



## תווך הסייבר: לקחים ממלחמת רוסיה-אוקראינה

מאת ד"ר אייל פינקו

מבט מבס"א, מס' 2,203, 22 ביוני 2023

**תקציר:** בראשיתה של מלחמת אוקראינה-רוסיה בוצעו על-ידי שני הצדדים תקיפות סייבר שנועדו לנטרל את התשתיות הלאומיות הקריטיות, את המערכות הבנקאיות ואת משרדי הממשלה השונים, ונעשה מאמץ להשפיע על מקבלי ההחלטות בצד השני, על האזרחים ועל החיילים. נעשה גם שימוש באיסוף מודיעיני. לסייבר לא היה תפקיד ממשי בהשבתת יכולות ותשתיות לאומיות, אך השימוש הנרחב בו יצר השפעות פסיכולוגיות ותודעתיות. השנה הראשונה למלחמה חידדה את הצורך בבנייה, שיפור ושדרוג אמצעי אבטחת מידע, בעיקר סביב תשתיות לאומיות קריטיות; את הצורך בחיזוק יכולות איסוף מידע בזמן אמת מהרשתות החברתיות; את הצורך בחיזוק המודעות והשמירה על ביטחון המידע; ואת הצורך לפתח תפיסה לאומית, אחידה, מתוזמנת ומתואמת בין הגופים הרלוונטיים.

### מבוא

מלחמת אוקראינה-רוסיה פרצה רשמית עם כניסת כוחות רוסים לאוקראינה ב-24 לפברואר 2022, לאחר שהצבא הרוסי החל בהכנות לפלישה כחודש לפני ובסיומו של אימון רב זרועי בן עשרה ימים וביצע מספר התקפות סייבר מקדימות.

המערכה באוקראינה המתנהלת עד כתיבת שורות אלו לוותה באירועי סייבר רבים ומתקשרים היטב, אשר לוו בהסברים אודותם ואודות השלכות שלהם מפי מיטב המומחים העולמיים, שציינו כי מלחמת הסייבר שינתה את פני המערכה הצבאית והשפיעה עליה, ואף כונתה בראשיתה "המלחמה הדיגיטלית הראשונה", אם כי אין לכינוי זה כל בסיס מציאותי, שכן כבר ב-2014 התנהלה מערכה משמעותי בסייבר בין רוסיה לבין אוקראינה.

המאמר יביא ניתוח של תפקיד תווך הסייבר במהלך המלחמה באוקראינה בשנתה הראשונה, ומה ניתן ללמוד מכך בעידן המלחמה המודרנית.

### אמינות המידע

בפתח הדברים ותיאור אירועי הסייבר שקדמו למערכה והתנהלו במסגרתה, יש לציין מגבלה קריטית בבסיס המידע המצוי. תיאורי תקיפות של שני הצדדים, הרוסי והאוקראיני, נסמכות על דיווחים תקשורתיים בלבד, על-פי פרסומים שהחליטו שני הצדדים לפרסם, כל אחד בהתאם למטרותיו וליעדיו. הפרסומים של שני הצדדים משמשים לא מעט ליצירת אפקטים תודעתיים במסגרת הלוחמה הפסיכולוגית

המתנהלת ביניהם וכלפי העולם הרחב. כפי שראינו במלחמה זו עד כה, ההונאה משני הצדדים היא רבה, הפייק ניוז, הדיסאינפורמציה והמיסאינפורמציה שולטים בזירת הלחימה, עד כדי כך שלא ניתן לדעת באמת מי מהצדדים דובר אמת, אם בכלל. ומכאן, כי תיאור התקיפות המופיע בפרק זה מבוסס על דיווחים, שמקורם בתקשורת, ושצוטטו כפי שהופיעו ומבלי לדעת לעיתים מהם האפקטים האמיתיים שהושגו.

יתר על כן, צריך לזכור, כי הפרסומים מתייחסים לתקיפות הועשות, תקיפות אשר תוצאותיהן ניכרות וברורות לעין. אין בסיס מידע אמיתי על מספר התקיפות השקטות, אלו אשר חדרו למערכות המחשבים של שני הצדדים, לטובת איסוף מודיעין או לכל הישג אחר, שאין כוונה לחושפו לעין.

### **תקיפות סייבר לקראת המלחמה**

רוסיה ניהלה מערכה נמוכת עצימות של תקיפות סייבר נגד אוקראינה כבר מ-2014 – 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 מכן הושחתו אתרים של משרדי הממשלה האוקראינים (כמו למשל משרד החינוך, משרד הפנים, משרד החוץ ואתרים נוספים) ומסרים המזהירים את תושבי אוקראינה מפני רוסיה פורסמו בהם. שירות ביטחון הפנים האוקראיני טען אז, כי במסגרת התקיפות לא נגנב דבר, אך בבדיקות שבוצעו על-ידי גורמים אמריקנים ומיקרוסופט התגלו וירוסים ברשתות האוקראיניות, בדגש על רשתות של תשתיות קריטיות, כגון משרד הביטחון האוקראיני, מתקני ייצור חשמל, מתקני גרעין ועוד. מידע קריטי נמחק מרשתות המידע של משרד הביטחון האוקראיני.

כשבועיים לפני המערכה נרתמה ארצות הברית ושלחה סיוע של מומחים ופתרונות טכנולוגיים להגנת התשתיות האוקראיניות.

### **תקיפות סייבר רוסיות במלחמה**

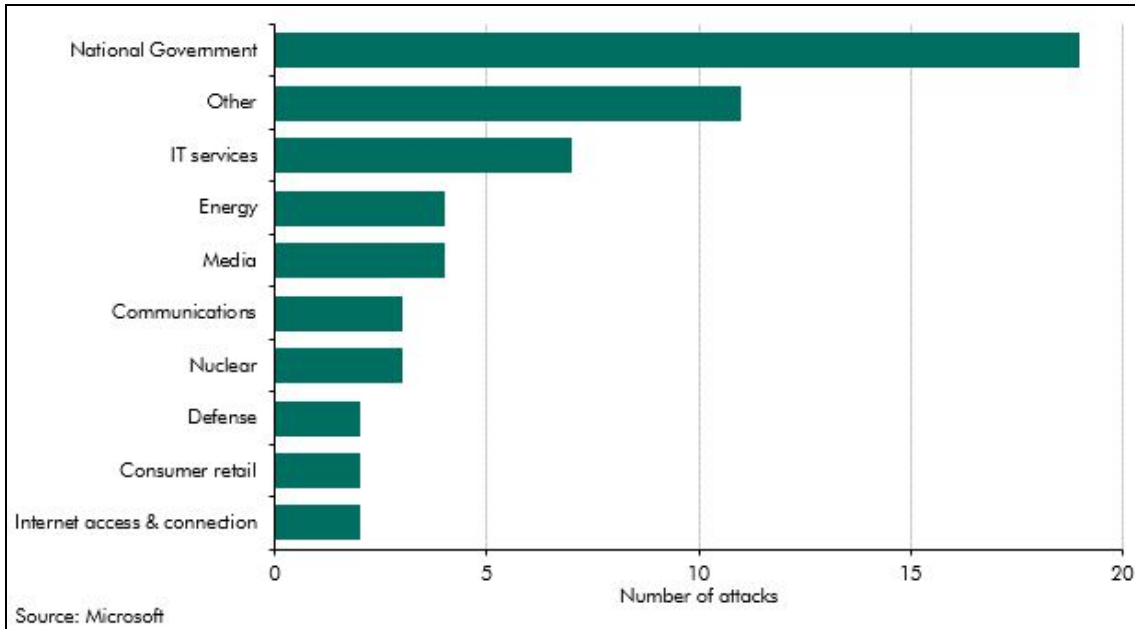
יום לפני פרוץ המלחמה וביומה הראשון החלו תקיפות סייבר רבות כנגד התשתיות הלאומיות של אוקראינה, משרדי ממשלה והמערכת הבנקאית. מרבית התקיפות היו תקיפות מניעת שירות (DDoS) והשחתת אתרים. אוקראינה שכבר ידעה סבל מתקיפות סייבר על חברת החשמל שלה במלחמה הראשונה ב-2014 והשבתת החשמל בחלקים של אוקראינה למשך כחצי יממה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

בחודשים הראשונים של המלחמה ניסו הרוסים שוב ושוב לתקוף מטרות אסטרטגיות, מוסדות בנקאיים ותשתיות לאומיות כגון את חברת החשמל, מתקני הגרעין ותשתיות תחבורה, מתוך תפיסה כי ניתן יהיה להשבית אוקראינה על-ידי הכנעת התשתיות הלאומיות שלה. אך התקיפות לא צלחו. הרוסים הפעילו תקיפות שונות שעיקרן היה מחיקת מידע משרתים ומחשבים.

בנוסף הופעלו תקיפות מחשבים ככוח מסייע למהלכי הכוחות הקרקעיים או כוחות האש. כך, למשל, באפריל 2022, יום לפני ההתקפה לכיבוש תחנת הכוח הגרעינית האוקראינית ב'פורוֹז'יה על-ידי כוחות קרקעיים, בוצעו 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 ויניצייה (כמאתיים קילומטרים מדרום מערב לבירה קייב) – מ-4 במרץ הם תקפו באמצעות סייבר את רשתות התקשורת במרחב ובמהלך השבועות הבאים ירו מספר מטחי טילים שנחתו בשדה התעופה

ובמפקדה עצמה. כך גם היה למשל בתקיפות הרוסיות על אתרי ממשל, צבא ותשתיות בעיר דניפרו: תקיפה שהחלה במבצע סייבר שיצרה מניעת שירות במחשבי המועצה ואתר האינטרנט שלה, ומיד אחר-כך מטח של 11 טילי שיוט על מטרות שונות בעיר.

האיור הבא מתאר את חלוקת תקיפות הסייבר הרוסיות על התשתיות האוקראיניות בחתך מגזר. התקיפות המתוארות באיור הן מראשית פברואר 2022 ועד אוקטובר 2022. ניתן לראות שמרבית התקיפות הרוסיות היו מכוונות כנגד מוסדות שלטון (כולל צבא), תשתיות IT ומגזר האנרגיה.



כמו-כן, באמצעות המדיה החברתית ותקיפת אתרי חדשות ורדיו יצרו וניהלו הרוסים משך חודשים רבים (עד היום) מבצעי השפעה בקנה מידה נרחב של דיסאינפורמציה ופייק-ניוז נגד השלטון האוקראיני ונאט"ו.

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

### תקיפות סייבר אוקראיניות במלחמה

האוקראינים הגיבו גם הם ובימים הראשונים של המלחמה השחיתו אתרי ממשלה רוסים, יצרו תקיפות מניעת שירות כנגדם, כשהם מנסים ליצור הבנה ברוסיה, כי אוקראינה תגיב על התוקפנות הרוסית גם בתווך הסייבר. הנשיא האוקראיני, זלנסקי, אף קרא להאקרים מרחבי העולם להתגייס לצבא הסייבר האוקראיני, לסייע לאוקראינה לתקוף אתרים ותשתיות רוסיות, ולהיות חלק מהמערכה על התודעה גם בתווך הסייבר.

האוקראינים גם הם פעלו רבות בתווך הסייבר ליצירת השפעה על אזרחי רוסיה, והאקרים, לרבות מתנדבי ארגון אנונימוס. ההאקרים האוקראינים פרצו לאתרי ממשל רוסים, שלחו הודעות עם מסרים לטלפונים הסלולריים של אזרחים רוסים בגנות המלחמה, פרצו לאתר הטלוויזיה הרוסית ושידרו בו מסרים, ואף פרצו לאתר סוכנות החלל הרוסית. ארגון אנונימוס טען כי הצליח לחדור ולהוריד את אתר שירות המודיעין הצבאי הרוסי, ה-FSB. מתקפות דומות לאלו בוצעו במהלך כל ימי הלחימה על-ידי

האקרים אוקראינים והאקרים שפעלו בהתנדבות עבור אוקראינה, מתוך מטרה להשפיע על דעת הקהל העולמית והרוסית, ולהפסקת המלחמה.

## **איסוף מודיעין בתווך הסייבר**

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

המודיעין הצבאי נאסף לפני ובמהלך המלחמה באמצעים שונים, כגון מודיעין אנושי (יומינט), מודיעין אותות (סיגינט), מודיעין חזותי (ויזינט) ובאמצעים שונים נוספים. השימוש הנרחב בתווך הסייבר - באינטרנט, מאפליקציות וברשתות תקשורת פתוחות מהווה 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 לכולנו נגישות ובשימוש בהם אנו 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 לא 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 בהם הם שוהים ופועלים. ניתוח המידע סייע לשני הצדדים, אבל בעיקר לצד האוקראיני, להבין ולזהות את מיקומי הכוחות היריבים, לייצר מהם מטרות בזמן קצר יחסית ובהתאם למיקומם להפעיל כנגדם חימושים. כך למשל במהלך יוני 2022, דיווחו הרוסים על כוונתם לסגת, אך תמונות וסרטונים שהועלו על-ידי חיילים רוסים לרשתות החברתיות הצביעו על שהרוסים אינם נסוגים והפרסום הרוסי הוא מהלך של הונאה בלבד. על-פי הפרסום, הסרטונים והתמונות דווחו על-ידי אזרחים אוקראיניים לשירותי הביטחון המקומיים.

קבוצת תקיפה רוסית, המכונה ארמגדון, תקפה בתקיפות ממוקדות, ומבוססות מודיעין ככל הנראה, אזרחים וארגונים באוקראינה על מנת לאסוף מודיעין אודות הלך הרוח באוקראינה, ומידע תשתיתי אחר נוסף, שסייע להם במערכה היבשתית ובהשבת התשתיות הלאומיות.

הממד השני של איסוף מודיעין במרחב הסייבר, הוא איסוף של 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 החזי מאתרי אינטרנט המפעילים לוויינים, הפך להיות הלוויין החדש של מדינות שאין ברשותן לווייני צילום.

## **דיון**

המלחמה באוקראינה אינה הראשונה בה התנהלה מערכה מקבילה בתווך הסייבר. ואולי דווקא החיבור שבין התווך הוירטואלי לתווך הפיזי, הוא שהופך את הסייבר למרכיב בסל המרכיבים של המלחמה המודרנית, מרכיב שמדינות וארגונים רבים חפצים להפעילו.

במלחמת אוקראינה הראשונה ב-2014 עשו הרוסים שימוש בתווך הסייבר על מנת ליצור אפקטים שיעזרו להם במערכה היבשתית. הדוגמה הבולטת לכך הייתה התקיפה על מערכת החשמל האוקראינית, תקיפה שהשאירה כרבע מיליון בתי אב ללא חשמל

משך שעות ארוכות. תקיפה זו בוצעה 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 כנגד תשתיות לאומיות, הן תקיפות המבוצעות מתוך התפיסה שהן מייצרות אפקטים פסיכולוגיים, כלכליים וצבאיים, המסייעים למערכה הצבאית הפיזית. תקיפות כאלו לוקחות זמן, אלו אינן תקיפות בזמן אמת, כמו אלו הלקוחות מסרטי "משימה בלתי אפשרית". על מנת לייצר תקיפת סייבר על תשתית לאומית בעיקר, נדרש איסוף מודיעין אודות היעד משך 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 המלחמה ב-2014, העלו את רמת האבטחה של התשתיות הלאומיות האוקראיניות, ולכן, רוב תקיפות הסייבר הרוסיות על התשתיות הלאומיות באוקראינה, אשר נועדו לסייע להם במהלך הקרקע, ככל הנראה נכשלו.

על כן, ובהתייחס כמובן למגבלות המידע המפורסם ולמהלכי ההונאה משני הצדדים, ניתן להסיק כי במערכה הזו, שלא בדומה למערכה הקודמת, לסייבר לא היה תפקיד ממשי בהשבתת יכולות ותשתיות לאומיות, ולמעשה, 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.

יחד עם זאת, הסייבר במערכה באוקראינה יצר אפקטים תודעתיים ופסיכולוגיים, שהשפיעו על השיח הציבורי העולמי, על נאט"ו, והאוכלוסיות בשתי המדינות. כך למשל תקיפות הסייבר הרוסיות יצרו דה-לגיטימיזציה כנגדם ואפשרו לאוקראינים לקבל סיוע נוסף בתחום הגנת הסייבר ממדינות העולם. מצד שני תקיפות הסייבר הרוסיות יצרו תחושת חרדה באוקראינה, תחושה שקשה לבודדה מסך כל תחושות הפחד והחרדה של האוכלוסייה המקומית מסך מהלכי המלחמה של רוסיה, אך סביר להניח שלתווך הסייבר יש תרומה מכובדת בהגברת רמת החרדה של האוכלוסייה האוקראינית.

יש לציין, כי התקשורת העולמית, ברובה, נתנה לגיטימיזציה לתקיפות הסייבר האוקראיניות ברוסיה, עודדה אותן, ואף לא הסתייגה ממהלכי הנשיא האוקראיני כשקרא ונתן לגיטימיזציה להאקרים מרחבי העולם להצטרף למערכה ולתקוף סייברית את רוסיה. באותה נשימה, כמובן שקבוצות התקיפה הרוסיות, המושתתות על אזרחים, זכו לגנאי ולגינוי.

כלומר ניתן לסכם כי במהלך השנה הראשונה למלחמה, לתווך הסייבר הייתה 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 תגבור יכולות התקיפה המדינתיות של שני היריבים על-ידי גיוס האקרים מכל העולם, להם אין קשר ישיר למערכה, על מנת שיסייעו בהשגת המטרות. מהלך מעניין, אשר בו קיבלו גורמי פשיעה בתווך הסייבר לגיטימיזציה לפעול, בעוד שהעולם המערבי אינו מביע הסתייגות מכך.

בתווך הסייבר בו 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, אך 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. כך שמושג העליונות בסייבר, בניגוד למושג העליונות הצבאי, הוא מושג רופף ודינמי, העשוי להשתנות בקצב גבוה.

ועל כן עניין גיוס האקרים חובבים או מקצוענים מכל קצווי תבל הוא עניין משמעותי, וגם בישראל הוא עלול להשפיע בכל מערכה עתידית. ישראל עשויה למצוא עצמה מתמודדת לא רק מול תקיפות סייבר איראניות, של חמאס ושל חיזבאללה, אלא גם מול כאלו שרואים 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 כנגדה יחד עם גורמי ציר הרשע.

מרכיב נוסף וחשוב בתווך הסייבר בשנה הראשונה למלחמה באוקראינה הוא תחום ההונאה. נעשה שימוש נרחב מאוד בעיקר באמצעות ערוצי חדשות ופרופילים מזויפים לקידום מהלכי הונאה מתוכננת אודות מהלכי הכוחות הצבאיים, מקומות ההתכנסות שלהם וכוונותיהם לתקיפה. כך 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 גרמו לצד השני להפעיל את כוחותיו, לתמרן לשם הגנה ולהיות בכוננות גם כשלא נדרש, ובכך להרגיל את האוקראינים לשיטת פעולה שירדים אותם לקראת המהלכים הצבאיים 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 ניתן להגיע למספר המלצות, שכדאי לפתחן במסגרת תהליכי בניין כוח והפעלה ברמת המדינה וברמה הצבאית/ביטחונית.

ההמלצה הראשונה - המלחמה חידדה את הצורך בבנייה, שיפור ושדרוג אמצעי אבטחת מידע (סייבר) במיוחד סביב תשתיות לאומיות קריטיות - חשמל, תחבורה, מים, המערכת הפיננסית, תקשורת, מערכת הבריאות, המערכת הביטחונית ועוד. בנוסף, נדרש לחזק את אמצעי ההגנה גם בחברות ובארגונים המהווים חלק משרשרת האספקה של התשתיות הלאומיות. אלו לרוב יהיו פגיעים יותר ומודעים פחות, ולכן יהוו נתיב תקיפה אל לב התשתיות הלאומיות.

ההמלצה השנייה היא חיזוק יכולות איסוף המידע בזמן אמת מהרשתות החברתיות, ואיסוף מידע אוטומטי אשר יזהה פרופילים ברשתות של חיילי היריב ויעקוב אחר פעילותם, מיקומם והאינטראקציה שהם מייצרים, כולל הבחנה האם מדובר במהלכי הונאה על-פי סימנים מחשידים. את אלו ניתן לפתח באמצעות מנגנוני בינה מלאכותית. יש לכלול ביכולות אלו גם זיהוי שימוש בטלפונים סלולריים של היריב, גם כאשר הוא פועל בקרב אוכלוסייה אזרחית, על מנת לעשות שימוש בהם לטובת יצירת מטרות בזמן אמת. יש להזכיר שבמלחמת לבנון השנייה, היו ככל הנראה בידי חיזבאללה יכולות כאלו והוא טיווח קבוצות חיילים באמצעותן. בעת הלחימה באוקראינה ב-2014, 2015, השתמש המודיעין הרוסי באפליקציה שהשתמשו בה קציני תותחנים אוקראינים כדי לאתר ולהכווין אש לעבר הסוללות שלהם.

ההמלצה השלישית, המהווה המשך לשנייה, היא חיזוק המודעות ושמירה על ביטחון המידע לפני ובמהלך הלחימה, 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 מאוד הן בזירה הביתית, הן מול היריב והן בזירה הבינלאומית הדיפלומטית, שהוכחה אינספור כקריטית.

ההמלצה החמישית והאחרונה נוגעת בצורך של יצירת עליונות קבועה בתווך 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 מלחמת אוקראינה הראשונה התחדדה חשיבותו של תווך הסייבר ככלי מלחמתי שמטרתו השבתת תשתיות לאומיות ליצירת אפקטים צבאיים, המהווים כלי בארגז הכלים של הכוחות המתמרנים, המסייע להם לתמרן בקלות רבה יותר.

המוכנות של התשתיות הלאומיות באוקראינה ואי-קיומן של כלי תקיפה חדשים בידי רוסיה, הכשילה את המאמץ הרוסי לנצל את תווך הסייבר כמאמץ נוסף במתקפתם על אוקראינה. יחד עם זאת, התחדד עד מאוד השימוש בתווך הסייבר ליצירת הונאה, השפעה 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 מאוד של אירועים שפורסמו את כיווני התקיפה והשימוש שנעשה בתווך הסייבר במלחמה.

הלקחים שילמדו בסופה של המלחמה ייושמו באופן כזה או אחר, או במידה כזאת או אחרת, בצבאות העולם, אך סביר להניח כי יהיו אלו הלקחים של אתמול שיושמו על המלחמה של המחר. על כן, מעבר ליישום הלקחים והתובנות בתווכי הלחימה השונים, חשוב יהיה לדון בהפתעות הבאות בשדה הקרב העתידי, על טכנולוגיות חדשות לרבות יכולות בינה מלאכותית ויישומן בהגנה, התקפה, איסוף מודיעין ולוחמה על התודעה.

סא"ל (מיל') ד"ר אייל פינקו, שירת בעברו בחיל הים ובמערכת הביטחון. מומחה בתחומי המודיעין, סייבר והביטחון הלאומי.