתית ובאמצעי התקשורת).