

הפצת מידע כזב ותקיפות סייבר לשם השפעה על בחירות



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 ולכן פגיעה בהליך בחירות נתפסת כפגיעה חמורה ביציבותו של שלטון דמוקרטי.

בשנים האחרונות ישנן עדויות לניסיונות שונים לפגוע 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.

המסמך שלהלן יציג בקצרה כמה מן ההיבטים המרכזיים של הנושא, בהם השיח הדמוקרטי באינטרנט וניסיונות ההשפעה עליו, תעמולה מקוונת ומלחמות סייבר. לאחר מכן יוצג מידע תמציתי על דרכי התמודדות אפשריות עם האתגרים בתחום זה.

מסמך זה נכתב כחלק מסדרת מסמכים בנושאים הקשורים לבחירות, שנכתבים במרכז המחקר והמידע של הכנסת לקראת הבחירות לכנסת ה-21.

מילון מונחים

לאורך המסמך ייעשה שימוש בכמה מונחים מקובלים בעיסוק בנושאים הנדונים. להלן מילון מונחים קצר:

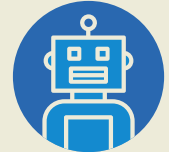
// מידע כזב (Fake News) //

מידע שקרי הנחזה כמידע חדשותי והפצתו, בין השאר באמצעות האינטרנט, נועדה להטעות את הציבור (מתורגם גם כ"חדשות כזב").



// "בוטים" (Social Bots או Bots) //

קיצור של "רובוטים". 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 פילייים ומידת השימוש לרעה שהם מגלמים שונה. המשותף להם הוא בשימוש בטכנולוגיות אוטומציה ליצירת זהות פיקטיבית כדי להשפיע על זרימת המידע ותפוצתו.



// "מיקרו-טרגטינג" (Micro-Targeting) //

שם כולל לטכניקות שונות לשם זיהוי תחומי עניין, עמדות, מאפיינים אישיים ועוד, במטרה להציע פרסום מותאם אישית, לחזות את השלכות הפרסום ובכך להשפיע על התנהגותם של פרטים בחברה (לדוגמה, ביחס להחלטת קנייה או להחלטה למי להצביע בבחירות). השימוש באינטרנט וברשתות חברתיות הוא כר פורה לכרייה ואיסוף של מידע אישי לשם ניתוח וחיזוי עמדות והתנהגויות.



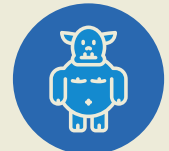
// "ויראליות" //

מושג המתאר תהליך של זרימת מידע (ברשת האינטרנט אך לא רק בה), במהלכו אנשים משתפים באופן סימולטני פרט מידע, כך שהמסר מתפשט מעבר לקשרים החברתיים שלהם, בדרך כלל לרשתות רחוקות יותר, כך שנוצר גידול חד במספר האנשים החשופים למידע. בין המדדים לויראליות: מהירות ההפצה, מספר הנחשפים לתוכן, והמרחק בין מקור המידע לתפוצה שלו.



// "טרול" //

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.



// סוחרי מידע (Data Brokers) //

חברות האוספות מידע מכלל המקורות הזמינים ברשת ומחוצה לה ומוכרות אותו לגופים שונים, למטרות שונות בהן: פרסום ממוקד, אימות זהות ומניעת הונאות. לפי **דוח של נציבות הסחר הפדראלית בארה"ב** (FTC) שניתח את המידע שזמין ב-9 חברות כאלה: לאחת מהחברות היה פילוח של המידע ל-3,000 מאפיינים ביחס לכל צרכן אמריקני! (כולל: "מצפה להיות הורה"; "בעל עניין בסוכרת"; "מיקוד בכולסטרול" ועוד).



// "דיפ-פייקס" (Deep fakes) //

טכנולוגיות וידאו ועיבוד תמונה שמאפשרות ליצור תוכן וידאו ברמת אמינות גבוהה כך שקשה לזהות את היותו מזויף. מומחים טוענים כי טכנולוגיות כאלה צפויות לשמש לשם ניסיונות השפעה ושיבוש הליכי בחירות בעתיד כיוון שהן מאפשרות להפיץ תוכן וידאו מזויף בעיתוי משמעותי וכך להשפיע על התנהגות בוחרים או על תפיסת אמינות ההליך.



שיח הבחירות באינטרנט: דיון ציבורי או זירה לקידום אינטרסים?

בעבר הייתה נטייה רווחת לראות באינטרנט זירה חדשה המאפשרת שיח ציבורי פתוח וער, שאינו מוגבל על-ידי כלי התקשורת המסורתיים ושיקולי העריכה המנחים אותם. השילוב בין אנונימיות, אינטראקטיביות וחסימי כניסה נמוכים, שאפיינו את הרשת, נתפס כאמצעי לשבירת ההגמוניה של אמצעי התקשורת על הידע והפצתו.

עם הזמן ירדה קרנה של האנונימיות ברשת ומקביל ניכרה עלייתם של שומרי סף חדשים בדמותן של חברות רב-לאומיות השולטות בדרכי הפצת המידע ובחיפוש שלו. ההבנה כי המדובר בזירה של ניהול אינטרסים: כלכליים, אישיים ולאומיים, הסירה חלק מן הקסם האוטופי-נאיבי של ראשית צמיחתה של הרשת.

במהלך שנת 2018 פורסמה בתקשורת פרשת "קיימברידג' אנליטיקה", בה נחשף כי מידע אישי של כ-80 מיליוני משתמשים -רובם אזרחים אמריקאים, שימש לשם תיוג פוליטי שלהם ופרסום ממוקד בהתאמה לו, טרם הבחירות בארה"ב ב-2016. פרשה זו הבהירה כי לא זו בלבד שמידע אישי הוא מטבע באמצעותו משתמשי הרשת על השירותים בה, אלא שמידע אישי משמש גם בניסיונות להשפיע על תודעת ההמון באשר לאופן בו הוא מממש את זכותו הדמוקרטית בהצבעה בקלפי. חששות דומים לניסיונות השפעה עלו גם בבריטניה ביחס למשאל העם על עזיבת האיחוד האירופי ("ברקזיט"); ובמערכות בחירות נוספות ברחבי העולם.

מרחב הסייבר: מאבק על תודעה ולא רק על תשתיות

בעוד העיסוק במדיניות ורגולציה של "ההגנה על תשתיות חיוניות" מפני מתקפות סייבר מתקיים מזה מספר שנים, רק בשלוש השנים האחרונות עלתה על סדר היום סוגיית ניסיונות ההשפעה על השיח הציבורי ועל בחירות בפרט, באמצעים דיגיטליים - ממחשבים, בתוכם:

- שימוש ב"רובוטים" (Bots) או ב"טרולים" ("ביריוני רשת") לשם הפצת מידע כזב, יצירת מחלוקות והשפעה על השיח
- טכנולוגיות "בינה מלאכותית" לשם יצירת תקשורת "דמוי אנושית" מותאמת אישית
- תקיפות סייבר "מסורתיות" (מתקפות ממוקדות לשם גניבת מידע; מתקפת מניעת שירות ועוד)

ההגנה על תשתיות חיוניות או ארגונים שונים מתקיפות סייבר היא אתגר שניתן לתחום את גבולותיו. "המלחמה על תודעת הציבור", לעומת זאת, עשויה להיעשות באמצעות מגוון כלים נרחב והיא מתנהלת בכלל המרחב המקוון (ולא רק במקומות ספציפיים או כלפי יעדים ספציפיים) ולכן היא סוגיה נרחבת ומורכבת יותר לטיפול.

מחקר מדיניות של המכון הישראלי לדמוקרטיה שפורסם לאחרונה, טוען כי ישנן שלוש זירות עיקריות למתקפות סייבר:

- תקיפת הליך הבחירות
 - תקיפת מפלגות ושחקנים פוליטיים
 - תקיפת רשתות חברתיות ואתרי חדשות
- שיטות הפעולה העיקריות על פי המחקר כוללות:
- הפצת מידע מטעה (דיסאינפורמציה)
 - איסוף מידע אישי ושימוש בו להשפעה
 - הפצה והגברה של מידע נכון אך מוטא
 - תקיפות סייבר של תשתיות קריטיות



"פייק ניוז"

המושג "פייק ניוז" צבר תהודה ותפוצה רבה בשנתיים האחרונות, אך למעשה ההיסטוריה של "חדשות כזב" ושל שימוש במידע מעוות או שקרי לשם השגת מטרות שונות היא ארוכת שנים וקיימת כבר מאז המצאת הדפוס לפני כ-500 שנה. למרות הנטייה לדבר על תפוצתן של ידיעות ברשת בעיקר במונחי מידת ה"ויראליות" שלהן, עדויות שונות מצביעות גם על ידיים מכוונות המשפיעות על התוכן המופץ בדרכים שונות, בהן:

הכוונה של עיתונאים ושל הציבור
אל המידע

ערבוב מכוון של מסמכים אמיתיים ופיקטיביים

הפצתן באמצעות ישויות פיקטיביות מרובות
הנשלטות על ידי מעט גורמים

יצירתן של ידיעות שקריות

מתעמולת המונים לתעמולה מותאמת אישית?

הניסיון להשפיע על עמדות וליצור קשר עם ציבור הבוחרים לשם קידום אינטרס פוליטי או אג'נדה איננו תופעה חדשה, וטכנולוגיות מידע היוו מאז ומתמיד חלק מן השינוי בדפוסי התעמולה וביכולת להתאים אותה לקהל ספציפי.

עם זאת, התפתחות רשת האינטרנט, הרשתות החברתיות וטכנולוגיות איסוף וניתוח מידע ספציפיות מאפשרות כיום לענקיות האינטרנט ולחברות הסוחרות במידע (Data Brokers) לספק פילוח מפורט של גולשים ברשת לפי מאפיינים שונים כגון: גזע; מגדר; אוריינטציה פוליטית ותחומי עניין, ברמת פירוט ודיוק גבוהים. מידע אישי זה משמש כדי להתאים את המסרים אליהם נחשפים גולשים מסוימים בהתאם להחלטות של מנהלי קמפיין. מנהלי קמפיין יכולים לבחור לא רק לעודד הצבעה למועמד מסוים אלא גם, למשל, לנסות ולעודד מצביעים של מפלגה מתחרה שלא להגיע לקלפי. כלי "מיקוד המטרה" מאפשרים להגדיר מסרים שונים לקהלי יעד שונים וכך לחשוף אותם למידע באופן שיעודד אותם לפעול באופן הרצוי למפרסם.



השימוש במיקרו-טרגטינג והשילוב שלו עם תופעות חברתיות של התנהגות ברשת בתוכן: "עדריות" ו"אהבת הדומה" משפיעים על החשיפה של משתמשי רשת לתוכן ולאנשים בעלי עמדות דומות לעמדותיהם. הרצון של ענקיות האינטרנט לספק תוכן "רלוונטי" ומעניין משפיע גם הוא על יצירת חשיפה מרובה למידע מסוגים מסוימים על פני מידע אחר. בשל סיבות אלה נוצרות "תיבות תהודה" וירטואליות (Echo Chambers) שמעצמות תפיסות ועמדות ומחזקות מגמות קיטוב.

על פי תשובת חברת "גוגל" לפניית מרכז המחקר והמידע של הכנסת, בשימוש בכלי "פרסום מותאם אישי" כללי המדיניות של החברה אוסרים על שימוש באידיאולוגיה פוליטית, דעות פוליטיות, השתתפות בשיח פוליטי ועוד, כקריטריון למיקוד מודעות.

שאלת הלגיטימיות של שימוש במידע מפורט ואישי לשם פרסום פוליטי ממוקד נידונה בשנתיים האחרונות בהרחבה על ידי רגולטורים ברחבי העולם. העמדות ביחס לנושא זה נעות בין ניסיון לאסור בחקיקה על שימוש ב"מיקרו-טרגטינג פוליטי", לבין קריאות להגברת השקיפות של מודעות פוליטיות (למשל: ציון העובדה כי זו מודעה פוליטית; הגורם המממן; עילת החשיפה של הפרסומת הזו לגולש ועוד).

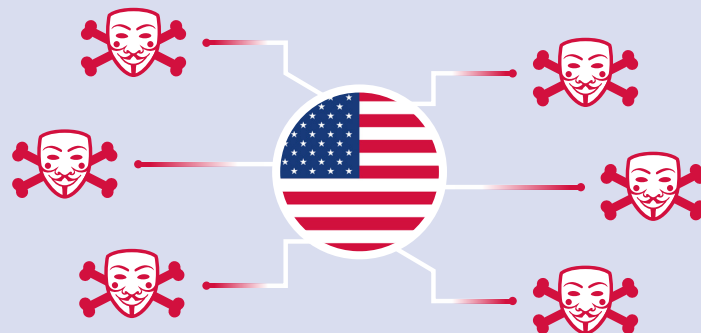
מלחמות סייבר

בינואר 2017 פרסם משרד הממונה על המודיעין הלאומי של ארצות הברית **דוח בנושא המעורבות הרוסית בבחירות לנשיאות ארצות הברית**. בדוח נטען כי ההוראה לנהל "קמפיין השפעה" (Influence Campaign) ביחס לבחירות נועד: לערער את אמון הציבור בתהליך הדמוקרטי בארה"ב, להוציא לעז על מועמדת מסוימת ולפגוע בסיכויי הבחירה שלה. עוד נטען כי ניסיונות ההשפעה נבעו בין היתר מכך שהממשל הזר פיתח העדפה ברורה למועמד מסוים בבחירות. על פי הדוח, 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.

על פי פרסומים בעיתונות, במהלך בחירות האמצע לקונגרס ב-2018 בארצות הברית, נקטו גורמי ממשל אמריקאים בתקיפות סייבר ממוקדות, במטרה למנוע מ"טרולים" רוסים ובפרט מ"הסוכנות למחקר אינטרנט" (Internet Research Agency) בסנט פטרסבורג להשפיע על מהלכן התקין של הבחירות. גם במידע שנתקבל מחברת "גוגל" בתשובה לפנייתנו צוין כי הוסרו 42 ערוצי "יוטיוב" של ה-IRA כמו גם 39 ערוצי "יוטיוב" המקושרים לרפובליקה האיסלמית של אירן.

אלו הן רק דוגמאות נקודתיות לפעילות במרחב הסייבר בהקשר של בחירות.

במסמך רשמי של ממשלת ארצות הברית המציג את אסטרטגיית הסייבר שלה נטען כי "יריבים פועלים כל העת מתחת לסף של עימות מזוין כדי להחליש את מוסדותינו ולהשיג יתרון אסטרטגי".



¹ אהבת הדומה - "הומופיליה" היא הנטייה האנושית להתחבר אל הדומים לנו (אתנית, גיאוגרפית או אידיאולוגית). נטייה זו יוצרת ברשת האינטרנט תופעות של "קבוצתיות" או "עדריות", 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.

"סוגיית הייחוס": מה בין השפעה של מדינה זרה להשפעה פנימית?

בשיח המדיניות בנושאי סייבר נודעת חשיבות רבה לשאלת היכולת לייחס פעולות ליריב ספציפי (Attribution). בניגוד לפעילויות במרחב הפיזי בהן קל יחסית לזהות את התוקף, במרחב המקוון קיים קושי בזהוי ובהתאמה בבחירת המענה. מחקרי מדיניות ושיח ציבורי רב ממוקדים בשאלת "התערבות זרה בהליכי בחירות" וההתמודדות מולה.

דוח של הממונה על המודיעין הלאומי בארצות הברית קבע זה מכבר כי בוצעו ניסיונות התערבות רוסיים בתהליכי הבחירות בארה"ב ב-2016, הן באמצעות תקיפות סייבר ממוקדות, והן באמצעות הפצת מידע כזב ומניפולציות שונות במטרה להשפיע על עמדות ולפגוע ביציבות השלטונית. מידע כזב הופץ תוך שימוש משולב ברשתות תקשורת "מסורתיות", לצד שימוש בבוטים וטרולים להפצת התוכן. בנוסף, ראש שירות הביטחון הכללי בישראל צוטט לאחרונה באומרו כי בכוונת מדינה זרה להתערב בבחירות בישראל.

בעקבות שאלות באשר לניסיונות של גורמים זרים להתערב בהליך הבחירות לכנסת ה-21, פרסמה ועדת הבחירות המרכזית כי הנושא מונח על סדר יומה ומטופל בשיתוף כלל גורמי המקצוע, בהם גופי הביטחון, וכי נציגי הוועדה נפגשו עם מנהלים ברשת החברתית פייסבוק, על מנת לבחון דרכים להתמודד עם ניסיונות כאמור.

בהינתן כי טכניקות השפעה דומות ניתנות ליישום גם על ידי שחקנים מתוך המדינה (לדוגמא: מפלגות, פוליטיקאים, גופים פרטיים ועוד) ראוי לבחון עד כמה יש מקום לאפיין את דפוס המענה או הגורם האחראי עליו בהתבסס על שאלת הייחוס. ולחלופין, האם המיקוד לא צריך להתייחס לשאלת הגבלת הפרקטיקות המיושמות ולא רק לשאלת הייחוס. היבט זה חשוב במיוחד שכן חברות או צדדים שלישיים עלולים לספק שירותים (בוטים, טרולים, חשבונות פיקטיביים, טכנולוגיות זיוף וידאו - Deep Fake ועוד), הן לשחקנים זרים והן לשחקנים מקומיים.

מהי האחריות של ענקיות הרשת?

שאלת אחריותן של ענקיות הרשת על המתרחש על גבי התשתיות או השירותים שלהן נידונה כבר זמן רב; האם הן "רק פלטפורמה" - תשתית או "צינור" לתעבורה וכפועל יוצא, אין להן אחריות על התוכן; או בקוטב השני - האם הן "מפרסם" או "מוציא לאור" הנושא במלוא האחריות לתוכן שלו.



תופעות רשת שונות כגון - הסתה; אלימות או בריונות; פדופיליה; וסוגי פשיעה נוספים היו מזה זמן במוקד שאלת הצורך להגביל את תפוצתן ברשת ושאלת האחריות על ביצוע ההגבלה או הנשיאה באחריות הפלילית והאזרחית במקרה של כישלון בהגבלת התפוצה. נראה כי סוגיות מידע הכזב והפרסום הפוליטי הן בבחינת "הקש ששבר את גב הגמל" הרגולטורי, והן מעודדות רגולטורים ברחבי העולם לבחון שוב את הצורך להגביל את ענקיות האינטרנט ולהטיל עליהן אחריות.

לשיטתם של המצדדים בכך, עילת ההגבלה והטלת האחריות נובעת הן מהכרה ב"נזק" הציבורי בתופעות הרשת האמורות והן מההבנה כי חברות האינטרנט הגדולות אינן רק "צינור" אלא משפיעות בצורה אקטיבית על סוגי התוכן אליהם ייחשפו המשתמשים בהתאם לשיקולים שלהן (כלכליים או אחרים) ומכאן כי הן דומות במובנים מסוימים לפחות, למוציא לאור ולא לספק תשתית. **בדוח של הפרלמנט הבריטי** שפורסם לאחרונה נטען כי חברות ההיי-טק הגדולות אינן "רק פלטפורמה" מחד ואינן "מוציא לאור" מאידך, ויש למצוא קטגוריה חדשה עבורן ומתוקפה להטיל עליהן אחריות משפטית על תוכן "פוגעני" או לא חוקי שהועלה על ידי משתמשים - לאחר העלאתו. הדוח גם מציע לקדם בחקיקה קוד אתי מחייב לחברות שיגדיר בין השאר מהו "תוכן פוגעני"; מה הן החובות החלות על החברות ביחס למחיקה שלו או מניעת העלאתו באמצעים טכנולוגיים מלכתחילה.

בגרמניה נכנס לתוקף בתחילת אוקטובר 2017 החוק לאכיפת התנהלות ברשת. החוק מחייב רשתות חברתיות עם יותר מ-2 מיליון משתמשים רשומים בגרמניה להסיר תוכן לא חוקי (המפר הוראות ספציפיות בחוק העונשין הגרמני בתוכן: עבירות של לשון הרע, עבירות הסתה, עבירות של הפצת סמלים או תעמולה הנוגדים את המשטר החוקתי של גרמניה, עבירות טרור, ועבירות של השמצת דת או ארגון דתי או אידיאולוגי). תוך 24 שעות מקבלת דיווח עליו. במקרים של ספק ביחס למעמד החוקי של התוכן, צריכה להתקבל החלטה תוך שבעה ימים, למעט במקרים יוצאים מן הכלל בהם יכולה להינתן אורכה.



מחסור במידע ונתונים על היקף התופעות בישראל

מרכז המחקר והמידע של הכנסת פנה אל גורמי ממשלה שונים בהם: מערך הסייבר במשרד ראש הממשלה, ועדת הבחירות המרכזית; מחלקת הסייבר בפרקליטות המדינה והממונה על הבחירות לרשויות המקומיות במשרד הפנים, בבקשה למידע ונתונים על מקרים של תקיפות סייבר; הפצת מידע כזב או כל התנהגות רשת לא תקינה אחרת שבוצעה בהקשר של הבחירות לכנסת והבחירות לרשויות המקומיות.

לצערנו לא נתקבל כל מידע קונקרטי המתאר מגמות ולא נתקבלו כל נתונים. נציגת מערך הסייבר ציינה בתשובתה לפנייתנו כי "המידע מסווג", אף כי לא התבקש כל מידע מזהה על אירועים פרטניים או מידע על דרכי פעולה מבצעיות, אלא מידע על היקף כולל של אירועים ועל מגמות כלליות בלבד. נציגת הפיקוח על הבחירות לרשויות המקומיות במשרד הפנים מסרה כי ככל שהתקבל מידע בנושאים אלו, הוא הועבר לרשות הסייבר או למשטרה ואין בידי המשרד ריכוז נתונים לגביו. ממחלקת הסייבר בפרקליטות המדינה טרם התקבלה כל תגובה, למרות תזכורות בנושא.

ככלל, לא ברור מהו היקף המידע והנתונים המצויים בנושא ביחס לישראל וכיצד לשפר את השקיפות בנושא בלי לפגוע בהיבטים של אבטחת מידע וסייבר. יחד עם זאת, נראה כי יש חשיבות בבירור נוסף בעניין זה, כחלק מן היכולת לפקח על רמת המודעות ועל אופן ההיערכות להתמודדות הנדרשת בקרב הגופים הנוגעים בדבר. בהקשר זה נציין כי **בדיון שנערך בוועדת המדע והטכנולוגיה של הכנסת** בנובמבר 2018 דיווח נציג של חברה עסקית אשר סיפקה שירות לאחת המפלגות במסגרת הבחירות לרשויות המקומיות, כי ביום הבחירות חוותה מערכת הטלפונים של מפלגה זו מתקפה אשר שיתקה אותה למשך חמש שעות, ובמהלכה הופנו לקווי המפלגה 85,000 שיחות בקצב של 300 שיחות בשנייה (כאשר כל שיחה הגיעה כביכול ממספר אחר). לא נמסרו דיווחים דומים (וממילא גם לא מקיפים יותר) על-ידי נציגי הגופים הרשמיים שנכחו בדיון, וכאמור לא ברור מה היקף המידע המצוי בידם בנושא.

נציין כי גם הפניות לנציגות החברות "גוגל" ו"פייסבוק" לא הניבו נתונים פרטניים ביחס לנושא בישראל, אך כפי שמצוין בטקסט בקצרה, התייחסו לסוגיות מדיניות הקשורות בנושא המסמך.

אז מה עושים בעניין? ומה (עוד) אפשר לעשות?

בהינתן כי מדובר בתופעות שונות שלהן מאפיינים שונים, אין "פתרון קסם" אחד שמספק מענה כולל לאתגרי השיח הדמוקרטי ברשת ולניסיונות ההשפעה על הליכי בחירות. פתרונות שונים ושחקנים שונים נוטלים חלק בתהליך. דוגמאות למענים אפשריים יוצגו להלן:

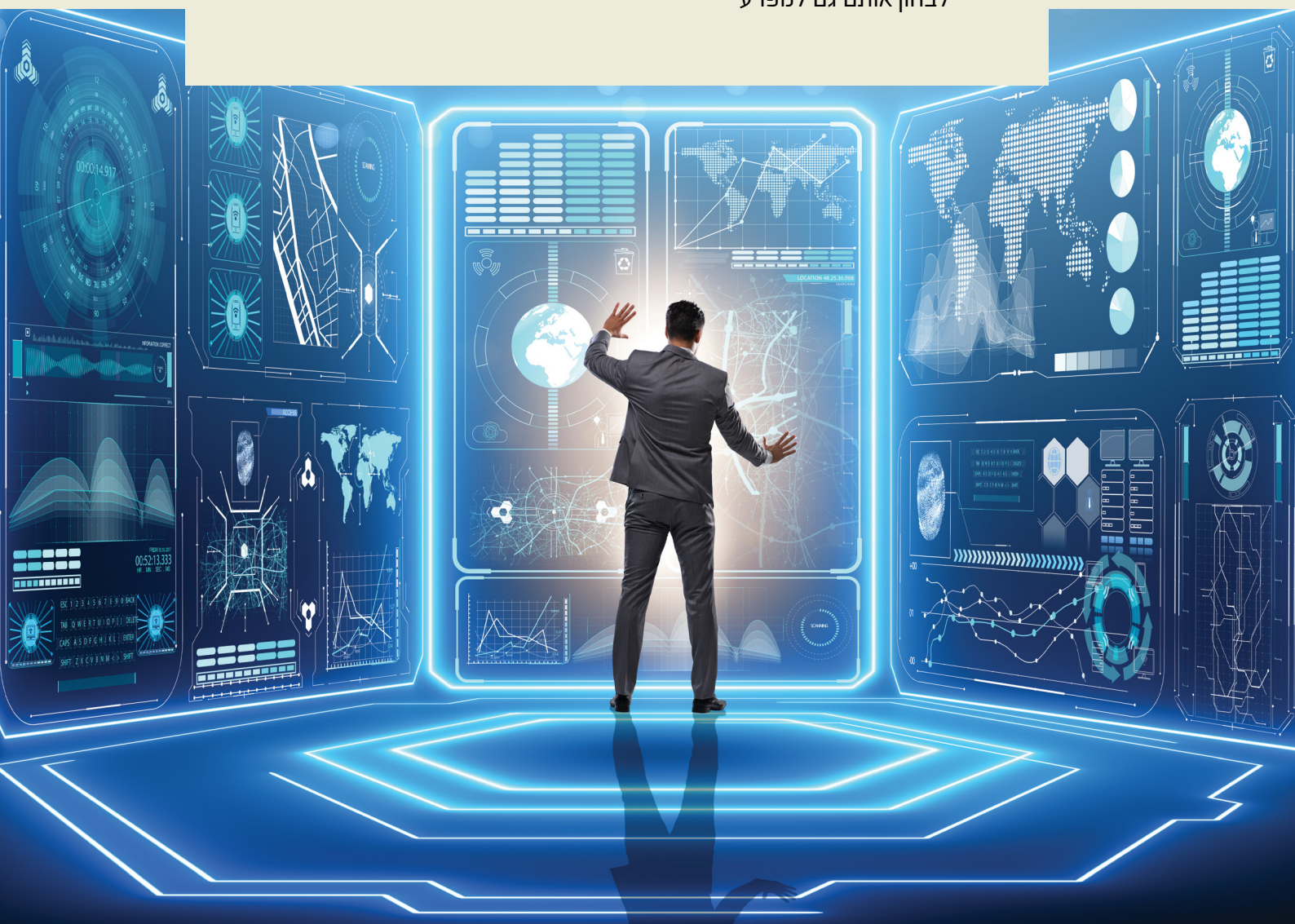
// חיזוק השקיפות ברשת //



כדי לצמצם את אי הוודאות ביחס לאמינות ולהקשר (Context) של מידע, נבחנים או ננקטים צעדים שונים הן מצד ענקיות האינטרנט ביוזמתן, והן מהלכים לחייב בחקיקה או בהסכמה חברתית כללי משחק משותפים וכללי שקיפות נדרשים. זירה ספציפית שבה נוקטות החברות במהלכים לשם חיזוק השקיפות היא פרסום פוליטי.

בין האלמנטים שמקדמת פייסבוק:

- אפשרות של משתמשים להבין מדוע הם נחשפים לפרסומות ספציפיות
- ביחס לפרסום פוליטי, יידרש הליך רישום ואישור לאימות זהות המפרסם ויוצג בראש המודעה מידע באשר למי שילם עבורה
- כמו כן, תוקם "ספרייה" שתכלול את כלל הפרסומים הפוליטיים כך שניתן יהיה לבחון אותם גם למפרע



יש לציין כי במקביל מועלות טענות מצד עמותות וספקים חיצוניים של שירותי אימות מידע ופרסום פוליטי ביחס להגבלות שמטילה פייסבוק עצמה על האפשרות של כלים חיצוניים לפעול כדי לשקף מידע מתוך הרשת החברתית.

על פי תשובת חברת "גוגל" בארה"ב, באירופה ובהודו הושק כלי המחייב גילוי נאות מגורמים המשלמים עבור מודעה הקשורה לבחירות, כולל הצגה על גבי המודעה של פרטי הגורם המשלם עבורה. נציגת "גוגל" ציינה כי בשל הקדמת הבחירות בישראל, לא תספיק החברה להציג כלי זה בישראל טרם הבחירות ולכן פרסום פוליטי איננו מזהה על ידי החברה. עוד צוין, כי החברה מאפשרת למשתמשים בשרותיה או בשירותים העושים שימוש בשירותי פרסום שלה לקבל מידע מדוע הם נחשפים לפרסום ספציפי.

// "בדיקת עובדות" (Fact Checking) //



כדי לצמצם את התפוצה של מידע כזב, מופעלים אתרים ייעודיים או ארגונים המספקים שירותים לשם בדיקת אמינותו של המידע. כך לדוגמה, האתר העצמאי PolitiFact עושה שימוש ויזואלי ומילולי במה שהוא מכנה "מד אמת" כדי לסווג את אמינותו של מידע בנושאים פוליטיים בעיקר בארה"ב. לדברי נציגת פייסבוק, החברה עושה בין השאר, שימוש בשירותים של צדדים שלישיים לשם "בדיקת עובדות" ביחס לכתבות, תמונות וסרטונים. תיוג של מידע כשקרי, יוריד את מקומו ב"ניוז-פיד"; דפים ואתרים שמפיצים מידע כזב מספר פעמים יוגבלו בתפוצת המידע שלהם, ובאפשרות לפרסם בפייסבוק. על פי תשובת חברת "גוגל" היא מעניקה משקל רב לשאלת מהימנותו של תוכן, בפרט ביחס לתוכן חדשותי ובדגש על אירועי משבר בזמן אמת - בהם היא תעדיף מידע פחות עדכני ממקור מהימן על פני מידע חדש יותר ממקור פחות אמיין. בנוסף, החברה הציגה ב"יוטיוב" שירותים המציגים באופן מובחן מידע חדשותי ממקורות אמינים.



// חסימה והסרת תוכן של "בוטים", "טרולים" והתארגנויות דומות //



ענקיות הרשת, לצד גופי ניטור ומעקב ממשלתיים או ארגוני מגזר שלישי, פועלים כדי להגביל את היקפי הפעילות של מערכות אוטומציה להפצת תוכן או שחקנים אנושיים הפועלים כקבוצה לשם קידום אינטרס באופן שאיננו אותנטי (מה שפייסבוק מכנה, Coordinated Inauthentic Behavior IX CIB).

פעולות כאלה יכולות להתבצע באמצעות:

- זיהוי מאפיינים מבניים (לדוגמה שימוש במספר מצומצם של כתובות IP מאזור מרוחק)
- זיהוי של תוכן כזב ומקורות ההפצה שלו
- זיהוי מאפיינים אחרים בתוכן - לדוגמה שגיאות שפה הנובעות משימוש בכלי תרגום אוטומטיים

הגופים העוסקים בניטור יכולים לדווח לחברה על שימוש לא הולם, או לחלופין לנקוט בעצמם בצעדים כנגד מקורות המידע. כך למשל נטען לאחרונה בתקשורת כי ארצות הברית ביצעה מתקפות סייבר ישירות כנגד "חוות טרולים" שפעלו מרוסיה לשם קידום אג'נדה זרה.

// חקיקה, הסדרה והגדרת סמכויות //



בין אם המדובר ביוזמות להטלת אחריות על ענקיות האינטרנט ביחס לתוכן המופץ על גביהן; בין אם המדובר בעדכון של חוקי תעמולה וסמכויות של ועדת הבחירות (שתי היוזמות מוצעות במסגרת דוח של הפרלמנט הבריטי בנושא דיסאינפורמציה ופייק ניוז שפורסם לאחרונה), ניתן לומר כי השיח הציבורי ביחס לאינטרנט השתנה בשנים האחרונות. מצידוד רווח בגישת השוק חופשי ונטול הרגולציה, לגישה הגורסת כי יש מקום לשקול חקיקה והסדרה בהיבטים מסוימים - הן לשם השוואת כללי המשחק בין חברות הפועלות במרחב הפיזי והמקוון (leveling the playing field) והן לשם הסדרת המרחב המקוון כשלעצמו. בישראל, מתקיים לאחרונה דיון באשר לאחריות ולסמכות במרחב הסייבר - הן סביב **תזכיר "חוק הגנת הסייבר"**; והן בקונטקסט של בחירות, בין השאר בשאלה האם לוועדת הבחירות המרכזית בישראל ישנם כלים מקצועיים ורגולטורים מספקים להתמודדות עם איומים במרחב זה. בדיון בוועדת המדע והטכנולוגיה של הכנסת ציינה מנכ"לית ועדת הבחירות, כי הוועדה היא גוף עצמאי על פי חוק אך מתייעצת עם גורמי המקצוע, בהם שירות הבטחון הכללי ומערך הסייבר.

// הסכמות ואמנות //



כלים נוספים לטיפול בסוגיית טוהר הבחירות והשפעה במרחב המקוון, הם כללי פעולה או הסכמות - אלה יכולים להיקבע הן ביחס לשחקנים הפוליטיים (מפלגות ואישיים פוליטיים) והן ביחס לפרקטיקות הנהוגות על ידי ענקיות הרשת עצמן.

כחלק מ"תכנית הפעולה כנגד דיסאינפורמציה" שמקדמת הנציבות האירופית, חתמו החברות האינטרנט: גוגל, פייסבוק וטוויטר באוקטובר 2018 על "קוד אתי" (Code of Practice) וולונטרי. בין העקרונות הקבועים בקוד: לפעול לצמצום ההכנסות מפרסום של אתרים ומשתמשים המציגים דיסאינפורמציה ומידע מוטעה; לשפר את השקיפות ביחס לפרסום פוליטי; לצמצם את השימוש בבוטים ולחסום חשבונות מזויפים; לסייע לאנשים בגיוון מקורות המידע והעמדות המוצגות להם ולתעדף תוכן ממקורות אמינים. על פי הקוד, מידי חודש אמורות החברות להציג דוח מפורט על התקדמותן במשימות אלה. פעולות אלה ננקטות, בין השאר, במטרה לוודא את טוהר הבחירות לפרלמנט האירופי שיתקיימו במאי 2019. בהצהרה של הנציבות האירופית מסוף פברואר 2019 צוין, בעקבות קבלת הדוחות מן ההחברות, כי הן לא סיפקו מידע מפורט ואמות מידה מספקות שיאפשרו לבחון את מידת התקדמותן.

בישראל, מקדם המכון הישראלי לדמוקרטיה חתימה של מפלגות ומועמדים מטעמן על אמנה שבין עקרונותיה: התחייבות שלא להשתמש בבוטים ובחשבונות מזויפים ולסמן תעמולה כך שתהיה מובחנת מתוכן עיתונאי; לא לעשות שימוש בתעמולה מותאמת אישית תוך שימוש במידע ביחס למצבם או נטיותיהם של המשתמשים; ולהקפיד על אבטחת מידע.





קידום המודעות לסיכון שבתקיפות סייבר, לניסיונות השפעה על השיח ולדרכים להתמודד איתם, הוא אמצעי משמעותי לשם צמצום מקרים כאלה. מערך הסייבר במשרד ראש הממשלה פרסם בפברואר 2019 מדריך המתמקד בהגנה על רשתות, תחנות קצה (מחשבים, טלפונים ניידים וכו'), אתרי אינטרנט, דוא"ל וכדומה.

ועדת הבחירות המרכזית פרסמה לאחרונה באתר הוועדה מידע תחת הכותרת "בוא נשמור את מערכת הבחירות נקייה מפייק ניוז". בין השאר, מתייחס המידע לשאלות: "כיצד להימנע מפייק ניוז" ו"איך בכל זאת קוראים חדשות ברשתות חברתיות". כמו כן, מצוינים בדף מספרי טלפון של מוקד החירום של משטרת ישראל למקרים של הפרת סדר ביום הבחירות או עבירות מחשב; והמוקד של המרכז לטיפול באירועי סייבר לתלונות על ניסיונות השפעה פסולה באמצעות פרופילים מזויפים וכו'.



איגוד האינטרנט בשיתוף עם המכון הישראלי לדמוקרטיה והקליניקה למשפט, טכנולוגיה וסייבר באוניברסיטת חיפה, פתחו דף אינטרנט המאפשר לגולשים לדווח על שימוש בבוטים, חשבונות מזויפים או תעמולה שאינה מזוהה. על פי הדף, הגופים ייבחנו את המידע שידווח ולאחר בחינת כל מקרה יחליטו האם יש מקום לפנות לגורמים הרלבנטיים בהם: פלטפורמת הרשת בה פורסם התוכן, משטרת ישראל והפרקליטות או ועדת הבחירות המרכזית.

צו המורה על שקיפות בתעמולה באינטרנט

בעקבות עתירה שהוגשה לוועדת הבחירות המרכזית, פרסם יו"ר הוועדה, השופט חנן מלצר, צו המורה על שקיפות בתעמולה באינטרנט. לפי הצו שפורסם ב-27 בפברואר 2019 חל איסור על מפלגות או הפועל מטעמן בתשלום או בתיאום ("המפרסמים") לפרסם פרסום שאינו מזוהה באינטרנט (כולל ברשתות חברתיות ובמנועי חיפוש). בכל פרסום, יידרשו המפרסמים לפרט לצד המודעה או בגופה את זהותו, שמו ומענו של מזמין המודעה ומידע ודרכי התקשרות עם מזמין המודעה. על פי הצו, האחריות תחול על המפרסמים עצמם, ופלטפורמות האינטרנט ינקטו בהליך "הודעה והסרה" על בסיס דיווח של משתמשים על הפרה של הצו. עוד ציין השופט בצו כי "כל פרסום אנונימי ברשת האינטרנט על ידי המפרסמים מקשה על גורמי הביטחון שלנו לפעול כדי להדוף חששות מפני התערבויות זרה בבחירות לכנסת ה-21 שעלולות להיעשות באופן אנונימי".

// רשימת מקורות //

- רועי גולדשמידט, **הפצת מידע כוזב ותקיפות סייבר לשם השפעה על מערכות בחירות**, מרכז המחקר והמידע של הכנסת, 11 ביוני 2017
- ירון אונגר, חדשות כזב ברשת האינטרנט והפגיעה בהליך הבחירות, הלשכה המשפטית של הכנסת, תחום חקיקה ומשפט משווה, 24 בפברואר 2019
- רון שמיר ואלי בכר, **התקפות סייבר על מערכת הבחירות- איך מתמודדים?**, המכון הישראלי לדמוקרטיה, פברואר 2019
- קרין נהון ושירה ריבנאי בהיר, "תעמולת בחירות בראי האינטרנט והרשתות החברתיות", חומר רקע לוועדת בייניש, ינואר 2016
- תהילה שוורץ אלטשולר וגיא לוריא, **מתחייבים לבחירות הוגנות ברשת**, המכון הישראלי לדמוקרטיה, 18 בפברואר 2019, כניסה: 19 במרס 2019
- אתר איגוד האינטרנט הישראלי, **הצטרפו למאבק ברשתות הבוטנים, הפרופילים המזויפים והתעמולה הלא מסומנת**, 10 במרס 2019, כניסה: 19 במרס 2019
- מערך הסייבר הלאומי, משרד ראש הממשלה, **הנחיות התגוננות למפלגות לקראת מערכת הבחירות**, 21 בפברואר 2019
- דודי סימן טוב, גבי סיבוי וגבריאיל אראל, "איומים קיברנטיים על תהליכים דמוקרטיים", המכון למחקרי ביטחון לאומי (INSS) סייבר, מודיעין וביטחון, כרך 1, גיליון 3, דצמבר 2017
- תבי"כ 8/21 (יושב ראש ועדת הבחירות המרכזית לכנסת ה-21) עו"ד שחר בן מאיר ועו"ד יצחק אבירם נ' מפלגת הליכוד ואחרים, החלטה, 27 בפברואר 2019
- ניבה אלקין-קורן, "המתווכים החדשים ביכיר השוק' הווירטואלית", ממשל ומשפט ו(2), 2003
- נועה אלפנט לפלר, מנהלת בכירה למדיניות ציבורית, Google ישראל, תשובה על פניית מרכז המחקר והמידע של הכנסת, דוא"ל, 3 במרס, 2019
- גורדנה קטלר, מנהלת מדיניות, פייסבוק ישראל, תשובה על פניית מרכז המחקר והמידע של הכנסת, דוא"ל, 18 בפברואר, 2019
- United States House Committee on Appropriations Subcommittee on Financial Services and General Government, Hearing on Election Security and the Integrity of Election Systems, [Securing America's Digital Democracy: Preparing for 2020](#) - Prepared Statement by Eric Rosenbach, February 27, 2019, accessed: March 19th 2019
- 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: March 19th 2019
- Christopher S. Chivvis, [Understanding Russian "Hybrid Warfare" And What Can Be Done About it](#), Testimony Presented Before the House Armed Services Committee on March 22, 2017, accessed: March 19th 2019
- US Cyber Command, [Achieve and Maintain Cyberspace Superiority, Command Vision for US Cyber Command](#), April 2018
- Federal Trade Commission, [Data Brokers A Call for Transparency and Accountability](#), May 2014, pp. 9-16
- Jenny Gesley, Germany: [Social Media Platforms to Be Held Accountable for Hosted Content Under "Facebook Act"](#), Library of Congress, Global Legal Monitor, July 11, 2017, accessed: March 19th 2019
- European Commission, [Statement on the Code of Practice Against Disinformation: Commission Asks Online Platforms to Provide More Details on Progress Made](#), February 28, 2019, accessed: March 19th 2019
- European Parliament, [Computational Propaganda Techniques](#), At a Glance, October 18, 2018, accessed: March 27th 2019
- UK Parliament, House of Commons Digital, Culture, Media and Sport Committee, [Disinformation and 'Fake News': Final Report](#), February 14, 2019
- UK Information Commissioner's Office, [Democracy disrupted? Personal Information and Political Influence](#), July 18, 2018
- 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
- Karin Nahon, Jeff Hemsley, "Going Viral", October 2013, Polity, p:16
- Jacob Soll, [The Long and Brutal History of Fake News](#), Politico Magazine, December 18, 2016, accessed: March 19th 2019
- Ellen Nakashima, [U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms](#), Washington Post, February 27, 2019, accessed: March 19th 2019

כתיבה: רועי גולדשמידט | אישור: יובל וורגן, ראש צוות | עיצוב והפקה: מחלקת הדפוס והפרסומים של הכנסת