המערכה בסייבר – מעורבות עולמית מכריעה

דולב כפיר

מלחמת רוסיה־אוקראינה, המלחמה הגדולה הראשונה של המאה ה־21, מספקת הזדמנות לדיון מחודש בתפקיד הסייבר בקונפליקטים. רוסיה, מעצמת סייבר מהשורה הראשונה, הפעילה במלחמה יכולות סייבר, במסגרת עימות צבאי עצים ראשון בעידן המידע. המונח "עידן המידע" מתייחס להבשלה של לפחות שלוש מהפכות טכנולוגיות: מהפכת האינטרנט; מהפיכת הענן, שדחפה ארגונים להתבסס על משאבי מחשוב ריכוזיים משותפים המופעלים על ידי ענקיות הטכנולוגיה; ומהפיכת ה"ביג־דאטא", ששינתה את דרך איסוף ואכסון המידע על ידי ממשלות וארגונים, ואת השימוש בו כבסיס לקבלת החלטות.

בעשורים האחרונים נקטה רוסיה לא אחת מתקפות סייבר מסוגים שונים: כך במלחמה בגיאורגיה (2008), דרך התערבות במערכת הבחירות לנשיאות ארצות הברית בשנת 2016, וכלה במתקפות המכונות NotPetya ו־Solarwinds, שבהן הציגה תחכום ופעלתנות מול ארגונים וחברות אוקראיניות ומערביות. לפיכך, רווחה ציפייה לחזות בהפעלה מאסיבית ומוצלחת של כלי סייבר בפלישה לאוקראינה בפברואר 2022. ואולם בפועל, נראה שלמתקפות הסייבר מהצד הרוסי הייתה השפעה מעטה על המערכה, אם כי רבות הדעות רבות ומגוונות אשר לסיבות לכך. שני הצדדים בעימות הפעילו במינונים שונים את שלושת המופעים העיקריים של כלי הסייבר: CNE (איסוף מודיעין), CNI (מלחמת תודעה ומידע), ו־CNA (התקפות על מערכות ממוחשבות). האופי החשאי ומיעוטו של איסוף בסייבר מקשה על תיאור הפעולות בתחום זה. וכמובן, מאמצים רבים של שני הצדדים לעיצוב דעת הקהל ולהונאה נתמכו בפעולות בסייבר וברשתות חברתיות.

מאמר זה יתמקד בהתקפות ולוחמת רשת (CNA), ובדינמיקה שנוצרה סביבן על ידי כלל השחקנים, כולל תאגידים וחברות אזרחיות, ובלקחים הנגזרים מכך עבור ישראל הן בתחום ההגנתי והן בתחום ההתקפי. זאת בידיעה כי בעיתוי הנוכחי יש מגבלות ללמידה ישראלית בגין חלקיות המידע, הטיות אפשריות במקורות הפתוחים וכן ההבדלים בין הזירה האוקראינית למקרה הישראלי.

עיקר האירועים בתחום זה באו לידי ביטוי בשבועות הראשונים למערכה, אז הוצאו לפועל התקפות סייבר, שתוכנו ככל הנראה בחודשים שהובילו לפלישה הרוסית. נראה שמאז, לא הוטלו למערכה מתקפות וכלי סייבר משמעותיים משני הצדדים. בטבלה מופיעות מתקפות,

שיזם הצד הרוסי בששת השבועות הראשונים למלחמה, כפי שסוכמו במסמך שפורסם על ידי חברת מיקרוסופט.[1]

Week 1 (February 23-March 2)	**Destructive Malware:** FoxBlade, Lasainraw (IsaacWiper), DesertBlade, malicious use of SecureDelete utility **Number of Destructive Incidents:** 22
Week 2 (March 3-9)	**Distructive Malware:** none **Number of Destructive Incidents:** 0
Week 3 (March 10-16)	**Destructive Malware:** FoxBlade, malicious use of SecureDelete utility **Number of Destructive Incidents:** 4
Week 4 (March 17-23)	**Destructive Malware:** DesertBlade, FiberLake, SonicVote, malicious use of SecureDelete utility **Number of Destructive Incidents:** 6
Week 5 (March 24-30)	**Destructive Malware:** FoxBlade, SonicVote, malicious use of SecureDelete utility **Number of Destructive Incidents:** 3
Week 6 and beyond (March 31 – April 8)	**Destructive Malware:** CaddyWiper, Industroyer 2.0 Number of Destructive Incidents 2

ההיערכות המוקדמת להגנה על אוקראינה והשפעתה

עד לפלישה עצמה התרחשו מה שניתן להגדיר **כשני גלים של מתקפות סייבר,** שהתאפיינו במגוון *כלי מחיקת מידע*, מתקפות *"מניעת שירות"* מסוג DDOS[2] על שירותים אינטרנטיים, ופעילות תעמולה והשפעה ברשתות חברתיות. לפני ובמהלך מתקפות אלו התגבש שיתוף פעולה מוגבר בין גורמי הגנה צבאיים ואזרחיים במערב, באוקראינה ובארצות הברית, על מנת לסכל את המתקפות הרוסיות. מצויות אינדיקציות רבות לכך שכבר בדצמבר 2021

1 "An overview of Russia's cyberattack activity in Ukraine", Social Report, Microsoft, 27.4.22.

2 מתקפות "מניעת שירות" (DDOS) הינן מתקפות לשיתוק החיבוריות לאינטרנט של רשת, ארגון או אתר אינטרנט, המתבססות על יצירת עומס בקשות רשתי. מתקפות DDOS מתאפיינות בהשפעה זמנית בזמינות השירות ובנזק נמוך וחולף יחסית.

החל להתגבש ולהתעצב שיתוף פעולה בין ארגוני הביון המערביים, חברות הענן והסייבר ופיקוד הסייבר האמריקאי, בניסיונות לסכל כלי סייבר רוסים. שיתוף פעולה זה יהפוך בהמשך לשיטת הפעולה הרווחת של כוחות המערב.

בתחילת דצמבר 2021 נשלח תחת מעטה סודיות לאוקראינה כח "סיכול איומי הסייבר" הגדול ביותר מסוגו עד היום, המורכב מעשרות חיילים מגיני סייבר (שילוב של אנשי מארינס והצי), בניצוח פיקוד הסייבר האמריקאי, והחל לעבוד כתף אל כתף עם האוקראינים ברשתות הממשלה, הצבא והתשתיות הקריטיות.זאת, תוך שיתוף פעולה עם הרשות האמריקנית הפדרלית לביטחון הסייבר, ה־NSA, פיקוד הסייבר האמריקאי ותאגידי הענן והסייבר. הערכה סבירה היא, שעוצמת ההישג הרוסי במתקפות המתעתדות לבוא הופחתה במידה ניכרת בעקבות החיכוך והלמידה המוקדמים שביצעו המעורבים עוד לפני תחילת התקיפות, באמצע ינואר 2022.

תקיפות הסייבר המקדימות לפלישה

התקיפות המקדימות לפלישה כללו מגוון נוזקות, מניעת שירות "מנגד" (DDOS) ואמצעים תודעתיים ותעמולתיים. ההתקפות הופעלו נגד חברות אחסון האתרים של עשרות האתרים הגדולים במדינה, משרדי ממשלה, ארגוני חברה אזרחית וחברות טכנולוגיה, במטרה לגרום להן נזק תפקודי. עיקרן היה השחתת אתרים.[3] המתקפות כללו שימוש בנוזקת מחיקה חדשה (בשם שניתן לה מאוחר יותר WhisperGate), ששימשה להשבתת שרתים ומחשבי ארגונים המארחים אתרי אינטרנט ומדיה בזמן שמסרי הפחדה הושתלו באתרים עצמם.

המתקפה הראשונה, ב־14 בינואר, הייתה תגובה לסיום סבב שיחות עקר בין רוסיה לארצות הברית, אוקראינה האיחוד האירופאי, ונאט"ו. הגל השני, הסמוך יותר לפלישה, כלל ניסיון לייצר נזק נרחב לשירותי מידע ציבורי וממשלתי, בדגש על שני הבנקים הגדולים באוקראינה. בניסיון שיתוק זה נראה שילוב יצירתי בין רכיבי "מניעת שירות" לשירותים הדיגיטליים של הבנק הגדול במדינה לבין הונאה באמצעים רשתיים על ידי שליחה המונית של הודעות SMS שדיווחו על אודות תקלה טכנית בכספומטים, וכן מיילים שהזהירו מהטמנת פצצות בסניפי הבנקים בערים הגדולות. במקביל הוצגו על מסכי המחשבים הנתקפים הודעות כופרה, ובהן דרישה לתשלום תמורת שחזור הקבצים שנמחקו או הוצפנו על ידי התוקפים.

3 השחתת אתרים (Defacement) – תקיפה של אתר אינטרנט שמטרתה, על פי רוב, היא החלפתדף הבית של האתר בדף המכיל מסרים של התוקף.

מתקפות במקביל לפלישה

התקיפות הסימולטניות לפלישה הוכנו ו"הותקנו" ימים ושבועות מראש ברשתות הארגונים הנתקפים ונמשכו במקביל להתפתחות הקרבות. מטרות התקיפה היו לגרום נזק על ידי מחיקת מידע נרחבת ברשתות אדמיניסטרציה ממשלתית, מגזר הפיננסים והאנרגיה, וקבלנים ממשלתיים מתחומים שונים, וכן יעדים ייחודיים דוגמת מעברי גבול סוכנויות ידיעות. בשלב זה נעשה שימוש באוסף חדש של נוזקות שהעיקרית בהן, HermeticWiper, היא נוזקה איכותית וכתובה היטב, בעלת יכולת התפשטות אוטונומית ברשת, שהותקנה בעשרות עד מאות רשתות ארגוניות.

בחודשים שלאחר מכן היו ניסיונות מהצד הרוסי לשבש נקודתית באמצעות נוזקות את תפקודם של ארגונים ושירותים: משרדים ושירותים ממשלתיים, תשתיות לאומיות ותשתיות מחשוב, אנרגיה , מדיה, ספקיות תקשורת, עסקים פרטיים, ועוד. ואולם הרושם הכללי הוא, שכוחות הסייבר הרוסים פעלו באופן ספוראדי וללא הישג משמעותי.

תקיפת ספקית התקשורת הלוויינית ViaSat

כשעה לפני הפלישה יזמו הרוסים מהלך שנועד לפגוע בפיקוד ושליטה האוקראיני הצבאי, על ידי שיתוק לצמיתות של כ־40 אלף טרמינלים לווייניים צבאיים ואזרחיים ברחבי אוקראינה. על פי פרסום רשמי של מחלקת המדינה האמריקאית, מטרת התקיפה הייתה "עיוור" של מערכות שליטה ופיקוד צבאיות אוקראיניות בתוך אלחוט לווייני. הטרמינלים שייכים לחברת ViaSat, שהינה חברה אירופאית בבעלות אמריקאית, המספקת באופן מוצהר שירותים דואליים (אזרחיים וצבאיים), שהצבא האוקראיני היה לקוח שלה.

תקיפה זו חייבה הכנות מבצעיות ומחקר מעמיק מהצד הרוסי, ועושה רושם שהופעלה על ידי גופים מבצעיים איכותיים ונפרדים מאלו שהפעילו את ההתקפות האחרות. הכח התוקף עבד במשך תקופה להשיג אחיזה ברשת הניהול המרוחק של הטרמינלים בלב חברת האם, פיתח פוגען ייעודי לטרמינלים אלו, ובהפעלה מתוזמנת התקין את הנוזקה כ"עדכון תוכנה" מרוחק וסלקטיבי רק למודמים בשטח אוקראינה. ההתאוששות היתיה איטית עד בלתי אפשרית, מאחר שהפגיעה התוכנתית מחייבת החלפת הטרמינל כולו והספקית נאלצה לשלוח פיזית לאוקראינה אלפי טרמינלים חדשים.

סיכול המתקפות על ידי המערב

מהלך הסיכול האפקטיבי של מתקפות אלה, שכאמור הוכן במידה רבה מראש, התבסס על שלושה רכיבים עיקריים:

1. פעולת צייד והגנה לחשיפה ולהסרת הנוזקות הרוסיות במהלך התקנתן וטרם הפעלתן בשטח, אשר שילב מודיעין מקדים ושותפות של חברות אבטחה.
2. מבצע משותף עם חברת אמזון ל"מילוט פיסי" של המידע הממשלתי הקריטי, אותו ניסו הרוסים למחוק במקביל לפלישה הצבאית.
3. פעולה משותפת עם חברת star-link, בבעלות אילון מאסק, למתן מענה מיידי לצורך תקשורת לווינית צבאית, לאחר ההתקפה הרוסית המוצלחת ששיתקה את תשתית הלווינות של חברת ViaSat.

שלוש פעולות אלו, שמייצגות היטב קשת מגוונת ורובסטית של מענים יצירתיים והפרואקטיביים של שחקני ההגנה, שמטו במפתיע את הקרקע מתחת לפעולות הסייבר הרוסיות.

חלקן של חברות פרטיות בפעולת סיכול זו היה גדול וקריטי. חברות אלה דיווחו על הנוזקות שניסו הרוסים להשתיל במערכות של ארגונים אוקראיניים; פעולה ישירה של מיקרוסופט חברות אנטיוירוס, בשיתוף האוקראינים, סיכלה מה שעלול היה להיות מחיקה רחבה ועמוקה יותר של הנכסים הדיגיטאליים הממשלתיים. בלט במיוחד המבצע למילוט המידע הקריטי האוקראיני לענן המערבי: ביום הפלישה התקיימה בשגרירות אוקראינה בארצות הברית פגישה בהולה בין מנהלים בכירים באמזון לבין השגריר האוקראיני. בפגישה העלו האוקראינים חשש כי יגרם נזק בלתי הפיך למאגרים הדיגיטליים של המדינה, הן באמצעים קינטיים והן דיגיטליים. עד הפלישה, מדיניות הגנת המידע של אוקראינה חייבה אחסון מידע קריטי אך ורק בשטחה הריבוני, משקולי עצמאות וחוסן.

בפגישה הוחלט על אודות מבצע "הצלה" למאגרי מידע קריטיים, שבמסגרתו הוברחו דרך פולין מתקני שינוע פיסיים מתוצרת אמזון, שכל אחד מהם מסוגל להכיל 80TB של מידע. במבצע ראשון זה הוברחו מרשם האוכלוסין, רישומי בעלות קרקעות (טאבו), רישומי המיסים והחינוך. מתקני השינוע נטענו במידע הקריטי ונשלחו למרכז של אמזון בדבלין, שם נטענו לענן AWS של אמזון. זו הייתה הסנונית הראשונה של "המילוט לענן", אשר בישרה את המשך נדידת מערכות המחשוב הקריטיות והממשלתיות באוקראינה לשירותי הענן המערבי, ככל שניתן. מאוחר יותר יתייחס למבצע זה מיכאלו פדרוב, השר האוקראיני לטרנספורמציה דיגיטאלי: "הנהגת AWS (שירות הענן של אמזון) קיבלה החלטה שהצילה

את הממשלה והכלכלה האוקראינית... מה שאנחנו הכי אוהבים בשותפות הזו עם חברות ענן הוא שהטילים הרוסיים לא יכולים להרוס את הענן״.[4]

כשעה לפני הפלישה שיתקו הרוסים באופן מוצלח את התקשורת הצבאית הלווינית האוקראינית. ככל שנקפו השעות התברר שהנזק אינו בר שיקום ונוצר חשש שניתוק הלוויין בשילוב אמצעים אלקטרוניים ישאיר את הצבא האוקראיני עיוור ונעדר תשתיות תקשורת אופרטיבית. על רקע זה פנו האוקראינים ל־SpaceX של אילון מאסק על מנת שיספק להם תקשורת לויינית אמינה ובטוחה באמצעות שירות הלוויינות נמוכת המסלול Starlink. מאסק נענה בחיוב ואספקת שירות זה שיפרה משמעותית גם את החיבוריות לאינטרנט האזרחי וגם התקשורת הצבאית.

תפיסת הסייבר הרוסית

מתוך ההחשיבה הרוסית, שלפיה המערב מנהל מאבק חתרני לערעור המשטר ברוסיה במגוון כלים כלכליים, סוציו־פוליטיים ותרבותיים, התפתחה חשיבה על מענה שמכונה לעיתים ״הגנה אקטיבית״, מתחת לסף המלחמה המיועד לנצל את החולשות במערכת המערבית לערעור מתמשך של יכולתה להמשיך לפגוע בחוסנה של רוסיה.

במסגרת זו מתמקדים הרוסים ב״לוחמת מידע״ (information warfare), המכוונת להשיג עליונות לצורך השפעה ולשיבוש מערכות המידע והרשתות, התהליכים והתפיסה הפסיכולוגית של היריב האזרחי והצבאי כאחד. בדיסציפלינה זו מתקיימת אבחנה בין ״מבצעי מידע״ למבצעי ״סייבר התקפי״, שבעצמם מחולקים ל־״סייבר פסיכולוגיים״ ומבצעי ״סייבר טכניים״. כלומר, גם אם מבצעי ה״סייבר הטכניים״ מכוונים ליצירת אפקטים טכנולוגיים (תקשורתיים, אנרגטיים וכו׳), מבחינה ארגונית ותפיסתית הם מהווים תת־קבוצה בקבוצה רחבה של כלים לתכליות של לוחמת המידע, המיועדים להשגת אפקטים קוגניטיביים ופסיכולוגים על כח האדם, האזרחים וקבלת ההחלטות של היריב.

לדברים אלה נודע החל מ־2013 הד באמירותיו של הרמטכ״ל הרוסי, ואלרי גראסימוב, שבתפיסה שהציג ביחס לשדה המערכה המתקדם הודגשו כלים ומבצעים שאינם קינטיים, מתחת לסף המלחמה, והם בעלי יכולת הכחשה, ליצירת הרתעה ופירוד אצל היריב. למרות

4 Katherine Tangalakis-Lippert , ״Amazon helped rescue the Ukrainian government and economy using suitcase-sized hard drives brought in over the Polish border: ׳You can׳t take out the cloud with a cruise missile׳״, *Insider*, 19.12.22.

הוויכוח על אודות מקורות החשיבה הרוסית והמקום של אסטרטגיית לוחמת המידע והתודעה מול המערב, אין חולקים כל כך על כי היא רכיב מתמשך בחשיבה ובפעילות הרוסית.

כך השתמשה רוסיה בתקיפות סייבר בעימותים עם אסטוניה (2007) וגאורגיה (2008), בפלישה לחצי חצי־האי קרים (2014), בתגובה להפלת המטוס הרוסי על ידי טורקיה (2015), ובשיבוש המשחקים האולימפיים בדרום־קוריאה (2018), תוך שיבוש, מניעת שירות ומחיקה, שנועדו להשבית מערכות אזרחיות וציבורית מגוונות. הגישה המבצעית הרוסית כוללת הפעלת קבוצות אזרחיות למחצה או אזרחיות לחלוטין, אך התכליות עקביות וכוללות פרסום מסרי תעמולה ושיתוק של מערכות ציבוריות של היריב, במקביל לעימותים ופגיעה יצירתית במערכות מידע כגון סקרי דעת קהל ומערכת גיוס מילואים.

אירועים בולטים שלא במסגרת עימות מזוין כללו את החדירה האיסופית לרשת משרד ההגנה האמריקאי על ידי על ידי "שתילה" שלDisk on key נגוע בחניה של מתקן של משרד ההגנה במזרח התיכון, והכנסתו בשוגג שלו ללפטופ מסווג; ניתוק מאות אלפי בתי אב מחשמל באוקראינה בשתי תקיפות שונות ב־2014; מתקפות Non-Petya (2018), שכללו השבתת רשתות של עשרות אחוזים מתוך כלל העסקים באוקראינה, [34] וגרימת נזק מערכתי של מעל 10 מיליארד דולר, כולל נזק אגבי מחוץ לאוקראינה ודחייה של שנת המס האוקראינית; וכן החדירה הרשתית החשאית (לא התקפית) למאות ארגונים חברות ורשתות משרדי ממשל אמריקאי רבים באמצעות תוכנות החברה – SolarWinds (2020) כ"שרשרת אספקה" בסייבר. מתקפה זו נחשבת להשגת הגבול היחידה הגדולה ביותר בהיסטוריה.

המגבלות של מתקפת הסייבר באוקראינה והסיבות להצלחתה החלקית

בהנחה שההיגיון המערכתי שבבסיס הפלישה היה "עריפת בזק", והחלפה של ההנהגה האוקראינית, היה למתקפת הסייבר מקום צנוע בתוכנית הכוללת, ובהתאם השפעה קטנה על התפתחותה. נראה שתפקידי הסייבר בתוכנית היו:

- דמורליזציה והפחדה מול האוכלוסייה וההנהגה.
- השבתה ושיתוק של מערכות ממשלתיות וציבוריות ביממות של ההשתלטות (ייתכן שבהשראת הצלחת "פיגוע הסייבר" NotPetya, שגרם לאנדרלמוסיה ציבורית וכלכלית לא קטנה ביוני 2017).

- אמצעי לשיבוש הפיקוד והשליטה הצבאי על ידי השבתת טרמינלי הלווין האוקראינים של Viasat.

הכשלים העיקריים שניתן לסמן בתוכנית הסייבר הרוסית הם:

- תכנון קשיח לתרחיש אחד ללא גמישויות, בדומה לתוכנית הצבאית הרחבה יותר.
- המשך התבססות על נוזקות הפועלות על מחשבים ורשתות מקומיות ,ללא התייחסות למהפכת הענן.
- חוסר יכולת להתמודד עם החשיפה היעילה והמוקדמת של פעולותיהם הרשתיות על ידי המודיעין המערבי וההגנה המסיבית והפרואקטיבית.
- חוסר השקעה והבשלה של יכולות חלקיות שהחזיקו ברשתות החשמל האוקראיניות.

אפשרויות תיאורטיות שהרוסים לא מימשו:

לא נצפתה השתלטות אפקטיבית על מערך המדיה והתקשורת האוקראיני: מתקפות הסייבר על תקשורת שבוצעו כללו השתלטות ספוראדית על אתרי אינטרנט ורדיו אינטרנט וכן מבצעי תודעה ברשתות החברתיות. עם זאת, הן לא כללו השתלטות אפקטיבית על השידורים הציבוריים האוקראיניים, המופצים דרך לווין, משדרי VHF וסטרימינג אינטרנטי.

לא נרשמה פגיעה עמוקה בתשתיות לאומיות, כגון אנרגיה ופיננסים. למרות השהייה ארוכת השנים של הרוסים ברשתות האוקראיניות, נראה שלא הייתה תוכנית מקיפה כזו.

ייתכן שלמגבלות אלה גרמו עלויות פיתוח גבוהות של נגישות סייבר ואמצעי לחימה בסייבר, לעומת התחליפים הקינטיים הזמינים בתא השטח האוקראיני (שידורי הטלוויזיה באוקראינה הושבתו בהפצצה); הנחת יסוד בצד הרוסי, שמדובר במבצע תפיסת שלטון פיסי קצר ויעיל אשר אינו דורש תוכניות גיבוי יקרות נוספות, ואף תפיסת תפקיד הסייבר במשבצת מוגבלת למדי או אפילו מעיין "אינרציה" להמשיך ולהשתמש בתפיסות ובכלים הקיימים.

בנוסף, במערכה באוקראינה מצפתה השפעתן של ההתפתחויות האחרונות בעולם הדיגיטלי: המעבר של ארגונים מאחסון מקומי (on premise) לענן הופך את היכולות להשמדת "דיסקים קשיחים" לפחות אפקטיבית ומחייב התפתחות של סט יכולות מותאם; והיכולת של המערכות המתקדמות שפותחו כדי להתמודד עם תקיפות ה"כופרה", ומאבטחות טוב יותר את המערכות העניות והאוטומטיות.

מתקפות המחיקה הרוסיות בעשור האחרון התבססו על השבתה ומחיקה של אמצעי אחסון מקומיים בארגוני המטרה. על רקע זה, המעבר האוקראיני להתבססות על מחשוב ענן תוך כדי המלחמה שמט את הקרקע מתחת לגישה הטכנולוגית הנוכחית של מתקפות המידע הרוסיות. יש לצפות שמגמה טכנולוגית זו תימשך.

מגמות ומאפייני פעולה של המערב

- קביעת נורמות סייבר ונורמות אתיות על ידי התעשיה ואכיפתן על המדינות המשתמשות, למשל, על ידי ניתוק רוסיה מתשתיות הענן. כשבועיים לאחר הפלישה החלו להודיע כל חברות הענן והשירותים הדיגיטליים על אודות הפסקת מתן שירות ומכירות לרוסיה. כחלק ממערך הסנקציות התנתקו לא רק ענקיות הענן, אלא חברות תשתית דיגיטלית רבות נוספות דוגמת אורקל, סאפ, פיי־פאל.
- תשתיות גלובלית דואלית (צבאית ואזרחית) שיחקו תפקיד בלחימה. יש לצפות שמגמה זו תמשיך ותתמיד, בייחוד כשחברות הטכנולוגיה שייכות לצד אחד במאבק הבין־גושי. חברות התשתית מעורבות והן גם משמשת מטרות לתקיפה, כמו במקרה של ViaSat.
- גיוס מערכות ההגנה וזיהוי האיומים של הענן הדיגיטלי ככלי במערכת סייבר צבאית. היכולת של שירותי הענן לאסוף מודיעין טכנולוגי על כלל נקודות הקצה באינטרנט, ושותפות של גופי "מחקר האיומים" של התאגידים במערכה, הבשילו לפעולה מסונכרת ואפקטיביות במאבק הסייבר. ההודעות והדוחות הרשמיים שפרסמו מיקרוסופט, גוגל, מטה, Fire-eye וחברות האנטיוירוס, הינם מהמקורות המפורטים הבודדים בנמצא.

לקחים ומשמעויות לישראל

סייבר כסימן מתריע: מתקפות הסייבר הרוסיות הופיעו, באופן מעניין, כסימן המקדים הראשון לפלישה כולה, עם התקנה ופרישת פוגענים "טריים מהמדף" כיממה לפני הפלישה. עלייה כזו בפעילות רשתית כהכנה למתקפת סייבר יכולה לשמש סימן מעיד ליוזמת תוכנית "פתע". על מנת להפעיל התקפות סייבר סימולטנית עם תוכנית כוללת, חייב התוקף לערוך הכנות חשאיות ברשתות הנתקף לפחות יממות מראש. קיים סט של אילוצים המאריך את "זמן היזימה" של מתקפת סייבר, כגון הכרח לוודא אחיזה במערכת הנתקפת, להתקין נוזקות ולוודא את תקינותן וכן זמני חילחול פקודות ברשת היעד. בנוסף נדרש התוקף

לעבוד בתצורה של "גלים" מול קבוצות מטרות בו זמנית, על מנת לצמצם את זמן חשיפה של נוזקות למערכות הגנה.

תופעה נוספת היא "אשליית חשאיות" של יחידות התקיפה בסייבר, אשר בהשפעתה ניתן להגביר פעילות באופן לא מחושב. במקרה של הפלישה לאוקראינה, הביטוי לכך היה החשיפה בטוויטר של פעילות מוגברת על ידי החברות ESET ו־SYMANTEC באחר הצהרים של היממה לפני הפלישה.

כתוקף, יש היגיון לתכנן את התוכנית הטכנולוגית כך שתצמצם את היקף ההתראה וזמני ההתראה למגן. בצד המגן, יש להבין ששיפור מודעות מצבית מול פעילות חשאית של האויב ברשתות יכול לשמש כלי להתראה אופרטיבית ו/או לחשוף ממד של תוכנית אופרטיבית שלמה יותר של היריב. תחום נוסף שראוי לנתח וללמוד ממנו הוא עבודת הסיכול המשולבת של כוחות ההגנה המערביים, ששילבו פרואקטיביות, פעולה עתירת מודיעין ושיתוף עמוק של חברות אזרחיות טכנולוגיות ליצירת ייתרון יחסי עצום על התוקפים.

המידע המדינתי כיעד אסטרטגי: מצד התוקף עולה ההזדמנות להשתמש במידע הקריטי ובפונקציות הקריטיות של האויב לא רק כיעד למחיקה ולשיבוש אלא כמנוף לחץ על היריב ו"כופר", או כבן ערובה אסטרטגי באנלוגיה לשטח בזמן לחימה קינטית. בכך יש לסייבר ייתרון מובנה על נשק קינטי מכיוון שהאפקט "הפיך" וניתן להחזיר גם את המידע בהחלטה. יש לבחון את הרעיון שנעילה של מערכות הפיננסים, האנרגיה והתקשורת יכולה לשמש מנוף לחץ בתרחיש הסלמה לקראת לחימה או במשא ומתן לסיומה.

הענן הציבורי הישראלי כיעד לתקיפה אסטרטגית עתידית: בתרחיש האוקראיני, בו התממש איום פיסי ודיגיטלי חריף ומיידי, התגלו יתרונות הענן הגלובלי נטול הטריטוריה – חסינות ממתקפה פיסית, חסינות יחסית ממתקפת סייבר בכלי מחיקה פשוטים, וכן יכולת התאוששות ושחזור מהירות. לענן יש כמובן גם חסרונות, בראש ובראשונה נדרש לקחת בחשבון תרחיש של "התקפת סייבר אסטרטגית" או אפילו "כופרה אסטרטגית" על המידע הלאומי, במטרה להפעיל לחץ על מדינת ישראל. יש לעצב מדיניות וכלים להתמודדות עם "כופרה אסטרטגית" שכזו.

ישראל נמצאת בתהליך של בניית ענן ציבורי משותף עם אמזון וגוגל, בשם "נימבוס", שבמסגרתו יבנו מרכזי אחסון בשטח מדינת ישראל, שיוכלו מצד אחד לספק שירותי ענן ציבורי אינטרנטי מודרניים ומצד שני לעמוד במדיניות אבטחת המידע הישראלית. יש לבחון את גישת אבטחת המרכזים האלה, במחשבה שהם עלולים להיות יעד ל"מתפס" אסטרטגי בניסיון להשמידם או להצפינם.

בנוסף, אפשר ללמוד ממבצע ההצלה האוקראיני במסגרת ניסיון לשפר את תוכניות החרום להתמודדות עם מתקפת מידע אסטרטגית, למשל לגבי תיעדוף מאגרי המידע שביצעה אוקראינה תחת מתקפה בזמן אמת. לפי הידוע לנו אוקראינה בחרה להבריח פיסית את מרשם האוכלוסין, מאגר הטאבו, רישומים רפואיים ועוד.

פרויקט הענן הציבורי הישראל נמצא רק בשלבים ראשונים של התפתחות ואויבי הסייבר הנוכחיים של ישראל אינם מתקדמים מספיק על מנת להפוך תרחיש כזה לאיום מיידי, אך תשתית הענן ותוכניות האבטחה של ישראל הן פרויקט שיתפתח ויתעצב לאורך עוד שנים רבות ויש לסמן איומים עתידיים אפשריים כמצפן תכנוני.

המשמעויות לישראל של המגמות ביחסים עם תאגידי הטכנולוגיה

נדרש לשאול כיצד מנהלת ישראל מדיניות מול התאגידים הטכנולוגים עתה, כשהם צד פעיל יותר גם בלחימה וגם באכיפת נורמות בינלאומיות – ולעיתים ללא המנגנונים המסורתיים של הממשל, הקונגרס והממסד הצבאי.

תאגידי הטכנולוגיה הינם לא רק כלי חדש לאכיפה של נורמות וסנקציות, אלא הם בעלי מערכות אינטרסים עצמאיות ויכולת קבלת החלטות עצמאית במידה רבה. כחצי שנה לאחר המהלך למתן שירותי Starlink חינם באוקראינה, פנתה החברה במכתב לפנטגון ובו התריעה שלא תוכל "לשלם את החשבון יותר", ודרשה מימון בשיעור מאות מיליוני דולרים להמשך השירות. דינמיקה כזו דורשת התחשבות ותכנון נכון של פעולות, הן בתחום הסייבר והן בתחום המדיני והצבאי הרחב יותר, בכלל הזירות. ניהול המדיניות צריך לכלול צעדים אקטיביים לחיזוק הלגיטימציה וחופש הפעולה, וגם לקיחה בחשבון של תרחישים שבהם מוטלות סנקציות והגבלות על שירותי תשתית הענן שזמינים למערכות התעשיה והממשל בישראל. ישראל צריכה לנהל מאמץ לגיטימציה ושיתופי פעולה על מנת להבטיח את המשך שיתוף הפעולה עם שירותי הענן בכל תרחיש, גם מסיבות כלכליות וגם מסיבות תפקודיות.

השותפות של איראן בציר ההתנגדות היא התחלה טובה, המקנה לישראל נקודות זכות, אך בתרחיש שישראל תבקש להנחית מכת סייבר (או לא בסייבר) מדינתית יהיו לכך השלכות על כלל המערכת הדיגיטלית הבינלאומית. כיצד נערכים לכך? כיצד שומרים על הלגיטימיות כשחקן אחראי וגם על היכולת לפעול באגרסיביות אם נדרש, והאם יש משמעויות לתעשיית הסייבר הישראלית, למשל ההתקפי?

השלכות אפשריות של הסלמה במלחמות הסייבר הבין גושיות למגן הישראלי

מסתמנת אפשרות, שמלחמת הסייבר הבין גושית – מדינות "ההתנגדות" מול ארצות הברית ונאט"ו – תלך ותסלים, כך שתהיה מתחת לסף של מלחמה כוללת אך תצמח לממדים חדשים. תאגידי הענן לקחו צד בעימות, תשתיותיהן פזורות ברחבי הגלובוס והן פגיעות למתקפות סייבר. בנוסף, גם תחום הלווינות המתחדש (לווינות תקשורת בגובה נמוך) יכול להיות חשוף לתקיפות סייבר הן בלחימה והן מחוץ לה. האם נראה בעתיד ניסיון לאתגר את הסדר החדש על ידי "השמדה" של אחת מספקיות הענן או הלווינות, או "כופרה אסטרטגית" נגדה?

בתרחיש כזה, ארצות הברית תצטרך להחליט כיצד להגיב, והאם התגובה תהיה מתקפת סייבר עוצמתית או הפעלת אמצעים אחרים. מדינת ישראל צריכה לשקול את המשמעויות עבורה כשותפה במארג הענן והטכנולוגיה המערבי ויכולה להיות חשופה למתקפות כאלו, בעקיפין או באופן ישיר.

בעוד מדינת ישראל צריכה להמשיך למצוא את האיזון בין הגושים במציאות שהלחצים לבחור צד עולים, יש לקחת בחשבון שבתחום המידע והטכנולוגיה ישראל מתבססת ומושקעת עמוק כלכלית, טכנולוגית וביטחונית באופן מובהק בצד תאגידי ה־Big Tech האמריקאיים.