תווך הסייבר / ד"ר אייל פינקו

מבוא

מלחמת רוסיה-אוקראינה פרצה רשמית עם כניסת כוחות רוסיים לאוקראינה ב־24 בפברואר 2022. הצבא הרוסי החל בהכנות לפלישה כחודש לפני, ובסיומו של אימון רב־זרועי בן עשרה ימים במהלכו ערך כמה התקפות סייבר מקדימות.

המערכה באוקראינה, המתנהלת עד כתיבת שורות אלה, לוותה באירועי סייבר רבים ומתוקשרים היטב, ובהסברים על אודותיהם והשלכותיהם מפי מיטב המומחים העולמיים. אלה ציינו כי מלחמת הסייבר שינתה את פני המערכה הצבאית והשפיעה עליה, ואף כונתה בראשיתה "המלחמה הדיגיטלית הראשונה". אין לכינוי כל בסיס מציאותי, שכן כבר ב־ 2014 התנהלה מערכה רחבה בסייבר בין רוסיה ואוקראינה.

מאמר זה ינתח את תפקיד תווך הסייבר במהלך המלחמה ומה ניתן ללמוד מהן בעידן המלחמה המודרנית.

בפתח הדברים אציין מגבלה קריטית בבסיס המידע המצוי. תיאורי תקיפות של שני הצדדים – הרוסי והאוקראיני – נסמכים על דיווחים תקשורתיים בלבד ופרסומים שהחליטו שני הצדדים לפרסם, כל אחד בהתאם למטרותיו ויעדיו. הם משמשים לא מעט ליצירת אפקטים תודעתיים במסגרת הלוחמה הפסיכולוגית ביניהם וכלפי העולם הרחב. כפי שראינו במלחמה עד כה, ההונאה משני הצדדים רבה, תעמולת הכזב (פייק ניוז), הדיס־אינפורמציה

והמיס־אינפורמציה שולטים בזירת הלחימה, עד שאי אפשר לדעת מי מהצדדים דובר אמת, אם בכלל.
יתרה מכך, הפרסומים מתייחסים לתקיפות רועשות, שתוצאותיהן ניכרות וברורות לעין. אין בסיס מידע אמיתי על מספר התקיפות השקטות, אלה שחדרו למערכות המחשבים של שני הצדדים לטובת איסוף מודיעין או לכל הישג אחר, שאין כוונה לחושפו לעין.

תקיפות סייבר לקראת המלחמה

כבר מ־2014 ניהלה רוסיה מערכה נמוכת עצימות של תקיפות סייבר נגד אוקראינה – הן תקיפות מודיעיניות (איסוף מידע), הן תקיפות תודעה (הפצת תעמולה רוסית) והן תקיפות לגרימת נזק לתשתיות (בין היתר נפגעו שלוש תחנות כוח לייצור חשמל). אולם תקיפות הסייבר שאפשר לשייכן למלחמה הנוכחית החלו כחודש וחצי לפני פרוץ הקרבות הקרקעיים. בראשית ינואר 2022 הזהיר מערך הסייבר הלאומי האמריקני את אוקראינה, כי תשתיות המדינה הקריטיות שלה תחת איום תקיפת סייבר.
כיומיים לאחר האזהרה הושחתו אתרים של משרדי הממשלה האוקראיניים (משרד החינוך, משרד הפנים, משרד החוץ ואתרים נוספים) ומסרים המזהירים את תושבי אוקראינה מפני רוסיה פורסמו בהם. שירות ביטחון הפנים האוקראיני טען כי במסגרת התקיפות לא נגנב דבר, אך בבדיקות שערכו גורמים אמריקניים וחברת מיקרוסופט התגלו וירוסים ברשתות האוקראיניות, בדגש על רשתות של תשתיות קריטיות כגון משרד הביטחון האוקראיני,

מתקני ייצור חשמל, מתקני גרעין ועוד. גם משרד הביטחון האוקראיני נפגע, כאשר מידע קריטי נמחק מרשתות המידע שלו. כשבועיים לפני המערכה נרתמה ארצות הברית, ושלחה סיוע של מומחים ופתרונות טכנולוגיים להגנת התשתיות האוקראיניות.

תקיפות סייבר רוסיות במלחמה

יום לפני פרוץ המלחמה וביומה הראשון החלו תקיפות סייבר רבות נגד התשתיות הלאומיות של אוקראינה, משרדי ממשלה והמערכת הבנקאית. מרבית התקיפות היו תקיפות מניעת שירות (DDoS – Distributed Denial of Service) והשחתת אתרים. אוקראינה שכבר ידעה סבל מתקיפות סייבר על חברת החשמל שלה במלחמה ב־2014, והשבתת החשמל בחלקים של אוקראינה למשך כחצי יממה דאז, כבר הייתה מוכנה במערכה הנוכחית.

בחודשים הראשונים של המלחמה ניסו הרוסים שוב ושוב לתקוף מטרות אסטרטגיות, מתוך תפיסה כי באמצעות הכנעת התשתיות הלאומיות שלה תיפול אוקראינה. אולם התקיפות לא צלחו. הרוסים הפעילו תקיפות שונות שעיקרן היה מחיקת מידע משרתים ומחשבים. נוסף על כך, הם תקפו מחשבים ככוח מסייע למהלכי הכוחות הקרקעיים או כוחות האש.

באפריל 2022, יום לפני ההתקפה לכיבוש תחנת הכוח הגרעינית האוקראינית בזָ׳פּוֹרוֹזְ׳יָה נערכו תקיפות סייבר על הרשתות הארגוניות של תחנת הכוח. תקיפות הסייבר לא השיגו את מטרתן, אך תחנת הכוח הגדולה במדינה נכבשה קרקעית. באופן דומה פעלו

הרוסים לשבש את תפקוד מפקדת זרוע האוויר של אוקראינה ששכנה בעיר וִינִיצְיָה (כמאתיים קילומטרים מדרום מערב לבירה קייב) – מ־4 במרס הם תקפו באמצעות סייבר את רשתות התקשורת במרחב, ובמהלך השבועות הבאים ירו מטחי טילים שנחתו בשדה התעופה ובמפקדה עצמה. כך היה בתקיפות הרוסיות על אתרי ממשל, צבא ותשתיות בעיר דְנִיפְּרוֹ, שהחלו במבצע סייבר שמנע שירות במחשבי המועצה ואתר האינטרנט שלה, ומיד אחר כך נורה מטח של 11 טילי שיוט על מטרות שונות בעיר.

עיון בחלוקת תקיפות הסייבר הידועות בחתך של מגזרים באוקראינה מראשית פברואר 2022 (כלומר, מספר שבועות לפני תחילת המתקפה הכוללת הרוסית) ועד אוקטובר 2022 מראה שמרבית התקיפות הרוסיות היו מכוונות נגד מוסדות שלטון (כולל צבא), תשתיות מרשתת (אינטרנט) ומגזר האנרגיה. עם זאת, בהשוואה לתדירות תקיפות הסייבר בשנתיים שקדמו למלחמה נמדדה ירידה ניכרת בתדירות ההתקפות מאז תחילת המלחמה.

בעקבות הפגיעה האוקראינית בגשר קרץ', המחבר את חצי-האי קרים לשטח רוסיה, ולאור כישלון תקיפות הסייבר על תשתית החשמל של אוקראינה, עברו הרוסים לתקוף תשתית זו בטילים ו-כטמ"מי-נפץ ותוך מספר שבועות פגעו בכ-40% ממנה – אם כי בגלל שתשתית זו נבנתה עם יתירות רבה ותודות לסיוע מהאיחוד האירופאי, ההשלכות של פגיעה זו היו מצומצמות יחסית והאוקראינים הצליחו להשיב את שירות החשמל לחלק ניכר מהאזורים שהוחשכו.

כמו כן, באמצעות המדיה החברתית ותקיפת אתרי חדשות ורדיו יצרו הרוסים וניהלו במשך חודשים רבים (עד היום) מבצעי השפעה בקנה מידה נרחב של דיס־אינפורמציה ותעמולת כזב נגד השלטון האוקראיני ונאט"ו.

בו בזמן ניהלו הרוסים מבצעי תקיפה באמצעות סייבר נגד ארצות הברית, בריטניה, גרמניה, פולין, לטביה ומדינות אחרות. מרבית המבצעים נועדו להשבית תשתיות לאומיות, אך גם לייצר הרתעה לבל יתערבו במערכה.

תקיפות סייבר אוקראיניות במלחמה

האוקראינים הגיבו גם הם, ובימים הראשונים למלחמה השחיתו אתרי ממשלה רוסיים, יצרו תקיפות מניעת שירות נגדם, תוך שהם מנסים ליצור הבנה ברוסיה כי יגיבו על התוקפנות הרוסית גם בתווך הסייבר. הנשיא האוקראיני ולודימיר זלנסקי אף קרא להאקרים מרחבי העולם להתגייס לצבא הסייבר האוקראיני, לסייע לה לתקוף אתרים ותשתיות רוסיות ולהיות חלק מהמערכה על התודעה בתווך הסייבר.

האוקראינים פעלו רבות בתווך הסייבר ליצירת השפעה על אזרחי רוסיה. ההאקרים האוקראינים, יחד עם עזרה מפעילי קבוצת אנונימוס, פרצו לאתרי ממשל רוסיים, שלחו הודעות עם מסרים לטלפונים הסלולריים של אזרחים רוסים בגנות המלחמה, פרצו לאתר הטלוויזיה הרוסית ושידרו בו מסרים ואף פרצו לאתר סוכנות החלל הרוסית. חברי קבוצת אנונימוס טענו כי הצליחו לחדור

ולהוריד את אתר שירות המודיעין הצבאי הרוסי, ה־FSB. מתקפות דומות נערכו במהלך כל ימי הלחימה על ידי האקרים אוקראינים ומתנדבים מחוץ למדינה שהגיעו לעזור מתוך מטרה להשפיע על דעת הקהל העולמית והרוסית, ולהפסקת המלחמה.

איסוף מודיעין בתווך הסייבר

מטרתו של המודיעין הצבאי במערכה הוא לאסוף מידע על אודות יכולות היריב, מהלכיו ותכנון המערכה שלו מחד גיסא, ולאסוף מודיעין למטרות, כלומר מיקום כוחות היריב כדי לאפשר את עצירתם והשמדתם במהירות וביעילות, למנוע תמרון ויכולתו להפעיל כוח אש מאידך גיסא.

המודיעין הצבאי נאסף לפני המלחמה ובמהלכה באמצעים שונים, כגון מודיעין אנושי (יומינט), מודיעין אותות (סיגינט), מודיעין חזותי (ויזינט) ובאמצעים שונים נוספים. השימוש הנרחב בתווך הסייבר – באינטרנט, מאפליקציות וברשתות תקשורת פתוחות, הוא פתח לאיסוף מודיעיני נרחב – האוסינט, האיסוף מאמצעים גלויים. לאיסוף המודיעין האוסינטי יש יתרונות רבים כאשר מידע רב קיים ברשתות החברתיות, באפליקציות שונות ובאתרי אינטרנט, להם יש לכולם נגישות ובשימוש בהם מותירים חתימה. מידע זה ניתן לאיסוף ולניתוח באמצעים טכנולוגיים שונים במהירות יחסית ובדיוק גבוה. עם זאת, קשה לעיתים לדעת מתי המידע שנאסף הוא אמין, מדויק, ומקורו אינו בהונאה של היריב.

בשנת המלחמה הראשונה עסקו שני הצדדים באיסוף מודיעין גלוי ממספר סוגים. הראשון בהם הוא איסוף מידע מרשתות חברתיות ואפליקציות מסרים, כאשר חיילים העלו תמונות וסרטונים ממקומות ששהו ופעלו בהם. ניתוח המידע סייע לשני הצדדים, אבל בעיקר לצד האוקראיני, להבין ולזהות את מיקומי הכוחות היריבים, לייצר מהם מטרות בזמן קצר יחסית ובהתאם למיקומם להפעיל נגדם חימושים. במהלך יוני 2022 דיווחו הרוסים על כוונתם לסגת, אך תמונות וסרטונים שהעלו חיילים רוסים לרשתות החברתיות הצביעו על שהם אינם נסוגים והפרסום הוא מהלך הונאה בלבד.
קבוצת תקיפה רוסית בשם ארמגדון השתמשה בתקיפות ממוקדות ומבוססות מודיעין ככל הנראה, אזרחים וארגונים באוקראינה כדי לאסוף מודיעין על אודות הלך הרוח במדינה, ומידע תשתיתי נוסף שיסייע להם במערכה היבשתית ובהשבתת התשתיות הלאומיות.
הממד השני הוא מידע חזותי, ובעיקר באמצעות רכש של תמונות לוויין המוצעות למכירה במחיר נמוך יחסית באתרים שונים. המידע החזותי שימש בעיקר לטובת חילול מטרות לתקיפה, והבנה על תמרון היריב. איסוף החוזי מאתרי אינטרנט המפעילים לווייניים הפך להיות הלוויין החדש של מדינות שאין ברשותן לווייני צילום.

דיון

המלחמה באוקראינה אינה הראשונה שבה התנהלה מערכה מקבילה בתווך הסייבר. אולי דווקא החיבור שבין התווך הווירטואלי לתווך

הפיזי הוא שהופך את הסייבר למרכיב בסל המרכיבים של המלחמה המודרנית, שמדינות וארגונים רבים חפצים להפעילו.

במלחמה ב־2014 השתמשו הרוסים בתווך הסייבר כדי ליצור אפקטים שיעזרו להם במערכה היבשתית. הדוגמה הבולטת הייתה התקיפה על מערכת החשמל האוקראינית, שהשאירה כרבע מיליון בתי אב ללא חשמל במשך שעות ארוכות. תקיפה זו נערכה על חברת החשמל האוקראינית כשנה וחצי לפני המהלך הצבאי, והותירה ברשת החשמל דלת אחורית שתאפשר לרוסים להפיל את הרשת בתזמון הרצוי להם.

תקיפות מסוג זה המבוצעות נגד תשתיות לאומיות, מתקיימות מתוך התפיסה שהן מייצרות אפקטים פסיכולוגיים, כלכליים וצבאיים, המסייעים למערכה הצבאית הפיזית. תקיפות כאלו לוקחות זמן, והן אינן תקיפות בזמן אמת כמו אלה הלקוחות מסרטי "משימה בלתי אפשרית". כדי לייצר תקיפת סייבר על תשתית לאומית בעיקר, נדרש איסוף מודיעין על היעד במשך זה רב, הכנת דרך פעולה מבצעית והחדרת פוגען מתאים (על בסיס המודיעין), שישהה ביעד בחשאי עד זמן ההפעלה הנדרש בתזמון ובמקום הנכון עבור המפעיל.

האוקראינים והאמריקנים, שהבינו את דפוס הפעולה הרוסי לאחר 2014, העלו את רמת האבטחה של התשתיות הלאומיות האוקראיניות. על כן רוב תקיפות הסייבר הרוסיות שנועדו לסייע להם במהלך הקרקעי, ככל הנראה נכשלו. בהתייחס כמובן למגבלות המידע המפורסם ולמהלכי ההונאה משני הצדדים, אפשר להסיק כי

במערכה הזו, שלא בדומה למערכה הקודמת, לסייבר לא היה תפקיד ממשי בהשבתת יכולות ותשתיות לאומיות. למעשה, על אף שהרוסים הצליחו למחוק מידע משרתים וממחשבי קצה (ולטענת האוקראינים רוב המידע שאבד היה מגובה באופן לא פגיע לתקיפות סייבר), הישגיהם היו דלים ובעיקר הציקו וגרמו לכאבי ראש לצד האוקראיני.

עם זאת, הסייבר במערכה באוקראינה יצר אפקטים תודעתיים ופסיכולוגיים שהשפיעו על השיח הציבורי העולמי, על נאט"ו ועל האוכלוסיות בשתי המדינות. תקיפות הסייבר הרוסיות יצרו דה־לגיטימיזציה נגדם, ואפשרו לאוקראינים לקבל סיוע נוסף בתחום הגנת הסייבר ממדינות העולם. מצד אחר תקיפות הסייבר הרוסיות יצרו תחושת חרדה באוקראינה, שקשה לבודדה מסך כל תחושות הפחד והחרדה של האוכלוסייה המקומית.

התקשורת העולמית, ברובה, נתנה לגיטימציה לתקיפות הסייבר האוקראיניות ברוסיה, עודדה אותן ואף לא הסתייגה ממהלכי הנשיא האוקראיני כאשר קרא להאקרים מרחבי העולם להצטרף למערכה. קבוצות התקיפה הרוסיות, המושתתות על אזרחים, זכו מנגד לגנאי ולגינוי.

במהלך השנה הראשונה למלחמה הייתה לתווך הסייבר השפעה זניחה ביצירת אפקטים צבאיים, שיבוש והשבתה של תשתיות לאומיות, והפעילות המרכזית בתווך הסייבר של שני היריבים הייתה סביב יצירת השפעה, לוחמה פסיכולוגית ולחימה על דעת הקהל המקומית והעולמית. עניין משמעותי בנושא יצירת ההשפעה היה

למעשה תגבור יכולות התקיפה המדינתיות של שני היריבים על ידי גיוס האקרים, לעיתים אף גורמי פשיעה בתווך הסייבר, מרחבי העולם. זאת בשעה שהעולם לא מביע הסתייגות לשימוש בהם.

בתווך הסייבר שבו יכולות התקיפה משתנות מדי יום בהתאם לחולשות המתגלות וכלי תקיפה חדשים, למדינות אין לאו דווקא יתרונות מול תוקפים אזרחיים. מדינה יכולה להשקיע מאמצים, כספים ומשאבי אנוש למציאת חולשות, יכולות תקיפה ויכולות הגנה. אולם בעולם הזה הדבר אינו בהכרח מקנה למדינות עליונות בתווך הסייבר, מכיוון שבכל רגע נתון האקרים יכולים לאתר חולשות חדשות, zero days, המעניקות להם יתרונות על פני הצד המתגונן.

בשורה התחתונה מושג העליונות בסייבר, בניגוד למושג העליונות הצבאי, הוא רופף ודינמי, ועשוי להשתנות בקצב גבוה. על כן עניין גיוס האקרים חובבים או מקצוענים מקצווי תבל הוא מהותי, וגם בישראל עלול להשפיע בכל מערכה עתידית. ישראל עשויה למצוא עצמה מתמודדת לא רק מול תקיפות סייבר איראניות, של חמאס ושל חזבאללה, אלא גם מול אלה הרואים לעצמם כמטרה לחסל את ישראל. לעולם לא נדע מי עשוי להתגייס למערכה הזו, לפני או תוך כדי, ואלו יכולות וחולשות חדשות הוא מחזיק בידו, כולל אזרחים ישראליים, העשויים לפעול נגדה.

מרכיב נוסף וחשוב בתווך הסייבר בשנה הראשונה למלחמה באוקראינה הוא תחום ההונאה. ערוצי חדשות ופרופילים מזויפים השתמשו בתווך זה לקידום מהלכי הונאה מתוכננת על אודות

מהלכי הכוחות הצבאיים, מקומות ההתכנסות שלהם וכוונותיהם לתקיפה. למשל כל מהלכי התמרון שעשו הרוסים שודרו באמצעות ערוצי החדשות שלהם, שצוטטו בערוצי חדשות עולמיים. מעת לעת היו אלו הכרזות על תמרונים שלא קרו, אך הביאו את הצד השני להפעיל את כוחותיו, לתמרן לשם הגנה ולהיות בכוננות גם כשלא נדרש. המטרה – להרגיל את האוקראינים לשיטת פעולה שתרדים אותם לקראת המהלכים הצבאים האמיתיים. המרכיב השלישי והאחרון הוא מרכיב איסוף המודיעין באמצעות הרשתות החברתיות, אתרי אינטרנט ואפליקציות שאפשר איכון וציון מטרות, הבנת התמרון הצבאי ומיקום הכוחות.

המלצות

מניתוח השימוש בתווך הסייבר בשנה הראשונה של המלחמה השנייה באוקראינה אפשר להגיע לכמה המלצות, שכדאי לפתחן במסגרת תהליכי בניין כוח והפעלה ברמת המדינה וברמה הצבאית והביטחונית. הראשונה, המלחמה חידדה את הצורך בבנייה, בשיפור ובשדרוג אמצעי אבטחת מידע, במיוחד סביב תשתיות לאומיות קריטיות – חשמל, תחבורה, מים, המערכת הפיננסית, תקשורת, מערכת הבריאות, המערכת הביטחונית ועוד. כמו כן, נדרש לחזק את אמצעי ההגנה גם בחברות ובארגונים שהם חלק משרשרת האספקה של התשתיות הלאומיות. אלה יהיו לרוב פגיעים יותר ומוּדעים פחות, ולכן יהוו נתיב תקיפה אל לב התשתיות הלאומיות.

ההמלצה השנייה היא חיזוק יכולות איסוף המידע בזמן אמת מהרשתות החברתיות, ואיסוף מידע אוטומטי שיזהה פרופילים ברשתות של חיילי היריב ויעקוב אחר פעילותם, מיקומם והאינטראקציה שהם מייצרים, כולל הבחנה האם מדובר במהלכי הונאה על פי סימנים מחשידים. את אלה אפשר לפתח באמצעות מנגנוני בינה מלאכותית.

יש לכלול ביכולות אלה זיהוי שימוש בטלפונים סלולריים של היריב, גם כאשר הוא פועל בקרב אוכלוסייה אזרחית, כדי להשתמש בהם לטובת יצירת מטרות בזמן אמת. יש להזכיר שבמלחמת לבנון השנייה היו ככל הנראה בידי חזבאללה יכולות כאלה, והוא טיווח קבוצות חיילים באמצעותן. בעת הלחימה באוקראינה ב־2014–2015 השתמש המודיעין הרוסי באפליקציה שקציני תותחנים אוקראינים השתמשו בה, כדי לאתר ולהכווין אש לעבר הסוללות שלהם.

ההמלצה השלישית, שהיא המשך לשנייה, היא חיזוק המודעות ושמירה על ביטחון המידע לפני הלחימה ובמהלכה, ואי חשיפת סודות צבאיים, לרבות מיקום הכוחות, גודלם ואופן הפעלתם. יש למנוע מחיילים לקחת איתם ולהפעיל את הטלפונים שלהם בעת פעילות מבצעית.

ההמלצה הרביעית נוגעת בצורך בפיתוח תפיסה לאומית, אחידה, מתוזמנת ומתואמת בין כלל הגופים הרלוונטיים ליצירת מהלכי הונאה והשפעה באמצעות הרשתות החברתיות וערוצי המדיה השונים. כאשר כל הגופים מתנהלים כתזמורת הם יכולים להשיג

השפעה גדולה מאד הן בזירה הביתית, הן מול היריב והן בזירה הבין־לאומית הדיפלומטית, שהוכחה פעמים אין־ספור כקריטית.
ההמלצה האחרונה נוגעת בצורך של יצירת עליונות קבועה בתוך הסייבר, שעיקרה פיתוח חולשות, פרצות ודרכי נגישות למערכות היריב. יכולת כזו יכולה להתבסס על פיתוח עצמי אך גם על רכש חולשות ברשת, בדגש בערוצי טלגרם ודארקנט, וכן על הפעלה של גופים פרטיים בשירות המדינה.

סיכום

אחרי 2014 התחדדה חשיבותו של תווך הסייבר ככלי מלחמתי שמטרתו השבתת תשתיות לאומיות ליצירת אפקטים צבאיים. הסייבר הפך לכלי בארגז הכלים של הכוחות המתמרנים, המסייע להם לתמרן בקלות רבה יותר. המוכנות של התשתיות הלאומיות באוקראינה ואי קיומם של כלי תקיפה חדשים בידי רוסיה, הכשילה את מאמצם לנצל את תווך הסייבר כמאמץ נוסף במתקפתם על אוקראינה. עם זאת, התחדד עד מאוד השימוש בתווך הסייבר ליצירת הונאה, להשפעה על דעת קהל ולאיסוף מודיעין.
אומנם ממדי ההסתרה וההונאה משני הצדדים הנלחמים אינם מאפשרים לדעת את האמת כולה על המתרחש באוקראינה, אך ניתן להסיק זאת מעשרות רבות של אירועים שפורסמו את כיווני התקיפה והשימוש שנעשה בתווך הסייבר במלחמה.
הלקחים שיילמדו בסוף המלחמה ייושמו במידה כזאת או אחרת בצבאות העולם, אך סביר להניח כי יהיו אלה לקחי האתמול

שייושמו על מלחמת המחר. על כן, מעבר ליישום הלקחים והתובנות בתווכי הלחימה השונים, חשוב לדון בהפתעות הבאות בשדה הקרב העתידי, על טכנולוגיות חדשות לרבות יכולות בינה מלאכותית ויישומן בהגנה, התקפה, איסוף מודיעין ולוחמה על התודעה.