פריצה לצורך השפעה - חוסן ככלי התמודדות עם לוחמת סב"ר בעלת יעדים תפקודיים ותודעתיים מצד איראן ושלוחותיה[1]

סא"ל ח', אושרי בר־גיל, רס"ן (מיל') ת'[2]

רמת התפתחותה הטכנולוגית המתקדמת של מדינת ישראל ומרכזיות הרובד הדיגיטלי מובילים לכך שתקיפת סב"ר עלולה להוביל לנזקים משמעותיים ברמה הלאומית - במישור האזרחי והצבאי כאחד. ממד הסב"ר משמש ליצירת הישגים מבצעיים אופרטיביים־תפקודיים לצד אלו התודעתיים, כפי שאנו עדים לכך בתקופה האחרונה, במטרה להעצים את אפקט הנזק ומשך השפעתו. **נקודת מוצא זו מצריכה מציאת מנגנוני מענה הולמים, אשר יקטינו את החשיפה לאיום ויפחיתו את הישגי היריב במערכה בעלת יעדים משולבים של פגיעה בתפקוד והשפעה על התודעה**. הכותבים סוקרים את התפתחות המערכה בסב"ר מצד איראן ושלוחותיה, מציגים תפיסות ומאמצים להתמודדות עם האיום ואף מספקים המלצות מערכתיות לקובעי המדיניות בתחום.

מבוא: מ'דיסאינפורמציה' ל'צעדים פעילים' ומבצעי תודעה

קרל פון קלאוזוביץ, שנולד מאות שנים לפני המצאת האינטרנט, טען כי: "המלחמה אינה אלא המשך המדיניות בתוספת אמצעים אחרים" (קלאוזוביץ, 1977, עמ' 65). השימוש במידע שגוי, שקרי ומסולף, דיסאינפורמציה בשפתנו, כדי לפגוע ברוח הלחימה, לפלג ולפגוע ביכולות האויב שימש באופן היסטורי חלק מ"המשכה של המדיניות

[1] המאמר מוקדש לזכרו של סמל אילן אלכסנדרוביץ' ז"ל, לוחם הנח"ל המוצנח שנפל במלחמת לבנון הראשונה (מבצע שלום הגליל). הכותבים מבקשים להודות לאנשים האלה על הערותיהם המחכימות אשר תרמו רבות למאמר זה: תא"ל (מיל') ארז דוד מייזל, עמית מחקר במחלקה להיסטוריה של צה"ל; אל"ם (מיל') מוטי טל, לשעבר רמ"ח תו"ל; סא"ל (מיל') מוטי קלנג, לשעבר ראש מכון המחקר למדעי ההתנהגות; סא"ל איתי חימיניס רע"ן פיתוח ידע, מרכז דדו; רס"ן ר' מחטיבת המחקר באמ"ן; רס"ן אור בר ממרכז דדו.

[2] סגן־אלוף ח' הוא ראש ענף בחטיבת ההגנה בסב"ר; רב־סרן אושרי בר־גיל הוא ראש מדור מחקר טכנולוגיה ודיגיטל במכון המחקר הצה"לי היישומי למדעי ההתנהגות. חוקר את היחסים בין אדם לטכנולוגיה בצה"ל; רב־סרן (מיל') ת' הוא מומחה הגנת סב"ר המשרת במילואים ביחידת מבקר צה"ל, בעברו שימש קצין בחטיבת המחקר באמ"ן.

בדרכים אחרות", לחימה של ממש, שכן הוא אפשר תוקפנות עדינה יותר שיכולה להיות מופעלת גם בזמן רגיעה תוך שימוש במסרים גלויים. כיום נוכל לראות מהלכים כאלו אפילו ברשתות חברתיות. עידן הדיסאינפורמציה המודרני החל בתחילת שנות ה־20 של המאה העשרים, כאשר הקג"ב הקים את "המשרד לתעמולת חוץ". ב־1923 הוא אף המציא מילה חדשה – "דיסאינפורמציה" – כדי לגרום לה להישמע צרפתית. בדרך זו אפילו מקור המונח נקבר יחד עם האמת (Singer & Brooking, 2018). לעומתו המערב העדיף את השימוש במונח "לוחמה פוליטית". לא משנה מה הביטוי שנבחר לתאר אותה, המטרה של אסטרטגיות אלו זהה: להחריף את המתחים והסתירות הקיימים בתוך הגוף הפוליטי של היריב באמצעות מינוף שמועות, סתירות ומידע מסולף וחלקי (Rid, 2020; גולדשמידט ווורגן, 2017).

קיימים חילוקי דעות היסטוריים על מידת האפקטיביות של השימוש באסטרטגיות אלו לשם השפעה על שינוי עמדות רחב ואיתן על מדיניות לאומית (Schia & Gjesvik, 2020). למרות חילוקי דעות אלה קיימת תמימות דעים כי השימוש הנרחב בדיסאינפורמציה לטובת מבצעי תודעה הואץ בשנים האחרונות בעקבות התרחבות השימוש במידע וברשת (Bennett & Livingston, 2020; Rid, 2020; Schia & Gjesvik, 2020; Singer & Brooking, 2018).

הגל הנוכחי של הדיסאינפורמציה בעולם נבנה אט אט וצמח עם העשור הראשון של המאה ה־21 בזכות השילוב של טכנולוגיות חדשות ותרבות אינטרנט. האומנות הישנה של השפעה פסיכולוגית־חברתית איטית ומיומנת שחייבה נוכחות פיזית, ושהייתה עתירת עבודה, הפכה להיות לפעולה בקצב גבוה מאוד המתאפשרת גם לבעלי כישורים נמוכים יותר והניתנת לביצוע מרחוק או אפילו במיקור חוץ. בשל כך 'צעדים פעילים', דוגמת הפצת דיסאינפורמציה ומבצעי השפעה מצד מדינות וארגוני טרור, הפכו לנפוצים בזירה העולמית והמקומית יותר מאי פעם (Rid, 2020).

עלייה בדומיננטיות הרשת כמרחב לחימה

דומיננטיות האינטרנט בחיינו והפיכתו לזירה מרכזית בפני עצמה בשדה הקרב המודרני הביאה לכך שכל קרב וירטואלי נראה אישי ונקודתי, אך כל סכסוך מתוּוָך ברשת הגלובלית באופן שמשנה את אופן הלחימה בסכסוכים. הקרב ברשת משנה את המשמעות של "מלחמה"; ניצחונות בקרבות המקוונים הם ניצחונות של ממש בעולם האמיתי; כל ניצחון ארעי מניע את האירועים בעולם הפיזי החל מפידים (Feeds), לכאורה חסרי משמעות, של סלבריטאים ועד להשפעה על תוצאות הבחירות במדינות שונות. כולנו חלק מהמלחמה הזו. כולנו, לרבות המידע אודותנו וזה שבבעלותנו, מחוברים לאינטרנט. תשומת הלב, הזיכרון והתודעה שלנו הם כמו פיסת טריטוריה שנויה במחלוקת שנלחמים עליה בעימותים, שאנחנו אפילו לא מודעים אליהם ומתרחשים סביבנו. כל מה שאנו צופים בו, אוהבים (לייק!) אותו או משתפים אותו, מייצג אדווה זעירה בשדה הקרב על התודעה בארץ ובעולם.

בסופו של דבר ההתפתחויות הטכנולוגיות והשינויים החברתיים שהם הביאו בעקבותיהן – חוסר ההסכמה ההולך וגובר על עובדות וטשטוש הגבולות בין עמדה, דעה ושקר בעידן ה"פוסט־אמת" – מחלחלים גם לזירת הביטחון הלאומי (Rid, 2020). **בעידן שבו מלחמות אינן מגיעות להכרעה ברורה הבאה לידי ביטוי בכיבוש שטח ונוכחות פיזית בו, מתעצמת חשיבות הקרב על הנרטיב**. איננו טוענים כי הכרעה היא עניין תודעתי בלבד, אך לראייתנו לדעת הקהל בארץ ובעולם, לרבות בקרב המשרתים בצה"ל והאזרחים מחוצה לו, יש השפעה רבה על האופן שבו נתפסת יכולתו של צה"ל ועמידתו במשימותיו, כפי שמתומצת בפסקה הזאת: "מאמץ התודעה של האויב מופעל ומפתח תוך לימוד קפדני של העוצמות והחולשות של מדינת ישראל וכוחה הצבאי. העיקרון המנחה אותו הוא צמצום העוצמה של צה"ל, קעקוע דמותו והצרת חופש הפעולה שלו באמצעים **א־סימטריים**" (מתוך התפיסה הצה"לית למבצעי תודעה, אמ"ץ־תוה"ד, עמ' 11).

כאמור, "המערכה על התודעה" אינה תופעה חדשה. לתודעה היה לאורך השנים משקל חשוב בעימותים בין מדינות וחברות גם בזירה המקומית במערכות שהתנהלו בין ישראל לירִיבותיה לאורך השנים (קופרווסר וסימן טוב, 2019, עמ' 227). **מבצעי תודעה המשתמשים ברשתות חברתיות כחלק ממערכה תודעתית והמכוונים להשפיע על ההיבטים שפורטו מעלה, עשויים לפגוע באופן משמעותי באמון הציבור בצה"ל בשגרה ובחופש הפעולה שלו בחירום ובכך לקזז חלק מיתרונותיו של צה"ל בלחימה וכצבא של מדינה דמוקרטית הנהנה מאמון הציבור בו. במצב כזה לגורמים שונים, במיוחד לאיראן המתחזקת חזית עקיפה מול ישראל, יש אינטרס רב לזרוע ספק במסריו וביכולותיו של צה"ל, דבר שמחייב גיבוש תפיסת מענה הולמת.**

חשיבות האמון והלגיטימציה הציבורית והחברתית לפעולות צה"ל ומדינת ישראל

במאמרו "השעונים שתקתקו בעצלתיים" (2011) מציע גיא ברוקר מספר היבטים מרכזיים המשפיעים על הלגיטימציה הציבורית והבין־לאומית לפעולת צה"ל, ושאיתם הוא נדרש להתמודד כדי לשמר לעצמו חופש פעולה. ההיבט הראשון הוא **הרגישות למחאה ציבורית או חברתית** שיש לה משקל רב במשטרים דמוקרטיים שבהם היעדר קונצנזוס מייצר קושי בפעולת הצבא. כך, למשל, המחאה הציבורית במהלך מלחמת לבנון הראשונה הייתה גורם מרכזי בניהולה (טובי ורטנר, 2007). ההיבט השני – **הרגישות לנפגעים בלחימה ובעורף** המוכרת בספרות הצבאית כאחת ממחוללי מגמת קיצור משך המלחמה בקרב צבאות מערביים ושהשפיעה גם על אופן ניהול המערכות בישראל, לרבות במבצע "עמוד ענן" ובמלחמת לבנון השנייה, כאשר תחושת הפגיעות של העורף תרמה משמעותית ללחץ לסיים את המלחמה. היבט אחר הוא **תפיסת ההישג** – תפיסת הציבור ומשרתי צה"ל את ההישג הצבאי למול המטרות שמוגדרות ללחימה משפיע על הלגיטימציה שמעניקה החברה הישראלית

לפעילות הצבאית. עוד היבט הוא **ההיבט ההומניטרי־מוסרי** של פעולת צה"ל השייך הן לחזית הבין־לאומית והן לפנים ישראלית. החברה הישראלית רואה בצה"ל צבא מוסרי, ופגיעה בתפיסה זו עשויה לפגוע בחופש הפעולה שלו. ההיבט האחרון הוא **לגיטימציה בין־לאומית**. כחלק מתהליכי הגלובליזציה העולמיים העוברים גם על ישראל, הזירה הבין־לאומית היא בעלת משקל הולך וגובר בניהול הלחימה. דעת הקהל הבין־לאומית משחקת תפקיד משמעותי בעיצוב הלגיטימציה הבין־לאומית.

אך מה הם האיומים המשפיעים על הלגיטימציה וחופש הפעולה של צה"ל? וכיצד ניתן להתגונן בפניהם? בכך בדיוק עוסק מאמר זה.

הלכה למעשה ניתן לומר שהאיום מזוהה. בישראל מתקיים ב־15 השנים האחרונות עיסוק נרחב למדי בתחום התודעה. מאמץ זה בא לידי ביטוי בחיזוק יחידת דובר צה"ל, בהקמת מטה הסברה לאומי במשרד ראש הממשלה, בקמפיין המדיני נגד תוכנית הגרעין של איראן שהתבסס ברובו על מודיעין, בפעולה מערכתית של המשרד לעניינים אסטרטגיים וגורמים בחברה האזרחית נגד איום BDS, בהקמת מסגרות ומחלקות בצה"ל העוסקות במהלכים מסוג זה ובפעילות הסברתית להכנת העורף לעימות. עם זאת, ההיערכות לאפשרות של השפעה עוינת על השיח הציבורי

במצב כזה לגורמים שונים, במיוחד לאיראן המתחזקת חזית עקיפה מול ישראל, יש אינטרס רב לזרוע ספק במסריו וביכולותיו של צה"ל, דבר שמחייב גיבוש תפיסת מענה הולמת

באופן כללי וגם על תהליכים דמוקרטיים בישראל, ובראשם הבחירות לכנסת, מקבלת חשיבות משנית במאמצים אלו. זאת למרות שהחלה להיווצר מודעות לחתרנות תודעתית ולהתערבות אפשרית במגוון של תהליכים עד כדי התערבות זרה בבחירות בישראל (גולדשמידט וורגן, 2017). צה"ל זיהה את חשיבות תחום התודעה ופיתח תפיסה מטכ"לית לנושא אשר פורסמה בשנת 2017. מטרתה הייתה לנסח את האתגרים לפעולת צה"ל בשל השתנות הסביבה הגלובלית. התפיסה ניתחה את מאמצי האויב להתמודדות עם יתרונה הצבאי היחסי באמצעות ערעור תחושות הביטחון והסולידריות הפנימית של האזרחים. **עם זאת, התפיסה מכווינה בעיקר את המאמצים כלפי חוץ ואיננה מקדישה את תשומת הלב המספקת לניתוח ההשפעות התודעתיות על משרתי צה"ל ואזרחי המדינה.**

מאפייני הלוחמה המשולבת

מהי הלוחמה המשולבת?

ניסיונות השפעה תודעתיים במטרה להשפיע על ביטחונן של מדינות שונות אינם תופעה חדשה. מקובל לשייך את השימוש באסטרטגיות אלו לתפיסות המתפתחות של "לוחמה משולבת" (Hybrid Warfare). מונח זה מתקדם מעבר לטשטוש הגבולות הרווח במלחמות המודרניות ומאופיין באלה:

1. שימוש במגוון כלים ומאמצי לחימה – כלכליים, משפטיים, פוליטיים, סב"ר, קינטיים ועוד;
2. שימוש זהיר ומדוד בהפעלה ישירה של כוח ;
3. רציפות והמשכיות מאמצי הלחימה השונים תוך שקלול ושינויי מתמיד בעצימותם;
4. מיקוד באוכלוסייה האזרחית ובפוליטיקה המקומית.

ארגז הכלים המגוון ללוחמה משולבת שוזר בין הכלים השונים הקיימים בו. תקיפות הסב"ר משמשות בין היתר להשפעה פוליטית וסחיטה על בסיס מידע ולמטרות השפעה תודעתית נוספות למשל, כלכלית ומסחרית. לעיתים אף נעשה שימוש בנציגים עקיפים בעלי אינטרסים משותפים (Proxy) (Chivvis, 2017).

"טרור הוא תיאטרון", הכריז בריאן ג'נקינס, אנליסט תאגיד ראנד, בדו"ח מ־1974 שהיה לאחד המחקרים המשמעותיים של תופעת הטרור: "**אם תצליח למקד מספיק תשומת לב זה לא משנה כמה חלש או חזק אתה באמת: אתה יכול לכופף אוכלוסיות למען דעתך ולהוביל את היריבים החזקים ביותר לכניעה**" (Jenkins, 1974). בשדה הקרב המשולב של סב"ר ותודעה נלחם צה"ל בצורה בלתי פוסקת, כזרוע הגנה בסב"ר, כמו על מנת לשמר את תחושת הביטחון, מעמדו והלגיטימיות הציבורית לפעולה צבאית בישראל. מלחמה זו מאותגרת באמצעות השילוב בין הלוחמה המשולבת, שמפעילים שחקנים שונים נגד ישראל מחד, וגדילה בשטח הפגיע שלה – במשתמשי הדיגיטל והרשתות החברתיות מאידך. אך מהם האיומים בממד הסב"ר שנגדם צה"ל נלחם ועל מה הוא מגן? בעוד שההגנה על תשתיות מידע, רשתות וארגונים מפני מתקפות סב"ר היא אתגר שניתן לתחום במידת מה, הקרב על התודעה מורכב יותר, מכיוון שהוא מתנהל בכל המרחב המקוון על שלל משתתפיו, ולא כלפי יעדים או ארגונים ספציפיים, ולעיתים הוא אף מתנהל במרחב ה'אדום' ו'הכחול' (זירת היריב והזירה הלאומית בהתאמה) במקביל ובערבוביה.

ככל שהתשתיות הדיגיטליות של מדינה מתוחכמות יותר ומעניקות לה יתרון גדול יותר, כך המדינה פגיעה יותר לקיזוז יתרון זה באמצעות מתקפת סב"ר שיעדיה תפקודיים. בצורה דומה גם ההון החברתי־תרבותי של דמוקרטיה מערבית שבה קיימת מידה גבוהה של לכידות ואמון בין האזרחים למוסדות, פגיע יותר למתקפת השפעה מאשר במדינות בעלות אמון נמוך. **מאפיינים אלו הופכים את העימות בין ישראל לשכנותיה לעימות א־סימטרי גם בממדי הסב"ר וההשפעה. לישראל,**

ביחס לאויבותיה, יש יותר 'שטח פנים' לתקיפת סב"ר והשפעה בדמות רשתות מידע, תשתיות דיגיטליות, שימוש ברשתות חברתיות ואמון ציבורי נרחב. כפועל יוצא, פוטנציאל הנזק עבורה גבוה יותר.

טיפולוגיה של מבצעי סב"ר בעלי יעדים תפקודיים ותודעתיים

דגנית פייקובסקי ואביתר מתניה (2019) טוענים שממד הסב"ר מאפשר פגיעה בהיבטים תפקודים ותודעתיים. הפגיעה יכולה להתבצע באמצעות חדירה, החדרת קוד עוין או תוכן עוין ושילובים שונים ביניהם. הרחבנו את הטיפולוגיה המוצעת על ידם בדוגמאות בהתאם לרוח המאמר:

דוגמאות לסוגי פגיעה שונים בממד הסב"ר		
סוגי הפגיעה	תכלית הפעולה	
	תכלית תפקודית	תכלית תודעתית
פגיעה בחסיון מידע (Confidentiality)	איסוף מידע להפקת מודיעין צבאי, אזרחי או מסחרי	חשיפת מידע חסוי והפיכתו לפומבי. לדוגמה, הדלפת מידע מביך או איום בהדלפה. מקרה שירביט או אטרף
פגיעה באמינות המידע (Integrity)	שיבוש ושינוי נתונים לצורך פגיעה פיזית או לצורך שיבוש תמונת המצב	הטיה של מידע או שתילה של מידע מוטה או כוזב ופרסומו לצורך שיבוש תמונת המציאות. לדוגמה, פרסומי כזב (פייק־ניוז), שימוש בפרופילים שקריים, הפצת שמועות, הסתה, שתילת ידיעות והשחתת אתרים.
פגיעה בזמינות המידע (Availability)	מניעת גישה למידע או שיבושו או מחיקתו ופגיעה בתשתיות קריטיות	מניעת היכולת לפרסם ולהפיץ מידע. לדוגמה, חסימת פלטפורמות שבאמצעותן מתקיימת תקשורת ועוברים מסרים של מפלגה או מועמדים בעת מערכת בחירות כדי למנוע את העברת המסרים.

נכון למועד כתיבת המאמר (שלהי 2021), בהתאם למגמה שעליה הצביעו מתניה ופייקובסקי, אנו רואים גידול בשימוש בתקיפות סב"ר לפגיעה תודעתית. המקרה האחרון, אשר פורסם ממש בימים אלו, הוא פרסום מאגר המשתמשים של אתר ההיכרויות לקהילה הגאה "אטרף" ואתרים נוספים שאוחסנו בחברת האחסון סב"ר סרב (Cyber Serve). מקרה זה מערב תקיפת סב"ר ששיקוליה כלכליים, בקשת כופר לתשלום בעבור מניעת הפרסום, עם איסוף מידע ושימוש במידע למטרות של תודעה והשפעה.[3] מקרה זה, כמו מקרים דומים נוספים לאחרונה, משויך לקבוצת Black Shadow הפועלת מאיראן, ועל כן בחלק הבא נתמקד בפעילותה של איראן, כמי שמובילה לוחמת סב"ר בעלת יעדים תפקודיים ותודעתיים כחלק מאסטרטגיית הלוחמה ההיברידית האי־סימטרית שלה נגד ישראל.

המגמות העולמיות שמות דגש חזק על התמודדות עם מבצעי תודעה, אך הרשות הלאומית להגנת הסב"ר אינה רואה בהתגוננות מפני מבצעי תודעה חלק ממשימותיה

מאפייני הפעילות האיראנית נגד ישראל בממד הסב"ר

נקודות ציון מרכזיות בהתפתחות לוחמת הסב"ר והתודעה האיראנית

הזירה הפנים־איראנית שימשה כר פורה לפיתוח והבשלת יכולת הסב"ר והתודעה של טהראן. עוד בשנים 1977–1979, בתקופת השאה, במהלך גלותו של ח'ומייני בצרפת, יועציו הקרובים סייעו לו לעצב תדמית ומסרים למספר קהלי יעד: הציבור האיראני במולדת ומחוצה לה, העולם המוסלמי והמערב. באיראן עצמה, נוסף על הפצת קלטות שמע וחוזי ועליהן נאומיו של ח'ומייני, הפיצו תומכיו פייק־ניוז, דוגמת האשמת משטר השאה בשריפה שפרצה בבית קולנוע באבאדאן ושהביאה למותם של קרוב ל־400 איש. לאחר השלמת המהפכה האסלאמית בפברואר 1979 הפכו הגורמים הנאמנים למשטר, בראשם משרד המודיעין ומשמרות המהפכה (להלן: "משה"מ"), ל"מתווכי המידע" החדשים העומדים מאחורי כלי תקשורת מרכזיים והמעצבים את מסריהם (Tabatabai, 2018).

במהלך השנים, כחלק מהמעקב המתמיד שמנהל שלטון האייתולות אחר אזרחיו מראשית דרכו, פותחו כלי טכנולוגיה וסב"ר שנועדו להתמודד עם השינוי בדפוסי התקשורת והמחאה. כבר בראשית שנות ה־2000 זוהו מספר קבוצות האקרים איראניות, אשר עסקו בעיקר בהשחתת אתרי אינטרנט בהיקף גדל והולך תוך פרסום מסרים פרו־איראניים ואנטי־מערביים (Dorothy, 2017).

[3] בימים אלו האירוע עדיין נמשך, ועל כן לא כל הפרטים ברורים. לעומת זאת תחושת הפגיעה בביטחון האישי ובפרטיות בממד הסב"ר מצד המשתמשים ברורה. לפרטים נוספים ראו: https://www.ynet.co.il/news/article/ryj092aif.

התוצאות השנויות במחלוקת של הבחירות לנשיאות איראן בשנת 2009 שהובילו להתעוררות תנועת מחאה אזרחית שנודעה בשם "התנועה הירוקה", ושהונעה על ידי פעילים באיראן ומחוצה לה, אשר השתמשו במדיה החברתית לצורך ניהול המאבק, חיזקה את ההבנה האיראנית בדבר הצורך לשלוט בתודעה (Libicki, 2015). בהמשך לכך, כחלק מהמענה למחאה, משה"מ הקימו קבוצות האקרים, אשר פעלו נגד אתרי חדשות של האופוזיציה ונגד אזרחים, לרבות זיהוי והפללה של האקרים שתמכו ב"תנועה הירוקה" והשחיתו אתרי אינטרנט של המשטר האיראני.

הבשלת יכולות הסב"ר האיראניות לימדה את השלטון בטהראן כי ההאקרים שסייעו בידיו להפלת אתרים "סוררים" למיניהם, מונעים בעיקר ממניעים כספיים. **בשל כך איראן יצרה רשת של "קבלני ביצוע" – קבוצות האקרים, אשר אינן מזוהות באופן רשמי עם טהראן אך נתמכות על ידה. גורמי מודיעין ומשה"מ היו מעבירים לאותן קבוצות רשימת תקיפות סב"ר בעלות יעדים בהיבטי תפקוד ותודעה, ואלו, בדומה למכרז רכש, התחרו לעיתים ביניהן ולעיתים שיתפו פעולה האחת עם האחרת במטרה להשיגם ולקבל תגמול כספי מטהראן** (Gundert et al., 2018).

תמונה 1: המהפכה הירוקה באיראן[4]

הזרז המקביל בממד הסב"ר התפקודי נתן תוצר כמעט במקביל בשנת 2010, עם גילוי התולעת סטוקסנט (Stuxnet), אשר נועדה לפגיעה תפקודית במתקני הגרעין של איראן. **אירוע זה היה גורם משמעותי בעיצוב אסטרטגיית הסב"ר האיראנית –**

[4] By [protected] from Tehran, IRAN - Iran electionUploaded by mangostar, CC BY-SA 2.0, https://commons.wikimedia.org/w/index.php?curid=7028729.

טהראן ראתה בתקיפה זו ובדומות שבאו לאחריה, הוכחה לאופן שבו יריבותיה משתמשות בסב"ר ככלי התקפי, והקימה כבר באותה שנה גופי סב"ר הגנתיים. יש אף המציינים כי "ביום שאחרי" סטוקסנט איראן שינתה באופן מהותי את גישתה ההתקפית בסב"ר: "והתחילה להפנות משאבים מודיעיניים, ביטחוניים ותעשייתיים לתחום ההתקפי ולצורך חדירה לתוך רשתות האויב. היה זה שינוי אסטרטגי. מינוף מרחב הסב"ר ככלי לאומי חדש להשגת מטרות גאו־פוליטיות כדוגמת הווירוס שאמון (Shamoon) שהשבית את מחשבי חברת הנפט הסעודית" (כהן, 2019. עמ' 72). **עדות לחשיבות הנושא בעיני המשטר אפשר לראות בדבריו של מפקד אגף הסב"ר בהרוז אסבאטי שהצהיר בריאיון ב־2015 כי: "יכולות סב"ר ואבטחת מידע חשובות לא פחות מהנושא הגרעיני"** (Bucala & Pendleton, 2015).

המאמץ האיראני לדומיננטיות בממד הסב"ר במזרח התיכון בפרט ובזירה הגלובלית בכלל רק גבר בשל הסנקציות ושאר האתגרים שעימם מתמודדת טהראן במישור הבין־לאומי בשנים האחרונות. בינואר 2019 אף הזהירה הסוכנות האירופית להגנת סב"ר (ENISA) כי הסנקציות עשויות להעצים את מידת המסוכנות הנשקפת מאיראן בממד זה (European Union Agency for Network and Information Security., 2019, p. 109). דוגמה להצלחותיה אפשר לראות בחשיפת מתקפה איראנית רחבת היקף שהצליחה להשתלט על חשבונות בתוכנת העברת המסרים "Telegram" שאותה תיאר גיל שוויד, מייסד חברת הגנת הסב"ר צ'ק פוינט, כך: "אחת ממתקפות הסב"ר היותר מורכבות שראיתי" (הלפרין, 2020). **פריצה זו, כמו אחרות אשר אירעו בשנים האחרונות, הוכיחו את רמת יכולת הסב"ר ההתקפי של איראן בפרט כמו כי לאף תוכנה או מערכת אין חסינות מלאה במרחב זה**. נכון ל־2021 יש המעריכים כי איראן תומכת ביותר מחמישים גופים וקבוצות שונות המבצעים בעבורה תקיפות סב"ר. הדבר מאפשר לאיראן ליישם אסטרטגיה של מלחמה משולבת באמצעות שימוש בכלים דיגיטליים (ולא קינטיים) למול שורה של יעדים במגזר הציבורי והפרטי בקרב יריבותיה השונות (Hochberg, 2021).

המערכה האיראנית בסב"ר נגד ישראל

המרחק הגאוגרפי הגדול בין ישראל לאיראן הצריך אותה למצוא דרכים שונות ומגוונות לפגוע ב"שטן הקטן". דרכים אלו כללו פעולה על ידי שליחים, הקמת בסיסים ברחבי המזרח התיכון או פעולה בממדים שבהם המרחק איננו משפיע, כמו מרחב הסב"ר והמידע. החל מ־2010, עת התגלתה התולעת סטוקסטנט, התרבו הדיווחים בישראל על אודות תקיפות סב"ר שבוצעו על ידי איראן לעיתים תוך שיתוף פעולה עם שלוחותיה חמאס וחיזבאללה. יכולות סב"ר ותודעה מבית מדרשה של טהראן מוצאות את דרכן גם לבעלות בריתה, אשר בחלק מהפעמים מבצעות את תקיפות הסב"ר בהתאם לבקשתה במטרה לאפשר לה יכולת הכחשה (Clarke, 2017; Schaefer, 2018). השימוש של איראן בלוחמת מידע בסב"ר נועד להמחיש

לאויביה שביכולתה לפגוע ב"בטן הרכה" שלהם, כלומר במרקם החיים האזרחי במדינותיהם (חיימיניס, 2019).

החוקר סם כהן מציין בסקירתו (2019) מספר אירועים בולטים מהמחצית הראשונה של העשור הקודם. במהלך השנים 2010–2013 אירעו תקיפות איראניות באמצעות קבוצות האקרים של חמאס וחיזבאללה נגד השב"כ, פיקוד העורף, משרד ראש הממשלה, משרד הביטחון, בנק ירושלים, צה"ל ורשתות תקשורת של "מערכות לאומיות חיוניות". מערכה נוספת[5] התרחשה בשנים 2012–2015 ופגעה בשורה של גופים ממשלתיים וחברות עסקיות בישראל ובעולם. מאפייני התוכנה הזדונית שבה השתמש "צבא הסב"ר של חיזבאללה" לביצוע תקיפות אלו, מלמדים כי היא פותחה על ידי איראן. נוסף על כך, ב־2018 נחשף קמפיין תודעה איראני רחב היקף, אשר כלל יותר מ־70 אתרי פייק־ניוז. במסגרת המבצע פעלה איראן למול מספר קהלי השפעה שונים בעולם, לרבות ישראל. זאת בדומה לאופן שבו הצגנו את פעילות גרעין תומכיו של ח'ומייני 40 שנה קודם לכן (ClearSky Security, 2018).

"טרור הוא תיאטרון", הכריז בריאן ג'נקינס, אנליסט תאגיד ראנד, בדו"ח מ־1974 שהיה לאחד המחקרים המשמעותיים של תופעת הטרור: "אם תצליח למקד מספיק תשומת לב זה לא משנה כמה חלש או חזק אתה באמת: אתה יכול לכופף אוכלוסיות למען דעתך ולהוביל את היריבים החזקים ביותר לכניעה"

גורמים שונים המשיכו לדווח על אודות תקיפות שונות שביצעה איראן בממד הסב"ר. בהקשר הישראלי בלטו שתי תקיפות הקשורות לבחירות שהתקיימו באפריל 2019 – דיווחים אודות פריצה לטלפון הנייד של בני גנץ, המועמד לראשות הממשלה והרמטכ"ל לשעבר, ערב בחירות 2019. כמו כן נחשף כי האיראנים הפעילו צבא של "בוטים" המגיבים באופן אוטומטי לאירועים שונים מתוך מטרה להשפיע על השיח בציבור הישראלי ועל תוצאות הבחירות. דפוס פעולה זה חזר על עצמו בבחירות אפריל 2021 (שפריר וגלוברמן, 2021).

החל משנת 2020 התרבו הדיווחים התקשורתיים המלמדים כי תקיפות הסב"ר מצד איראן הן בעלות פוטנציאל נזק גבוה במיוחד. באפריל של אותה שנה אירעה סדרת מתקפות סב"ר נגד מתקני מים בישראל. ראש מערך הסב"ר הלאומי יגאל אונא הצהיר אז כי: "כל הקווים נחצו, החלה מלחמה מסוג חדש".[6] כחצי שנה לאחר מכן טען שר המודיעין אלי כהן שאיראן מנסה להשפיע על דעת הקהל בישראל

[5] המכונה בשם "Volatile Cedar".

[6] https://www.ynet.co.il/digital/technews/article/HJTQdS9b00.

ומשקיעה משאבים נרחבים בתעמולה ובחתרנות המכוונים לקהל בארץ (הלפרין, 2020).

בעקבות שורה של מתקפות כופרה שאירעו באותה שנה, עלתה ההשערה כי כחלק מלוחמה היברידית ממשיכה איראן "להציק" למשק הישראלי בעזרת מתקפות סב"ר שמתחזות למתקפות כופרה (שיעדיהן תפקודיים ופיננסיים), אך למעשה מדובר בתקיפות סב"ר שיעדיהן תודעתיים – פגיעה בתחושת הביטחון של האזרחים (ברקוביץ וטרבלסי, 2021). לדפוס זה היו כמה דוגמאות, אך המפורסמת שבהן היא המתקפה על חברת הביטוח שירביט. **תקיפה זו הייתה אבן דרך באשר להבנת פוטנציאל הנזק הנרחב שעלול להיגרם כתוצאה מתקיפת סב"ר שיעדיה תפקודיים ותודעתיים כאחד' ושמבוצעת על ידי שחקנים מדינתיים עוינים לישראל**.

איראן חולקת את מומחיותה בתחום לוחמת הסב"ר וההשפעה עם שותפותיה ל"ציר ההתנגדות". **לפי מספר חברות מודיעין סב"ר שיפר מערך הסב"ר של החמאס באופן ניכר את יכולותיו בשנים האחרונות בזכות טהראן המספקת לו הדרכות, כלים ומימון** (דהן, 2021). במסגרת זאת, במהלך מבצע "שומר החומות" (מאי 2021) נחשפה רשת של פרופילים מזויפים ברשתות החברתיות שפעלה ליצירת דמורליזציה בציבור הישראלי בין היתר באמצעות מסרים, כמו "הפתרון הוא לברוח לחו"ל". לפי דיווח תקשורתי בישראל הצטבר מידע כי רשת זו הופעלה על ידי איראן.[7] כמו כן משפיעני רשת ערבים שיתפו וחזרו על פוסטים וציוצים מסוג זה, ובכך הם העצימו את תפוצתם. לפי הדיווח: "האיראנים לא הסתפקו בכך; הם השתתפו באופן פעיל בתדלוק המהומות והמאורעות, כולל ובמיוחד בטלגרם".[8]

בשלהי מאי 2021, בתום מבצע "שומר החומות", התפרסמו ידיעות תקשורתיות כי המשטרה ומערכת הביטחון הציעו בשיאו של המבצע וההתפרעויות בערים המעורבות לחסום לחלוטין כל גישה לרשתות החברתיות בישראל, בהן פייסבוק, טיקטוק ואינסטגרם. עוד פורסם כי ראש הממשלה בנימין נתניהו תמך בכך. יודגש כי חסימה של רשתות חברתיות מעולם לא התקיימה בישראל, והיא נחשבת צעד חריג ביותר שלא מתקיים במדינות דמוקרטיות (לוי, 2021).

באוקטובר 2021 ציינה חברת מיקרוסופט במסגרת "דוח ההגנה הדיגיטלי השנתי" כי איראן הגדילה פי ארבעה (!) את מספר הניסיונות לביצוע תקיפות סב"ר נגד ישראל במהלך שנה זאת.[9]

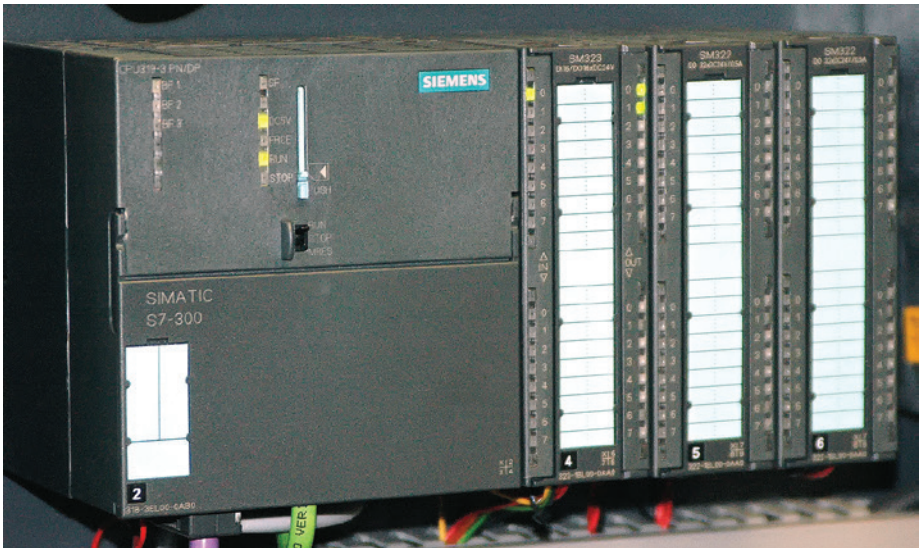
נוכח האמור עולה השאלה כיצד אפשר להתמודד עם מתקפות משולבות אלו? נתחיל בהצגת תפיסה המציעה מודל ליצירת חוסן למבצעי סב"ר בעלי יעדים תפקודיי ותודעתיים ולאחר מכן נסקור דרכי התמודדות והמלצות נוספות.

---

7 https://www.themarker.com/advertising/.premium-1.9818498.

8 שם.

9 https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report?rtc=1.



תמונה 2: אחד הרכיבים בהם פגעה התולעת סטוקסנט – בקר תעשייתי מתוצרת חברת סימנס (צילום: Ulli1105)[10]

מודל מוצע ליצירת חוסן לתקיפות סב"ר בעלי יעדים תפקודיים ותודעתיים

הילכו שניים יחדיו בלתי אם נועדו?

בספרות העולמית בתחום קיימות המלצות רבות הנוגעות לדין הבין־לאומי בהיבטי סב"ר והפעלת השפעה זרה, ניסיונות לרגולציה רב־לאומית על הרשתות החברתיות והמלצות חשובות נוספות ורחבות שיידרש זמן רב למימושן. בחרנו להביא בפרק זה המלצות ישימות הכרוכות ב"כאן" (ישראל, צה"ל), ו"עכשיו" (ניתנות למימוש בעתיד הקרוב) מתוך הבנה כי נוכח ההישענות הרבה של מדינת ישראל בתחומי החיים השונים, התפקודיים והתודעתיים, על מערכות ורשתות דיגיטליות מדובר באיום משמעותי המתדפק על דלתנו, ואין לנו את הפריבילגיה להמתין לפתרונות גלובליים וארוכי טווח בהתמודדות איתו.

כפי שראינו מעלה, בעידן של מלחמות היברידיות מבצעי סב"ר בעלי יעדים תפקודיים ותודעתיים שלובים זה בזה מתוך מטרה להעצים את הישגי האויב באמצעות המידע שחשף. מתוך כך אנו מאמינים כי לטובת יצירת חוסן להתמודדות עם שתי התכליות של מבצעי הסב"ר המענה צריך להיות הוליסטי. בספרות קיימות הגדרות רבות למונח חוסן, לטובת עבודה זו בחרנו את הגדרתם של פדן ואלרן (2018, עמ' 7): "החוסן מבטא את היכולת של מערכת מאוימת להכיל בגמישות את ההפרעה הנכפית עליה ואת הנסיגה התפקודית הבלתי נמנעת הבאה בעקבותיה, להתאושש ממנה במהירות ולחזור לתפקוד מערכתי מלא או אף משופר".

[10] By Ulli1105 - Own work, CC BY-SA 2.5, https://commons.wikimedia.org/w/index.php?curid=1623227.

כדי לפתח חוסן לאיומים בממד זה המלצתנו המרכזית היא אימוץ גישה פרואקטיבית המושאלת מתפיסת החוסן למתקפות סב"ר ולהרחיב אותה גם לפעילויות מבצעי תודעה. בדומה להגדרת החוסן המערכתית, 'חוסן סב"ר' (cyber resiliency) מוגדר כיכולת לצפות, להתמודד להתאים ולהתאושש מתנאים מקשים, מלחצים, מתקיפות או מפגיעה במערכות המשתמשות או מתאפשרות באמצעות משאבי סב"ר, והדבר נכון הן ליעדים תפקודיים של תקיפות סב"ר והן ליעדים תודעתיים.

איור 1: שלושת השלבים בהתמודדות עם אירוע סב"ר

חלק מרכזי במציאת דרכי ההתמודדות מתחיל באפיון של הנפגעים מפעולות אלו. אף על פי שהצגנו קודם לכן שהן עשויות להגביל את מרחב הפעולה והלגיטימציה, צה"ל אינו נפגע ישיר של פעילויות אלו אלא עקיף בלבד. לכן קיימת גישה שסבורה כי נכון לתת למערך הלאומי לטפל באירועים הללו מתוך ראייה לאומית רחבה יותר. כך, למשל, לא נכון שצה"ל יפנה ישירות לציבור בתוכניות של חינוך והסברה לפיתוח מיומנויות מידע ביקורתיות. בעוד כי ברורים לנו היתרונות של גישה זו ושיתוף הזרועות עם מערך הסב"ר הלאומי, אנו מציעים כי בייחוד בתוכו פנימה – על צה"ל לקחת יוזמה אקטיבית יותר בגיבוש תפיסה ובביצוע של המלצות קונקרטיות יותר לשמירה על החוסן האישי והארגוני.

התפיסה שאנו מציעים במאמר זה מבוססת על תפיסת חוסן הסב"ר (Cyber Resiliency) של מכון התקינה האמריקאי (NIST) וכוללת שלושה נדבכים מרכזיים הכרוכים זה בזה בצורה מעגלית: הכנה, הכלה והתאמה (Ross et al., 2019). כדי לתת מענה לאתגרים הכרוכים במענה למבצעי תודעה והשפעה ביצענו התאמות משמעותיות לתפיסה. בין היתר איחוד שלבי ההכלה וההתאוששות לשלב אחד מסיבות שאותן נפרט בהמשך. בחלק זה נציג את יישום תפיסת החוסן בסב"ר עם התאמות והדגשים שיאפשרו לה יישום והתמודדות עם מבצעי תודעה ולאחר מכן המלצות קונקרטיות הנגזרות ממנה.

כיצד מתכוננים למתקפת סב"ר?

שלב ראשון: הכנה

- **דע מול מי אתה עומד – איסוף מודיעין ייעודי**

במטרה להבין ככל הניתן את תמונת המצב של היריב בהיבטי יכולות נדרש להקצות יכולות איסוף. איסוף זה יכול להתבצע תוך שימוש בכלי האיסוף הקיימים, לרבות ניצול המודיעין הגלוי (OSINT) שבו קבוצות האקרים שונות נוטות להתרברב בהישגיהן מחד גיסא, כמו רשת ה־Dark Net ופורומים סגורים המשמשים פעמים רבות כר לשיתוף פעולה בין תוקפים שונים, הן ברמה אידיאולוגית והן ברמת פיתוח כלי תקיפה, מאידך גיסא. כמו כן, נדרש להרחיב את איסוף המודיעין על אודות מושכי השפעה שלילית חשודים (ברמה הלאומית) ברשת, יצירת כלי ניתוח ואיסוף מידע על בוטים, פרופילים מזויפים ורשתות מתואמות למבצעי תודעה וחשיפתם באופן קבוע.

- **גיבוש קריטריונים ברורים לחוסן ומיסודם**

בהתאם לרמת החשיפה וקריטיות התהליכים, אשר מתבססים על המערכות והרשתות השונות, יש להגדיר וליישם את רף החוסן הנדרש על צורותיו – רכש ציוד מחשוב נוסף, יצירת תהליכים מקבילים וכדומה. ראוי לבחון את תפיסת החוסן הפוטנציאלי במסגרת תרגולים ומבדקים (ראו לעיל) כדי לוודא את הטמעתה הנאותה. מורכב יותר לקבוע קריטריונים ברורים להתמודדות עם מבצעי תודעה, אך בהחלט אפשר לסמן קווים אדומים מרכזיים שאנו סבורים שיפגעו בחוסן של החברה, ולתכנן מראש מקרים ותגובות להתמודד איתם. מקרים ותגובות אלו יכולים להיות מתורגלים באופן שוטף ונדרשים לניטור שוטף כדי לבחון חריגות מהם.

- **תרגול תרגול תרגול – ביצוע מבדקים טכנולוגיים וסקרי סיכונים למיניהם**

ביצוע סקרי סיכונים, בדיקות חדירות, סקירת קוד ויתר כלי הבדיקה הרלוונטיים שיסייעו בזיהוי פגיעות וסיכונים שונים בממד הסב"ר. זיהוי זה יאפשר הפחתה, לעיתים משמעותית, בהשלכות שייגרמו כתוצאה מניצול הפערים הקיימים. כמו כן, עצם המודעות להם, גם אם ינוצלו לשם תקיפה, היא בעלת ערך להקטנת מרחב אי־הוודאות והמשאבים הנדרשים להתמודדות עימם. נדרש לתת הדגש לתרגול נוסף של התמודדות עם מבצעי תודעה והשלכות שליליות שעשויות להשפיע על אמון הציבור בצה"ל ועל פגיעה בלגיטימציה בו. התרגול יאפשר בניית פק"לים ומסרים מוכנים מראש להתמודדות עם מצבים כאלו. התרגול יאמן את המפקדים להביא בחשבון את זירת ההשפעה בסב"ר בקבלת החלטותיהם.

- **ניטור – פיתוח מנגנוני פיקוח ובקרה**

יישום ואכיפה של שימוש בכלי ניטור לסוגיהם במטרה להגדיל את הסבירות לזיהוי תקיפת סב"ר בפרק הזמן הקצר ביותר שניתן. כלים אלו צריכים לדגום

מגוון רחב ומגוון של מדדים, החל בנפח תעבורה מידע ברשת, היקף פניות לשרתים, תקינות פעילות מערכות מידע ועוד. נדרש להביא בחשבון תקיפות שמבצעות קבוצות מתוחכמות (APT), אשר עלולות שלא להתגלות באמצעות ניטור. הניטור צריך לכלול גם אפיקי השפעה, כגון רשתות חברתיות ומדדים, כמו אמון הציבור המשרתים בצה"ל. ניטור שכזה יאפשר להבחין בפעילויות תודעה חריגות בזמן שגרה, לצבור ניסיון בהבנת התופעות בנושאים הללו ולפתח יכולות לחירום. ניטור קבוע גם יאפשר לזהות חשבונות פיקטיביים, בוטים ושאר מרעין בישין המנסים להשפיע על חיילי צה"ל או להכין תשתית לפעילויות סב"ר נוספות דרך הרשתות החברתיות.

שלב שני: הכלה וההתאוששות

שלב זה מתייחס לפרק הזמן שבין תחילת השפעתה של תקיפה, שטרם זוהתה, דרך זיהויה בפועל ועד להכלתה, אם היא אינה יוצרת נזק נוסף. הוא כולל את המענה המיידי הנדרש לאירוע ואת בניית החוסן להמשך התפקוד.

- **מענה לאירוע שהתרחש**

הגדרה וביצוע של מכלול הפעולות הנדרש במטרה להקטין את הנזק הנגרם, לתחם אותו ולפעול ביעילות להכרעת התקיפה. במישור זה תרגול תדיר של מענה לאירוע סב"ר במתארי תקיפה מגוונים תוך שיתוף חברי צוות הסב"ר, מנהלים עסקיים, ספקים מרכזיים, דוברים, צנזורה ועוד, חיוני לצורך שיפור אפקטיביות המענה באירוע אמת, כפי שהוצג מעלה.

- **חוסן לשם המשכיות תפקודית**

במקביל למתן מענה בשלביו השונים של האירוע נדרש להשתמש במרכיבי החוסן הרלוונטיים, דוגמת משאבי מחשוב, ציוד פיזי, תהליך ידני ועוד, במטרה לאפשר המשכיות תפקוד. בדומה להמשכיות עסקית, יש להגדיר את הקריטריונים במסגרת תפיסת החוסן, כפי שהוצג מעלה.

איחדנו בין שלב ההכלה וההתאוששות, שכן בדומה לתפיסת הביטחון של ישראל, אשר מדגישה את הצורך להעביר את המלחמה לשטחו של האויב, אנו צריכים לבנות את הכוח בצורה שתאפשר לנו לספוג בלי להיות מוכרעים, ובמקביל ליציאה לתקיפת נגד כחלק משלב ההתאוששות צריך למנוע מהיריב הישג ולהעסיק אותו בנושאים אחרים. אין לנו את הפריווילגיה לעצור את העשייה ולרדת מתחת לרף הכשירות, האמון או הלגיטימציה לצורך התאוששות. הדבר נכון לתקיפות סב"ר בעלות יעדים תפקודיים ותודעתיים כאחד. בעת אירוע משמעותי, אשר יפגע באמון ובלגיטימציה של צה"ל, צריך יהיה לזהות היטב את המוקדים לנזק ולפעול ביעילות כדי לתחם אותם למקורות ולמוקדים ספציפיים, ולאחר מכן לטובת הגדלת החוסן נדרש יהיה לחשוף אותם ולהתמודד איתם לגופו של 'חשבון' (פיקטיבי או אמיתי) ולגופו של עניין.

שלב שלישי: התאמה

במסגרת השלב, בהתאם להפקת הלקחים מהאירוע, מבוצעים השינויים וההתאמות הנדרשות בתהליכים ובמשאבים הטכנולוגיים, הפיזיים והאנושיים מתוך רצון לצמצם את החשיפה לסיכון ולהקטין את ההשפעה בתקיפה הבאה.

לסיכום, בחלק זה הצענו עקרונות לתפיסת חוסן סב"ר הממזערת את הפגיעה התפקודית והתודעתית כאחד, בשונה מן התפיסה המקורית המתייחסת לפגיעה ביעדים תפקודיים בלבד. הדגשנו את הרכיבים הנדרשים לטובת ההתמודדות אפקטיבית עם מבצעי השפעה. חשוב לציין כי בעוד שאפשר להפעיל חלקים ממנה כדי לעמוד ביעדי החוסן בממד זה, אנו סוברים כי ללא בנייה של תפיסה שלמה והוליסטית השפעת חלקים אלו תהיה מוגבלת ולא תצליח להתמודד עם הנזקים התודעתיים שבראשם נמצאים פגיעה בלגיטימציה, פגיעה באמון ובתחושת הביטחון, ויצירת אווירה ביקורתית כלפי פעילות צה"ל.

דרכי התמודדות והמלצות נוספות

נוסף על ההמלצות התפיסתיות המופיעות מעלה, ראינו לנכון לפרט על דרכי התמודדות נוספות הנפוצות בעולם ולאחריהן לספק סט מצומצם יותר של המלצות קונקרטיות לקובעי המדיניות לשם פיתוח החוסן למבצעי תודעה. אימוץ דרכי ההתמודדות וההמלצות אינם בהכרח תלויים במימוש התפיסה המופיעה מעלה.

בדיקת עובדות וחינוך לחשיבה ביקורתית

חלק מהפתרונות לבעיית המדיה החברתית שלנו עשוי להיות למעשה יותר מדיה חברתית – רק בשימוש אחר. הטכנולוגיה משמשת לפתור מגוון רחב של בעיות ברחבי העולם, ומספר גדל והולך של מדינות אינן משתמשות במדיה החברתית רק כדי להפחיד או לנחם את אזרחיהן. הן גם משתמשות בה כדי להרחיב את המודעות הציבורית לאופני צריכת המידע ומאפשרות גישה לתוכניות הכשרה, לחקור תרמיות ושקרים ולפעולות המקדמות צרכים אזרחיים.

במחקר של דפוסי צריכת מידע מדדו חוקרים מאוניברסיטת סטנפורד שלוש קבוצות – סטודנטים לתואר ראשון, דוקטורים להיסטוריה ובוחן עובדות מקצועי – על האופן שבו הם העריכו את הדיוק של מידע מקוון. למרבה ההפתעה גם הסטודנטים לתואר ראשון וגם הדוקטורים קיבלו ציון נמוך. ממצאי המחקר העלו שאף על פי שניתן להעריך שהם בהחלט אינטליגנטיים, הם פנו למידע "אנכית" – הם נשארו בתוך השקפת עולם אחת וניתחו את התוכן של מקור אחד בלבד. כתוצאה מכך הם ניתנו למניפולציה בקלות.

ניתן להסיק מכך שהתמודדות עם מידע שגוי אינה עניין של אינטליגנציה גרידא, אלא פיתוח סט הכישורים המתאימים (Bergstrom & West, 2020). כישורים אלו כוללים, בין היתר, זיהוי של מקורות מידע אמינים, יכולת לצלול ולהצליב פרטים,

יכולת זיהוי של פרטים מחשידים ויכולת שימוש באתרי בדיקת עובדות (WHO, 2020).

מנהיגים בקהילות שלהם, הווירטואליות והממשיות, הם גורמים בעלי השפעה רבה על אופני צריכת המידע. ארגונים שונים מבצעים הכשרות למובילי קהילות ולמנהיגים על האופנים שהם יכולים ליצור חוסן קהילתי לצריכה של מידע שקרי, שגוי ומסולף. אך לא רק מנהיגים, מספיק שחבר קבוצה מחליט שלא להפיץ מידע שהוא אינו בטוח בנכונותו, מבצע בדיקה או אפילו שואל את המפיץ האם הוא בטוח במה ששלח, כדי לפגוע באפקטיביות של מאמצי מידע. פינלנד, אסטוניה, ליטא ושוודיה, מדינות שכנות לברית המועצות, אשר התמודדו עם מאמצי השפעה ומידע מצידה, פיתחו לאורך השנים תוכניות ל'חיסון' של האוכלוסייה למאמצי התודעה הסובייטיים. 'מערכת החיסון' המדינתית שהן פיתחו כוללת תוכניות מקיפות לחינוך האזרחים, ניטור המידע הפומבי למציאת מידע לא מבוסס וחובת הזדהות בעת התערבות זרה בתקשורת (Singer & Brooking, 2018). את אופן השפעתם

"טרור הוא תיאטרון", הכריז בריאן ג'נקינס, אנליסט תאגיד ראנד, בדו"ח מ־1974 שהיה לאחד המחקרים המשמעותיים של תופעת הטרור: "אם תצליח למקד מספיק תשומת לב זה לא משנה כמה חלש או חזק אתה באמת: אתה יכול לכופף אוכלוסיות למען דעתך ולהוביל את היריבים החזקים ביותר לכניעה"

של מאמצי אוריינות דיגיטלית למלחמה בקורונה המחיש ארגון הבריאות העולמי באמצעות איור שהראה כי מספיק מעט אנשים אשר "הטילו ספק במידע שקיבלו", "לא העבירו את ההודעה הלאה" או "וידאו עם שולח ההודעה את אמיתותה" כדי לצמצם בכמעט 80% את כמות הנחשפים להודעה שקרית.[11]

כיצד אפשר ליישם זאת אצלנו?

מרכיב מפתח בתוכנית כרוך בהכשרת קהל משתמשי הרשתות החברתיות בצה"ל להיות צרכנים ביקורתיים יותר של מידע במדיה חברתית (ובכלל). לשם כך נדרש לפתח בקרב חיילי צה"ל ומפקדיו את הכישורים והיכולות לזהות חדשות מזויפות, לשקול את אמינות המקורות במדיה החברתית ולהכיר בתפקידם בהתמודדות עם תוכן כזה או בהגבלת הפצתו. לממלאי תפקידים שונים – מפקדים, מנהלי קהילות, משתתפים בקהילות וכדומה – יש תחומי אחריות שונים. על בסיס המחקרים שנסקרו והראו כי מספיקים שניים או שלושה אנשים בקהילה שמסוגלים ויודעים

11 https://www.who.int/news-room/spotlight/let-s-flatten-the-infodemic-curve.

למסגר את המידע הנמסר באופן ביקורתי (O'Connor & Weatherall, 2019) , מומלץ לפעול ליצירת הכשרות מתאימות בקנה מידה רחב, בייחוד למנהלי הקהילות ואנשים שמזוהים כבעלי פרופיל השתתפות חברתי משמעותי, ושיכולים לסייע לפתח חוסן בקהילות שבהן הם משתתפים. אפשרות נוספת היא באמצעות יצירת פרסומים בנושא שיפורסמו בעת הצורך. מובן שהמשימה היא רחבה ולאומית, ונדרש לשתף פעולה עם פיתוח ויישום של הכשרות רלוונטיות לצריכה ביקורתית של מידע כבר בעת הלימודים במערכת החינוך.

בהסתכלות פנים־צה"לית באופן כללי פעילות חיילי ומפקדי צה"ל ברשתות החברתיות מצומצמת. אנו ממליצים לבחון אפשרות לאמץ באופן ממוסד פעילות ברשתות החברתיות על ידי חיילים ומפקדים תוך מתן כלים מתאימים להשפעה והתמודדות עם השפעות זרות ברשתות השונות. אנו מעריכים שבאמצעות הדרכות מתאימות ומתוך החיכוך הכרוך בפעילות ברשתות החברתיות יתפתחו מיומנויות צריכה ביקורתית של מידע שישמשו גם בזמן חירום ויאפשרו לחיילים ולמפקדים לתרום לחוסן הלאומי בתחום. כמובן ששימוש רב יותר עשוי להיות כרוך ביותר סיכונים, ועל כן נדרש ניטור שוטף שיאפשר התרעות כאשר מזהים או חושדים כי יריבים מתמקדים בהשפעה על חיילי צה"ל ומפקדיו בקמפיינים להשפעה מקוונת.

שימוש בטכנולוגיה לזיהוי מידע שקרי ומניעת הפצתו

הדוגמה מעלה מציגה מה אנחנו כבני אדם יכולים לעשות לטובת המלחמה בדיסאינפורמציה, אך לא בהכרח צריך שותפים אנושיים למלחמה זו. ניתן לשאוב רעיונות טכנולוגים למלחמה במידע שקרי ממקרים אחרים של ניסיונות להפיץ מידע, שעשוי לעורר עניין רב, אך יש צורך למנוע את הפצתו הרחבה, דוגמת המלחמה בפדופיליה. במאמץ להילחם בפדופיליה פותחה מערכת בקרת תוכן המכונה PhotoDNA. מסד הנתונים הסודי מארח יותר ממיליון אובייקטים ויזואליים ומשווה כל תמונה או וידאו שמפורסמים ברשתות החברתיות עם מסד עצום זה המכיל תמונות, אשר סווגו כפדופיליות, כדי למצוא תאימות ולוודא כי התמונה המועלית לרשת איננה מכילה או מעודדת פדופיליה. מערכת זו התפתחה בעקבות החובות החוקיות המוטלות על הרשתות החברתיות, ואפשר לצפות שכל פלטפורמת מדיה חברתית גדולה תאמץ בסופו של דבר את הכלי.

אם כך יקרה, הדבר יצמצם משמעותית מאוד את הפדופיליה ואת מקרי פורנוגרפיית ילדים ברשתות החברתיות (Singer & Brooking, 2018). בעקבות הצלחתה של מערכת PhotoDNA הכריזה פייסבוק על מאמץ דומה למנוע מקרים של הפצת 'פורנו נקמה' – תמונות שצולמו בעורמה או בלא רשות ושמופצות ברשתות החברתיות כדי לנקום במצולמת. פייסבוק מאפשרת העלאה של התמונות והסרטונים, אשר מהם המצולמת חוששת, כדי ליצור 'טביעת אצבע' דיגיטלית שתאפשר לרשת לזהות ולמנוע את הפצתם (Statt, 2017). באופן דומה ייתכן שאפשר ליצור 'טביעת

אצבע' דיגיטלית לידיעות שקריות, ויזואליות או טקסטואליות המופצות ברשתות החברתיות ובכך לנטר אותן ולמנוע הפצתן. טכנולוגיות כאלו יכולות לשמש "כיפת ברזל" להגנה מפני מבצעי תודעה.

מכיוון שמדובר בביעה גלובלית, קיימים מגוון של כלים להתמודדות עם הבעיות הללו.[12] החל בתוספים לדפדפן שיודעים להתריע על מידע הנחשד כמזויף,[13] אתרים הבודקים מידע חשוד על ידי קהילות מומחים,[14] לרבות אתרים הבודקים את אמינות מקורות המידע עצמם, אתרי החדשות יכולים למנוע הצגה של מקורות החשודים כמזויפים.[15] קיימים גם סוגים אחרים של פתרונות טכנולוגיים הכוללים אפשרויות שונות לזיהוי ואחזור מידע (קוגוסובסקי, 2021). לאחרונה חוקרי מכון ראנד האמריקאי הציגו יכולת מרשימה לזיהוי ידיעות שקריות תוך שימוש בבינה מלאכותית (Marcellino et al., 2021). על אף מורכבותם הטכנית פתרונות אלו עשויים להיות יעילים במיוחד במדינה קטנה, כמו ישראל אשר רוב אוכלוסייתה משתמשת בשפה ייחודית (עברית). שיתוף הפעולה מצד פלטפורמות המדיה הוא משמעותי, ואנו ממליצים על בניית צוותי פעולה משותפים במטרה לשפר את הכלים והמידע, אשר יאפשרו להילחם בצורה טובה יותר בתופעה זו. שיתוף הפעולה בין המדינות לפלטפורמות המדיה החברתית הצליח לאפשר התמודדות מוצלחת (יחסית) עם התוכן שהופץ על ידי ארגון דאע"ש, למשל.

המגמות העולמיות שמות דגש חזק על התמודדות עם מבצעי תודעה, אך הרשות הלאומית להגנת הסב"ר אשר לימים הפכה עם מטה הסב"ר הלאומי למערך הסב"ר שאותו אנו מכירים כיום) אינה רואה בהתגוננות מפני מבצעי תודעה חלק ממשימותיה. כך אפשר ללמוד מתשובת ראש הרשות המופיעה במחקר שערך מרכז המחקר והמידע של הכנסת: "הרשות איננה אחראית לטיפול בתוכן המופץ במרחב הסב"ר וככל שמדובר בהפצת מידע כוזב לשם השפעה על הבחירות, השפעה על דעת הקהל ועל עמדות פוליטיות, אין הרשות עוסקת בכך" (גולדשמידט ווורגן, 2017).

ישראל היא המדינה הדמוקרטית היחידה במערב שבה צנזורה מעוגנת במסגרת החוק עוד מימי המנדט הבריטי (1933 – "פקודת העיתונות"; 1945 – "תקנות ההגנה לשעת חירום"). כבר לפני למעלה מעשרים שנה(!) היו אנשי תקשורת בישראל שזיהו את ההתפתחות הטכנולוגית כגורם בעל השפעה ניכרת על פעולת הצנזורה. העיתונאי גיא קוטב, במאמרו "סוף עידן הצנזורה" (1999), כותב כי הטכנולוגיות התקשורתיות החדשות הביאו לגסיסתו של מוסד זה, אשר ממשיך להתקיים רק הודות להיענות מצד אנשי התקשורת. האתגרים שמציב בפניה העידן הדיגיטלי,

---

12 לאחרונה אף התקיים דיון בועדת החוץ והביטחון של הכנסת בנושא. לפרטים ראו: https://www.pc.co.il/featured/339531/.

13 https://slate.com/technology/2016/12/introducing-this-is-fake-slates-tool-for-stopping-fake-news-on-facebook.html/.

14 https://metafact.io/.

15 https://www.newsguardtech.com/.

בייחוד עליית התקשורת המקוונת אשר עוקפת את המדיה המסורתית, דורשים ממנה לשנות את פניה (אלטשולר & לוריא, 2016). עם זאת מיקומה ומעמדה הייחודי של הצנזורה בישראל וקשריה עם התקשורת הממוסדת יכולים לסייע לה לבצע את השינוי הנדרש לטובת בניית יכולות חדשות לניטור, סינון ובקרת התוכן והמידע למניעת נזק אפשרי. התאמה כזו עשויה לאפשר לה לשמש מרכז לתיאום וסנכרון המלחמה בפעילויות תודעה המופעלות על ידי מדינות זרות המנסות לערער את הביטחון והחוסן של מדינת ישראל. גופים דומים כאלו קיימים בכמה מדינות כמו ארה"ב, אוסטרליה, דנמרק ובלגיה (Bodine-Baron et al., 2018; קופרווסר וסימן טוב, 2019). העברה של סמכויות לגוף כזה ומתן כלים צריכה להיות מלווה בחקיקה מתאימה כדי שיוכל למלא את ייעודו. עם זאת, אנו סוברים כי נדרש יהיה לתת את הדעת היכן יהיה מקומו של גוף שכזה, האם כחלק ממערך הסב"ר הלאומי או בתצורה אחרת.

מלחמה קינטית בהשפעה קיברנטית

מפיצי־על, מונח שחדר לחיינו בעקבות הקורונה, משחקים תפקיד משמעותי בעולם הסב"ר. ל"מפיץ־על" בעולם הווירטואלי יש יכולת לתקוף באופן נרחב לשם השגת יעדים בתחום המערכת המשולבת. כדי לפגוע באותם "מפיצי־על" מפעילות מדינות כוח קינטי. עוד באוגוסט 2015, ארה"ב חיסלה מהאוויר את ג'ונאיד חסין, מוסלמי יליד בריטניה שנודע כהאקר "TriCk", ושבהיותו בן 17 פרץ לתיבת המייל של ראש ממשלת בריטניה לשעבר בלייר ולאחר מכן סייע לדאע"ש להוציא לפעול תקיפות בממד הסב"ר. ארבע שנים לאחר מכן התנקשה וושינגטון בדובר דאע"ש כניסיון להתמודד עם השפעתו ברשתות החברתיות לגיוס פעילים, משאבים ועידוד לפעילות נגד ארה"ב (Washington, 2019).

גם ישראל יישמה אסטרטגיה זו בהתאם לצרכיה. בפברואר 2016 עצרו כוחות הביטחון את מג'ד עווידה, אחד מההאקרים הבולטים באותה עת שסייע לחמאס, אשר הצליח בין היתר לחדור למערך השידור של מזל"ט צה"לי שעקב אחרי פעילי טרור ברצועה ולעקוב אחר שידוריו. עווידה נדון לתשע שנות מאסר. כשלוש שנים לאחר מכן, במאי 2019, לאחר סיכול מוצלח של פעילות סב"ר התקפית מצד חמאס, תקף צה"ל מבנה שממנו פעל מערך הסב"ר של הארגון (Newman, 2019; שחף, 2019).

במהלך מבצע "שומר החומות" (מאי 2021) ביצע צה"ל שורה של פעולות הפצצה וסיכול ממוקד נגד מערך הסב"ר של החמאס, לרבות סיכול ראש מערך הסב"ר בארגון ג'ומעה טחאלה ופעילים נוספים, לצד תקיפה של יותר מעשרה מרכזי מבצעים. ייתכן שפגיעה זו בוצעה בין היתר כסגירת מעגל בעקבות הניסיון של הארגון לבצע פעולת סב"ר התקפית במאי 2019, אשר סוכלה על ידי גורמי הביטחון בישראל.[16] **תקיפות**

[16] https://www.ynet.co.il/digital/technews/article/HkIluANKd

אלו של ישראל הן דוגמה להתקפה קינטית המשמשת תגובה לפעילות במרחב הקיברנטי. אפשר לראות בה את צידה השני של הלוחמה המשולבת – זו אשר מעתיקה את הלחימה לממד נוסף, קינטי, הן במטרה למנוע את פעילות הסב"ר ההתקפי עצמה והן כדי להעביר מסר לתוקפים ושולחיהם.

סיכום

פול ויריליו, הפילוסוף של הטכנולוגיה, טוען כי כל טכנולוגיה חדשה מביאה איתה את הקטסטרופה שלה הנובעת מנקודת הכשל הייחודית לה. במילותיו: "המצאת הספינה הביאה איתה את אפשרות טביעתה, המצאת המטוס הביאה איתה את אפשרות התרסקותו, המצאת הרכב הביאה את תאונת הדרכים" (Virilio, 1984/1991; Virilio & Redhead, 2004). כל עוד מידע זורם דיגיטלית ובקצב מהיר יותר – כך קשה לסנן את הבר מן התבן ולמנוע פגיעה של גורמים זרים בהיבטים תפקודיים ותודעתיים באמצעות ממד זה. ככל שתגדל ההסתמכות שלנו על המערכות הדיגיטליות לגווניהן, כך אנחנו חושפים את עצמנו ל"תאונות" מסוג חדש וצריכים להשקיע מאמץ בצמצום הסיכונים כדי ליהנות מהתועלות הדיגיטליות ללא חשש. כיום ניכר כי פעילות הלוחמה המשולבת בממד זה עולה, רף הכניסה לתחום וסט הכישורים הנדרש נמוך מן העבר (והולך ופוחת לאורך ציר זמן), ואנו מסיקים שהאיום לדמוקרטיות המערביות, לרבות ישראל, הולך וגדל.

הטרור הוא תיאטרון, וההצגה הכי טובה בעיר או בכפר הגלובלי מבוססת על שימוש בממד הסב"ר להשגת יעדים תודעתיים. כיום עצם הדיווח על פריצה, גם אם לא נעשתה, מייצר גלי נזק תודעתיים נרחבים, שיח ציבורי ער ותחושת פגיעה בביטחון הלאומית והאישי, בלי שנורתה יריה אחת, וללא שהשתמשו ביכולות סב"ר התקפיות מתקדמות. בעשור הקודם וביתר שאת בימים אלה המשטר באיראן אימץ ושכלל את השימוש בלוחמת סב"ר משולבת בעלת יעדים תפקודיים ותודעתיים ככלי אסטרטגי לאומי. בשנתיים האחרונות ניכרת עלייה בהיקף תקיפות הסב"ר האיראניות, בין שבוצעו באופן ישיר על ידה ובין מי מ"קבלני הביצוע" שלה, אשר זוהו על ידי גורמים שונים בקהילת הסב"ר. הגידול בתחכום ובהיקף הנזק של תקיפות אלה רק מחדד את סימן השאלה באשר לאלו, אשר טרם זוהו ושמבוצעות נכון לכתיבת שורות אלה ממש, ומצריך מאיתנו תפיסת הגנה מתאימה למתקפות משולבות אלו. מכיוון שפגיעת סב"ר במערכות הדיגיטליות היא שאלה של היכן ומתי, ולא של אם, אנחנו מציעים את תפיסת החוסן בסב"ר שתאפשר לנו להתמודד ולא לקרוס. בדיוק לשם כך נדרש מאיתנו לפתח את התפיסות ואת הכלים הנדרשים להתמודדות עם ממד לחימה מאתגר זה בעת הנוכחית.

מילון מונחים

מתקפת סייבר - פעולות המתבצעות באמצעות רשתות מחשב ומיועדות למנוע גישה אל מערכת מידע, אל רשת מידע או אל נתונים שנמצאים בהן, לפגוע בהן, ולשבש או להרוס אותן (Greenberg, 2019b; Singer, 2014).

חוסן סייבר (Cyber Resiliency) - היכולת לצפות, להתמודד, להתאים ולהתאושש מתנאים מקשים, מלחצים, מתקיפות או מפגיעה במערכות המשתמשות או מאופשרות באמצעות משאבי סייבר (Ross et al., 2019).

זיוף עמוק (Deep Fake) - טכנולוגיות אשר מאפשרות יצירת וידאו או אודיו סינתטיים הנראים כמציאותיים. המונח נולד מהלחם המילים זיוף (fake) ו'למידה עמוקה' (deep learning), שהיא טכניקה בלמידת מכונה (אורפז, 2020).

דיסאינפורמציה - הפצת מידע שגוי, שקרי או מסולף במטרה להשפיע על דעת הקהל ומקבלי ההחלטות (Bennett & Livingston, 2020; O'Connor & Weatherall, 2019; Rid, 2020).

מבצע או תודעה - יישום מתואם, משולב ומסונכרן של יכולות דיפלומטיות, אינפורמטיביות, צבאיות וכלכליות, כמו גם יכולות לאומיות אחרות, בעיתות שלום, בזמני משבר, במצבי עימות ובמצבים אחרי עימות. זאת במטרה להשפיע על התנהגויות או על החלטות של קהלי יעד זרים, כך שיאמצו עמדות ההולמות את האינטרסים של יוזמי המבצע (Larson et al., 2009).

מבצע מידע - נועד לאסוף, לחשוף ולהפיץ מידע אודות היריב על מנת להשיג יתרון תחרותי. תחת מבצעי מידע כלולים מבצעי לוחמה אלקטרונית, תקיפות סייבר, לוחמה פסיכולוגית, דיפלומטיה ציבורית ואמצעים נוספים שמטרתם להשפיע על קהל היעד (JOINT PUBLICATION 3-13, 2014).

יכולת הכחשה (Deniability) - אחד המאפיינים הייחודיים של מתקפות סייבר לסוגיהן הוא שכמעט בלתי אפשרי לזהות את מקור המתקפה ומי עמד מאחוריה. עבור הצד המתגונן הדבר מייצר בעיית ייחוס אשר עשויה להקשות על נקיטת פעולת־נגד. גם במקרים בהם המדינה מזוהה והתקיפה מיוחסת לה, יכולת הכחשה מאפשרת לה להכחיש את מעורבותה ולדחות את ההאשמות (Valeriano & Maness, 2014).

Advanced Persistent Threat (APT) - קבוצות תוקפים יציבות ומתקדמות, ככל הנראה מופעלות על ידי מדינות. קבוצות אלו מסומנות ומזוהות בצורה מספרית על מנת לעקוב אחריהן טוב יותר.

רשימת מקורות

- אורפז, ענבל (2020). "Deepfake: מקרה בוחן להשפעת פייק ניוז על הביטחון הלאומי". *INSS*.
- אלטשולר, ש. תהילה ולוריא, גיא (2016). "צנזורה וסודות ביטחוניים בעידן הדיגיטלי". מחקר מדיניות 113. **המכון הישראלי לדמוקרטיה**.
- אמיתי, זיו (12.4.20). "מתקפת הסב"ר על שירביט – מי עומד מאחוריה ולמה זה מדאיג". *TheMarker*.
- בר־גיל, אושרי (2020). בעולממד"ה 2# – הקורונה כאינפודמיה. מכון המחקר היישומי למדעי ההתנהגות בצה"ל [דו"ח פנימי].
- ברקוביץ', אורי וטרבלסי, נבו (2.5.2021) "חוקרים את המקרה": H&M ישראל מתמודדת עם תקיפת סב"ר איראנית". *Globes*.
- ברוקר, גיא (2011). "השעונים שתקתקו בעצלתיים: התנהלות הצבא במתח שבין לגיטימציה לבין מגבלות הפעלת הכוח". **בין הזירות** 10, עמ' 12–33.
- גולדשמידט, רועי ווורגן, יובל (2017). "הפצת מידע כוזב באינטרנט ותקיפות סב"ר לשם השפעה על בחירות". **הכנסת מרכז המחקר והמידע.** עמ' 1–15.
- הטוני, יוסי (8.11.2021) "פייסבוק מחקה חשבונות איראניים שקידמו את המחאה נגד נתניהו". **אנשים ומחשבים**.
- הלפרין, יניב (22.10.2021) "גיל שויד: 'העתיד של עולם הסב"ר – מפחיד'". **אנשים ומחשבים**.
- הלפרין, יניב (25.11.2021) שר המודיעין: "איראן מנסה להשפיע ברשת על דעת הקהל הישראלית". **אנשים ומחשבים**.
- חיימיניס, איתי (2019). "לוחמת המידע של איראן". בתוך יוסי קופרוסר ודוד סימן טוב (עורכים), **המערכה על התודעה: היבטים אסטרטגיים ומודיעיניים**. עמ' 269–279.
- טובי, שרית ורטנר, דוד. (2007). "מי מפחד מתנועות חברתיות? מגמות ואתגרים עבור צה"ל". **בין הזירות** 7 עמ' 74–86.
- כהן, שגיא (6.9.2018)." זה לא אתר ישראלי, זאת תעמולה איראנית". *Ynet*.
- פדן, כרמית ואלרן, מאיר (2018). "יישובים ב'עוטף עזה' – מקרה בוחן לחוסן החברתי בישראל". (2006–2016). *INSS*.
- קוגוסובסקי, מנדי (3.5.21). "הצבא האמריקני נלחם בדיפ־פייק". *Israel Defense*.
- קופרווסר, יוסי וסימן טוב, דוד (2019). "המערכה על התודעה: היבטים אסטרטגיים ומודיעיניים". **המכון למחקרי ביטחון לאומי**.
- רובינשטיין, רועי (31.1.2019). "דו"ח: צבא ה'בוטים' האיראני שמנסה להשפיע על הבחירות בישראל". *Ynet*.
- לאונרד, רוג'ר אשלי (1977). **על המלחמה – מדריך קצר לקלאוזביץ** (תרגם: עמנואל לוטם), מערכות ומשרד הביטחון – ההוצאה לאור, תל אביב.
- שחף, טל (8.5.2019). "יכולות הסב"ר של חמאס נפגעו אנושות". *Ynet*.
- שפריר, רועי וגלוברמן, דרור (7.4.21). "האיראנים מכים שוב: פייסבוק הסירה רשת שהתערבה בבחירות ותקפה את נתניהו". *Mako*.
- תפיסה תחומית מטכלית למבצעי תודעה. צה"ל/תוה"ד, פנימי.

- Bellingcat-Truth in a Post-Truth World. (2018, November 20).
- Bennett, W. L., and Livingston, S. (2020). *The disinformation age: Politics, technology, and disruptive communication in the United States*. Cambridge University Press.
- Bergstrom, C. T., and West, J. D. (2020). *Calling Bullshit: The Art of Skepticism in a Data-Driven World* (Illustrated edition). Random House.
- Bodine-Baron, E., Helmus, T. C., Radin, A.and Treyger, E. (2018). *Countering Russian Social Media Influence* (RR2740-RC). RAND.
- Bush, D. (30.07.2020). "Two Faces of Russian Information Operations: Coronavirus Coverage in Spanish". *Stanford Internet Observatory*.
- Chivvis, C. (2017). *Understanding Russian "Hybrid Warfare": And What Can Be Done About It*. RAND.
- Clarke, C. P. (19.09.2017). "How Hezbollah Came to Dominate Information Warfare". *The RAND Blog*.
- Greenberg, A. (2019). *Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers* (First edition). Doubleday.
- Greenberg, A. (23.08.2019). "The WIRED Guide to Cyberwar". *Wired*.
- Hochberg, L. (23.2.2021). "Iran's cyber future". *Middle East Institute.*
- Jenkins, B. M. (1974). *International Terrorism: A New Kind of Warfare* (No. P5261). RAND Corporation.
- US Army JOINT PUBLICATION 3-13. (2014). *Information Operations* (JP 3-13).
- Larson, E. V., Darilek, R. E., Gibran, D., Nichiporuk, B., Richardson, A., Schwartz, L. H., and Thurston, C. Q. (2009). "Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities" (MG-654-A). RAND.
- Libicki, M. C. (16.12.2015). "Iran: A Rising Cyber Power?". The RAND Blog.
- Marcellino, W., Helmus, T. C., Kerrigan, J., Reininger, H., Karimov, R. I., and Lawrence, R. A. (2021). "Detecting Conspiracy Theories on Social Media: Improving Machine Learning to Detect and Understand Online Conspiracy Theories". *Rand*.
- Newman, Li. H.(6.5.2019). "What Israel's Strike on Hamas Hackers Means For Cyberwar". *Wired*.
- Nichols, T. (2017). "The death of expertise: The campaign against established knowledge and why it matters". *Oxford University Press.*
- O'Connor, C. & Weatherall, J. O. (2019). "The misinformation age: How false beliefs spread". *Yale University Press*.
- Rid, T. (2020). *Active Measures: The Secret History of Disinformation and Political Warfare* (Illustrated edition). Farrar, Straus and Giroux.
- Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2019). "Developing cyber resilient systems: A systems security engineering approach". National Institute of Standards and Technology. SP 800160- vol. 2.
- Sabbagh, D., and Roth, A. (16.07.2020). "Russian state-sponsored hackers target Covid19-vaccine researchers". *The Guardian.*
- Schaefer, B. (12.3.2018)."The Cyber Party of God: How Hezbollah Could Transform Cyberterrorism". *Georgetown Security Studies Review.*

- Schia, N. N., and Gjesvik, L. (2020). "Hacking democracy: Managing influence campaigns and disinformation in the digital age". *Journal of Cyber Policy* 5, p. 1-16.
- Scott, M. (19.11.2020). "In race for coronavirus vaccine, Russia turns to disinformation". *POLITICO*.
- Singer, P. W. (2014). "Cybersecurity and cyberwar: What everyone needs to know". *Oxford University Press.*
- Singer, P. W., & Brooking, E. T. (2018). "*Likewar: The weaponization of social media*. Eamon Dolan/Houghton Mifflin Harcourt.
- Statt, N. (7.11.2017). "Facebook's unorthodox new revenge porn defense is to upload nudes to Facebook". *The Verge*.
- Stengel, R. (2019). "Information Wars: How We Lost the Global Battle Against Disinformation and What We Can Do About It". *Atlantic Monthly Press.*
- Summers, J. (25.10.2017). "Countering Disinformation: Russia's Infowar in Ukraine". The Henry M. Jackson School of International Studies.
- Thomas, Z. (13.2.2020). "Misinformation on coronavirus causing "infodemic"." *BBC News*.
- Valeriano, B., and Maness, R. C. (2014). "The dynamics of cyber conflict between rival antagonists, 2001-11". *Journal of Peace Research*, *51*(3), p. 347-360. https://doi.org/10.1177/0022343313518940.
- Virilio, P. (1991). *Lost Dimension*. Semiotext. (Original work published 1984).
- Virilio, P. and Redhead, S. (2004). "The Paul Virilio reader". *Columbia University Press.*
- Washington, I. C. Osseiran, N. and Donati J. (28.10.2019). "Islamic State Spokesman Killed in U.S. Airstrike". *Wall Street Journal.*
- World Health Organization. (25.08.2020). "Immunizing the public against misinformation".