הכנסת
מרכז המחקר והמידע

י״ז בסיון תשע״ז

11 ביוני 2017

הפצת מידע כוזב באינטרנט ותקיפות סייבר לשם השפעה על בחירות

מסמך זה נכתב לבקשת יו״ר ועדת המדע והטכנולוגיה של הכנסת, חה״כ אורי מקלב, לקראת דיון משותף עם ועדת המשנה להגנה בסייבר של ועדת החוץ והביטחון בנושא ״הפצת מידע כוזב ותקיפות סייבר לשם השפעה על מערכות בחירות״. המסמך שאיננו ממצה נושא נרחב וסבוך זה, מציג רקע קצר על רשת האינטרנט והדמוקרטיזציה של השיח הציבורי שיוחסה לה; על השימוש בלוחמת סייבר – גניבה, הפצה ושיבוש מידע; על הפצה של מידע כוזב ועל השימוש של גורמים שונים, לרבות מדינות, בכלים משולבים – כולל שימוש במדיה מסורתית ודיגיטלית, ובתקיפות סייבר, במטרה להשפיע על תודעתם של האזרחים, ובפרט לשם השפעה על מערכות בחירות מחוץ למדינתם. בסוף המסמך מוצג דיון קצר בנושא.

רקע

לפני כעשור או יותר הייתה נטייה רווחת לראות באינטרנט זירה חדשה המאפשרת דמוקרטיזציה של השיח הציבורי ושחרור משומרי הסף המסורתיים של התקשורת. השילוב בין אנונימיות, אינטראקטיביות וחסמי כניסה נמוכים (מחשב, מקלדת וחיבור לאינטרנט היו ״כל מה שדרוש״) נתפסו כאמצעי לשבירת ההגמוניה של אמצעי התקשורת על הידע והפצתו.[1] ירידת קרנה של האנונימיות ברשת ועלייתם של מתווכים או שומרי סף חדשים בדמותן של חברות רב-לאומיות השולטות בדרכי הפצת מידע או בחיפוש שלו, וההבנה כי המדובר בזירה של ניהול אינטרסים: כלכליים, אישיים ולאומיים, הסירה חלק מן הקסם האוטופי-נאיבי של ראשית צמיחתה של הרשת.[2]

שלב נוסף שניתן לראות בו ניסיון להשיב את השליטה בתודעת הציבור או לחלופין לראות בו ביטוי לכאוס שבהעדר שליטה במדיה, מסומן בשנים האחרונות בהפצתם של שקרים וחצאי אמיתות המוצגים כתיאור עובדתי ומתפשטים כאש בשדה קוצים באינטרנט – תופעה שזכתה לאחרונה לכינוי "Fake News" (״חדשות מזויפות״). **למרות הנטייה לדבר על תפוצתן של ידיעות ברשת בעיקר במונחי מידת ה״ויראליות״[3] שלהן, מתגלות לאחרונה עדויות שונות המצביעות גם על ידיים מכוונות המשפיעות על התוכן המופץ בדרכים שונות, בהן: יצירתן של ידיעות שקריות, הפצה שלהן באמצעות ישויות פיקטיביות**

---

[1] ראו למשל: ניבה אלקין-קורן, ״המתווכים החדשים ב׳כיכר השוק׳ הווירטואלית״, **ממשל ומשפט** ו(2).

[2] להרחבה על יחסי הכוח במדיה הדיגיטלית ראו:

Karine Nahon, "**Where there is Social Media there is Politics",** in: Routledge Companion to Social Media and Politics, 2016, (Eds.) Bruns A., Skogerbo E., Christensen C., Larsson O.A. and Enli G.S., NYC, NY: Routledge, pp. 39-55.

[3] החוקרים נהון והמסלי מגדירים ויראליות בספרם בנושא כך: ״ויראליות היא תהליך של זרימות מידע חברתיות שבמהלכו אנשים משתפים באופן סימולטני פרט מידע, בתקופה קצרה בתוך רשתות החברתיות שלהם, (לאו דווקא באמצעות ׳מדיה חברתית׳) והיכן שבמהלכו המסר מתפשט מעבר לרשתות [החברתיות] שלהם, בדרך כלל לרשתות רחוקות יותר, אשר כתוצאה מכך נוצר גידול חד במספר האנשים החשופים למידע״. המדדים לוויראליות הם בין השאר: מהירות ההפצה; מספר הנחשפים לתוכן; והמרחק בין מקור המידע לרשתות החברתיות אליהן הוא הגיע.

Karin Nahon, Jeff Hemsley, "**Going Viral**", October 2013, Polity, p:16.

מרובות הנשלטות על ידי מעט גורמים, ערבוב מכוון של מסמכים אמיתיים ופיקטיביים, אמת ובדיה, והכוונה של עיתונאים ושל הציבור אל המידע.

פרקטיקות של ניסיון של מדינות זרות לעצב את התודעה של הציבור במדינה אחרת ולהשפיע על החלטות שלו בנושאים שונים שעל סדר היום אינן תופעה חדשה וישנן עדויות שונות על שימוש בפרקטיקות דומות מזה שנים רבות. עם זאת, רשת האינטרנט הפכה לזירה חדשה ומועצמת של ניסיונות כאלה כפי שיוצג להלן במסמך.

קיומן של בחירות כלליות, חופשיות, חוזרות ונשנות במרווחי זמן הקבועים בחוק הוא מאפיין מרכזי ומהותי של השיטה הדמוקרטית. בחירות נתפסות כשיא של ההליך הדמוקרטי ומבטאות השתתפות אזרחית ומרכיב מרכזי בבניית אמון הציבור במדינה ובמוסדותיה. בשל המשמעות המרובה של תהליך הבחירות במדינה הדמוקרטית, פגיעה בהליכי הבחירות או התערבות חיצונית בהם עלולה להיות בעלת השלכות חמורות. בשנים האחרונות ישנן עדויות לניסיונות שונים לפגוע, תוך שימוש בכלים שונים במרחב הסייבר, בתהליך הבחירות הדמוקרטי הן באמצעות שימוש בכלים טכנולוגיים לפגיעה במערכות מידע המשמשות בתהליכי הצבעה; והן באמצעות ניסיונות השפעה חיצוניים על אמון הציבור או עמדותיו ביחס למועמדים או למוסדות הדמוקרטיים עצמם.[4]

1. מושגים מרכזיים: "פרופגנדה", "דיסאינפורמציה", ו"פייק-ניוז"

המושגים פרופגנדה, דיסאינפורמציה ו"פייק ניוז" משמשים לעיתים בערבוביה, אך בהכללה כולם מסמנים מידה מסוימת של מניפולציה או שיבוש שיטתי של מידע. **בעוד המושג הרחב של פרופגנדה מצוי בשימוש כבר מאז המאה ה-17, והמושג "דיסאינפורמציה" נטבע במהלך המלחמה הקרה בין ארצות הברית ורוסיה, המושג "פייק ניוז" הוא חדש יחסית. עם זאת, התופעות אותן נועדו המושגים הללו להגדיר הן ככלל, לא חדשות.** פרקטיקות של הפצה והטמעה של מידע וניסיונות שונים להשפיע על תודעת הציבור או האויב אינן חדשות. בסקירה של הפרלמנט האירופי בנושא, נטען כי בעוד "פרופגנדה היא הפצה מכוונת של מידע ורעיונות" בייחוד "בצורה מוטה או מטעה", והיא קשורה לרוב לשכנוע פוליטי ולוחמה פסיכולוגית, הרי ש"דיסאינפורמציה" היא "הונאה שיטתית ומכוונת" ומכאן כי היא ניסיון השפעה חריף יותר.[5]

בטיוטה של אמנה בינלאומית בנושא אבטחת מידע אותה ניסתה לקדם ממשלת רוסיה בשנת 2011 צוין כי דיסאינפורמציה היא איום מפתח על שלום וביטחון בינלאומי ב"מרחב המידע" (Information Space). עוד נכתב באותו המסמך כי "לוחמת מידע" (Information warfare) היא עימות במרחב המידע במטרה לגרום נזק למערכות מידע וכן שילוב של קמפיינים פסיכולוגיים המוניים כנגד אוכלוסייה של מדינה במטרה לפגוע ביציבות החברה והממשל.[6]

1.1. חדשות כוזבות - "פייק ניוז"

כאמור לעיל המושג "פייק ניוז" צבר תהודה ותפוצה רבה בשנתיים האחרונות. כתבת מגזין בנושא טענה כי למעשה ההיסטוריה של "חדשות כוזבות" ושל שימוש במידע מעוות או שקרי לשם השגת מטרות שונות

---

[4] דודי סימן טוב, גבי סיבוני וגבריאל אראל, "**איומים קיברנטיים על תהליכים דמוקרטיים**", המכון למחקרי ביטחון לאומי (INSS) טרם פורסם.

[5] European Parliament, "Understanding Disinformation and Fake News", At a Glance, April 2017, accessed: June 7, 2017.

[6] Draft Convention on International Information Security, Ibid.

היא ארוכת שנים.[7] כדוגמא לטענה הם מציינים את עלילת הדם שהתרחשה בעיר טרנטו באיטליה בשנת 1475 במסגרתה ייחסו את הריגתו של ילד נוצרי בן שנתיים וחצי בשם סימונינו ליהודי העיירה ואלו נעצרו ועונו וחמישה עשר מהם נמצאו אשמים והועלו על המוקד. סימונינו הפך לקדוש שהוכר על ידי הכנסייה, ויוחסו לו מיני ניסים, ועלילות נוספות אודות שתיית דם ילדים נוצרים נפוצו ברחבי אירופה כחלק מעלייתה של תופעת האנטישמיות.[8] הכתבה האמורה טוענת כי "חדשות כוזבות" קיימות כבר מאז המצאת הדפוס לפני כ-500 שנה.[9]

לטענת פרופ' קרין נהון, המקרים של מידע כוזב לחלוטין מייצגים רק חלק קטן מן המידע הנפוץ באינטרנט, ונכון יותר לתאר את רוב פריטי המידע (אייטמים) ככאלה המכילים מידע שמידת מהימנותו נמוכה או ככזה הממסגר נתונים או מידע באופן שישרת אינטרס או פרספקטיבה אחת. עם זאת, לטענתה הבעייתיות של מידע שגוי או מסולף גדולה במיוחד בתקופות של אירועים כמו מלחמה או בחירות בהן העומס התקשורתי גבוה במיוחד ושומרי הסף נוטים להפיץ מידע באופן מהיר ללא בדיקה מעמיקה שלו טרם פרסומו. כפועל יוצא הציבור איננו "בודק את העובדות" אלא מגבש עמדות על בסיס מידע שגוי או מבסס עמדות שהוא כבר מאמין בהן על מידע כזה. נהון גורסת כי **הרשתות החברתיות והוויראליות של מידע ברשת הגדילו את היכולת לעשות שימוש בדיסאינפורמציה בתקופת בחירות ולהשפיע על האופן שבו אנשים בוחרים.**[10]

בסקירה של הפרלמנט האירופי בנושא נטען כי ניתן לראות במושג "פייק ניוז" ביטוי לתופעה נרחבת יותר המאתגרת את הדמוקרטיה, המכונה "עידן הפוסט-אמת" (Post Truth Era). מילון אוקספורד מגדיר את "פוסט אמת" כ"קשור ל או מסמן נסיבות בהן עובדות אובייקטיביות משפיעות פחות בעיצוב דעת הקהל מפנייה לרגש או לאמונה אישית". עוד נטען בדוח הפרלמנט האירופי כי ביטויים של בעלי תפקידים בממשל האמריקני הנוכחי בהם טיעונים ביחס ל"עובדות אלטרנטיביות", והתייחסויות לרשתות תקשורת נפוצות כאל "פייק ניוז"; "אויבי העם" ועוד, הם ביטויים לעידן זה, וכי ארגונים העוסקים בחופש תקשורתי ראו בביטויים של נציגי ממשל בארצות הברית איום על חופש התקשורת שנתפס כ"כלב השמירה של הדמוקרטיה".[11]

1.2. שימוש ברובוטים (Bots) להפצת מידע כוזב ומאפייני התנהגות רשת נוספים

חוץ מהניסיונות לעמוד על מאפייניו של תוכן שהוא "ויראלי", **הניסיונות לבצע מניפולציות על דעת הקהל או על התפוצה של מידע ברשת נעשים גם באמצעות מה שמכונה "רובוטים חברתיים" (Social bots).** רובוטים אלה הם למעשה אלגוריתמים ממוחשבים שנועדו ליצור התחזות למשתמשי רשת אמיתיים, לרכוש ולנהל זהויות במדיה חברתית וכך לשמש כפלטפורמה להפצה מכוונת של תוכן. הפצת תוכן כאמור יכולה להיעשות לשם מימוש אינטרסים שונים – מסחריים, פוליטיים או פליליים ומידת השימוש לרעה שהם מגלמים שונה, אך המשותף להם הוא בשימוש בטכנולוגיות אוטומציה ליצירת זהות פיקטיבית כדי להשפיע על זרימת המידע ותפוצתו.

---

[7] "The Long and Brutal History of Fake News", Politico Magazine, Jacob Soll, December 18, 2016. Accessed: June 7, 2017.

[8] קדושתו של סימונינו בוטלה בהמשך על ידי הכנסייה.

[9] "The Long and Brutal History of Fake News", Politico Magazine, Jacob Soll, December 18, 2016. Accessed: June 7, 2017.

[10] פרופ' קרין נהון, בית הספר למידע אוניברסיטת וושינגטון והמרכז הבינתחומי הרצליה, שיחת טלפון, 28 במאי, 2017.

[11] European Parliament, "Fake News and the EU's Response", At a Glance, April 2017, accessed: June 7, 2017.

בין ההשפעות שחוקרים מייחסים לשימוש ברובוטים העוסקים באיסוף והפצה של מידע ברשת נטען כי היו מקרים שבהם מידע כוזב ברשת על אירוע טרור או על חברה מסחרית כלשהי השפיע על דפוסי המסחר הבורסאי במניות. השפעות אלה עשויות לנבוע מיצירת חרדה בשל אירוע שלא התרחש או בשל יצירת עניין מפוברק בחברה כלשהי. זאת בהתבסס הן על מגמות של ויראליות והן על השפעה של רובוטים העוסקים באגרגציה (איסוף ועיבוד) של מידע חדשותי ואחר לשם הפצתו או כדי להסיק ממנו ביחס לעתיד להתרחש בבורסה. עוד נטען כי השימוש ברובוטים במדיה חברתית עשוי להשפיע על תפיסת המציאות של משתמשי רשת וזאת כאמור באמצעות התחזות למשתמשים אמיתיים, איסוף עוקבים, פרסום של תוכן מהרשת בדפוס שנראה כאנושי ועוד.[12]

במאמר המבוסס על ניתוח וניטור של תוכן מהרשת החברתית "טוויטר" נטען כי מניתוח ה"ציוצים" והזהויות בטוויטר בין ה- 16 בספטמבר ל-21 באוקטובר 2016, עולה כי כ-400,000 חשבונות (שיעור המייצג כ-15% מן החשבונות שנטלו חלק במחקר) שהשתתפו בשיחות ביחס לבחירות לנשיאות ארצות הברית הופעלו כפי הנראה באמצעות רובוטים, וכי רובוטים אלה נטלו חלק בכ-19% מן השיחות בנושא בתקופה האמורה. לטענת החוקרים השימוש ברובוטים והשפעתם על השיח סביב הבחירות עלולים לגרום למספר בעיות ממשיות: 1) ההשפעה יכולה להיות מופצת מחדש בין חשבונות חשודים רבים שעלולים להיות מופעלים למטרות זדוניות; 2) הפצה של מידע מוכוון כאמור יכולה לגרום ליצירתו של קיטוב בשיח הפוליטי ברשת; 3) היקף הפצתו של מידע מוטעה או מידע לא מבוסס יכולה להיות מועצמת.[13]

בהקשר להטיות בזרימת המידע ברשת, יש לציין שתי תופעות: אהבת הדומה ורצון להתבלטות - המשפיעות על ההתנהגות ברשת. אהבת הדומה- "הומופיליה" היא הנטייה האנושית להתחבר אל הדומים לנו (אתנית, גיאוגרפית או אידיאולוגית). נטייה זו היוצרת ברשת האינטרנט תופעות של "קבוצתיות" או "עדריות" היא ראשית תופעה חברתית, אך היא גם מועצמת על ידי ספקיות שירות ברשת דוגמת רשתות חברתיות או מנועי חיפוש המציפים לנו אנשים או מידע התואם את עמדותינו, מתוך הכרה בנטייה החברתית להעדיף אנשים או עמדות הקרובות לאלה שלנו. הבעיה במצב זה היא בכך שרבים עדיין רואים בייצוג האינטרנטי של המתרחש בעולם מעין "מפה" אמיתית שלו, ולא מבינים כי זהו ייצוג סובייקטיבי המותאם למשתמש וקשור למיקום הגיאוגרפי שלו, למצבו הכלכלי-חברתי, הבינאישי ועוד. בהקשר לבחירות, מציינת פרופ' נהון כי בבחירות לכנסת ה-20 ציינו גולשים רבים ממחנה השמאל כי לפי התכנים אליהם נחשפו בפייסבוק הם שיערו כי השמאל עתיד לנצח בבחירות. להיבטי ההשפעה על זרימת המידע כאמור השפעה רבה, שכן לדוגמא במקרה האמור, ההנחה כי "השמאל הולך לנצח" עלולה הייתה למשל להוביל מצביע שמאל לא לפקוד את הקלפי מתוך תחושה ש"בכל מקרה ננצח".[14]

למרות הנטייה לראות בריבוי הדעות של הרשת אפשרות לפתיחות וגיוון בשוק הדעות, מחקרים שונים הצביעו על שילוב של אלמנטים בהם: עומס מידע, אהבת הדומה ורצון להתבלטות בתוכן, לצד תחושת אנונימיות כמאפיינים שגררו הקצנה, קיטוב ואף תופעות של הסתה.[15]

---

[12] Ferrara et al, "The Rise of Social Bots", Communication of the ACM, Vol. 59, No.7, July 2016. Accessed: June 7, 2017.

[13] Bessi, A., and Ferrara, E., "Social Bot Distort the 2016 U.S Presidential Election Online Discussion", First Monday, Vol. 21, No.11, November 2016. Accessed: June 7, 2017.

[14] קרין נהון ושירה ריבנאי בהיר, "תעמולת בחירות בראי האינטרנט והרשתות החברתיות", חומר רקע לוועדת ביניש, ינואר 2016.

[15] שם. וכן:

Media Manipulation And Disinformation Online, Alice Marwick and Rebecca Lewis, Data and Society, May, 2017. Accessed: June 7, 2017.

יש לציין כי למרות העיסוק הרב בהשפעות של מדינות זרות על תהליכי בחירות במדינות שונות, בפרט ביחס למקרה של ארצות הברית, **מחקר נרחב שפורסם לאחרונה מעלה טענות לפיהן שימוש מניפולטיבי של אזרחים או קבוצות עניין בתוך ארצות הברית (שאינם חלק ממאמץ מדינתי להשפעה) על סביבת הרשת, הפצתו של מידע כוזב ועוד השפיעו על סדר היום הציבורי טרם הבחירות ועל דפוסי הסיקור של המועמדים השונים.** המחקר טוען כי מוטיבציות שונות, של שחקנים פרטיים או קבוצות עניין, כמו: הפקת תמורה כלכלית, זכיה במעמד ובתשומת לב, וקידום אידיאולוגיה של קבוצות מסוימות (Sub Culture) תוך ניצול מאפייני רשת, השפיעו על הפצה של שמועות ומידע כוזב ותרמו להשפעה על סדר היום. בין השאר טוענות מחברות המסמך כי תוכן שהחל את דרכו בערוצי מדיה דיגיטליים משניים, עבר בהדרגה לערוצי תקשורת הנתפסים כ"רציניים" וממוסדים יותר והשפיעו על הטיות נרחבות יותר בדפוסי הסיקור של המועמדים ועל "מתן קול" באופן לא מידתי לתופעות או עמדות שוליים ולמידע כוזב.[16]

1.3. "צעדים פעילים"(Active Measures) ו"מלחמה היברידית"

בדיון שנערך בוועדה לענייני מודיעין בסנאט האמריקני בסוף מרץ 2017 העיד פרופ' רוי גודסון (Godson), מומחה לממשל ולשעבר יועץ למועצה לביטחון לאומי, בנושא דיסאינפורמציה. גודסון מגדיר "צעדים פעילים" (Active Measures) כמושג שנועד לתאר טכניקות גלויות וסמויות להשפיע על אירועים והתנהגויות של או ב-מדינות אחרות (ולטענתו נעשה בו שימוש על ידי הממשל הרוסי). צעדים כאמור עשויים לכלול: השפעה על מדיניות של מדינה אחרת; ערעור הביטחון במנהיגות ובמוסדות המדינה; פגיעה ביחסים בין מדינות אחרות ופגיעה באמינות והחלשה של מתנגדים ממשלתיים או לא ממשלתיים. צעדים אלה עושים לעיתים קרובות שימוש בהונאה של "המטרה" (ממשלות זרות, אליטות, הציבור הרחב) ושיבוש של תפיסת המציאות שלה. ערוצי ההפעלה של "צעדים פעילים" עשויים לכלול אפיקי השפעה רשמיים דוגמת ערוצי פרופגנדה ממומנים, יחסים דיפלומטיים ודיפלומטיית תרבות; ואפיקי השפעה סמויים יותר – דיסאינפורמציה מילולית או כתובה, סוכני השפעה וארגוני קש (המסתירים תחת חזות לגיטימית פעילות כזו).[17]

גודסון ציין בעדותו בפני הסנאט כי השימוש ב"צעדים פעילים" קיים ברוסיה ובעבר בברית המועצות יותר ממאה שנה וכי טכניקות ההשפעה הללו מקנות לכלכלה חלשה יחסית ומוסדות פוליטיים לא יציבים יתרון טקטי ואסטרטגי לשם השפעה על תוצאות פוליטיות מחוץ לארצם. עם זאת, גודסון ציין בעדותו כי גם ארצות הברית ודמוקרטיות ליברליות אחרות עשו מאמצים להשפיע על ערכים שהן דוגלות בהן במדינות זרות: חיזוק או שימור מגמות או ישויות בעלות אלמנטים דמוקרטיים, חיזוק עקרונות ליברליים כמו זכויות אדם, חופש דת, שלטון חוק ועוד, וזאת בין השאר גם כדי לחזק מדיניות חוץ כלכלית ואסטרטגיה צבאית. לטענת גודסון, רוסיה ממשיכה לעשות שימוש ב"צעדים פעילים" במשך שנים רבות והממשל הנוכחי העלה את העצימות של מאמצי השפעה כאלה כדי להגדיל את כוחה ואת השפעתה של רוסיה ולקדם את והאינטרסים שלה, ללא צורך בהסלמה למלחמה או הפעלת כוח ישיר בהיקפים נרחבים.[18]

---

[16] Media Manipulation And Disinformation Online, Alice Marwick and Rebecca Lewis, Data and Society, May, 2017.

[17] Written Testimony of ROY GODSON to the Senate Select Committee on Intelligence, Open Hearing, March 30, 2017, "Disinformation: A Primer in Russian Active Measures and Influence Campaigns." accessed: June 7, 2017.

[18] Ibid.

בדיון אחר בפני הוועדה לכוחות מזוינים של בית הנבחרים בארצות הברית במרץ 2017 ציין מומחה אחר בנושא, ד"ר צ'ויוויס (Chivvis), כי קידום האינטרסים הרוסים נעשה באמצעות מה שחוקרים מכנים **"לחימה היברידית" (Hybrid Warfare)**. בין המאפיינים העיקריים של לחימה היברידית ציין החוקר את: 1) השימוש הזהיר או הנבון בלחימה או כוח ישיר; 2) המשכיות הלחימה ושינויי מתמיד בעצימות שלה; 3) ומיקוד באוכלוסייה עצמה. צ'ויוויס ציין כי "ארגז הכלים" ללוחמה היברידית כולל בתוכו שלל כלים בהם: "מבצעי מידע"; "תקיפות סייבר"; שימוש בנציגים עקיפים בעלי אינטרסים משותפים; השפעה כללית; השפעה פוליטית ועוד.[19]

עוד ציין צ'ויוויס בעדותו כי לבד מן העדויות על התערבות רוסית בבחירות לנשיאות ארצות הברית, מועלים חששות להתערבות של גורמים זרים גם ביחס לבחירות הצפויות בגרמניה, בצרפת[20] ובאיטליה וטענות כאמור הועלו גם ביחס לניסיונות השפעה על משאל העם בבריטניה על עזיבת האיחוד האירופי.

מן האמור עד כה עולות כמה תובנות בסיסיות שנראה כי אינן פרטיקולאריות למקרה מסוים:

1. **תקיפות סייבר או מהלכים לשיבוש מידע גברו בשנים האחרונות, אך הם אינם תופעה חדשה;**
2. **תקיפות סייבר או שיבוש מידע אינם בהכרח יעד כשלעצמו אלא נועדו, לעיתים קרובות, כדי להשיג אינטרסים נרחבים יותר.**
3. **תקיפות סייבר או שיבוש מידע הם כלים שמפעילים לא רק יחידים (האקרים/פושעים/ארגונים קטנים) אלא גם ארגונים מדינתיים סדורים שיש להם משאבים בסדרי גודל שונים ואינטרסים שונים.**
4. **בעוד ההגנה על תשתיות חיוניות או ארגונים שונים מתקיפות סייבר היא אתגר שניתן לתחום את גבולותיו, המלחמה על התודעה של הציבור שעשויה להיעשות באמצעות שיבוש מידע, הפצה של מידע כוזב ועוד היא מורכבת עוד יותר כיוון שהיא מתנהלת בכלל המרחב המקוון ולא רק במקומות ספציפיים או כלפי יעדים ספציפיים.**

2. דוחות על ניסיונות השפעה או תקיפות סייבר בהליכי בחירות או משאל עם

להלן יוצג מידע ביחס לטענות בדבר ניסיונות השפעה על הבחירות האחרונות לנשיאות ארצות הברית, מתוך דוח קהילת המודיעין של ארצות הברית; וכן מידע בדבר החששות למתקפת סייבר והשפעה על הליכי משאל העם בבריטניה בשאלת ההשתייכות לאיחוד האירופי מתוך דוח של בית הנבחרים הבריטי.

בפתח הדברים חשוב לציין כי ההתייחסות במסמך לנושא הטענות להשפעה רוסית על הבחירות לנשיאות ארצות הברית איננה ממוקדת ב"שאלת הייחוס" – האם רוסיה נקטה או לא נקטה בפעולות שמייחסים לה, אלא מהווה פתח להצגה עקרונית נרחבת של הנושא. במאמר מוסגר יצוין כי יש מקום לשער כי גם מדינות אחרות נוקטות או עשויות לנקוט בצעדים המיוחסים לרוסיה. ההרחבה ביחס למקרה זה נובעת מריבוי העדויות וההתייחסות לנושא והיא יכולה לשמש כדי לסמן אותו בצורה ברורה. אין באמור כמובן, כדי להביע עמדה בנושא זה.

---

[19] "Understanding Russian "Hybrid Warfare" And What Can Be Done About it", Christopher S. Chivvis, Testimony presented before the House Armed Services Committee on March 22, 2017. Accessed: June 7, 2017.

[20] עדותו ניתנה במרץ 2017, טרם הבחירות בצרפת.

2.1. דוח קהילת המודיעין על ניסיונות ההשפעה על הבחירות לנשיאות ארצות הברית[21]

בינואר 2017 פרסם משרד הממונה על המודיעין הלאומי של ארצות הברית (ODNI) דוח תחת הכותרת "הערכת הפעולות והכוונות של רוסיה בבחירות האחרונות לנשיאות ארצות הברית: התהליך האנליטי וייחוס אירועי סייבר".[22] למרות שכאמור לעיל שאלת הייחוס ככלל ובפרט במקרה ספציפי זה איננה במוקד עניינו, מן הדוח עולים ממצאים חשובים המבהירים את דפוסי הפעילות והאיומים השונים במרחב הסייבר ובמידת מה גם מחוצה לו ביחס למערכות בחירות, ולכן להלן יוצגו נקודות מרכזיות מן הנטען בדוח.[23]

בפתח הדוח נכתב כי הניסיונות להשפיע על מערכת הבחירות בשנת 2016 הם הביטוי העדכני של השאיפה ארוכת השנים של מוסקבה לערער על סדר היום הדמוקרטי-ליברלי המובל על ידי ארצות הברית, אך פעולות אלה מסמנות הסלמה ברמת הישירות, רמת הפעילות והיקף המאמץ בהשוואה לניסיונות קודמים. כותבי הדוח – שמייצג את ההערכות המשותפות של שלוש סוכנויות הביון המרכזיות בארצות הברית[24], מעריכים כי מקורה של ההוראה לנהל "קמפיין השפעה" (Influence Campaign) ביחס לבחירות במטרה לערער את אמון הציבור בתהליך הדמוקרטי בארה"ב, להוציא לעז על מועמדת מסוימת ולפגוע בסיכויי הבחירה שלה – הוא בדרג הגבוה ביותר, דהיינו בראש המדינה שיזמה זאת. בנוסף, הם מעריכים כי ניסיונות ההשפעה נבעו בין היתר מכך שהממשל הזר פיתח העדפה ברורה למועמד מסוים בבחירות. על פי הדוח, טקטיקות ההתנהלות של הממשל הרוסי השתנו תוך כדי מערכת הבחירות בהתאם להערכות באשר לסיכוי ההצלחה של המועמדים. נטען כי קמפיין ההשפעה עשה שימוש באסטרטגיות משולבות שכללו פעולות גלויות וסמויות –תקיפות סייבר לצד שימוש בסוכנויות ידיעות במימון מדינתי, מתווכים מצד שלישי ומשתמשי מדיה חברתית שפעלו תמורת תשלום.

עוד נטען כי סוכנויות הביון הרוסי פעלו במבצעים לתקיפת סייבר כנגד מטרות ספציפיות המשויכות למערכת הבחירות בשתי המפלגות הגדולות וכן ביצעו איסוף של מודיעין כנגד מכוני מחקר מובילים (Think Tanks) וקבוצות לובי מרכזיות שהסוכנויות גרסו כי צפויה להיות להן השפעה מרכזית על הפוליטיקה האמריקאית; וכי כבר ביולי 2015 השיגו שירותי הביון הללו גישה אל רשתות המחשבים של הוועידה הלאומית הדמוקרטית והם שמרו על גישה זו לפחות עד יוני 2016. כלומר, אין המדובר בהתארגנות קצרת מועד אלא בהערכות יסודית וממוקדת.[25]

---

[21] Office of the Director of National Intelligence, Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution, 6 January 2017. Accessed: June 7, 2017.

[22] יצוין כי המידע שפורסם בדוח הוא חלקי בלבד וכי טרם גילויו לציבור הוסרו ממנו חלקים חסויים.

[23] עם מועד סיום כתיבת מסמך זה, פורסמו בתקשורת ידיעות לפיהן ממידע חסוי שנחשף על ידי עובדת חברה קבלנית של ה-NSA בארצות הברית עולות בין השאר טענות על ניסיונות תקיפה רוסית של מערכות מידע של ועדות קלפי, כולל איסוף מידע על חלק מעובדי ועדות קלפי וניסיונות פישינג ממוקדים כדי להשיג פרטי גישה למערכות מידע. ראו למשל:

ABC News, "Leaked NSA doc highlights deep flaws in US election system", June 6, 2017.

[24] CIA; FBI; NSA

[25] בעדות בפני הוועדה של הסנאט לענייני מודיעין ב-30 במרץ 2017 העיד פרופ' תומס ריד העוסק באבטחת מידע כי בין ה-10 למרץ ל-7 באפריל 2016 סימנו שירותי ביון רוסים (GRU) 109 עובדים בקמפיין של קלינטון ושלחו להם 214 הודעות דואר אלקטרוני למטרת "פישינג" (כדי להשיג סיסמאות וגישה למחשב ולתוכן המצוי בו); הם שלחו גם דוא"ל למייל הישיר של קלינטון בניסיון לגנוב לה סיסמא באמצעות קישורית (לינק) לשינוי פרטי הסיסמא שלה. לאחר גניבתו של מידע, בתוכו דוא"ל ומסמכים רשמיים מלפחות 13 אזרחים אמריקאים בעלי תפקידים בכירים בממשל, הוא הופץ בצורה שיטתית ובמועדים שנקבעו בכוונה באמצעות אתר וויקיליקס.

Disinformation a Primer In Russian Active Measures and Influence Campaigns, Hearings Before The Select Committee on Intelligence, United States Senate, 30 March 2017, Thomas Rid, Opening Statement.

בדוח מצוין כי סוכנויות הביון האמורות עשו שימוש בהפצה של מידע שנגנב במהלך תקיפות סייבר והעבירו מידע כזה לגופי תקשורת שונים וכן לוויקיליקס; וכי הסוכנויות השיגו ושמרו על גישה לגורמים שונים בוועדות הבחירות ברמה המקומית וברמת המדינה. עם זאת, המשרד לביטחון המולדת מעריך כי סוג המערכות שסומנו או סוכנו על ידי הסוכנויות הזרות לא כללו אומדנים או סקרי בחירות.

בנוסף הדוח מציין כי הפרופגנדה הרוסית עשתה שימוש בערוצי מדיה שונים שרמת הזיקה שלהם למדינה שונה ונעה בין בעלות מלאה וגלויה לבין זיקות סמויות או מועטות יותר. הסיקורים של הבחירות בערוצים שבבעלות המדינה היו בעלי סנטימנט חיובי כלפי טראמפ, ושלילי כלפי קלינטון. מומחה לנושא טוען כי השימוש המקצועי ב"טרולים"[26] במדיה החברתית – כדי שיציגו עמדות מוכוונות מראש בעד טראמפ, החל כבר בדצמבר 2015.

בסיכום עיקרי הדברים נכתב בדוח כי ההערכה היא כי רוסיה תסיק מסקנות ותפיק לקחים מקמפיין ההשפעה על הבחירות לנשיאות ארצות הברית כדי להשפיע בעתיד גם על מערכות בחירות, במדינות נוספות ברחבי העולם, בהן ביחס לבנות ברית של ארצות הברית. מחברי הדוח מעריכים כי מיד לאחר הבחירות החל המודיעין הרוסי לסמן ולפעול כנגד יעדים ספציפיים בממשל בהם: פקידי ממשל; אנשים הקשורים למכוני מחקר ומדיניות; ארגוני מגזר שלישי בתחומי ביטחון לאומי ומדיניות חוץ, וזאת כדי להכין אפשרויות לקמפיין השפעה עתידי וכדי ללמוד על היעדים והתוכניות העתידיות של הממשל הנוכחי.

מעניין לציין כי בעדותו של ראש ה- CIA לשעבר ג'ון ברנן בפני ועדת המודיעין של בית הנבחרים של הקונגרס האמריקאי במאי 2017 ציין ברנן כי ההתערבות הרוסית בבחירות לנשיאות ארצות הברית נעשתה חרף מחאות ואזהרות מפורשות של הממשל האמריקאי שלא להתערב בהליך. ברנן ציין בעדותו כי הוא שוחח בנושא זה בצורה ישירה ומפורשת עם הראש הפ-ס-ב (FSB) שירות הביטחון הפדרלי הרוסי, וכי האחרון הכחיש את המעורבות הרוסית אך ציין כי יעביר את המסר לראש ממשלתו.[27]

2.2. דוח בית הנבחרים הבריטי בנושא לקחים ממשאל העם בעניין ההשתייכות לאיחוד האירופי[28]

ביום ה-23 ביוני 2016 התקיים בבריטניה משאל עם בשאלת ההישארות או העזיבה של בריטניה את האיחוד האירופי. דוח של הוועדה למנהל ציבורי ועניינים חוקתיים של בית הנבחרים הבריטי בנושא מציין כי ב-7 ביוני קרס אתר ההרשמה להצבעה. אתר ההרשמה ששימש כדי לאפשר למי שזכאי ומעוניין להצביע ושפרטיו אינם מצויים ברשות המדינה להירשם להצבעה, קרס שעות ספורות בטרם הוא נסגר לרישום להצבעה במשאל העם בעניין האיחוד האירופי. כפועל יוצא מן הקריסה נדרשה הממשלה לשנות תקנות בחוק באופן מיידי.[29] משרד הקבינט הבריטי ושירותי ממשל זמין הבריטים טענו כי הסיבה לקריסת האתר

---

[26] המושג "טרול" נועד לסמן משתמש רשת העושה שימוש מניפולטיבי ברשת או במשתמשים אחרים למטרות שונות, החל בלעג ובזלזול וכלה בהרס מוניטין של פרטים או ארגונים וחשיפה של מידע אישי מביך. השימוש הרב במושג "טרול" כולל תחתיו שלל התנהגויות א-סוציאליות שונות.

Media Manipulation And Disinformation Online, Alice Marwick and Rebecca Lewis, Data and Society, May, 2017, p: 4.

[27] "Open Hearing on the Russia Investigation Task Force", U.S House of Representatives Permanent Select Committee on Intelligence, May 23, 2017.

[28] House of Commons, Public Administration and Constitutional Affairs Committee, "Lessons learned from the EU Referendum", Twelfth Report of Session 2016–17, Published on 12 April 2017. Accessed: June 7, 2017.

[29] בשל קריסת האתר והחשש מהשפעה על אפשרויות ההשתתפות של האזרחים, ביצעה הממשלה ב-10 ביוני שינוי בתקנות משאל העם כך שתאריך ההרשמה להצבעה הוארך עד ה- 10 ביוני בחצות הלילה, תקנות אלה אושרו על ידי הפרלמנט הבריטי.

היתה "ביקוש חסר תקדים לשירות". דוח ועדת הבחירות בנושא ציין כי בעיית הביקוש הוחמרה בשל שיעור גבוה של רישומים חוזרים (38%) היינו אנשים שכבר היו רשומים ונרשמו שוב; ושיעור זה היה אף גבוה יותר בתקופת האורכה (בין ה-7 ל-9 ביוני) כאשר 46% מן הרישומים להצבעה היו רישומים חוזרים. יו"ר ועדת הבחירות הבריטית ציינה בפני הוועדה כי בשלב מסוים במהלך משאל העם הופצה שמועה בפייסבוק לפיה על המצביעים להירשם בשנית כדי לוודא את אפשרות ההצבעה שלהם, מה שכנראה גרר השפעה נוספת על היקף ההרשמות הכפולות .

הוועדה למנהל ציבורי ועניינים חוקתיים של בית הנבחרים הבריטי מציינת בדוח שלה כי למרות שאין בידי הוועדה ראיות ישירות, יש חשיבות למודעות לאפשרות של התערבות זרה בבחירות או משאל עם. למרות דוח שטען כי המדובר בבעיה טכנית, בעיה של פערים בבעלות טכנית ובניהול סיכונים, **יש אינדיקציות שהקריסה של האתר נגרמה בשל מתקפת מניעת שירות מכוונת (DDOS)**. הוועדה מציינת כי היא מודעת לקלות שביצירת מתקפת מניעת שירות באמצעות בוטנטים[30] וכי העילות למתקפה כזו יכולות להיות מסחריות, חוקיות או פוליטיות.[31] עם זאת, התזמון וההיקף הם אינדיקציה לכך שייתכן ומדובר במתקפה מכוונת. הוועדה מציינת בהקשר זה כי **ההגנה ויכולת ההתאוששות מהתערבות זרה במערכות IT (טכנולוגיות מידע) שהן קריטיות למימוש התהליך הדמוקרטי, צריכה להיעשות מעבר להיבטים הטכניים-טכנולוגיים.** לטענת הוועדה, ההבנה של ארצות הברית ובריטניה את המושג "סייבר" היא בעיקרה טכנית וממוקדת ברשתות מחשבים, בעוד מדינות אחרות דוגמת רוסיה וסין נוקטות גישה קוגניטיבית המבוססת על תובנות בפסיכולוגיות המונים והשימוש בהן כלפי אינדיבידואלים. ההשלכות של ההבנה השונה של מתקפות סייבר – כאל טכניות טהורות או כאל כאלה הנעות מעבר לדיגיטלי לכיוון של השפעה על דעת הקהל, הן משמעותיות - מצוין בדוח הוועדה. עוד צוין כי הוועדה מודאגת מאוד מההאשמות להתערבות זרה במשאל העם.[32]

בהקשר זה יצוין כי במאמר העוסק באיומים קיברנטיים על תהליכים דמוקרטיים נטען כי בישראל מערכת הבחירות איננה מוגדרת כתשתית קריטית וכפועל יוצא איננה מצויה בהנחיה ישירה ובכפיפות לגופים האמונים על הגנת הסייבר בישראל, בפרט הרשות הלאומית להגנת סייבר. מחברי המאמר גורסים כי בשל חשיבותן של בחירות להליך הדמוקרטי והחשש מערעור היציבות השלטונית ואמון הציבור במוסדות הדמוקרטיים יש להגדיר את התהליך והתשתיות המשמשות לבחירות כתשתיות ותהליכים קריטיים. יתרה מכך נטען במאמר כי בעוד קיימת הכרה של הגופים המנחים בתחומי הסייבר באשר להשלכות הישירות של תקיפה של תשתיות מחשוב דוגמת מחשבי ועדת הבחירות המרכזית ופריצה למאגר הבוחרים, נראה כי אין הבנה מספקת של מה שמחברי המאמר מכנים "הגנה על השיח הפוליטי מפני זיהומים חיצוניים".[33]

---

[30] רשתות רובוטים המנסות לגשת לאתר בו זמנית ויוצרות עליו עומס המוביל לקריסתו.

[31] מסחריות: פגיעה באתר מתחרה; חוקיות: ניסיון של גוף אכיפה להגביל פעילות של אתר פלילי

[32] House of Commons, Public Administration and Constitutional Affairs Committee, "Lessons learned from the EU Referendum", Twelfth Report of Session 2016–17, Published on 12 April 2017.

[33] דודי סימן טוב, גבי סיבוני וגבריאל אראל, "**איומים קיברנטיים על תהליכים דמוקרטיים**", המכון למחקרי ביטחון לאומי (INSS) טרם פורסם.

3. ניסיונות התמודדות עם הפצת מידע כוזב

להלן יוצג מידע על ניסיונות התמודדות של גופים שונים בעולם עם הפצה של מידע כוזב ועם איומי סייבר. יש לציין כי בשל מגבלות הזמן והעדכניות של הנושא, לא נעשו פניות ישירות בעניין לגורמים בינלאומיים לצורך מסמך זה.

בסקירה של הפרלמנט האירופי בנושא ההתמודדות עם "פייק ניוז" מצוין כי נשיא הפרלמנט האירופי בדצמבר 2016, מרטין שולץ', קרא ל"פתרון אירופי" לבעיית המידע הכוזב. המשנה לנשיא הנציבות האירופית והאחראי על נושא השוק הדיגיטלי המשותף וכלכלת וחברת המידע, אנדרוס אנסיפ, ציין כי הוא מודאג מסוגיית המידע הכוזב והפציר בספקיות שירותי המדיה החברתית לחזק את המאמץ שלהן להיאבק בתופעת המידע הכוזב. עוד ציין אנסיפ, כי ניתן יהיה להשלים את צעדי הרגולציה העצמית של הספקיות באמצעות "סוג מסוים של הבהרות" (שלא פורט מה הן), מצד האיחוד האירופי. שר המשפטים הגרמני הציע במרס 2017 לקנוס חברות מדיה חברתית שלא מצליחות להסיר תוכן מסית/שנאה (Hate Speech) ומידע כוזב בסכום של עד 50 מיליוני אירו.[34]

בספטמבר 2015 הוקם במסגרת מוסדות האיחוד האירופי **"כוח משימה"** במטרה להיאבק בדיסאינפורמציה. הצוות, המורכב מעשרה מומחים לתקשורת, נועד לפתח קמפיינים ותוצרים שיסבירו את מדיניות האיחוד האירופי במספר מדינות מזרח אירופיות (ארמניה, אזרבייג'ן, ביילורוסיה, גיאורגיה, מולדובה ואוקראינה). בין משימותיו: "קמפיינים תקשורתיים אסטרטגיים יזומים, המבוססים על ניתוח של תחומי מפתח במדיניות ויצירת נראטיב חיובי של האיחוד האירופי"[35]; ניתוח של מגמות דיסאינפורמציה, אספקת הסברים חלופיים למאבק בדיסאינפורמציה; וניפוץ מיתוסים (Myth Busting).[36]

עם זאת, בנובמבר 2016 קיבל הפרלמנט האירופי החלטה במסגרתה הוא מזהיר מפרופגנדה רוסית כנגד האיחוד האירופי וקרא לחיזוק כוח המשימה – כולל הקצאת משאבים וכוח אדם מספק, וזאת על רקע העדר תקציב ייעודי נפרד לכוח המשימה והעובדה כי כוח האדם של הצוות מבוסס על איגום כוח אדם מגופים שונים במוסדות האיחוד האירופי. בנוסף, במרץ 2017 פרסם צוות של מומחי אבטחת מידע, משפטנים והיסטוריונים מכתב פתוח שבו הם קוראים לנציגי האיחוד האירופי להקצות משאבים לשם מימוש משימותיו של צוות המשימה. עוד צוין במכתב כי "האירופאים צריכים לדעת מי מבצע עליהם מניפולציות וכיצד".[37]

אתרים שונים וארגונים שונים – החל מספקי מדיה חברתית וכלה בארגונים מדינתיים או מגזר שלישי עוסקים בניסיונות משותפים ונפרדים להגביל את השפעתו של מידע כוזב בכלים שונים, בהם מנגנוני ניטור ואתרים ל"בדיקת עובדות".

---

[34] European Parliament, "Fake News and the EU's Response", At a Glance, April 2017, accessed: June 7, 2017.
בהקשר זה מעניין לציין כי בכתבה במגזין ניוזוויק נטען כי פייסבוק הבטיחה כי תגדיל את הצוות העוסק בבחינת תוכן ל-700 עובדים עד סוף שנת 2017 ובנוסף תשלם לצדדים שלישיים על שירותי "בדיקת עובדות" באירופה.
Newsweek, "The Bot Who Cried Wolf – How Germany is Cracking Down on Fake News", June 9, 2017, Pp: 22-25.

[35] "Proactive Strategic communication campaigns, based on focused analysis that explains key policy areas and creates a positive Eu narrative".

[36] EEAS, "Questions and Answers about the East StratCom Task Force", 14 January 2017, accessed June 7, 2017.

[37] European Parliament, "Fake News and the EU's Response", At a Glance, April 2017, accessed: June 7, 2017.

לקראת הבחירות לנשיאות צרפת הוקם אתר בשם **Crosscheck** בשיתוף פעולה של 37 גופי מדיה שונים מצרפת ומחוצה לה, בתוכם אתרי מדיה חברתית, במטרה לבדוק מידע המופץ אודות המועמדים לבחירות בצרפת (בין השאר, תמונות, סרטונים, הערות ומידע נוסף על המועמדים). האתר הוקם באמצעות ארגון קואליציה שהוקם על ידי תשעה ארגונים מייסדים בשם First Draft ביוני 2015 במטרה להעלות את המודעות לאתגרים של אמת ואמון בעידן הדיגיטלי. בספטמבר 2016 הוא הורחב ונוטלים בו חלק גופי שידור מרכזיים וגופי מדיה דיגיטלית בולטים (בהם פייסבוק וטוויטר, BBC, CNN ועוד), גופי אקדמיה, ועוד. הארגון פועל שלא למטרת רווח.[38]

בארצות הברית פועלים אתרים ל"בדיקת עובדות". האתר העצמאי PolitiFact עושה שימוש ויזואלי ומילולי במה שהוא מכנה "מד אמת" כאשר הקטגוריות של סיווג המידע כוללות: אמת; אמת ברובו; חציו אמת; בעיקר שגוי; שגוי; ו"על ראש הגנב בוער הכובע" (Pants on fire) כקטגוריה המבטאת שקר גמור.[39]

פייסבוק פרסמה בחודשים האחרונים מידע על ניסיונותיה להתמודד עם מידע מוטעה וחדשות כוזבות. על פי ההודעה של פייסבוק החברה נלחמת בהפצה של חדשות כוזבות בשלושה ערוצים עיקריים: פגיעה בתמריץ הכלכלי של יצירה והפצה של תוכן כוזב; בנייה של כלים שיסייעו לצמצם את תפוצתו של מידע כוזב; סיוע לאנשים לקבל החלטה מודעת ביחס למידע כוזב.[40]

ביחס לפגיעה בתמריץ הכלכלי להפצה של תוכן כוזב, טוענת פייסבוק כי חלק ניכר מהחדשות הכוזבות מונעות מתמריץ פיננסי. מפיצי הספאם[41] הללו מתחזים לאתרי תוכן חדשותי לגיטימי, מפיצים תרמיות שמטרתן לעודד כניסה לאתרים שלהם שהם לרוב בעיקר מודעות. כדי לצמצם את התמריץ נעשה מאמץ לזהות תוכן כוזב – הן באמצעות קהילת המשתמשים; הן באמצעות ארגונים העוסקים בבדיקת עובדות והן באמצעות שימוש בכלי "למידת מכונה"[42] לשם סיוע בזיהוי תרמיות וחשבונות ספאם ואכיפת המדיניות של החברה. בנוסף תפוצתו של תוכן בפיד החדשותי (News Feed) תלויה במידת האמון של מקורו.

ביחס לפיתוח והטמעה של כלים חדשים, מציינת החברה כי היא מפתחת כלי דירוג שונים וכלי דיווח במטרה לזהות באופן אוטומטי או על ידי דיווח גולשים תוכן בעייתי.

ביחס לסיוע בהחלטה מודעת באשר לתוכן כוזב, מציינת החברה כי היא פועלת לסיוע באספקת ההקשר למידע שהמשתמשים נחשפים אליו ומתן אפשרות לקבל פרספקטיבות נוספות ביחס לנושא שעליו הם קוראים. בין השאר, פייסבוק שותפה ליותר מ-25 ארגונים מכלל המגזרים ביוזמה ליושרה בחדשות (News Integrity). על פי הפרסום היוזמה האמורה נעשית בתקצוב כולל של 14 מיליוני דולר, במטרה

---

[38] CrossCheck, Firstdraftnews.

[39] PolitiFact.

[40] Facebook Newsroom, Adam Mosseri, "Working to Stop Misinformation and False News", April 6, 2017, accessed June 7, 2017.

[41] ספאם הוא מושג שנועד לתאר "דואר זבל" – כזה הנשלח כדי לקדם את מכירתו של מוצר או הפצתו של מידע של בעל עניין באופן אגרסיבי, אך בהקשר כאן נשעה שימוש במושג זה גם כדי לתאר הפצתו של תוכן כוזב, תוך הדגשת המניע הפיננסי בהפצה.

[42] Machine Learning, הכוונה לשימוש בבינה מלאכותית כדי ליצור מנגנוני ניטור וזיהוי אוטומטיים של מידע כוזב, לא אמין, "ספאם" וכדומה.

לקדם אוריינות חדשות, להגביר את האמון בעיתונות ברחבי העולם ולשפר את הידע המשפיע על השיח הציבורי.[43]

4. התייחסות גופי מטה וממשל בישראל לנושא

כאמור, מוקד הדיון הנוכחי הוא במתקפות סייבר ושימוש במידע כוזב לשם השפעה על מערכות בחירות. בהקשר זה פנה מרכז המחקר והמידע של הכנסת לשני גופי מטה מרכזיים הקשורים לנושא: ועדת הבחירות המרכזית לכנסת; והרשות הלאומית להגנת סייבר. עם זאת, עשויות להיות רשויות נוספות הקשורות להיבטים בנושא, בפרט ביחס להיבטים של חתרנות מדינית או פגיעה באושיות השלטון.

4.1. התייחסות ועדת הבחירות המרכזית לכנסת[44]

מרכז המחקר והמידע של הכנסת פנה אל מנכ"לית ועדת הבחירות המרכזית לכנסת, עו"ד אורלי עדס, בבקשה למענה על שאלות הנוגעות לנושא הדיון. להלן יוצגו עיקרי תשובתה.

באשר למאגרים והמערכות הייעודיות המצויות ברשות ועדת הבחירות המרכזית:

ועדת הבחירות המרכזית מפעילה מערכות מידע שונות לצורך מימוש משימותיה בהן: מערכת לחישוב שיעור ההצבעה, מערכת לשיבוץ נציגי סיעות ומערכת הצגת תוצאות אמת. הוועדה סירבה לפרט מעבר לאמור בשל שיקולי אבטחת מידע.

באשר לכוונת הוועדה לחזק את השימוש במנגנוני דיגיטציה:

נעשית בחינה מתמדת של אפשרויות השימוש בטכנולוגיה לייעול הליך הבחירות, הן בהיבטי ארגון ושיטות והן בהיבטי ניהול עבודת הקלפי ומחשוב תהליך ההצבעה. בימים אלה מפותחת מערכת לגיוס, מיון והסמכה של מזכירי ועדות קלפי.

בנוסף, נבחנת האפשרות למחשב את עבודת ועדת הקלפי (מחשוב פרוטוקול הועדה ולא הליך ההצבעה עצמו), אך ככל שתוקם מערכת כזו היא לא תפעל בחיבור לרשת האינטרנט כדי להגן על המידע. ועדת הבחירות ציינה בתשובתה כי "יחד עם זאת **משהליך הבחירות הוא מנשמת אפה של הדמוקרטיה, ומשמדובר בשינוים משמעותיים והרה גורל להליך הדמוקרטי, הבחינה בתחומים אלה מתבצעת בזהירות המרבית הנדרשת מתוך הבנה שבבחירות ארציות אין 'חזרה גנרלית' ואין 'מועד ב'.**" ונושא אבטחת המידע מהווה שיקול מרכזי בכל ההיבטים (ההדגשה אינה במקור).

באשר לפנקס הבוחרים:

פנקס הבוחרים מנוהל על ידי משרד הפנים וועדת הבחירות המרכזית מקבלת עותק ממנו לצורך שימוש בו במתן מידע על מקום הצבעה בקלפי בהתאם לחוק הבחירות. עוד ציינה מנהלת הוועדה כי האחריות הבלעדית לפנקס הבוחרים ולמסירתו לרשימות המועמדים היא של משרד הפנים.

באשר להנחיה של ועדת הבחירות בתחומי הגנת הסייבר:

ועדת הבחירות המרכזית היא גוף סטטוטורי עצמאי בדומה לנשיא המדינה ולמבקר המדינה ולכן איננה גוף מונחה לפי החוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998. **הגורם האחראי על ההגנה על**

---

[43] Ibid.

[44] עו"ד אורלי עדס, מנכ"לית ועדת הבחירות המרכזית לכנסת, מכתב תשובה לפניית מרכז המחקר והמידע של הכנסת, 4 ביוני 2017.

מאגרי המידע והגנת הסייבר שלה הוא אגף מבצעים, מחשוב ותפעול של הוועדה. עם זאת, בעת שפותחה המערכת הממוחשבת לניהול הבחירות, יזמה הוועדה פנייה לרשות לאבטחת מידע בשירות הביטחון הכללי לשם ייעוץ, ופיתוח המערכת לווה בייעוץ מצד הרשות האמורה. עוד צוין בתשובת ועדת הבחירות, כי היא מצויה בקשרי עבודה עם הגופים השונים הפועלים בתחומי הגנת הסייבר: מטה הסייבר הלאומי; הרשות הלאומית להגנת הסייבר; היחידה להגנת הסייבר בממשלה (יה"ב); הרשות לאבטחת מידע בשירות הביטחון הכללי.

באשר להגנה והערכות לתקיפות סייבר

הוועדה דנה באופן שוטף בסוגיות של תקיפות סייבר ותרחישים שונים ושיקולי הגנת סייבר ואבטחת מידע הם שיקולים מרכזיים בכל יישום של מערכת מידע, קיימת או חדשה. הוועדה יזמה פעילות שנערכת בימים אלה מול הרשות הלאומית להגנת סייבר, לצרוך קבלת שירות ממנה בהגנה על מערכות שונות ובמקרים של אירועי סייבר רחבי היקף, דוגמת מתקפת הסייבר הנרחבת שאירעה לאחרונה, קיים קשר ישיר בין הוועדה לבין הרשות הלאומית להגנת הסייבר, ובין השאר ננקטו פעולות מידיות לשם צמצום נוסף של החשיפה למתקפה. בנוסף, הוועדה התקשרה עם יחידת ממשל זמין כדי להתארח בסביבה ממשלתית מאובטחת המונחית על ידי גורמי הגנת הסייבר בישראל.

4.2. התייחסות הרשות הלאומית להגנת סייבר[45]

מרכז המחקר והמידע של הכנסת פנה ראש הרשות הלאומית להגנת הסייבר (להלן הרשות), מר בוקי כרמלי, בבקשה למענה על שאלות הנוגעות לנושא הדיון. להלן יוצגו עיקרי תשובתו.

באשר לתחומי האחריות של הרשות, ציין כרמלי:

הרשות אחראית להגנה על מערכות מדינה קריטיות ואחרות במרחב הסייבר האזרחי מפני מתקפות סייבר בהן: חדירה, שיבוש, הרס, פגיעה בתפקוד רציף וכדומה. **באשר להליך הבחירות, הרי שעצמאותה וסמכויותיה של ועדת הבחירות המרכזית עומדות מעל כל הנחיה או סמכות שבידי הרשות. עם זאת, הרשות רואה עצמה מחויבת לתמוך ולסייע בתהליכים, השיטות והאמצעים המאפשרים הגנה על הליך הבחירות מפני מתקפות סייבר, וכן בהעלאת המודעות של משתמשי המערכות לסיכונים ולאיומים בהערכות ובהליך הבחירות עצמו.** (ההדגשה איננה במקור).

באשר להיבט של הפצת מידע כוזב, מדגיש ראש הרשות:

הרשות איננה אחראית לטיפול <u>בתוכן המופץ</u> במרחב הסייבר וככל שמדובר בהפצת מידע כוזב לשם השפעה על הבחירות, השפעה על דעת הקהל ועל עמדות פוליטיות, אין הרשות עוסקת בכך. כרמלי מציין בתשובתו כי בישראל פועלים גופים נוספים האחראים, בין היתר, למניעת פגיעה באושיות המשטר ולמניעת חתרנות מדינית ואשר על כן, פעילותה של הרשות במרחב הסייבר בהיבטים הקשורים לבחירות חייבת להיעשות בתיאום עם הגופים הנוספים להם אחריות וייעוד באותו מרחב. (ההדגשה איננה במקור).

באשר לפעילות לשם הגנה על הליכי בחירות צוין:

הרשות מבצעת ניתוח סיכונים משותף יחד עם גופי הממשל להם אחריות לרציפות התפקודית בתחומי החיים השונים ובשיתוף גופי הביטחון הרלבנטיים במאמץ להגן על אינטרסים לאומיים שונים, הן ביחס להליכי בחירות והן ביחס להליכים אחרים במדינה. עם זאת, ברור כי לא קיימת הגנה הרמטית על כל

[45] בוקי כרמלי, ראש הרשות הלאומית להגנת הסייבר, מכתב תשובה לפניית מרכז המחקר והמידע של הכנסת, 6 ביוני 2016.

המערכות, כל הזמן, מפני כל איום אפשרי ולכן ישנה חשיבות להעלאת מודעות ולהתנהגות מונעת- זאת בנוסף להגנה על מערכות מידע, תקשורת, הפצה ועוד.

יצוין כי בתשובת הרשות לא ניתנה התייחסות לשאלות נוספות שהפנה אליה מרכז המחקר והמידע של הכנסת בתוכן: שאלת הצורך בהנחיה ספציפית של ראשי מפלגות או צוותם כדי למנוע תקיפות ממוקדות; שאלת השלכותיהן של העדויות בדבר התערבות בהליכי בחירות במדינות אחרות על איום סייבר עבור מדינת ישראל ומוסדותיה.

4.3. התייחסות הרשות למשפט טכנולוגיה ומידע במשרד המשפטים[46]

הרשות למשפט טכנולוגיה ומידע במשרד המשפטים (להלן: רמו"ט או הרשות), עוסקת בהגנת הפרטיות במידע אישי ובמאגרי מידע. להלן תוצג בקצרה התייחסות רמו"ט להיבטים של הגנה על מידע מפנקס הבוחרים.

על פי רמו"ט, **מידע שמתקבל מפנקס הבוחרים מותר לשימוש רק לצורך קשר עם הבוחר בתקופת הבחירות, ולאחריה יש להשמיד מידע זה ואין לעשות בו שימוש** (על ידי המפלגה או על ידי ספקי שירות שלה). במהלך השנים ביצעה רמו"ט פיקוח על השימוש שנעשה בפנקס הבוחרים, שמופץ בישראל למפלגות, סיעות ורשימות מידי מערכת בחירות. **במהלך פעולות אכיפה נמצא שפנקס הבוחרים, מועתק ונמסר לידי מי שאינם מורשים לעשות בו שימוש, נשמר אצלם ומזין מאגרי מידע לא חוקיים שבהם סוחרים גורמים במשק. רמו"ט פעלה והביאה לסגירת פעילותן של חברות שעשו שימושים אלו.** בנוסף פעלה הרשות גם במקרים בהם מפלגה לא קיימה את חובתה להחזיר את פנקס הבוחרים למפקח על הבחירות. עוד צוין בדברי הרשות כי היא בוחנת את השימוש במאגרי מידע אחרים בתקופת בחירות, המשמשים לפניות לאנשים על בסיס ידיעות מוקדמות עליהם, שעשויות לתרום להשפעה על אופן הצבעתם.

בנוסף, לפני מערכת בחירות מוציא ראש רמו"ט הודעה למפלגות המציינת, כי על-פי חוק הגנת הפרטיות, השימוש במידע אודות אדם מותנה בהסכמתו ובמטרה לשמה נאסף ממנו המידע.

5. דיון

רשת האינטרנט ומרחב הסייבר הם סביבה גלובאלית, מחוברת ומורכבת והיכולת לתחום את גבולותיה ולהשליט עליה רגולציה או דפוסי התנהלות המקובלים במרחב הפיזי מוגבלת מאוד. שחקנים שונים, קטנים או גדולים, אינדיבידואלים או מדינתיים ובשם אינטרסים שונים: מסחריים, פליליים או פוליטיים פועלים כל העת במרחב זה.

הרגישות של תהליכי בחירות כלליות מזמנת אתגרים הן בהיבטי הגנת סייבר- מערכות מחשב ומערכות מידע המשמשות בהליך הבחירות על שלביו השונים; והן בהיבטי ההגנה על דפוסי השיח הדמוקרטי מן הניסיון לבצע עליו מניפולציות. מניפולציה כאמור יכולה להיעשות באמצעים שונים, ולמרות שכפי שעולה מן המסמך ניסיונות כאלה אינם תופעה חדשה, מגוון הכלים, ההיקף, יכולת ההסתרה שלהם ועוד, הופכים את האינטרנט לכר נרחב לאיום זה. פריצה למידע אישי או רגיש, יצירתו של מידע כוזב, שליטה בעיתוי פרסומו, הפצה וחשיפה של סוגי המידע השונים וערבוב ביניהם, כמו גם שילוב של כלי השפעה שונים, בהם מדיה מסורתית, סוכני השפעה ועוד, אלו טקטיקות המופעלות על ידי שחקנים שונים, כפי שעולה מעדויות מן העולם.

[46] עו"ד לימור שמרלינג מגזניק, מנהלת קשרי ממשל, הרשות למשפט, טכנולוגיה ומידע, משרד המשפטים, דוא"ל, 8 ביוני 2017.

בעוד קל יחסית לתחום את גבולותיהן של מערכות המידע והמחשוב הנוגעות לניהול מערכות בחירות; נראה כי קשה עד בלתי אפשרי לתחום את גבולות השיח הדמוקרטי- פוליטי המתנהל ביתר שאת דווקא בסמוך למועדן של בחירות. בנוסף, קיים חשש מיצירת תרבות של השתקה, צנזורה ומנגנוני כוח שלטוני מוכוונים שיגבילו או ייתפסו כמגבילים את חופש הביטוי. למרות זאת, נראה כי היחלשותם של מנגנוני תקשורת יסודיים, מבוססים וותיקים והתפתחותו של שוק דעות כאוטי וממועט במנגנוני ריסון או אימות עובדות, עלולים להוביל לירידה באמון במידע ממקורות שונים ואולי אף לפגיעה באפקטיביות שלו עבור השיח הציבורי. כך, למרות הגיוון כביכול של שוק הדעות האינטרנטי, העובדה כי סביבת החיים כיום מתאפיינת בין השאר בעומס יתר של מידע (Information Overload), מאפייני הרשת ודפוסי התנהגות רשתית עשויים לגרום לקיטוב וליצירת קבוצות בעלי דעה הומוגניות.

לא ברור האם וכיצד יש להתמודד עם סוגיית ההפצה של מידע כוזב, ומהו התפקיד של המדינה בעניין או חלקם של שחקנים אחרים דוגמת גופי תקשורת או גופי מגזר שלישי. נראה כי אין כיום כלים מספקים כדי לאמוד את מידת ההשפעה של מידע כוזב על מערכות בחירות. עם זאת, הכרה בתופעה ויצירת מודעות ציבורית וממסדית, כולל עידוד אוריינות ומודעות בדפוסי צריכה של מדיה, פיתוח מיומנויות קריאה ביקורתית, סינון מידע וגיוון מקורותיו, עשויים להיות צעדים ראשונים במיתון ההשפעה שלה.

כתיבה: רועי גולדשמידט

אישור: יובל וורגן, ראש צוות