התערבות זרה והשפעה איראנית ברשתות החברתיות בישראל

ענבל אורפז ודודי סימן טוב[1]

מאמר זה כולל הצגה של תופעת ההתערבות הזרה האיראנית ברשתות החברתיות בישראל בשנים 2020 - 2022. מטרתו להעמיק בתופעה, לאפיין אותה, לדון בהשלכותיה ולהציע מדיניות להתמודדות עימה. מהמחקר עולה שגורמי התערבות זרה בשיח הישראלי ברשתות החברתיות במקרים שנבחנו במסגרת המחקר, אינם מצדדים בקבוצה מסוימת בחברה הישראלית או באג'נדה מסוימת ומטרתם להעמיק שסעים בחברה הישראלית כדי להחלישה. המאמר פותח בתיאור של הרשתות המרכזיות שפעלו בשיח הישראלי בשנים האחרונות, בהמשך מוצג ניתוח של התופעה וזיהוי דפוסי הפעולה המרכזיים של המבצעים ובסופו יובאו המלצות למדינות, לממשלה, לגורמי חברה אזרחית ולציבור.

מבוא[2]

בעידן הדיגיטלי הפכו הרשתות החברתיות לכיכר העיר הווירטואלית בשגרה ובחירום. מעל 70% מהציבור הישראלי משתמשים ברשתות חברתיות[3] למגוון שימושים: לצריכת מידע, להבעת דעות מגוונות, לקבלת המלצות על מוצרים ולשמירה על קשר עם חברים. אך לא רק אזרחי ישראל משתמשים במרחב הווירטואלי ברשתות החברתיות בישראל. לעיתים, חשבונות שמפרסמים תכנים שפונים לקהל הישראלי אומנם נראים "ישראלים", אך עומדים מאחוריהם גורמים עוינים שמעוניינים להתערב ולשבש את השיח הישראלי כדי לקדם את מטרותיהם האסטרטגיות.

לראשונה בישראל מחקר המציע מבט מעמיק על מִבְצָעֵי התערבות זרה ברשתות החברתיות בישראל שהתנהלו בשנים האחרונות. מטרת המחקר להעמיק בתופעה, לאפיין אותה, לדון בהשלכותיה ולהציע מדיניות להתמודדות עימה.

ממאמר זה עולה שגורמי התערבות זרה בשיח הישראלי ברשתות החברתיות במקרים שנבחנו במסגרת המחקר, אינם מצדדים בקבוצה מסוימת בחברה הישראלית או באג'נדה מסוימת ומטרתם העיקרית היא להעמיק שסעים בחברה הישראלית כדי להחלישה. המאמר מציע מבט מעמיק על מבצעי התערבות זרה ברשתות החברתיות בישראל שהתנהלו בשנים האחרונות. מאחורי רוב מבצעי ההשפעה שנחקרו במסגרת מחקר זה עומדת ככל הנראה איראן, אך בתקופה האחרונה ישנן עדויות למבצעי השפעה של גורמים נוספים.

המאמר פותח בתיאור של הרשתות המרכזיות שפעלו בשיח הישראלי בשנים האחרונות, בהמשך מוצג ניתוח של התופעה וזיהוי דפוסי הפעולה המרכזיים של המבצעים ובסופו יובאו המלצות למדינות, לממשלה, לגורמי חברה אזרחית ולציבור. מטרתו היא לבחון חשד להתערבות זרה בשיח הישראלי ברשתות החברתיות בישראל, לאפיין את התופעה ולהציע מדיניות להתמודדות עימה.

תיחום תקופת המחקר: המחקר כולל דיון במבצעי התערבות זרה שפעלו ברשתות החברתיות בישראל בשנים 2020 עד סוף 2022.
שאלות המחקר שנבחנו:

- מה הם דפוסי הפעולה של מבצעי התערבות זרה ברשתות החברתיות?
- כיצד אפשר לקשור פעילות החשודה כלא אותנטית ברשתות החברתיות לגורמי השפעה זרים ומה מנסים להשיג הגורמים העומדים מאחוריהם?
- מה אפשר ללמוד מאופן הטיפול ברשתות שנחשפו?
- כיצד משפיעות הרשתות על הביטחון הלאומי, על הדמוקרטיה ועל החוסן הלאומי?
- כיצד נכון לטפל בבעיה הזו שמסכנת את חוסנו של העורף הישראלי ברמה הלאומית?

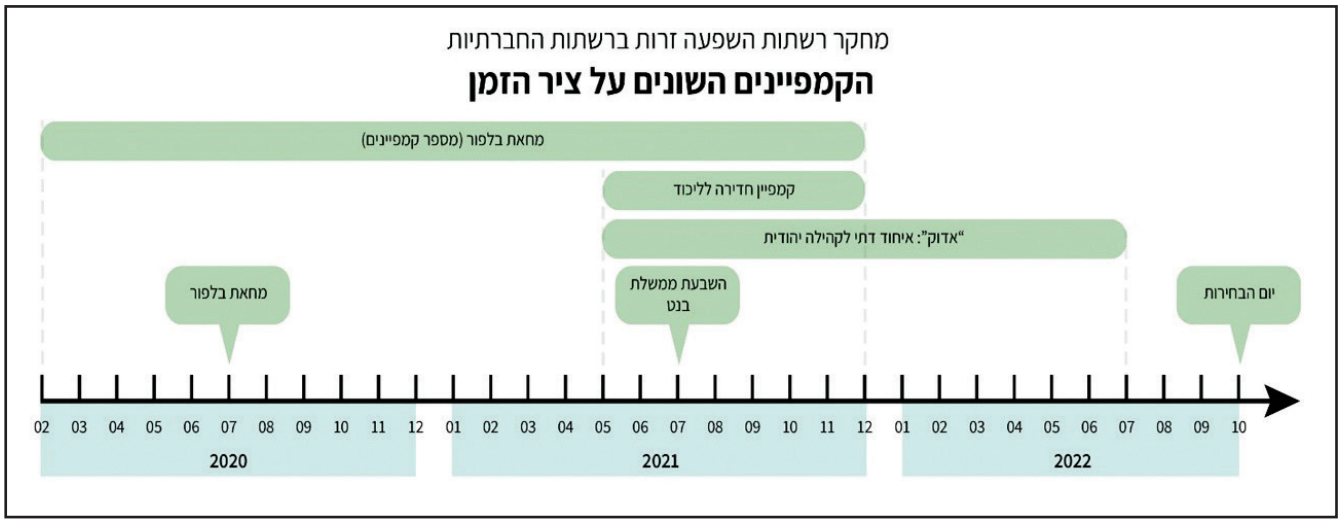
---

1 ענבל אורפז, יועצת חדשנות אסטרטגית ויועצת לרשות החדשנות. בעבר, עיתונאית TheMarker וחוקרת בתוכנית ליפקין שחק במכון למחקרי ביטחון לאומי. ערכה את המחקר בחוקרת במכון למחקרי ביטחון לאומי. דודי סימן טוב הוא סגן ראש המכון לחקר המתודולוגיה של המודיעין וחוקר בכיר במכון למחקרי ביטחון לאומי.

2 המחקר בוצע במכון למחקרי ביטחון לאומי בתוך שיתוף פעולה בין המכון ועמותת FakeReporter. המחברים מודים לענבר יסעור ולניצן יסעור, לאחיה ש"ץ מ-FakeReporter ולעוזרי המחקר עמוס הרביץ ושובל בן־יאיר.

3 https://www.cbs.gov.il/he/publications/doclib/2022/1873_well_being_2021/prt11_5_h.pdf

תרשים 1: ציר זמן - מבצעי התערבות זרה ברשתות החברתיות בישראל שנכללו במחקר ואירועים מרכזיים בישראל בתקופה זו



פרק ראשון:
תיאור מבצעי ההתערבות הזרה במחקר

מבצעי ההתערבות הזרה שחקרנו במחקר זה פעלו באמצעות חשבונות שאת ההתנהגות שלהם ברשתות החברתיות אפשר לאפיין כלא אותנטית ובאמצעות חשבונות שאפשר לקבוע בסבירות גבוהה שהמפעילים שלהם הם גופים מדינתיים זרים. בהמשך המסמך נפרט כיצד נקבע בנוגע לכל חשבון האם אינו אותנטי, זר או איראני. במסמך שפרסמה חברת Meta[4] שבבעלותה נמצאת פייסבוק, הדן במבצעי השפעה שהתקיימו בשנים 2017–2020, היא הגדירה את מבצעי ההשפעה כ"מאמצים מתואמים לבצע מניפולציה או לשבש את השיח הציבור למען מטרה אסטרטגית".

במחקר זה התמקדנו בשלוש קבוצות של מבצעי התערבות שכוונו לקהלי יעד בישראל מתחילת שנת 2020 ועד סוף 2022. כללנו גם מיפוי ראשוני של רשתות שפעלו סביב מערכת הבחירות בנובמבר 2022.

1. רשתות המתחזות לפעילים במחאת בלפור (פברואר 2020 - דצמבר 2021)

תחת קטגוריה זו כללנו לפחות חמישה מבצעים ורשתות שזוהו על ידי פייסבוק ו־FakeReporter שיש ביניהם קווי דמיון מבחינת תכנים ודפוסי פעילות. המשותף למבצעים הוא שהם כללו התחזות לקבוצות פעילים ממחאת בלפור (למשל "הדגלים השחורים", "אין מצב"). המבצעים פעלו החל מראשית 2020 עד סוף 2021. המידע בנוגע לחלק מהמבצעים חלקי ביותר, מאחר שפייסבוק שיתפה את המידע על אודותיהם בפרסומים שלה אחרי שהוסרו החשבונות, התיעוד שלהם והמידע על אודותיהם מוגבל.

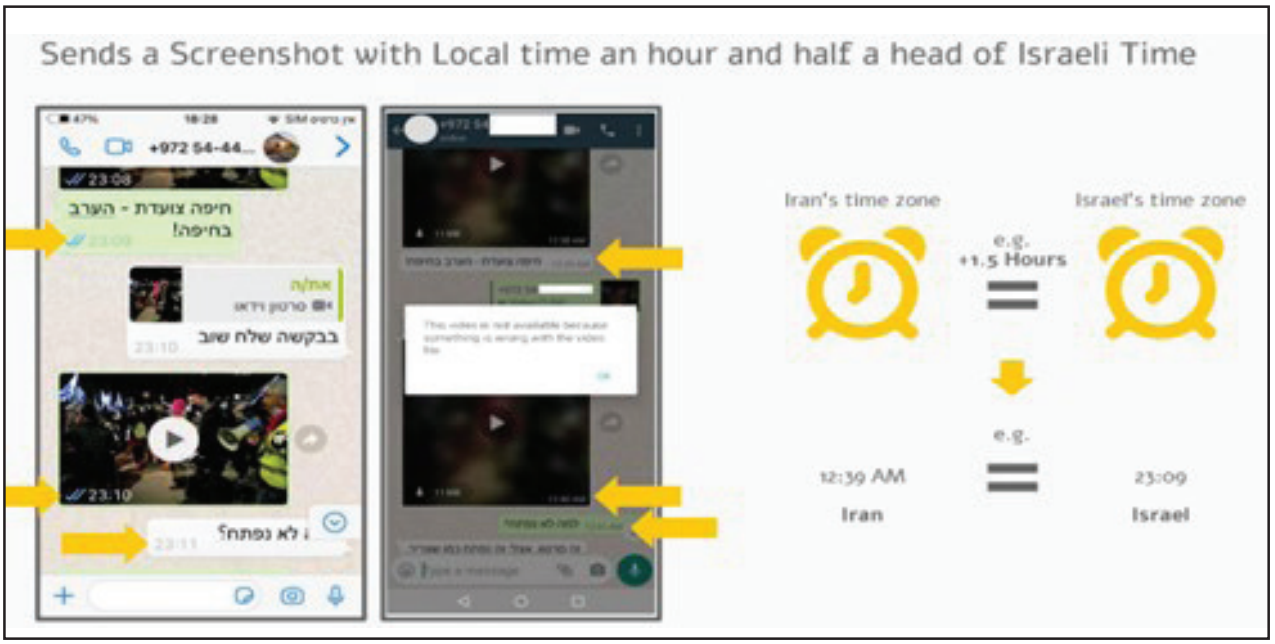
במבצעי התערבות אלה נעשה שימוש במגוון הפלטפורמות והכלים העומדים לרשות מתכנני קמפיינים, כולל חשבונות פייסבוק, אינסטגרם, וואטסאפ וטוויטר, הקמת אתר אינטרנט, קבוצות פייסבוק וערוצי טלגרם. במבצעים השונים נעשה שימוש בשיטות פעולה שונות מבחינת שימוש בשפות (אחת הרשתות פעלה בעברית וגם באנגלית), התחזות לארגוני מחאה קיימים ולאנשים פרטיים, תיוג עשרות אלפי חשבונות באינסטגרם ועוד.

המבצע הראשון - black lags IL - זוהה על ידי פייסבוק ונחשף בדוח שפרסמה Meta בנובמבר 2020.[5] הרשת החברתית הסירה את החשבונות שהיו חלק מהמבצע, וטענה שגורמים איראניים עמדו מאחוריו. לפי הדוח של הרשת החברתית זוהו 12 חשבונות פייסבוק, שני עמודי פייסבוק ו־307 חשבונות באינסטגרם שהיו חלק מהמבצע. כ־1,100 חשבונות עקבו אחר אחד או יותר מהדפים וכ־9,500 אנשים עקבו אחרי חשבון אינסטגרם אחד או יותר מהרשת.

4 Threat Report: The State of Influence Operations 2017-2020, *Facebook*, May 2021. From: https://about.fb.com/wp-content/uploads/2021/05/IO-Threat-Report-May-20-2021.pdf

5 Detailed Report: October 2020 Coordinated Inauthentic Behavior Report *Facebook*, October 2020. From: https://about.fb.com/wp-content/uploads/2020/11/October-2020-CIB-Report.pdf

תרשים מס' 2: התכתבות בין מפעיל ברשת שפנתה לפעילים במחאת בלפור לפעיל שמדגים פער שעות שאופייני לאיזור זמן אירני



בדוח של חברת Graphika נטען כי לא הושקעו משאבים משמעותיים בבניית חשבונות אותנטיים. כך למשל, כל אחד מהשמות "Leah" ו־"Ori" נבחר עבור תריסר חשבונות ברשת. חשבונות האינסטגרם נוצרו לפי תבנית שם מלא ושנת לידה. כמו כן, הם מציינים גם שלא נעשה מאמץ לבחור בתמונות פרופיל אמינות - הם השתמשו בתמונות של מאגר התמונות של Getty (כולל חותמת המים של החברה שהופיעה על השמות) או שהשתמשו בחשבונות בעלי שמות עבריים בתמונות פרופיל שבהן הופיעו נשים ערביות לובשות חיג'אב.[6]

בפייסבוק מציינים כי בזמן שהרשת הוסרה היא הייתה בשלב מוקדם של בניית קהל העוקבים שלה. הרשת השתמשה בחשבונות מזויפים שרובם נוצרו באותה פרק זמן. במשך הזמן החשבונות הללו שינו את שמותיהם ופעלו כדי לקדם מטרות שונות שמשרתות יעדים שונים של מבצעי השפעה אירניים. החשבונות פרסמו תמונות, memes ותכנים בעברית ובערבית. בחלק מהמקרים פורסמו תכנים זהים, למשל אותה תמונה, על ידי חשבונות שונים ברשת. התכנים נגעו לאירועים אקטואליים, בהם הפגנות נגד נתניהו וביקורת על המדיניות שלו בנושא מגפת הקורונה.

אחד הדברים המעניינים שעולים מהדוח של חברת Graphika הוא שגם בפעילות מול הקהל הישראלי השתנו התכנים ובכל שלב בפעילות הרשת נגעו בנושא אחר בהתאם לגורמים שהיו במרכז השיח בישראל ויכלו לעורר מחלוקות: בחודשים הראשונים של שנת 2020, עם פרוץ מגפת הקורונה, התמקדו התכנים בביקורת על מדיניות נתניהו בהתמודדות עם המגפה. לפי הדוח, בתקופה זו הייתה ההתמקדות במתח בין הממשלה והאזרחים ובמחיר הגבוה שהמגפה גובה. בחודש יולי באותה שנה החלו חשבונות ברשת לפרסם תכנים המזוהים עם "הדגלים השחורים" - תנועת מחאה שהחלה לפעול ולמחות באותה תקופה נגד נתניהו.

בדוח של גרפיקה מצוין כי באחד המקרים פורסמו בחשבון שהשתייך לרשת פרטי חשבון PayPal שאפשר להעביר אליו כסף לתרומות למבצע. לא ידוע האם בוצעו תרומות לחשבון. עוד לפי פייסבוק: מפעילי הרשת ניסו להסתיר את הזהות שלהם, אך בחברה מצאו קשרים ביניהם לבין ישויות הקשורות ל־EITRC, חברת IT הפועלת מטהרן.

בדצמבר 2020 החלו להתקבל בצוות, שלימים התגבש כ־FakeReporter, דיווחים על אודות אדם חשוד שהצטרף לקבוצות וביקש בשיחות ישירות שניהל עם החברים בהן לשלוח לו תמונות מהפגנות בישראל. בהתכתבויות עם החשוד עלו סימנים שקושרים אותו

6 Lea Ronzaud, Ira Hubert and Ben Nimmo, Capture the Flag: Iranian Operators impersonate Anti-Netanyahu "Black Flag" Protesters, Amplify Iranian Narratives, *Graphika*, November 2020. From: https://public-assets.graphika.com/reports/graphika_report_capture_the_flag.pdf

תרשים מס' 3: מס' הודעות שפורסמו בחודש בערוץ הטלגרם של אדו"ק (מבוסס Telemetrio)

לגורמים איראניים: עברית קלוקלת, סימני שאלה הפוכים (؟) האופייניים לשפה הפרסית, צילומי מסך של טלפון עם ממשק בשפה הפרסית ופער שעות של 1.5 שעות (הפער בין ישראל ואיראן). נוסף על כך זוהו ניסיונות לגייס תרומות מאזרחים ישראלים.

כחלק מהמערך שזוהה וקשור למבצע ההתחזות של Movements BB, נמצא, נוסף על הנוכחות הזרה בקבוצות הוואטסאפ ויצירת הקשר עם האזרחים הישראלים, גם אתר אינטרנט המתחזה לאתר של "הדגלים השחורים". לאתר זה עלו התמונות ששותפו עם המפעילים ועדכונים על הפגנות. במסגרת המבצע נרכשו במהלך נובמבר 2020 שלושה שמות דומיין, בדומה למבצע flags black il. נוסף על כך הוקמו עבורו כ־10 חשבונות ברשתות החברתיות, כולל חשבון בערבית. אחד האתרים וערוץ הטלגרם עדיין פועלים ברשת. החשבונות עקבו אחר פעילים מרכזיים במחאה.

המבצע פורסם בערוץ "כאן 11",[7] ומפעיליו הגיבו על כך בסרטון שיצרו והופץ בערוץ הטלגרם של המבצע. בעקבות הכתבה בטלוויזיה הישראלית סגרו פייסבוק וטוויטר את החשבונות הרלוונטיים.

2. "אדוק" - האיחוד הדתי הוירטואלי למען הקהילה הדתית (2020-2021)

רשת "אדוק" פעלה בכמה פלטפורמות - כולל פייסבוק, טוויטר וערוץ טלגרם - ופרסמה תכנים בעלי אוריינטציה ימנית הנוגעים לחברה החרדית. חברת Meta אישרה ל־BBC שמאחורי הרשת עומדים מפעילים איראניים. חשבונות הפייסבוק והטוויטר המשויכים לרשת נסגרו על ידי הפלטפורמות, אך ערוץ הטלגרם שלה ממשיך לפעול.

השם של המבצע נגזר מראשי התיבות שהמציאו מפעילי הרשת אדוק - "האיחוד הדתי הוירטואלי למען הקהילה הדתית". בערוץ הטלגרם מפורטים הנושאים שבהם עוסק הערוץ: "הקול של הציבור הדתי, חדשות בזמן אמת, חדשות חרדיות בזמן אמת, אנחנו פועלים במאבק באלימות (משטרתית וערבית), אנטי חילוני, שאלות מעניינות בהלכה, סיפורי צדיקים".

נראה כי מטרת מבצע אדו"ק היא להעמיק את הפילוג והשיסוע בישראל. מספר הרשומים לערוץ הטלגרם של אדוק הגיע ב־20 במרץ 2022 לשיא של 770 משתמשים. אף שמדובר במערך מושקע שהפיץ תכנים באופן עקבי ושיטתי, הוא לא הגיע לחשיפה נרחבת ולא ידוע על השפעה קונקרטית שאפשר לייחס לו על הציבור הישראלי. עם זאת, ייתכן שישנה השפעה שלא זוהתה או שייעשה בעתיד שימוש במערך.

רוב התכנים שפורסמו בערוץ הטלגרם מועתקים מצייצני רשת חרדים אמיתיים. הדמויות שהפעילו את העמוד וקבוצת הפייסבוק של המבצע, השתמשו בתמונות גנובות של אדם רוסי יהודי שנפטר. עוד מאפיינים של הרשת הם העתקת תכנים מחשבונות אותנטיים שמשרתים את האג'נדה של הרשת, יצירת נכסים מזויפים לבניית אותנטיות (לוגו, המצאת שם ל"איחוד" - אדו"ק, הקמת עמוד מיוחד כחלק מבניית הזהות המזויפת), הוספה של הלוגואים של הרשת לתמונות שהיא מפרסמת, הסתה, גזענות, שיח שנאה, ניסיון

7 אורן אהרוני, תחקיר: מי מנסה להתחזות לפעילי הדגלים השחורים?, כאן, 3 במארס 2021. https://www.kan.org.il/content/kan-news/politic/281335/

לפנות לרגש, עושים שימוש בהאשטגים קבועים (#מספיק_זה_מספיק, #חדשות_חמות וכו'), שיתוף התכנים של הרשת לתוך קבוצות וערוצים שפונים לקהל ימני וחרדי.

הרשת נועדה לקדם סדר יום חרדי בעל אוריינטציה ימנית. הרשת פרסמה אמירות נגד המשטרה והדהדה טענות בדבר אוזלת ידו של צה"ל. ברשת היה עיסוק גם בסוגיות אחרות שעל סדר היום כמו קורונה (בתקופות שיא של המגפה), יוקר המחייה בישראל וכו'. כמו כן פרסמה הרשת סוגיות הלכתיות[7] בפינות תוכן קבועות תחת ההאשטג סוגיות_מעניינות_בהלכה ושעות כניסת שבת בכל שבוע.

FakeReporter חשפו את פעילות הרשת בחשבון הטוויטר שלהם ב־3 בפברואר 2021.[8] הרשת סוקרה ברשת BBC,[9] ובתגובה לפניית הכתב לקבלת תגובה מ־Meta, התקבל אישור שמפעילי הרשת הם אירנים. ב־4 בפברואר, יום לאחר חשיפת הרשת, הגיבו מפעיליה על חשיפתה ועל סגירת חשבונות הפייסבוק והטוויטר שלה.

3. יצירת קשר עם פעילים פוליטיים בסביבת נתניהו (יולי 2021-דצמבר 2021)

רשת חשבונות זו התגלתה בעקבות דיווח שהתקבל בנובמבר 2021 שלפיו חשבון חשוד יצר קשר עם אזרחית ישראלית וניסה לדובב אותה בנוגע להפגנות תמיכה בימין. בעקבות הדיווח התגלו כעשרה חשבונות פייסבוק וטוויטר מזויפים, שהיו חברים בכ־90 קבוצות בפייסבוק, יותר ממחציתן של תומכי נתניהו. החשבונות ברשת פרסמו תכנים בעיקר נגד הממשלה שכיהנה באותו זמן בראשות נפתלי בנט. ככל הנראה הרשת ניסתה להגביר את גובה הלהבות בישראל באמצעות תדלוק הפגנות ופעילות מחאה.

החשבונות המזויפים הגיבו לפעילים פוליטיים בולטים, וישנן עדויות לכך שהצליחו ליצור קשר ישיר עם חלקם ולקבל את מספרי הטלפון שלהם. החשבונות הדהדו את המסרים זה של זה, היו ביניהם קשרי חברות וירטואליים, לעיתים הם שיתפו תכנים זהים וזמני הפעילות שלהם היו דומים. החשבונות גם הגיבו לפעילים פוליטיים אמיתיים. החשבונות ברשת יצרו תכנים מקוריים שנועדו, בין היתר, לקדם הפגנות אמיתיות שנערכו בישראל.

באחד המקרים עוצבה ושותפה על ידי מפעילי הרשת הזמנה להפגנה בספטמבר 2021 שבה שולבו תמונות של חשבונות מזויפים שהיו חלק מהרשת, עם תמונות של פעילים פוליטיים אמיתיים שהופיעו בכרזה. לאחר מכן שותפה הכרזה על ידי פעילים פוליטיים בקבוצות הקשורות לליכוד. פעולות שונות שנקטו החשבונות ברשת מצביעות על היכרות עמוקה עם מערך הפעילים הפוליטיים בישראל.

החשבונות שזוהו כחלק מהרשת נפתחו החל מיולי 2021, ודיווחים ראשונים על פעילות חשודה על ידם הגיעו בנובמבר באותה שנה. ב־29.12.2021 שודרה כתבה בנוגע למבצע ההתערבות בחדשות 12,[10] בעקבותיה הסירו פייסבוק וטוויטר את החשבונות שהשתייכו לרשת.

4. הבחירות לכנסת ה־25 - נובמבר 2022

במהלך תקופת המחקר, התקיימו הבחירות לכנסת ה־25 בנובמבר 2022. בתקופת הבחירות, התגלו רשתות בעלות סממנים דומים לרשתות אחרות שנבדקו והופעלו על ידי גורמים אירניים, אך לא בוצעה לגביהם העמקה במחקר זה.

לפני הבחירות: מבצע לפיצול רשימת מפלגת הציונות הדתית

לפני הבחירות הוקמה רשת מתוכה זוהו כ־40 חשבונות טוויטר שקראו לפיצול במפלגת הציונות הדתית. החשבונות נפתחו ב־2.8.2022 ופרסמו תכנים מועתקים, כולל קריקטורות ובדיחות, והשתמשו בתמונות של גברים המועסקים לכאורה בחברת "רימקס". התכנים שפורסמו לא עוררו חשד, עד שיום לפני הגשת רשימות המפלגות לכנסת, ב־14 בספטמבר, החלו הפרופילים לפרסם קריקטורות בהן מופיע בן גביר וקריאה לפיצול במפלגת הציונות הדתית באמצעות ההאשטאג #רוץ_לבד_בבחירות. ב־18.10.2022 דיווחה FakeReporter על המבצע למערכת הביטחון ולטוויטר, ופרסמו את המידע על אודותיו לציבור הרחב בערוצים של הארגון וב"הארץ". ב־19 באוקטובר הוסרו החשבונות.

---

8 https://twitter.com/fakereporter/status/1489164051011846144

9 Tom Bateman, Iran accused of sowing Israel discontent with fake Jewish Facebook group, *BBC*, 3 February 2022. https://www.bbc.com/news/world-middle-east-60229146

10 דפנה ליאל, תחקיר: כך רשת אירנית מפיצה תכנים בישראל - במטרה ללבות את הוויכוח הפוליטי, *12N*, 29 בדצמבר 2021. https://www.mako.co.il/news-digital/2021_q4/Article-5496b9571470e71026.htm

יום הבחירות: מבצע לדיכוי הצבעה

מבצע נוסף פעל ביום הבחירות וכלל שני שלבים שמאחוריהם, על פי דפוסי הפעילות, עמד ככל הנראה אותו גורם. קבוצת החשבונות הראשונות במבצע הוסרה לפני יום הבחירות, וקבוצה נוספת נכנסה לפעילות ביום הבחירות. בשלב הראשון, פעלו מאות חשבונות טוויטר שנפתחו בחלון זמנים קצר ב־17.10 ולא פרסמו תכנים עד 28.10 - שלושה ימים לפני הבחירות. יומיים לפני הבחירות הם החלו בציוץ מתואם של אלפי ציוצים. הפרופילים התחזו לאזרחים ישראלים, בעיקר מתנגדי נתניהו, וקראו להחרמת הבחירות. ב־31.10 - יום לפני הבחירות - דיווחו FakeReporter על הרשת למערכת הביטחון ולרשת טוויטר. ביום הבחירות הפרופילים הוסרו ופורסמה כתבה בנושא בניו יורק טיימס שזכתה להתייחסויות בתקשורת הישראלית.

ביום הבחירות החל השלב השני במבצע שהיה בעל סממנים דומים, וכלל פרסום תכנים זהים לאלו שפורסמו בשלב הראשון. רשת זו פעלה גם בשפה הערבית וקידמה תכנים הקשורים לדיכוי הצבעה. כמה מאות חשבונות טוויטר נפתחו ב־22.10 ופעלו ביום הבחירות. ביום הבחירות דיווחו FakeReporter למערכת הביטחון ולטוויטר על החשבונות - ואלו הסירו אותם.

לאחר הבחירות: קמפיין הונאת בחירות

רשת חשבונות שפעלו בפייסבוק, טוויטר, אינסטגרם וטלגרם וטענו להונאת בחירות, לאי־קבלה של תוצאות הבחירות וכן קראו להתקהלות מחאה מול משרד ראש הממשלה ביום שאחרי הבחירות. ברשת פעלו כ־15 חשבונות ועקבו אחריהם יותר מאלף חשבונות פיקטיביים, ככל הנראה, כדי להגביר את האמינות של חשבון מרכזי במבצע. הרשת דווחה לגורמי הביטחון על ידי FakeReporter. מקבץ הרשתות שפעלו סביב יום הבחירות מעיד על העניין הרב שגילו גורמים מחוץ לישראל בהתערבות באירועים מרכזיים במדינה, ומעלה שאלות בנוגע למידת ההשפעה שלהם על תקינות הבחירות.

פרק שני:
מאפיינים משותפים של מבצעי ההתערבות שנחקרו

בחלק זה יוצגו דפוסי הפעולה ("מודוס אופרנדי") של הגורמים שמנהלים את מבצעי ההתערבות. אפשר להשתמש בהם לזיהוי של מבצעי התערבות עתידיים, והם מצביעים על מאפיינים המחייבים בחינה נוספת. עם זאת, חשוב לציין שקיים תהליך למידה ושינוי גם בקרב המפעילים של מבצעי ההתערבות לאורך זמן, וחלק מהמאפיינים צפויים להשתנות. אחד השינויים המרכזיים של השנה האחרונה, שמשפיע גם על האופן בו מתנהלים מבצעי ההשפעה, קשור להפיכתן של טכנולוגיות בתחום הבינה המלאכותית היוצרת (AI Generative) לנגישות וזמינות.

להלן רשימה של מאפיינים שזיהינו כשכיחים במבצעי ההתערבות במחקר:

מאפיינים הקשורים לתוכן:

- שמות משתמש: לרוב החשבונות הפיקטיביים שמשויכים למבצעי ההתערבות ניתנו שמות עבריים. שמות אלה נועדו לגרום לקהל הישראלי דובר העברית - קהל היעד של המבצעים שנבדקו - להאמין שמדובר בחשבונות אותנטיים של אנשים אמיתיים, ולא בחשבונות פיקטיביים שמאחוריהם עומדים גורמי התערבות זרה.
- תמונות פרופיל לחשבונות הפיקטיביים: תמונות פרופיל שבהן השתמשו במבצעי ההתערבות היו, בעיקרן, תמונות גנובות או תמונות שאי־אפשר לאתר את מקורן. בין היתר נעשה שימוש בתמונות שנגנבו ממאגרי תמונות סטוק, תמונות סלפי שקשה לזהות את המצולמות בהן, כי הפנים מוסתרות בטלפון, תמונות של שחקניות פורנו שעברו עיוותים כך שאי־אפשר לאתר את המקור שלהן וכו'.
- **תוכן הפוסטים:**

◄ החשבונות המשתייכים למבצעי ההתערבות נוטים להגיב בפוסטים שהם מפרסמים על אירועים אקטואליים המתרחשים בישראל. באופן זה הם מגבירים את האמינות שלהם כישראלים הבקיאים בהתרחשויות בארצם, עוסקים בנושאים שנמצאים במרכז השיח המקומי וזוכים לתשומת לב גדולה יותר.

◄ במקרים רבים התכנים שמפרסמים החשבונות הפיקטיביים הם גנובים, כלומר הועתקו מאנשים אמיתיים (בהם: עיתונאים, צייצנים בולטים, תכנים וירואליים, פרסומים של גופי חדשות וכו').

◄ עיסוק בנושאים מעוררי מחלוקת בחברה הישראלית: הגיוון בנושאים שבהם עוסקות הרשתות השונות מעיד שאין להן עניין לצדד בגורמים מסוימים במערכת הפוליטית או בחברה בישראל או לפעול נגדם, אלא לזהות סוגיות שיכולות להעמיק שסעים בחברה הישראלית וכאלה שמעוררות תגובות בעלות עוצמה חזקה ברשתות החברתיות.

- שפה עילגת ודקדוק לא תקני בתכנים המקוריים: לעיתים, הפוסטים המקוריים (כלומר כאלה שלא הועתקו ממקורות אחרים של דוברי עברית ברמה גבוהה) כתובים בעברית עילגת. הדבר יכול לנבוע מכך שהכותבים אינם דוברים את השפה כשפת אם, למדו אותה משמיעה או מכך שנעשה שימוש במנוע תרגום אוטומטי (דוגמת Translate Google) שגורם לשימוש לא מדויק ונכון בשפה. כמו כן, לעיתים בתכנים המקוריים בעברית נעשה שימוש במונחים לא נכונים (לדוגמה: "שומרי הגבול" במקום "משמר הגבול").

מאפיינים הקשורים לדפוס הפעילות של החשבונות במבצעים:

- החשבונות הפיקטיביים המשתייכים למבצעים פועלים במגוון פלטפורמות במקביל, למשל נפתחים חשבונות בעלי אותו שם או משתמשים בתמונות פרופיל שבהן נראה אותו אדם בו זמנית בטוויטר, פייסבוק, אינסטגרם וכולי. באופן זה גדלה האמינות של החשבונות המזויפים בעיני אלה שמעוניינים לבדוק את האותנטיות שלהם - ככל שהנוכחות האינטרנטית רחבה יותר ומושקעת יותר, כך יכול להתקבל הרושם שמדובר באדם אמיתי.

- מבצעי ההתערבות משתמשים במערכים הכוללים קבוצות, קהילות ועמודים שמקימים המפעילים שלהם. לעמודים ולקבוצות ניתנים שמות של התארגנויות המייצגות את המבצע (למשל - "אין מצב", Movements BB, אדוק וכו'). נוסף על כך הם בונים דמויות פיקטיביות שמקדמות את התכנים של הקבוצות והעמודים של ההתארגנויות או מפעילות אותם.

- ניכר כי ברוב המבצעים המערכים פועלים לאורך זמן ממושך. במהלך תקופת הפעילות, החשבונות המשתייכים לרשת מפרסמים באופן שיטתי תכנים ממגוון סוגים. כך נבנית בהדרגה האמינות של החשבונות השייכים לרשת.

- החשבונות הפיקטיביים המשתייכים למבצעים פועלים באופן מתואם ביניהם. למשל, הם מפרסמים פוסטים בזמנים קבועים (בשעות פעילות שנראות כמו עבודת משמרות).

- המשתמשים הפיקטיביים במערכים של מבצעי ההתערבות חברים בקבוצות פייסבוק פופולריות בעלות הקשר פוליטי ממגוון סוגים (למשל, בנימין נתניהו הקבוצה הרשמית, מהפך 2021 וכו') ומפרסמים בהם תכנים. כך הם מצליחים לייצר תהודה ולחשוף את התכנים שלהם לקהל אותנטי.

פרק שלישי:
גורמים המחשידים חשבונות ברשתות החברתיות וישויות דיגיטליות כהתנהגות מתואמת ולא אותנטית

רשימת המאפיינים הבאה יכולה להעיד על פעילות מתואמת שאינה אותנטית ברשת. לא מספיק שיופיע מאפיין אחד כדי לקבוע ברמת ודאות גבוהה שמדובר בהתנהגות לא אותנטית:

- שימוש בתמונות פרופיל גנובות, מזויפות או מבוססות בינה מלאכותית, שאי־אפשר לזהות את הדמויות המופיעות בהן וכו';
- פרסום תכנים מועתקים ממשתמשים אמיתיים (משפיענים, גופי תקשורת וכו');
- חזרתיות ושכפול אותן תגובות למשתמשים אחרים (פיקטיביים או אמיתיים) מספר פעמים;
- יחסי עוקב-נעקב בין חשבונות חשודים - דבר המאפשר לעיתים לזהות חשבונות פיקטיביים נוספים;
- שמות משתמש חשודים - למשל, כאלו שיש בהם רק שם פרטי (כולל חזרה מספר רב של פעמים על אותו שם בקבוצת חשבונות שנפתחים באותו מועד), או קבוצה של חשבונות עם שמות משתמש בעלי תבנית קבועה;

- חברות בעשרות קבוצות פייסבוק, חלקן הגדול בנושאים פוליטיים או נושאים שקשורים לעולמות התוכן של המבצע;
- פתיחת קבוצות (פייסבוק, וואטסאפ) וערוצים בטלגרם שנושאים את שם הפעילות ונועדו לקדם את התכנים של המבצע;
- פרסום תכנים בשעות פעילות קבועות (פירוט נוסף על סוגיית התזמון בפרק העוסק בניתוח הטכנולוגי).

גורמים המחשידים פעילות מתואמת לא אותנטית כהתערבות זרה:

רשימת המאפיינים להלן יכולה לסייע להבדיל בין פעילות מתואמת לא אותנטית שהיא מקומית לבין התערבות זרה. רבים מהסימנים הנכללים ברשימה זו קשורים לשימוש בשפה ובהבנת ההקשר התרבותי-חברתי, מאחר שבאופן זה אפשר להבחין בין גורם ישראלי לבין גורם זר. חשוב לציין שככל שמשתפרות טכנולוגיות הבינה המלאכותית, חלק מסימנים מחשידים אלו עשויים להיעלם. ביניהם אפשר לציין את המאפיינים האלה:

- טעויות בעברית בכתיבת תכנים מקוריים או בהתכתבות עם ישראלים;
- סימני שאלה הפוכים שיכולים להעיד על שימוש במקלדת בשפות הערבית או הפרסית;
- הדהוד תכנים ושיתוף בנושאים שנויים במחלוקת ולעיתים מסיתים;
- מערכים מושקעים הפועלים בכמה פלטפורמות לאורך זמן שמאחוריהם עומד ארגון משמעותי בעל משאבים ותשתיות לעריכת מבצע השפעה;
- אישור של הפלטפורמות (פייסבוק, טוויטר) שמדובר ברשתות שפועלות מחוץ לישראל. לרוב הפלטפורמות לא יציינו מהו המקור המדויק של הפעילות;
- פער זמנים בהשוואה לשעון ישראל (בצילומי מסך לדוגמה);
- שימוש במספרי טלפון מחוץ לישראל (למשל, של רשת Jawal הפלסטינית או אזורי חיוג אחרים שאינם 972) למשתמשי וואטסאפ.

גורמים המחשידים שמדובר בהתערבות זרה איראנית:

בחלק מהמקרים ישנן עדויות שמאפשרות לקבוע ברמת ודאות גבוהה מאוד שמדובר במבצע שבוצע על ידי גורם איראני:

- צילומי מסך שהתקבלו ממפעיל של מערך השפעה שמעידים על כך שהטלפון נמצא באזור הזמן של איראן או שנראה בהם ממשק טלפון בשפה הפרסית;
- ייעוץ בלשני (סמנטי) שקיבלנו בנוגע לטקסטים מקוריים (לא מועתקים ממשתמשים אחרים או גופי תקשורת) שמעיד על טעויות לשוניות בעברית האופייניות לדוברי פרסית;
- דיווחים של פייסבוק בדוחות התקופתיים שלהם שמאשרים שמצאו רשתות לא אותנטיות כחלק ממבצעי התערבות שפעלו בישראל.

על בסיס הגורמים המחשידים שהוזכרו **אפשר להעריך שאיראן עומדת מאחורי מרבית המבצעים שנבדקו במחקר** זה. לפי התכנים ואופי הפעילות של מבצעי ההתערבות נראה כי המטרה של המפעילים היא להגביר את הקיטוב הפנימי בישראל, ולכן הם בוחרים לעסוק בסוגיות שנויות במחלוקת ולעיתים להגביר ולהקצין מסרים (למשל, באמצעות השוואה של מנהיגים ישראלים להיטלר והכנסת מסרים אנטישמיים).

ההתמקדות בתכנים שקשורים לסוגיות פנים־ישראליות, כמו למשל תקופת בחירות או מחאה פוליטית, עשויה להצביע על רצון של מפעילי המבצעים להתערב בשיח הפנימי בישראל ולשבש או להשפיע על תהליכים דמוקרטיים.

נוסף על מטרות שקשורות למאמצי תודעה והשפעה על הלכי רוח, ישנם מאמצים ברורים בחלק מהמבצעים ליצור קשר ישיר עם

ישראלים. במבצעים שנחקרו היו אלה פעילים פוליטיים. בניגוד לצעדים שנועדו להשפיע על הלכי רוח בחברה, יצירת קשר ישיר עם אזרחים ישראלים יכולה להוביל לסוג אחר של התערבויות זרות הקשורים להפעלת אזרחים ישראלים על ידי גורם זר ועוין ללא ידיעתם.

פרק רביעי: התערבות זרה ברשתות החברתיות בישראל - מה למדנו?

נוסף על ערכו של מחקר זה כמחקר ראשון מסוגו הבוחן לעומק מבצעי התערבות זרה בישראל, אנו תופסים אותו גם כבעל ערך מתודולוגי לטובת ביצוע מחקרים דומים בעתיד, על האופן שבו נכון לנהל אותם והכלים והטכנולוגיות הנדרשים לשם כך.

תובנות הנוגעות למבצעי התערבות זרה ברשתות החברתיות:

- **התמקדות בנושאים מעוררי מחלוקות - התאמת התכנים ושינוים לנושאים מעוררי מחלוקת בכל תקופה:** הרשתות שנחקרו עוסקות במנעד רחב של נושאים שנמצאים בלב הציבוריות הישראלית. נראה כי מפעילי מבצעי ההתערבות הם בעלי היכרות אינטימית עם האירועים האקטואליים בישראל, ומתאימים את התכנים והנושאים של כל מבצע לנושאים שהם מזהים ככאלה שעשויים להיות שנויים במחלוקת. בין הנושאים שבהם עוסקות הרשתות: בעד/נגד ראשי ממשלה מכהנים, בחירות בישראל וכו'. התכנים המשותפים ברשתות גם משקפים בקיאות באקטואליה הישראלית - יוקר המחיה, קורונה וכו'.

- **השקעת משאבים בבניית מבצעי התערבות כסימן להתערבות מדינתית:** ניכר כי מושקעים מאמצים משמעותיים בבניית חשבונות שיש להם עומק, כלומר כאלה שמפרסמים תכנים רבים ובמשך זמן מה. באופן זה החשבונות הפיקטיביים צוברים אמינות, והקהילות והערוצים שהם מנהלים גדלים באופן אורגני על ידי אנשים שמצרפים את החברים שלהם. הדבר מעיד כי מאחורי המבצעים עומדים גוף או גופים מדינתיים, בעלי משאבים גדולים המושקעים בהתערבות בנעשה בישראל.

- **פעילות בשגרה לצד אירועים מיוחדים: מבצעי ההתערבות הזרה ברשתות החברתיות פועלים בשגרה וסביב אירועים מיוחדים:** כפי שעולה ממבצעי ההתערבות שחקרנו, המפעילים שלהם מזהים הזדמנויות בציבוריות הישראלית ועולמות תוכן להתמקד בהם. בתוך כך, המבצעים פועלים באופן שוטף, ללא תלות בהכרח באירוע שיא אקטואלי, אך ישנם מבצעים המתמקדים באירועים אקטואליים נקודתיים ופועלים סביבם (למשל, בחירות לכנסת).

- **מיעוט תגובות לצד למידה של הציבור הישראלי:** על אף המשאבים הרבים שהושקעו בהפעלת רוב מבצעי ההתערבות שנחקרו, נראה כי רובם לא הצליחו לייצר תהודה רבה ולעורר תגובות של משתמשים ישראלים. עם זאת, יש שני סוגים של תגובות שחשוב לשים לב אליהן ולמשמעויות שלהן: ראשית, משתמשים בישראל הפכו מודעים לכך שישנה ברשתות החברתיות נוכחות של גורמי השפעה עוינים, והם מתריעים על כך ומגיבים להם בהתאם. ואומנם, במהלך השנים שבהן דן המחקר, עלתה המודעות לתופעה, בין היתר הודות לפרסומים בכלי תקשורת מובילים בארץ ובעולם. המודעות לכך שגורמים זרים מעורבים בשיח שהוא לכאורה פנימי, עלולה ליצור תחושה של חוסר ביטחון, חוסר אמון וחדירות. עם זאת, ייתכן שהדברים לא זכו לתהודה רבה בקרב הציבור בישראל משום שהם משולבים בשיח שנאה פנימי וקשה להפריד בין התערבות זרה (המתחזה לשיח פנימי) לשיח פנימי אותנטי.

כמו כן, במבצעים מתוחכמים יותר, כמו חדירה לקבוצות וואטסאפ ויצירת קשרים אישיים באמצעותם, נוצרו מצבים שבהם אזרחים ישראלים קיבלו ושלחו חומרים לגורמים עוינים מבלי שידעו זאת. זהו כמובן סיכון לביטחון הלאומי של ישראל וניצול של אזרחים תמימים שאינם יודעים להבחין במשתמשים פיקטיביים ומייחסים אמינות לחשבונות, קבוצות וערוצים פיקטיביים. כמובן שהתמודדות הציבור תלויה גם ברמת האוריינות הדיגיטלית של הציבור וישנן אוכלוסיות שהן פגיעות יותר במובן זה.

אתגרים הכרוכים במחקר מבצעי התערבות ברשתות החברתיות

"תקרת זכוכית" של החברה האזרחית: קושי להוכיח זיקה לגורמים זרים ללא עזרת צד שלישי. מחקר זה ממחיש שללא עזרת גורמי צד שלישי - למשל סיוע של הפלטפורמות הטכנולוגיות עצמן או גורמים במערכת הביטחון - ארגוני חברה אזרחית מוגבלים ביכולת שלהם לקבוע באופן ודאי שחשבונות הם פיקטיביים ושמבצעי התערבות נעשים על ידי גורמים זרים. ארגוני חברה אזרחית יכולים לחשוד ברמת ודאות גבוהה שפעילות אינה אותנטית. אך ברוב המקרים שנבחנו - למעט אלו שבהם הייתה תקשורת ישירה עם מפעילי המבצע והתקבלו מהם סימנים מעידים על כך שהם איראנים - אי־אפשר היה לקבוע זאת באופן מוחלט.

"מחקר אנלוגי בעולם דיגיטלי": אחד הקשיים המרכזיים בביצוע המחקר היה שרובו הסתמך על ניתוח מידע שנאסף על ידי FakeReporter ונשמר ברובו בצילומי מסך סטטיים של חשבונות ותכנים. חלק גדול מהתכנים כבר הוסרו מהרשת בזמן ביצוע המחקר. הדבר הקשה על הוספת ממד אנליטי וסטטיסטי לניתוח, ביצוע ניתוחים סמנטיים ויכולת לחפש ולזהות דפוסים ברשתות השונות, והגביל את התובנות שיכולנו להסיק בתנאים הקיימים. כמו כן, בגלל שיטת איסוף המידע, הכיסוי של הרשתות היה חלקי ולא כלל את כל התכנים שפורסמו בחלק מהרשתות והמידע הנוגע אליהן באופן שוטף אלא צילומי מסך מקריים של חלק מהתכנים שפורסמו.

קושי בהערכת ההשפעה של מבצעי התערבות והסיכון שהם מהווים לביטחון ישראל

אתגר מרכזי הנלווה למחקר מבצעי התערבות זרה ברשתות החברתיות הוא הקושי לאמוד את ההשפעה שלהם על ביטחון ישראל, הדמוקרטיה הישראלית והחוסן הלאומי, בדומה לקושי במדידת מאמצים שיווקיים אחרים שנועדו להשפיע על דעת קהל וההשפעות שלהם אינן בהכרח מדידות. בחלק גדול מהרשתות שנבדקו במחקר זה התנהלו המבצעים לאורך תקופה ממושכת מבלי שנראה שהיו להם הישגים משמעותיים (כמו למשל, צבירת מספר גדול של עוקבים). אולם ברוב המקרים קשה להעריך באופן מדויק את מידת ההשפעה של מבצעים על הביטחון הלאומי בישראל, גם כשקיים פוטנציאל נזק מסוגים שונים. כך למשל, במהלך מחאת בלפור ב־2020 הקריא קצין משטרה בכיר בשידור טלוויזיה קריאה לאלימות נגד שוטרים שהתברר שהסתמכה על חשבון מזויף שהתחזה לאחד מארגוני המחאה[11] - דבר שעשוי לגרום להעמקת השסעים והמתיחות בחברה בישראל ושהשפיע על השיח הישראלי. כפועל יוצא מהקושי לאמוד את ההשפעה של מבצעי ההתערבות הזרה ברשתות החברתיות ואת הכוונות של הגורמים שעומדים מאחוריהן, לרוב קיים גם קושי לאמוד את הסכנות הפוטנציאליות הנובעות מהמבצעים.

פרק חמישי:
התמודדות עם מבצעי התערבות זרה ברשתות החברתיות בישראל

ההתמודדות עם איום ההתערבות הזרה ברשתות החברתיות מחייבת טיפול שיטתי ומערכתי בשיתוף של מגוון הגורמים הנוגעים לנושא - מערכת הביטחון, חברות הטכנולוגיה המפעילות את הפלטפורמות שבהן נערכים המבצעים, התאמת הרגולציה בישראל להתמודדות עם הבעיה, עירוב הציבור באמצעות התקשורת וארגוני חברה אזרחית לצורך זיהוי ראשוני של החשבונות החשודים.

היעדר טיפול מערכתי באיום מבצעי ההתערבות הזרה בישראל ברשתות החברתיות בישראל

המסקנה המרכזית העולה מן המחקר היא שכיום חסרה הסתכלות מערכתית לטיפול באתגר ההתערבות הזרה ברשתות החברתיות בישראל באופן מאורגן ושיטתי, מרגע הופעת האיום ועד הסרתו על ידי חברות המדיה החברתית. כלומר יש צורך במחקר שוטף, שיטתי ומתמשך מסוג המחקר שבוצע בנייר זה. נוסף על כך לשיטתנו חסרה הסתכלות רחבה משלב זיהוי הרשתות - בין היתר באמצעות שיתוף הציבור בישראל - המחקר שלהן ואמידת האיום שהן מהוות, חשיפת הרשתות לציבור באמצעות התקשורת ולבסוף הסרתן מהמרשתת.

קושי של מערכת הביטחון לפעול במרחב האזרחי הגלוי ברשתות החברתיות

מבצעי ההתערבות הזרה מתנהלים לרוב במרחב האזרחי הגלוי של הרשתות החברתיות המאפשר ערבוב של גורמים ישראליים וזרים, ומאתגר במהותו את מערכת הביטחון הישראלית בבואה לטפל בהם. האתגר איננו רק טכני, אלא נובע גם מהחשש לפגוע בחופש הביטוי של אזרחים ישראלים, ומכך שלעיתים אי־אפשר לקבוע בוודאות שמדובר בגורמים זרים. קרי: ייתכן שהגורמים שמנסים להשפיע על השיח הישראלי באמצעות התנהגות מתואמת לא אותנטית הם מקומיים. שילוב של גורמי חברה אזרחית עשוי לצמצם את הפגיעה ביסודות הדמוקרטיים משום שמי שמאתר את החשדות הם אזרחים ולא גורמי ביטחון. נוסף על כך גורמי מודיעין מעדיפים, באופן טבעי, לפעול באזורים החשאיים וזו סיבה נוספת שהם פחות פועלים באזורים הגלויים שברשת.

תפקיד הרשתות החברתיות בהתמודדות עם התערבות זרה

החברות המפעילות את הרשתות החברתיות - ובראשן טוויטר ו־Meta שבבעלותה פייסבוק, וואטסאפ ואינסטגרם - ממלאות תפקיד מכריע בהתמודדות עם מבצעי ההתערבות הזרים. ראשית, לחברות יש גישה למידע והן יכולות להשתמש בו כדי לזהות

11 המשטרה: הטענה שמפגינים קראו לאלימות הסתמכה על פייק ניוז | חדשות 13

ניסיונות לבצע מבצעי התערבות זרה וללמוד אותם לאורך זמן. נוסף על כך באפשרותן להסיר את החשבונות שהם חלק מהמבצעים. כיום היכולות הטכנולוגיות שלהן בתחום השפה גורמות לכך שסינון התכנים והזיהוי של תכנים שמפירים את חוקי הקהילה של Meta בשפה העברית אינם מספקים.

החקיקה הקיימת בישראל אינה מתאימה לטיפול במבצעי התערבות זרה ברשתות החברתיות משום שאינה מספקת מענה לצורך של האזרחים ליצור קשר ישיר עם הפלטפורמות, אין כתובת מדינתית ברורה לתלונות אזרחים על המתרחש ברשתות, אין איסור על מסחר במשתמשים פיקטיביים, אין חקיקה שמטילה חובה על הפלטפורמות לנטר ולהסיר חשבונות פיקטיביים ואין שיתוף פעולה בינלאומי מספק עם מדינות אחרות המתמודדות עם איומים ברשתות החברתיות בהקשר החקיקתי, חקירתי, דיפלומטי ומודיעיני.

עניין נוסף הוא היעדרו של ערוץ תקשורת ישיר המאפשר פנייה של אזרחים ישראלים לחברות הטכנולוגיה שבבעלותן נמצאות הרשתות החברתיות או לגורם אחר שיוכלו לדווח להם על חשד למבצעי התערבות זרה ועל הפצת דיסאינפורמציה ברשתות בכלל.[12]

דילמת החשיפה התקשורתית: הגברת המודעות בציבור או חיזוק הגורמים העוינים?

שאלה מרכזית העולה ממחקר זה נוגעת לחשיפת מבצעי התערבות זרה: האם לתת להם במה תקשורתית כשהם מתגלים, ואם כן - באיזה תזמון (לפני הסרת החשבונות מהרשת ומיצוי המידע שפורסם במבצע או אחרי)?. מצד אחד, אחת הגישות המרכזיות המקובלות בעולם להתמודדות עם דיסאינפורמציה ופוסט אמת היא באמצעות חינוך הציבור לאוריינות דיגיטלית.[13] מהבחינה הזו, חשיפת מבצעי התערבות זרה ברשתות החברתיות בישראל מסייעת לשיפור המודעות של הציבור ולהגברת החשדנות שלו כלפי חשבונות פיקטיביים או חשודים ככאלה. כלומר יש לחשיפה התקשורתית ערך בשיפור האוריינות הדיגיטלית בקרב הציבור הרחב ואפשר לרתום את הציבור לקחת חלק פעיל בזיהוי החשבונות החשודים.

עם זאת, חשוב להבין גם את מחיר החשיפה וההשלכות ארוכות הטווח שלה. ראשית, חשיפת הרשתות מחזקת את המפעילים שלהן ומעניקה להם תמריץ להמשיך להפעיל מבצעי התערבות מתוך הבנה שיש להם השפעה על הציבור הישראלי, שהם זוכים לתהודה ושהם משפיעים על סדר היום במדינה. נוסף על כך חשיפת הרשתות בתקשורת גורמת למפעילים שלהן לדעת שגורמים ישראליים גילו אותם, ואי־אפשר להמשיך במחקר של הרשת ואיסוף מידע נוסף על ההתפתחות שלה, המטרות וכו'. כמו כן, ברגע שהרשתות נחשפות, הן עלולות לשמש כלי לניגוח פוליטי ובאופן זה לשרת את המטרות של המפעילים שמאחורי המבצעים להעמיק את הפילוג והשיסוע בחברה הישראלית.

פרק שישי:
המלצות לפעולה, מדיניות וחקיקה

המלצות מערכתיות:

אחת המסקנות הבולטות היא שכיום אין אף גוף במערכת הישראלית שמבצע מחקר שיטתי ועקבי בנוגע לאיום ההתערבות הזרה ברשתות החברתיות בישראל. כתוצאה מכך, הטיפול בנושא נופל בין הכיסאות ותלוי בגופים שונים - במערכת הביטחון, בחברות הטכנולוגיה ובחברה האזרחית - שעוסקים בנושא באופן בלתי מתואם. הגם שהנושא הוא תחת אחריות שב"כ, ישנם גורמים לכך שאין לו מענה מיטבי.

ההמלצה שלנו היא להקים גוף שיעסוק במחקר רשתות השפעה באופן מעמיק ושוטף (ולא רק באופרציה שקשורה בהסרה שלהן בזמן אמת אלא גם בזיהוי דפוסי פעילות, מאפיינים, וכו'). לגוף זה צריכות להיות יכולות מחקריות מודיעיניות לצד יכולות טכנולוגיות ואנליטיות. גוף כזה יוכל לעבוד בסנכרון ובתיאום עם כלל השחקנים הרלוונטיים ולשקלל את כלל המשמעויות, כולל ההחלטה באילו מקרים אפשר לחשוף לציבור רשתות השפעה זרה, וכך יסדיר את מערכת היחסים שבין גופי המודיעין לארגוני החברה האזרחית.

12 ריבונות דיגיטלית: איך הממשלה החדשה צריכה להתמודד עם הפצת פייק ניוז ומבצעי השפעה (פרק פודקאסט), קול האמת, *המכון למחקרי ביטחון לאומי (INSS)*, 2021. https://www.inss.org.il/he/publication/truth1/

13 דוגמה להתמודדות עם מיסאינפורמציה בפינלנד באמצעות חינוך הציבור לאוריינות דיגיטלית - ראו:
Jenny Gross, How Finland Is Teaching a Generation to Spot Misinformation, The New York Times, 10 https://www.nytimes.com/2023/01/10/world/europe/finland-misinformation-classes.html

מחקר מערכתי של הנושא באופן שוטף יאפשר להגיע לתובנות עמוקות יותר על דפוסי הפעולה של היריב, לזהות טוב יותר ומהר יותר מבצעי התערבות ברשתות, לתת מענה למבצעי התערבות בחירום ובשגרה, לעקוב אחר הלמידה וההתפתחות של מבצעי ההתערבות ולצייד גם את הציבור בכלים להתמודדות איתם. אנו ממליצים לחזק את המחקר של השפעה והתערבות זרות ברשתות החברתיות הן במערכת הביטחונית הן בקרב גורמים אזרחיים כמו מכוני מחקר ועמותות.

בתוך כך, על קהילת המודיעין - בהובלת השב"כ - להרחיב את העיסוק באיום ההתערבות הזרה ברשתות החברתיות בישראל. הרחבה זו משמעה פעולה רציפה ולא רק בעת בחירות, כמו גם כניסה של גורמים נוספים מעבר לשב"כ להתמודדות עם איום זה.

מחקר זה עסק ברשתות שפעלו ברשתות החברתיות שבהן מפורסם תוכן בעברית בלבד. חשוב להמשיך לחקור וללמוד מבצעי התערבות שהיעד שלהם הוא אזרחים ישראלים דוברי שפות נוספות (ערבית, רוסית, אמהרית וכו').

חשוב להרחיב את המחקר לפלטפורמות נוספות שבהן נעשה שימוש במבצעי התערבות, כגון TikTok ו־Linkedin שלא נבדקו כלל במחקר זה. לאורך זמן יש להרחיב את המעקב לרשתות חברתיות חדשות שיצמחו. כמו כן, יש לעקוב אחרי שימוש בטכנולוגיות חדשות שבהן משתמשים המפעילים של מבצעי ההתערבות, דוגמת שימוש בטכנולוגיות AI Generative.

המלצות הקשורות למשרדי ממשלה

מול גורמי הממשלה יש להגביר את המודעות לאיום ההתערבות וההשפעה הזרה בתהליכים דמוקרטיים בכלל, וברשתות החברתיות בפרט, כאיום משמעותי חדש על החוסן והביטחון הלאומי. לשם כך יש ליצור מודעות לאיום, להגדיר בעלי תפקידים במשרדי ממשלה רלוונטיים האמונים על הטיפול בבעיה (משרד המודיעין, משרד המשפטים), גורמי אכיפה (משטרה) והרשויות הרלוונטיות (ועדת הבחירות המרכזית, מערך הסייבר הלאומי, מל"ל, מערך הדיגיטל הלאומי). נוסף על כך יש להנגיש לציבור אפשרות להתלונן על חשד להתערבות זרה או שאינה אותנטית ברשתות. הגברת המודעות של גורמי הממשלה תוכל להביא לקידום הרגולציה הנדרשת על הרשתות החברתיות.

המלצות הקשורות לרגולציה בישראל

יש צורך בחקיקה שתחייב את פלטפורמות הרשתות החברתיות הגדולות ליצור ערוץ תקשורת ישיר עבור תושבות ותושבי ישראל לצורך דיווח על תלונות ובירורים הקשורים בתוכן ויצירת כתובת מדינתית ברורה לתלונות על המתרחש ברשתות. בנוסף, יש להוביל חקיקה שתאסור מסחר במשתמשים פיקטיביים ושתעניק כלים לרשויות המדינה לפעול כנגד המפעילים של החשבונות הפיקטיביים; חקיקה אשר תטיל חובה על הפלטפורמות לנטר ולהסיר חשבונות פיקטיביים; קיום שיתופי פעולה עם מדינות זרות בהתמודדות עם הסיכונים הנוצרים ברשתות חברתיות, בהקשר החקיקתי, החקירתי, הדיפלומטי והמודיעיני. במסגרת זו יש לפקח ולהגביל את הארכיטקטורה של הפלטפורמות על המנוע האלגוריתמי והמודל העסקי שלהן, בתוך שמירה על חופש הביטוי של משתמשי הקצה. לבסוף, יש צורך בעדכון חקיקת הפרטיות בישראל.

המלצות הנוגעות לרשתות החברתיות

ראשית, יש לדרוש מחברות הטכנולוגיה להשקיע בהקצאת משאבים וטכנולוגיות המותאמים לשפות המדוברות בישראל (ובראשן עברית וערבית). המלצות רלוונטיות אפשר לגזור גם מהמסקנות של הדוח החיצוני שפרסמה פייסבוק בעקבות מבצע "שומר החומות". יש גם לדרוש מהפלטפורמות להקצות צוותי ניטור ומחקר מקומיים ולהפעיל בודקי עובדות המבינים את השפה והתרבות בישראל. יש לוודא שהשירות מותאם לפניות של הציבור הישראלי מבחינת שעות הפעילות (אזור זמן) ושיש זמינות לפניות של משתמשים, גופים אזרחיים וגופים מדינתיים בפרק זמן מספק ולפני שאירועים ברשתות יוצאים משליטה.

"הוועדה להתאמת המשפט לאתגרי החדשנות והאצת הטכנולוגיה" (ועדת דוידי) שפעלה מטעם משרד המשפטים בממשלה ה־36, קראה להקמת גוף להסדרת הפעילות במרחב הדיגיטלי.[14] כיום הפנייה לפלטפורמות מטעם המדינה נעשית על ידי מחלקת הסייבר במשרד המשפטים. 94% מהפניות למחלקת הסייבר להסיר מידע מהרשתות החברתיות בשנת 2020 נעשו על ידי גופים ביטחוניים

14 רני נויבאור, רעות אופק ואביחי כהנא, סיכום עבודת הועדה להתאמת המשפט לאתגרי החדשנות והאצת הטכנולוגיה, בנושא טכנים לא חוקיים במרחב הדיגיטלי. *משרד המשפטים הישראלי*, אוקטובר 2022. https://www.gov.il/BlobFolder/guide/davidi-committee-main/he/committee-summary.pdf

שהגישו מעל 4,000 פניות. בפסק דין עדאלה נגד פרקליטות המדינה-מחלקת הסייבר קבע בג"צ כי "פעילות מחלקת הסייבר במתכונת הקיימת היא חיונית לשמירה מיידית על הביטחון הלאומי ועל הסדר החברתי, אך אין היא חפה מקשיים, הנוגעים בעיקר לבעיית ההסמכה בחקיקה ראשית פרטנית לפעולות המחלקה". משרד המשפטים לא הוסמך בחקיקה לפעול מול הפלטפורמות החברתיות ולכן ההמלצה של בג"צ בפסיקה הייתה להסדיר את ההסמכה בחקיקה.

בו בזמן פעלה בכנסת ה־36 ועדה במשרד התקשורת לבחינת האסדרה על פלטפורמות תוכן דיגיטליות.[15] אחת מהצעות הוועדה, שאומצו בדצמבר 2022 על ידי שר התקשורת הקודם,[16] הייתה הקמת מועצה ציבורית שמטרתה להגביר את הפיקוח על הרשתות החברתיות. לפי ההצעה, החברים במועצה ייבחרו על ידי הממשלה ועל ידי ראשי ארגוני חברה אזרחית. מועצה כזו תוכל לסייע גם ביצירת כתובת לתלונות הציבור באשר לחשד להתערבות זרה וכן בגיבוש מדיניות בנושא.[17]

כלל האצבע שאנו מציעים הוא לקבוע הסרה מהרשתות החברתיות של כל פעילות מתואמת שאינה אותנטית החשודה כזרה, ללא תלות במידת ההשפעה שלה, המסרים שפורסמו בה או מעשים שבוצעו בעקבות פעילותה. חשוב להגיע להבנה עם חברות הטכנולוגיה שישתפו מידע בנוגע למבצעי התערבות זרה שהן מזהות ברשתות החברתיות שהיעד שלהן הוא ישראל, כדי להעמיק את המחקר וההבנה בנוגע לפעילות היריב בשקיפות מרבית.

המלצות הקשורות לחברה האזרחית

מחקר זה ממחיש את חשיבות מכוני המחקר וארגוני החברה האזרחית בהתמודדות עם תופעת ההתערבות הזרה ברשתות החברתיות בישראל. לאלה יש אפשרות לזהות כשמתעורר חשד למעורבות זרה ברשתות החברתיות, להגביר את המודעות של הציבור לתופעה, ולקדם מחקר של התופעה (כולל למידה מ־Best Practices הנהוגות במדינות אחרות). עם זאת, המחקר גם ממחיש את מגבלות יכולות החברה האזרחית להתמודד עם הבעיה ואת הצורך לשתף פעולה עם גורמים מדינתיים ועם חברות הטכנולוגיה המפעילות את הפלטפורמות כדי לתת מענה מלא לבעיה. לכן, במתן מענה מערכתי יש לשלב ארגוני חברה אזרחית, משפיעני רשת, חברות טכנולוגיה וגורמים אחרים שיפעלו בשיתוף פעולה ובתיאום עם יתר הגופים הרלוונטיים.

המלצות הנוגעות לציבור בישראל

שיפור האוריינות הדיגיטלית של הציבור קריטי כדי שאזרחי ישראל ילמדו לזהות חשבונות פיקטיביים שפועלים בסביבה הדיגיטלית שלהם ומנסים להטעות אותם במסגרת מבצעי התערבות. יש להטיל את האחריות על גוף שיעסוק בנושא בשגרה ולא רק סביב אירועים כמו בחירות לכנסת או מלחמה. אחת האפשרויות היא להטמיע את הנושא בתוכנית הלימודים תחת משרד החינוך ולמנות את מערך הדיגיטל הלאומי להיות אחראי על קידום האוריינות הדיגיטלית בקרב האוכלוסייה הבוגרת.

נוסף על כך יש ליזום שיתופי פעולה עם גורמים רלוונטיים סביב אירועים אקטואליים שעלולים לשמש כר פורה למבצעי התערבות זרה, למשל, פיקוד העורף בתקופת מבצעים צבאיים, ועדת הבחירות המרכזית סביב מערכות בחירות וכו'. הסוגיה המרכזית היא למנות גוף שיהיה אחראי לנושא בזמן שגרה ויקבל תקציבים למאמצי הסברה וחינוך של הציבור. המועצה הציבורית שהוזכרה קודם לכן, ושהיו בה נציגי ציבור, יכולה להיות הבסיס לגוף כזה. עוד גופים שיכולים להיות רלוונטיים לנושא הם מערך הסייבר הלאומי, משרד המודיעין, ארגוני חברה אזרחית, ומכוני מחקר שיכולים לאפיין את התופעה ולפתח דרכים להתמודדות עימה.

כאשר יוקם ערוץ תקשורת בין הציבור לחברות הטכנולוגיה שמפעילות את הרשתות החברתיות, ותוקם כתובת מדינתית ברורה שהציבור יוכל לדווח בה על תקריות ביטחוניות ברשתות החברתיות - חשוב יהיה להביא לידיעת הציבור את קיומם ולעודד אותם להשתמש בהם. כך יוכל הציבור להתלונן גם על ניסיונות ליצירת אינטראקציה על ידי גורמים זרים.

---

15 דו"ח המלצות הוועדה, הצוות המייעץ לבחינת האסדרה על פלטפורמות לתוכן דיגיטליות, *משרד התקשורת הישראלי*, 14 בדצמבר 2022. /https://www.gov.il/he pages/14122022 ; https://www.gov.il/BlobFolder/reports/14122022/he/Report-digital-platforms.pdf

16 דוח הצוות המייעץ לשר התקשורת לבחינת האסדרה על פלטפורמות תוכן דיגיטליות - ר' הערה 15.

17 תמיר הימן, דוד סימן טוב ועמוס הרביץ. "פיקוח על הרשתות החברתיות בישראל - הביצד", מבט על, גיליון 1679, *המכון למחקרי ביטחון לאומי (INSS)*, 4 בינואר 2023 https://www.inss.org.il/he/publication/social-media/.

המלצות הנוגעות לתקשורת המסורתית

תקשורת ההמונים המסורתית - ערוצי הטלוויזיה, אתרי החדשות, הרדיו והעיתונים - ממלאה תפקיד ציבורי בהגברת המודעות של הציבור למבצעי התערבות זרה ברשתות החברתיות. לכן חשוב לחשוף חלק מהמבצעים כחלק ממאמצי שיפור האוריינות הדיגיטלית של הציבור. עם זאת, קיימת סכנה שחשיפה תקשורתית תדרבן את הגורמים שמפעילים את מבצעי ההתערבות ותעודד אותם להמשיך לנסות להתערב בשיח ברשתות בישראל. בשקלול הטיעונים השונים, המסקנה שאליה הגענו היא שככלל ראוי לפרסם את ניסיונות ההתערבות, וכי השיקול של יצירת מודעות של הציבור (כחלק ממעטה ההגנה ויצירת חוסן) עולה בחשיבותו על הניסיון שלא לתת הד לפעילות חתרנית זרה. עם זאת, במקרים שבהם נשקפת סכנה לביטחון הלאומי או שאפשר להעמיק את המחקר ולהגיע לתובנות משמעותיות מהמשך מעקב אחרי הצעדים של הרשת - יש לשקול דחייה של הפרסום על אודות קיומה. לשם כך ראוי לשקול הקמת פורום התייעצות ביטחוני-אזרחי.

נוסף על כך ראוי להגביר את המודעות גם של העיתונאים המתמחים בנושאי סיקור מדיניים, ביטחוניים וכולי באמצעי התקשורת השונים בנוגע לקיומם של מבצעי התערבות ברשתות, ובכלל בנוגע לדיסאינפורמציה ברשתות כדי להעמיק את הבנתם והשפעתם על הדמוקרטיה הישראלית, עקב הזליגה של אירועים מהרשת גם לתקשורת המסורתית.

המלצות שקשורות למחקרים עתידיים

כדי להבין את תמונת המצב העדכנית ואת הגישות העדכניות ביותר לביצוע מבצעי התערבות זרה ברשתות החברתיות, יש צורך במחקר שוטף ושיטתי שיאפשר לזהות את דפוסי הלמידה של היריב. כלומר, לראות כיצד המבצעים משתנים ומתפתחים לאורך זמן. יש לבדוק כיצד המבצעים משתנים, והאם אפשר להצביע מה גורם לשינוי במבצעים (האם הגורם לשינוי הוא מהלכים של ישראל, צעדים שנוקטות הרשתות החברתיות עצמן וכו'). השינויים במבצעים יכולים לנבוע מהתפתחויות טכנולוגיות, למשל, הפיכת טכנולוגיות בינה מלאכותית יוצרת לזמינות ונגישות, באופן שיאתגר חלק מהתובנות שהוצגו במחקר זה (למשל, זיהוי מבצעי השפעה זרים על בסיס אלמנטים הקשורים בשפה, צמצום הצורך בגניבת תמונות משום שניתן לייצר תמונות שנראות אמינות לחשבונות פיקטיביים ועוד). בשנת 2022 יותר משני שלישים מהרשתות המתואמות הלא אותנטיות שנמצאו ב-Meta השתמשו בחשבונות שהיו בהם תמונות שנוצרו באמצעות טכנולוגית GAN, ובחברה מעריכים שהמפעילים שלהם חושבים שתמונות אלה גורמות לחשבונות להראות יותר אותנטיים ומקוריים וכך להטעות גורמים שחוקרים מבצעי השפעה ומתבססים על מידע גלוי. כך שמדובר באתגר משמעותי שישפיע על הקושי לזהות מבצעי השפעה ולחקור אותם.

השינויים במבצעים יכולים לנבוע גם מצמיחתן של פלטפורמות חברתיות חדשות או הגדלת השימוש בהן, כמו לדוגמה טלגרם או טיקטוק. גם האופן שבו פועלים החשבונות הפיקטיביים במבצעי ההשפעה השתנה, ובמבצעים שהוצגו במחקר ניכר מעבר למבצעים קטנים וממוקדים יותר מבחינת כמות החשבונות הפועלים בהם בהשוואה למבצעים גדולים ורועשים יותר בעבר.

מחקר שיטתי ועקבי מסוג זה של מבצעי ההשפעה צריך להתבסס על מקורות מידע מגוונים, כולל הקמת מערך עיסוק מידע וניתוח ממוכן, לצד איסוף ומעקב אחר מידע הנאסף ומפורסם על ידי גופי מחקר וחברה אזרחית בארץ ובעולם. עבודת הזיהוי, ההתראה והמחקר צריכה להיות משימה משולבת של אנליסטים מיומנים, ושל כלים טכנולוגיים המספקים יכולת להתמודד עם כמויות המידע הגדולות ולשמר את המידע בצורה יעילה. בנוסף על כך, צריכה להיות להם היכולת להתריע בדחיפה על אירועים בעלי משמעות ברשת.

מבין כלל האתגרים בתחום (התראה, זיהוי דמויות פיקטיביות ותגובה), קיים קושי מיוחד בייחוס החשבונות לארגונים ולאנשים העומדים מאחוריהם וכן הפללה או הוכחה וודאית ולא רק משוערת של קשר "קונספירטיבי" ביניהם. הקושי הזה נובע באופן מובנה מההגנה על פרטיות המשתמשים אותה מספקות הרשתות החברתיות. ההגנה הזו כוללת מיסוך (הסתרה) של נתוני זיהוי ופרטים נוספים על המשתמשים. כחלק מכך לא ניתן לגלות כתובות IP, כתובות דוא"ל, מיקומים גיאוגרפיים ומספרי טלפון של חשבונות בכלל, ובפרט של אלו אשר מהם מתבצעת פעילות לא אותנטית. לעומת זאת נראה שהפוטנציאל בשימוש בכלים אוטומטיים להתראה, קישור ומעקב אחר מבצעי התערבות עשוי להיות אפקטיבי ביותר.

התחומים שאנו ממליצים לשים עליהם דגש בהקשר הטכנולוגי:

1. השקעה במאגר מידע עקבי מתעדכן לאורך זמן - שכבת יסוד לכל "מפעל התגוננות" צריכה להיות יכולת "קצירה" ו"אגירה" של מידע מהרשתות הרלוונטיות לאורך זמן. איומי ההשפעה מבוזרים על מגוון פלטפורמות גדול (TikTok, וואטסאפ, טלגרם, פייסבוק, טוויטר, אינסטגרם, Redit ועוד). עבור כל אחד מהשירותים הללו יש צורך בשיטות "קצירה" שונות של המידע ונדרש לאסוף אותו לאורך זמן על מנת ליישם סטטיסטיקות ולבצע הפללה בדיעבד של חשבונות זדוניים.

2. השקעה בכלים מבוססי מטא-דאטה לזיהוי פעילות החשודה כמתואמת ולא טבעית ברשת.

3. השקעה בכלי עיבוד סמנטי ועיבוד מבוסס תוכן כדי לאתר באופן אוטומטי מסרים "מתסיסים", להפליל טעויות כתיב של מנסחים בשפות מקור זרות (דורש מחקר) וזיהוי תוכן שמיוצר על ידי אלגוריתמי deepfake כחלק מהתמודדות עם האתגר הגובר שתואר בתחום ה-AI Generative.