

מבצעי השפעה בסייבר – מאפיינים ותובנות¹

דגנית פייקובסקי ואביתר מתניה²

מבוא

הדיווחים על הניסיון להשפיע על הבחירות לנשיאות ארצות הברית בשנת 2016 באמצעות פעולות בסייבר מציפים שתי תופעות שונות במערכה בסייבר. התופעה הראשונה היא הרחבת מעגל המטרות של איומי הסייבר: ממערכות מחשוב של תשתיות קריטיות המספקות שירותים חיוניים ומוחשיים, אל מטרות שהן תשתיות, תהליכים ומגזרים המספקים שירותים פחות מוחשיים, אך חיוניים לקיומה של החברה והמדינה. כך, למשל, ניתן לחדור למערכות מחשוב לניהול בחירות לאומיות לצורך שינוי תוצאות ההצבעה בקלפיות או לפגיעה בריכוז התוצאות, או לחדור למערכות מחשוב של מפלגות, כלי תקשורת, חברות לעריכת סקרי דעת קהל, ואף של הציבור עצמו, כדי לפגוע בתפקודן התקין.

התופעה השנייה היא מימוש דפוס הפעולה המוכר של מבצעי השפעה על התודעה, תוך ניצול מאפייניו הייחודיים של מרחב הסייבר. זאת, באמצעות השפעה על סדר היום, על תפיסת המציאות ועל קבלת ההחלטות בתקופת מערכת הבחירות הקודמת להליך ההצבעה עצמו, בדרך שיש בה כדי להטות את תוצאות הבחירות (מבלי לשבש אותן ישירות) ו/או לזרוע ספק באשר לאמינותן, לטוהר הבחירות, ולהליך הדמוקרטי בכלל. כך, למשל, ניתן לפרסם מידע אמיתי, מוטה או כוזב, במטרה להשפיע על דעת

1 מאמר זה אינו מייצג דעה או אסטרטגיה רשמית של מדינת ישראל או של מערך הסייבר הלאומי, אלא מהווה ניתוח ודעה אישית של הכותבים.

2 ד"ר דגנית פייקובסקי מתמחה באסטרטגיה ותכנון מדיניות בתחומי המדע והטכנולוגיה. כיום היא משמשת כראש תחום בכיר באגף אסטרטגיה והתעצמות במערך הסייבר הלאומי. פרופסור אביתר מתניה הוא המקים של מערך הסייבר הלאומי ובעבר עמד בראשו. כיום הוא מכהן כראש התוכנית ללימודי ביטחון וכאיש סגל בית הספר למדע המדינה מממשל ויחסים בין-לאומיים באוניברסיטת תל אביב.

הקהל ולהסיט אותה לכיוון מסוים שיתבטא בדפוסי ההצבעה. דרך פעולה נוספת באותו הקשר היא הדהוד של מסרים בהיקף נרחב ברשתות החברתיות במטרה לעצב את השיח בכיוון מסוים.³ חשוב לציין כי גם כאשר קהלי היעד הרלוונטיים (מקבלי החלטות ו/או הציבור) מודעים לפגיעה בתפקודן של מערכות המחשוב, פגיעה זו עדיין עלולה להשפיע על תודעתם.

התחום בו מתמקד מאמר זה הוא באזור שבו מתקיימת חפיפה בין פעולות תקיפה בסייבר לבין פעולות השפעה על התודעה, קרי, פעולות בסייבר שמטרתן העיקרית היא להשפיע על התודעה במישרין (מכאן ואילך נכנה אותן בקיצור "השפעה על התודעה בסייבר"). מצד אחד, פעולות אלו הן חלק מהמכלול של המערכה בסייבר, ומצד שני, הן חלק מהמכלול של מלחמות המידע, של מבצעים פסיכולוגיים ושל ניסיון להשפיע על מקבלי ההחלטות באמצעות מעטפת שלמה של מידע ונרטיבים. מכיוון שהפעולות המתוארות במאמר זה נמצאות בתווך בין תקיפות בסייבר ובין השפעה על התודעה, הניתוח שלהן יעשה משני הכיוונים במקביל. בהתאם לכך, תקיפת סייבר הגורמת לפגיעה פיזית מתוך כוונה לשחק מערכת חיונית, כמו מערכת חשמל או מים, אינה חלק מנושא של מאמר זה, למרות שעשויות להיות לה גם השפעות לוואי תודעתיות. לעומת זאת, אם התקיפה בוצעה בכוונה לגרום לבהלה או לערער את אמון הציבור במערכת, אזי יש לראות בה תקיפת סייבר בעלת השפעה ישירה על התודעה. בדומה לכך, תקיפת סייבר שמטרתה היא שינוי תוצאות הבחירות באמצעות שינוי הנתונים, מבלי שדבר התקיפה הגיע למודעותו של הצד הנתקף, אינה תקיפה שמטרתה השפעה על התודעה.

תופעת ההשפעה על התודעה בסייבר הופכת בהדרגה לדפוס פעולה אטרקטיבי במקומות שונים בעולם, וקיימת אפשרות שהיא תתעצם ותשתכלל עוד. לפיכך, יש צורך לעמוד על טיבן של שתי התופעות שפורטו לעיל, שההשפעה התודעתית בסייבר היא חלק מהן, תוך שימת דגש על המאפיינים המשותפים להן, אך גם, ואולי בעיקר, על המאפיינים הייחודיים של כל אחת מהן.

המאמר עוסק בגורמים שהביאו להפיכתם של מבצעי ההשפעה על התודעה לדפוס פעולה אטרקטיבי דווקא בסייבר, וכן בהבדלים שבין דפוס פעולה זה ובין המערכה המוכרת בסייבר. בעוד שהמערכה המקובלת בסייבר נועדה לגרום פגיעה תפקודית מוחשית ביריב, והשפעתה על התודעה (אם בכלל היא קיימת) היא בעקיפין, תכליתם של מבצעי ההשפעה על התודעה היא פגיעה ביריב באמצעות השפעה ישירה על תודעתו.

3 דודי סימן טוב, גבי סיבוני, גבריאל אראל, "איומים קיברנטיים על תהליכים דמוקרטיים", **סייבר מודיעין וביטחון**, כרך 1, גיליון 3, דצמבר 2017, עמ' 59-69.

ניתוח שתי תופעות אלו הינו חיוני במיוחד עבור מדינות דמוקרטיות. כדי להיערך באופן אפקטיבי להתגוננות מפניהן, נדרשות מדינות להכיר בכך שמדובר בשתי תופעות שונות, למרות שהן עלו על סדר היום העולמי במשותף. לפיכך, ההתמודדות עם כל אחת מהן צריכה להיות שונה.

טענתנו העיקרית היא, כי מנקודת המבט של המערכה בסייבר, מבצעי השפעה על התודעה במרחב הסייבר ובאמצעות כלי סייבר מגלמים שינוי תפיסתי בעל משמעות. זאת, מאחר שמבצעים אלה נשענים על הנחות יסוד שונות מאלו שעליהן נשענת המערכה המוכרת בסייבר, שעיקרה פגיעה בתפקוד התקין של מערכות מחשוב. הגנה אפקטיבית מפני האיום של מבצעי השפעה על התודעה בסייבר מחייבת תפיסה שתכתב עם מאפייניו הייחודיים של איום זה ועם הנחות היסוד שלו. יתרה מכך, כדי להתגונן באפקטיבית מפני האיום שמציבים מבצעי השפעה על התודעה בסייבר, מתחייבת היערכות לאומית כוללת מולם ושיתוף פעולה בין מגוון גופים, שארגוני הגנת הסייבר הם רק חלק מהם.

חלקו הראשון של המאמר עוסק בניתוח המאפיינים הכלליים של מבצעי השפעה על התודעה, שמבצעי השפעה על התודעה במרחב הסייבר מהווים, כאמור, חלק מהם. חלק זה גם עוסק בניתוח המאפיינים האנושיים והחברתיים עליהם מתבססים העוסקים במבצעים אלה. בחלקו השני מתמקד המאמר בתרומתן הספציפית של הרשתות החברתיות, שפעולה בהן הופכת את מבצעי ההשפעה על התודעה בסייבר לאטרקטיביים כל כך. החלק השלישי עוסק בהרחבת מעגל המטרות של איומי הסייבר, וביתר פירוט – במשותף ובשונה בין פעולות בסייבר שתכליתן פגיעה תפקודית ובין פעולות בסייבר שתכליתן פגיעה תודעתית, שביחד מהוות את כלל האיומים בסייבר. בסיום המאמר מוצגות תובנות ראשוניות הנוגעות לפערים שאנו מזהים בדרכי ההתמודדות עם אתגרי המערכה על התודעה בסייבר. פערים אלה מחייבים גיבושה של תפיסה כוללת, שתאפשר התמודדות אפקטיבית עם מבצעי השפעה על התודעה בסייבר.

אסטרטגיה של השפעה על התודעה

השפעה על התודעה היא היכולת לשנות ו/או לעצב את תפיסותיו של האחר, וכתוצאה מכך לשבש ו/או לשנות את התנהגותו, החלטותיו ויכולותיו. זאת, באמצעות העלאת או הורדת של נושאים מסדר היום הציבורי והטיית השיח ביחס לנושאים אלה.⁴ השפעה על התודעה מבוססת על מספר מאפיינים חברתיים ואנושיים: הראשון הוא הקושי האנושי להבחין בין מידע שקרי ובין מידע אמיתי והקושי לשחזר לאחור מה היה אמיתי ומה שקרי. המאפיין השני הוא הנטייה לקיצורי דרך בהערכת אמינותם של

4 קרין נהון, שירה ריבנאי, "תעמולת בחירות בראי האינטרנט והרשתות החברתיות", חומר רקע לוועדת בייניש, ינואר 2016, עמ' 5.

מסרים במצב של שטף ועומס מידע. מאפיין שלישי הוא נטייתם של אנשים להאמין למידע התואם את השקפת עולמם, גם אם מדובר במסרים שקריים, ולקבל ולהאמין להצהרות ולטענות אם הן נתמכות בעובדות, אפילו הן כוזבות. מצג של אובייקטיביות מחזק אמינות של מסר תעמולתי, למשל, פרסומו באתר חדשות.

מבצעי השפעה על התודעה הם דפוס פעולה ותיק ומוכר, שנועד לשרת מגוון תכליות מדיניות, ביטחוניות, כלכליות וחברתיות. מבצעי השפעה על התודעה ברמה המדינית נועדו להשיג את יעדיהם, בין היתר, באמצעות פגיעה בביטחון האישי והכלכלי, ערעור האמון והתמיכה של הציבור במוסדות המדינה ופגיעה בלכידות החברתית. האמצעים להשגת תכליות אלו כוללים התערבות פעילה במערכות ובתהליכים, או הפעלת מנופים שונים (כלכליים ואחרים) כדי להניע לפעולה או להניא מפעולה, השגת מידע ושימוש בו ליצירת מסרים, הפצה של מסרים ויצירת תהודה להשגת אפקט מרבי. הערוצים להעברת המסרים הם המדיה המסורתית (עיתונות, רדיו, וטלוויזיה), וכן המדיה החדשה, קרי, האינטרנט והיישומים השונים שמעליו, כמו הרשתות החברתיות. מובילי דעה משמשים לעיתים כ"סוכנים לא מודעים" לחיזוק אמינותם של המסרים ולהגדלת תפוצתם.⁵

אסטרטגיה של מבצעי השפעה על התודעה היא לרוב חלק מתפיסה מערכתית מרובת ערוצים ואמצעים, המכונה לעיתים "לוחמת מידע" (Information Warfare). אסטרטגיה זו נועדה לתמרן שחקנים להתנהגות רצויה, לעיתים בניגוד לאינטרסים שלהם, ועושה זאת, בין השאר, באמצעות סילוף תמונת המציאות והשפעה עליה וכן הפעלת מנופים מסוגים שונים. פעולות אלו מתבצעות כלפי מקבלי החלטות וכלפי ציבורים של יריבים וידידים, הן בעת שלום והן בעת מלחמה.⁶

בעת האחרונה הולכים ומתעצמים מבצעי השפעה על התודעה באמצעות שימוש בסייבר. הסייבר מספק את התשתית ואת הכלים – לגיטימיים ובלתי לגיטימיים כאחד – למימוש מבצעים אלה. לצורך זה נעשה שימוש במידע שמקורו, לפחות באופן חלקי, הוא במערכות ממוחשבות ובמאגרי מידע. העלייה בהיקפם של מבצעי ההשפעה על התודעה בסייבר הופכת אותם בעיני רבים לאיום משמעותי. על פי הדוחות של מנהל המודיעין הלאומי של ארצות הברית (Director of National Intelligence – DNI), העוסקים בהערכת האיומים הגלובליים, מבצעי השפעה, ובמיוחד מבצעי השפעה על

5 רון שליפר, "הלוחמה הפסיכולוגית ב'עפרת יצוקה'", **מערכות**, 432, אוגוסט 2010, עמ' 19–20.

6 דימה אדמסקי, "אומנות אופרטיבית קיברנטית: מבט מזווית לימודי האסטרטגיה ומפרספקטיבה השוואתית", **עשתונות**, גיליון 11, אוגוסט 2015, עמ' 28–48.

התודעה בסייבר תוך שימוש בכלי סייבר, נתפסים בארצות הברית כאיום משמעותי, שעצימותו וחשיבותו הולכות וגדלות.⁷

האטרקטיביות שבהפעלת מבצעי השפעה על התודעה בסייבר והרשתות החברתיות

התעצמותו ההולכת וגוברת של האיום הכרוך במבצעי השפעה על התודעה בסייבר נובעת מכך שמרחב הסייבר, ובמיוחד היישומים השונים של הרשתות החברתיות, מספקים פלטפורמות טכנולוגיות וכלים חדשים למימוש מבצעי השפעה בקצב ובעוצמה שלא הכרנו בעבר. בזכות הסייבר, הנגישות למגוון יעדים לצורך איסוף מידע והפצתו, וכן זמינותם, הופכות לקלות, יעילות ומהירות, וכל זאת בעלות נמוכה יחסית. מבחינתו של התוקף, האטרקטיביות של הפעלת מבצעי השפעה בסייבר נובעת מהאפשרות להשיג באמצעותם הישגים מדיניים ביעילות רבה ובעלות נמוכה באופן משמעותי מהעלות של הפעלת כלים מסורתיים (שהקיצוני שבהם הוא הפעלת כוח צבאי). למגמה זו מצטרף השינוי הפרדיגמטי המתמשך באופן ניהול המלחמה בעשורים האחרונים, המביא, לעיתים, להעדפת הפעולה בסייבר על פני פעולה במישורים אחרים, ובמיוחד במישור העימות הצבאי הישיר.⁸

הרשתות החברתיות⁹ ממלאות כיום תפקיד מרכזי במימוש מבצעי השפעה בסייבר, בהיותן "זירת קרב" מרכזית, כמו גם אפיק תקיפה יעיל למימוש מבצעי השפעה על התודעה. יש לכך מספר סיבות: ראשית, מספר המשתמשים ברשתות החברתיות לצריכת מידע וליצירת אינטראקציה ישירה מכל מקום ובכל זמן, גדל בשנים האחרונות

7 Daniel, R. Coats, Director of National Intelligence, "Statement for the Record – Worldwide Threat Assessment of the US Intelligence Community", Senate Select Committee on Intelligence, May 11, 2017; James, R. Clapper, Director of National Intelligence, "Statement for the Record – Worldwide Threat Assessment of the US Intelligence Community", Senate Armed Services Committee, February 9, 2016; James, R. Clapper, Director of National Intelligence, "Statement for the Record – Worldwide Threat Assessment of the US Intelligence Community", Senate Armed Services Committee, February 26, 2015; James, R. Clapper, Director of National Intelligence, "Statement for the Record – Worldwide Threat Assessment of the US Intelligence Community", Senate Select Committee on Intelligence, January 29, 2014; James, R. Clapper, Director of National Intelligence, "Statement for the Record – Worldwide Threat Assessment of the US Intelligence Community", Senate Select Committee on Intelligence, March 12, 2013; James, R. Clapper, Director of National Intelligence, "Statement for the Record – Worldwide Threat Assessment of the US Intelligence Community", Senate Select Committee on Intelligence, February 10, 2011.

8 עוד על תהליכים אלה ראו: Ned Lebow, *Why Nations Fight* (New York: Cambridge University Press, 2010).

9 פלטפורמות דוגמת "פייסבוק", "ווטסאפ", "אינסטגרם", "לינקדאין", ו"טוויטר".

באופן מעריכי (אקספוננציאלי).¹⁰ בנוסף, הפצת מידע ברשתות החברתיות מתבצעת במהירות בתוך קבוצות ובין קבוצות. לעיתים, זרימת המידע והתפשטותו נעשות במהירות כה גבוהה, עד שקשה מאוד, עד בלתי אפשרי, לעצור את התהליך. מצב זה מכונה "ויראליות של זרימת המידע".¹¹

לכך מצטרפת סיבה נוספת – הארכיטקטורה הטכנולוגית של הרשתות החברתיות. ארכיטקטורה זו, אשר נועדה לנהל עבור המשתמשים את שטף המידע באמצעות סינון עודף מידע וחשיפה למידע מותאם אישית, היא מרכיב משמעותי באטרקטיביות של הרשתות החברתיות כמצע למימוש מבצעי השפעה.¹² המצב, שבו המשתמשים ברשתות החברתיות נחשפים רק לחלק קטן מכלל המידע הזורם ברשת, מסייע, גם אם באופן לא מכוון, ליעול מבצעי ההשפעה על התודעה, מאחר שהוא מעצים תכנים מסוימים וממקד את החשיפה אליהם.¹³

גורם נוסף אותו ניתן להציג כפועל לטובת מבצעי ההשפעה על התודעה הוא האפשרות שניתנת למשתמשים ברשתות החברתיות ליצור ולהפיץ מידע ולקיים אינטראקציה עם אחרים באופן ישיר ובלתי אמצעי, ובכך יוצרת אשליה של פלורליזם, גם אם המצב האמיתי הוא שונה מהותית. במבצעי השפעה על התודעה עושים התוקפים שימוש בחשבונות מזויפים, דוגמת "בוטים" או "אונאָטרים", כדי להשפיע על סדר היום הציבורי וליצור רושם שדעת הקהל נוטה לכיוון מסוים. יש להניח שככל שהציבור יהיה מודע יותר לקיומם של מבצעי השפעה על התודעה ברשתות החברתיות, כך הוא יגלה ביקורת רבה יותר כלפי הנעשה בממד זה, ובסופו של דבר יעילותו של דפוס פעולה זה עשויה להיפגע.¹⁴

פגיעה תפקודית ופגיעה תודעתית בסייבר

יש הבדל בין איומי הסייבר בהיבט התפקודי ובין איומי הסייבר בהיבט התודעתי. יחד עם זאת, שני האיומים חולקים מספר מאפיינים משותפים. כך, פגיעה תפקודית עשויה להסב נזק תודעתי בעל משמעות, שבמקרים מסוימים עשוי להיות גבוה מהנזק התפקודי עצמו, ולכן עשוי להוות את התמריץ העיקרי לפעולה (כלומר לתקיפה). למשל, אפשר להניח כי הפסקת חשמל בעיר גדולה, הנמשכת שעות בודדות ומתבררת

10 בשנת 2010 עמד מספר המשתמשים ברשתות החברתיות בעולם על 0.97 מיליארד, ואילו ב-2017 הוא כבר עמד על 2.62 מיליארד משתמשים. ראו: <https://bit.ly/2gRTQQk>

11 Karine Nahon, Hemsley Jeff, *Going Viral* (Cambridge: Polity Press, 2013).

12 כדי לייצר עבור המשתמשים חוויית גלישה התואמת את תפיסת עולמם, הפלטפורמה לומדת את תחומי העניין ואת הרגליהם של המשתמשים, לעיתים בממשק עם מידע מפלטפורמות אחרות.

13 נהון וריבנאי, "תעמולת בחירות בראי האינטרנט והרשתות החברתיות", עמ' 3-5; שיחה עם ד"ר תהילה אלטשולר, המכון הישראלי לדמוקרטיה, אוגוסט 2017.

14 שם, עמ' 4.

בציבור כתוצר של פעולה מכוונת מצד יריב, תיצור בהלה, חשש, אי־ודאות ואי־אמון, כלומר תגרום נזק תודעתי שיהיה גדול בהרבה מהנזק התפקודי הישיר שנגרם מהיעדר חשמל למשך מספר שעות.

התבוננות בשני האיומים מעלה כי בשניהם גם מתקיימת הרחבה של מעגל הנתקפים הפוטנציאלי. המערכה בסייבר התאפיינה עד לאחרונה בתפיסה מצמצמת, שהתמקדה בעיקר בפגיעה תפקודית ביעדים צבאיים ו/או אזרחיים, המהווים תשתיות קריטיות לתפקוד המוחשי והממשי של החברה או המשק. פגיעה ביעדים מסוג זה מהווה פגיעה חמורה בביטחון הלאומי ו/או בחוסן הכלכלי של הצד הנתקף. לצד זאת, אנו עדים בשנים האחרונות לפעולות, שתכליתן היא פגיעה תפקודית בסייבר, המופנות גם כלפי מערכות ותהליכים חברתיים וערכיים. במידה רבה מדובר במערכות ותהליכים אליהם מכוונות גם פעולות להשפעה על התודעה. במילים אחרות, ניתן לתאר את השינוי במערכה בסייבר בכך שמכלול הסביבה של הנתקף – תשתיות פיזיות, נכסים מוחשיים (כמו ידע או סודות) ונכסים לא מוחשיים (כמו מוניטין או אמון) – מהווה כיום את היעד לפעולה, בין אם תכליתה היא פגיעה תפקודית ובין אם תכליתה היא השפעה תודעתית. כאשר מדובר בפגיעה במערכות שאינן בגדר תשתית פיזית חיונית, המשותף לשני האיומים הוא שבשניהם קיים קושי לאמוד במדויק את הנזק ו/או לעשות שימוש בתבחינים המקובלים של נזק כלכלי או של אובדן חיי אדם כדי להעריך את גודל האיום.

הרחבת מעגל הנתקפים מעלה מאפיין נוסף המשותף לשני האיומים, והוא המתח המתעורר במצב שבו משטר דמוקרטי, המושתת על עקרונות חופש הביטוי, חופש העיתונות, הזכות לפרטיות והפרדת רשויות, מבקש להגן על גופים ותהליכים מרכזיים של הדמוקרטיה, שקיימת בהם הפרדת רשויות ונדרש לשמור בהם על זכויות יסוד, מפני האיומים שתוארו לעיל (פגיעה תפקודית או מניפולציה של מידע ובאמצעות מידע). כדי להבטיח שמנגנוני ההגנה מול שני האיומים הללו לא ינוצלו לרעה, על משטר דמוקרטי לבסס מערך של איזונים ובלמים, שיפחיתו את הסיכונים שלהם לדמוקרטיה. לצד המאפיינים המשותפים לאיום בפגיעה תפקודית ולאיום בהשפעה על התודעה, קיימים מספר הבדלים עקרוניים בין שני האיומים: שניהם מגלמים שתי תכליות (הישגים מצופים) שונות לפגיעת סייבר, הגם ששתיהן עושות שימוש באיסוף מידע, בשיבוש מידע או במניעת מידע.¹⁵ ניתן לסווג את הפגיעה במידע לשלוש קבוצות עיקריות (מוכר גם כמודל CIA): פגיעה בחסיון המידע (Confidentiality of Data),

15 לשם פשטות, אנו מציגים כאן את ההבדלים בין פגיעה תפקודית לפגיעה תודעתית במידע בלבד, ומתעלמים מתקיפות סייבר נגד מערכות פיזיות שאינן מערכות מידע, כמו למשל גנרטורים ומערכות של חברת החשמל.

פגיעה באמינות המידע (Integrity of Data) ופגיעה בזמינות המידע (Availability of Data).

טבלה מספר 1: סיווג פעולות חדירה בלתי מורשות למערכות ממוחשבות

מהות הפעולה		סוגי הפגיעה
תכלית תפקודית	תכלית תודעתית	פגיעה בחסיון המידע (Confidentiality)
איסוף מידע להפקת מודיעין צבאי / אזרחי / מסחרי	חשיפת מידע חסוי והפיכתו לפומבי. לדוגמה: הדלפת מידע מביך או איום בהדלפה	
שיבוש ושינוי נתונים לצורך פגיעה פיזית או לצורך שיבוש תמונת המצב	הטיה של מידע ו/או שתילה של מידע מוטה או כוזב ופרסומו לצורך שיבוש תמונת המציאות	פגיעה באמינות המידע (Integrity)
מניעת גישה למידע או שיבוש/העלמתו	מניעת היכולת לפרסם/להפיץ מידע. לדוגמה: חסימת פלטפורמות שבאמצעותן מתקיימות תקשורת ועוברים מסרים של מפלגה או מועמד/ת בעת מערכת בחירות, כדי למנוע את העברת המסרים	פגיעה בזמינות המידע (Availability)

פעולות התקפיות בסייבר לתכלית תפקודית נעשות באמצעות חדירה בלתי מורשית למערכות מחשב על ידי שימוש בקוד עוין. בנוסף לכך קיימת חדירה בלתי מורשית שעניינה איתות ליריב או איסוף מידע. במבצעי השפעה על התודעה מתרחשת מניפולציה על התודעה של היריב באמצעות העברת מידע, מניעתו או שיבושו, כמו פרסום של מידע כוזב או הדלפה של מידע חסוי. ניתן לכנות פעולה זו שימוש בתוכן עוין. חשוב להדגיש שפעולה כזאת מלווה לעיתים גם בחדירה בלתי מורשית למערכות מחשב, אך הדבר אינו הכרחי, ופעולות השפעה רבות אינן נדרשות לכך.

ניתן לאפיין שני דפוסי פעולה עיקריים שבהם נעשה שימוש בתוכן עוין. הראשון הוא שימוש בתוכן עוין בלבד, ללא חדירה זדונית למערכות מחשב, למשל על ידי הדלפת מידע, שימוש ב"אונֶאָטָארים" כדי להציף נושאים לסדר היום, הטיית השיח לכיוונים התואמים את האינטרסים של התוקף, הסתה לטרור, הפצת שמועות או הפחדה. הדפוס השני מגלם שילוב בין שימוש בקוד עוין ובין שימוש בתוכן עוין. כלומר, לצורך השגת המטרה מבוצעת חדירה בלתי מורשית למערכות מידע, אלא שהחדירה היא רק אמצעי בדרך לבצע מניפולציה באמצעות מידע. דוגמאות לכך הן: חדירה בלתי מורשית למערכות מידע של חברות סקרי דעת קהל במטרה להטות את התוצאות, ובכך להזין את הציבור בפרשנות שגויה על הלכי הרוח בנושא שבגיניו בוצע הסקר; גניבת מידע לשם הדלפה; חדירה בלתי מורשית לרשימות תפוצה במטרה להגיע לפרטי הקשר ולאמצעי הקשר לצורך העברת מסרים עוינים; חדירה למערכות של אמצעי תקשורת

המונים ו/או פלטפורמות אינטרנטיות לקשר עם הציבור של הגורם המותקף (אתר אינטרנט וחשבונות ברשתות החברתיות) לצורך השחתה, הפסקת פעילות, שיבוש מידע והפצת מידע כוזב.



איור מספר 1: השפעה באמצעות קוד עיון ו/או באמצעות תוכן עיון

מאפיין נוסף של תופעת ההשפעה על התודעה בסייבר, המבדיל אותה חלקית מתופעת הפגיעה התפקודית, נוגע למידת החשאיות שלה. ככל שההתרחשות הזדונית אינה ידועה, וגם לא ידוע שקיימת "יד מכוונת" מאחוריה, כך עולה האפקטיביות של ההשפעה על התודעה. מחיר ההיחשפות במקרה כזה עלול להיות גבוה, עד כדי פגיעה בתכליתו של מבצע ההשפעה כולו. לכן, ההעדפה היא כמעט תמיד לפעולות סמויות "מתחת לפני השטח" במתווה של No-logo Strategy. גם תקיפות סייבר לפגיעה תפקודית במערכות מחשב או לשיבוש מידע מבוצעות לעיתים באופן סמוי כדי לא להסגיר את דרך הביצוע, או כדי להימנע מקבלת אחריות פומבית. אלא שכשהן פוגעות בתפקודן של מערכות מחשב, עצם ההתרחשות הופכת לאירוע ידוע.

סיכום: משמעויות עבור מדינות דמוקרטיות

במאמר זה התמקדנו בהבחנה בין שני הסוגים של תקיפה בסייבר: תקיפה שנועדה לפגוע בתפקוד של מערכות מחשב, שכמעט תמיד כרוכה בחדירה בלתי מורשית למערכות אלו; תקיפה תודעתית בסייבר, שלא עושה בהכרח שימוש בחדירה בלתי מורשית. חשוב לציין ולהבין שהבחנה זו היא בעיקרה תוצר של גישה תרבותית-דמוקרטית המקבלת את כללי המשחק הדמוקרטיים המערביים, לפיהם לא ראוי ולא חוקי לחדור

למערכות מחשב של אחרים (דבר שמושרש גם בתפיסות, בנורמות ובחקיקה). לכן, תפיסה זו רואה בכל פעולה נגד תפקודן של מערכות מחשב אקט תוקפני הדורש הגנה ברורה על ידי שימוש באמצעים שונים – משפטיים, משטריים או ביטחוניים. תוצר מרכזי של תפיסה דמוקרטית זו הוא חשש כבד מהתערבות בתחום התוכן, הנרטיבים והמדיה בכלל, והעדפה לאפשר חופש ביטוי כמעט מוחלט כחלק מההליך הדמוקרטי. כתוצאה מכך, במשטרים דמוקרטיים קיימת מבוכה רבתי באשר לדרכים הנכונות למנוע או לצמצם מבצעי תודעה בסייבר ולהתגונן בפניהם, וזאת מתוך חשש למעורבות ממשלתית כזו או אחרת במדיה ובחירויות הדמוקרטיות לסוגיהן.

התמודדות הגנתית אפקטיבית עם מבצעי השפעה על התודעה בסייבר צריכה להיעשות מול מכלול התופעה ואיומיה ומתוך הבנה שהתוקף אינו מבדיל בהכרח בין שני סוגי התקיפה בסייבר. כתוצאה מכך, ההבחנה הסובייקטיבית, הקיימת בהתבוננות מנקודת המבט הדמוקרטית, מציבה אתגר כבד משקל בפני המתגונן הדמוקרטי: כיצד לפתח מדיניות לאומית מערכתית כוללת, שתביא לידי ביטוי את מגוון התחומים הרלוונטיים להתמודדות עם מבצעי השפעה תודעתית בסייבר ותשלב כוחות ממגוון גופים האמונים על הממדים השונים של האיומים ושל המענה להם. כל זאת, תוך שמירת הסייבר כמרחב פתוח, המאפשר זרימה חופשית של ידע ושירותים ושמירה על זכויות יסוד, ובהן הזכות לחופש הביטוי ולפרטיות. מדובר באתגר ובדילמה לא פשוטים, שיתכן ואין הכרח להידרש אליהם במדינות לא דמוקרטיות. למדינות כאלו קל יותר, לפיכך, לגבש תפיסת הגנה מערכתית שאינה עושה בידול בין פעולות שנועדו לתכלית תפקודית ובין פעולות שנועדו לתכלית תודעתית – לא ברמה הרעיונית, לא ברמה הארגונית ולא ברמה המבצעית.

על בסיס תובנות אלו אנו סבורים, מנקודת המבט הדמוקרטית, כי חלק מרכזי בהתמודדות עם האתגר שמציבה התופעה של הפעלת מבצעי השפעה על התודעה בסייבר, הוא זיהוי ומיפוי כלל הגורמים והשחקנים שמעורבותם נדרשת לצורך הגנה אפקטיבית, כמו גם הממשקים ביניהם. מדובר, בין השאר, במודיעין לצורך זיהוי, סיכול והרתעה; בטכנולוגיית סייבר לצורך התמודדות עם פעולות שעיקרן חדירה בלתי מורשית למערכות ממוחשבות; בחקיקה ובאכיפה לצורך התמודדות עם הסתה והפצת תוכן עוין; בהסברה לצורך נטרול השפעה של תכנים עוינים; בהעלאת המודעות ובחינוך לביקורתיות לתכנים ברשת. ראוי גם לבחון את האפשרות לנצל לצורך זה ידע ויכולות הקיימים באקדמיה ובשוק הפרטי.

נשאלת השאלה מהו מקומם של גופי הגנת הסייבר הלאומיים בהתמודדות עם מבצעי השפעה תודעתיים בסייבר, או במילים אחרות, מדוע לא להטיל עליהם, בנוסף לאחריותם על הגנת מרחב הסייבר הלאומי או האזרחי מפני תקיפות החודרות למערכות מחשב, גם את האחריות להגנה מפני מבצעי תודעה? לכאורה, אלה הם

הגופים הטבעיים להתמודדות כזאת, שכן, כפי שהודגש לעיל, התוקף אינו עושה, בדרך כלל, את ההבחנה בין חדירה למערכות מחשוב – תחום שגופי הגנת סייבר אחראים להגן מפניו – ובין מבצעי השפעה תודעתיים. מדוע, אם כך,

לא להרחיב את אחריותם של גופי ההגנה הללו גם למטלה טבעית זו?

אין להטיל על גופי הגנת הסייבר את הטיפול

בהתגוננות מפני מבצעי

השפעה על התודעה

באמצעות הסייבר. יחד

עם זאת, אין לשלול

את השתתפותם של

גופי ההגנה בסייבר

במאמץ הלאומי הכולל

להתמודדות מערכתית עם

האיום של מבצעים אלה.

התשובה לכך נעוצה לדעתנו בשני נימוקים מהותיים הנגזרים ממאפייניהם של ארגוני הגנה אלה: הנימוק הראשון הוא שגופי הגנת הסייבר במדינות רבות הם גופים של מערכות הביטחון או של המשטרה. הטלת האחריות עליהם גם להגנה מפני תוכן עוין, ולא רק מפני חדירה עוינת, מנוגדת במהותה לאיזונים הקיימים במשטרים דמוקרטיים. תהיה זו, לפיכך, שגיאה להטיל עליהם אחריות שבגינה הם יחדרו לגופי מדיה, יתעניינו בתכניהם ויחליטו לגביהם.

הנימוק השני הוא שגם במדינות שבהן גופי הגנת הסייבר

אינם חלק ממערכת הביטחון או המשטרה, דוגמת מערך הסייבר הלאומי בישראל, יש סיבה טובה לא לחבר את שתי המטרות הללו. הסיבה היא האמון הרב שגופים אלה זקוקים לו בעבודתם עם המגזר האזרחי במדינה המאופיינת כדמוקרטיה. רק אמון גבוה בין גוף ממשלתי ובין ארגונים פרטיים יאפשר לגוף ההגנה הממשלתי גישה למידע, לנתח אותו בראייה לאומית ולפעול עם הארגונים הפרטיים ב"מגרש" שלהם. אמון זה הוא רכיב מהותי ביכולתו של גוף ההגנה ממשלתי להגן על מרחב הסייבר האזרחי. בלעדיו, יהיו סמכויותיו של גוף ההגנה אשר יהיו, הוא לא יוכל לממש את אחריותו זאת. השגת אמון כזה מבוססת, בראש ובראשונה, על כך שגופי הגנת הסייבר לא יתעניינו בתוכן ויעסקו אך ורק בהגנה מפני חדירה למערכות המחשוב. אמון זה עלול להיפגע באופן אנוש אם לגופי ההגנה יהיה מה לומר ומה לקבוע בנושאי תוכן. נימוקים והסברים אלה מובילים למסקנה כי אין להטיל על גופי הגנת הסייבר הקיימים את הטיפול בהתגוננות מפני מבצעי השפעה על התודעה באמצעות הסייבר. יחד עם זאת, אין לשלול את השתתפותם של גופי ההגנה בסייבר במאמץ הלאומי הכולל להתמודדות מערכתית עם האיום של מבצעים אלה.

המתח בין הצורך להגן מפני פעולות השפעה על התודעה באמצעות הסייבר ובין הצורך והחובה לשמור על זכויות היסוד האזרחיות מחדד את חשיבות הדיון הציבורי בשאלה "מהם כללי המשחק", או במילים אחרות, מהי השפעה אסורה ואילו כלים ושיטות אינם לגיטימיים. על כן, יש לייחד מאמץ להעמקת הדיון בסוגיות שיאפשרו לגבש הגדרה מהם גבולות הלגיטימיות של פעולות ההשפעה במרחב הסייבר. מדובר, בין היתר (אך לא רק):

- א. בהגדרת גבולות הלגיטימיות של פעולות בקנה מידה המוני שנועדו ליצור השפעה על התודעה. לדוגמה: פעולות באמצעות רשתות "בוטים".¹⁶
- ב. בהגדרת גבולות הלגיטימיות של פגיעה בגופים ובתהליכים ערכיים וחיוניים לחברה ולמדינה באמצעות פעולות במרחב הסייבר.
- ג. בהגדרת גבולות הלגיטימיות של מעורבות גופי ההגנה במאמצים נגד פעולות המשלבות בין קוד עוין ובין תוכן עוין, ובכלל זה היכולת להתמודד עם מצבים של חדירה בלתי מורשית למערכות מידע ממוחשבות בגופים או בתהליכים ערכיים וחיוניים לחברה ולמדינה, וזאת במגוון היבטים וכלים. לדוגמה: התמודדות עם שימוש לרעה במידע בלתי מסווג שהושג באמצעות חדירה בלתי מורשית למערכות מידע ממוחשבות.
- ד. בבחינת האפשרות לפיתוח מנגנונים מדינתיים ובין-לאומיים שיספקו מסגרת לפעולה ויגדירו את האחריות של החברות המפעילות את הרשתות החברתיות אל מול האיומים.¹⁷ זאת, תוך התייחסות לארכיטקטורה של איסוף המידע על המשתמשים, סינון וזרימת המידע אליהם והתמודדות עם הוויראליות בהעברת מסרים.

העצימות ההולכת
וגדלה של השימוש
במבצעי השפעה על
התודעה בסייבר מחייבת
התייחסות ייעודית
למאפיינים הייחודיים
של דפוס פעולה זה. יש
לעשות זאת תוך שמירת
הסייבר כמרחב פתוח
וחופשי, במקביל להמשך
השמירה על זכויות היסוד
האזרחיות.

סוגיה נוספת בעלת חשיבות להתמודדות אפקטיבית עם פעולות השפעה על התודעה בסייבר נוגעת לאמון הציבור במוסדות המדינה. מבצעי השפעה נועדו, בין היתר, לפגוע ביציבות החברתית ולערער את אמון הציבור במערכות ובמוסדות המדינה. על כן, רמת אמון גבוהה של הציבור בגוף שכלפיו נעשה שימוש בתוכן עוין היא רכיב משמעותי ביכולת להתמודד באופן יעיל עם מבצע השפעה.¹⁸ יש להשקיע מחשבה באשר לדרכים לחיזוק ולביסוס האמון בין הציבור ובין מוסדות המדינה השונים. מנקודת מבטו של ארגון הגנת הסייבר, אחת הדרכים לעשות זאת היא לטפח קשר שוטף וישייר עם הציבור ולבסס יכולת להבטיח כי בעת משבר ניתן

16 לדוגמה, במאמר שהתפרסם ב"ניו יורק טיימס" ב-15 ביולי 2017, תחת הכותרת "Please Prove You're not a Robot", הציע החוקר Tim Wu מאוניברסיטת קולומביה להגדיר botnets כ"אויבי האנושות", בדומה לפיראטים.

17 Tim Wu המשיך וטען במאמר הדעה שלו כי בהיעדר תמריץ כלכלי לחברות המפעילות את הרשתות החברתיות, קשה להתמודד עם בעיית ה-botnets.

18 לדוגמה, רון שליפר טוען כי "מדיום יעיל שבו השתמש החמאס במבצע 'עופרת יצוקה' היה הפצת שמועות. בין היתר הוא הפיץ שמועות בנוגע למספר הנפגעים שיש לצה"ל, אך מאחר ודובר צה"ל נהנה מאמינות גבוהה, לא נגרם נזק עקב השמועות הכוזבות". ראו: שליפר, "הלוחמה הפסיכולוגית ב'עופרת יצוקה'", עמ' 22.

יהיה לברר את אמינות המערכות הממוחשבות ואת אמינות המידע בהן בתוך זמן קצר, ולשתף בכך את הציבור.¹⁹

לסיכום, תופעת ההשפעה על התודעה בסייבר הופכת לדפוס פעולה נפוץ ולאיזם בעל משמעות על היכולת המדינתית לקבל החלטות באופן עצמאי. ההיערכות ההגנתית במסגרת המערכה בסייבר התמקדה עד כה בעיקר בהגנה מפני פגיעה תפקודית. העצימות ההולכת וגדלה של השימוש במבצעי השפעה על התודעה בסייבר מחייבת התייחסות ייעודית למאפיינים הייחודיים של דפוס פעולה זה. יש לעשות זאת תוך שמירת הסייבר כמרחב פתוח וחופשי, במקביל להמשך השמירה על זכויות היסוד האזרחיות.

Rand Waltzman, "The Weaponization of Information – The need for Cognitive Security", 19 Testimony presented before the Senate Armed Services Committee, Subcommittee on Cybersecurity, Rand Corporation, April 27, 2017, p. 6.