11 במארס 2021

מבצעי השפעה: שילוב של תקיפה טכנולוגית ומניפולציה על תכנים[1]

דוד סימן טוב ואוהד זיידנברג[2]

מאמר זה מנתח תופעה חדשה יחסית בעולם מתקפות הסייבר, אשר משלבת מתקפות טכנולוגיות ומניפולציה על תכנים. אומנם התופעה של השפעה על תכנים אינה חדשה במסגרת הקרב על התודעה, וכך גם תקיפה טכנולוגית של מערכות מחשוב ותשתיות ממוחשבות, אולם שילובן יחד הוא תופעה של השנים האחרונות, וביתר שאת לאור המתקפה המיוחסת לרוסיה בבחירות 2016 בארצות הברית. במסגרת המאמר נציג מספר דגמי מתקפות המשלבים מניפולציה על תוכן ותקיפות סייבר טכנולוגיות ונדון בהבדלים בין הדגמים השונים מבחינת משמעויות והשלכות (מעטפת ידע ויכולות טכנולוגיות), כפי שאלו באים לידי ביטוי ברשת האינטרנט בשילוב עם הרשתות החברתיות.

המאמר בוחן מתקפות המיוחסות למדינות ואשר בדרך כלל עומדים מאחוריהן גורמי מודיעין. כלומר, מדובר בפעולות הכוללות היבטים חשאיים. לפיכך קיימים מבצעי השפעה הכוללים השפעה על תכנים בלבד, למשל באמצעות דיפלומטיה ציבורית, אשר אינם נבחנים במאמר. חשיבות ניתוח התופעות שעליה מצביע המאמר היא כפולה. הדבר עשוי לשרת גורמים המעוניינים להשפיע על מערכת יריבה ואשר נדרשים לשכלל את יכולת התקיפה שלהם, ולצד זאת הדבר עשוי לסייע בידי אלה הנדרשים להיערך ולסכל מתקפות מסוג זה, המהוות אתגר ראשי לתהליכים דמוקרטיים, ובראשם מערכות בחירות. בראשית המאמר סקירת ספרות המעלה את המושגים המרכזיים בשיח על אודות מבצעי השפעה בסייבר ולוחמת מידע. הפרק השני מסווג את התקיפות שמצאנו לפי מספר אשכולות, שהשוני ביניהן הוא התמהיל בין תקיפות טכנולוגיות לבין המעטפת הנדרשת מבחינת שליטה בתכנים. הפרק המסכם מציג ניתוח של ההבדלים בין התופעות השונות.

פרק ראשון: סקירת ספרות

התפתחות מבצעי ההשפעה בסייבר, בייחוד ברשתות החברתיות, טומנת בחובה הזדמנויות נרחבות למינוף הטכנולוגיה ככלי להעברת מסרים להמונים. בעוד שהדיון על מתקפות סייבר שתכליתן שיבוש מערכות מחשוב ותשתית מוכר בשיח הציבורי והמקצועי, ניתן להבחין באופיין ההיברידי והייחודי של המתקפות למטרות השפעה, אשר מבוססות על שילוב של תקיפות סייבר ומניפולציה של תכנים.

לוחמת מידע בעידן הקיברנטי

המניפולציה של מידע לתכליות מדיניות, כלכליות וביטחוניות נפוצה לאורך ההיסטוריה האנושית. מבצעי ההשפעה בעבר נעזרו בכלים שונים לערעור הביטחון האישי והתמיכה הציבורית במוסדות המדינה ולפגיעה בלכידות החברתית.[3] לעומת זאת, התחזקות שחקנים לא-מדינתיים והתפתחות המרחב הקיברנטי הובילו להתפתחותה של לוחמת מידע היברידית המשלבת בין

היבטים קינטיים, פוליטיים, תרבותיים וטכנולוגיים.[4] כנגזרת מכך, מבצעים המזוהים עם לוחמת המידע כוללים גם שימוש בפיתוחים טכנולוגיים, אלמנטים של תחבולה והונאה וכלים של המדיה הדיגיטלית הגלויה.[5]

האמצעים שבהם משתמשות מדינות לביצוע מניפולציה במידע והיעדים שלהן מגוונים ותלויים בתרבות האסטרטגית של אותה מדינה. כך למשל, דוקטרינת לוחמת המידע הרוסית מזוהה בטרמינולוגיה הצבאית כ'מאבק מידע'. מטרתה לשבש ולשתק את מאמציו המערכתיים של היריב על ידי השגת עליונות בתחום המידע ותהליכי קבלת ההחלטות. הדפוסים המרכזיים המזוהים עם מבצעי ההשפעה הרוסיים כוללים שימוש במרכיב רגשי, יצירת ספק וחוסר ודאות, פנייה באמצעות מסרים מגוונים וחיפוש חולשות חברתיות בצד הנתקף. לפיכך, מאבק המידע נעזר בכלים שונים, לרבות לוחמה פסיכולוגית, הטעיה, הונאה, מערכות לוחמה אלקטרונית, מתקפות סייבר ומערכי דיסאינפורמציה.[6, 7]

לוחמת המידע האיראנית מהווה נדבך מרכזי בפרדיגמה רחבה יותר, המבוססת על לוחמה פוליטית שאינה צבאית, נוכח נחיתותה של איראן בלוחמה קונוונציונלית ביחס לאויביה. מכון RAND מגדיר אותה 'לוחמה פוליטית', משמע לוחמה חסויה המשתמשת במרכיבי העוצמה המדיניים לשם השפעה על קבלת ההחלטות או על עיצוב המדיניות במדינת היריבה.[8] האמצעים שבהם משתמשת איראן כוללים דיפלומטיה ציבורית, מבצעי השפעה בסייבר ותקשורת אסטרטגית, אשר מסייעים לה להרחיב את השפעתה במזרח תיכון, לחזק את השפעת מאמציה הצבאיים ולתמוך בעקרונותיה האידיאולוגיים והדתיים.[9]

מהפכת הביג דאטה והבינה מלאכותית, שמשמעותה היא היכולת לעבד כמויות ענק של נתונים, מאפשרת לייעל את לוחמת המידע ולהשפיע על תודעת ההמונים בצורה רחבת היקף ומותאמת לקהלי יעד. גישתן של ענקיות הטכנולוגיה לנתוני עתק הופכת אותן לשחקניות מרכזיות במערכה על התודעה. לאותן חברות יש יכולת "לטרגט" (targeting) את קהל היעד ביעילות ובדיוק רב יחסית ולהכווין את התכנים שאליהם נחשפים המשתמשים, ומכאן נגזר מעמדן וכוחן כמתווכות תכנים וידע בעידן הרשתי. מבצעי השפעה על ציבורים גדולים נועדו לשנות את עמדותיו המוגדרות של ציבור מסוים, ולכן "הפצצת" מידע ושיבוש סביבת המידע בפלטפורמות המקובלות מקשים על הפרט להבין את המציאות שבה הוא חי ולגבש תוכנית פעולה רלוונטית. לפיכך, הצד התוקף מצליח ליצור יתרון יחסי במערכת התודעה הכוללת.[10]

נוסף לעיבוד נתוני עתק, לוחמת המידע המודרנית מצריכה הבנה של היתרונות שמתאפשרים על ידי המבנה הייחודי של המרחב הקיברנטי. בין המאפיינים הרלוונטיים ניתן לציין את הקושי לייחס תקיפה ואת האנונימיות המתאפשרת לתוקפים. יתרה מכך, ארכיטקטורת הרשת מובילה לקשיים רגולטוריים נוכח היעדר הירכיה מוצהרת ושימור ניטרליות הרשת, אשר יוצרת מעטה של אנונימית לגולשים ומאפשרת לגורמים המעוניינים להשפיע לנצל את מאפייני העולם הרשתי לטובתם.[11]

זאת ועוד, מבצעי ההשפעה במרחב הקיברנטי פונים לציבורים גדולים ונוטים לבצע שימוש במסרים גלובליים ואוניברסליים לעיצוב השיח הציבורי, אך תוך שימת דגש על יצירת תכנים

מותאמים אישית לכל גולש. הכוונה האישית למשתמש יוצרת מודוס אופרנדי ריאקטיבי המבסס שיח בין התוקף לבין מושאי ההשפעה, אשר תוצאתו אינה תלויה בלעדית בתוקף. לפיכך, הטמעת דפוסי תקיפה דרך פלטפורמות רשתיות המונגשות לכלל הציבור מעידה במידה רבה על שאיפת התוקף להרחיב את קהל היעד, לאפשר לקורבן "לקחת חלק" ואף ליצור מכפיל כוח למתקפה. לראיה, ניתן לציין מתקפות למניעת שירות או חולשות תשתיתיות בתוך המערכות שנועדו להשבתת מערכות מחשוב בלבד או לגרימת הרס, כפי שעלה עם נוזקת "סטקסנט" באיראן בשנת 2011. זאת בשונה ממתקפות שמבוססות על עירוב מושא ההשפעה באמצעות שיח במדיה החברתית או על החדרת תכנים והפצתם במדיה החברתית, כפי שעלה במעורבות הרוסית בבחירות בשנת 2016.

בהמשך להיבט הריאקטיבי של המתקפה, חשוב לציין את השפעת ההיבט הכמותי במרחב הקיברנטי נוכח האפשרות לטרגט ציבורים גדולים ביעילות ובדיוק ברשתות החברתיות. כנגזרת מכך, הדהוד תכנים במבצעי השפעה מקוונים והדגשתם יוצרים מעין אפקט דומינו, שבו משתמש יחיד נחשף לתוכן רלוונטי ומותאם אישית עבורו. בהמשך, בוחר המשתמש כיצד להגיב לתוכן בפעולה וולונטרית. מנעד התגובות נע בין כתיבת תגובה, שיתוף או ציוץ של אותו התוכן, כך שהוא נשמר בצורה מסוימת בקרב קהל החברים האינטרנטי של אותו משתמש. לפיכך, מתן חופש פעולה למשתמש בתגובה למבצע ההשפעה מבסס את אופייה הדינמי של לוחמת המידע במרחב הקיברנטי, אשר תלויה בהדהוד המתקפה ובתְחזוקה על ידי קורבנותיו.

הדיון על עירוב הקורבן במבצעי ההשפעה במרחב הקיברנטי מזכיר את המתקפות המסורתיות המבוססות על הנדסה חברתית, אשר להן נודעות השלכות תודעתיות ופסיכולוגיות בספרות על אודות ניצול הפגיעות האנושית.[12,13] אולם בשונה מהנדסה חברתית, אשר מוכוונת על ידי התוקף מלמעלה למטה (Top-Down) לשם סיוע למבצעים המקוונים המסורתיים, אופיים של מבצעי ההשפעה בסייבר תלוי בתגובת הקורבן ובאופן התייחסותו לדפוס התקיפה, ולכן יש שיגדירו אותם כשילוב בין הכוונה מעלה-מטה לבין מטה-מעלה. לפיכך, האפשרות לסכל את מבצעי השפעה במדיה החברתית היא מורכבת, שכן יש צורך לעצב או למנוע את פעולות קהל היעד הנתקף, ולא רק את פעולות התוקף.[14]

מבצעי השפעה בסייבר

נקודת מבט מודרנית על התנהגותם של שחקנים מדינתיים ולא-מדינתיים במרחב הקיברנטי מדגישה את נקודת החיבור בין דפוסי תקיפה טכנולוגית לבין המערכה על התודעה, וזאת על ידי מבצעי השפעה מבוססי תוכן שעשויים לשרת מטרות שאינן טכנולוגיות. מקובל בספרות להבחין בין סוגי מתקפות סייבר בהתאם למטרותיהן - מתקפות CNA (Computer Network Attack) שגורמות נזק ומניעת תפקוד למערכות מחשוב, ומתקפות CNE (Computer Network Exploitation) שמיועדות לגניבת מידע ולריגול. דפוס תקיפה נוסף הוא מבצעי השפעה בסייבר, שמזוהה בתור CNI (Computer Network Influence) או בתור Cyber Influence Operations.[15,16] הגדרתם של החוקרים ברנגטו וונדאל למושג היא:

"Operations which affect the logical layer of cyberspace with the intention of influencing attitudes, behaviours, or decisions of target audiences".[17]

נוכח הגדרה זו, יש המזהים את דפוס התקיפה בהקשר של השפעה על טרנדים חברתיים ועיצוב הדעה הציבורית כגון בחירות, וזאת דרך ביסוס מניפולציה במידע והפצת מידע כוזב.[18] לפיכך, מטרת ההשפעה בסייבר היא לעצב את תודעת היריב באמצעים שאינם קינטיים ולזרוע תחושות של פחד, אי-ודאות וספק אצל הקורבן.[19,20,21]

מחקר נוסף בסוגיה יצר הבחנה בין מתקפות סייבר וריגול לבין מבצעי השפעה בסייבר, וציין כי האחרונים מהווים איומים ביטחוניים מבוססי תוכן, שמשלבים ניצול של המרחב הדיגיטלי על מנת להשפיע על התודעה והקוגניציה האנושית. כותב המאמר, בארי סנדר, הרחיב את תחולת המושג לכל פעולה שמבוצעת על ידי מדינה או שחקנים שהתנהגותם מזוהה עם מדינה על פי המשפט הבינלאומי, כאשר הם מנצלים מידע במרחב הקיברנטי על מנת להשפיע על השיח הפוליטי במדינה זרה.[22]

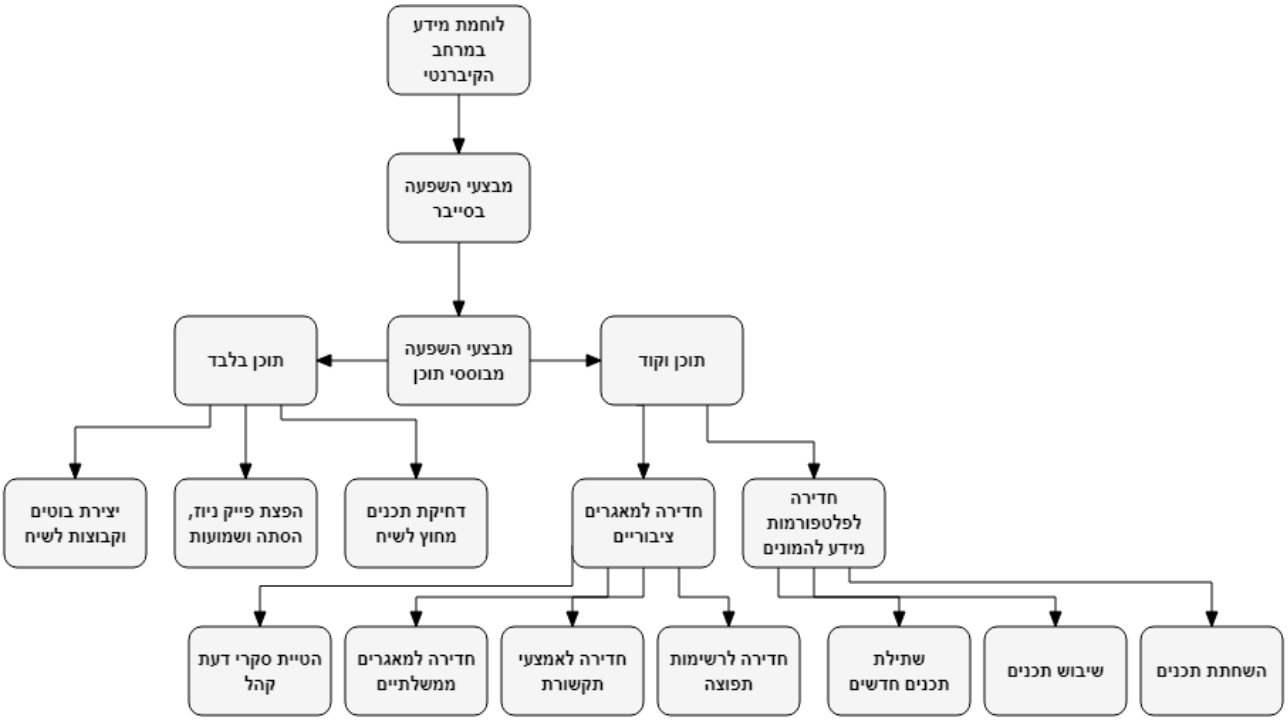
סנדר מוסיף כי עליית הרשתות החברתיות העלתה את שיעור מבצעי ההשפעה בסייבר, כפי שעולה בפרשת המעורבות הרוסית בבחירות האמריקאיות בשנת 2016. נובע מכך, שניתן להבחין בהתפתחות הייחודית של מבצעי ההשפעה בסייבר בעידן הרשתות החברתיות, אשר העצימה את היכולת המבצעית והתודעתית של אותם מבצעים בהיבט הכמותי והתוכני. לפיכך, אם בעבר מבצעי ההשפעה בסייבר נאלצו להסתמך על אמצעי התקשורת והמדיה המסורתיים ועל נגישות מוגבלת לקהל היעד שצורך את אותו אמצעי, הרי אבולוציית תקשורת ההמונים והאפשרות לטרגט משתמשים במדיה החברתית שינו את כללי המשחק במערכה על התודעה. אם כן, ניתן לראות במדיה החברתית תשתית שמרחיבה את האפשרויות לעריכת מבצעי השפעה, והופכת את מתקפות ה-CNI לנפוצות ומונגשות לציבורים גדולים במידה משמעותית יותר מזו שהייתה לפני פרוץ הרשתות החברתיות.

הזיקה הפנימית בין המתקפות עולה באפיון המסורתי של מתקפות ה-CNE. בעידן הרשתי, אופי המידע הנאסף על היעד הוא מגוון, כגון מידע טכנולוגי להבנת מבנה רשתות המחשבים, מידע למימוש פעילות אקטיבית עתידית כמו פריצה לחשבונות אישיים או מידע תוכני כגון גניבה של סודות מדינה או מידע מסחרי. לפיכך, יש שיראו בחלק ממתקפות ה-CNE פוטנציאל להשפעה ולהעברת מסרים, בדומה למתקפות ה-CNI. הרציונל של דמיון בין המתקפות הוא שלאחר חשיפת המידע הרגיש מתחזקות תחושות של חדירות ופגיעות אצל הקורבן, אשר ניתנות לניצול ולחשיפה לכלל על ידי התוקף ועשויות לשמש כלי ליצירת השפעה.[23] מעבר לכך, ניתן לציין מתקפות CNE שמטרתן הבלעדית היא חשיפה, ולכן תכלית הריגול אינה רק השגת הידע כשלעצמו אלא חשיפה של מידע רגיש ומניפולציה שלו על ידי התוקף.

בהתאם לאמור לעיל, עצם האבחנה בין מתקפות הסייבר השונות, המבוססות על תקיפת סייבר, לבין מבצעי השפעה בסייבר היא מעורפלת, ויש שיאמרו כי היא הולכת ומְטשטשת נוכח התחזקות המערכה על התודעה. אם כן, ניתן לומר כי החלוקה המסורתית לדפוסי המתקפות על פי מטרותיהן משתנה בעידן הרשתי, ומתווספות מתקפות רב-שלביות. במתקפות אלו, פעילות של

איסוף מידע וריגול יכולה לקדם מבצעי השפעה בסייבר. לא מן הנמנע שמתקפת CNA שתגרום נזק רב ביעד רגיש ומוכר לציבור תשמש אמצעי לקידום השפעה, בין בכוונה תחילה ובין במקריות. הדבר מעיד על יחסי הגומלין המתהווים בין מטרות התקיפה במרחב הקיברנטי, במסגרת מודל היברידי המשלב בין מתקפה מתווכת למתקפה ראשית להשגת יעדי התוקפים הראשוניים והדינמיים. הזליגה בין מטרות המתקפות השונות מעידה על ריבוי הדפוסים הטכנולוגיים האפשריים לתוקף לצורך השגת מטרותיו הראשוניות, ואף על ניצול הזדמנויות שאינן מתוכננות ותלויות בהשתלשלות התקיפה.

איור 1 כולל מיפוי של התפתחות ההמשגה של מבצעי השפעה מבוססי תוכן, בהתאם לשינויים שחלו בדפוסי התקיפה במרחב הקיברנטי.



איור 1 - קטגוריזציה של מבצעי ההשפעה מבוססי טכנולוגיה

כלים, שיטות ודפוסי פעולה

פייקובסקי ומתניה[24] מתייחסים לאופיים של מבצעי השפעה מקוונים בתור נקודת השקה של מבצעים פסיכולוגיים, המערכה בסייבר ומלחמות המידע, שנועדו להשפיע על מקבלי ההחלטות על ידי יצירת מעטפת של מידע ונרטיבים. מאמרם עוסק במתקפות סייבר מודרניות, המשמשות לשיבוש תהליכים חברתיים וערכיים על ידי מתקפות המשלבות בין תוכן עוין לבין מתקפת סייבר באמצעות כלים טכנולוגיים שונים.

נקודת מבט צרה יותר על לוחמת המידע במרחב הקיברנטי עשויה להתייחס לדפוסי התקיפה הרלוונטיים לשימוש. לראיה, ישנן תקיפות שמאפשרות שתילת תכנים ברשתות חברתיות והשתלטות על דפי האינטרנט המוצגים לגולשים. כמו כן, השימוש בבוטים ובאוואטרים לקידום

מבצעי השפעה מאפשר העלאת תכנים או שיבושם ברחבי הרשת, וזאת בזכות האוטומציה ותפוקתם הרבה ביחס למשתמש אנושי נורמטיבי.[25] יתרה מכך, תוקפים יכולים לפרוץ לאתרים ולחשבונות לגיטימיים ולשבש את המידע בהם, או להפיץ מידע אלטרנטיבי. סוגיית המעורבות בתכנים מעלה את תופעת הדיסאינפורמציה והפייק ניוז, שמתעצמת במרחב הקיברנטי, וזאת בדגש על פרסום ברשתות החברתיות או על ידי הדלפות מכוונות לפלטפורמות מקוונות. המידע המטעה נועד לחזק נרטיבים פוגעניים ומסיתים, ולכן השימוש בפלטפורמה מקוונת מסייע להפיץ תכנים לקהלים נרחבים.[26,27]

פרק שני: מבצעי השפעה מבוססי מתקפות סייבר טכנולוגיות בשילוב עם מניפולציה על תכנים

קמפיינים ופעולות סייבר התקפיות יכולים ליצור את אפקט ההשפעה, הן במכוון והן כאפקט הרתעתי לאחר יצירת פעולת השיוך (Attribution). פעולת שיוך זו כוללת את החיבור בין הפעולה ההתקפית לבין התוקף עצמו, בין הצבעה על גורם התקפי בעל שם מתוך עולם הסייבר, אשר לעיתים מזוהה עם מדינה או עם בעל עניין בפעילות מסוג זה, ובין הפניית אצבע מאשימה כלפי העומדים מאחורי ביצוע התקיפה. בשונה מאפקט השפעה במכוון, אפקט ההרתעה המאוחרת הוא דווקא הטריוויאלי יותר, שכן הוא משלב בתוכו את ההרתעה המושגת לרוב מפעילות התקפית שכזו.

ניתן לחלק את השימוש בפלטפורמה הדיגיטלית למטרות זדוניות לשני קטבים עיקריים. הקוטב הראשון כולל בתוכו תקיפות סייבר "קלאסיות" – שימוש בכלים שנכתבו למטרות התקפיות או ניצול חולשות במערכות קיימות על מנת להסב נזק כלשהו לנתקף כגון גניבת מידע, הרס, שיבוש תהליכים וריגול. הקוטב השני כולל בתוכו את ניצול המרחב הווירטואלי לצורך מבצעי השפעה. מבצעים אלו מתבססים, בעיקרם, על התכנים ופחות על התחכום הטכנולוגי. בשנים האחרונות נוצר ממשק בין מתקפות הסייבר הקלאסיות לבין מבצעי ההשפעה. אנו מזהים שלושה סוגים עיקריים של שילוב בין תקיפות סייבר לבין תוכן, שעליהם נרחיב בפרק זה.

בפרק זה נציג מספר מרכיבים של מבצעי השפעה הכוללים מתקפות סייבר שונות. נתחיל בסקירה קצרה על מתקפות סייבר "קלאסיות", כאלו שהממד ההשפעתי שלהן אינו חלק ממטרות התקיפה או מכלי התקיפה אשר באים לידי ביטוי בתקיפה. תקיפות אלו מכונות על ידינו תקיפות מבוססות הרתעה מאוחרת – מבצעי השפעה שבהם אין כל תוכן, אך הפעילות מייצרת אפקט של הרתעה מאוחרת בקרב הנתקף והציבור הכללי. לאחר מכן נעבור אל מבצעי השפעה הכוללים תשתית קיברנטית מסוימת, נעבור דרך מבצעי השפעה בהובלת גורמים הַאקטיביסטים,[28] אירועי מתקפות סייבר המייצרים רכיבי השפעה ולבסוף חיבור בין פעילות סייבר התקפית לבין תוכן זדוני.

מתקפות סייבר "קלאסיות", בדגש על מתקפות CNE ו- CNA

מתקפות מסוג זה מהוות נקודת פתיחה למבצעי תקיפת סייבר שייצרו ממשק עם מבצעי ההשפעה באמצעות תכנים זדוניים. מתקפות אלו לרוב אינן מיועדות באופן ישיר ליצור השפעה תודעתית כלשהי על הנתקף, אלא לפגוע בו באופן ישיר או עקיף באמצעות השגת נגישות או פגיעה כלשהי בנכס הטכנולוגי שלו.

ניתן להצביע בהקשר זה על שני אירועים משמעותיים אשר הֻקנו מעמד לתוקף שהואשם בתקיפה. האירוע הראשון מסוג זה הוא תקיפת אתר העשרת האורניום האיראני בנתנז באמצעות תולעת המחשב "סטקסנט", אשר על פי דיווחים זרים, בין היתר של אדוארד סנודן, בוצעה על ידי ארצות הברית וישראל.[29] אירוע נוסף הוא מתקפת Not Petya, שבה הותקפו אלפי חברות אוקראיניות בנוזקת (malware) הרס שהתחזתה לנוזקת כופר. תקיפה זו, שנמשכה יומיים והביאה לנזק רב ברחבי אוקראינה, שויכה למודיעין הרוסי (GRU), על פי שירותי הביטחון האוקראיניים (SBU), חברת ESET וה-CIA.[30]

מבצעי תודעה והשפעה בקמפיינים קלאסיים של דיסאינפורמציה

<u>מבצע דיסאינפורמציה גלובלי - מערך Global Disinformation Operation (GDO)</u>

מדינה בולטת בתחום של הפצת דיסאינפורמציה באמצעות אתרי חדשות כוזבים היא איראן. בשנת 2018 נחשפו שלושה מערכי דיסאינפורמציה עתירי ממדים בהכוונה איראנית, אשר לכל אחד מהם יעד תקיפה אחר ודפוסי פעולה שונים.

המערך הראשון בשם Ayatollah BBC פעל במשך שש שנים ומטרתו הייתה להשפיע על הציבור באיראן, להפיץ מידע כוזב על כלי תקשורת מערביים המשדרים בשפה הפרסית ולערער את הלגיטימיות שלהם בקרב הציבור באיראן. למערך זה היו שתי זרועות: רשת אתרים המתחזים לשורה של כלי תקשורת מערביים הפועלים באיראן ומשדרים בשפה הפרסית כדוגמת BBC, Voice of America ורדיו "פרדא" - שלוחה של "קול אירופה החופשית" - הממומן על ידי הקונגרס האמריקאי.

באמצעות אתרים אלו ניסתה איראן לערער את הלגיטימיות של אותם כלי תקשורת, להפחיד את הקוראים ב"סימונם" על ידי המשטר ובהטעיה. חלק ניכר מאותם כלי תקשורת שאליהם התחזו צונזרו על ידי מנועי החיפוש האיראניים (כדוגמת yooz ו-parsijoo), כאשר האתרים המזויפים נותרו על כנם.[31] המערך כלל גם רשת אתרים מזויפים המתחזים לכלי תקשורת עצמאיים שאינם מוכרים, אשר הפיצו דיסאינפורמציה מסיתה נגד כלי התקשורת שאליהם התחזו, ובה בעת הסתה ממשית נגד העיתונאים המקומיים שעובדים באותן רשתות.

מערך שני הופעל מייד לאחר ההתנקשות בעיתונאי הסעודי ג'מאל ח'אשוקג'י. במסגרת מערך זה פעלה איראן כדי להשפיע על דעת הקהל הסעודית לאחר רצח העיתונאי ולהתסיס את העם נגד משטרו.

בסוף שנת 2018 נחשף מערך עתיר ממדים שהפעילה איראן במטרה להפיץ דיסאינפורמציה אשר תשרת את מטרותיה, באמצעות רשת אתרים מזויפים שהפעילה בכל רחבי העולם (GDO).[32] המערך פעל ברחבי העולם במשך שש שנים ללא הפרעה והצליח להגיע לעשרות ואף למאות אלפי אנשים ברחבי העולם. מערך זה כלל עשרות ואף מאות אתרי פייק ניוז ודיסאינפורמציה שהופעלו על ידי איראן. כל אתר כזה התחזה לגוף תקשורת פיקטיבי במדינת היעד שאליה כוונו מאמצי איראן. האתרים עודכנו בתדירות גבוהה ושוטפת והועלו אליהם עשרות כתבות חדשות מזויפות,

המשתמשות במתודות שונות של הפצת דיסאינפורמציה. אחת השיטות הללו נקראת false connection ובה מחברים מפיצי המידע הכוזב כותרת מזויפת, אמצעים ויזואליים ואמצעים טכנולוגיים אל תוכן שאינו תואם את האמצעי.

כל אתר כלל לוגו משלו, לעיתים אף לוגו לכל שפה. למשל האתר Yemen Press כלל לוגו שונה לגרסת האתר בערבית, בפרסית ובאנגלית. כמו כן הוקמו עבור המערך עמודים המזדהים בשם כלי התקשורת המזויף ברשתות החברתיות השונות, רשת ענפה של פרופילים מזויפים המפיצה את כתבות המערך ברשתות השונות ואפליקציות ייעודיות. נוסף על כך, בחלק ניכר מהאתרים המזויפים נכתבה כתובת פיזית אשר לכאורה נמצאה בה המערכת. במחקר שביצעה מערכת רויטרס על אותן כתובות נמצאו מקומות שאינם קיימים, או שקיים בהם דבר שאינו מערכת עיתון, למשל מזבלות.[33] בשונה מהמערכים הקודמים שצוינו לעיל, מערך זה כלל רכיבים רבים מאוד שתכליתם הייתה להַתְמים את האתרים (ליצור להם מראה תמים ואמין).

מכאן ניתן ללמוד על מערכי דיסאינפורמציה באיכות גבוהה שני דברים עיקריים:

- נדרשים אמצעי הסוואה רבים על מנת להפעיל אתר דיסאינפורמציה אחד, כאלו שיציגו מראה "תמים" לנחשף לדיסאינפורמציה וייתנו תוקף אמין לאתר. ככל שנדרשת אמינות גבוהה יותר, יש להשקיע אמצעים רבים יותר להסוואה כאתר תמים.
- כדי להפעיל מערך דיסאינפורמציה ברמה גבוהה נדרשים הן משאבים טכנולוגיים להפעלת האתר ואמצעי הַתְממה והן משאבים שאינם טכנולוגיים, ליצירת המסר והתוכן הרלוונטי.

במסגרת המערך הקימו האיראנים רשת גופי תקשורת פיקטיביים לצורך הפצת המידע הכוזב, ולא התחזו לגופי תקשורת קיימים. למרות ההיקף הרחב והשימוש בתשתיות רבות, בין היתר רשתות חברתיות ואף אפליקציות ייעודיות לאותם אתרים, לא נראה כי איראן פעלה במערך זה גם כדי לפגוע בנכסיהם של צרכני המידע, אלא רק לחשוף אותם למידע כפי שהיא מבינה אותו או רוצה לקדמו.

מתקפות CNA ו-CNE כתשתית למתקפת CNI על בסיס תוכן אמיתי

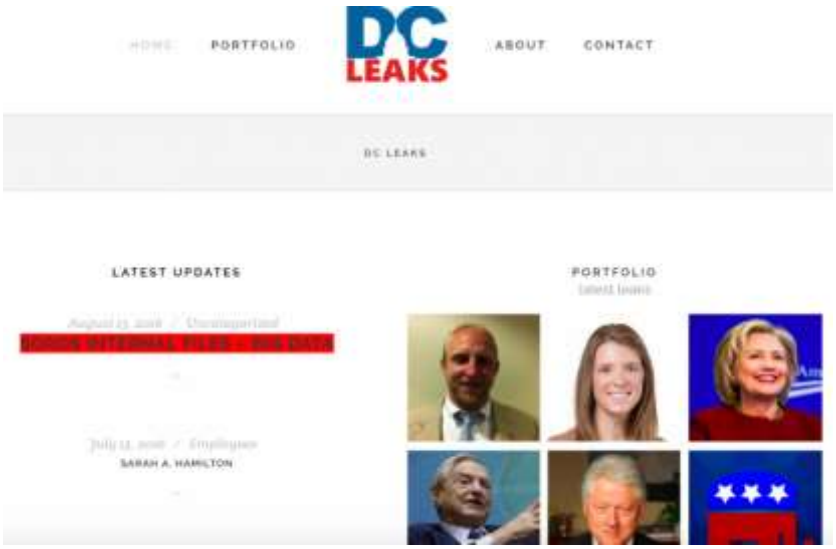
עתה נדון בשילוב מתקפות סייבר הכוללות רכיב תוכני: מתקפות CNA ו-CNE כתשתית למתקפות CNI בהתבסס על תוכן אמיתי, מתקפות CNA ו-CNE כתשתית למתקפות CNI בהתבסס על תוכן מזויף ושילוב בין תקיפות CNI לבין תקיפות CNE ו-CNA לכדי מבצע אחד העונה על מספר מטרות.

<u>בחירות 2016 בארצות הברית</u>

המתקפה על מטה ועידת המפלגה הדמוקרטית (DNC), שהתבצעה ככל הנראה מינואר 2015 ועד החודשים שקדמו ליוני 2016, היא דוגמה לשילוב בין ריגול והשפעה. בשונה מהתקיפות הקודמות, אשר התאפיינו בעיקר במתקפה עוצמתית שמטרתה פגיעה בתשתיות ולא יצירת השפעה, המתקפה על ה-DNC היא אבן דרך משמעותית בשילוב בין מתקפות סייבר למבצעי השפעה.

במסגרת תקיפה זו פעלה קבוצת תקיפה בשם Fancy Bear (הנקראת גם APT28),[34] המזוהה עם ה-GRU הרוסי, על מנת להשתלט על נכסים דיגיטליים של מטה ועידת המפלגה הדמוקרטית כדוגמת שרתי הדוא"ל שלהם. החדירה למערכות המחשוב של ה-DNC הייתה באמצעות Spear-Phishing שכלל מתודות שונות של הנדסה חברתית ונשלח לעובדים ספציפיים ב-DNC. כך לדוגמה, אחר מהדומיינים שהוקמו לצורך תקיפת עובדי ה-DNC הוא misdepatrment[.]com. ניתן לראות כי סדר האותיות הוחלף בצורה המקשה על הנתקף לשים לב לכך.

אחד העובדים בוועידה, אשר נלכד בתרמית של הקבוצות הרוסיות, הדביק בנוזקה את מערכת המחשוב של ה-DNC ואפשר לתוקפים לגשת למידע חשאי, בעיקר לשרתי דוא"ל של ועידת המפלגה הדמוקרטית שכללו עשרות אלפי התכתבויות. לאחר שנגנב המידע הרלוונטי הוא הודלף באמצעות גורם עלום בשם Guccifer 2.0 באתר הנקרא DCleaks, וכן באמצעות אתר ייעודי שהוקם על ידי התוקפים לצורך הדלפת המידע.[35]



איור 2: צילום מסך מתוך אתר DCleaks, שהיה האתר המרכזי שבו השתמשה הקבוצה על מנת להפיץ את המידע על ועידת המפלגה הדמוקרטית[36]

לאחר כחודש של הדלפות בהיקף מצומצם, גורמים בזהות בדויה יצרו קשר עם אתר WikiLeaks והעבירו להם 19,252 תכתובות דוא"ל ו-8,034 צרופות. אלו פורסמו ב-22 ביולי 2016 לעיני כול. המידע עצמו כלל עשרות תכתובות רגישות הרלוונטיות לפעילות המפלגה, אך גם מידע כללי שלא היה רלוונטי לאיש. גם בלי לבחון את תוכן המסמכים, מתקפה זו יצרה אפקטים משמעותיים בתחום ההשפעה:

- ההדלפות הראשוניות פגעו בשמה הטוב ובמעמדה של מטה ועידת המפלגה הדמוקרטית – "כיצד יכולה המפלגה לנהל מדינה אם אינה מסוגלת לאבטח את המידע שלה?" שאלות כאלו ואחרות הועלו על ידי ראש המפלגה הרפובליקנית טראמפ באומרו "רוסיה, אם את מקשיבה, אני מקווה שתוכלי למצוא את 30 אלף המיילים המחוקים שחסרים".

- חרף הכחשות גורפות מהקרמלין, אשר כללו גם את הצהרתו של דובר הקרמלין דימיטרי פסקוב, שטען כי "אני דוחה לחלוטין את האפשרות שהממשלה [של רוסיה] או גורם מהממשלה היה מעורב בכך [בפריצה או הדלפת תכתובות הדוא"ל]". [37]

- הפריצה מיצבה את רוסיה כגורם בולט ביותר במרחב הסייבר וכגורם המוביל את הדיסאינפורמציה העולמית. מאז הבחירות ניתן לזהות עיסוק הולך וגובר בקבוצות התקיפה הרוסיות ובפרט 28APT בקרב חוקרי סייבר ועיתונאים מרחבי העולם, וכמו כן ניתן לראות את מיצובה של רוסיה בחזית הדיסאינפורמציה העולמית.

בחינת שרת שמות של הקבוצה, אשר נחשף, באותה עת מעידה על מאמצים מצד רוסיה להכין תשתיות לתקיפת סייבר, ובה בעת היא יכולה להעיד גם על ניסיונות להפיץ באמצעותם דיסאינפורמציה.[38] כך לדוגמה, הדומיין vice-news[.]com שמקושר לתשתית התקיפה על ה-DNC יכול לשמש אתר להפצת דיסאינפורמציה, בעוד שהדומיין mail.hm.qov[.]hu מתחזה לאתר של ממשלת הונגריה וככל הנראה שימש אתר פישינג,[39] אולי למקורביו של ג'ורג' סורוס אשר הופיע תכופות באתר זה.[40] כלומר, קבוצת Fancy Bear פעלה במקביל הן מבחינת מתקפות סייבר קלאסיות והן מבחינת מתקפות ששילבו תוכן זדוני.

כמו כן יש לציין כי קבוצה זו לא פעלה באמצעות אתר בלבד. ברשת טוויטר, לדוגמה, הוקם חשבון ייעודי ל-DCleaks שמטרתו יכולה להיות כפולה – מצד אחד להפיץ את האתר לכמה שיותר אנשים ומצד אחר לייצר מצג נוסף של אמינות לאתר.

איור 3 : ציוץ מתוך חשבון הטוויטר של DCleaks העוסק במיליארדר ההונגרי ג'ורג' סורוס[41]

בדפוס פעולה זה:

- עיקר השילוב בין תקיפות סייבר לתוכן זדוני היה בחיבור שבין גניבת מידע באמצעים קיברנטיים כדוגמת נוזקות ואתרי פישינג, חילוץ המידע על ידי התוקף ושימוש במידע זה באופן פומבי (ואף בלתי מסונן), על מנת להשיג מטרות הידועות לתוקף.

- ניתן לראות כי להתקפה פשוטה זו הייתה השפעה כלל-עולמית, הן על הבחירות - במידה מועטה שאולי לא ניתן לבחון בכלים מדידים, אך בהכרח על תפיסת איום ההתערבות הקיברנטי במערכות בחירות שונות.

- יש לציין כי במתקפות מהסוג זה לרוב אין כמעט כל חשיבות לתוכן הנגנב, אלא לעצם גניבתו והדלפתו. מבצעים מסוג זה יוצרים בקרב מתנגדיו של הקורבן את הרושם כי הוא פגיע, אינו יודע לשמור על נכסיו, סחיט ואף אינו אחראי וכשיר להנהגה. זאת משום שהיקף החומרים הגדול אינו מאפשר לציבור הרחב לסקור באופן אובייקטיבי את כולו, אלא רק לדון בעצם ההדלפה.

מתקפות CNA ו-CNE כתשתית למתקפות CNI על בסיס תוכן מזויף, מתריס או כזה שנבחר בקפידה

<u>קבוצת האקטיבסטים טורקים</u>

אירוע נוסף המתאפיין בפעילות האקטיבסטית נגד ישראל, אשר נראה כי מטרתו הייתה ליצור הדים דווקא בסביבת התוקף, הוא מתקפות על ישראל מצד קבוצת פצחנים טורקים הנקראת "אילדיז טים" (ayyıldız tim) ומזדהה כ"צבא הסייבר של טורקיה".[42] במסגרת מתקפות אלו פעלה הקבוצה ליצירת הישגים תודעתיים למתקפות ושילבה בין נוזקות, שמטרתן לגנוב פרטי התחברות לאתרים שונים וביניהם טוויטר, לבין שימוש בחשבונות הפרוצים על מנת להביך את הנתקפים או לפרסם בשמם הודעות תמיכה שונות בממשל הטורקי. כך לדוגמה, חשבון הטוויטר של המנכ"ל לשעבר של משרד החוץ הישראלי דורי גולד נפרץ על ידי הקבוצה באמצעות מתקפת Spear-Phishing שכללה נוזקה.[43]

איור 4 : הודעת הפריצה לטוויטר של דורי גולד על ידי קבוצת "אילדיז טים" הטורקית

הקבוצה ניצלה את חשבונו של גולד כדי לצייץ ממנו – במשך תקופה קצרה – מסרי תמיכה בטורקיה ועמדות אנטי-ישראליות. במסגרת גל התקיפות הללו פעלה הקבוצה גם לפגוע בעיתונאים טורקים המתגוררים במדינות אחרות, כדוגמת עיתונאי חברת פוקס ניוז. השילוב בין מתקפת הסייבר למסרים הכוזבים שהופצו באמצעות גישה לחשבונות הנתקפים הוא אופן נוסף של שילוב כזה ושל מבצע השפעה המשלב תקיפת סייבר ונוזקות.

תקיפה כזו מחייבת היכרות מוקדמת עם הגורם המשמש פלטפורמה להשפעה על דעת הקהל. במקרה שהוצג לעיל הופץ מסר עוין בחשבון של דורי גולד, אשר כלל אך ורק את המסר עצמו (המסר המזויף והמתריס). פעולה זו מאפשרת לתוקפים להפיץ את רעיונותיהם ודעותיהם בקלות. לעומת זאת, הנזק היה מינורי יחסית, שכן בעת שחזור החשבון ו/או דיווח לרשת החברתית הרלוונטית - התוכן יימחק מהרשת.

ההצלחה המרכזית בהפצה של תוכן מסוג זה היא עצם היכולת להפיץ את התוכן, ולא התוכן עצמו. במקרה אחר בקמפיין של הקבוצה היא הפיצה צילום מסך מתוך עמוד ההודעות הפרטיות של פרופיל אחד בלבד מבין הפרופילים הנדונים. צילום מסך זה הוכיח כי אחד הנתקפים, אשר נחשב מקורב לבנו של נשיא ארצות הברית לשעבר דונלד טראמפ, ואף תמך בנשיא בפומבי במסגרת תפקידו כשדר Fox News, השתיק את בנו של הנשיא בחשבון הטוויטר שלו כך שלא יראה הודעות אשר מתקבלות ממנו. במקרה זה התוכן עצמו לא היה מזויף, אך הוא נבחר בקפידה כדי להביך את המותקף.

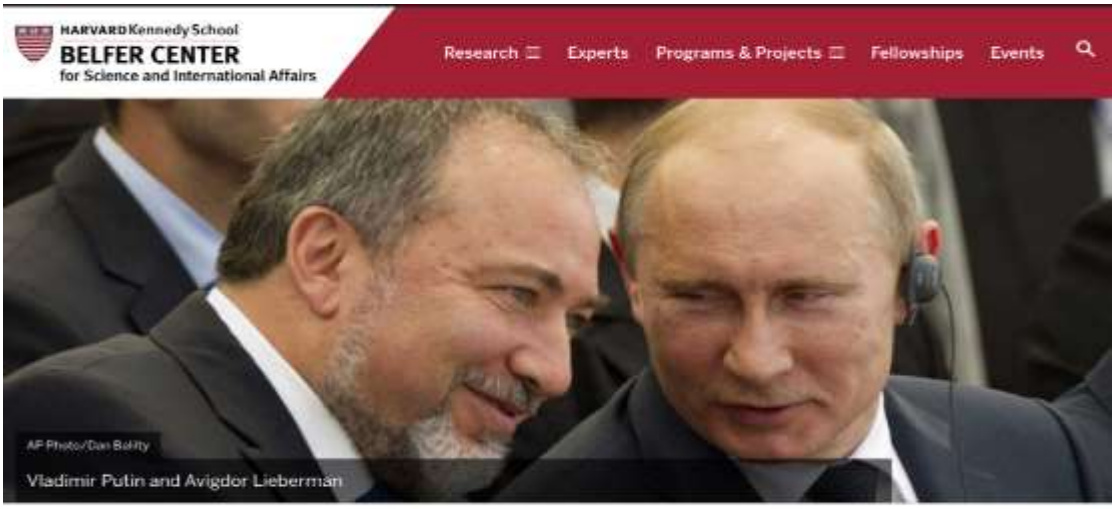
מתקפות CNI משולבות במתקפות CNA/CNE

בשנת 2019 נחשף מערך איראני המכונה "Endless Mayfly".[44] במסגרת הדוח שהופץ על המערך נסקרו שני אירועים שונים: האחד, מערך הדיסאינפורמציה הכלל-עולמי (GDO) שנדון לעיל; והשני, מערך דיסאינפורמציה שכלל בתוכו אתרים המתחזים לאתרי תקשורת לגיטימיים בכל העולם כדוגמת אל-ג'זירה, הארץ, ה-Independent, RT, הגארדיאן ועוד. אתרים אלו מזוהים כ-inauthentic website ו-inauthentic personas, בדומה לניסוח שבו בוחרת חברת פייסבוק להשתמש כאשר היא מסירה פרופילים מהרשת החברתית שנועדו להפצת דיסאינפורמציה (מלבד היותם מזויפים).

במסגרת המערך נחשפו עשרות אתרים מתחזים שכללו את התוכן הזדוני. אתרים אלו כללו לרוב כתבה אחת בלבד המכילה את המידע הכוזב, כאשר שאר האתר הכיל במקרים מסוימים הפניה (redirect) לאתר המקורי, ואילו במקרים אחרים הציג הודעת שגיאה. מטרת הכתבות הפיקטיביות אשר הופיעו באתרים אלו אינה ברורה, אך מפרופיל הכתבות ניתן ללמוד כי הן עסקו בסוגיות שבראש סדר היום, וניכר כי האיראנים השקיעו מחשבה בפיתוח התוכן הזדוני ובמעקב שוטף אחרי הלך הרוח הפוליטי במדינת היעד. אי לכך, מטרתם של האתרים שכללו כתבה אחת בלבד אינה ברורה.

מרבית המקרים כללו התחזות איראנית לגופי תקשורת ובהם הופיעה כתבה פיקטיבית, לעיתים תוך ציטוט אנשים שלא אמרו מעולם את הדברים המיוחסים להם. כך לדוגמה, במסגרת המערך הוקם אתר המתחזה למרכז בלפר, השייך לאוניברסיטת הרווארד. האתר הוקם סמוך

להתפטרותו של שר הביטחון הישראלי דאז אביגדור ליברמן מתפקידו. באתר הופצה כתבה שציטטה נאום של ראש המוסד לשעבר תמיר פרדו, שלפיה ראש הממשלה דאז נתניהו רצה לפטר את שר הביטחון ליברמן עקב היותו מרגל לטובת המודיעין הרוסי - דברים שלא נאמרו מעולם על ידי ראש המוסד לשעבר. עם זאת, יש לציין כי אכן מספר ימים קודם לכן נאם פרדו במרכז בלפר, וכך ניתן לראות את הידע המעמיק של מפעילי מערך זה הן באירועים הפוליטיים בישראל והן בשיח הקיים ברשתות החברתיות, ואף ניתן ללמוד מכך כי המפעילים ניסו להשיג שעת כושר לפרסום הדברים – קרי, הופעתו של תמיר פרדו במרכז בלפר.[45]



SHARE

PRESS RELEASE – *Belfer Center for Science and International Affairs, Harvard Kennedy School*

Resignation or Dismissal? Ex-Mossad Chief Tamir Pardo Says Lieberman Dismissed by Netanyahu

November 14, 2018

On Thursday, November 8, 2018, the Belfer Center for Science and International Affairs host a seminar with Tamir Pardo, former Mossad President Tamir Pardo between 2011 and 2016, on "Developments in the Middle East." Mr. Pardo criticized Russia's policies in the Middle East, pointing out the delivery of S-300s to Syria as a destabilizing factor in regional security, and said that Israel is aware of Russia's disrupting policies, and Israel would not take permission from anyone for

האתרים הופצו באמצעות שיטות של "הנדסה חברתית", בעיקרן פנייה אישית לגורמים ספציפיים המזוהים עם אנשי תקשורת שונים מעיתונים מסוימים (בין היתר, עיתונים שאליהם התחזו במסגרת המערך). פלטפורמות ההפצה כללו פלטפורמות מסרים מיידים כדוגמת ווטסאפ והפצה באמצעות מדיות חברתיות שונות כדוגמת חשבונות מזויפים ברשת החברתית טוויטר. במהלך המחקר זיהו החוקרים שחשפו את המערך כי התוקפים הללו הקימו עמוד התחזות לטוויטר - הפלטפורמה המרכזית שבה הופץ המידע.

הפרופילים המזויפים השונים כללו גם הם שיטות התממה שונות ומרובות כדוגמת התחזות ל-"Political Analyst & Writer" בפרופיל שהתחזה לבחורה בשם Mona A. Rahman והפיץ מסרים נגד ממשלת ערב הסעודית. פרופיל זה ניסה לגרום לאנשים לצאת להפגין נגד הממשל הסעודי ברחבי לונדון, בעיקר לאחר רצח ג'מאל חאשוקג'י. מפעילי פרופיל זה נהגו לתייג בציוצים

שהופצו עיתונאי אמריקאי-סעודי בשם Ali AlAhmed. פרופיל נוסף אשר פעל בתשתית נקרא Bina Melamed והפיץ כתבות לעיתונאים באמצעות direct message ברשת טוויטר, או לחלופין תייג אותם גם כן בכתבות המזויפות או בפוסטים הקוראים לפעולה.

המערך פעל בארבעה שלבים מרכזיים. השלב הראשון התרחש בין אפריל 2016 לאפריל 2017 ובו הופצו מסרים ברשת טוויטר, בעיקר נגד ערב הסעודית, על ידי שש דמויות מזויפות אשר השתייכו לכאורה לארגון "Peace, Security, and Justice Community". השלב השני התרחש בין אפריל 2017 לאוקטובר 2017, ובו הוקמו מספר אתרים מתחזים שהופצו על ידי מספר דמויות נוספות, שניסו "לצוד" עיתונאיים ואקטיביסטים. השלב השלישי החל במקביל לשלב השני, ובו החלו מפעילי התשתית להפיץ אתרים מזויפים באמצעות תיוג של עיתונאים בתגובות לכתבות הללו, וכן ניסו לקדם את ההאשטג "#ShameOnSaudiArabia" ברשת טוויטר. בשלב הרביעי והאחרון, אשר בוצע מדצמבר 2017 ועד נובמבר 2018, החלו הפרופילים המזויפים ליצור קשר ישיר עם אותם עיתונאים. יש לציין כי לאחר הפצת התוכן הזדוני נמחק האתר המזויף ובוצעו שיטות הסתרה שונות כגון הפניה לאתר המקורי, וזאת על מנת לטשטש את עקבות התוקפים ולנסות להסוות את התקיפה.[46]

לסיכום:

- מערך זה כלל אתרים מתחזים לאתרי חדשות מוכרים ברחבי העולם, הפיץ את המידע לגורמים ספציפיים באמצעות הווטסאפ ולגורמים כלליים יותר, ביניהם עיתונאים ועוקבים אחרי עיתונאים ברשתות החברתיות, ובסבירות גבוהה-בינונית התכוון להפיץ או הפיץ קובצי APK נגועים בנוזקה.

- מערך זה מתוחכם יותר מהמערך שהופעל בפריצה הרוסית ל-DNC ומה-GDO שהופעל על ידי איראן מבחינת היקף הפלטפורמות השונות, והוא שילב מאמצים לתקיפת סייבר באמצעות תוכן זדוני ומזויף שאינו אמצעי "הנדסה חברתית" מובהק.

- מטרת מערך זה אינה מובהקת. מחד גיסא ניתן לטעון כי הוא אינו מערך פייק ניוז כלל וכלל אלא שלב הנדסה חברתית ארוך ומתוחכם הרבה יותר. מאידך גיסא, חלק ניכר מהכתבות הפיקטיביות הופצו בפומבי ברשתות החברתיות והופנו לעיתונאים, אך גם לציבור הרחב. בשונה מאתרי פישינג רגילים, במקרה זה השקיעו המפעילים גם בכתיבת כתבה שקרית, שתוכננה לא רק לגרום לנתקף לרצות לקרוא אותה אלא גם להעביר הלאה את המסר הכולל את הדיסאינפורמציה. אם כך, ניתן לראות במערך זה את הדוגמה החזקה ביותר עד היום לשילוב בין תקיפות סייבר לבין תוכן זדוני.

סיכום

במאמר נבחנו מספר מתארים של שילוב בין תקיפות טכנולוגיות לבין מניפולציה על תכנים, תוך שימוש במרחב הווירטואלי.

מתקפות סייבר קלאסיות מסוג CNA מצריכות שימוש של התוקף היחיד או קבוצת התומכים במספר כלי תקיפה טכניים, בין כאלה המתבססים על פיתוח נוזקות בצורה עצמאית באמצעות

צוות תוקף ובין שמתבססים על "נוזקות מדף" (commodity tools) - כאלו שניתן לרכוש ברשת האינטרנט ולהשתמש בהן לצורך המתקפה. את צוות הפיתוח מקיפים לרוב אנשי מעטפת כמו למשל אנשי IT, גורמי עיצוב גרפי שונים, גורמי שפה - אם התוקף מתכוון לתקוף יעדים שאינם דוברים את שפתו - נתונים פיננסיים ועוד. מעטפת זו אינה העיקר בתקיפה, שכן המטרה העיקרית של התוקף היא להשיג את הנגישות לנתקף. תפקיד המעטפת הוא לסייע לתוקף להשיג את מטרותיו, ואי לכך, לעיתים התוקפים עצמם מהווים את אותה מעטפת ומבצעים את שני התפקידים, כאשר המומחיות שלהם היא פיתוח כלי סייבר התקפי ותפעולם.

לעומת זאת, מבצעי השפעה במרחב הווירטואלי - מתקפות מסוג CNI - מצריכים יחס הפוך בין שכבת המעטפת לבין צוות הפיתוח. במבצעי השפעה רבים מקימים ה"תוקפים" מערך פייק ניוז הכולל אתר או שורה של אתרים מזויפים שבהם מופץ התוכן הזדוני, אך לא יאונה כל רע למכשירו האלקטרוני של הנתקף בעת הגלישה באתרים אלו. אי לכך, נעשה שימוש בפלטפורמה זהה גם ברשתות החברתיות – הפצת דיסאינפורמציה באמצעות חשבונות מזויפים. מתקפות אלו, אם כך, מצריכות בעיקר את אותם אנשי מעטפת – כותבי תוכן, מעצבים גרפיים, אומני דיסאינפורמציה, גורמים כלכליים ומומחי רשתות חברתיות. הדגש על אנשי הפיתוח מופחת, אם בכלל קיים (במקרה של שימוש ברשתות חברתיות). דבר זה הופך את מתקפות ה-CNI למתקפות נפוצות, אשר מופעלות לפעמים מטעם משרדי פרסום ולא מטעם תוקפי סייבר מתוחכמים.

מהניתוח שבוצע במאמר עולה כי עבור מבצעי תקיפות סייבר - שהחלו לפני עשור ויותר וכללו פגיעה בתפקוד של מערכות מחשב או מבצעי ריגול - נדרש חלק מזערי של שימוש בתכנים, בעיקר לצורך החדרת הנוזקות באמצעות הנדסה חברתית. סוג התקיפות השני שהוצג במאמר כולל פרסום מידע שהושג במסגרת תקיפות סייבר. הגם שאין שינוי באופי התקיפה, ניכר כאן שינוי בתכליתה. ייתכן שפרסום כזה עלול גם לחשוף יכולות תקיפה או לחסום פרצה. זאת ועוד, פרסום כזה, אם מדובר בהיקפי מידע גדולים, מחייב הקמת תשתית שבה ניתן לשלוט בקצב הפרסום ובעיתויו.

סוג התקיפות השלישי מתאר שילוב הולך וגובר של גורמי תוכן ותקיפה טכנולוגית כבר בראשית הדרך. בהקשר זה ניתן ללמוד על מספר מאפיינים של מתקפות סייבר המשלבות תוכן זדוני:

- הפלטפורמה המוכרת של אתרים זדוניים המפיצים תוכן זדוני או קבצים נגועים בנוזקה אינה מספקת, ויש צורך בהקמת מעטפת שתשלים את תקיפת הסייבר ותכלול פרופילים לדוגמה ברשתות החברתיות, על מנת להצליח להגיע אל הנתקפים בצורה ישירה.
- מתקפת סייבר המשלבת תוכן זדוני ובעלת מטרות של השפעה חייבת לכלול מספר שכבות שונות המספקות אמינות לתוקף, בשונה לדוגמה ממתקפות סייבר קלאסיות, אשר בהן יכול התוקף להשתמש בכתובת דוא"ל אחת על מנת להפיץ אתר פישינג אחד. במתקפות מהסוג התודעתי, הנתקף ישלב לרוב רכיבים נוספים של אמינות – פעילות ברשתות החברתיות, הצגת מצג שווא כאילו מדובר בחברה קיימת, שילוב תוכן ויזואלי ואף מיקום.

[1] מאמר זה פורסם לראשונה (באנגלית) בספר Cybersecurity and Legal-Regulatory Aspects בעריכת גבי סיבוני ולימור עציוני, ינואר 2021 https://www.worldscientific.com/worldscibooks/10.1142/11793

[2] דוד סימן טוב - חוקר בכיר בתוכנית ביטחון לאומי ודמוקרטיה בעידן של פוסט-אמת ופייק ניוז על שם ליפקין-שחק במכון למחקרי ביטחון לאומי. שירת בקהילת המודיעין הישראלית ומכהן גם כסגן המכון לחקר המתודולוגיה של המודיעין במרכז למורשת המודיעין.
אוהד זיידנברג - חוקר מודיעין סייבר בכיר, מתמקד בעיקר בתקיפות במזרח התיכון ומומחה לענייני איראן. לשעבר חוקר ומפקד ביחידת 8200. במסגרת תפקידו חוקר קמפיינים של מתקפות סייבר אשר בעיקרן ממומנות ומוצאות לפועל על ידי מדינות ושחקנים בינלאומיים. מתמחה בניצול הפלטפורמה הדיגיטלית לצורכי מבצעי השפעה וקמפיינים של דיסאינפורמציה.

[3] דגנית פייקובסקי ואביתר מתניה, "מבצעי השפעה בסייבר – מאפיינים ותובנות". בתוך המערכה על התודעה: היבטים אסטרטגיים ומודיעיניים. עורכים: יוסי קופרוסר ודודי סימן טוב. המכון למחקרי ביטחון לאומי, מזכר 191, (מאי 2019).

[4] Yuriy Danyk, Tamara Maliarchuk, and Chad Briggs. "Hybrid War: High-tech, Information and Cyber Conflicts", *Connections*, Vol.16 (2),(2017): 5-24.

[5] Robin Brown, "Information operations, public diplomacy & spin: The United States & the politics of perception management". : *Journal of Information Warfare*, Vol.1 (2002): 40-50

[6] דימה אדמסקי, "אומנות אופרטיבית קיברנטית: מבט מזווית לימודי האסטרטגיה ומפרספקטיבה השוואית", עשתונות, מס' 11, המכללה לביטחון לאומי (אוגוסט 2015): 39-41.

[7] ורה מיכלין-שפיר, דוד סימן טוב ונופר שעשוע, "רוסיה כמעצמת מידע". בתוך המערכה על התודעה: היבטים אסטרטגיים ומודיעיניים. עורכים: יוסי קופווסר ודודי סימן טוב. המכון למחקרי ביטחון לאומי, מזכר 191, (מאי 2019).

[8] Linda Robinson, Todd C. Helmus, Raphael S. Cohen, Alireza Nader, Andrew Radin, Madeline Magnuson, and Katya Migacheva, *The Growing Need to Focus on Modern Political Warfare* (Santa Monica, CA: RAND Corporation, 2019), 5-24.

[9] איתי חימיניס, "לוחמת המידע של איראן", בתוך המערכה על התודעה: היבטים אסטרטגיים ומודיעיניים. עורכים: יוסי קופרוסר ודודי סימן טוב, מזכר 191, המכון למחקרי ביטחון לאומי (2019).

[10] חיים אסא, "השפעה על שינוי עמדות בציבורים גדולים", בתוך המערכה על התודעה: היבטים אסטרטגיים ומודיעיניים. עורכים: יוסי קופרוסר ודודי סימן טוב, מזכר 191, המכון למחקרי ביטחון לאומי (2019).

[11] Dunlap and J. Charles, "The Hyper-Personalization of War: Cyber, Big Data, and The Changing Face of Conflict". *Georgetown Journal of International Affairs* 15 (2014): 108-118.

[12] Jason R. C. Nurse, "Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit", *The Oxford Handbook of Cyberpsychology* (2018).

[13] Charles E. Lively, Jr., "Psychological Based Social Engineering", SANS Institute, GSEC Option 1 version 1.4 (December 2003).

[14] Herbert Lin. and Jackie Kerr, "On Cyber-Enabled Information/Influence Warfare and Manipulation". In *Oxford Handbook of Cybersecurity* (2018).

[15] דניאל ברן ויוסי לוי, "תופעת סייבר המדינה האסלאמית – מה המערב לא מבין?" בין הקטבים - סייבר: אתגר והזדמנויות במרחבים חדשים, גיליון 3, מרכז דדו (דצמבר 2014).

[16] יעל לוקסמן-בהט, כנס הסייבר הבינלאומי השנתי ה-6, סדנת יובל נאמן למדע, טכנולוגיה וביטחון, אוניברסיטת תל אביב (2016).

[17] Pascal Brangetto and Matthijs A. Veenendaal, "Influence Cyber Operations: The use of cyberattacks in support of Influence Operations". *2016 8th International Conference on Cyber Conflict (CyCon)* (May 2016): 113-126.

[18] IAI, "Israel Aerospace Industries Hosting a Think Tank as part of the European Union Horizon 2020 Dogana R&D Program", (2018, June 17).

[19] גבי וסיבוני ועופר אסף, קווים מנחים לאסטרטגיה לאומית במרחב הסייבר, מזכר 149, המכון למחקרי ביטחון לאומי, , (2015): 19-18.

[20] Piret Pernik, *Hacking for Influence - Foreign Influence Activities and Cyber-attacks*, International Centre for Defence and Security (February 2018).

[21] Daniel P. Bagge, *Unmasking Maskirovka: Russia's Cyber Influence Operations*. (New York: Defense Press, 2019).

[22] Barrie Sander, "The Sound of Silence: International Law and the Governance of Peacetime Cyber Operations". 2019 11th International Conference on Cyber Conflict, T. Minárik et al. (eds), NATO CCD COE Publications (May 2019): 1-21.

[23] יובל סיני, *Digital Whisper*, גיליון 76 (אוקטובר 2016): 6-9, "Transportation Cyber Security"".

[24] פייקובסקי ומתניה, שם.

[25] Emilio Ferrara, Onur Varol, Clayton Davis, Filippo Menczer, Alessandro Flammini, "The rise of social bots". *Communications of the ACM*, , Vol. 59 No. 7, (July 2016): 96-104.

[26] Michele Maasberg, Emmanuel Ayaburi, Charles Z. Liu, and Yoris A. Au, "Exploring the Propagation of Fake Cyber News: An Experimental Approach", *Proceedings of the 51st Hawaii International Conference on System Sciences*, (2018): 3717-3726.

[27] Lion Gu, Vladimir Kropotov, and Fyodor Yarochkin, *The Fake News Machine: How Propagandists Abuse the Internet and Manipulate the Public*, Forward-Looking Threat Research (FTR), Trend Micro, (2017).

[28] האקטיביסטים - האקרים שפועלים ממניעים חברתיים.

[29] "Als Zielobjekt markiert" Der Enthüller Edward Snowden über die geheime Macht der NSA. *Der Spiegel* 28/2013. https://www.spiegel.de/spiegel/print/d-102241618.html

[30] Nakashima, E. Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes, *The Washington Post*, January 13, 2018. https://wapo.st/2Ml4L95

[31] ClearSky Research Team. "Ayatollah BBC – An Iranian Disinformation Operation against Western Media Outlets". ClearSky Cyber Security, February 28, 2018. https://www.clearskysec.com/bbc/

[32] ClearSky Research Team , "Global Iranian Disinformation Operation", ClearSky Cyber Security, November 30, 2018.https://www.clearskysec.com/global-iranian-disinformation-operation/

[333333] Jack Stubbs and Christopher Bing, "Special Report: How Iran spreads disinformation around the world", *Reuters*, November 30 , 2018, https://www.reuters.com/article/us-cyber-iran-specialreport/special-report-how-iran-spreads-disinformation-around-the-world-idUSKCN1NZ1FT

[34] איום מתמשך מתקדם (Advanced Persistent Threat) הוא איום חשאי המבוצע ברשת מחשבים. האיום מבוצע בדרך כלל על ידי מדינה או קבוצה בחסות מדינה, בעלת גישה בלתי מורשית לרשת מחשבים, שנותרת בלתי מזוהה לתקופה ממושכת. לאחרונה המונח מתייחס גם לקבוצות שאינן ממומנות על ידי מדינות, אשר מבצעות חדירות ופריצות ממוקדות בקנה מידה גדול למטרות ספציפיות.

[35] Threatconnect Research ,Does a BEAR Leak in the Woods?. ThreatConnect, August 12, 2016. https://threatconnect.com/blog/does-a-bear-leak-in-the-woods/;
Feike Hacquebord, *Two Years of Pawn Storm : Examining an Increasingly Relevant Threat* . Trend Micro (2017). https://documents.trendmicro.com/assets/wp/wp-two-years-of-pawn-storm.pdf

[36] DC Leaks: Little Known Site Dumps Data on George Soros. RiskBased Security, August 13, 2016. https://www.riskbasedsecurity.com/2016/08/13/dc-leaks-little-known-site-dumps-data-on-george-soros/

[37] Andrew Roth, "Russia denies DNC hack and says maybe someone 'forgot the password'". *The Washington Post*, June 15, 2016, https://wapo.st/2Y81I76

[38] Name Serve (שרת שמות) מתרגם שמות דומיין לכתובות IP. זה מאפשר למשתמש גישה לאתר על ידי הקלדת שם הדומיין במקום כתובת ה- IP בפועל של האתר. "Name Server." Techterms. https://techterms.com/definition/nameserver

[39] פישינג - מתודה לגניבת מידע בקרב הנתקף. לרוב משתמשים התוקפים במתודות הנדסה חברתית שונות על מנת לשטות בנתקף ולגרום לו למסור את המידע הרגיש.

[40] Threatconnect Research Team, "What in a name server?" ThreatConnect Security, July 7, 2016. https://threatconnect.com/blog/whats-in-a-name-server/

[41] השימוש בפלטפורמת רשת חברתית הוא אמצעי נוסף להפצה, אך גם אמצעי נוסף ליצירת אמינות בקרב הנתקפים. בהקשר של צילום המסך, אנא שימו לב למיקום ב-Manhattan ולא בוושינגטון DC, או לחלופין במדינת התוקף – רוסיה.

[42] אריאל ויטמן, "תקיפת סייבר טורקית על אתרים ישראלים", ישראל היום, 21 במאי 2018. https://www.israelhayom.co.il/article/557371

[43] Spear-Phishing היא מתודה מקבילה לפישינג, ובה מותקף יעד ספציפי באמצעות תשתית אשר לרוב מתוכננת עבורו.

[44] Etienne Maynier, John Scott-Railton, Alberto Fittarelli, Ned Moran, and Ron Deibert, Gabrielle Lim , "Burned After Reading - Endless Mayfly's Ephemeral Disinformation Campaign", The Citizen Lab, May 14, 2019 https://citizenlab.ca/2019/05/burned-after-reading-endless-mayflys-ephemeral-disinformation-campaign/

[45] רן בר-זיק, "קמפיין פייק ניוז נגד ליברמן: 'תמיר פרדו טען כי הוא סוכן רוסי'", הארץ, 14 בנובמבר 2018. https://www.haaretz.co.il/captain/net/.premium-1.6655180

[46] במהלך הניתוח הטכני של מערך זה הצליחו למצוא החוקרים קשר טכנולוגי למספר אפליקציות הנגועות בנוזקה שמתחזות לרשת החברתית טוויטר. חפיפה זו התבססה על חפיפה תשתית (לדוגמה – אחסון של אתרים על שרת פרטי וייחודי), או לחלופין דמיון מוחלט בנתוני ה-Whois של האתרים הללו.