

מתקפות סייבר והשפעתה במלחמת "חרבות הברזל" ב-

7 באוקטובר 2023

[Link to the English Version](#) [CLICK Cyber](#)
[Attacks and its influence in the](#)
[Oct. 7th "Iron Swords" WAR](#)

ב-8 חודשי לחימה חוותה ישראל מתקפות סייבר ומבצעי השפעה עוינת שטרם גרמו לנזק משמעותי. עם זאת, הזמן אינו פועל לטובתה: ההשקעה הישראלית בהגנה מפני איומי סייבר רחוקה מלהספיק, ואויביה מפיקים לקחים במאמץ לשפר את יכולותיהם. הצורך של ישראל להגדיל את השקעותיה בתחום, שהודגש על ידי המלחמה, יכול להוות במקביל הזדמנות עבור ישראל להפוך למובילה עולמית בהגנה מפני מתקפות משולבות של לוחמת סייבר ומבצעי השפעה [0].



כוחות צה"ל ברצועת עזה | צילום: אתר דובר צה"ל

הקצב המהיר שבו מתפתחות טכנולוגיות בעידן המודרני מעצב מחדש היבטים שונים של החברה האנושית, כולל אופי הסכסוך והלחימה בשדה הקרב. טכנולוגיות משבשות ומשבשות את האופן שבו מדינות ושחקנים לא-מדינתיים מתחרים על השגת יתרון צבאי ויוצרות הזדמנויות לבניית שיתוף פעולה חדש. במצב כזה, הבנת ההשלכות של טכנולוגיות אלה על סכסוכים עתידיים הופכת הכרחית.

מלחמת "חרבות הברזל", שפרצה ב-7 באוקטובר 2023, ממחישה כי למרות יתרונה היחסי של ישראל בתחום הסייבר, יריבותיה אינן זקוקות למשאבים יקרים או לתחכום טכנולוגי יוצא דופן כדי להשפיע על תהליכי קבלת ההחלטות בישראל, תוך חתירה לערעור אמון הציבור במערכות המדינה ולהעמקת השסעים הפנימיים. בשנים האחרונות נוצרו טכנולוגיות מתקדמות כגון בינה מלאכותית (AI), מודלים של שפה גדולה (LLM) ודיפ-פייקנגישות וזולות. כתוצאה מכך, שחקנים מדינתיים ולא מדינתיים ברחבי העולם – כולל יריבותיה של ישראל – כבר החלו לשלב טכנולוגיות אלה במאמציהם לבצע מתקפות סייבר ולהשפיע על פעולותיהם. [1]

יריב שרוצה לפעול נגד חברה דמוקרטית באמצעות שילוב של מתקפות סייבר ומבצעי השפעה, יכול היום להשיג מטרות אופרטיביות ואף אסטרטגיות

מאפייניו הייחודיים של ממד הסייבר – מרחב חוצה גבולות הנגיש כמעט מכל מקום בעולם – הופכים אותו למדיום המאפשר גם לשחקנים בעלי יכולות מוגבלות לבצע תקיפות ומבצעים מסוג זה. למעשה, יריב שרוצה לפעול נגד חברה דמוקרטית באמצעות שילוב של מתקפות סייבר ומבצעי השפעה יכול כעת להשיג מטרות אופרטיביות ואף אסטרטגיות.

הצלחתו האפשרית של שחקן עוין זה נובעת ממספר חולשות קריטיות מהן סובלות חברות דמוקרטיות: ראשית, הן תלויות יותר בתשתיות טכנולוגיות אזרחיות וממשלתיות, ולכן רגישות יותר למתקפות סייבר ולמבצעי השפעה מאשר יריב חלש, הנשען פחות על טכנולוגיה ביום-יום; שנית, משום שמנהיגים במדינות דמוקרטיות מושפעים באופן טבעי יותר מדעת הקהל; ושלישית, משום שאויבי המדינות הדמוקרטיות אינם נרתעים מניצול מרחב הסייבר לפגיעה בתשתיות אזרחיות.

במלחמת "חרב ברזל", שלושת התנאים הללו פועלים לרעת ישראל. מאמר זה מבקש למפות את נקודות התורפה שהתגלו במהלך המלחמה ויציע דרכים שבהן ישראל יכולה לשפר את יכולתה להגן על עצמה במרחב הסייבר.

סייבר המשמש שחקן "חלש" מבחינה פיסית הוא אחד השחקנים החזקים במלחמות העתיד!

נגישות טכנולוגית אינה מוגבלת לתחנות כוח טכנולוגיות. [2]

השפעה – לארגוני הטרור ולמדינות החסות שלהם כלים רבים להשפיע על אויב בעל עליונות טכנולוגית בשדה הקרב. ארגוני הטרור מנצלים את העובדה שמרחב הסייבר מאפשר גם לשחקנים בודדים ונחותים טכנולוגית להשפיע באופן משמעותי על יריביהם, בעוצמה שאינה הולמת את גודלם ואת יכולותיהם הפיזיות.

מחד גיסא, מגוון האמצעים של ארגוני הטרור במרחב הסייבר מוגבל בשל היעדר נגישות לטכנולוגיה בבעלות מדינות או חברות פרטיות מתקדמות טכנולוגית, ואין להם את המשאבים הנדרשים להכשרת מומחים ולביצוע מו"פ טכנולוגי כמו במדינות הנחשבות למעצמות טכנולוגיות. מנגד, לארגוני הטרור יש כיום גישה לשוק החופשי ולסחר "שחור" בכלי סייבר, מאגרי מידע מודלפים וכלי מודיעין פתוחים, באופן המאפשר להם לפעול באופן התקפי במרחב הסייבר. [3]

בהתאם לכך, בשנים האחרונות התמחו ארגוני הטרור ומדינות החסות שלהם בביצוע פעולות להשפעה על החברה האזרחית, בעיקר במדינות דמוקרטיות. השימוש ברשתות חברתיות נפוץ ורשתות טלוויזיה מאוד במדינות אלו,

והחברות המפעילות אותן אוספות מידע רב על משתמשיהן ובמקביל קובעות, באמצעות הפיד האלגוריתמי, איזה מידע יצרכו.

תוקפים שמכירים את אופן הפעולה של המערכות הללו יכולים לתמרן אותן כדי להפיץ תוכן רב – מטעה באמצעות בוטים וגורמים מתחזים ברשת הפיס בוק הלינק דין ורשתות הפצת ידעיות, מזויף או לא נעים – במהירות ולחלקים גדולים באוכלוסייה. צעדים אלה נועדו לשבש את תפיסת המציאות כפי שהיא קיימת בקרב קהלי יעד שונים, אפילו בהפצת סרטוני וידאו מכוונים באופן המאתגר את אפשרויות התגובה וגיבוש צעדי פעולה אפקטיביים. כך הצד היוזם יוצר לעצמו יתרון במערכה הכוללת. [4]

מחקר אקדמי שבדק את התנהגות המשתמשים בפייסבוק סביב בחירות 2020 בארה"ב מצא, למשל, כי פוסטים של חשבונות בעלי אמינות נמוכה היו גלויים פי שישה מפוסטים שפורסמו על ידי מקורות מהימנים, כמו ארגון הבריאות העולמי. [5]

תקיפה ושיבוש – אסטרטגיה יעילה נוספת מכוונת לפגיעה בתשתית המידע של היריב. אלה יכולות בדרך כלל התקפות על מערכות ממוחשבות במגזר הציבורי והפרטי. התקפות מסוג זה יכולות ללבוש מספר צורות: מניעת שירות מבוזרת DDos והשחתת אתרים; גילוי מידע מסווג/אישי על כל ארגון או אישיות על ידי פרסום מסמכים סודיים (Hack&Leak, Doxing/Doxxing); פריצה למערכות מידע; ועוד.

המתקפה הבסיסית ביותר במרחב הסייבר היא שיבוש שגרת החיים, אך ללא גרימת נזק משמעותי, בלתי הפיך או מתמשך; התקיפות המתקדמות והמתוחכמות ביותר יכולו נגד מטרות תשתית קריטיות, כגון מים, חשמל, גז ודלק, או ינסו לפגוע במערכות שליטה ובקרה, כולל מטרות צבאיות.

הנדסה חברתית – מגמה נוספת שהתעצמה בשנים האחרונות היא פריצה למאגרי מידע לצורך איסוף מידע אישי. מידע זה מוצלב עם מידע שנאסף ממדיה חברתית (במיוחד פייסבוק ולינקדאין) כדי לבצע התקפות הנדסה חברתית שתוכננו בהתאמה אישית. [6]

במספר קמפיינים של הנדסה חברתית בשנים האחרונות, האקרים של חמאס פעלו ברשתות החברתיות כדי להערים על חיילי צה"ל להוריד ללא ידיעתם תוכנות זדוניות למכשירים הסלולריים שלהם. זאת בנוסף להתקנת סוסים טרויאניים במכשירי היעד על ידי הפצת יישומים זדוניים. [7] במתקפות סייבר כאלה, התוקף מקבל גישה לתמונות, מידע אישי ומספרי טלפון. בהתקפות מתוחכמות יותר, הוא יכול אפילו להשיג גישה שתהפוך את המכשיר לכלי ריגול בכך שתאפשר לו להתחבר לבלוטות, מצלמה, מיקרופון וכו'.

לוחמת סייבר נגד ישראל ב"חרבות ברזל"

בשנים האחרונות מגלים ארגוני טרור כמו חמאס וחזבאללה עניין גובר במרחב הסייבר, לא פעם בסיוע איראן. בתקופה זו נעשו ניסיונות רבים לפעול נגד ישראל – עד כה, ללא הצלחה משמעותית. [8] במלחמת חרב ברזל ניכר כי חמאס שיפרה את יכולות הסייבר שלה, הגם שגם בעת הזו היא לא הצליחה להסב לישראל נזק אסטרטגי בתחום זה. כולל פרסום סרטוני וידאו מוכתבים של אסירים וחטופים כדי להשפיע על דעת הקהל בישראל.

פרק זה יסקור מתקפות סייבר משמעותיות במהלך המלחמה כנגד שלושה איומי ייחוס שמומשו במהלך המלחמה: מבצעי ריגול סייבר לאיסוף מודיעין, מבצעי השפעה ברשתות חברתיות ותקיפת אתרים ותשתיות.

א. פעולות ריגול סייבר לאיסוף מודיעין

במהלך מלחמת חרב הברזל יישמה איראן אסטרטגיה רחבה לפעול נגד ישראל באמצעות פעולות השפעה במרחב הדיגיטלי. איראן ביצעה תקיפות סייבר והפצת מידע כוזב כדי להשפיע על תהליכי קבלת החלטות בישראל, לפלג את דעת הקהל ולעצב נרטיבים. [9] דו"ח של מיקרוסופט שפורסם בפברואר 2024 אף טען כי מאז פרוץ המלחמה כ-43% מפעילות הסייבר האיראנית התמקדה בישראל. [10]

דו"ח שפרסמה באותו חודש מנדיאנט, חברת מודיעין הסייבר של גוגל, הצביע על כך שפעולות הסייבר של איראן ושל קבוצות הקשורות לחיזבאללה הפכו ממוקדות יותר ומבוזרות פחות במהלך המלחמה. הם נועדו, בין היתר, לערער את התמיכה הציבורית בהמשך המלחמה, בדגש על ניסיונות לערער את הלגיטימיות של ישראל ולהצדיק את פעולותיה הצבאיות. [11]

מחקר של חברת הסייבר Sentinel One, שפורסם בדצמבר 2023, במהלך המלחמה, התמקד בקבוצת תקיפה המזוהה עם חמאס הפועלת תחת השם הבדוי "עזה סייברנג". המחברים העריכו כי מדובר במערכת מאורגנת הפועלת באופן דומה ליחידות סייבר צבאיות או ממשלתיות. [12]

בדיווחים קודמים של חברות סייבר שונות נטען כי יחידה זו עוסקת באיסוף מודיעין. כך למשל, חברת קספרסקי הרוסית טענה ב-2019 כי אותה יחידת סייבר הפעילה מערכת איסוף כזו מאז 2017 באמצעות מבצעי ריגול סייבר נגד גופים ממשלתיים ברחבי המזרח התיכון. על פי ההערכות, הפעילות החלה בסביבות שנת 2012, כאשר היא עדיין כוונה רק נגד ישראל וגורמים פלסטינים המתחרים בחמאס. [13]

ב. קמפיינים להשפעה ברשתות החברתיות
על פי דיווח של מיקרוסופט, מאז פרוץ המלחמה הגבירה איראן את השפעתה ואת מאמצי תקיפת הסייבר שלה נגד ישראל. [14] הרפובליקה האסלאמית מנהלת קמפיינים מתוחכמים יותר ויותר של השפעה ברשתות החברתיות, תוך פריסת רשתות של אוטארים (דמות וירטואלית ברשת חברתית המופעלת על ידי בני אדם), בוטים (חשבון מדיה חברתית המנוהל על ידי אלגוריתם המדמה אדם) ו"בובות גרב" (חשבון מזויף שנוצר על ידי אדם כדי להונות משתמשים אחרים).

לרשות איראן ושלוחיה עומדים מגוון רחב של כלים טכנולוגיים לניהול קמפיינים להשפעה ולמודעות ברשתות החברתיות. שילוב אמצעים אלה עם טכנולוגיות משבשות כגון בינה מלאכותית גנרטיבית ודיפ-פייק, [15] עשוי להוביל להישגים במערכה המדינית נגד ישראל, שמטרתה העיקרית היא דה-לגיטימציה לפעולה הצבאית הישראלית. חברת החשמל של ישראל בולמת עשרת אלפים תקיפות סיבר יומיות. כנ"ל בתי חולים ואקדמיה חלקם כבר שימשו לראשונה בסכסוך הנוכחי. כך, למשל, גורם לא מוכר (ככל הנראה קשור לרוסיה) הפעיל פעולת השפעה נגד ישראל באמצעות טכנולוגיית דיפ-פייק, המאפשרת מניפולציה משכנעת של תמונות וסרטונים אנושיים. אותו גורם פרסם סרטון דיפ-פייק שבו מופיע סרטון אותנטי של חייל צה"ל. הסרטון השקרי כלל קריאה ליהודי אוקראינה להתגייס לצה"ל ולהילחם למען ישראל בעזה. [16]

במקרה אחר חשפו חוקרי מיקרוסופט כי האקרים המזוהים עם איראן שיבשו שירותי סטרימינג באיחוד האמירויות, בריטניה וקנדה כדי לשדר "שידור חדשות מזויפות" באמצעות דיפ-פייק. ה"שידור" כלל דיווח על המלחמה בעזה, בו הציג מגיש החדשות המזויפות תמונות לא מאומתות שלטענתו הראו פלסטינים הרוגים ופצועים כתוצאה מפעילות צה"ל בעזה. [17]

אנליסטים בחברה גילו כי קבוצת התקיפה האיראנית, המכונה Cotton Sandstorm, פרסמה גם סרטונים בפלטפורמת המסרים של טלגרם המראים אותה מבצעת את מתקפת הסייבר. אלה כללו פריצה לשלושת שירותי הסטרימינג הללו ושיבוש ערוצי החדשות עם שידור הפייק ניוז. במקביל, בכירים במיקרוסופט ציינו, כי בחודש הראשון למלחמה חלה עלייה של 28% בחשיפת אתרי חדשות המזוהים עם איראן

טכנולוגיית הדיפ-פייק טרם הבשילה במלואה לטובת שימוש מבצעי למטרות בעימות הנוכחי, ומומחים הצליחו להפריך את אמינות הסרטונים השקרניים שנוצרו באמצעותה. עם זאת, האתגר שמציב השימוש בטכנולוגיה מפגיעה כזו הוא משמעותי, שכן הוא מקדים בהרבה את ההתקדמות האיטית בפיתוח מענים טכנולוגיים אפקטיביים נגדה.

דו"ח שפרסם מערך הסייבר הלאומי בסוף דצמבר 2023 מצא כי במהלך המלחמה זוהו כ-15 קבוצות תקיפה מרכזיות שפעלו נגד ישראל במרחב הסייבר, וחלקן חולקות מודיעין זו עם זו. קבוצות אלו מזוהות עם איראן, חמאס וחזבאללה. [18]

לדברי מחברי הדו"ח, ניתן לראות קווי דמיון בין הטכניקות והטקטיקות בהן נעשה שימוש במהלך חרבות הברזל לבין אלו המשמשות בסכסוכים אחרים ברחבי העולם, כגון מלחמת רוסיה-אוקראינה. אלה כוללים שימוש בלוחמה פסיכולוגית כאמצעי להדהוד מתקפות סייבר ושימוש ברשתות חברתיות; ניסיונות להשפיע על הרשתות החברתיות, כולל פרסום פייק ניוז, דיסאינפורמציה ומניפולציה של מידע; מיחזור חומרים ישנים והצגתם כחדשים; וקריאה לתוקפים להצטרף לפיגועים שונים. [19]

ג. תקיפת אתרים ותשתיות

על פי דיווח של Cloudflare, כאשר מחבלי חמאס חדרו לעוטף עזה בבוקר ה-7 באוקטובר, החלו התקפות DDoS עוצמתיות נגד אתרים רבים ברשת הישראלית, בעיקר אלה של כלי תקשורת וחברות תוכנה. בהמשך, לצד כניסת כוחות צה"ל למערכה הקרקעית ברצועת עזה, חלה עלייה משמעותית במספר תקיפות הסייבר. 10 אלף ביום תקיפות מול חברת חשמל חברת המי אקדמיה ובתי חולים בישראל. את חלקן ניתן לייחס להתקפות יזומות של האקטיביסטים, אחרות התאפיינו ברמת תחכום גבוהה יותר והתמקדו במערכות תקשורת הפועלות בישראל. [20]

בסוף נובמבר 2023 הודיעה קבוצת ההאקרים האיראנית Cyber Av3ngers כי כל מוצר או ציוד מתוצרת ישראלית הוא מטרה עבורה. אחת התקיפות כוונה נגד תשתיות מתוצרת חברה ישראלית שהותקנו במתקני מים ובמקומות אחרים בארצות הברית. קבוצות אחרות הדגישו התקפות "אפליקטיביות" – התקפות מוצפנות המחקות פעילות של משתמשים לגיטימיים ועוקפות את רוב מערכות ההגנה. [21] בין קבוצות אלה נמנית קבוצת Killnet הרוסית [22], שתקפה גופים ממשלתיים ואתרי חדשות ישראליים תוך הבעת עמדה פוליטית פרו-חמאסית מובהקת. [23]

בנוסף, ניתן להניח כי מערכות ארוכות טווח לריגול סייבר ואיסוף מודיעין עדיין קיימות במהלך המלחמה נגד מטרות ביטחוניות ואזרחיות ישראליות – הן לאיסוף מטרות, לביצוע הערכות מודיעין וניתוח הלכי רוח בציבור הישראלי, אך גם למידע שעשוי להועיל למבצעי השפעה ולהפצת מידע כוזב.

איראן ושלוחיה סובלים מנחיתות טכנולוגית ברורה בלוחמת הסייבר בהשוואה לישראל. לאור זאת, הם מתמקדים במבצעי השפעה, שיש להם חסם טכנולוגי נמוך ולישראל אין יתרון ברור מולו. מטרת פעולות אלה היא לקדם תכנים ומסרים שנועדו להשפיע על התודעה של הצד השני.

הרשתות החברתיות הפכו לפלטפורמה לדיסאינפורמציה (מידע שגוי, לא מדויק או מטעה המופץ במטרה מכוונת להטעות), מידע מוטעה (מידע שגוי, לא מדויק או מטעה שאינו מופץ במטרה מכוונת להטעות) ותוכן מזיק (הפצת מידע אמין במטרה לפגוע בצד שלישי).

המלחמה הוכיחה עד כה את יעילותם של אויבי ישראל בזירת האינטרנט וברשתות החברתיות, שם נחלו הצלחות טקטיות ונקודתיות. הצלחות אלה, שעשויות להיות להן השלכות אסטרטגיות בעתיד, צריכות להדאיג את ישראל, שכן הן מעידות על שיפור ביכולותיה בתחום זה.

הדרך קדימה

באוקטובר 2022 פרסם צבא ארצות הברית מהדורה מעודכנת של מדריך לוחמת השדה (FM 3.0, Multidomain Operations). אחד החידושים במדריך זה הוא חלוקת ההשפעה של הפעולה האופרטיבית לשלושה צירי פעולה שונים: הציר הפיזי, ציר המידע והציר האנושי. השלושה פועלים בצורת לולאה: כל פעולה פיזית יוצרת מידע חדש, שבתורו משפיע על האופן שבו אנשים מקבלים החלטות, ומוביל אותם לבצע פעולות פיזיות שונות. ההנחה העומדת בבסיס תפיסה זו היא שלמרות השימוש הגובר בטכנולוגיה, "קונפליקטים מנהלים על ידי בני אדם". [24]

לוחמת סייבר היא תחום בעל חשיבות גוברת בשדה הקרב המודרני, שכן היא מאפשרת לצדדים נחותים טכנולוגית להשתמש באמצעי תקשורת כדי להשפיע על תהליכי קבלת ההחלטות של יחידים או קבוצות בצד השני. בכך, החליש עשוי לצמצם, בעלות נמוכה, את הפער הטכנולוגי מול יריבו.

למרות המשאבים המוגבלים שישראל משקיעה ברמת המדינה בהגנה מפני השפעות זרות, בשלב זה של מלחמת חרב ברזל טרם נצפו מתקפות סייבר ומבצעי השפעה אסטרטגית נגד המדינה ולא נגרם לה נזק של ממש. עם זאת, סביר להניח כי ארגוני הטרור מפקימים לקחים ולומדים כיצד לשפר את יכולות הסייבר שלהם למאמצי השפעה, במטרה להציב איום משמעותי יותר בממד זה בעתיד הקרוב.

מתקפות סייבר עתידיות עלולות לשבש את זרימת המידע האמין לאזרחי ישראל, להטות את דעת הקהל לכיוונים לטובת התוקפים ולפגוע ביכולת הממשלה לקבל החלטות

תרחישים עתידיים אפשריים הם תקיפות שיטתיות ברמת תחום טכנולוגית גבוהה. כולל שיתוף פרסומי סרטוני וידאו מגמתיים ברשתות ובעולם של חטופים אסירים ותמונות של פגיעות באזרחים ילדים נשים בהם מואשמת ישראל ולאורך זמן דבר שיכול להטות את דעת הקהל נגד ישראל בעולם! ולהפעיל לחץ עולמי ובין לאומי על ישראל בגלל פרסום מוטה ומוגזם (ולא פעולות ספורדיות, כפי שקורה כיום). בהתבסס על דוגמאות עדכניות, אלה עשויות לכלול התקפות על תשתיות קריטיות, כגון התקפות על ספקיות תקשורת ואתרי חדשות – כפי שקרה במלחמת רוסיה-אוקראינה – ומבצעי השפעה רחבי היקף, מהסוג שחוותה ארה"ב לפני בחירות 2016 ו-2020. התקפות כאלה נגד ישראל עלולות לשבש את זרימת המידע האמין לאזרחיה, להטות את דעת הקהל לכיוונים הנוחים לתוקפים ובסופו של דבר לפגוע ביכולתם של גורמי השלטון לקבל החלטות מושכלות.

אל מול מאמצים אלה, על ישראל לעדכן ולשדרג את תפיסת ההגנה ההוליסטית שלה בתחום מבצעי הסייבר וההשפעה, ולהגביר את שיתוף הפעולה בין הממשלה ובעלות בריתה לבין ענקיות הטכנולוגיה. הפערים הקיימים, המאפשרים ליריביה של ישראל לתקוף אותה במרחב ההשפעה והתודעה, עלולים להוות נקודת תורפה משמעותית ביכולתה של המדינה להגן על תשתיות אזרחיות קריטיות, כגון אתרי חדשות וכלי תקשורת בעת מלחמה.

על מנת לבלום אפיק התקפה אפשרי זה, על מדינת ישראל להקים מערך הגנה ייעודי למרחב ההשפעה, שיכלול חדר הגנה לזיהוי מבצעי השפעה נגד מטרות במדינת ישראל (ביטחוני ואזרחית) ומאמץ לאתרון בשלבים מוקדמים של היווצרותן. מערכת זו תכלול גם צוות תגובה למבצעי השפעה, לצד צוותים טכנולוגיים לפיתוח יכולות לזיהוי וייחוס פומבי של העומדים מאחורי מתקפות סייבר ומבצעי השפעה.

ישראל יכולה ללמוד הרבה ממדינה קטנה אחרת, שבעבר הלא רחוק עמדה בפני מתקפת סייבר עוינת רחבת היקף והצליחה למנף אותה כדי להפוך במהירות למעצמה עולמית בתחום הגנת הסייבר. בשנת 2007 התמודדה אסטוניה עם סדרה של מתקפות סייבר מצד רוסיה, שהוכרו כ"מלחמת הסייבר הראשונה בהיסטוריה". בשיא הפיגועים נותקו 58 אתרים אסטוניים בבת אחת, ביניהם אתרים ממשלתיים ורוב העיתונים והבנקים.

בתום "מלחמה" זו, אסטוניה החליטה להפוך למובילה עולמית באבטחת סייבר. כיום היא מייצגת למדינות רבות בנושא וחתמה על הסכמים לפיתוח הכשרה ושיתוף פעולה בתחום אבטחת הסייבר עם אוסטרליה, לוקסמבורג, דרום קוריאה ונאט"ו.

על ישראל לשאוף להפוך למרכז להנגשת מידע על איומי השפעה, ולחלוק מידע זה עם הקהילה הבינלאומית וענקיות הטכנולוגיה באמצעות פעילות מדינית ודיפלומטית

מלחמת "חרבות הברזל" מציבה בפני ישראל את הצורך וההזדמנות ללמוד מהמודל האסטוני. ברמה הלאומית, ישראל יכולה להפוך למרכז להנגשת מידע על איומי השפעה, ולחלוק מידע זה עם הקהילה הבינלאומית וענקיות הטכנולוגיה

באמצעות פעילות מדינית ודיפלומטית. מעבר לשיתוף מידע, מוצע לקדם הקמת מרכז מצוינות בין-מגזרי (אקדמיה, מגזר פרטי וממשלתי) ללימוד שיטות פעולה בתחום הסייבר, לחקר השפעת טכנולוגיות פציעה על שדה הקרב התודעתי ולמחקר ופיתוח כלים טכנולוגיים לזיהוי איומי השפעה בשיתוף גורמים בינלאומיים.

ישראל יכולה גם לפעול להפיכתה למודל בינלאומי להשקעות במחקר ופיתוח בתחום ההגנה מפני מתקפות סייבר ומבצעי השפעה. זאת, תוך עידוד וצמיחה של סטארט-אפים ומיזמי חברה אזרחית, ובאמצעות שיתופי פעולה עם מדינות זרות, חברות בינלאומיות וגופים רלוונטיים אחרים המתמודדים עם אתגרים דומים ברחבי העולם.

שורה של מתקפות סייבר ברחבי העולם על מוסדות פוליטיים, מפלגות, תאגידים וחברות, מוסדות פיננסיים ותשתיות לאומיות קריטיות הציבו את איום הסייבר במקום גבוה בסדר העדיפויות של מדינות וארגונים ברחבי העולם. לאלה יש להוסיף היום איומים וסיכונים חדשים, המשתמשים במרחב הסייבר לביצוע פעולות השפעה, לרבות איסוף מודיעין לצורך מיקוד קהלי יעד באמצעות פריצה למאגרי מידע, ויצירת תוכן שנראה אמין כדי לפגוע במרחב המידע של יריביהם. טכנולוגיות הבינה המלאכותית, שהתפתחו מאוד בשנים האחרונות והפכו נגישות לציבור הרחב, מאפשרות לתוקפים למסד תהליכי אוטומציה ליצירה והפצה של תוכן זה, במהירות ובהפצה בכמה סדרי גודל גדולים יותר ממה שהתאפשר כמה שנים קודם לכן.

במציאות כזו, מדינת ישראל זקוקה לשינוי תפיסה אסטרטגית ולהשקעה משמעותית כדי להפוך למרכז ידע ולפלטפורמה בינלאומית לשיתוף פעולה בין-מגזרי בתחומי סייבר, השפעה ומודעות, טכנולוגיות משבשות, לוחמה בטרור ודיסאינפורמציה

סייבר כלים מסחריים הקיימים בשוק (שפותחו באסטוניה בתחילה) להגנה מפני התקפה ולוחמת סייבר בשדה הקרב העתידי מחולקים לשלושה תחומים: (תוספת - עמי אלעזרי)

באוקטובר 2022 פרסם צבא ארצות הברית מהדורה מעודכנת של מדריך לוחמת השדה (FM 3.0, Multidomain) (פעולות). אחד החידושים במדריך זה הוא חלוקת ההשפעה של הפעולה האופרטיבית לשלושה צירי פעולה שונים: הן ברמה הטקטית והן ברמת המידע בין המפקדה לפיקוד **הציר הפיזי**, ברמה הטקטית בשדה הקרב העתידי חשוב להגן על מערכות דיגיטליות של העברת מודיעין ומידע חזותי ואחר מהמפקדה לדרג הלוחם בצורה לא קווית, אך באמצעות העברת מידע סולרי, לעיתים בפס רחב המציג ללוחם את המטרות, מפה מודיעינית של כוחו ופקודות ביצוע, מערכת שיודעת להגן על פריצה או חסימה של קווי השידור של המידע הנ"ל היא הכרחית

ציר המידע בשדה הקרב העתידי לוחמים, טייסים, מפקדי טנקים, גלדי מחט, מפקדי אוגדות מקבלים מידע על מפת הקרב על מסכים ומטרות אמיתיות (בחיל האוויר נעים מהר) פקודות ותוצאות מידע זה חייב להיות מוגן מפני פריצה, חסימה או יצירת זיוף

והציר האנושי

שיבוש קבלת החלטות או בגלל חסימת מידע או יצירת פייק ניוז . השלושה פועלים בצורת לולאה: כל פעולה פיזית יוצרת מידע חדש, שבתורו משפיע על האופן שבו אנשים מקבלים החלטות, ומוביל אותם לבצע פעולות פיזיות שונות. יש לוודא באמצעות הגנה ביטחונית כפולה או משולשת על ציר העברת המידע על המוניטורים למקבלי ההחלטות, למשל תוכנה שבודקת שמה שמוצג בסוף על מסך מקבל ההחלטות הוא המקור שנשלח ממקורות מודיעין או מעריכים! אחרת תהיה השפעה קטסטרופלית על מקבל ההחלטות בכל הרמות

מצלמות סייבר חכמות IR AI FR

תחום חדש שנכנס למלחמת הסייבר העתידית הוא מצלמות מעקב ששומרות על גבולות, כבישים, כבישים מהירים וצמתי תחבורה

מצלמות חכמות הן מצלמות שהוספנו להן אלמנטים חדשים: חיישני אינפרא אדום וראיית לילה. מיקוד עמוק, 360 מעלות. ומעבר אוטומטי לתחומי עניין בחלל בהתאם לכיוון חיישנים אחרים בשילוב אלמנט סייבר למינויים, כגון זיהוי פנים, זיהוי כלי רכב, זיהוי כלי טיס, כולל כטב"מים. ו

כלקח מאירוע התצפית בעוטף עזה של יחידת התצפיתניות במלחמת חרב הברזל

כאשר נפגעו חלק גדול מהמצלמות עוד לפני החדירה למוצב ואולם הצפייה ורצח וחטיפת התצפיתניות

1. תקן צבאי מחמיר: על המצלמות להיות ברמה צבאית, מוגנות מפני פגיעה בגיד ומוסוות שלא ייפגעו.

2. אלומות הצפייה אינן חייבות להיות בחזית, כך שהצופים יהיו פגיעים חוזי ניתן להעביר אחורה לפיקוד

3. ניתן להעביר חוזים מוצפנים עד לפקוד או עד למרכזי צפיה ביחידת ההצפנה

מקורות

[0] **דניאל כהן** הוא ראש התוכנית למדיניות וטכנולוגיה במכון אבא אבן לדיפלומטיה ויחסי חוץ ועמית מחקר במכון הבינלאומי ללוחמה בטרור (ICT), שניהם באוניברסיטת רייכמן (המרכז הבינתחומי הרצליה). בנוסף, הוא חוקר בכיר במרכז הבינתחומי לחקר הסייבר ע"ש בלווטניק (ICRC) באוניברסיטת תל אביב. דניאל עובד כיועץ במגזר הממשלתי הציבורי ובהיי-טק. הוא דוקטורנט במחלקה לניהול באוניברסיטת בר אילן בתחום ממשק אדם-בינה מלאכותית ומודיעין איומי סייבר.

[1] האקונומיסט (מקוון), "מומחה לסיכוני בינה מלאכותית חושב שממשלות צריכות לפעול כדי להילחם בדיסאינפורמציה", *האקונומיסט*, 6 בפברואר 2024. <https://www.economist.com/by-invitation/2024/02/06/an-ai-risk-expert-thinks-governments-should-act-to-combat-disinformation; Microsoft Threat Intelligence>, "להקדים את שחקני האיום בעידן הבינה המלאכותית", *האבטחה של Microsoft*, 14 בפברואר 2024. <https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai>

[2] גבי סיבוני, דניאל כהן ואביב רוטברט, "איום ארגוני הטרור במרחב הסייבר", **צבא ואסטרטגיה**, כרך 5, גיליון 3, דצמבר 2013, עמ' 3-25.

[3] שם.

[4] דניאל כהן ואופיר בראל, *השימוש בלוחמת סייבר במבצעי השפעה*, תל-אביב: המרכז הבין-תחומי לחקר הסייבר ע"ש בלווטניק, אוקטובר 2017.

[5] אליזבת דווסקין, "מידע שגוי בפייסבוק קיבל פי שישה יותר קליקים מאשר חדשות עובדתיות במהלך בחירות 2020, לפי מחקר", *ושינגטון פוסט*, 4 בספטמבר 2021. <https://www.washingtonpost.com/technology/2021/09/03/facebook-misinformation-nyu-study/>

[6] " <https://www.israelhayom.co.il/tech/tech-news/article/14909838> ,

[7] "להתחזות לעולים חדשים ולפתות לוחמים וקצינים: סוכלה מתקפת סייבר של חמאס", **ישראל היום**, 16 בפברואר 2020. <https://www.israelhayom.co.il/article/733915>

[8] ראו:

גבי סיבוני וסמי קרונפלד, "מתקפת סייבר איראנית במהלך מבצע "צוק איתן", **מבט על**, גיליון 598, 25 באוגוסט 2014. (**קישור**); דני זקן, "יכולות חמאס, עתיד הסייבר: האלוף ערן ניב משרטט כיצד יראה שדה הקרב", **גלובס**, 11.2.2023. <https://www.globes.co.il/news/article.aspx?did=1001437716>; דניאל כהן ודניאל לוין, "צוק איתן בראי הגנת סייבר", בתוך ענת קוריץ ושלמה ברום (עורכים), **צוק איתן – משמעויות ולקחים**, תל אביב: המכון למחקרי ביטחון לאומי, 2014, עמ' 55-58. (**קישור**); פרנאז פאסיהי ורוגן ברגמן, "ישראל ואיראן מרחיבות את מלחמת הסייבר לתקיפת מטרות אזרחיות", **ניו יורק טיימס**, 27 בנובמבר 2021.

<https://www.nytimes.com/2021/11/27/world/middleeast/iran-israel-cyber-hack.html>

[9]. <https://www.maariv.co.il/news/military/Article-1060859>

[10] קלינט ווטס, "איראן מאיצה את פעולות הסייבר נגד ישראל מההתחלה הכאוטית", *Microsoft Threat Analysis Center*, 6 בפברואר 2024. <https://blogs.microsoft.com/on-the-issues/2024/02/06/iran-accelerates-cyber-ops-against-israel>

[11] סנדרה ג'ויס ושיין האנטלי, "כלי המוצא הראשון: מלחמת ישראל-חמאס בסייבר", **מודיעין מנדיאנט**, 14 בפברואר 2024. <https://blog.google/technology/safety-security/tool-of-first-resort-israel-hamas-war-in-cyber>

[12] אלכסנדר מילנקוסקי, "עזה Cybergang | חזית מאוחדת נגד אופוזיצית חמאס", **סנטינל לאבס**, 14 בדצמבר 2023. <https://www.sentinelone.com/labs/gaza-cybergang-unified-front-targeting-hamas-opposition>

[13] צוות קספרסקי, "כנופיית הסייבר בעזה וקמפיין SneakyPastes שלה", **קספרסקי**, 10 באפריל 2019. <https://www.kaspersky.com/blog/gaza-cybergang/26363>

[14] ווטס, "איראן מאיצה

[15] דרק הוקינס, "אבטחת הסייבר 202: סרטוני דוקומנטרי עלולים להכניס את משבר החדשות המזויפות להילוך גבוה, מזהירים מחוקקים", **ווישינגטון פוסט**, 31 ביולי 2018.

<https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-the-cybersecurity-202-doctored-videos-could-send-fake-news-crisis-into-202/2018/07/31/overdrive-lawmakers-warn/5b5f39c91b326b0207955e39>

[16] <https://www.haaretz.co.il/news/security/2023-11-21/ty-article/.premium/0000018b-eca1-d6b8-a5ab-eceb38280000>