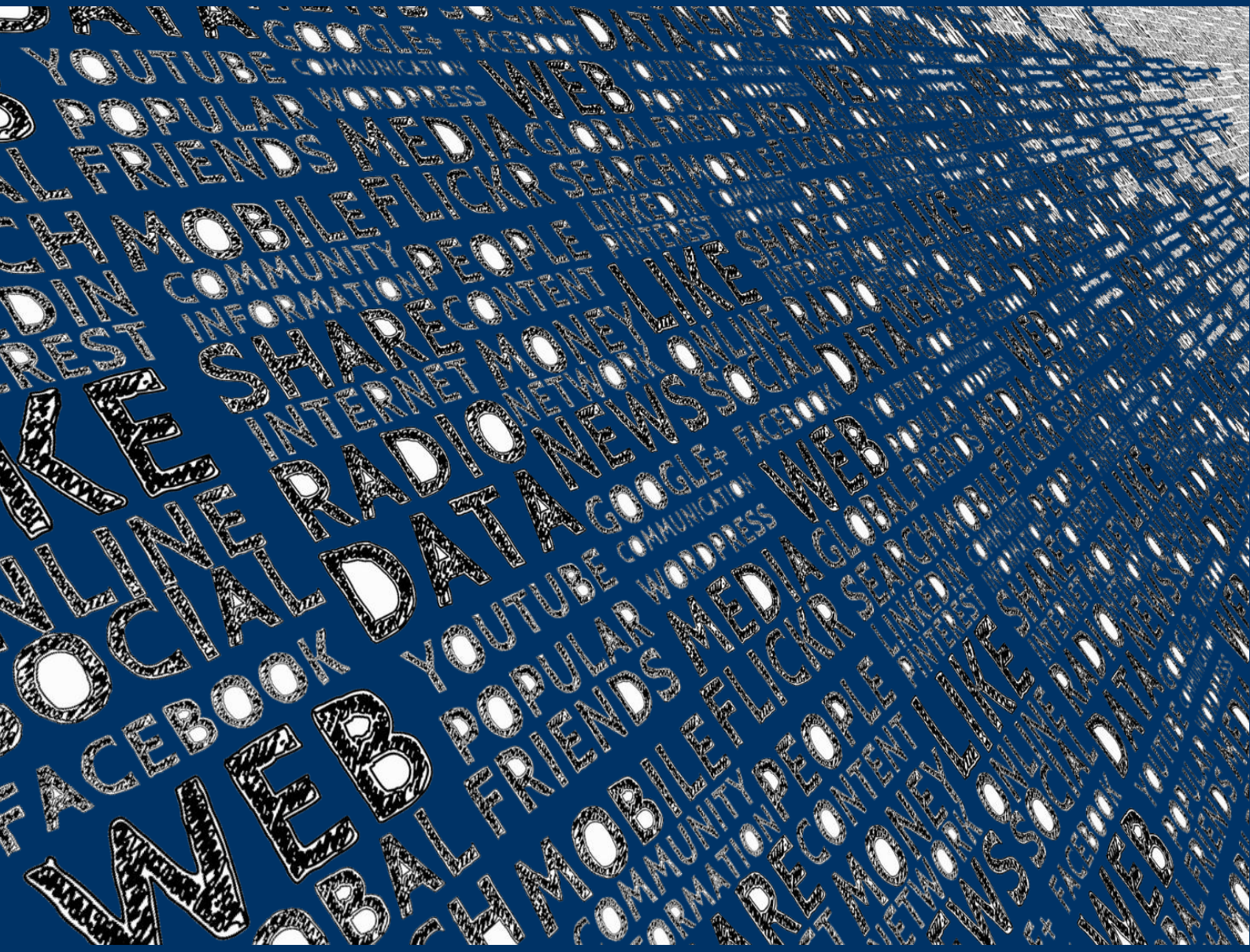
IDC HERZLIYA 25
ICT International Institute for Counter-Terrorism
With the Support of Keren Daniel



טרור דיגיטלי במערכת הבחירות בישראל?

על מעורבות ארגוני טרור ומדינות תומכות טרור במערכת הבחירות

פרופ׳ גבי וימן וצוות דסק טרור ותקשורת

מבוא

לפני כשנתיים, בעקבות ההוכחות הברורות להתערבות רוסית במערכת הבחירות לנשיאות בארה"ב הודיע הממשל האמריקני לעשרות מדינות בעולם כי מערכות הבחירות שלהן היו יעד עבור "פעילי סייבר של ממשלת רוסיה". אין ספק כיום כי באמצעים מקוונים הצליחו הרוסים להתערב במערכות הבחירות של מרבית מדינות המערב ובכללן ארה"ב, גרמניה, בריטניה, צרפת, איטליה, מונטנגרו ועוד. ההוכחות לכך הביאו אפילו את פוטין להודות בחצי פה: לדבריו ייתכן שהאקרים פטריוטים מרוסיה ביצעו מתקפות סייבר "נגד מדינות שהיו להן יחסים מתוחים עם מוסקבה ועשו זאת ביוזמתם בלבד". אולם רשויות הביון האמריקני חשבו אחרת ולאחרונה משרד המשפטים האמריקני הגיש כתבי אישום נגד 12 קציני מודיעין רוסים, כולם עובדי הממשל של פוטין, בחשד שפעלו תחת יד מכוונת להטיית הבחירות בארה"ב. דו"ח שהוכן לוועדת המודיעין של הסנאט האמריקני חשף את קמפיין הדיסאינפורמציה הרוסי, שכלל מיליוני פוסטים ברשתות החברתיות שנועדו להשפיע על הבחירות לנשיאות בשנת 2016. סוכנים רוסים ניצלו את כל הרשתות החברתיות האפשריות, בהן טוויטר, פייסבוק ויוטיוב, כדי להשפיע על השיח המקוון הנוגע למועמדותו של דונלד טראמפ. המטרה של הרוסים, לפי הדיווח, הייתה לבלבל, להסיח את הדעת ולהשפיע על המצביעים. מי שהוביל את המאמצים מטעם הקרמלין היא "סוכנות המחקר האינטרנטי", גוף של ממשלת רוסיה, שפרסם פוסטים בנושאים כמו גזע, הגירה ונשק כדי ליצור מחלוקות ופילוג בקרב הבוחרים האמריקאים. הסוכנים הרוסים, שנגד חלקם כבר הוגשו כתבי אישום בארה"ב בגין התערבות פלילית בבחירות, חילקו את האלקטורט האמריקאי לקבוצות מפתח ולכל קבוצה העבירו מסרים מסוימים.[1]

דו"ח שהוכן לוועדת המודיעין של הסנאט האמריקני חשף את קמפיין הדיסאינפורמציה הרוסי, שכלל מיליוני פוסטים ברשתות החברתיות שנועדו להשפיע על הבחירות לנשיאות בשנת 2016

גם בישראל גבר החשש מהתערבות רוסית במערכת הבחירות הקרובה. ביטוי לכך נתן ראש השב"כ, נדב ארגמן, על "מעצמה זרה" שמתערבת במערכת הפוליטית בישראל באמצעות האינטרנט.[2] תשומת הלב מתרכזת כמובן ברוסיה: הרוסים הפגינו, במספר תקיפות מאורגנות, יכולות מרשימות של חדירה, פצחנות, התערבות ושיבוש באמצעים מקוונים. האקרים רוסים בשליחות פוטין תקפו כבר את אסטוניה (2007) ואת גיאורגיה (2009), פרצו למטה הבחירות של המפלגה הדמוקרטית בארה"ב, שתלו וירוסים מתקדמים בתוך מערכות המיילים של ארגוני ממשלה בגרמניה וגם בפרלמנט הגרמני ובמשרדי מפלגתה של הקנצלרית אנגלה מרקל, ניהלו מתקפת סייבר על

[1] "Five Takeaways From New Reports on Russia's Social Media Operations", *New York Times*, December 17, 2018, https://www.nytimes.com/2018/12/17/us/politics/takeaways-russia-social-media-operations.html

[2] ראש השב"כ נדב ארגמן הופיע ב 7.1.2019 בכנס אגודת ידידי אוניברסיטת תל אביב ובמהלכו דיבר על "מהלך שעלול להשפיע על תוצאות הבחירות" הקרובות שייערכו ב-9 באפריל והזהיר מפני "התערבות של מדינה זרה", ראו https://www.ynet.co.il/articles/0,7340,L-5443404,00.html

מערכות בחירות במדינות רבות ובהן באוקראינה (2014), ארה"ב (2016), צרפת (2017), גרמניה (2017) ובהולנד (2017) והתערבו במשאלי העם בבריטניה, הולנד, איטליה וספרד (2017). במתקפות אלה שולבו אמצעים "קשים" (כמו שיבוש מערכות מחשב של ניהול הבחירות, פריצות למחשבי מנהלי הקמפיינים, הדלפות מתוך נתוני מפלגות ועוד) ואמצעים "רכים" הכוללים בעיקר חדירה לשיח הציבורי והשפעה עליו על-ידי פלישה לרשתות חברתיות.[3]

האיום אינו רק מרוסיה

האם רק רוסיה מאיימת על מערכת הבחירות בישראל? מן הראוי לכלול במפת האיומים המקוונים גם תנועות טרור ומדינות תומכות טרור. כבר בעבר נרשמו ניסיונות של ארגוני טרור ושולחיהם להתערב במערכת הבחירות בישראל. הם עשו זאת, עד כה, בעיקר על-ידי מתקפות טרור סמוך ליום הבחירות. היו לכך השפעות על תוצאות הבחירות. במחקר מתמשך על מספר מערכות בחירות בישראל נמצא כי פיגוע טרור שבוצע בתוך שלושה חודשים לפני הבחירות השפיע על עלייה של מספר מנדטים בתמיכה במפלגות מגוש הימין באזור בו בוצע הפיגוע.[4]

ארגוני הטרור נערכים גם למעורבות במערכת הבחירות 2019. כך למשל, דובר החמאס, פוזי ברהום, הדגיש כי "ההתנגדות האמיצה לא תאפשר לעשות שימוש בדם הפלסטיני כדלק עבור קמפייני הבחירות של הכיבוש, אלא היא מבקשת לשמור על דם הפלסטינים והאינטרסים של בני העם הפלסטיני ...".[5] מנגד, בימים האחרונים פורסם בכלי התקשורת הישראלים כי המועצה החשאית של החמאס החליטה על הסלמה הדרגתית עד הבחירות בישראל מבלי להיגרר למלחמה. זאת בכדי לסחוט הישגים נוספים מישראל בתקופה הקרובה. לדברי מקורות פלסטינים, הנהגת חמאס מבינה כי עד מועד הבחירות נתניהו לחיץ יותר כיוון שהוא אינו רוצה במלחמה ולכן אפשר לכפות עליו להיכנס לשלב השני בהבנות הרגיעה.[6] חמאס אינו הארגון היחיד העוקב אחרי מערכת הבחירות בישראל, גם חזבאללה מנהל מול ישראל, בסיוע איראן, לוחמה פסיכולוגית מאז שנות התשעים. מזכ"ל חזבאללה, חסן נסראללה, הדגיש ב-27 בינואר 2019 בראיון שפורסם באתר moqawama.org:

"אינני רוצה להתערב בבחירות שלהם (של ישראל) מכיוון שבעבורנו נתניהו, ברק ו[כל] פלוני [ישראלי], בין אם הוא מת או בחיים, איננו שונה בדבר". יש להבין "שהאדם הזה [הכוונה לנתניהו] במיוחד בשבועות ובחודשים

---

[3] וימן, גבי. "האם פוטין יתערב גם במערכת הבחירות בישראל?", *העין השביעית*, 18.12.2018, https://www.the7eye.org.il/313117;
"Senate reports show scope of Russian election meddling", *CNN Politics*, December 2018, https://edition.cnn.cm/videos/politics/2018/12/17/russia-2016-report-social-media-ath-vpx.cnn

[4] ברבי, קלוד ואסטבן קלור, "האם ציבור הבוחרים מושפע מטרור? עדות ישירה מהבחירות בישראל", מוסד שמואל נאמן, https://www.neaman.org.il/Are-Voters-Sensitive-Terrorism-Evidence-Electorate-HEB

[5] 22.1.2019. https://twitter.com/HamasInfoEn/status/1087825799993061377

[6] 28.1.2019. https://twitter.com/kann_news/status/1089585334323736582

עד הבחירות עשוי לבצע שגיאות בהערכת התוצאות של המשברים שלו ושל שאיפותיו. זהו אדם שיקריב כל דבר כדי להישאר ראש הממשלה או כדי להישאר מחוץ לכלא״.[7]

אך ארגוני טרור אינם מסתפקים רק במתקפות קונבנציונליות מ״הסוג הישן״, הם בהחלט מודעים לקיומה של לוחמת סייבר, לכלים דיגיטליים ולשימוש בפלטפורמות מקוונות לתקיפה. ישראל הותקפה רבות על-ידי פעילי ארגוני טרור ותומכיהם בתקיפות סייבר שניסו לשבש מערכות חיוניות, לשבש אתרים, לפרוץ לחשבונות ועוד. השאלה הנשאלת היא מה ימנע מארגונים כמו חמאס, חזבאללה, הג׳האד האסלאמי הפלסטיני וממשלים תומכי טרור כמו איראן או סוריה להפעיל טרור דיגיטלי נגד מערכת הבחירות בישראל? בכנס סייבר שנערך לקראת סוף ינואר השנה ציין בנימין נתניהו, ראש ממשלת ישראל, כי ״איראן מתקיפה את ישראל בסייבר על בסיס יומי. אנחנו עוקבים אחרי זה ומונעים את זה מדי יום״.[8]

התערבות במערכת הבחירות באמצעות פריצות מחשבים ואמצעים מקוונים אחרים מצריכה, כמו כל פשע אחר, עמידה בשני תנאים: מוטיבציה ויכולת. המוטיבציה, כפי שראינו בעבר, קיימת. לארגוני טרור ומדינות תומכות טרור יש עניין רב בשיבוש מערכת הבחירות בישראל וגם בהשפעה על תוצאותיה. אך מה לגבי היכולת לפגוע במערכת הבחירות ישראל? לארגוני טרור במזרח-התיכון יש ידע וניסיון בהפעלת לוחמה פסיכולוגית ברשת ובכלל זה התערבות ברשתות חברתיות. בשנת 2017 ניהל החמאס מתקפת סייבר ברשתות החברתיות במסגרתה הוא פתח עשרות פרופילים מזויפים של נשים צעירות ויפות שפנו אל חיילי צה״ל וסחטו מהם מידע מסווג ורגיש. עשרות חיילים נפלו בפח. בחודש יולי 2018 חידש חמאס את המאמץ והפעיל שוב פרופילים מזויפים ברשתות חברתיות כדי להשתלט על ניידים ומחשבים של חיילים וחיילות. הפעם הצליח ארגון הטרור לשדרג את השיטות שלו ולנסות לצוד חיילים וחיילות גם באמצעות אפליקציית הוואטסאפ ורשתות חברתיות אחרות. החמאס אינו יחיד או שונה: כל ארגוני הטרור במזרח-התיכון פעילים ברשתות חברתיות ומנוסים בהתערבות זדונית ברשתות אלה.

הרשתות החברתיות פרוצות לכל ויכולת הניהול, הבקרה וחסימת התכנים נתונה בידי חברות פרטיות כמו פייסבוק, גוגל ומיקרוסופט שעל אוזלת ידן כבר למדנו

לאחרונה נערך מחקר מקיף שסוקר את נקודות החולשה הדיגיטליות במערכת הבחירות הישראלית.[9] המחקר שנערך על-ידי שני בכירי השב״כ לשעבר, רון שמיר ואלי בכר, מזהה את האיומים השונים ומסווג אותם לשלושה סוגים: 1. מתקפות על תהליך ביצוע הבחירות; 2. מתקפות על שחקנים פוליטיים כמו מפלגות, מטות בחירות, מועמדים וקמפיינים; ו-3. מתקפות על הרשתות החברתיות, שעלולות להוות זירה להשפעה

[7] https://www.moqawama.org/essaydetails.php?eid=35453&cid=330

[8] נמר, סתיו, "נתניהו: "איראן מתקיפה את ישראל בסייבר על בסיס יומי"", מעריב און-ליין, 29.1.2019 https://www.maariv.co.il/business/tech/Article-682404

[9] שמיר, רון ואלי בכר, "התקפות סייבר על מערכת הבחירות – איך מתמודדים?", המכון הישראלי לדמוקרטיה ותוכנית המחקר להגנת הסייבר, הפקולטה למשפטים, האוניברסיטה העברית בירושלים, ינואר 2019.

על דעת הקהל והשיח החברתי. ישראל, מעצמת סייבר מוכרת, מסוגלת להתגונן מפני מתקפות מהסוג "הקשה" על מערכות ביצוע הבחירות. הישראלים מתנסים מדי יום באלפי ניסיונות לחדירה ושיבוש של מערכות מחשבים בשירות הממשל, הצבא, הבנקים, אנרגיה, תחבורה ועוד. הניסיון הרב בצד פיתוח חומות הגנה משוכללות יציבו אתגר קשה בפני ההאקרים של ארגוני הטרור, איראן או סוריה. אך מה לגבי תקיפות "רכות" ופחות אלימות? כאן, ההגנה הישראלית תתקשה יותר: הרשתות החברתיות פרוצות לכל ויכולת הניהול, הבקרה וחסימת התכנים נתונה בידי חברות פרטיות כמו פייסבוק, גוגל ומיקרוסופט שעל אוזלת ידן כבר למדנו.

אוואטרים, בוטים וטרולים בשרות הטרור

כיצד יוכלו ארגוני טרור ותומכיהם להתקיף את השיח הפוליטי בישראל? באמצעות רשתות חברתיות ניתן להפיץ שמועות כזב, לקדם "פייק ניוז", להתסיס את השיח ולהקצינו, לפגוע במועמדים ומפלגות, להרחיב שסעים חברתיים ולדרדר את מערכת הבחירות לתהומות של קיצוניות, חוסר אמון, פלגנות ואלימות. כדי לעשות זאת עומדים לרשותם של הטרוריסטים כלים דיגיטליים המוכרים היטב גם מהעולם המסחרי ברשת: "אוואטרים", "בוטים" ו"טרולים". **אווטאר** זו דמות דיגיטלית פיקטיבית המופיעה ברשת ומתחזה לישות אמתית. כך, למשל, אפשר למצוא משתמשים פיקטיביים ברשתות חברתיות המצוידים בשם, פרופיל, תמונות כביכול אמתיות אך בפועל מדובר בדמות דמיונית שמטרתה לקדם מסרים מסוימים. **בוט** הוא תוכנה המיועדת לבצע פעולות ברשת דרך חיקוי משתמש רגיל, כלומר מעין רובוט המתחזה למשתמש אנושי. ניתן להקים רשת בוטים כלומר רשת של עשרות או אף אלפי פרופילים מזויפים ואוטומטיים. בוטים כאלה יכולים באופן מתוכנת לגרום ליותר חשיפה לפוסטים מסוימים (או יותר לייקים, שיתופים ותגובות) ובכך להשפיע על האלגוריתם המקדם אותם ברשת החברתית ולהגדיל את החשיפה. כפי שדווח לאחרונה, במערכת הביטחון בישראל העריכו כי כ-30%(!) מכלל השיח ברשתות החברתיות הוא תוצר של בוטים.[10] **טרול** הוא משתמש שכל מטרתו ליצור פרובוקציה ולהלהיט את השיח. טרול יכתוב דברים מעוררי מחלוקת, שקריים או מכפישים לשם קידום אינטרס. טרול יכול להיות משתמש אמתי, אבל גם אווטאר או בוט.

במערכת הביטחון בישראל העריכו כי כ-30%(!) מכלל השיח ברשתות החברתיות הוא תוצר של בוטים

ארגוני הטרור עושים שימוש בבוטים המהווים רכיב בקמפיין התעמולה אותו הם מקדמים. כך לדוגמא, בחודש ינואר 2019 עלה בערוץ טלגרם בוט השייך לקבוצה התומכת בארגון דאעש ובאמצעותו הוצע מגוון אפשרויות עבור הגולשים: הצטרפות לחשבון הטלגרם של הקבוצה והצטרפות לקבוצת פעילים שתהא אחראית על הפצת חומרי תעמולה של הארגון ברשתות החברתיות דוגמת פייסבוק וטוויטר.

[10] אילנאי, איתי, ""פלישת הבוטים הפוליטיים", *ידיעות אחרונות*, מוסף סוף השבוע, 18.1.2019, עמ' 22-30.

בוט המאפשר יצירת קשר עם בעל חשבון טוויטר של אסיף עבד אל-רחמן, מפקד בכיר סלפי ג'האדי בסוריה

בוט המאפשר הצטרפות לחשבון הטלגרם של דאעש

בוט שפורסם בחשבון טלגרם התומך בארגון דאעש ובו הצעה לתומכי הארגון להצטרף דרך הבוט לקבוצה שתהא אמונה על הפצת חומרי תעמולה של הארגון ברשתות החברתיות

בוט של סוכנות החדשות אבאא של ארגון היאת תחריר אל-שאם בסוריה, המאפשר לתומכי הארגון לשלוח כתבות לסוכנות. בבאנר שהועלה לטלגרם נכתב "היה כתב עבור אבאא.. שלח אלינו חדשות בלעדיות מהאתר שלך"; "שתפו אותנו בדעותיך ובהצעותיך".

גורמים עוינים, ובהם ארגוני טרור ומדינות החסות שלהם, עלולים להפעיל אוואטרים, בוטים וטרולים כדי לפגוע במערכת הבחירות על-ידי השחתה מכוונת של השיח הציבורי

לתקיפה מקוונת באמצעים אלה של מערכת פוליטית זרה, מערכת בחירות, משאלי עם או שיח פוליטי יש יתרונות רבים כאשר מדובר בארגון טרור או תומכי טרור. ראשית, משום שהיא מאפשרת להתערב מרחוק, בעלות נמוכה יחסית, באנונימיות מלאה, וללא צורך בנשק או חומרי חבלה. די במחשב ומקלדת. שנית, משום שהיא מאפשרת גם לקבוצות קטנות, ארגונים ויחידים לנהל מתקפות אפקטיביות. שלישית, משום שיש במתקפות כאלה כדי לערער את הסדר החברתי, להשחית את השיח הפוליטי ולערער את אמון הציבור בשיטה הדמוקרטית ובמערכת הפוליטית כולה. אלה תמיד היו משאת נפשם של ארגוני טרור בכל ההיסטוריה הארוכה של טרור. החברה הישראלית ערב בחירות 2019 היא חברה מפוצלת, מרובדת ושסועה. יש בה עימותים על רקע דתי, כלכלי, חברתי, אתני, לאומי ואידאולוגי. שיח מתסיס ומשסה עלול להעמיק שסעים, להרחיב פערים וליצור קיטוב והקצנה. גורמים עוינים, ובהם החשודים המיידים הם ארגוני טרור ומדינות החסות שלהם, עלולים להפעיל אוואטרים, בוטים וטרולים כדי לפגוע במערכת הבחירות על-ידי השחתה מכוונת של השיח הציבורי. חשוב להבין כי מטרתו של טרור הייתה תמיד לערער משטר ויציבות במדינת אויב. על זריעת מחלוקות והעמקתן, יצירת אי-אמון במשטר, בשלטונות ובמוסדות החברה הדמוקרטית עשויים ארגוני טרור להשיג את מטרתם גם ללא שימוש בפצצות, טילים או פיגועים.

ידע זולג ממדינות חסות לטרור

כאמור, לארגוני הטרור במזרח-התיכון, מדאעש ועד חמאס וחזבאללה, יש את הידע הנדרש להפעיל מעורבות זדונית ברשתות חברתיות וחלקם אף התנסו בכך בעבר. ידע זה אף עלול לזלוג אל ארגוני הטרור ממדינות תומכות טרור. כך למשל, איראן וגם סוריה מצוידות ביחידות האקרים המשרתות את המשטר. במהלך חודש נובמבר 2018, נודע כי איראן הפעילה רשת של 98 אתרים להפצת "פייק ניוז" ב-28 מדינות שונות, ובהן ישראל[11]. הפעילות האיראנית כוונה בעיקר נגד מדינות שידועות כבעלות אינטרסים מנוגדים לאיראן, כמו ארה"ב, בריטניה, אמריקה הלטינית, הודו, סעודיה, ישראל, טורקיה ותימן. כ-40 מהאתרים הפיצו דיווחים בערבית, 22 מהם באנגלית והיתר בעוד עשרות שפות שונות. לאתרי הפייק ניוז האיראניים, נוספו גם חשבונות ברשתות החברתיות, טוויטר, פייסבוק ואינסטגרם. החשבונות שימשו הן כחשבונות רשמיים של האתרים והן כחשבונות מזויפים שהתחזו לגולשים שהפיצו את הכתבות. אך לא רק איראן מעורבת בכך: על-פי מעקב שניהל נועם רותם, יש עשר רשתות בוטים שמופעלות מערב הסעודית, רוסיה, ארה"ב וישראל הפועלות כיום ברשת החברתית טוויטר ומפיצות תכנים הפונים לקהל הישראלי.[12]

במהלך חודש נובמבר 2018, נודע כי איראן הפעילה רשת של 98 אתרים להפצת "פייק ניוז" ב-28 מדינות שונות, ובהן ישראל

בתוך כך, נמצא כי פייסבוק, גוגל וטוויטר הסירו אלפי חשבונות שמקורם באיראן במהלך שנת 2018. פייסבוק מסרה בהודעה, כי איראן ניסתה לקדם תעמולה איראנית באמצעות חשבונות מזויפים שחלקם נמצאו כקשורים לכלי תקשורת שבבעלות איראן. טוויטר מסרה אף היא, כי מחקה חשבונות שמקורם ברוסיה ובאיראן ונועדו להשפיע על בחירות האמצע בארה"ב על-ידי מסרים נגד טראמפ ונגד החזקת נשק. המטרה של איראן היא לקדם נרטיב, שיעלה בקנה אחד עם האינטרסים שלה בפייסבוק, אינסטגרם, טוויטר, גוגל ויוטיוב ולהשפיע על השיח הפוליטי הפנימי בתוך ארה"ב.[13] איראן שממשיכה בהתמדה לחמש ארגוני טרור במזרח-התיכון עלולה להעביר את הידע המתקדם והניסיון המצטבר שלה גם בלוחמת סייבר מתוחכמת לארגוני חסותה.

---

[11] "Global Iranian Disinformation Operation", Clearsky LTD, November 30, 2018.

[12] ברקוביץ, אורי, " האקרים חשפו: רשת בוטים סעודית פועלת בישראל", *גלובס*, 22.1.2019, https://www.globes.co.il/news/article.aspx?did=1001269980

[13] "Facebook deletes Iran-linked pages over effort to sow discord among US voters", *The Guardian*, October 26, 2018, https://www.theguardian.com/technology/2018/oct/26/facebook-iran-pages-deleted-fake-divisive-content-us-uk-voters
"These are the liberal memes Iran used to target Americans on Facebook", *USA TODAY*, August 24, 2018, https://www.usatoday.com/story/tech/news/2018/08/24/how-iran-targeted-u-s-facebook-youtube-and-twitter-liberal-memes/1079882002/
"Facebook, Google and Twitter remove hundreds of accounts from Russia and Iran that tried to influence US elections", *CNBC*, August 22, 2018, https://www.cnbc.com/2018/08/22/facebook-and-twitter-dismantle-disinformation-campaigns-tied-to-iran-and-russia.html
"Revealed: Iran's 'clumsy' troll army pushed one million tweets in effort to destabilize region", *The National*, October 18, 2018, https://www.thenational.ae/world/mena/revealed-iran-s-clumsy-troll-army-pushed-one-million-tweets-in-effort-to-destabilise-region-1.781713

האיראנים גם מנסים להתערב במערכת הבחירות בישראל באמצעות בוטים: דו"ח של חברתVocativ האמריקנית, שהתפרסם בסוף חודש ינואר 2019, מעלה כי ברשתות החברתיות הישראליות אפשר למצוא כיום נוכחות גוברת של בוטים פעילים המופעלים מאיראן, והם מגיבים באופן אוטומטי ומתוכנת מראש לכל התפתחות בישראל ובמערכת הבחירות. כך התגלו כ-350 חשבונות איראניים פיקטיביים ברשתות חברתיות שונות, שמטרתם לייצר שיח סביב מוקדי מחלוקת בחברה הישראלית. המסרים של האיראנים נמצאים בעמודי פייסבוק, טוויטר וקבוצות טלגרם ומגיעים, על-פי ההערכות, לחשיפה פוטנציאלית של כחצי מיליון ישראלים מדי חודש.[14] איראן שממשיכה בהתמדה לחמש ארגוני טרור במזרח התיכון עלולה להעביר את הידע המתקדם והניסיון המצטבר שלה גם בלוחמת סייבר מתוחכמת לארגוני חסותה.

איך מתגוננים?

ראשית, ניתן ללמוד מניסיונן של מדינות אחרות להתגונן מפני מתקפות דיגיטליות על המערכות הפוליטיות והשיח הפוליטי. ניכר כי הפתרון אינו פשוט ומצריך שילוב של אמצעים שונים ופיתוח כלים חדשים לניטור, לזיהוי תקיפה, לייחוס התקיפה ולבלימת התקיפה. ניטור השיח המקוון לשם איתור תקיפות הוא אמצעי בו נקטו מספר מדינות: במדינות אחדות הוחלט להקים גופי מחקר ומעקב ציבוריים ופרטיים שיפעלו כדי לבדוק את המופץ ברשתות, לחשוף שקרים ומניפולציות ולדווח לציבור. גופים כאלה הם למשל ה־StopFake האוקראיני, או ה- European External Action Service (EEAS) של האיחוד האירופי. הניטור הוא כמובן אתגר לא קל המצריך משאבים וכלים מתוחכמים אך מסובכת עוד יותר היא בעיית הזיהוי של התקיפה והתוקף. כדי לדעת מי עומד מאחורי התקיפה הוצעו מספר טכנולוגיות מתקדמות שמאפשרות לזהות ולסמן את התוקף.[15] לבסוף, שורת צעדים הוצעו בחברות שונות ל"חיסון" הציבור: כאן מדובר בהסברה לציבור כדי לזהות מידע מזויף, כיצד להימנע מהפצת מידע כוזב ועוד.[16]

מערך מורכב של פעולות ואמצעים לניטור, זיהוי ובלימה בצד קידום מודעות ציבורית מצריך מאמץ מרוכז ומתואם, רגולציה ומשאבים

---

[14] דו"ח: צבא ה"בוטים" האיראני שמנסה להשפיע על הבחירות בישראל, Ynet, 31.1.2019, https://www.ynet.co.il/articles/0,7340,L-5455832,00.html#autoplay

[15] Lazer et al., The Science of Fake News, 359 (6380) *Science* 1094 (2018)
Constanze Stelzenmuller, The Impact of Russian Interference on Germany's 2017 Elections (Testimony before the U.S. Senate Select Committee on Intelligence June 28, 2017), https://tinyurl.com/ycx4fent

[16] Darrell M. West, "How to Combat Fake News and Disinformation", Brookings (December 18, 2017).

מערך מורכב של פעולות ואמצעים לניטור, זיהוי ובלימה בצד קידום מודעות ציבורית מצריך מאמץ מרוכז ומתואם, רגולציה, משאבים ועוד. לשם כך נדרשת ישראל לכונן גוף מתקדם וחדש לניטור הרשת, להגנה מפני תקיפת השיח, לתקיפת התוקפים ועוד. שמיר ובכר מציעים להקים גוף ייעודי - יחידת ניטור - שיעסוק בניטור תכנים ברשת. הוא לא יעקוב אחר גופים או יחידים שמזוהים כישראלים וכן לא יעסוק בצנזורה של תכנים ברשת. מטרתו תהיה לזהות ניסיון של גופים, ארגונים או מדינות מחוץ לישראל המבקשים לפגוע בשיח הפוליטי בישראל. הם מציעים כי גוף זה שיהיה חלק ממערך הסייבר הלאומי יפעיל תבחינים לזיהוי תכנים שהם חלק ממתקפה של ישות זרה על מערכת הבחירות בישראל. לכשיתגלה מהלך כזה, הוא ידווח ליושב ראש ועדת הבחירות המרכזית ולשב"כ. גופים אלה יתאמו את ההסדרים לעניין האחריות לטיפול בתקיפה ולסיכולה. אולם עד שיוקם גוף כזה ובהתחשב בקרבת הבחירות ומידיות האיומים – ספק רב אם נוכל להקים חומות הגנה דיגיטליות מפני תקיפות ברשת.

בהתחשב בקרבת הבחירות ומידיות האיומים - ספק רב אם נוכל להקים חומות הגנה דיגיטליות מפני תקיפות ברשת

הצלחת מתקפות הסייבר על מערכות הבחירות במדינות רבות מעלה שאלות קשות לגבי יכולת ההתגוננות. ללא ספק נדרש מערך של פעולות הגנה כדי לחזק את יכולתן של דמוקרטיות להתגונן ביעילות מפני התקפות כאלה.

אולם, יש לזכור כי אשר דמוקרטיה ליברלית מבקשת להפעיל אמצעי הגנה עולות החששות לפגיעה בעקרונות הדמוקרטיה הליברלית כגון פרטיות, חופש הביטוי וחופש המידע. רק איזון נכון בין שיקולים של שמירה על בטחון לאומי ובין אלה של הבטחת ערכי הדמוקרטיה - יהיה הפתרון הנכון. אולם, האיום אינו מסתיים ביום הבחירות: לארגוני הטרור ומדינות הטרור יש בהחלט עניין רב להמשיך ולתקוף את השיח הפוליטי, את ההרמוניה החברתית ויציבות החברה הישראלית גם לאחר הבחירות. ישראל, שהשכילה בעבר להגן על עצמה מפני מרבית מתקפות הסייבר תיאלץ להילחם גם בזירת הרשתות החברתיות, אלה העכשוויות ואלה של העתיד.

האיום אינו מסתיים ביום הבחירות: לארגוני הטרור ומדינות הטרור יש בהחלט עניין רב להמשיך ולתקוף את השיח הפוליטי, את ההרמוניה החברתית ויציבות החברה הישראלית גם לאחר הבחירות

המכון למדיניות נגד טרור (ICT) הוקם בשנת 1996 במסגרת המרכז הבינתחומי, הרצליה והפך עד מהרה לאחר ממרכזי המצוינות המובילים בעולם בתחום חקר והוראה אקדמית של סוגיית הטרור.

המכון למדיניות נגד טרור הינו מכון המחקר ומרכז המצוינות היחיד שמתמחה אך ורק בסוגיית הטרור כאשר כל משאביו וכח האדם המחקרי שלו מוקדשים למטרה זו בלבד. במסגרת זו, עושה המכון שימוש בדיסציפלינות אקדמיות בינתחומיות ורב תחומיות מגוונות, ביניהן: מדע המדינה, יחסים בינלאומיים, פסיכולוגיה, סוציולוגיה, משפטים, כלכלה, מחשבים, ביולוגיה, ועוד.

המכון מקיים מעקב שוטף באמצעות כשלושים עובדיו וכמאה עמיתיו (אנשי ביטחון לשעבר ואנשי אקדמיה מאוניברסיטאות שונות בישראל) אחר ארגוני הטרור בזירת המזרח-התיכון ובזירה הגלובאלית - אחר שיטות פעולתם, היערכותם, האידיאולוגיה, המניעים והשיח שלהם, שיתופי-פעולה ויריבויות פנים ובינ-ארגוניות, מערכות היחסים שלהם עם מדינות נותנות חסות, מעמדם ומצבם הכלכלי, ועוד. במסגרת זו, חוקר המכון גם תהליכים אזוריים במזרח-התיכון ובזירה הגלובאלית שמשפיעים על התפתחותם ופעילותם של ארגוני הטרור.

<u>אודות דסק "טרור ותקשורת"</u>

דסק טרור ותקשורת עוסק בניתוח מעורבות ארגוני הטרור ומדינות תומכות טרור במרחב התקשורתי. במסגרת זו, בוחן הדסק את פלטפורמות הפצת המסרים של הטרוריסטים, מבצע ניתוח תקשורתי של המסרים ומפלח את קהלי היעד הרלוונטיים.

בנוסף, מאמרי הדסק יסקרו את דרכי ההתמודדות עם פעילות ענפה זו, בין היתר התמודדות עם מעורבות גורמים זרים, ובכללם ארגוני הטרור, בשיח פוליטי ובבחירות, התמודדות עם התפתחות המסרים של ארגוני הטרור בפלטפורמות התקשורתיות השונות ועוד.

<u>צוות החוקרים:</u>

פרופ' גבי וימן, ראש הדסק	ד"ר ערגה אטד
ד"ר איתן עזאני	לורנה אטיאס-לבובסקי
ד"ר מורן ירחי	נאווה גטאון
ד"ר מיכאל ברק	דורון רוקח
ד"ר לירם שטנצלר-קובלנץ	