המערכה החשאית של מִבצעי השפעה בסייבר וכיצד לזהותם

דוד טיורי

הרשתות החברתיות הן דרך יעילה להשפיע על החברה וההתנהגות האנושית ולעצב דעת קהל. מבצעי השפעה בסייבר פירושם שימוש בכלי סייבר ושיטות סייבר כדי לתמרן את דעת הקהל. מדינות רבות משתמשות כיום במרחב הסייבר, ובמיוחד ברשתות החברתיות, כדי לנהל מבצעי השפעה כחלק מלוחמת מידע כוללת. מרבית הפעולות הללו נעשות באופן מוסווה, ולכן עצם הזיהוי שלהן מהווה אתגר. יתר על כן, לא פשוט להבדיל בין פעולות השפעה לגיטימיות ובין פעולות זדוניות. מאמר זה מתאר מִבצעי השפעה בסייבר, את פוטנציאל הנזק שלהם וכיצד הם מתנהלים. כמו כן, הוא מנתח את האתגרים הניצבים בפני זיהוי מִבצעי השפעה בסייבר ומפרט כמה פרמטרים אינדיקטיביים לזיהוי כזה.

מילות מפתח: השפעה בסייבר, מבצע השפעה, רשת חברתית, הנדסה חברתית, לוחמת סייבר

מבוא

העידן הדיגיטלי שינה את האופן שבו אנו מתקשרים. שיחות ומערכות יחסים בין אנשים מתקיימות כיום ברשת ובאמצעות תקשורת דיגיטלית. רשתות חברתיות, כמו "פייסבוק" ו־"אינסטגרם", ואפליקציות חברתיות כמו "ווטסאפ" ו־"טלגרם", מאפשרות לנו לשמור על קשר עם חברים ומשפחה, לשתף פוסטים, מסרונים, תמונות וסרטונים, לחלוק את החוויות שלנו זה עם זה, להתעדכן בסטטוס החברים שלנו ולקרוא פוסטים שהם כותבים.

רשתות חברתיות שנמצאות בשימוש נרחב על ידי רבים בכל רחבי העולם הן גם דרך יעילה להשפיע על החברה וההתנהגות האנושית ולעצב את דעת הקהל.

דוד טיורי הוא סגן ראש מינהל להנדסה במינהל סייבר לאומי ותעופה, מפעל הסייבר, אלתא מערכות בע"מ, התעשייה האווירית לישראל. המחבר מבקש להודות למר אהרון (רוני) אילת ולמר מארק אלינס, שעברו על מאמר זה ותרמו את הארותיהם.

על ידי שיתוף פוסט, ציוץ דעה, השתתפות בדיון בפורום או שיתוף תמונה בעלת ערך רגשי או פוליטי, אנו יכולים להשפיע על דעות של אחרים ואולי אף לשכנע אותם. דמיינו שהייתם יכולים לקחת חלק במאות ואלפי שיחות דיגיטליות; במצב כזה היה לכם סיכוי להשפיע על קהילות גדולות.

שימוש בכלים ובשיטות של סייבר כדי לתמרן את דעת הקהל נקרא "מבצע השפעה בסייבר" ("Cyber Influence Operation"). יכולות להיות מטרות שונות למבצעים מסוג זה: השפעה פסיכולוגית, פגיעה במורל ובמוּדעות הציבור, ערעור תחושת השליטה והיכולת להגן על שגרת החיים, ועוד. פעולות כאלו עלולות לגרום לנזק (פסיכולוגי), ולכן הן מכונות גם "מתקפות סייבר להפצת דיסאינפורמציה".

מדינות רבות משתמשות כיום במרחב הסייבר, ובמיוחד ברשתות החברתיות, כדי להוציא לפועל מְבצעי השפעה כחלק מלוחמת מידע כוללת. מרבית המבצעים הללו נעשים בצורה חשאית, כך שבמקרים שהמבצע נחשף קשה להוכיח מי עומד מאחוריו. מבצעי השפעה יכולים להיות מיועדים לקהל הרחב ואז לכלול אמירות כלליות, או להיות מופנים לקהל יעד ספציפי ואז לכלול מסרים ממוקדים שישיגו השפעה אפקטיבית יותר ושליטה בתוצאות. דוגמה לתוצאה כזו יכולה להיות הצבעה למועמד או למפלגה ספציפיים בבחירות, כפי שניתן היה לראות בבחירות לנשיאות ארצות הברית בשנת 2016.

זיהוי מבצעי השפעה בסייבר מהווה אתגר. לא קל לזהות השפעה, ובמיוחד קשה להבחין בין פעולת השפעה לגיטימית לזדונית. קידום מוצר או רעיון תמים הוא דבר לגיטימי, אפילו כפעולת השפעה. הסתה, קידום מעשים רדיקליים או אלימים, או התערבות בבחירות דמוקרטיות הם דוגמאות לשימוש זדוני בפעולות השפעה. חשוב שממשלות, באמצעות ארגוני ביטחון וגופי אכיפת החוק שלהן, יצליחו לזהות מבצעי השפעה זדוניים, כדי שניתן יהיה למנוע אותם או לפחות לצמצם את נזקיהם. נכון להיום, אין דרך שיטתית לזהות מבצעי השפעה בסייבר או להבדיל בין פעולות השפעה לגיטימיות לזדוניות.

בפרקים הבאים יתאר המאמר מהם מבצעי השפעה בסייבר ומה היכולת שלהם להסב נזק, כיצד מתנהלים מבצעי השפעה בסייבר ואילו טקטיקות הם מנצלים. המאמר גם ינתח את האתגרים בזיהוי מבצעי השפעה בסייבר ויפרט כמה פרמטרים אינדיקטיביים העוזרים בזיהוי. בחלק האחרון שלו יציג המאמר מקרי בוחן של מְבצעי השפעה בסייבר.

מבצעי השפעה בסייבר

מבצע השפעה בסייבר מוגדר כ־"מאמצים ממוקדים להכיר ולערב קהלים חשובים באמצעות תכניות, נושאים, מסרים ומוצרים המתואמים ביניהם, במטרה ליצור,

לחזק ולשמר תנאים הנוחים לקידום מדיניות, מטרות ואינטרסים מסוימים".[1] במילים אחרות, מבצעי השפעה בסייבר מייצרים מסרים ואינטראקציות במטרה להביא קהלי יעד לשנות את דעתם ו/או התנהגותם. אם המטרה היא שליטה בתגובות של חברי הקבוצה, הדבר נקרא "ניהול תפיסה" ("Perception Management").

תיאוריה דומה ל"ניהול תפיסה", שנחקרה בעיקר ברוסיה, נקראת "שליטה רפלקסיבית" ("Reflexive Control").[2] "שליטה רפלקסיבית" מוגדרת כדרך להעביר לשותף או ליריב מידע שהוכן במיוחד כדי להביא אותו לקבל החלטה שיוזם הפעולה מעוניין בה. "רפלקס" מתייחס לתהליך של חיקוי היגיון היריב, או התנהגות אפשרית שלו, באופן שיגרום לו להחליט אחרת מִשרצה תחילה. ניתן ליישם "שליטה רפלקסיבית" על תהליכי קבלת החלטות של מדינה דרך השפעה על משאבי המידע שלה. הדרך הטובה ביותר להשיג מטרה זו היא לייצר מידע מסוים, או מידע שגוי, כך שישפיע על משאב מידע ספציפי. הצלחה בהשגת "שליטה רפלקסיבית" על היריב תאפשר להשפיע על תכניותיו, על עמדתו לגבי סיטואציה מסוימת, או על האופן שבו יילחם. במילים אחרות, הצד המשפיע יצליח להשליט את רצונו על הצד השני ולגרום לו לקבל החלטה שאינה הולמת מצב נתון.

מונח הקרוב במשמעותו להשפעה בסייבר ולקוח מההקשר הצבאי הוא "תמרון משפיע" ("Influencing Maneuver"). בתהליך זה נעשה שימוש בפעולות סייבר כדי לחדור למעגל ההחלטות של האויב, ואולי אף לאלץ את מעגל ההחלטות לבצע פעולות ישירות או עקיפות. מדובר בצורת תמרון רחבה, שנועדה להשיג ולשמר עליונות ודומיננטיות במידע ולשמור על חופש התמרון במרחב הסייבר.[3] "תמרון משפיע" יכול לשמש לפעולות ישירות או עקיפות. דוגמה להשפעה ישירה של התמרון הן פעולות כמו פגיעה במערכות פיקוד ושליטה או מניפולציה סמויה בנתונים, שיספיקו כדי לערער את הביטחון שיש למפקד במערכות ויאטו את מעגלי ההחלטות. פעולות עקיפות יכללו הזנת התקשורת בנתונים לקויים ושגויים כדי לאלץ תגובה רצויה מסוימת אצל היריב. מאמר זה מתמקד בפעולות עקיפות.

מבצעי השפעה הופכים בהדרגה למקור דאגה מרכזי בכל העולם. הם מופיעים תחת שמות וביטויים שונים – חדשות כוזבות (Fake News), דיסאינפורמציה, קמפיין פוליטי שבו המשתתפים מתחזים לאזרחים רגילים (Political Astroturfing),

1 Eric V. Larson and others, *Understanding Commanders' Information Needs for Influence Operations* (Santa Monica: Rand Corporation, 2009).

2 Timothy L. Thomas, "Russia's Reflexive Control Theory and the Military", *Journal of Slavic Military Studies* 17, no. 2 (2004): 237-256.

3 Scott D. Applegate, "The Principle of Maneuver in Cyber Operations", *2012 4th International Conference on Cyber Conflict (CYCON 2012)*, (Tallinn: NATO CCD COE Publications, 2012), https://www.ccdcoe.org/publications/2012proceedings/3_3_Applegate_ThePrincipleOfManeuverInCyberOperations.pdf

מתקפות מידע וכדומה. מבצעי השפעה יכולים להיות חלק מלוחמה היברידית ולהשתלב במתקפות סייבר מסורתיות (כמו שימוש בתוכנה זדונית), בפעולה צבאית קונבנציונלית או במתקפות קינטיות חשאיות.[4]

למבצע השפעה יכולות להיות מטרות שונות והשפעות/נזקים פוטנציאליים שונים. בעיתות שלום, מטרת מבצעי השפעה יכולה להיות קידום רעיונות רצויים או הכוונת אוכלוסיות לכיוון הרצוי, כמו למשל מפלגה פוליטית המנהלת קמפיין לשכנע את בוחריה להצביע לה. אולם, אם אותה פעולה תתבצע על ידי מדינה זרה, הדבר ייחשב, כמובן, כהתערבות חיצונית בענייניה הפנימיים של מדינה ריבונית. התערבות זרה עלולה לפגוע באמון שיש לאזרחים בממשלתם, שכן הם לא יוכלו להיות בטוחים שאותה ממשלה היתה נבחרת לולא ההתערבות הזרה.

בתקופות של סכסוך או מלחמה, מטרת מבצעי ההשפעה יכולה להיות יצירת שיח נגד הממשלה, הסתת דעת הקהל נגד פעולות הממשלה (למשל, נגד המלחמה), פגיעה במורל הציבורי (למשל, לעורר תחושת חוסר ביטחון בפעולות הממשלה), וכן הלאה. כל זאת, כדי ליצור תחושה שלממשלה אין שליטה או יכולת להגן על שגרת החיים, וכך להביא להחלשת צבאה של המדינה בשדה הקרב.

מבצעי השפעה יכולים להתמקד בציבור הרחב או לפנות לקהל ספציפי בעזרת מאגרי נתונים מקוונים או רשתות חברתיות. מבצעי השפעה המכוונים לקהל הרחב יכללו אמירות כלליות שצפויה להן השפעה מזערית בלבד על יחידים ברמת המיקרו, אך עדיין הן ישיגו את האפקט הרצוי ברמת המאקרו. מבצעי השפעה המכוונים לקהלים ספציפיים ישתמשו באמירות המותאמות במיוחד לקהלים אלה כדי להיות יעילות יותר.

כיצד מתנהלים מבצעי השפעה בסייבר

השלב הראשון בניהול מבצע השפעה אפקטיבי בסייבר הוא הגדרת המטרה והגישה להשגתה. הגישה יכולה להיות בקמפיין חיובי – קידום נושא מסוים, חיזוקו ושיפור דעת הקהל לגביו – או בקמפיין שלילי – תקיפת מתנגדים, החלשת יריבים ויצירת דעת קהל שלילית. השלב השני הוא זיהוי קהל היעד: הציבור הרחב, קבוצות ממוקדות או קבוצה קטנה של משפיענים; קבוצות קיצוניות או כאלו שבקונצנזוס; המגדר, הגיל, הגזע, הדת וכדומה שישרתו את המטרה בצורה הטובה ביותר. השלב השלישי הוא בחירת הרשתות והפורומים החברתיים שבהם תתבצע פעולת ההשפעה וקביעת האינטראקציה בין המדיה שנבחרה ובין גורמים

4 "Army Researchers Join International Team to Understand, Defeat 'Disinformation' Cyberattacks", *ARL Public Affairs*, December 5, 2017, https://www.army.mil/article/197316/army_researchers_join_international_team_to_understand_defeat_disinformation_cyberattacks.

מתווכים אחרים. השלב הרביעי הוא קביעת הכלים להפצת המסרים: פרופילים מזויפים, בוטים או טרולים. לפרופילים מזויפים יש אולי מוניטין טוב יותר יחסית לשאר הכלים, אך הם יזדקקו למעורבות אנושית. בוטים ניתן לתכנת כדי להגיב אוטומטית לתוכן מוגדר, אך קל יותר לזהות אותם כבוטים. טרולים משמשים להעברת תכנים שליליים אגרסיביים, לרוב כאשר המטרה היא לתקוף יריבים. השלב האחרון בניהול מבצעי השפעה הוא הגדרת המסרים המתאימים ופרסום אינטנסיבי שלהם, בהתאם למטרה ולקהל שהוגדרו. תרשים 1 מתאר את השלבים בהוצאה לפועל של מבצע השפעה בסייבר.

תרשים 1. השלבים בהוצאה לפועל של מבצעי השפעה בסייבר

תעמולה היתה מאז ומתמיד דרך נפוצה להשפיע על אנשים. התעמולה המודרנית יעילה מאוד, מכיוון שהיא מסתמכת על מדיה דיגיטלית וחברתית. היא יכולה להגיע בקלות לאנשים רבים או לקבוצות נבחרות, ולהשתמש במספר רב של פוסטים כדי להשיג את מטרתה. מבצעי השפעה בסייבר יכולים להשתמש בטכניקות כמו תעמולה כדי להשפיע בצורה מוצלחת על אנשים.[5] דוגמאות לכך הן:

- **גירוי רגשות עזים**, כמו פחד, תקווה, כעס, תסכול ואהדה, כדי לכוון את הקהל אל המטרה הרצויה. זהו משחק מוחות שבו מפעיל ההשפעה המיומן יודע לנצל את הפחדים והדעות הקדומות של אנשים, להתאים פסיכולוגית את המסרים לרגשות, וכך ליצור תחושה של התרגשות ועוררות, המדכאת חשיבה ביקורתית ומתסיסה רגשות.
- **פישוט מידע ורעיונות** על ידי שימוש במידע שחלקו מדויק ואמיתי וחלקו חצאי אמיתות, דעות, שקרים והטעיות. מבצע השפעה מוצלח יספר סיפורים פשוטים

5 "Recognizing Propaganda", *Mind Over Media*, https://propaganda.mediaeducationlab.com/techniques.

שנשמעים מוכרים ואמינים, לרוב תוך שימוש במטפורות, דימויים וחזרות, כדי לגרום להם להיראות טבעיים או "אמיתיים". פישוט יתר הוא אמצעי יעיל: ביטויים קצרים, קליטים וזכירים מחליפים חשיבה ביקורתית. פישוט יתר של מידע אינו תורם לידע או להבנה, אולם מכיוון שבני אדם נוטים מטבעם לצמצום מורכבויות, טכניקה כזו של פעולת השפעה יכולה להיות אפקטיבית.

- **מתן מענה לצרכים ולערכים של קהל היעד** באמצעות העברת מסרים, נושאים ושפה הפונים ישירות, והרבה פעמים גם באופן בלעדי, לקבוצות ספציפיות ומובחנות בתוך האוכלוסייה. מפעיל השפעת סייבר עשוי לפנות לאנשים דרך תחושת הזהות הגזעית או האתנית שלהם, התחביבים, ידועים האהובים עליהם, האמונות והערכים, או אפילו השאיפות והתקוות האישיות לעתיד. משימה זו הופכת לקלה ויעילה יותר כאשר עושים שימוש בפרופילים שונים ברשתות החברתיות, מכיוון שניתן להתאים כל פרופיל לקהל היעד וכך להשיג תוצאה מיטבית. לפעמים הפניה תהיה לערכים האנושיים הבסיסיים ביותר, כמו הצורך לאהוב ולהיות נאהב, לחוש תחושת שייכות ותחושת מקום. מסרים הפונים ישירות לצרכים, לתקוות ולפחדים של קבוצות ספציפיות הופכים את פעולת ההשפעה לאישית ורלוונטית. כאשר המסר רלוונטי באופן אישי, אנשים שמים לב אליו וסופגים דרכו מידע ורעיונות מרכזיים.
- **תקיפת יריבים** כסוג של לוחמה פוליטית וחברתית שנועדה לזהות ולהשמיץ את המתנגדים. ניתן להטיל ספק בלגיטימיות, באמינות, ברמת הדיוק ואפילו באופי של יריבים וברעיונותיהם. מכיוון שאנשים נמשכים מטבעם לעימותים, פעולת השפעה יכולה לעשות שימוש אסטרטגי במחלוקות כדי לזכות בתשומת לב. תקיפת יריבים גם מעודדת חשיבה מסוג "או–או" או "אנחנו והם", המדכאת חשיבה על מידע ורעיונות מורכבים יותר. מבצעי השפעה יכולים לשמש גם כדי להכפיש אנשים, להרוס את המוניטין שלהם, להחריג קבוצות אוכלוסייה ספציפיות, להסית לשנאה או לעודד אדישות.

האתגרים הניצבים בפני זיהוי מבצע השפעה בסייבר

כדי לזהות מבצעי השפעה בסייבר, עלינו לזהות תחילה השפעה חברתית או השפעה בסייבר. לכן, אחד האתגרים הבסיסיים הוא להגדיר מהי השפעה חברתית וכיצד למדוד אותה ברשת. השפעה חברתית מוגדרת כ־"שכנוע אחרים, במודע או שלא במודע, במחשבות, באמונות ובמעשים שלך".[6] כשבאים להגדיר השפעה חברתית, משתמשים בשלוש קטגוריות: **שחקנים**, **אינטראקציות** ו**רשתות**.

6 D.M. Kahan, "Social Influence, Social Meaning and Deterrence", *Virginia Law Review* 83, no. 2 (1997): 349-395.

מפעילי סייבר יעדיפו במקרים רבים לפנות למשפיענים, כדי להגיע לקהל הגדול ביותר האפשרי. ישנם אינדיקטורים שונים כדי לדעת מהו הפוטנציאל של **שחקן משפיע** (משפיען): בעל מוח יצירתי, קובע טרנדים, בעל נוכחות והשפעה חברתית, פעיל ברשתות החברתיות, כריזמטי, בעל מומחיות, בעל סמכות, בעל מספר עוקבים/חברים גדול ועוד. לשחקן יש השפעה ברשת אם המסרים שלו או שלה משותפים גם מחוץ לאותה רשת; אם המסר משותף על ידי אחרים באותה רשת; אם לשחקן יש מספר גדול של אנשי קשר; אם השחקן גורם לכך שעוד אנשים יקראו את המסר; אם המהירות שבה המסר מופץ ברשת היא גבוהה.

את **האינטראקציה המשפיעה** ניתן למדוד בעזרת אינדיקטורים שונים. חוקרים הולנדים גילו שהשפעת האינטראקציה תלויה במידה רבה במספר השיתופים שקיבל המסר; בסוג התגובות שהמסר מעורר; במספר הפעמים שהמסר צוטט; במספר הקוראים/המאזינים שהמסר הגיע אליהם; האם המסר הביא לכניסת מספר רב של מבקרים ייחודיים.[7]

בין האתרים הנפוצים והמשפיעים ביותר על אינטראקציות במרחב הסייבר ניתן לציין אתרי בלוגים ברשת. להלן קריטריונים לבדיקת השפעה בהקשר של בלוגים ברשת:[8]

- **דירוג המרכזיות ברשת** – מודד את המוניטין של האדם: האם הוא או היא אישיות מרכזית ברשת או בעלת מספר מוגבל בלבד של אנשי קשר?
- **דירוג היפר־קישוריות** – מודד את מספר הקישורים לבלוג כקריטריון השפעה.
- **דירוג התנועה באתר** – מודד את מספר המבקרים באתר האינטרנט.
- **דירוג הפעילות בקהילה** – מתייחס למספר התגובות שהבלוג מעורר.

מחקרים נוספים קישרו אינדיקטורים ל**רשת חברתית (אישית) משפיעה**. אלה כוללים את המרחק החברתי בין שני שחקנים, מידת ההדדיות, כמות הקשרים השונים בין שני שחקנים ברשת (multiplexity), גודל הרשת, צפיפות הרשת, קישוריות, מרכזיות, ערך רגשי, לכידות קבוצתית ואשכולות (האם ניתן לחלק את הרשת לקבוצות קוהרנטיות). אינדיקטורים מוגדרים אלה יכולים לשמש לאיתור שחקנים, אינטראקציות ורשתות של בעלי השפעה, שבתורם יעזרו לנו לזהות טוב יותר השפעה חברתית. תרשים 2 מסכם את האינדיקטורים להשפעה חברתית.

---

7 Wouter Vollenbroek, Sjoerd de Vries, Efthymios Constantinides and Piet Kommers, "Identification of Influence in Social Media Communities", *International Journal of Web Based Communities* 10, no. 3 (2014): 280-297.

8 Dave Karpf, "Measuring Influence in the Political Blogosphere: Who's Winning and How Can We Tell?", *Politics and Technology Review* (2008): 33-41, http://www.the4dgroup.com/BAI/articles/PoliTechArticle.pdf.

שחקן משפיע	אינטראקציה משפיעה	רשת חברתית משפיעה
מוחות יצירתיים (Active Minds)	מספר הפעמים שמסר שותף	המרחק החברתי בין שני שחקנים
קובעי טרנדים		הדדיות
נוכחות והשפעה חברתית	מספר התגובות שמסר עורר	גודל הרשת
פעילות חברתית	מספר הפעמים שמסר צוטט	צפיפות הרשת
כריזמה		קישוריות
מומחיות	מספר הקוראים/מאזינים שמסרים הגיעו אליהם	מרכזיות
סמכות	אם מסר עורר מספר גדול של מבקרים ייחודיים	ערך רגשי
מספר החברים		לכידות קבוצתית

תרשים 2. אינדיקטורים להשפעה חברתית

לאחר שמזהים השפעה חברתית, האתגר הבא הוא להבחין בין פעולות השפעה לגיטימיות ובין כאלו שהן זדוניות. לעיתים הלגיטימיות של פעולת ההשפעה היא בעיני המתבונן. רוב האנשים יסכימו כי הסתה וקידום מעשים קיצוניים או אלימים מהווים פעולות השפעה זדוניות, וכי קידום רעיון תמים הוא בדרך כלל בגדר חופש דיבור לגיטימי. אבל מה לגבי אמירות או רעיונות פוליטיים שיוצאים נגד הנהגת המדינה? הדבר תלוי בערכי המדינה ובמשטר שלה. הבה נניח שמדובר במשטר דמוקרטי, שבו אדם יכול לבקר כל דבר וכל איש, לרבות את מנהיג המדינה. גם אז, אם הדבר נעשה על ידי צבא בוטים שתוכנתו להפיץ באופן אוטומטי אמירות נגד מפלגת השלטון, לגיטימיות ההצהרות אינה ודאית, במיוחד לאור העובדה שהשימוש בבוטים אסור על ידי מרבית המדינות. אם צבא בוטים כזה היה מנוהל על ידי שחקן זר, זה היה נחשב, ככל הנראה, התערבות זרה בדמוקרטיה של מדינה ריבונית.

כדי להשיג השפעה אפקטיבית, נעשה לא פעם שימוש בידיעות כוזבות. כך, למשל, ערב הסעודית ואיחוד האמירויות פעלו כדי להסית את דעת הקהל האמריקאית ומדינות ערביות אחרות נגד קטר, וזאת באמצעות קמפיינים באינטרנט וברשתות חברתיות שהאשימו את קטר בתמיכה בטרור ובערעור היציבות באזור. קטר דחתה האשמה זו, שבסופו של דבר התבררה כלא נכונה. עם זאת, תוצאת הקמפיינים

של ערב הסעודית ואיחוד האמירויות היתה שמדינות ערביות ניתקו את היחסים הדיפלומטיים שלהן עם קטר במהלך יוני 2017.[9]

ניתן להסכים כי השימוש בחדשות כוזבות אינו לגיטימי ומעיד על השפעה זדונית, אך האתגר האמיתי הוא עצם הזיהוי שלהן. לרוב, חדשות כוזבות מתפרסמות לצד ידיעות אותנטיות, וכך הן מקשות על זיהוין ככאלו. גם זיהוי תמונות מזויפות מהווה אתגר, לאור שפע הכלים המתקדמים הזמינים כיום לעריכת תמונות. המצב מסתבך עוד יותר כאשר פוסט מסוים עשוי לכלול גם עובדות נכונות, גם ידיעות כוזבות וגם דעות, שבאופן טבעי הן סובייקטיביות ומותאמות לערכים ולאמונות שבהם מחזיק הכותב. פוסט כזה יזכה ברשתות החברתיות לתגובות שישקפו את דעותיהם ונקודות המבט של המגיבים, וכך יגבר עוד יותר הקושי לזהות את האלמנטים השקריים.

אתגר נוסף בזיהוי מְבצעי השפעה בסייבר הוא הצורך לעשות זאת כמעט בזמן אמת. החדשות ברשתות החברתיות מתפשטות במהירות, ולעיתים קורה שעד שעובדה מתגלה כשקרית, הנזק כבר נעשה ופעולת ההשפעה מתקדמת לעבר מטרתה. כך, למשל, הפצת חדשות כוזבות או כוזבות למחצה על מועמד ימים ספורים לפני הבחירות, עשויה לשנות את התוצאות.

לאחר שזיהינו מבצע השפעה בסייבר, בדרך כלל נרצה לדעת מי עומד מאחוריו ולאסוף הוכחות לכך. הקושי במקרה זה נובע מכך שהאנשים או הארגון שמאחורי מבצעי ההשפעה מסווים את עקבותיהם. הם מסתירים את זהותם האמיתית באמצעות שימוש בבוטים ובפרופילים מזויפים ברשתות החברתיות ועל ידי הסתרת פרטי התקשורת שלהם (כמו ה־IP) בעזרת דפדפנים ייעודיים לגלישה אנונימית או שרתי פרוֹקְסי.

פרמטרים לזיהוי מְבצעי השפעה בסייבר

כדי לזהות מבצעי השפעה בסייבר, יש לנטר ולנתח את התכנים המתפרסמים ברשתות החברתיות השונות – טקסטים, תמונות וסרטוני וידאו – באמצעות חקר ביצועים ואלגוריתמים מתקדמים ותוך שקלול פרמטרים רבים של תוכן ותקשורת. להלן פרמטרים אינדיקטיביים שעוזרים לזהות מבצע השפעה בסייבר:

- **שימוש באווטארים, בוטים וטרולים**. פעולת השפעה טובה תסתיר את מפעיליה כדי להגיע לתוצאות היעילות ביותר. ישנן מספר דרכים להגיע לאנונימיות של פעולת ההשפעה. שניים מהכלים הנפוצים ביותר הם אווטארים ובוטים. אווטארים הם זהויות וירטואליות ברשתות החברתיות שמסתירות את זהותו

9 Josh Wood, "How a Diplomatic Crisis among Gulf Nations Led to a Fake News Campaign in the United States", *PRI*, July 24, 2018, https://www.pri.org/stories/2018-07-24/how-diplomatic-crisis-among-gulf-nations-led-fake-news-campaign-united-states.

האמיתית של המפעיל. בוטים הם סוכנים קטנים שמתוכנתים להגיב אוטומטית לפוסטים ספציפיים או לפרסם פוסטים אוטומטיים כדי לקדם את הרעיון/המוצר שאליו תוכנתו. יש טקטיקות רבות לזיהוי בוטים. חוקרים מצאו מספר תכונות המאפשרות לזהות בוט, כמו למשל חשבון פעיל ללא הפסקה, נפח גבוה של שיתוף ציוצים, תגובות לתוכן המכיל מילות מפתח מסוימות, שימוש בתמונות פרופיל גנובות, שם פרופיל מומצא, פערים משמעותיים בפעילות בחשבון, ועוד.[10]

- **פרסום פוסטים וחדשות שמקורם בגורמים מחוץ למדינה**. כאשר אנשים מנסים לשכנע אנשים אחרים ולקדם את רעיונותיהם או אמונותיהם, הדבר מהווה פעולה לגיטימית, כל עוד הם עושים זאת בתוך מדינתם או פועלים ממדינה אחרת ללא הסתרת זהותם. אבל אם איש ממדינה אחרת מתחזה לאזרח מקומי, זוהי פעילות חשודה המחייבת בדיקה. דוגמה טובה לכך תהיה ניסיון להשפיע על תוצאות הבחירות במדינה אחרת. ראוי לציין שלא פשוט לגלות את המקור האמיתי לתוכן שפורסם. מפעילים יכולים להשתמש בשרת VPS (שרת וירטואלי פרטי) הממוקם במדינת היעד, וכך להסוות את המיקום האמיתי של המעורבים. הם גם יכולים להשתמש בחשבונות דוא"ל הממוקמים במדינת היעד ומקושרים לזהויות מזויפות או גנובות, כדרך לגבות את הזהויות המקוונות. זהויות כאלו יכולות לשמש גם להלבנת תשלומים דרך חשבונות PayPal ומטבעות דיגיטליים.
- **פרסום ידיעות כוזבות**. זוהי אחת השיטות היעילות ביותר להשפעה על דעת הקהל, כפי שניתן היה לראות במקרים של הבחירות בארצות הברית ובצרפת. חוקרים מאוניברסיטת סטנפורד גילו כי 62 אחוזים מהאמריקאים הבוגרים צורכים את החדשות שלהם דרך רשתות חברתיות, כי סיפורי החדשות הכוזבות הפופולריים ביותר זכו לשיתוף רב ב־"פייסבוק", וכי מספר גבוה של אנשים שנחשפו לחדשות כוזבות דיווחו כי הם מאמינים להן.[11] פירוש הדבר הוא שהפצת חדשות כוזבות ברשתות חברתיות היא טקטיקה טובה למבצעי השפעה, ולכן אינדיקטור טוב לזיהוי שלהם.
- **פרסום מספר רב של פוסטים בנושא ספציפי**. כדי להגיע לכמה שיותר אנשים וכדי להגדיל את ההשפעה, יש צורך לפרסם מספר רב של פוסטים בנושא שבו רוצים להשפיע. לדוגמה, אם מדינה מסוימת מתכננת פעולה צבאית נגד מדינה אחרת, המדינה המותקפת יכולה לפרסם מספר רב של פוסטים וציוצים נגד

10 Bill Fitzgerald and Kris Shaffer, "Spot a Bot: Identifying Automation and Disinformation on Social Media", *Data for Democracy*, June 5, 2017, https://medium.com/data-for-democracy/spot-a-bot-identifying-automation-and-disinformation-on-social-media-2966ad93a203.

11 Hunt Allcott and Matthew Gentzkow, "Social Media and Fake News in the 2016 Election", *Journal of Economic Perspectives* 31, no. 2 (Spring 2017): 211-236, https://web.stanford.edu/~gentzkow/research/fakenews.pdf.

הפעולה, שיתייחסו לנזקים האפשריים לכלכלה, יפריזו במספר הנפגעים, יתמקדו בפגיעה בזכויות האדם, וכדומה.

- **שינוי פתאומי בדעת הקהל**. כאשר מסתכלים על קבוצות ספציפיות בפורומים וברשתות חברתיות ומגלים שינויים שהתרחשו בדעת הקהל בתוך פרקי זמן קצרים, הדבר יכול לרמוז על התערבות זרה, מכיוון ששינויים בדעת הקהל נוטים מִטְבעם להיות הדרגתיים. לדוגמה, אם מועמד מוביל בתקופת בחירות מאבד לפתע את ההובלה בתוך יום או יומיים, יש בכך אינדיקציה להתערבות חיצונית אפשרית.
- **פרסום ביטויים שליליים קיצוניים**. יש נטייה להשתמש בביטויים שליליים, במיוחד בקבוצות או בפורומים רלוונטיים, כדרך להשיג שינוי מהיר ויעיל בדעת הקהל. לכן, ביטויים כאלה עשויים להצביע על קיומה של פעולת הסתה. לדוגמה, אם קבוצה פוליטית מושמצת על ידי הטלת ספק בלגיטימיות ובאמינות שלה, תוך שימוש בביטויים שליליים במיוחד, הדבר צריך להדליק נורה אדומה.

תרשים 3 מתאר את הפרמטרים האינדיקטיביים לזיהוי מבצעי השפעה בסייבר. פרמטר בודד אינו מספיק כדי להצביע על מבצע השפעה, אך שילוב של מספר פרמטרים יכול ללמד על קיומו של מבצע כזה. ניתן גם לבצע אוטומציה של התהליך בעזרת אלגוריתם שישלב את כל האינדיקטורים, אם כי אלה עשויים להשתנות בהתאם למצב. נכון יהיה להקנות לפרמטרים האינדיקטיביים משקל שונה בהתאם להֶקשר שלהם.

תרשים 3. פרמטרים אינדיקטיביים לזיהוי מבצעי השפעה בסייבר

מקרה בוחן: התערבות רוסיה בבחירות לנשיאות ארצות הברית ב־2016

בשנים האחרונות נחשפו מקרים רבים של מבצעי השפעה בסייבר, אך אין ספק שאחד הידועים שבהם הוא ההתערבות הרוסית בבחירות לנשיאות ארצות הברית בשנת 2016. ניתוח המקרה מעלה כי כמעט כל הפרמטרים שהוזכרו לעיל רלוונטיים לזיהוי ההשפעה הרוסית באותן בחירות:

- **רוסים המפרסמים פוסטים בארצות הברית**: ב־7 באוקטובר 2016 יצאו משרד מנהל המודיעין הלאומי (ODNI) והמשרד לביטחון המולדת (DHS) של ארצות הברית בהצהרה משותפת, לפיה קהילת המודיעין האמריקאית קובעת בביטחון כי ממשלת רוסיה הורתה על פריצה לשרתי הדוא"ל של המפלגה הדמוקרטית האמריקאית במטרה להתערב בתהליך הבחירות בארצות הברית.[12] שני דוחות שהוגשו לוועדת המודיעין של הסנאט האמריקאי על ידי חוקרים עצמאיים חשפו כי בין השנים 2013 ל־2017 הצליחו גורמי מודיעין רוסיים להגיע למיליוני משתמשים ברשתות החברתיות בארצות הברית.[13]
- **שימוש באווטארים וטרולים**: על פי דוח של מנהל המודיעין הלאומי של ארצות הברית, הקמפיין הרוסי היה רב־ממדים וכלל מדיה במימון ממשלת רוסיה, תעמולה גלויה ומשתמשים וטרולים בתשלום ברשתות החברתיות.[14] דוחות מראים כי הטרולים השתמשו באתרי אינטרנט רבים להפצת הנרטיבים שלהם,[15] וגורמים רשמיים ב־"פייסבוק" מסרו כי מאז יוני 2015 נוצרו 470 חשבונות מזויפים, אשר שימשו במהלך מערכת הבחירות האמריקאית ב־2016 חברה רוסית בשם Internet Research Agency (IRA). חברה זו ידועה בכך שהיא משתמשת בחשבונות טרולים כדי לפרסם פוסטים ברשתות החברתיות ותגובות (טוקבקים) באתרי חדשות.[16]

---

12 "Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security", *Department of Homeland Security*, October 7, 2016, https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.

13 Alex Ward, "4 Main Takeaways from New Reports on Russia's 2016 Election Interference", *Vox*, December 17, 2018, https://www.vox.com/world/2018/12/17/18144523/russia-senate-report-african-american-ira-clinton-instagram.

14 "Assessing Russian Activities and Intentions in Recent US Elections", *Office of the Director of National Intelligence*, January 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

15 "Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security".

16 Scott Shane and Vindu Goel, "Fake Russian Facebook Accounts Bought $100,000 in Political Ads", *The New York Times*, September 6, 2017, https://www.nytimes.com/2017/09/06/technology/facebook-russian-political-ads.html.

- **ידיעות כוזבות**: בינואר 2017 העיד מנהל המודיעין הלאומי של ארצות הברית כי רוסיה התערבה בבחירות 2016 גם באמצעות הפצה וקידום של חדשות כוזבות ברשתות החברתיות.[17] חברת IRA כיוונה משתמשים שמרנים אל כמעט 110 פוסטים ב־"פייסבוק", לרבות תמונות מזויפות המראות הודעות על שגיאה במכונות ההצבעה או בפתקי ההצבעה, והציגה להם מידע כוזב על הונאת בחירות רחבה, שלכאורה נועדה לסייע למועמדת הילרי קלינטון לנצֵח.[18]
- **פרסום ידיעות רבות על המועמדים**: אחד מסיפורי הידיעות הכוזבות על הילרי קלינטון שותף 800,000 פעמים.[19] ב־"אינסטגרם" נרשמו כ־187 מיליון מעורבויות של כעשרים מיליון משתמשים בתכנים של חברת IRA שהיו קשורים לבחירות, וב־"פייסבוק" נרשמו 76.5 מיליון מעורבויות של כ־126 מיליון איש.[20]
- **ריבוי ביטויים שליליים על המועמדים**: על פי משרד מנהל המודיעין הלאומי של ארצות הברית, רוסיה העלתה את הסיכויים של דונלד טראמפ להיבחר לנשיא על ידי פגיעה באמינותה של הילרי קלינטון ויצירת תדמית ציבורית שלילית שלה.[21] כאשר נראה היה למוסקבה שקלינטון עשויה לזכות בנשיאות, קמפיין ההשפעה הרוסי החל להתמקד בערעור הלגיטימיות שלה ובכרסום סיכוייה להגיע לנשיאות, כולל הטלת חשדות בטוהר הבחירות. על פי "הפרויקט לחקר תעמולה ממוחשבת" ("Computational Propaganda Research Project"), חברת IRA הרוסית הפעילה טקטיקות רבות כדי לעצב דעת קהל בארצות הברית, ועשתה זאת על ידי הפצת מידע שגוי בפלטפורמות הרשתות החברתיות, ניצול פלטפורמות אלו לצורך מבצעי השפעה מבחוץ והעצמת דברי שטנה ותוכן פוגעני באמצעות חשבונות מזויפים או בוטים פוליטיים.[22]

---

17 Ellen Nakashima, Karoun Demirjian and Philip Rucker, "Top US Intelligence Official: Russia Meddled in Election by Hacking, Spreading of Propaganda", *The Washington Post,* January 5, 2017, https://www.washingtonpost.com/world/national-security/top-us-cyber-officials-russia-poses-a-major-threat-to-the-countrys-infrastructure-and-networks/2017/01/05/36a60b42-d34c-11e6-9cb0-54ab630851e8_story.html.

18 "Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security".

19 Nakashima, Demirjian and Rucker, "Top US Intelligence Official: Russia Meddled in Election by Hacking, Spreading of Propaganda".

20 Ward, "4 Main Takeaways from New Reports on Russia's 2016 Election Interference".

21 Ibid.

22 Philip N. Howard, Bharath Ganesh and Dimitra Liotsiou, "The IRA, Social Media and Political Polarization in the United States, 2012-2018", *Computational Propaganda Research Project*, *2018*, https://int.nyt.com/data/documenthelper/534-oxford-russia-internet-research-agency/c6588b4a7b940c551c38/optimized/full.pdf.

מקרי בוחן נוספים

כאמור, בחירות 2016 בארצות הברית לא היו המבצע הידוע הראשון או האחרון של השפעה בסייבר. להלן כמה מבצעי השפעה נוספים:

- במאי 2014 שיגרו האקרים פרו רוסיים סדרה של מתקפות סייבר במשך מספר ימים במטרה לשבש את הבחירות לנשיאות אוקראינה. מתקפות אלו כללו פריצה לדוא"ל ופרסום תוכנו, ניסיון לשנות הצבעות ועיכוב בפרסום התוצאות הסופיות באמצעות מתקפות מניעת שירות.[23]
- בדצמבר 2016 טען חבר הפרלמנט הבריטי בן ברדשאו כי רוסיה התערבה בקמפיין שנערך לקראת משאל העם על ה־"ברקזיט" (יציאת בריטניה מהאיחוד האירופי).[24]
- במהלך הבחירות לנשיאות צרפת ב־2017, חשבונות אוטומטיים שיתפו בחדשות כוזבות על הבחירות, שחלק גדול מהן הגיע ממקורות שנחשפו להשפעה רוסית.[25] ההשפעה הרוסית חדרה לשיח הפוליטי בצרפת דרך תכנים הנוגעים לסוגיות בין־לאומיות. התכנים היו מכוונים לערער מקורות תקשורת מסורתיים, להפחית בחשיבותם של נושאים שהועלו נגד הפעילות הרוסית, ובאופן כללי להסיט את המוקד והאשמה לעֵבר שחקנים אחרים. התכנים גם נועדו לרכך את הביקורת על רוסיה ולקדם תמיכה בעמדותיה הפוליטיות, ובעקיפין לקדם לנשיאות מועמדים הדוגלים באותן עמדות.

מִבצעי השפעה בסייבר יכולים לזהם גם את המרחב המסחרי. חברת "נייקי" מצאה עצמה תחת מתקפה דיגיטלית (קמפיין מבצעי מתואם) לאחר שיצאה בספטמבר 2018 בקמפיין הפרסומי עם קולין קפרניק.[26] היעדים של מתקפת הסייבר על חברת "נייקי" כללו פגיעה במכירותיה ובשווי המניה שלה. ניתן היה לזהות את המבצע בעזרת הפרמטרים האינדיקטיביים הבאים:

- **שימוש באווטארים ובבוטים**: קבוצות מסוימות קידמו חרם נגד חברת "נייקי" בכך שארגנו "תיבות תהודה" אשר נועדו לגייס ציוצים או לייצר תעבורה ממוחשבת

23 Mark Clayton, "Ukraine Election Narrowly Avoided 'Wanton Destruction' from Hackers", *Christian Science Monitor*, June 17, 2014, https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers.

24 Joe Watts, "Labour MP Claims It's Highly Probable Russia Interfered with Brexit Referendum", *Independent*, December 13, 2016, https://www.independent.co.uk/news/uk/politics/russian-interference-brexit-highly-probable-referendum-hacking-putin-a7472706.html.

25 Pierre Haski, "Patterns of Disinformation in the 2017 French Presidential Election", *Bakamo*, 2017, https://www.bakamosocial.com/frenchelection/.

26 Jay Solomon and Aftan Snyder, "Lessons for Brands from the anti-Nike-Kaepernick Social Effort", *PRNEWS*, February 22, 2019, https://www.prnewsonline.com/social+media-Nike-Kaepernick-APCO-bots-Twitter.

(בניגוד לתעבורה אנושית) באמצעות בוטים. בדיקת המשתמשים הפעילים העלתה כי 426 מתוך 668 המשתמשים שתקפו את "נייקי" ונדגמו היו אווטארים.

- **פרסום מספר רב של פוסטים נגד "נייקי"**: אחד הקמפיינים המתואמים כלל 300 משתמשים והפיק 2,133 ציוצים ושיתופים בתוך פרק זמן קצר.
- **שימוש במספר רב של ביטויים שליליים**: המשתמשים פרסמו לפחות עשרה ציוצים שליליים או מילות מפתח חוזרות במהלך הקמפיין.
- **שינוי פתאומי בדעת הקהל**: שווי המניה של "נייקי" נפל ב־3.2 אחוזים יום לאחר שהקמפיין החל לפעול.

מסקנות

הרשתות החברתיות, הנמצאות בשימוש רחב של אנשים רבים בכל רחבי העולם, הן גם דרך יעילה להשפיע על התנהגות חברתית ולעצב דעת קהל. מבצעי השפעה בסייבר עושים שימוש בכלים ובשיטות של סייבר כדי לתמרן את דעת הקהל. מדינות רבות משתמשות כיום במרחב הסייבר, ובמיוחד ברשתות החברתיות, כדי להוציא לפועל מבצעי השפעה בסייבר, כחלק מלוחמת מידע כוללת שמתנהלת ברובה באופן חשאי. מבצע השפעה שמנסה להתערב בענייניה הפנימיים של מדינה אחרת עלול לפגוע באמון שיש לאזרחים בממשלתם. בנוסף, הוא ינסה לעורר שיח, פעולות והפגנות נגד הממשלה ולפגוע במורל הציבורי. מכאן החשיבות שממשלות וגופי ביטחון יידעו לזהות מבצעי השפעה בסייבר ולמנוע אותם, או לפחות לצמצם את השפעתם השלילית. למרות שידוע כיצד מבצעי השפעה בסייבר מתנהלים ובאילו טקטיקות הם משתמשים, הזיהוי שלהם אינו משימה קלה, שכן מפעילי ההשפעה משתמשים בטקטיקות הסוואה שונות.

מאמר זה ביקש להציג מספר פרמטרים אינדיקטיביים לזיהוי מבצעי השפעה בסייבר שמתבססים על פרסום תכנים, בעיקר ברשתות החברתיות. עצם מציאת הפרמטרים שנדונו במאמר הוא אתגר בפני עצמו. כל פרמטר בנפרד אינו אינדיקציה מספקת לקמפיין השפעה, אך ביחד הם מעניקים נקודת פתיחה טובה לניתוח מצבים, ושימוש משולב בו־זמני בהם יכול לספק אינדיקציה טובה לקיומו של מבצע השפעה.

מקרה הבוחן של מבצע ההשפעה הרוסי בבחירות 2016 לנשיאות ארצות הברית הוא דוגמה מושלמת, שכן הוא עונה על כמעט כל הפרמטרים האינדיקטיביים המסייעים לזיהוי, אפילו בשלב המוקדם ביותר. הדבר מאפשר ללמוד שהפרמטרים האינדיקטיביים שהוזכרו לעיל יכולים לשמש כדרך שיטתית לגילוי מבצעי השפעה בסייבר. גישה מעשית כזו מציעה אפשרות לגילוי מוקדם של המבצע הבא של השפעה בסייבר באמצעות ניטור מתמיד של אמצעי התקשורת הרלוונטיים, וזאת אפילו על ידי אנליסטים שאינם מומחים.

ברמה הלאומית, "תמונת מצב הסייבר" כוללת את מצב התשתיות הלאומיות הקריטיות של המדינה, את מצב הסייבר של גופי הביטחון והממשל, אירועי סייבר ישירים, לרבות ניסיונות למתקפות סייבר, וכן מתקפות סייבר שנעשו בפועל, כולל הנזק שנגרם מהן. יחד עם זאת, עליה לכלול גם פעולות סייבר עקיפות, כמו מבצעי השפעה בסייבר שהוציאו לפועל מדינות אחרות. יש לראות במבצעים אלה מלחמות חשאיות ולטפל בהם בהתאם, לרבות על ידי הקצאת משאבים לזיהוים וסיכולם. בכל מקרה, מומלץ לערוך מחקרים נוספים, שינסו לזהות עוד פרמטרים אינדיקטיביים, יתרמו לאוטומציה של תהליכי זיהוי של מבצעי ההשפעה ויציעו דרכים להתגונן מפני פעולות אלו.