איום התערבות זרה בבחירות 2019 בישראל ודרכי ההתמודדות מולו

פנינה שוקר וגבי סיבוני

בשנים האחרונות מתרבים הניסיונות של מדינות זרות להשפיע על התהליכים הדמוקרטיים במדינות יריבות להן. משרת הניסיונות היא לפגוע בתהליך הבחירות באותן מדינות באמצעות תקיפות סייבר על מערכות המחשוב התומכות תהליך זה, או להשפיע על תוצאות הבחירות באמצעות מאמצי השפעה. התבוננות על תהליך הבחירות בישראל מאפשרת לבחון קיומם של ניסיונות השפעה כאלה עליה ולהציע דרכים להתמודד עימם. המאמר מציע להפריד בין מאמצי השפעה זרים ובין מאמצי השפעה פנימיים, שהינם חלק מההליך הדמוקרטי, ומתווה כיווני פעולה לשיפור ההתמודדות עם ניסיונות ההשפעה הזרים.

מילות מפתח: בחירות, מאמצי השפעה, סייבר, הליך דמוקרטי, רשתות חברתיות

מבוא

האפשרות שמדינה זרה תנסה להשפיע על ההליך הדמוקרטי בישראל זכתה לעיסוק אינטנסיבי במערכת הבחירות לכנסת ה־21. ביולי 2017 העלה הרמטכ"ל דאז, רא"ל גדי איזנקוט, את האפשרות של התערבות זרה בדמוקרטיה הישראלית, אותה הציג כאתגר מרכזי. במסגרת דיון בכנסת ציין איזנקוט שתי תופעות הקשורות בהתערבות אפשרית כזו: ניסיונות להשפיע על תוצאות הבחירות באמצעות שיבוש ופגיעה במערכות המחשוב התומכות אותן; ניסיונות השפעה על תודעת הבוחרים על ידי מניפולציה המונית, וזאת באמצעות פרסומים ברשתות החברתיות ובאתרי אינטרנט.[1]

1 עמוס הראל, "רשות הסייבר מגבשת תכנית להגנה מפני התערבות זרה בבחירות בישראל", **הארץ**, 13 ביולי 2017.

פנינה שוקר היא וקרת (מלגאית ניובאואר) במכון למחקרי ביטחון לאומי ודוקטורנטית במחלקה למדעי המדינה באוניברסיטת בר אילן.
ד"ר גבי סיבוני הוא מנהל תכנית ביטחון סייבר במכון למחקרי ביטחון לאומי.

עם היוודע דבר הקדמת הבחירות ל־2019, רבו אזהרות מצד בכירים בדרג המדיני והביטחוני בישראל מפני התערבות זרה אפשרית בהן: בדצמבר 2018 הצהיר הנשיא ריבלין בכנס לאוטמן לחינוך כי "בעלי אינטרסים רוצים להסיח את הדעת מהעובדות אל הספקולציות וההשמצות ... בעולם ה'פייקניוז' צריך להבטיח את זכות האזרחים לנגישות לעובדות ללא עיוותים".[2] מדברי הנשיא לא היה ברור האם הוא מתכוון להתערבות זרה או לשיח הפוליטי בתוך המדינה.

בתחילת ינואר 2019 התריע ראש השב"כ, נדב ארגמן, כי מדינה זרה מתכוונת להתערב בבחירות בישראל וכי ההתקפה עשויה להתבצע בתחום הסייבר באמצעות פצחנים (האקרים).[3] בסוף אותו חודש הצהיר גם ראש הממשלה נתניהו בכנס CyberTech כי איראן מנסה להשפיע על הבחירות בישראל דרך חשבונות מזויפים ברשת וכי היא מבצעת מתקפות סייבר נגד ישראל "על בסיס יומי".[4] לדברי מבקר המדינה, יוסף שפירא, "התערבות זרה שתפגע באמינות המערכות ובאמינות התוצאות עלולה להביא לפגיעה עמוקה ואנושה באמון הציבור בשלטון".[5]

אמירות אלו שיקפו חשש מהותי ששרר בקרב בכירי הדרג המדיני והצבאי־ביטחוני בישראל מפני התערבות זרה בבחירות של אפריל 2019 לכנסת, שלראשונה בתולדות מדינת ישראל התנהלו בצילו של חשש כזה. זהו הרקע לעיסוקו של המאמר בסכנת ההתערבות הזרה בבחירות 2019 ובמאמצי ההתגוננות שננקטו כדי להתמודד עם תופעה זו. המאמר אינו מתייחס להיבטים של ניסיונות השפעה ומניפולציה תודעתית הנעשים במסגרת השיח הפוליטי והדמוקרטי בישראל, שהינם, וצריכים להיות, חלק מחופש הביטוי במדינה ואשר הדמוקרטיה הישראלית נדרשת ויכולה להכיל אותם.

החלק הראשון של המאמר יסקור את תופעת ההתערבות הזרה בבחירות, על מאפייניה, תוך פירוט של ביטוייה במערכות בחירות שונות ברחבי העולם. חלקו השני יציג את ההתארגנויות השונות להתמודדות עם התופעה בהקשר הישראלי. בסיכום המאמר ייבחנו דרכים אפשריות לשיפור ההתמודדות עם אתגרים דומים בעתיד.

תיאור התופעה

בשנים האחרונות גוברת תופעה לפיה גורמים זרים (מדינות וגורמים לא מדינתיים) עושים שימוש בטכניקות דיגיטליות במטרה לפגוע בתהליך הדמוקרטי של מדינות

2 "נשיא המדינה בכנס דב לאוטמן: 'לעבור מפוליטיקה של זהויות לפוליטיקה של רעיונות'", *Ynet*, 27 בדצמבר 2018.

3 אמיר בוחבוט, יקי אדמקר, "ראש השב"כ הזהיר: מדינה זרה מתכוונת להתערב בבחירות בישראל", **וואלה**, 8 בינואר 2019.

4 איתי שיקמן, "מנטרים תקיפות סייבר איראניות כל הזמן", *Ynet*, 29 בינואר 2019.

5 בוחבוט ואדמקר, "ראש השב"כ הזהיר: מדינה זרה מתכוונת להתערב בבחירות בישראל".

יריבות. זאת, באמצעות תקיפות סייבר על מערכות המחשוב התומכות את תהליך הבחירות באותן מדינות (מסדי נתונים, תוכנות למיניהן ומערכות תקשורת) במטרה לשבש את הנתונים, לגנוב אותם כדי לעשות בהם שימוש, או לפגוע ביכולת הפעולה של מערכות אלו. לצד פעילות זו נחשפו בשנים האחרונות שיטות שונות של מבצעי השפעה רחבי היקף שנועדו להשפיע על תודעת הבוחרים. המטרות של ניסיונות אלה יכולות להיות מגוונות: החל מניסיונות לערער את אמון הציבור בתהליך הדמוקרטי וכלה בניסיונות להשפיע על התמיכה במפלגות ובמועמדים שונים. חלק מהניסיונות אף נועד להניא אנשים מלהשתתף בבחירות על בסיס זהותם או מעמדם הסוציו־אקונומי.[6] ניסיונות השפעה אלה נעשים בעיקר באמצעות הרשתות החברתיות.

בניגוד לתפיסה לפיה הרשת החברתית מאפשרת היחשפות למגוון רחב של דעות שונות, ניכר כי "פייסבוק" – הרשת החברתית הפופולרית ביותר – דווקא מייצרת חללים סגורים של גולשים בעלי דעות הומוגניות. חללים סגורים אלה נוצרים בזכות פעולות כגון הסרת חברים, חסימתם או הוצאתם מרשימת המעקב ב"פייסבוק", או פעולות שמבצעים הגולשים נגד כל מי שמבטאים דעות פוליטיות שונות משלהם, במיוחד כשמדובר בחברי רשת שהקשרים איתם הם רופפים ודלים. כך, "פייסבוק" יכולה ליצור פירוד, ואולי אפילו קיטוב או הקצנה, של דעות פוליטיות, ולאו דווקא מתינות וסובלנות למגוון רחב של דעות שונות. בנוסף לכך, תוכנת הרשת, שאוספת, בין היתר, מידע על רשימת החברים של המשתמש, תציג עבורו תחומים מסוימים בהתאם להעדפותיו האישיות. זהו היבט נוסף שיוצר סביבה חברתית הומוגנית,[7] דבר הנובע מהנטייה האנושית להתחבר אל הדומים לנו (אתנית, גיאוגרפית או אידיאולוגית) – תופעה המכונה הומופיליה. נטייה זו, היוצרת ברשת האינטרנט תופעות של "עדריות", מועצמת על ידי הרשתות החברתיות או על ידי מנועי חיפוש המנגישים מידע התואם את עמדותינו.

הבעיה במצב זה היא בכך שרבים עדיין רואים בייצוג האינטרנטי של המתרחש בעולם מעין "מפה" אמיתית, כאשר בפועל זהו ייצוג סובייקטיבי המותאם למשתמש וקשור למיקום הגיאוגרפי שלו, למצבו הכלכלי־חברתי, הבין־אישי ועוד. פרופ' נהון מציינת, בהקשר לבחירות בישראל, שבבחירות לכנסת ה־20 ציינו גולשים רבים ממחנה השמאל כי לפי התכנים אליהם נחשפו ב"פייסבוק", הם שיערו כי

---

6 Chris Tenove, Joran Buffie, Spencer McKay and David Moscrop, *Digital Threats to Democratic Elections: How Foreign Actors Use Digital Techniques to Undermine Democracy* (The University of British Columbia: Center for the Study of Democratic Institutions, 2018), p. 26.

7 Nicholas A. John and Shira Dvir-Gvirsman, "'I Don't Like You Any More': Facebook Unfriending by Israelis During the Israel–Gaza Conflict of 2014", *Journal of Communication* 65, no. 6 (2010): 953-974.

השמאל עתיד לנצח בבחירות. להיבטי ההשפעה על זרימת המידע יש, כאמור, השפעה רבה, שכן אם ניקח לדוגמה את המקרה האמור, ההנחה כי "השמאל הולך לנצח" עלולה הייתה לגרום למצביעי שמאל לא לפקוד את הקלפי מתוך תחושה ש"בכל מקרה ננצח".[8]

הניסיונות לבצע מניפולציות על דעת הקהל או על התפוצה של מידע ברשת נעשים, בין היתר, באמצעות מה שמכונה "בוטים". בוט (באנגלית: bot, קיצור של robot) הוא סוכן תוכנה המיועד למגוון שימושים. השימוש העיקרי בבוטים הרלוונטי למאמר זה נועד ליצור דימוי של משתמש אנושי ברשתות חברתיות, או של כלי תוכנה, להגברת התפוצה של פוסטים ברשתות אלו. לעיתים, תוכנות מסייעות לנהל מספר רב של ישויות במקביל. בצורה זו ניתן להפיץ מגוון תכנים למימוש אינטרסים שונים – מסחריים, פוליטיים או פליליים – שמידת השימוש לרעה שהם מגלמים שונה, אך המשותף להם הוא השימוש בטכנולוגיות אוטומציה כדי להשפיע על זרימת המידע ותפוצתו.[9]

ניתן לייצר דיסאינפורמציה, להפיצה ולמקד אותה במטרה להגביר מחלוקות קיימות, כגון סכסוכים בין־מפלגתיים, לנעוץ טריזים בין בעלי ברית ולערער את הנורמות המשותפות של הדיון הדמוקרטי. למשל, רוסיה השתמשה בפלטפורמות של מדיה חברתית בבחירות 2016 לנשיאות ארצות הברית כדי להפיץ מסרים כביכול מטעם מוסלמים תומכי הילרי קלינטון. במסגרת זו נרכשו שטחי מודעות ב"פייסבוק", שנכתבו בהם מסרים כגון "תמכו בהילרי; הצילו את המוסלמים האמריקאים". המטרה הייתה ליצור זיקה בין האסלאם הפוליטי ובין קלינטון.[10] בנוסף, התנהלה פעילות רבה שכוונה להשפיע על השחורים בארצות הברית לצאת למחאות ולעודד את המוחים לעורר הפרות סדר.[11]

דיסאינפורמציה יכולה לשמש גם כדי להרתיע אנשים מלהשתתף בסקרים. מחקר על הבחירות מראה כי מודעות בחירות מנסות רק לעיתים נדירות לשכנע אנשים להצביע עבור מועמד שונה מזה שעבורו הם מתכננים להצביע, וכי הן יכולות להיות אפקטיביות יותר בהעלאת שיעורי ההצבעה או הורדתם ולהשפיע על הצבעות לטובת מועמדים ידועים פחות. בנוסף לכך, ניתן לפגוע בהשתתפות

8 "הפצת מידע כוזב באינטרנט ותקיפות סייבר לשם השפעה על בחירות", מרכז המחקר והמידע של הכנסת, יוני 2017.

9 שם.

10 דוד סימן טוב ויותם רוזנר, "חתרנות תודעתית: התערבות רוסית בבחירות לנשיאות בארצות הברית כאיום חדש על המערב", **מבט על** 1031, המכון למחקרי ביטחון לאומי, 8 במארס 2018.

11 לאוניד נבזלין, "הטרול המסוכן בעולם", **ליברל**, פברואר 2019.

דמוקרטית על ידי שחקנים המשתמשים בטכניקות דיגיטליות כדי לסחוט, לאיים או להטריד מועמדים.[12]

לטענת פרופ׳ נהון, הבעייתיות של מידע שגוי או מסולף גדולה במיוחד בתקופות של אירועים כמו מלחמה או בחירות, בהן העומס התקשורתי גבוה במיוחד ואמצעי התקשורת נוטים להפיץ מידע באופן מהיר, ללא בדיקה מעמיקה שלו טרם פרסומו. כפועל יוצא מכך, הציבור אינו "בודק את העובדות", אלא מגבש עמדות על בסיס מידע שגוי, או מבסס על מידע כזה עמדות שהוא כבר מאמין בהן. נהון גורסת כי הרשתות החברתיות והוויראליות של מידע ברשת הגדילו את היכולת לעשות שימוש בדיסאינפורמציה בתקופת בחירות ולהשפיע על האופן שבו אנשים בוחרים.[13]

לסיכום, היכולת להצביע ולהשפיע – האופן הבסיסי ביותר של השתתפות פוליטית – מאוימת כיום על ידי התערבות דיגיטלית זרה. כאמור, התערבות כזו יכולה להיות באמצעות פגיעת סייבר במערכות המחשוב התומכות את הליך הבחירות, שמטרתה היא לפגוע ב**תהליך הבחירות**, או באמצעות מבצעי דיסאינפורמציה המיועדים להשפיע על **תוצאות הבחירות**.[14]

ניסיונות השפעה על מערכות בחירות בעולם

בשנים האחרונות זוהו מקרים רבים של התערבות מדינות בתהליכי הבחירות במדינות אחרות באמצעות טכנולוגיה שמבוססת על רשת האינטרנט. בין המדינות שזוהו בעשור האחרון כמי שהפעילו מבצעי השפעה על בחירות באמצעות כלי סייבר בולטת במיוחד רוסיה (אם כי זו אינה היחידה). ניסיונות ההתערבות שלה במערכות בחירות כללו את אוקראינה (2014), ארצות הברית (2016), צרפת, גרמניה והולנד (2017), ובמשאלי עם – את בריטניה, הולנד, איטליה וספרד (2017).[15]

אירוע ההתערבות בבחירות הבולט ביותר בשנים האחרונות, שתוצאתו ממשיכה להשפיע על ארצות הברית ועל העולם כולו, הוא מעורבותה של רוסיה בבחירות לנשיאות ארצות הברית ב־2016. בתחילת ינואר 2017 פרסמה קהילת המודיעין האמריקאית את הערכתה לפיה רוסיה התערבה בבחירות אלו במגוון אמצעים במטרה לפגוע בסיכויי בחירתה של מועמדת המפלגה הדמוקרטית הילרי קלינטון ולקדם את בחירתו של דונלד טראמפ.[16] הדוח קובע כי ניסיונות אלה של רוסיה כללו

12 Tenove et al., *Digital Threats to Democratic Elections*.

13 "הפצת מידע כוזב באינטרנט ותקיפות סייבר לשם השפעה על בחירות".

14 Tenove et al., *Digital Threats to Democratic Elections*.

15 אלי בכר ורון שמיר, "התקפות סייבר על מערכות הבחירות: איך מתמודדים?", **מחקר מדיניות 136**, המכון הישראלי לדמוקרטיה ותוכנית המחקר להגנת הסייבר, ירושלים, 2019, עמ׳ 9–10.

16 "Assessing Russian Activities and Intentions in Recent US Elections", *Office of the Director of National Intelligence*, January 2017.

מבצעים בתחום הסייבר, לרבות מבצעי השפעה ברשתות החברתיות, שבמסגרתם הופצה דיסאינפורמציה על מספר נרטיבים מתחרים בו־זמנית באמצעות בוטים, טרולים והאקרים, וזאת במטרה להעמיק מחלוקות קיימות בחברה האמריקאית ולערער את האמון במוסדות המערביים ובהליך הדמוקרטי בכללותו.[17]

בפברואר וביולי 2017 הגיש התובע המיוחד, רוברט מולר, כתבי אישום מפורטים נגד עשרים אזרחי רוסיה בגין התערבות במערכת הבחירות לנשיאות ארצות הברית. למרות פרסומים אלה, טרם ניתן הסבר ברור כיצד מעורבות רוסית זאת השפיעה בפועל על התנהלות הבחירות ועל תוצאותיהן. גם המחקר הבולט ביותר שנעשה בנושא זה לא קבע נחרצות כי מאמץ ההשפעה הרוסי אכן נשא פרי, אלא רק מניח זאת בסבירות גבוהה, המתבססת על ההלימה הנסיבתית בין המאמצים הרוסיים ובין השתנות השיח הציבורי והתקשורתי והתוצאות המפתיעות של הבחירות.[18] ראוי לציין כי בשלהי מארס 2019 פרסם מולר את מסקנותיו הסופיות, אשר אוששו למעשה את מסקנות הדוח של ועדת המודיעין של הסנאט מ־2017, כי רוסיה ערכה קמפיין פריצות למערכות מחשב וקמפיין דיסאינפורמציה שנועדו להעמיק שסעים בחברה האמריקאית ולהשפיע על בחירות 2016. מולר זיהה שתי זרועות של הקמפיין מטעם הקרמלין: קמפיין מידע כוזב שבוצע בידי ארגון הידוע בשם סוכנות מחקר האינטרנט ופריצות למערכות מחשב בידי גופי מודיעין רוסיים שפעלו נגד אנשי המפלגה הדמוקרטית.[19]

אלא שניכר כי לא רק רוסיה התערבה בבחירות דמוקרטיות; גם סין עשתה זאת בבחירות 2018 בקמבודיה,[20] ולאחרונה הולכים ורבים הדיווחים על מאמצים סיניים להתערב גם בבחירות בארצות הברית, מה שהביא להצהרתו של הנשיא טראמפ על כך שסין חותרת להשפיע על תוצאות בחירות האמצע שהתקיימו בנובמבר 2018 לקונגרס האמריקאי ולמוסדות נוספים בארצות הברית.[21]

בשלהי ינואר 2019 פרסמו "פייסבוק" ו"טוויטר" במקביל כי חשפו מאמץ השפעה חשאי בסייבר שהופעל על ידי איראן כלפי ישראל. המאמץ כלל תכנים

17 Andrew Radin, Elina Treyger, "Countering Russian Social Media Influence", *RAND Corporation*, November 2018.

18 Kathleen Hall Jamieson, *Cyber-War: How Russian Hackers and Trolls Helped Elect A President* (Oxford: Oxford University Press, 2018).

19 "Report On The Investigation Into Russian Interference In The 2016 Presidential Election", *U.S. Department of Justice, Special Counsel Robert S. Mueller*, March 2019.

20 Scott Henderson, Steve Miller, Dan Perez, Marcin Siedlarz, Ben Wilson, Ben Read, "Chinese Espionage Group TEMP.Periscope Targets Cambodia Ahead of July 2018 Elections and Reveals Broad Operations Globally", *FireEye*, July 10, 2018.

21 Abigail Grace, "China's Influence Operations Are Pinpointing America's Weaknesses", *FP*, October 4, 2018.

שנועדו לחזק את הנרטיב האיראני ביחס להתפתחויות במזרח התיכון ובנושא הסכסוך הישראלי־פלסטיני, ובנוסף להם כלל ביקורת על ראש הממשלה נתניהו, מדיניותו ומשפחתו, ככל הנראה כחלק מניסיון להטות את דעת הקהל הישראלית ערב הבחירות לכנסת. מדובר בקשר נסיבתי, ולא ברור האם המהלך שיוחס לאיראן אכן נועד להשפיע על הבחירות בישראל.[22]

במועד כתיבת שורות אלו לא ברור עד כמה היוו בחירות 2019 בישראל יעד להתערבות זרה, ובאיזו מידה (אם בכלל) התערבות כזו צלחה. כך או כך, מדינת ישראל קיימה מספר מאמצי הגנה לקראת הבחירות ובמהלכן.

מאמצי התגוננות מפני התערבות זרה בבחירות 2019 בישראל

תקיפות סייבר בהקשר לבחירות בישראל יכולות להתרחש בשלושה ממדים אפשריים: הראשון, תקיפת סייבר "קלאסית"[23] המיועדת לפגוע בתהליך הבחירות וכוללת תקיפת של מערכות המחשוב התומכות אותן, של מערכות המחשוב של המפלגות ושל חברות סקרים; הממד השני הינו תקיפת מפלגות פוליטיות ושחקנים פוליטיים באמצעים שונים: גניבת חומר אישי ופוליטי ופרסומו בעיתוי מתאים מבחינת יעדי התקיפה, שיבוש היערכות המפלגה לבחירות ועוד; הממד השלישי כולל ניסיונות השפעה על תוצאות הבחירות באמצעות מאמצים להטיית דעת הקהל ברשתות החברתיות.

מענה לאיומים מסוג זה הוא אתגר מורכב, המחייב הפרדה בין מאמצי ההשפעה המבוצעים על ידי המפלגות עצמן – תהליך לגיטימי שעל כל חברה דמוקרטית להכיל – ובין מאמצי השפעה של גורמים זרים. זאת, גם מאחר שכל מענה עלול לטמון בחובו פגיעה אפשרית בפרטיות כתוצאה מניטור הרשתות החברתיות. איום הסייבר "הקלאסי" מחייב מאמצי הגנה של בעלי העניין עצמם: ועדת הבחירות המרכזית, המפלגות, חברות סקרים ושאר הגורמים העלולים להיות חשופים לתקיפת סייבר כזאת. מערך הסייבר הלאומי לקח על עצמו להנחות את כלל הגורמים הרלוונטיים ואף פעל כדי לסייע לוועדת הבחירות המרכזית להתמודד עם איום זה.

ההתארגנות המדינתית לקראת הבחירות לכנסת ה־21 באה לידי ביטוי בהקמת "צוות בחירות מיוחד" בהובלת מערך הסייבר הלאומי ובהשתתפות גורמי ביטחון ומשרד המשפטים. הצוות התכנס באופן שוטף ופעילותו התבססה על למידה

22 הגר בוחבוט, "פייסבוק הסירה מאות עמודים שהכילו פייק ניוז איראני", *Ynet*, 31 בינואר 2019.

23 פגיעת סייבר "קלאסית" מוגדרת כפגיעה במערכות המחשוב ובבסיסי הנתונים התומכים את הליך הבחירות וההליך הדמוקרטי במטרה לפגוע במהלך הבחירות התקין. זאת, לעומת ניסיונות השפעה באמצעות פעולות ברשתות החברתיות או חשיפה של מידע בעייתי על מועמדים ומפלגות, שמטרתם השפעה על תוצאות הבחירות.

מניסיונן של מדינות אחרות ויישומה באמצעות תרגולים של הגופים הרלוונטיים – ועדת הבחירות המרכזית וגופים נוספים במערכת הפוליטית והאזרחית (כמו חברות סקרים). הדבר היווה התקדמות משמעותית בהיערכות המדינה מול איומים לשבש את התהליך הדמוקרטי, הגם שמדובר בהיערכות בהקשר של הבחירות בלבד, תוך שימת דגש על התערבות טכנולוגית. ההיערכות המדוברת לא עסקה במתן מענה לאיומים אחרים שפורטו קודם לכן, וגם לא בשילוב של החברה האזרחית במענה, כפי שקורה במדינות אחרות (למשל בדנמרק).[24]

בפברואר 2019 שלח מערך הסייבר הלאומי לכל המפלגות בישראל מסמך מיוחד שנועד לסייע להן להתגונן בפני איומים שונים. המסמך מפרט נהלים והנחיות בנוגע להקשחת המערכות, האתרים, אמצעי התקשורת ושאר התשתיות הווירטואליות שלהן, ועוסק בהגנה על מחשבים אישיים, רשתות תקשורת פנימיות של המפלגות, דואר אלקטרוני, טלפונים ניידים, שעונים חכמים ומרכזיות טלפון. פרק נרחב במיוחד במסמך מוקדש להגנה על אתרי האינטרנט של המפלגות וכולל פירוט מדוקדק של הנדרש לעשות לצורך זה.[25]

למרות פעילות זו, גורמים הקשורים למערך הסייבר הלאומי הבהירו כי גוף זה אינו צריך לעסוק בתכנים הקשורים במערכת הבחירות וכי הוא אינו מתכוון לפעול כדי לסכל קמפיינים תודעתיים באמצעות עיסוק בתכנים. אף על פי כן, בדיון שנערך בכנסת באוקטובר 2018, ערב הבחירות לרשויות המקומיות, הציג מערך הסייבר הלאומי שיתוף פעולה עם חברת "פייסבוק" בהסרת פרופילים מזויפים.[26] המהלך נתקל בביקורת של נציגי איגוד האינטרנט הישראלי שטענו כי מערך הסייבר הלאומי אינו מוסמך לעסוק בכך, גם לא באופן עקיף.[27]

עם היוודע דבר הקדמת הבחירות בישראל הכריזה חברת "פייסבוק" על הקמת חדר מצב במטרה לנטר מידע ממגוון מקורות, בין השאר ממפלגות ומגולשים פרטיים, הנוגע לפוסטים ולקמפיינים המפרים את תנאי השימוש של "פייסבוק". לפי הפרסום, חדר המצב נועד להגיב במהירות על הפרות של כללי ההתנהגות. לצורך זה העסיקה "פייסבוק" צוות צנזורה, שעשה שימוש בכלי בינה מלאכותית כדי להציף תכנים שנחשדו בהפרת תנאי השימוש. כלי אחר של הצוות היה דחיקה

24 "סיכום דיון סימולציה בנושא השפעה בלתי לגיטימית על השיח הציבורי והפוליטי באמצעים דיגיטליים לקראת בחירות 2019 בישראל", המכון למחקרי ביטחון לאומי, המכון הישראלי לדמוקרטיה ואיגוד האינטרנט הישראלי, 26 בפברואר 2019.

25 רן בר־זיק, "מערך הסייבר הוציא מדריך התגוננות למפלגות: האם הן ילמדו את הלקח?", **הארץ**, 20 בפברואר 2019.

26 טל שחף, "מערך הסייבר הלאומי: פעלנו עם פייסבוק וטוויטר להסרת אלפי חשבונות מזויפים", **גלובס**, 15 באוקטובר 2018.

27 עומר כביר, "נחשפו אלפי חשבונות פייק ניוז, שניסו להשפיע על הבחירות המוניציפליות בארץ", **כלכליסט**, 15 באוקטובר 2018.

לאחור של קמפיינים בעייתיים, אפילו אם הם ממומנים, כדי להפחית את הכדאיות שבהפצתם. "פייסבוק" גם סיפקה הדרכה לחברי הכנסת ולעוזרים הפרלמנטריים, שהתעניינו לדעת מה לא לעשות כדי לא ליפול במסגרת ההגדרות של שימוש לרעה בפלטפורמה, ואף העניקה ייעוץ להגנת החשבונות הפוליטיים מחשש לפריצה אליהם והוצאת הודעות מזויפות מתוכם.[28]

באמצע פברואר 2019 הכריזה חברת "פייסבוק" על הגברת מאמציה למנוע את הטיית הבחירות בישראל, שכללו "ניקוי אורוות" בבסיסי העוקבים של הפוליטיקאים. במסגרת המבצע הוסרו מהרשת חשבונות מזויפים ואוטומטיים (בוטים), והם נגרעו גם מדפי המתמודדים והמפלגות. "פייסבוק" אף הציעה לעוסקים בתחום המדיה כלי דיווח על רשתות של משתמשים מזויפים.[29] זאת ועוד, באמצע מארס 2019 נכנס לתוקפו בישראל כלי השקיפות במודעות פוליטיות של "פייסבוק", ובכך הפכה ישראל למדינה החמישית בעולם שבה נכנס לשימוש כלי זה, שנועד להתמודד עם האיום של מעורבות זרה וכן עם תעמולה אנונימית.[30]

בתחילת ינואר 2019 הגישו מספר עורכי דין עתירה לוועדת הבחירות המרכזית, שביקשה להחיל את חוקי תעמולת הבחירות גם על התעמולה באינטרנט. העתירה כללה פנייה אל יו"ר הוועדה להוציא צו מניעה שיאסור על המפלגות המשתתפות בבחירות, או על גופים שפועלים בשמן בתשלום או לא בתשלום, לפרסם כל פרסום, הודעה, תגובה, "טוקבק" או "לייק" שאינם נושאים את שם המפלגה או את שם המועמדים שמטעמם הם התפרסמו. בנוסף לכך, העותרים ביקשו לאסור בצו על מפלגות לשלם לכל גוף שיעשה זאת מטעמן או בשמן ולהחיל את הצו על כל פרסום ברשתות החברתיות, בהודעות SMS ובתוכנות מסרים מידיים.[31] יושב ראש ועדת הבחירות המרכזית נענה לעתירה והוציא בשלהי פברואר 2019 צו תקדימי המחייב מפלגות להזדהות כמי שעומדות מאחורי כל סוג של תעמולה באינטרנט וברשתות החברתיות. בנימוקו להחלטה זו הדגיש יושב ראש הוועדה כי מעבר לחבות המשפטית, פרסום תעמולתי אנונימי מקשה על גורמי הביטחון של המדינה להדוף חששות מפני התערבות זרה בבחירות לכנסת ה־21.[32]

---

28 אורי ברקוביץ', אושרית גן אל וטל שחף, "בוטים, פייק ניוז או סטוריז: מה יקבע את גורל הבחירות הקרובות", **גלובס**, 27 בדצמבר 2018.

29 ענת ביין לובוביץ', "פייסבוק יוצאת במבצע להסרת חשבונות מזויפים בישראל; על הכוונת: הבוטים של נתניהו וגבאי", **גלובס**, 20 בפברואר 2019.

30 הגר בוחבוט, "רגע לפני הבחירות: טופס מהיר לדיווח על בוטים וכלי השקיפות של פייסבוק", *Ynet*, 14 במארס 2019.

31 יסמין יבלונקו וטל שחף, "חוק עתיק והתנגדות נתניהו: האם ניתן לפקח על תעמולה באינטרנט?", **גלובס**, 8 בינואר 2019.

32 דניאל דולב, "הסוף לתעמולה אנונימית: מפלגות יחויבו להזדהות בפרסומות ברשת", **וואלה**, 27 בפברואר 2019.

בסוף פברואר 2019 פנתה שורה של מומחי אינטרנט ואבטחת מידע לוועדת הבחירות המרכזית בבקשה שתפעל לקראת הבחירות לאיתור ניסיונות להתחזות באינטרנט, במיוחד ברשתות החברתיות. המומחים הביעו חשש שגורמים זרים ינסו להתערב בבחירות בישראל באמצעות הרשתות החברתיות על ידי הפצת מידע כוזב והפעלת מניפולציות נוספות, וקראו למינוי גורם שישמש כתובת לדיווחים על חשבונות מזויפים ברשתות החברתיות שנועדו להשפיע על מהלך הבחירות. המודל שביקשו הפונים ליצור דומה לזה שמפעילה ישראל נגד הסתה ברשתות החברתיות.

כיום אין למדינה סמכות חוקית לאלץ רשתות כגון "פייסבוק" או "טוויטר" להסיר פרסומים. עם זאת, קיים ממשק המאפשר דיווח ובקשה להסיר פרסום שמהווה הסתה או עבירה על החוק: מחלקת הסייבר בפרקליטות המדינה פונה לרשת הרלוונטית ומבקשת להסיר פרסום כזה. לפי נתונים שפרסמה הפרקליטות, בכ־85 אחוזים מהמקרים הרשתות נעתרות לפנייה ומסירות את הפרסומים.[33]

בנוסף לנאמר לעיל היו מספר יוזמות אזרחיות שפעלו לסמן תעמולה באופן ברור ואחיד, לא לעשות שימוש בחשבונות מזויפים ברשת ולהקפיד על סימון בוטים. במסגרת זו התחייבו היוזמים לא לעשות שימוש במידע פרטי של אנשים כדי להשפיע עליהם בעזרת מניפולציה רגשית, וכן לאבטח את מידע הקמפיין, בכלל זה על ידי הצפנת מסרים אישיים ואבטחת מאגרי מידע.[34] כך גם נוצר טופס מקוון מיוחד המאפשר למשתמשי הרשתות החברתיות לדווח בצורה מהירה ויעילה על בוטים, חשבונות החשודים כמזויפים ותעמולת בחירות אנונימית, ובדרך זו לטפל באופן מהיר ויעיל יותר בבעיה מול הפלטפורמות השונות.[35]

ניכר כי רוב מאמצי ההתגוננות מפני התערבות זרה בבחירות היו יוזמות אזרחיות, ולא ידוע על התארגנות ייעודית מדינתית להתגוננות כזאת, חרף הצהרתו של שירות הביטחון הכללי כי "ביכולתה של מערכת הביטחון לאפשר קיומן של בחירות דמוקרטיות וחופשיות".[36] גם ועדת הבחירות המרכזית פרסמה הודעה לפיה "יחד עם גורמי ביטחון, הוועדה למדה את שאירע במדינות אחרות ומגבשת מתווה פעולה".[37] נכון למועד כתיבת שורות אלו, לא ברור האם היו ניסיונות

---

33 דניאל דולב, "פנייה ליו"ר ועדת הבחירות: 'פעל נגד ניסיונות להשפיע על הבחירות ברשת'", **וואלה**, 25 בפברואר 2019.

34 גיא לוריא ותהילה שוורץ אלטשולר, "מתחייבים לבחירות הוגנות ברשת", המכון הישראלי לדמוקרטיה, 18 בפברואר 2019.

35 בוחבוט, "רגע לפני הבחירות: טופס מהיר לדיווח על בוטים וכלי השקיפות של פייסבוק".

36 אמנון אברמוביץ, "השב"כ: 'יש לנו את הכלים לסכל ניסיונות השפעה זרה בבחירות'", **חדשות 12**, 8 בינואר 2019.

37 דפנה ליאל, "בחירות 2019: מגבשים מתווה נגד התערבות זרה", **חדשות 12**, 9 בינואר 2019.

התערבות זרים בבחירות לכנסת ה־21 ועד כמה צלחו המאמצים לסכל ניסיונות כאלה (אם היו בכלל).

בשולי הדברים יש מקום לציין כי מבקר המדינה הצהיר בתחילת 2019 כי הורה לכל הגורמים במשרדו להיערך לביקורת גם ברשתות החברתיות ובכל המרחב הקיברנטי, וכן לבדוק את היערכות הרשויות להתגוננות מפני מתקפת סייבר על המערכות הממוחשבות שנדרשות לתקינות הליך הבחירות.[38]

סיכום

מטרתו של מאמר זה הייתה לסקור את דרכי ההתגוננות שננקטו נגד אפשרות של התערבות זרה בבחירות לכנסת ב־2019, וזאת לאור ניסיונות דומים שנעשו בדמוקרטיות אחרות במרוצת השנים האחרונות. ניסיונות כאלה כמעט ולא נחשפו עד עתה לציבור בישראל. מה שנחשף נגע בעיקר לשימוש בחשבונות בלתי מזוהים או בחשבונות מזויפים במסגרת השיח הפוליטי הפנימי.

התמקדות הדיון הציבורי בשיח הפנימי מציפה את הצורך בהסדרת השימוש ברשתות במהלך בחירות בפרט, ובהליך הדמוקרטי בכלל. במסגרת זו נדרש, ראשית, להפריד בין מספר היבטים של התופעה, ובראשם השימוש בבוטים. מפלגות עשויות להפעיל או לשכור שירותים מחברות המפעילות בוטים לצורך קידום עמדותיהן או לפגיעה ולהכפשה של מועמדי היריב. מוצע לקבוע שהפעלת בוטים הינה לגיטימית, ובלבד שתעמוד בהוראת ראש ועדת הבחירות המרכזית באשר לצורך לפרסם את שם המפלגה או את שמות המועמדים שמטעמם מופץ המידע.

באשר לתופעת הפרסום של מידע כוזב, קשה לראות כיצד ניתן להקים מנגנון מהיר ורלוונטי (שאינו הליך משפטי) שיקבע מהו מידע כוזב ומהו מידע שאינו כוזב. המרחק בין מנגנון כזה ובין פגיעה חמורה בחופש הביטוי הינו קטן מאוד. לכן, מוצע לאפשר לגורמים פנימיים לפרסם כל מידע, גם אם יהיו מי שיגדירו אותו כמידע כוזב, וזאת כחלק מהשיח הדמוקרטי הלגיטימי. כל אדם או ארגון שיחושו נפגעים מפרסום זה יוכלו לממש את זכותם לקבל סעד ממערכת המשפט במסגרת תביעת דיבה או תביעת נזיקין.

לבסוף, באשר לשימוש בפרופילים בלתי מזוהים על ידי אזרחי המדינה (לא על ידי מפלגות), חברת "טוויטר" מאפשרת קיומו של חשבון אנונימי. לחשבון כזה יש חשיבות רבה מאחר והוא מאפשר למי שאינם יכולים, או אינם רוצים, לחשוף את זהותם (לדוגמה: עובדי מדינה או אחרים המבקשים לשמור על פרטיותם) להשתתף בשיח הפוליטי, ובכך לממש את זכותם להבעת דעה ולחופש ביטוי. שונה הדבר באופן מהותי באשר לפעילות של גורמים זרים שנועדה להשפיע על

38 בוחבוט ואדמקר, "ראש השב"כ הזהיר: מדינה זרה מתכוונת להתערב בבחירות בישראל".

ההליך הדמוקרטי; פעילות זרה כזאת מהווה התערבות גסה בהליך הדמוקרטי, אינה צריכה להיחשב כלגיטימית ומחייבת מאמצי התגוננות וסיכול.

ניכר כי ההתגוננות העיקרית נגד ניסיונות התערבות זרה בבחירות לכנסת בשנת 2019 נעשתה בממד ההגנה מפני מתקפות סייבר קלאסיות. נכון להיום, טרם נחשפה לציבור בישראל יכולת מאורגנת ושיטתית (אם יכולת כזו בכלל קיימת) להגן מפני ניסיונות השפעה מצד גורמים זרים. מערך הגנה מפני ניסיונות השפעה זרים צריך לכלול מספר מרכיבי יסוד. הראשון שבהם הוא יכולת מודיעינית שמטרתה לאסוף מידע ממגוון מקורות, הן גלויים והן חשאיים. לצד יכולת איסוף זו, נדרשת יכולת מחקר וניתוח שתאפשר לגבש תמונת מצב באשר לקיומו של מאמץ זר ועוין להשפיע על ההליך הדמוקרטי במדינה. יכולת זו תידרש לנסות להפריד בין השיח הפנימי (הלגיטימי) ובין השיח החיצוני, אותו יש לסכל.

ניתן לאפיין מספר דרכים לסיכול ניסיונות זרים: הראשונה שבהן היא חשיפת מבצע ההשפעה לציבור, כמובן במגבלות חיסיון והגנת מקורות, ככל שהדבר נדרש. חשיפה כזאת תוכל להוציא את העוקץ ממבצע ההשפעה ולהקטין את השפעתו על הציבור; שנית, ניתן לפנות לחברות הרשת הרלוונטיות, לחשוף בפניהן את המידע ולדרוש את הסרתו ואת חסימת החשבונות המשמשים במסגרת ניסיון זה; לבסוף, ניתן לפעול פרואקטיבית מול הגורם שעומד מאחורי המבצע כדי לסכל את מזימתו.

בנייה של יכולת כזאת מחייבת התארגנות בין־ארגונית וטכנולוגית. מוצע להקים צוות משימה בין־ארגוני מיוחד (צמ"ם) שירכז את הפעילות ויישען על היכולות של כלל ארגוני הביטחון בישראל. בשל הרגישות המובנת, ניתן להכפיף את פעולתו של צוות זה לוועדת הבחירות המרכזית או לגורם אפוליטי אחר. צוות המשימה המיוחד יידרש לרכוש, ובמידת הצורך לאפיין ולפתח, כלים טכנולוגיים שיוכלו לסייע לו בתהליך המבצעי שתואר לעיל.

בשנתיים הקרובות מתוכננות להתקיים למעלה מעשרים מערכות בחירות באירופה ובצפון אמריקה. ניתן להניח שלמדינות שכנות ולמעצמות יהיו אינטרסים מובהקים בבחירות אלו, ואף קיימת אינדיקציה לכך שיהיה ניסיון להתערב בהן.[39] אי לכך, הפקת לקחים מהאפקטיביות של מהלכי ההתגוננות מפני התערבות זרה בבחירות בישראל עשויה להיות בעלת משמעות רבה גם עבור המדינות שבהן צפויות בחירות.

39 Michael Chertoff, Anders Fogh Rasmussen, "The Unhackable Election: What it Take to Defend Democracy", *Foreign Affairs* 98, no. 1 (2019): 157.